



AVG Anti-Virus

Kullanıcı Kılavuzu

Belge revizyonu 2011.21 (16.5.2011)

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 libbzip2 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 Seçenekleri	9
4. AVG Yükleme Süreci	10
4.1 Hoş geldiniz	10
4.2 AVG lisansınızı etkinleştirin	11
4.3 Yükleme türünü seçin	12
4.4 Özel seçenekler	13
4.5 AVG Security Toolbar'ı yükle	14
4.6 Yükleme ilerlemesi	15
4.7 Yükleme başarılı oldu	15
5. Yüklemeden Sonra	17
5.1 Ürün kaydı	17
5.2 Kullanıcı arayüzüne erişim	17
5.3 Tüm bilgisayarın taranması	17
5.4 Eicar testi	17
5.5 AVG varsayılan yapılandırması	18
6. AVG Kullanıcı Arayüzü	19
6.1 Sistem Menüsü	20
6.1.1 Dosya	20
6.1.2 Bileşenler	20
6.1.3 Geçmiş	20
6.1.4 Araçlar	20
6.1.5 Yardım	20
6.2 Güvenlik Durumu Bilgisi	22
6.3 Hızlı Bağlantılar	23
6.4 Bileşen Genel Görünümü	24
6.5 İstatistikler	25
6.6 Sistem Tepsisi Sembolü	25
6.7 AVG gadget'ı	26

7. AVG Bileşenleri	29
7.1 Virüsten Koruma	29
7.1.1 Virüsten Koruma İlkeleri	29
7.1.2 Virüsten Koruma Arayüzü	29
7.2 Casus Yazılımdan Koruma	30
7.2.1 Casus Yazılımdan Koruma Prensipleri	30
7.2.2 Casus Yazılımdan Koruma Arayüzü	30
7.3 Bağlantı Tarayıcı	32
7.3.1 Link Scanner Prensipleri	32
7.3.2 Link Scanner Arayüzü	32
7.3.3 Arama Kalkanı	32
7.3.4 Surf-Shield	32
7.4 Yerleşik Kalkan	35
7.4.1 Yerleşik Kalkan İlkeleri	35
7.4.2 Yerleşik Kalkan Arayüzü	35
7.4.3 Yerleşik Kalkan Tespiti	35
7.5 Aile Güvenliği	40
7.6 AVG LiveKive	40
7.7 E-Posta Tarayıcısı	40
7.7.1 E-posta Tarayıcısı Prensipleri	40
7.7.2 E-posta Tarayıcısı Arayüzü	40
7.7.3 E-posta Tarayıcısı Tespiti	40
7.8 Güncelleme Yöneticisi	44
7.8.1 Güncelleme Yöneticisi Prensipleri	44
7.8.2 Güncelleme Yöneticisi Arayüzü	44
7.9 Lisans	46
7.10 Uzaktan Yönetim	47
7.11 Online Shield	48
7.11.1 Online Shield İlkeleri	48
7.11.2 Online Shield Arayüzü	48
7.11.3 Online Shield Algılaması	48
7.12 Anti-Rootkit	51
7.12.1 Anti-Rootkit Prensipleri	51
7.12.2 Rootkit Önleme Arayüzü	51
7.13 PC Analyzer	52
7.14 Kimlik Koruması	54
7.14.1 Kimlik Koruması Prensipleri	54

7.14.2 Kimlik Koruması Arayüzü	54
7.15 Güvenlik Araç Çubuğu	56
8. AVG Security Toolbar	58
8.1 AVG Security Toolbar Arayüzü	58
8.1.1 AVG logosu düğmesi	58
8.1.2 AVG Secure Search (powered by Google) tarafından desteklenen arama kutusu ..	58
8.1.3 Sayfa Durumu	58
8.1.4 AVG Haberleri	58
8.1.5 Haberler	58
8.1.6 Geçmiş sil	58
8.1.7 E-posta Bildiricisi	58
8.1.8 Hava Durumu Bilgileri	58
8.1.9 Facebook	58
8.2 AVG Security Toolbar Seçenekleri	65
8.2.1 Genel Sekmesi	65
8.2.2 Yararlı Düğmeler Sekmesi	65
8.2.3 Güvenlik Sekmesi	65
8.2.4 Gelişmiş Seçenekler Sekmesi	65
9. AVG Gelişmiş Ayarlar	69
9.1 Görünüm	69
9.2 Sesler	71
9.3 Hatalı Durumları Yoksay	73
9.4 Virüs Kasası	74
9.5 PUP İstisnaları	74
9.6 Online Shield	77
9.6.1 Web Koruması	77
9.6.2 Anlık Mesajlaşma	77
9.7 Bağlantı Tarayıcı	81
9.8 Taramalar	82
9.8.1 Tüm Bilgisayarı Tara	82
9.8.2 Kabuk Uzantısı Tarama	82
9.8.3 Belirli Dosyaları veya Klasörleri Tara	82
9.8.4 Çıkarılabilir Aygıt Tarama	82
9.9 Programlar	87
9.9.1 Programlı Tarama	87
9.9.2 Virüs Veritabanı Güncelleme Programı	87
9.9.3 Program Güncelleme Planı	87

9.10 E-Posta Tarayıcısı	97
9.10.1 Sertifika	97
9.10.2 Posta Filtreleme	97
9.10.3 Sunucular	97
9.11 Yerleşik Kalkan	105
9.11.1 Gelişmiş Ayarlar	105
9.11.2 Hariç tutulan öğeler	105
9.12 Önbellek Sunucusu	109
9.13 Kök Kullanıcı Takımlarına Karşı Koruma (Anti-Rootkit)	110
9.14 Güncelleme	111
9.14.1 Proxy	111
9.14.2 Çevirmeli	111
9.14.3 URL	111
9.14.4 Yönetme	111
9.15 AVG korumasını geçici olarak devre dışı bırak	118
9.16 Ürün Geliştirme Programı	118
10. AVG Tarama	121
10.1 Tarama Arayüzü	121
10.2 Öntanımlı Taramalar	122
10.2.1 Tüm Bilgisayarın Taranması	122
10.2.2 Belirli Dosyaları veya Klasörleri Tara	122
10.2.3 Anti-Rootkit Tarama	122
10.3 Windows Gezgini'nde Tarama	132
10.4 Komut Satırı Tarama	133
10.4.1 CMD Tarama Parametreleri	133
10.5 Tarama Planlama	135
10.5.1 Program Ayarları	135
10.5.2 Tarama Şekli	135
10.5.3 Taranacaklar	135
10.6 Tarama Sonuçları Genel Görünümü	145
10.7 Tarama Sonuçları Ayrıntıları	146
10.7.1 Sonuçlara Genel Bakış Sekmesi	146
10.7.2 Bulaşma Sekmesi	146
10.7.3 Casus Yazılım Sekmesi	146
10.7.4 Uyarılar Sekmesi	146
10.7.5 Rootkit'ler Sekmesi	146
10.7.6 Bilgi Sekmesi	146



10.8 Virüs Kasası	153
11. AVG Güncellemeleri	156
11.1 Güncelleme Seviyeleri	156
11.2 Güncelleme Türleri	156
11.3 Güncelleme İşlemi	156
12. Olay Geçmişi	158
13. SSS ve Teknik Destek	160



1. Giriş

Bu kullanıcı el kitabı, **AVG Anti-Virus** için kapsamlı dokümantasyon sağlar.

AVG Anti-Virus programını satın aldığınız için tebrik ederiz!

AVG Anti-Virus PC'niz için tam güvenlik ve rahatlık sağlamak üzere tasarlanmış ödüllü AVG ürünlerinden biridir. Diğer tüm AVG ürünlerinde olduğu gibi, AVG'nin ünlü ve ödüllü güvenlik korumasını kullanımı daha kolay ve daha verimli biçimde sunmak adına **AVG Anti-Virus** ürünü de baştan sona yeniden tasarlanmıştır. Yeni **AVG Anti-Virus** ürününüz daha agresif ve daha hızlı taramayı bir araya getiren akıcı bir arayüze sahiptir. Güvenliğiniz için daha fazla sayıda güvenlik özelliği otomatik hale getirilmiştir ve yeni 'akıllı' kullanıcı seçenekleri sayesinde gerekli ayarlamaları kendi güvenlik ihtiyaçlarınız doğrultusunda yapabilirsiniz. Artık güvenliğinizden ödün vermek yok!

AVG, bilişim ve ağ kurma faaliyetlerinizi korumak için tasarlanmış ve geliştirilmiştir. AVG'nin sağladığı eksiksiz korumanın tadını çıkartın.

Tüm AVG ürünlerinin sundukları

- Bilgisayarınızı ve İnterneti kullanma şeklinizle ilgili koruma: bankacılık ve alışveriş, internette gezinme ve arama yapma, sohbet etme ve e-posta gönderip alma veya dosya indirme ve sosyal ağlara bağlanma. Yani AVG'de size uygun bir koruma ürünü vardır.
- Tüm dünyada 110 milyondan fazla kullanıcının güvendiği ve çok deneyimli araştırmacıların desteklediği sorunsuz koruma
- 24 saat uzman desteği alan koruma



2. AVG Yükleme Gereksinimleri

2.1. Desteklenen İşletim Sistemleri

AVG Anti-Virus 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 Anti-Virus yazılımını yalnızca Kimlik Koruma (IDP) bileşeni olmaksızın yükleyebilirsiniz.

2.2. Minimum ve Önerilen Donanım Gereksinimleri

AVG Anti-Virus için minimum donanım gereksinimleri:

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

AVG Anti-Virus için önerilen donanım gereksinimleri:

- Intel Pentium CPU 1,8 GHz
- 512 MB RAM bellek
- 1400 MB boş sabit disk alanı (yükleme için)



3. AVG Yükleme Seçenekleri

AVG, yükleme CD'niz üzerinde bulunan yükleme dosyasından yüklenebilir veya en güncel yükleme dosyasını AVG'nin web sitesinden (<http://www.avg.com/>) indirebilirsiniz.

AVG'yi yüklemeye başlamadan önce yeni yükleme dosyasını kontrol etmek için AVG web sitesini (<http://www.avg.com/>) ziyaret etmenizi önemle öneririz. Bu şekilde, en güncel AVG Anti-Virus sürümünü yüklediğinizden emin olabilirsiniz.

Yükleme işlemi sırasında lisans/satış numaranızı girmeniz istenecektir. Yüklemeye başlamadan önce söz konusu numarayı hazırladığınızdan emin olun. Satış numarası, CD ambalajı üzerinde bulunabilir. AVG'yi çevrimiçi mağazadan satın aldıysanız lisans numaranız e-posta aracılığıyla gönderilecektir.



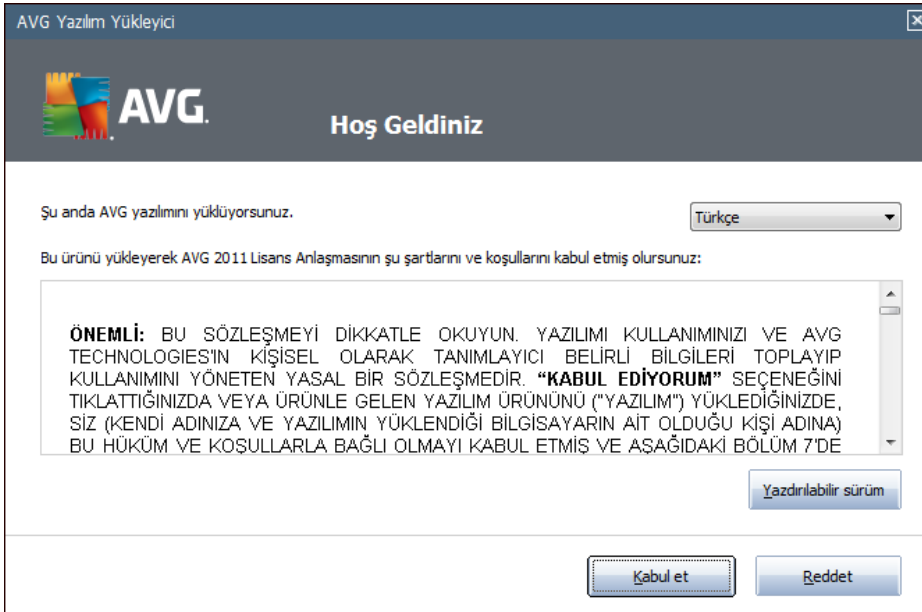
4. AVG Yükleme Süreci

Bilgisayarınıza **AVG Anti-Virus** programını yüklemek için, en güncel yükleme dosyasını edinmeniz gerekir. Kutulu versiyonların içinden çıkan CD'de bulunan yükleme dosyasını da kullanabilirsiniz fakat söz konusu dosya güncel olmayabilir. Bu nedenle en güncel kurulum dosyasını çevrimiçi ortamdan indirmenizi öneriyoruz. Dosyayı AVG web sitesinden (<http://www.avg.com/>), [Destek Merkezi / İndir](#) kısmından indirebilirsiniz.

Yükleme işlemi, her adımda neler yapmanız gerektiğine dair kısa tanımlamalar içeren bir dizi iletişim kutusu pencerelerinden oluşur. Aşağıda iletişim kutularının her biri için kısa bir açıklama sunuyoruz:

4.1. Hoş geldiniz

Yükleme süreci **Hoş geldiniz** iletişim penceresiyle başlar. Burada, yükleme süreci için kullanılacak dili ve AVG kullanıcı arayüzünün varsayılan dilini seçebilirsiniz. İletişim penceresinin üst bölümünde, seçim yapabileceğiniz aşağı açılır menü listesini bulabilirsiniz:



Dikkat: Bu bölümde, yükleme sürecinin dilini seçmekte olduğunuzu unutmayın. Seçtiğiniz dil, otomatik olarak yüklenen İngilizce dille birlikte AVG kullanıcı arayüzünün varsayılan dili olarak yüklenecektir. Kullanıcı arayüzü için daha fazla dil yüklenmesini istiyorsanız, lütfen bu dilleri [Özel Seçenekler](#) adı verilen şu ayarlama iletişim kutularından birinde tanımlayın.

Ayrıca, bu iletişim kutusu AVG lisans sözleşmesinin tam metnini de sağlar. 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.



4.2. AVG lisansınızı etkinleştirin

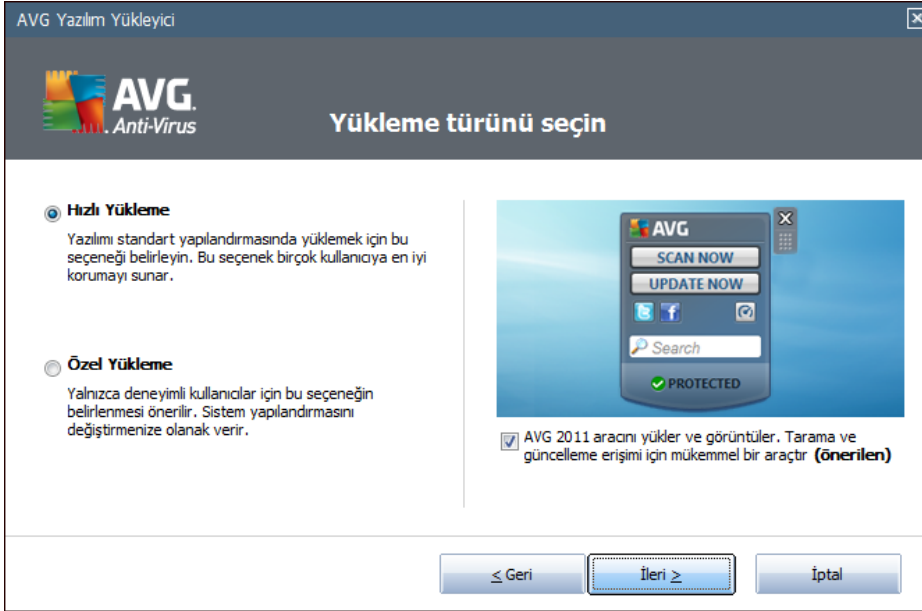
Lisansınızı Etkinleştirin iletişim kutusunda, lisans numaranızı verilen metin alanına yazmanız istenir.

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

Yükleme işlemine devam etmek için **İleri** düğmesine basın.



4.3. Yükleme türünü seçin



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

Kullanıcıların çoğu için AVG'yi program geliştiricisi tarafından öntanımlı ayarlarla tam otomatik modda yükleyen **Hızlı Kurulum** önerilmektedir. Bu yapılandırma, minimum kaynak kullanımı ile maksimum güvenliği bir araya getirir. Gelecekte söz konusu yapılandırmayı değiştirme ihtiyacı duyarsanız söz konusu işlemi istediğiniz zaman doğrudan AVG uygulamasından yapabilirsiniz. **Hızlı Yükleme** seçeneğini belirlerseniz, aşağıdaki [AVG Security Toolbar'ı Yükle](#) iletişim kutusuna geçmek için **İleri** düğmesine basın.

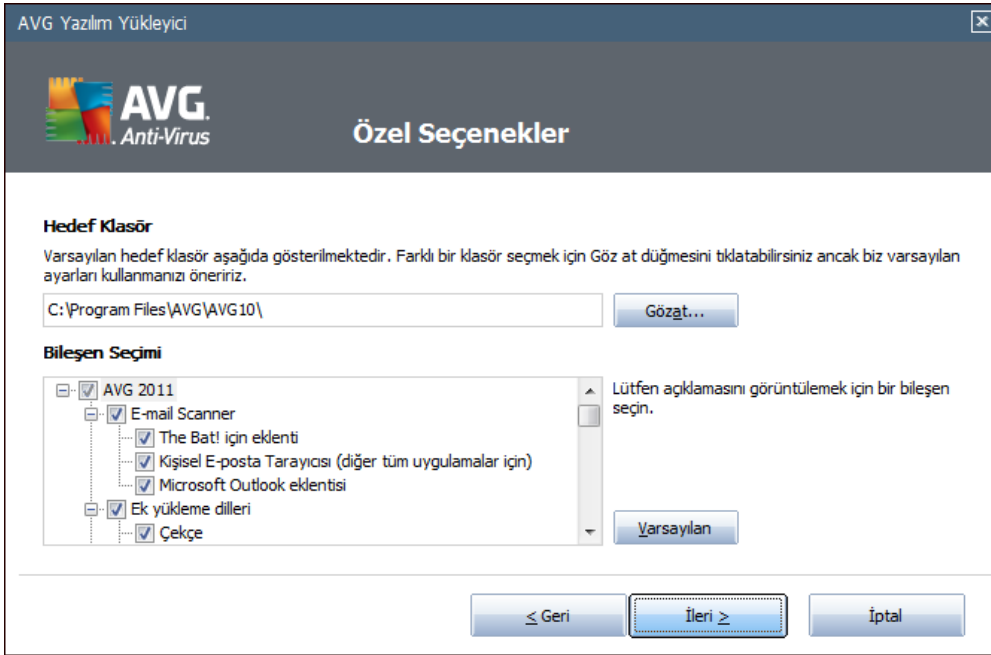
Özel Yükleme, AVG'yi standart olmayan ayarlarla kurmak için geçerli bir nedeni olan deneyimli kullanıcılar tarafından kullanılmalıdır. Örn. belirli sistem gereksinimlerini karşılamak için. Bu seçeneği belirledikten sonra, [Özel Seçenekler](#) iletişim kutusuna gitmek için **İleri** düğmesine basın.

İletişim kutusunun sağ bölümünde, [AVG gadget'ı](#) 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 Anti-Virus** yazılımınızın en önemli özelliklerine (yani, [taramaya](#) ve [güncellemeye](#)) hemen erişmenize olanak veren Windows kenar çubuğundan ulaşabilirsiniz.



4.4. Özel seçenekler

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



Hedef Klasör

İletişim kutusunun **Hedef Klasör** bölümünde, **AVG Anti-Virus** yazılımının yüklenmesi gereken konumu belirtmeniz beklenir. Varsayılan olarak AVG, C: sürücüsünde bulunan program dosyaları klasörüne yüklenecektir. Bu konumu değiştirmek istiyorsanız, sürücü yapısını görüntülemek ve ilgili klasörü seçmek için **Gözet** düğmesini kullanın.

Bileşen Seçimi

Bileşen Seçimi bölümünde, yüklenebilecek tüm **AVG Anti-Virus** 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.

Devam etmek için **İleri** düğmesine basın.



4.5. AVG Security Toolbar'ı yükle



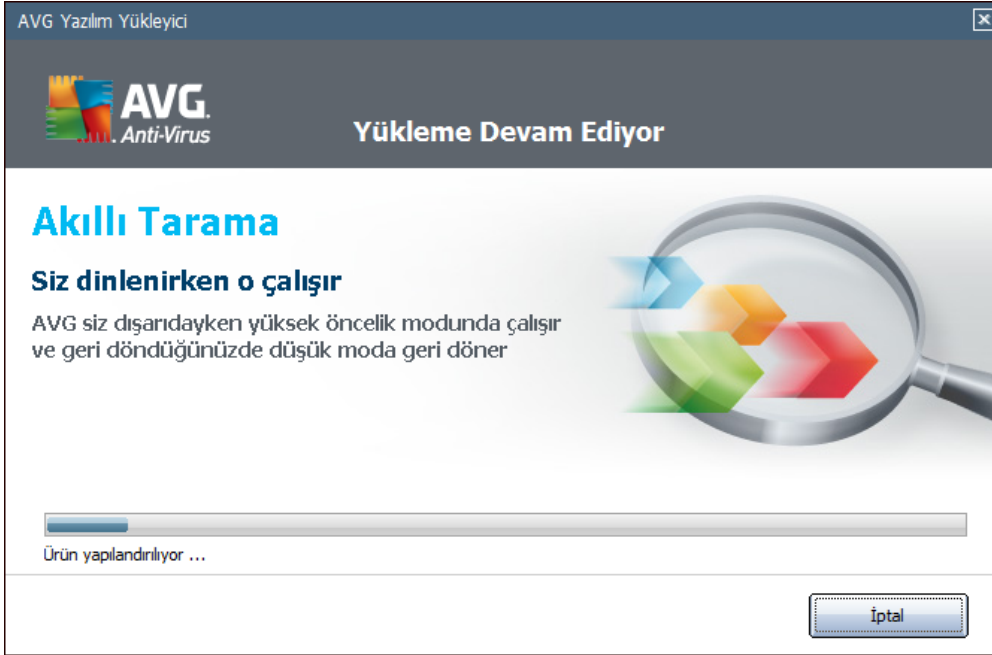
AVG Security Toolbar'ı yükle iletişim kutusunda, [AVG Security Toolbar](#) uygulamasını yüklemek isteyip istemediğinize karar verebilirsiniz. Varsayılan ayarları değiştirmezseniz, İnternet'te gezinirken size daha kapsamlı koruma sağlamak için bu bileşen otomatik olarak İnternet tarayıcınıza yüklenir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



4.6. Yükleme ilerlemesi

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



Yükleme işlemi bittiğinde, bir sonraki iletişim kutusuna yönlendirilirsiniz.

