



AVG Internet Security 2012

Kullanıcı Kılavuzu

Belge revizyonu 2012.01 (1.9.2011)

Telif Hakkı AVG Technologies CZ, s.r.o. Tüm hakları saklıdır.
Tüm diğer ticari markalar ilgili sahiplerine aittir.

Bu ürün, RSA Data Security, Inc. MD5 Message-Digest Algorithm özelliğini kullanmaktadır, Telif Hakkı (C) 1991-2, RSA Data Security, Inc. Oluşturma Tarihi: 1991.

Bu üründe, C-SaCzech kütüphanesi, Telif Hakkı (c) 1996-2001 Jaromir Dolecek (dolecek@ics.muni.cz) kodları kullanılmaktadır.

Bu ürün sıkıştırma kitaplığı zlib ürününü kullanmaktadır, Telif Hakkı (c) 1995-2002 Jean-loup Gailly ve Mark Adler.

Bu ürün sıkıştırma kitaplığı libzip2 kullanır, Telif Hakkı (c) 1996-2002 Julian R. Seward.



İçindekiler

1. Giriş	7
2. AVG Yükleme Gereksinimleri	8
2.1 Desteklenen İşletim Sistemleri	8
2.2 Minimum ve Önerilen Donanım Gereksinimleri	8
3. AVG Yükleme Süreci	9
3.1 Hoş geldiniz	9
3.2 Lisansınızı etkinleştirme	11
3.3 Yükleme türünü seçin	12
3.4 Özel seçenekler	13
3.5 AVG Security Toolbar'ı yükle	14
3.6 Yükleme ilerlemesi	15
3.7 Yükleme başarılı oldu	16
4. Yüklemeden Sonra	18
4.1 Ürün kaydı	18
4.2 Kullanıcı arayüzüne erişim	18
4.3 Tüm bilgisayarın taraması	18
4.4 Eicar testi	18
4.5 AVG varsayılan yapılandırması	19
5. AVG Kullanıcı Arayüzü	20
5.1 Sistem Menüsü	21
5.1.1 Dosya	21
5.1.2 Bileşenler	21
5.1.3 Geçmiş	21
5.1.4 Araçlar	21
5.1.5 Yardım	21
5.1.6 Destek	21
5.2 Güvenlik Durumu Bilgisi	29
5.3 Hızlı Bağlantılar	30
5.4 Bileşen Genel Görünümü	30
5.5 Sistem Tepsisi Simgesi	32
5.6 AVG gadget'ı	33
6. AVG Bileşenleri	36



6.1 Virüslerden Koruma	36
6.1.1 Tarama Motoru	36
6.1.2 Yerleşik Koruma	36
6.1.3 Casus Yazılımdan Koruma	36
6.1.4 Virüslerden Koruma Arayüzü	36
6.1.5 Resident Shield Tespitleri	36
6.2 LinkScanner	42
6.2.1 LinkScanner Arayüzü	42
6.2.2 Search-Shield tespitleri	42
6.2.3 Surf-Shield tespitleri	42
6.2.4 Online Shield tespitleri	42
6.3 E-posta Koruması	48
6.3.1 E-posta Tarayıcısı	48
6.3.2 Anti-Spam	48
6.3.3 E-posta Koruması Arayüzü	48
6.3.4 E-posta Koruması Tespitleri	48
6.4 Güvenlik Duvarı	52
6.4.1 Güvenlik Duvarı Prensipleri	52
6.4.2 Güvenlik Duvarı Profilleri	52
6.4.3 Güvenlik Duvarı Arayüzü	52
6.5 Anti-Rootkit	56
6.5.1 Anti-Rootkit Arayüzü	56
6.6 Sistem Araçları	57
6.6.1 İşlemler	57
6.6.2 Ağ Bağlantıları	57
6.6.3 Otomatik başlat	57
6.6.4 Tarayıcı Uzantıları	57
6.6.5 LSP Görüntüleyici	57
6.7 PC Analyzer	63
6.8 Identity Protection	64
6.8.1 Identity Protection Arayüzü	64
6.9 Uzaktan Yönetim	67
7. Uygulamalarım	68
7.1 LiveKıve	68
7.2 Family Safety	69
7.3 PC Tuneup	69
8. AVG Security Toolbar	71



9. AVG Gelişmiş Ayarlar	73
9.1 Görünüm	73
9.2 Sesler	76
9.3 AVG korumasını geçici olarak devre dışı bırak	77
9.4 Virüslerden Koruma	78
9.4.1 Yerleşik Kalkan	78
9.4.2 Önbellek Sunucusu	78
9.5 E-posta koruması	84
9.5.1 E-Posta Tarayıcısı	84
9.5.2 İstenmeyen E-postaya Karşı Koruma	84
9.6 LinkScanner	101
9.6.1 LinkScanner ayarları	101
9.6.2 Online Shield	101
9.7 Taramalar	105
9.7.1 Tüm bilgisayar taraması	105
9.7.2 Kabuk uzantısı tarama	105
9.7.3 Belirli dosyaların veya klasörlerin taranması	105
9.7.4 Çıkarılabilir aygıt tarama	105
9.8 Programlar	111
9.8.1 Programlı Tarama	111
9.8.2 Güncelleme Planı Tanımlamalar	111
9.8.3 Program Güncelleme Planı	111
9.8.4 Anti-Spam Güncelleme Zamanlaması	111
9.9 Güncelleme	122
9.9.1 Proxy	122
9.9.2 Çevirmeli	122
9.9.3 URL	122
9.9.4 Yönetme	122
9.10 Anti-Rootkit	129
9.10.1 İstisnalar	129
9.11 Identity Protection	130
9.11.1 Identity Protection Ayarları	130
9.11.2 İzin Verilenler Listesi	130
9.12 Potansiyel Olarak İstenmeyen Programlar	133
9.13 Virüs Kasası	136
9.14 Ürün Geliştirme Programı	136
9.15 Hata durumunu yoksay	139



9.16 Uzaktan Yönetim	140
10. Güvenlik Duvarı Ayarları	142
10.1 Genel	142
10.2 Güvenlik	143
10.3 Alanlar ve Bağdaştırıcıların Profilleri	144
10.4 IDS	145
10.5 Günlükler	147
10.6 Profiller	149
10.6.1 Profil Bilgileri	149
10.6.2 Tanımlanan Ağlar	149
10.6.3 Uygulamalar	149
10.6.4 Sistem Hizmetleri	149
11. AVG Tarama	160
11.1 Tarama Arayüzü	160
11.2 Öntanımlı Taramalar	161
11.2.1 Tüm Bilgisayarın Taranması	161
11.2.2 Belirli Dosyaları veya Klasörleri Tara	161
11.2.3 Anti-Rootkit Tarama	161
11.3 Windows Gezgini'nde Tarama	171
11.4 Komut Satırı Tarama	172
11.4.1 CMD Tarama Parametreleri	172
11.5 Tarama Programlama	174
11.5.1 Program Ayarları	174
11.5.2 Tarama Şekli	174
11.5.3 Taranacaklar	174
11.6 Tarama Sonuçları Genel Görünümü	184
11.7 Tarama Sonuçları Ayrıntıları	185
11.7.1 Sonuçlara Genel Bakış Sekmesi	185
11.7.2 Bulaşma Sekmesi	185
11.7.3 Casus Yazılım Sekmesi	185
11.7.4 Uyarılar Sekmesi	185
11.7.5 Rootkit'ler Sekmesi	185
11.7.6 Bilgi Sekmesi	185
11.8 Virüs Kasası	192
12. AVG Güncellemeleri	195
12.1 Güncelleme başlatma	195



12.2 Güncelleme ilerlemesi	195
12.3 Güncelleme Seviyeleri	196
13. Olay Geçmişi	197
14. SSS ve Teknik Destek	199



1. Giriş

Bu kullanıcı el kitabı, **AVG Internet Security 2012** için kapsamlı dokümantasyon sağlar.

AVG Internet Security 2012 çevrimiçi yaptığınız her şey için koruma katmanları sağlar. Bu, kimlik hırsızlıklarından, virüslerden ya da zararlı siteleri ziyaret etmekten endişe duymanıza gerek olmadığı anlamına gelir. AVG Koruyucu Bulut Teknolojisi ve AVG Topluluk Koruma Ağı da dahil edilmiştir; bu, en son tehdit bilgilerini topladığımız ve en iyi korumayı aldığınızdan emin olmak için topluluğumuzla paylaştığımız anlamına gelmektedir:

- AVG Firewall, Anti-Spam ve Identity Protection ile güvenle alışveriş yapın ve bankacılık işlemlerinizi gerçekleştirin
- AVG Social Networking Protection ile sosyal ağlarda güvenli kalın
- LinkScanner'ın gerçek zamanlı koruması ile güven içinde gezinin ve arama yapın



2. AVG Yükleme Gereksinimleri

2.1. Desteklenen İşletim Sistemleri

AVG Internet Security 2012 aşağıdaki işletim sistemlerine sahip iş istasyonlarını koruma amaçlıdır:

- Windows XP Home Edition SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Vista (x86 ve x64, tüm sürümleri)
- Windows 7 (x86 ve x64, tüm sürümler)

(ve belirli işletim sistemleri için daha yeni hizmet paketleri)

Not: [Kimlik Koruma](#) bileşeni Windows XP x64'te desteklenmez. Bu işletim sisteminde, AVG Internet Security 2012 yazılımını yalnızca Kimlik Koruma (IDP) bileşeni olmak sizin yükleyebilirsiniz.

2.2. Minimum ve Önerilen Donanım Gereksinimleri

AVG Internet Security 2012 için minimum donanım gereksinimleri:

- Intel Pentium CPU 1,5 GHz
- 512 MB RAM bellek
- 1000 MB boş sabit disk alanı (yükleme için)

AVG Internet Security 2012 için önerilen donanım gereksinimleri:

- Intel Pentium CPU 1,8 GHz
- 512 MB RAM bellek
- 1550 MB boş sabit disk alanı (yükleme için)



3. AVG Yükleme Süreci

Yükleme dosyasını nerede bulabilirim?

Bilgisayarınıza **AVG Internet Security 2012** programını yüklemek için, en güncel yükleme dosyasını edinmeniz gerekir. **AVG Internet Security 2012** uygulamasının doğru sürümünü yüklediğinizden emin olabilmek için yükleme dosyasını AVG web sitesinden (<http://www.avg.com/>) indirmeniz önerilir. **Destek Merkezi / İndirme** bölümü her AVG sürümü için yükleme dosyalarına ayrıntılı bir genel bakış sunar.

Hangi dosyaları indirip yüklemeniz gerektiğinden emin değilseniz, web sayfasının altındaki **Ürün seç** hizmetini kullanmak isteyebilirsiniz. Hizmet, üç basit soruya verilen yanıtların ardından tam olarak ihtiyacınız olan dosyaları tanımlar. Kişisel ihtiyaçlarınız için özelleştirilmiş, indirilebilir dosyaların tam listesine yönlendirilmek için **Devam** düğmesine basın.

Yükleme nasıl bir süreçtir?

Yükleme dosyasını sabit diskinize indirme ve kaydetme işlemi tamamlandıktan sonra yükleme işlemi başlatabilirsiniz. Yükleme, bir dizi kolay ve anlaşılır iletişim kutusundan oluşur. Her iletişim kutusunda yükleme sürecinin her adımında ne yapılması gerektiği kısaca açıklanır. Devamında, her iletişim penceresi için ayrıntılı bir açıklama sunulur:

3.1. Hoş geldiniz

Yükleme süreci **AVG Yükleyiciye hoş geldiniz** iletişim kutusu ile başlar:

Yükleme dilini seçin



Bu iletişim kutusunda yükleme süreci için kullanılan dili seçebilirsiniz. Dil menüsü açmak için iletişim kutusunun sağ köşesindeki açılır kutuyu tıklatın. İstedığınız dili seçtiğinizde yükleme süreci bu dille devam eder.

Dikkat: Şu anda yalnızca yükleme süreci dilini seçmektesiniz. AVG Internet Security 2012 uygulaması seçilen dilde yüklenir ve İngilizce her zaman otomatik olarak yüklenir. Ancak, daha fazla dil yüklemek ve AVG Internet Security 2012 uygulamasında bu dillerden biriyle çalışmak mümkündür. [Özel Seçenekler](#) adlı kurulum iletişim kutularından birinde alternatif dil seçimlerinizi onaylamanız istenir.

Lisans Sözleşmesi

Ayrıca, **AVG Yükleyci hoş geldiniz** iletişim kutusu AVG lisans sözleşmesinin tam metnini içerir. Lütfen bunu dikkatlice okuyun. Okuduğunuzu, anladığınızı ve sözleşmeyi kabul ettiğinizi onaylamak için, **Kabul Et** düğmesine basın. Lisans sözleşmesini kabul etmiyorsanız **Kabul Etmiyorum** düğmesine basın, böylece yükleme süreci anında iptal edilecektir.

AVG Gizlilik Politikası

Bu kurulum iletişim kutusu, lisans sözleşmesinin yanı sıra AVG gizlilik politikası hakkında da daha fazla bilgi seçeneği sunar. İletişim kutusunun sol alt köşesinde **AVG Gizlilik Politikası** bağlantısını görebilirsiniz. AVG Technologies gizlilik politikası ilkelerinin tam metnini bulabileceğiniz AVG web sitesine (<http://www.avg.com/>) yönlendirilmek için bu bağlantıyı tıklatın.

Kontrol düğmeleri

İlk kurulum iletişim kutusunda yalnızca iki kontrol düğmesi mevcuttur:

- **Kabul Et** - Lisans sözleşmesini okuduğunuzu, anladığınızı ve kabul ettiğinizi onaylamak için tıklatın. Yükleme devam eder ve bir sonraki kurulum iletişim kutusuna geçersiniz.
- **Reddet** - Lisans sözleşmesini reddetmek için tıklatın. Kurulum süreci derhal sonlandırılır. **AVG Internet Security 2012** yüklenmez!



3.2. Lisansınızı etkinleştirme

Lisansınızı Etkinleştirin iletişim kutusunda, lisans numaranızı verilen metin alanına yazmanız istenir:

AVG Yazılım Yükleyici

AVG Lisansınızı Etkinleştirin

Lisans Numarası:

Örnek: IQNP6-9BCA8-PUQU2-A5HCK-GP338L-93OCB

AVG 2012 yazılımınızı çevrimiçi satın aldıysanız, lisans numaranız e-posta ile gönderilmiştir. Yanlış yazmayı önlemek için numarayı e-postanızdan kopyalayarak bu ekrana yapıştırmanızı öneririz.

Yazılı bir mağazadan satın aldıysanız, lisans numarasını paketin içindeki ürün kayıt kartı üzerinde bulabilirsiniz. Numarayı doğru biçimde kopyaladığınızdan emin olun.

≤ Geri İleri ≥ İptal

Lisans numarası nereden bulunabilir

Satış numarası, **AVG Internet Security 2012** kutusundaki CD paketinde bulunabilir. Lisans numarası **AVG Internet Security 2012** programını çevrimiçi satın aldıktan sonra alacağınız onay e-postasında olacaktır. Sayıları gösterdiği gibi gitmelisiniz. Lisans numarasının dijital formu mevcut ise (*e-postada*) girmek için kopyala ve yapıştır yönteminin kullanılması önerilmektedir.

Kopyala ve Yapıştır yöntemi nasıl kullanılır

Kopyala ve Yapıştır yöntemini kullanarak **AVG Internet Security 2012** lisans numarasını programa girmek, numaranın doğru biçimde girilmesini garanti altına alır. Lütfen şu adımları takip edin:

- Lisans numaranızın bulunduğu e-postayı açın.
- Lisans numarasının başında sol fare düğmesine tıklatın, düğmeyi tutup numaranın sonuna kadar sürükleyin ve düğmeyi bırakın. Numaranın vurgulanması gerekir.
- **Ctrl** tuşunu basılı tutun ve **C** tuşuna basın. Bu işlem numarayı kopyalar.
- Kopyalanan numarayı yapıştırmak istediğiniz konumu tıklatın.
- **Ctrl** tuşunu basılı tutun ve **V** tuşuna basın. Bu işlem numarayı seçilen konuma yapıştırır.

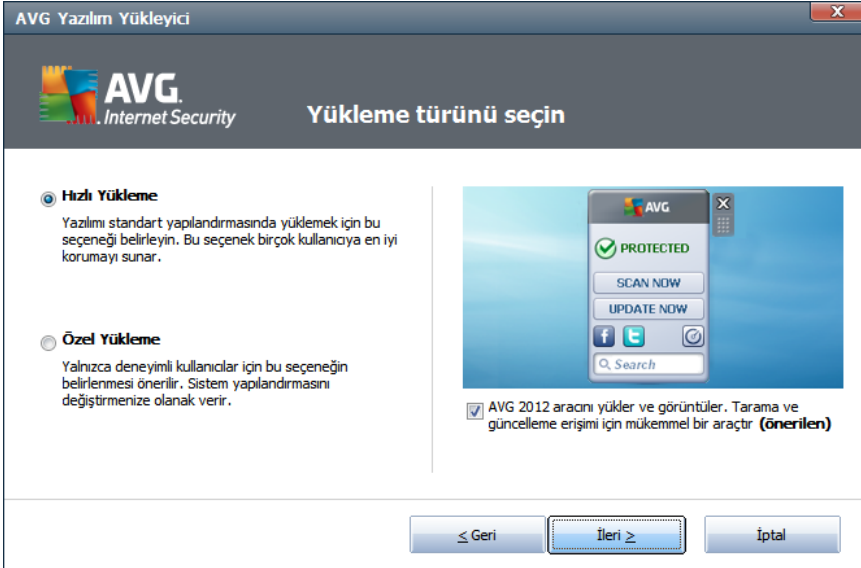


Kontrol düğmeleri

Çoğu kurulum iletişim kutusunda olduğu gibi üç kontrol düğmesi mevcuttur:

- **Geri** - Önceki kurulum iletişim kutusuna, bir adım geriye gitmek için tıklatın.
- **İleri** - Kurulumla devam etmek ve bir adım ilerlemek için tıklatın.
- **İptal** - Kurulum işleminden hemen çıkmak için tıklatın; **AVG Internet Security 2012** kurulmaz!

3.3. Yükleme türünü seçin



Yükleme türleri

Yükleme türünü seçin iletişim kutusu iki yükleme seçeneği sunar: **Hızlı Yükleme** ve **Özel Yükleme**.

Kullanıcıların çoğu için **AVG Internet Security 2012** uygulamasını program geliştiricisi tarafından önceden tanımlanmış ayarlarla tam otomatik moda yükleyen hızlı kurulum seçeneği önerilmektedir. Bu yapılandırma, minimum kaynak kullanımı ile maksimum güvenliği bir araya getirir. Gelecekte söz konusu yapılandırmayı değiştirme ihtiyacı duyarsanız söz konusu işlemi doğrudan **AVG Internet Security 2012** uygulamasından yapabileceksiniz. **Hızlı Yükleme** seçeneğini belirlerseniz, aşağıdaki [AVG Security Toolbar'ı Yükle](#) iletişim kutusuna geçmek için **İleri** düğmesine basın.

Özel yükleme **AVG Internet Security 2012** uygulamasını standart olmayan ayarlarla kurmak için geçerli bir nedeni olan deneyimli kullanıcılar tarafından kullanılmalıdır. Örn. belirli sistem gereksinimlerini karşılamak için. Bu seçeneği belirledikten sonra, [Özel Seçenekler](#) iletişim kutusuna gitmek için **İleri** düğmesine basın.



AVG gadget'ı yüklemesi

İletişim kutusunun sağ bölümünde, [AVG gadget'](#) ile ilgili onay kutusunu bulabilirsiniz (*Windows Vista/Windows 7'de desteklenir*). Bu gadget'ı yüklemek istiyorsanız, ilgili onay kutusunu işaretleyin. [AVG gadget'ına](#), bunun ardından **AVG Internet Security 2012** yazılımınızın en önemli özelliklerine (yani, [taramaya](#) ve [güncellemeye](#)) hemen erişmenize olanak veren Windows kenar çubuğundan ulaşabilirsiniz.

Kontrol düğmeleri

Çoğu kurulum iletişim kutusunda olduğu gibi üç kontrol düğmesi mevcuttur:

- **Geri** - Önceki kurulum iletişim kutusuna, bir adım geriye gitmek için tıklatın.
- **İleri** - Kurulumla devam etmek ve bir adım ilerlemek için tıklatın.
- **İptal** - Kurulum işleminden hemen çıkmak için tıklatın; **AVG Internet Security 2012** kurulmaz!

3.4. Özel seçenekler

Özel Seçenekler iletişim kutusu yükleme parametrelerinin iki parametresini ayarlamanıza olanak verir:



Hedef Klasör

İletişim kutusunun **Hedef Klasör** bölümünde, **AVG Internet Security 2012** yazılımının yüklenmesi gereken konumu belirtmeniz beklenir. Varsayılan olarak, **AVG Internet Security 2012**, C: sürücüsündeki program dosyaları klasörüne kurulur. Bu konumu değiştirmek istiyorsanız, sürücü



yapısını görüntülemek ve ilgili klasörü seçmek için **Gözet** düğmesini kullanın.

Bileşen Seçimi

Bileşen Seçimi bölümünde, yüklenebilecek tüm **AVG Internet Security 2012** bileşenleriyle ilgili genel bir görünüm bulunur. Varsayılan ayarların size uygun olmaması halinde belirli bileşenleri kaldırabilir ya da ekleyebilirsiniz.

Ancak, yalnızca satın aldığınız AVG sürümü dahilinde bulunan bileşenler arasından seçim yapabilirsiniz!

Bileşen Seçimi listesindeki tüm öğeleri vurgulayın, böylece ilgili bileşenin kısa açıklaması bu bölümün sağ tarafından görüntülenir. Her bileşenin işlevleri ile ilgili ayrıntılı bilgiler için, bu belgedeki [Bileşen Genel Görünümü](#) bölümüne bakın. Yazılım satıcısı tarafından önceden ayarlanmış varsayılan yapılandırmayı geri getirmek için, **Varsayılan** düğmesini kullanın.

Kontrol düğmeleri

Çoğu kurulum iletişim kutusunda olduğu gibi üç kontrol düğmesi mevcuttur:

- **Geri** - Önceki kurulum iletişim kutusuna, bir adım geriye gitmek için tıklattın.
- **İleri** - Kurulumla devam etmek ve bir adım ilerlemek için tıklattın.
- **İptal** - Kurulum işleminden hemen çıkmak için tıklattın; **AVG Internet Security 2012** kurulmaz!

3.5. AVG Security Toolbar'ı yükle





AVG Security Toolbar'ı yükleyin iletişim kutusunda, [AVG Security Toolbar](#) uygulamasını yüklemek isteyip istemediğinize karar verebilirsiniz. Varsayılan ayarları değiştirmeyerseniz, İnternet'te gezinirken size daha kapsamlı koruma sağlamak için bu bileşen otomatik olarak İnternet tarayıcınıza yüklenir (*şu anda desteklenen tarayıcılar Microsoft İnternet Explorer v. 6.0 ve üstü ve Mozilla Firefox v. 3.0 ya da üstüdür*).

Ayrıca *AVG Secure Search (powered by Google)* arama motorunu varsayılan arama sağlayıcınız olarak atamaya karar verme seçeneğiniz de bulunmaktadır. Öyle istiyorsanız, ilgili onay kutusunu işaretli bırakın.

3.6. Yükleme ilerlemesi

Yükleme ilerlemesi iletişim kutusu yükleme sürecinin ilerleme durumu gösterir ve herhangi bir müdahale gerektirmez:



Yükleme işlemi bittiğinde, otomatik olarak bir sonraki iletişim kutusuna yönlendirilirsiniz.

Kontrol düğmeleri

Bu iletişim kutusunda yalnızca bir kontrol düğmesi mevcuttur - **İptal**. Yalnızca devam eden yükleme sürecini durdurmak istiyorsanız bu düğmeyi kullanmalısınız. Böyle bir durumda **AVG İnternet Security 2012** uygulamasının yüklenmeyeceğini lütfen unutmayın!



3.7. Yükleme başarılı oldu

Yükleme başarılı oldu iletişim kutusu, **AVG Internet Security 2012** yazılımınızın tam olarak yüklendiğini ve yapılandırıldığını onaylar:



Ürün Geliştirme Programı

Bu iletişim kutusunda, genel internet güvenliği seviyesini yükseltmek için anonim olarak bilgi toplayan Ürün Geliştirme Programı'na katılıp katılmayı seçebilirsiniz (*ayrıntılar için [AVG Gelişmiş Ayarları / Ürün Geliştirme Programı](#) bölümüne bakabilirsiniz*). Bu bildirim kabul ediyorsanız **AVG 2012 web güvenliği ve Ürün Geliştirme Programı'na katılmayı kabul ediyorum ...** seçeneğini işaretleyin (*seçenek varsayılan olarak onaylıdır*).

Bilgisayar yeniden başlatma

Yükleme sürecini tamamlamak için, bilgisayarınızı yeniden başlatmanız gerekir: hemen başlatmak için **Şimdi Başlat** veya bu işlemi ertelemek için **Daha Sonra Başlat** seçin.

İşletme lisansı yükleme

Herhangi bir AVG işletme lisansı kullanıyorsanız ve Uzaktan yönetim ögesinin yükleneceğini önceden seçtiyseniz (*bkz. [Özel Seçenekler](#)*), Yükleme başarılı oldu iletişim kutusu şu arayüzle görüntülenecektir:



AVG Yazılım Yükleyici

 **Yükleme başarılı oldu**

AVG 2012 ürününü yüklediğiniz için teşekkür ederiz.

AVG Veri Merkezi belirtimi:

[Gizlilik Politikası](#) bağlantısındaki ilkelere göre (AVG sizi kişisel olarak tanımlayabilecek bilgileri saklamayacak ve sizinle hiçbir şekilde iletişime geçmeyecektir) [ürün geliştirme programı](#) bölümüne katılarak güvenliğimi artırmak istiyorum

Kurulum işlemini tamamlamak için bilgisayarınızı yeniden başlatmanız gerekiyor.

[Şimdi Yeniden Başlat \(önerilen\)](#) [Daha Sonra Yeniden Başlat](#)

AVG DataCenter parametrelerini belirtmeniz gerekiyor - lütfen bağlantı dizisini sunucu:bağlantı noktası biçiminde AVG DataCenter uygulamasına sağlayın. Bu bilgi o anda yoksa, alanı boş bırakın, böylece yapılandırmayı [Gelişmiş Ayarlar / Uzaktan Yönetim](#) iletişim kutusu içinde daha sonra da ayarlayabilirsiniz. AVG Uzaktan yönetim hakkında ayrıntılı bilgi edinmek için lütfen AVG Business Edition kullanıcı kılavuzuna başvurun; bu kılavuz, AVG web sitesinden (<http://www.avg.com/>) indirilebilir.

Bu belgenin [Bileşen Genel Görünümü](#) bölümüne bakın. Yazılım satıcısı tarafından önceden ayarlanmış varsayılan yapılandırmayı geri getirmek için, **Varsayılan** düğmesini kullanın.

Kontrol düğmeleri

İletişim kutusunda şu kontrol düğmeleri mevcuttur:

- **Şimdi Yeniden Başlat (önerilir)** - Yeniden başlatma, **AVG Internet Security 2012** yükleme sürecini tamamlamak için zorunludur. Bilgisayarınız hemen yeniden başlatmanız önerilir. Ancak yeniden başlatmanın ardından **AVG Internet Security 2012** tam olarak yüklenir ve siz de güvenli ve korumalı duruma geçersiniz.
- **Daha Sonra Yeniden Başlat** - Herhangi bir nedenle bilgisayarınızı şu anda yeniden başlatamıyorsanız, bu işlemi daha sonraya erteleyebilirsiniz. Ancak, hemen yeniden başlatmanız önerilir. Ancak yeniden başlatmanın ardından, **AVG Internet Security 2012** bilgisayarınızı tam olarak koruyabilir!



4. Yüklemeden Sonra

4.1. Ürün kaydı

AVG Internet Security 2012 kurulumunu tamamladıktan sonra, lütfen ürününüzü çevrimiçi olarak AVG web sitesinde (<http://www.avg.com/>) kaydettirin. Kayıt işleminin ardından AVG Kullanıcı hesabınıza erişebileceğiniz, AVG Güncelleme bültenini alacak ve sadece kayıtlı kullanıcılara sunulan diğer hizmetlerden yararlanacaksınız.

Ürünü kaydettirmenin en kolay yolu doğrudan **AVG Internet Security 2012** kullanıcı arayüzünü kullanmaktır. Ana menüde [Yardım/Şimdi kaydolun](#) öğesini seçin. AVG web sitesindeki (<http://www.avg.com/>) **Kayıt** sayfasına yönlendirilirsiniz. Lütfen sayfadaki talimatları izleyin.

4.2. Kullanıcı arayüzüne erişim

[AVG ana iletişim kutusuna](#) çeşitli yöntemlerle ulaşabilirsiniz:

- [AVG sistem tepsisi sembolü](#)
- Masaüstünüzdeki AVG simgesini çift tıklayın
- [AVG gadget](#)'ının alt bölümünde bulunan durum satırını çift tıklayın ([yükleyin](#); Windows Vista/Windows 7 işletim sistemlerinde desteklenir)
- **Başlat/Programlar/AVG 2012/AVG Kullanıcı Arayüzü**

4.3. Tüm bilgisayarın taraması

AVG Internet Security 2012 yüklemesinden önce bilgisayarınıza virüs bulaşmış olması ihtimali bulunmaktadır. Bu nedenle bilgisayarınızda virüs bulunmadığından emin olmak için [Tam bilgisayar taraması](#) yapmanız gerekmektedir.

[Tam bilgisayar taraması](#) konusunda talimatlar için lütfen [AVG Taraması](#) bölümünü inceleyin.

4.4. Eicar testi

AVG Internet Security 2012 programının düzgün olarak yüklendiğini onaylamak için EICAR testini çalıştırabilirsiniz.

EICAR testi, virüsten koruma sistemin çalıştığından emin olmak üzere kullanılan standart ve kesinlikle güvenli bir yöntemdir. Gerçek bir virüs olmadığı için yayılmasında sakınca yoktur ve herhangi bir virüs kodu içermemektedir. Ürünlerin çoğu sanki bir virüsmüş gibi tepki verir (*ancak "EICAR-AV-Test" adı altında rapor ederler*). EICAR virüsünü www.eicar.com adresinde bulunan EICA'nın web sitesinden indirebilir ve bunun yanı sıra EICAR testi hakkında tüm gerekli bilgileri edinebilirsiniz.

eicar.com dosyasını indirmeye çalışın ve sabit diskinize kaydedin. Siz test dosyasını indirmeyi onaylar onaylamaz [Online Shield](#) (*Link Scanner bileşenin parçasıdır*) bu durum için bir uyarı verir. Bu



bildirim, AVG'nin bilgisayarınıza doğru bir şekilde yüklenmiş olduğunu gösterir.



<http://www.eicar.com> web sitesinden EICAR 'virüs' sıkıştırılmış sürümünü (örn. *ecar_com.zip* biçiminde) de indirebilirsiniz. [Online Shield](#) bu dosyayı indirmenizi ve yerel diskinize kaydetmenizi sağlar, ancak [Resident Shield \(Virüslerden Koruma bileşeni içinde\)](#) paketi açmaya çalıştığınızda 'virüsü' algılar.

AVG'nin EICAR test dosyasını virüs olarak algılamaması halinde program yapılandırmasını yeniden kontrol etmeniz gerekir!

4.5. AVG varsayılan yapılandırması

AVG Internet Security 2012 varsayılan yapılandırması (yani, uygulamanın yüklemeye başlamadan önce doğru şekilde nasıl ayarlanacağı) yazılım satıcısı tarafından ayarlanabilir, böylece optimum performans elde etmek için tüm bileşenler ve işlemler ayarlanabilir.

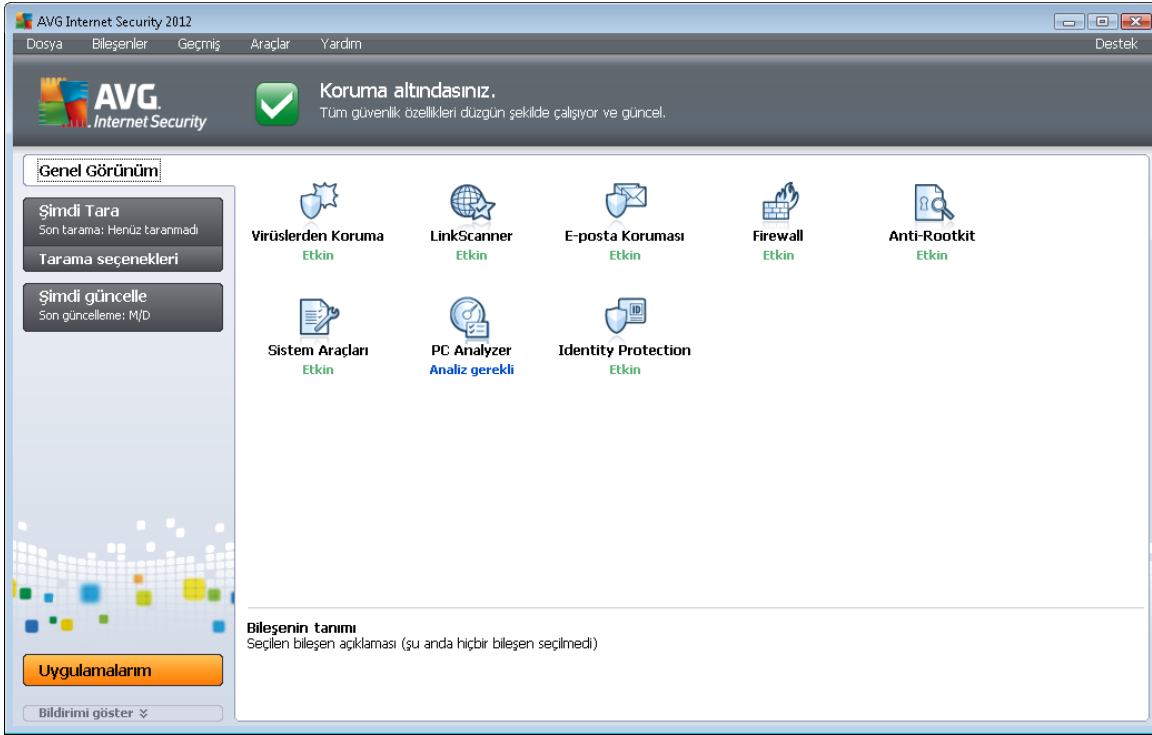
Bunun için iyi bir nedeniniz olmadıkça AVG yapılandırmasını değiştirmeyin! Ayarlarda yapılacak her tür değişiklik sadece deneyimli bir kullanıcı tarafından gerçekleştirilmelidir.

[AVG bileşenlerinde](#) yapılan bazı ufak değişikliklere ilgili bileşenin kullanıcı arayüzünden ulaşabilirsiniz. İhtiyaçlarınızı daha iyi karşılaması açısından AVG yapılandırmasını değiştirme ihtiyacı hissederseniz [AVG Gelişmiş Ayarlar](#)'na gidin: sistem menüsü öğesini seçin **Araçlar/Gelişmiş ayarlar** ve AVG yapılandırmasını yeni açılan [AVG Gelişmiş Ayarlar](#) penceresinde düzenleyin.



5. AVG Kullanıcı Arayüzü

AVG Internet Security 2012 ana pencerede açılır:



Ana pencere çok sayıda bölüme ayrılır:

- **Sistem Menüsü** (penceredeki en üst sistem çubuğu), tüm **AVG Internet Security 2012** bileşenlerine, servislerine ve özelliklerine ulaşmanızı sağlayan standart dolaşım yöntemidir - [ayrıntılar >>](#)
- **Güvenlik Durumu Bilgileri** (pencerenin üst bölümü) **AVG Internet Security 2012** programınızın mevcut durumu hakkında bilgi sunar - [ayrıntılar >>](#)
- **Hızlı Bağlantılar** (pencerenin sol bölümü) en önemli ve en sık kullanılan **AVG Internet Security 2012** görevlerine hızlı bir şekilde erişebilmenizi sağlar - [ayrıntılar >>](#)
- **Uygulamalarım** (pencerenin sol alt bölümü) **AVG Internet Security 2012** için mevcut ek uygulamalara bir genel bakış penceresi açar: [LiveKive](#), [Family Safety](#) ve [PC Tuneup](#)
- **Bileşenlere Genel Bakış** (pencerenin orta kısmı) yüklü tüm **AVG Internet Security 2012** bileşenleri hakkında genel bilgi verir - [ayrıntılar >>](#)
- **Sistem Tepsisi Simgesi** (ekranın sağ alt köşesi, sistem tepsisi üzerinde) mevcut **AVG Internet Security 2012** durumunu gösterir - [ayrıntılar >>](#)
- **AVG gadget'ı** (Windows kenar çubuğu, Windows Vista/7'de desteklenir) **AVG Internet Security 2012** taramasına ve güncellemesine hızlı biçimde erişmenizi sağlar - [ayrıntılar >>](#)



5.1. Sistem Menüsü

Sistem menüsü tüm Windows uygulamalarında kullanılan standart bir dolaşım yöntemidir. **AVG Internet Security 2012** ana penceresinin en üstünde yatay olarak konumlandırılmıştır. Belirli AVG bileşenlerine, özelliklerine ve hizmetlerine ulaşmak için sistem menüsünü kullanın.

Sistem menüsü beş ana bölüme ayrılmıştır:

5.1.1. Dosya

- **Çıkış** - **AVG Internet Security 2012**'nin kullanıcı arayüzünü kapatır. Ancak AVG uygulaması arkaplanda çalışmaya devam edecek ve bilgisayarınız korunmaya devam edecektir.

5.1.2. Bileşenler

Sistem menüsünün [Bileşenler](#) ögesi, yüklenen tüm AVG bileşenlerine ilişkin bağlantılar içerir ve kullanıcı arayüzünde bunların varsayılan iletişim kutusu sayfalarını açar:

- **Sisteme genel bakış** - [yükli tüm bileşenlerle ve durumlarıyla birlikte varsayılan kullanıcı arayüzü iletişim kutusuna geçer](#)
- **Virüslerden Koruma** sisteminizdeki virüs, casus yazılım, solucan, truva atı ve istenmeyen yürütülebilir dosyaları veya kitaplıkları tespit eder ve sizi kötü amaçlı reklam yazılımlarından korur - [ayrıntılar >>](#)
- **LinkScanner** internette arama ve gezinme sırasında sizi web tabanlı saldırılara karşı korur - [ayrıntılar >>](#)
- **E-posta Koruması** gelen e-posta mesajlarınızı istenmeyen e-postalara karşı denetler ve virüsleri, kimlik avı saldırılarını veya diğer tehditleri engeller - [ayrıntılar >>](#)
- **Firewall** her ağ bağlantı noktasındaki tüm iletişimleri denetleyerek sizi kötü amaçlı saldırılardan korur ve tüm sızma girişimlerini engeller - [ayrıntılar >>](#)
- **Anti-Rootkit** uygulamalar, sürücüler ve kitaplıklarda gizlenmiş tehlikeli kök dizinler için tarama yapar - [ayrıntılar >>](#)
- **Sistem Araçları**, AVG ortamı ve işletim sistemi bilgileri hakkında ayrıntılı bir özet sunar - [ayrıntılar >>](#)
- **PC Analyzer** analizörü, bilgisayarınızın durumu hakkında bilgi verir - [ayrıntılar >>](#)
- **Identity Protection** dijital varlıklarınızı yeni ve bilinmeyen tehditlere karşı korumak üzere sürekli tetiktedir - [ayrıntılar >>](#)
- **Güvenlik Araç Çubuğu** seçili AVG işlevini doğrudan İnternet tarayıcınızdan kullanmanıza olanak sağlar - [ayrıntılar >>](#)
- **Uzaktan Yönetim** yalnızca [yükleme süreci](#) esnasında bu bileşenin yüklenmesini istediğinizi belirtmeniz halinde AVG Business Sürümlerinde görüntülenir



5.1.3. Geçmiş

- [Tarama sonuçları](#) - AVG test arayüzüne ve özellikle [Tarama Sonuçlarına Genel Bakış](#) penceresine gider
- [Resident Shield tespiti](#) - [Resident Shield](#)
- [E-mail Scanner tespiti](#) - [E-posta Koruması](#) bileşeni tarafından tehlikeli olduğu tespit edilen posta eklentileri hakkında genel bilgi veren bir pencere açar
- [Online Shield bulguları](#) - [LinkScanner](#) bileşeni içindeki [Online Shield](#) tarafından tespit edilen tehlikeler hakkında genel bilgi veren bir iletişim kutusu açar
- [Virüs Kasası](#) - Belirli bir neden doğrultusunda AVG'nin tespit edilmiş temizlenemeyen tüm bulaşmaları sildiği karantina alanının arayüzünü açar ([Virüs Kasası](#)) Karantina altında bulunan bulaşmış dosyalar, yalıtılmıştır, bilgisayarınızın güvenliği garanti altındadır ve aynı anda bulaşmış dosyalar ileride tamir edilebilecekleri göz önünde bulundurulur olarak depolanır
- [Etkinlik geçmişi kayıt defteri](#) - kaydedilen tüm **AVG Internet Security 2012** eylemler hakkında genel bilgi veren bir geçmiş kayıt defteri arayüzü açar
- [Güvenlik Duvarı](#) - [Kayıt Defterleri](#) sekmesinde Güvenlik Duvarı ayarları arayüzünü açar ve Güvenlik Duvarı etkinlikleri hakkında ayrıntılı bilgi verir.

5.1.4. Araçlar

- [Bilgisayarı tara](#) - [AVG tarama arayüzüne](#) geçer ve tüm bilgisayar taramasını başlatır.
- [Seçilen klasörü tara...](#) - [AVG tarama arayüzüne](#) geçer ve bilgisayarınızın dolaşım ağacından taranmasını istediğiniz dosya ve klasörleri seçmenizi sağlar.
- [Dosyayı tara...](#) - sabit diskinizin dolaşım ağacından seçtiğiniz tek bir dosyayı isteğe bağlı olarak tarayabilmenizi sağlar.
- [Güncelle](#) - otomatik olarak güncellemesi **AVG Internet Security 2012** işlemini başlatır.
- [Dizinden güncelle...](#) - sabit diskinizde bulunan belirli bir dosyanın içinde yer alan güncelleme dosyalarını alarak güncelleme işlemini gerçekleştirir. Diğer bir yandan bu seçim sadece acil durumlarda önerilmektedir. Örn. Internet bağlantısı olmadığı durumlarda (*Örneğin bilgisayarınıza virüs bulaşmış ise ve Internet bağlantınız kesildiyse; bilgisayarınız bir ağa bağlıysa fakat Internet erişimi yok ise vb.*). Yeni açılan pencereden, daha önce güncelleme dosyasını depoladığınız klasörü seçin ve güncelleme işlemini başlatın.
- [Gelişmiş ayarlar...](#) - AVG Internet Security 2012 yapılandırmasını düzenleyebileceğiniz [AVG gelişmiş ayarlar](#) iletişim kutusunu açar. Genel olarak uygulamanın yazılım üreticisi tarafından tanımlanan varsayılan ayarlarının muhafaza edilmesi önerilir.
- [Güvenlik Duvarı ayarları...](#) - [Güvenlik Duvarı](#) bileşeninin gelişmiş yapılandırmasına ilişkin bağımsız bir pencere açar.



5.1.5. Yardım

- **İçindekiler** - AVG yardım dosyalarını açar
- **Çevrimiçi Yardım Alın** - Müşteri destek merkezi sayfasında AVG web sitesini (<http://www.avg.com/>) açar
- **AVG Web Sayfanız** - AVG web sitesini (<http://www.avg.com/>) açar
- **Virüsler ve Tehditler Hakkında** - tanımlanan virüs hakkında ayrıntılı bilgi edinebildiğiniz çevrimiçi [Virüs Ansiklopedisini](#) açar
- **Yeniden Etkinleştir - Yükleme işleminin AVG'yi Kişiselleştir** iletişim kutusuna girilen verilerle [AVG'yi Etkinleştir](#) iletişim kutusunu açar. Bu iletişim kutusunda satış numaranızı (*AVG'yi yüklerken kullandığınız numara*) ya da eski lisans numaranızı (*örn. yeni bir AVG ürününe geçerken*) değiştirmek için lisans numaranızı girebilirsiniz.
- **Şimdi kaydolun** - AVG web sitesinin (<http://www.avg.com/>) kayıt sayfasına bağlanır. Lütfen kayıt bilgilerinizi doldurun; sadece AVG ürünlerini kaydettiren müşterilerimiz ücretsiz teknik destek alabilecektir.

Not: AVG Internet Security 2012 deneme sürümünü kullanıyorsanız, sonraki iki öge, Şimdi satın al ve Etkinleştir olarak görünür ve programın tam sürümünü hemen satın almanızı sağlar. Bir-satış numarasıyla yüklenmiş AVG Internet Security 2012 için, öğeler Kaydet ve Etkinleştir olarak görünür.

- **AVG Hakkında** - **AVG Technologies CZ**'nin iletişim bilgileri, lisans sözleşmesi, sistem bilgileri, program ve virüs veritabanı sürümü ve program adı hakkında bilgi veren beş sekmeli **Bilgi** iletişim kutusunu açar.

5.1.6. Destek

Destek bağlantısı, yardım ararken ihtiyaç duyabileceğiniz tüm bilgileri içeren yeni bir **Bilgi** iletişim kutusu açar. İletişim kutusunda kurulu AVG programınız (*program / veritabanı sürümü*) ile ilgili temel bilgiler, lisans ayrıntıları ve hızlı destek bağlantıları listesi bulunur.

Bilgi iletişim kutusu altı sekmeye ayrılmıştır:



Sürüm sekmesi üç bölüme ayrılmıştır:



- **Destek Bilgileri** - AVG Internet Security 2012 Sürüm, virüs veritabanı, [Virüslerden Koruma](#) veritabanı sürümü ve [LinkScanner](#) sürümü hakkında bilgi verir.
- **Kullanıcı Bilgileri** - Lisanslı kullanıcı ve şirket hakkında bilgi verir.
- **Lisans Ayrıntıları** - Lisansınız hakkında bilgi verir (*ürün adı, lisans türü, lisans numarası, son kullanma tarihi ve kullanıcı sayısı*). Bu bölümde **Kaydet** bağlantısını kullanarak **AVG Internet Security 2012** uygulamanızı çevrimiçi kaydettirebilirsiniz; böylece [AVG teknik desteği](#) tam kapsamda kullanabilirsiniz. Ayrıca, **Yeniden etkinleştir** bağlantısını kullanarak **AVG'yi etkinleştir** iletişim kutusunu açabilirsiniz: satış numaranızı (*AVG Internet Security 2012 kurulumu sırasında kullandığınız*) değiştirmek veya mevcut lisans numaranızı bir başkasıyla değiştirmek (*örn. daha üst bir AVG ürününe yükseltme yaparken*) için ilgili alana *lisans numaranızı girin*.

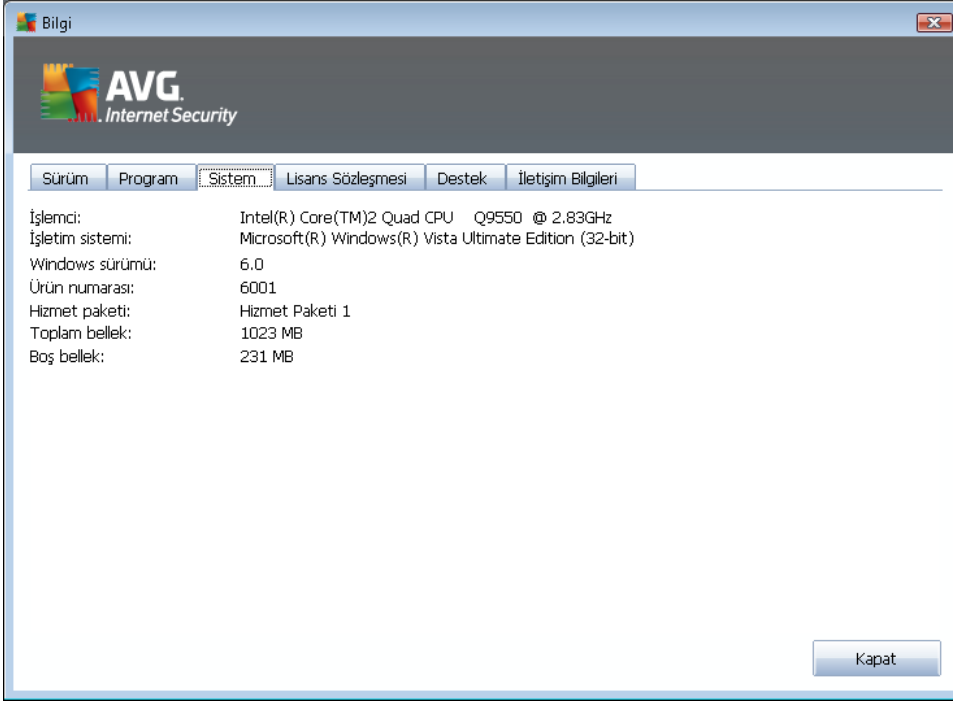


Program sekmesinde **AVG Internet Security 2012** program dosyası sürümü ve üründe kullanılan üçüncü partileri kodları hakkında bilgi bulabilirsiniz:



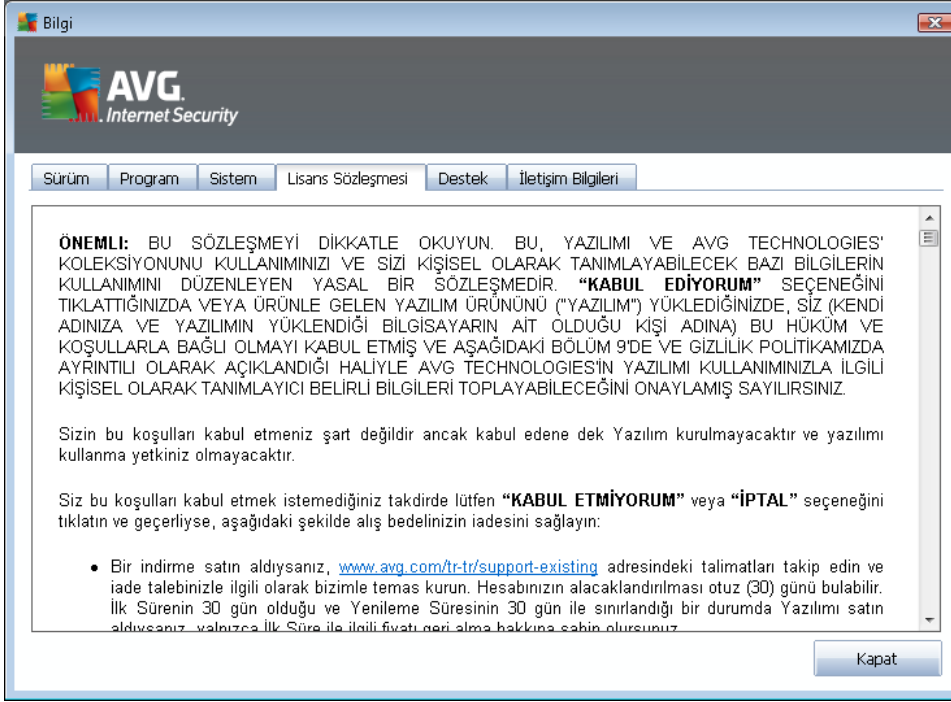


Sistem sekmesi işletim sistemi parametrelerinin listesini sunar (*işlemci türü, işletim sistemi ve sürümü, üretim numarası, kullanılan hizmet paketleri, toplam bellek boyutu ve boş bellek boyutu*):

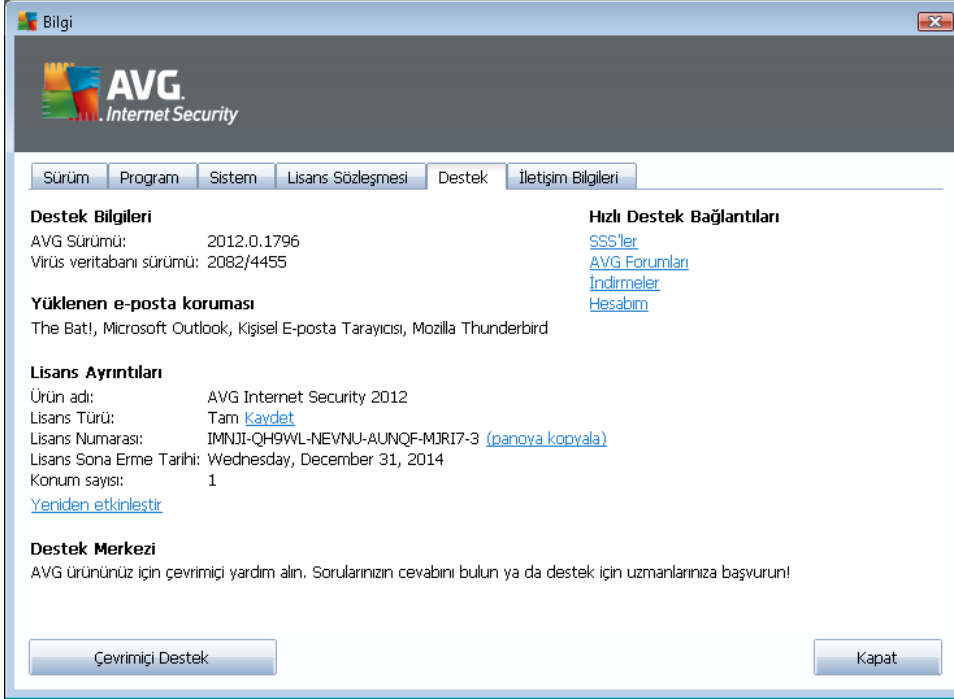




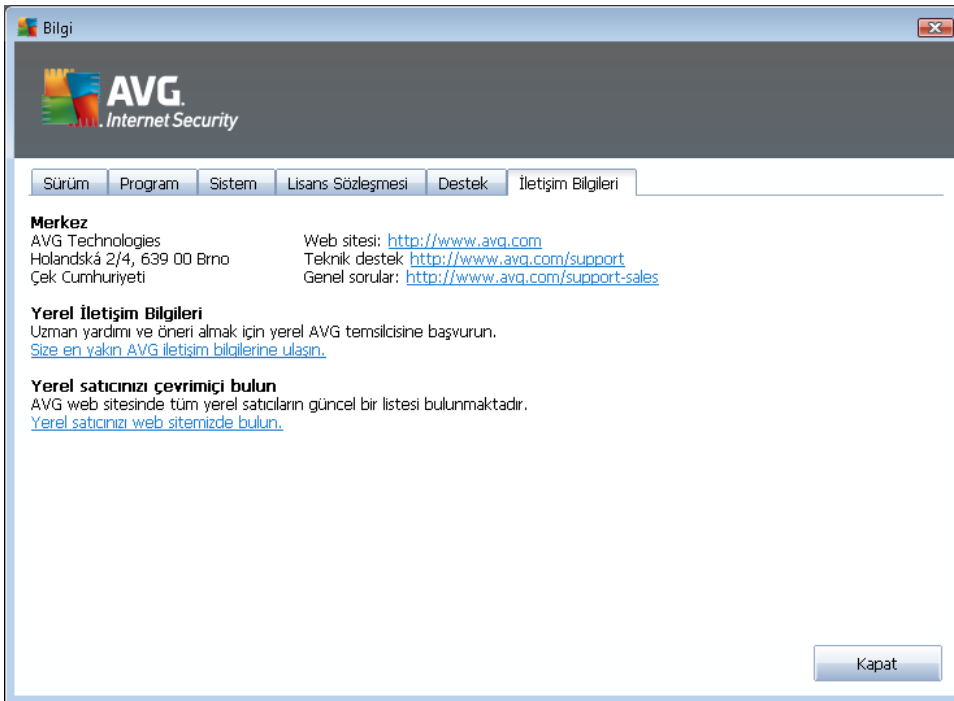
Lisans Sözleşmesi sekmesinde siz ve AVG Technologies arasındaki lisans sözleşmesinin tam metnini okuyabilirsiniz:



Destek sekmesi müşteri desteğiyle iletişim kurma imkanlarının listesini sunar. Ayrıca, AVG web sitesi (<http://www.avg.com/>), AVG forumları, SSS vb. bölümlerin bağlantılarını sağlar. Müşteri destek ekibiyle iletişim kurduğunuzda kullanabileceğiniz bilgileri de burada bulabilirsiniz:



İletişim sekmesi AVG Technologies ve AVG yerel temsilcileri ve satıcılarında iletişim kurulabilecek kişilerin listesini sunar:





5.2. Güvenlik Durumu Bilgisi

Güvenlik Durumu Bilgisi bölümü **AVG Internet Security 2012** ana penceresinin üst kısmında yer alır. Bu bölümde **AVG Internet Security 2012** programınızın mevcut güvenlik durumu hakkında her zaman bilgi bulabilirsiniz. Lütfen bu bölümde betimlenmesi muhtemel simgeleri ve anlamlarını inceleyin:



- Yeşil simge **AVG Internet Security 2012 uygulamasının tamamen işlevsel olduğunu belirtir**. Bilgisayarınız tamamen korunmaktadır, günceldir ve yüklü tüm bileşenler doğru çalışmaktadır.



- Turuncu simge, bir ya da birden fazla bileşenin yanlış yapılandırıldığını ve söz konusu bileşenlerin özelliklerine/ayarlarına dikkat etmeniz gerektiğini gösterir. **AVG Internet Security 2012** uygulamasında herhangi bir kritik sorun yoktur ve muhtemelen bir nedenden dolayı bileşenlerden bazılarını geçici olarak kapatmayı seçmiş olabilirsiniz. Hala korunuyorsunuz!. Diğer bir yandan lütfen bileşenin ayarlarını inceleyin! Adı **Güvenlik Durumu Bilgisi** kısmında sağlanır.

Turuncu simge, bir bileşenin hata durumunu herhangi bir nedenle yok saydığınızda da görünür. **Bileşen durumunu yoksay** seçeneğine, **AVG Internet Security 2012** ana penceresinin [bileşen genel görünümü](#) penceresindeki ilgili bileşen simgesi üzerinde bağlam menüsünden (*sağ fare tıklatmasıyla açılır*) erişilebilir. Bileşenin hata durumunun farkında olduğunuzu göstermek için bu seçeneği belirleyin, ancak belirli bir neden doğrultusunda **AVG Internet Security 2012** uygulamasının u şekilde çalışmasını istiyorsanız [sistem tepsisi simgesi](#) ile uyarılmazsınız. Özel durumlar için bu seçeneği kullanmanız gerekebilir ancak en kısa zamanda **Bileşen durumunu yoksay** seçeneğini devre dışı bırakmanız önerilir.



- Kırmızı simge **AVG Internet Security 2012 uygulamasının kritik durumda olduğunu belirtir!** Bir veya daha fazla bileşen düzgün çalışmıyor ve **AVG Internet Security 2012** uygulaması bilgisayarınızı koruyamıyordur. Lütfen rapor edilen sorunu çözmek için gerekli ilgiyi gösterin. Hatayı kendi başınıza çözemiyorsanız [AVG teknik destek](#) ekibi ile iletişim kurun.

AVG Internet Security 2012 uygulamasının en verimli performansı ayarlayamaması durumunda, Onar adlı yeni bir düğme (alternatif olarak, sorun birden fazla bileşenle ilgiliyse, Tümünü onar düğmesi) görüntülenir. Program denetimini ve yapılandırmasını otomatik olarak başlatmak için bu düğmeye basın. Bu özellik, AVG Internet Security 2012 uygulamasını en verimli performansa ayarlamanın ve maksimum güvenlik düzeyine ulaşmanın kolay bir yoludur!

Güvenlik Durumu Bilgisi fonksiyonuna gereken özeni göstermeniz ve herhangi bir sorunun rapor edilmesi halinde anında sorunu çözmeye çalışmanız önerilmektedir. Aksi takdirde bilgisayarınız risk altında olacaktır!

Not: *AVG Internet Security 2012 durum bilgilerine istediğiniz zaman [sistem tepsisi simgesinden](#) de ulaşabilirsiniz.*



5.3. Hızlı Bağlantılar

Hızlı bağlantılar, AVG Internet Security 2012 [kullanıcı arayüzünün](#) sol tarafında yer alır. Bu bağlantılar tarama ve güncelleme gibi en önemli ve en sık kullanılan uygulama özelliklerine anında erişebilmenizi sağlar. Hızlı bağlantılara kullanıcı arayüzündeki tüm iletişim kutularından erişilebilir:



Hızlı bağlantılar grafik olarak üç bölüme ayrılmıştır:

- **Genel Bakış** - açık durumdaki herhangi bir AVG arayüzünden [yükli bileşenlerin tümünün görüntülediği genel bakış penceresine](#) gitmen için bu bağlantıyı kullanın. (*Ayrıntılar için [Bileşen Genel Görünümü](#) bölümüne bakın*)
- **Şimdi tara** - Varsayılan olarak, düğme başlatılan son taramanın bilgilerini sağlar (*tarama türü ve başlatılan son taramanın tarihi gibi*). Aynı taramayı tekrar başlatmak için **Şimdi tara** komutunu tıklayın. Başka bir tarama başlatmak istiyorsanız, **Tarama seçenekleri** bağlantısını tıklayın. Bu şekilde taramaları çalıştırabileceğiniz, taramaların zamanını ayarlayabileceğiniz veya bunların parametrelerini düzenleyebileceğiniz [AVG tarama arayüzünü](#) açarsınız. (*Ayrıntılar için [AVG Tarama](#) bölümüne bakın*)
- **Şimdi güncelle** - Bağlantı son başlatılan [güncellemenin](#) tarih ve saatini sağlar. Güncelleme işlemini hemen başlatmak ve ilerlemesini izlemek için bu düğmeye basın. (*Ayrıntılar için [AVG Güncellemeleri](#) bölümüne bakın*)

Hızlı bağlantılara [AVG Kullanıcı Arayüzünden](#) her zaman erişilebilir. Belirli bir işlemi (tarama veya güncelleme) başlatmak üzere hızlı bağlantılardan birini kullandığınızda, uygulama yeni bir iletişim kutusunda açılacaktır fakat söz konusu pencereden de hızlı bağlantılara ulaşabilirsiniz. Ayrıca, çalışan işlem grafik olarak gezinme paneline yansıtılır ve böylece o anda **AVG Internet Security 2012** uygulamasında çalışmakta olan tüm başlatılmış işlemler üzerinde tam kontrolünüz olur.

5.4. Bileşen Genel Görünümü

Bileşen Genel Görünümü bölümleri

Bileşen Genel Görünümü bölümü AVG Internet Security 2012 [kullanıcı arayüzünün](#) orta kısmında yer alır. Bölüm iki bölüme ayrılır:

- **Yükli tüm bileşenlere genel bakış** yükli bileşenler için grafik panellerden oluşur. Her panel bileşenin simgesi ile etiketlenir ve ilgili bileşenin o anda aktif olup olmadığına dair bilgi sunar.



- **Bileşenin açıklaması** iletişim kutusunun alt kısmında yer alır. Açıklama bileşenin temel işleviyle ilgili kısa bir özettir. Seçilen bileşenin mevcut durumu hakkında bilgi de sağlar.

Yüklü bileşen listesi

AVG Internet Security 2012 içinde, **Bileşen Genel Görünümü** kısmı aşağıdaki bileşenler hakkında bilgiler içerir:

- **Virüslerden Koruma** sisteminizdeki virüs, casus yazılım, solucan, truva atı ve istenmeyen yürütülebilir dosyaları veya kitaplıkları tespit eder ve sizi kötü amaçlı reklam yazılımlarından korur - [ayrıntılar >>](#)
- **LinkScanner** internette arama ve gezinme sırasında sizi web tabanlı saldırılara karşı korur - [ayrıntılar >>](#)
- **E-posta Koruması** gelen e-posta mesajlarınızı istenmeyen e-postalara karşı denetler ve virüsleri, kimlik avı saldırılarını veya diğer tehditleri engeller - [ayrıntılar >>](#)
- **Firewall** her ağ bağlantı noktasındaki tüm iletişimleri denetleyerek sizi kötü amaçlı saldırılardan korur ve tüm sızma girişimlerini engeller- [ayrıntılar >>](#)
- **Anti-Rootkit** uygulamalar, sürücüler ve kitaplıklarda gizlenmiş tehlikeli kök dizinler için tarama yapar - [ayrıntılar >>](#)
- **Sistem Araçları**, AVG ortamı ve işletim sistemi bilgileri hakkında ayrıntılı bir özet sunar - [ayrıntılar >>](#)
- **PC Analyzer** analizörü, bilgisayarınızın durumu hakkında bilgi verir - [ayrıntılar >>](#)
- **Identity Protection** dijital varlıklarınızı yeni ve bilinmeyen tehditlere karşı korumak üzere sürekli tetiktedir - [ayrıntılar >>](#)
- **Güvenlik Araç Çubuğu** seçili AVG işlevini doğrudan İnternet tarayıcınızdan kullanmanıza olanak sağlar - [ayrıntılar >>](#)
- **Uzaktan Yönetim** yalnızca [yükleme süreci](#) esnasında bu bileşenin yüklenmesini istediğinizi belirtmeniz halinde AVG Business Sürümlerinde görüntülenir

Erişilebilir eylemler

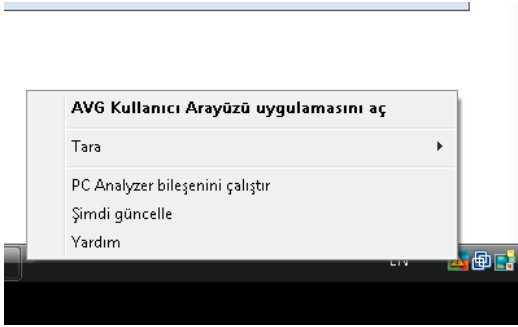
- **Bileşen genel görünümü ekranında bileşeni seçmek için fareyi ilgili bileşen simgesi üzerinde hareket ettirin.** Aynı anda [kullanıcı arayüzünün](#) kısmında bileşenin temel fonksiyonları hakkında açıklamalar görüntülenir.
- **Bileşenin kendi arayüzünü açmak ve temel istatistik verileri görüntülemek için bileşen simgesini tek tıklatın.**
- **Bağlam menüsünü birkaç seçenekle genişletmek için fareyi bileşen simgesi üstünde sağ tıklatın:**







- **Aç** - Bileşenin kendi iletişim kutusunu açmak için bu seçeneği tıklatın (*bileşen simgesi üzerinde tek tıklatma gibi*).
- **Bu bileşenin durumunu yoksay** - [Bileşenin hata durumunun](#) farkında olduğunuzu ancak belirli bir nedenle bu durumu muhafaza etmek istediğinizi ve [sistem tepsisi simgesi](#) ile uyarılmak istemediğinizi göstermek için bu seçeneği seçin.
- **Gelişmiş ayarlarda aç ...** - Bu seçenek yalnızca, [gelişmiş ayarlar](#) olma ihtimali bulunan bazı bileşenlerle kullanılabilir.

5.5. Sistem Tepsisi Simgesi

AVG Sistem Tepsisi Simgesi (Windows görev çubuğunuzda, ekranınızın sol alt köşesinde) **AVG Internet Security 2012** uygulamanızın mevcut durumunu gösterir. **AVG Internet Security 2012 kullanıcı arayüzü** ana penceresinin açık ya da kapalı olduğu önemli olmaksızın devamlı olarak sistem tepsinizde bulunur:



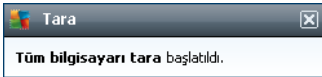
AVG Sistem Tepsisi Simgesi görünümü

-  Tam renkli ve başka öge bulunmayan simge tüm **AVG Internet Security 2012** bileşenlerinin etkin ve tamamen çalışır durumda olduğunu gösterir. Ancak, simge bileşenlerden biri tam çalışır durumda olmasa da (kullanıcı [bileşen durumunu yoksaymaya](#) karar verdiğinde) bu şekilde görünebilir. (*Bileşenin durumunu yoksayma seçeneğini onaylayarak, [bileşenin hata durumunun](#) farkında olduğunuzu, ancak kimi nedenlerle durumun böyle kalmasını ve durum hakkında uyarı almak istemediğinizi ifade edersiniz.*)
-  Üzerinde ünlem işareti bulunan simge bir bileşenin (*veya daha fazla bileşenin*) [hata durumunda](#) olduğunu gösterir. Bu tip uyarılara mutlaka dikkat edin ve düzgün ayarlanmamış bileşenin yapılandırma sorununu gidermeye çalışın. Bileşen yapılandırması değişikliklerini gerçekleştirebilmek için sistem tepsisi simgesini çift tıklatarak [uygulamanın kullanıcı arayüzünü](#) açın. Hangi bileşenin [hata durumunda](#) olduğuyla ilgili ayrıntılı bilgi için lütfen [güvenlik durumu bilgisi](#) bölümüne bakın.
-  Sistem tepsisi tam renkli olarak yanıp sönen ve dönen bir ışıkla da görünebilir. Bu grafik gösterim o anda başlatılan bir güncelleme işlemi işaret eder.
-  Tam renkli ve ok işaretli simge ise **AVG Internet Security 2012** taramasının o anda çalışmakta olduğunu gösterir.



AVG Sistem Tepsisi Simgesi bilgileri

AVG Sistem Tepsisi Simgesi, **AVG Internet Security 2012** uygulamanızdaki geçerli etkinlikler ve programdaki olası durum değişiklikleri (örn. *zamanı ayarlanmış bir tarama veya güncellemenin otomatik başlatılması, Güvenlik duvarı profil anahtarı, bir bileşenin durumundaki değişiklik, hata durumu oluşumları...*), hakkında sistem tepsi sembolünde açılır bir pencere yoluyla bilgi de verir:



AVG Sistem Tepsisi Simgesi yoluyla erişilebilen işlemler

AVG Sistem Tepsisi Simgesi, **AVG Internet Security 2012** [kullanıcı arayüzüne](#) erişmek için bir hızlı bağlantı olarak da kullanılabilir; bunun için simgeyi çift tıklatmak yeterlidir. Simgeyi sağ tıklayarak aşağıdaki seçenekleri sunan kısa bir bağlam menüsü açarsınız:

- **AVG Kullanıcı Arayüzünü Aç** - **AVG Internet Security 2012** [kullanıcı arayüzünü](#) açmak için tıklatın.
- **Taramalar** - [Önceden tanımlanan taramalar](#) bağlam menüsünü açmak için tıklatın ([Tüm Bilgisayar Taraması](#), [Belirli Dosyaları veya Klasörleri Tara](#), [Anti-Rootkit taraması](#)) ve gereken taramayı seçin, tarama hemen başlayacaktır.
- **Güvenlik Duvarı** - Temel parametreleri ayarlayabileceğiniz [Güvenlik Duvarı](#) ayarlama seçenekleri bağlam menüsünü açmak için tıklayın: Bu parametreler, [Güvenlik duvarı durumu](#) ([Güvenlik duvarı etkin/Güvenlik duvarı devre dışı/Acil durum modu](#)), [oyun moduna geçme](#) ve [Güvenlik duvarı profilleri](#)'dir.
- **PC Analyzer**'ı çalıştır - [PC Analyzer](#) bileşenini başlatmak için tıklayın.
- **Çalışan taramalar** - Bu öğe yalnızca bilgisayarınızda o anda çalışan bir tarama olması durumunda görüntülenir. Bunun ardından, bu tarama için taramanın önceliğini ayarlayabilir, alternatif olarak çalışan taramayı durdurabilir veya duraklatabilirsiniz. Ek olarak, şu işlemlere erişilebilir: [Tüm taramalar için önceliği ayarla](#), [Tüm taramaları duraklat](#) veya [Tüm taramaları durdur](#).
- **Şimdi güncelle** - Anında [güncelleme](#) işlemini başlatır.
- **Yardım** - Başlangıç sayfasında yardım dosyasını açar.



5.6. AVG gadget'ı

AVG gadget'ı Windows masaüstünde görüntülenir (*Windows Kenar Çubuğu*). Bu uygulama yalnızca Windows Vista ve Windows 7 işletim sistemlerinde desteklenir. **AVG gadget'ı** en önemli **AVG Internet Security 2012** işlevlerine, yani [taramaya](#) ve [güncellemeye](#) hemen erişim sağlar:



Tarama ve güncellemeye hızlı erişim

Gerektiğinde, **AVG gadget'ı** hemen bir tarama veya güncelleme başlatabilmenizi sağlar:

- **Şimdi tara - tüm bilgisayarın taranmasını** doğrudan başlatmak için [Şimdi tara](#) bağlantısını tıklatın. Tarama sürecinin ilerlemesini gadget'ın alternatif kullanıcı arayüzünden izleyebilirsiniz. Kısa istatistikler genel görünümü, taranan nesnelere, tespit edilen tehditlerin ve temizlenen tehditlerin sayısı ile ilgili bilgiler verir. Tarama sırasında,  tarama sürecini istediğiniz zaman duraklatabilir  veya durdurabilirsiniz. Tarama sonuçlarıyla ilgili ayrıntılı veriler için lütfen standart [Tarama sonuçları genel görünümü](#) iletişim kutusuna başvurun. Bu iletişim kutusu, **Ayrıntıları göster** seçeneği aracılığıyla doğrudan araç üzerinden açılabilir (*ilgili tarama sonuçları Kenar çubuğu aracı taraması*) altında listelenir.




- **Şimdi güncelle** - güncellemesini doğrudan gadget içerisinden başlatmak için **Şimdi güncelle** **AVG Internet Security 2012** bağlantısını tıklatın:





Sosyal ağlara erişim


AVG gadget'ı büyük sosyal ağlara bağlanmanızı sağlayan hızlı bir bağlantı da sunar. Twitter, Facebook veya LinkedIn'deki AVG topluluklarına bağlanmak için ilgili düğmeyi kullanın:

- **Twitter bağlantısı**  - Twitter'da gönderilen en son AVG yayınlarının genel görünümünü sunan yeni bir **AVG gadget'ı** arayüzü açar. İnternet tarayıcınızı yeni bir pencerede açmak için, **AVG Twitter yayınlarının tümünü görüntüle** bağlantısını izleyin, böylece doğrudan Twitter web sitesine, özellikle de AVG ile ilgili haberler için atanan sayfaya yönlendirilirsiniz:



- **Facebook bağlantısı**  - İnternet tarayıcınızı Facebook web sitesinde açar, özellikle de **AVG topluluğu** sayfasında
- **LinkedIn**  - bu seçenek yalnızca ağ kurulumu içerisinde kullanılabilir (*başka bir deyişle, AVG Business Editions lisanslarından biriyle AVG'yi kurduğunuz anlaşıldıktan sonra*) ve LinkedIn sosyal ağı içerisindeki **AVG SMB Community** web sitesinde internet tarayıcınızı açar

Gadget ile erişilebilen diğer özellikler

- **PC Analyzer**  - kullanıcı arayüzünü [PC Analyzer](#) bileşeni içinde açar
- **Arama kutusu** - bir anahtar kelime yazın ve varsayılan web tarayıcınızda yeni açılan bir pencerede arama sonuçlarını hemen alın



6. AVG Bileşenleri

6.1. Virüslerden Koruma

Virüslerden Koruma bileşeni **AVG Internet Security 2012** ürününüzün köşe taşlarından biridir ve bir güvenlik programının birçok temel özelliğini bir araya getirir:

- [Tarama Motoru](#)
- [Yerleşik Koruma](#)
- [Casus Yazılımdan Koruma](#)

6.1.1. Tarama Motoru

Virüslerden Koruma bileşenin temel özelliği olan tarama motoru tüm dosyaları ve dosya etkinliklerini bilinen virüslere karşı tarar (*açılan/kapatılan dosyalar, vb.*). Tespit edilen virüsler, harekete geçmeden engellenecek ve ardından silinecek ya da [Virüs Kasasında](#) karantinaya alınacaktır.

AVG Internet Security 2012 korumasının en önemli özelliği bilinen hiçbir virüsün bilgisayar bulaşamamasıdır!

Tespit yöntemleri

Virüsten koruma yazılımlarının çoğu buluşsal taramayı kullanır. Diğer bir deyişle, dosyalar virüs imzası olarak adlandırılan tipik virüs özelliklerine karşı taranır. Bu, yeni bir virüs mevcut virüslerin tipik özelliklerinden bazılarında sahipse söz konusu virüsten koruma tarayıcısının yeni ve bilinmeyen bir virüsü tespit edebileceği anlamına gelmektedir. **Virüslerden Koruma** aşağıdaki tespit yöntemlerini kullanır:

- Tarama - belirli bir virüsün özelliklerine sahip karakter dizeleri aranır
- Buluşsal analiz - sanal bir bilgisayar ortamında taranan nesnenin komutları dinamik bir şekilde canlandırılır
- Jenerik tespit - belirli bir virüs ya da virüs grubunun komut özelliklerinin tespitidir

Tek bir teknoloji bir virüsün tespit edilmesinde ya da tanımlanmasında yetersiz kalabileceken **Anti-Virus** yazılımı, bilgisayarınızın virüslerden korunmasını sağlamak için, çok sayıda teknolojiyi bir araya getirir. **AVG Internet Security 2012**, bunun yanı sıra sistemde potansiyel anlamda istenmeyen çalıştırılabilir uygulamaları ya da DLL kitaplıklarını da inceleyebilmekte ve tespit edebilmektedir. Söz konusu tehlikeleri Potansiyel Olarak İstenmeyen Programlar olarak adlandırırız (*farklı casus yazılım, reklam yazılımı türleri vb.*). Buna ek olarak, **AVG Internet Security 2012** sistem kayıt defterinizi şüpheli girdilere, geçici internet dosyalarına ve izleme tanımlama bilgilerine karşı da tarar ve söz konusu potansiyel olarak istenmeyen nesnelere de diğer bulaşmalarla aynı şekilde çözebilmenize olanak tanır.



AVG Internet Security 2012 bilgisayarınıza kesintisiz koruma sağlar!

6.1.2. Yerleşik Koruma

AVG Internet Security 2012, size yerleşik koruma adı altında sürekli koruma sağlar. **Virüslerden Koruma** bileşeni açılan, kaydedilen ve kopyalanan her dosyayı tek tek tarar (*belirli uzantılara sahip olanları veya hiç uzantısı olmayanları*). Bilgisayarın sistem alanlarını ve çıkarılabilir ortamları korur (*flash disk vb.*). Erişilen bir dosyada virüs tespit ederse geçerli işlemi durdurur ve virüsün kendisini etkinleştirmesine izin vermez. Normalde, yerleşik koruma "arkaplanda" çalıştığından işlemin farkına bile varmazsınız. Ancak tehditler bulunduğu anda haberdar olursunuz; aynı anda, **Virüslerden Koruma** tehdidin etkinliği engeller ve tehdidi kaldırır.

Yerleşik koruma, başlatma sırasında bilgisayarınızın belleğine yüklenir ve bu özelliği daima açık tutmanız çok önemlidir.