4.7. Yükleme başarılı oldu





Yükleme başarılı oldu iletişim kutusu, **AVG Anti-Virus** yazılımınızın tam olarak yüklendiğini ve yapılandırıldığını onaylar.

Bu iletişim kutusunda, ürünle ilgili tüm bilgileri ve haberleri alabilmek için iletişim bilgilerinizi verin. Kayıt formunun altında şu iki seçeneği göreceksiniz:

- **Evet, bana güvenlik haberlerini ve AVG 2011 özel tekliflerini e-posta ile bildir** - İnternet güvenliği küresinde nelerin yeni olduğu ve AVG ürününe özel teklifler, gelişmeler ve yükseltmeler hakkında bilgi almak istediğinizi belirtmek için bu onay kutusunu işaretleyin.
- **AVG 2011 web güvenliği ve Ürün Geliştirme Programı'na katılmayı kabul ediyorum ...** - toplam İnternet güvenliği seviyesini artırmak için tespit edilen tehditler hakkında nereden geldiği belli olmayan bilgiler toplayan Ürün Geliştirme Programı'na katılmak istediğinizi kabul ettiğinizi belirtmek üzere bu onay kutusunu işaretleyin (ayrıntılar için, [AVG Gelişmiş Ayarları / Ürün Geliştirme Programı](#) bölümüne bakın).

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

Not: Herhangi bir AVG işletme lisansı kullanıyorsanız ve Uzaktan yönetim öğesinin yükleneceğini önceden seçtiyseniz (bkz. [Özel Seçenekler](#)), Yüklemeye başarılı oldu iletişim kutusu şu arayüzle görüntülenecektir:

AVG DataCenter parametrelerini belirtmeniz gerekiyor - lütfen bağlantı dizesini sunucu: bağlantı noktası biçiminde AVG DataCenter uygulamasına sağlayın. Bu bilgi o anda yoksa, bu 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.



5. Yüklemeden Sonra

5.1. Ürün kaydı

AVG Anti-Virus yüklemesini bitirdikten sonra, lütfen ürününüzü AVG web sitesinin (<http://www.avg.com/>), **Kayıt** sayfasından kaydedin (*doğrudan sayfada verilen yönergeleri izleyin*). Kayıt işleminin ardından AVG Kullanıcı hesabınıza erişebileceğiniz, AVG Güncelleme bültenini alacak ve sadece kayıtlı kullanıcılara sunulan diğer hizmetlerden yararlanacaksınız.

5.2. Kullanıcı arayüzüne erişim

[AVG Kullanıcı Arayüzü](#)'ne çeşitli yöntemlerle ulaşabilirsiniz:

- [AVG sistem tepsi simgesi](#)
- Masaüstünüzdeki AVG simgesini çift tıklayın
- [AVG gadget](#)'inin alt bölümünde bulunan durum satırını çift tıklayın ([yükleyin](#); Windows Vista/ Windows 7 işletim sistemlerinde desteklenir)
- **Başlat/Programlar/AVG 2011/AVG Kullanıcı Arayüzü**
- [AVG Security Toolbar](#)'dan **AVG'yi Başlat**

5.3. Tüm bilgisayarın taraması

AVG Anti-Virus 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.

5.4. Eicar testi

AVG Anti-Virus 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. Test dosyasının indirme işlemini onaylar onaylamaz, [Online Shield](#) bir uyarıyla virüse tepki verecektir. 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 **Yerleşik Kalkan** paketi açmaya çalıştığınızda 'virüsü' algılar. **AVG'nin EICAR test dosyasını virüs olarak algılamaması halinde program yapılandırmasını yeniden kontrol etmeniz gerekir!**

5.5. AVG varsayılan yapılandırması

AVG Anti-Virus varsayılan yapılandırması (yani, uygulamanın yükledikten sonra doğru şekilde nasıl ayarlanacağı) yazılım satıcısı tarafından ayarlanabilir, böylece optimum performans elde etmek için tüm bileşenler ve işlevler ayarlanabilir.

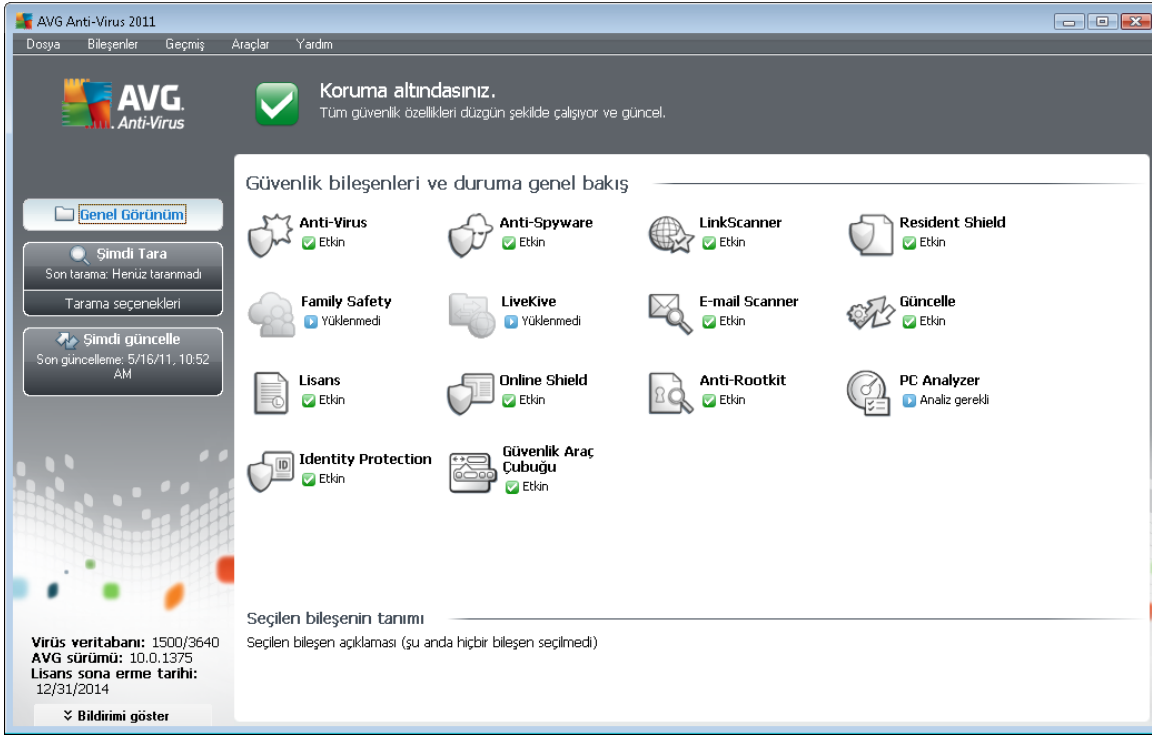
Bunun için iyi bir nedeniniz olmadıkça AVG yapılandırmasını değiştirmeyin! Ayarlarda yapılacak her tür değişiklik sadece deneyimli bir kullanıcı tarafından gerçekleştirilmelidir.

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



6. AVG Kullanıcı Arayüzü

AVG Anti-Virus, ana pencerede açılır:



Ana pencere çok sayıda bölüme ayrılır:

- **Sistem Menüsü** (penceredeki en üst sistem çubuğu) tüm AVG bileşenlerine, hizmetlerine ve özelliklerine ulaşmanızı sağlayan standart dolaşım yöntemidir - [ayrıntılar >>](#)
- **Güvenlik Durumu Bilgileri** (pencerenin üst bölümü) AVG programının mevcut durumu hakkında bilgi sunar - [ayrıntılar >>](#)
- **Hızlı Bağlantılar** (pencerenin sol bölümü) en önemli ve en sık kullanılan AVG görevlerine hızlı bir şekilde erişebilmenizi sağlar - [ayrıntılar >>](#)
- **Bileşenlere Genel Bakış** (pencerenin orta kısmı) yüklü AVG bileşenleri hakkında genel bilgi verir - [ayrıntılar >>](#)
- **İstatistikler** (pencerenin sol alt kısmı) programın çalışmasına ilişkin istatistik verileri görüntüler - [ayrıntılar >>](#)
- **Sistem Tepsisi Simgesi** (ekranın sağ alt köşesi, sistem tepsisi üzerinde) AVG'nin mevcut durumunu gösterir - [ayrıntılar >>](#)
- **AVG gadget'ı** (Windows kenar çubuğu, Windows Vista/7'de desteklenir) AVG taramasına ve güncellemesine hızlı erişim için olanak verir - [ayrıntılar >>](#)



6.1. Sistem Menüsü

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

Sistem menüsü beş ana bölüme ayrılmıştır:

6.1.1. Dosya

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

6.1.2. Bileşenler

Sistem menüsünün **Bileşenler** ögesi, yüklenen tüm AVG bileşenlerine ilişkin bağlantılar içerir ve kullanıcı arayüzünde bunların varsayılan iletişim kutusu sayfalarını açar:

- **Sisteme genel bakış** - [yüklü tüm bileşenlerle ve durumlarıyla birlikte varsayılan kullanıcı arayüzü iletişim kutusuna geçer](#)
- **Anti-Virus** yazılımı, bilgisayarınızı bilgisayarınıza girmeye çalışan virüslerden korur - [ayrıntılar >>](#)
- **Anti-Spyware** yazılımı, bilgisayarınızın casus yazılımlardan ve reklam yazılımlarından korunmasını sağlar - [ayrıntılar >>](#)
- **LinkScanner** İnternet tarayıcısında görüntülenen arama sonuçlarını kontrol eder - [ayrıntılar >>](#)
- **E-posta Tarayıcısı** gelen ve giden tüm postaları virüslere karşı kontrol eder - [ayrıntılar >>](#)
- **Aile Güvenliği** çocuklarınızın çevrimiçi faaliyetlerini izlemenize ve onları uygunsuz web sitesi içeriklerinden korumanıza yardımcı olur - [ayrıntılar >>](#)
- **LiveKive** verileriniz için çevrimiçi otomatik yedekleme sağlar - [ayrıntılar >>](#)
- **Yerleşik Kalkan** arka planda çalışır ve dosyalar kopyalanır, açılır ve kaydedilirken söz konusu dosyaları tarar - [ayrıntılar >>](#)
- **Güncelleme Yöneticisi** tüm AVG güncellemelerini denetler - [ayrıntılar >>](#)
- **Lisans**, lisans numarasını, türünü ve son kullanma tarihini görüntüler - [ayrıntılar >>](#)
- **Online Shield** bir web tarayıcısı tarafından indirilen tüm verileri tarar - [ayrıntılar >>](#)
- **Anti-Rootkit** kötü amaçlı yazılımları gizlemeye çalışan programları ve teknolojileri tespit eder - [ayrıntılar >>](#)
- **PC Analyzer** analizörü, bilgisayarınızın durumu hakkında bilgi verir - [ayrıntılar >>](#)



- **Kimlik Koruması** - kişisel dijital değerlerinizi kimlik hırsızlarına karşı korumaya odaklanan kötü amaçlı yazılımlardan koruma bileşenidir - [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

6.1.3. Geçmiş

- **Tarama sonuçları** - AVG test arayüzüne özellikle **Tarama Sonuçlarına Genel Bakış** penceresine gider
- **Yerleşik Kalkan tespiti** - **Yerleşik Kalkan**
- **E-posta Tarayıcısı tespiti** - **E-posta Tarayıcısı** bileşeni tarafından tehlikeli olarak tespit edilen posta mesajları ekleri hakkında genel bilgi veren bir iletişim kutusu açar
- **Online Shield Tespitleri** - **Online Shield**
- **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 bulundurularak depolanır
- **Etkinlik geçmişi kayıt defteri** - kaydedilen tüm **AVG Anti-Virus** eylemler hakkında genel bilgi veren bir geçmiş kayıt defteri arayüzü açar

6.1.4. 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** - **AVG Anti-Virus** güncelleme işlemini otomatik olarak 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. İnternet bağlantısı olmadığı durumlarda (*Örneğin bilgisayarınıza virüs bulaşmış ise ve İnternet bağlantınız kesildiyse; bilgisayarınız bir ağa bağlıysa fakat İnternet erişimi yok ise vb.*). Yeni açılan pencereden, daha önce güncelleme dosyasını depoladığınız klasörü seçin ve güncelleme işlemini başlatın.
- **Gelişmiş ayarlar** - yapılandırmasını düzenleyebileceğiniz **AVG Anti-Virus** gelişmiş ayarlar iletişim kutusunu açar. Genel olarak uygulamanın yazılım üreticisi tarafından tanımlanan varsayılan ayarlarının muhafaza edilmesi önerilir.

6.1.5. 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 [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 sitesi (<http://www.avg.com/>) kayıt sayfasına bağlanır. Lütfen kayıt bilgilerinizi doldurun. Sadece AVG ürünlerini kaydettiren müşterilerimiz ücretsiz teknik destek alabilecektir.

Not: AVG Anti-Virus deneme sürümünü kullanıyorsanız, sonraki iki öge, **Şimdi satın al** ve **Etkinleştir** olarak görünür, programın tam sürümünü hemen satın almanızı sağlar. Bir satış numarasıyla yüklenmiş **AVG Anti-Virus** için, öğeler **Kaydet** ve **Etkinleştir** olarak görünür. Daha fazla bilgi için, lütfen bu bekgenin [Lisans](#) bölümüne bakın.

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

6.2. Güvenlik Durumu Bilgisi

Güvenlik Durumu Bilgisi bölümü, AVG'nin ana penceresinin üst kısmında bulunmaktadır. Bu bölümde **AVG Anti-Virus** programınızın mevcut güvenlik durumu hakkında her zaman bilgi bulabilirsiniz. Lütfen bu bölümde betimlenmesi muhtemel simgeleri ve anlamlarını inceleyin:



- Yeşil simge AVG'nizin tam olarak çalıştığını gösterir. 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'de herhangi bir kritik sorun yoktur ve muhtemelen bir nedenden dolayı bileşenlerden bazılarını geçici olarak kapatmayı seçmiş olabilirsiniz. Ancak AVG tarafından korunmaya devam edersiniz. Diğer bir yandan lütfen bileşenin ayarlarını inceleyin! Adı **Güvenlik Durumu Bilgisi** kısmında sağlanır.

Bu simge, herhangi bir nedenle [bir bileşenin hata durumunu göz ardı etmeyi seçtiyseniz](#) de görüntülenecektir ("**Bileşen durumunu göz ardı et**") seçeneğine, AVG ana penceresinin



*bileşenlere genel bakış kısmında bulunan ilgili simgeyi sağ tıklayarak açtığınız bağlam menüsünden ulaşabilirsiniz). Özel durumlar için bu seçeneği kullanmanız gerekebilir ancak en kısa zamanda **Bileşen durumunu gözardı et** seçeneğini devre dışı bırakmanız önerilir.*



- Kırmızı simge, AVG'nin kritik durumda olduğunu gösterir! Bir ya da daha fazla bileşen doğru çalışmıyor ve AVG bilgisayarınızı koruyamıyor anlamına gelir. Lütfen rapor edilen sorunu çözmek için gerekli ilgiyi gösterin. Hatayı kendi başınıza çözemiyorsanız [AVG teknik destek](#) ekibi ile iletişim kurun.

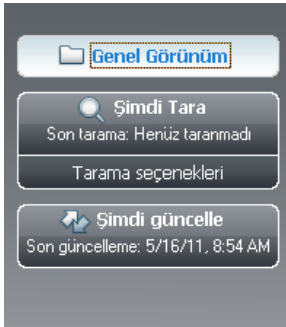
AVG'nin en verimli performansı ayarlayamaması durumunda, Onar adlı yeni bir düğme (alternatif olarak, sorun birden fazla bileşenle ilgiliyse, Tümünü onar düğmesi) görüntülenir. Program denetimini ve yapılandırmasını otomatik olarak başlatmak için bu düğmeye basın. Bu, AVG'yi en verimli performansa ayarlamanın ve maksimum güvenlik seviyesine getirmenin kolay 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 durum bilgilerine [sistem tepsisi simgesinden](#) de ulaşabilirsiniz.

6.3. Hızlı Bağlantılar

Hızlı Bağlantılar ([AVG Kullanıcı Arayüzü](#)'nın sol kısmında) en sık kullanılan ve en önemli AVG özelliklerine hemen erişebilmenizi sağlar:



- **Genel Bakış** - açık durumdaki herhangi bir AVG arayüzünden yüklü bileşenlerin tümünün görüntülediği varsayılan genel bakış penceresine gitmek için bu bağlantıyı kullanın - bkz. bölüm [Bileşenlere Genel Bakış >>](#)
- **Şimdi tara** - varsayılan olarak bu düğme, başlatılmış son tarama hakkında bilgiler verir (*tarama türü, son başlatma tarihi*). Aynı tarama işlemini tekrar başlatmak için **Şimdi tara** komutunu çalıştırabilir veya taramaları çalıştırabileceğiniz, programlayabileceğiniz veya parametrelerini ayarlayabileceğiniz AVG tarama arayüzünü açmak için **Tarama seçenekleri** bağlantısını izleyebilirsiniz; [AVG Scanning bölümüne bakın>>](#)
- **Şimdi güncelle** - güncelleme sürecinin son başlatıldığı tarihi belirtir. Güncelleme arayüzünü açmak için düğmeye basın ve AVG güncelleme sürecini hemen çalıştırın (bkz. bölüm [AVG](#)



[Güncellemeleri >>](#)

Bu bağlantılara kullanıcı arayüzünden istediğiniz zaman ulaşabilirsiniz. Belirli bir işlemi başlatmak üzere hızlı bağlantılardan birini kullandığınızda GUI yeni bir iletişim kutusunda açılacaktır fakat söz konusu iletişim kutusundan da hızlı bağlantılara ulaşabilirsiniz. Buna ek olarak çalışan işlem grafiksel olarak da betimlenmektedir.

6.4. Bileşen Genel Görünümü

Bileşen Genel Görünümü bölümü, [AVG Kullanıcı Arayüzü](#)'nün orta kısmında bulunur. Bölüm iki bölüme ayrılır:

- Yanlarında ilgili bileşenin simgesinin ve aktif ya da pasif olduğuna dair durum bilgisinin bulunduğu yüklü tüm bileşenlerin genel görünümü
- Seçili bileşenin açıklaması

AVG Anti-Virus içinde, **Bileşen Genel Görünümü** kısmı aşağıdaki bileşenler hakkında bilgiler içerir:

- **Anti-Virus** yazılımı, bilgisayarınızı bilgisayarınıza girmeye çalışan virüslere karşı korur - [ayrıntılar >>](#)
- **Anti-Spyware** yazılımı, bilgisayarınızın casus yazılımlardan ve reklam yazılımlarından korunmasını sağlar - [ayrıntılar >>](#)
- **LinkScanner** İnternet tarayıcısında görüntülenen arama sonuçlarını kontrol eder - [ayrıntılar >>](#)
- **E-posta Tarayıcısı** gelen ve giden tüm postaları virüslere karşı kontrol eder - [ayrıntılar >>](#)
- **Yerleşik Kalkan** arka planda çalışır ve dosyalar kopyalanır, açılır ve kaydedilirken söz konusu dosyaları tarar - [ayrıntılar >>](#)
- **Aile Güvenliği** çocuklarınızın çevrimiçi faaliyetlerini izlemenize ve onları uygunsuz web sitesi içeriklerinden korumanıza yardımcı olur - [ayrıntılar >>](#)
- **LiveKive** verileriniz için çevrimiçi otomatik yedekleme sağlar - [ayrıntılar >>](#)
- **Güncelleme Yöneticisi** tüm AVG güncellemelerini denetler - [ayrıntılar >>](#)
- **Lisans**, lisans numarasını, türünü ve son kullanma tarihini görüntüler - [ayrıntılar >>](#)
- **Online Shield** bir web tarayıcısı tarafından indirilen tüm verileri tarar - [ayrıntılar >>](#)
- **Anti-Rootkit** kötü amaçlı yazılımları gizlemeye çalışan programları ve teknolojileri tespit eder - [ayrıntılar >>](#)
- **PC Analyzer**, bilgisayarınızın durumu hakkında bilgi verir - [ayrıntılar >>](#)
- **Kimlik Koruması** - kişisel dijital değerlerinizi kimlik hırsızlarına karşı korumaya odaklanan



kötü amaçlı yazılımlardan koruma bileşenidir - [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

Bileşenlere genel bakış ekranında bileşeni seçmek için üzerine bir defa tıklayın. Aynı anda kullanıcı arayüzünün alt kısmında bileşenin temel fonksiyonları hakkında açıklamalar görüntülenir. Bileşenin kendi arayüzünü açmak ve temel istatistiki verileri görüntülemek için simgeyi çift tıklayın.

Bir bağlam menüsü açmak için bileşenin simgesini sağ tıklayın: bileşenin grafik arayüzünü açmanın yanı sıra **Bileşenin durumunu göz ardı et** seçimini de yapabilirsiniz. [Bileşenin hata durumunun](#) farkında olduğunuzu göstermek için bu seçeneği belirleyin, ancak belirli bir neden doğrultusunda AVG'nizin bu şekilde çalışmasını ve [sistem tepsisi simgesi](#) ile uyarılmamayı istiyorsunuzdur.

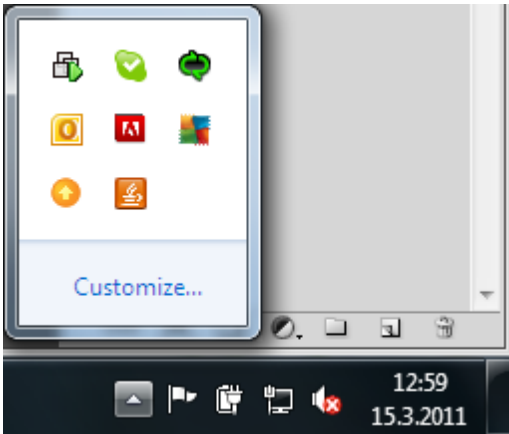
6.5. İstatistikler

İstatistikler bölümü [AVG Kullanıcı Arayüzü](#)'nün sol alt kısmında yer alır. Programın çalışması hakkında bir dizi bilgi içerir:

- **Virüs VT** - o anda yüklü virüs tabanı sürümü hakkında bilgi verir
- **AVG sürümü** - yüklü AVG sürümü hakkında sizi bilgilendirir (numara 10.0.xxxx biçimindedir ve burada 10.0 ürün serisi sürümü iken xxxx üretim numarasını gösterir)
- **Lisansın son kullanılma tarihi** - AVG lisansınızın son kullanılma tarihini gösterir

6.6. Sistem Tepsisi Sembolü

Sistem Tepsisi Sembolü (Windows araç çubuğunda), **AVG Anti-Virus** programınızın geçerli durumunu gösterir. AVG ana penceresinin açık ya da kapalı olduğu önemli olmaksızın devamlı olarak sistem tepsinizde bulunur:





Tamamen renkli ise  **Sistem Tepsisi Sembolü**, tüm AVG bileşenlerinin aktif ve tamamen fonksiyonel olduğunu gösterir. Buna ek olarak, AVG hata durumundayken de AVG sistem tepsisi sembolü tamamen renkli görüntülenebilir, ancak bu, durumun tamamen farkındasınız ve bilerek [Bileşen durumunu göz ardı et](#) seçimini yapmışsınız demektir. Ünlem işareti içeren bir simge  bir sorun olduğunu gösterir (*etkin olmayan bileşen, hata durumu vb.*). Ana pencereyi açmak ve bileşeni düzenlemek için **Sistem Tepsisi Sembolünü** çift tıklayın.

Sistem tepsisi sembolü geçerli AVG etkinlikleri ve programdaki olası durum değişiklikleri (örn. *programlanmış bir taramanın veya güncellemenin otomatik başlatılması, bir bileşenin durumundaki değişiklik, hata durumu oluşumları...*), AVG sistem tepsisi sembolünde açılır bir pencere yoluyla hakkında bilgi de verir:



Sistem Tepsisi Sembolü AVG ana penceresine istediğiniz zaman ulaşabilmeniz için hızlı bir bağlantı olarak da kullanılabilir - sadece simgeyi iki defa tıklayın. **Sistem Tepsisi Sembolü** sağ tıklayarak aşağıdaki seçenekleri sunan kısa bir bağlam menüsü açarsınız:

- **AVG Kullanıcı Arayüzünü Aç** - [AVG Kullanıcı Arayüzünü açmak için tıklayın](#)
- **Taramalar** - şu bağlam menüsünü açmak için tıklayın
- **PC Analyzer'ı çalıştır** - [PC Analyzer](#) bileşenini başlatmak için tıklayın
- **Çalışan taramalar** - bu öge 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

6.7. 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 Anti-Virus** işlevlerine, yani [taramaya](#) ve [güncellemeye](#) hemen erişim sağlar:

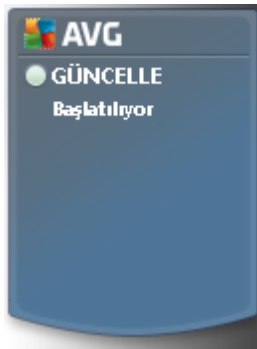


AVG gadget'ı şu hızlı erişim seçeneklerini sunar:

- **Şimdi tara** - [tüm bilgisayarın taramasını](#) doğrudan başlatmak için **Şimdi tara** bağlantısını tıklayın. Tarama sürecinin ilerlemesini gadget'ın alternatif kullanıcı arayüzünden izleyebilirsiniz. Kısa istatistikler genel görünümü, taranan nesnelerin, 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** - AVG güncellemesini doğrudan gadget içerisinden başlatmak için **Şimdi güncelle** bağlantısını tıklayın:



- **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
- **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



7. AVG Bileşenleri

7.1. Virüsten Koruma

7.1.1. Virüsten Koruma İlkeleri

Virüsten koruma yazılımlarının tarama motorları bilinen tüm virüslere karşı tüm dosya ve dosya eylemlerini (dosyaların açılması/kapatılması vb.) tarar. Tespit edilen virüsler, harekete geçmeden engellenecek ve ardından silinecek ya da karantinaya alınacaktır. 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 bazılarını sahipse söz konusu virüsten koruma tarayıcısının yeni ve bilinmeyen bir virüsü tespit edebileceği anlamına gelmektedir.

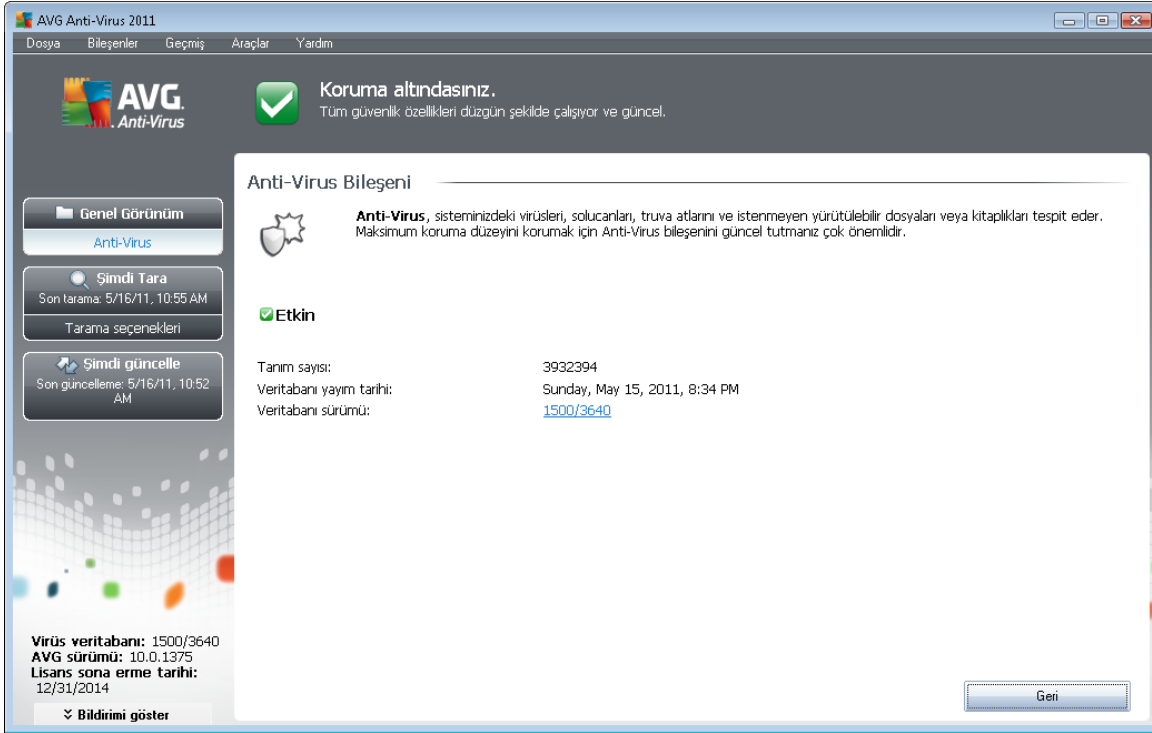
Antivirüs korumasının en önemli özelliği, bilgisayarınıza hiçbir virüsün bulaşmamasının sağlanmasıdır!

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:

- 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

AVG bunun yanı sıra sistemde potansiyel anlamda istenmeyen çalıştırılabilir uygulamaları ya da DLL kütüphanelerini de inceleyebilmekte ve tespit edebilmektedir. Söz konusu tehlikeleri Potansiyel Olarak İstenmeyen Programlar (farklı casus yazılım, reklam yazılımı türleri vb) olarak adlandırırız. Buna ek olarak AVG, sistem kayıt defterinizi şüpheli girdilere, geçici Internet dosyalarına ve izleme tanımlama bilgilerine karşı da tarar ve söz konusu potansiyel olarak istenmeyen nesneleri de diğer bulaşmalarla aynı şekilde çözebilmenize olanak tanır.

7.1.2. Virüsten Koruma Arayüzü



Anti-Virus bileşeninin arayüzünde bileşenin fonksiyonlarına, bileşenin mevcut durumu hakkında bilgiye (*Anti-Virus bileşeni aktiftir.*) ve **Anti-Virus** istatistikleri hakkında kısa bilgilere ulaşabilirsiniz.

- **Tanım sayısı** - bu sayı virüs veritabanının güncel sürümünde tanımlanan virüs sayısını verir
- **Veritabanı yayını** - virüs veritabanının en son güncellendiği tarih ve saati gösterir
- **Veritabanı sürümü** - o anda yüklü en son virüs veritabanı sürümünün numarasını tanımlar ve bu numara virüs veritabanı her güncellendiğinde artar

Bu bileşenin arayüzü kapsamında sadece bir adet çalıştırma düğmesi bulunur (**Geri**) - Varsayılan [AVG Kullanıcı Arayüzüne](#) (bileşenlere genel bakış) dönmek için bu düğmeye basın.

7.2. Casus Yazılımdan Koruma

7.2.1. Casus Yazılımdan Koruma Prensipleri

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.

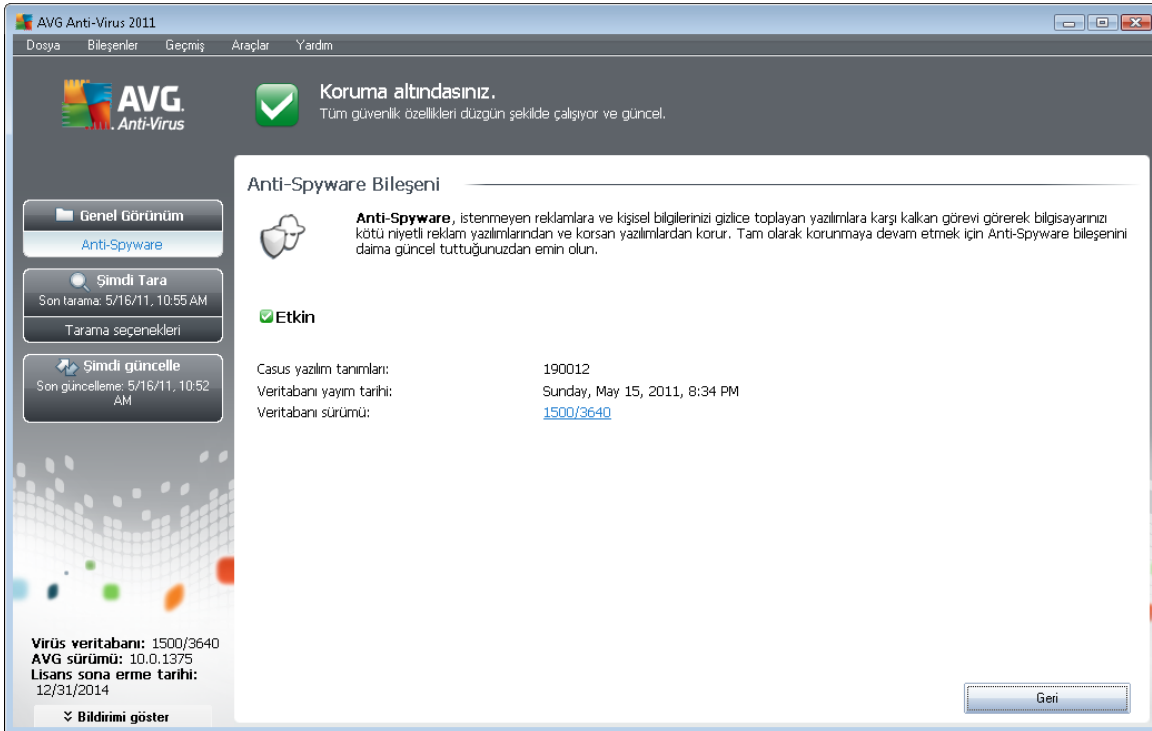
Şu anda bilinen en yaygın bulaşma kaynağı, potansiyel anlamda tehlikeli öğeler içeren web



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 çalıştığınız zaman arka planda uygulamaları tarayan **Anti-Spyware** gibi devamlı olarak arka planda çalışan bir tarayıcı kullanmaktır.

Kötü amaçlı yazılımın bilgisayarınıza AVG yüklenmesinden önce bulaşmış olması ya da **AVG Anti-Virus** programınızı en güncel [veritabanı ve program güncellemeleriyle güncel tutmayı ihmal etmeniz gibi potansiyel riskler de bulunmaktadır](#). Bu nedenle AVG, tarama özelliğini kullanarak tüm bilgisayarınızı kötü amaçlı ve casus yazılımlara karşı tarayabilmenize olanak tanır. Ayrıca, uykuda olan ve etkin olmayan kötü amaçlı yazılımları da (yani, bilgisayara indirilmiş ancak henüz etkinleştirilmemiş olanları) tespit eder.

7.2.2. Casus Yazılımdan Koruma Arayüzü



Anti-Spyware bileşeninin arayüzü bileşenin işlevi ile ilgili kısa genel bilgiler, bileşenin mevcut durumu ve bazı **Anti-Spyware** istatistikleri hakkında bilgiler sağlar:

- **Casus yazılım tanımları** - sayı, en son casus yazılım veri tabanı sürümünde tanımlanan casus yazılım örneği sayısını gösterir.
- **Veritabanı yayını** - casus yazılım veritabanının en son güncellendiği tarih ve saati gösterir.
- **Veritabanı sürümü** - en son casus yazılım veritabanı sürümünün numarasını tanımlar ve bu numara virüs veritabanı her güncellendiğinde artar

Bu bileşenin arayüzü kapsamında sadece bir adet çalıştırma düğmesi bulunur (**Geri**) - Varsayılan [AVG Kullanıcı Arayüzüne](#) (bileşenlere genel bakış) dönmek için bu düğmeye basın.



7.3. Bağlantı Tarayıcı

7.3.1. Link Scanner Prensipleri

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.

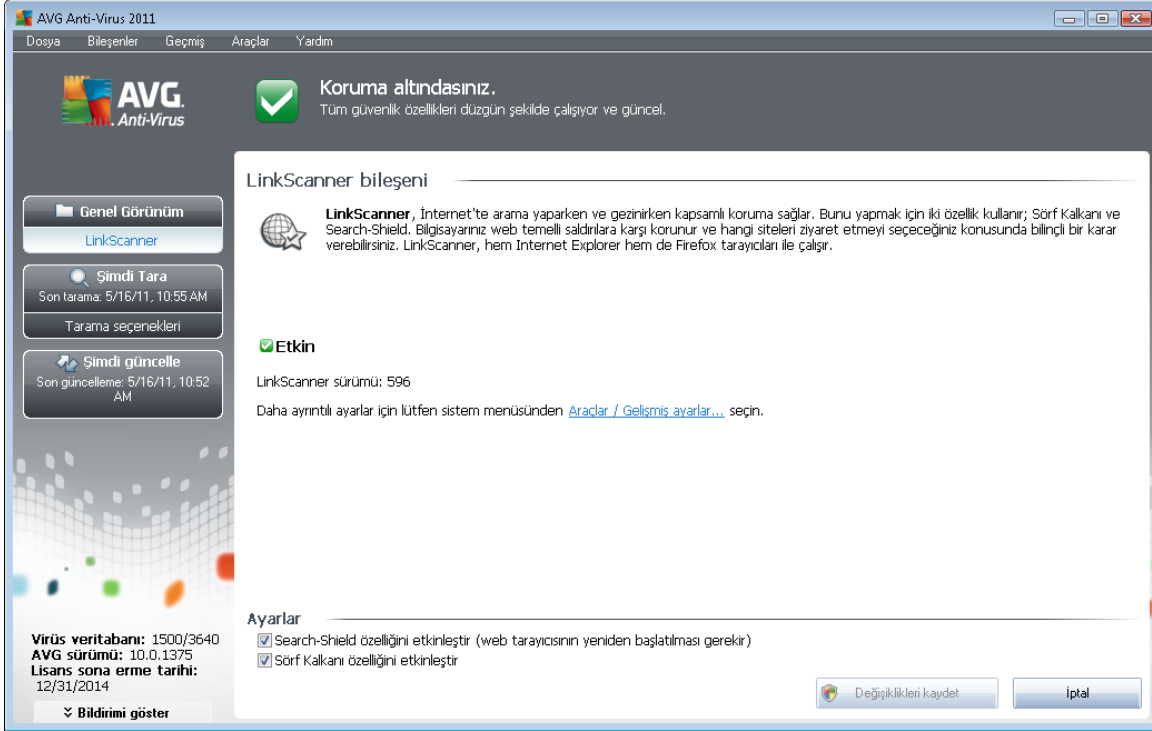
LinkScanner teknolojisi iki özellik içerir, [Search-Shield](#) ve [Surf-Shield](#):

- [Search-Shield](#) tehlikeli olabileceği bilinen web sitelerinin listesini (*URL adreslerini*) içerir. Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg veya SlashDot ile arama yapıldığında, aramanın tüm sonuçları bu listeye göre denetlenir ve bir karar simgesi görüntülenir (*Yahoo aramaları için yalnızca "kötüye kullanılan 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.

Not: LinkScanner sunucu platformlarında kullanılmak için tasarlanmamıştır!

7.3.2. Link Scanner Arayüzü

[LinkScanner](#) bileşeninin arayüzü, bileşenlerin işlevleri hakkında kısa açıklamalar sağlar ve işlevin geçerli durumu ile ilgili bilgiler verir. Ayrıca en yeni [LinkScanner](#) veritabanı sürümü numarası (*Link Scanner sürümü*) hakkında bilgiler bulabilirsiniz.



LinkScanner Ayarları

İletişim kutusunun en alt bölümünde birçok seçeneği düzenleyebilirsiniz:

- **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 uyarı simgeleriyle ilgili danışma: arama motoru tarafından döndürülen içeriği önceden denetler.
- **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.

7.3.3. Arama Kalkanı

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, **AVG Link Scanner** 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.

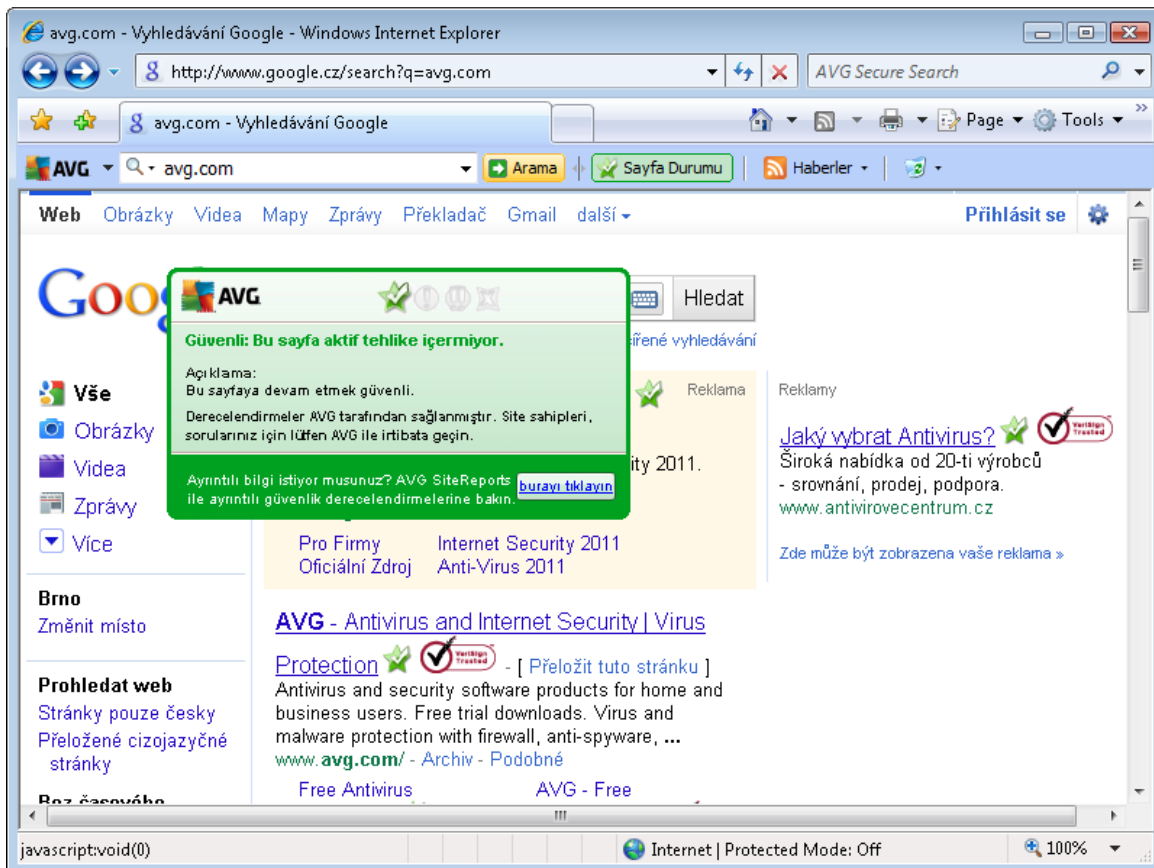


Bağlantı verilen sayfa etkin tehlike içermiyor! Kendi güvenliğiniz için, bu sayfayı ziyaret etmenize izin verilmeyecek.



Bağlantılı sayfaya erişilemediğinden taranamadı.