6.1.3. Casus Yazılımdan Koruma

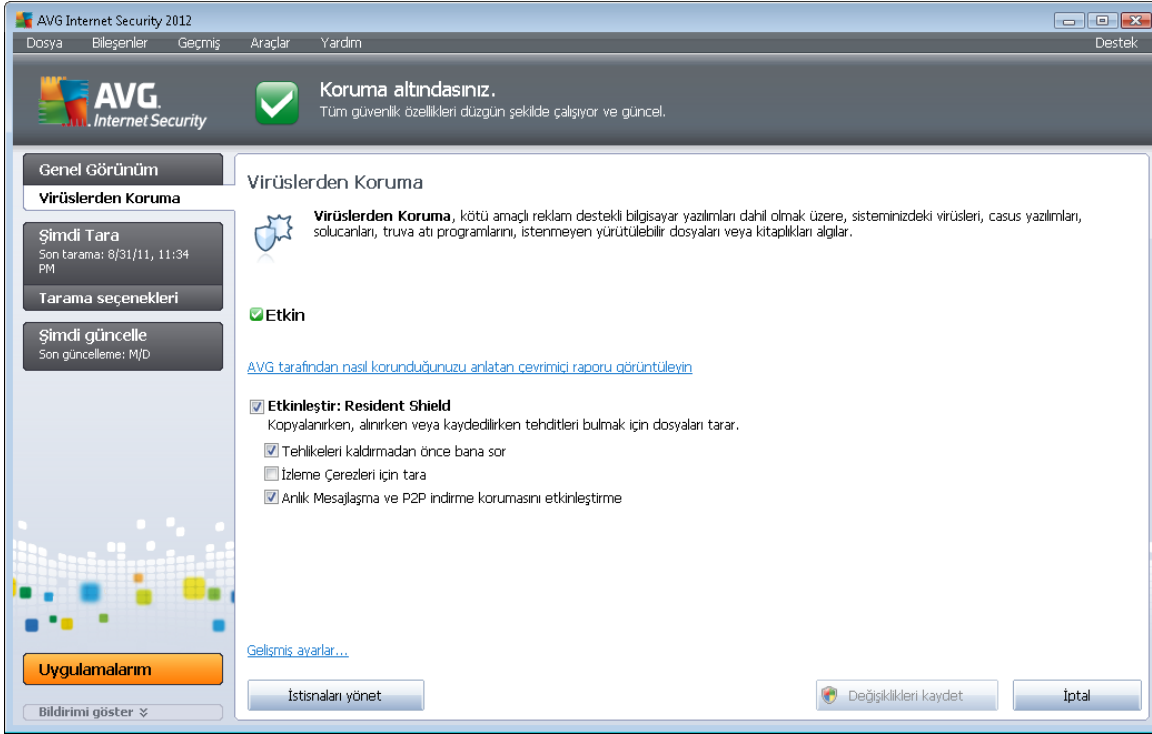
Casus Yazılımdan Koruma bilinen casus yazılım tanımlarını belirlemek için kullanılan bir casus yazılım veritabanı içerir. AVG casus yazılım uzmanları en son casus yazılım şablonlarını ortaya çıktıkları anda tanımlamak ve açıklamak için yoğun şekilde çalışır ve tanımlamaları casus yazılım veritabanına eklerler. Güncelleme işlemi yaptığınızda, bu yeni tanımlamalar bilgisayarınıza indirilir ve en son casus yazılım türlerine karşı daima güvenli şekilde koruma altında olmanız sağlanır. **Casus Yazılımdan Koruma** bilgisayarınızı kötü amaçlı yazılım/casus yazılımlara karşı tamamen taramanıza olanak sağlar. Ayrıca, uykuda olan ve etkin olmayan kötü amaçlı yazılımları da (yani, bilgisayara indirilmiş ancak henüz etkinleştirilmemiş olanları) tespit eder.

Casus yazılım nedir?

Casus yazılımlar, genellikle kullanıcının bilgisi ya da izni olmaksızın kullanıcının bilgisayarından bilgi toplayan kötü amaçlı bir yazılım türü olarak tanımlanırlar. Bazı casus yazılım uygulamaları genellikle belirli bir amaç doğrultusunda kurulur ve sıklıkla reklam, açılan pencereler veya farklı istenmeyen yazılım türleri içerirler. Şu anda bilinen en yaygın bulaşma kaynağı, potansiyel anlamda tehlikeli öğeler içeren web siteleridir. E-posta ya da solucan ve virüsler yoluyla aktarım gibi diğer bulaşma yöntemleri de oldukça etkilidir. En önemli korunma, yerleşik bir kalkan olarak çalışan ve siz çalıştırdığınız zaman arka planda uygulamaları tarayan **Anti-Spyware** gibi devamlı olarak arka planda çalışan bir tarayıcı kullanmaktır.

6.1.4. Virüslerden Koruma Arayüzü

Virüslerden Koruma bileşeni arayüzü bileşenin işlevselliği, bileşenin mevcut durum bilgisi (*Etkin*) ve bileşenin temel yapılandırma seçenekleri hakkında kısa bilgiler sağlar:



Yapılandırma seçenekleri

İletişim kutusu **Virüslerden Koruma** bileşeni özelliklerinin bazı temel yapılandırma seçeneklerini sağlar. Bunların kısa açıklamaları:

- **AVG tarafından nasıl korunduğunuzu anlatan çevrimiçi raporu görüntüleyin** - Bağlantı sizi AVG web sitesinde (<http://www.avg.com/>) belirli bir sayfaya yönlendirir. Bu sayfada belirli bir zaman diliminde ve toplam olarak bilgisayarınızda gerçekleştirilen tüm **AVG Internet Security 2012** etkinliklerine ayrıntılı bir istatistiksel genel bakış bulabilirsiniz.
- **Yerleşik Kalkanı Etkinleştir** - Bu seçenek yerleşik korumayı kolayca açmanıza/ kapatmanıza olanak sağlar. Yerleşik Kalkan dosyalar kopyalanırken, açılırken ya da kaydedilirken söz konusu dosyaları tarar. Herhangi bir virüs ya da bir tehlike tespit edildiği zaman anında uyarılırsınız. Varsayılan olarak, bu işlev açıktır ve böyle bırakmanız önerilir! Yerleşik koruma açık durumdayken tespit edilen bulaşmalar hususunda gerçekleştirilecek eylemi belirleyebilirsiniz:
 - **Tüm tehlikeleri otomatik kaldır / Tehlikeleri kaldırmadan önce bana sor** - Bu seçeneklerden birini işaretleyin. Bu seçimin güvenlik seviyesi üzerinde herhangi bir etkisi yoktur ve sadece tercihlerinizi yansıtır.



- **İzleme Çerezleri için tara** - Önceki seçeneklerde bağımsız olarak, izleme çerezlerini taramak isteyip istemediğinize karar verebilirsiniz. (Çerezler bir sunucu tarafından web tarayıcısına ve oradan da siteye her ulaşıldığında değiştirilmeksizin tarayıcı tarafından geri gönderilen metin parçalarıdır. HTTP çerezleri, site tercihleri veya elektronik alışveriş sepetlerinin içerikleri gibi kullanıcılar hakkındaki belirli bilgilerin kimliklerinin doğrulanması, takibi ve sürdürülmesi için kullanılır.) Belirli durumlarda maksimum güvenlik seviyesine ulaşmak için bu seçeneği kullanabilirsiniz fakat varsayılan olarak kapalıdır.
- **Anlık Mesajlaşma korumasını etkinleştir** - Anlık mesajlaşma iletişiminin (örn. ICQ, MSN Messenger, ...) virüs içermediğini doğrulamak istiyorsanız bu öğeyi işaretleyin.
- **Gelişmiş ayarlar...** - **AVG Internet Security 2012** [Gelişmiş ayarlar](#) konumunda ilgili iletişim kutusuna yönlendirilmek için bağlantıyı tıklatın. Bu konumda bileşenin yapılandırmasını ayrıntılı biçimde düzenleyebilirsiniz. Ancak, tüm bileşenlerin varsayılan yapılandırmasının **AVG Internet Security 2012** uygulaması tarafından en üstün performans ve en yüksek güvenlik sağlayacak biçimde ayarlandığını lütfen unutmayın. Değiştirmek için gerçek bir nedeniniz yoksa, varsayılan yapılandırmayı korumanız önerilir!

Kontrol düğmeleri

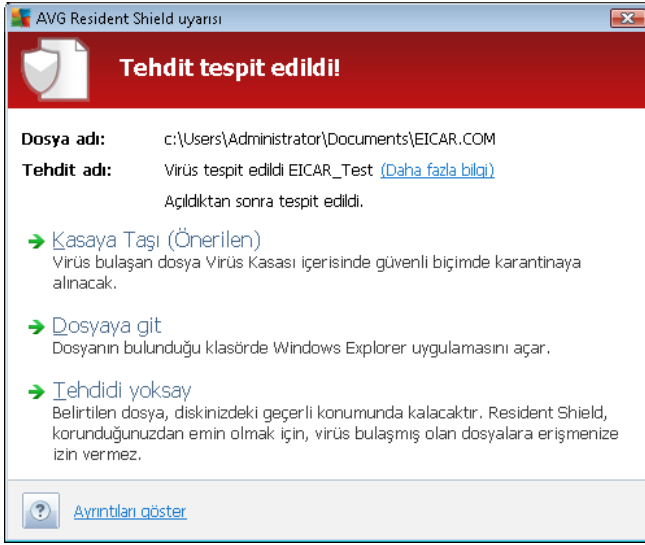
İletişim kutusunda kullanabileceğiniz düğmeler:

- **İstisnaları yönet** - [Resident Shield - İstisnalar](#) adında yeni bir iletişim kutusu açar. İletişim kutusuna [Gelişmiş ayarlar / Virüslerden Koruma / Resident Shield / İstisnalar yolu izlenerek de ulaşılabilir](#) (ayrıntılı açıklama için lütfen ilgili bölüme bakın). İletişim kutusunda Resident Shield taramasının dışında tutulması gereken dosyaları ve klasörleri belirleyebilirsiniz. Bu gerekli değilse, hiçbir öğeyi hariç tutmamanızı önemle öneririz! İletişim kutusundaki kontrol düğmeleri:
 - **Yol Ekle** - Yerel disk menü ağacından teker teker seçerek taramada hariç tutulacak dizini (veya dizinleri) belirleyin.
 - **Dosya Ekle** - Yerel disk menü ağacından teker teker seçerek taramada hariç tutulacak dosyaları belirleyin.
 - **Öğeyi Düzenle** - Seçilen dosyaya giden yolu düzenlemenize olanak verir.
 - **Öğeyi Kaldır** - Listedenden seçili öğeye götüren yolu silmenize olanak verir.
- **Değişiklikleri kaydet** - Bu iletişim kutusunda gerçekleştirilen tüm bileşen ayarları değişikliklerini kaydedin ve **AVG Internet Security 2012** ana [kullanıcı arayüzüne](#) dönün (bileşenlere genel bakış).
- **İptal** - Bu iletişim kutusunda gerçekleştirilen tüm bileşen ayarları değişikliklerini iptal edin. Hiçbir değişiklik kaydedilmez. **AVG Internet Security 2012** ana [kullanıcı arayüzüne](#) geri dönersiniz (bileşenlere genel bakış).

6.1.5. Resident Shield Tespitleri

Tehdit tespit edildi!

Yerleşik Kalkan dosyalar kopyalanırken, açılırken ya da kaydedilirken söz konusu dosyaları tarar. Herhangi bir virüs ya da bir tehlike tespit edildiği zaman aşağıdaki iletişim kutusu ile anında uyarılırsınız:



Bu iletişim kutusunda, tespit edilmiş ve bulaşmış olarak atanan dosya ile ilgili bilgiler (*Dosya adı*), tanınan bulaşmanın adı (*Tehdit adı*) ve bilinen bir tehditse, tespit edilen bulaşma hakkında ayrıntılı bilgiler bulabileceğiniz [Virüs ansiklopedisi](#) sayfasına yönlendiren bir bağlantı bulabilirsiniz (*Diğer bilgiler*).

Artık hangi işlemin yapılması gerektiğine karar vermeniz gerekir. Birçok alternatif seçenek mevcuttur. **Belirli durumlarda (bulaşmış dosyanın türüne ve bulunduğu konuma göre) tüm seçeneklerin her zaman kullanılamayacağını lütfen unutmayın!**

- **Tehdidi Deneyimli Kullanıcı olarak kaldır** - Tehdidi ortak kullanıcı olarak kaldırmak için yeterli haklara sahip olmadığınızı düşünüyorsanız bu kutuyu işaretleyin. Deneyimli Kullanıcılar kapsamlı erişim haklarına sahiptir ve tehlikenin belirli bir sistem klasöründe bulunması durumunda, tehdidi başarılı şekilde kaldırmak için bu kutuyu kullanmanız gerekebilir.
- **Temizle** - bu düğme yalnızca tespit edilen bulaşma temizlenebilecekse görüntülenir. Ardından, bulaşma dosyadan silinir ve dosya orijinal durumuna geri getirilir. Dosyanın kendisi virüsse, bunu silmek (*yani [Virüs Kasası](#)'na taşımak*) için bu işlevi kullanın.
- **Kasaya Taşı** - Virüs [Virüs Kasasına](#)
- **Dosyaya git** - Bu seçenek sizi şüpheli nesnenin tam konumuna yönlendirir (*yeni Windows Gezgini penceresi açar*)



- **Yoksay** - çok geçerli bir nedeninizin olmaması halinde KESİNLİKLE bu seçeneği belirlememenizi öneriyoruz!

Not: Tespit edilen objenin büyüklüğü, Virüs Kasası'ndaki boş alan sınırını aşabilir. Bu durumda, bulaşmış nesneyi Virüs Kasasına taşımaya çalıştığınızda size bu sorun hakkında bilgi veren bir uyarı iletisi görüntülenir. Ancak Virüs Kasası boyutu düzenlenebilir. Sabit diskinizin gerçek boyutunun uyarlanabilir yüzdesi olarak tanımlanır. Virüs Kasasının boyutunu arttırmak için, 'Virüs Kasası boyutunu sınırlandır' seçeneği aracılığıyla [AVG Gelişmiş Ayarlardaki Virüs Kasası](#) iletişim kutusuna gidin.

İletişim kutusunun alt bölümünde **Ayrıntıları göster** bağlantısını bulabilirsiniz - bulaşma tespit edilirken çalışan süreç ve sürecin tanımı hakkında ayrıntılı bilgilerin olduğu açılır pencereyi açmak için bu seçeneği tıklayın.

Yerleşik Kalkan tespitlerine genel bakış

[Yerleşik Kalkan](#) tarafından tespit edilen tüm tehditlerin tüm genel görünümü, [Geçmiş / Yerleşik Kalkan tespiti](#) sistem menüsü seçeneğinden erişilebilen **Yerleşik Kalkan tespiti** iletişim kutusundan bulunabilir:

The screenshot shows the AVG Internet Security 2012 interface. The main window displays a status bar at the top indicating 'Koruma altındasınız.' (Protected) with a green checkmark. Below this, the 'Genel Görünüm' (General View) section is active, showing a table of detection results for the Resident Shield. The table has columns for 'Bulaşma' (Infection), 'Nesne' (Object), 'Sonuç' (Result), 'Tespit zamanı' (Detection time), 'Nesne Türü' (Object type), and 'İşlem' (Action). A single entry is visible: 'Virüs tespit edildi EIC...' with a result of 'Bulaşmış' (Infected) and a detection time of '8/31/2011, 11:37:07 PM'. The interface also includes buttons for 'Şimdi Tara' (Scan Now), 'Tarama seçenekleri' (Scan options), 'Şimdi güncelle' (Update Now), and 'Uygulamaları' (Applications). At the bottom, there are buttons for 'Listeyi yenile' (Refresh list), 'Seçileni kaldır' (Remove selected), 'Tüm tehditleri kaldır' (Remove all threats), and 'Geri' (Back).

Bulaşma	Nesne	Sonuç	Tespit zamanı	Nesne Türü	İşlem
Virüs tespit edildi EIC...	c:\Users\Administrator\...	Bulaşmış	8/31/2011, 11:37:07 PM	dosya	C:\Wind

Yerleşik Kalkan tespiti [Yerleşik Kalkan](#) tarafından tespit edilip tehlikeli olduğu görülen ve temizlenen ya da [Virüs Kasasına](#) taşınan nesnelere hakkında genel bilgi vermektedir. Tespit edilen tüm nesnelere için aşağıdaki bilgiler verilir:

- **Bulaşma** - Algılanan nesnenin açıklaması (Muhtemelen adı da)



- **Nesne** - nesnenin konumu
- **Sonuç** - tespit edilen nesne ile gerçekleştirilen eylem
- **Algılama zamanı** - Nesnenin algılandığı tarih ve saat
- **Nesne Türü** - tespit edilen nesnenin türü
- **İşlem** - tespit edilmesi amacıyla potansiyel tehlike taşıyan nesneyi uyarıcı işlem nedir

İletişim kutusunun alt kısmında, listenin altında yukarıda listelenen tespit edilen nesnelerin toplam sayısı hakkında bilgi bulabilirsiniz. Buna ek olarak tespit edilen nesneler listesini ayrı bir dosyada dışa aktarabilir (**Listeyi Dosyaya Aktar**) ve tespit edilen nesneler hakkındaki tüm girişleri silebilirsiniz (**Listeyi Temizle**). **Listeyi Yenile** düğmesi, **Yerleşik Kalkan** tarafından tespit edilen buluntular listesini günceller. **Geri** düğmesi, sizi varsayılan [AVG ana iletişim kutusuna](#) (bileşenlere genel bakış) geri götürür.

6.2. LinkScanner

LinkScanner sizi web üzerinde "günden güne" artan tehditlere karşı korur. Bu tehditler idari web sitelerinden, tanınmış markaların web sitelerinden tutun, küçük işletmelerin web sitelerine kadar her tür web sitesinde gizlenmiş olabilir. **LinkScanner** görüntülemekte olduğunuz web sitesinde bulunan tüm bağlantıların arkasındaki web sayfalarını analiz ederek ve siz söz konusu bağlantıyı tıklamak üzereyken o anda güvenli olup olmadığından emin olarak sizi korur.

LinkScanner sunucu platformları korumasında kullanılmak için tasarlanmamıştır!

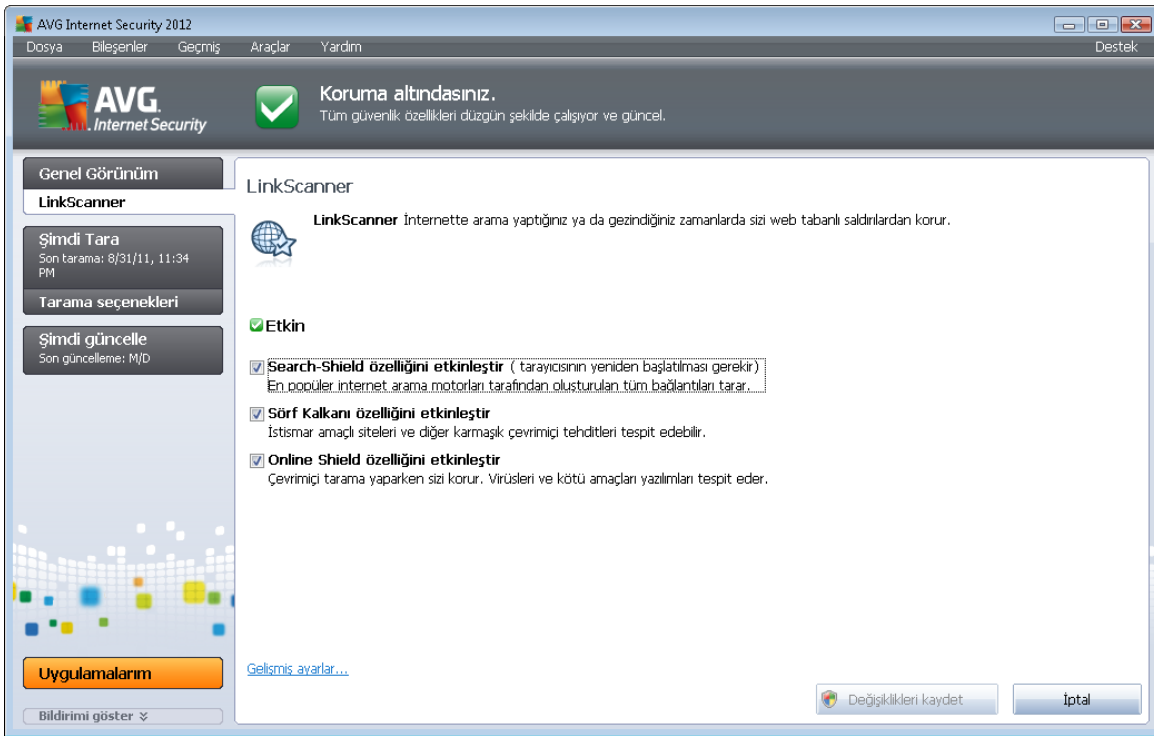
LinkScanner teknolojisi aşağıdaki temel özelliklerden oluşur:

- **Search-Shield** tehlikeli olabileceği bilinen web sitelerinin listesini (URL adreslerini) içerir. Google, Yahoo!, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask ve Seznam ile arama yaparken, tüm arama sonuçları bu listeye göre kontrol edilir ve bir karar simgesi gösterilir (*Yahoo! arama sonuçları için yalnızca "yararlanılan web sitesi" karar simgeleri gösterilir*).
- **Surf-Shield** ziyaret etmekte olduğunuz web sitelerinin adresi önemli olmaksızın web sitelerinin içeriğini tarar. Bazı web siteleri **Search-Shield** tarafından tespit edilmemiş olsa bile (örneğin, yeni ve zararlı bir web sitesi oluşturulduğunda ya da daha önce temiz olan bir web sitesine zararlı yazılım bulaştığında) tehdit, siz siteyi ziyaret etmeden hemen önce **Surf-Shield** tarafından tespit edilecek ve engellenecektir.
- **Online Shield** internette gezinme sırasında gerçek zamanlı koruma gibi çalışır. Ziyaret ettiğiniz web sitelerinin içeriklerini ve sitelerin içindeki muhtemel dosyaları, ilgili web sitesi henüz tarayıcınızda görünmeden ya da bilgisayarınıza indirilmeden tarar. **Online Shield** ziyaret etmek üzere olduğunuz sayfadaki virüs ve casus yazılımları tespit eder ve indirmeyi derhal durdurur; böylece hiçbir tehdit bilgisayarınıza ulaşamaz.
- **AVG Accelerator** daha düzgün çevrimiçi video oynatmaya izin verir ve ilave indirmeleri daha kolay hale getirir. Video hızlandırma işlemi çalışırken sistem tepsisi açılır penceresi ile bilgilendirilirsiniz.



6.2.1. LinkScanner Arayüzü

[LinkScanner](#) bileşeninin arayüzü, bileşenlerin işlevleri hakkında kısa açıklamalar sağlar ve işlevin geçerli durumu (*Etkin*) ile ilgili bilgiler verir:








İletişim kutusunun alt kısmında bileşenin bazı temel yapılandırma seçenekleri bulunur:

- **[Search-Shield'i etkinleştir](#)** - (*varsayılan olarak açık*): Yalnızca Arama Kalkanı işlevini kapatmak için iyi bir nedeniniz varsa kutunun işaretini kaldırın.
- **[Surf-Shield'i etkinleştir](#)** - (*varsayılan olarak açık*): Erişim sağlandığı anda güvenlik açığı olan web sitelerine karşı etkin (*gerçek zamanlı*) koruma. Bilinen kötü amaçlı site bağlantıları ve güvenlik açığından yararlanan içerikler, kullanıcı bir web tarayıcısı (*ya da HTTP kullanan diğer bir program*) aracılığıyla erişim sağladığında engellenir.
- **[Online Shield'i etkinleştir](#)** - (*varsayılan olarak açık*): Olası virüsler ve casus yazılımlara karşı ziyaret etmek üzere olduğunuz web sayfalarının gerçek zamanlı taranması. Bunlar tespit edilirse, indirme derhal durdurulur ve böylece hiçbir tehdit bilgisayarınıza ulaşamaz.

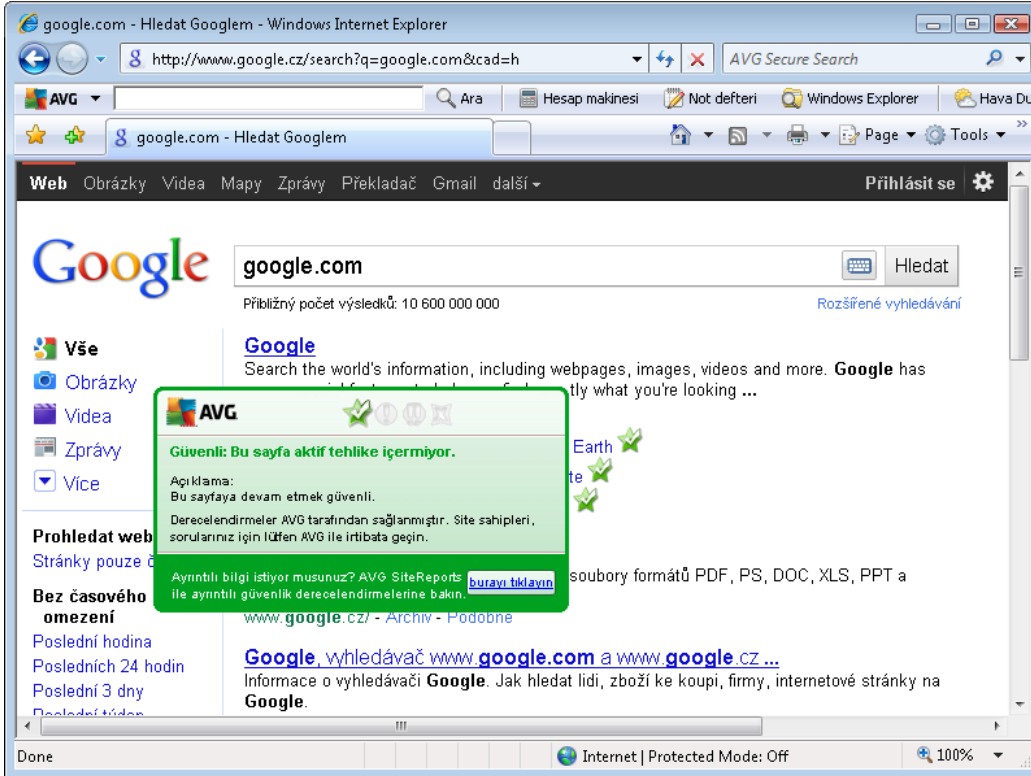
6.2.2. Search-Shield tespitleri

İnternet'te **Arama Kalkanı** açıkken arama yaptığınızda, en popüler arama motorlarından (*Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg, ve SlashDot*) döndürülen tüm arama sonuçları tehlikeli veya şüpheli bağlantılar içerip içermedikleri konusunda değerlendirilir. Bu bağlantıları kontrol ederek ve kötü bağlantıları işaretleyerek, [LinkScanner](#) sizi tehlikeli veya şüpheli bağlantıları tıklatmadan önce uyarır, böylece yalnızca güvenli web sitelerine gittiğinizden emin olursunuz.

Arama sonuçları sayfasında bağlantı değerlendirilirken bağlantının yanında bağlantı teyidi işleminin devam etmekte olduğunu gösteren bir grafik işareti görürsünüz. Değerlendirme işlemi tamamlandığında, ilgili bilgilendirme simgesi görüntülenir:

-  Bağlantı verilen sayfa güvenli (*bu simge güvenli Yahoo! JP arama sonuçları*).
-  Bağlantılı sayfa tehlike içermiyor, ancak bazı şeyler şüpheli (*orijin ve davranış olarak şüpheli olduğundan e-alışveriş vb. için önerilmez*).
-  Bağlantılı sayfa güvenli olabilir, ancak şu anda doğrudan herhangi bir tehlike bulunmasa bile tehlikeli ya da kod olarak şüpheli olabilecek sayfalara bağlantılar içermekte.
-  Bağlantı verilen sayfa etkin tehlike içeriyor! Kendi güvenliğiniz için, bu sayfayı ziyaret etmenize izin verilmeyecek.
-  Bağlantılı sayfaya erişilemediğinden taranamadı.

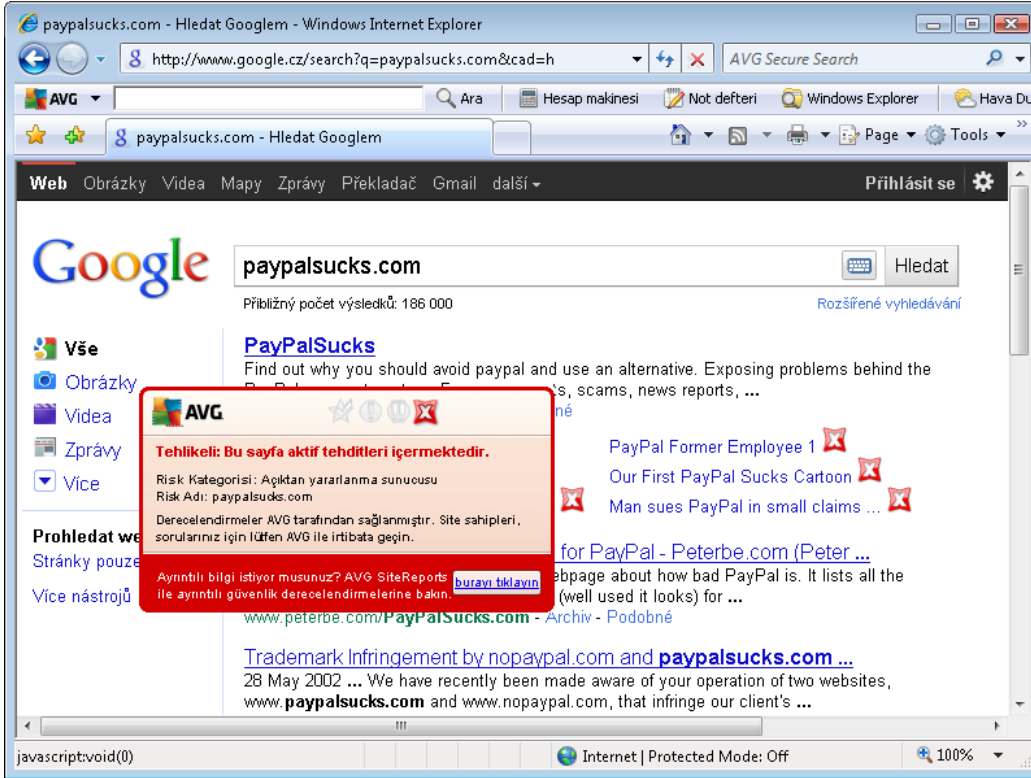
Tek tek değerlendirme simgesinin üzerine gelindiğinde, sorgulanan belirli bağlantıyla ilgili bilgiler gösterilir. Bilgiler, tehditle ilgili ek detayları (*varsa*) içerir:



6.2.3. Surf-Shield tespitleri

Bu güçlü koruma, açmaya çalıştığınız web sayfalarının kötü amaçlı içeriğini engeller ve bilgisayarınıza karşıdan yüklenmesini önler. Bu özellik etkin durumdayken, tehlikeli bir site bağlantısı tıklatıldığında ya da URL'si yazıldığında otomatik olarak web sayfasını açmanız engellenir, bu sayede etkilenmeniz önlenmiş olur. Etkilenen siteyi ziyaret ederek güvenlik açıkları olan web sayfalarının bilgisayarınızı kolaylıkla etkileyebileceğini unutmamak önemlidir, bu nedenle açıklardan yararlanma veya diğer ciddi tehlikeler içeren tehlikeli bir web sayfası isteğinde bulunduğunuzda, [LinkScanner](#), tarayıcınızın bu sayfayı göstermesine izin vermez.

Kötü amaçlı bir web sitesiyle karşılaşırsanız, [LinkScanner](#) sizi şuna benzer bir ekranla uyaracaktır:



Bu tür bir web sitesine girmek oldukça risklidir ve önerilemez!

6.2.4. Online Shield tespitleri

Online Shield ziyaret ettiğiniz web sitelerinin içeriklerini ve sitelerin içindeki muhtemel dosyaları, ilgili web sitesi henüz tarayıcınızda görünmeden ya da bilgisayarınıza indirmeden tarar. Bir tehdit tespit edilirse aşağıdaki iletişim kutusu vasıtasıyla hemen uyarılırsınız:



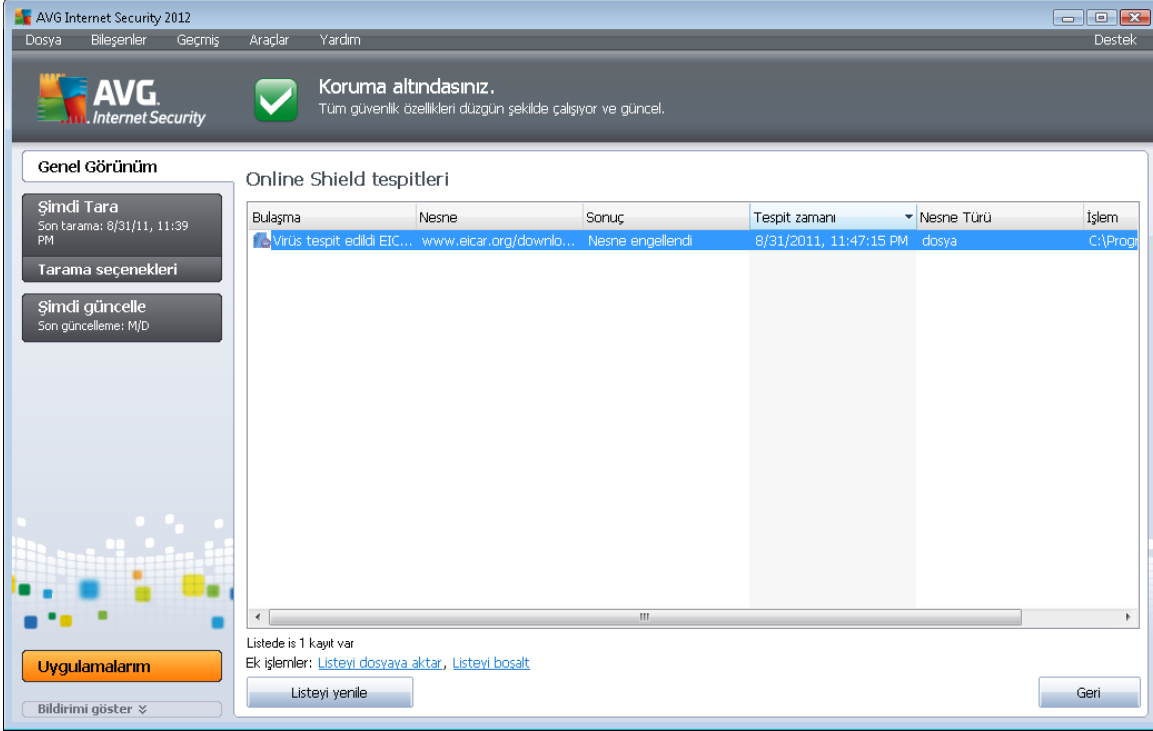
Bu iletişim kutusundan, tespit edilen ve bulaşmış (*Dosya adı*) olarak atanan dosya verilerini, tanınan bulaşmanın adını (*Tehdit adı*) ve (*biliniyorsa*) tespit edilen bulaşma ile ilgili ayrıntılı bilgiler edinebileceğiniz *Virüs ansiklopedisi*'ne yönlendiren bir bağlantı bulabilirsiniz. Bu iletişim kutusunda aşağıdaki düğmeler bulunur:

- **Ayrıntıları göster** - bulaşma tespit edildiğinde çalışan işlem ve işlemin tanımı ile ilgili bilgileri bulabileceğiniz yeni bir açılır pencere açmak için, **Ayrıntıları göster** düğmesini tıklayın.



- **Kapat** - uyarı iletişim kutusunu kapatmak için bu düğmeyi tıklayın.

Şüpheli web sayfası açılmayacaktır ve tehlike algılama **Online Shield bulguları** listesi günlüğüne alınacaktır - algılanan tehlikelere bu genel bakışa sistem menüsünün [Geçmiş / Web Shield Tespitleri](#) ögesinden erişilebilir.



Tespit edilen tüm nesnelere için aşağıdaki bilgiler verilir:

- **Bulaşma** - Algılanan nesnenin açıklaması (*Muhtemelen adı da*)
- **Nesne** - Nesne kaynağı (*web sayfası*)
- **Sonuç** - tespit edilen nesne ile gerçekleştirilen eylem
- **Algılama zamanı** - Tehlikenin algılandığı ve engellendiği tarih ve saat
- **Nesne Türü** - tespit edilen nesnenin türü
- **İşlem** - tespit edilmesi amacıyla potansiyel tehlike taşıyan nesneyi uyarı işlemidir

İletişim kutusunun alt kısmında, listenin altında yukarıda listelenen tespit edilen nesnelere toplam sayısı hakkında bilgi bulabilirsiniz. Buna ek olarak tespit edilen nesnelere listesini ayrı bir dosyaya dışarı aktarabilirsiniz (**Listeyi Dosyaya Aktar**) ve tespit edilen nesnelere hakkındaki tüm girişleri silebilirsiniz (**Listeyi Temizle**).

Kontrol düğmeleri



- **Listeyi yenile - Online Shield**
- **Geri** - varsayılan [AVG ana iletişim kutusuna](#) (bileşenlere genel bakış) geri döndürür

6.3. E-posta Koruması

Virüsler ve truva atları yaygın olarak e-postalar aracılığıyla yayılır. Yemleme ve istenmeyen postalar, e-postaları daha büyük risk kaynakları haline getirmektedir. Ücretsiz e-posta hesaplarının zararlı e-postaları alma ihtimali daha yüksek olup (*nadiren istenmeyen posta önleme teknolojisine sahip olmaları nedeniyle*) ev kullanıcıları büyük çoğunlukla söz konusu e-postaları kullanır. Bunun yanı sıra, bilmedikleri sitelerde dolaşan ve çevrimiçi formları kişisel bilgileri ile dolduran (*e-posta adresleri gibi*) ev kullanıcıları, e-posta saldırılarına sıklıkla maruz kalmaktadır. Şirketler genellikle kurumsal e-posta hesapları kullanmakta ve riskleri en aza indirmek için istenmeyen posta önleme filtrelerinden yararlanmaktadır.

E-posta Koruması bileşeni, alınan veya gönderilen her e-posta iletisini taramakla sorumludur. Bir e-postada virüs tespit edildiğinde, hemen [Virüs Kasasına](#) kaldırır. Söz konusu bileşen belirli türde e-posta eklerine filtre uygulayabilir ve virüs bulunmayan iletilere bir onay metni ekleyebilir. **E-posta Koruması** iki işlevden oluşur:

- [E-mail Scanner](#)
- [Anti-Spam](#)

6.3.1. E-posta Tarayıcısı

Kişisel E-posta Tarayıcısı bileşeni gelen/giden e-postaları otomatik olarak tarar. AVG'de kendi eklentisi olmayan e-posta istemcileri ile bunu kullanabilirsiniz (*ancak, AVG'nin desteklediği e-posta istemcilerinin, başka bir deyişle Microsoft Outlook ve The Bat istemcilerinin e-posta iletilerini tarayabilirsiniz*). Öncelikli olarak, Outlook Express, Mozilla, Incredimail, vb. gibi e-posta uygulamaları ile kullanılması gerekir.

[yüklemesi sırasında](#), e-posta kontrolü için oluşturulmuş otomatik sunucular bulunur: biri gelen e-postaları kontrol etmek, ikincisi ise giden e-postaları kontrol etmek içindir. Bu iki sunucu kullanılarak e-postalar otomatik olarak 110 ve 25 bağlantı noktalarında (*e-posta göndermek/almak için standart bağlantı noktaları*) kontrol edilir.

E-Posta Tarayıcısı Internet'te e-posta istemcisi ve e-posta sunucuları arasında arayüz olarak çalışır.

- **Gelen posta:** Sunucudan bir ileti alırken, **E-posta Tarayıcısı** bileşeni bunun virüs içerip içermediğini kontrol eder, virüslü ekleri kaldırır ve sertifika ekler. Tespit edildikleri zaman virüsler anında [Virüs Kasasında](#) karantina altına alınacaktır. Ardından ileti, e-posta istemcisine aktarılır.
- **Giden posta:** İleti e-posta istemcisinden E-posta Tarayıcısına gönderilir; o da iletiyi ve eklerinin virüslü olup olmadığını kontrol eder ve sonra mesajı SMTP sunucuna gönderir (*giden e-postaları tarama varsayılan olarak devre dışıdır ve elle ayarlanabilir*).

E-posta Tarayıcısının sunucu platformlarında kullanılması hedeflenmemiştir!



6.3.2. Anti-Spam

Anti-Spam nasıl çalışır?

Anti-Spam gelen tüm e-posta iletilerini denetler ve istenmeyen e-postaları istenmeyen posta olarak işaretler. **Anti-Spam** özel metin dizesi ekleyerek e-postanın konusunu değiştirebilir (*istenmeyen posta olarak tanımlanır*). Böylece, e-posta istemcinize göre e-postalarınızı filtreleyebilirsiniz. **Anti-Spam** bileşeni, her e-posta iletilisini işlemek için çeşitli inceleme yöntemleri kullanır ve istenmeyen e-postaları karşı mümkün olan en üst seviyede koruma sağlar. **Anti-Spam** istenmeyen postayı algılamak için düzenli olarak güncellenen veritabanı kullanır. [RBL sunucularını](#) kullanmak ("*bilinen istenmeyen posta göndericisi*") e-posta adreslerinden oluşan genel veritabanları ve [Beyaz listenize](#) (*hiçbir zaman istenmeyen posta olarak işaretleme*) ve [Kara listenize](#) (*her zaman istenmeyen posta olarak işaretle*) elle e-posta adresleri eklemek mümkündür.

Spam (istenmeyen e-posta) nedir?

Spam, ürün veya hizmet reklamı yapmak amacıyla bir seferde çok sayıda e-posta adresine toplu olarak gönderilen ve kullanıcıların posta kutularını dolduran istenmeyen e-postalardır. Spam, müşterinin kendi isteğiyle almayı kabul ettiği yasal ticari e-posta anlamına gelmez. Spam kişi için sıkıcı olmanın yanında genellikle aldatma, virüs veya saldırı amaçlı içerik de olabilir.

6.3.3. E-posta Koruması Arayüzü

E-Posta Koruması iletişim kutusunda bileşenlerin fonksiyonları ve mevcut durumu hakkında bilgi bulabilirsiniz (*Etkin*). Özel bir AVG web sitesi sayfasında (<http://www.avg.com/>), **AVG Internet**



Security 2012 faaliyetleri ve tespitleri hakkında ayrıntılı istatistikleri görmek **AVG'nin sizi nasıl koruduğuna dair çevrimiçi bir rapor görüntüleyin** bağlantısını tıkklatın.

Temel E-posta Koruması ayarları

E-posta Koruması iletişim kutusunda bileşenin işlevlerinin bazı temel özellikleriyle ilgili başka düzenlemeler yapabilirsiniz:

- **Gelen iletileri tara** (varsayılan olarak açık) - Hesabınıza teslim edilen tüm e-postalarda virüs taraması yapılması için bu öğeyi işaretleyin.
- **Giden iletileri tara** (varsayılan olarak kapalı) - Hesabınızdan gönderilen tüm e-postaların virüslere karşı taranmasını onaylamak için öğeyi işaretleyin.
- **E-posta taranırken bildirim penceresi görüntüle** (varsayılan olarak açık) - E-postanızın taranması sırasında [sistem tepsisinde AVG simgesi](#) üzerinde görüntülenen bildirim iletişim kutusu aracılığıyla bilgilendirilmek istediğinizi onaylamak için bu öğeyi işaretleyin..
- **Anti-Spam'i Etkinleştir** (varsayılan olarak açık) - Gelen e-postalarınızın istenmeyen e-postalara karşı filtrelenmesini istiyorsanız işaretleyin.

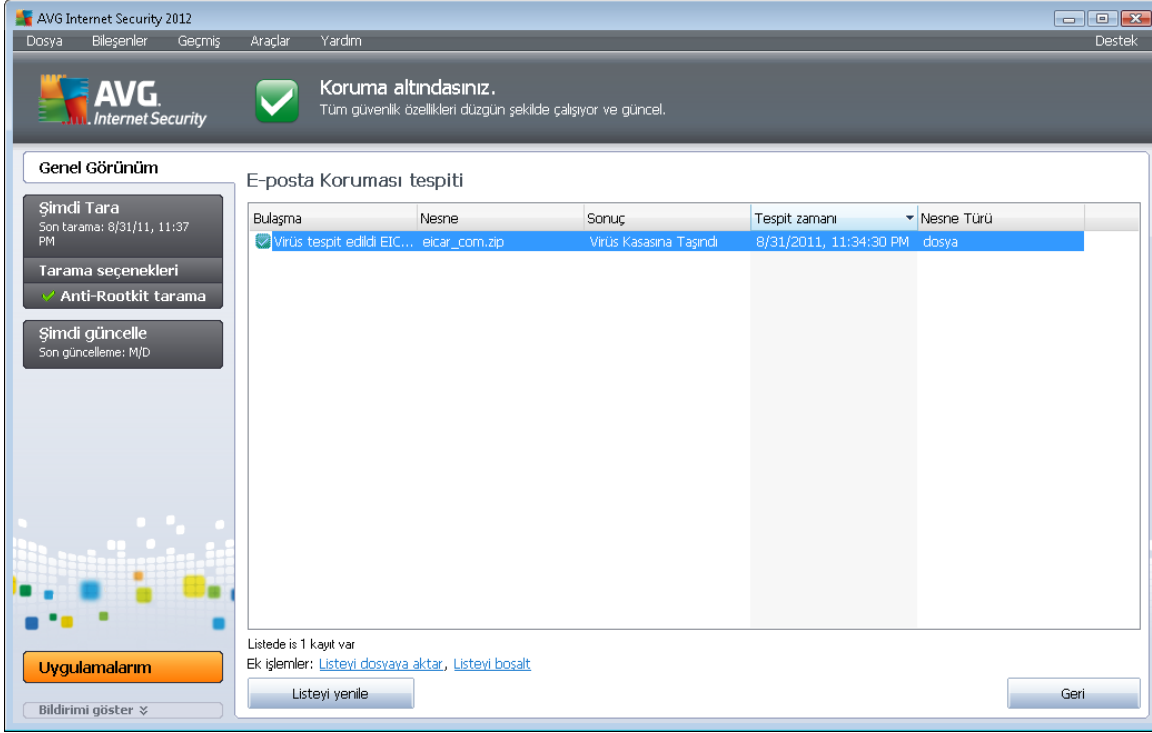
Yazılım satıcısı, en iyi performansın sunulabilmesi için tüm AVG bileşenlerini kurmuştur. Bunun için iyi bir nedeniniz olmadıkça AVG yapılandırmasını değiştirmeyin. Ayarlarda yapılacak her tür değişiklik sadece deneyimli bir kullanıcı tarafından gerçekleştirilmelidir. AVG yapılandırmasını değiştirmeniz gerekiyorsa sistem menüsü öğesi Araçlar/Gelişmiş ayarlar'ı seçin ve yeni açılan [AVG Gelişmiş Ayarlar](#) iletişim kutusunda AVG yapılandırmasını düzenleyin.

Kontrol düğmeleri

E-posta Koruması iletişim kutusunda bulunan kontrol düğmeleri şunlardır:

- **Değişiklikleri kaydet** bu iletişim kutusunda yapılan her tür değişikliği kaydetmek ve uygulamak için bu düğmeye basın
- **İptal** - varsayılan [AVG ana iletişim kutusuna](#) (bileşenlere genel bakış) dönmek için bu düğmeye basın

6.3.4. E-posta Koruması Tespitleri



Buluşma	Nesne	Sonuç	Tespit zamanı	Nesne Türü
✓	Virüs tespit edildi EIC... eicar_com.zip	Virüs Kasasına Taşındı	8/31/2011, 11:34:30 PM	dosya

E-mail Scanner tespiti iletişim kutusunda (*sistem menüsü seçeneği Geçmiş / E-mail Scanner tespiti üzerinden erişebilirsiniz*) [E-Posta Koruması](#) bileşeni tarafından tespit edilen tüm bulguların listesini görebilirsiniz. Tespit edilen tüm nesnelere ilişkin aşağıdaki bilgiler verilir:

- **Bulaşma** - Algılanan nesnenin açıklaması (Muhtemelen adı da)
- **Nesne** - nesnenin konumu
- **Sonuç** - tespit edilen nesne ile gerçekleştirilen eylem
- **Algılama zamanı** - Şüpheli nesnenin algılandığı tarih ve saat
- **Nesne Türü** - tespit edilen nesnenin türü

İletişim kutusunun alt kısmında, listenin altında yukarıda listelenen tespit edilen nesnelere ilişkin toplam sayısı hakkında bilgi bulabilirsiniz. Buna ek olarak tespit edilen nesnelere ilişkin listesini ayrı bir dosyaya dışarı aktarabilir (**Listeyi Dosyaya Aktar**) ve tespit edilen nesnelere ilişkin tüm girişleri silebilirsiniz (**Listeyi Temizle**).

Kontrol düğmeleri

E-posta Tarayıcısı algılama arayüzünde bulunan kontrol düğmeleri şunlardır:

- **Listeyi yenile** - Algılanan tehlikelerin listesini günceller.



- **Geri** - Sizi önce görüntülenen iletişim kutusuna geri döndürür.

6.4. Güvenlik Duvarı

Güvenlik Duvarı, trafiği engellemek/izin vermek suretiyle iki ya da daha fazla ağ arasında gerçekleşen erişimi kontrol eden bir sistemdir. **Güvenlik Duvarı** dahili ağı dışarıdan (*genellikle internetten*) kaynaklanan saldırılara karşı koruyan bir dizi kural içerir ve ağ bağlantı noktalarının her birinde gerçekleşen iletişimi kontrol eder. İletişim tanımlanan kurallar doğrultusunda değerlendirilir ve ardından söz konusu işleme izni verilir ya da engellenir. **Güvenlik Duvarı** sisteme yetkisiz girilmeye çalışıldığını tespit ederse söz konusu teşebbüs "engeller" ve söz konusu kişinin bilgisayarınıza erişimini engeller.

Güvenlik Duvarı, tanımlı yazılım uygulamaları için ve tanımlanan bağlantı yuvaları üzerinden dahili/ harici iletişime (her iki yönde, giriş ya da çıkış) izin vermek ya da engellemek üzere yapılandırılır. Örneğin, güvenlik duvarı, Microsoft Explorer kullanılarak sadece içeri ve dışarı veri akışına izin verecek şekilde de yapılandırılabilir. Diğer web tarayıcıları tarafından web verilerini aktarmaya yönelik teşebbüsler engellenecektir.

Güvenlik Duvarı, kişisel açıdan tanımlanabilir verilerin sizin izniniz olmaksızın bilgisayarınızdan gönderilmesini engeller. Bilgisayarın İnternet ya da yerel ağ üzerinden diğer bilgisayarlarla yaptığı veri değişimini kontrol eder. **Güvenlik Duvarı** kurumlarda ağa bağlı diğer bilgisayarları tek bir bilgisayar tarafından ortaya konan saldırılara karşı da korur.

Güvenlik Duvarı tarafından korunmayan bilgisayarlar bilgisayar korsanları ve kimlik hırsızları için kolay bir hedef haline gelir.

Öneri: Genellikle tek bir bilgisayarda birden fazla güvenlik duvarı kullanılmadı önerilmez. Birden fazla güvenlik duvarı kullanırsanız bilgisayarın güvenliği geliştirilemez. Bu iki uygulama arasında bazı çakışmaların oluşması mümkündür. Bu yüzden bilgisayarınızda yalnızca bir güvenlik duvarı kullanmanız ve diğer tümünün etkinliğini kaldırmanız önerilir, böylece olası çakışmalar ve bununla ilgili sorunlar ortadan kaldırılır.

6.4.1. Güvenlik Duvarı Prensipleri

AVG Internet Security 2012 uygulamasında, **Güvenlik Duvarı** bilgisayarınızdaki her ağ bağlantı noktasının trafiğini kontrol eder. **Güvenlik Duvarı**, tanımlanan kurallara bağlı olarak hem bilgisayarınızda çalışan (*ve internet/yerel ağ yoluyla bağlanmak isteyen*) uygulamaları hem de bilgisayarınıza bağlanmayı deneyerek dışarıdan bilgisayarınıza girmeye çalışan uygulamaları değerlendirir. **Güvenlik Duvarı** bu uygulamaların her biri için ağ bağlantı noktaları üzerinde iletişime izin verir ya da iletişimi yasaklar. Varsayılan olarak, uygulama bilinmiyorsa (*örneğin Güvenlik Duvarı kuralları tanımlanmamışsa*), **Güvenlik Duvarı** iletişim girişimine izin vermek veya girişimi engellemek isteyip istemediğinizi soracaktır.

AVG Güvenlik Duvarının sunucu platformlarında kullanılması hedeflenmemiştir!

AVG Güvenlik Duvarı ne yapabilir:

- Bilinen [uygulamaların](#) iletişim girişimlerine otomatik olarak izin verir veya bunları engeller ya da sizden onay ister



- İhtiyaçlarınıza uygun olarak önceden belirlenmiş kurallar içeren tam [profiller](#) kullanın
- [Çeşitli ağlara bağlanırken veya çeşitli ağ bağdaştırıcıları kullanırken otomatik olarak profilleri değiştirin](#)

6.4.2. Güvenlik Duvarı Profilleri

[Güvenlik Duvarı](#), bilgisayarınızın bir alanda bulunmasına, bağımsız bir bilgisayar veya bir dizüstü bilgisayar olmasına bağlı olarak özel güvenlik kuralları tanımlamanıza olanak tanır. Bu seçeneklerin her biri için farklı bir koruma seviyesi gerekir ve bu seviyeler de ilgili profillerin kapsamındadır. Kısaca, [Güvenlik Duvarı](#) Profili [Güvenlik Duvarı](#) bileşeni için özel bir yapılandırma ve bu şekilde önceden tanımlanmış çok sayıda yapılandırmayı kullanabilirsiniz.

Kullanılabilir profiller

- **Tümüne izin ver** - üretici tarafından önceden ayarlanan ve daima kullanılabilir olan bir [Güvenlik Duvarı](#) sistem profilidir. Bu profil etkinleştirildiği zaman tüm ağ iletişimine izin verilir ve güvenlik kuralları uygulanmaz çünkü [Güvenlik Duvarı](#) koruması kapatılmıştır (Diğer bir deyişle tüm uygulamalara izin verilir ancak paketler kontrol edilmeye devam eder- filtreleme işlemlerini tamamen engellemek için Güvenlik Duvarını tamamen kapatmanız gerekir). Sistem profili çoğaltılamaz, silinemez ve ayarları değiştirilemez.
- **Tümünü engelle** - üretici tarafından önceden ayarlanan ve daima kullanılabilir olan bir [Güvenlik Duvarı](#) sistem profilidir. Bu profil etkinleştirildiğinde, tüm ağ iletişimi engellenir, bilgisayara dış ağlardan erişilemez ve bilgisayar da dışarıya erişemez. Sistem profili çoğaltılamaz, silinemez ve ayarları da değiştirilemez.
- **Özel profiller** - özel profiller özellikle de sık sık çeşitli ağlara bağlanıyorsanız otomatik profil değiştirme özelliğinden yararlanmanızı sağlar (*örn. dizüstü bilgisayarlar*). Özel profiller **AVG Internet Security 2012** kurulumundan sonra otomatik olarak oluşturulur ve [Güvenlik Duvarı](#) politika kuralları için gereksinimleri karşılar. Mevcut özel profiller:
 - **İnternete doğrudan bağlı** - ortak masaüstü ev bilgisayarları veya internete ekstra koruma olmaksızın doğrudan bağlı dizüstü bilgisayarlar için uygundur. Seçenek dizüstü bilgisayarınızı çeşitli bilinmeyen ve muhtemelen güvenli de olmayan ağlara bağlarken önerilir (*internet kafe, otel odası vb.*). Bu profilin en sıkı [Güvenlik Duvarı](#) politikası kuralları bu tür bilgisayarların yeteri kadar korunmasını sağlar.
 - **Etki alanlı bilgisayar** - yerel bir ağdaki (tipik olarak okul ve işyeri ağı) bilgisayarlar için uygundur. Ağın profesyonel olarak yönetildiği ve bazı ek önlemlerle korunduğu var sayılır, bu nedenle güvenlik seviyesi yukarıda bahsedilen paylaşılan klasörlere, disk birimlerine vb. erişim izni veren durumlardan daha düşük olabilir.
 - **Küçük ev veya ofis ağı** - küçük bir ağdaki (tipik olarak ev veya küçük işletme ağı) bilgisayarlar için uygundur. Genellikle, bu türden ağlarda "merkez" yönetici yoktur ve yalnızca yazıcıyı, tarayıcıyı veya [Güvenlik Duvarı](#) kurallarının yansıtması gereken benzer cihazları paylaşan birbirine bağlı birden fazla bilgisayar bulunur.

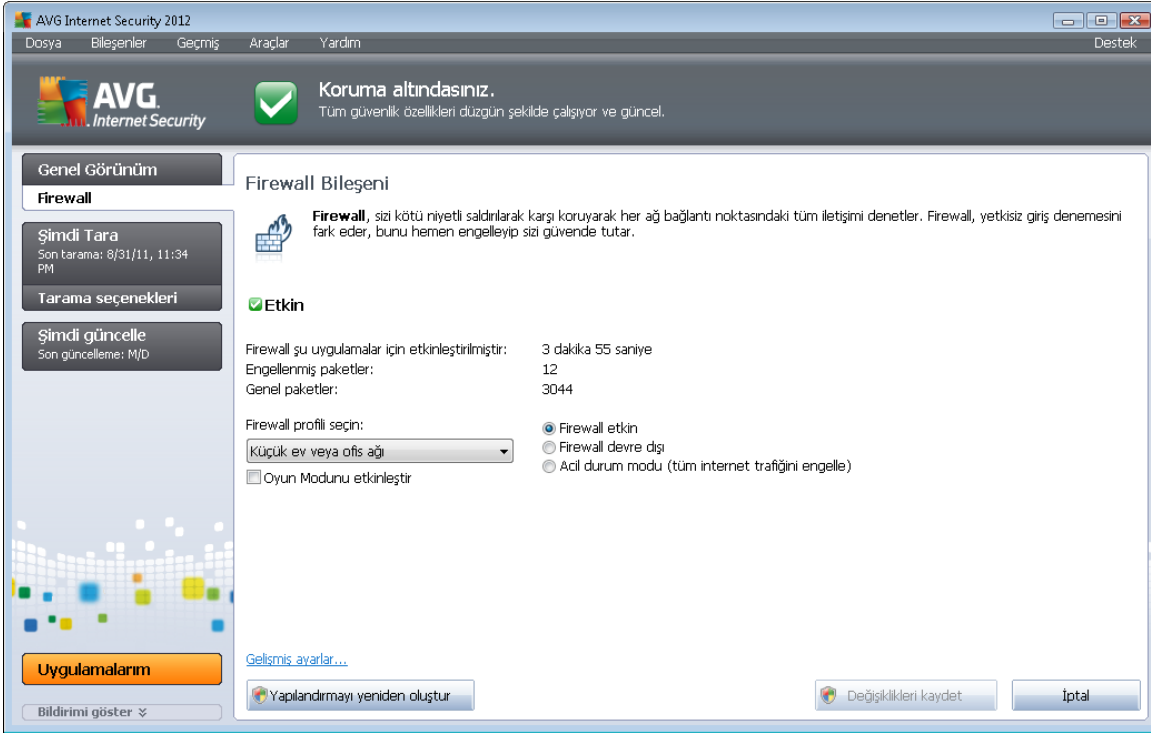
Profil Değiştirme



Profil Değiştirme özelliği, belli bir ağ bağdaştırıcısı kullanıldığında veya belli bir ağ türüne bağlanıldığında [Güvenlik Duvarının](#) otomatik olarak tanımlanan profile geçmesini sağlar. Ağ alanına henüz bir profil atanmadıysa, bu alana bir sonraki bağlantıda, Güvenlik Duvarı bir profil atanmasını belirten bir [iletişim kutusu](#) görüntüleyecektir. Tüm yerel ağ arabirimleri ve alanlarına profiller atayabilir ve [Alan ve Bağdaştırıcı Profilleri](#) iletişim kutusundan başka ayarlar belirleyebilirsiniz; ayrıca bu iletişim kutusunda, kullanmak istememeniz durumunda özelliği devre dışı bırakabilirsiniz (*ardından tüm bağlantı türleri için varsayılan profil kullanılacaktır*).

Genel olarak, dizüstü bilgisayar olan ve çeşitli bağlantı türleri kullanan kullanıcılar bu özelliği yararlı bulacaktır. Bir masaüstü bilgisayarınız varsa ve yalnızca bir bağlantı türü kullanıyorsanız (*örn. kablolu İnternet bağlantısı*), büyük ihtimalle hiç kullanmanız gerekmeyeceğinden profil değiştirme özelliği için endişelenmeniz gerekmeyecektir.

6.4.3. Güvenlik Duvarı Arayüzü



Güvenlik Duvarı Bileşeni olarak adlandırılan ana iletişim kutusu bileşenin işlevi hakkında temel bilgileri, bileşenin durumunu (*Etkin*) bileşen istatistiklerine kısa bir genel bakış sağlar:

- **Güvenlik Duvarı etkinleştirildi** - [Güvenlik Duvarı](#) çalıştırıldığından beri geçen süre
- **Engellenen paketler** - kontrol edilen tüm paketler içinde engellenen paket sayısı
- **Paketlerin tamamı** - [Güvenlik Duvarı](#) çalışırken taranan toplam paket sayısı

Temel Güvenlik Duvarı ayarları

- **Güvenlik Duvarı profili seç** - açılır menüden tanımlı bir profil seçin (*profillerin ayrıntılı açıklaması ve önerilen kullanımı için [Güvenlik Duvarı Profilleri](#) bölümüne bakın*)
- **Oyun Modunu etkinleştir** - Tam ekran uygulamalar (*oyunlar, sunumlar, filmler vs.*) çalışırken, [Güvenlik Duvarının](#) bilinmeyen uygulamalarla ilgili iletişime izin vermek isteyip istemediğinizi soran iletişim kutularının görüntülenmemesi için bu seçeneği işaretleyin. Söz konusu anda bilinmeyen bir uygulamanın ağ üzerinden başka bir programla iletişim kurmaya çalışması halinde [Güvenlik Duvarı](#) mevcut profildeki ayarlara göre ilgili teşebbüse otomatik olarak izin verecek ya da bu teşebbüsü engelleyecektir. **Not:** Oyun modu etkin haldeyken, zamanlanan tüm görevler (taramalar, güncellemeler) uygulama kapatılana kadar ertelenecektir.
- Ayrıca, bu temel ayarlar bölümünde [Güvenlik Duvarı](#) bileşenin geçerli durumunu tanımlayan üç seçenekten birini seçebilirsiniz:
 - **Güvenlik Duvarı etkin** (*varsayılan olarak*) - bu seçeneği belirleyerek seçili [Güvenlik Duvarı](#) profilinde tanımlanan kurallar dizisi kapsamında "izin verilen" uygulamalarla iletişim kurulmasına olanak vermiş olursunuz.
 - **Güvenlik duvarı devre dışı** - bu seçenek [Güvenlik Duvarı](#)'nı tamamen kapatır ve tüm ağ trafiğine izin verilir ancak denetlenmez!
 - **Acil durum modu (Tüm Internet trafiğini engeller)** - bu seçeneği belirleyerek her ağ bağlantı noktasındaki trafiğin tümünü engellersiniz; [Güvenlik Duvarı](#) hala çalışır ancak tüm ağ trafiği durdurulur.

Lütfen unutmayın: Yazılım satıcısı tüm AVG Internet Security 2012 bileşenlerini optimum performans sağlayacak şekilde ayarlamıştır. Bunun için iyi bir nedeniniz olmadıkça AVG yapılandırmasını değiştirmeyin. Ayarlarda yapılacak her tür değişiklik sadece deneyimli bir kullanıcı tarafından gerçekleştirilmelidir. Güvenlik Duvarı konfigürasyonunu değiştirmeniz gerekiyorsa sistem menüsünden **Araçlar/Güvenlik duvarı ayarları** ögesini seçin ve yeni açılan [Güvenlik Duvarı Ayarları](#) iletişim kutusunda Güvenlik duvarı yapılandırmasını düzenleyin.

Kontrol düğmeleri

- **Yapılandırmayı yeniden oluştur** - geçerli [Güvenlik Duvarı](#) yapılandırmasının üzerine yazmak ve otomatik tespite bağlı olarak varsayılan yapılandırmaya geri dönmek için bu düğmeye basın.
- **Değişiklikleri kaydet** bu iletişim kutusunda yapılan her tür değişikliği kaydetmek ve uygulamak için bu düğmeye basın.
- **İptal** - varsayılan [AVG ana iletişim kutusuna](#) (*bileşenlere genel bakış*) dönmek için bu düğmeye basın.



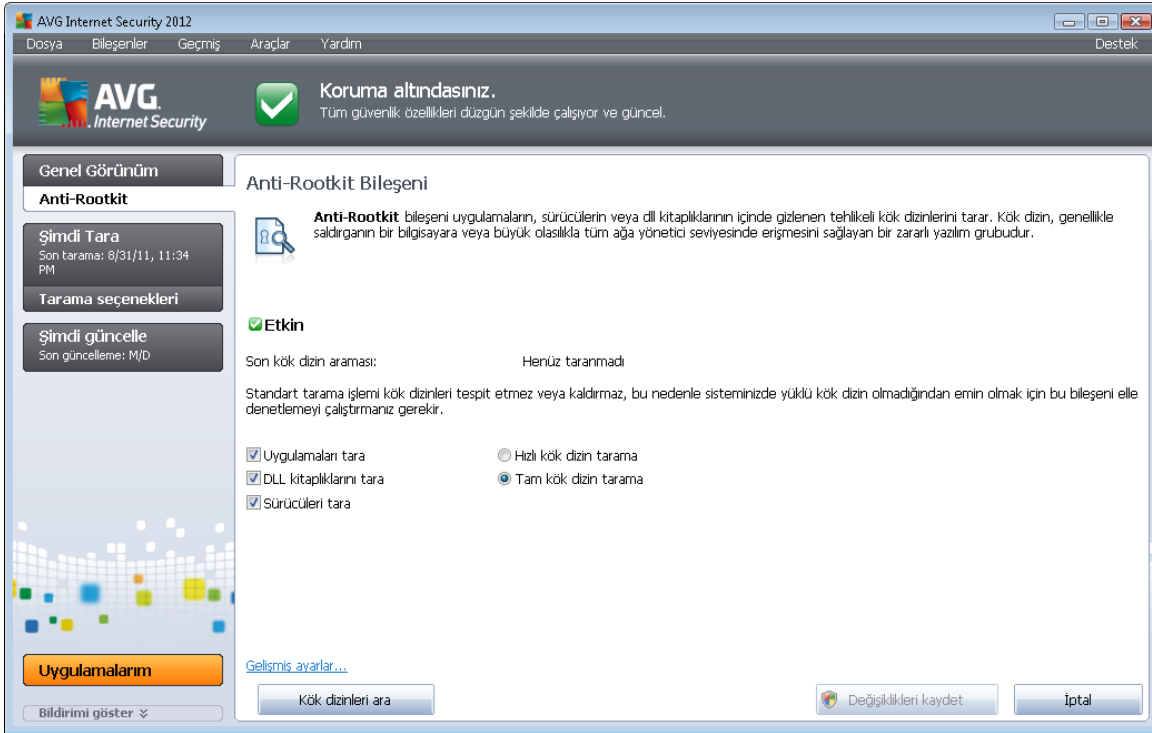
6.5. Anti-Rootkit

Anti-Rootkit tehlikeli kök dizinleri, diğer bir deyişle bilgisayarınızdaki tehlikeli yazılımları gizleyen program ve teknolojileri etkili bir biçimde tespit edip silen özel bir araçtır. **Anti-Rootkit** öntanımlı kurallar setine göre rootkit'leri algılayabilir. Lütfen tüm kök dizinlerin tespit edildiğini (*sadece bulaşanlar değil*) unutmayın. **Anti-Rootkit** bir kök dizini bulduğunda, bu kök dizinde mutlaka virüs olduğu anlamına gelmez. Bazen kök dizinleri sürücülerde kullanılır ya da doğru uygulamaların bir parçası olabilir.

Kök dizin nedir?

Kök dizin (rootkit), sistem yöneticisinin izni olmaksızın yasal olmayan şekillerde bilgisayar sisteminin kontrolünü ele almak için tasarlanmış bir programdır. Kök dizin, donanım üzerinde çalışan işletim sisteminin kontrolünü ele geçirmeyi hedeflediği için donanımsal açıdan erişime gerek duymaz. Kök dizinler genellikle standart işletim sisteminin güvenlik mekanizmalarını dönüştürerek ya da istila ederek sistem üzerindeki varlıklarını gizlerler. Çoğunlukla Truva Atı biçimindedirler, dolayısıyla kullanıcıları sistemleri üzerinden çalışacak kadar güvenli olduklarına inandırırılar. İzleme programlarının çalışan işlemlerini gizlemek ya da işletim sisteminin sistem bilgilerini ya da dosyalarını saklamak, bunu sağlamak için kullanılan teknikler arasında bulunmaktadır.

6.5.1. Anti-Rootkit Arayüzü



Anti-Rootkit iletişim kutusu bileşenlerin işlevleri ile ilgili kısa bir açıklama sağlar, bileşenin mevcut durumu konusunda bilgilendirir (*Etkin*) ve **Anti-Rootkit** testinin en son başlatıldığı zamanla ilgili bilgiler de verir (*Son kök dizin araması*). **Anti-Rootkit** iletişim kutusu [Araçlar/Gelişmiş Ayarlar](#) bağlantısını da sağlar. **Anti-Rootkit** bileşeninin gelişmiş yapılandırma ortamına yönlendirilmek için



bu bağlantıyı kullanın.

Yazılım satıcısı, en iyi performansın sunulabilmesi için tüm AVG bileşenlerini kurmuştur. Bunun için iyi bir nedeniniz olmadıkça AVG yapılandırmasını değiştirmeyin. Ayarlarda yapılacak her tür değişiklik sadece deneyimli bir kullanıcı tarafından gerçekleştirilmelidir.

Temel Anti-Rootkit ayarları

Kök dizin mevcudiyet taramasının bazı temel işlevlerini iletişim kutusunun en alt kısmında ayarlayabilirsiniz. Öncelikle, taranmasını istediğiniz nesnelere belirlemek üzere ilgili kutuları işaretleyin:

- **Uygulamaları tara**
- **DLL kitaplıklarını tara**
- **Sürücülerini tara**

Bunun ardından kök dizin tarama modunu da seçebilirsiniz:

- **Hızlı kök dizin tarama** - Çalışan tüm işlemleri, yüklü sürücülerini ve sistem klasörlerini (genellikle c:\Windows) tarar.
- **Tam kök dizin tarama** - Çalışan tüm işlemleri, yüklü sürücülerini, sistem klasörünü (genellikle c:\Windows), ayrıca tüm yerel diskleri (flash disk dahil, ancak disket/CD sürücülerini hariç) tarar.

Kontrol düğmeleri

- **Kök dizinleri tara** - Kök dizin tarama işlemi [Tüm bilgisayarın taranması](#) işlevinin temel bir parçası olmadığı için, kök dizin taramasını bu düğmeyi kullanarak doğrudan **Anti-Rootkit** arayüzünden başlatabilirsiniz.
- **Değişiklikleri kaydet** - Bu arayüzde yapılan tüm değişiklikleri kaydetmek ve varsayılan [AVG ana iletişim kutusuna](#) (bileşenlere genel bakış) dönmek için bu düğmeye basın.
- **İptal** - Yapılan değişiklikleri kaydetmeksizin varsayılan [AVG ana iletişim kutusuna](#) (bileşenlere genel bakış) dönmek için bu düğmeye basın.

6.6. Sistem Araçları

Sistem Araçları AVG Internet Security 2012 ortamının ve işletim sisteminin ayrıntılı bir özeti sunan araçlardır. Bileşen şunlara genel bakış sağlar:

- [İşlemler](#) - bilgisayarınızda o anda etkin işlemlerin (yani, çalışan uygulamaların) listesidir
- [Ağ bağlantıları](#) - Geçerli olarak etkin bağlantıların listesi



- [Otomatik başlat](#) - Windows sistem başlatma sırasında çalıştırılan tüm uygulamaların listesi
- [Tarayıcı Uzantıları](#) - İnternet tarayıcınıza yüklü eklentilerin (örn. uygulamalar) listesidir
- [LSP Görüntüleyici](#) - Katmanlı Hizmet Sağlayıcıların (LSP) listesidir

Ayrıca, belirli genel görünümler değiştirilebilir ancak bu işlemin sadece çok deneyimli kullanıcılar tarafından yapılması önerilir!

6.6.1. İşlemler

Güvenlik Seviyesi	İşlem adı	İşlem yolu	Pencere	P
■ ■ ■ ■	SYSTEM	SYSTEM		4
■ ■ ■ ■	SIDEBAR.EXE	C:\PROGRAM FILES\WINDOWS SIDEBAR\SIDEBAR.EXE		12
■ ■ ■ ■	MDM.EXE	C:\PROGRAM FILES\COMMON FILES\MICROSOFT SHARED\VS7DEBUG\MDM.EXE		27
■ ■ ■ ■	WMIPRVSE.EXE	C:\WINDOWS\SYSTEM32\WBEM\WMIPRVSE.EXE		421
■ ■ ■ ■	SMSS.EXE	C:\WINDOWS\SYSTEM32\SMSS.EXE		39
■ ■ ■ ■	VMWARETRAY.EXE	C:\PROGRAM FILES\VMWARE\VMWARE TOOLS\VMWARETRAY.EXE		42
■ ■ ■ ■	AVGRSX.EXE	C:\PROGRAM FILES\AVG\AVG2012\AVGRSX.EXE		42
■ ■ ■ ■	AVGCSRVSX.EXE	C:\PROGRAM FILES\AVG\AVG2012\AVGCSRVSX.EXE		46
■ ■ ■ ■	VMWAREUSER.EXE	C:\PROGRAM FILES\VMWARE\VMWARE TOOLS\VMWAREUSER.EXE		62
■ ■ ■ ■	AVGTRAY.EXE	C:\PROGRAM FILES\AVG\AVG2012\AVGTRAY.EXE		63
■ ■ ■ ■	CSRSS.EXE	C:\WINDOWS\SYSTEM32\CSRSS.EXE		67

İşlemler iletişim kutusunda, bilgisayarınızda o anda aktif olan işlemlerin (çalışan uygulamaların) bir listesi bulunur. Liste birkaç sütuna ayrılmıştır:

- **Önem Düzeyi Seviyesi** - önem düzeyini en az önemli olandan (■ ■ ■ ■) en önemliye (■ ■ ■ ■) kadar dört seviyeli ölçekte, ilgili sürecin grafiksel olarak tanımlanmasıdır
- **İşlem adı** - çalışan işlemin adıdır
- **İşlem yolu** - çalışan işlemin fiziksel yoludur
- **Pencere** - mevcut ise uygulamanın pencere adını gösterir
- **PID** - işlem tanımlama numarası, benzersiz bir Windows işlem tanımlayıcısıdır

Kontrol düğmeleri



İşlemler sekmesinde bulunan kontrol düğmeleri şunlardır:

- **Yenile** - Geçerli duruma göre işlemlerin listesini günceller
- **İşlemi Sonlandır** - Bir veya daha fazla uygulama seçebilir ve sonra bu düğmeye basarak bunları sonlandırabilirsiniz. **Gerçek bir tehdit oluşturduklarından tam olarak emin olmadıkça, bağlantıları sonlandırmamanızı öneririz.**
- **Geri** - sizi varsayılan [AVG ana iletişim kutusuna](#) (bileşenlere genel bakış) geri döndürür

6.6.2. Ağ Bağlantıları

Uygulama	Protokol	Yerel Adres	Uzak Adres	Durum
[Sistem İşlemi]	UDP	AutoTest-VST32:138		
[Sistem İşlemi]	TCP	AutoTest-VST32:139	AutoTest-VST32:0	Dinliyor
[Sistem İşlemi]	TCP	AutoTest-VST32:445	AutoTest-VST32:0	Dinliyor
[Sistem İşlemi]	TCP6	[0:0:0:0:0:0:0:0]:445	[0:0:0:0:0:0:0:0]:0	Bilinmiyor
[Sistem İşlemi]	TCP	AutoTest-VST32:49187	192.168.183.1:445	Bağlandı
[Sistem İşlemi]	UDP	AutoTest-VST32:137		
[Sistem İşlemi]	TCP6	[0:0:0:0:0:0:0:0]:5357	[0:0:0:0:0:0:0:0]:0	Bilinmiyor
[Sistem İşlemi]	TCP	AutoTest-VST32:5357	AutoTest-VST32:0	Dinliyor
wininit.exe	TCP6	[0:0:0:0:0:0:0:0]:49152	[0:0:0:0:0:0:0:0]:0	Bilinmiyor
wininit.exe	TCP	AutoTest-VST32:49152	AutoTest-VST32:0	Dinliyor
svchost.exe	UDP6	[0:0:0:0:0:0:0:0]:5355	[0:0:0:0:0:0:0:0]:0	Bilinmiyor
svchost.exe	TCP6	[0:0:0:0:0:0:0:0]:49154	[0:0:0:0:0:0:0:0]:0	Bilinmiyor
svchost.exe	UDP	AutoTest-VST32:500		
svchost.exe	UDP6	[0:0:0:0:0:0:0:0]:500		
svchost.exe	UDP	AutoTest-VST32:5355		
svchost.exe	UDP6	[0:0:0:0:0:0:0:1]:64015		
svchost.exe	UDP	AutoTest-VST32:1900		
svchost.exe	TCP6	[0:0:0:0:0:0:0:0]:49156	[0:0:0:0:0:0:0:0]:0	Bilinmiyor
svchost.exe	UDP	AutoTest-VST32:64017		

Ağ Bağlantıları iletişim kutusu, geçerli etkin bağlantıların listesini görüntüler. Liste aşağıdaki sütunlara bölünmüştür:

- **Uygulama** - bağlantıyla ilgili uygulamanın adıdır (*Windows 2000'de bu bilgilere ulaşılamaz*)
- **Protokol** - bağlantı sırasında kullanılan aktarım protokolü türü:
 - TCP - İnternet üzerinden veri aktarımı yapabilmek için İnternet protokolü (IP) ile birlikte kullanılan protokol
 - UDP - TCP protokolüne alternatif
- **Yerel adres** - yerel bilgisayarın IP adresi ve kullanılan bağlantı noktası numarası
- **Uzak adres** - uzak bilgisayarın IP adresi ve bağlandığı bağlantı noktası numarası



Mümkünse, uzak bilgisayarın barındırıcı adını da gösterecektir.

- **Durum** - en muhtemel mevcut durumu görüntüler (*Bağlı, Sunucu kapatılmaldır, Dinlemede, Aktif kapanma tamamlandı, Pasif kapalı, Aktif kapalı*)

Yalnızca harici bağlantıları listelemek için, listenin altındaki iletişim kutusunun alt bölümündeki **Yerel bağlantıları gizle** onay kutusunu işaretleyin.

Kontrol düğmeleri

Ağ Bağlantıları sekmesinde bulunan kontrol düğmeleri şunlardır:

- **Bağlantıyı Sonlandır** - Listeden seçilen bir ya da daha fazla bağlantıyı sonlandırır
- **İşlemi Sonlandır** - listeden seçilen bağlantılarla ilgili bir veya daha fazla uygulamayı kapatır
- **Geri** - varsayılan [AVG ana iletişim kutusuna](#) (bileşenlere genel bakış) geri döndürür .

Kimi zaman bağlı durumda sadece uygulamaların sonlandırılması mümkün olmaktadır. Gerçek bir tehdit oluşturduklarından tam olarak emin olmadıkça, bağlantıları sonlandırmamanızı öneririz.

6.6.3. Otomatik başlat

Adı	Konum	Yol
WindowsWelcomeCenter	\REGISTRY\USER\S-1-5-20\Software\Micr...	rundll32.exe oobefldr.dll,ShowWelcomeCen...
Sidebar	\REGISTRY\USER\S-1-5-20\Software\Micr...	%ProgramFiles%\Windows Sidebar\Sidebar...
vProt	\REGISTRY\MACHINE\SOFTWARE\Microso...	"C:\Program Files\AVG Secure Search\vprot...
WindowsWelcomeCenter	\REGISTRY\USER\S-1-5-19\Software\Micr...	rundll32.exe oobefldr.dll,ShowWelcomeCen...
C:\Windows\system32\mshta.exe "%1"...	\REGISTRY\MACHINE\SOFTWARE\Classes...	C:\Windows\system32\mshta.exe "%1" %*
SilkTest Agent	\REGISTRY\MACHINE\SOFTWARE\Microso...	"C:\Automation\startagent.bat"
AVG_TRAY	\REGISTRY\MACHINE\SOFTWARE\Microso...	"C:\Program Files\AVG\AVG2012\avgtray.exe"
VMware User Process	\REGISTRY\MACHINE\SOFTWARE\Microso...	"C:\Program Files\VMware\VMware Tools\V...
Sidebar	\REGISTRY\USER\S-1-5-21-2323238519-...	C:\Program Files\Windows Sidebar\sideb...e...
SHELL	\INI\system.ini\BOOT\SHELL	SYS:Microsoft\Windows NT\CurrentVersion...
VMware Tools	\REGISTRY\MACHINE\SOFTWARE\Microso...	"C:\Program Files\VMware\VMware Tools\V...
hffsrsv	\REGISTRY\MACHINE\SOFTWARE\Microso...	c:\windows\hffext\hffsrsv.exe
Adobe Reader Speed Launcher	\REGISTRY\MACHINE\SOFTWARE\Microso...	"C:\Program Files\Adobe\Reader 8.0\Reade...
Sidebar	\REGISTRY\USER\S-1-5-19\Software\Micr...	%ProgramFiles%\Windows Sidebar\Sideb...
Appinit_DLLs	\REGISTRY\MACHINE\SOFTWARE\Microso...	qaphooks.dll

Otomatik başlat iletişim penceresinde, Windows sistemi başlatılırken yürütülen tüm uygulamaların listesini gösterir. Genellikle, birçok zararlı uygulama kendini otomatik olarak başlangıç kayıt defteri



girişine ekler.

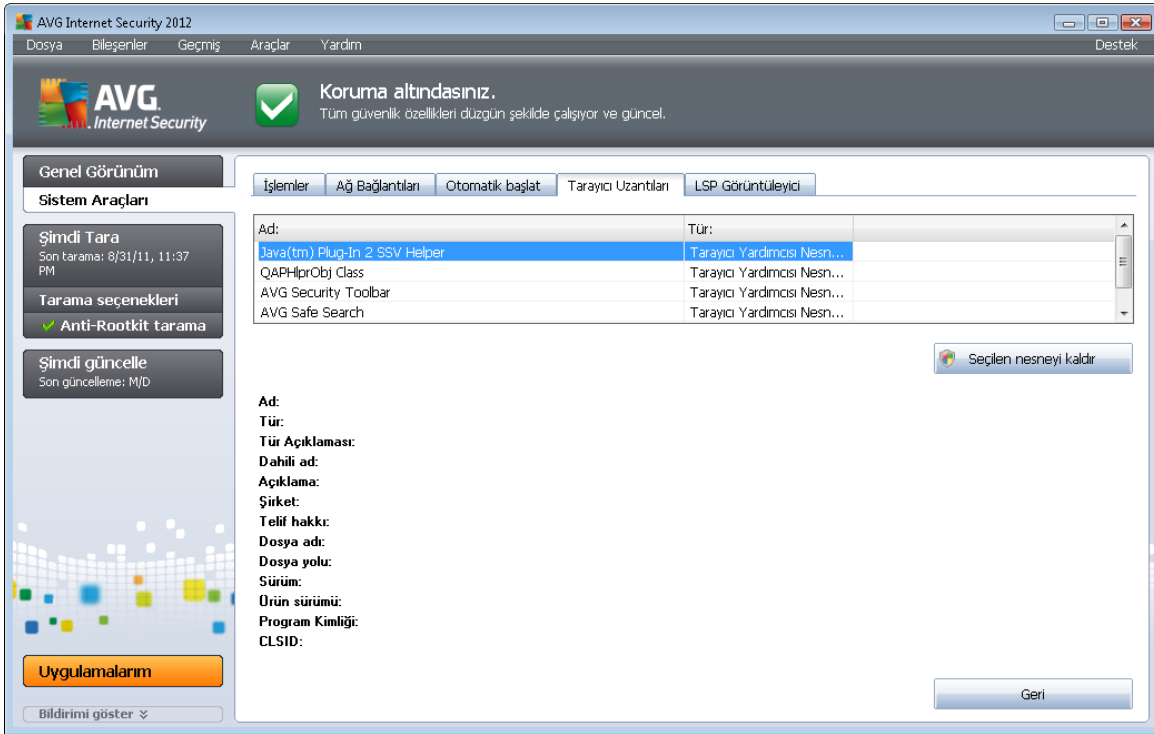
Kontrol düğmeleri

Otomatik başlat sekmesinde bulunan kontrol düğmeleri şunlardır:

- **Seçileni kaldır** - seçilen bir veya daha fazla girişi silmek için düğmeye basın.
- **Geri** - sisi varsayılan [AVG ana iletişim kutusuna](#) (bileşenlere genel bakışa) geri döndürür.

Gerçek bir tehdit oluşturduklarından tam olarak emin olmadıkça, listedeki uygulamaları silmemenizi öneririz.

6.6.4. Tarayıcı Uzantıları



Tarayıcı Uzantıları iletişim kutusunda İnternet tarayıcınıza yüklenen eklentilerin listesi (yani *uygulamalar*) bulunur. Bu liste, normal uygulama eklentilerini ve potansiyel kötü amaçlı programları içerebilir. İletişim kutusunun alt bölümünde görüntülenecek seçili eklenti hakkında ayrıntılı bilgi edinmek için listedeki bir nesneyi tıklayın.

Kontrol düğmeleri

Tarayıcı Uzantıları sekmesinde bulunan kontrol düğmeleri şunlardır:

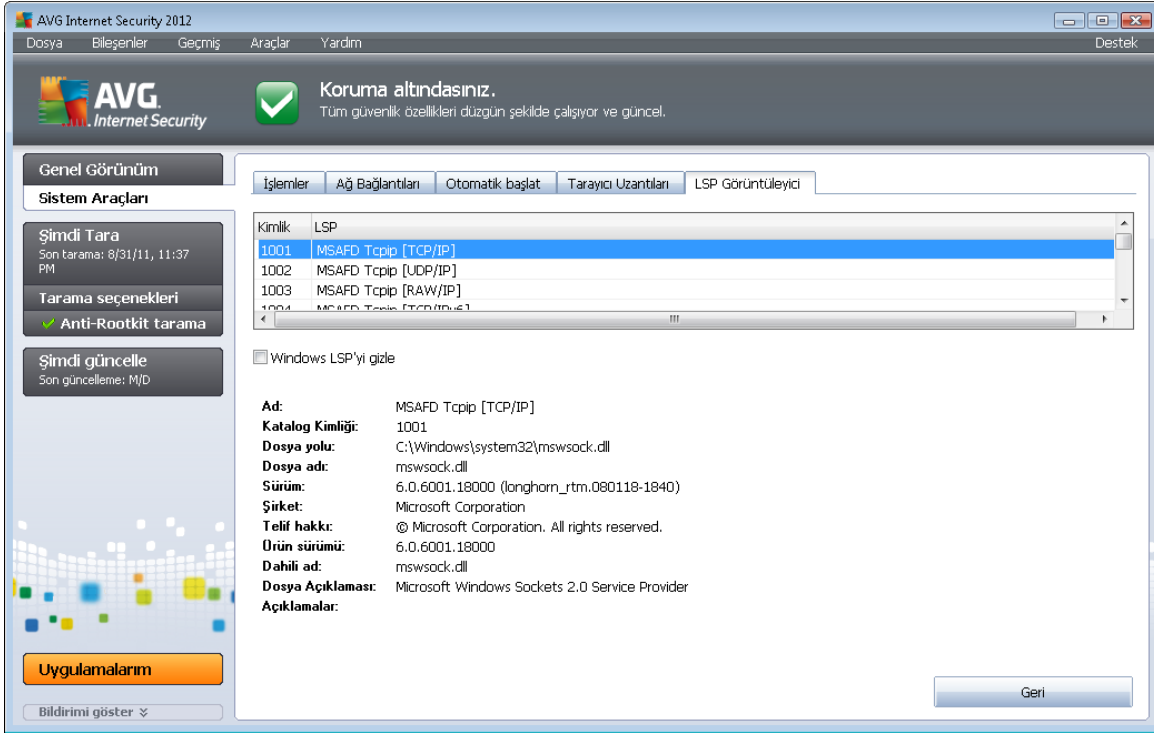
- **Seçili nesneyi kaldır** - Listede geçerli olarak vurgulanan eklentiyi kaldırır. **Gerçek bir**



tehdit oluşturduklarından tam olarak emin olmadıkça, listedeki eklentileri silmemenizi öneririz.

- **Geri** - sizi varsayılan [AVG ana iletişim kutusuna](#) (bileşenlere genel bakışa) geri döndürür.

6.6.5. LSP Görüntüleyici



LSP Görüntüleyici iletişim kutusu, Katmanlı Hizmet Sağlayıcıların (LSP) listesini görüntüler.

Katmanlı Hizmet Sağlayıcı (LSP), Windows işletim sisteminin ağ hizmetlerine bağlanan bir sistem sürücüsüdür. Bilgisayara giren ve bilgisayardan çıkan tüm verilere erişimi olduğu gibi, bu verileri değiştirebilme özelliği de vardır. Windows'un İnternet de dahil olmak üzere başka bilgisayarlara bağlanmanıza izin vermesi için bazı LSP'ler gereklidir. Ancak, bazı kötü niyetli uygulamalar da kendilerini bir LSP gibi göstererek yüklenebilir ve bilgisayarınızın aktardığı tüm verilere erişim sağlayabilir. Bu nedenle, bu inceleme tüm olası LSP tehditlerini kontrol etmenize yardımcı olabilir.

Bazı şartlar altında, bozulan LSP'leri onarmak da mümkündür (*örneğin, dosya kaldırıldığında ancak kayıt defteri girişlerine dokunulmadığında*). Onarılabilir bir LSP bulunduğu anda, sorunun giderilmesi için yeni bir düğme görüntülenir.

Kontrol düğmeleri

LSP Görüntüleyici sekmesinde bulunan kontrol düğmeleri şunlardır:

- **Windows LSP'yi gizle** - Windows LSP'yi listeye eklemek için bu seçeneğin işaretini kaldırın.



- **Geri** - sizi varsayılan [AVG ana iletişim kutusuna](#) (bileşenlere genel bakış) geri döndürür.

6.7. PC Analyzer

PC Analyzer bileşeni bilgisayarınızı sistem sorunları açısından tarayabilir ve size bilgisayarınızın genel performansını düşürebilecek öğelerin şeffaf bir genel görünümünü verebilir. Bileşenin kullanıcı arayüzünde, ilgili kategorileri (yani kayıt defteri hatalarını, gereksiz dosyaları, bölümlendirmeyi ve bozuk kısayolları) gösteren dört satıra ayrılmış bir tablo görebilirsiniz:

Kategorisi	Hatalar	Önem derecesi
Kayıt Defteri Hataları Hatalar sistem kararlılığını etkiler		
Gereksiz Dosyalar Bu dosyalar disk alanını doldurur		
Parçalanma Disk erişim hızını düşürür		
Bozuk Kısayollar Gezginin tarama hızını düşürür		

- **Kayıt Defteri Hataları**, size Windows Kayıt Defterindeki hata sayısını verir. Kayıt Defterini onarmak, oldukça yüksek bilgi gerektirdiğinden, kendi kendinize denemenizi veya onarmanızı önermeyiz.
- **Gereksiz Dosyalar**, mevcut olmasa da çalışabileceğiniz dosyaların sayısını size verir. Normal olarak, bunlar çeşitli türlerde geçici dosyalar ve Geri Dönüşüm Kutusundaki dosyalar olabilir.
- **Bölümlendirme**, bölümlendirilmiş sabit disk yüzdesini hesaplar, başka bir deyişle, dosyalar artık fiziksel diskin farklı parçalarına dağıtılmıştır. Bu sorunu gidermek için bazı bölümlendirme araçları kullanabilirsiniz.
- **Bozuk Kısayollar**, artık çalışmayan, mevcut olmayan konumlara karşılık gelen vb. kısayolları size bildirir.

Sisteminizi analiz etmeye başlamak için, **Şimdi analiz et** düğmesine basın. Bundan sonra, analiz sürecini ve sonuçlarını söz konusu tabloda doğrudan izleyebilirsiniz:



Kategorisi	Hatalar	Önem derecesi
Kayıt Defteri Hataları Hatalar sistem kararlılığını etkiler	138 hata bulundu Ayrıntılar...	
Önemsiz Dosyalar Bu dosyalar disk alanını doldurur	233 hata bulundu Ayrıntılar...	
Parçalanma Disk erişim hızını düşürür	10% parçalanmış Ayrıntılar...	
Bozuk Kısayollar Gezginin tarama hızını düşürür	13 hata bulundu Ayrıntılar...	

Sonuçlar genel görünüm, tespit edilen sistem sorunlarının (**Hatalar**) sayısını, test edilen ilgili kategorilere göre verir. Analiz sonuçları **Önem Düzeyi** sütununda bir eksen üzerinde grafiksel olarak da görüntülenecektir.

Kontrol düğmeleri

- **Şimdi analiz et** (analiz başlamadan önce görüntülenir) - bilgisayarınızın analizini hemen başlatmak için bu düğmeye basın
- **Şimdi onar** (analiz tamamlandıktan sonra görüntülenir) - AVG web sitesinin (<http://www.avg.com/>) sayfaya **PC Analyzer** bileşeni ile ilgili ayrıntılı ve güncel bilgiler vermesi için bu düğmeye basın
- **İptal** - analiz çalışmasını durdurmak veya analiz tamamlandıktan sonra varsayılan [AVG ana iletişim kutusuna](#) (bileşenler genel görünümüne) geri dönmek için bu düğmeye basın

6.8. Identity Protection

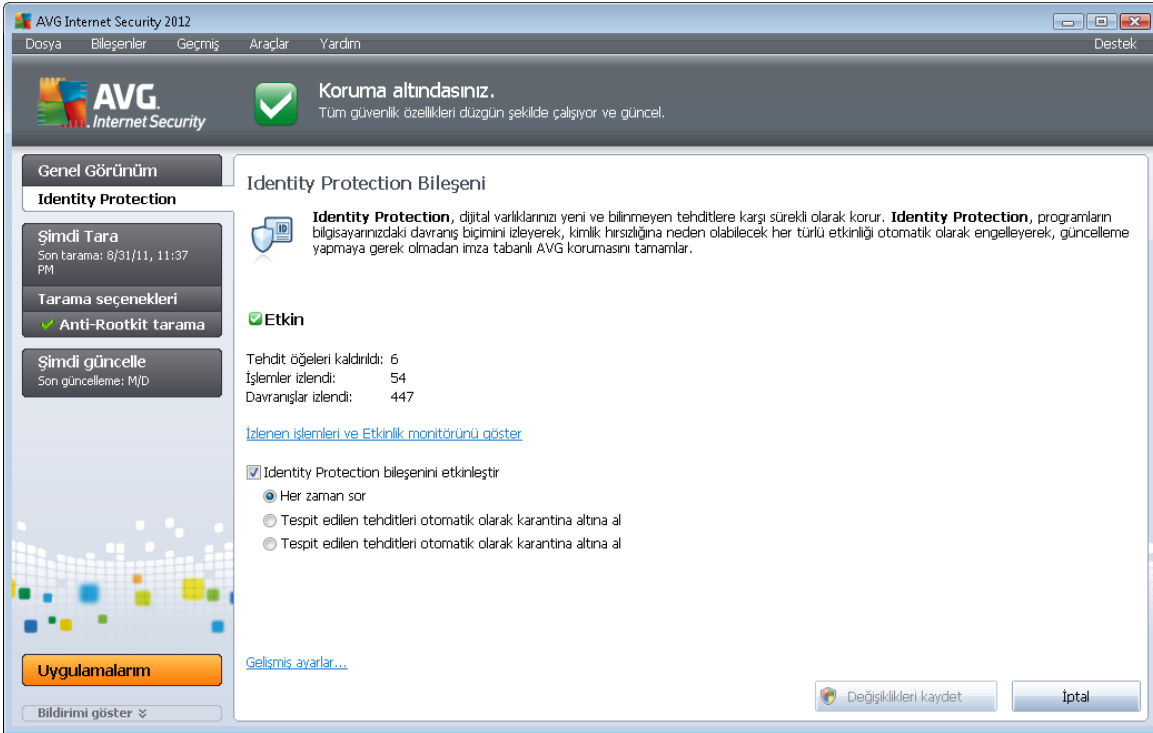
Kimlik Koruması kötü amaçlı yazılımlara karşı koruma bileşenidir, davranış teknolojilerini kullanarak ve yeni virüsler için ilk günden koruma sağlayarak sizi her türlü kötü amaçlı yazılımlardan (*casus yazılım, robotlar, kimlik hırsızlığı...*) korur. **Identity Protection**, PC'nizdeki parolalarınızı, banka hesabı ayrıntılarınızı, kredi kartı numaralarınızı ve diğer kişisel dijital bilgilerinizi tüm kötü amaçlı yazılımlarla (*kötü amaçlı yazılım*) çalan kimlik hırsızlığı üzerine odaklanmıştır. PC'nizde çalışan tüm programların doğru çalıştığından emin olmanızı sağlar. **Kimlik Koruması**, sürekli olarak şüpheli davranışları belirleyip engeller ve tüm yeni kötü amaçlı yazılımlara karşı bilgisayarınızı korur.



Identity Protection, yeni ve hatta bilinmeyen tehlikelere karşı bilgisayarınıza gerçek zamanlı bir koruma sağlar. Tüm işlemleri (*gizli olanlar da dahil*) ve 285 üzerinde farklı davranış modelini izler ve sisteminizle ilgili kötü amaçlı herhangi bir durum meydana gelip gelmediğini belirleyebilir. Bu nedenle, virüs veritabanında henüz açıklanmamış tehditleri bile açığa çıkarabilir. Bilgisayarınıza bilinmeyen bir kod gelirse söz konusu kod kötü amaçlı davranışlara karşı hemen gözlenir ve izlenir. Dosyanın kötü amaçlı olduğu tespit edilirse, **Identity Protection** kodu [Virüs Kasasına](#) kaldırır ve sistemde yapılan tüm değişiklikleri (*kod bulaşmaları, kayıt defteri değişiklikleri, bağlantı noktası açma vb.*) geri alır. Korunmak için tarama başlatmanız gerekmez. Bu teknoloji çok öngörülüdür, nadiren güncellemeye gereksinim duyar ve her an korur.

Identity Protection, [Virüslerden Koruma](#)'ya ilave bir korumadır. **Bilgisayarınız için tam koruma sağlamak üzere her iki bileşenin de bilgisayarınızda yüklenmiş olmasını önemli tavsiye ederiz!**

6.8.1. Identity Protection Arayüzü



Identity Protection iletişim kutusu bileşenin temel işlevi, durumu (*Etkin*) ve bazı istatistiksel veriler hakkında kısa açıklamalar sunar:

- **Kaldırılan kötü amaçlı yazılım öğeleri** - kötü amaçlı yazılım olarak algılanan ve kaldırılan uygulama sayısını verir
- **İzlenen işlemler** - Geçerli olarak çalışan IDP tarafından izlenen uygulama sayısı
- **İzlenen davranışlar** - İzlenen uygulamalarda çalışan belirli eylemlerin sayısı

Aşağıda [İzlenen süreçleri ve Etkinlik monitörünü görüntüle](#) bağlantısını bulabilirsiniz. Bu bağlantı sizi [Sistem araçları](#) bileşeninin kullanıcı arayüzüne götürecektir. Burada izlenen tüm süreçlerle ilgili



ayrıntılı bilgiler bulabilirsiniz.

Temel Identity Protection ayarları

İletişim kutusunun alt kısmında bileşenin işlevinin bazı temel özelliklerini düzenleyebilirsiniz:

- **Kimlik Korumasını Etkinleştir** - (varsayılan olarak açıktır): IDP bileşenini etkinleştirmek ve diğer düzenleme seçeneklerini açmak için işaretleyin.

Bazı durumlarda, **Kimlik Koruması** güvenilir bir dosyanın şüpheli veya tehlikeli olduğunu rapor edebilir. **Kimlik Koruması** tehditleri davranışlarına göre tespit edeceği için, bu genellikle bazı programlar basılan tuşları izlediğinde, diğer programları yüklediğinde veya yeni bir sürücü bilgisayara yüklendiğinde meydana gelir. Bu yüzden, şüpheli etkinlik algılandığında **Kimlik Koruması** bileşeninin nasıl davranacağını belirten şu seçeneklerden birini belirleyin:

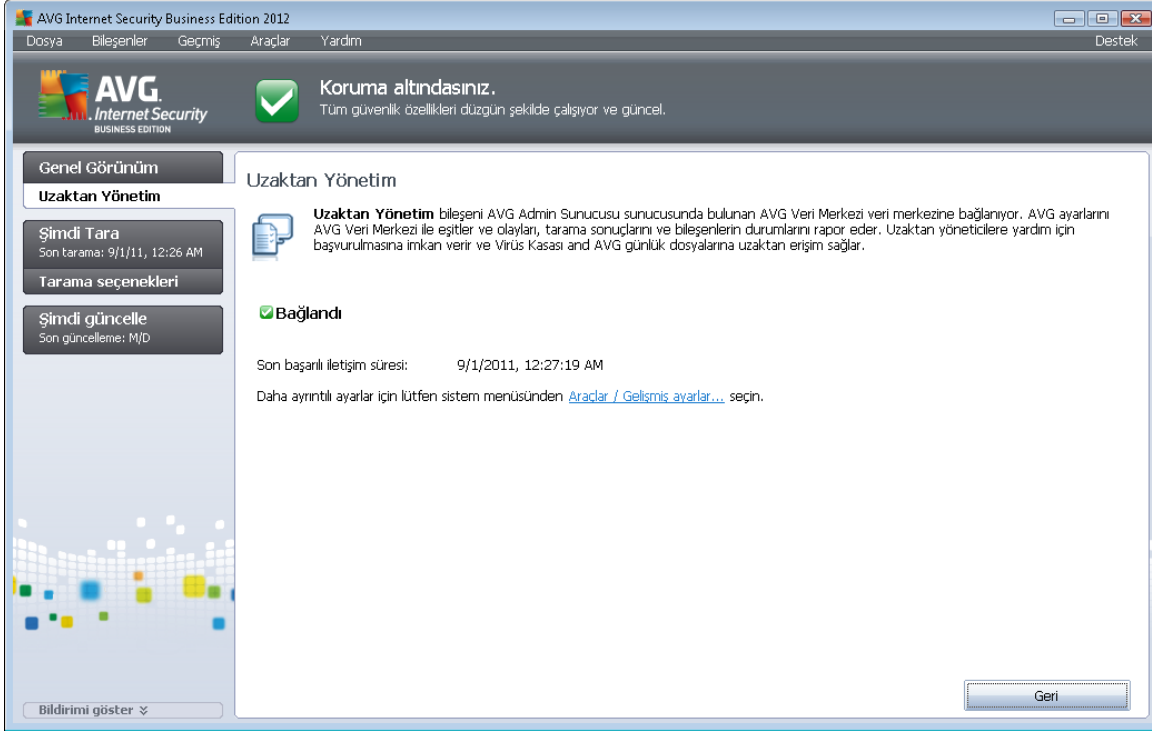
- **Her zaman sor** - bir uygulama kötü amaçlı yazılım olarak algılanırsa, engellenmesini isteyip istemediğiniz sorulacaktır (*bu seçenek, varsayılan olarak açıktır ve geçerli bir nedeniniz yoksa değiştirmemeniz önerilir*)
- **Algılanan tehlikeleri otomatik olarak karantinaya al** - Kötü amaçlı yazılım olarak algılanan tüm uygulamalar otomatik olarak engellenecektir
- **Bilinen tehlikeleri otomatik olarak karantinaya al** - yalnızca kesin olarak kötü amaçlı yazılım olduğu algılananlar engellenecektir

Kontrol düğmeleri

Identity Protection arayüzünde bulunan kontrol düğmeleri şunlardır:

- **Değişiklikleri kaydet** bu iletişim kutusunda yapılan her tür değişikliği kaydetmek ve uygulamak için bu düğmeye basın
- **İptal** - varsayılan [AVG ana iletişim kutusuna](#) (*bileşenlere genel bakış*) dönmek için bu düğmeye basın

6.9. Uzaktan Yönetim



Uzaktan Yönetim bileşeni ancak ürününüzün Business Edition sürümünü kurmuş olmanız durumunda **AVG Internet Security 2012** kullanıcı arayüzünde görüntülenir (*kurulum için kullanılan lisans hakkında bilgi için [Destek](#) sistem menü öğesinden açılabilen [Bilgi](#) iletişim kutusunun [Sürüm](#) sekmesine bakın*). **Uzaktan Yönetim bileşeni** iletişim kutusunda, bileşen etkin olup olmadığı ve sunucuya bağlı olup olmadığı hakkında bilgiler bulabilirsiniz. **Uzaktan Yönetim** bileşeninin **Gelişmiş Ayarlar / Uzaktan Yönetim** penceresinin içinde yapılmalıdır.

AVG Uzaktan Yönetim sistemindeki bileşen seçenekleri ve işlevselliği ile ilgili ayrıntılı bilgi edinmek için lütfen özel olarak bu başlığa ayrılmış olan ilgili dokümantasyona başvurun. Bu belge AVG web sitesi (<http://www.avg.com/>), **Destek merkezi / İndir / Dokümantasyon** bölümünden indirilebilir.

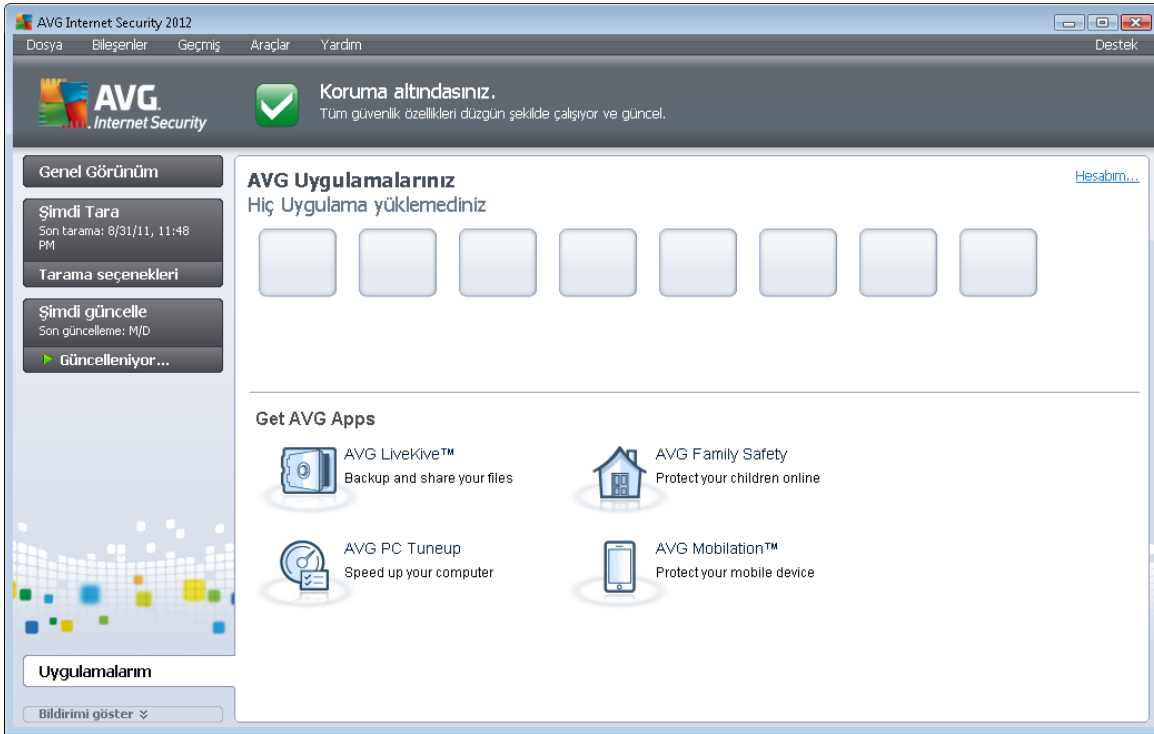
Kontrol düğmeleri

- **Geri** - varsayılan [AVG ana iletişim kutusuna](#) (bileşenlere genel bakış) dönmek için bu düğmeye basın.



7. Uygulamalarım

[LiveKive](#), [Family Safety](#) ve [PC Tuneup](#) uygulamalarından her biri bağımsız bir AVG ürünü olarak mevcuttur ve **AVG Internet Security 2012** yüklemenizin isteğe bağlı parçasıdır. **AVG Uygulamalarınız** iletişim kutusunda (*doğrudan AVG ana iletişim kutusundaki Uygulamalarım düğmesi ile erişilebilir*) zaten yüklü olan ve isteğe bağlı olarak yüklenebilecek uygulamalara dair genel bakış bulabilirsiniz:



7.1. LiveKive

LiveKive güvenli sunuculara çevrimiçi veri yedeklemesi yapmak için hazırlanmıştır. **LiveKive** tüm dosyalarınızı, fotoğraflarınızı ve müzik dosyalarınızı güvenli bir yerde yedekleyerek bunları ailenizle ve arkadaşlarınızla paylaşmanıza ve iPhones ve Android cihazları da dahil olmak üzere söz konusu dosyalara web etkinliği olan tüm cihazlardan erişmenize olanak sağlar. **LiveKive** özellikleri:

- Bilgisayarınızın ve/veya sabit sürücünüzün bozulması durumunda alınacak güvenlik önlemi
- Verilerinize İnternete bağlı herhangi bir cihazdan erişin
- Kolay düzenleme
- Yetkilendirdiğiniz biriyle paylaşma

Daha ayrıntılı bilgi için bileşeni de indirebileceğiniz özel AVG web sayfasını ziyaret edin. Bunun için [Uygulamalarım](#) iletişim kutusundaki LiveKive bağlantısını kullanabilirsiniz.



7.2. Family Safety

Family Safety çocuklarınızın uygunsuz web sitelerine, medya içeriklerine ve çevrimiçi aramalara karşı korunmasına yardımcı olur ve çevrimiçi faaliyetleriyle ilgili size rapor sağlar. Çocuklarınızdan her biri için uygun koruma düzeyi ayarlayabilir ve benzersiz girişler aracılığıyla onları ayrı ayrı gözlemleyebilirsiniz.

Daha ayrıntılı bilgi için bileşeni de indirebileceğiniz özel AVG web sayfasını ziyaret edin. Bunun için [Uygulamalarım](#) iletişim kutusundaki Family Safety bağlantısını kullanabilirsiniz.

7.3. PC Tuneup

PC Tuneup uygulaması bilgisayarınızın hızının ve genel performansının nasıl iyileştirilebileceğine yönelik ayrıntılı sistem analizi ve düzeltme işlemi için gelişmiş bir araçtır. **PC Tuneup** özellikleri:

- Disk Temizleyici - Bilgisayarı yavaşlatan gereksiz dosyaları kaldırır.
- Disk Birleştirici - Disk sürücülerini birleştirir ve sistem dosyaları yerleşimini en iyi duruma getirir.
- Kayıt Defteri Temizleyici - Bilgisayarın istikrarını artırmak için kayıt defteri hatalarını onarır.
- Kayıt Defteri Birleştirici - Bellek tüketen boşlukları gidermek için kayıt defterini sıkıştırır.
- Disk Doktoru - Bozuk kesimleri, kayıp kümeleri ve dizin hatalarını tespit eder ve onarır.
- İnternet İyileştirici - "Hepsine uyan tek boyut" ayarlarını belirli bir internet bağlantısına uyarlar.
- İz Temizleyici - Bilgisayar ve internet kullanımı geçmişini temizler.
- Disk Silici - Hassas verilerin kurtarılmasını engellemek için disklerdeki boş alanları temizler.
- Dosya Öğütücü - Disk veya USB çubuğundaki seçilen dosyaları kurtarılamayacak biçimde siler.
- Dosya Kurtarma - Disk, USB çubuk ve kameralardaki yanlışlıkla silinen dosyaları kurtarır.
- Yenilenen Dosya Bulucu - Disk alanını tüketen yenilenen dosyaları bulmaya ve silmeye yardımcı olur.
- Hizmet Yöneticisi - Bilgisayarınızı yavaşlatan gereksiz hizmetleri devre dışı bırakır.
- Başlatma Yöneticisi - Kullanıcıya Windows başlatma sırasında otomatik olarak başlayan programları yönetme olanağı sağlar.
- Kaldırma Yöneticisi - İhtiyacınız olmayan yazılım programlarını tamamen kaldırır.
- Kaldırma Yöneticisi - Kullanıcıya yüzlerce gizli Windows ayarını yapma olanağı sağlar.
- Görev Yöneticisi - Çalışan tüm işlemleri, hizmetleri ve kilitli dosyaları listeler.



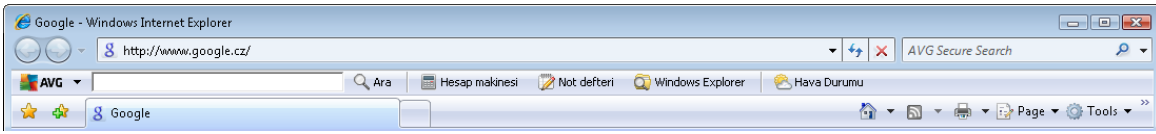
- Disk Sihirbazı - Bilgisayarda en çok yeri hangi dosyaların kapladığını gösterir.
- Sistem Bilgileri - Kurulu donanım ve yazılım hakkında ayrıntılı bilgiler sağlar.

Daha ayrıntılı bilgi için bileşeni de indirebileceğiniz özel AVG web sayfasını ziyaret edin. Bunun için [Uygulamalarım](#) iletişim kutusundaki PC Tuneup bağlantısını kullanabilirsiniz.



8. AVG Security Toolbar

AVG Security Toolbar, [LinkScanner](#) bileşeni ile sıkı bir entegrasyon içinde çalışan bir araçtır ve internet taramaları sırasında güvenliğinizi en üst düzeyde sağlar. **AVG Internet Security 2012** içinde **AVG Security Toolbar** kurulumu isteğe bağlıdır; [kurulum işlemi](#) sırasında bileşenin kurulup kurulmayacağına karar vermeniz istenir. **AVG Security Toolbar** internet tarayıcınızdan doğrudan kullanılabilir. Şu anda desteklenen internet tarayıcıları: Internet Explorer (*sürüm 6.0 üstü*), ve/veya Mozilla Firefox (*sürüm 3.0 ve üstü*). Diğer tarayıcılar desteklenmez (*Avant Browser gibi alternatif internet tarayıcıları kullanıyorsanız beklenmeyen davranışlarla karşılaşabilirsiniz*).



AVG Security Toolbar'ın içerdiği öğeler:

- **Açılır menülü AVG logosu:**
 - **AVG Secure Search Kullan- AVG Secure Search** motorunu kullanarak doğrudan **AVG Security Toolbar**'dan arama yapabileceğinizi sağlar. Tüm arama sonuçları [Search-Shield](#) hizmetince denetlenir ve çevrimiçi güvenliğinizi mutlak biçimde sağlar.
 - **Geçerli Tehdit Düzeyi** - Web'de geçerli tehdit seviyesinin grafik görünümünü içeren virüs laboratuvarı web sayfasını açar.
 - **AVG Tehdit Laboratuvarları** - AVG web sitesindeki **Site Raporu** sayfasını açar (<http://www.avg.com/>) ve burada belirli tehditler için aramaya yapıp her biri hakkında ayrıntılı bilgiler alabilirsiniz.
 - **Araç Çubuğu Yardımı** - Tüm **AVG Security Toolbar** işlevlerini kapsayan çevrimiçi yardımı açar.
 - **Ürün Geribildirim Gönder- AVG Security Toolbar** hakkında görüşlerinizi bildirebileceğiniz bir form içeren bir web sayfası açar.
 - **Hakkında...** - Geçerli olarak kurulu **AVG Security Toolbar** sürümü hakkında bilgilerin yer aldığı yeni bir pencere açar.
- **Arama alanı** - Görüntülenen tüm arama sonuçları yüzde yüz güvenli olduğundan kesin biçimde güvenli ve rahat olmak için internet aramalarında **AVG Security Toolbar** kullanın. Anahtar sözcük veya ifadeyi arama alanına girin ve **Ara** düğmesine (*veya Enter*) basın. Tüm arama sonuçları sürekli olarak [Search-Shield](#) hizmetince kontrol edilir ([LinkScanner](#) bileşeni içinde).
- Şu uygulamalara hızlı erişim için kısayol düğmeleri: **Hesap Makinesi**, **Not Defteri**, **Windows Explorer**
- **Hava** - Düğme, yaşadığınız yerin o gün ve sonraki iki günü kapsayan hava durumu hakkında bilgi sağlayan yeni bir iletişim kutusu açar. Bilgiler her 3-6 saatte bir düzenli olarak

güncellenir. İletişim kutusunda istediğiniz konumu el ile seçebilir ve sıcaklık değerlerinin Celsius veya Fahrenheit cinsinden gösterilmesini tercih edebilirsiniz.



The Weather Channel
weather.com

Brno, Czech Republic
Updated: 8/31/11 11:30 PM Local Time
[[change location](#)]

°F °C
Sunrise: 06:07
Sunset: 07:40

 **16°C**

 Tonight Hi: N/A Lo: 13°C	 Thursday Hi: 24°C Lo: 13°C	 Friday Hi: 25°C Lo: 13°C
---	---	---

- **Facebook** - Bu düğme doğrudan **AVG Security Toolbar** içinden [Facebook](#) sosyal paylaşım ağına bağlanabilmenizi sağlar. *davranış*.

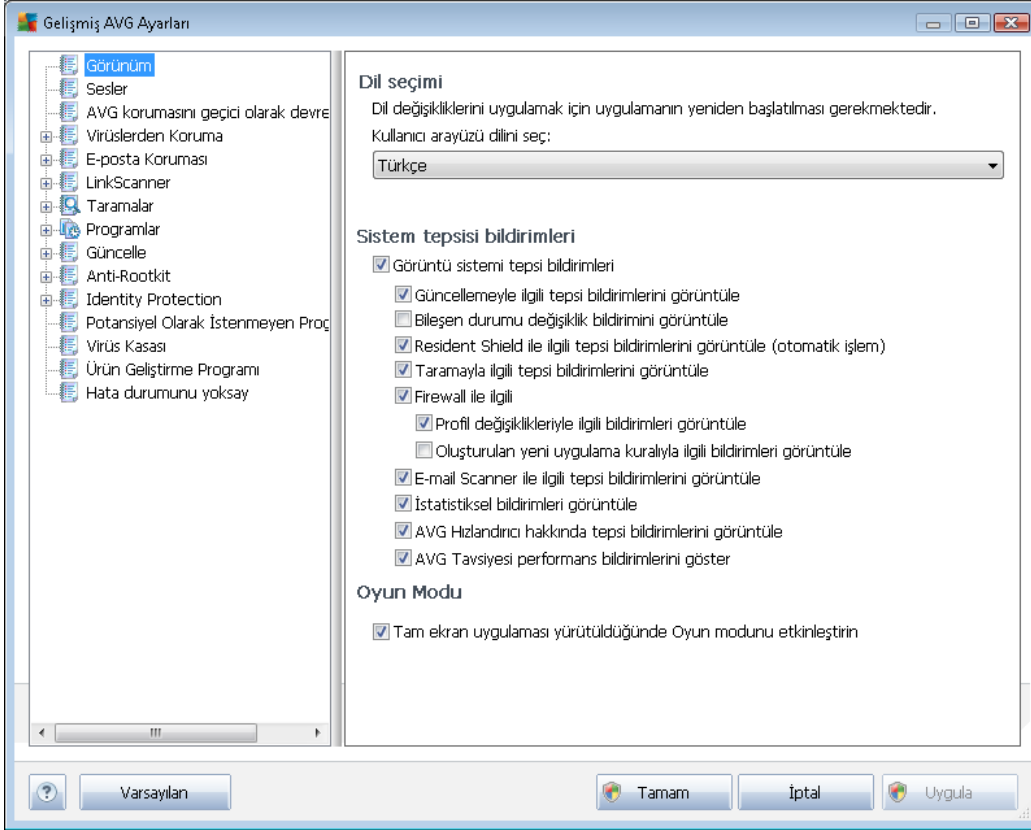


9. AVG Gelişmiş Ayarlar

AVG Internet Security 2012 Gelişmiş yapılandırma iletişim kutusu **Gelişmiş AVG Ayarları** adlı yeni bir pencerede açılır. Pencere iki bölüme ayrılır: sol tarafta program yapılandırma seçeneklerini gösteren ağaç tipli menü bulunmaktadır. İletişim penceresini pencerenin sağ kısmında görüntülemek için (*nin ya da belirli bir bileşenin*) yapılandırmasını değiştirmek istediğiniz bileşeni seçin.

9.1. Görünüm

Menü ağacının ilk ögesi olan **Görünüm**, **AVG Internet Security 2012 kullanıcı arayüzünün** genel ayarlarına ilişkindir ve uygulama davranışı için bazı temel seçenekleri sağlar:



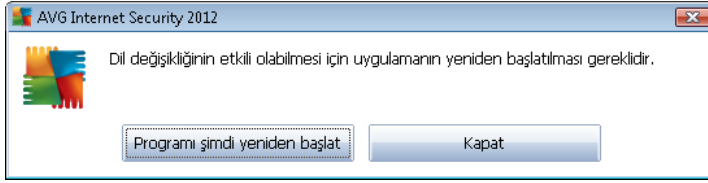
Dil seçimi

Dil seçimi bölümünde açılır menüden istediğiniz dili seçebilirsiniz. Seçilen dil **AVG Internet Security 2012 kullanıcı arayüzünün** tamamı için kullanılır. Aşağı açılır menü **yükleme işlemi** sırasında yüklenmesini istediğiniz dilleri (*bkz. Özel seçenekler*) ve İngilizceyi sunar (*İngilizce daima varsayılan olarak yüklenir*). **AVG Internet Security 2012** uygulamasını başka bir dile geçirmek için yeniden başlatmanız gerekir. Lütfen şu adımları takip edin:

- Aşağı açılır menüde istediğiniz uygulama dilini seçin
- **Uygula** düğmesine (*iletişim kutusunun sağ alt tarafında*) basarak seçiminizi onaylayın



- Onaylamak için **Tamam** düğmesine basın
- Uygulamanın dilini değiştirmek için **AVG Internet Security 2012**
- Programın yeniden başlatılmasını onaylamak için **Programı şimdi yeniden başlat** düğmesine basın ve dil değişikliğinin gerçekleşmesi için bir saniye bekleyin:



Sistem tepsi bildirimleri

Bu bölümde **AVG Internet Security 2012** uygulama durumu hakkında sistem tepsi üzerinde beliren bildirimleri kaldırabilirsiniz. Varsayılan olarak, sistem bildirimlerinin görüntülenmesine izin verilir. Bu yapılandırmayı korumanız kesinlikle önerilir! Sistem bildirimleri örneğin tarama veya güncelleme işlemi başlatma ya da bir **AVG Internet Security 2012** bileşeni durum değişikliği hakkında bilgi verir. Bu duyurulara kesinlikle dikkat etmeniz gerekir!

Ancak, belirli bir neden dolayısıyla bu yolla bilgilendirilmek istemiyorsanız ya da sadece belirli bildirimlerin görüntülenmesini istiyorsanız (*belirli AVG Internet Security 2012 bileşenlerine ilişkin*) tercihlerinizi aşağıdaki seçenekleri işaretleyerek ya da işaretlemeyerek tanımlayabilir ve belirleyebilirsiniz:

- **Sistem tepsi bildirimlerini görüntüle** (*açık, varsayılan olarak*) - Varsayılan olarak tüm bildirimler görüntülenir. Tüm sistem bildirimleri kapatmak için bu öğenin işaretini kaldırın. Açıldığı zaman hangi bildirimlerin görüntüleneceğini seçebilirsiniz:
 - **Güncellemeyle** ilgili tepsi bildirimlerini görüntüle (*açık, varsayılan olarak*) - **AVG Internet Security 2012** güncellemesi işleminin başlaması, ilerleyişi ve bitişi hakkında bilgilerin görüntülenmesini isteyip istemediğinize karar verin.
 - **Bileşen durum değişikliği hakkında bildirimleri görüntüle** (*kapalı, varsayılan olarak*) - Bileşenleri etkin olup olmadığı ya da muhtemel sorunları hakkında bildirimlerin görüntülenmesini isteyip istemediğinize karar verin. Bir bileşenin hata durumu rapor edilirken bu fonksiyon, **sistem tepsi simgesinin** herhangi bir **AVG Internet Security 2012** bileşeninde meydana gelen sorunu rapor eden kullandığı bilgilendirici fonksiyonuna eşdeğerdir.
 - **Resident Shield ile ilgili tepsi bildirimlerini görüntüle** (*otomatik işlem*) (*açık, varsayılan olarak*) - Dosya kaydetme, kopyalama ve açma işlemleriyle ilgili bilgilerin görüntülenmesine veya gizlenmesine (*bu yapılandırma yalnızca Resident Shield Otomatik temizleme seçeneği açık sağ gösterilir*) karar verin.
 - **Tarama** ile ilgili bildirimleri görüntüle (*açık, varsayılan olarak*) - Programlı taramaların otomatik olarak başlaması, ilerleyişi ve sonuçları hakkında bilgilerin görüntülenmesini isteyip istemediğinize karar verin.



- **Firewall ile ilgili tepsi bildirimlerini görüntüle** (açık, varsayılan olarak) - **Firewall** durum ve işlemleri hakkında, örneğin bileşenin etkinleştirilmesi/devre dışı bırakılması uyarıları, olası trafik engelleme vb. hakkında bilgilerin görüntülenip görüntülenmeyeceğine karar verin. Bu öge iki adet belirli seçim seçeneği daha sağlar (her biri hakkında daha fazla bilgi için lütfen bu belgedeki [Güvenlik Duvarı](#) bölümüne bakın):
 - **Profil değişiklikleriyle ilgili bildirimleri görüntüle** (açık, varsayılan olarak) - **Firewall** profilleri otomatik değişiklikleri hakkında sizi bilgilendirir.
 - **Oluşturulan yeni uygulama kurallarıyla ilgili bildirimleri görüntüle** (kapalı, varsayılan olarak) - Bir güvenlik listesine bağlı olarak yeni uygulamalar için **Firewall** kurallarının otomatik oluşturulmasıyla ilgili sizi bilgilendirir.
- **E-mail Scanner ile ilgili tepsi bildirimlerini görüntüle** (açık, varsayılan olarak) - Gelen ve giden e-posta mesajlarının taranmasına ilişkin bildirimleri görüntülemek isteyip istemediğinize karar verin.
- **İstatistiksel uyarıları görüntüle** (açık, varsayılan olarak) - Düzenli istatistiksel inceleme uyarılarının sistem tepsisinde görüntülenmesine izin vermek için bu seçeneği işaretli halde bırakın.
- **AVG Accelerator hakkında tepsi bildirimini görüntüle** (açık, varsayılan olarak) - **AVG Accelerator** etkinlikleri hakkındaki bilgilerin görüntülenmesini isteyip istemediğinize karar verin. **AVG Accelerator** hizmetidaha düzgün çevrimiçi video oynatmaya izin verir ve ilave indirmeleri daha kolay hale getirir.
- **AVG Advice performans bildirimlerini görüntüle** (açık, varsayılan olarak) - **AVG Advice** desteklenen internet tarayıcılarının (*Internet Explorer, Chrome, Firefox, Opera ve Safari*) performansını izler ve tarayıcınızın önerilen bellek miktarının fazlasını kullanması durumunda sizi bilgilendirir. Böyle bir durumda bilgisayarınızın performansı ciddi bir düşüş gösterebilir; işlemleri hızlandırmak için internet tarayıcınızı yeniden başlatmanız önerilir. Bilgilenmek için **AVG Advice performans bildirimlerini görüntüle** ögesini açık tutun.



Oyun modu

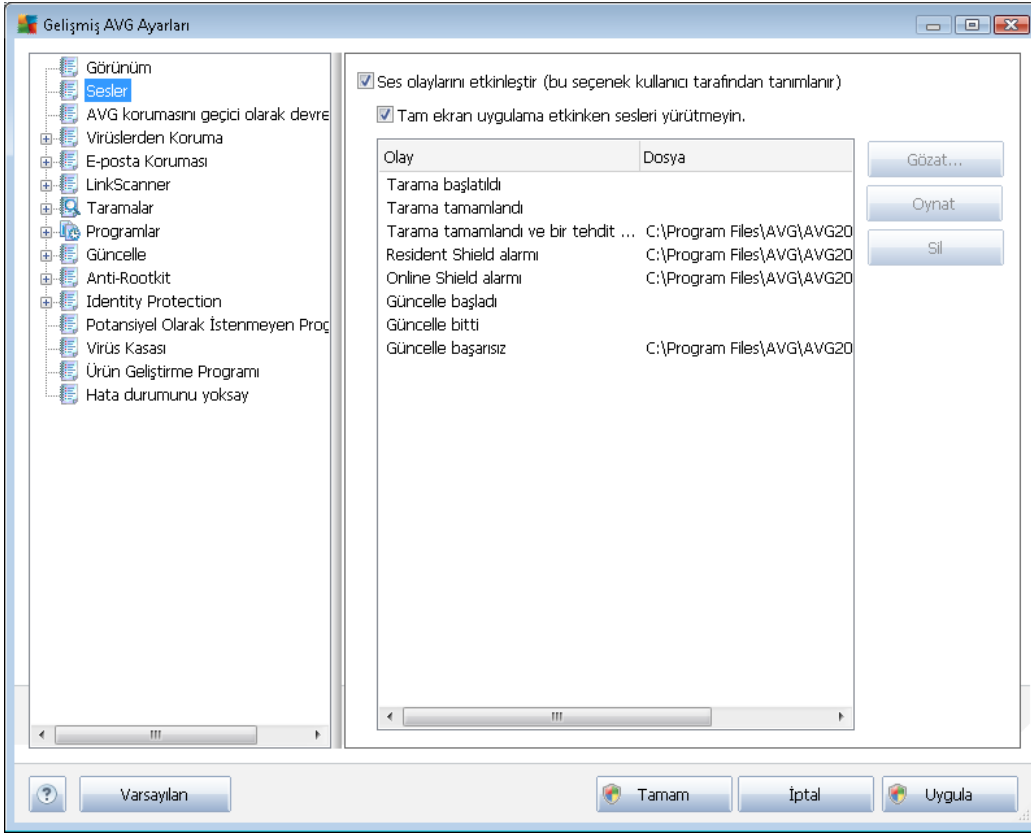
Bu AVG işlevi, olası AVG bilgi balonlarının (örn. programlı bir tarama başlatıldığında gösterilir) rahatsız edici olabilen (uygulamayı küçültebilir veya grafiklerini bozabilir) tam ekran uygulamaları için



tasarlanmıştır. Bu durumu önlemek için, **Tam ekran uygulaması çalıştırılırken oyun modunu etkinleştir** seçeneğini işaretli bırakın (*varsayılan ayar*).

9.2. Sesler

Sesler iletişim kutusu içinde, belirli **AVG Internet Security 2012** eylemleri hakkında bir ses bildiriyle bilgilendirilmek isteyip istemediğinizi belirleyebilirsiniz:



Bu ayarlar yalnızca mevcut kullanıcı hesabı için geçerlidir. Bu nedenle bilgisayar üzerindeki kullanıcıların her birine ait ses ayarları vardır. Sesli bildirimlere izin vermek istiyorsanız, ilgili tüm eylemler listesini etkinleştirmek için **Sesli uyarıları etkinleştir** seçeneğini işaretli bırakın (*seçenek varsayılan olarak açıktır*). Ayrıca, rahatsız edici olabilecekleri durumlarda sesli bildirimleri kapatmak için **tam ekran uygulama etkinken sesleri yürütme** seçeneğini işaretlemek isteyebilirsiniz (*ayrıca bu belgedeki [Gelişmiş Ayarlar/Görünüm](#) bölümünün Oyun modu kısmına bakın*).

Kontrol düğmeleri

- **Gözet** - Diskinizde atamak istediğiniz ilgili ses dosyasını aramak için, listeden ilgili eylem seçilmiş olarak **Gözet** düğmesini kullanın. (*Şu anda yalnızca *.wav seslerinin desteklenmekte olduğunu lütfen unutmayın!*)
- **Çal** - Seçili sesi dinlemek için, listede olayı vurgulayın ve **Çal** düğmesine basın.

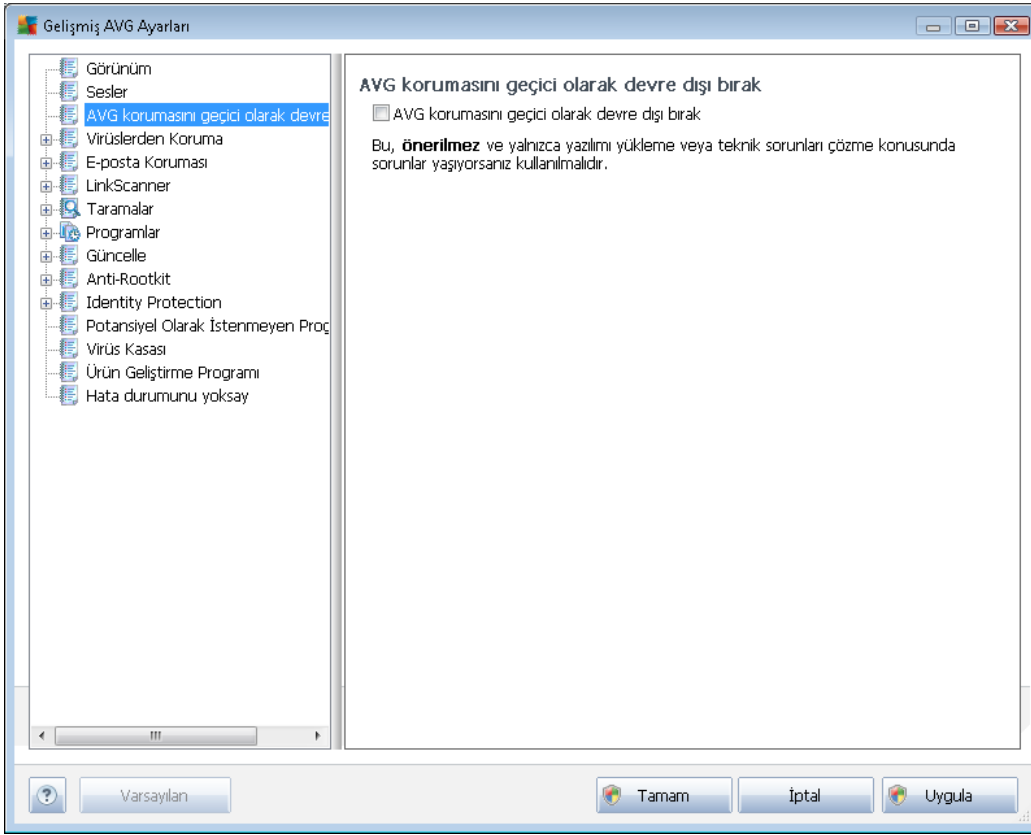


- **Sil** - Belirli olaya atanan sesi kaldırmak için **Sil** düğmesini kullanın.

9.3. AVG korumasını geçici olarak devre dışı bırak

AVG korumasını geçici olarak devre dışı bırak iletişim kutusunda, **AVG Internet Security 2012** yazılımınız tarafından güvende tutulan tüm korumayı bir seferde kapatma seçeneğiniz vardır.

Mutlaka gerekli değilse, bu seçeneği kullanmamanız gerektiğini lütfen unutmayın!



Çoğu durumda, yeni yazılımı veya sürücülerini yüklemeyen önce ve hatta yükleyici veya yazılım sihirbazı yükleme işlemi sırasında istenmeyen kesintilerin olmamasını sağlamak için çalışan program ve uygulamaların kapatılmasını önerse bile **AVG Internet Security 2012** uygulamasını devre dışı bırakmak **gerekmez**. Yükleme sırasında gerçekten sorun yaşıyorsanız, öncelikle [yerleşik korumayı devre dışı bırakmayı deneyin](#) (*Yerleşik Kalkanı etkinleştir*). **AVG Internet Security 2012** uygulamasını geçici olarak devre dışı bırakmanız gerekirse, işinizi bitirdikten sonra yeniden etkinleştirmeniz gerekir. Virüslerden korunma yazılımınız devre dışı bırakılmışken İnternete veya bir ağa bağlanırsanız, bilgisayarınız saldırılara açık durumda olur.

AVG koruması geçici olarak nasıl devre dışı bırakılır

- **AVG korumasını geçici olarak devre dışı bırak** onay kutusunu işaretleyin ve **Uygula** düğmesine basarak seçiminizi onaylayın



- Yeni açılan **AVG korumasını geçici olarak devre dışı bırak** iletişim kutusunda **AVG Internet Security 2012** uygulamanızı ne kadar süreyle devre dışı bırakmak istediğinizi belirleyin. Koruma, varsayılan olarak 10 dakika süreyle kapatılır. Bu süre, yeni bir yazılım yükleme gibi herhangi bir işlem için yeterli olacaktır. İlk baştaki sürenin ancak 15 dakikaya uzatılabileceğini ve güvenlik nedenlerinden ötürü bu sınırın aşılamayacağını unutmayın. Belirlenen zaman aralığından sonra devre dışı bırakılan tüm bileşenler otomatik olarak tekrar etkinleştirilir.

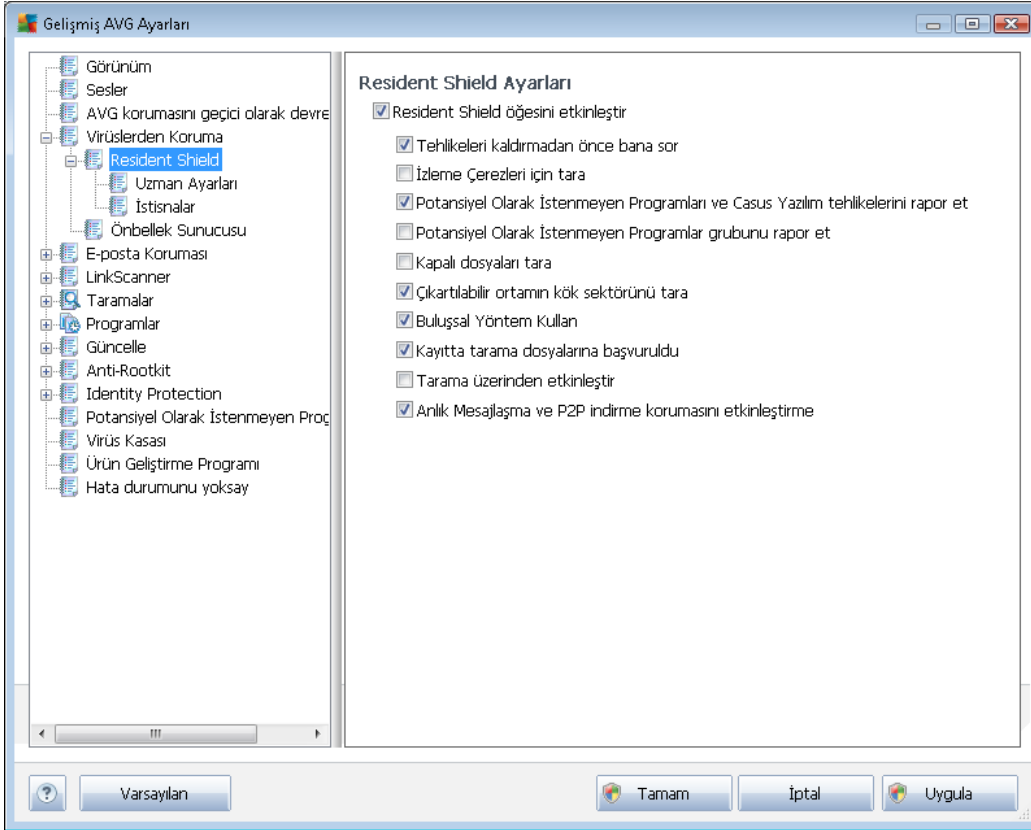


9.4. Virüslerden Koruma

Konu metnini buraya girin.

9.4.1. Yerleşik Kalkan

Yerleşik Kalkan dosya ve klasörlerinizi çevrimiçi ortamda virüslere, casus yazılımlara ve diğer zararlı yazılımlara karşı korur.



Yerleşik Kalkan Ayarları iletişim kutusunda yerleşik kalkan korumasını **Yerleşik Kalkanı Etkinleştir** ögesini işaretleyerek ya da işaretini kaldırarak etkinleştirebilir ya da devre dışı bırakabilirsiniz (*bu seçenek varsayılan olarak açıktır*). Ayrıca yerleşik kalkanın hangi özelliklerinin etkinleştirileceğini seçebilirsiniz:

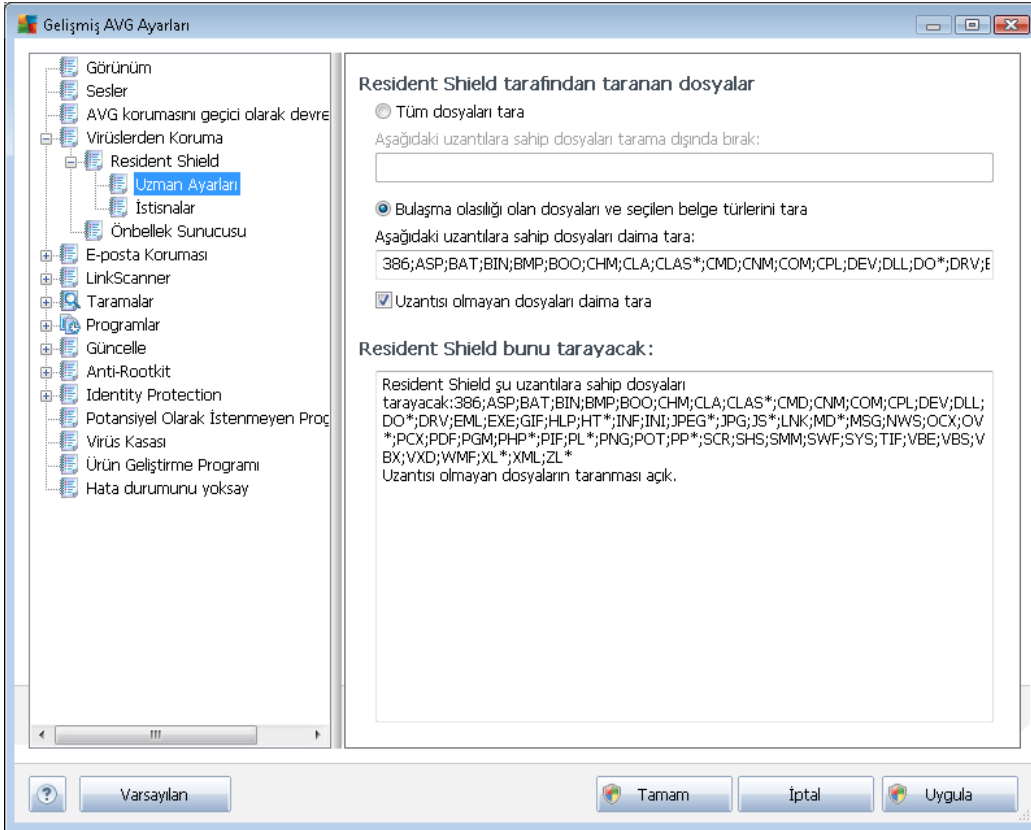
- **Tanımlama bilgilerini izlemek için tara** (*varsayılan olarak kapalı*) - Bu parametre, tanımlama bilgilerinin tarama işlemi sırasında tespit edilmesi gerektiğini belirtir. (*HTTP tanımlama bilgileri, site tercihleri veya elektronik alışveriş sepetlerinin içerikleri gibi kullanıcılar hakkındaki belirli bilgilerin kimliklerinin doğrulanması, takibi ve sürdürülmesi için kullanılır.*)
- **Potansiyel Olarak İstenmeyen Programları ve Casus Yazılım tehditlerini rapor et** (*varsayılan olarak açık*) - [Anti-Spyware](#) motorunu etkinleştirmek ve virüslerin yanı sıra casus yazılımları da denetlemek için işaretleyin. [Casus yazılım](#), şüpheli kötü amaçlı yazılım kategorisini ifade eder: Genellikle güvenlik riski oluşturmasına rağmen bu programlardan bazıları bilerek yüklenebilir. Bilgisayarınızın güvenliğini artırdığından, bu özelliği etkin durumda tutmanızı öneriyoruz.
- **Potansiyel Olarak İstenmeyen Programlar gelişmiş grubunu rapor et** (*varsayılan olarak kapalı*) - [Casus yazılımların](#), yani doğrudan üreticiden alınan tamamen zararsız olan, ancak



daha sonra kötüye kullanılabilecek programların genişletilmiş paketinin tespit edilmesi için işaretleyin. Bu, bilgisayar güvenliğinizi daha da artıran ek bir önlemdir, ancak yasal programları da engelleyebilir ve bu yüzden varsayılan olarak kapalıdır.

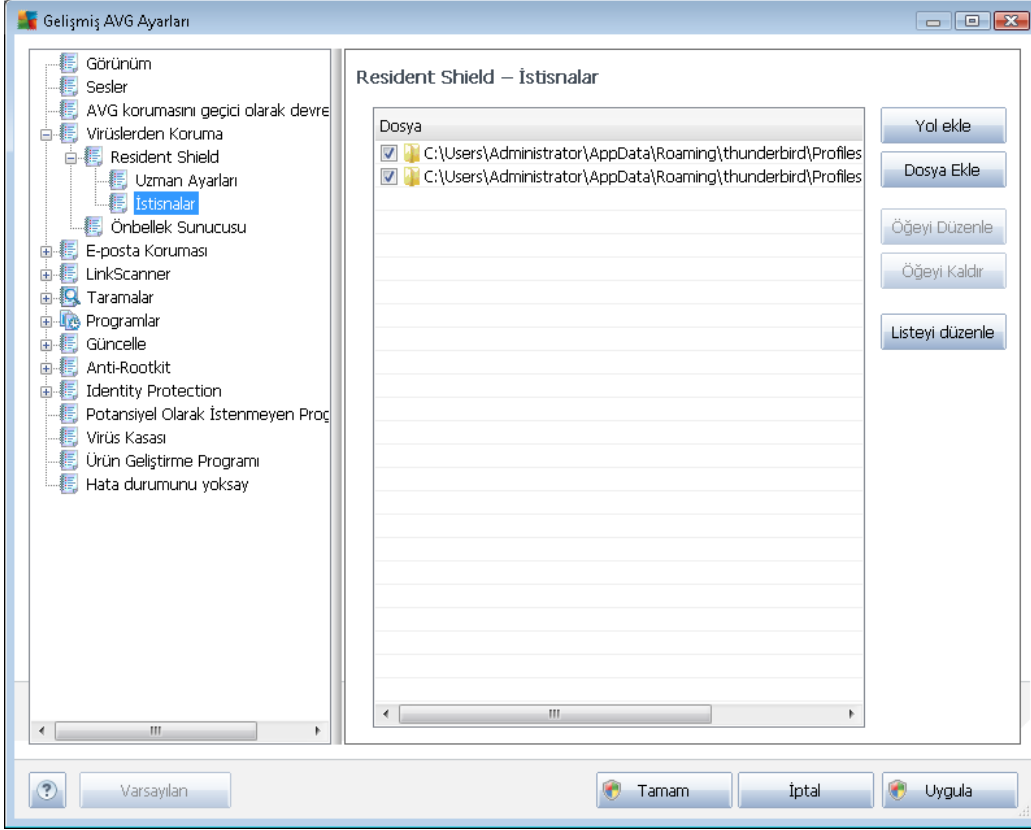
- **Dosyaları kapatılırken tara** (varsayılan olarak kapalı) - İşlem sonunda tarama, AVG'nin etkin nesnelere hem açılırken hem de kapatılırken taradığından emin olmanızı sağlar. Bunun yanı sıra bu özellik, bilgisayarınızı karmaşık virüslere karşı korumanıza da yardımcı olur.
- **Çıkarılabilir ortamların önyükleme kesimini tara** (varsayılan olarak açıktır)
- **Buluşsal Analiz Kullan** - (varsayılan olarak açık) [Buluşsal analiz](#), tespit etme işlemi sırasında kullanılır (taranan nesnenin komutlarının sanal bilgisayar ortamında dinamik olarak canlandırılması).
- **Tüm tehditleri otomatik olarak kaldır** (varsayılan olarak kapalı) - Tespit edilen tüm bulaşmalar, bir temizleme işlemi mevcutsa iyileştirilir ve temizlenemeyen tüm bulaşmalar kaldırılır.
- **Kayıt defterindeki dosyaları tara** (varsayılan olarak açık) - Bilinen bulaşmanın sonraki bilgisayar başlangıcında çalıştırılmasını önlemek için, başlangıç kayıt defterine eklenmiş tüm çalıştırılabilir dosyaları AVG tarar.
- **Kapsamlı taramayı etkinleştir** (varsayılan olarak kapalı) - Belirli durumlarda (çok acil bir durum olduğunda) nesnelere derinlemesine işleme olasılığını denetleyecek çok hassas algoritmaları etkinleştirmek için bu seçeneği işaretleyebilirsiniz. Ancak, bu yöntemin çok fazla zaman aldığını unutmayın.
- **Anlık Mesajlaşma korumasını ve P2P indirme korumasını etkinleştir** (varsayılan olarak açık) - Anlık mesajlaşma iletişimi (örn. ICQ, MSN Messenger, ...) ve P2P indirmelerinin virüssüz olduğunu doğrulamak istiyorsanız bu seçeneği işaretleyin.

Yerleşik Kalkan tarafından taranan dosyalar penceresinde taranan dosyaların yapılandırılması mümkündür (*belirli dosya uzantılarına göre*):



Tüm dosyaları tara veya yalnızca **Bulaşma olasılığı olan dosyaları ve seçilen belge türlerini tara** seçim yapmak için ilgili onay kutusunu işaretleyin. İkinci seçenekte karar kılersanız, taramanın dışında tutulması gereken dosyaları tanımlayan bir uzantılar listesi ve her durumda taranması gereken dosyaları tanımlayan bir uzantılar listesinden tarama işlemini daha fazla özelleştirebilirsiniz.

Aşağıda bahsi geçen **Yerleşik Kalkan tarayacak** bölümü, **Yerleşik Kalkan**'ın gerçekte ne taradığı ile ilgili detaylı bilgiler görüntüleyerek geçerli ayarları daha fazla özetler.



Yerleşik Kalkan - İstisnalar iletişim kutusu **Yerleşik Kalkan** taraması sırasında hariç tutulması gereken klasörleri seçebilmenizi sağlar.

Bu gerekli değilse, hiçbir öğeyi hariç tutmamanızı önemle öneririz!

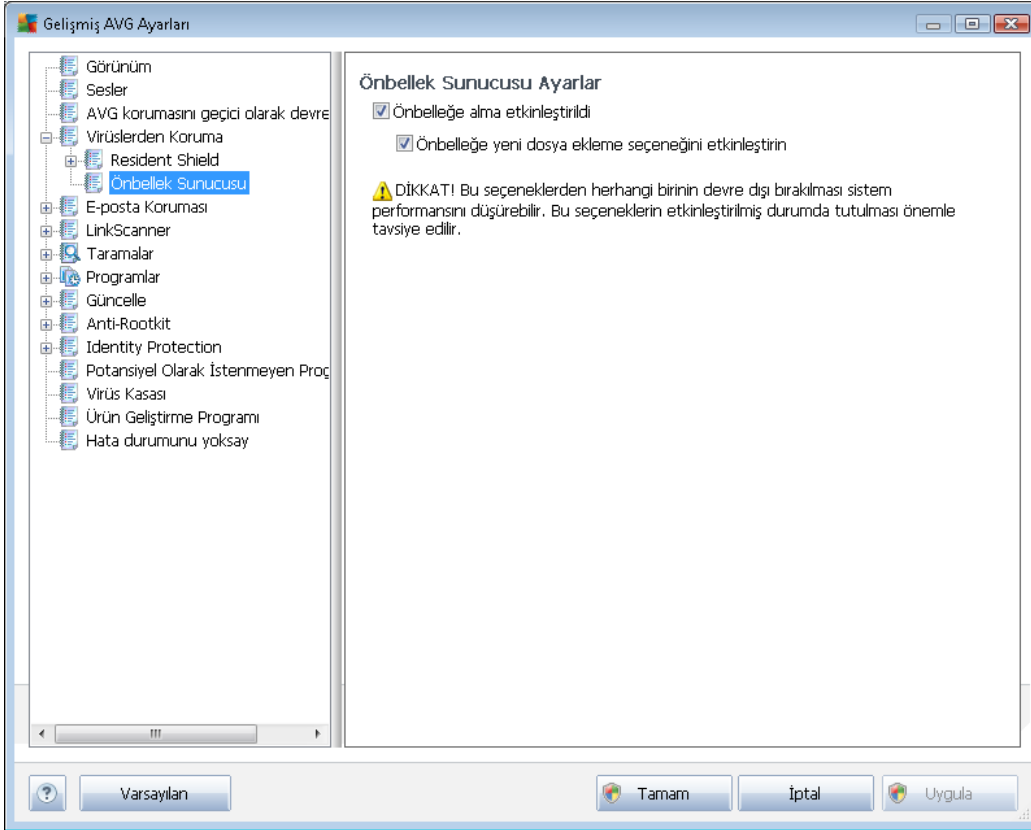
Kontrol düğmeleri

İletişim kutusunda aşağıdaki kontrol düğmeleri bulunur:

- **Yol Ekle** - yerel disk menü ağacından teker teker seçerek taramada hariç tutulacak dizini (dizinleri) belirleyin.
- **Dosya Ekle** - yerel disk menü ağacından teker teker seçerek taramada hariç tutulacak dosyaları belirleyin.
- **Öğeyi Düzenle** - seçilen dosyaya giden yolu düzenlemenize olanak verir
- **Öğeyi Kaldır** - listeden seçili öğeye götüren yolu silmenize olanak verir
- **Listeyi Düzenle** - tanımlanan istisnaların tüm listesini, standart metin düzenleyici gibi çalışan yeni bir iletişim kutusunda düzenleyebilmenizi sağlar

9.4.2. Önbellek Sunucusu

Önbellek Sunucusu Ayarları iletişim kutusu tüm **AVG Internet Security 2012** tarama türlerini hızlandırmak için tasarlanan önbellek sunucusu sürecini işaret eder:



Önbellek sunucusu güvenilir dosyaların bilgilerini toplar ve saklar (*bir dosya güvenilir bir kaynak tarafından dijital imza ile imzalandığında güvenilir sayılır*). Böylece bu dosyalar otomatik olarak güvenli varsayılır ve yeniden taramalarına gerek duyulmaz; bu nedenle tarama sırasında bu dosyalar atlanır.

Önbellek Sunucusu Ayarları iletişim kutusu aşağıdaki yapılandırma seçeneklerini sunar:

- **Önbelleğe alma etkin** (*varsayılan olarak açıktır*) - **Önbellek Sunucusu**'nu kapatmak için kutunun işareti kaldırın ve önbellek belleğini boşaltın. Lütfen, kullandığınız her bir dosya virüs ve casus yazılım için ilk kez tarandığından taramanın yavaş olabileceğini ve bilgisayarınızın genel performansının azalacağını unutmayın.
- **Önbelleğe yeni dosyaların eklenmesini etkinleştir** (*varsayılan olarak açıktır*) - önbelleğe daha fazla dosya eklenmesini durdurmak için kutunun işaretini kaldırın. Önceden önbelleğe alınmış her dosya korunacak ve önbelleğe alma tamamen kapatılıncaya kadar veya virüs veritabanının bir sonraki güncellenmesine kadar kullanılacaktır.

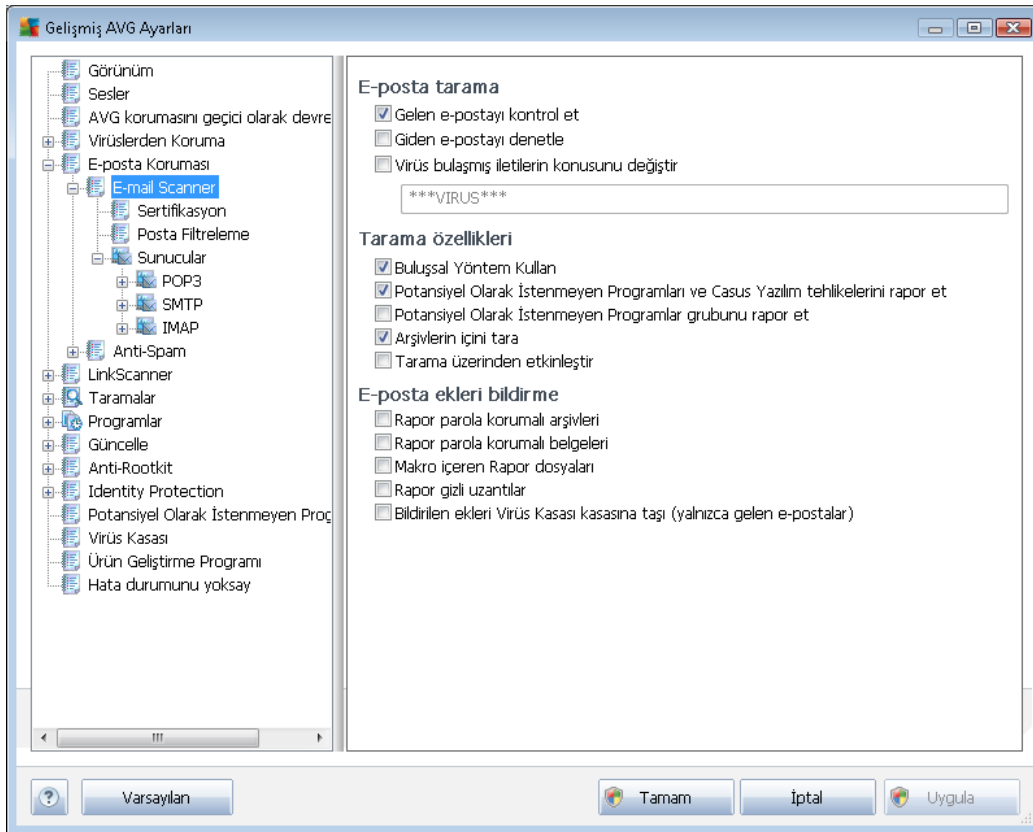
Önbellek sunucusunu kapatmak için iyi bir nedeniniz yoksa, kesinlikle varsayılan ayarları korumanızı ve seçeneğin açık kalmasını öneririz! Aksi durumda, sistem hızı ve performansında ciddi bir düşüş görebilirsiniz.