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

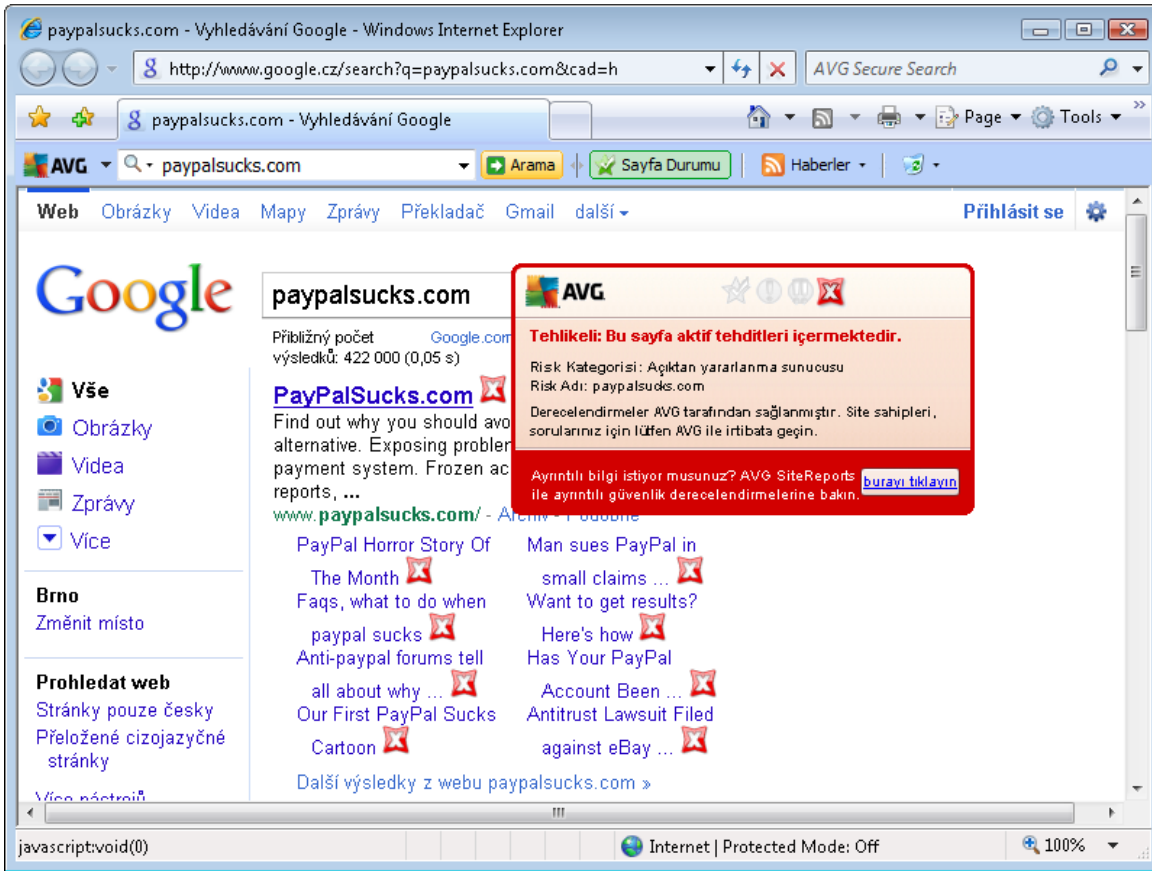


7.3.4. Surf-Shield

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, [AVG Link Scanner](#), tarayıcınızın bu sayfayı göstermesine izin vermez.

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



Bu tür bir web sitesine girmek oldukça risklidir ve önerilemez!

7.4. Yerleşik Kalkan

7.4.1. Yerleşik Kalkan İlkeleri

Yerleşik Kalkan bileşeni, bilgisayarınızın sürekli olarak korunmasını sağlar. Açılan, kaydedilen veya kopyalanan her dosyayı tarar ve bilgisayarın sistem alanlarını korur. **Yerleşik Kalkan** erişilen bir dosyada virüs tespit ederse geçerli işlemi durdurur ve virüsün kendisini etkinleştirmesine izin vermez. Normal olarak, "arka planda" çalıştığından işlemi fark etmezsiniz ve yalnızca tehdit bulunması durumunda bilgilendirilirsiniz; aynı anda, **Yerleşik Kalkan** tehdidin etkinleştirilmesini engeller ve tehdidi kaldırır. **Yerleşik Kalkan** sistemin başlatılması sırasında bilgisayarınızın belleğine yüklenir.

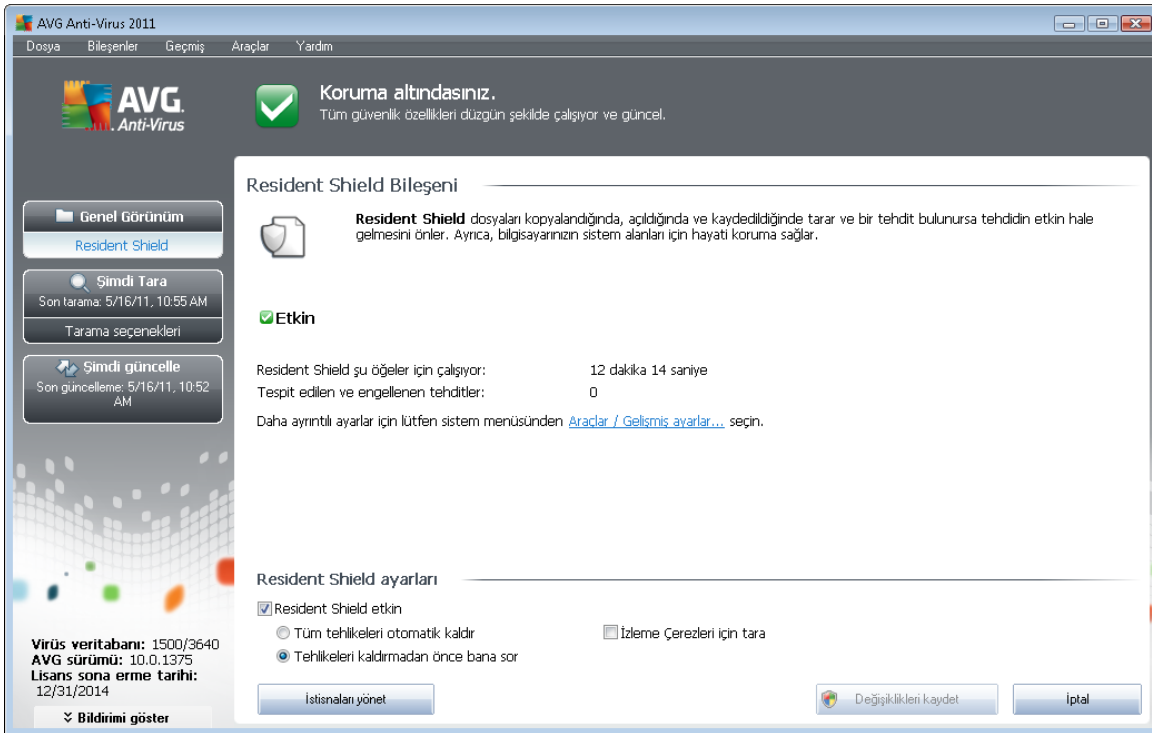


Yerleşik Kalkan ne yapabilir:

- Çeşitli türdeki olası tehditleri tarar
- Çıkarılabilir ortamı (*flash disk vb.*) tarar
- Özel uzantıları olan veya uzantıları olmayan dosyaları tarar
- Tarama istisnalarına olanak tanır: kesinlikle taranmaması gereken özel dosyalar veya klasörler

Uyarı: Yerleşik Kalkan, başlatma sırasında bilgisayarınızın belleğine yüklenir ve bu özelliği her zaman açık durumda tutmanız önemlidir!

7.4.2. Yerleşik Kalkan Arayüzü



Yerleşik Kalkan işlemlerinin genel görünümü ve bileşenin durumu hakkındaki bilgilerin yanı sıra, **Yerleşik Kalkan** arayüzü bazı istatistik verilerini de sunar:

- **Yerleşik Kalkan** 'den beri etkin - bileşenin en son çalıştırıldığı tarihten itibaren geçen zamanı gösterir
- **Tespit edilen ve engellenen tehlikeler** - çalıştırılması/açılması engellenen tespit edilen bulaşma sayısı (*ihtiyaç duyulursa bu değer sıfırlanabilir; Öm. istatistiki amaçlar doğrultusunda - Değeri sıfır*)



Yerleşik Kalkan ayarları

İletişim kutusunun alt kısmında **Yerleşik Kalkan ayarları** adı altında bir bölüm göreceksiniz; burada bileşenin fonksiyonlarının temel ayarlarından bazılarını düzenleyebilirsiniz (*diğer bileşenlerde de olduğu gibi ayrıntılı yapılandırma, sistem menüsünün Araçlar/Gelişmiş ayarlar ögesinden yapılabilmektedir*).

Yerleşik Kalkan Etkin seçeneği yerleşik korumayı kolaylıkla açıp kapatabilmenizi sağlar. Varsayılan olarak bu fonksiyon açıktır. Yerleşik koruma açık durumdayken tespit edilen bulaşmalar hususunda gerçekleştirilecek eylemi (silmeyi) belirleyebilirsiniz:

- o otomatik olarak (**Tüm tehlikeleri otomatik olarak sil**)
- o ya da sadece kullanıcının onayının ardından (**Tehlikeleri silmeden önce bana sor**)

Bu seçimin güvenlik seviyesi üzerinde herhangi bir etkisi yoktur ve sadece tercihlerinizi yansıtır.

Her iki durumda da **İzleme tanımlama bilgilerini tara** işlemini yapmayı veya yapmamayı seçebilirsiniz. Belirli durumlarda maksimum güvenlik seviyesine ulaşmak için bu seçeneği kullanabilirsiniz fakat varsayılan olarak kapalıdır. (*tanımlama bilgileri = bir sunucu tarafından web tarayıcısına ve oradan da siteye her ulaşıldığında değiştirilmek sizin tarayıcı tarafından geri gönderilen metin parçalarıdır. HTTP tanımlama bilgileri, site tercihleri veya elektronik alışveriş sepetlerinin içerikleri gibi kullanıcılar hakkındaki belirli bilgilerin kimliklerinin doğrulanması, takibi ve sürdürülmesi için kullanılır.*)

Lütfen dikkat: 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 menüsünden ilgili ögeyi seçin **Araçlar/Gelişmiş ayarlar** ve yeni açılan [AVG Gelişmiş Ayarlar](#) iletişim kutusunda AVG yapılandırmasını düzenleyin.

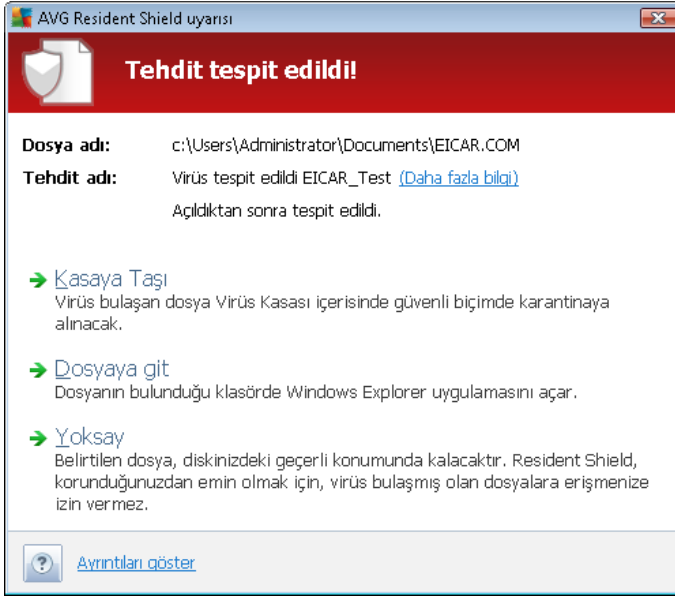
Kontrol düğmeleri

Yerleşik Kalkan arayüzünde bulunan kontrol düğmeleri şunlardır:

- **İstisnaları yönet** - **Yerleşik Kalkan** taramasında hariç tutulması gereken klasörleri ve dosyaları tanımlayabileceğiniz [Yerleşik Kalkan - Hariç Tutulan Öğeler](#) iletişim kutusunu açar.
- **Değişiklikleri kaydet** bu iletişim kutusunda yapılan her tür değişikliği kaydetmek ve uygulamak için bu düğmeye basın
- **İptal** - Varsayılan [AVG kullanıcı arayüzüne](#) dönmek için bu düğmeye basın (*bileşenlere genel bakış*)

7.4.3. Yerleşik Kalkan Tespiti

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*).

Ayrıca, bundan sonra hangi önlemlerin alınması gerektiğine karar vermeniz gerekir. Aşağıdaki seçenekler kullanılabilir:

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 virüse, bunu silmek (*yani [Virüs Kasası](#)'na taşımak*) için bu işlevi kullanın.
- **Kasaya Taşı** - Virüs AVG [Virüs Kasasına](#)
- **Dosyaya git** - Bu seçenek sizi şüpheli nesnenin tam konumuna yönlendirir (*yeni Windows Gezgini penceresi açar*)

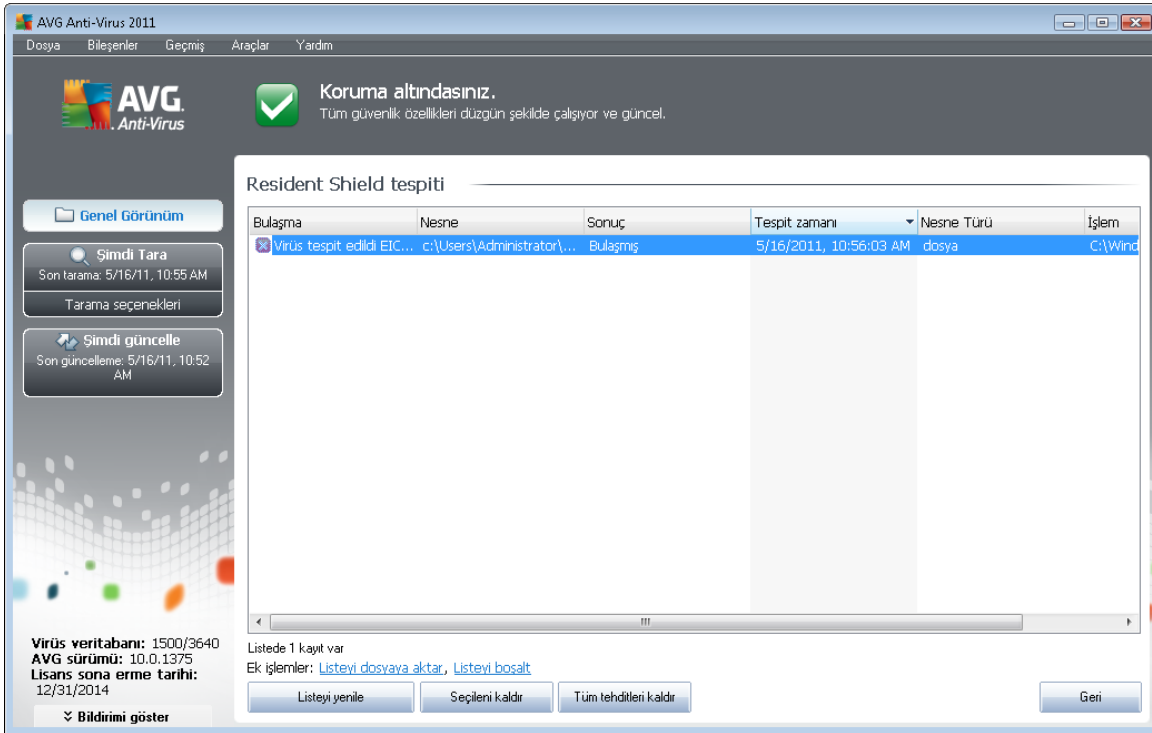


- **Yoksay** - çok geçerli bir nedeninizin olmaması halinde KESİNLİKLE bu seçeneği belirlememenizi öneriyoruz!

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 uyarılanabilir yüzdesi olarak tanımlanır. Virüs Kasanızın 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](#) tarafından tespit edilen tüm tehditlerin tüm genel görünümü, [Geçmiş / Yerleşik Kalkan tespiti](#) sistem menüsü seçeneğinden erişilebilen **Yerleşik Kalkan tespiti** iletişim kutusundan bulunabilir:



Yerleşik Kalkan tespiti [Yerleşik Kalkan](#) tarafından tespit edilip tehlikeli olduğu görülen ve temizlenen ya da [Virüs Kasasına](#) taşınan nesneler hakkında genel bilgi vermektedir. Tespit edilen tüm nesneler 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 uyaran 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 kullanıcı arayüzüne](#) geri götürür (*bileşenlere genel bakış*).

7.5. Aile Güvenliği

AVG 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.

Bileşen, **AVG Family Safety** ürünü makinenize yüklendiğinde etkin olur. Yüklendiği bir **AVG Family Safety** ürününüz yoksa **AVG Anti-Virus** kullanıcı arayüzü içerisindeki ilgili simgeyi tıklayın. Bu şekilde, gereken tüm ayrıntıları bulabileceğiniz ürün web sitesine yönlendirilirsiniz.

7.6. AVG LiveKive

AVG 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.

Bileşen yalnızca **AVG LiveKive** ürünü makinenizde yüklenmişse etkin olur. Yüklendiği bir **AVG LiveKive** ürününüz yoksa, **AVG Anti-Virus** kullanıcı arayüzündeki ilgili simgeyi tıklattığınızda gerekli tüm ayrıntıları bulabileceğiniz ürün web sitesine yönlendirilirsiniz.

7.7. E-Posta Tarayıcısı

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.



7.7.1. E-posta Tarayıcısı Prensipleri

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.

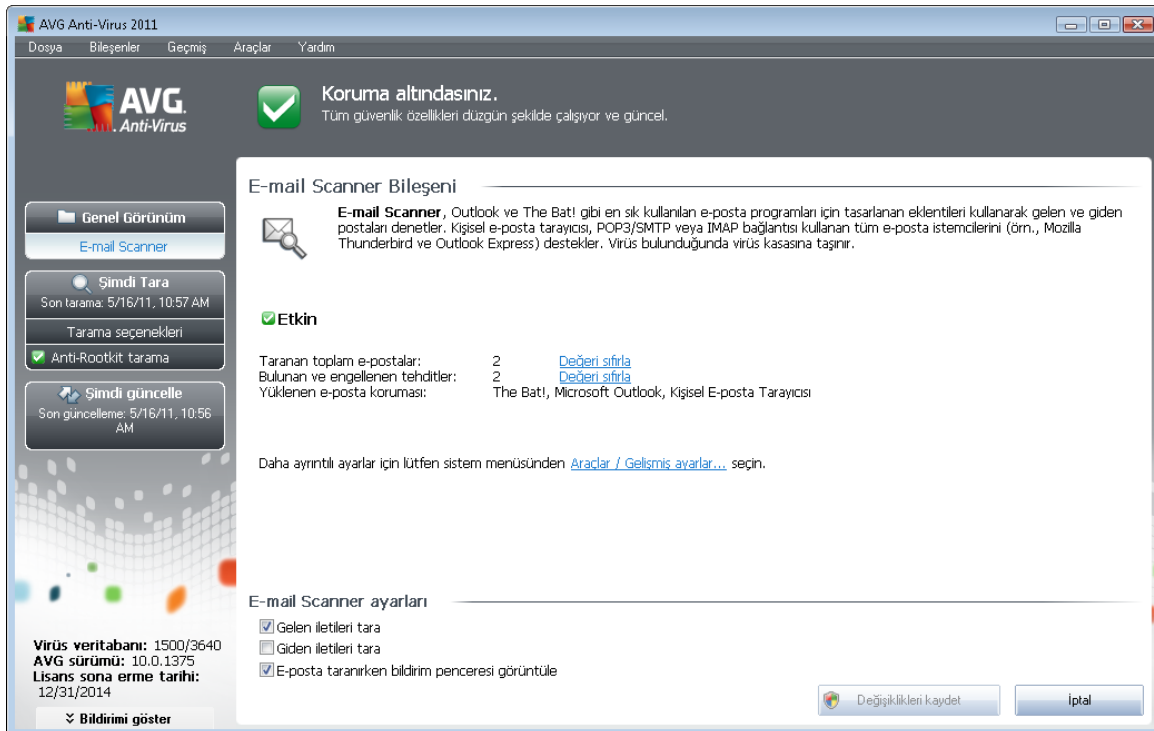
AVG [yüklemesi sırasında](#), e-posta kontrolü için oluşturulmuş otomatik sunucular bulunur: biri gelen e-postaları kontrol etmek, ikincisi ise giden e-postaları kontrol etmek içindir. Bu iki sunucu kullanılarak e-postalar otomatik olarak 110 ve 25 bağlantı noktalarında (*e-posta göndermek/almak için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

Not: AVG E-posta Tarayıcısının sunucu platformlarında kullanılması hedeflenmemiştir!

7.7.2. E-posta Tarayıcısı Arayüzü





E-posta Tarayıcısı bileşeninin iletişim kutusunda bileşenlerin işlevleri, mevcut durumu ve şu istatistiklerle ilgili kısa bilgiler bulabilirsiniz:

- **Taranan toplam e-posta sayısı - E-posta Tarayıcısı** son çalıştırıldığından beri kaç adet e-postanın tarandığı hakkında bilgi verir (*gerekirse bu değer sıfırlanabilir; Öm. istatistiki amaçlar için - Değeri Sıfırla*)
- **Bulunan ve engellenen tehditler - E-posta Tarayıcısı** son çalıştırıldığından beri e-posta mesajları içinde tespit edilen bulaşmaların sayısı hakkında bilgi verir
- **Yüklü e-posta koruma** - Varsayılan ve yüklü e-posta istemcisine ilişkin belirli bir e-posta koruma eklentisi hakkında bilgi verir

E-posta Tarayıcısı ayarları

İletişim kutusunun alt kısmında bileşenin fonksiyonlarının ana özelliklerinden bazılarını düzenleyebileceğiniz **E-posta Tarayıcısı ayarları** adı altında bir bölüm bulunmaktadır.

- **Gelen iletileri tara** - Hesabınıza teslim edilen tüm e-postalarda virüs taraması yapılması için bu öğeyi işaretleyin. Varsayılan olarak, bu öğe açıktır ve bu ayarı değiştirmemeniz önerilir!
- **Giden mesajları tara** - Hesabınızdan gönderilen tüm e-postaların virüslere karşı taranmasını onaylamak için öğeyi işaretleyin. Varsayılan olarak bu öğe kapalıdır.
- **E-posta taranırken bildirim görüntüle** - Postanız [E-posta Tarayıcısı](#) bileşeni ile taranırken sistem tepsisinde AVG simgesi üzerinde görüntülenen bildirim iletişim kutusu aracılığıyla bilgilendirilmek istediğinizi onaylamak için bu öğeyi işaretleyin. Varsayılan olarak, bu öğe açıktır ve bu ayarı değiştirmemeniz önerilir!

E-posta Tarayıcısı bileşeninin gelişmiş konfigürasyonuna **Araçlar/Gelişmiş ayarlar** ögesinden ulaşabilirsiniz ancak gelişmiş yapılandırmanın sadece uzman kullanıcılar tarafından gerçekleştirilmesi önerilmektedir!

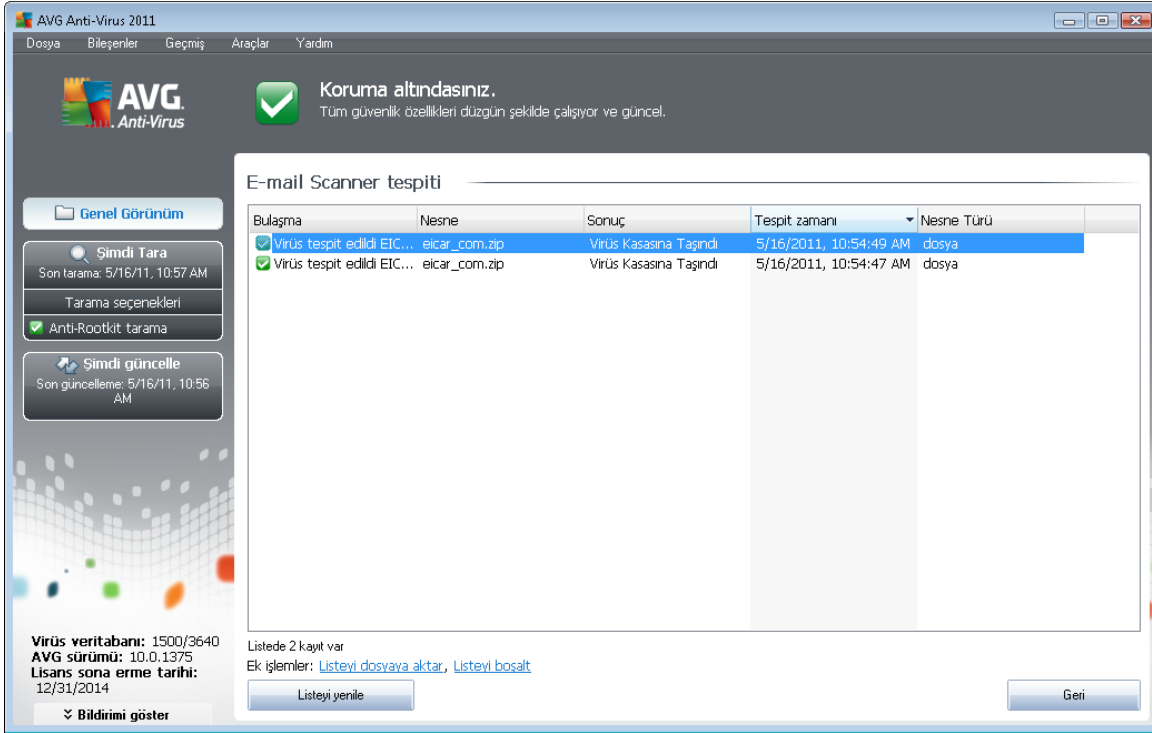
Lütfen dikkat: Yazılım satıcısı, en iyi performansın sunulabilmesi için tüm AVG bileşenlerini kurmuştur. Bunun için iyi bir nedeniniz olmadıkça AVG yapılandırmasını değiştirmeyin. Ayarlarda yapılacak her tür değişiklik sadece deneyimli bir kullanıcı tarafından gerçekleştirilmelidir. AVG yapılandırmasını değiştirmeniz gerekirse sistem menüsünden ilgili öğeyi seçin **Araçlar/Gelişmiş ayarlar** ve yeni açılan [AVG Gelişmiş Ayarlar](#) iletişim kutusunda AVG yapılandırmasını düzenleyin.

Kontrol düğmeleri

E-posta Tarayıcısı arayüzünde bulunan kontrol düğmeleri şunlardır:

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

7.7.3. E-posta Tarayıcısı Tespiti



E-Posta Tarayıcısı Tespiti iletişim kutusunda (*sistem menüsü seçeneği Geçmiş / E-Posta Tarayıcısı Tespiti* üzerinden erişebilirsiniz) **E-Posta Tarayıcısı** bileşeni tarafından tespit edilen tüm bulguların listesini görebilirsiniz. Tespit edilen tüm nesneler için 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 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**).

Kontrol düğmeleri

E-posta Tarayıcısı algılama arayüzünde bulunan kontrol düğmeleri şunlardır:

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



- **Geri** - sizi önce görüntülenen iletişim kutusuna

7.8. Güncelleme Yöneticisi

7.8.1. Güncelleme Yöneticisi Prensipleri

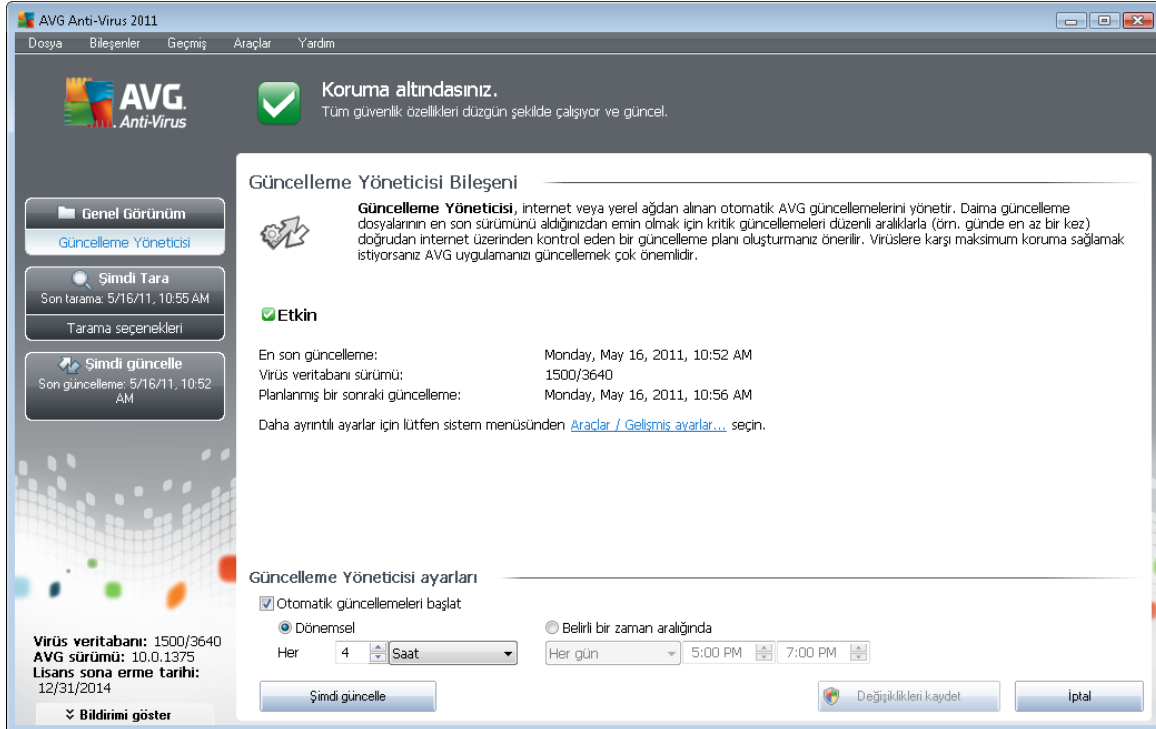
Güvenlik yazılımlarının hiçbirisi, rutin olarak güncellenmediği takdirde sizi çeşitli tehlikelere karşı korumayı garanti edemez! Virüs yazarları, yazılım ve işletim sistemlerinde yararlanabilecekleri güvenlik açıkları aramaktadır. Her gün yeni virüsler, yeni kötü amaçlı yazılımlar ve yeni bilgisayar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

AVG'nizi rutin olarak güncellenmeniz çok önemlidir!

Güncelleme Yöneticisi rutin güncelleme işlemini kontrol etmenize yardımcı olur. Bu bileşen kapsamında, güncelleme dosyalarını Internet'ten ya da yerel ağdan otomatik olarak indirmeyi seçebilirsiniz. Gerekli virüs tanımı güncellemelerinin mümkün ise her gün yapılması gerekmektedir. Daha az önem taşıyan program güncellemeleri haftada bir yapılabilir.

Not: Güncelleme türleri ve seviyeleri hakkında ayrıntılı bilgi edinmek için lütfen [AVG Güncellemeleri](#) bölümünü inceleyin.

7.8.2. Güncelleme Yöneticisi Arayüzü



Güncelleme Yöneticisi'nin arayüzü bileşenin işlevselliği ve geçerli durumu hakkında bilgiler verir ve

İlgili istatistik verilerini sağlar:

- **En yeni güncelleme** - en son veri tabanı güncellemesinin tarihini ve süresini belirler
- **Virüs veritabanı sürümü** - o anda yüklü en son virüs veritabanı sürümünün numarasını tanımlar ve bu numara virüs veritabanı her güncellendiğinde artar
- **Bir sonra programlanan güncelleme** - bir sonraki veritabanı güncellemesinin tarihini ve süresini belirtir

Güncelleme Yöneticisi ayarları

İletişim kutusunun alt kısmında güncelleme işlemi kurallarında bazı değişiklikler yapabileceğiniz **Güncelleme Yöneticisi ayarları** bölümünü görebilirsiniz. Güncelleme dosyalarını otomatik olarak (**Güncellemeyi otomatik başlat**) ya da istek üzerine indirmeyi seçebilirsiniz. Varsayılan olarak **Güncellemeyi otomatik başlat** seçeneği etkindir ve bu ayarı değiştirmeden muhafaza etmeniz önerilir! Güvenlik yazılımlarının doğru şekilde çalışması için en yeni güncelleme dosyalarının düzenli aralıklarla indirilmesi çok önemlidir!

Bunun yanı sıra güncellemenin ne zaman başlatılacağını da belirleyebilirsiniz:

- **Periyodik olarak** - zaman aralığını belirleyin
- **Belirli bir zaman aralığında** - güncellemenin başlatılması gereken günün tam zamanını tanımlayın

Varsayılan olarak her 4 saatte bir güncelleme işlemi yapılır. Değiştirmek için geçerli bir nedeniniz yoksa bu ayarı olduğu şekilde muhafaza etmeniz önerilir!

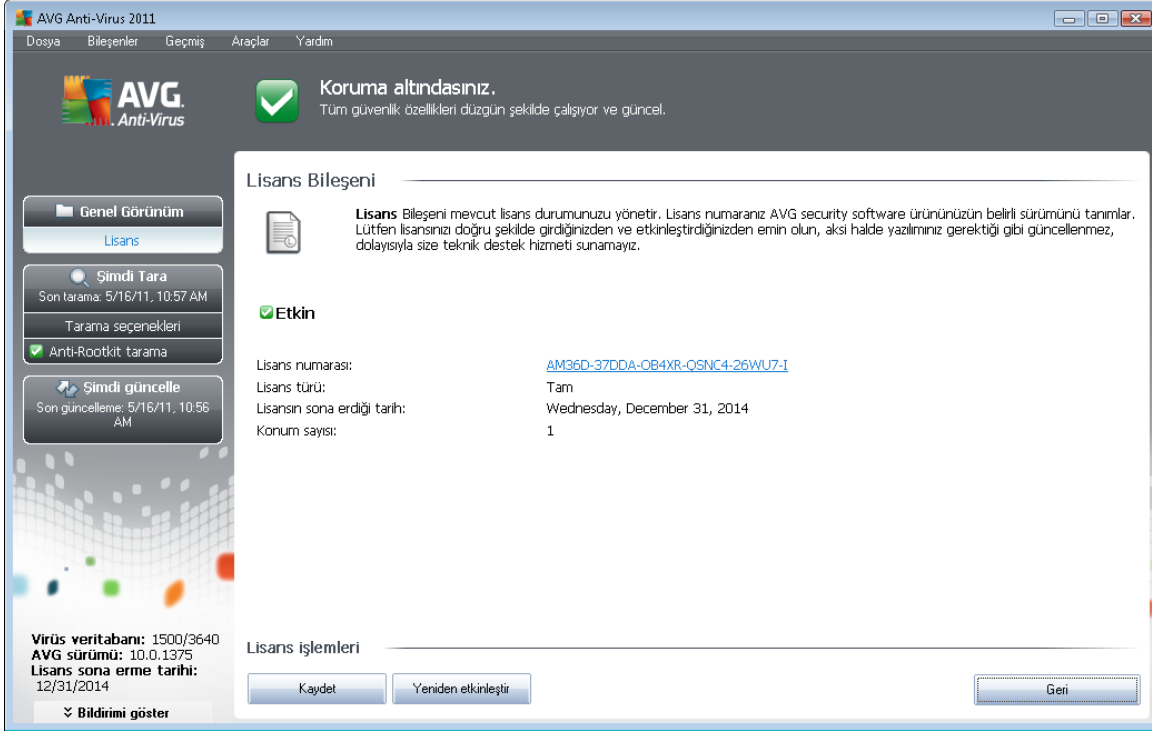
Lütfen dikkat: Yazılım satıcısı, en iyi performansın sunulabilmesi için tüm AVG bileşenlerini kurmuştur. Bunun için iyi bir nedeniniz olmadıkça AVG yapılandırmasını değiştirmeyin. Ayarlarda yapılacak her tür değişiklik sadece deneyimli bir kullanıcı tarafından gerçekleştirilmelidir. AVG yapılandırmasını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

Kontrol düğmeleri

Güncelleme Yöneticisi arayüzünde bulunan kontrol düğmeleri şunlardır:

- **Şimdi güncelle** - istek üzerine [güncelleme işlemini hemen](#) başlatır
- **Değişiklikleri kaydet** - bu iletişim kutusunda yapılan her tür değişikliği kaydetmek ve uygulamak için bu düğmeye basın
- **İptal** - Varsayılan [AVG kullanıcı arayüzüne](#) dönmek için bu düğmeye basın (*bileşenlere genel bakış*)

7.9. Lisans



Lisans bileşeninin arayüzünde bileşenlerin işlevlerini, mevcut durumunu açıklayan kısa metinler ve şu bilgileri bulabilirsiniz:

- **Lisans numarası**- lisans numarasının kısa biçimini verir (*güvenlik nedeniyle son dört simge eksiktir*). Lisans numaranızı girerken çok dikkatli olmalı ve gösterildiği gibi girmelisiniz. Bu yüzden, lisans numarasıyla ilgili bir düzeltme için her zaman "kopyala ve yapıştır" yöntemini kullanmanızı önemle öneririz.
- **Lisans türü** - Yüklenen ürün türünü belirtir.
- **Lisans sonu** -bu tarih, lisans numaranızın geçerlilik süresini belirler. Bu tarihten sonra **AVG Anti-Virus** uygulamasını kullanmaya devam etmek istiyorsanız lisansınızı yenilemeniz gerekir. Lisans yenileme işlemi, [AVG web sitesinden](#) çevrimiçi gerçekleştirilebilir.
- **Kullanıcı sayısı** - **AVG Anti-Virus** programınızı yükleme hakkınız olan çalışma istasyonu sayısıdır.

Kontrol düğmeleri

- **Kaydol** - AVG web sitesi (<http://www.avg.com/>) kayıt sayfasına bağlanır. Lütfen kayıt bilgilerinizi doldurun; sadece AVG ürünlerini kaydettiren müşterilerimiz ücretsiz teknik destek alabilecektir.
- **Yeniden Etkinleştir** - **yükleme işleminin** AVG'yi Kişiselleştir [iletişim kutusuna girilen verilerle](#) AVG'yi Etkinleştir [iletişim kutusunu açar](#). Bu iletişim kutusunda satış numaranızı (

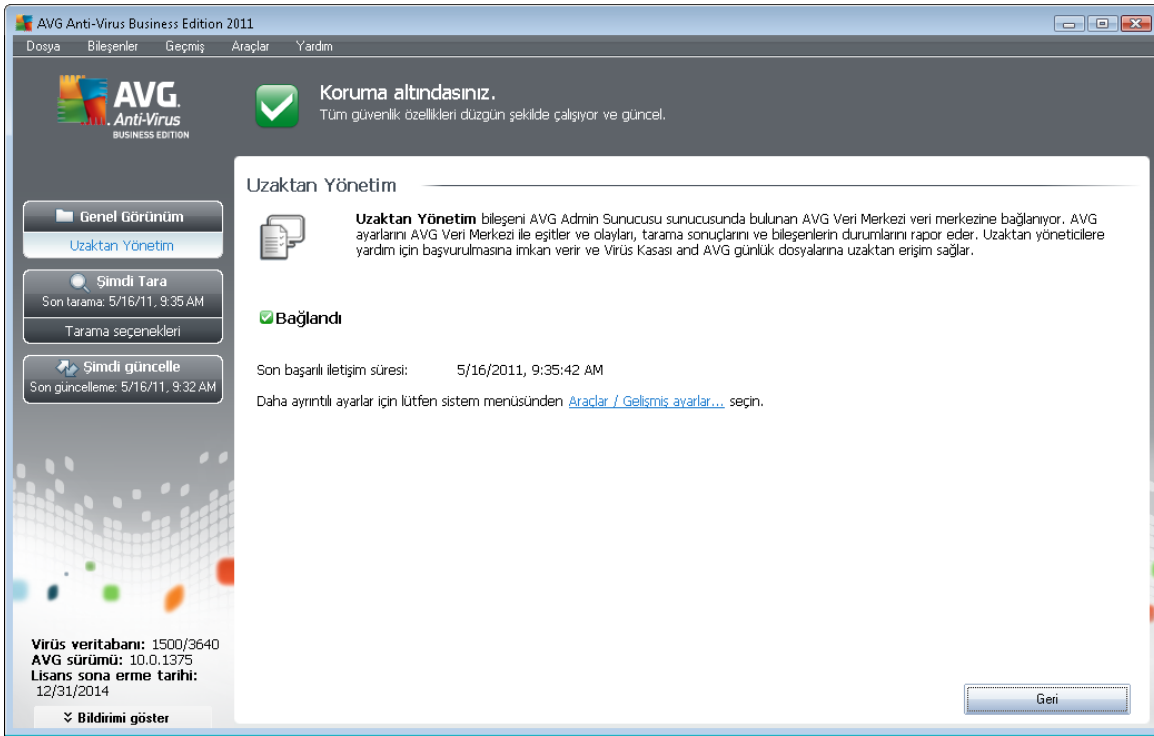


AVG'yi yüklerken kullandığınız numara), ya da eski lisans numaranızı (Örn. yeni bir AVG ürününe geçerken) değiştirmek için lisans numaranızı girebilirsiniz.

Not: AVG Anti-Virus deneme sürümünü kullanıyorsanız, **düğmeler Şimdi satın al ve Etkinleştir** olarak görünür, programın tam sürümünü hemen satın almanızı sağlar. Bir satış numarasıyla yüklenmiş **AVG Anti-Virus** için, **düğmeler Kaydet ve Etkinleştir** olarak görünür.

- **Geri** - varsayılan [AVG kullanıcı arayüzüne](#) dönmek için bu düğmeye basın (*bileşenlere genel bakış*).

7.10. Uzaktan Yönetim



Uzaktan Yönetim bileşeni yalnızca ürününüzün işletme sürümünü yüklemişseniz **AVG Anti-Virus** kullanıcı arayüzünde görüntülenir (*bkz. [Lisans](#) bileşeni*). **Uzaktan Yönetim** iletişim kutusunda, bileşen etkin 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 sitesinden](#) (www.avg.com), **Destek merkezi / İndir / Dokümantasyon** bölümünden indirilebilir.

Kontrol düğmeleri

- **Geri** - varsayılan [AVG kullanıcı arayüzüne](#) dönmek için bu düğmeye basın (*bileşenlere genel bakış*).



7.11. Online Shield

7.11.1. Online Shield İlkeleri

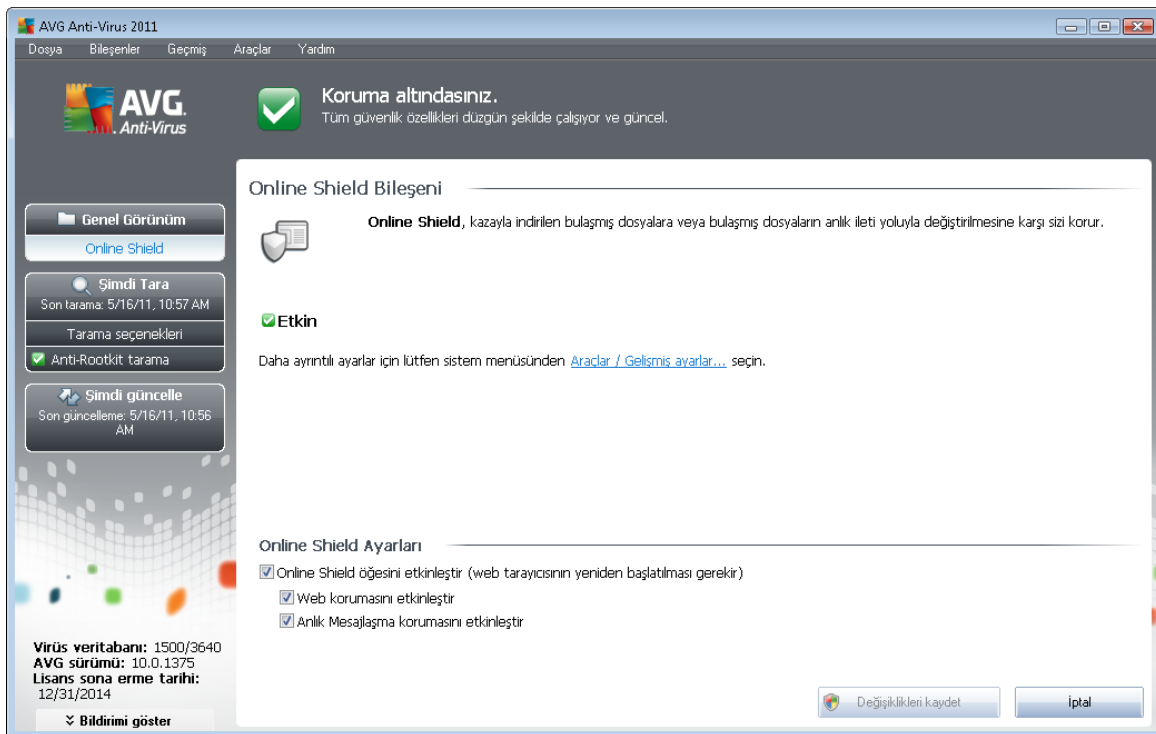
Online Shield, ziyaret ettiğiniz web sitelerinin içeriğini (*muhtemel dosyalar da dahil olmak üzere*), hatta henüz web tarayıcınızda görünmeden ya da bilgisayarınıza indirilmeden önce tarayan gerçek zamanlı bir koruma yöntemidir.