9.5. E-posta koruması

E-posta koruması bölümünde [E-mail Scanner](#) ve [Anti-Spam](#) için ayrıntılı yapılandırmalar düzenleyebilirsiniz:

9.5.1. E-Posta Tarayıcısı

E-Posta Tarayıcısı iletişim kutusu üç bölüme ayrılmıştır:



E-posta tarama

Bu bölümde, gelen ve/veya giden e-posta iletileri için bu temel bilgileri ayarlayabilirsiniz:

- **Gelen e-postayı denetle** (varsayılanda açıktır) - e-posta istemcinize gelen tüm e-postaları tarama seçeneğini açmak/kapatmak için işaretleyin
- **Giden e-postayı denetle** (varsayılanda kapalıdır) - hesabınızdan gönderilen tüm e-postaları tarama seçeneğini açmak/kapatmak için işaretleyin
- **Virüs bulaşmış iletilerin konusunu değiştir** (varsayılanda kapalıdır) - taranan e-posta iletilerinin bulaşmış olarak tespit edilmesi durumunda size bildirilmesini istiyorsanız, bu öğeyi işaretleyin ve metin alanına istediğiniz metni yazın. Ardından bu metin, daha kolay tanımlanması ve filtrelenmesi için tespit edilen her e-posta iletilerinin "Konu" alanına eklenecektir. Varsayılan değer *****VİRÜS***** olarak belirlenmiştir ve bu değeri korumanızı öneririz.



Tarama özellikleri

Bu bölümde, e-posta iletilerinin nasıl taranacağını belirleyebilirsiniz:

- **Buluşsal Yöntem Kullan** (varsayılanda açıktır) - e-posta iletilerini tararken buluşsal tespit yöntemi kullanmak için işaretleyin. Bu seçenek açık olduğunda, e-posta eklerini yalnızca uzantıya göre filtrelemezsiniz; ekin gerçek içeriği de göz önünde bulundurulur. Filtreleme işlemi [Posta Filtreleme](#) iletişim kutusundan ayarlanabilir.
- **Potansiyel Olarak İstenmeyen Programları ve Casus Yazılım tehditlerini rapor et** (varsayılanda açıktır) - [Anti-Spyware](#) motorunu etkinleştirmek ve virüslerin yanı sıra casus yazılımları da taramak için işaretleyin. [Casus yazılım](#), şüpheli kötü amaçlı yazılım kategorisini ifade eder: Genellikle güvenlik riski oluşturmasına rağmen bu programlardan bazıları bilerek yüklenebilir. Bilgisayarınızın güvenliğini artırdığından, bu özelliği etkin durumda tutmanızı öneriyoruz.
- **Potansiyel Olarak İstenmeyen Programlar gelişmiş grubunu rapor et** (varsayılanda kapalıdır) - bu parametre [casus yazılımların](#), yani doğrudan üreticiden alınan tamamen zararsız olan, ancak daha sonra kötüye kullanılacak programların genişletilmiş paketinin tespit edilmesi için işaretleyin. Bu, bilgisayar güvenliğinizi daha da artıran ek bir önlemdir, ancak yasal programları da engelleyebilir ve bu yüzden varsayılan olarak kapalıdır.
- **Arşivlerin içeriğini tara** (varsayılanda açıktır) - e-posta iletilerine eklenen arşivlerin içeriklerini taramak için işaretleyin.
- **Kapsamlı taramayı etkinleştir** (varsayılanda kapalıdır) - belirli durumlarda (örneğin, bilgisayarınıza virüs veya kötü amaçlı yazılım bulaştığından şüpheleniliyorsa) yalnızca emin olmak üzere bilgisayarınızın bulaşma olması çok zor olan alanlarını bile tarayan en kapsamlı tarama algoritmalarını etkinleştirmek için bu seçeneği işaretleyebilirsiniz. Ancak, bu yöntemin çok fazla zaman aldığı unutulmalıdır.

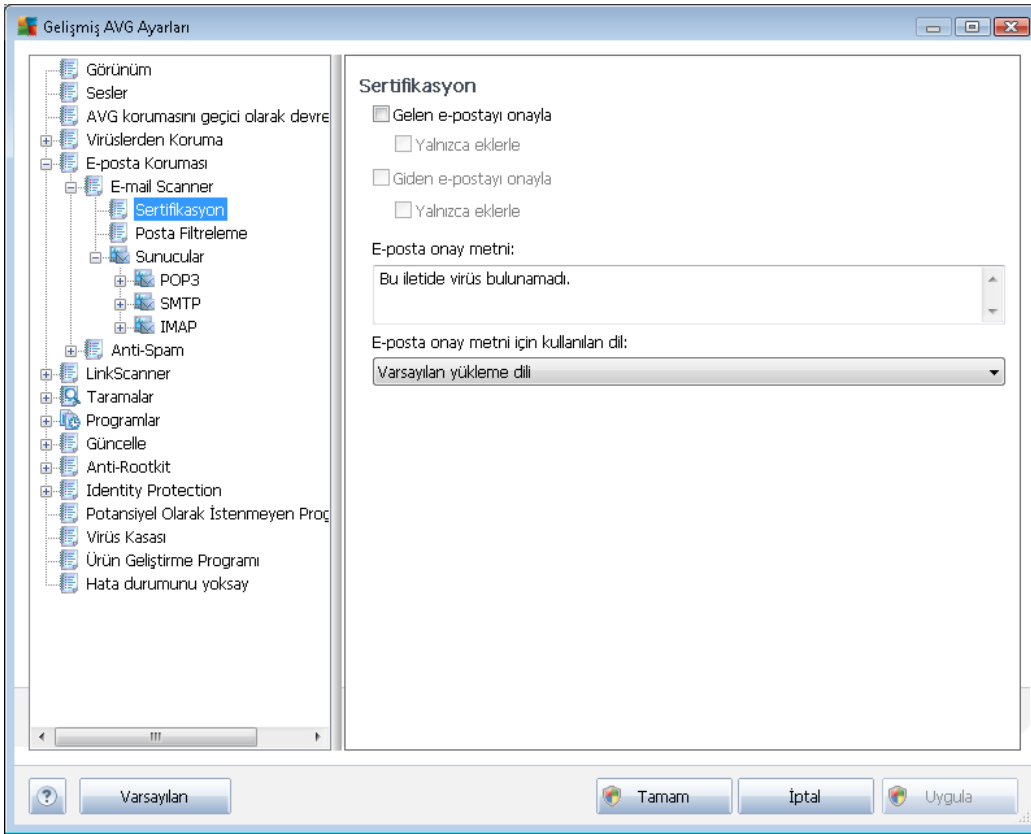
E-posta eklerini bildirme

Bu bölümde, potansiyel olarak tehlikeli ve şüpheli olan dosyalar için ek raporlar ayarlayabilirsiniz. Lütfen bir uyarı iletişim kutusu görüntülenmeyeceğini unutmayın. Yalnızca e-posta iletilerinin sonuna bir onay metni eklenir ve bu tür tüm raporlar [E-posta Tarayıcısı tespiti](#) iletişim kutusunda listelenir:

- **Parola korumalı arşivleri bildir** - parolayla korunan arşivler için (ZIP, RAR vb.) virüs taraması mümkün değildir. Bunların potansiyel olarak tehlikeli olduklarını bildirmek üzere kutuyu işaretleyin.
- **Parola korumalı belgeleri bildir** - parolayla korunan belgeler için virüs taraması mümkün değildir. Bunların potansiyel olarak tehlikeli olduklarını bildirmek üzere kutuyu işaretleyin.
- **Makro içeren dosyaları bildir** - Makro, bazı görevlerin kullanıcı için daha kolay hale getirilmesini amaçlayan önceden tanımlanmış adımlar dizisidir (MS Word makroları yaygın olarak bilinir). Makro, potansiyel olarak tehlikeli talimatlar içerebilir. Makro içeren dosyaların şüpheli olarak bildirilmesini sağlamak için kutuyu işaretleyebilirsiniz.

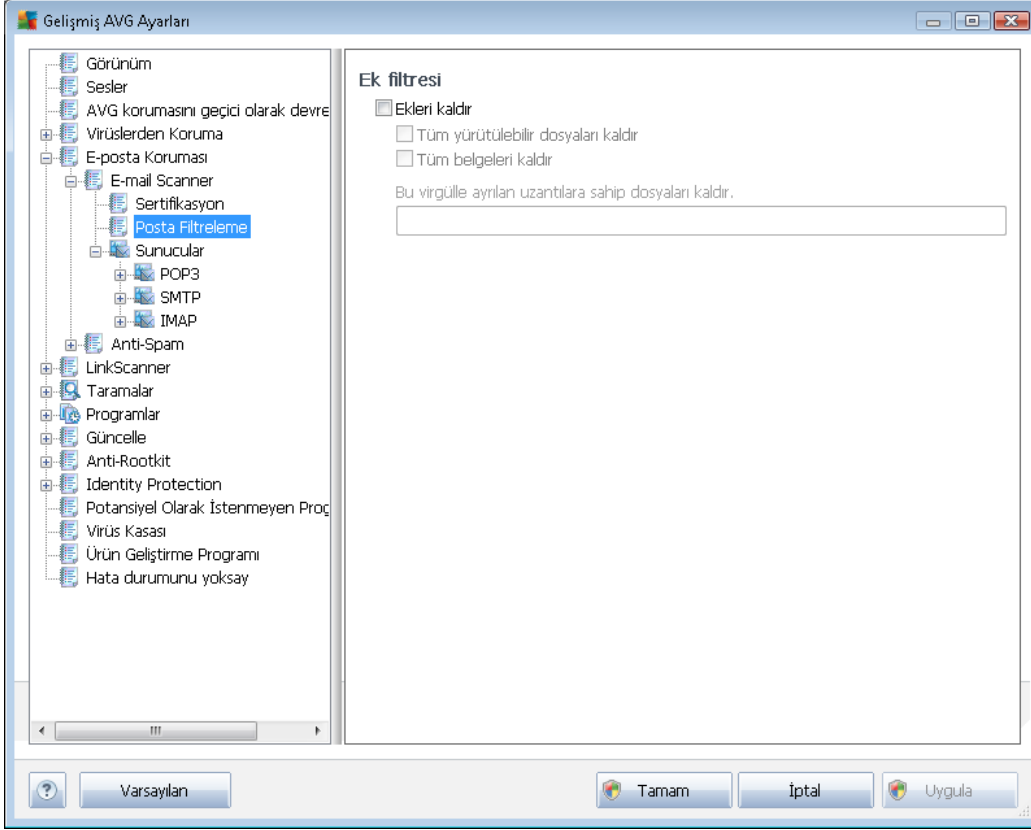
- **Gizlenen uzantıları bildir** - gizli uzantılar şüpheli bir çalıştırılabilir dosyayı (örn. "birşey.txt.exe") zararsız bir düz metin dosyası gibi (örn. "birşey.txt") gösterebilir; bunları potansiyel olarak tehlikeli olarak bildirmek için kutuyu işaretleyin.
- **Rapor edilen ekleri Virüs Kasasına taşı** - taranan e-posta iletilisinin ekinde gizli bir eklenti tespit edildiğinde parola korumalı arşivler, parola korumalı belgeler, makro içeren belgeler ve/veya dosyalar hakkında e-posta vasıtasıyla bilgilendirilmek isteyip istemediğinizi belirtin. Tarama işlemi sırasında bu tür bir mesaj tespit edilirse tespit edilen bulaşmış nesnenin [Virüs Kasasına](#) taşınmasını isteyip istemediğinizi belirtin.

Sertifika iletişim kutusunda gelen ve/veya giden e-postaları onaylamaya (**Gelen e-postayı onayla**) veya onaylamamaya (**Giden e-postayı onayla**) karar vermek için çeşitli onay kutularını işaretleyebilirsiniz. Bu seçeneklerin her biri için **Yalnızca ekleri olanlar** parametresini işaretleyip onayın yalnızca ekleri olan e-postalara eklenmesini sağlayabilirsiniz:



Varsayılan olarak, onay mesajı şunun gibi temel bilgiler içerir: *Bu iletide virüs bulunamadı gibi*. Ancak, bu bilgiler ihtiyaçlarınıza göre artırılabilir veya değiştirilebilir: **E-posta onay metni** alanına istediğiniz onay metnini yazın. **E-posta onay metni için kullanılan dil** bölümünde onayın otomatik olarak oluşturulan kısmının (*Bu iletide virüs bulunamadı*) hangi dilde görüntüleneceğini de belirleyebilirsiniz.

Not: İstenen dilde yalnızca varsayılan metnin görüntüleneceğine ve özelleştirilmiş metninizin otomatik olarak çevrilmeyeceğine dikkat edin!



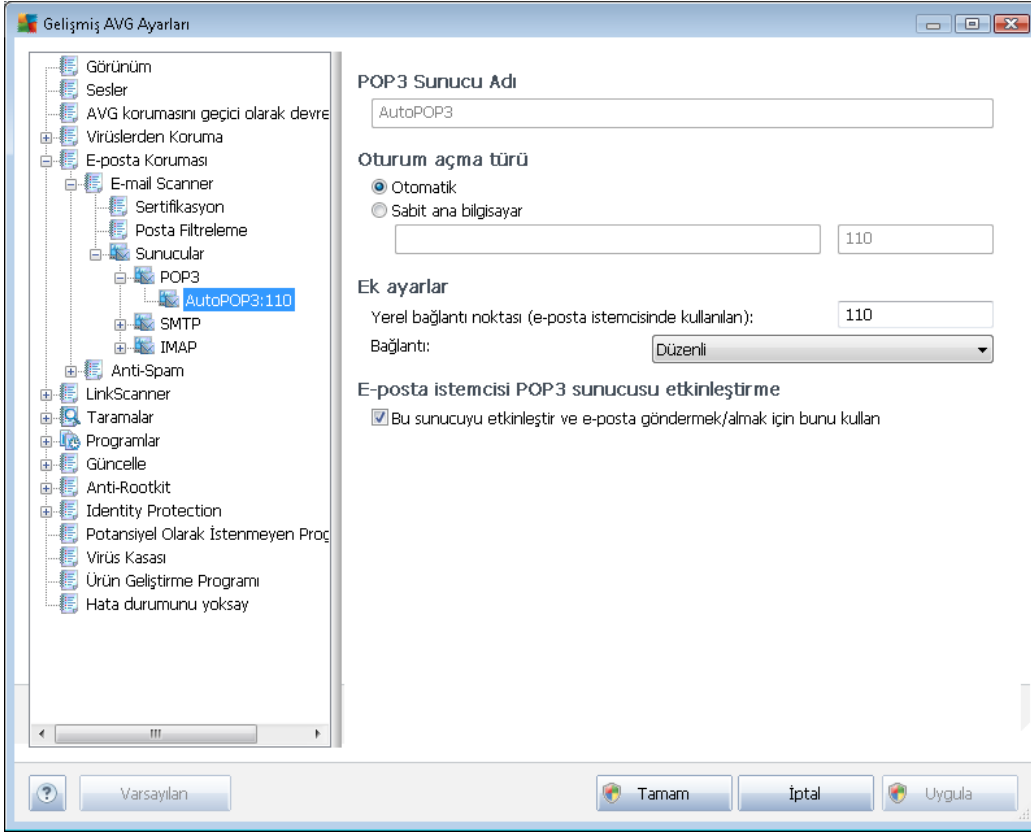
Ek filtresi iletişim kutusu, e-posta mesajlarının eklentilerinin taranmasına ilişkin parametreleri ayarlayabilmeyi sağlar. Varsayılan olarak **Eklentileri sil** seçeneği kapalıdır. Etkinleştirmeye karar verirsiniz tüm e-posta mesajlarının eklentileri, bulaşmış nesne ya da potansiyel olarak tehlikeli nesne olarak algılanacak ve silinecektir. Belirli ek türlerinin silinmesini istiyorsanız ilgili seçeneği seçin:

- **Tüm çalıştırılabilir dosyaları sil** - tüm *.exe dosyaları silinecektir
- **Tüm belgeleri kaldır** - tüm *.doc, *.docx, *.xls, *.xlsx dosyaları silinecektir
- **Virgülle ayrılmış şu uzantılara sahip dosyaları kaldır** - Tanımlanan uzantılara sahip tüm dosyalar kaldırılacaktır

Sunucular bölümünde [E-posta Tarayıcısı](#) sunucularının parametrelerini düzenleyebilirsiniz:

- [POP3 sunucusu](#)
- [SMTP sunucusu](#)
- [IMAP sunucusu](#)

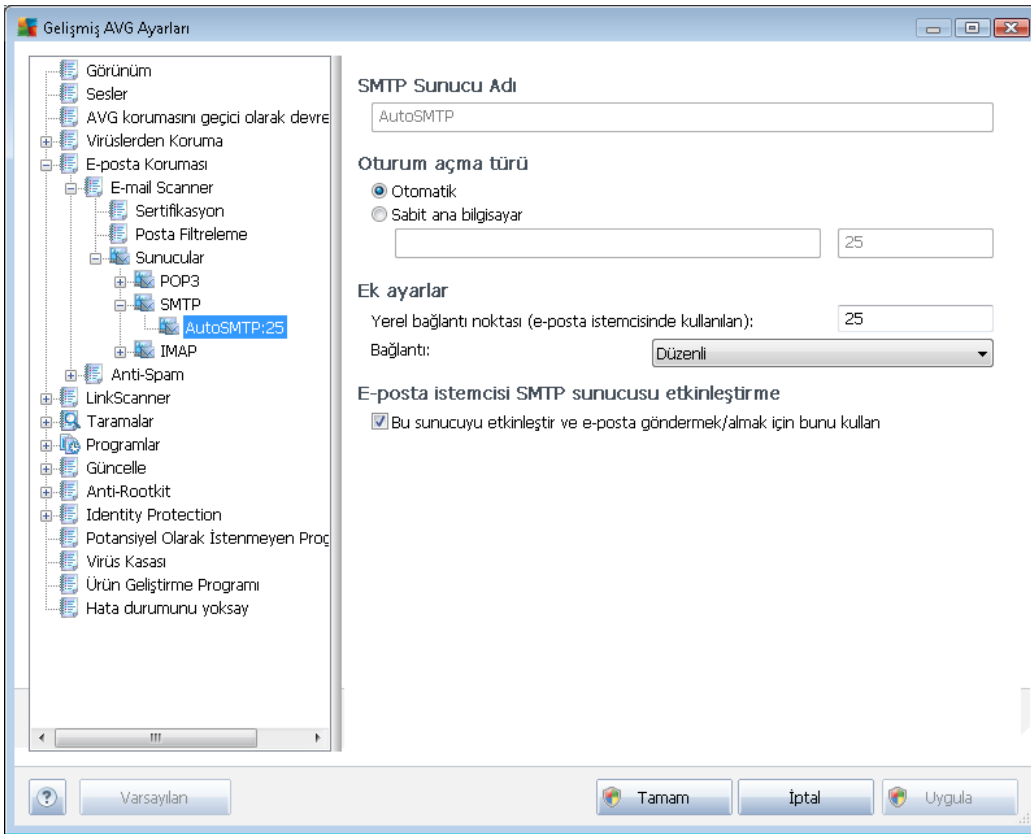
Ayrıca, **Yeni sunucu ekle** düğmesiyle gelen ve giden postalar için yeni sunucu tanımlayabilirsiniz.



(**Sunucular / POP3** ile açılan) bu iletişim kutusunda, gelen postalar için POP3 protokolü kullanarak yeni bir [E-posta Tarayıcısı](#) sunucusu kurabilirsiniz:

- **POP3 Sunucusunun Adı** - bu alanda yeni eklenen sunucuların adını belirtebilirsiniz (*bir POP3 sunucusu eklemek için, sol menü ağacının POP3 ögesinin üzerinde sağ fare düğmesini tıklayın*). Otomatik olarak oluşturulan "AutoPOP3" sunucusu için bu alan devre dışı bırakılmıştır.
- **Oturum açma tipi** - gelen postalar için kullanılan posta sunucularının belirlenmesi sırasında kullanılan yöntemi tanımlar:
 - **Otomatik** - Oturum açma işlemi, e-posta istemcinizin ayarlarına göre otomatik olarak gerçekleştirilir.
 - **Sabit ana bilgisayar** - Bu durumda, program her zaman burada belirtilen sunucuyu kullanır. Lütfen posta sunucunuzun adresini veya adını belirtin. Oturum açma adı değişmez. Ad için, IP adresinin yanı sıra (*örneğin, 123.45.67.89*) etki alanı adı da (*örneğin, pop.acme.com*) kullanabilirsiniz. Posta sunucusu standart olmayan bir bağlantı noktası kullanıyorsa, bu bağlantı noktasını ayrı olarak iki nokta üst üste kullanarak sunucu adının arkasına yazabilirsiniz (*örn. smtp.acme.com:8200*). POP3 iletişimi için standart bağlantı noktası 110'dur.

- **Diğer ayarlar** - daha ayrıntılı parametreleri belirler:
 - **Yerel bağlantı noktası** - Posta uygulamanızın iletişim kurması beklenen bağlantı noktasını belirler. Posta uygulamanızda, bu bağlantı noktasını POP3 iletişimi bağlantı noktası olarak belirtmeniz gerekir.
 - **Bağlantı** - kullanılacak bağlantı türünü aşağı açılır menüden belirtebilirsiniz (normal/SSL/SSL varsayılan). SSL bağlantıyı tercih ederseniz, gönderilen veri, üçüncü bir taraf tarafından izlenme riski olmayacak şekilde şifrelenir. Bu özellik de, yalnızca hedef posta sunucusu tarafından desteklendiğinde kullanılabilir.
- **E-posta istemcisi POP3 sunucusu etkinleştirme** - belirtilen POP3 sunucusunu etkinleştirmek veya devre dışı bırakmak için bu öğeyi işaretleyin/işaretini kaldırın.



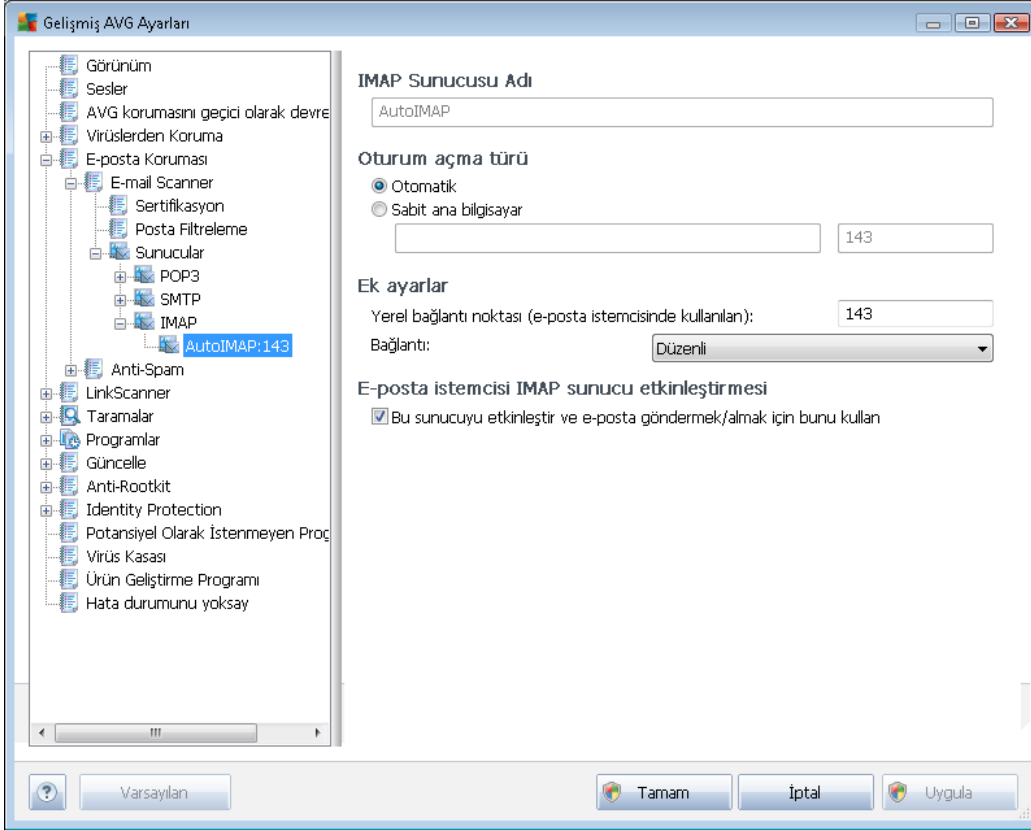
Bu iletişim kutusunda (**Sunucular /SMTP üzerinden açılır**) yeni bir [E-posta Tarayıcısı](#) sunucusu belirlemek üzere giden postalar için SMTP protokolünü kullanabilirsiniz:

- **SMTP Sunucusunun Adı** - bu alanda yeni eklenen sunucuların adını belirtebilirsiniz (bir SMTP sunucusu eklemek için, sol menü ağacının SMTP öğesinin üzerinde sağ fare düğmesini tıklayın). Otomatik olarak oluşturulan "AutoSMTP" sunucusu için bu alan devre dışı bırakılmıştır.
- **Oturum açma tipi** - giden postalar için kullanılan posta sunucularının tanımlanması



sırasında kullanılan yöntemdir:

- **Otomatik** - oturum açma işlemi, e-posta istemcinizin ayarlarına göre otomatik olarak gerçekleştirilir
- **Sabit ana bilgisayar** - bu durumda, program her zaman burada belirtilen sunucuyu kullanır. Lütfen posta sunucunuzun adresini veya adını belirtin. Ad için, IP adresinin yanı sıra (örneğin, 123.45.67.89) etki alanı adı da (örneğin, smtp.acme.com) kullanabilirsiniz. *Posta sunucusu standart olmayan bir bağlantı noktası kullanıyorsa, bu bağlantı noktasını ayırıcı olarak iki nokta üst üste kullanarak sunucu adının arkasına girebilirsiniz (örn. smtp.acme.com:8200).* SMTP iletişimi için standart bağlantı noktası 25'tir.
- **Diğer ayarlar** - daha ayrıntılı parametreleri belirler:
 - **Yerel bağlantı noktası** - Posta uygulamanızın iletişim kurması beklenen bağlantı noktasını belirler. Posta uygulamanızda, bu bağlantı noktasını SMTP iletişimi bağlantı noktası olarak belirtmeniz gerekir.
 - **Bağlantı** - bu açılır aşağı menüden, kullanılacak bağlantı türünü belirtebilirsiniz (*normal/SSL/SSL varsayılan*). SSL bağlantıyı tercih ederseniz, gönderilen veri, üçüncü bir taraf tarafından izlenme riski olmayacak şekilde şifrelenir. Bu özellik, yalnızca hedef posta sunucusu tarafından desteklendiğinde kullanılabilir.
- **E-posta istemcisi SMTP sunucusu aktivasyonu** - yukarıda belirtilen SMTP sunucusunu etkinleştirmek/devre dışı bırakmak için bu kutuyu işaretleyin/işaretini kaldırın



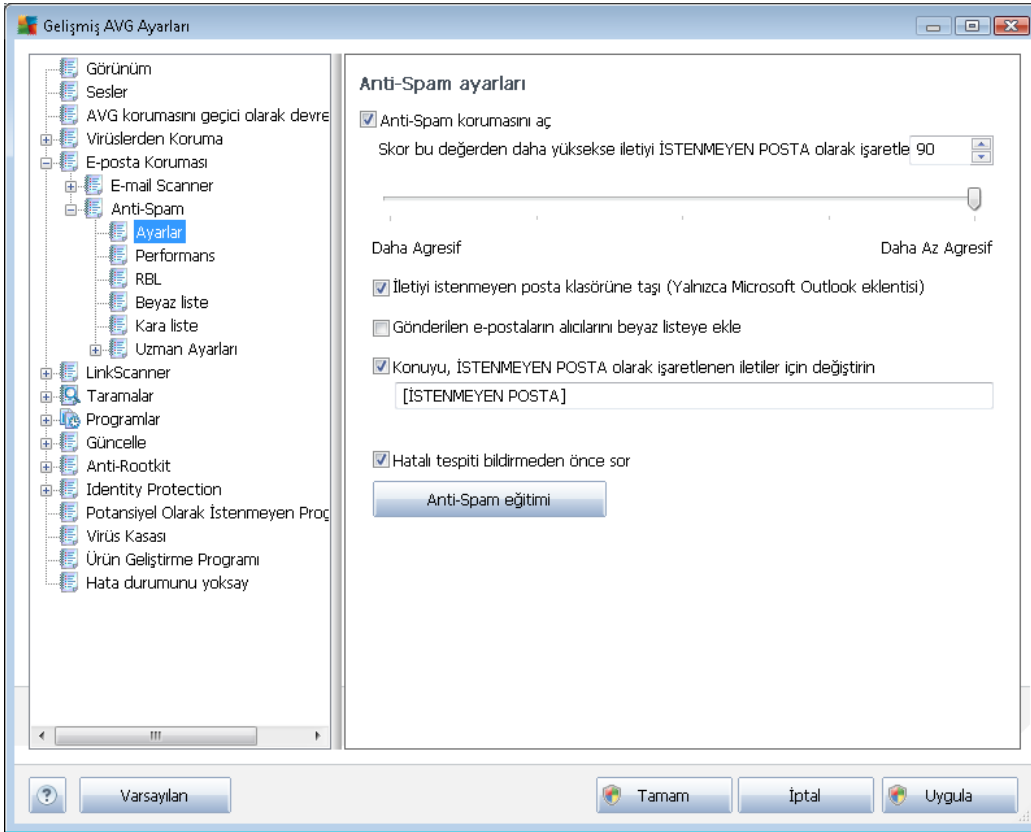
Bu iletişim kutusunda (**Sunucular /IMAP üzerinden açılır**) yeni bir [E-posta Tarayıcısı](#) sunucusu belirlemek üzere giden postalar için SMTP protokolünü kullanabilirsiniz:

- **IMAP Sunucusunun Adı** - bu alanda yeni eklenen sunucuların adını belirtebilirsiniz (*bir IMAP sunucusu eklemek için, sol menü ağacının IMAP ögesinin üzerinde sağ fare düğmesini tıklayın*). Otomatik olarak oluşturulan "AutoIMAP" sunucusu için bu alan devre dışı bırakılmıştır.
- **Oturum açma tipi** - giden postalar için kullanılan posta sunucularının tanımlanması sırasında kullanılan yöntemdir:
 - **Otomatik** - oturum açma işlemi, e-posta istemcinizin ayarlarına göre otomatik olarak gerçekleştirilir
 - **Sabit ana bilgisayar** - bu durumda, program her zaman burada belirtilen sunucuyu kullanır. Lütfen posta sunucunuzun adresini veya adını belirtin. Ad için, IP adresinin yanı sıra (*örneğin, 123.45.67.89*) etki alanı adı da (*örneğin, smtp.acme.com*) kullanabilirsiniz. Posta sunucusu standart olmayan bir bağlantı noktası kullanıyorsa, bu bağlantı noktasını ayırıcı olarak iki nokta üst üste kullanarak sunucu adının arkasına yazabilirsiniz (*örneğin, smtp.acme.com:8200*). IMAP iletişiminin standart bağlantı noktası 143'tür.
- **Diğer ayarlar** - daha ayrıntılı parametreleri belirler:

- **Yerel bağlantı noktası** - posta uygulamanızın iletişim kurması beklenen bağlantı noktasını belirler. Bundan sonra, posta uygulamanızda, bu bağlantı noktasını IMAP iletişimi bağlantı noktası olarak belirtmeniz gerekir.
- **Bağlantı** - bu açılır aşağı menüden, kullanılacak bağlantı türünü belirtebilirsiniz (*normal/SSL/SSL varsayılan*). SSL bağlantıyı tercih ederseniz, gönderilen veri, üçüncü bir taraf tarafından izlenme riski olmayacak şekilde şifrelenir. Bu özellik, yalnızca hedef posta sunucusu tarafından desteklendiğinde kullanılabilir.
- **E-posta istemcisi IMAP sunucusu aktivasyonu** - yukarıda belirtilen IMAP sunucusunu etkinleştirmek/devre dışı bırakmak için bu kutuyu işaretleyin ve kutunun işaretini kaldırın

9.5.2. İstenmeyen E-postaya Karşı Koruma

Konu metnini buraya girin.



İstenmeyen Posta Önleme ayarları iletişim kutusunda **İstenmeyen Posta Önleme korumasını aç** onay kutusunu işaretleyerek/işaretini kaldırarak e-posta iletişiminin istenmeyen posta önleme taramasına izin verebilir ya da engelleyebilirsiniz. Bu seçenek varsayılan olarak açıktır ve geçerli bir neden olmadıkça her zaman bu yapılandırmayı korumanız önerilir.

Sonra, daha fazla ya da daha az agresif değerlendirme ölçütleri de seçebilirsiniz. **İstenmeyen Posta Önleme** filtresi, çeşitli dinamik tarama teknikleri sayesinde mesajlardan her birine bir puan verir (*mesajın içeriğinin İSTENMEYEN POSTA'ya ne kadar yakın olduğunu belirlemek üzere*). Değer girerek ya da kaydırma çubuğunu sağa ya da sola hareket ettirerek (*değer aralığı 50 ile 90*



arasındadır) **Puan'dan fazla ise istenmeyen posta olarak işaret**le ögesini ayarlayabilirsiniz.

Genel olarak eşiği 50 ila 90 arasında bir değere ayarlamanızı veya gerçekten emin değilseniz 90 olarak ayarlamanızı öneririz. Burada puan eşiği hakkında genel bilgi verilmektedir:

- **Değer 80-90** - istenmeyen posta olması muhtemel e-posta mesajları filtrelenecektir. İstenmeyen posta olmayan bazı postalar yanlışlıkla istenmeyen posta şeklinde etiketlenebilir.
- **Değer 60-79** - Oldukça etkili bir yapılandırma olarak değerlendirilir. İstenmeyen posta olması muhtemel e-posta mesajları filtrelenecektir. İstenmeyen posta olmayan mesajların da yakalanma ihtimali vardır.
- **Değer 50-59** - Çok agresif yapılandırma. İstenmeyen posta olmayan e-posta iletilerinin de gerçek istenmeyen posta iletileri ile birlikte yakalanma ihtimali çok yüksektir. Bu eşik aralığı normal kullanım için önerilmez.

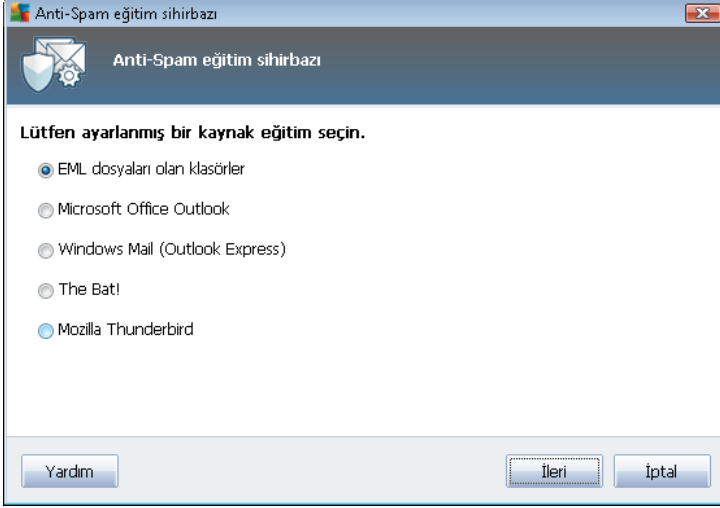
İstenmeyen Posta Önleme ayarları iletişim kutusunda, tespit edilen istenmeyen postalara ne yapılacağını da belirleyebilirsiniz:

- **Mesajı önemsiz posta klasörüne taşı** - algılanan istenmeyen mesajların, otomatik olarak e-posta istemcinizin önemsiz posta klasörüne taşınmasını istiyorsanız bu seçeneği seçin;
- **Gönderilen e-postaların göndericilerini beyaz listeye** ekle - gönderilen e-postaların göndericilerinin tümüne güvendiğinizi onaylamak ve söz konusu kişilerin e-posta hesaplarından gönderilen e-postaların daima alınmasını istediğinizi teyit etmek için bu kutuyu işaretleyin.
- **İstenmeyen posta olarak işaretlenmiş mesajların konusunu değiştir** - İstenmeyen posta olarak işaretlenmiş e-postaların konu alanına belirli bir kelime ya da ibarenin yazılmasını istiyorsanız bu onay kutusunu işaretleyin; istenen metin, etkinleştirilen metin alanına yazılabilir.
- **Hatalı tespiti bildirmeden önce sor** - [yükleme süreci](#) sırasında [Ürün Geliştirme Programı](#) 'na katılmayı kabul ettiğinizde sağlanır. Kabul ettiyseniz, tespit edilen tehditlerin AVG'ye bildirilmesine izin verirsiniz. Bu raporlama otomatik olarak yapılır. Ancak, gerçekten istenmeyen posta olarak sınıflandırılması gerekip gerekmediğinden emin olmak için, tespit edilen istenmeyen posta AVG'ye bildirilmeden önce sorulmasını istediğinizi onaylamak için bu onay kutusunu işaretleyebilirsiniz.

Kontrol düğmeleri

Anti-Spam'ı Eğitin düğmesi, [bir sonraki bölümde](#) ayrıntılarla açıklanan [Anti-Spam eğitim sihirbazı](#)'nı açar.

İstenmeyen Posta Önleme Eğitim Sihirbazının ilk iletişim kutusu, eğitim için kullanmak istediğiniz e-posta iletileri kaynağını seçmenizi belirtir. Genellikle yanlışlıkla İSTENMEYEN POSTA olarak işaretlenen e-postaları ya da tanınmayan gereksiz mesajları kullanmak isteyeceksiniz.



Aşağıdaki seçenekler arasından seçim yapabilirsiniz:

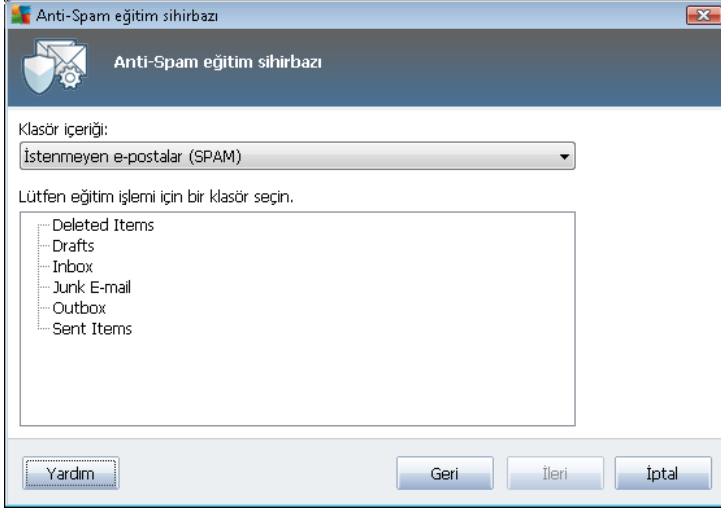
- **Özel bir e-posta istemcisi** - listelenen e-posta istemcilerinden birini kullanıyorsanız (*MS Outlook, Outlook Express, The Bat!*), ilgili seçeneği belirlemeniz yeterlidir
- **EML dosyalı klasörler** - Başka bir e-posta programı kullanıyorsanız, öncelikle iletileri belirli bir klasöre kaydetmeniz (*.eml* biçiminde) veya e-posta istemcisi ileti klasörlerinin konumunu biliyor olmanız gerekir. Sonra, **EML dosyaları içeren klasör** seçeneğini seçin; bu, sonraki adımda istenen klasörü bulmanızı sağlayacaktır

Eğitim sürecinin daha hızlı ve kolay olması için, klasörlerdeki e-postaları önceden sıralayabilirsiniz; böylece eğitim için kullanacağınız klasör yalnızca eğitim iletilerini (istenen veya istenmeyen) içerecektir. Ancak, e-postaları daha sonra filtreleyebileceğiniz için bu gerekli değildir.

Uygun seçeneği seçin ve sihirbaza devam etmek için **İleri** ögesini tıklayın.

Bu adımda görüntülenen iletişim kutusu daha önceki seçimlerinize bağlıdır.

EML dosyalarının bulunduğu klasörler



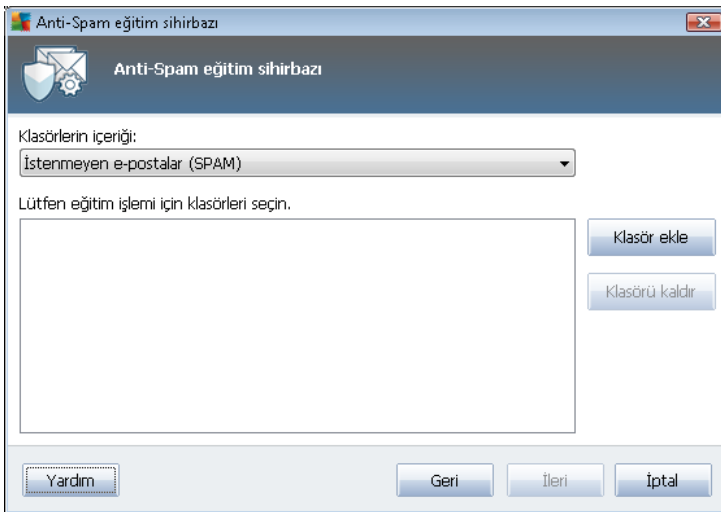
Bu iletişim kutusunda, eğitim için kullanmak istediğiniz iletilerin bulunduğu klasörün konumunu bulun. .eml **dosyalarının (kaydedilen e-posta iletileri) bulunduğu klasörün konumunu seçmek için** Klasör ekle düğmesine basın. Seçilen klasör, iletişim kutusunda görüntülenir.

Klasörlerin içeriği: açılır menüsünde, aşağıdaki iki seçenektan birini ayarlayın: seçilen klasör istenen (HAM) veya istenmeyen (SPAM) iletileri içerir. Bir sonraki adımda iletileri filtreleyebileceğinizi unutmayın; bu nedenle klasörün yalnızca eğitim e-postalarını içermesi zorunlu değildir. **Klasörü sil** düğmesine basarak istenmeyen klasörleri listeden silebilirsiniz.

Tamamladığınız zaman [Mesaj filtreleme seçenekleri](#) penceresine geçmek için **İleri** öğesini tıklayın.

Özel e-posta istemcileri

Seçeneklerden birini onayladığınız zaman yeni bir iletişim kutusu açılacaktır.

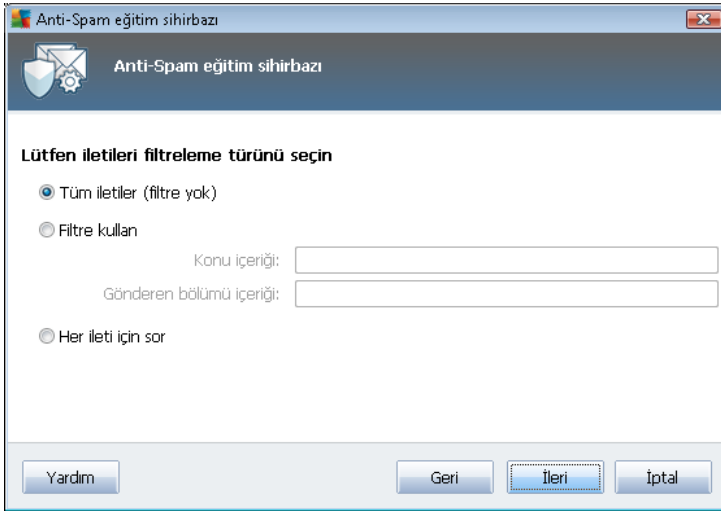


Not: Microsoft Office Outlook kullanıyor olmanız halinde ilk olarak MS Office Outlook profilini

seçmeniz istenecektir.

Klasörlerin içeriği: açılır menüsünde, aşağıdaki iki seçenektten birini ayarlayın: seçilen klasör istenen (*HAM*) veya istenmeyen (*SPAM*) iletileri içerir. Bir sonraki adımda iletileri filtreleyebileceğinizi unutmayın; bu nedenle klasörün yalnızca eğitim e-postalarını içermesi zorunlu değildir. Seçilen e-posta istemcisinin ağaç menüsü iletişim kutusunun ana bölümünde görüntülenir. Lütfen istediğiniz klasörü ağaç menüden bulun ve fareyle vurgulayın.

Tamamladığınız zaman [Mesaj filtreleme seçenekleri](#) penceresine geçmek için **İleri** ögesini tıklayın.

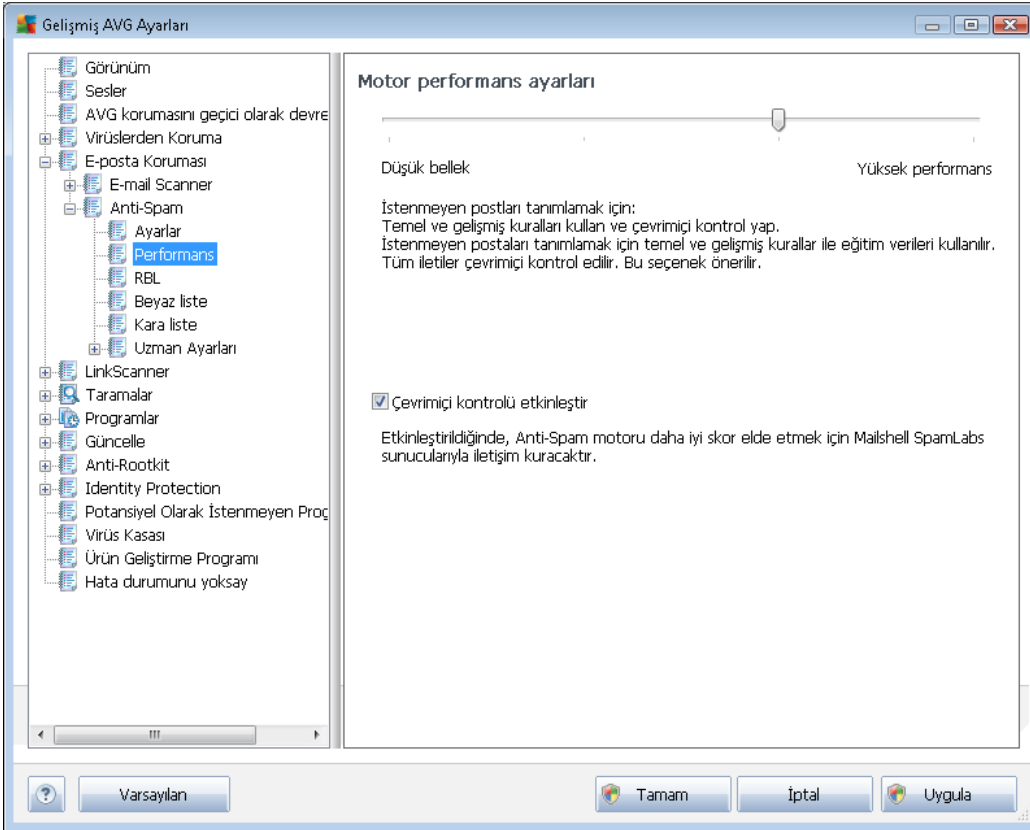


Bu iletişim kutusunda, e-posta iletileri filtrelemesini ayarlayabilirsiniz.

- **Tüm iletiler (filtre yok)** - Seçilen klasörün yalnızca eğitim için kullanmak istediğiniz iletileri içerdiğinden eminseniz, **Tüm iletiler (filtre yok)** seçeneğini işaretleyin.
- **Filtre kullan** - Daha gelişmiş filtreleme için **Filtre kullan** seçeneğini işaretleyin. E-posta konu ve/veya gönderici alanında arama yapmak için bir kelime (*ad*), bir kelime bölümü veya cümle parçası girebilirsiniz. Girilen kriterle tam olarak eşleşen tüm mesajlar, başka bir uyarı yapılmaksızın eğitim için kullanılacaktır. Her iki metin alanına da giriş yaptığınızda, yalnızca iki durumdan biriyle eşleşen adresler kullanılacaktır!
- **Her ileti için sor** - Klasörün içerdiği iletilerden emin değilseniz ve Sihirbazın her ileti için size sormasını istiyorsanız (*eğitim için kullanılıp kullanılmayacağını belirleyebilirsiniz*), **Her ileti için sor** seçeneğini işaretleyin.

Uygun seçenek seçildiği zaman **İleri** ögesine tıklayın. Bir sonraki iletişim kutusu tamamen bilgi amaçlıdır ve sihirbaz sizi işlem mesajları hakkında bilgilendirmeye hazırdır. Eğitime başlamak için yeniden **İleri** düğmesine basın. Daha önce seçtiğiniz koşullar doğrultusunda eğitim başlayacaktır.

Motor performans ayarları iletişim kutusu, (solda bulunan dolaşım alanında **Performans** ögesi altında bağlantısı verilen) **Anti-Spam** bileşeninin performans ayarlarının yapılmasını sağlar:



Tarama performans seviyesini **Düşük bellek / Yüksek performans** modları arasında yapılandırmak için çubuğu sola ya da sağa kaydırın.

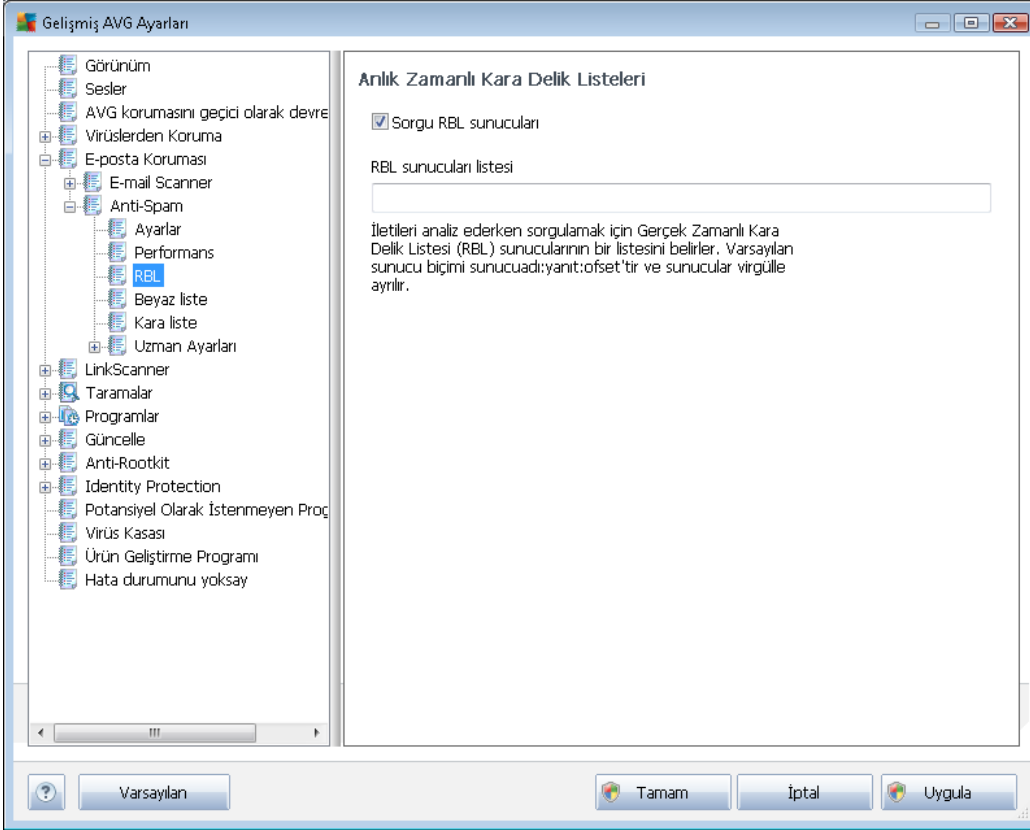
- **Düşük bellek** - tarama işlemi sırasında istenmeyen postaların tespit edilmesi için herhangi bir kural kullanılmayacaktır. Tanımlama için sadece eğitim verileri kullanılacaktır. Bu mod, bilgisayar donanımlarınız çok eski değil ise genel kullanım için önerilmemektedir.
- **Yüksek performans** - Bu mod, belleği oldukça yoğun şekilde kullanacaktır. Tarama işlemi sırasında istenmeyen postaları ayırt etmek için şu özellikler kullanılacaktır: kurallar ve istenmeyen posta veritabanı önbelleği, temel ve gelişmiş kurallar, istenmeyen postayı gönderenin IP adresi ve gönderici veritabanları.

Çevrimiçi taramayı etkinleştir ögesi varsayılan olarak açıktır. Ana sunucular ile iletişim kurmak vasıtasıyla [istenmeyen postaları](#) daha hassas şekilde tespit edilmesini sağlar. Diğer bir deyişle, taranan veriler çevrimiçi [Ana](#) veritabanları ile karşılaştırılacaktır.

Genellikle varsayılan ayarları kullanmanız ve geçerli bir nedeniniz varsa söz konusu ayarları değiştirmeniz önerilir. Yapılandırma sadece uzman kullanıcılar tarafından değiştirilmelidir!



RBL ögesi **Gerçek Zamanlı Kara Delik Listeleri** adlı bir düzenleme iletişim kutusu açar ve **Sorgu RBL sunucuları** işlevini açabilir/kapatabilirsiniz:

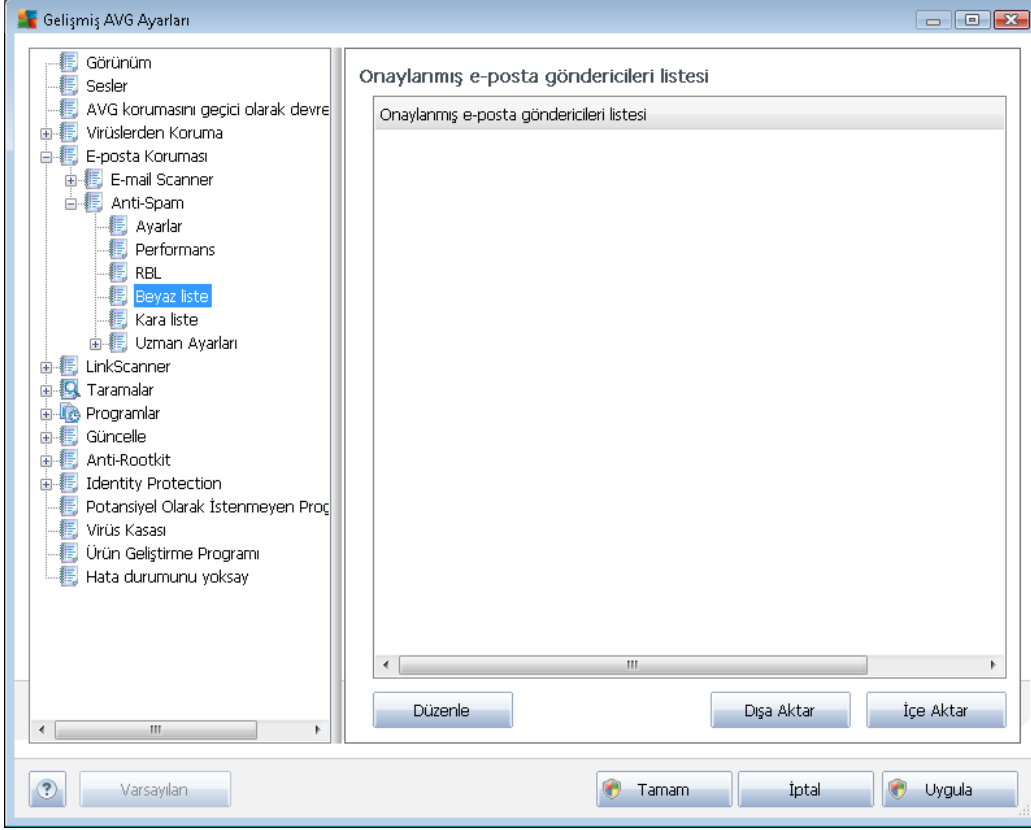


RBL (Gerçek Zamanlı Kara Delik Listesi) sunucusu, bilinen istenmeyen posta gönderen kişilerin kapsamlı bir veritabanının bulunduğu bir DNS sunucusudur. Bu özellik açıldığı zaman tüm e-posta mesajları RBL sunucusu veritabanı ile karşılaştırmalı olarak kontrol edilecek ve veritabanı girişlerinden herhangi biri ile aynı ise istenmeyen posta olarak etiketlenecektir. RBL Sunucularının veritabanları en son güncel istenmeyen posta parmak izlerini içerir, en iyi ve en doğru istenmeyen posta tespit hizmetini sağlar. Bu özellik, normalde [Anti-Spam](#) motoru tarafından tespit edilmeyen büyük miktarlarda istenmeyen posta alan kullanıcılar için yararlıdır.

RBL sunucuları listesi belirli RBL sunucu konumlarını tanımlayabilmenizi sağlar (her mesajın RBL sunucu veritabanından doğrulanmasını gerektirdiğinden, bu özelliğin etkinleştirilmesi bazı sistem veya yapılandırılarda e-posta alım işlemlerinde yavaşlamaya neden olabilir).

Sunucuya herhangi bir kişisel bilgi gönderilmez!

Beyaz Liste ögesi, mesajları hiçbir zaman istenmeyen posta olarak algılanmayacak olan onaylanan gönderen e-posta adresleri ve etki alanı adlarının genel bir listesini içeren **Onaylanmış e-posta gönderenleri listesi** adlı bir iletişim kutusu açar.



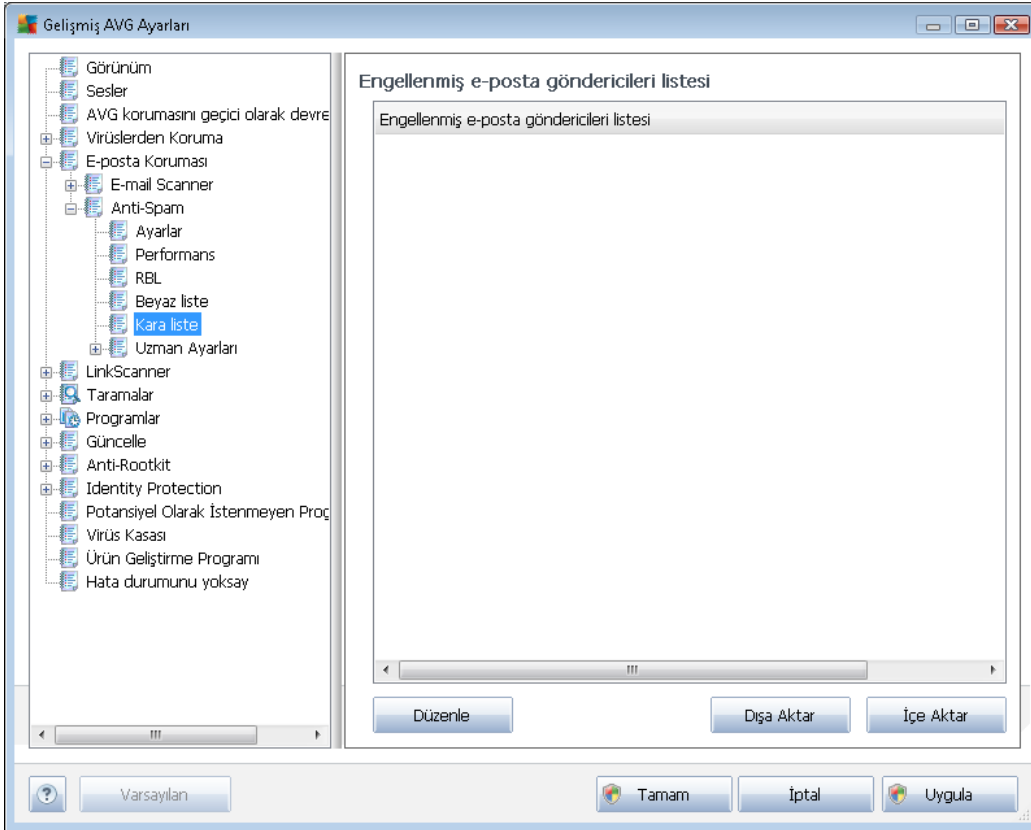
Düzenleme arayüzünde asla istenmeyen posta (istenmeyen posta) göndermeyecek göndericilerden oluşan bir liste düzenleyebilirsiniz. Bunun yanı sıra istenmeyen mesaj göndermediğini bildiğiniz tüm etki alanı adlarını içeren (ör. avg.com) bir liste de oluşturabilirsiniz. Hazırlanan gönderen ve/veya etki alanı adı listesine sahip olduğunuzda, aşağıdaki yöntemlerden biriyle bunları girebilirsiniz: her e-posta adresini doğrudan girerek veya adreslerin tam listesini bir defada içe aktararak.

Kontrol düğmeleri

Şu kontrol düğmeleri bulunur:

- **Düzenle** - adres listesini manüel olarak doldurabileceğiniz iletişim kutusunu açmak için bu düğmeye basın (*bunun yanı sıra kopyala ve yapıştır* yöntemini de kullanabilirsiniz). Satır başına bir öge ekleyin (*gönderen, etki alanı adı*).
- **Dışa Aktar** - Kayıtları belli bir amaçla dışa aktarmaya karar vererseniz, bu düğmeye basarak dışa aktarabilirsiniz. Tüm kayıtlar temel metin dosyasına kaydedilecektir.
- **İçe aktar** - hazırladığınız e-posta adreslerinin/alan adlarının bulunduğu bir metin dosyasına sahipseniz, bu düğmeyi seçerek kolayca içe aktarabilirsiniz. Dosya içeriğinin her satır için yalnızca bir öge (*adres, alan adı*) içermesi gerekir.

Kara liste öğesi engellenmiş gönderici e-posta adresleri ve iletileri her zaman gereksiz posta olarak işaretlenecek alan adlarının global bir listesinin bulunduğu bir iletişim kutusu açar.



Düzenleme arayüzünde, istenmeyen ileti (*istenmeyen posta*) göndermesini beklediğiniz göndericilerin bir listesini oluşturabilirsiniz. Ayrıca istenmeyen mesajlar beklediğiniz veya aldığınız tam alana adlarının (*örn. spammingcompany.com*) bir listesini oluşturabilirsiniz. Listelenen adreslerden/alan adlarından gelecek tüm e-postalar istenmeyen posta olarak tanımlanacaktır. Hazırlanan gönderen ve/veya etki alanı adı listesine sahip olduğunuzda, aşağıdaki yöntemlerden biriyle bunları girebilirsiniz: her e-posta adresini doğrudan girerek veya adreslerin tam listesini bir defada içe aktararak.

Kontrol düğmeleri

Şu kontrol düğmeleri bulunur:

- **Düzenle** - adres listesini manüel olarak doldurabileceğiniz iletişim kutusunu açmak için bu düğmeye basın (*bunun yanı sıra kopyala ve yapıştır yöntemini de kullanabilirsiniz*). Satır başına bir öğe ekleyin (*gönderen, etki alanı adı*).
- **Dışa Aktar** - Kayıtları belli bir amaçla dışa aktarmaya karar vererseniz, bu düğmeye basarak dışa aktarabilirsiniz. Tüm kayıtlar düz bir metin dosyasına kaydedilecektir.



- **İçe aktar** - mevcut durumda hazırlamış olduğunuz bir gönderici / barındırma adı listesi varsa bu düğmeye basarak söz konusu dosyayı içe aktarabilirsiniz.

Gelişmiş Ayarlar bölümü Anti-Spam bileşenine ilişkin kapsamlı ayar seçenekleri sunar. Bu ayarlar özellikle deneyimli kullanıcılar, genel olarak e-posta sunucuları için en iyi korumayı sağlamak üzere istenmeyen postalardan korunmayı yapılandırmaya gereksinim duyan ağ yöneticileri için tasarlanmıştır. Bu nedenle, her bir iletişim kutusu için ayrıca yardım sunulmamaktadır. Ancak, ilgili her seçenek için kullanıcı arayüzünde doğrudan kısa bir açıklama bulunmaktadır.

Spamcatcher (MailShell Inc.) uygulamasının gelişmiş ayarlarıyla ilgili bilgileriniz yeterli değilse, hiçbir ayarı değiştirmemenizi önemle öneririz. Uygun olmayan her değişiklik performansın düşmesine veya bileşenin hatalı çalışmasına neden olabilir.

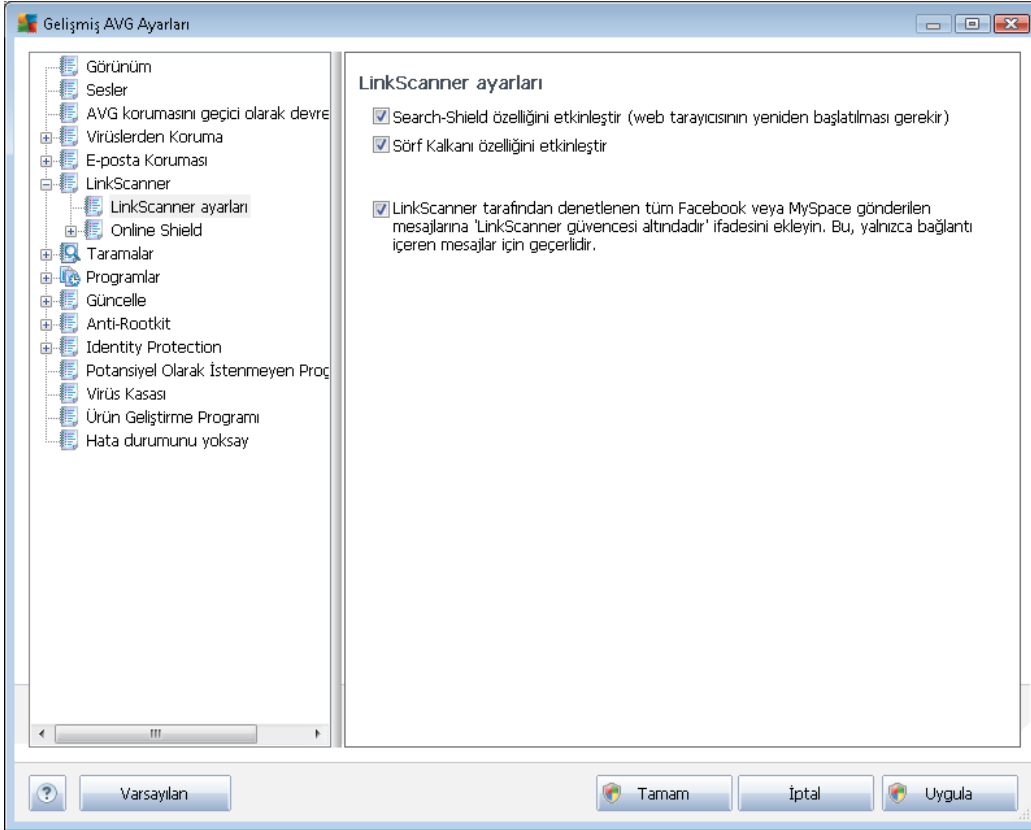
[Anti-Spam](#) yapılandırmasını gelişmiş seviyede değiştirmeniz gerektiğini düşünüyorsanız lütfen kullanıcı arayüzünde belirtilen talimatları izleyin. Genellikle iletişim pencerelerinin her birinde belirli bir özellik bulursunuz ve söz konusu özelliği düzenleyebilirsiniz - ilgili özellik aynı iletişim kutusunda tanımlanır.

- **Önbellek** - parmak izi, etki alanı, LegitRepute
- **Eğitim** - maksimum kelime girişi, otomatik eğitim eşiği, ağırlık
- **Filtreleme** - dil listesi, ülke listesi, onaylanan IP'ler, engellenen IP'ler, engellenen ülkeler, engellenen karakter setleri, sahte göndericiler
- **RBL** - RBL sunucuları, çoklu eşleşme, eşik, zaman aşımı, maksimum IP'ler
- **İnternet bağlantısı** - zaman aşımı, proxy sunucusu, proxy sunucusu kimlik doğrulaması

9.6. LinkScanner

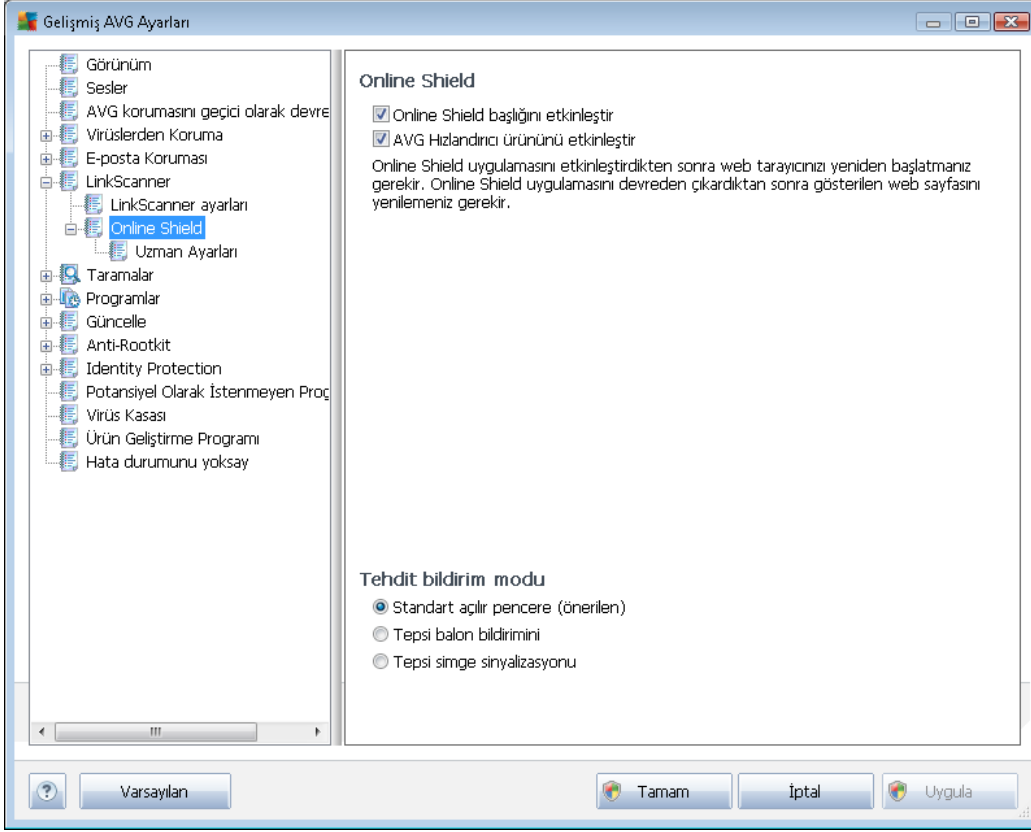
9.6.1. LinkScanner ayarları

[LinkScanner ayarları](#) iletişim kutusu, [LinkScanner](#) uygulamasının temel özelliklerini açıp kapatmanızı sağlar:



- **Arama Kalkanı'nı Etkinleştir** - (varsayılan olarak açıktır): Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg veya SlashDot ile yapılan aramalarda, arama motoru tarafından döndürülen içeriği önceden denetleyerek tavsiye niteliğinde uyarı simgeleri görüntüler.
- **Surf-Shield'i etkinleştir** - (varsayılan olarak açıktır): erişim sağlandığı anda güvenlik açığı olan web sitelerine karşı (anlık zamanlı) koruma sağlamak için etkinleştirin. Bilinen kötü amaçlı site bağlantıları ve güvenlik açığından yararlanan içerikler, kullanıcı bir web tarayıcısı (ya da HTTP kullanan diğer bir program) aracılığıyla erişim sağladığında engellenir.
- **'LinkScanner Tarafından Korunmaktadır' ibaresi ekle ...** - (varsayılan olarak açık): Facebook ve MySpace'den gönderilen etkin hiper bağlantıları içeren iletilerde [LinkScanner](#) denetimi ile ilgili sertifikasyon bildirimini girmek istediğinizi onaylamak için bu öğeyi işaretleyin.

9.6.2. Online Shield

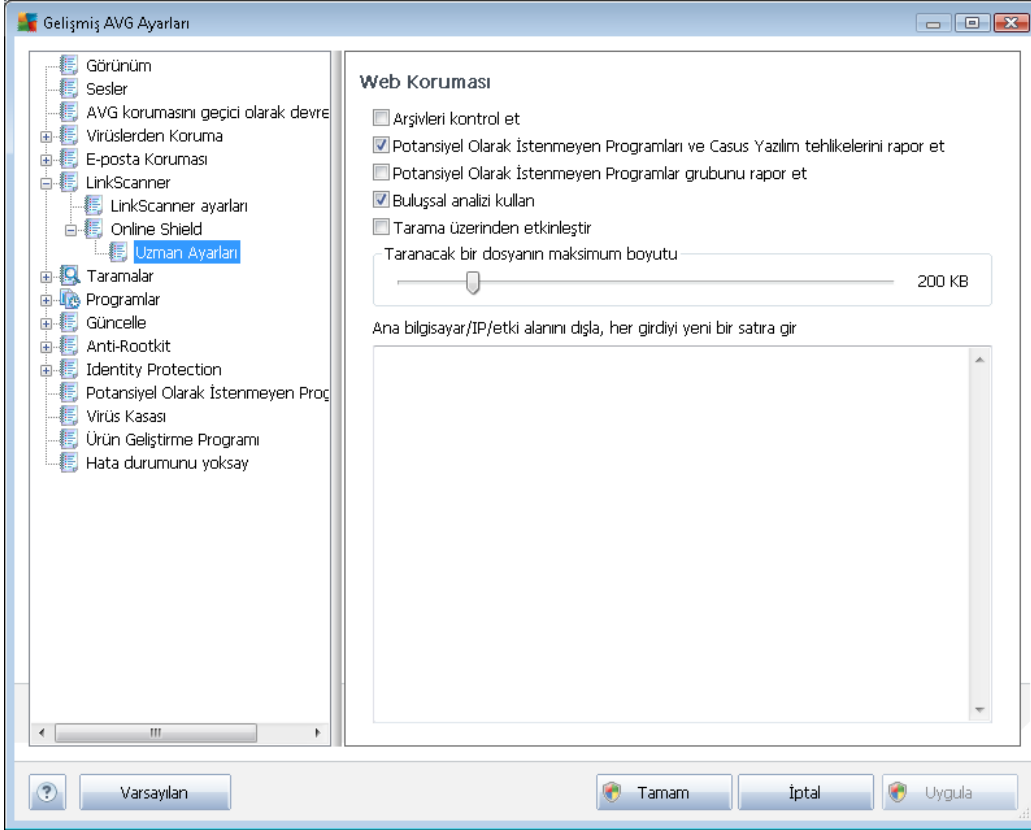


Online Shield iletişim kutusu şu seçenekleri sunar:

- **Online Shield'ı etkinleştir** (varsayılan olarak açık) - **Online Shield** hizmetinin tamamını etkinleştirir/devre dışı bırakır. Diğer **Online Shield** gelişmiş ayarları için lütfen [Web Koruması](#) adındaki sonraki iletişim kutusuna geçin.
- **AVG Accelerator'ı etkinleştir** (varsayılan olarak açık) - Daha düzgün çevrimiçi video oynatma ve ilave indirmeleri kolaylaştırma olanağı sağlayan **AVG Accelerator** hizmetini etkinleştirir/devre dışı bırakır.

Tehdit bildirim modu

İletişim kutusunun alt kısmında algılanması muhtemel tehdit hakkında ne şekilde bilgilendirilmek istediğinizi seçin: standart açılır iletişim kutusuyla, tepsi balon bildirimleriyle ya da tepsi simgesi bilgileriyle.



Web Koruması - web sitelerinin içeriğinin taranmasına ilişkin bileşen yapılandırmasını düzenleyebilirsiniz. Düzenleme arayüzü ile aşağıdaki temel seçenekleri yapılandırabilirsiniz:

- **Web korumasını etkinleştir** - bu seçenek **Online Shield**'in www sayfalarının içeriğinin taranmasını gerçekleştirmek gerektiğini onaylar. Bu seçeneğin etkin konumda olmasına rağmen (*varsayılan olarak*) söz konusu öğeleri açıp kapatabilirsiniz:
 - **Arşivleri denetle** - (*varsayılanda kapalıdır*): muhtemelen www sayfasında görüntülenecek arşivlerin içeriğini tarayın.
 - **Potansiyel Olarak İstenmeyen Programları ve Casus Yazılım tehditlerini rapor et** (*varsayılan olarak açık*) - [Anti-Spyware](#) motorunu etkinleştirmek ve virüslerin yanı sıra casus yazılımları da taramak için işaretleyin. [Casus yazılım](#), şüpheli kötü amaçlı yazılım kategorisini ifade eder: Genellikle güvenlik riski oluşturmasına rağmen bu programlardan bazıları bilerek yüklenebilir. Bilgisayarınızın güvenliğini artırdığından, bu özelliği etkin durumda tutmanızı öneriyoruz.
 - **Potansiyel Olarak İstenmeyen Programlar gelişmiş grubunu rapor et** - (*varsayılanda kapalıdır*): [casus yazılımların](#), yani doğrudan üreticiden alınan tamamen zararsız olan, ancak daha sonra kötüye kullanılacak programların genişletilmiş paketinin tespit edilmesi için işaretleyin. Bu, bilgisayar güvenliğinizi daha da artıran ek bir önlemdir, ancak yasal programları da engelleyebilir ve bu yüzden varsayılan olarak kapalıdır.



- **Buluşsal analiz yöntemini kulan** - (varsayılanda açıktır): görüntülenecek web sitesinin içeriği [buluşsal analiz](#) yöntemi kullanılarak taranır (*taranan nesnenin komutlarının sanal bir bilgisayar ortamında dinamik olarak canlandırılması*).
- **Kapsamlı taramayı etkinleştir** (varsayılanda kapalıdır) - belirli durumlarda (*bilgisayarınıza bulaşma olmasından şüpheleniliyorsa*) yalnızca emin olmak üzere bilgisayarınızın bulaşma olması çok zor olan alanlarını bile tarayan en kapsamlı tarama algoritmalarını etkinleştirmek için bu seçeneği işaretleyebilirsiniz. Ancak, bu yöntemin çok fazla zaman aldığını unutmayın.
- **Taranacak maksimum dosya bölümü büyüklüğü** - Dahil edilen dosyalar görüntülenen sayfada mevcutsa, bunları bilgisayarınıza indirmeden önce de içeriklerini tarayabilirsiniz. Ancak büyük dosyaların taranması zaman alabilir ve web sayfasının indirilmesi de önemli ölçüde yavaşlayabilir. **Online Shield** ile taranacak dosyanın maksimum boyutunu belirlemek için kaydırma çubuğunu kullanabilirsiniz. İndirilen dosya belirtilen dosya boyutundan daha büyük olsa ve buna bağlı olarak Online Shield ile taranmaya bile korunmaya devam edersiniz: dosya, bulaşmış olması halinde **Yerleşik Kalkan** tarafından tespit edilecektir.
- **Barındırma/IP/etki alanını dışla** - metin alanına *Online Shield* tarafından taranmasını istemediğiniz bir sunucunun tam adını (**barındırma, IP adresi, maskeli IP adresi ya da URL**) ya da *etki alanı adını girin*. Bu nedenle, bu işlemi yapmadan önce web sitesinin içeriğinin zararlı olmadığından emin olmanız gerekir.

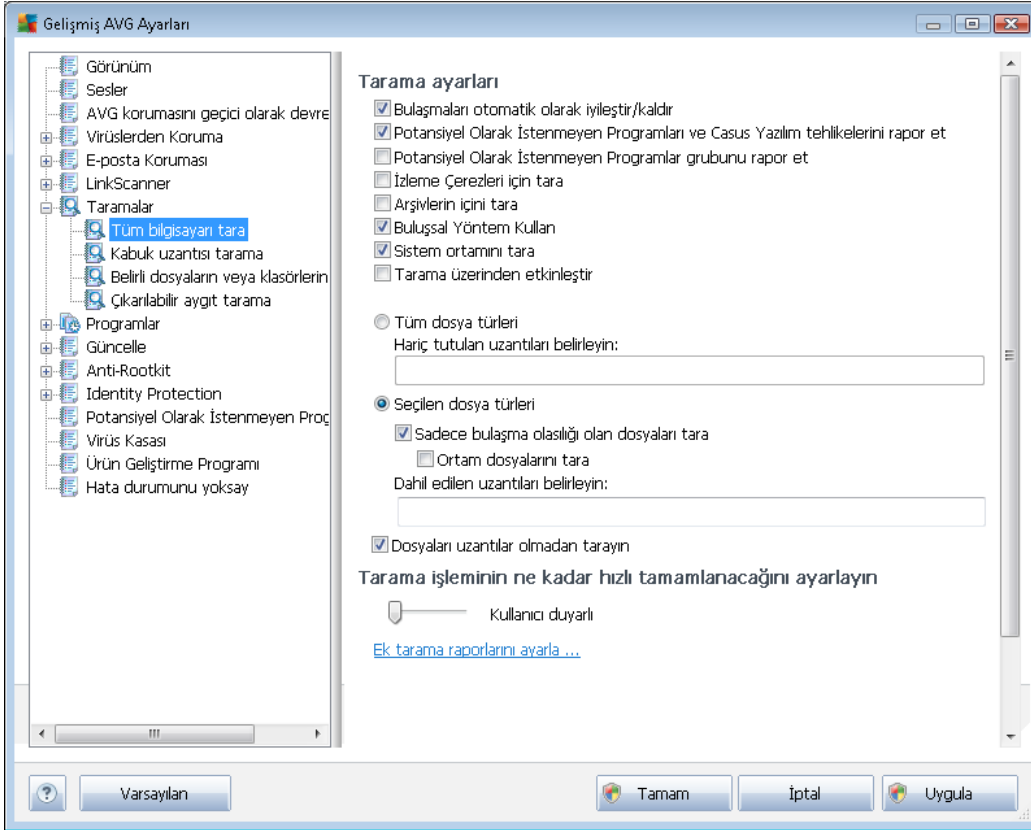
9.7. Taramalar

Gelişmiş tarama ayarları, yazılım geliştiricisi tarafından tanımlanan belirli tarama türlerine ilişkin dört kategoriye bölünmüştür:

- **[Tüm bilgisayarın taranması](#)** - tüm bilgisayarın standart öntanımlı taramasıdır
- **[Kabuk Uzantı Taraması](#)** - seçilen nesnenin doğrudan Windows Gezgini ortamında taranması işlemidir
- **[Belirli Dosya veya Klasörleri Tarama](#)** - bilgisayarınızın seçilen alanlarının tarandığı standart öntanımlı taramadır
- **[Çıkarılabilir Aygıt Taraması](#)** - bilgisayarınıza bağlanan çıkarılabilir aygıtların taranması işlemidir

9.7.1. Tüm bilgisayar taraması

Tüm Bilgisayarı Tara seçeneği, yazılım satıcısı tarafından belirlenmiş varsayılan tarama yöntemlerinden birinin parametrelerini düzenleyebilmenize olanak tanır, [Tüm bilgisayar tara](#):



Tarama ayarları

Tarama ayarları bölümünde isteğe bağlı olarak açılıp kapatılabilecek tarama parametreleri listelenmiştir:

- **Bulaşmayı otomatik temizle/sil** - (varsayılan olarak açıktır). Tarama işlemi sırasında bir virüs tanımlanırsa ve temizlenmesi mümkünse otomatik olarak temizlenir. Bulaşmış dosya otomatik olarak temizlenemezse, bulaşmış nesne [Virüs Kasası](#)'na taşınır.
- **Potansiyel Olarak İstenmeyen Programları ve Casus Yazılım tehditlerini rapor et** (varsayılanda açıktır) - [Anti-Spyware](#) motorunu etkinleştirmek ve virüslerin yanı sıra casus yazılımları da taramak için işaretleyin. Casus yazılım, şüpheli kötü amaçlı yazılım kategorisini ifade eder: genellikle bir güvenlik riskini oluşturmasına rağmen bu programlardan bazıları bilerek yüklenebilir. Bilgisayarınızın güvenliğini artırdığından, bu özelliği etkin durumda tutmanızı öneriyoruz.
- **Potansiyel Olarak İstenmeyen Programlar gelişmiş grubunu rapor et** (varsayılanda kapalıdır) - bu parametre casus yazılımların, yani doğrudan üreticiden alınan tamamen



zararsız olan, ancak daha sonra kötüye kullanılacak programların genişletilmiş paketinin tespit edilmesi için işaretleyin. Bu, bilgisayar güvenliğinizi daha da artıran ek bir önlemdir, ancak yasal programları da engelleyebilir ve bu yüzden varsayılan olarak kapalıdır.

- **İzleme Tanımlama Bilgilerini Tara** (varsayılan olarak kapalıdır) - [Anti-Spyware](#) bileşeninin bu parametresi, tarama sırasında tespit edilmesi istenen tanımlama bilgilerini tanımlar; (*HTTP tanımlama bilgileri kimlik doğrulaması, izleme ve kullanıcılar hakkındaki site tercihleri veya elektronik alışveriş sepetlerinin içeriği gibi belirli bilgilerin korunması için kullanılır*).
- **Arşivleri tara** (varsayılan olarak kapalıdır) - bu parametre, ZIP, RAR vb. arşiv dosyalarının içinde sıkıştırılmış dosyaların bile taranmasını sağlar.
- **Buluşsal Analiz Yöntemlerini Kullan** (varsayılan olarak açıktır) - buluşsal analiz yöntemi (*taranan nesnenin komutlarının sanal bir bilgisayar ortamında dinamik olarak canlandırılması*) tarama sırasında kullanılacak virüs tespiti yöntemlerinden biridir.
- **Sistem ortamını tara** (varsayılan olarak açıktır) - tarama işlemi, bilgisayarınızın sistem alanlarını da kontrol edecektir.
- **Kapsamlı taramayı etkinleştir** (varsayılan olarak kapalıdır) - belirli durumlarda (*bilgisayarınıza bulaşma olmasından şüpheleniliyorsa*) yalnızca emin olmak üzere bilgisayarınızın bulaşma olması çok zor olan alanlarını bile tarayan en kapsamlı tarama algoritmalarını etkinleştirmek için bu seçeneği işaretleyebilirsiniz. Ancak, bu yöntemin çok fazla zaman aldığı unutmayın.

Ayrıca, taramak isteyip istemediğinize karar vermelisiniz

- **Tüm dosya türleri** , virgülle ayrılmış (*kaydedilirken virgüller noktalı virgüle dönüşür*) dosya uzantıları listesi sağlayarak taramadan hariç tutulacakların taranmaması için tanımlama olasılığı sağlar;
- **Seçili dosya türleri** - Yalnızca virüs bulaşabilme olasılığı olan dosyaları taramayı istediğinizi belirtebilirsiniz (*virüs bulaşmayan dosyalar taranmayacaktır, örneğin, bazı düz metin dosyaları veya bazı diğer çalıştırılmayan dosyalar*); ortam dosyaları (*video, ses dosyaları - bu onay kutusunun işaretini kaldırırsanız, bu dosyalar genellikle çok büyük olduğundan ve virüs bulaşma olasılıkları çok az olduğundan tarama süresini daha da azaltır*). Tekrar, her zaman taranması gereken dosyaları uzantılarına göre belirtebilirsiniz.
- İsteğe bağlı olarak, **Uzantıları olmayan dosyaları taramaya** da karar verebilirsiniz ve bu seçenek varsayılan olarak açıktır ve gerçekten bir nedeniniz yoksa değiştirmeniz önerilir. Uzantısı olmayan dosyalar şüpheli olabilir ve her zaman taranmalıdır.

Taramanın ne kadar hızlı tamamlanacağını ayarla

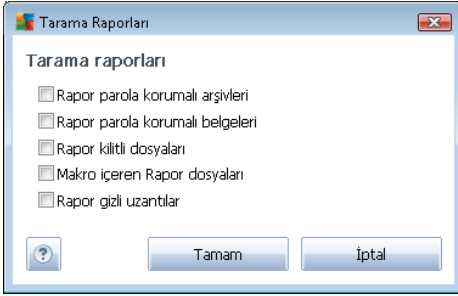
Taramanın ne kadar hızlı tamamlanacağını ayarla bölümünde, sistem kaynakları kullanımına bağlı olarak istediğiniz tarama hızını seçebilirsiniz. Bu seçenek varsayılan olarak otomatik kaynak kullanımının *kullanıcıya duyarlı* düzeyine ayarlanmıştır. Tarama işleminin daha hızlı ilerlemesini istiyorsanız tarama işlemi daha kısa sürecektir fakat tarama işlemi sırasında sistem kaynakları



oldukça yüklü bir şekilde kullanılacak ve bilgisayar üzerindeki diğer işlemleri yavaşlatacaktır (*bu seçenek bilgisayarınız açıkken kullanılmadığı sırada seçilebilir*). Öte yandan tarama süresini uzatarak da sistem kaynaklarının kullanımını azaltabilirsiniz.

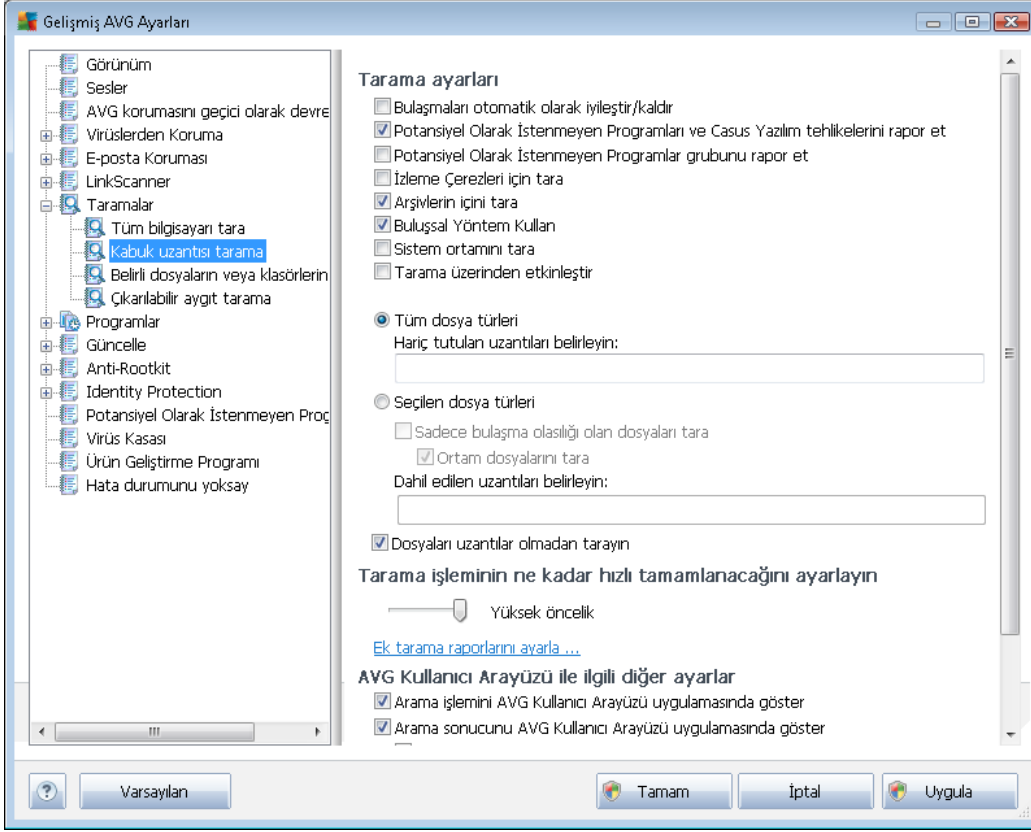
Ek tarama raporlarını ayarla...

Diğer tarama raporlarını belirle... bağlantısına tıklayarak hangi tarama bulgularının rapor edileceğine ilişkin seçimleri yapabileceğiniz **Tarama raporları** iletişim kutusu penceresini açabilirsiniz:



9.7.2. Kabuk uzantısı tarama

Daha önce bahsettiğimiz [Tüm bilgisayar taraması](#) ögesine benzer olan bu öge, **Kabuk uzantı taraması** olarak adlandırılır, taramayı düzenlemek için yazılım satıcısı tarafından önceden tanımlanmış birkaç seçenek de sunar. Bu sefer, yapılandırma [doğrudan Windows Gezgini üzerinden başlatılan belirli nesnelerin taraması](#) esasına dayanmaktadır (*kabuk uzantısı*), [Windows Gezgini'nde Tarama](#) bölümüne bakın:



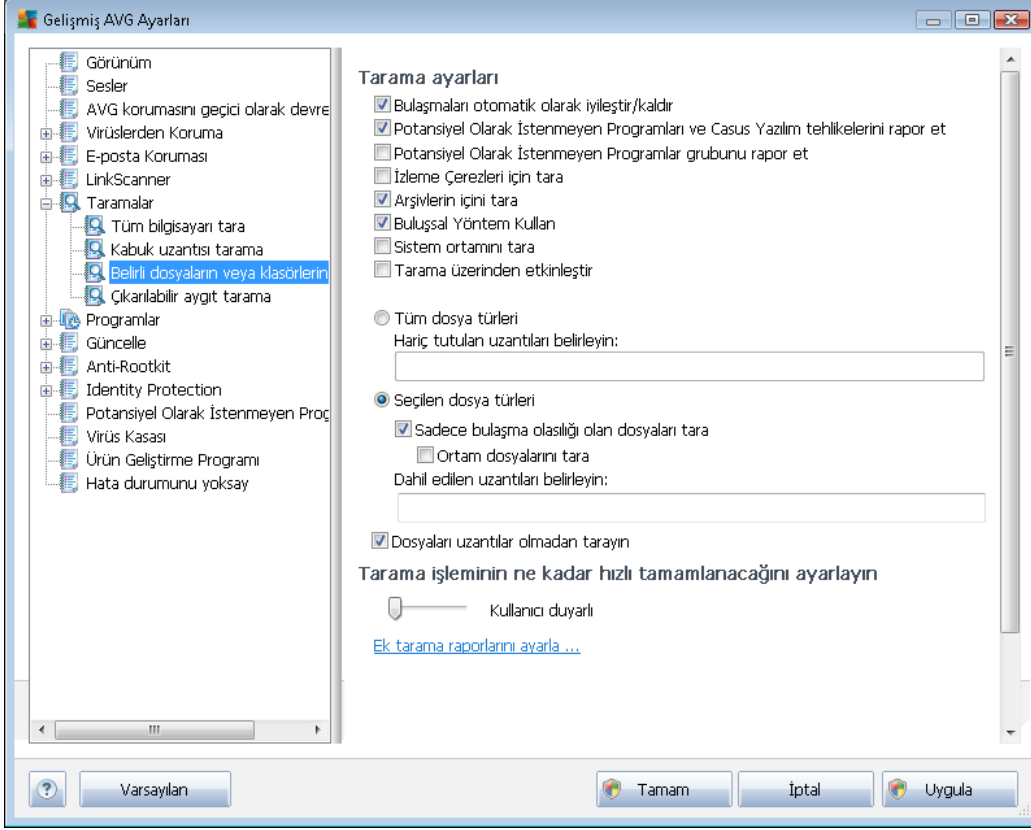
Parametre listesi, [Tüm bilgisayar tarama](#) öğesinin parametre listesi ile aynıdır. Bununla birlikte, varsayılan ayarlar farklılık gösterebilir (örneğin, *Tüm bilgisayarın taraması işlevi arşivleri denetlemez ancak Kabuk Uzantısı Tarama başka bir işlem yaparken sistem ortamını tarar*).

Not: Belirli parametrelerin açıklaması için, lütfen [AVG Gelişmiş Ayarları / Taramalar / Tüm bilgisayarın taraması](#) bölümüne bakın.

[Tüm bilgisayar tarama](#) iletişim kutusuyla karşılaştırıldığında **Kabuk uzantısı tarama** iletişim kutusu tarama sürecinde ve tarama sonuçlarında AVG kullanıcı arayüzünden erişilebilir olmasını isteyip istemediğinizi belirleyebileceğiniz **AVG Kullanıcı Arayüzü ile ilgili diğer ayarlar** adlı bölümü de içerir. Tarama sırasında bir bulaşma tespit edilmesi durumunda tarama sonucunun görüntülenmesi gerektiğini de tanımlayabilirsiniz.

9.7.3. Belirli dosyaların veya klasörlerin taranması

Belirli dosyaları veya klasörleri tara işlevinin düzenleme arayüzü [Tüm Bilgisayar Taraması](#) işlevinin düzenleme iletişim kutusu ile aynıdır. Tüm konfigürasyon seçenekleri aynıdır; diğer bir yandan [Tüm bilgisayar taraması](#) için varsayılan ayarlar daha kesindir:

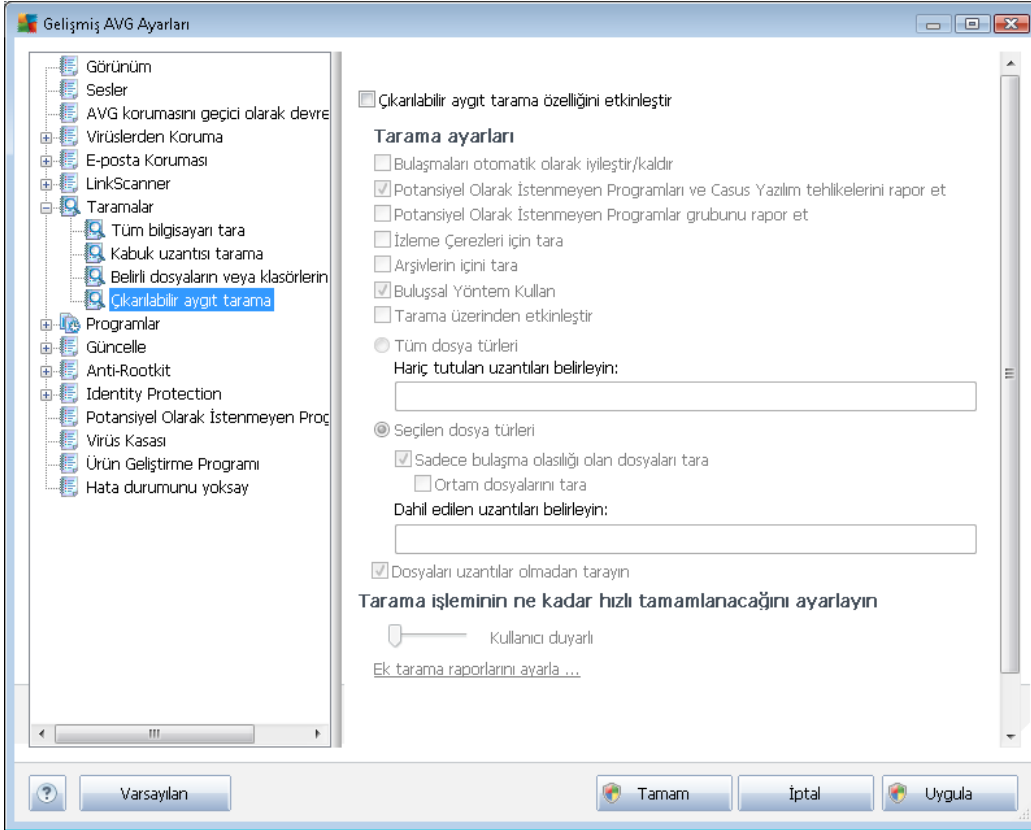


Bu yapılandırma iletişim kutusunda ayarlanan tüm parametreleri [Belirli dosya ya da klasörleri tara](#) ile tarama sırasında seçilen alanlar için geçerlidir!

Not: [Belirli parametrelerin açıklaması için, lütfen AVG Gelişmiş Ayarları / Taramalar / Tüm bilgisayarın taraması](#) bölümüne bakın.

9.7.4. Çıkarılabilir aygıt tarama

Çıkarılabilir aygıt tarama için düzenleme arayüzü de [Tüm bilgisayarın taranması](#) düzenleme iletişim kutusu ile aynıdır:



Çıkarılabilir aygıt tarama bilgisayarınıza çıkarılabilir bir aygıt taktığınız anda otomatik olarak başlar. Varsayılan olarak söz konusu tarama işlemi kapalıdır. Diğer bir yandan başlıca bulaşma kaynaklarından biri olduğu için söz konusu çıkarılabilir aygıtların potansiyel tehditlere karşı taranması hayati önem taşımaktadır. Bu tarama özelliğinin istendiği zaman otomatik olarak başlatılacak şekilde hazır bulundurulması için **Çıkarılabilir aygıt taramayı etkinleştir** seçeneğini işaretleyin.

Not: Belirli parametrelerin açıklaması için, lütfen [AVG Gelişmiş Ayarları / Taramalar / Tüm bilgisayarın taranması](#) bölümüne bakın.

9.8. Programlar

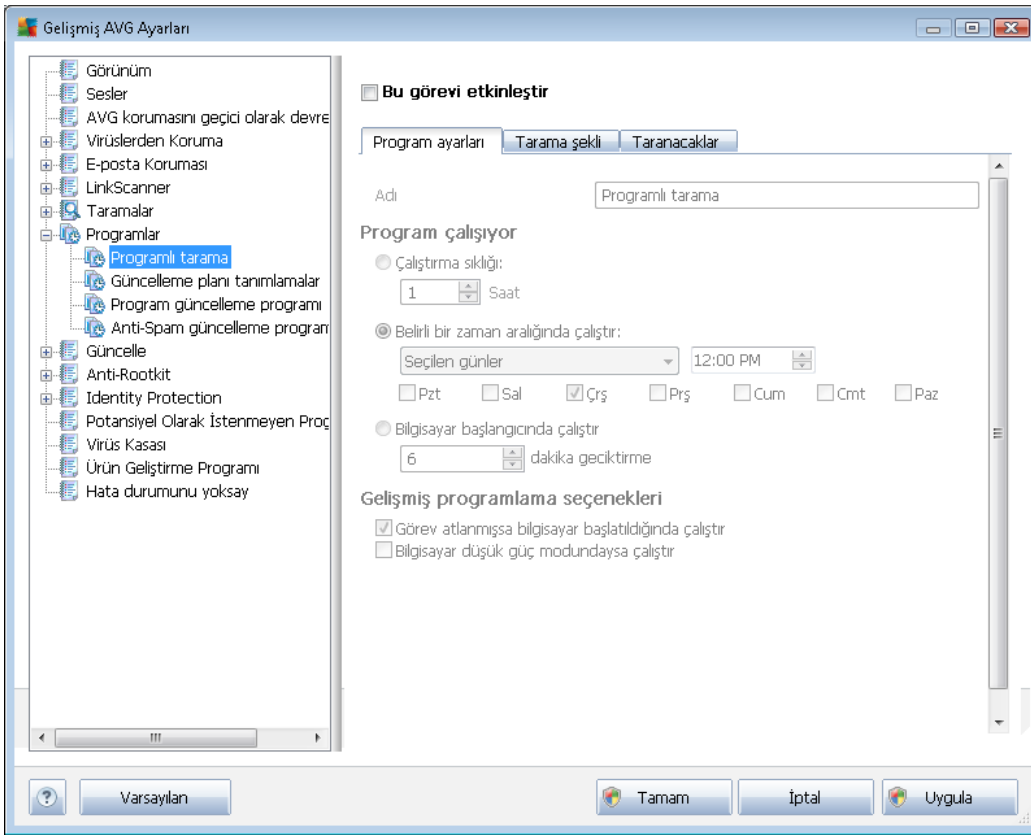
Programlar bölümünde aşağıdaki bileşenlerin öntanımlı ayarlarını düzenleyebilirsiniz:

- [Zamanlanan tarama](#)
- [Güncelleme planı tanımlamalar](#)
- [Program güncelleme programı](#)

- [Anti-Spam güncelleme programı](#)

9.8.1. Programlı Tarama

Üç sekmede zamanlanan tarama parametreleri düzenlenebilir (veya yeni bir zamanlama ayarlanabilir). Her sekmede **Bu görevi etkinleştir** ögesini işaretleyerek veya söz konusu ögenin işaretini kaldırarak zamanlanan testi geçici olarak devre dışı bırakabilir ve gerektiğinde yeniden açabilirsiniz:



Daha sonra, **Ad** adındaki metin alanında (tüm varsayılan programlamalar için devre dışı bırakılmış) bu programlamaya program satıcı tarafından atanan ad bulunur. Yeni eklenen zamanlamalar için (sol gezinti ağacındayken **Taramayı programla** ögesi üzerinde sağ tıklatarak yeni bir zamanlama ekleyebilirsiniz) kendi adınızı belirtebilirsiniz ve bu durumda metin alanı düzenleme için açılacaktır. Programladığınız taramaları diğerlerinden kolaylıkla ayırabilmek için her zaman taramalarınıza kısa, açıklayıcı adlar vermeye çalışın.

Örnek: Taramayı "Yeni Tarama" veya "Taramam" adıyla adlandırmanız uygun değildir çünkü bu adlar, taramanın fiilen neyi kontrol ettiğini açıklamaz. Diğer bir yandan "Sistem alanları taraması" oldukça açıklayıcı bir isim olacaktır. Ayrıca, taramanın adında söz konusu taramanın tam bilgisayar taraması ya da sadece seçilen dosya ya da klasörlerin taraması olup olmadığını belirtmenize gerek yoktur - taramalarınız [seçilen dosya ya da klasörleri tara](#) işlevinin farklı şekillerinden ibaret olacaktır.

Bu iletişim kutusunda taramanın aşağıdaki parametrelerini de tanımlayabilirsiniz:



Program çalışıyor

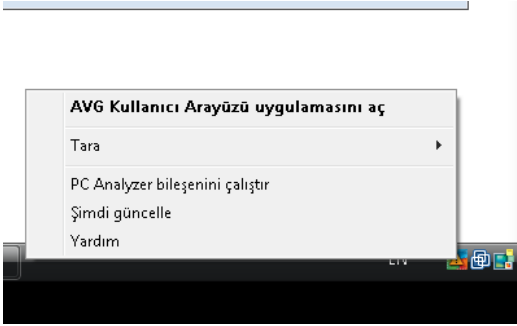
Burada, yeni programlanan tarama başlatması için zaman aralıkları belirtebilirsiniz. Zamanlama belirli bir sürenin ardından tekrarlanan tarama başlatması ile (*Her ...'de bir*) ya da kesin bir tarih ve saat tanımlayarak (*Belirli bir zaman aralığında çalıştır ...*), veya tarama başlangıcıyla ilgili bir olay tanımlanarak (*Bilgisayar başlangıcında çalıştır*) tanımlanabilir.

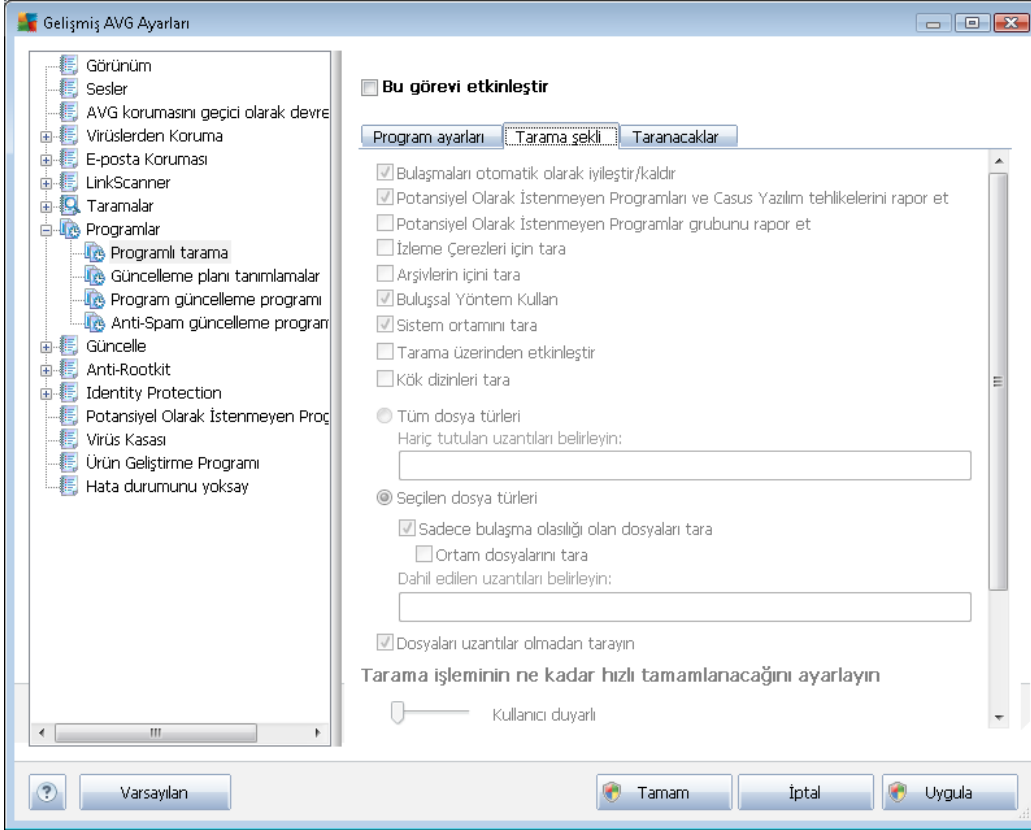
Gelişmiş zamanlama seçenekleri

Bu bölümde, bilgisayar düşük güç modundaydı veya tamamen kapatılmışsa hangi koşullar altında taramanın başlatılması/başlatılmaması gerektiğini tanımlamanızı sağlar. Programlanan tarama belirttiğiniz saatte başlatıldığında, [AVG sistem tepsisi simgesi](#) üzerinde bir açılır pencere ile bu konuda bilgilendirileceksiniz:



Bunun ardından yeni bir [AVG sistem tepsisi simgesi](#) görüntülenir (*üzerinde beyaz bir ok bulunur ve tamamen renklidir*) ve programlanan taramanın başladığını bildirir. Çalışan taramayı duraklatmaya hatta durdurmaya karar verebileceğiniz ve o anda çalışmakta olan taramanın önceliğini değiştirebileceğiniz bağlam menüsü açmak için, çalışan taramayı sağ tıklayın:





Tarama Şekli sekmesinde, isteğe bağlı olarak açılıp/kapatılabilen tarama parametrelerine ilişkin bir liste bulabilirsiniz. Varsayılan olarak birçok parametre devreye sokulur ve işlevsellik de tarama sırasında uygulanacaktır. **Söz konusu ayarları değiştirmek açısından geçerli bir nedeniniz yoksa öntanımlı konfigürasyonu olduğu gibi muhafaza etmeniz önerilir.**

- **Bulaşmayı otomatik temizle/sil** (varsayılan olarak açıktır): tarama işlemi sırasında herhangi bir virüs tanımlanırsa ve temizlenmesi mümkünse otomatik olarak temizlenir. Bulaşmış dosya otomatik olarak temizlenemezse, bulaşmış nesne [Virüs Kasası](#)'na taşınır.
- **Potansiyel Olarak İstenmeyen Programları ve Casus Yazılım tehlikelerini rapor et** - (varsayılan olarak açıktır): [Anti-Spyware](#) motorunu etkinleştirmek ve virüslerin yanı sıra birlikte casus yazılımları da taramak için işaretleyin. Casus yazılım, şüpheli kötü amaçlı yazılım kategorisini ifade eder: genellikle bir güvenlik riskini oluşturmasına rağmen bu programlardan bazıları bilerek yüklenebilir. Bilgisayarınızın güvenliğini artırdığından, bu özelliği etkin durumda tutmanızı öneriyoruz.
- **Potansiyel Olarak İstenmeyen Programlar gelişmiş grubunu rapor et** (varsayılanda kapalıdır) - bu parametre casus yazılımların, yani doğrudan üreticiden alınan tamamen zararsız olan, ancak daha sonra kötüye kullanılacak programların genişletilmiş paketinin tespit edilmesi için işaretleyin. Bu, bilgisayar güvenliğinizi daha da artıran ek bir önlemdir, ancak yasal programları da engelleyebilir ve bu yüzden varsayılan olarak kapalıdır.
- **İzleme Tanımlama Bilgilerini Tara** (varsayılan olarak kapalıdır): [Anti-Spyware](#) bileşeninin



bu parametresi, tarama sırasında tespit edilmesi istenen tanımlama bilgilerini tanımlar (*HTTP tanımlama bilgileri kimlik doğrulaması, izleme ve kullanıcılar hakkındaki site tercihleri veya elektronik alışveriş sepetlerinin içeriği gibi belirli bilgilerin korunması için kullanılır*).

- **Arşivleri tara** - (varsayılan olarak kapalıdır): bu parametre, tarama işleminin ZIP, RAR gibi belirli bir arşiv türü ile sıkıştırılmış olsa bile tüm dosyaların taranması gerektiğini tanımlar.
- **Buluşsal Analiz Yöntemlerini Kullan** - (varsayılan olarak açıktır). Buluşsal analiz yöntemi (taranan nesnenin komutlarının sanal bir bilgisayar ortamında dinamik olarak canlandırılması) tarama sırasında kullanılacak virüs tespiti yöntemlerinden biridir.
- **Sistem ortamını tara** - (varsayılan olarak açıktır). Tarama işlemi, bilgisayarınızın sistem alanlarını da kontrol edecektir.
- **Kapsamlı taramayı etkinleştir** (varsayılanda kapalıdır) - belirli durumlarda (bilgisayarınıza bulaşma olmasından şüpheleniliyorsa) yalnızca emin olmak üzere bilgisayarınızın bulaşma olması çok zor olan alanlarını bile tarayan en kapsamlı tarama algoritmalarını etkinleştirmek için bu seçeneği işaretleyebilirsiniz. Ancak, bu yöntemin çok fazla zaman aldığı unutmayın.
- **Kök dizinleri tara** (varsayılan olarak kapalıdır). Kök izin tespitini tüm bilgisayarın taranmasına eklemek için bu öğeyi işaretleyin. Rootkit tespiti işlemi [Anti-Rootkit](#) bileşeninden de yapabilirsiniz;

Ayrıca, taramak isteyip istemediğinize karar vermelisiniz

- **Tüm dosya türleri** - virgülle ayrılmış (kaydedilirken virgüller noktalı virgüle dönüşür) dosya uzantıları listesi sağlayarak taramadan hariç tutulacakların taranmaması için tanımlama olasılığı sağlar;
- **Seçili dosya türleri** - Yalnızca virüs bulaşabilme olasılığı olan dosyaları taramayı istediğinizi belirtebilirsiniz (virüs bulaşmayan dosyalar taranmayacaktır, örneğin, bazı düz metin dosyaları veya bazı diğer çalıştırılmayan dosyalar); ortam dosyaları (video, ses dosyaları - bu onay kutusunun işaretini kaldırırsanız, bu dosyalar genellikle çok büyük olduğundan ve virüs bulaşma olasılıkları çok az olduğundan tarama süresini daha da azaltır). Tekrar, her zaman taranması gereken dosyaları uzantılarına göre belirtebilirsiniz.
- İsteğe bağlı olarak, **Uzantıları olmayan dosyaları taramaya** da karar verebilirsiniz ve bu seçenek varsayılan olarak açıktır ve gerçekten bir nedeniniz yoksa değiştirmeniz önerilir. Uzantısı olmayan dosyalar şüpheli olabilir ve her zaman taranmalıdır.

Taramanın ne kadar hızlı tamamlanacağını ayarla

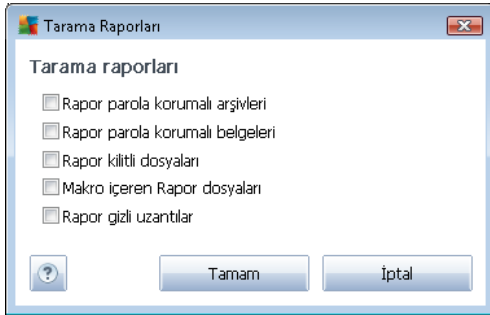
Taramanın ne kadar hızlı tamamlanacağını ayarla bölümünde, sistem kaynakları kullanımına bağlı olarak istediğiniz tarama hızını seçebilirsiniz. Bu seçenek varsayılan olarak otomatik kaynak kullanımının kullanıcıya duyarlı düzeyine ayarlanmıştır. Tarama işleminin daha hızlı ilerlemesini istiyorsanız tarama işlemi daha kısa sürecektir fakat tarama işlemi sırasında sistem kaynakları oldukça yüklü bir şekilde kullanılacak ve bilgisayar üzerindeki diğer işlemleri yavaşlatacaktır (bu seçenek bilgisayarınız açıkken kullanılmadığı sırada seçilebilir). Öte yandan, tarama süresini



uzatarak sistem kaynaklarının kullanımını azaltabilirsiniz.

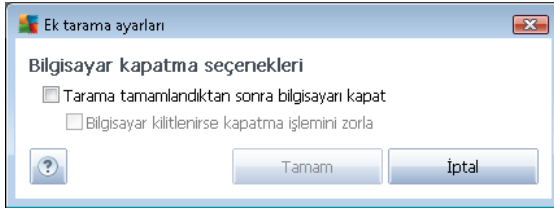
Ek tarama raporlarını ayarla

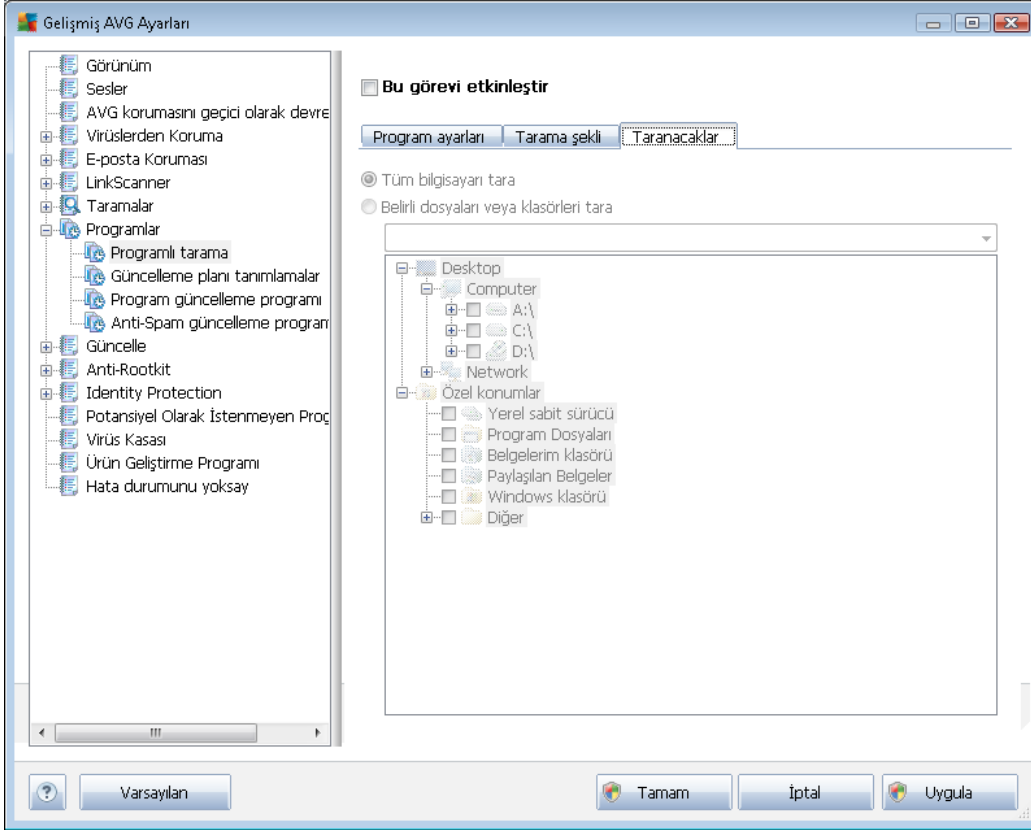
Tarama bulgularının rapor edilmesi gerekip gerekmediğini tanımlamak üzere birden fazla öğeyi ayarlayabileceğiniz **Tarama raporları** olarak adlandırılan bağımsız bir iletişim penceresi açmak için **Ek tarama raporlarını ayarla...** bağlantısını tıklayın:



Ek tarama ayarları

Ekstra tarama ayarları'na tıklamak yeni bir **Bilgisayar Kapatma seçenekleri** iletişim kutusunu açar. Burada tarama işlemi bittikten sonra bilgisayarın otomatik olarak kapanmasını ayarlayabilirsiniz. Bu seçeneği seçerseniz (**Tarama bittikten sonra bilgisayarı kapat**) bilgisayar mevcut durumda kilitli olsa bile bilgisayarın kapatılmasını sağlayan bir seçeneğin bulunduğu bir pencere açılacaktır (**Bilgisayar kilitliyse bilgisayarı kapanmaya zorla**).

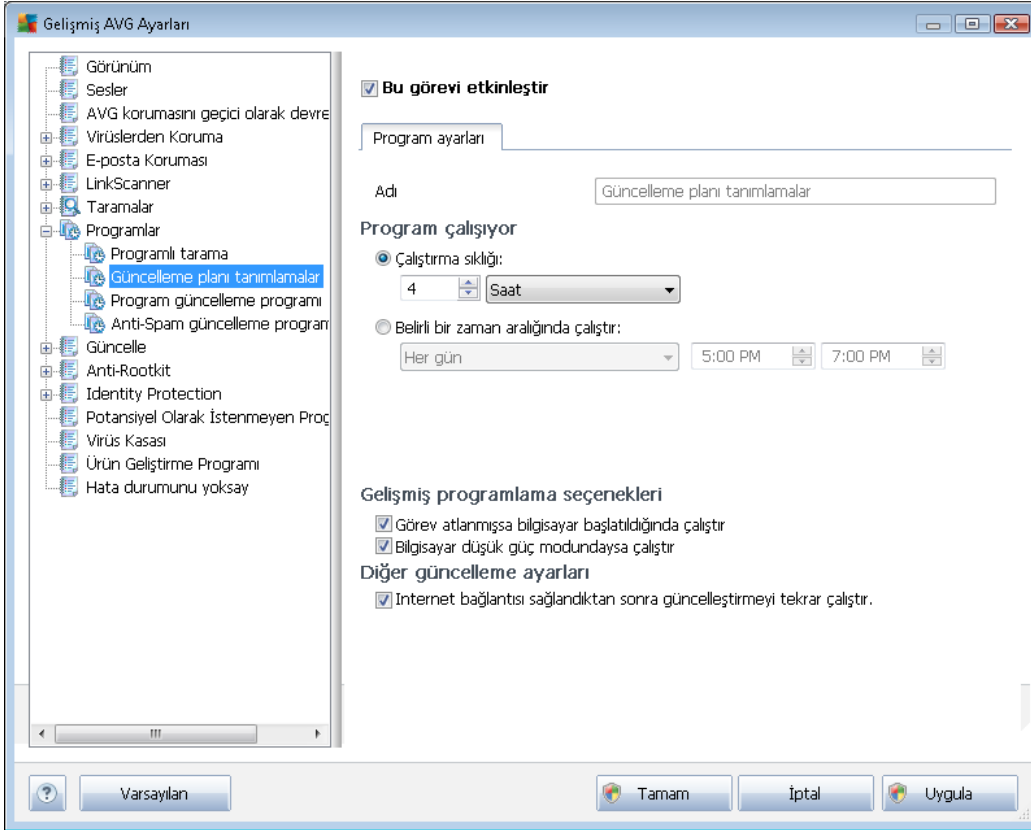




Taranacaklar sekmesinde, [tüm bilgisayarı tarama](#) veya [belirli dosya veya klasörleri taramayı](#) programlamak isteyip istemediğinizi belirleyebilirsiniz. Belirli dosya ve klasörleri taramayı seçerseniz, bu iletişim penceresinin alt kısmında görüntülenen ağaç yapısı etkinleşir ve taranacak klasörleri seçebilirsiniz.

9.8.2. Güncelleme Planı Tanımlamalar

Gerçekten gerekiyorsa Bu görevi etkinleştir öğesinin işaretini kaldırarak zamanlanmış tanımları geçici olarak devre dışı bırakabilir ve daha sonra tekrar açabilirsiniz:



Bu iletişim kutusunda tanımlar güncelleme zamanlaması parametrelerinden bazılarını ayrıntılarıyla yapılandırabilirsiniz. **Ad** adındaki metin alanında (*tüm varsayılan programlamalar için devre dışı bırakılmış*) bu programlamaya program satıcısı tarafından atanan ad bulunur.

Program çalışıyor

Bu bölümde, yeni programlanan tanımlar güncellemesini başlatmak için zaman aralıkları belirtin. Zamanlama, belirli bir süreden sonra (**Çalıştırma sıklığı...**) tekrarlanan güncelleme başlatması olarak veya belirli bir tarih ve saat (**Belirli bir saatte çalıştır...**) tanımlanarak tanımlanabilir.

Gelişmiş programlama seçenekleri

Bu bölümde, bilgisayar düşük güç modundaydı veya tamamen kapatılmışsa hangi koşullar altında tanımlar güncellemesinin başlatılması/başlatılmaması gerektiğini belirleyebilirsiniz.

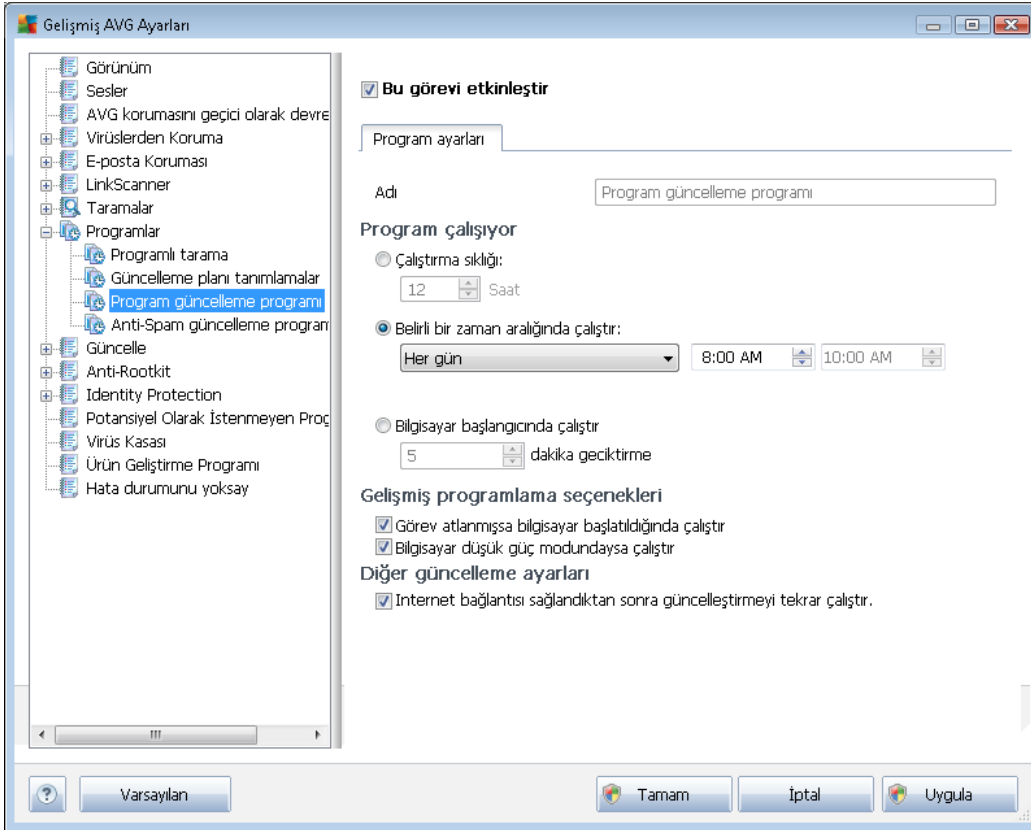


Diğer güncelleme ayarları

Son olarak, **Internet bağlantısı kurulduğunda güncellemeyi yeniden çalıştır** seçeneğini işaretleyerek Internet bağlantısı bozulduğunda ve güncelleme işlemi başarısız olduğunda, Internet bağlantısı yeniden sağlanır sağlanmaz yeniden başlatıldığından emin olun. Programlı güncelleme işlemi sizin belirlediğiniz tarih ve saatte başladıktan sonra [AVG sistem tepsi simgesi](#) üzerinde açılan bir açılır pencere vasıtasıyla bilgilendirileceksiniz ([Gelişmiş Ayarlar/Görünüm](#) iletişim kutusunun varsayılan yapılandırmasını değiştirmemiş olmanız kaydıyla).

9.8.3. Program Güncelleme Planı

Gerçekten gerekliyse Bu görevi etkinleştir öğesinin işaretini kaldırarak zamanlanmış programı geçici olarak devre dışı bırakabilir ve daha sonra tekrar açabilirsiniz:



Ad adındaki metin alanında (tüm varsayılan programlamalar için devre dışı bırakılmış) bu programlamaya program satıcısı tarafından atanan ad bulunur.

Program çalışıyor

Burada, yeni programlanan program güncellemesinin başlaması için zaman aralıklarını girin. Zamanlama belirli bir sürenin ardından tekrarlanan güncelleme ile (**Her ...'de bir**) ya da kesin bir tarih ve saat tanımlayarak (**Belirli bir saatte çalıştır...**) ya da (**Bilgisayar başlangıcında**) ilgili bir



programın güncellemesiyle tanımlanabilir.

Gelişmiş programlama seçenekleri

Bu bölümde, bilgisayar düşük güç modundaydı veya tamamen kapatılmışsa hangi koşullar altında program güncellemesinin başlatılması/başlatılmaması gerektiğini belirleyebilirsiniz.

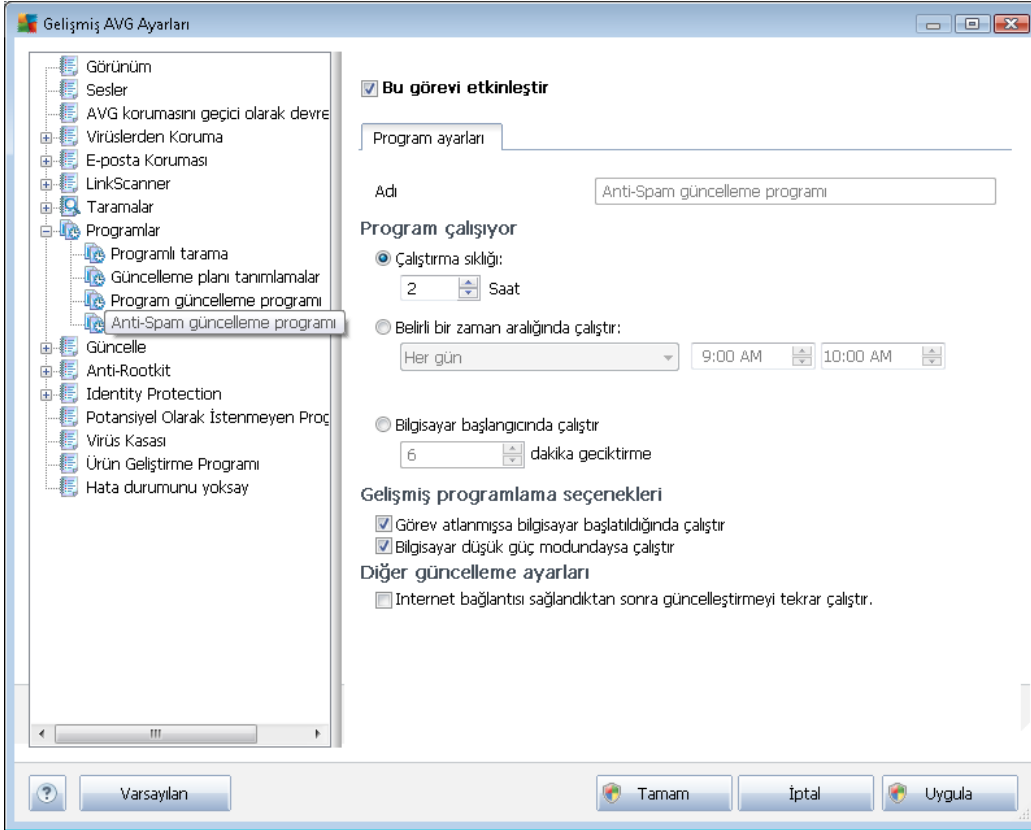
Diğer güncelleme ayarları

Internet bağlantısı kurulduğunda güncellemeyi yeniden çalıştır seçeneğini işaretleyerek Internet bağlantısı bozulduğunda ve güncelleme işlemi başarısız olduğunda, Internet bağlantısı yeniden sağlanır sağlanmaz yeniden başlatıldığından emin olun. Programlı güncelleme işlemi sizin belirlediğiniz tarih ve saatte başladıktan sonra [AVG sistem tepsi simgesi](#) üzerinde açılan bir açılır pencere vasıtasıyla bilgilendirileceksiniz ([Gelişmiş Ayarlar/Görünüm](#) iletişim kutusunun varsayılan yapılandırmasını değiştirmemiş olmanız kaydıyla).

Not: Programlanmış bir program güncellemesinin zaman çakışması oluşursa ve programlı tarama gerçekleşirse, güncelleme işlemi daha yüksek önceliğe sahiptir ve tarama kesilir.

9.8.4. Anti-Spam Güncelleme Zamanlaması

Gerçekten gerekliyse, **Bu görevi etkinleştir** öğesinin işaretini kaldırarak zamanlanmış [Anti-Spam](#) güncellemesini geçici olarak devre dışı bırakabilir ve daha sonra tekrar açabilirsiniz:



Bu iletişim kutusunda güncelleme zamanlaması parametrelerinden bazılarını ayrıntılarıyla yapılandırabilirsiniz. **Ad** adındaki metin alanında (*tüm varsayılan programlamalar için devre dışı bırakılmış*) bu programlamaya program satıcısı tarafından atanan ad bulunur.

Programlı çalıştırma

Burada, yeni programlanan [Anti-Spam](#) güncellemesinin başlaması için zaman aralığı girin. Zamanlama belirli bir sürenin ardından tekrarlanan [Anti-Spam](#) güncellemesi ile (**Her ... 'de bir**) ya da kesin bir tarih ve saat tanımlayarak (**Belirli zaman aralıklarıyla çalıştır**) ya da (**Bilgisayar başlangıcında**) ilgili bir programın güncellemesiyle tanımlanabilir.

Gelişmiş zamanlama seçenekleri

Bu bölümde, bilgisayar düşük güç modundayken veya tamamen kapatılmışsa hangi koşullar altında [Anti-Spam](#) güncellemesinin başlatılması/başlatılmaması gerektiğini belirleyebilirsiniz.



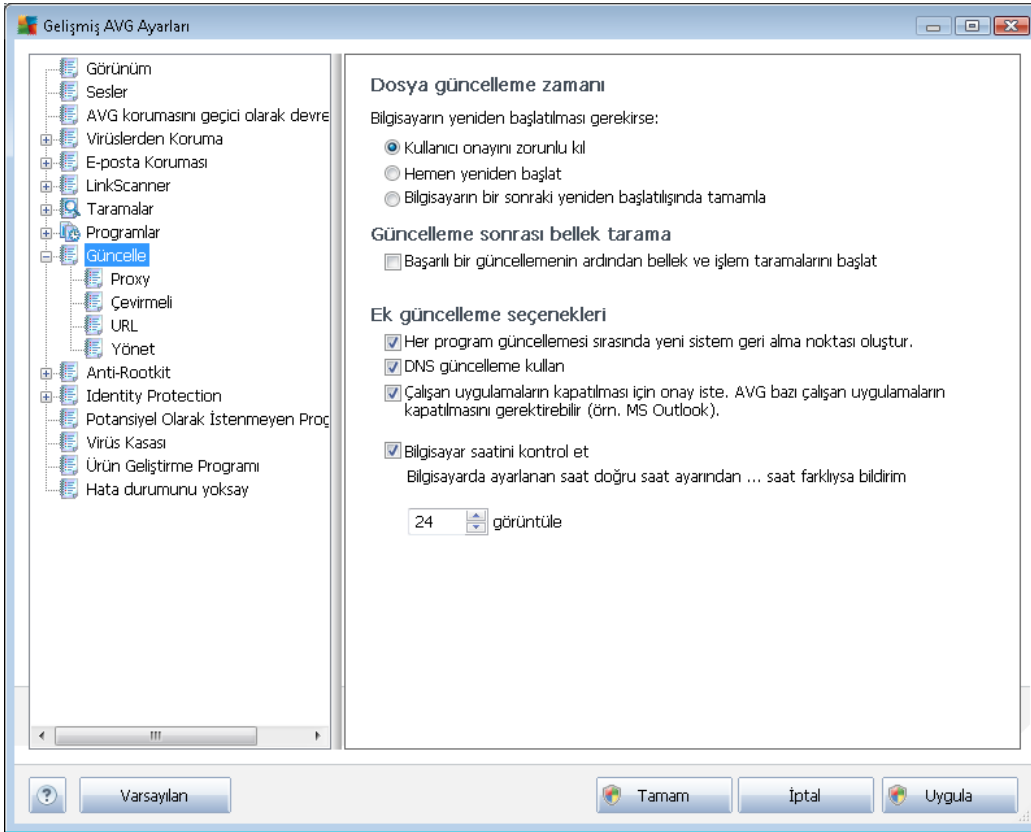
Diğer güncelleme ayarları

İnternet bağlantısı kurulduğunda güncellemeyi yeniden çalıştır seçeneğini işaretleyerek internet bağlantısı bozulduğunda ve [Anti-Spam](#) güncelleme işlemi başarısız olduğunda, internet bağlantısı yeniden sağlanır sağlanmaz yeniden başlatılmasını sağlayın.

Planlanan tarama işlemi sizin belirlediğiniz tarih ve saatte başladıktan sonra [AVG sistem tepsi simgesi](#) üzerinde açılan bir açılır pencere vasıtasıyla bilgilendirileceksiniz ([Gelişmiş Ayarlar/Görünüm iletişim penceresinin öntanımlı yapılandırılmayı değiştirmemiş olmanız kaydıyla](#)).

9.9. Güncelleme

Güncelle navigasyonu öğesi, [AVG güncellemesine](#) ilişkin genel parametreleri belirleyebileceğiniz yeni bir iletişim kutusu açar:



Dosya güncelleme zamanı

Bu bölümde güncelleme işlemi bilgisayarınızın yeniden başlatılmasını gerektiriyorsa üç seçenek arasından birini belirleyebilirsiniz. Güncellemenin tamamlanması işlemi, bilgisayarınızın bir sonraki yeniden başlatılma sürecine zamanlanabilir veya yeniden başlatma işlemi hemen yapılabilir:



- **Kullanıcıdan onay iste** (varsayılan) - [güncelleme işleminin](#) tamamlanması için gereken bilgisayarın yeniden başlatılması süreci için onayınız istenir
- **Hemen yeniden başlat** - [güncelleme işlemi](#) tamamlanır tamamlanmaz onayınız istenmeden bilgisayarınız yeniden başlatılacaktır
- **Bilgisayarın bir sonraki yeniden başlatılmasında tamamla** - [güncelleme işleminin](#) tamamlanması bilgisayarın bir sonraki yeniden başlatılmasına kadar ertelenir. Lütfen bu seçeneğin yalnızca bilgisayarın düzenli olarak (en azından günde bir kez) yeniden başlatıldığını bilmeniz halinde önerildiğini unutmayın!

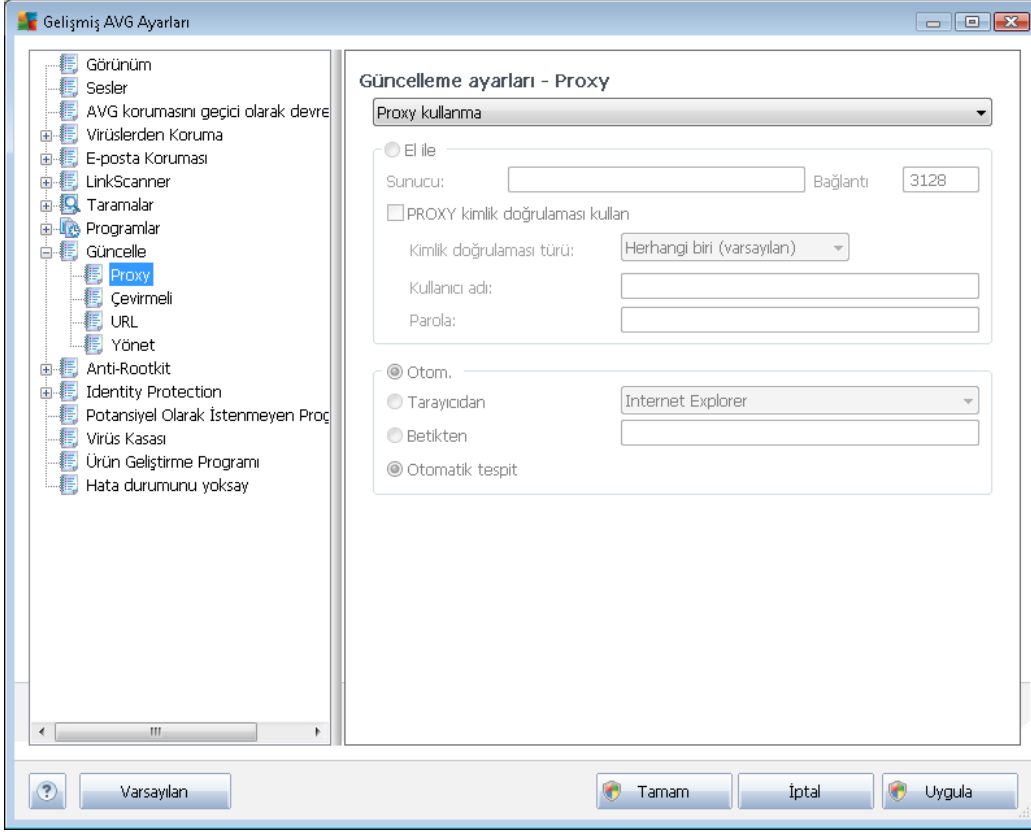
Güncelleme sonrası bellek tarama

Başarıyla tamamlanan her güncelleme sonrasında yeni bir bellek taraması başlatmak istediğinizi tanımlamak için bu onay kutusunu işaretleyin. En son indirilen güncelleme yeni virüs tanımlarını içerebilir ve bunlar taramaya hemen uygulanır.

Ek güncelleme seçenekleri

- **Her program güncellemesinden sonra sistem geri yükleme noktası oluştur** - AVG programının güncelleme işlemi başlamadan önce her seferinde geri yükleme noktası oluşturulur Güncelleme işleminin başarısız olması ve işletim sisteminizin çökmesi halinde işletme sisteminizi bu noktaya geri döndürebilirsiniz. Bu seçeneğe Başlat/Tüm Programlar bilgisayarınızın günde en az bir kere açıldığından emin olduğunuz durumlarda önerilir/ Donatılar /Sistem Araçları /Sistem Geri Yükleme menüsünden erişebilirsiniz fakat değişikliklerin sadece uzman kullanıcılar tarafından yapılması önerilmektedir. Bu fonksiyonu kullanmak istiyorsanız bu kutucuğu işaretleyin.
- **DNS güncellemesini kullan** (varsayılan olarak açıktır) - bu öge işaretlendiğinde güncelleme işlemi başlatıldığında **AVG Internet Security 2012** en yeni veritabanı sürümüyle ve DNS sunucusundaki en yeni program sürümüyle ilgili bilgileri arar. Yalnızca en küçük, kesin olarak gerekli güncelleme dosyaları indirilir ve uygulanır. Bu şekilde, indirilen toplam veri miktarı en düşük seviyede tutulur ve güncelleme süreci daha hızlı bir şekilde gerçekleştirilir.
- **Çalışan uygulamaları kapatmak için onay iste** (varsayılan olarak açıktır) güncelleme işleminin tamamlanması için gerekirse izniniz olmaksızın geçerli olarak çalışan uygulamaların kapatılmamasını sağlayacaktır.
- **Bilgisayar saatini kontrol et** - Bilgisayar saati ile doğru saat arasındaki fark belirlenen süreden uzun olduğunda bilgilendirilmek isterseniz bu seçeneği işaretleyin.

9.9.1. Proxy



Proxy sunucusu, İnternet'e daha güvenli bir şekilde bağlanmanızı sağlayan bağımsız bir sunucu ya da bilgisayarınızda çalışan bir hizmet programıdır. Belirlenen ağ kuralları doğrultusunda, İnternet'e doğrudan ya da bir proxy sunucusu üzerinden ulaşabilirsiniz; aynı anda her iki işleme de izin verilir. Bunun ardından **Güncelleme ayarları - Proxy** iletişim kutusunun ilk ögesinden aşağıdaki seçimleri yapmanız gerekmektedir:

- **Proxy kullan**
- **Proxy kullanma** - varsayılan ayarlar
- **Proxy kullanarak bağlanmayı dene; başarısız olursa doğrudan bağlan**

Proxy sunucusunu kullanan herhangi bir seçeneği seçerseniz daha ayrıntılı bilgi girmeniz istenecektir. Sunucu ayarları manüel ya da otomatik olarak yapılandırılabilir.

Manüel yapılandırma

Manüel yapılandırmayı seçerseniz (ilgili iletişim kutusu bölümünü etkinleştirmek için **Manüel seçeneğini işaretleyin**) aşağıdaki bilgileri girmeniz gerekir:

- **Sunucu** - sunucunun IP adresini ya da sunucunun adını girin



- **Bağlantı Noktası** - İnternet erişimine açık bağlantı noktasının numarasını girin (*varsayılan olarak bu değer 3128 olarak atanmıştır fakat isteğiniz doğrultusunda değiştirebilirsiniz - emin değilseniz lütfen ağ yöneticiniz ile irtibat kurun*)

Proxy sunucusunda her kullanıcı için farklı kurallar yapılandırılabilir. Proxy sunucunuz bu şekilde yapılandırılmış ise proxy sunucusu üzerinden yapılan İnternet bağlantınıza ilişkin kullanıcı adı ve parolanızı onaylamak için **PROXY kimlik doğrulamasını kullan** seçeneğini işaretleyin.

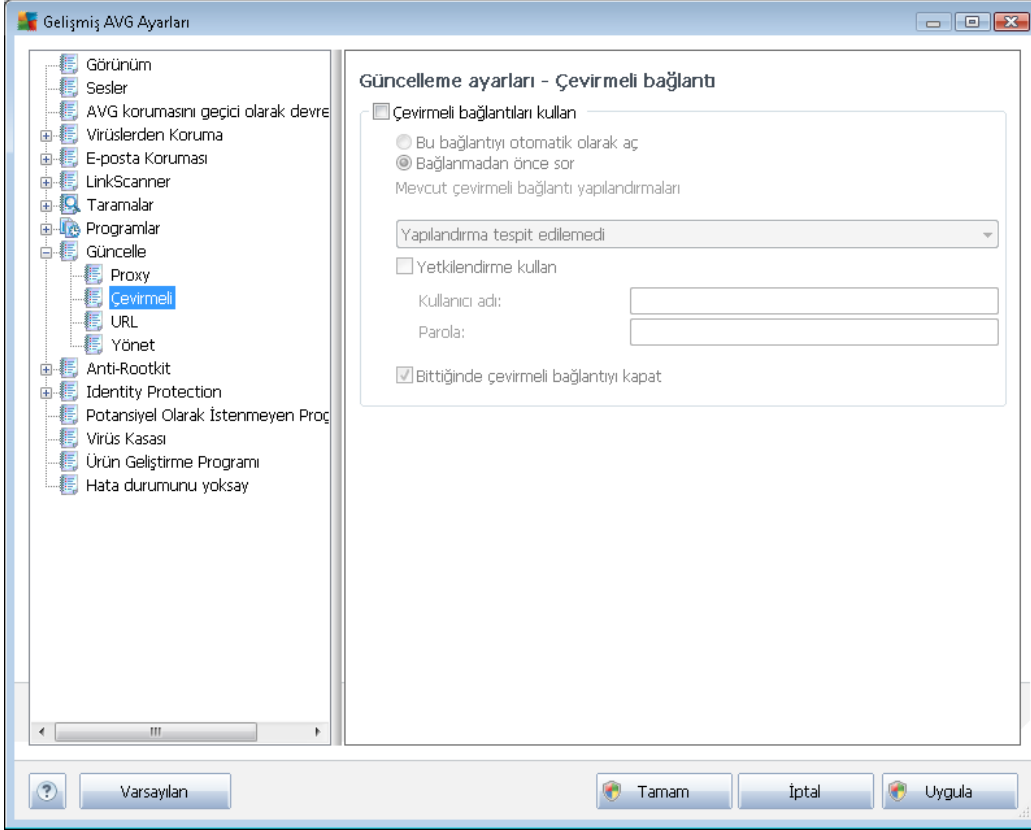
Otomatik yapılandırma

Otomatik yapılandırmayı seçerseniz (*ilgili iletişim kutusunu etkinleştirmek için Oto seçeneğini işaretleyin*) ardından proxy yapılandırmasının nereden alınacağını belirleyin:

- **Tarayıcıdan** - Yapılandırma varsayılan İnternet tarayıcınızdan okunacaktır
- **Komut satırından** - yapılandırma, proxy adresine dönme fonksiyonu olan indirilmiş bir komut satırından okunacaktır
- **Otomatik Tespit Et** - yapılandırma otomatik olarak doğrudan proxy sunucusundan tespit edilecektir

9.9.2. Çevirmeli

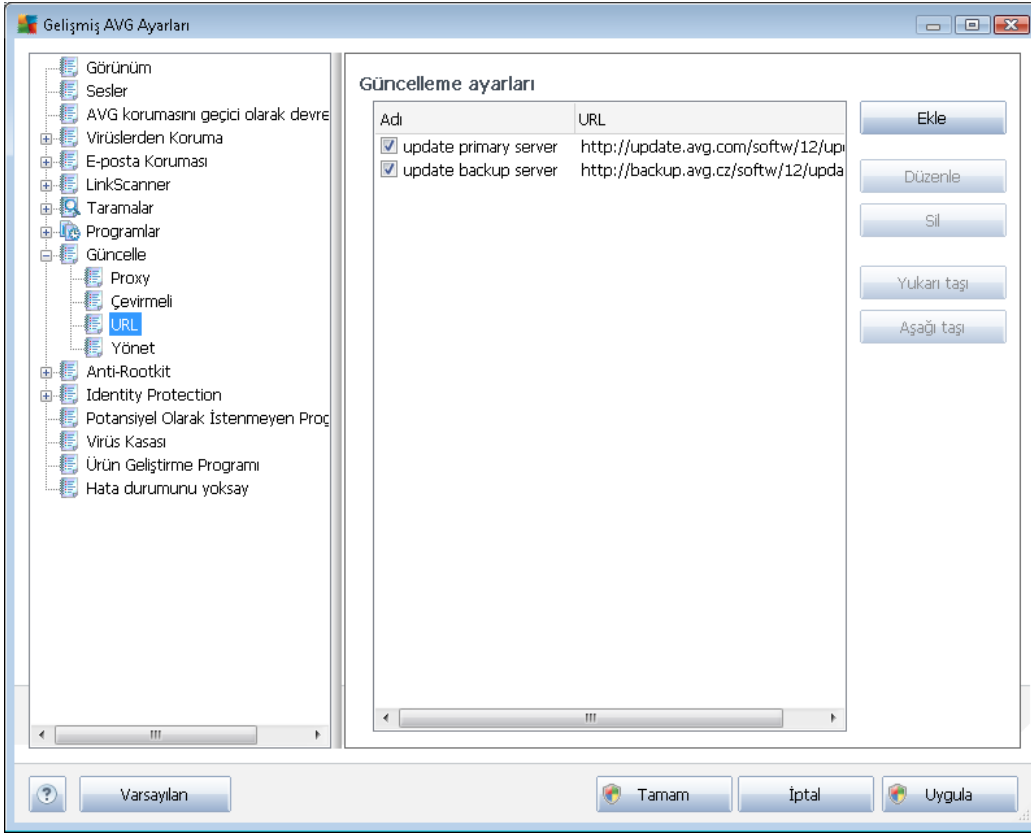
İsteğe bağlı olarak **Güncelleme ayarlarında tanımlanan tüm parametreler - Çevirmeli Bağlantı** iletişim kutusu İnternet'e çevirmeli bağlantı ile bağlanılmasına ilişkindir. **Çevirmeli bağlantı kullan** seçeneği seçilip alanlar etkinleştirilene kadar iletişim kutusunun alanları pasif olacaktır:



İnternet'e otomatik olarak bağlanmak isteyip istemediğinizi (***Bu bağlantıyı otomatik olarak aç***) ya da bağlantıyı her seferinde manüel olarak kurmak isteyip istemediğinizi (***Bağlanmadan önce sor***) seçin. Otomatik bağlantılarda güncellemenin tamamlanmasının ardından bağlantının kesilmesini isteyip istemediğinizi de seçin (***Tamamlandığı zaman çevirmeli bağlantıyı kes***).

9.9.3. URL

URL iletişim kutusunda güncelleme dosyalarının indirilebileceği bir dizi internet adresi bulunur:



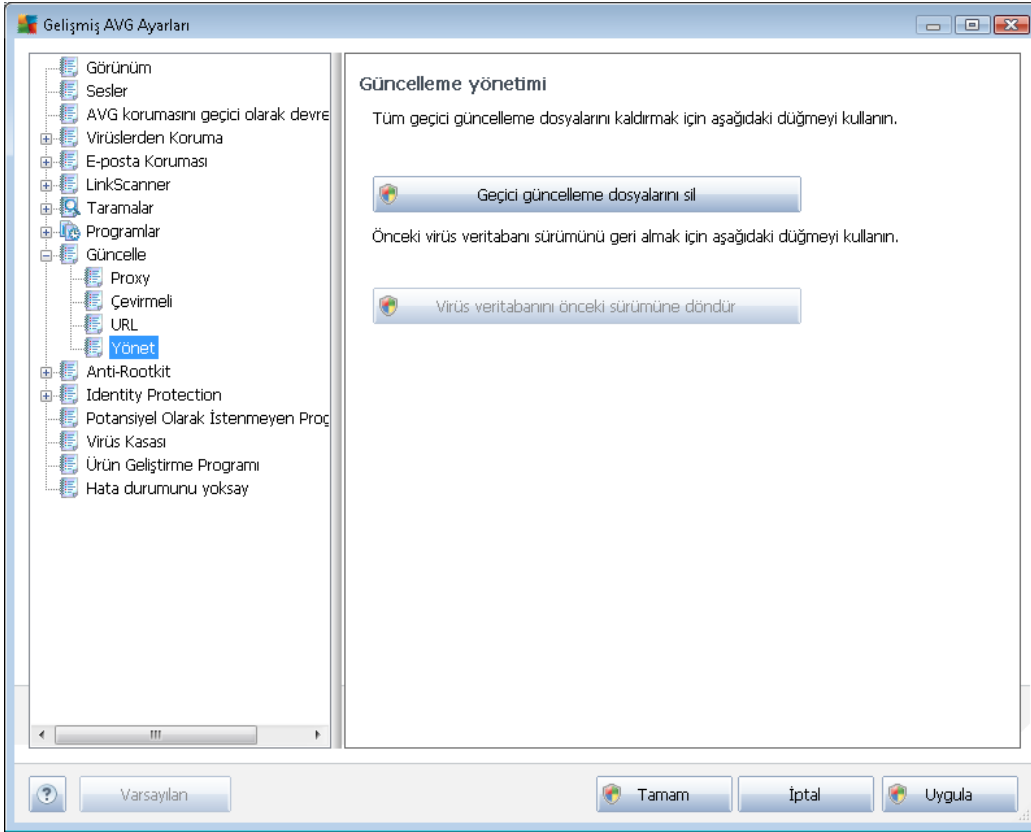
Kontrol düğmeleri

Liste ve liste öğeleri aşağıdaki kontrol düğmeleri kullanılarak düzenlenebilir:

- **Ekle** - Listenize yeni bir URL eklemek için kullanacağınız iletişim kutusunu açar
- **Düzenle** - seçilen URL parametrelerini düzenleyebileceğiniz iletişim kutusunu açar
- **Sil** - seçilen URL'yi listeden seçer
- **Yukarı Taşı** - seçilen URL'yi listede bir sıra yukarı taşır
- **Aşağı Taşı** - seçilen URL'yi listede bir sıra aşağı taşır

9.9.4. Yönetme

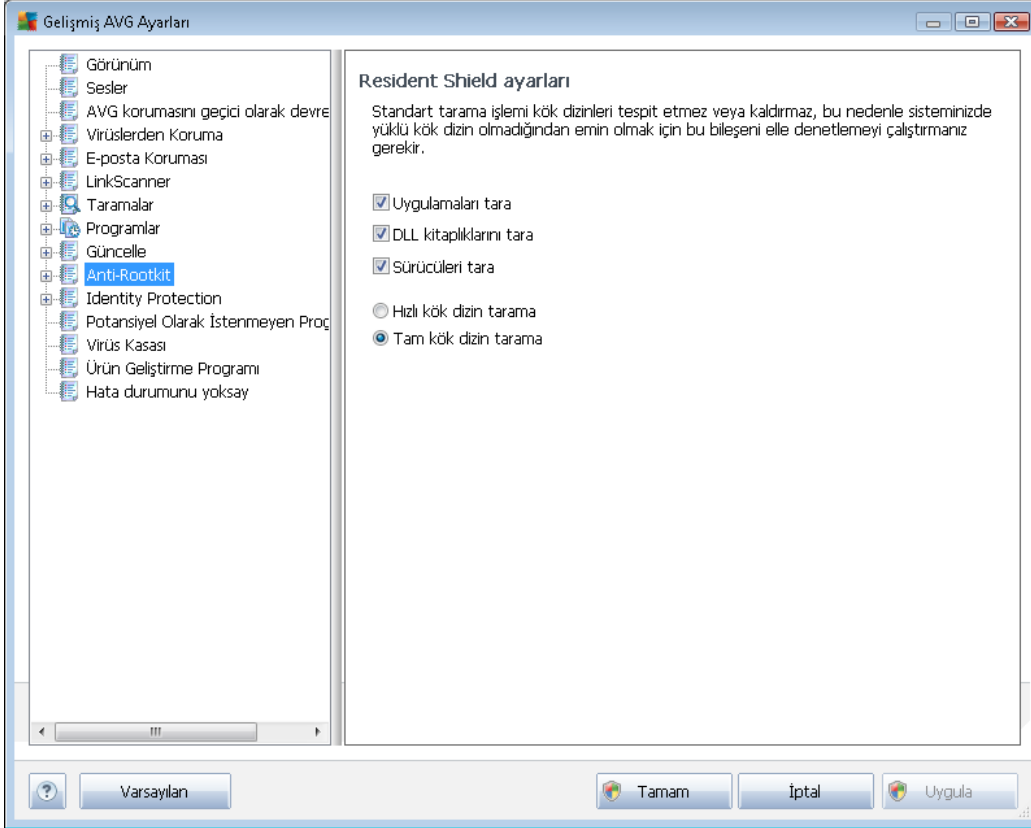
Güncelleme yönetimi iletişim kutusu, iki adet düğme ile ulaşılabilen iki seçenek sunmaktadır:



- **Geçici güncelleme dosyalarını sil** - tüm gereksiz güncelleme dosyalarını sabit diskinizden silmek için bu düğmeye basın (*öntanımlı olarak söz konusu dosyalar 30 gün boyunca saklanır*)
- **Virüs veritabanını bir önceki sürüme döndür** - En güncel virüs veritabanını sabit diskinizden silmek ve daha önce kaydedilmiş sürüme dönmek için bu düğmeye basın (*yeni virüs tabanı sürümü, bir sonraki güncellemenin bir parçası olacaktır*)

9.10. Anti-Rootkit

Anti-Rootkit ayarları iletişim kutusunda [Anti-Rootkit](#) bileşenin yapılandırmasını düzenleyebilirsiniz:



İletişim kutusu içinde sağlanan [Anti-Rootkit](#) bileşenin tüm işlemlerinin düzenlenmesine [Anti-Rootkit bileşenin arayüzünden](#) de ulaşabilirsiniz.