Online Shield, ziyaret ettiğiniz sayfanın tehlikeli javascript içerdiğini tespit ederse, sayfanın görüntülenmesini engeller. Buna ek olarak bir sayfada bulunan zararlı yazılımı tanır ve bilgisayarınıza girişini engellemek için indirme işlemini durdurur.

Not: AVG Online Shield'ın sunucu platformlarında kullanılması hedeflenmemiştir!

7.11.2. Online Shield Arayüzü

Online Shield bileşeninin arayüzünde, bu tür koruma tipinin davranışı tanımlanır. Ek olarak, bileşenin mevcut durumu hakkında bilgiler bulabilirsiniz. Bunun ardından, iletişim kutusunun alt kısmında bu bileşenin işlevlerini düzenleyebileceğiniz için temel seçenekleri bulabilirsiniz:



Online Shield Ayarları

İlk olarak **Online Shield'ı Etkinleştir** öğesini seçerek ya da seçmeyerek **Online Shield'ı** istediğiniz zaman açıp kapatabilirsiniz. Bu seçenek varsayılan olarak etkin ve **Online Shield** bileşeni aktiftir.



Diğer bir yandan, bu ayarları değiştirmek açısından geçerli bir nedeniniz yoksa bileşeni devre dışı bırakmamanızı öneririz. Bu öge işaretlenirse ve **Online Shield** çalışıyorsa, iki yapılandırma seçeneği daha etkinleştirilir:

- **Web korumasını etkinleştir-** bu seçenek **Online Shield** 'in web sitesi içeriğinin taranması gerektiğini onaylar.
- **Anlık Mesajlaşma Korumasını etkinleştir-** **Online Shield**'in anlık mesajlaşma iletişiminin(ör., ICQ, MSN Messenger, ...) virüs içermediğini doğrulamasını istiyorsanız bu ögeyi işaretleyin.

Lütfen dikkat: 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 menüsünden ilgili ögeyi seçin **Araçlar/Gelişmiş ayarlar** ve yeni açılan [AVG Gelişmiş Ayarlar](#) iletişim kutusunda AVG yapılandırmasını düzenleyin.

Kontrol düğmeleri

Online Shield arayüzünde bulunan kontrol düğmeleri şunlardır:

- **Değişiklikleri kaydet**bu iletişim kutusunda yapılan her tür değişikliği kaydetmek ve uygulamak için bu düğmeye basın
- **İptal** - varsayılan [AVG kullanıcı arayüzüne](#) dönmek için bu düğmeye basın (*bileşenler genel görünüm*)

7.11.3. Online Shield Algılaması

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:**

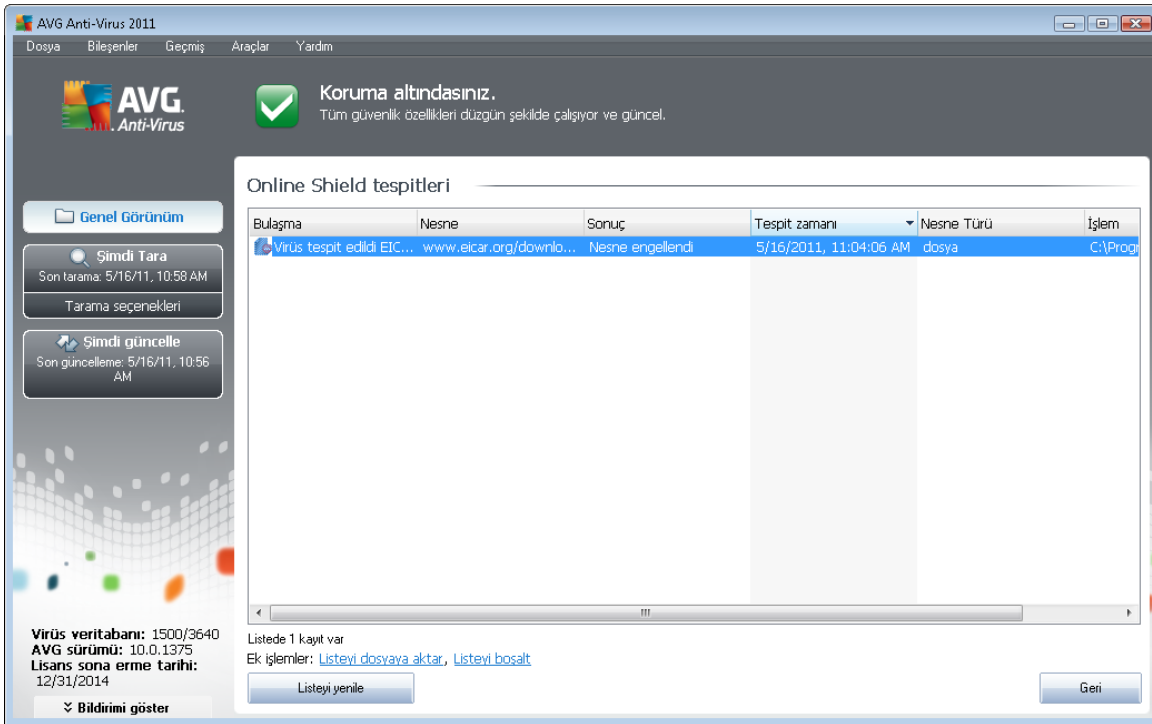
- **Ayrıntıları göster** - bulaşma tespit edildiğinde çalışan işlem ve işlemin tanımı ile ilgili bilgileri bulabileceğiniz yeni bir açılır pencere açmak için, **Ayrıntıları göster** düğmesini



tıklatın.

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

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



Tespit edilen tüm nesneler 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 uyaran 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, **Online Shield** tarafından algılanan bulgular listesini günceller. **Geri** düğmesi, sizi varsayılan [AVG kullanıcı arayüzüne](#) geri götürür (*bileşenlere genel bakış*).

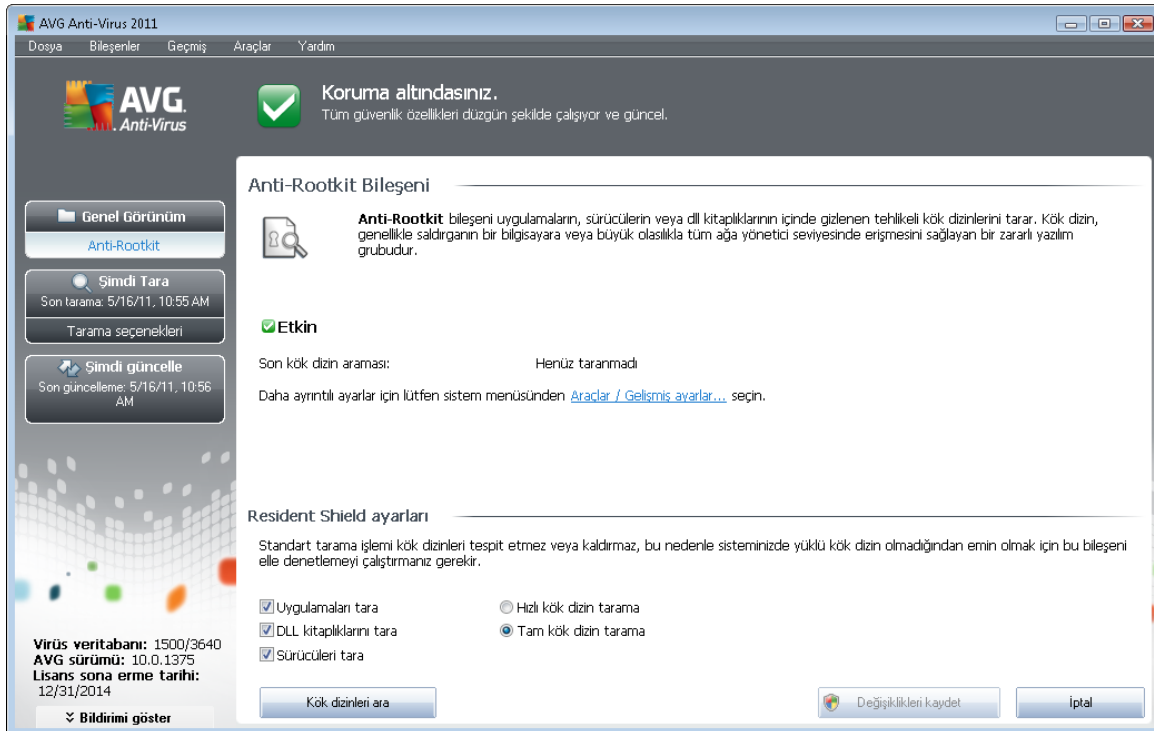
7.12. Anti-Rootkit

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.

7.12.1. Anti-Rootkit Prensipleri

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

7.12.2. Rootkit Önleme Arayüzü



Anti-Rootkit kullanıcı arayüzü bileşenlerin işlevleri ile ilgili kısa bir açıklama sağlar, bileşenin mevcut durumu konusunda bilgilendirir 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.



Lütfen dikkat: 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.

Anti-Rootkit ayarları

İletişim penceresinin alt kısmında kök dizin varlığı taraması sırasında kullanılan işlemlerden bazılarını düzenleyebileceğiniz **Anti-Rootkit ayarlarını** bulabilirsiniz. Öncelikle, taranmasını istediğiniz nesneleri belirlemek üzere ilgili kutuları işaretleyin:

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

Bunun ardından kök kullanıcı tarama modunu da seçebilirsiniz:

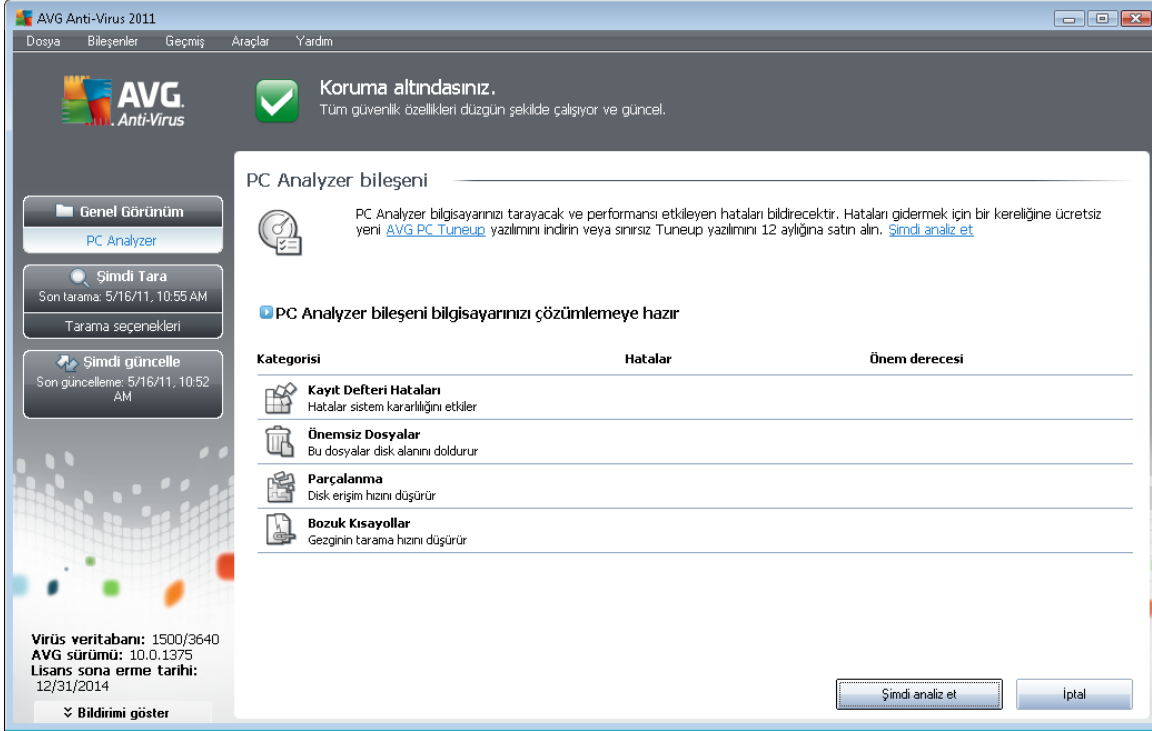
- **Hızlı kök dizin tarama** - çalışan tüm işlemleri, yüklü sürücüler ve sistem klasörlerini (genellikle c:\Windows) tarar
- **Tam kök dizin tarama** - çalışan tüm işlemleri, yüklü sürücüler, sistem klasörünü (genellikle c:\Windows), ayrıca tüm yerel diskleri (flash disk dahil ancak disket/CD sürücüler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

Kontrol düğmeleri

- **Kök dizinleri tara** - kök dizin taraması [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 kullanıcı arayüzüne](#) (bileşenlere genel bakış) dönmek için bu düğmeye basın.
- **İptal** - yapılan değişiklikleri kaydetmeksizin varsayılan [AVG kullanıcı arayüzüne](#) (bileşenlere genel bakış) dönmek için bu düğmeye basın.

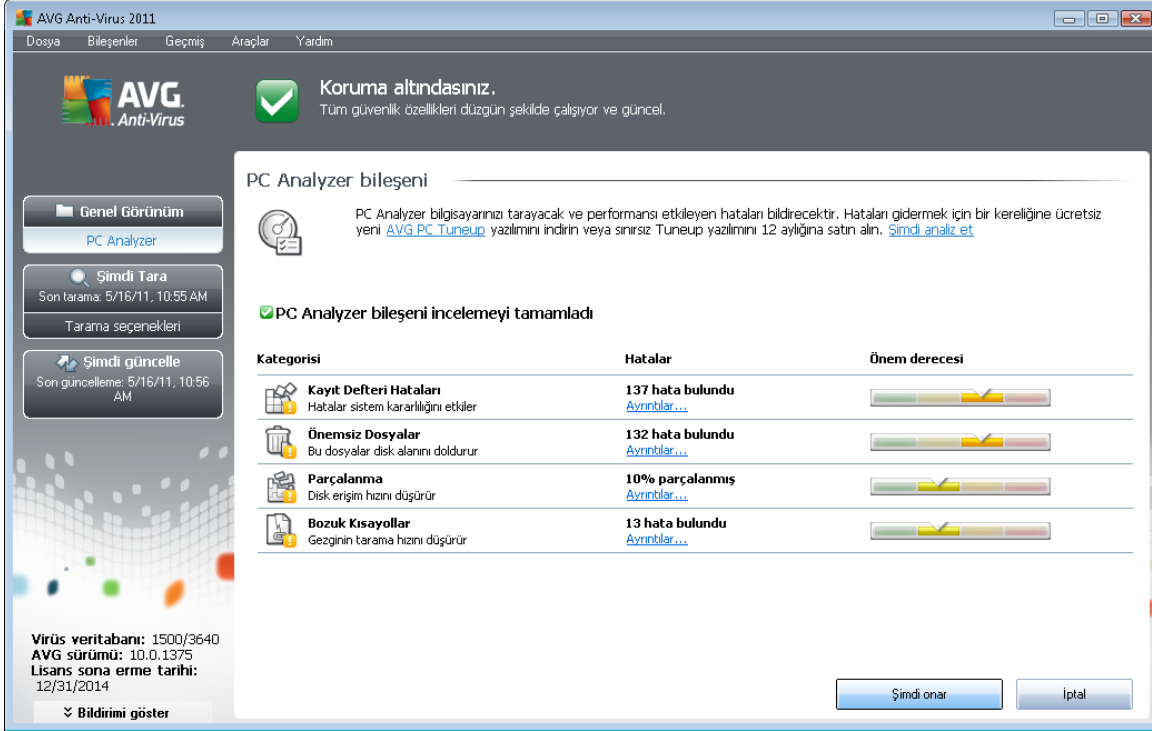
7.13. PC Analyzer

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:



- **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:



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 analiz işlemini 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** - analizin çalışmasını durdurmak veya analiz tamamlandıktan sonra varsayılan **AVG kullanıcı arayüzüne** (bileşenler genel görünümüne) geri dönmek için bu düğmeye basın

7.14. Kimlik Koruması

AVG Kimlik Koruması, 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 odaklanan bir kötü amaçlı yazılıma karşı üründür. PC'nizde çalışan tüm programların doğru çalıştığından emin olmanızı sağlar. **AVG Kimlik Koruması**, sürekli olarak şüpheli davranışları belirleyip engeller ve tüm yeni kötü amaçlı yazılımlara karşı bilgisayarınızı korur.

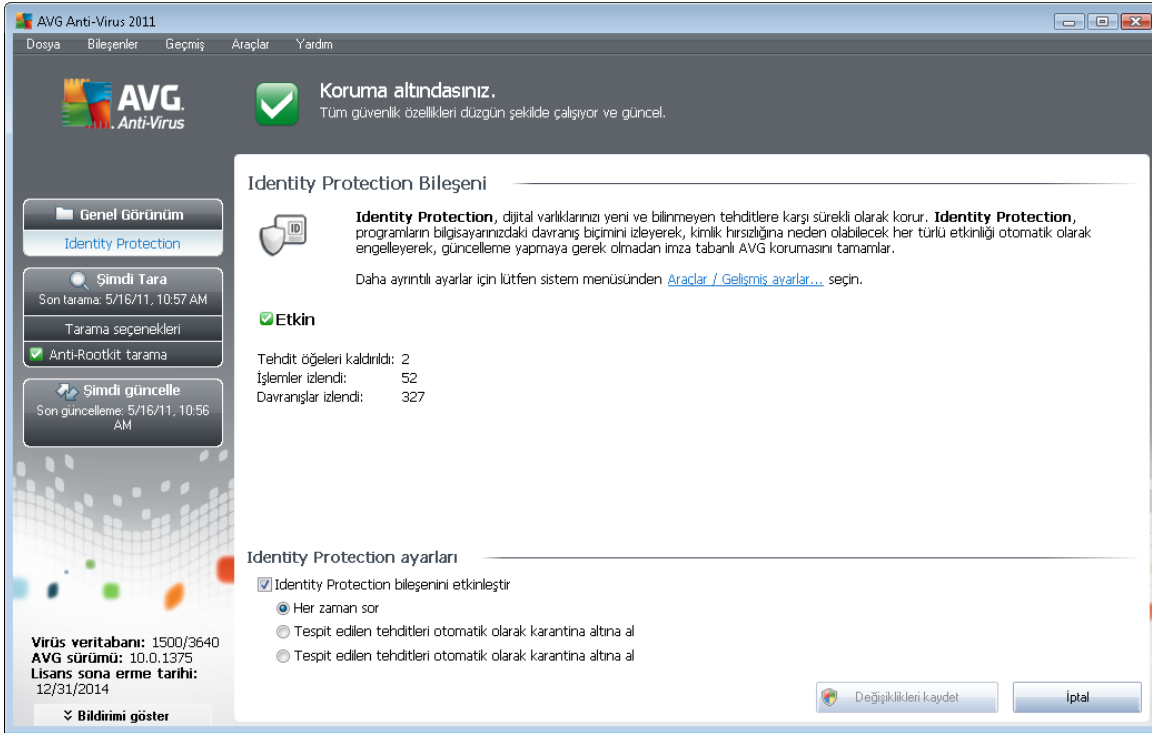


7.14.1. Kimlik Koruması Prensipleri

AVG 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. Kötü amaçlı yazılımlar karmaşıklıklaştıkça ve PC'nizi kimlik hırsızlığı için uzak saldırılara karşı açık hale getiren normal program biçiminde geldikçe, **AVG Kimlik Koruması** bu yeni yürütme tabanlı kötü amaçlı yazılımlara karşı bilgisayarınızı korur. [AVG Virüsten Koruma](#) programının tamamlayıcısıdır ve imza mekanizmasını ve tarama özelliğini kullanarak sizi dosya tabanlı ve bilinen virüslere karşı korur.

PC'nizin korumasını tamamlamanız için hem [AVG Virüsten Koruma](#) hem de AVG Kimlik Koruması bileşenlerini yüklemenizi önemle öneririz.

7.14.2. Kimlik Koruması Arayüzü



Kimlik Koruması bileşeni, bileşenin temel işlevi, durumu ve bazı istatistiksel veriler hakkında kısa açıklamalar sunar:

- **Kötü amaçlı yazılım öğeleri kaldırıldı** - 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

Kimlik Koruması ayarları



İletişim kutusunun alt kısmında bileşen işlevlerinin bazı temel özelliklerini düzenleyebileceğiniz **Kimlik Koruması ayarları** bölümü bulunmaktadır:

- **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

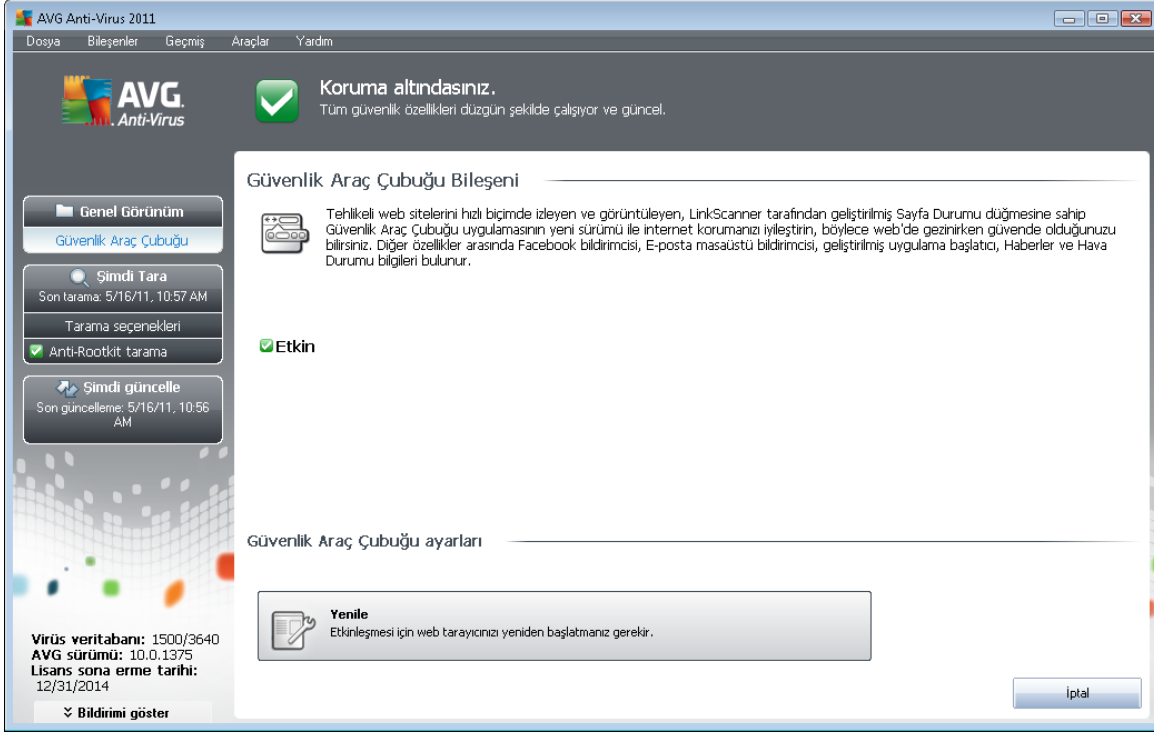
Kontrol düğmeleri

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 kullanıcı arayüzüne](#) dönmek için bu düğmeye basın (*bileşenlere genel bakış*)

7.15. Güvenlik Araç Çubuğu

Güvenlik Araç Çubuğu, isteğe bağlı bir web tarayıcısı araç çubuğudur ve web'de gezinirken gelişmiş AVG koruması ile çeşitli özellik ve araçlar sağlamaktadır. Şu anda **Güvenlik Araç Çubuğu** Internet Explorer (6.0 veya üzeri) ve Mozilla Firefox (3.0 veya üzeri) web tarayıcıları tarafından desteklenmektedir:



Güvenlik Araç Çubuğu bileşeninin tüm ayarlarına doğrudan web tarayıcınızdaki [Güvenlik Araç Çubuğu](#)ndan erişilebilir.