Taranmasını istediğiniz nesnelere belirlemek üzere ilgili kutuları işaretleyin:

- **Uygulamaları tara**
- **DLL kitaplıklarını tara**
- **Sürücülerini tara**

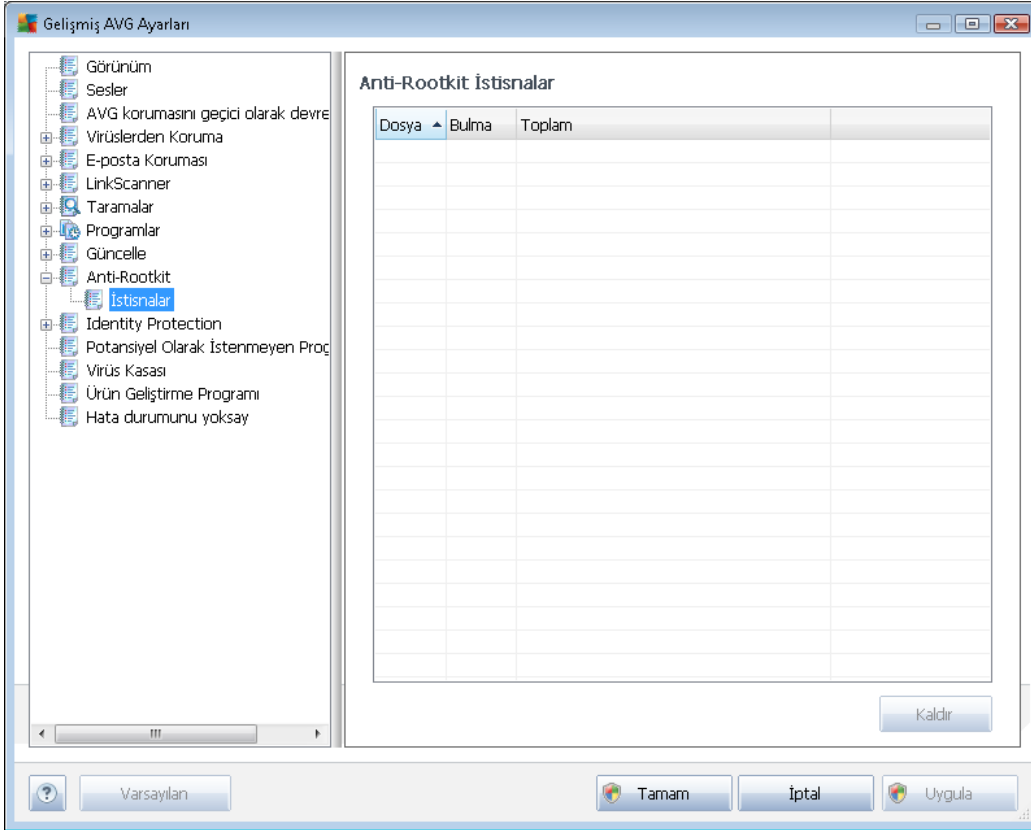
Bunun ardından kök dizin tarama modunu da seçebilirsiniz:

- **Hızlı kök dizin tarama** - çalışan tüm işlemleri, yüklü sürücülerini ve sistem klasörlerini (genellikle *c:\Windows*) tarar
- **Tam kök dizin tarama** - çalışan tüm işlemleri, yüklü sürücülerini, sistem klasörünü (genellikle *c:\Windows*), ayrıca tüm yerel diskleri (*flash disk dahil, ancak disket/CD sürücülerini hariç*) tarar



9.10.1. İstisnalar

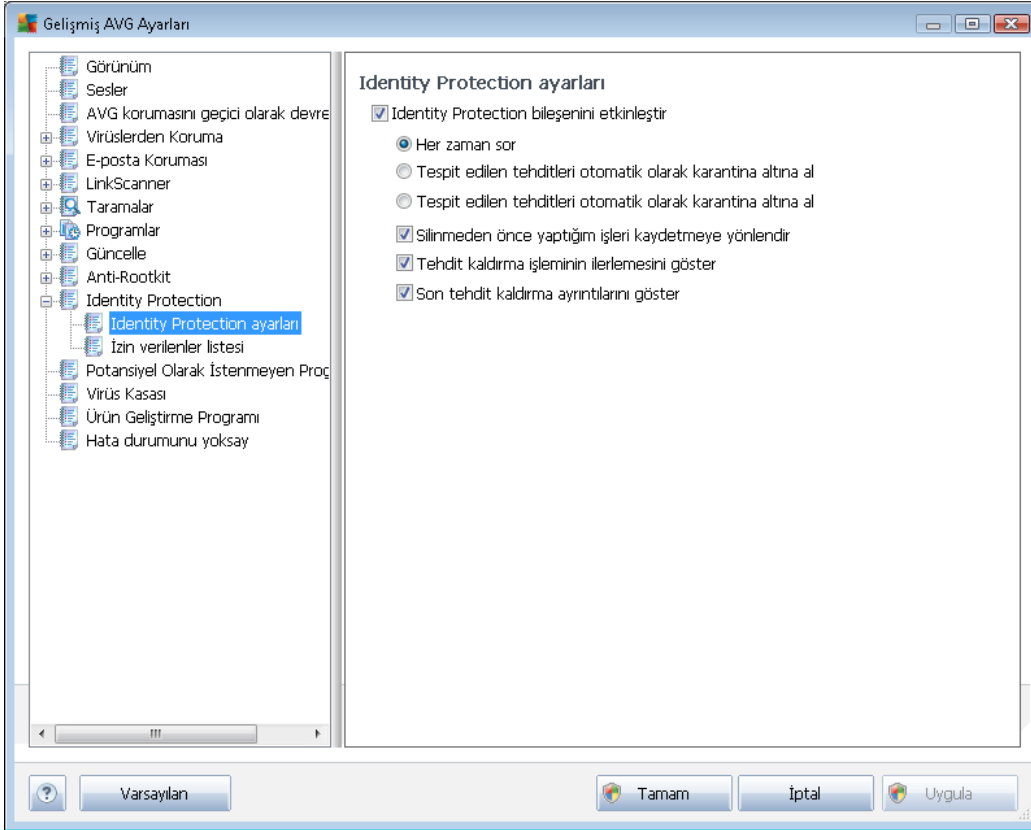
Anti-Rootkit İstisnaları iletişim kutusunda belirli dosyaları bu taramanın dışında tutulması için belirleyebilirsiniz (*örneğin yanlışlıkla kök dizin olarak silinebilecek bazı sürücüler*):



9.11. Identity Protection

9.11.1. Identity Protection Ayarları

Kimlik Koruması ayarları iletişim kutusu [Kimlik Koruması](#) bileşeninin temel özelliklerini açmanızı/ kapatmanızı sağlar:



Kimlik Korumasını Etkinleştir (varsayılanda açıktır) - [Kimlik Koruması](#) bileşenini kapatmak için işaretleyin.

Zorunlu olmadıkça, bu işareti kaldırmamanızı önemle tavsiye ederiz!

[Identity Protection](#) etkinleştirildiğinde, bir tehlike algılandığında ne yapacağınızı belirtebilirsiniz:

- **Her zaman sor** (varsayılan olarak açıktır) - bir tehlike algılandığında, çalıştırmak istediğiniz bir uygulamanın kaldırılmamasından emin olmak için karantinaya alınması gerekir gerekmediği size sorulacaktır.
- **Algılanan tehlikeleri otomatik olarak karantinaya al** - Algılanan tüm olası tehlikelerin [Virüs Kasası](#) güvenilir alanına hemen taşınmasını istediğinizi tanımlamak için bu onay kutusunu işaretleyin. Varsayılan ayarlarda, bir tehlike algılandığında, çalıştırmak istediğiniz hiçbir uygulamanın kaldırılmaması için size uygulamanın karantinaya alınması gerekir gerekmediği sorulacaktır.
- **Bilinen tehlikeleri otomatik olarak karantinaya al** - kötü amaçlı yazılım olasılığı algılanan tüm uygulamaların otomatik olarak ve hemen [Virüs Kasası](#)'na alınmasını istiyorsanız bu öğeyi işaretli bırakın.

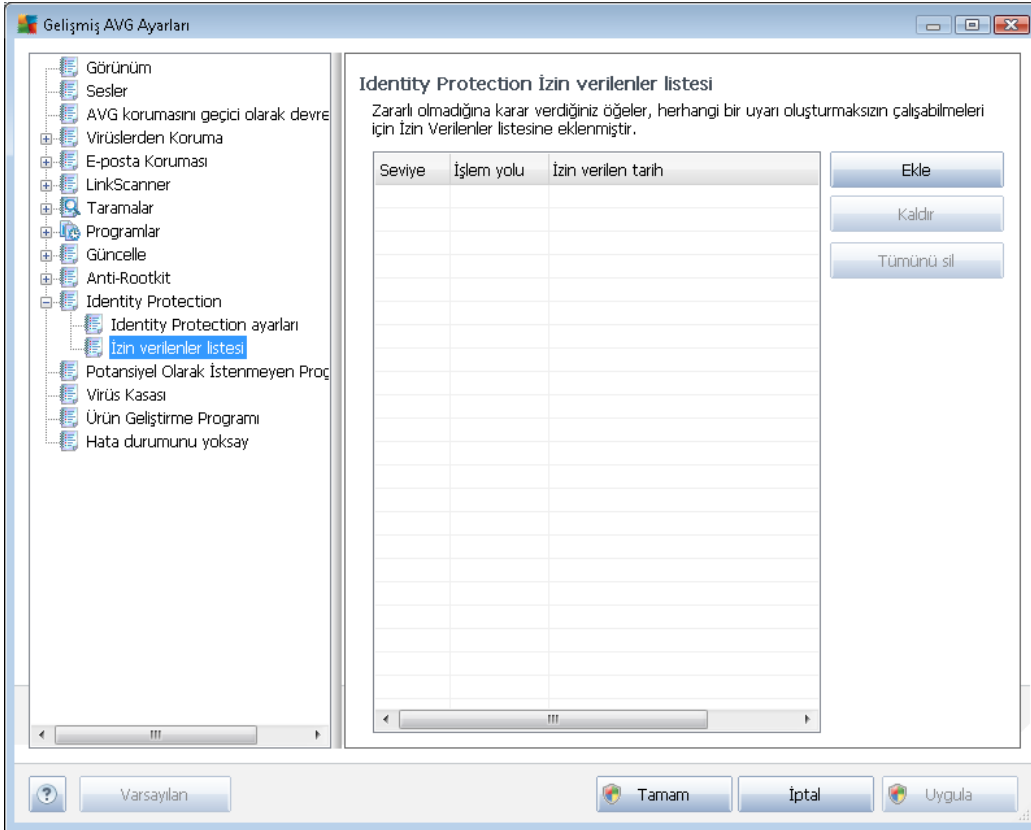


Ayrıca, belirli öğeleri isteğe bağlı olarak etkin daha fazla [Identity Protection](#) işlemlerine atayabilirsiniz:

- **Kaldırmadan önce işi kaydetmek isteyip istemediğimi sor** - (varsayılan olarak açık) - olası kötü amaçlı yazılım olarak algılanan uygulama karantinaya alınmadan önce uyarılmak istiyorsanız bu öğeyi işaretli bırakın. Uygulamayı çalıştırmak istiyorsanız, projeniz kaybolabilir ve önce kaydetmeniz gerekir. Varsayılan olarak, bu öğe açıktır ve böyle kalmasını önemle öneririz.
- **Kötü amaçlı yazılım kaldırma sürecini göster** - (varsayılan olarak açık) - bu öğe açıkken, kötü amaçlı bir yazılım algılandığında, kötü amaçlı yazılımın karantinaya alınma işlemini gösteren yeni bir iletişim kutusu açılır.
- **Son kötü amaçlı yazılım kaldırma ayrıntılarını göster** - (varsayılan olarak açık) - bu öğe açıkken, **Identity Protection**, karantinaya kaldırılan her nesne hakkında ayrıntılı bilgi görüntüler (*güvenlik seviyesi, konum vb.*).

9.11.2. İzin Verilenler Listesi

Kimlik Koruması ayarları iletişim kutusu içinde **Algılanan tehlikeleri otomatik olarak karantinaya al** öğesinin işaretini kaldırmaya karar vererseniz, tehlikeli olabilecek bir kötü amaçlı yazılım her algılandığında, kaldırmak isteyip istemeyeceğiniz sorulacaktır. Şüpheli uygulamayı (*davranışına göre algılandı*) güvenli olarak atarsanız ve bilgisayarınızda kalmasını onaylarsanız, uygulama **Kimlik Koruması İzin Verilenler listesi** olarak adlandırılan listeye eklenecek ve bir daha potansiyel olarak tehlikeli şeklinde bildirilmeyecektir:



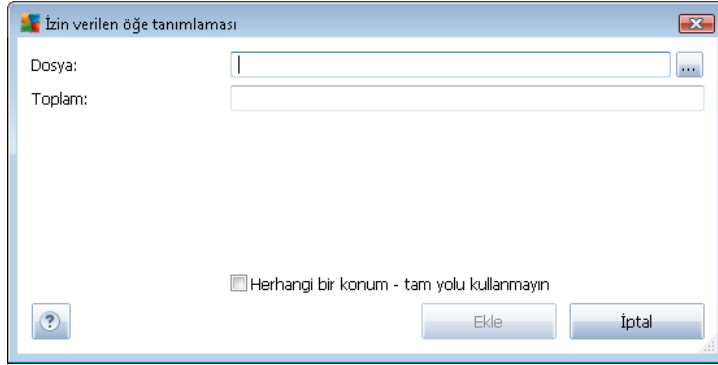
Kimlik Koruması İzin Verilenler listesi her uygulamada aşağıdaki bilgileri sağlar:

- **Seviye** - ilgili sürecin önem derecesinin en düşükten (■□□□) en kritiğe (■□■□) dört seviyeli ölçekte grafiksel olarak tanımlanmasıdır
- **İşlem yolu** - uygulamanın (süreç) çalıştırılabilir dosya konumuna götüren yoldur
- **İzin tarihi** - uygulamayı elle güvenli olarak atadığınız tarihtir

Kontrol düğmeleri

Kimlik Koruması İzin Verilenler listesi iletişim kutusu içerisinde bulunan kontrol düğmeleri şunlardır:

- **Ekle** - izin verilenler listesine yeni bir uygulama eklemek için bu düğmeye basın. Aşağıdaki iletişim kutusu açılır:

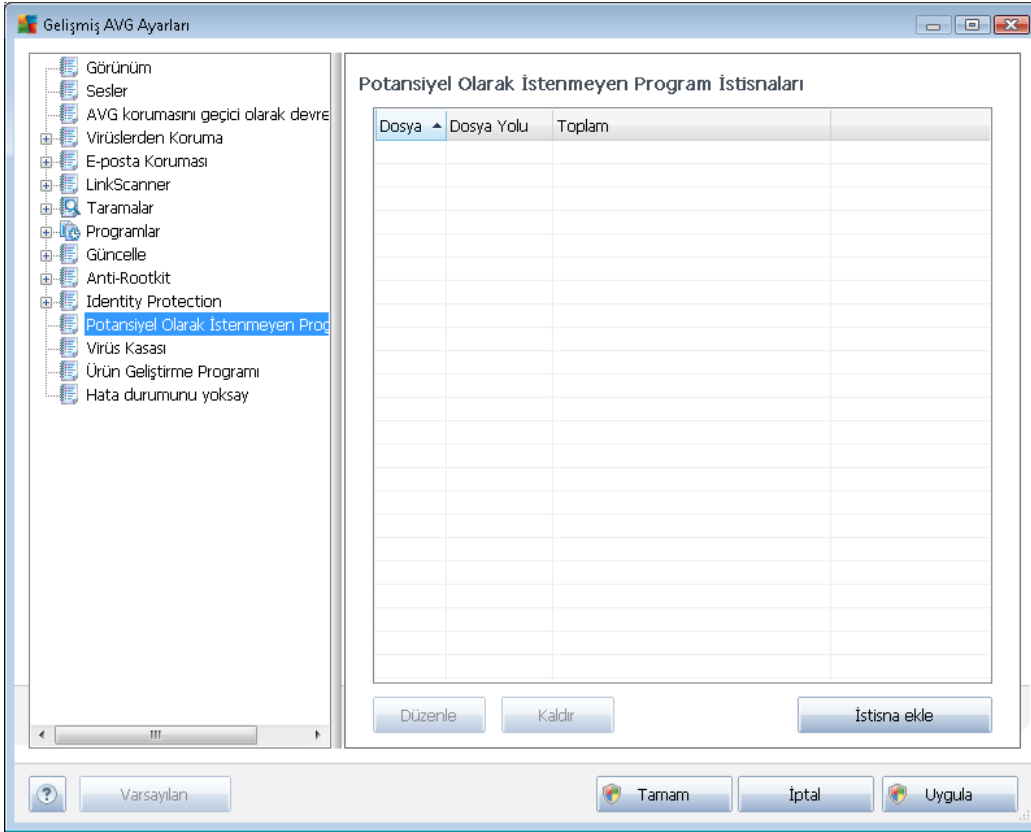


- **Dosya** - istisna olarak işaretlemek istediğiniz dosyanın (*uygulama*) tam yolunu yazın
- **İmzayı Kontrol Et** - seçilen dosyanın benzersiz 'imzasını' görüntüler. Bu sağlama, AVG'nin seçilen dosyayı diğer dosyalardan ayırmasını sağlamak üzere otomatik oluşturulan karakter dizeleridir. Sağlama, dosyanın başarıyla eklenmesinin ardından oluşturulur ve görüntülenir.
- **Herhangi bir yerde - tam yolu kullanmayın** - bu dosyayı sadece belirli bir konumda istisna olarak atamak istiyorsanız bu onay kutusunu işaretlemeyin
- **Kaldır** - seçili uygulamayı listeden kaldırmak için basın
- **Tümünü kaldır** - listelenen tüm uygulamaları kaldırmak için basın

9.12. Potansiyel Olarak İstenmeyen Programlar

AVG Internet Security 2012, bunun yanı sıra sistemde potansiyel anlamda istenmeyen çalıştırılabilir uygulamaları ya da DLL kütüphanelerini de inceleyebilmekte ve tespit edebilmektedir. Bazı durumlarda kullanıcı belirli istenmeyen programların (bilerek yüklenen programlar) bilgisayarında bulunmasını tercih edebilir. Bunlardan bazıları reklam yazılımları ve özellikle ücretsiz yazılımlardır. Bu

tür reklam yazılımları **AVG Internet Security 2012** tarafından *potansiyel olarak istenmeyen program* olarak tespit edilip raporlanabilir. Söz konusu programın bilgisayarınızda bulunmasını istiyorsanız ilgili programı, potansiyel olarak istenmeyen program istisnası şeklinde atayabilirsiniz:



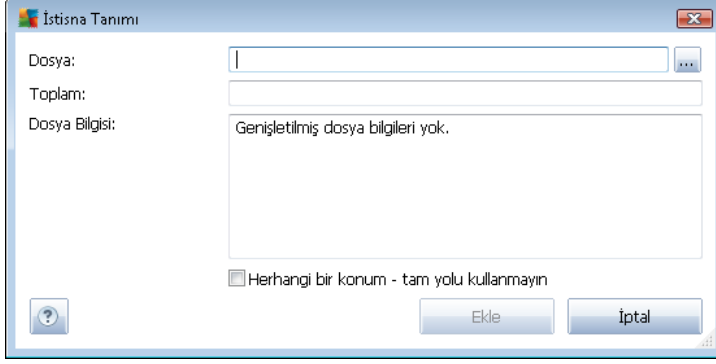
Potansiyel Olarak İstenmeyen Program İstisnaları iletişim kutusunda, potansiyel olarak istenmeyen programlardan tanımlanan ve mevcut durumda geçerli istisnalar bulunmaktadır. Listeyi düzenleyebilir, varolan öğeleri silebilir veya yeni istisnalar ekleyebilirsiniz. Aşağıdaki bilgiler her bir istisna için listede bulunabilir:

- **Dosya** - İlgili uygulamanın tam adını sağlar
- **Dosya Yolu** - Uygulamanın konumuna olan yolu gösterir
- **İmzayı Kontrol Et** - seçilen dosyanın 'imzasını' görüntüler. Bu sağlama, AVG'nin seçilen dosyayı diğer dosyalardan ayırmasını sağlamak üzere otomatik oluşturulan karakter dizeleridir. Sağlama, dosyanın başarıyla eklenmesinin ardından oluşturulur ve görüntülenir.

Kontrol düğmeleri

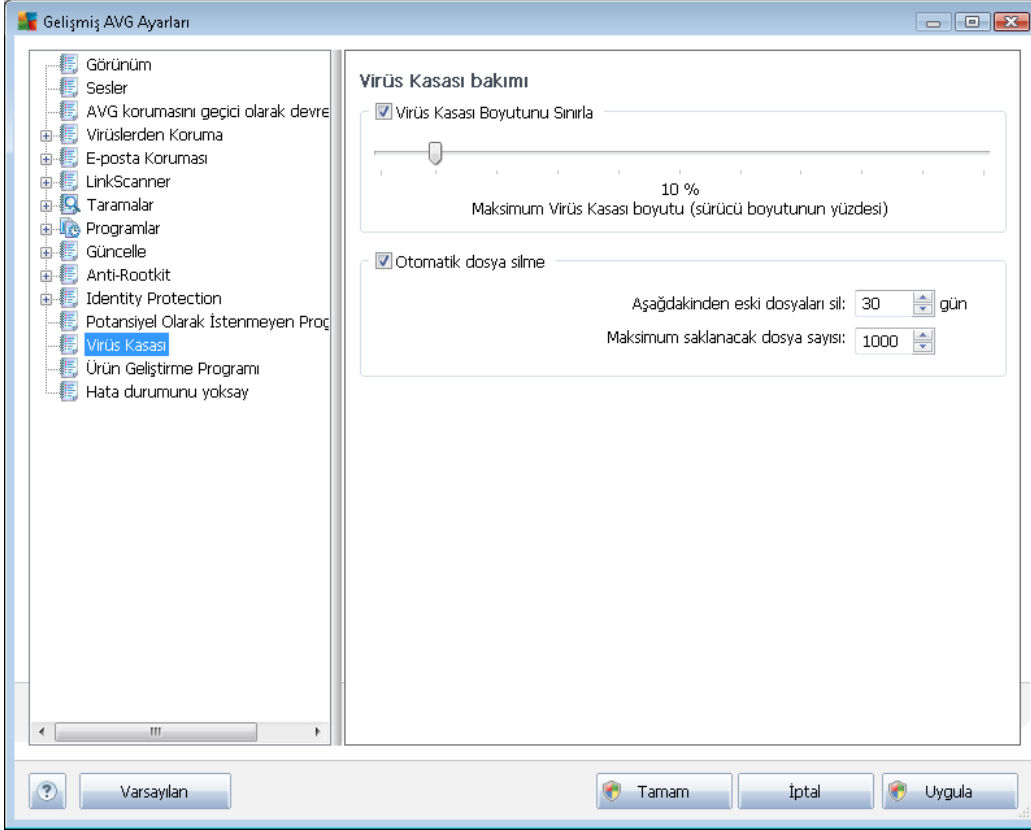
- **Düzenle** - önceden tanımlanmış olan bir istisnanın parametrelerini düzenleyebileceğiniz bir düzenleme iletişim kutusu açar (*yeni istisna tanımı iletişim kutusuyla aynı, aşağıya bakın*)
- **Sil** - seçilen öğeyi istisnalar listesinden siler

- **İstisna ekle** - oluşturulacak yeni istisnanın parametrelerini tanımlayabileceğiniz yeni bir düzenleme iletişim kutusu açar:



- **Dosya** - istisna olarak belirlemek istediğiniz dosyanın tam yolunu girin
- **İmzayı Kontrol Et** - seçilen dosyanın "özel imzasını" görüntüler. Bu sağlama, AVG'nin seçilen dosyayı diğer dosyalardan ayırmasını sağlamak üzere otomatik oluşturulan karakter dizeleridir. Sağlama, dosyanın başarıyla eklenmesinin ardından oluşturulur ve görüntülenir.
- **Dosya Bilgisi** - dosya hakkında (lisans/sürüm bilgileri vb.) mevcut tüm bilgileri görüntüler.
- **Herhangi bir yerde - tam yolu kullanma** - söz konusu dosyayı sadece belirli bir konumda istisna olarak atamak istiyorsanız bu kutucuğu işaretlemeyin. Onay kutusu işaretlenirse, belirtilen dosya nerede bulunduğuna bağlı olmaksızın istisna olarak atanır (ancak, belirli dosya için yine de tam yolu doldurmanız gerekir, bundan sonra dosya aynı ada sahip iki dosyanın sisteminizde görüntülenme olasılığının benzersiz bir örneği olarak kullanılır).

9.13. Virüs Kasası



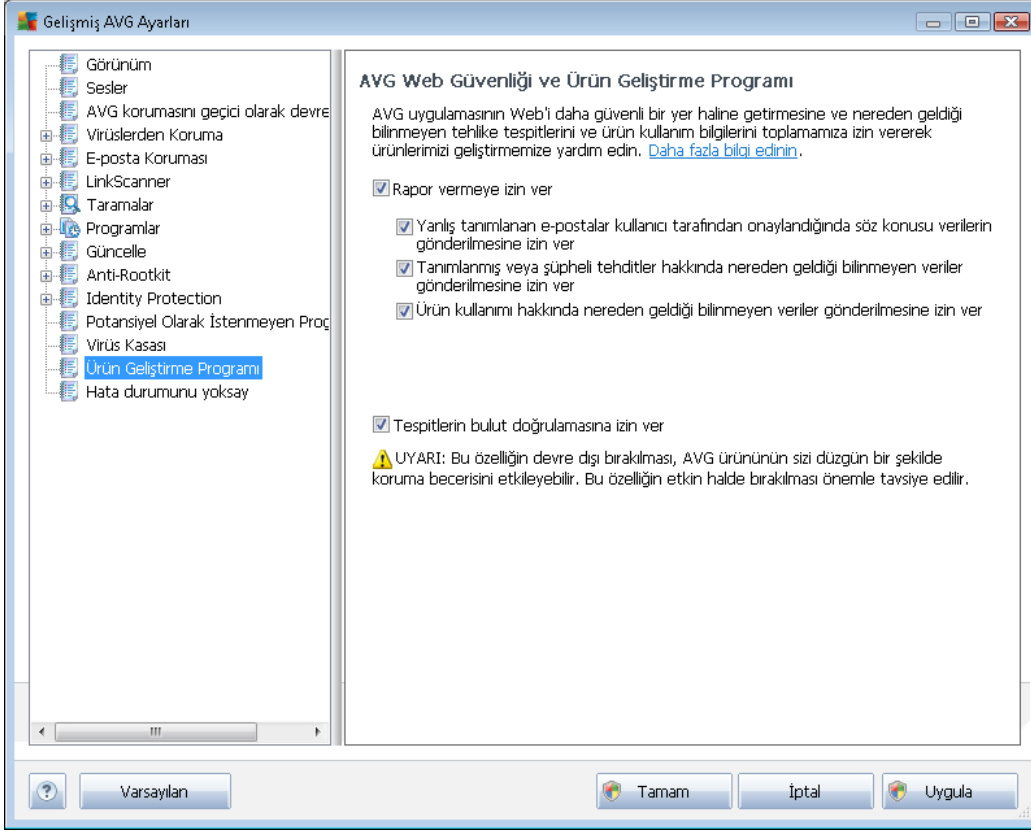
Virüs Kasası bakımı iletişim kutusu, [Virüs Kasası](#)'nda depolanan nesnelerin yönetimi hususunda çeşitli parametreleri tanımlayabilmenizi sağlar:

- **Virüs Kasası boyutunu sınırla** - [Virüs Kasasının](#) maksimum boyutunu ayarlamak için kaydırıcıyı kullanın. Söz konusu boyut, sabit diskinizin boyutu ile doğru orantılı olacaktır.
- **Otomatik dosya silme** - Bu bölümde nesnelerin [Virüs Kasasında](#) depolanacakları maksimum süreyi (... **Günden eski dosyaları sil**), [Virüs Kasasında](#) depolanacak maksimum dosya sayısını (**Depolanacak maksimum dosya sayısı**) belirleyebilirsiniz.

9.14. Ürün Geliştirme Programı

AVG Web Güvenliği ve Ürün Geliştirme Programı iletişim kutusu sizi AVG ürün geliştirme programına katılmaya ve genel İnternet güvenliği düzeyini artırmamıza yardım etmeye davet eder. Tespit edilen tehditlerin AVG'ye bildirilmesini etkinleştirmek için **Raporlamaya izin ver** seçeneğini işaretli tutun. Bu, dünyanın her tarafındaki katılımcılardan en son tehditlere ilişkin güncel bilgileri toplamamıza ve koruma özelliklerini herkes için geliştirmemize yardımcı olacaktır.

Raporlama işlemi otomatik olarak gerçekleştirilir; bu nedenle sizi herhangi bir şekilde rahatsız etmez. Raporlar kişisel bilgilerinizi içermez. Tespit edilen tehditlerin rapor edilmesi isteğe bağlıdır, ancak, bu seçeneği açık bırakmanızı rica ediyoruz. Böylece hem siz hem de diğer AVG kullanıcıları için korumayı geliştirmeye devam edebiliriz.



Günümüzde, normal virüslerin dışında çok fazla tehdit bulunmaktadır. Kötü amaçlı yazılımların ve tehlikeli web sitelerinin yazarları çok yenilikçidir ve yeni tehdit türleri oldukça sık ortaya çıkar, bunların oldukça büyük bir çoğunluğu ise İnternet üzerindedir. Bu tehditlerin en yaygın olanları şunlardır:

- **Virüs**, kendi kendini kopyalayan ve yayılan zararlı bir koddur ve genellikle zarar oluşana kadar fark edilmez. Bazı virüsler ciddi bir tehdit oluşturur, dosyaları siler veya istediği şekilde değiştirir. Bazı virüsler ise görünüşte zararsız olan müzik çalma gibi işlemler yapar. Ancak, temel olarak sahip oldukları çoğalma özelliği nedeniyle tehlikelidir. En basit virüs bile bilgisayarınızın tüm belleğini bir anda ele geçirebilir ve bilgisayarın çökmesine neden olur.
- **Solucan**, normal virüsün aksine, "taşıyıcı" nesneye gerek duymayan bir virüs alt kategorisidir; genellikle e-posta yoluyla kendini diğer bilgisayarlara gönderir ve e-posta sunucuları ve ağ sistemlerinde aşırı yüklenmeye neden olur.
- **Casus yazılım**, genellikle kötü amaçlı kategorisinde (*kötü niyetli yazılım = virüsler de dahil tüm kötü amaçlı yazılımlar*) yer alan programlardır (genellikle Truva atlarıdır). Bu tür yazılımların amacı kişisel bilgileri, şifreleri, kredi kartı numaralarını çalmak veya bir bilgisayarın içine sızarak saldırganın bilgisayarı uzaktan yönetmesini sağlamaktır. Elbette, bunların hepsi bilgisayar sahibinin izni veya bilgisi olmadan yapılır.
- **Potansiyel olarak istenmeyen programlar**, tehlikeli olabilecek ancak bilgisayarınız için mutlaka tehlikeli olması gerekmeyen bir casus yazılım türüdür. Özel bir PUP örneği reklam



yazılımlardır. Bu yazılımlar, genellikle açılır pencerelerde reklam görüntülemek üzere tasarlanır. Can sıkıcıdır ancak gerçekte zararlı değildir.

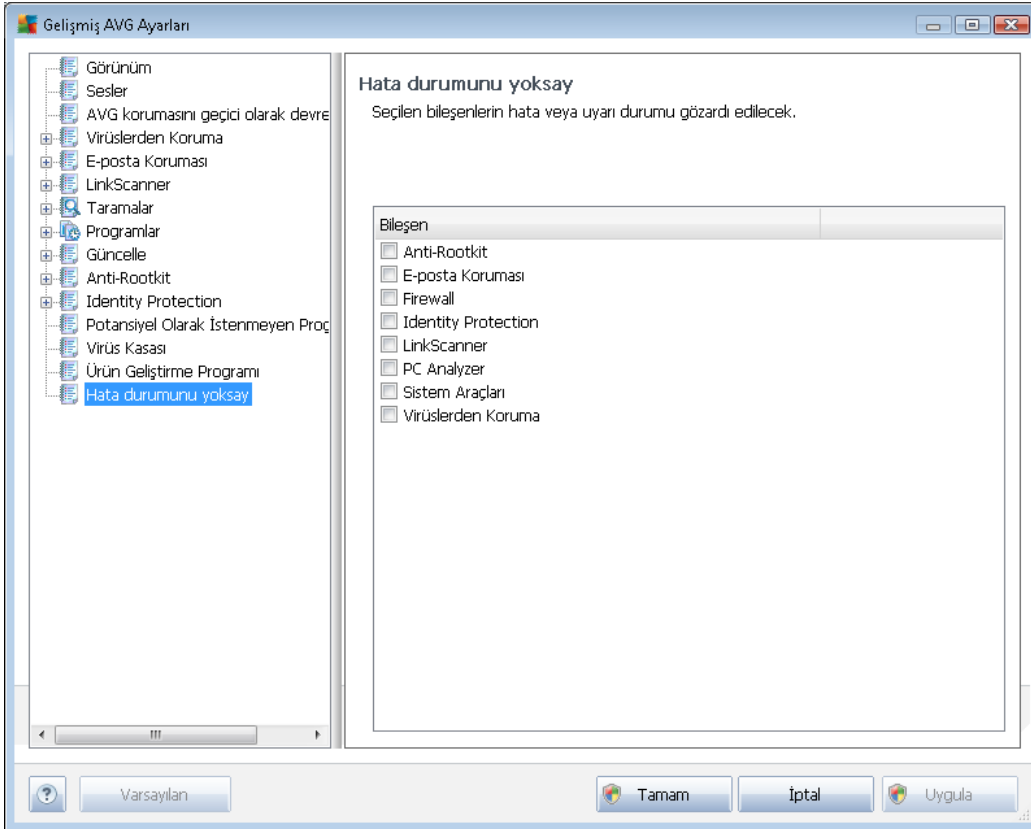
- **İzleme çerezleri** de bir casus yazılım türü olarak değerlendirilebilir. Bu küçük dosyalar web tarayıcısında saklandığından ve tekrar ziyaret ettiğinizde "ana" web sitesine otomatik olarak gönderildiğinden, tarama geçmişiniz ve benzer diğer bilgiler gibi verileri içerebilir.
- **Güvenlik açığı yazılımı**, işletim sistemindeki, İnternet tarayıcısındaki veya gerekli diğer programlardaki bir açıktan faydalanan kötü amaçlı bir koddur.
- **Kimlik Avı**, kendilerini güvenilir veya tanınmış kuruluş gibi göstererek hassas kişisel verileri elde etme girişimidir. Genel olarak, potansiyel kurbanlara, örneğin banka hesabı bilgilerini güncellemelerini isteyen toplu postalarla ulaşılır. Bunu yapmak için, kişilerden verilen bağlantıyı ziyaret etmeleri istenir. Bu bağlantı sahte bir banka web sitesine yönlendirir.
- **Aldatmaca (Hoax)** tehlikeli, uyarda bulunan veya yalnızca rahatsız edici ve gereksiz bilgiler içeren toplu e-postalardır. Yukarıdaki tehditlerin çoğu, yayılmak için aldatıcı e-posta iletilerini kullanır.
- **Kötü amaçlı web siteleri**, bilgisayarınıza bilerek kötü amaçlı yazılım yükleyen sitelerdir. Saldırıya uğrayan siteler de aynısını yapar ancak bunlar kötü amaçlı ziyaretçiler tarafından zarar verilen yasal web siteleridir.

AVG Internet Security 2012 sizi farklı türlerdeki tüm bu tehditlerden korumak için özel bileşenler içerir. Bu bileşenlerin kısa bir açıklaması için lütfen [Bileşen Genel Görünümü](#) bölümüne bakın.



9.15. Hata durumunu yoksay

Hata durumunu yoksay iletişim kutusunda, bilgilendirilmek istemediğiniz bileşenleri seçebilirsiniz:



Varsayılan olarak listede herhangi bir bileşen seçilmemiştir. Bileşenlerden herhangi biri hatalı duruma düşerse aşağıdaki yöntemlerden biri vasıtasıyla uyarılacaksınız demektir:

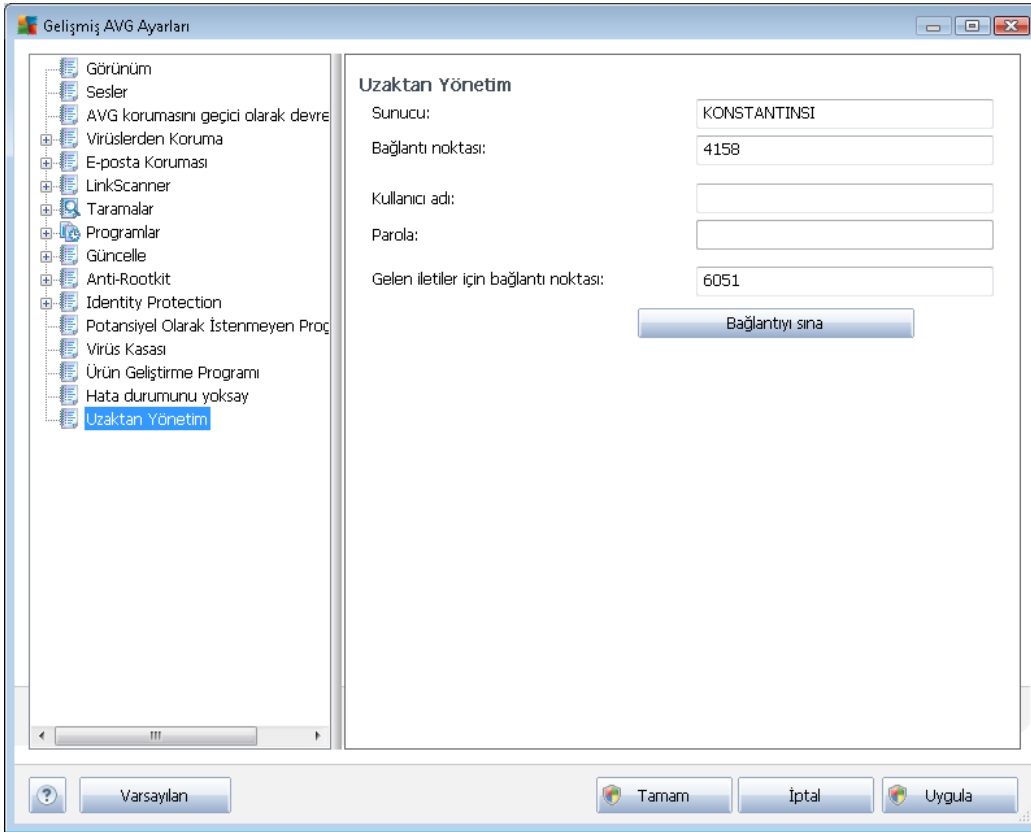
- [sistem tepsisi simgesi](#) - AVG'nin tüm bileşenleri doğru şekilde çalışırken simge, 4 renkli görünecektir ancak herhangi bir aksaklık olursa simgenin yanında sarı bir ünlem işareti görülür,
- AVG ana penceresinin [Güvenlik Durumu Bilgileri](#) bölümünde mevcut sorun açıklanır

Bileşenlerden birini geçici bir süre kapatmanız gereken bir durum ile karşılaşabilirsiniz (*bileşenlerin geçici süre kapatılması önerilmez. Tüm bileşenleri daima açık durumda tutmanız ve varsayılan yapılandırmayı muhafaza etmeniz gerekir ancak aksi durumlarla karşılaşabilirsiniz*). Bu durumda sistem tepsisi simgesi, bileşenin hata durumunda olduğunu otomatik olarak bildirir. Ancak bu durumda gerçek bir hatadan söz edemeyiz çünkü hatayı siz başlatmışsınızdır ve potansiyel riskin farkında olmalısınız. Aynı zamanda, simge gri renkli görüntüledikten sonra daha sonra meydana gelecek hataları rapor edemez.

Bu durumda yukarıdaki pencerede hata durumunda olan (*ya da kapatılmış*) bileşenleri seçebilirsiniz ve söz konusu durum hakkında bilgilendirilmek istemeyebilirsiniz. Aynı seçenek (*Bileşen durumunu yok say*) doğrudan [AVG ana ekranının bileşenlere genel bakış penceresinden de](#) kullanılabilir.

9.16. Uzaktan Yönetim

Uzaktan Yönetim ögesi ve ilgili iletişim kutusu, ancak **AVG Internet Security 2012** ürününüzü AVG Business Edition lisanslarından birini kullanarak kurduğunuz ve kurulum sırasında **Uzaktan Yönetim** bileşenin kurulmasını onaylamış olmanız durumunda, menü ağacında görüntülenir. Uzaktan yönetim kurulumu ve yapılandırması hakkında ayrıntılı bilgi için lütfen AVG web sitesi (<http://www.avg.com/>), [Destek Merkezi / İndirme](#) bölümünden indirilebilen AVG Network Edition belgelerine bakın.



Uzaktan Yönetim ayarları, AVG istemci istasyonunu uzak yönetici sisteme bağlamaya ilişkindir. İlgili istasyonu uzaktan yönetime bağlamak istiyorsanız lütfen aşağıdaki parametreleri girin:

- **Sunucu** - AVG Admin Sunucusunun yüklü olduğu sunucu adı (ya da sunucunun IP adresi)
- **Bağlantı Noktası** - AVG istemcisinin AVG Admin Sunucusu ile iletişim kurduğu bağlantı noktası numarasıdır (*varsayılan olarak 4158 numaralı bağlantı noktası kullanılmaktadır - bu bağlantı noktası numarasını kullanırsanız herhangi bir işlem yapmanıza gerek kalmaz*)
- **Oturum Açma Bilgileri** - AVG istemcisi ile AVG Admin Sunucusu arasındaki ilişki güvenli bir bağlantı ise kullanıcı adınızı girin...
- **Parola** - ... parolanızı girin
- **Gelen mesajlar için bağlantı noktası** - AVG istemcisinin AVG Admin Sunucusu'ndan



gelen mesajları kabul ettiği bağlantı noktası numarasıdır

Kontrol düğmeleri

Bağlantıyı sına düğmesi, yukarıda belirtilen verilerin tümünün geçerliliğini onaylamanıza yardımcı olur ve DataCenter'a başarıyla bağlanmak için kullanılabilir.

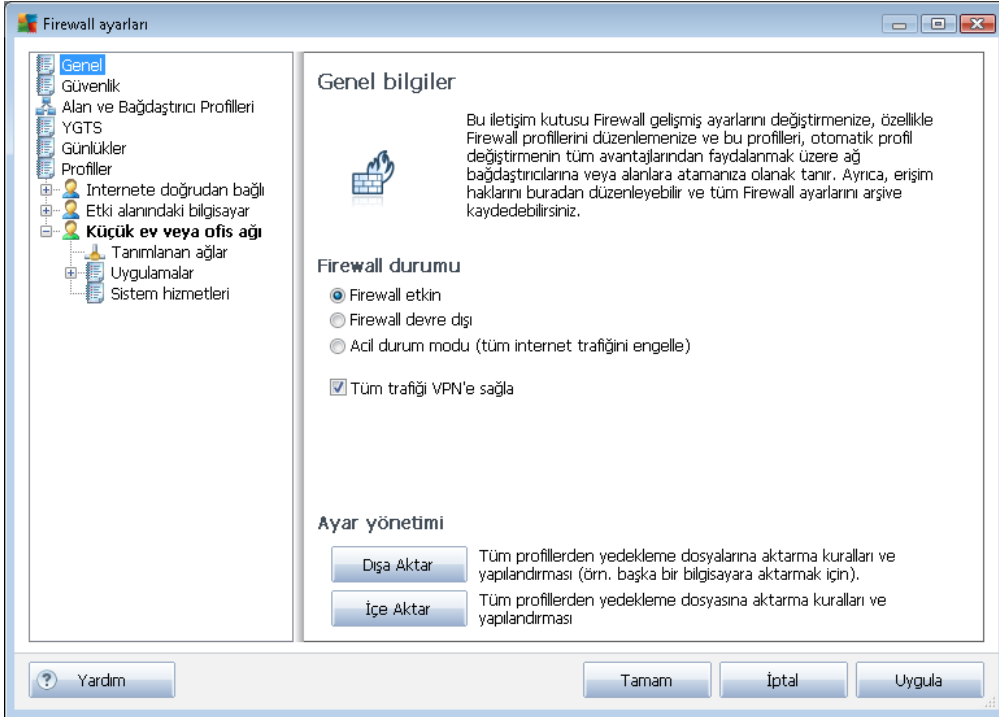
10. Güvenlik Duvarı Ayarları

[Güvenlik Duvarı](#) yapılandırması, çeşitli iletişim kutularında bileşenin gelişmiş parametrelerini yapılandırabileceğiniz yeni bir pencere açar.

Ancak, yazılım satıcısı tüm AVG Internet Security 2012 bileşenlerini optimum performans sağlayacak şekilde ayarlamıştır. Bunun için iyi bir nedeniniz olmadıkça varsayılan yapılandırmayı değiştirmeyin. Ayarlarda yapılacak her tür değişiklik sadece deneyimli bir kullanıcı tarafından gerçekleştirilmelidir!

10.1. Genel

Genel bilgiler iletişim kutusu iki bölüme ayrılır:



Güvenlik Duvarı durumu

Güvenlik Duvarı durumu bölümünde, gereksinim duyulduğunda [Güvenlik Duvarı](#) durumunu değiştirebilirsiniz:

- **Güvenlik Duvarı etkin** - seçilen [Güvenlik Duvarı profilinde](#) tanımlanan kural dizisi kapsamında "izin verilen" olarak atanmış uygulamalarla iletişim kurulmasına izin vermek için bu seçeneği belirleyin..
- **Güvenlik duvarı devre dışı** - bu seçenek [Güvenlik Duvarı](#)'nı tamamen kapatır ve tüm ağ trafiğine izin verilir ancak denetlenmez!

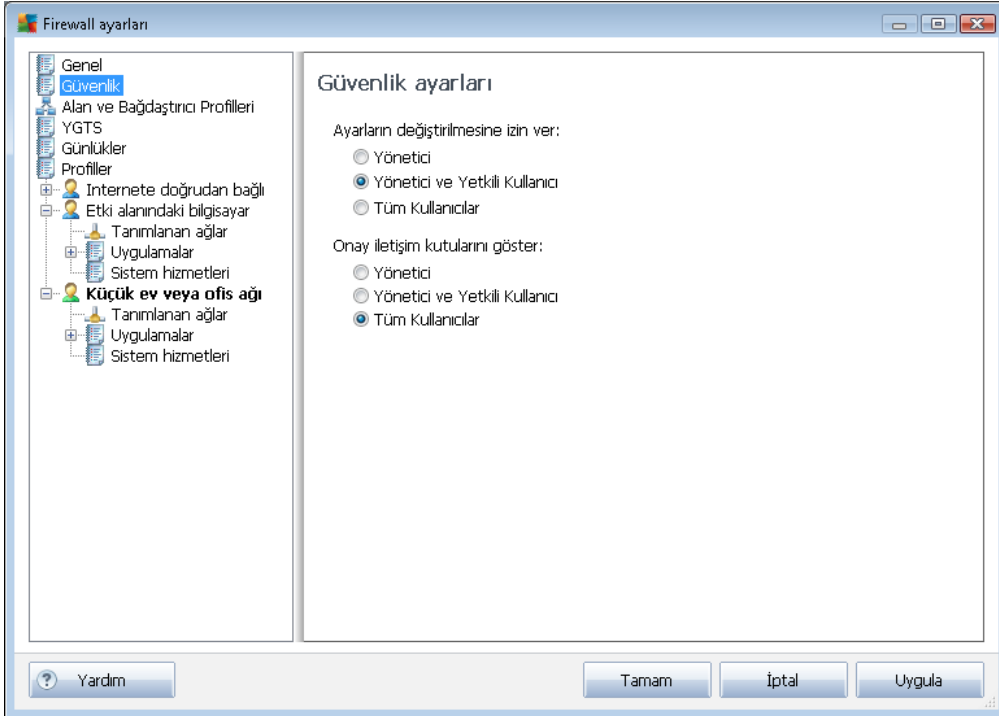
- **Acil durum modu (Tüm İnternet trafiğini engeller)** - bu seçeneği belirleyerek her ağ bağlantı noktasındaki trafiğin tümünü engellersiniz; [Güvenlik Duvarı](#) hala çalışır ancak tüm ağ trafiği durdurulur.
- **VPN'ye olan tüm trafiği etkinleştir (varsayılan olarak açık)** - VPN (Sanal Özel Ağ) bağlantısı kullanıyorsanız, (örn., evden ofise bağlanmak için) kutuyu işaretlemenizi öneririz. **AVG Firewall** otomatik olarak ağ bağdaştırıcılarınız arasında arama yapar, VPN bağlantısı için kullanılanları bulur ve hedef ağa bağlanmak için tüm uygulamalara izin verir (*yalnızca belirli Güvenlik Duvarı kuralı oluşturulmamış olan uygulamalar için geçerlidir*). Genel ağ bağdaştırıcıları olan standart bir sistemde bu basit adım sayesinde VPN'de kullanmanız gereken her uygulama için ayrıntılı bir kural oluşturmanıza gerek kalmaz.

Not: VPN bağlantısını tümüyle etkinleştirmek için, şu sistem protokolleriyle iletişim kurulmasına izin vermeniz gerekir: GRE, ESP, L2TP, PPTP. Bu işlem [Sistem hizmetleri iletişim kutusunda](#) yapılabilir.

Ayar yönetimi

Ayar Yönetimi bölümünde, [Güvenlik Duvarı](#) yapılandırmasını **Dışa** veya **İçe Aktarabilirsiniz**; örneğin tanımlanan [Güvenlik Duvarı](#) kurallarını ve ayarlarını yedekleme dosyalarına aktarabilir veya tüm yedekleme dosyalarını içe aktarabilirsiniz.

10.2. Güvenlik



Güvenlik Ayarları penceresinde seçilen profil önemli olmaksızın [Güvenlik Duvarı'nın](#) genel kurallarını tanımlayabilirsiniz.



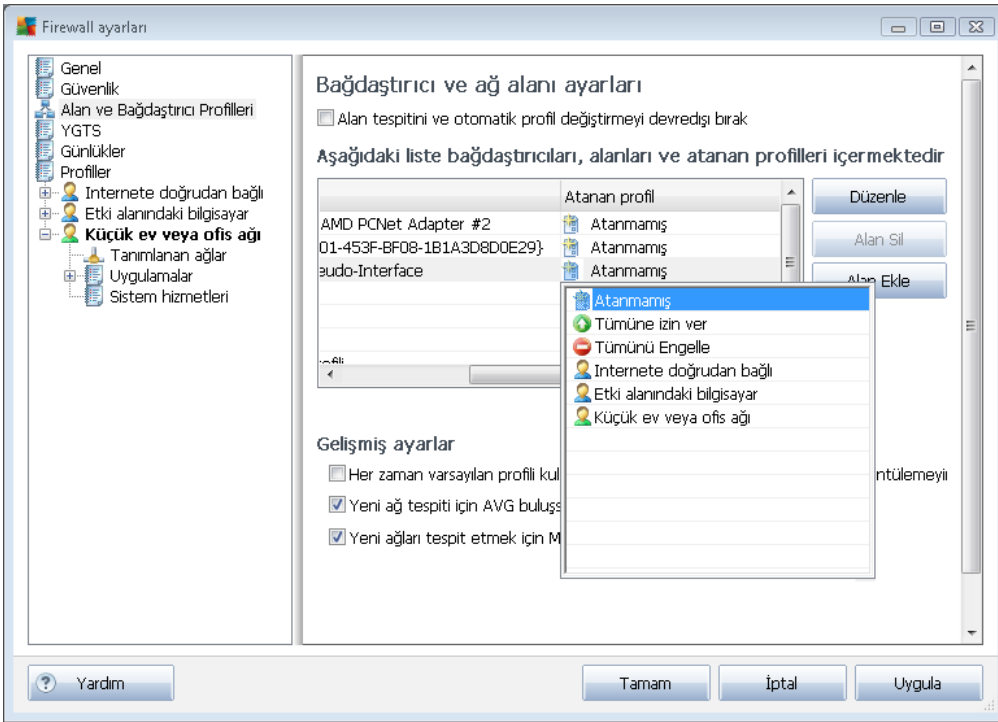
- 'a yeniden yapılandırma izni ver - [Güvenlik Duvarı](#) yapılandırmasını kimin değiştirebileceğini belirleyin
- için onay iletişim kutularını göster - onay iletişim kutusunun kim için görüntülenmesini istediğinizi belirtin (*öntanımlı [Güvenlik Duvarı](#) kuralları kapsamında bulunmayan durumlarda karar vermenizi isteyen pencereler*).

Her iki durumda da aşağıdaki kullanıcı gruplarından birine özel bir yetki verebilirsiniz:

- **Yönetici** - bilgisayarı tamamen kontrol eder ve kullanıcı gruplarına yetki verme hakkı bulunur.
- **Yönetici ve Kullanıcı** - yönetici, gruplara kullanıcı atayabilir (*Kullanıcı*) ve yeni grup üyelerinin yetkilerini tanımlar.
- **Tüm Kullanıcılar** - belirli bir gruba atanmayan diğer kullanıcılar.

10.3. Alanlar ve Bağdaştırıcıların Profilleri

Adaptörler ve ağ alanları ayarları iletişim kutularında ilgili ağlara atıfta bulunarak belirli adaptörlerin tanımlı profillerine ilişkin ayarları düzenleyebilirsiniz



- **Alan tespiti ve otomatik profil geçişini devre dışı bırak** (*varsayılan olarak kapalı*) - Tanımlanan profillerden biri, sırasıyla tek bir alana olmak üzere bir ağ arayüzü türüne atanabilir. Özel profiller tanımlamak istemiyorsanız, bir ortak profil kullanılacaktır. Ancak,



profilleri birbirinden ayırıp farklı adaptörlere ve alanlara atamaya karar verir ve daha sonra, herhangi bir nedenle söz konusu işlemi geçici olarak kapatmak isterseniz **Alan tespiti ve otomatik profil geçişini devre dışı bırak** seçeneğini işaretleyin.

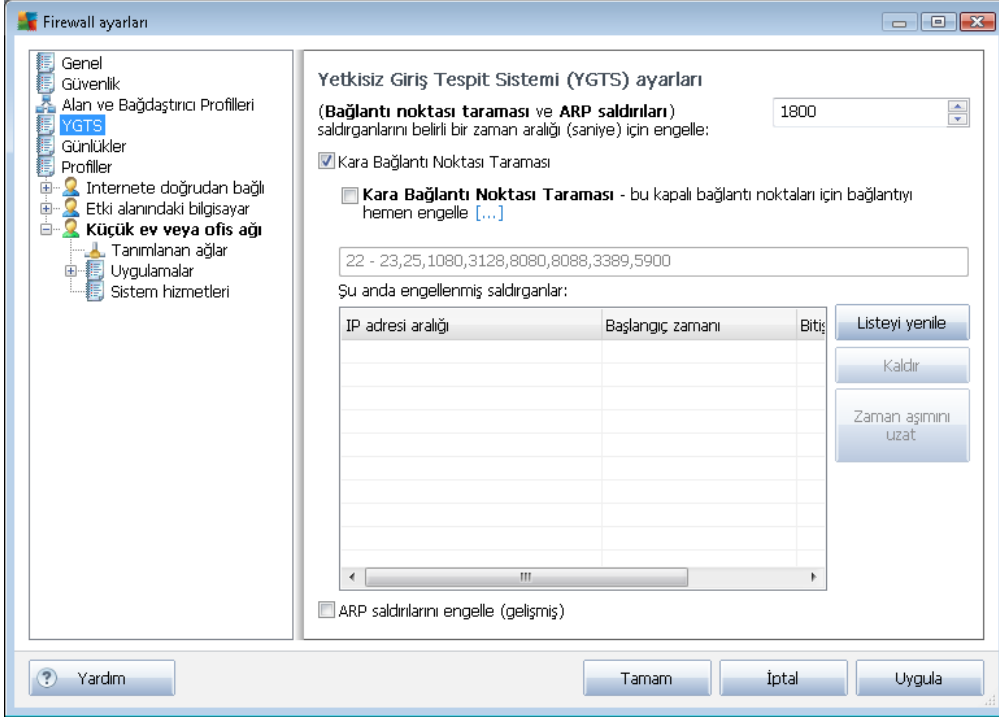
- **Adaptör, alan ve atanan profil listesi** - Bu listede tespit edilen adaptör ve alanlara ilişkin genel açıklamalar bulabilirsiniz Her birine, tanımlanan profiller menüsünden belirli bir profil atayabilirsiniz. Bu menüyü açmak için adaptör listesindeki ilgili öğeyi sol tıklatın (*Atanan profil sütununda*) ve bağlam menüsünden profili seçin.

Gelişmiş ayarlar

- **Her zaman varsayılan profili kullan ve yeni ağ tespiti iletişim kutusunu görüntüleme** - Bilgisayarınız yeni bir ağa her bağlandığında, [Güvenlik Duvarı](#) sizi uyarır ve ağ bağlantı türünü seçmenizi ve bunu bir [Güvenlik duvarı profili](#)'ne atamanızı isteyen bir iletişim kutusu görüntüler. Bu iletişim kutusunun görüntülenmesini istemiyorsanız, bu kutuyu işaretleyin.
- **Yeni ağ tespiti için AVG buluşsal yöntemlerini kullan** - Öğesi AVG'nin kendi mekanizması ile yeni tespit edilen bir ağ hakkında bilgi toplanmasına olanak sağlar (*ancak bu seçenek yalnızca VISTA OS ve üzeri sürümlerde kullanılabilir*).
- **Yeni ağ tespiti için Microsoft buluşsal yöntemlerini kullan** - Yeni ağla ilgili bilgileri Windows hizmetinden almaya olanak verir (*bu seçenek yalnızca Windows Vista ve üstünde kullanılabilir*).

10.4. IDS

Yetkisiz Giriş Algılama Sistemi, bilgisayarınızın belirli bağlantı noktaları üzerinden yapılan şüpheli iletişim girişimlerini tanımlamak ve engellemek için tasarlanan özel bir davranış analizi özelliğidir. IDS parametrelerini **Yetkisiz Giriş Tespit Sistemi (IDS) ayarları** iletişim kutusunda yapılandırabilirsiniz:



Yetkisiz Giriş Tespit Sistemi (IDS) ayarları iletişim kutusu şu yapılandırma seçeneklerini sunar:

- **Saldırganları (bağlantı noktası tarama ve ARP saldırıları) belirli bir zaman aralığı için engelle** - Burada bir bağlantı noktası üzerinde şüpheli bir iletişim girişimi tespit edildiğinde bağlantı noktasının kaç saniye engellenmesi gerektiğini ayarlayabilirsiniz. Varsayılan olarak, zaman aralığı 1800 saniyeye (30 dakikaya) ayarlıdır.
- **Bağlantı Noktası Taramasını Engelle (varsayılan olarak açık)**- Bilgisayara dışarıdan tüm TCP ve UDP bağlantı noktaları üzerinden yapılan iletişim girişimlerini engellemek için kutuyu işaretleyin. Bu tür herhangi bir bağlantı için, beş girişime izin verilir ve altıncısı engellenir. Öğe varsayılan olarak açıktır ve bu ayarların korunması önerilir. **Bağlantı Noktası Taramasını Engelle** seçeneğini açık tutarsanız, daha ayrıntılı yapılandırma seçenekleri de kullanılabilir (*aksi durumda aşağıdaki öğe devre dışı bırakılır*):
 - **Kara Bağlantı Noktası Taraması** - Aşağıdaki metin alanında belirtilen bağlantı noktaları üzerinden yapılacak herhangi bir iletişim girişimini hemen engellemek için kutuyu işaretleyin. Aynı bağlantı noktaları veya bağlantı noktası aralıkları virgüllerle ayrılmalıdır. Bu özelliği kullanmak isterseniz, önerilen bağlantı noktalarının yer aldığı önceden tanımlı bir liste bulabilirsiniz.
 - Şu anda engellenen saldırganlar - Bu bölümde, o anda [Güvenlik Duvarı](#) tarafından engellenmekte olan iletişim girişimlerinin listesi verilir. Engellenen girişimlerin eksiksiz geçmişi, [Günlükler](#) iletişim kutusundan görüntülenebilir (*Bağlantı noktası tarama günlükleri sekmesi*).
- **ARP saldırılarını engelle (gelişmiş) (varsayılan olarak kapalı)** - **IDS** tarafından potansiyel olarak tehlikeli şekilde tespit edilen yerel ağ içerisindeki özel türden iletişim girişimlerini engellemek için bu seçeneği işaretleyin. **Önceden tanımlı zaman aralığı için**

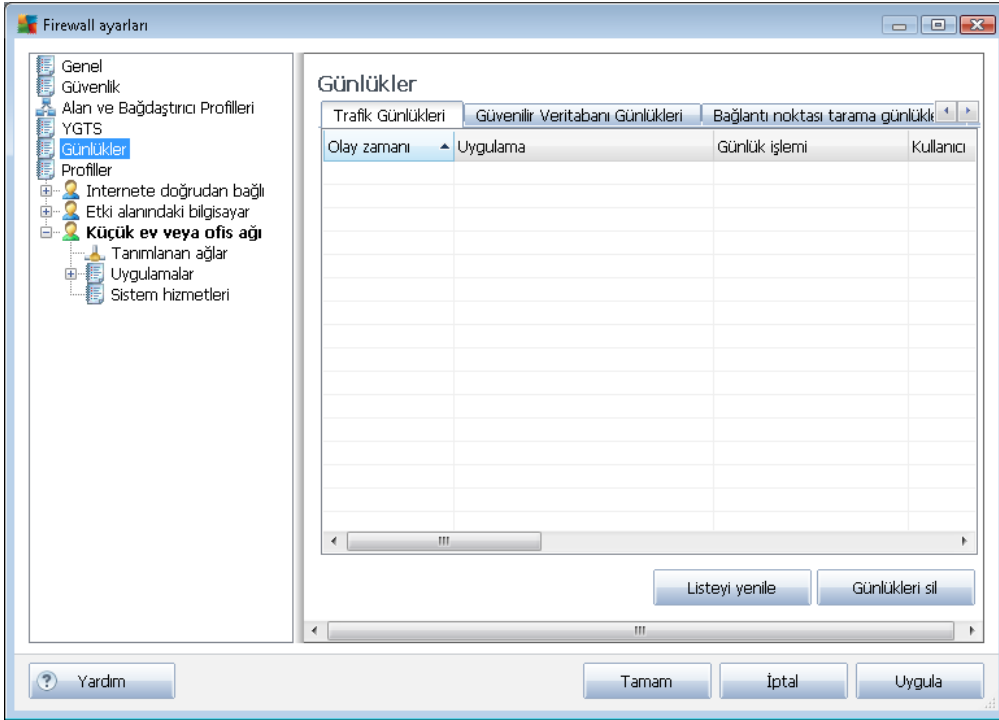


saldırıları engelle seçeneğinde ayarlanan zaman ayarı geçerli olur. Yalnızca yerel ağların türü ve risk düzeyi konusunda bilgi sahibi gelişmiş kullanıcıların bu özelliği kullanmasını öneririz.

Kontrol düğmeleri

- **Listeyi yenile** - (en son engellenen tüm girişimleri eklemek üzere)listeyi güncellemek için bu düğmeye basın.
- **Kaldır** - seçili engellemeyi iptal etmek için basın
- **Zaman aşımını uzat** - seçili girişimin engelleneceği zaman aralığını uzatmak için basın. Belirli saat ve tarih veya sınırsız zaman aralığı ayarlamanıza olanak veren genişletilmiş seçeneklere sahip yeni bir iletişim kutusu görüntülenir.

10.5. Günlükler



Günlükler iletişim kutusu günlüğe kaydedilen tüm [Güvenlik Duvarı](#) eylemlerinin ve olaylarının bir listesini ilgili parametrelerin ayrıntılı açıklamalarıyla dört sekmede incelemenize olanak verir (*olay saati, uygulama adı, ilgili günlük eylemi, kullanıcı adı, PID, trafik yönü, protokol türü, uzak ve yerel bağlantı noktalarının sayısı vb.*):

- **Trafik Günlükleri** - Ağa bağlanmak için denenen tüm uygulamaların etkinliği hakkında bilgi sunar.
- **Güvenilir Veritabanı Günlükleri** - Güvenilir veritabanı, her zaman çevrimiçi iletişime izin



verebilen sertifikalı ve güvenilir uygulamalar hakkında bilgi toplayan AVG dahili veritabanıdır. Yeni bir uygulama ağı ilk bağlanmaya çalışıldığında (örn. bu uygulama için henüz güvenlik duvarı kuralı belirtilmediğinde), ilgili uygulama için ağ iletişimine izin verilip verilmeyeceğini öğrenmek önemlidir. İlk önce, AVG Güvenilir veritabanını arar ve uygulama listelenmişse otomatik olarak ağa erişim izni verir. Ancak bundan sonra, veritabanında uygulama hakkında mevcut bilgi yoksa, uygulamanın ağa erişmesine izin vermek isteyip istemediğiniz tek bir iletişim kutusuyla size sorulur.

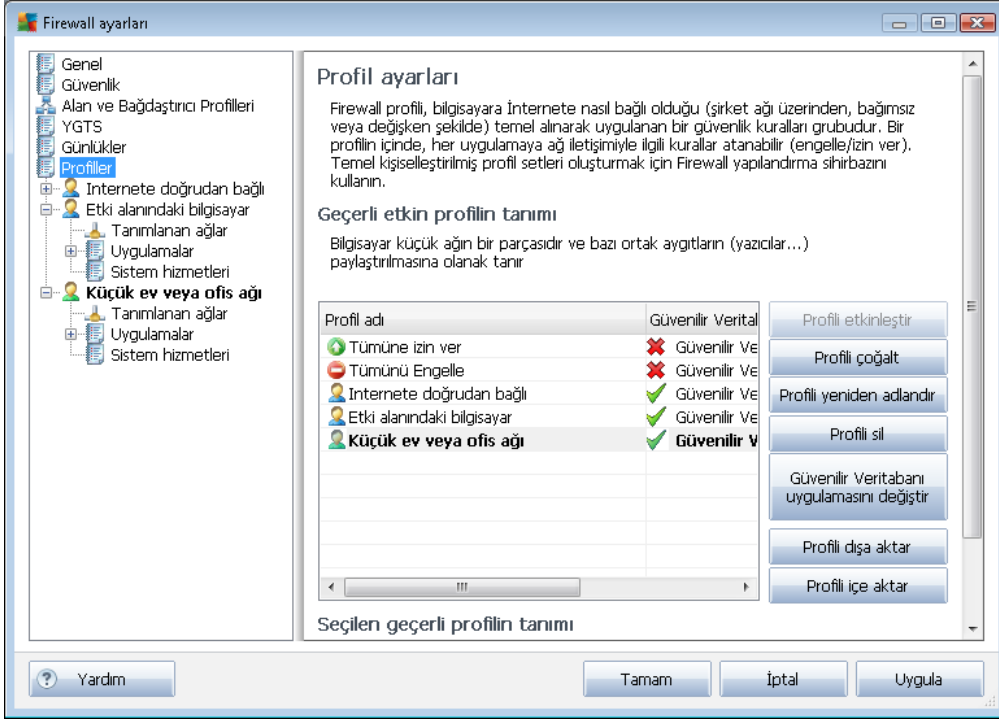
- **Bağlantı noktası tarama günlükleri** - tüm [Yetkisiz Giriş Tespit Sistemi](#) eylemleri ile ilgili kayıtları verir.
- **ARP günlükleri** - [Yetkisiz Giriş Tespit Sistemi](#) tarafından potansiyel olarak tehlikeli olarak tespit edilen yerel ağ içerisindeki özel türde iletişim girişimlerini engelleme ile ilgili günlük bilgileridir ([ARP saldırılarını engelle](#) seçeneği).

Kontrol düğmeleri

- **Listeyi yenile** - kaydedilen tüm parametreler seçilen davranış özelliklerine göre düzenlenebilir: kronolojik olarak (*tarihler*) ya da alfabetik olarak (*diğer sütunlarda*) - sadece ilgili sütun başlığını tıklatın. O anda görüntülenen bilgileri yenilemek için **Listeyi yenile** düğmesini kullanın.
- **Günlükleri sil** - Tablodaki tüm girişleri silmek için basın.

10.6. Profiller

Profil ayarları iletişim kutusunda mevcut profil listesini görebilirsiniz:



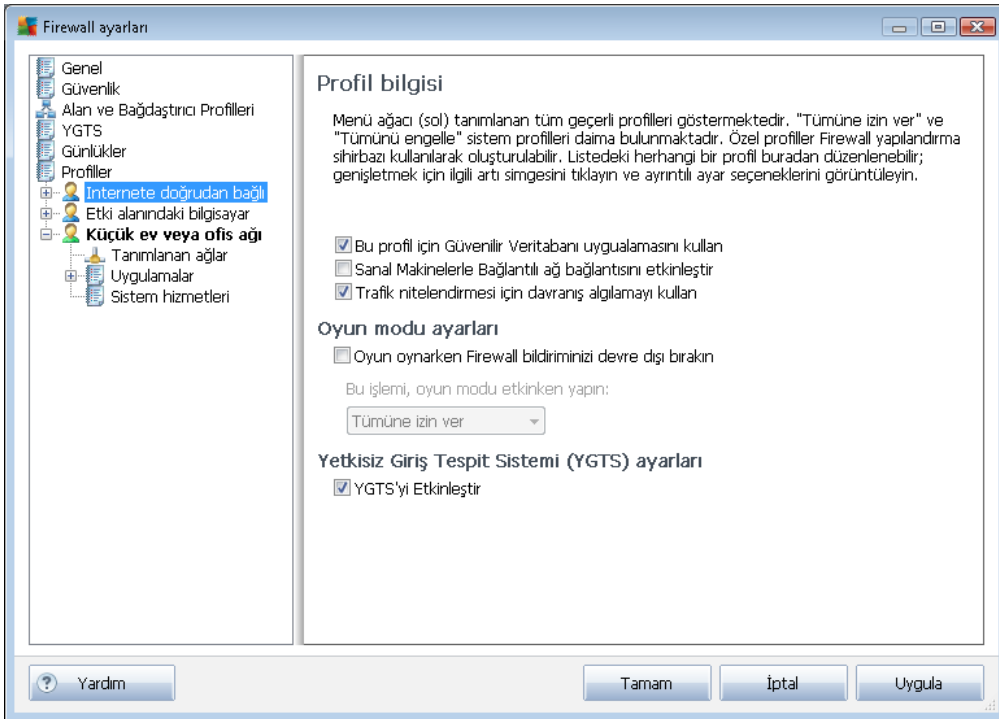
Sistem profilleri (*Tümüne izin ver*, *Tümünü engelle*) düzenlenemez. Ancak, tüm özel [profiller](#) (*İnternete doğrudan bağlı*, *Etki alanlı bilgisayar*, *Küçük ev veya ofis ağı*) aşağıdaki kontrol düğmeleri kullanılarak bu iletişim kutusundan düzenlenebilir:

- **Profil etkinleştir** - Bu düğme, seçilen profili etkin kılar ve seçilen söz konusu profil, [Güvenlik Duvarı](#) tarafından trafiği kontrol etmek üzere kullanılır.
- **Profil çoğalt** - Seçilen profilin bir kopyasını oluşturur, daha sonra söz konusu çoğaltılmış kopyanın ayarları üzerinde değişiklikler yaparak yeni bir profil oluşturabilirsiniz.
- **Profil yeniden adlandır** - Seçili profil için yeni bir ad tanımlamanıza olanak verir.
- **Profil sil** - Seçilen URL'yi listeden siler.
- **Güvenilir Veritabanına Geç** - Seçili profil için *Güvenilir Veritabanı* bilgilerini kullanmayı seçebilirsiniz (*Güvenilir Veritabanı AVG dahili veritabanıdır, her zaman çevrimiçi olarak iletişim kurmasına izin verilen güvenilir ve sertifikalı uygulamalardan veriler toplar.*).
- **Profil dışa aktar** - Daha sonra kullanılmak amacıyla profil konfigürasyonunu farklı bir dosyaya kaydeder.
- **Profil içe aktar** - Yedekleme amaçlı oluşturulmuş yapılandırma dosyasındaki verilere göre profil ayarlarını yapılandırır.

İletişim kutusunun alt kısmında mevcut durumda seçili profil hakkında bilgiler bulabilirsiniz.

Profil iletişim kutusundaki listede bulunan tanımlı profillerin sayısına göre solda bulunan dolaşım ağacının yapısı değişecektir. Tanımlı profillerin her biri **Profil** öğesi altında ayrı bir kol oluşturur. Profiller şu iletişim kutularında düzenlenebilir (*iletişim kutuları tüm profiller için aynıdır*):

10.6.1. Profil Bilgileri



Profil Bilgileri iletişim kutusu, profilin belirli parametrelerine ilişkin olarak profillerin her birinin konfigürasyonunu ayrı pencerelerde düzenleyebileceğiniz ilk bölümdür.

- **Bu profil için Güvenilir Veritabanı'nı kullan** - (varsayılan olarak açık) - *Güvenilir Veritabanı (yani, çevrimiçi iletişim kurmakta olan güvenilir ve sertifikalı uygulama ile ilgili bilgiler toplayan dahili AVG veritabanı) seçeneğini etkinleştirmek için bu seçeneği işaretleyin. İlgili uygulama için henüz bir kural belirtilmemişse, uygulamanın ağa erişmesine izin verilip verilmeyeceği bilinmelidir. AVG önce Güvenilir Veritabanını arar ve uygulama listelenirse, güvenilir olduğu düşünülür ve ağ üzerinden iletişime kurmasına izin verilir. Aksi halde, uygulamanın ağ üzerinden iletişime kurup kurmamasına karar vermeniz istenecektir) seçeneği işaretleyin*
- **Sanal Makine Köprülü ağını etkinleştir** - (varsayılan olarak kapalı) - *WMware'deki sanal makinelerin ağa doğrudan bağlanmasına izin vermek için bu öğeyi işaretleyin.*
- **Trafik nitelendirmesi için davranış algılamasını kullan** - (varsayılan olarak açık) - *Bu seçeneği [Güvenlik Duvarının](#) bir uygulamayı değerlendirirken [Kimlik Koruma](#) işlevini kullanması için işaretleyin - [Kimlik Koruma](#), uygulamanın şüpheli davranışlar gösterip göstermediğini veya güvenilir olup olmadığını gösterir ve çevrimiçi iletişime izin verilip verilmediğini söyleyebilir.*



Oyun modu ayarları

Oyun modu ayarları bölümünde ilgili öğeyi işaretleyerek [Güvenlik Duvarı](#) bilgileri mesajlarının bilgisayarınızda bir tam ekran uygulamanın çalıştırıldığı zamanlarda bile görüntülenmesini isteyip istemediğinize karar verebilir ve kararınızı onaylayabilirsiniz (*bunlar genellikle oyunlardır ancak tüm tam ekran uygulamalar, örneğin, PPT sunumları için geçerlidir*), zira bu bilgi mesajları bir şekilde rahatsız edici olabilir.

Oyun oynarken Güvenlik Duvarı bildirimlerini devre dışı bırak öğesini işaretlerseniz ilgili herhangi bir kural belirlenmemiş olup ağa bağlanmaya çalışan yeni uygulamalar hakkında gerçekleştirilecek eylemi seçmek üzere açılır menüye girin (*genellikle soru iletişim kutuları ile sonuçlanan uygulamalar*).

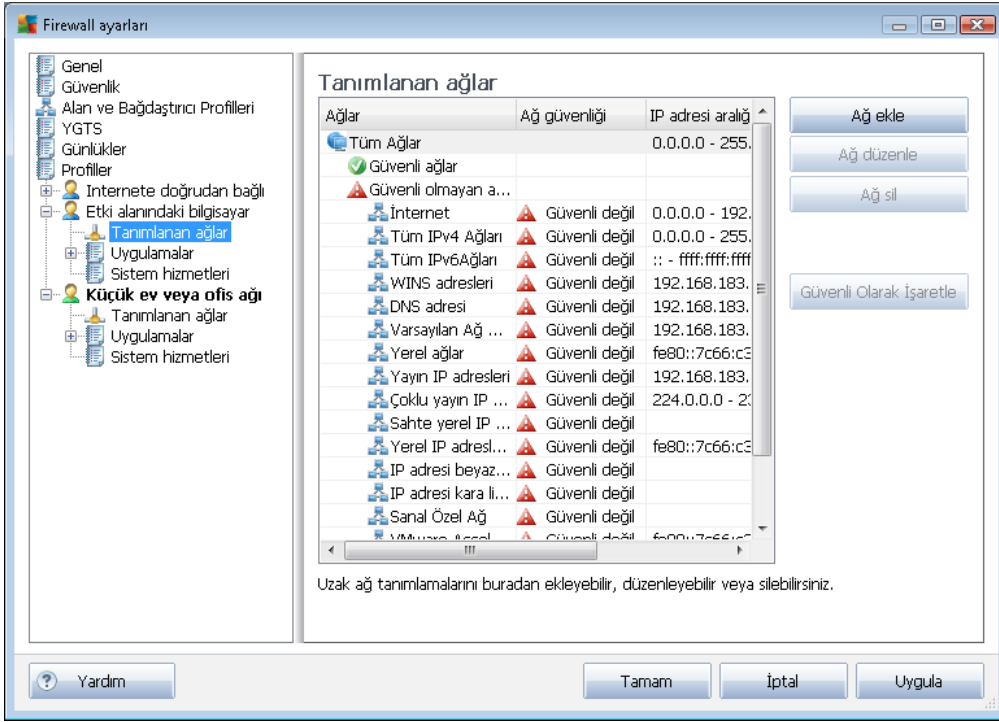
Oyun modu açıkken, programlanan tüm görevler (*taramalar, güncellemeler*) uygulama kapatılana kadar bekletilecektir.

Yetkisiz Giriş Tespit Sistemi (IDS) ayarları

Bilgisayarınızın belirli bağlantı noktaları üzerinden yapılan şüpheli iletişim girişimlerini tanımlamak ve engellemek üzere tasarlanmış özel davranış analizini etkinleştirmek için, **IDS'yi etkinleştir** onay kutusunu işaretleyin (*bu özelliğin ayarları hakkında ayrıntılı bilgi almak için, bu belgenin [IDS](#) bölümüne bakın*).

10.6.2. Tanımlanan Ağlar

Tanımlanan ağlar penceresinde, bilgisayarınızın bağlı olduğu ağlar görüntülenir.

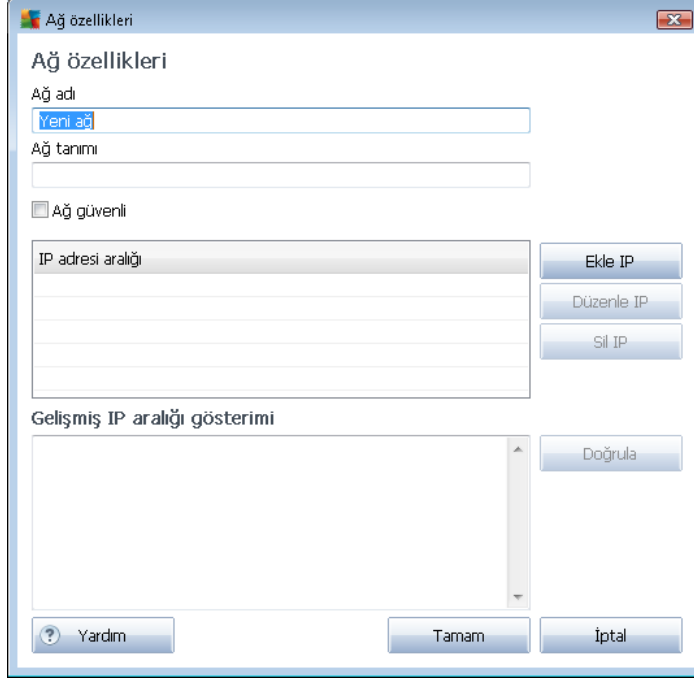


Liste algılanan her ağla ilgili aşağıdaki bilgileri sağlar:

- **Ağlar** - Bilgisayarın bağlı olduğu tüm ağların adlarını listeler.
- **Ağ güvenliği** - Varsayılan olarak, tüm ağlar güvenli değil olarak kabul edilir; yalnızca bir ağın güvenli olduğundan eminseniz, bu ağ güvenli olarak atayabilirsiniz (*ilgili ağa yönelik liste öğesini tıklayın ve içerik menüsünden Güvenli seçeneğini seçin*) - tüm güvenli ağlar, uygulamanın [Güvenli olana izin ver](#) olarak ayarlanan uygulama kuralı ile iletişim kurabileceği gruba eklenir.
- **IP adresi aralığı** - Her ağ aralığı otomatik olarak tespit edilir ve IP adresi aralığı formunda belirtilir.

Kontrol düğmeleri

- **Ağ ekle** - Yeni tanımladığınız ağın parametrelerini düzenleyebileceğiniz **Ağ özellikleri** penceresini açar:

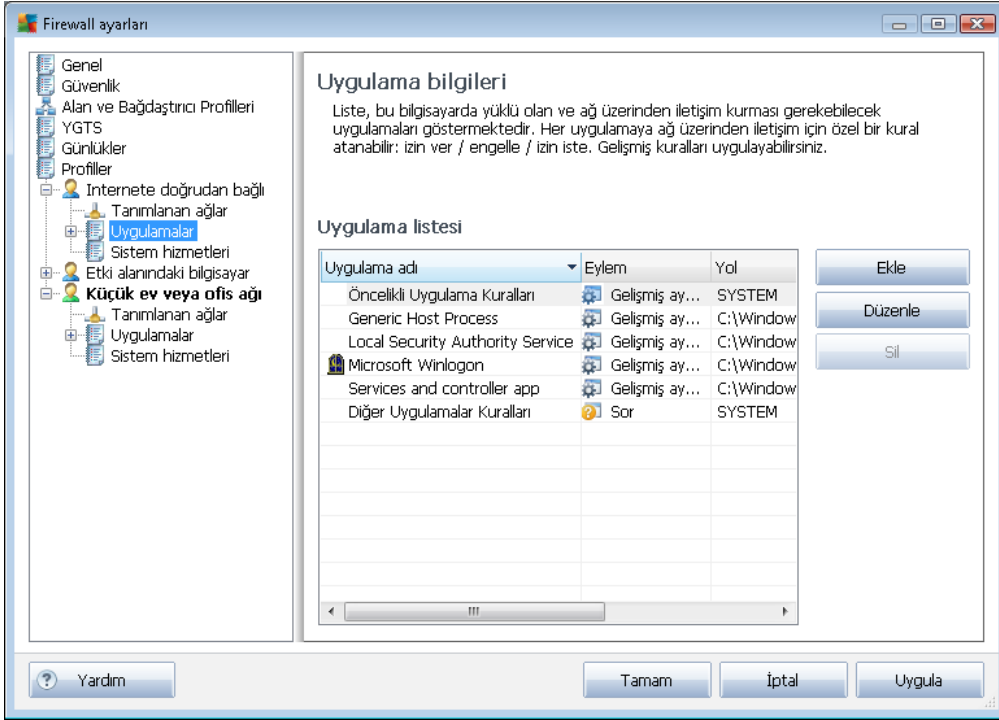


Bu pencerede **Ağ adını** belirleyebilir, **Ağ açıklaması** girebilir ve ağı güvenli ağlar listesine ekleyebilirsiniz. Yeni ağ, **IP ekle** düğmesi ile (ya da **IP Düzenle / IP Sil**) açılan bağımsız bir iletişim kutusundan manüel olarak tanımlanabilir; bu pencerede IP aralığını ya da maskesini sağlamak suretiyle ağı tanımlayabilirsiniz. Yeni oluşturulan bir ağın bölümleri olarak tanımlanması gereken çok sayıda için, **Gelişmiş IP aralığı gösterimi** seçeneğini kullanabilirsiniz: Tüm ağların listesini ilgili metin alanına (her standart biçim desteklenmektedir) girin ve biçimin tanıdığından emin olmak için **Doğrula** düğmesine basın. Ardından onaylamak ve verileri kaydetmek için **Tamam** tuşuna basın.






- **Ağı düzenle** - Mevcut durumda tanımlanmış ağın parametrelerini düzenleyebileceğiniz **Ağ özellikleri** iletişim kutusunu açar (*yukarı bakınız*) (*bu pencere ağ ekleme penceresi ile aynıdır, bir önceki paragrafta verilen açıklamaları okuyunuz*).
- **Ağı sil** - Seçilen ağ ile ilgili notları ağ listesinden siler.
- **Güvenli olarak işaretle** - Varsayılan olarak, tüm ağlar güvensiz olarak ele alınır ve yalnızca ilgili ağın güvenli olduğundan eminseniz, güvenli olarak atamak için bu düğmeyi kullanabilirsiniz (*ve tam tersi olarak ağ güvenli olarak atandığında, düğmenin metni "Güvenli değil olarak işaretle"ye değişir*).

10.6.3. Uygulamalar

Uygulama bilgileri iletişim kutusu, ağ üzerinden iletişim kurması gerekebilecek tüm yüklenmiş programları ve atanmış işlemin simgesini listeler:



Uygulama listesi'ndeki uygulamalar, bilgisayarınızda tespit edilenlerdir (ve atanmış ilgili işlemlerdir). Kullanılabilir işlem türleri:

-  - Tüm ağlar için iletişime izin ver
-  - Sadece Güvenli olarak tanımlanan ağlar için iletişime izin ver
-  - İletişimi engelle
-  - Soru iletişim kutusu görüntüle (uygulama, ağ üzerinden iletişim kurmaya çalışıldığında kullanıcı, izin verme veya engelleme konusunda karar verebilecektir)
-  - Gelişmiş ayarlar tanımlandı

Lütfen, yalnızca yüklenmiş olan uygulamanın tespit edilebileceğini unutmayın. Daha sonra yeni bir uygulama yüklemeniz durumunda, bu uygulama için Güvenlik Duvarı kurallarını tanımlamanız gerekeceğini unutmayın. Varsayılan olarak, yeni uygulama ağ üzerinden ilk defa bağlanmaya çalışıldığında, Güvenli Veritabanlarına göre Güvenlik Duvarı onun için otomatik olarak bir kural oluşturacak veya iletişime izin vermek mi yoksa engellemek mi istediğinizi soracaktır. İkinci durumda, yanıtınızı kalıcı bir kural (daha sonra bu iletişim kutusunda listelenecek) olarak kaydedebileceksiniz.

Elbette, yeni uygulama için hemen kural tanımlayabilirsiniz. Bu iletişim kutusunda, **Ekle**



seçeneğine basın ve uygulama bilgilerini girin.

Liste, uygulamaların dışında iki özel öge içerir:

- **Öncelikli Uygulama Kuralları** (listenin üst kısmında) tercihe bağlıdır ve her zaman tek bir uygulamanın kurallarından önce uygulanır.
- **Diğer Uygulama Kuralları** (listenin alt kısmında bulunur) örneğin bilinmeyene veya tanımlanmayan bir uygulama için özel uygulama kuralları uygulanmadığında "son örnek" olarak kullanılır.

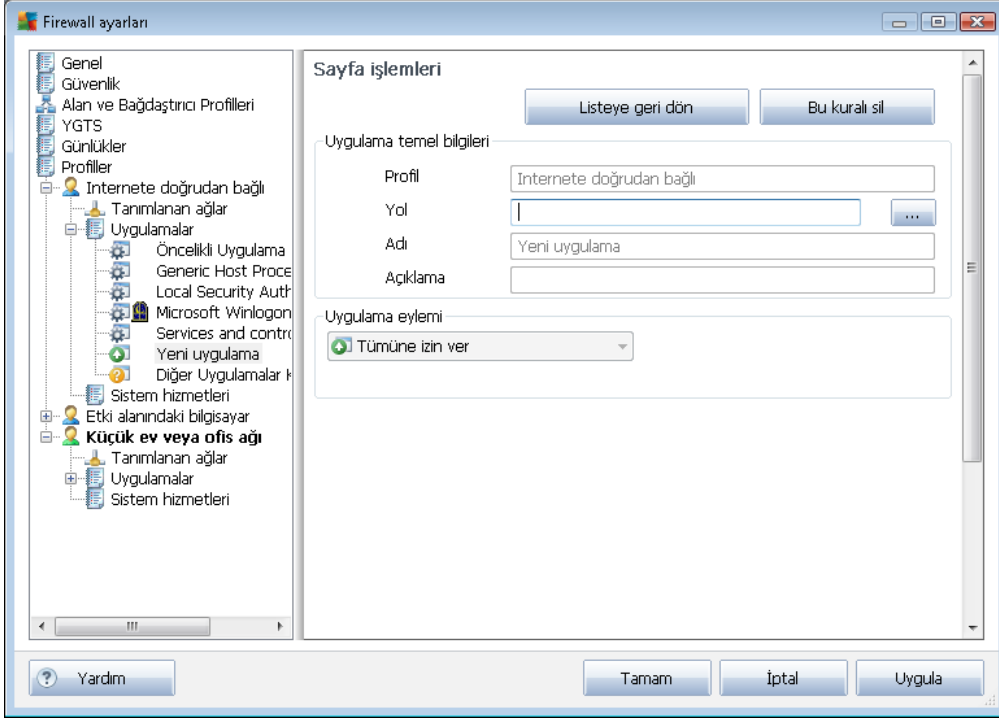
Bu öğelerin genel uygulamalardan farklı ayar seçenekleri bulunur ve bunlar yalnızca deneyimli kullanıcılara yöneliktir. Ayarları değiştirmemenizi önemle öneririz!

Kontrol düğmeleri

Liste, aşağıdaki denetim düğmeleri kullanılarak düzenlenebilir:

- **Ekle** - Yeni uygulama kurallarını tanımlamak için boş bir [Sayfa İşlemleri](#) iletişim kutusu açar.
- **Düzenle** - Mevcut bir uygulamanın kural kümesinin düzenlenmesi için sağlanan verilerle aynı [Sayfa İşlemleri](#) iletişim kutusu açar.
- **Sil** - Seçilen uygulamayı listeden siler.

Sayfa işlemleri iletişim kutusunda ilgili uygulamaya ilişkin ayarları ayrıntılı şekilde belirleyebilirsiniz:



Kontrol düğmeleri

İletişim kutusunun üstünde iki kontrol düğmesi mevcuttur:

- **Listeye dön** - Tanımlanan tüm uygulama kurallarının genel bir görünümünü görüntülemek için düğmeye basın.
- **Bu kuralı sil** - Görüntülenmekte olan uygulama kuralını silmek için düğmeye basın. **Bu eylemi geri alamayacağınızı lütfen unutmayın!**

Uygulama temel bilgileri

Bu bölümde, uygulama **Adını** ve isteğe bağlı olarak bir **Açıklama** girin (*bilgiyle ilgili kısa bir yorum*). **Yol** alanına, uygulamanın (*çalıştırılabilir dosya*) diskteki tam yolunu girin; alternatif olarak, uygulamayı "..." düğmesine bastıktan sonra ağaç menü yapısında kolaylıkla bulabilirsiniz.

Uygulama işlemi

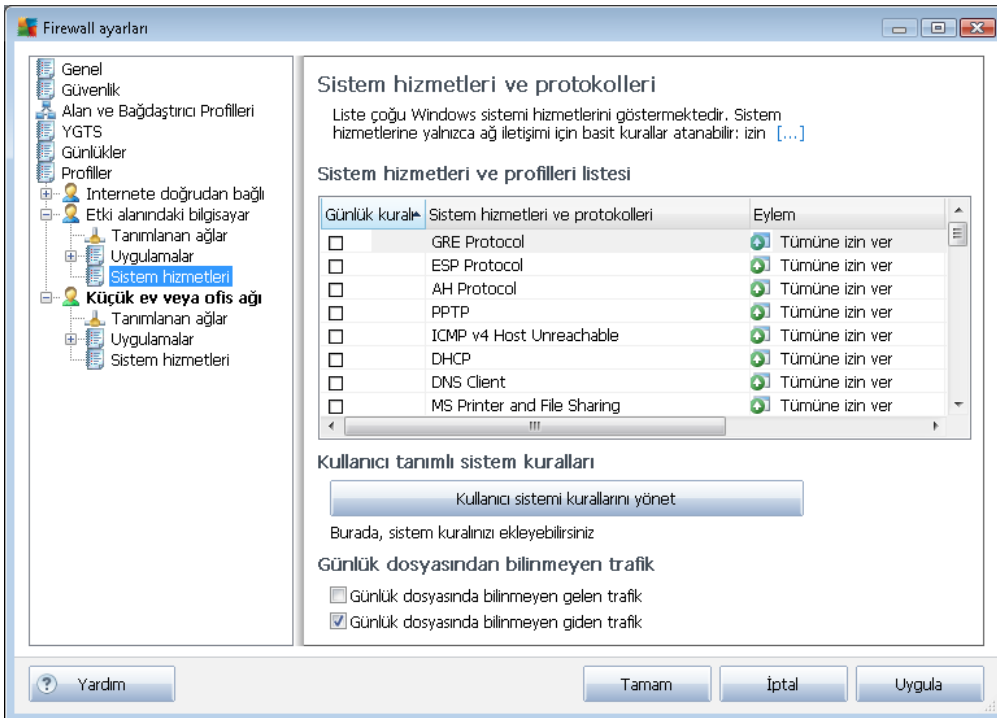
Aşağı açılır menüden söz konusu uygulama için [Güvenlik Duvarı](#) kuralını seçebilirsiniz (yani, uygulama ağ üzerinden iletişim kurmayı denediğinde [Güvenlik Duvarı](#)'nın ne yapacağı gibi):

- **Tümüne izin ver** - Uygulamanın, sınırlama olmaksızın tanımlanan tüm ağlar ve adaptörler üzerinden iletişim kurmasına izin verir.
- **Güvenli olana izin ver** - Uygulamanın yalnızca güvenli (*güvenilir*) olarak tanımlanan ağlar üzerinden iletişim kurmasına izin verir.
- **Engelle** - Otomatik olarak iletişimi yasaklar; uygulamanın herhangi bir ağa bağlanmasına izin verilmez.
- **Sor** - O andaki iletişim girişimine izin vermek veya engel olmak istediğinizi belirtebileceğiniz bir iletişim kutusu görüntüler.
- **Gelişmiş ayarlar - Uygulama ayrıntısı kuralları** kısmında, iletişim kutusunun alt tarafında daha kapsamlı ve ayrıntılı ayar seçenekleri görüntüler. Ayrıntılar liste sırasına göre uygulanır; bu yüzden önceliklerini ayarlamak için listedeki kuralları **Yukarı taşıyabilir** veya **Aşağı taşıyabilirsiniz**. Listedeki belirli bir kurala tıkladıktan sonra, iletişim kutusunun alt kısmında kural ayrıntıları değerlendirilmesi görüntülenir. Altı çizili mavi her değer ilgili ayarlar iletişim kutusunda tıklatılarak değiştirilebilir. Vurgulu kuralı silmek için, **Kaldır** ögesine basın. Yeni kural tanımlamak için, gerekli tüm ayrıntıları belirlemenizi sağlayan **Kural ayrıntısı değiştir** iletişim kutusunu açmak üzere **Ekle** düğmesini kullanın.

10.6.4. Sistem Hizmetleri

Sistem hizmetleri ve protokolleri iletişim kutusu içinde yapılacak tüm düzeltmeler YALNIZCA DENEYİMLİ KULLANICILAR içindir!

Sistem hizmetleri ve protokolleri iletişim kutusu, ağ üzerinden iletişim kurulması gerekebilecek Windows standart sistem hizmetlerini ve protokollerini listeler:





Sistem hizmetleri ve protokolleri listesi

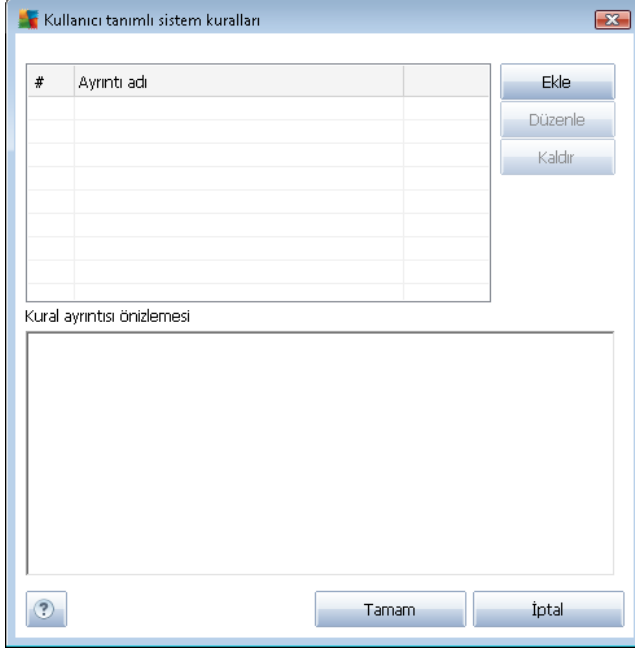
Grafik aşağıdaki sütunları içerir:

- **Kural eylemini günlüğe al** - Bu kutu, [günlükler](#) içindeki her kural uygulamasını kaydetme seçeneğini açmanızı sağlar.
- **Sistem hizmeti ve protokolleri** - Bu sütun ilgili sistem hizmetinin adını gösterir.
- **Eylem** - Bu sütun atanan eylemin simgesini görüntüler:
 - Tüm ağlar için iletişime izin ver
 - Sadece Güvenli olarak tanımlanan ağlar için iletişime izin ver
 - İletişimi engelle
- **Ağlar** - Bu sütun sistem kuralının hangi belirli ağda geçerli olduğunu bildirir.

Listedeki öğelerin ayarlarını düzenlemek için (*atanan eylemler de dahil* olmak üzere), öğeyi sağ tıklayın ve **Düzenle**'yi seçin. **Ancak, sistem kurallarının düzenlenmesi yalnızca gelişmiş kullanıcılar tarafından yapılmalıdır ve sistem kurallarını düzenlememeniz önemle önerilir!**

Kullanıcı tanımlı sistem kuralları

Kendi sistem hizmeti kuralınızı tanımlamak üzere yeni bir iletişim kutusu açmak için (*aşağıdaki resme bakın*), **Kullanıcı sistemi kurallarını yönet** düğmesine basın. **Kullanıcı tanımlı sistem kuralları** iletişim kutusunun en üst kısmında geçerli olarak düzenlenen sistem kuralının tüm ayrıntılarına genel bakış görüntülenir, alt kısımda seçili ayrıntı görüntülenir. Kullanıcı tanımlı kural ayrıntıları ilgili düğmeyle düzenlenebilir, eklenebilir veya silinebilir. Üreticinin tanımladığı kural ayrıntıları yalnızca düzenlenebilir:



Kural ayrıntısı ayarlarının gelişmiş ayarlar olduğunu ve Güvenlik Duvarı yapılandırması üzerinde tam denetime sahip olması gereken ağ yöneticilerine yönelik tasarlandığını lütfen unutmayın. İletişim protokolleri türleri, ağ bağlantı noktası numaraları, IP adresi tanımları vb. hakkında bilginiz yoksa, lütfen bu ayarları değiştirmeyin! Yapılandırmayı gerçekten değiştirmeniz gerekiyorsa, belirli ayrıntılar için lütfen ilgili iletişim kutusunun yardım dosyalarına başvurun.

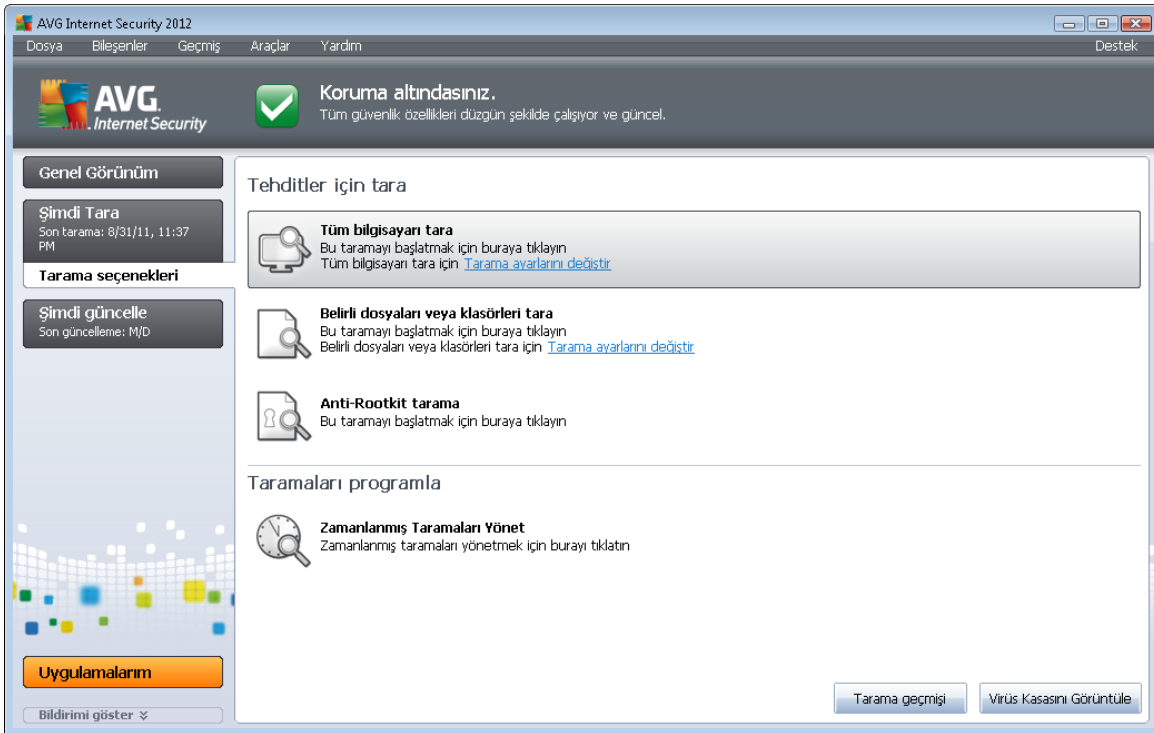
Günlük dosyasından bilinmeyen trafik

- **Bilinmeyen gelen trafiği kaydet** (varsayılan olarak kapalı) - Dışarıdan bilgisayara yapılan her bilinmeyen bağlantı girişimini [Günlüklere](#) kaydetmek için bu kutuyu işaretleyin.
- **Bilinmeyen giden trafiğini kaydet** (varsayılan olarak açık) - Bilgisayarın dışarıdaki bir konuma bağlanmak için yaptığı bilinmeyen her girişimi [Günlüklere](#) kaydetmek için bu kutuyu işaretleyin.

11. AVG Tarama

Varsayılan olarak, **AVG Internet Security 2012** ilk taramadan sonra olduğu gibi hiçbir taramayı çalıştırmaz, her zaman korumada olan **AVG Internet Security 2012** ürününün yerleşik bileşenleri ile mükemmel olarak korunuyor olmanız ve hiçbir kötü amaçlı yazılımın bilgisayarınıza hiçbir surette girmesine izin vermemeniz gerekir. Elbette belirli aralıklarda çalıştırılacak bir [tarama planlayabilir](#) veya bir taramayı gereksinimlerinize göre manuel olarak başlatabilirsiniz.

11.1. Tarama Arayüzü



AVG tarama arayüzüne [Tarama seçenekleri hızlı bağlantısı](#) aracılığıyla erişilebilir. **Tehditleri tara** iletişim kutusuna geçmek için bu bağlantıyı tıklayın. Bu iletişim kutusunda aşağıdakiler bulunmaktadır:

- [öntanımlı taramalara](#) genel bakış - yazılım satıcısı tarafından tanımlanan üç tarama türü isteğe bağlı olarak hemen veya programlı olarak kullanılmaya hazırdır:
 - [Tüm bilgisayarın taranması](#)
 - [Belirli dosyaları veya klasörleri tara](#)
 - [Rootkit Önleme tarama](#)
- [tarama programlama](#) bölümü - İhtiyacınız doğrultusunda yeni programlar oluşturabilir ya da yeni taramalar tanımlayabilirsiniz.



Kontrol düğmeleri

Tarama arayüzünde bulunan genel kontrol düğmeleri şunlardır:

- **Tarama geçmişi** - tüm tarama geçmişi ile birlikte [Tarama sonuçlarına genel bakış](#) iletişim kutusunu açar
- **Virüs Kasasını Görüntüle** - tespit edilen bulaşmaların karantina altına alındığı [Virüs Kasasını](#) yeni bir pencerede açar.

11.2. Öntanımlı Taramalar

AVG Internet Security 2012 programının ana özelliklerinden biri istek üzerine taramadır. İsteğe bağlı taramalar, muhtemel bir virüs hakkında şüpheye düştüğünüz an bilgisayarınızın istediğiniz kısmında istediğiniz zaman yapabileceğiniz taramalardır. Kısacası, bilgisayarınızda virüs olduğunu düşünmeseniz bile söz konusu taramaların düzenli aralıklarla yapılması önerilmektedir.

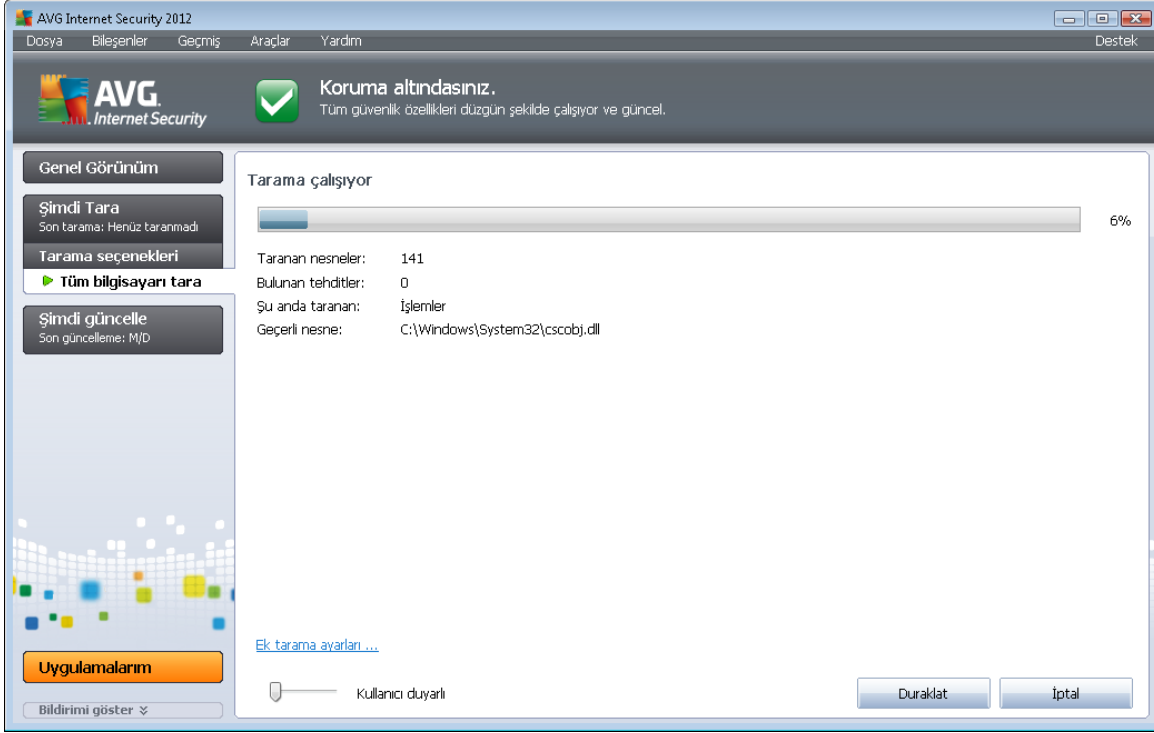
AVG Internet Security 2012 içinde, yazılım satıcısının önceden tanımladığı aşağıdaki tarama türlerini bulacaksınız:

11.2.1. Tüm Bilgisayarın Taranması

Tüm Bilgisayarın taranması - tüm bilgisayarı muhtemel bulaşmalara ve/veya potansiyel olarak istenmeyen programlara karşı tarar. Bu tarama, bilgisayarınızın tüm sabit disklerini tarayacak, virüsleri tespit edecek ve temizleyecek ya da tespit edilen bulaşmayı [Virüs Kasasına](#) taşıyacaktır. Bilgisayarın tümü haftada en az bir defa taranmalıdır.

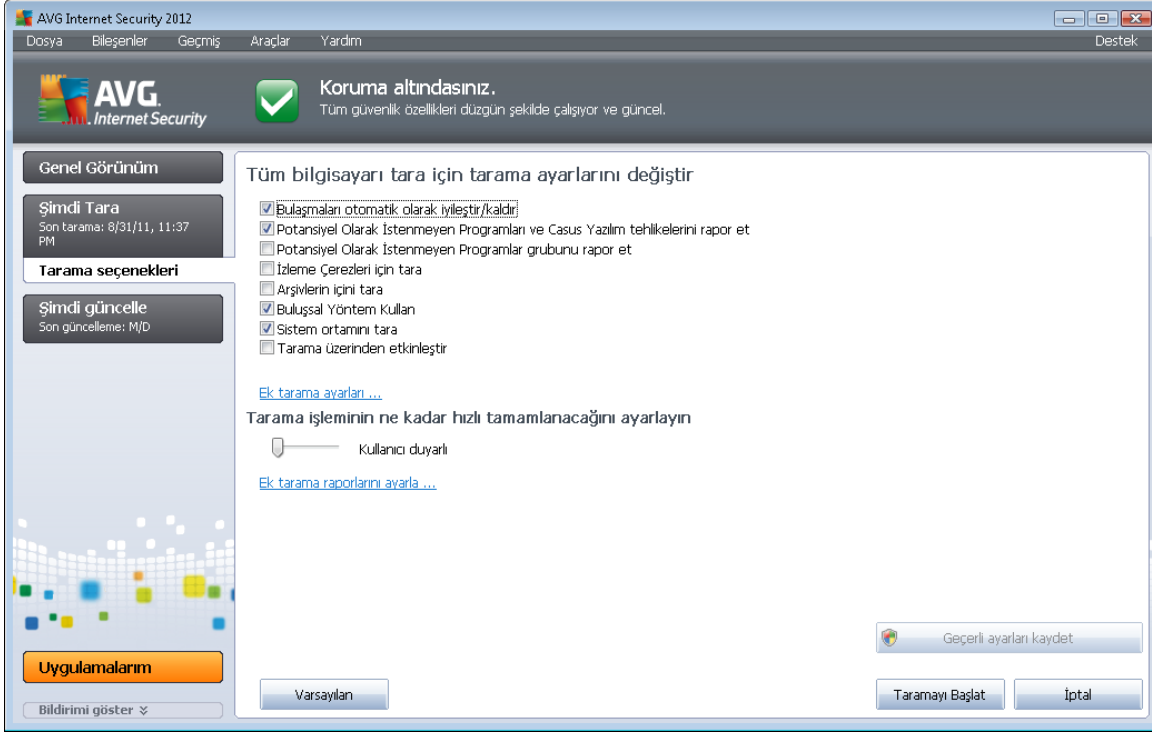
Tarama başlatma

Tüm bilgisayarın taranması, taramanın simgesi tıklatılarak doğrudan [tarama arayüzünden](#) başlatılabilir. Bu tarama türü için başka belirli ayarlamaların yapılmasına gerek yoktur, tarama **Tarama yapılıyor** iletişim kutusunda anında başlayacaktır (*bkz. ekran görüntüsü*). Tarama işlemi gerekirse geçici olarak kesilebilir (**Duraklat**) ya da iptal edilebilir (**Durdur**).



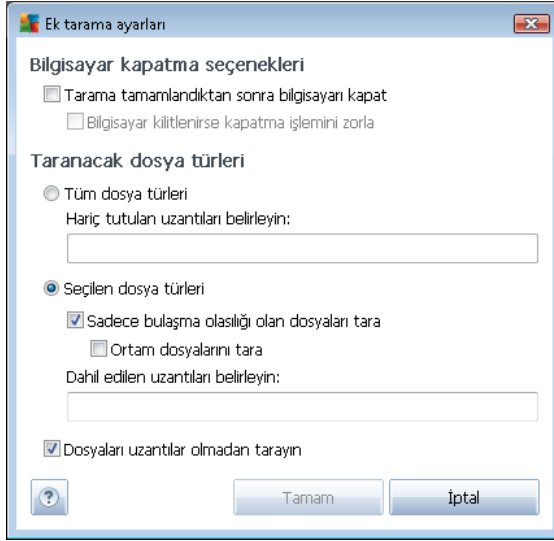
Tarama yapılandırması düzenleme

Tüm bilgisayarın taranması işlevinin önceden tanımlı varsayılan ayarlarını düzenleme seçeneğiniz vardır. **Tüm bilgisayarın taranması için tarama ayarlarını değiştir** iletişim kutusunu açmak için **Tarama ayarlarını değiştir** bağlantısına basın (**Tüm bilgisayarın taranması** işlevinin **Tarama ayarlarını değiştir** seçeneği ile **tarama arayüzünden** erişilebilir. **Geçerli bir nedeniniz olmadığı müddetçe varsayılan ayarları değiştirmek için bu ayarları korumanız önerilir!**



- **Tarama parametreleri** - tarama parametreleri listesindeki belirli parametreleri gereksinimleriniz doğrultusunda açıp kapatabilirsiniz.
 - **Bulaşmayı otomatik temizle/sil** - (varsayılan olarak açıktır). Tarama işlemi sırasında bir virüs tanımlanırsa ve temizlenmesi mümkünse otomatik olarak temizlenir. Bulaşmış dosya otomatik olarak temizlenemezse, bulaşmış nesne [Virüs Kasası](#)'na taşınır.
 - **Potansiyel Olarak İstenmeyen Programları ve Casus Yazılım tehditlerini rapor et** (varsayılanda açıktır) - [Anti-Spyware](#) motorunu etkinleştirmek ve virüslerin yanı sıra casus yazılımları da taramak için işaretleyin. Casus yazılım, şüpheli kötü amaçlı yazılım kategorisini ifade eder: genellikle bir güvenlik riskini oluşturmasına rağmen bu programlardan bazıları bilerek yüklenebilir. Bilgisayarınızın güvenliğini artırdığından, bu özelliği etkin durumda tutmanızı öneriyoruz.
 - **Potansiyel Olarak İstenmeyen Programlar gelişmiş grubunu rapor et** (varsayılanda kapalıdır) - bu parametre casus yazılımların, yani doğrudan üreticiden alınan tamamen zararsız olan, ancak daha sonra kötüye kullanılacak programların genişletilmiş paketinin tespit edilmesi için işaretleyin. Bu, bilgisayar güvenliğinizi daha da artıran ek bir önlemdir, ancak yasal programları da engelleyebilir ve bu yüzden varsayılan olarak kapalıdır.
 - **İzleme Tanımlama Bilgilerini Tara** (varsayılan olarak kapalıdır): [Anti-Spyware](#) bileşeninin bu parametresi, tarama sırasında tespit edilmesi istenen tanımlama bilgilerini tanımlar (*HTTP tanımlama bilgileri kimlik doğrulaması, izleme ve kullanıcılar hakkındaki site tercihleri veya elektronik alışveriş sepetlerinin içeriği gibi belirli bilgilerin korunması için kullanılır*).

- **Arşivleri tara** (varsayılan olarak kapalıdır) - bu parametre, ZIP, RAR vb. arşiv dosyalarının içinde sıkıştırılmış dosyaların bile taranmasını sağlar.
 - **Buluşsal Analiz Yöntemlerini Kullan** (varsayılan olarak açıktır) - buluşsal analiz yöntemi (taranan nesnenin komutlarının sanal bir bilgisayar ortamında dinamik olarak canlandırılması) tarama sırasında kullanılacak virüs tespiti yöntemlerinden biridir.
 - **Sistem ortamını tara** (varsayılan olarak açıktır) - tarama işlemi, bilgisayarınızın sistem alanlarını da kontrol edecektir.
 - **Kapsamlı taramayı etkinleştir** (varsayılanda kapalıdır) - belirli durumlarda (bilgisayarınıza bulaşma olmasından şüpheleniliyorsa) yalnızca emin olmak üzere bilgisayarınızın bulaşma olması çok zor olan alanlarını bile tarayan en kapsamlı tarama algoritmalarını etkinleştirmek için bu seçeneği işaretleyebilirsiniz. Ancak, bu yöntemin çok fazla zaman aldığını unutmayın.
- **Ek tarama ayarları** - Bağlantı, şu parametreleri belirtebileceğiniz yeni bir **Ek tarama ayarları** iletişim kutusu açar:

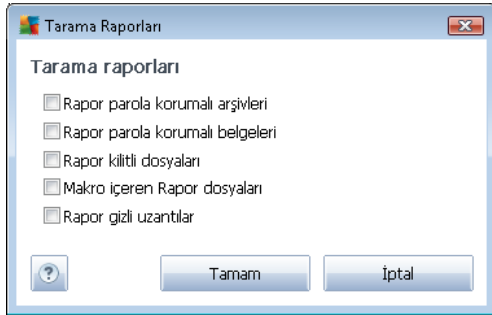


- **Bilgisayar kapatma seçenekleri** - Çalışan tarama işlemi bittiğinde bilgisayarın otomatik olarak kapatılması gerekip gerekmediğine karar verir. Bu seçeneği seçerseniz (**Tarama bittikten sonra bilgisayarı kapat**) bilgisayar mevcut durumda kilitli olsa bile bilgisayarın kapatılmasını sağlayan bir seçeneğin bulunduğu bir pencere açılacaktır (**Bilgisayar kilitliyse bilgisayarı kapanmaya zorla**).
- **Tarama için dosya türleri** - Nelerin taranmasını istediğinize de karar vermelisiniz:
 - **Tüm dosya türleri** taranmaması gereken virgülle ayrılmış dosya uzantılarının listesini sağlayarak taramada istisnaları tanımlama seçeneğiyle;
 - **Seçili dosya türleri** - Yalnızca virüs bulaşabilme olasılığı olan dosyaları taramayı istediğinizi belirtebilirsiniz (*virüs bulaşmayan dosyalar taranmayacaktır, örneğin,*

bazı düz metin dosyaları veya bazı diğer çalıştırılmayan dosyalar); ortam dosyaları (video, ses dosyaları - bu onay kutusunun işaretini kaldırırsanız, bu dosyalar genellikle çok büyük olduğundan ve virüs bulaşma olasılıkları çok az olduğundan tarama süresini daha da azaltır). Tekrar, her zaman taranması gereken dosyaları uzantılarına göre belirtebilirsiniz.

➤ İsteğe bağlı olarak, **Uzantıları olmayan dosyaları taramaya** da karar verebilirsiniz ve bu seçenek varsayılan olarak açıktır ve gerçekten bir nedeniniz yoksa değiştirmemeniz önerilir. Uzantısı olmayan dosyalar şüpheli olabilir ve her zaman taranmalıdır.

- **Taramanın ne kadar hızlı tamamlanacağını ayarlayın** - tarama sürecinin önceliğini değiştirmek için kaydırma çubuğunu kullanabilirsiniz. Bu seçenek varsayılan olarak otomatik kaynak kullanımının *kullanıcıya duyarlı* düzeyine ayarlanmıştır. Alternatif olarak, sistem kaynakları kullanımını minimize etmek için tarama işlemini yavaşlatabilir (*bilgisayarda çalışmanız gerektiği ancak taramanın ne kadar sürdüğünü önemsemediğiniz durumlar için uygundur*) veya sistem kaynaklarını daha yoğun kullanmak suretiyle daha hızlı bir şekilde (ör., *bilgisayar geçici bir süreyle kullanılmadığında*) çalıştırabilirsiniz.
- **Tarama raporu oluştur** - bağlantı üzerinden **Tarama Raporları** isimli bir iletişim kutusu açılır ve buradan ne tip buluntuların rapor edileceğini seçebilirsiniz:



Uyarı: Bu tarama parametreleri, yeni tanımlanan taramanın parametreleri ile aynıdır - [AVG Taraması / Tarama Planlama/ Tarama Tipi](#) bölümünde açıklandığı doğrultuda. **Tüm bilgisayarı tara** fonksiyonunun varsayılan yapılandırmasını değiştirmeye karar verirsiniz yeni ayarlarınızı, belirli dosya ya da klasörlerin taranması için kullanılacak varsayılan yapılandırma olarak atayabilirsiniz.

11.2.2. Belirli Dosyaları veya Klasörleri Tara

Belirli dosyaları veya klasörleri tara - bilgisayarınızın sadece taranması için seçtiğiniz alanlarını tarar (seçilen klasörler, sabit diskler, disket sürücüler, CD'ler vb.). Virüs tespiti ve temizlenmesi sırasında tarama işlemi, tüm bilgisayar taraması ile aynıdır. Bulunan virüsler temizlenir ya da [Virüs Kasası](#)'na taşınır. Belirli dosyaları veya klasörleri tara işlevi, kendi testlerinizi ve gereksinimlerinize bağlı olarak bunların programlamasını ayarlamak için kullanılabilir.

Tarama başlatma

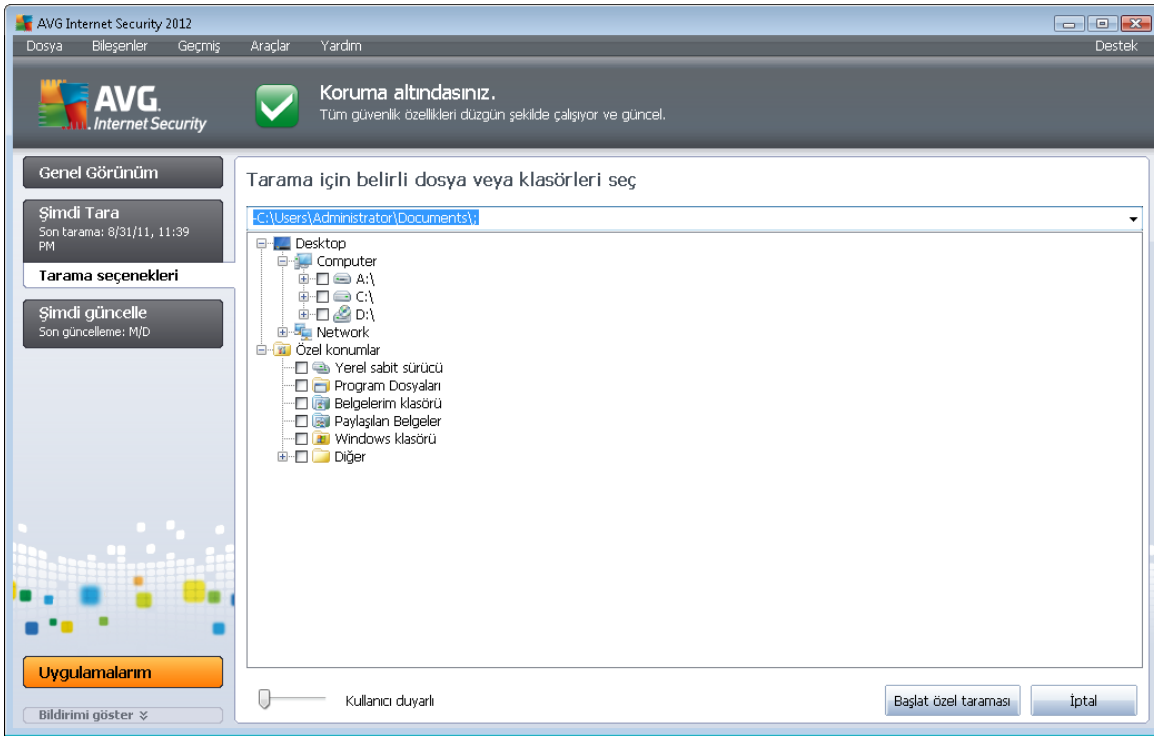
Belirli dosya ve klasörleri tara işlevi, tarama simgesi tıklanarak doğrudan [tarama arayüzünden](#) başlatılabilir. Yeni bir **Taramak için belirli dosya ve klasörleri seçin** iletişim kutusu açılır.



Bilgisayarınızın ağaç görünümünden taranmasını istediğiniz klasörleri seçin. Seçilen klasörlerin her birine giden yol, otomatik olarak oluşturulacak ve iletişim kutusunun üst kısmındaki metin alanında görüntülenecektir.

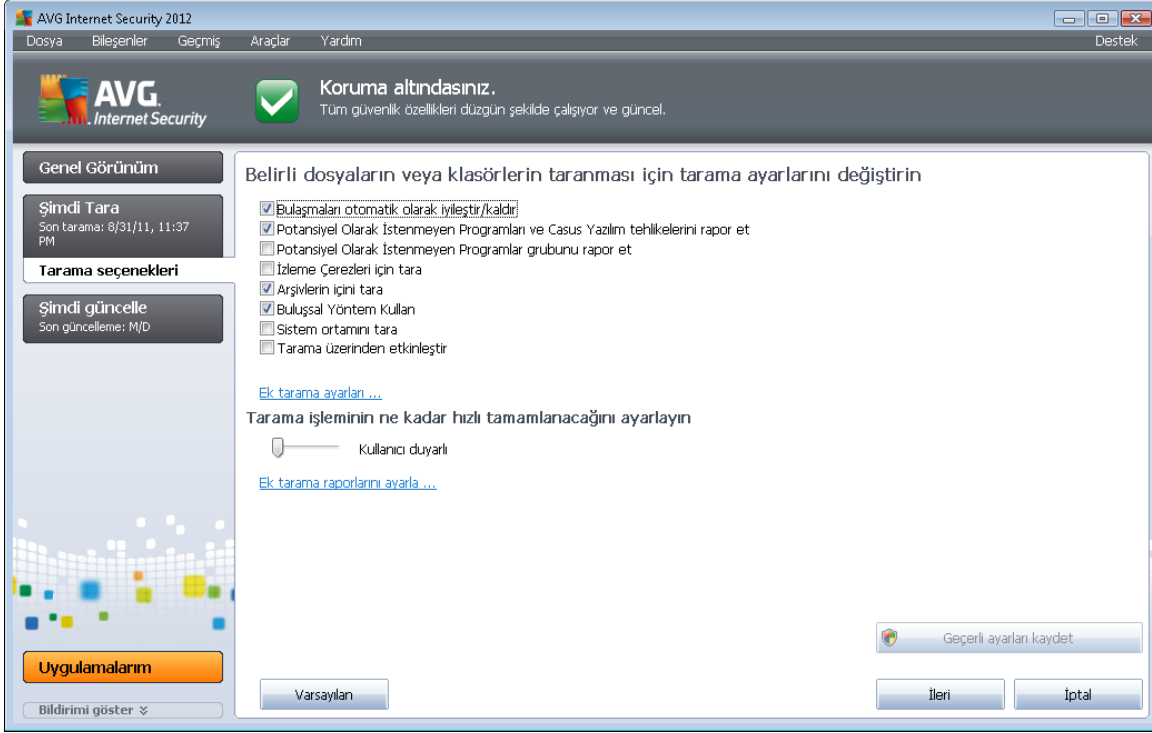
Belirli bir klasör taranırken içinde bulunan klasörlerin taranmaması gibi bir ihtimal de vardır. Bunu yapabilmek için otomatik olarak oluşturulan yolun başına "-" işareti koyun (*ekran görüntülerini inceleyin*). Klasörün tümünü tarama dışında tutmak için "!" parametresini kullanın.

Son olarak, taramayı başlatabilmek için **Taramayı başlat** düğmesine basın. Tarama işleminin kendisi temel olarak [Tüm bilgisayar tarama](#) ile aynıdır.



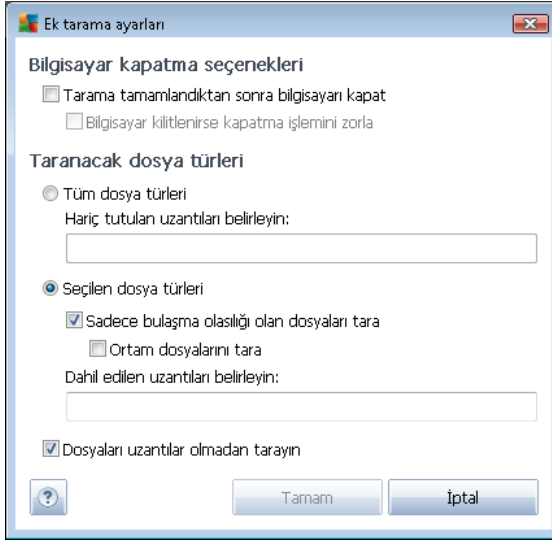
Tarama yapılandırması düzenleme

Belirli dosya ve klasörleri tara fonksiyonunun varsayılan ayarlarını düzenleme opsiyonunuz da bulunmaktadır. **Tarama ayarlarını değiştir** bağlantısına tıklayarak **Belirli dosya ve klasörlerin taranmasına ilişkin tarama ayarlarını değiştir** iletişim kutusuna gidin. **Geçerli bir nedeniniz olmadığı müddetçe varsayılan ayarları değiştirmek için bu ayarları korumanız önerilir!**



- **Tarama parametreleri** - tarama parametreleri listesindeki belirli parametreleri gereksinimleriniz doğrultusunda açıp kapatabilirsiniz.
 - **Bulaşmayı otomatik temizle/sil** - (varsayılan olarak açıktır). Tarama işlemi sırasında bir virüs tanımlanırsa ve temizlenmesi mümkünse otomatik olarak temizlenir. Bulaşmış dosya otomatik olarak temizlenemezse, bulaşmış nesne [Virüs Kasası](#)'na taşınır.
 - **Potansiyel Olarak İstenmeyen Programları ve Casus Yazılım tehditlerini rapor et** (varsayılanda açıktır) - [Anti-Spyware](#) motorunu etkinleştirmek ve virüslerin yanı sıra casus yazılımları da taramak için işaretleyin. Casus yazılım, şüpheli kötü amaçlı yazılım kategorisini ifade eder: genellikle bir güvenlik riskini oluşturmasına rağmen bu programlardan bazıları bilerek yüklenebilir. Bilgisayarınızın güvenliğini artırdığından, bu özelliği etkin durumda tutmanızı öneriyoruz.
 - **Potansiyel Olarak İstenmeyen Programlar gelişmiş grubunu rapor et** (varsayılanda kapalıdır) - bu parametre casus yazılımların, yani doğrudan üreticiden alınan tamamen zararsız olan, ancak daha sonra kötüye kullanılacak programların genişletilmiş paketinin tespit edilmesi için işaretleyin. Bu, bilgisayar güvenliğinizi daha da artıran ek bir önlemdir, ancak yasal programları da engelleyebilir ve bu yüzden varsayılan olarak kapalıdır.
 - **İzleme Tanımlama Bilgilerini Tara** (varsayılan olarak kapalıdır): [Anti-Spyware](#) bileşeninin bu parametresi, tarama sırasında tespit edilmesi istenen tanımlama bilgilerini tanımlar (*HTTP tanımlama bilgileri kimlik doğrulaması, izleme ve kullanıcılar hakkındaki site tercihleri veya elektronik alışveriş sepetlerinin içeriği gibi belirli bilgilerin korunması için kullanılır*).

- **Arşivleri tara** (varsayılan olarak açıktır) - bu parametre, ZIP, RAR vb. arşiv dosyalarının içinde sıkıştırılmış dosyaların bile taranmasını sağlar.
 - **Buluşsal Analiz Yöntemlerini Kullan** - (varsayılan olarak kapalıdır). Buluşsal analiz yöntemi (taranan nesnenin komutlarının sanal bir bilgisayar ortamında dinamik olarak canlandırılması) tarama sırasında kullanılacak virüs tespiti yöntemlerinden biridir.
 - **Sistem ortamını tara** (varsayılan olarak kapalıdır) - tarama işlemi, bilgisayarınızın sistem alanlarını da kontrol edecektir.
 - **Kapsamlı taramayı etkinleştir** (varsayılanda kapalıdır) - belirli durumlarda (bilgisayarınıza bulaşma olmasından şüpheleniliyorsa) yalnızca emin olmak üzere bilgisayarınızın bulaşma olması çok zor olan alanlarını bile tarayan en kapsamlı tarama algoritmalarını etkinleştirmek için bu seçeneği işaretleyebilirsiniz. Ancak, bu yöntemin çok fazla zaman aldığını unutmayın.
- **Ek tarama ayarları** - bağlantı, şu parametreleri belirtebileceğiniz yeni bir **Ek tarama ayarları** iletişim kutusu açar:

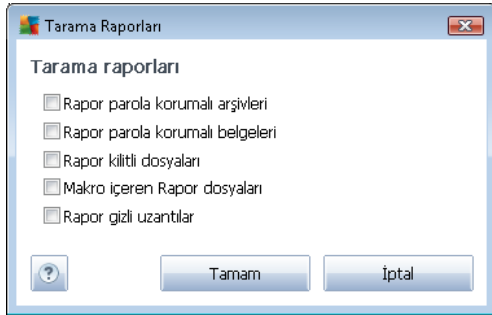


- **Bilgisayar kapatma seçenekleri** - Çalışan tarama işlemi bittiğinde bilgisayarın otomatik olarak kapatılması gerekip gerekmediğine karar verir. Bu seçeneği seçerseniz (**Tarama bittikten sonra bilgisayarı kapat**) bilgisayar mevcut durumda kilitli olsa bile bilgisayarın kapatılmasını sağlayan bir seçeneğin bulunduğu bir pencere açılacaktır (**Bilgisayar kilitliyse bilgisayarı kapanmaya zorla**).
- **Taranacak dosya türleri** - nelerin taranmasını istediğinize de karar vermelisiniz:
 - **Tüm dosya türleri** taranmaması gereken virgülle ayrılmış dosya uzantılarının listesini sağlayarak taramada istisnaları tanımlama seçeneğiyle;
 - **Seçili dosya türleri** - yalnızca virüs bulaşabilme olasılığı olan dosyaları taramayı istediğinizi belirtebilirsiniz (*virüs bulaşmayan dosyalar taranmayacaktır, örneğin,*

bazı düz metin dosyaları veya bazı diğer çalıştırılmayan dosyalar); ortam dosyaları (video, ses dosyaları - bu onay kutusunun işaretini kaldırırsanız, bu dosyalar genellikle çok büyük olduğundan ve virüs bulaşma olasılıkları çok az olduğundan tarama süresini daha da azaltır). Tekrar, her zaman taranması gereken dosyaları uzantılarına göre belirtebilirsiniz.

➤ İsteğe bağlı olarak, **Uzantıları olmayan dosyaları taramaya** da karar verebilirsiniz ve bu seçenek varsayılan olarak açıktır ve gerçekten bir nedeniniz yoksa değiştirmemeniz önerilir. Uzantısı olmayan dosyalar şüpheli olabilir ve her zaman taranmalıdır.

- **Tarama işlemi önceliği** - tarama işlemi önceliğini değiştirmek için kaydırma çubuğunu kullanabilirsiniz. Bu seçenek değeri, varsayılan olarak, otomatik kaynak kullanımının kullanıcıya duyarlı düzeyine ayarlanmıştır. Alternatif olarak, sistem kaynakları kullanımını minimize etmek için tarama işlemi yavaşlatabilir (*bilgisayarda çalışmanız gerektiği ancak taramanın ne kadar sürdüğünü önemsemediğiniz durumlar için uygundur*) veya sistem kaynaklarını daha yoğun kullanmak suretiyle daha hızlı bir şekilde (*ör., bilgisayar geçici bir süreyle kullanılmadığında*) çalıştırabilirsiniz.
- **Tarama raporu oluştur** - bağlantı üzerinden **Tarama Raporları** isimli bir iletişim kutusu açılır ve buradan ne tip buluntuların rapor edileceğini seçebilirsiniz:



Uyarı: Bu tarama parametreleri, yeni tanımlanan taramanın parametreleri ile aynıdır - [AVG Taraması / Tarama Planlama/ Tarama Tipi](#) bölümünde açıklandığı doğrultuda. **Belirli dosya veya klasörleri tara** fonksiyonunun varsayılan yapılandırmasını değiştirmeye karar vererseniz yeni ayarlarınızı, belirli dosya ya da klasörlerin taranması için kullanılacak varsayılan yapılandırma olarak atayabilirsiniz. Buna ek olarak söz konusu yapılandırma tüm yeni programlı taramalarınız için şablon görevi görecektir (tüm özelleştirilmiş taramalar, Seçilen dosya ya da klasörleri tara fonksiyonunun mevcut yapılandırmasına dayanmaktadır).

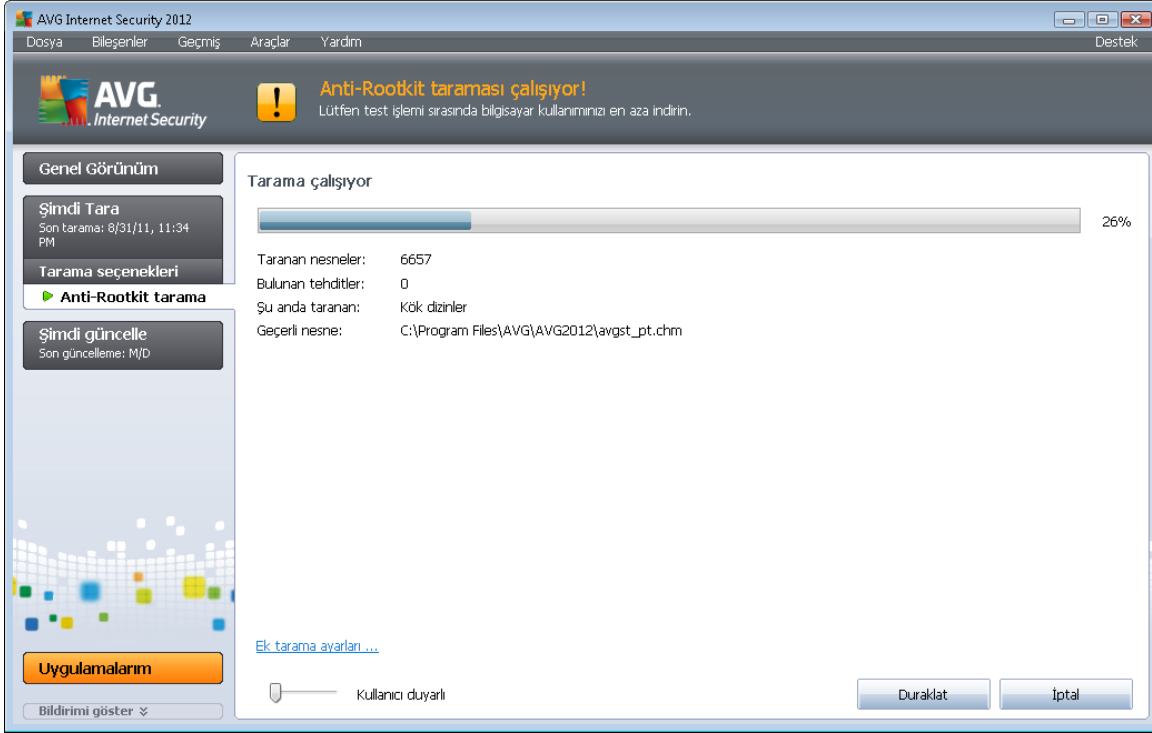
11.2.3. Anti-Rootkit Tarama

Anti-Rootkit tarama, bilgisayarınızı olası kök dizine karşı (*bilgisayarınızdaki kötü amaçlı yazılım etkinliği içerebilecek programlar ve teknolojiler*) açısından tarar. Bir kök dizin algılanırsa, bu, bilgisayarınızda mutlaka virüs olduğu anlamına gelmez. Bazı durumlarda, belirli sürücüler veya normal uygulamaların bölümleri kök dizin olarak yanlış algılanabilir.

Tarama başlatma



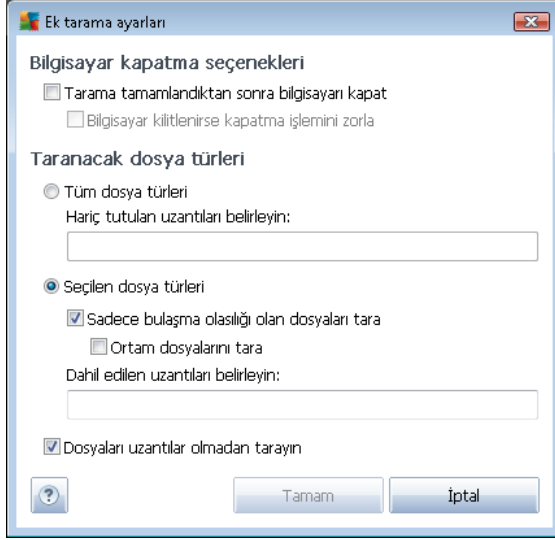
Anti-Rootkit tarama işlevi, tarama simgesi tıklanarak doğrudan [tarama arayüzünden](#) başlatılabilir. Bu tarama türü için belirli ayarlamaların yapılmasına gerek yoktur, tarama, **Tarama yapılıyor** iletişim kutusunda **hemen başlayacaktır** (ekran görüntüsüne bakın). Tarama işlemi gerekirse geçici olarak kesintiye uğratılabilir (**Duraklat**) ya da iptal edilebilir (**Durdur**).



Tarama yapılandırması düzenleme

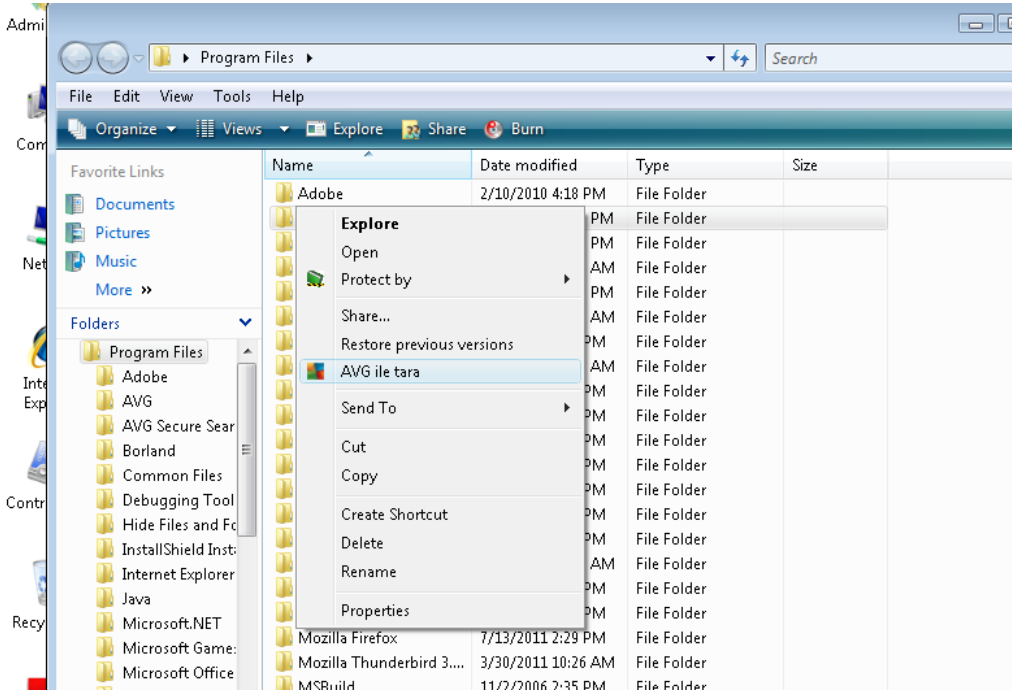
Anti-Rootkit tarama varsayılan ayarlarda her zaman başlatılır ve tarama parametrelerinin düzenlenmesine yalnızca [AVG Gelişmiş Ayarları/Anti-Rootkit](#) iletişim kutusundan erişilebilir. Tarama arayüzünde, şu yapılandırma kullanılabilir (ancak yalnızca tarama çalışırken):

- **Otomatik tarama** - tarama işlemi önceliğini değiştirmek için kaydırma çubuğunu kullanabilirsiniz. Bu seçenek değeri, varsayılan olarak, otomatik kaynak kullanımının *kullanıcıya duyarlı* düzeyine ayarlıdır. Alternatif olarak, sistem kaynakları kullanımını minimize etmek için tarama işlemi yavaşlatabilir (*bilgisayarda çalışmanız gerektiği ancak taramanın ne kadar sürdüğünü önemsemediğiniz durumlar için uygundur*) veya sistem kaynaklarını daha yoğun kullanmak suretiyle daha hızlı bir şekilde (*ör., bilgisayar geçici bir süreyle kullanılmadığında*) çalıştırabilirsiniz.
- **Ek tarama ayarları** - bu bağlantı yeni bir **Ek tarama ayarları** iletişim kutusu açar; burada **Anti-Rootkit taraması** ile ilgili olası bilgisayar kapatma koşullarını tanımlayabilirsiniz (**Tarama işlemi tamamlandığında bilgisayarı kapat, büyük olasılıkla Bilgisayar kilitletirse kapatmaya zorla**):



11.3. Windows Gezgini'nde Tarama

Bilgisayarın tümünde ya da seçilen bölümlerinde gerçekleştirilen öntanımlı taramaların yanı sıra **AVG Internet Security 2012**, doğrudan Windows Gezgini ortamında bulunan belirli nesnelere hızlı bir şekilde taramasını da sağlamaktadır. Bilinmeyen bir dosyayı açmak istiyor fakat içeriğinden emin olamıyorsanız isteğe bağlı olarak tarayabilirsiniz. Bu adımları takip edin:



- Windows Gezgini'nde taramak istediğiniz dosyayı (ya da klasörü) seçin
- Bağlam menüsünü açmak için nesneye fare ile sağ tıklayın



- *ile Tara* seçeneğini seçerek dosyanın AVG tarafından taranmasını sağlayın **AVG Internet Security 2012**

11.4. Komut Satırı Tarama

AVG Internet Security 2012 içinde, taramayı komut satırından çalıştırma seçeneği vardır. Bu seçeneği, sunucularda ya da bilgisayar yeniden başlatıldıktan sonra otomatik olarak çalıştırılacak komut metinlerinin oluşturulması sırasında kullanabilirsiniz. Komut satırında AVG'nin grafik kullanıcı arayüzünde sunulan parametrelerden daha fazlasını kullanarak tarama işlemini gerçekleştirebilirsiniz.

AVG taramasını komut satırından çalıştırmak için AVG'nin yüklendiği klasörde aşağıdaki komutu çalıştırın:

- **32 bit OS için avgscanx**
- **64 bit OS için avgscana**

Komut sözdizimi

Komut söz dizimi aşağıdaki gibidir:

- **Tam bilgisayar taraması yapılırken avgscanx /parametre ...** Örn. **avgscanx /comp**
- **avgscanx /parameter /parameter ..** Birden fazla parametre kullanıldığı zaman bunlar bir sıra halinde dizilmeli ve bir boşluğun yanı sıra bir de tire işareti ile ayrılmalıdır
- Parametrelerden biri için belirli bir değer verilmesi gerekiyorsa (**/scan** parametresi taranmak üzere bilgisayarınızın seçilen alanları hakkında bilgi talep eder ve sizin de seçilen bölüme ilişkin veri yolunu tam olarak sağlamanız gerekir). Değerler noktalı virgül ile birbirinden ayrılır. Örn: **avgscanx /scan=C:\;D:**

Tarama parametreleri

Mevcut parametrelerin tam görünümünü görüntülemek için, **/?** parametresi ile birlikte ilgili komutu yazın. ya da **/HELP** (örn. **avgscanx /?**). Zorunlu olan tek parametre, bilgisayarın hangi alanlarının taranması gerektiğini belirlemek için kullanılan **/SCAN** parametresidir. Seçenekler hakkında daha ayrıntılı açıklama almak için [komut satırı parametrelerine genel bakış](#) bölümüne bakın.

Tarama işlemini başlatmak için **Enter** tuşuna basın. Tarama sırasında işlemi **Ctrl+C** veya **Ctrl+Pause** tuşlarına basarak durdurabilirsiniz.

CMD taraması grafik arayüzünden başlatıldı

Bilgisayarınızı Windows Güvenli Modda çalıştırdığınız zaman komut satırı taramasını grafik kullanıcı arayüzünden başlatma ihtimaliniz de bulunmaktadır. Taramanın kendisi komut satırından başlatılacaktır, **Komut Satırı Oluşturucu** iletişim kutusu, en yaygın tarama parametrelerini konforlu grafik arayüzünde görüntüler.



Söz konusu iletişim kutusuna sadece Windows Güvenli Moddan ulaşılabildiği için iletişim kutusu hakkında ayrıntılı bilgi almak için doğrudan iletişim kutusundan açılan yardım dosyasını inceleyin.

11.4.1. CMD Tarama Parametreleri

Komut satırı taramasında kullanılan parametrelerin listesi aşağıda verilmiştir:

- **/SCAN** [Belirli dosya ya da klasörleri tara](#) /SCAN=yol;yol (örn. /SCAN=C:\
D:\)
- **/COMP** [Tüm Bilgisayarın Taranması](#)
- **/HEUR** [Bulgusal analizi kullan](#)
- **/EXCLUDE** Tarama işleminden izin yolu veya dosyaları hariç tutun
- **/@** Komut dosyası /dosya adı/
- **/EXT** Bu uzantıları tarayın /örneğin EXT=EXE,DLL/
- **/NOEXT** u uzantıları tarama /örneğin NOEXT=JPG/
- **/ARC** Arşiveri tara
- **/CLEAN** Otomatik olarak temizle
- **/TRASH** Bulaşan dosyaları [Virüs Kasasına taşı](#)
- **/QT** Hızlı test
- **/MACROW** Makroları rapor et
- **/PWDW** Parola ile korunan dosyaları rapor et
- **/IGNLOCKED** Kilitli dosyaları göz ardı et
- **/REPORT** /dosya adı/ dosyasına rapor et
- **/REPAPPEND** Rapor dosyasına ekle
- **/REPOK** Bulaşmamış dosyaları Tamam olarak raporla
- **/NOBREAK** CTRL-BREAK ile işlemin kesilmesine izin verme
- **/BOOT** MBR/BOOT kontrolünü etkinleştir
- **/PROC** Aktif işlemleri tara
- **/PUP** ["Potansiyel olarak istenmeyen programları"](#) rapor et
- **/REG** Kayıt defterini tara



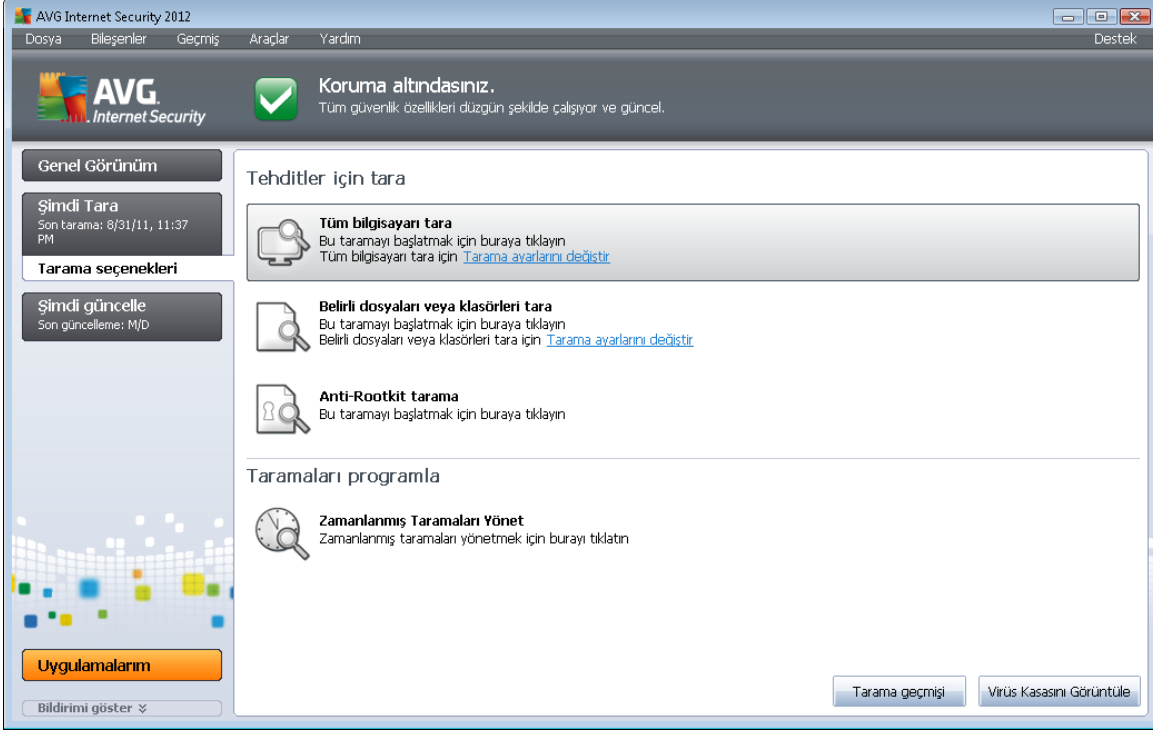
- **/COO** Tanımlama bilgilerini tara
- **/?** Bu konuyla ilgili yardımı görüntüle
- **/HELP** Bu konuyla ilgili yardımı görüntüle
- **/PRIORITY** Tarama önceliğini belirle /Düşük, Oto, Yüksek/ (bkz. [Gelişmiş ayarlar / Taramalar](#))
- **/SHUTDOWN** Tarama tamamlandıktan sonra bilgisayarı kapat
- **/FORCESHUTDOWN** Tarama tamamlandıktan sonra bilgisayarı kapatmayı zorla
- **/ADS** *Alternatif Veri Akışlarını Tara (sadece NTFS)*
- **/ARCBOMBSW** Yeniden sıkıştırılmış arşiv dosyalarını bildir

11.5. Tarama Programlama

AVG Internet Security 2012 ile, taramayı talep üzerine (örneğin bilgisayarınıza virüs bulaştığından şüphelenirseniz) veya programlanan bir plan doğrultusunda başlatabilirsiniz. Taramaların bir program doğrultusunda yapılması önemle önerilir. Bu şekilde, bilgisayarınızın bulaşma ihtimaline karşı korunduğundan emin olursunuz ve ne zaman tarama yapmanız gerektiği konusunda endişelenmenize gerek kalmaz.

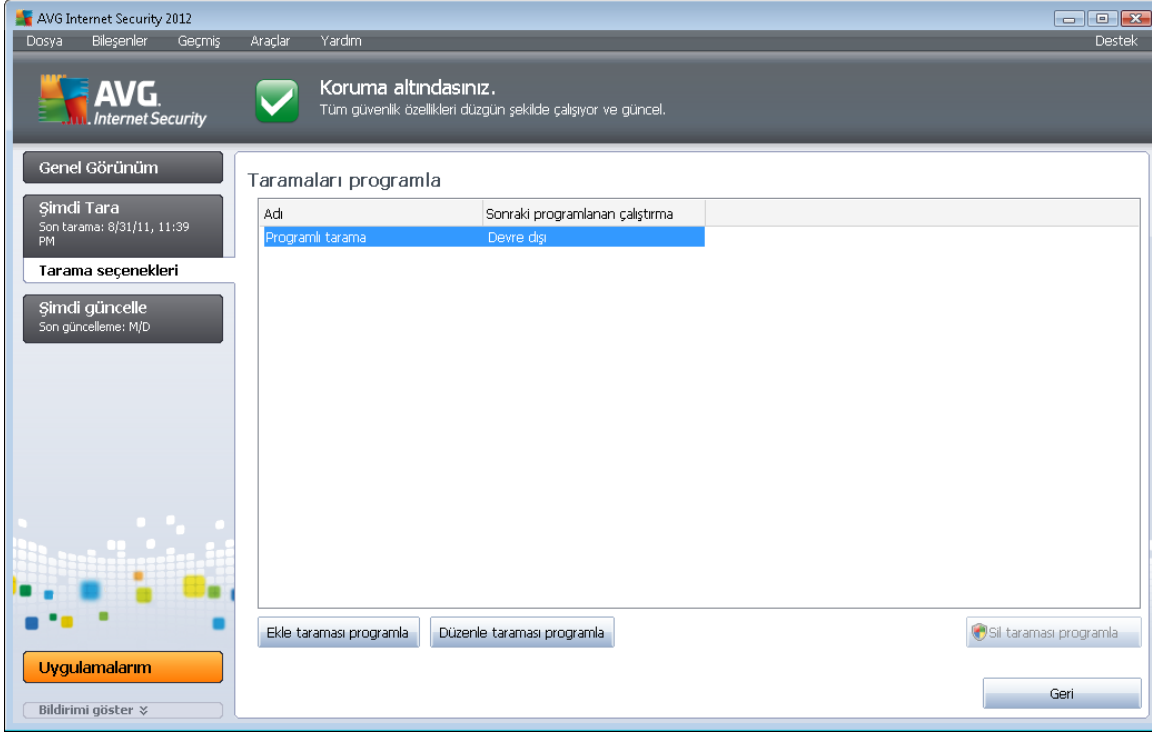
[Tüm bilgisayar taraması](#)'nı en az haftada bir kez düzenli olarak başlatmanız gerekir. Diğer bir yandan, mümkün olması halinde programlı taramanın varsayılan yapılandırmasında ayarlandığı gibi tüm bilgisayar taramasını günlük olarak yapın. Bilgisayarınız "daima açık" ise taramaları çalışma saatlerinden sonra gerçekleştirilecek şekilde programlayabilirsiniz. Bilgisayarınızı arada sırada kapatıyorsanız taramayı, taramaları [görev yerine getirilemediğinde bilgisayarın başlaması ile başlat](#) şeklinde programlayın.