8. AVG Security Toolbar

AVG Security Toolbar [LinkScanner](#) bileşeni ile birlikte çalışan yeni bir araçtır. **AVG Security Toolbar**, [LinkScanner](#) işlevlerini denetlemek ve davranışını ayarlamak için kullanılabilir.

AVG Anti-Virus yüklemesi sırasında araç çubuğunu yüklemeyi seçerseniz, araç çubuğu web tarayıcınıza (*Internet Explorer 6.0 ya da üstü ve Mozilla Firefox 3.0 ya da üstü*) otomatik olarak eklenir. Diğer İnternet tarayıcıları şu anda desteklenmemektedir.

Not: Başka bir İnternet tarayıcısı (örn. Avant Browser) kullanmanız durumunda beklenmedik bir davranışla karşılaşabilirsiniz.

8.1. AVG Security Toolbar Arayüzü

AVG Security Toolbar, **MS Internet Explorer** (sürüm 6.0 ya da üstü) ve **Mozilla Firefox** (sürüm 3.0 ya da üstü) ile çalışmak üzere tasarlanmıştır. **AVG Security Toolbar**'ı yüklemeye karar verirsiniz ([AVG yükleme süreci](#) sırasında bileşeni yüklemek isteyip istemediğiniz sorulur), bileşen web tarayıcınızda adres çubuğunun hemen altına yerleştirilecektir:



AVG Security Toolbar aşağıdakileri içerir:

8.1.1. AVG logosu düğmesi

Bu düğme genel araç çubuğu öğelerine erişim sağlar. [AVG web sitesine](#) yönlendirilmek için logo düğmesini tıklayın. AVG simgesinin yanındaki işaretçi tıklatıldığında aşağıdakiler açılır:

- **Araç Çubuğu Bilgisi** - araç çubuğunun koruyucu özelliklerinin yanı sıra **AVG Security Toolbar** ana sayfasına giden bir bağlantı bulunur
- **AVG'yi Başlat** - **AVG Anti-Virus** [kullanıcı arayüzünü açar](#)
- **AVG Bilgileri** - **AVG Anti-Virus** ile ilgili önemli güvenlik bilgileri bağlantısını izleyen şu bağlantılara sahip bir bağlam menüsü açar:
 - **Tehditler Hakkında** - en son çıkan tehditlerle ilgili bilgiler, virüs temizleme önerileri, AVG güncelleme bilgileri, [Virüs veritabanına](#) erişim ve ilgili diğer bilgiler hakkında en önemli verileri sağlayan sayfada [AVG web sitesini](#) açar
 - **AVG Haberleri** - AVG ile ilgili en güncel basın açıklamalarını sağlayan web sayfasını açar
 - **Geçerli Tehdit Düzeyi** - web'de geçerli tehdit seviyesinin grafik görünümünü içeren virüs laboratuvarı web sayfasını açar
 - **AVG Tehdit Laboratuvarı** - [AVG Site Raporları](#) web sitesini açar. Burada, belirli

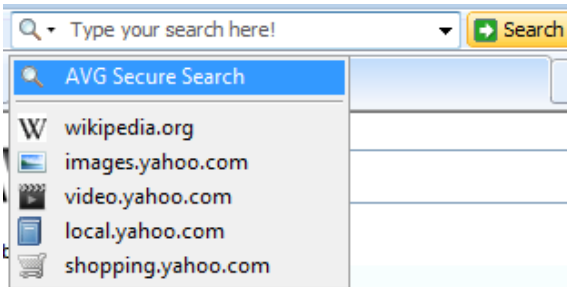
tehditleri adına göre arayabilir ve her biri hakkında ayrıntılı bilgiler edinebilirsiniz

- **Seenekler - AVG Security Toolbar** ayarlarınızı gereksinimlerinize göre dzenleyebileceğiniz bir yapılandırma iletiřim kutusu aar (bkz. sonraki blm, [AVG Security Toolbar Seenekleri](#))
- **Gemiři Sil - AVG Security Toolbar** ierisinde tm gemiři silmenize veya arama gemiřini, tarayıcı gemiřini, indirme gemiřini ve erezleri ayrı olarak silmenize olanak verir.
- **Gncelle - AVG Security Toolbar**
- **Yardım** - bu yardım dosyasını ama, [AVG teknik desteęi](#) ile iletiřim kurma, rnle ilgili geribildirimlerinizi gnderme ya da ara ubuęunun geerli srm ile ilgili ayrıntıları grntleme seeneklerini sunar

8.1.2. AVG Secure Search (powered by Google) tarafından desteklenen arama kutusu

AVG Secure Search (powered by Google) kutusu web'i AVG Secure Search (powered by Google) kullanarak aramanın kolay ve gvenli yoludur. Arama kutusuna bir kelime veya cmlcik girin, **Ara** dğmesine veya **Enter** tuřuna basarak doęrudan AVG Secure Search (powered by Google) sunucusunda aramayı bařlatın; bu ařamada hangi sayfanın grntlenmekte olduęu nemli deęildir. Arama kutusunda arama gemiřiniz de listelenir. Arama kutusundan yapılan aramalar [Search-Shield](#) koruması kullanılarak analiz edilir.

Alternatif olarak, arama alanında Wikipedia'ya veya bazı dięer belli arama hizmetlerine geebilirsiniz, resme bakın:



8.1.3. Sayfa Durumu

Doęrudan ara ubuęundan, bu dğme o anda grntlenen web sayfasını [Surf-Shield](#) bileřeninin kriterine gre deęerlendirmesini grntler:

-  - Baęlantı verilen sayfa gvenlidir
-  - Sayfa bir bakıma řphelidir.
-  - Sayfa tehlikeli olabilecek sayfalara baęlantılar ieriyor.
-  - Baęlantı verilen sayfa etkin tehlikeler ieriyor! Kendi gvenlięiniz iin, bu sayfayı



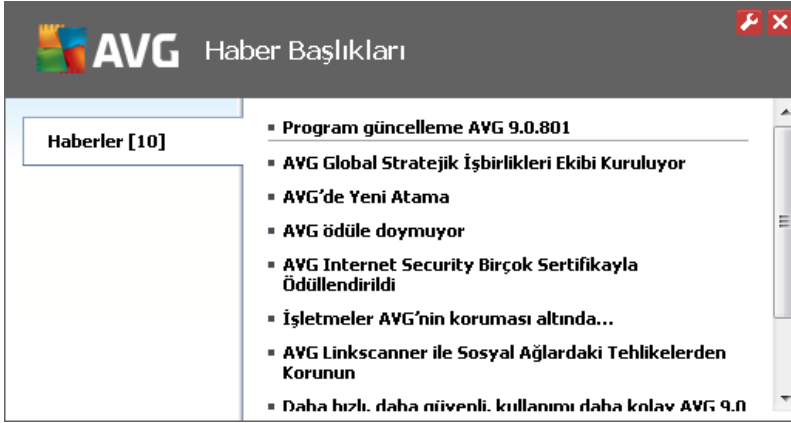
ziyaret etmenize izin verilmeyecek.

- ? - Sayfaya erişilemediğinden taranamadı.

Belirli web sayfası hakkında ayrıntılı veriler içeren bir bilgi paneli açmak için düğmeyi tıklayın.

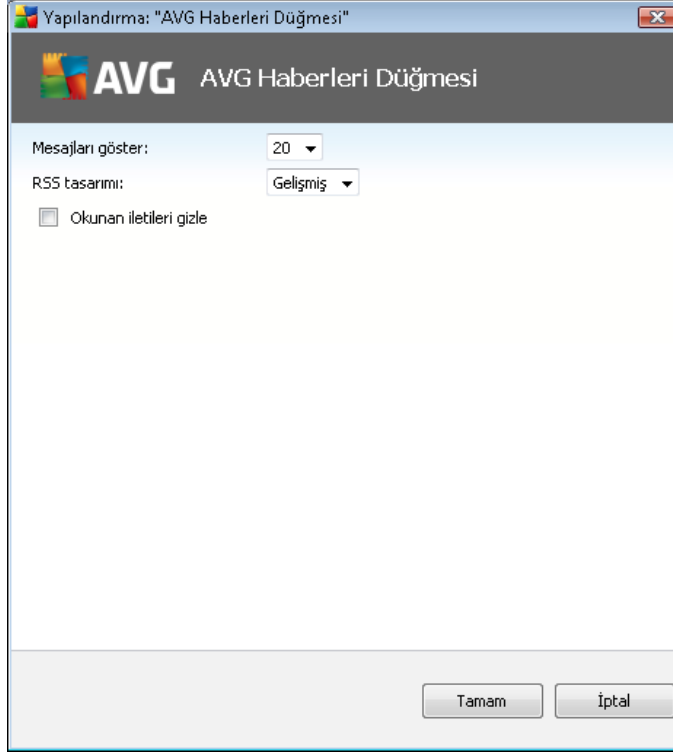
8.1.4. AVG Haberleri

Doğrudan **AVG Security Toolbar** içerisinde, bu düğme hem basından gelen hem de şirketin basın bültenlerinden AVG ile ilgili en son **Haber başlıklarının** genel görünümünü açar:



Sağ üst köşede, iki kırmızı kontrol düğmesi görebilirsiniz:

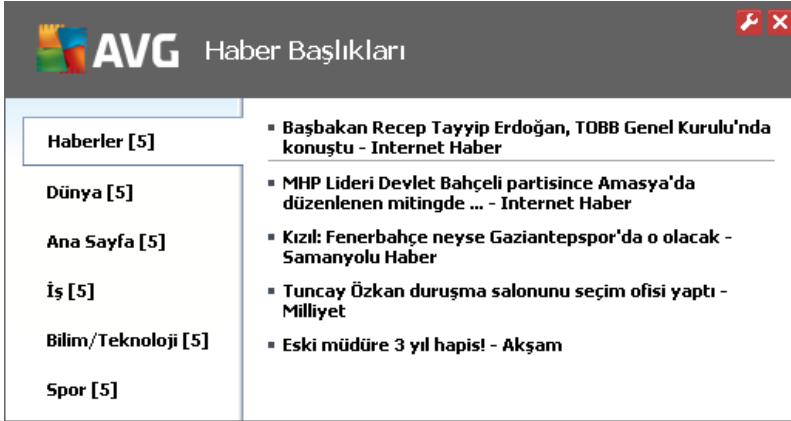
-  - söz konusu düğme, **AVG Security Toolbar** içerisinde **AVG Haberleri** düğmesinin parametrelerini belirtebileceğiniz düzenleme iletişim kutusunu açar:



- **İletileri göster** - bir seferde görüntülenmesini istediğiniz ileti sayısını değiştirebilirsiniz
- **RSS tasarımı** - haberler genel görünümünün mevcut ekranı için Gelişmiş/Temel mod arasında seçim yapın (*varsayılan olarak, Gelişmiş mod seçilidir - yukarıdaki resme bakın*)
- **Okunmuş iletileri gizle** - okunmuş her iletinin artık görüntülenmemesi gerektiğini onaylamak için bu öğeyi işaretleyin, böylece yeni iletiler alınabilir
-  - o anda açık olan haberler genel görünümünü kapatmak için bu düğmeyi tıklatın

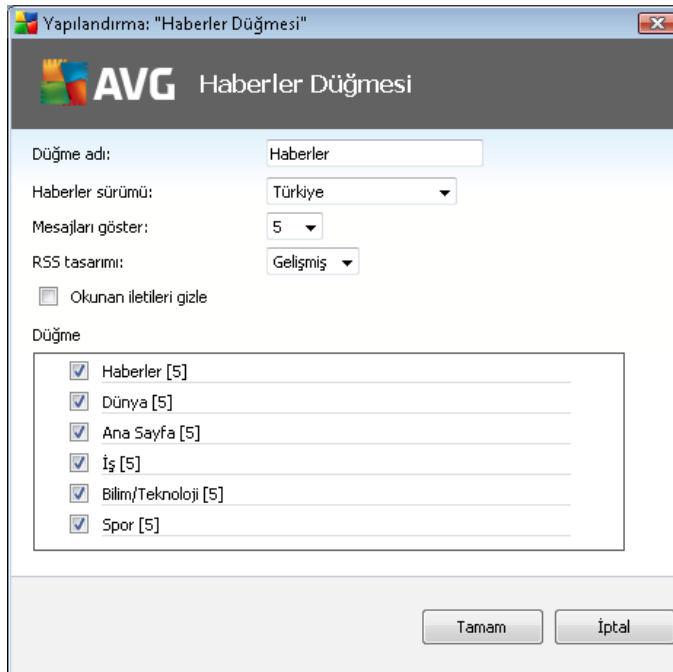
8.1.5. Haberler

AVG Security Toolbar içerisinde doğrudan yapılanla aynı biçimde, bu düğme, birden fazla bölüme ayrılmış seçili medyadan en son haberlerin genel görünümünü açar:



Sağ üst köşede, iki kırmızı kontrol düğmesi görebilirsiniz:

-  - söz konusu düğme, **AVG Security Toolbar** içerisinde **Haberler** düğmesinin parametrelerini belirtebileceğiniz düzenleme iletişim kutusunu açar:



- **Düğme adı - AVG Security Toolbar**
- **Haberler sürümü** - seçili bölgeden haberleri görüntülemek için listeden bir ülke seçin
- **İletileri göster** - bir seferde görüntülenecek ileti sayısını belirtin
- **RSS tasarımı** - haberler genel görünümünün tasarımını seçmek için Temel/Gelişmiş seçenekleri arasından seçim yapın (**varsayılan olarak gelişmiş tasarım ayarlanmıştır, yukarıdaki resme**



bakın)

- **İletileri gizle** - okunmuş tüm iletilerin haberler genel görünümünde artık gösterilmemesi ve yeni bir başlıkla değiştirilmemesi gerektiğini onaylamak için bu öğeyi işaretleyin
- **Düğme görünümleri** - bu alanda haberlerin, **AVG Security Toolbar** haberler genel görünümünde hangi sırayla gösterilmesi gerektiğini ayarlayabilirsiniz
 - - o anda açık olan haberler genel görünümünü kapatmak için bu düğmeyi tıklatın

8.1.6. Geçmiş sil

Bu düğmeyi kullanarak, tarayıcınızın geçmişini **AVG logosu -> Geçmiş sil** seçeneği ile sildiğiniz gibi silebilirsiniz.

8.1.7. E-posta Bildiricisi

E-posta Bildiricisi düğmesi, yeni gelmiş e-posta iletileri hakkında bilgilendirilme seçeneğini doğrudan **AVG Security Toolbar** arayüzünde etkinleştirmenize olanak verir. Bu düğme, e-posta hesabınızın ve e-posta görüntüleme kurallarınızın parametrelerini tanımlayabileceğiniz şu iletişim kutusunu açar. Lütfen bu iletişim kutusundaki talimatları izleyin:

- **Hesap türü** - E-posta hesabınızın kullandığı protokol türünü belirtir. Şu alternatifler arasından seçim yapabilirsiniz: *Gmail*, *POP3* veya aşağı açılır menüde *Diğer* öğesinden sunucu adını seçebilirsiniz (*şu anda, Yahoo! JP Mail veya Hotmail*). Hesabınızın kullandığı e-posta sunucusu türünden emin değilseniz e-posta sağlayıcınızdan veya internet servis sağlayıcınızdan bilgi almaya çalışın.

- **Giriş** - Aşağıdaki bölümde *e-posta adresinizi* tam olarak ve ilgili *parolanızı* sağlayın. *Otomatik Giriş* seçeneğini işaretli bırakın, böylece verileri tekrar tekrar girmek zorunda kalmazsınız.
- **Test hesabı** - Bu düğmeyi girilen ayrıntıları test etmek için kullanın.
- **Sıfırlama Ayarları** - Yukarıda girilen e-posta adresi ayrıntılarını hızlı bir şekilde kaldırır.
- **Yeni e-posta olup olmadığını her ... dakikada bir kontrol et** - Yeni e-posta iletilerinin kontrol edileceği zaman aralığını tanımlayın (*aralık 5 ile 120 dakika arasındadır*) ve yeni e-postanın geldiği hakkında ne zaman ve nasıl bilgilendirileceğinizi belirtin.
- **Yeni e-posta uyarılarına izin ver** - Yeni e-postalar alındığında görüntülenecek bildirimleri devre dışı bırakmak için bu seçeneğin işaretini kaldırın.
 - **Yeni e-posta alındığında sesli uyarı ver** - Yeni e-posta mesajları alındığında oynatılacak sesli uyarıları devre dışı bırakmak için bu seçeneğin işaretini kaldırın.
 - **Uyarı penceresini 5 saniyenin ardından kapat** - Yeni e-posta mesajları alındığında görüntülenen uyarıyı 5 saniyenin ardından otomatik olarak kapatmak için bu seçeneği işaretleyin.

8.1.8. Hava Durumu Bilgileri

Hava Durumu düğmesi, doğrudan **AVG Security Toolbar** arayüzü içinden seçtiğiniz hedefteki mevcut sıcaklıkla ilgili bilgiler verir (*her 3-6 saatte bir güncellenir*). Ayrıntılı hava durumu bilgilerini içeren yeni bir bilgi paneli açmak için bu düğmeyi tıklayın:



Brno, CZ
[[konum değiştir](#)]

 **13° C**

Rüzgar hızı: 11,27 km/s
Gün doğumu: 05:08
Gün batımı: 20:29

 **PZT**
Merhaba: 18 °C
Lo: 8 °C

 **SAL**
Merhaba: 21 °C
Lo: 9 °C

Güncellenmiş 05/16/2011 10:02:01 **YAHOO! NEWS** [Tam Hava Durumu >](#)

Düzenleme seçeneklerinde şunlar bulunur:

- **Konumu değiştir** - **Konumunuzu arayın** adlı yeni bir iletişim kutusu açmak için **Konumu değiştir** metnini tıklayın. İstediğiniz konumun adını metin alanına yazın ve **Ara** düğmesini tıklayarak onaylayın. Sonra, aynı adın tüm konumlar listesinden aradığınız hedefi seçin. Son



olarak, seçili konum için hava durumu bilgilerini sağlayan bilgi penceresi görüntülenecektir.

- **Fahrenheit/Santigrat derece dönüştürücü** - bilgi panelinin sağ üst köşesinde, Fahrenheit ve Santigrat derece ölçekleri arasında seçim yapabilirsiniz. Seçiminize bağlı olarak, sıcaklık bilgileri seçili ölçekte verilecektir.
- **Tam Hava Tahmini**- tam ve ayrıntılı hava tahminiyle ilgileniyorsanız, özelleştirilmiş hava durumu web sitesine ulaşmak için **Tam Hava Tahmini** bağlantısını kullanın.

8.1.9. Facebook

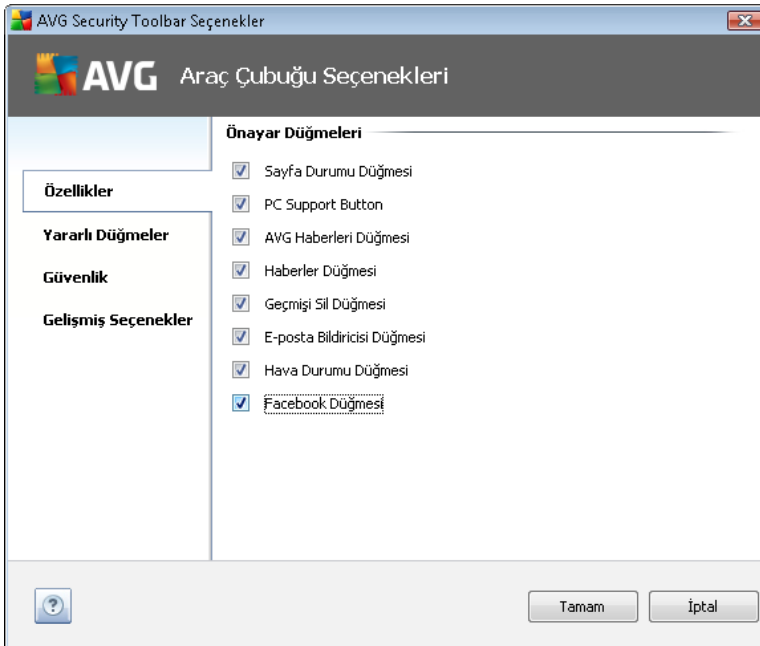
Facebook düğmesi, [Facebook](#) sosyal ağına doğrudan **AVG Security Toolbar**'dan bağlanmanıza olanak verir. Bu düğmeyi tıklattın, böylece giriş davetiyesi görüntülenir. **Facebook girişi** iletişim kutusunu açmak için tekrar tıklattın. Erişim verilerinizi girin ve **Bağlan** düğmesine basın. Henüz [Facebook](#) hesabınız yoksa, doğrudan **Facebook'a Kayıt Ol** bağlantısını kullanarak bir hesap oluşturabilirsiniz.