Yeni tarama programları oluşturmak için [AVG tarama arayüzünü](#) inceleyin ve **Tarama programla** adı altındaki bölümü bulun:



Taramaları programla

Geçerli olarak zamanlanmış taramaların bir listesini bulabileceğiniz yeni bir **Taramaları programla** iletişim kutusunu açmak için **Taramaları programla** bölümündeki grafik simgeyi tıklayın:

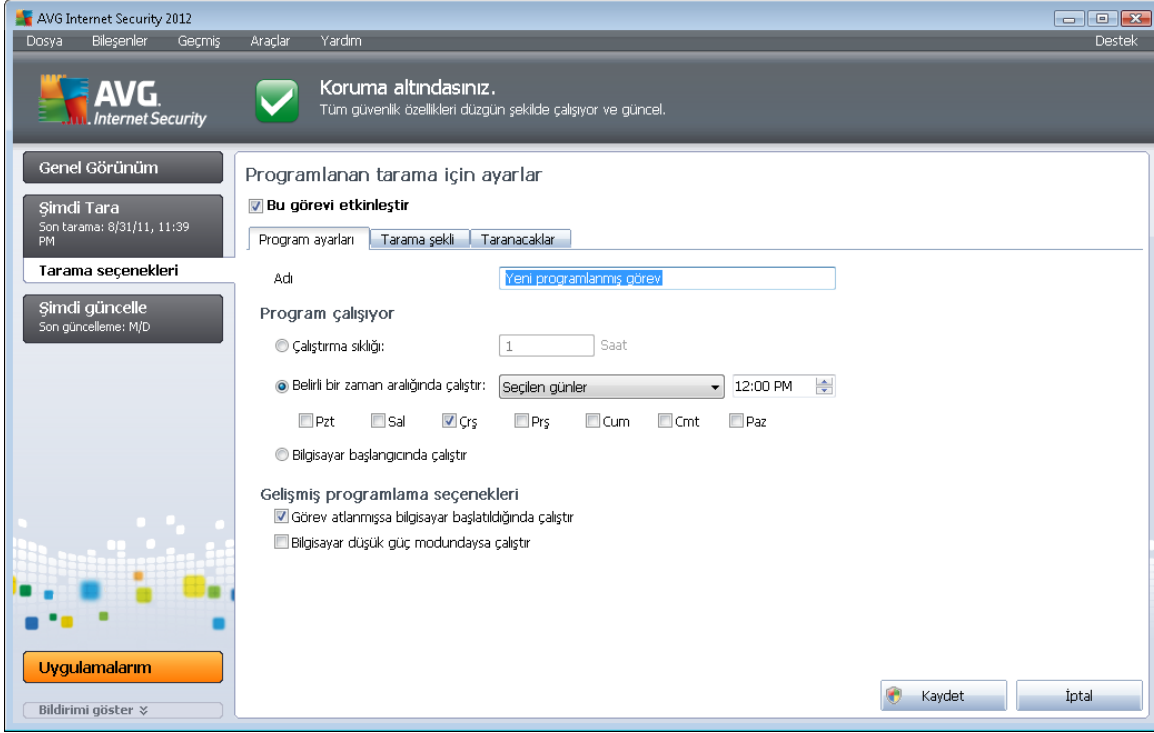


Şu kontrol düğmelerini kullanarak taramaları düzenleyebilir/ekleyebilirsiniz:

- **Tarama programı ekle** - düğme, **Programlanan tarama ayarları** iletişim kutusunu ve [Programlama Ayarları](#) sekmesini açar. Bu iletişim kutusunda yeni tanımladığınız taramanın parametrelerini belirleyebilirsiniz.
- **Tarama programını düzenle** - bu düğme, programlanan taramalar listesinden mevcut bir taramayı seçtiyseniz kullanılabilir. Bu durumda düğme etkinleşir ve **Programlanan tarama ayarları** iletişim kutusuna ve [Programlama ayarları](#) sekmesine geçmek için düğmeyi kullanabilirsiniz. Seçilen tarama parametreleri, zaten belirlenmiştir ve düzenlenebilir.
- **Tarama programını sil** - bu düğme, programlanan taramalar listesinden mevcut bir taramayı seçmeniz halinde etkinleşir. Bu tarama, ilgili kontrol düğmesine basılarak listeden silinebilir. Diğer bir yandan sadece kendi taramalarınızı silebilirsiniz; varsayılan ayarlar içinde **Tüm bilgisayar taraması programı** öntanımlıdır ve kesinlikle silinemez.
- **Geri** - [AVG tarama arayüzüne geri döner](#)

11.5.1. Program Ayarları

Yeni bir test programlamayı ve testin düzenli olarak başlamasını istiyorsanız, **Programlanan test ayarları** iletişim kutusuna girin, (**Taramaları programla iletişim kutusundaki Tarama programı ekle** düğmesini tıklayın). Bu iletişim kutusu üç sekmeye ayrılmıştır: **Programlama ayarları** (aşağıdaki resme bakın; doğrudan yönlendirileceğiniz varsayılan sekmedir), [Tarama türü](#) ve [Taranacaklar](#).



Planlama ayarları sekmesinde **Bu görevi etkinleştir** ögesini işaretleyerek ya da işareti kaldırarak planlanan taramayı geçici olarak devre dışı bırakabilir ve ihtiyaç duyduğunuzda yeniden açabilirsiniz.

Sonra oluşturmak ve programlamak üzere olduğunuz taramanın adının verir. **İsim** ögesini kullanarak metin alanına bir isim girin. Programladığınız taramaları diğerlerinden kolaylıkla ayırabilmek için taramalarınıza kısa, açıklayıcı isimler vermeyi deneyin.

Örnek: Taramayı "Yeni Tarama" veya "Taramam" adıyla adlandırmanız uygun değildir çünkü bu adlar, taramanın fiilen neyi kontrol ettiğini açıklamaz. Diğer bir yandan "Sistem alanları taraması" oldukça açıklayıcı bir isim olacaktır. Ayrıca, taramanın adında söz konusu taramanın tam bilgisayar taraması ya da sadece seçilen dosya ya da klasörlerin taraması olup olmadığını belirtmenize gerek yoktur - taramalarınız seçilen dosya ya da klasörleri tara işlevinin farklı şekillerinden ibaret olacaktır.

Bu iletişim kutusunda taramanın aşağıdaki parametrelerini de tanımlayabilirsiniz:

- **Planlama çalışıyor** - yeni planlanan taramanın başlaması için zaman aralığı girin. Zamanlama belirli bir sürenin ardından tekrarlanan tarama ile (**Her ...'de bir**) ya da kesin bir tarih ve saat tanımlayarak (**Belirli bir saatte çalıştır ...**), ya da (**Bilgisayar başlangıcında**) ilgili bir programın taranmasıyla tanımlanabilir.
- **Gelişmiş planlama seçenekleri** - bu bölümde, bilgisayar düşük güç modundayken veya tamamen kapatılmışsa hangi koşullar altında taramanın başlatılması/başlatılmaması gerektiğini belirleyebilirsiniz.

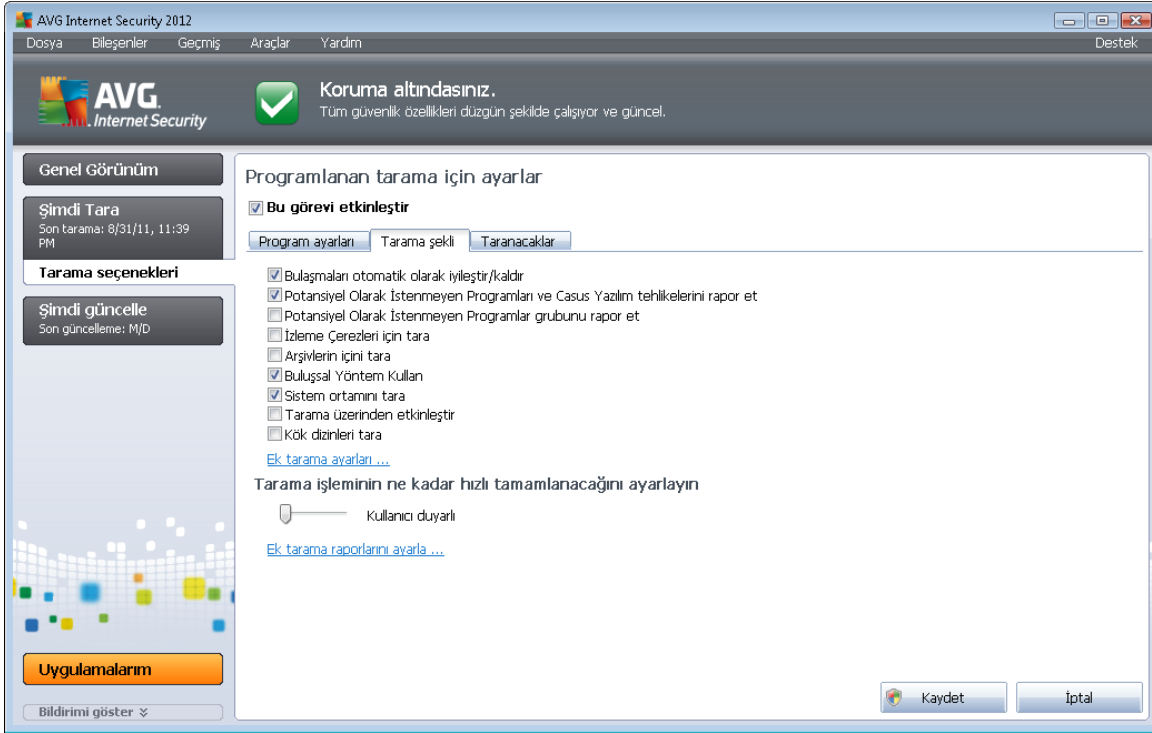
Programlı tarama iletişim kutusuna dair ayarların kontrol düğmeleri



Programlı tarama ayarları iletişim kutusunda üç adet sekme bulunmaktadır (*Programlama ayarları*, [Tarama şekli](#) ve [Taranacaklar](#)) ve hangi sekmede olduğunuz önemli olmaksızın aşağıdaki düğmelerin fonksiyonları aynıdır:

- **Kaydet** - bu sekmede veya bu iletişim kutusunun başka herhangi bir sekmesinde gerçekleştirdiğiniz tüm değişiklikleri kaydeder ve [AVG tarama arayüzü varsayılan penceresine](#) geri döner. Bu nedenle tüm sekmelerdeki test parametrelerini yapılandırmak istiyorsanız gereksinimlerinizin tamamını belirledikten sonra bunları kaydetmek için düğmeye basın.
- **İptal** - bu iletişim kutusunun bu sekmesinde veya başka bir sekmesinde yaptığınız değişiklikleri iptal eder ve [AVG tarama arayüzü varsayılan iletişim kutusuna geri döner](#).

11.5.2. Tarama Şekli



Tarama Şekli sekmesinde, isteğe bağlı olarak açılıp/kapatılabilen tarama parametrelerine ilişkin bir liste bulabilirsiniz. Varsayılan olarak birçok parametre devreye sokulur ve işlevsellik de tarama sırasında uygulanacaktır. Söz konusu ayarları değiştirmek açısından geçerli bir nedeniniz yoksa varsayılan yapılandırmayı olduğu gibi muhafaza etmeniz önerilir:

- **Bulaşmayı otomatik olarak temizle/kaldır** (varsayılanda açıktır): Tarama sırasında virüs tanımlanırsa, bir giderme yazılımı mevcutsa otomatik olarak temizlenir. Etkilenen dosyanın otomatik olarak silinmiyor olması halinde ya da bu seçeneği kapatmayı seçerseniz bir virüs tespit edildiğinde bilgilendirileceksiniz ve tespit edilen bulaşma hakkında ne yapılacağına karar vermek zorunda kalacaksınız. Önerilen işlem, bulaşmış dosyayı [Virüs Kasasına](#) kaldırmaktır.
- **Potansiyel Olarak İstenmeyen Programları ve Casus Yazılım tehditlerini rapor et** (

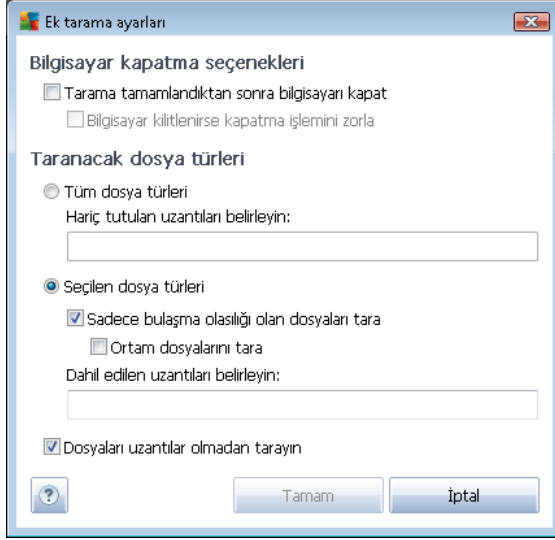


varsayılan olarak açıktır): [Anti-Spyware](#) motorunu etkinleştirmek ve virüslerin yanı sıra casus yazılımları da denetlemek için işaretleyin. Casus yazılım, şüpheli kötü amaçlı yazılım kategorisini ifade eder: genellikle bir güvenlik riskini oluşturmasına rağmen bu programlardan bazıları bilerek yüklenebilir. Bilgisayarınızın güvenliğini artırdığından, bu özelliği etkin durumda tutmanızı öneriyoruz.

- **Potansiyel Olarak İstenmeyen Programlar gelişmiş grubunu rapor et** (*varsayılanda kapalıdır*) - bu parametre casus yazılımların, yani doğrudan üreticiden alınan tamamen zararsız olan, ancak daha sonra kötüye kullanılacak programların genişletilmiş paketinin tespit edilmesi için işaretleyin. Bu, bilgisayar güvenliğinizi daha da artıran ek bir önlemdir, ancak yasal programları da engelleyebilir ve bu yüzden varsayılan olarak kapalıdır.
- **İzleme Tanımlama Bilgilerini Tara** (*varsayılan olarak kapalıdır*): [Casus Yazılımdan Korunma](#) bileşeninin bu parametresi, tarama sırasında tespit edilmesi istenen tanımlama bilgilerini tanımlar (*HTTP tanımlama bilgileri kimlik doğrulaması, izleme ve kullanıcılar hakkındaki site tercihleri veya elektronik alışveriş sepetlerinin içeriği gibi belirli bilgilerin korunması için kullanılır*).
- **Arşivleri Tara** - (*varsayılan olarak kapalıdır*). Bu parametreler, tarama işleminin ZIP, RAR gibi bazı arşiv türleri ile sıkıştırılmış olsa bile tüm dosyaları denetlemesini tanımlar.
- **Buluşsal Analiz Yöntemlerini Kullan** - (*varsayılan olarak açıktır*). Buluşsal analiz yöntemi (*taranan nesnenin komutlarının sanal bir bilgisayar ortamında dinamik olarak canlandırılması*) tarama sırasında kullanılacak virüs tespiti yöntemlerinden biridir.
- **Sistem ortamını tara** - (*varsayılan olarak açıktır*). Tarama işlemi, bilgisayarınızın sistem alanlarını da kontrol edecektir.
- **Kapsamlı taramayı etkinleştir** (*varsayılanda kapalıdır*) - belirli durumlarda (*bilgisayarınıza bulaşma olmasından şüpheleniliyorsa*) yalnızca emin olmak üzere bilgisayarınızın bulaşma olması çok zor olan alanlarını bile tarayan en kapsamlı tarama algoritmalarını etkinleştirmek için bu seçeneği işaretleyebilirsiniz. Ancak, bu yöntemin çok fazla zaman aldığı unutmayın.
- **Kök izinleri tara** (*varsayılan olarak kapalıdır*). Kök izin tespitini tüm bilgisayarın taranmasına eklemek için bu öğeyi işaretleyin. Kök izin tespiti, [Anti-Rootkit](#) bileşeni içinde de bulunur.

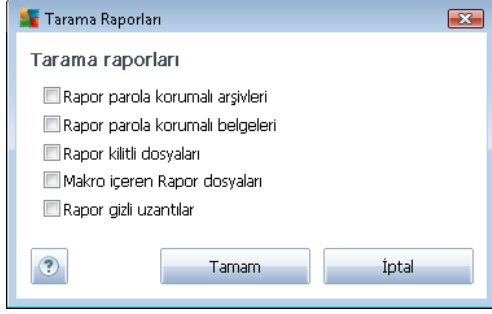
Sonra, tarama yapılandırmasını şu şekilde değiştirebilirsiniz:

- **Ek tarama ayarları** - Bağlantı, şu parametreleri belirtebileceğiniz yeni bir **Ek tarama ayarları** iletişim kutusu açar:



- **Bilgisayar kapatma seçenekleri** - Çalışan tarama işlemi bittiğinde bilgisayarın otomatik olarak kapatılması gerekip gerekmediğine karar verir. Bu seçeneği seçerseniz (**Tarama bittikten sonra bilgisayarı kapat**) bilgisayar mevcut durumda kilitli olsa bile bilgisayarın kapatılmasını sağlayan bir seçeneğin bulunduğu bir pencere açılacaktır (**Bilgisayar kilitliyse bilgisayarı kapanmaya zorla**).
- **Tarama için dosya türleri** - Nelerin taranmasını istediğinize de karar vermelisiniz:
 - **Tüm dosya türleri** taranmaması gereken virgülle ayrılmış dosya uzantılarının listesini sağlayarak taramada istisnaları tanımlama seçeneğiyle;
 - **Seçili dosya türleri** - Yalnızca virüs bulaşabilme olasılığı olan dosyaları taramayı istediğinizi belirtebilirsiniz (*virüs bulaşmayan dosyalar taranmayacaktır, örneğin, bazı düz metin dosyaları veya bazı diğer çalıştırılmayan dosyalar*); ortam dosyaları (*video, ses dosyaları - bu onay kutusunun işaretini kaldırırsanız, bu dosyalar genellikle çok büyük olduğundan ve virüs bulaşma olasılıkları çok az olduğundan tarama süresini daha da azaltır*). Tekrar, her zaman taranması gereken dosyaları uzantılarına göre belirtebilirsiniz.
 - İsteğe bağlı olarak, **Uzantıları olmayan dosyaları taramaya** da karar verebilirsiniz ve bu seçenek varsayılan olarak açıktır ve gerçekten bir nedeniniz yoksa değiştirmemeniz önerilir. Uzantısı olmayan dosyalar şüpheli olabilir ve her zaman taranmalıdır.
- **Taramanın ne kadar hızlı tamamlanacağını ayarlayın** - Tarama sürecinin önceliğini değiştirmek için kaydırma çubuğunu kullanabilirsiniz. Bu seçenek varsayılan olarak otomatik kaynak kullanımının *kullanıcıya duyarlı* düzeyine ayarlanmıştır. Alternatif olarak, sistem kaynakları kullanımını minimize etmek için tarama işlemi yavaşlatabilir (*bilgisayarda çalışmanız gerektiği ancak taramanın ne kadar sürdüğünü önemsemediğiniz durumlar için uygundur*) veya sistem kaynaklarını daha yoğun kullanmak suretiyle daha hızlı bir şekilde (*ör., bilgisayar geçici bir süreyle kullanılmadığında*) çalıştırabilirsiniz.
- **Tarama raporu oluştur** - bağlantı üzerinden **Tarama Raporları** isimli bir iletişim kutusu

açılır ve buradan ne tip buluntuların rapor edileceğiniz seçebilirsiniz:

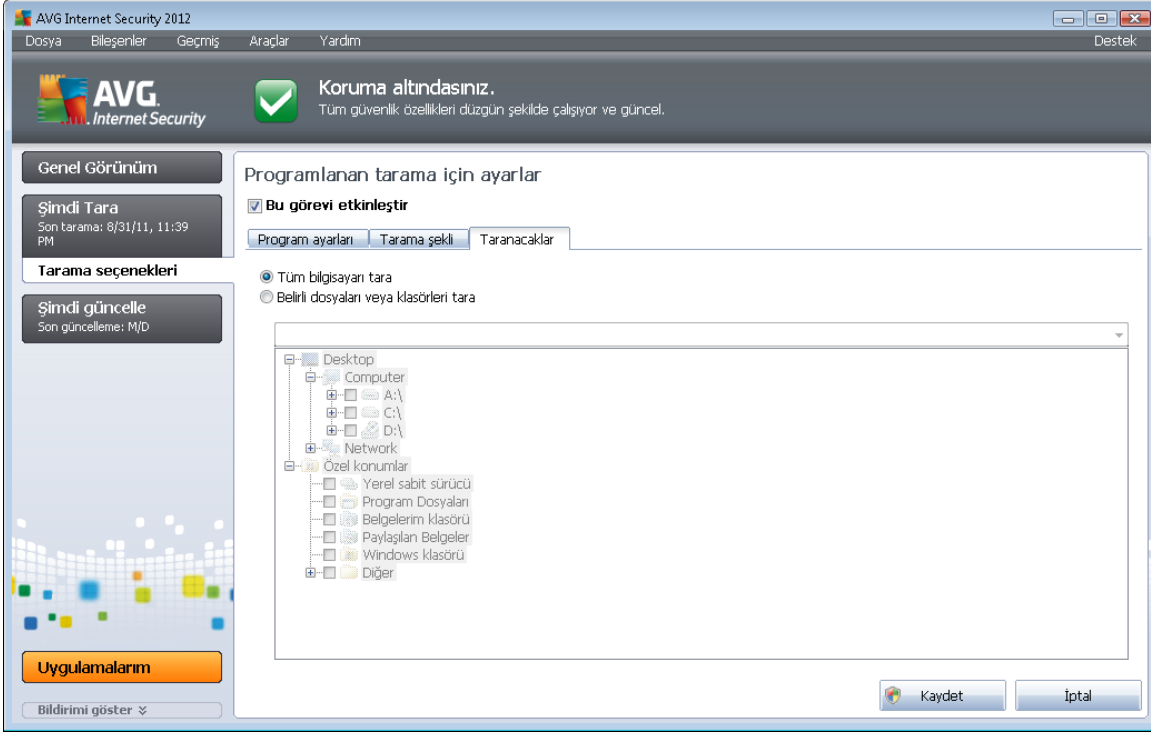


Kontrol düğmeleri

Programlı tarama ayarları iletişim kutusunun her üç sekmesinde ([Programlama ayarları](#), [Tarama şekli](#) ve [Taranacaklar](#)) iki kontrol düğmesi bulunmaktadır ve hangi sekmede olduğunuz önemli olmaksızın bunların fonksiyonları aynıdır:

- **Kaydet** - bu sekmede veya bu iletişim kutusunun başka herhangi bir sekmesinde gerçekleştirdiğiniz tüm değişiklikleri kaydeder ve [AVG tarama arayüzü varsayılan penceresine](#) geri döner. Bu nedenle tüm sekmelerdeki test parametrelerini yapılandırmak istiyorsanız gereksinimlerinizin tamamını belirledikten sonra bunları kaydetmek için düğmeye basın.
- **İptal** - bu iletişim kutusunun bu sekmesinde veya başka bir sekmesinde yaptığınız değişiklikleri iptal eder ve [AVG tarama arayüzü varsayılan iletişim kutusuna geri döner](#).

11.5.3. Taranacaklar



Taranacaklar sekmesinde, [tüm bilgisayarı tarama](#) veya [belirli dosya veya klasörleri taramayı](#) programlamak isteyip istemediğinizi belirleyebilirsiniz.

Belirli dosya ve klasörlerin taranmasını seçmeniz durumunda, bu iletişim kutusunun alt tarafında görüntülenen ağaç yapısı etkinleşir ve taranacak klasörleri belirleyebilirsiniz (*taramak istediğiniz klasörü buluncaya kadar artı işaretini tıklatarak öğeleri genişletin*). İlgili kutuları işaretleyerek birden fazla klasör seçebilirsiniz. Seçilen klasörler, iletişim kutusunun üstünde bulunan metin alanında görüntülenir; açılır menü seçilen tarama geçmişini daha sonra kullanılmak üzere saklar. Alternatif olarak, istediğiniz klasörün tam yolunu elle girebilirsiniz (*birden fazla yol girerseniz, bunları ekstra boşluk bırakmadan noktalı virgülle ayırmanız gerekir*).

Ağaç yapısı içinde **Özel konumlar** adında bir dal da görürsünüz. Aşağıda, ilgili onay kutusu işaretlendiğinde taranacak konumların listesi bulunmaktadır:

- **Yerel sabit sürücüler** - bilgisayarınızdaki tüm sabit sürücüler
- **Program dosyaları**
 - C:\Program Files\
 - 64-bit'lik sürümde C:\Program Files (x86)
- **Belgelerim klasörü**



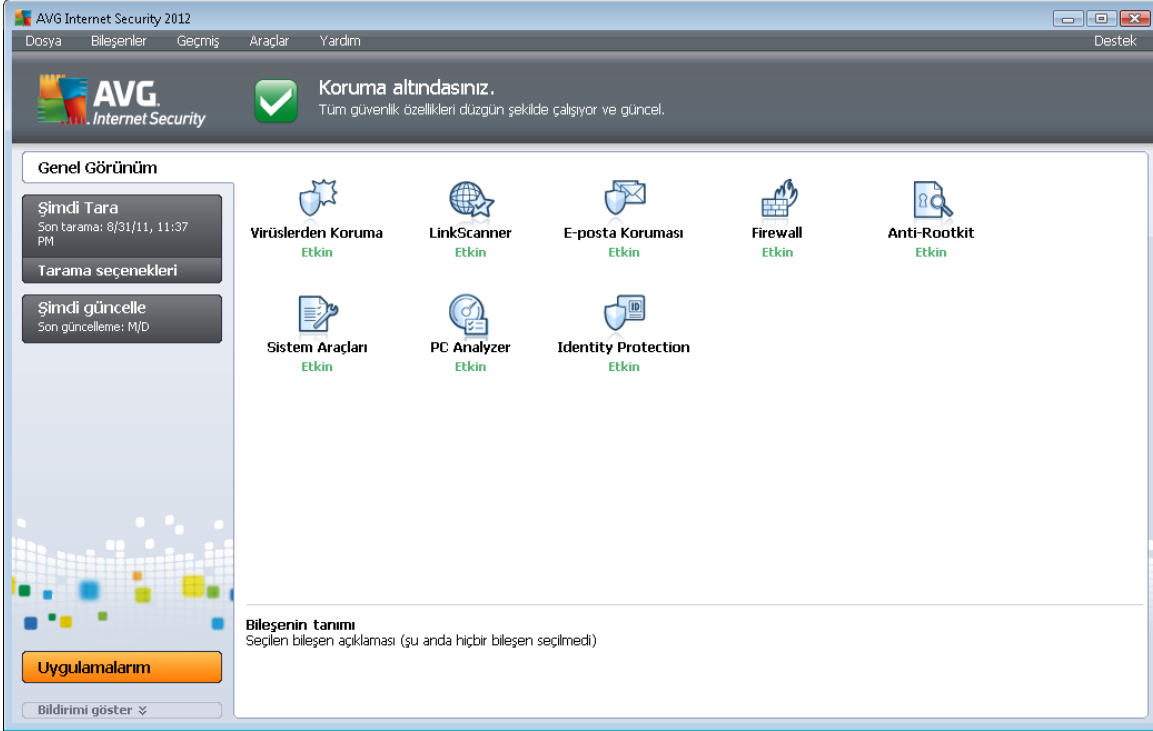
- *Win XP için:* C:\Documents and Settings\Default User\Belgelerim\
- *Windows Vista/7 için:* C:\Users\user\Documents\
- **Paylaşılan Belgeler**
 - *Win XP için:* C:\Documents and Settings\All Users\Documents\
 - *Windows Vista/7 için:* C:\Users\Public\Documents\
- **Windows klasörü** - C:\Windows\
- **Diğer**
 - *Sistem sürücüsü* - işletim sisteminin yüklü olduğu sabit sürücü (genellikle C:)
 - *Sistem klasörü* - C:\Windows\System32\
 - *Geçici Dosyalar klasörü* - C:\Documents and Settings\User\Local\ (*Windows XP*) veya C:\Users\user\AppData\Local\Temp\ (*Windows Vista/7*)
 - *Geçici İnternet Dosyaları* - C:\Documents and Settings\User\Local Settings\Geçici İnternet Dosyaları\ (*Windows XP*) veya C:\Users\user\AppData\Local\Microsoft\Windows\Geçici İnternet Dosyaları (*Windows Vista/7*)

Kontrol düğmeleri

Aynı iki kontrol düğmesi **Programlanan tarama için ayarlar** iletişim kutusunun her üç sekmesinde de mevcuttur ([Program ayarları](#), [Tarama türü](#) ve [Taranacaklar](#)):


- **Kaydet** - bu sekmede veya bu iletişim kutusunun başka herhangi bir sekmesinde gerçekleştirdiğiniz tüm değişiklikleri kaydeder ve [AVG tarama arayüzü varsayılan penceresine](#) geri döner. Bu nedenle tüm sekmelerdeki test parametrelerini yapılandırmak istiyorsanız gereksinimlerinizin tamamını belirledikten sonra bunları kaydetmek için düğmeye basın.
- **İptal** - bu iletişim kutusunun bu sekmesinde veya başka bir sekmesinde yaptığınız değişiklikleri iptal eder ve [AVG tarama arayüzü varsayılan iletişim kutusuna geri döner](#).


11.6. Tarama Sonuçları Genel Görünümü




Tarama sonuçlarına genel bakış penceresine, [AVG tarama arayüzünde Tarama geçmişi](#) düğmesine basarak ulaşabilirsiniz. İletişim kutusunda, daha önce başlatılan tüm taramalar ve sonuçları hakkında bilgi bulunmaktadır.

- **Adı** - taramanın amacı; [öntanımlı taramalardan](#) birinin adı ya da [programladığınız taramaya](#) verdiğiniz adlardan biri olabilir. Her ismin yanında tarama sonucunu belirten bir simge bulunmaktadır:

 - yeşil simge tarama sırasında herhangi bir bulaşmanın tespit edilemediğini gösterir

 - mavi simge tarama sırasında bir bulaşmanın tespit edildiğini ancak bulaşmış nesnenin otomatik olarak silindiğini gösterir

 - kırmızı simge tarama sırasında bir bulaşmanın tespit edildiğini, ancak bulaşmış nesnenin silinemediğini gösterir!

Simgeler bütün halinde ya da yarı kesilmiş olabilir - bütün halindeki simge, tarama işleminin doğru şekilde tamamlandığını ve bitirildiğini gösterirken yarı kesilmiş simge, taramanın iptal edildiğini ya da kesildiğini gösterir.

Not: *Taramaların her biri hakkında ayrıntılı bilgi almak için lütfen [Ayrıntıları Görüntüle](#) düğmesine (bu pencerenin alt kısmındadır) basarak ulaşabileceğiniz [Tarama Sonuçları](#) penceresini inceleyin.*



- **Başlangıç zamanı** - taramanın başlatıldığı tarih ve saati gösterir.
- **Bitiş zamanı** - taramanın bittiği tarih ve saati gösterir.
- **Taranan nesnelere** - tarama sırasında kontrol edilen nesne sayısıdır
- **Bulaşmalar** - tespit edilen / silinenvirüs bulaşması sayısı
- **Casus yazılım** - tespit edilen / silinen casus yazılım sayısı
- **Uyarılar** - algılanan [şüpheli nesnelere](#)
- **Kök dizinler** - algılanan [kök dizinler](#)
- **Tarama kaydı bilgileri** - tarama işlemine ve sonucuna ilişkin bilgiler (genellikle işlemin tamamlanmasının ya da kesilmesinin hemen ardından görüntülenir)

Kontrol düğmeleri

Tarama sonuçlarına genel bakış penceresindeki kontrol düğmeleri şunlardır:

- **Ayrıntıları görüntüle** - seçili taramada ayrıntılı verileri görüntülemek için [Tarama sonuçları](#) iletişim kutusuna geçmek için basın
- **Sonucu sil** - seçili öğeyi tarama sonuçlarına genel bakıştan silmek için basın
- **Geri** - [AVG tarama arayüzünün öntanımlı iletişim penceresine geri döner](#)

11.7. Tarama Sonuçları Ayrıntıları

[Tarama Sonuçlarına Genel Bakış](#) penceresinde belirli bir tarama türü seçildiyse tarama ve seçilen taramanın sonuçları hakkında ayrıntılı bilgi veren **Tarama Sonuçları** penceresini açmak için **Ayrıntıları görüntüle** düğmesine tıklayabilirsiniz. İletişim penceresi çok sayıda sekme ayrılır:

- [Sonuçlara Genel Bakış](#) - bu sekme daima görüntülenir ve tarama işlemi tanımayan istatistik verileri sunar.
- [Bulaşmalar](#) - bu sekme tarama sırasında virüs bulaşması tespit edilirse görüntülenir
- [Casus yazılım](#) - bu sekme tarama sırasında casus yazılım tespit edilirse görüntülenir
- [Uyarılar](#) - bu sekme, örneğin tarama sırasında tanımlama bilgileri algılandıysa görüntülenir
- [Kök kullanıcı](#) - bu sekme tarama sırasında kök kullanıcı tespit edilirse görüntülenir
- [Bilgi](#) - bu sekme, yukarıdaki kategorilerde sınıflandırılmayan potansiyel tespit edildiğinde görüntülenir; ardından söz konusu sekmede buluntu hakkında bir uyarı mesajı görüntülenir. Ayrıca, burada taranamayan nesnelere hakkında bilgi de bulacaksınız (örn. *parola korumalı arşivler*).



11.7.1. Sonuçlara Genel Bakış Sekmesi

Tarama sonuçları sekmesinde aşağıdaki hususlar hakkında ayrıntılı istatistikler ve bilgi bulabilirsiniz:

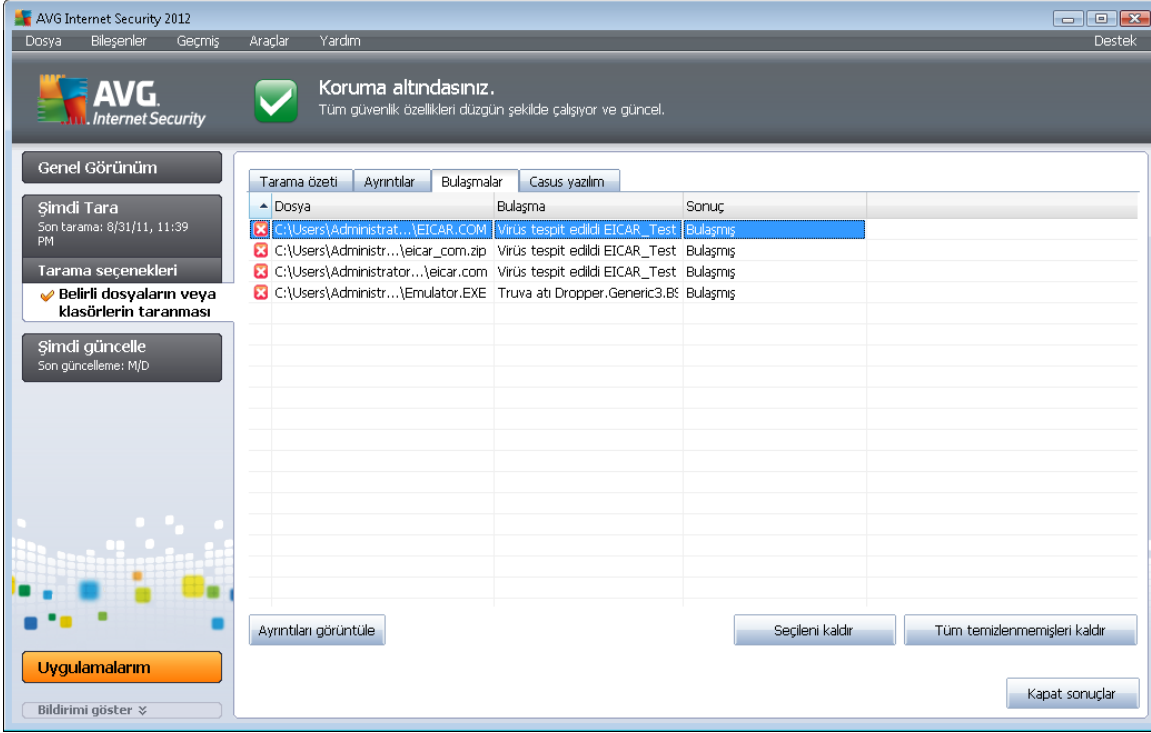
- tespit edilen virüs bulaşmaları / casus yazılım
- silinen virüs bulaşmaları / casus yazılım
- kaldırılmayan ya da temizlenemeyen virüs bulaşması / casus yazılım sayısı

Buna ek olarak, tarama başlangıcı hakkında tarih ve zaman verileri, toplam taranan nesne sayısı, tarama süresi ve tarama sırasında ortaya çıkan hataların sayısı hakkında da bilgi bulabilirsiniz.

Kontrol düğmeleri

Bu iletişim kutusunda sadece bir adet düğme bulunmaktadır. **Sonuçları kapat** düğmesi [Tarama sonuçlarına genel bakış](#) iletişim kutusuna dönmenizi sağlar.

11.7.2. Bulaşma Sekmesi



AVG Internet Security 2012

Dosya Bileşenler Geçmiş Araçlar Yardım Destek

AVG Internet Security

Koruma altındasınız.
Tüm güvenlik özellikleri düzgün şekilde çalışıyor ve güncel.

Genel Görünüm

Şimdi Tara
Son tarama: 8/31/11, 11:39 PM

Tarama seçenekleri

Belirli dosyaların veya klasörlerin taraması

Şimdi güncelle
Son güncelleme: M/D

Uygulamaları

Bildirimi göster

Tarama özeti Ayrıntılar Bulaşmalar Casus yazılım

Dosya	Bulaşma	Sonuç
C:\Users\Administrat...\\EICAR.COM	Virüs tespit edildi EICAR_Test	Bulaşmış
C:\Users\Administrat...\\eicar_com.zip	Virüs tespit edildi EICAR_Test	Bulaşmış
C:\Users\Administrator...\\eicar.com	Virüs tespit edildi EICAR_Test	Bulaşmış
C:\Users\Administrat...\\Emulator.EXE	Truva atı Dropper.Generic3.BE	Bulaşmış

Ayrıntıları görüntüle

Seçileni kaldır

Tüm temizlenmemişleri kaldır

Kapat sonuçlar

Tarama sırasında bir virüs bulaşması tespit edilirse ilgili **Bulaşmalar** sekmesi sadece **Tarama Sonuçları** iletişim kutusunda görüntülenir. Sekme, şu bilgileri sağlayan üç bölüme ayrılmıştır:

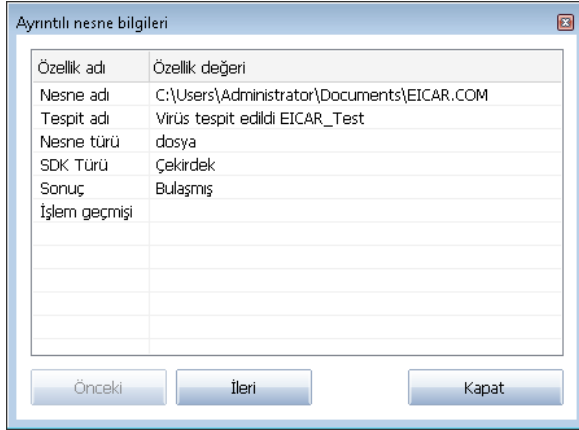
- **Dosya** - bulaşmış nesnenin orijinal konumunun tam dizin yolu
- **Bulaşmalar** - tespit edilen virüsün adı (*belirli virüs türleri hakkında ayrıntılı bilgi almak için lütfen çevrimiçi [Virüs Ansiklopedisine](#) danışın*)
- **Sonuç** - tarama sırasında tespit edilen bulaşmış nesnenin mevcut durumunu tanımlar:
 - **Bulaşanlar** - bulaşan nesne tespit edildi ve orijinal konumunda bırakıldı (*örneğin belirli bir tarama işlemi sırasında otomatik temizleme seçeneğini devre dışı bıraktıysanız*)
 - **Temizlenenler** - bulaşmış nesne otomatik olarak temizlenmiştir ve orijinal konumunda bırakılmıştır
 - **Virüs Kasasına Taşınanlar** - bulaşmış nesne [Virüs Kasası](#) karantinasına taşınmıştır
 - **Silinenler** - bulaşmış nesne silinmiştir
 - **PUP istisnalarına eklenenler** - bulgu bir istisna olarak değerlendirilmiş ve PUP istisnaları listesine eklenmiştir (*gelişmiş ayarların [PUP İstisnaları](#) penceresinden yapılandırılır*)

- **Kilitli dosya - taranamayanlar** - ilgili nesne kilitlidir ve bu nedenle AVG tarafından taranamamaktadır
- **Potansiyel olarak tehlikeli nesne** - nesnenin potansiyel anlamda tehlikeli olduğu tespit edilmiş fakat nesneye herhangi bir virüs bulaşmamıştır (*örneğin makro içeriyor olabilir*); bilgi sadece uyarı amaçlıdır
- **Eylemi tamamlamak için bilgisayarınızın yeniden başlatılması gerekmektedir** - bulaşmış nesne silinememektedir ya da nesneyi tamamen silmek için bilgisayarınızın yeniden başlatılması gerekmektedir

Kontrol düğmeleri

Bu iletişim kutusunda kullanılabilir üç kontrol düğmesi var:

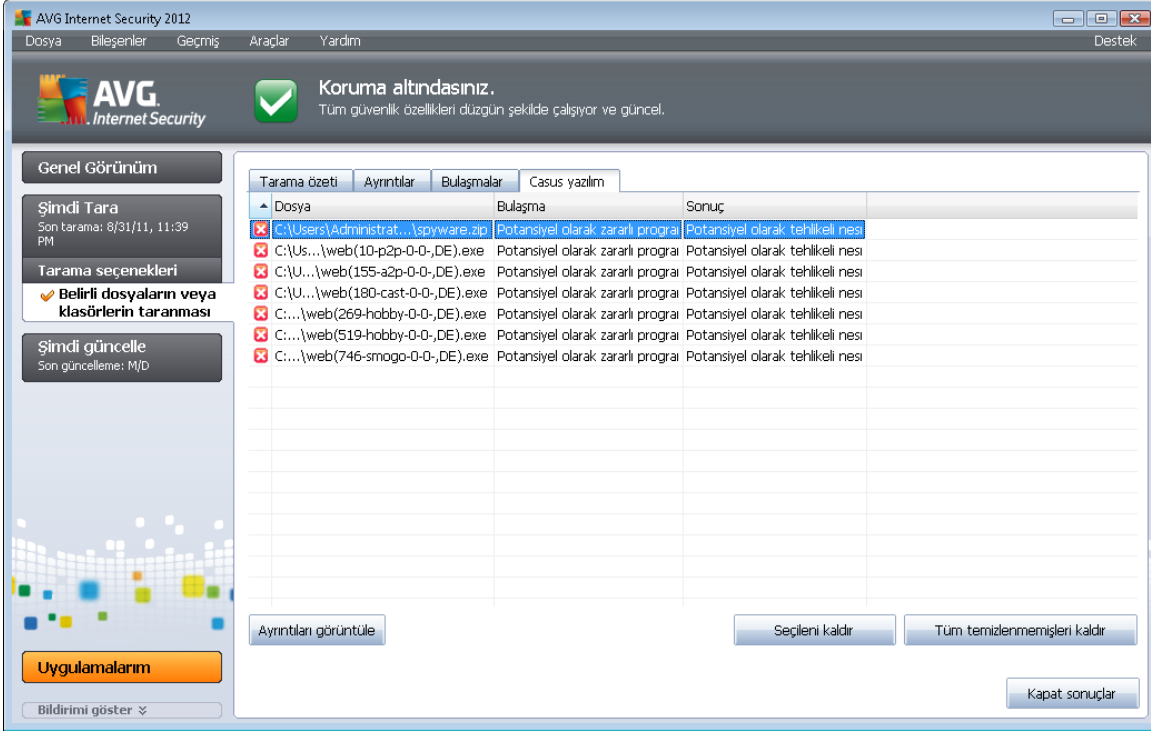
- **Ayrıntıları görüntüle** - düğme Ayrıntılı nesne bilgileri adlı yeni bir iletişim kutusu penceresi açar:



Bu iletişim kutusunda, tespit edilen bulaşıcı nesne ile ilgili ayrıntılı bilgiler bulabilirsiniz (örn. *bulaşmış nesnenin adı ve konumu, nesne tipi, SDK tipi, tespit sonucu ve tespit edilen nesne ile ilgili eylemlerin geçmişi*). **Geri İleri** düğmelerini kullanarak belirli bulgular hakkında ayrıntılı bilgi görüntüleyebilirsiniz. Bu iletişim kutusunu kapatmak için **Kapat** düğmesini tıklayın.

- **Seçileni kaldır** - seçili nesneyi [Virüs Kasası](#)
- **Temizlenmeyen tüm bulaşmaları sil** - bu düğme temizlenemeyen ya da [Virüs Kasası](#)
- **Sonuçları kapat** - ayrıntılı bilgi penceresini kapatır ve [Tarama sonuçlarına genel bakış](#) iletişim kutusuna döner

11.7.3. Casus Yazılım Sekmesi



Tarama özeti	Ayrıntılar	Bulaşmalar	Casus yazılım
	Dosya	Bulaşma	Sonuç
	C:\Users\Administrat...spyware.zip	Potansiyel olarak zararlı program	Potansiyel olarak tehlikeli nesne
	C:\Us...web(10-p2p-0-0-,DE).exe	Potansiyel olarak zararlı program	Potansiyel olarak tehlikeli nesne
	C:\U...web(155-a2p-0-0-,DE).exe	Potansiyel olarak zararlı program	Potansiyel olarak tehlikeli nesne
	C:\U...web(180-cast-0-0-,DE).exe	Potansiyel olarak zararlı program	Potansiyel olarak tehlikeli nesne
	C:...web(269-hobby-0-0-,DE).exe	Potansiyel olarak zararlı program	Potansiyel olarak tehlikeli nesne
	C:...web(519-hobby-0-0-,DE).exe	Potansiyel olarak zararlı program	Potansiyel olarak tehlikeli nesne
	C:...web(746-smogo-0-0-,DE).exe	Potansiyel olarak zararlı program	Potansiyel olarak tehlikeli nesne

Tarama sırasında bir casus yazılım tespit edilirse ilgili **Casus Yazılım** sekmesi sadece **Tarama Sonuçları** iletişim kutusunda görüntülenir. Sekme, şu bilgileri sağlayan üç bölüme ayrılmıştır:

- **Dosya** - bulaşmış nesnenin orijinal konumunun tam dizin yolu
- **Bulaşmalar** - tespit edilen casus yazılımın adı (*belirli virüs türleri hakkında ayrıntılı bilgi almak için lütfen çevrimiçi [Virüs Ansiklopedisine](#) bakın*)
- **Sonuç** - tarama sırasında tespit edilen nesnenin mevcut durumunu tanımlar:
 - **Bulaşanlar** - bulaşan nesne tespit edildi ve orijinal konumunda bırakıldı (örneğin belirli bir tarama işlemi sırasında otomatik temizleme seçeneğini devre dışı bıraktıysanız)
 - **Temizlenenler** - bulaşmış nesne otomatik olarak temizlenmiştir ve orijinal konumunda bırakılmıştır
 - **Virüs Kasasına Taşınanlar** - bulaşmış nesne [Virüs Kasası](#) karantinasına taşınmıştır
 - **Silinenler** - bulaşmış nesne silinmiştir
 - **PUP istisnalarına eklenenler** - bulgu bir istisna olarak değerlendirilmiş ve PUP istisnaları listesine eklenmiştir (gelişmiş ayarların [PUP İstisnaları](#) penceresinden yapılandırılır)
 - **Kilitli dosya - taranmayanlar** - ilgili nesne kilitlidir ve bu nedenle AVG tarafından

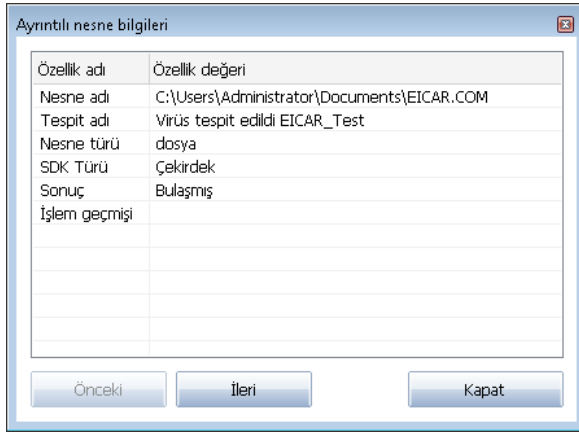
taranamamaktadır

- **Potansiyel olarak tehlikeli nesne** - nesnenin potansiyel anlamda tehlikeli olduğu tespit edilmiş fakat nesneye herhangi bir virüs bulaşmamıştır (örneğin makro içeriyor olabilir); bilgi sadece uyarı amaçlıdır
- **Eylemi tamamlamak için bilgisayarınızın yeniden başlatılması gerekmektedir** - bulaşmış nesne silinememektedir ya da nesneyi tamamen silmek için bilgisayarınızın yeniden başlatılması gerekmektedir

Kontrol düğmeleri

Bu iletişim kutusunda kullanılabilir üç kontrol düğmesi var:

- **Ayrıntıları görüntüle** - düğme Ayrıntılı nesne bilgileri adlı yeni bir iletişim kutusu penceresi açar:



Bu iletişim kutusunda, tespit edilen bulaşıcı nesne ile ilgili ayrıntılı bilgiler bulabilirsiniz (örn. *bulaşmış nesnenin adı ve konumu, nesne tipi, SDK tipi, tespit sonucu ve tespit edilen nesne ile ilgili eylemlerin geçmişi*). **Geri İleri** düğmelerini kullanarak belirli bulgular hakkında ayrıntılı bilgi görüntüleyebilirsiniz. Bu iletişim kutusunu kapatmak için **Kapat** düğmesini tıklayın.

- **Seçilene kaldır** - seçili nesneyi [Virüs Kasası](#)
- **Temizlenmeyen tüm bulaşmaları sil** - bu düğme temizlenemeyen ya da [Virüs Kasası](#)
- **Sonuçları kapat** - ayrıntılı bilgi penceresini kapatır ve [Tarama sonuçlarına genel bakış](#) iletişim kutusuna döner

11.7.4. Uyarılar Sekmesi

Uyarılar sekmesinde, tarama sırasında tespit edilip "şüpheli duyulan" nesnelere (*tipik olarak dosyalar*) hakkında çeşitli bilgiler görüntülenir. Yerleşik Kalkan tarafından tespit edildiği zaman tespit edilen dosyalara erişim engellenir. Bu şekilde tespit edilen buluntulardan bazıları gizli dosyalar, tanımlama bilgileri, şüpheli kayıt anahtarları, parola korumalı belgeler ya da arşivlerdir. Bu dosyalar



bilgisayarınıza ya da güvenliğinize karşı doğrudan tehlike teşkil etmez. Bu dosyalar hakkında verilen bilgiler, bilgisayarınızda reklam yazılımı ya da casus yazılım tespit edildiği durumlarda oldukça yararlıdır. Test sonuçlarında yalnızca **AVG Internet Security 2012** tarafından tespit edilen Uyarılar varsa, işlem yapmak gerekmez.

Aşağıda bu tür nesnelere ilişkin en yaygın örnekler kısaca açıklanmıştır:

- **Gizli dosyalar** - Gizli dosyalar, Windows'da varsayılan olarak görülmez durumdadır ve bazı virüsler ya da diğer tehditler dosyalarını söz konusu gizli dosyalara kaydederek algılanma ihtimallerini ortadan kaldırmaya çalışır. **AVG Internet Security 2012** zararlı olabileceğinden şüphelendiğiniz gizli bir dosya rapor ederse, bunu [Virüs Kasasına](#) taşıyabilirsiniz.
- **Tanımlama Bilgileri** - Tanımlama bilgileri, kullanıcılara ilişkin bilgileri kaydetmek ve daha sonra söz konusu bilgileri web site şablonlarını yükleme ve kullanıcı adını girmek üzere web siteleri tarafından kullanılan düz metin dosyalarıdır.
- **Şüpheli kayıt anahtarları** - Bazı kötü amaçlı yazılımlar, sistem başlatıldığında yüklendiğinden emin olmak ya da işletim sistemi üzerindeki etkisini artırmak üzere bilgilerini Windows kayıt defterine kaydeder.

11.7.5. Rootkit'ler Sekmesi

Rootkit'ler sekmesi, siz [Anti-Rootkit taraması](#)'nı başlattıysanız tarama sırasında algılanan rootkit'ler hakkında bilgi görüntüler.

[Rootkit](#), sistem yöneticisinin izni olmaksızın yasal olmayan şekillerde bilgisayar sisteminin kontrolünü ele almak için tasarlanmış bir programdır. Kök izin, donanım üzerinde çalışan işletim sisteminin kontrolünü ele geçirmeyi hedeflediği için donanımsal açıdan erişime gerek duymaz. Kök dizinler genellikle standart işletim sisteminin güvenlik mekanizmalarını dönüştürerek ya da istila ederek sistem üzerindeki varlıklarını gizlerler. Çoğunlukla Truva Atı biçimindedirler, dolayısıyla kullanıcıları sistemleri üzerinden çalışacak kadar güvenli olduklarına inandırır. İzleme programlarının çalışan işlemlerini gizlemek ya da işletim sisteminin sistem bilgilerini ya da dosyalarını saklamak, bunu sağlamak için kullanılan teknikler arasında bulunmaktadır.

Bu sekmenin yapısı temel olarak [Bulaşmalar sekmesi](#) ya da [Casus Yazılım sekmesi](#) ile aynıdır.

11.7.6. Bilgi Sekmesi

Bilgi sekmesinde, bulaşma ya da casus yazılım şeklinde sınıflandırılmayan "buluntular" hakkında bilgi bulunmaktadır. Bunlar tehlikeli şekilde etiketlenebilir ancak söz konusu öğeler hususunda dikkatli olmalısınız. **AVG Internet Security 2012** taraması, virüs bulaşmamış ancak şüpheli dosyaları tespit edebilir. Bu dosyalar [Uyarı](#) veya Bilgi olarak rapor edilir.

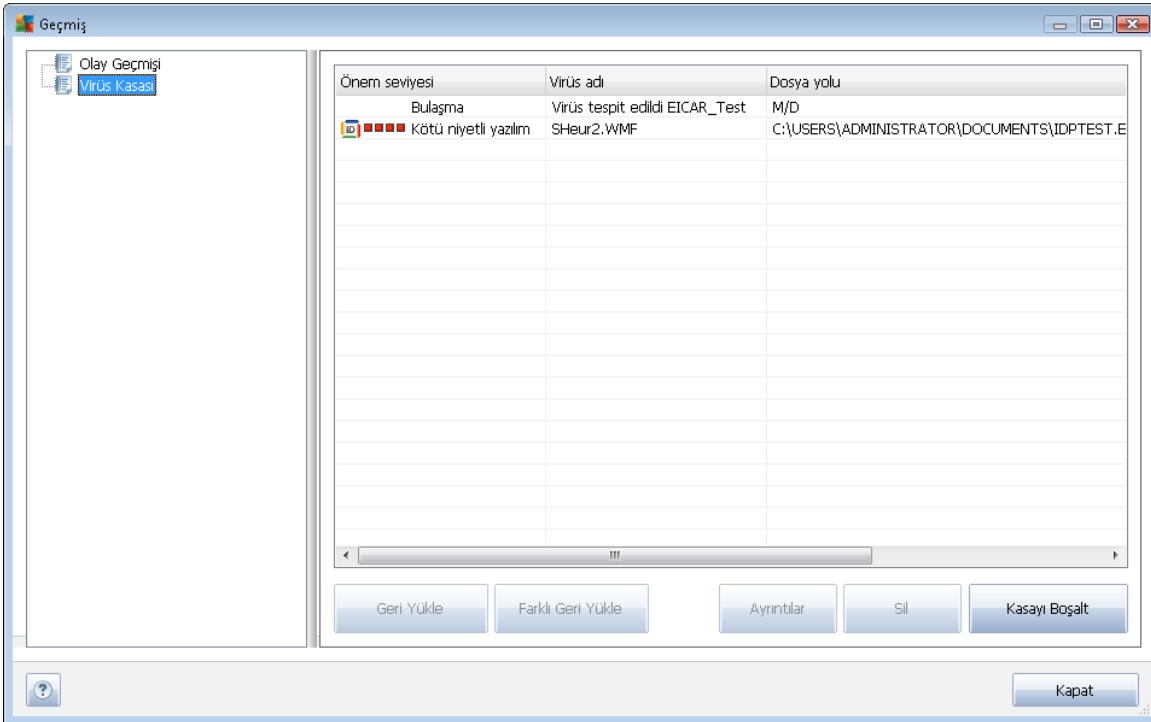
Önem derecesi **Bilgiler** aşağıdaki nedenlerden birine bağlı olarak rapor edilebilir:

- **Çalışma zamanı paketli** - Dosya, dosyanın taranmasını önleme çabası olarak değerlendirilebilecek yaygın olmayan paketleyicilerinden biri kullanılarak paketlenmiştir. Diğer bir yandan bu tür dosyalar her rapor edildiğinde virüs teşkil etmezler.
- **Çalışma zamanı paketi yinelemeli** - Yukarıdakine benzerdir, ancak yaygın yazılımlar arasında nispeten daha az sıklıkta kullanılır. Söz konusu dosyalar şüphelidir ve kaldırılmaları ya da incelenmeleri için bize gönderilmeleri göz önünde bulundurulmalıdır.



- **Parola ile korunan arşiv ya da belge** - Parola ile korunan dosyalar, **AVG Internet Security 2012** (ya da genellikle diğer kötü amaçlı yazılımlara karşı koruma programları) tarafından taranamaz.
- **Makro içeren belge** - Rapor edilen belge, zararlı olabilecek makrolar içermektedir.
- **Gizli uzantı** - Gizli uzantılı dosyalar resimler gibi görünebilir, ancak aslında çalıştırılabilir dosyalar olabilir (örn. *resim.jpg.exe*). İkinci uzantı, varsayılan olarak Windows'da görünür değildir ve **AVG Internet Security 2012** yanlışlıkla açılmalarını engellemek için bu tür dosyaları rapor eder.
- **Uygun olmayan dosya yolu** - Önemli bir sistem dosyası varsayılan yoldan başka bir yerden çalışıyorsa (örn. *winlogon.exe* Windows klasöründen başka bir yerde çalışıyorsa) bu durumu rapor eder. **AVG Internet Security 2012** Bazı durumlarda virüsler, sistemde fark edilmemek için standart sistem işlemlerinin adını alır.
- **Kilitli dosya** - Rapor edilen dosya kilitli, bu yüzden **AVG Internet Security 2012** tarafından taranamıyor. Bu, genellikle bir dosyanın sistem tarafından kullanılmakta olduğu anlamına gelir (örn. *takas dosyası*).

11.8. Virüs Kasası



Virüs Kasası AVG taramaları sırasında tespit edilen şüpheli/bulaşmış nesnelerin yönetilmesi için güvenli bir ortamdır. Tarama sırasında bulaşmış bir nesne tespit edildikten sonra AVG, söz konusu bulaşmayı otomatik olarak temizleyemiyorsa şüpheli nesne hakkında ne yapmak istediğiniz sorulur. Önerilen çözüm, nesneyi daha sonra ilgilenmek üzere **Virüs Kasasına** taşımaktır. **Virüs Kasası**'nı satın almanın ana amacı silinen bir dosyayı belirli bir süre için saklamasıdır, böylece dosyayı orijinal



konumunda artık istemediğinizden emin olabilirsiniz. Dosyanın yokluğu sorun oluşturuyorsa, bu dosyayı analize gönderebilir veya orijinal konumuna geri yükleyebilirsiniz.

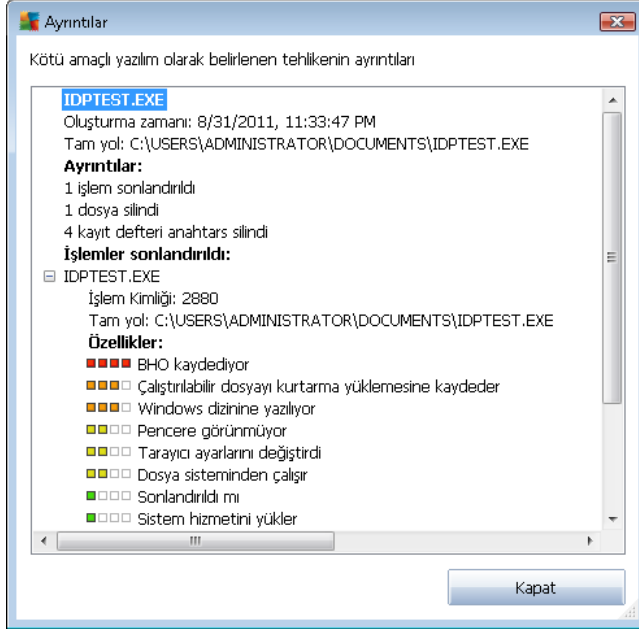
Virüs Kasası arayüzü, yeni bir pencerede açılır ve karantina altındaki bulaşmış nesnelere hakkında genel bilgi içerir:

- **Önem Düzeyi** - **AVG Internet Security 2012** uygulamanızın içine [Kimlik Koruma](#) bileşenini yüklemeye karar verdiğinizde, ilgili tehdidin önem seviyesinin kusursuzdan (■□□□) çok tehlikeliye kadar (■□□■) dört seviyeli bir ölçekte grafik olarak gösterimi ve bulaşma türü hakkındaki bilgiler (*bulaşma seviyesine bağlı olarak - listelenen tüm nesnelere virüs bulaşmıştır veya bulaşma olasılığı vardır*)
- **Virüs Adı** - [Virüs Ansiklopedisi](#)'ne göre (*çevrimiçi*) tespit edilen bulaşmanın adını görüntüler
- **Dosya yolu** - Bulaşmış dosyanın orijinal konumuna giden tam yol
- **Orijinal nesne adı** - Tabloda listelenmekte olan tespit edilmiş nesnelere, tarama işlemi sırasında AVG tarafından verilen standart isim ile etiketlenmiştir. Nesnenin bilinmeyen farklı bir adı olması halinde (*Örn. bir e-posta ekinin adının ekin mevcut içeriğine yanıt vermemesi halinde*), söz konusu isim bu sütunda gösterilecektir.
- **Saklama tarihi** - Şüpheli dosyanın tespit edildiği ve Virüs Kasası'na kaldırıldığı tarih ve saat

Kontrol düğmeleri

Virüs Kasası arayüzünden ulaşabileceğiniz kontrol düğmeleri şunlardır:

- **Geri Yükle** - bulaşmış dosyayı sabit diskinizdeki orijinal konumuna geri yükler
- **Farklı Geri Yükle** - bulaşmış dosyayı seçili klasöre taşır
- **Ayrıntılar** - bu düğme yalnızca [Identity Protection](#) tarafından algılanan tehlikeler içindir. Tıklatıldığında, tehlike ayrıntılarının özet genel görünümünü görüntüler (*hangi dosyalar/ işlemler etkilendi, işlemin özellikleri vb.*). IDP'nin algıladığı dışındaki diğer tüm öğeler için, bu düğmenin gri ve devre dışı olduğunu unutmayın!



- **Sil** - bulaşmış dosyayı **Virüs Kasasından** tamamen ve geri dönüştürülemez şekilde siler
- **Kasayı Boşalt** - **Virüs Kasası** içeriğini tamamen temizler. Dosyaları **Virüs Kasası**'ndan kaldırdığınızda, bu dosyalar diskten geri alınmayacak biçimde kaldırılır (**Geri Dönüşüm Kutusu'na taşınmaz**).



12. AVG Güncellemeleri

Güvenlik yazılımlarının hiçbiri, rutin olarak güncellenmediği takdirde sizi çeşitli tehlikelere karşı korumayı garanti edemez! Virüs yazarları, yazılım ve işletim sistemlerinde yararlanabilecekleri güvenlik açıkları aramaktadır. Her gün yeni virüsler, yeni kötü amaçlı yazılımlar ve yeni bilgisayar saldırıları gerçekleştirilmektedir. Bu nedenle yazılım geliştiricileri, tespit edilen güvenlik açıklarını kapatmak üzere devamlı olarak güncellemeler ve güvenlik paketleri yayınlamaktadır.

Yeni ortaya çıkan tehditler ve bunların yayılma hızı dikkate alındığında **AVG Internet Security 2012** ürününüzü düzenli olarak güncellemek hayati bir önem kazanır. En iyi çözüm, otomatik güncellemenin yapılandırıldığı program varsayılan ayarlarına güvenmektir. **AVG Internet Security 2012** ürününüzün virüs veritabanı güncel değilse, programın en yeni tehditleri tespit edemeyeceğini lütfen unutmayın!

AVG'nizi rutin olarak güncellemeniz çok önemlidir! Gerekli virüs tanımı güncellemelerinin mümkün ise her gün yapılması gerekmektedir. Daha az önem taşıyan program güncellemeleri haftada bir yapılabilir.

12.1. Güncelleme başlatma

Mümkün olan en yüksek güvenliği sağlamak için, **AVG Internet Security 2012** varsayılan olarak her dört saatte bir yeni güncellemeleri kontrol etmeye ayarlanmıştır. AVG güncellemeleri belirli bir takvime göre değil yeni tehditlerin miktarı ve ciddiyetine göre yayınlandığından, bu kontrol AVG virüs veritabanınızın sürekli güncel tutulması açısından çok önemlidir.

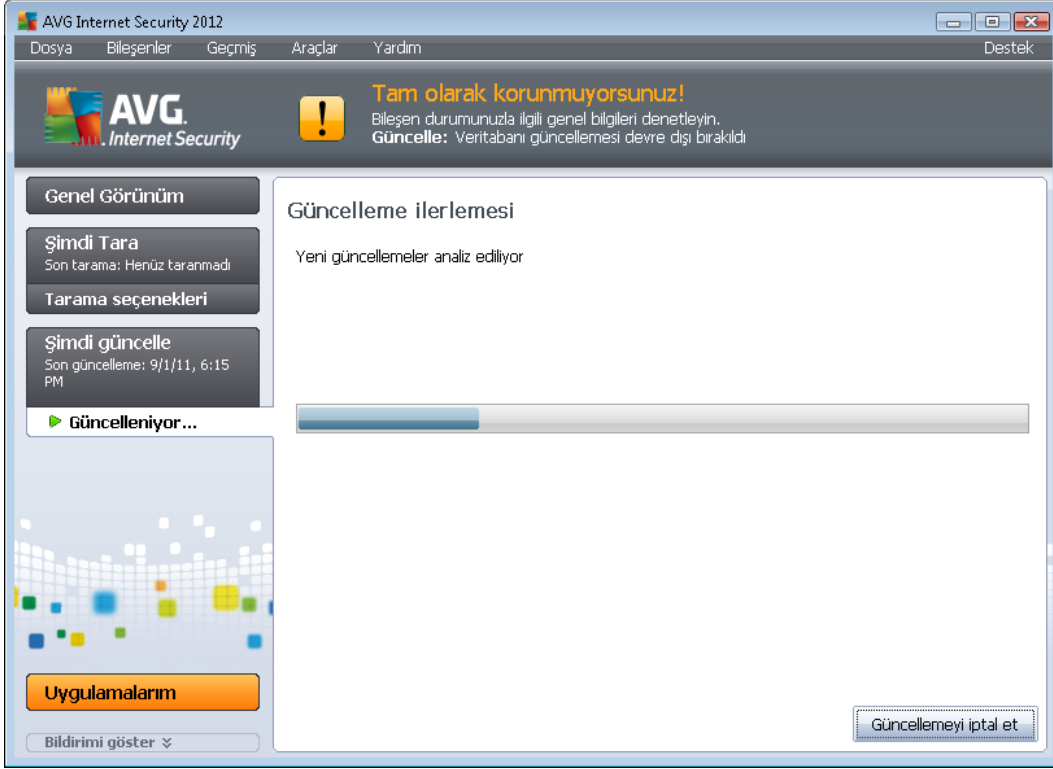
Güncelleme başlatmalarının sayısını azaltmak istiyorsanız, kendi güncelleme başlatma parametrelerinizi ayarlayabilirsiniz. Ancak, günde en az bir kez güncellemeyi başlatmanız kesinlikle önerilir! Yapılandırma [Gelişmiş ayarlar/Programlar](#) bölümünde, aşağıdaki iletişim kutularından düzenlenebilir:

- [Güncelleme planı tanımlamalar](#)
- [Program güncelleme programı](#)
- [Anti-Spam güncelleme programı](#)

Yeni güncelleme dosyalarını hemen kontrol etmek istiyorsanız, ana kullanıcı arayüzündeki [Şimdi güncelle](#) hızlı bağlantısını kullanın. Bu bağlantıya her zaman herhangi bir [kullanıcı arayüzü](#) iletişim kutusundan ulaşabilirsiniz.

12.2. Güncelleme ilerlemesi

Güncellemeye başladıktan sonra AVG, yeni güncelleme dosyasının olup olmadığını aramaya başlayacaktır. Varsa, **AVG Internet Security 2012** dosya ve güncellemeleri indirmeye başlar ve güncelleme işlemini kendisi başlatır. Güncelleme işlemi sırasında güncelleme işleminin ilerleyişinin yanı sıra ilgili istatistik parametreleri de görüntüleyebileceğiniz **Güncelleme** arayüzüne yeniden yönlendirileceksiniz (*güncelleme dosyasının boyutu, alınan veriler, indirme hızı, kalan süre...*):



Not: Her AVG program güncellemesi başlatılmadan önce sistem geri yükleme noktası oluşturulur. Güncelleme işleminin başarısız olması ve işletim sisteminizin çökmesi halinde işletme sisteminizi bu noktaya geri döndürebilirsiniz. Seçeneğe Windows menüsü yoluyla erişilebilir: Başlat / Tüm Programlar / Aksesuarlar / Sistem araçları / Sistem Geri Yükleme. Yalnızca deneyimli kullanıcılara önerilir!

12.3. Güncelleme Seviyeleri

AVG Internet Security 2012 seçilebilecek iki güncelleme düzeyi sunar:

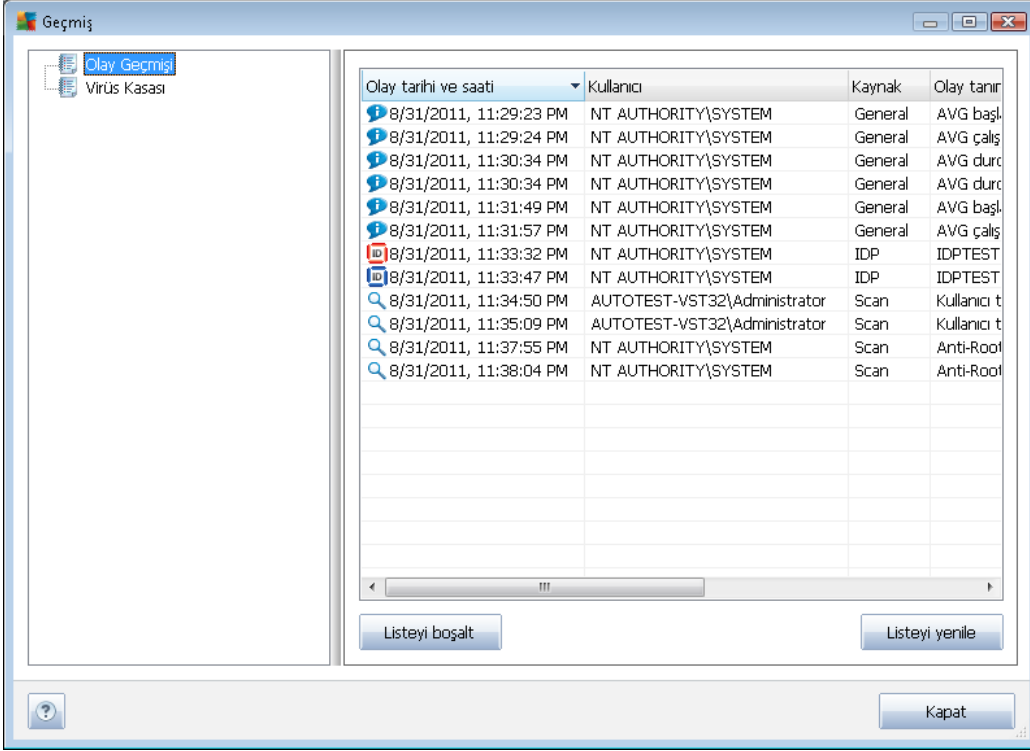
- **Tanım güncellemeleri** güvenilir virüsten koruma, istenmeyen posta önleme ve kötü amaçlı yazılımlara karşı koruma için gerekli değişiklikleri içerir. Genellikle kodu değiştirmez ve yalnızca tanımlama veritabanını günceller. Bu güncelleme sunulur sunulmaz yüklenmelidir.
- **Program güncellemeleri** çeşitli program değişikliklerini, onarımları ve iyileştirmeleri içerir.

Bir [güncelleme programlarken](#), her iki güncelleme düzeyi için de belirli parametreler tanımlamak mümkündür:

- [Güncelleme planı tanımlamalar](#)
- [Program güncelleme programı](#)

Not: Programlanmış bir program güncellemesinin zaman çakışması oluşursa ve programlı tarama gerçekleşirse, güncelleme işlemi daha yüksek önceliğe sahiptir ve tarama kesilir.

13. Olay Geçmişi



Olay tarihi ve saati	Kullanıcı	Kaynak	Olay tanımı
8/31/2011, 11:29:23 PM	NT AUTHORITY\SYSTEM	General	AVG başl.
8/31/2011, 11:29:24 PM	NT AUTHORITY\SYSTEM	General	AVG çalış
8/31/2011, 11:30:34 PM	NT AUTHORITY\SYSTEM	General	AVG durd
8/31/2011, 11:30:34 PM	NT AUTHORITY\SYSTEM	General	AVG durd
8/31/2011, 11:31:49 PM	NT AUTHORITY\SYSTEM	General	AVG başl.
8/31/2011, 11:31:57 PM	NT AUTHORITY\SYSTEM	General	AVG çalış
8/31/2011, 11:33:32 PM	NT AUTHORITY\SYSTEM	IDP	IDPTEST
8/31/2011, 11:33:47 PM	NT AUTHORITY\SYSTEM	IDP	IDPTEST
8/31/2011, 11:34:50 PM	AUTOTEST-VST32\Administrator	Scan	Kullanıcı t
8/31/2011, 11:35:09 PM	AUTOTEST-VST32\Administrator	Scan	Kullanıcı t
8/31/2011, 11:37:55 PM	NT AUTHORITY\SYSTEM	Scan	Anti-Rooft
8/31/2011, 11:38:04 PM	NT AUTHORITY\SYSTEM	Scan	Anti-Rooft

Geçmiş iletişim kutusuna [sistem menüsü](#) üzerinden **Geçmiş/Olay Geçmişi Günlüğü** ögesi aracılığıyla ulaşabilirsiniz. Bu iletişim kutusunda, **AVG Internet Security 2012** uygulamasının çalışması sırasında oluşan önemli olayların bir özetini bulabilirsiniz. **Geçmiş** aşağıdaki etkinlik türlerini kaydeder:

- AVG uygulamasının güncellemeleri hakkında bilgi
- Tarama başlangıcı, sonu veya taramanın durdurulması hakkında bilgi (*otomatik olarak gerçekleştirilen taramalar dahil olmak üzere*)
- Olay konumu da dahil olmak üzere virüs tespitine bağlı olaylar hakkında bilgi ([Yerleşik Kalkan](#) veya [tarama](#) ile)
- Diğer önemli olaylar

Her olay için, şu bilgiler listelenir:

- **Olay tarihi ve zamanı** olayın gerçekleştiği kesin tarihi ve zamanı belirtir
- **Kullanıcı** olayın gerçekleştiği sırada oturum açmış olan kullanıcının adını gösterir
- **Kaynak**, kaynak bileşeni veya AVG sisteminin olayı tetikleyen bölümü hakkında bilgi verir
- **Olay açıklaması**, tam olarak ne olduğu hakkında kısa bir açıklama sağlar



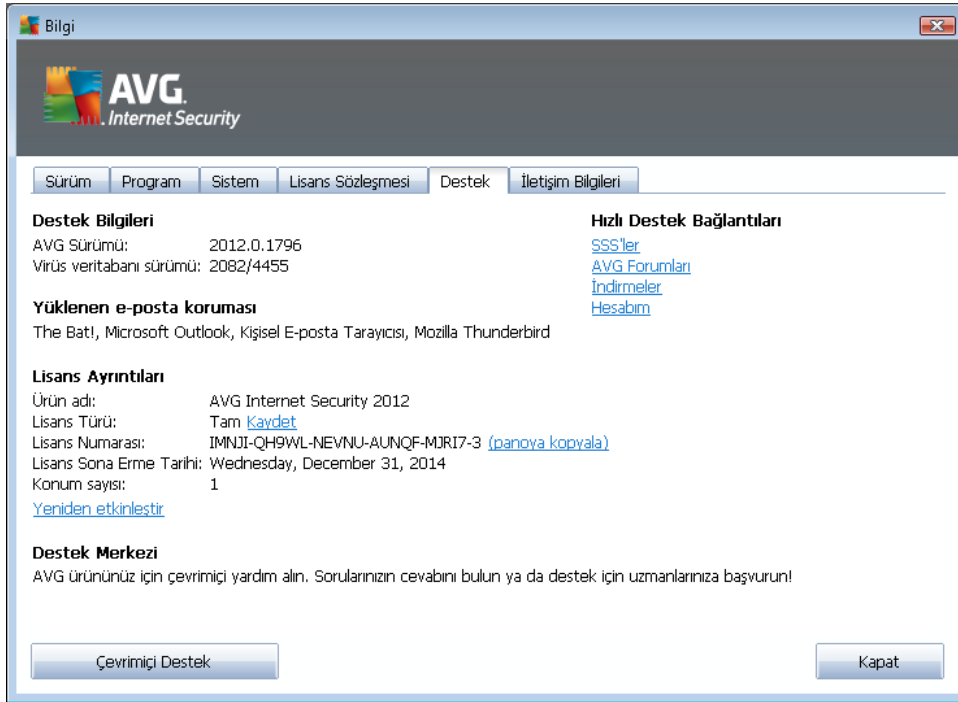
Kontrol düğmeleri

- **Listeyi boşalt** - olaylar listesindeki tüm girişleri silmek için bu düğmeye basın
- **Listeyi yenile** - olaylar listesindeki tüm girişleri güncellemek için bu düğmeye basın

14. SSS ve Teknik Destek

AVG Internet Security 2012 uygulamanızın satışıyla ilgili veya teknik sorunlarınız olması durumunda yardım için birçok yol mevcuttur. Lütfen aşağıdaki seçeneklerden birini seçin:

- **Müşteri desteği ile irtibat kurun:** Doğrudan AVG uygulamanız içinden profesyonel müşteri desteğimiz ile irtibat kurabilirsiniz. 7/24 AVG müşteri desteğiyle irtibat kurmak üzere çevrimiçi iletişim formuna yönlendirilmek için **Yardım / Çevrimiçi Yardım AI** ana menü öğesini seçin. Lisans numaranız otomatik olarak doldurulur. Devam etmek için lütfen web sayfasındaki talimatları izleyin.
- **Destek (ana menü bağlantısı):** AVG uygulama menüsünde (*ana kullanıcı arayüzünün en üstünde*) yardım bulmaya çalışırken ihtiyacınız olabilecek tüm bilgileri içeren yeni bir iletişim kutusu açan **Destek** bağlantısı bulunur. İletişim kutusunda kurulu AVG programınız (*program / veritabanı sürümü*) ile ilgili temel bilgiler, lisans ayrıntıları ve hızlı destek bağlantıları listesi bulunur:



- **Yardım dosyasında sorun giderme:** Doğrudan **AVG Internet Security 2012** yardım dosyasından erişilebilen yeni bir **Sorun giderme** bölümü mevcuttur. Bu bölüm, bir kullanıcı teknik bir sorun hakkında profesyonel yardım aradığında en sık karşılaşılan durumlar hakkında bir liste sunar. Lütfen sizin sorununuzu en iyi açıklayan durumu seçin ve sorunun çözümüne dair ayrıntılı talimatlar almak için tıklatın.
- **AVG web sitesi Destek Merkezi:** Sorunuzun çözümünü AVG web sitesinde de (<http://www.avg.com/>) arayabilirsiniz. **Destek Merkezi** bölümünde hem satış sorunları hem de teknik sorunlarla ilgili tematik olarak gruplandırılmış konular bulabilirsiniz.
- **Sık sorulan sorular:** AVG web sitesinde (<http://www.avg.com/>) ayrı ve çok ayrıntılı bir sık sorulan sorular bölümü de bulabilirsiniz. Bu bölüme **Destek Merkezi / SSS** menü



seçeneğinden erişilebilir. Burada da tüm sorular satış, teknik ve virüs kategorileri şeklinde sınıflandırılmıştır.

- **Virüsler ve tehlikeler hakkında:** Virüs sorunlarına ayrılmış özel bir AVG web sitesi (<http://www.avg.com/>) bölümü. Çevrimiçi tehlikeler hakkında sınıflandırılmış bilgiler sunan bir sayfaya girmek için menüde **Destek Merkezi / Virüsler ve tehlikeler hakkında** ögesini tıklatın. Virüs, casus yazılım silme talimatları ve nasıl güvenli kalacağınıza dair öneriler de bulabilirsiniz.
- **Tartışma forumu:** Ayrıca <http://forums.avg.com> adresindeki AVG kullanıcıları tartışma forumunu kullanabilirsiniz.