[Facebook](#) kayıt sürecini bitirdikten sonra, **AVG Sosyal Uzantısı** uygulamasına izin vermek için davet edileceksiniz. Bu uygulama araç çubuğu için işlevsel olarak gereklidir - [Facebook](#) bağlantısına bu nedenle izin vermeniz önerilir, bu yüzden çalışmasına izin verdiğinizden emin olun. Ardından, [Facebook](#) bağlantısı etkinleştirilir ve **AVG Security Toolbar** içindeki **Facebook** düğmesi standart [Facebook](#) menü seçeneklerini sunar.

8.2. AVG Security Toolbar Seçenekleri

Tüm **AVG Security Toolbar** parametrelerinin yapılandırılmasına **AVG Security Toolbar** paneli içinden doğrudan erişilebilir. Düzenleme arayüzü, **Araç Çubuğu Seçenekleri** adlı yeni iletişim kutusunda dört bölüme ayrılarak **AVG / Seçenekler** araç çubuğu menü öğesinden açılır:

8.2.1. Genel Sekmesi

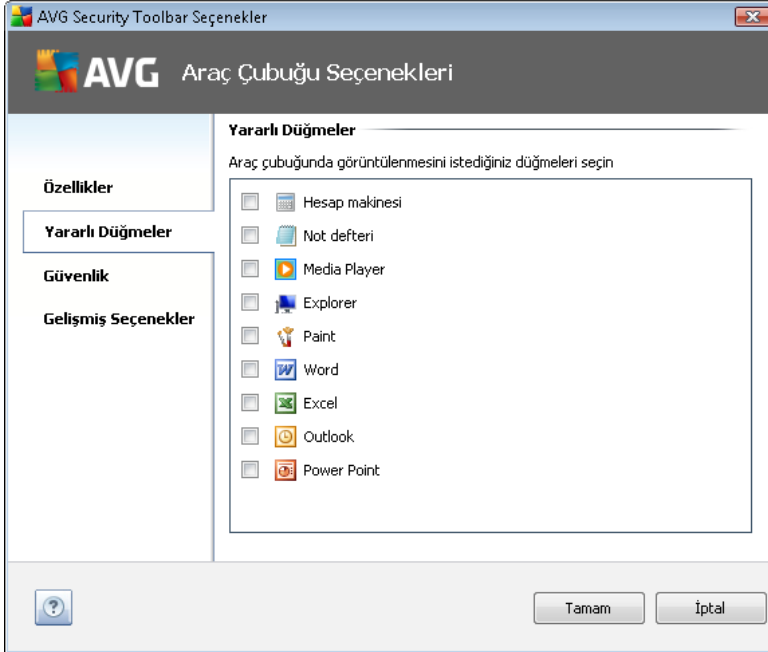




Bu sekmede, **AVG Security Toolbar** panelinden görüntülenmesi veya gizlenmesi gereken araç çubuğu kontrol düğmelerini belirtebilirsiniz. İlgili düğmeyi görüntülemek istediğiniz durumlarda seçeneğini işaretleyin. Her araç çubuğu düğmesinin işlevinin ayrıntılarını da bulabilirsiniz:

- **Sayfa Durumu Düğmesi** - bu düğme o anda açık olan sayfanın güvenlik durumu hakkında bilgilerin **AVG Security Toolbar**
- **AVG Haberler Düğmesi** - düğme, AVG ile ilgili en son basın açıklamalarını içeren bir web sayfası açar
- **Haberler Düğmesi** - düğme, günlük basın haberlerine yapılandırılmış bir genel bakış sağlar
- **Geçmiş Sil Düğmesi** - bu düğme Tüm geçmişi sil veya Arama geçmişini sil, Tarayıcı geçmişini sil, İndirme geçmişini sil veya Tanımlama bilgilerini sil işlemlerini doğrudan AVG Security Toolbar panelinden yapmanıza olanak verir
- **E-posta Bildirici Düğmesi** - bu düğme yeni gelen e-posta iletilerinin **AVG Security Toolbar** arayüzü içinde görüntülenmeye olanak sağlar
- **Hava Durumu Düğmesi** - bu düğme seçili bir konumdaki hava durumu bilgilerini hemen gösterir
- **Facebook Düğmesi** - bu düğme [Facebook](https://www.facebook.com) sosyal ağına doğrudan bağlantı sunar

8.2.2. Yararlı Düğmeler Sekmesi



Yararlı Düğmeler sekmesi, bir listeden uygulamalar seçmenizi ve simgelerinin araç çubuğu arayüzünde görüntülenmesini sağlar. Simge, ilgili uygulamayı hemen başlatmak için hızlı bir bağlantı görevi görür.

8.2.3. Güvenlik Sekmesi

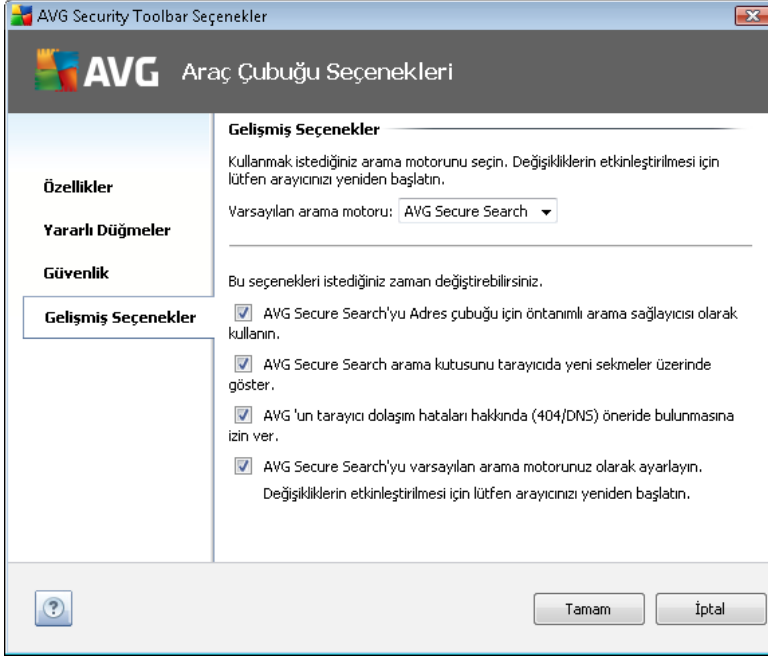


Güvenlik sekmesi iki bölüme ayrılmıştır, **AVG Tarayıcı Güvenliği** ve **Derecelendirmeler**, burada belirli onay kutularını kullanmak istediğiniz **AVG Security Toolbar** işlevselliğini ayarlamak için işaretleyebilirsiniz:

- **AVG Tarayıcı Güvenliği** - **Search-Shield** ve/veya **Surf-Shield** hizmetini etkinleştirmek veya kapatmak için bu öğeyi işaretleyin
- **Derecelendirmeler** - kullanmak istediğiniz **Search-Shield** bileşeni yoluyla arama sonuçları derecelendirmeleri için kullanılan grafiksel sembolleri seçin:
 -  sayfa güvenli
 -  sayfa şüpheli gibi
 -  sayfa tehlikeli olabilecek sayfalara bağlantılar içeriyor
 -  sayfa etkin tehlikeler içeriyor
 -  sayfaya erişilemedi ve bu yüzden taranamadı

Bu belirli tehlike seviyesi hakkında uyarılmak istendiğinizi onaylamak için ilgili seçeneği işaretleyin. Ancak, etkin ve zararlı tehlikeleri içeren sayfalara atanan kırmızı işaretin görüntüsü kapatılamaz. **Tekrar, değiştirmeniz için geçerli bir nedeniniz yoksa program satıcısı tarafından ayarlanan varsayılan yapılandırmayı korumanız önerilir.**

8.2.4. Gelişmiş Seçenekler Sekmesi



Gelişmiş Seçenekler sekmesinde ilk olarak varsayılan olarak hangi arama motorunu kullanmak istediğinizi seçin. Şu seçenekleriniz bulunmaktadır: *AVG Secure Search (powered by Google)*, *Baidu*, *WebHledani*, *Yandex* ve *Yahoo! JP*. Varsayılan arama motoru değiştirildiğinde değişikliğin etkili olabilmesi için lütfen İnternet tarayıcınızı yeniden başlatın.

Ayrıca belirli **AVG Security Toolbar** ayarlarını *etkinleştirebilir veya kapatabilirsiniz (listelenen başlık varsayılan AVG Secure Search (powered by Google) ayarlarına işaret eder)*:

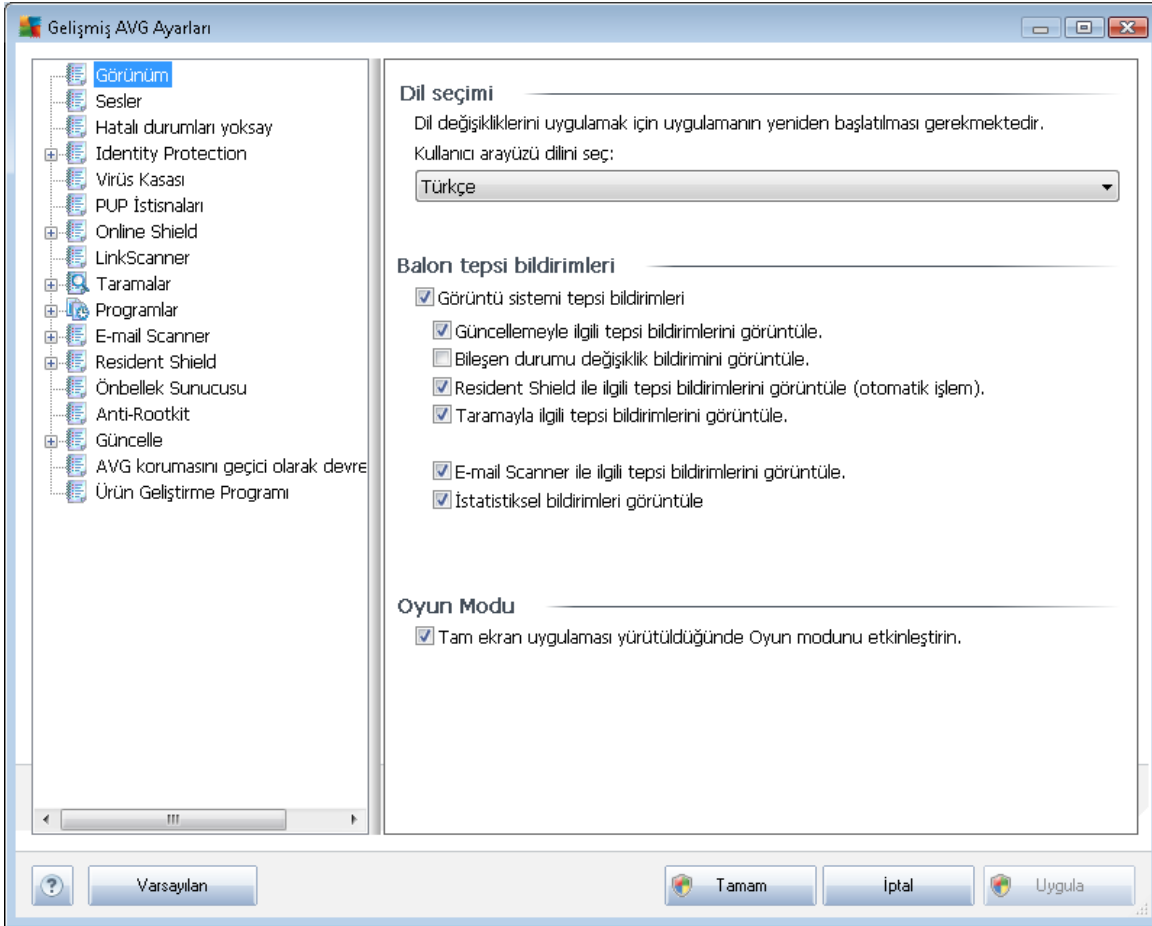
- **AVG Secure Search (powered by Google) Adres çubuğu için arama sağlayıcısını ayarla ve sakla** - bu seçenek işaretlendiğinde, doğrudan İnternet tarayıcınızın adres çubuğuna arama anahtar kelimesini girmenize olanak sağlar ve Google hizmeti otomatik olarak ilgili web sitelerini aramak için kullanılır.
- **AVG'nin tarayıcı navigasyon hataları (404/DNS) hakkında öneride bulunmasına izin ver** - web'de arama yaparken var olmayan veya görüntülenemeyen (404 hatası) bir sayfaya gelerseniz, otomatik olarak konuyla ilgili alternatif sayfaların bulunduğu bir web sayfasına yönlendirilirsiniz.
- **Varsayılan arama sağlayıcısı olarak ayarla ve sakla** **AVG Secure Search (powered by Google)** - Google **AVG Security Toolbar** içerisindeki web araması için varsayılan arama motorudur ve bu seçeneği etkinleştirerek aynı zamanda web tarayıcınızın da varsayılan arama motoru olabilir.

9. AVG Gelişmiş Ayarlar

AVG Anti-Virus 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 kullanıcı arayüzünün](#) genel ayarlarını ve uygulamanın bazı temel seçeneklerini gösterir:

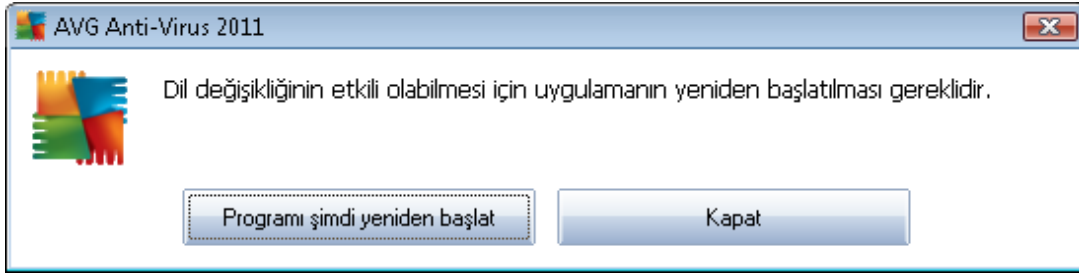


Dil seçimi

Dil seçimi bölümünde açılır menüden istediğiniz dili seçebilirsiniz. Bunun ardından seçtiğiniz dil tüm [AVG Kullanıcı Arayüzünde](#) kullanılır. Aşağı açılır menü, (*varsayılan olarak yüklenen*) İngilizce'ye ek olarak yalnızca [yükleme süreci](#) sırasında önceden seçmiş olduğunuz yükleme dillerini sunar (*bkz. [Özel Seçenek](#) bölümü*). Diğer bir yandan uygulamayı başka bir dile çevirme işlemini bitirmek için kullanıcı arayüzünü yeniden başlatmanız gerekir. Şu adımları izleyin:



- Uygulamada kullanılmasını istediğiniz dili seçin ve **Uygula** düğmesine (sağ alt köşede) basarak seçiminizi onaylayın.
- Onaylamak için **Tamam** düğmesine basın
- AVG kullanıcı arayüzündeki dil değişikliğinin uygulamayı yeniden başlatmayı gerektirdiğini bildiren yeni iletişim kutusu penceresi açılır:



Balon tepsi bildirimleri

Bu bölümde uygulama durumu hakkında sistem tepsi üzerinde beliren balon bildirimlerini kaldırabilirsiniz. Balon bildirimlerinin varsayılan olarak görüntülenmesine izin verilir ve söz konusu yapılandırmanın değiştirilmemesi önerilir! Balon bildirimleri, genellikle AVG bileşenlerinin durum değişiklikleri hakkında bilgi verir ve bunlara dikkat etmeniz gerekir!

Diğer bir yandan, belirli bir nedenden dolayı söz konusu bildirimlerin görüntülenmesini istemiyorsanız ya da sadece belirli bildirimlerin görüntülenmesini istiyorsanız (belirli AVG bileşenlerine ilişkin) tercihlerinizi aşağıdaki seçenekleri işaretleyerek ya da işaretlemeyerek tanımlayabilir veya belirtebilirsiniz:

- **Sistem tepsi bildirimlerini görüntüle** - bu öğe varsayılan olarak işaretlidir (*açık*tır) ve bildirimler görüntülenir. Tüm balon bildirimleri kapatmak için bu öğenin işaretini kaldırın. Açıldığı zaman hangi bildirimlerin görüntüleneceğini seçebilirsiniz:
 - **Güncelleme** hakkında bildirimleri görüntüle - AVG güncelleme sürecinin başlaması, ilerleme ve tamamlanma hakkında bilgilerin görüntülenmesini isteyip istemediğinize karar verin;
 - **Bileşenlerin durum değişiklikleri hakkında bildirimleri görüntüle** - bileşenlerin aktif ya da pasif olup olmadığı ya da muhtemel sorunları hakkında bildirimlerin görüntülenmesini isteyip istemediğinize karar verin. Bir bileşenin hata durumu rapor edilirken bu işlev, [sistem tepsi simgesinin](#) herhangi bir AVG bileşeninde meydana gelen sorunu rapor ederken kullandığı bilgilendirici işleve eşdeğerdir (renk değişimi);
 - **Yerleşik Kalkan ile ilgili tepsi bildirimlerini görüntüle** - kayıt, kopyalama ve açma işlemleriyle ilgili bilgilerin görüntülenmesine veya gizlenmesine karar verin (*bu yapılandırma yalnızca Yerleşik Kalkan Otomatik temizle seçeneği açık*sa gösterilir).
 - **Tarama** ile ilgili bildirimleri görüntüle - programlı taramaların otomatik olarak başlaması, ilerlemesi ve sonuçları hakkında bilgilerin görüntülenmesini isteyip



istemediđinize karar verin;

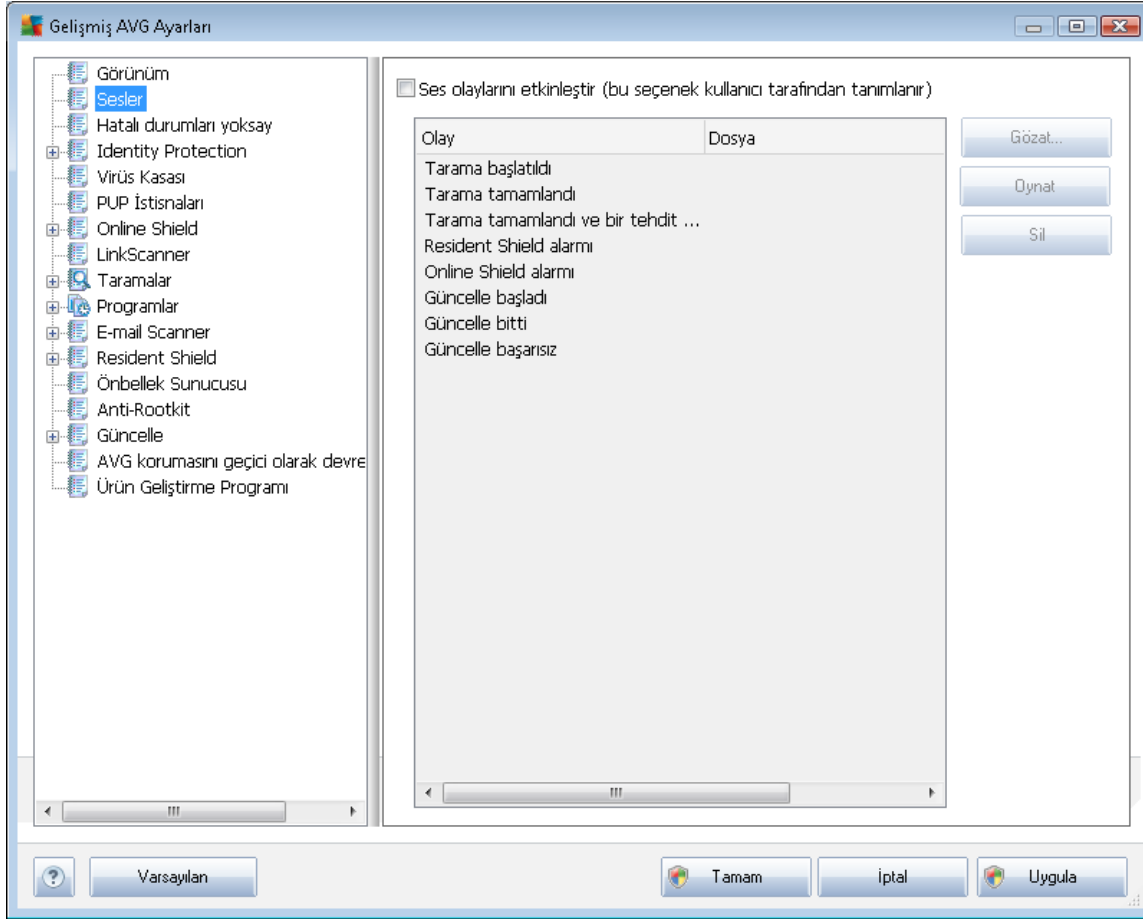
- o **E-posta Tarayıcısı ile ilgili tepsi bildirimlerini g r nt le** - Gelen ve giden e-posta mesajlarının taranmasına ilişkin bildirimleri g r nt lemek isteyip istemediđinize karar verin.
- o **İstatistiksel uyarıları g r nt le** - d zenli istatistiksel inceleme uyarılarının sistem tepsisinde g r nt lenmesine izin vermek i in bu se eneđi i aretli halde bırakın.

Oyun modu

Bu AVG i levi, olası AVG bilgi balonlarının ( m. programlı bir tarama ba latıldıđında g sterilir) rahatsız edici olabilen (*uygulamayı k   ltebilir veya grafiklerini bozabilir*) tam ekran uygulamaları i in tasarlanmı tır. Bu durumu  nlemek i in, **Tam ekran uygulaması  alı tırılırken oyun modunu etkinle tir** se eneđini i aretli bırakın (*varsayılan ayar*).

9.2. Sesler

Sesler ileti im kutusu i inde, belirli AVG eylemleri hakkında bir ses bildirimiyle bilgilendirilmek isteyip istemediđinizi belirtebilirsiniz. İstiyorsanız, AVG eylemleri listesini etkinle tirmek i in **Ses olaylarını etkinle tir** se eneđini (*varsayılan olarak kapalıdır*) i aretleyin:

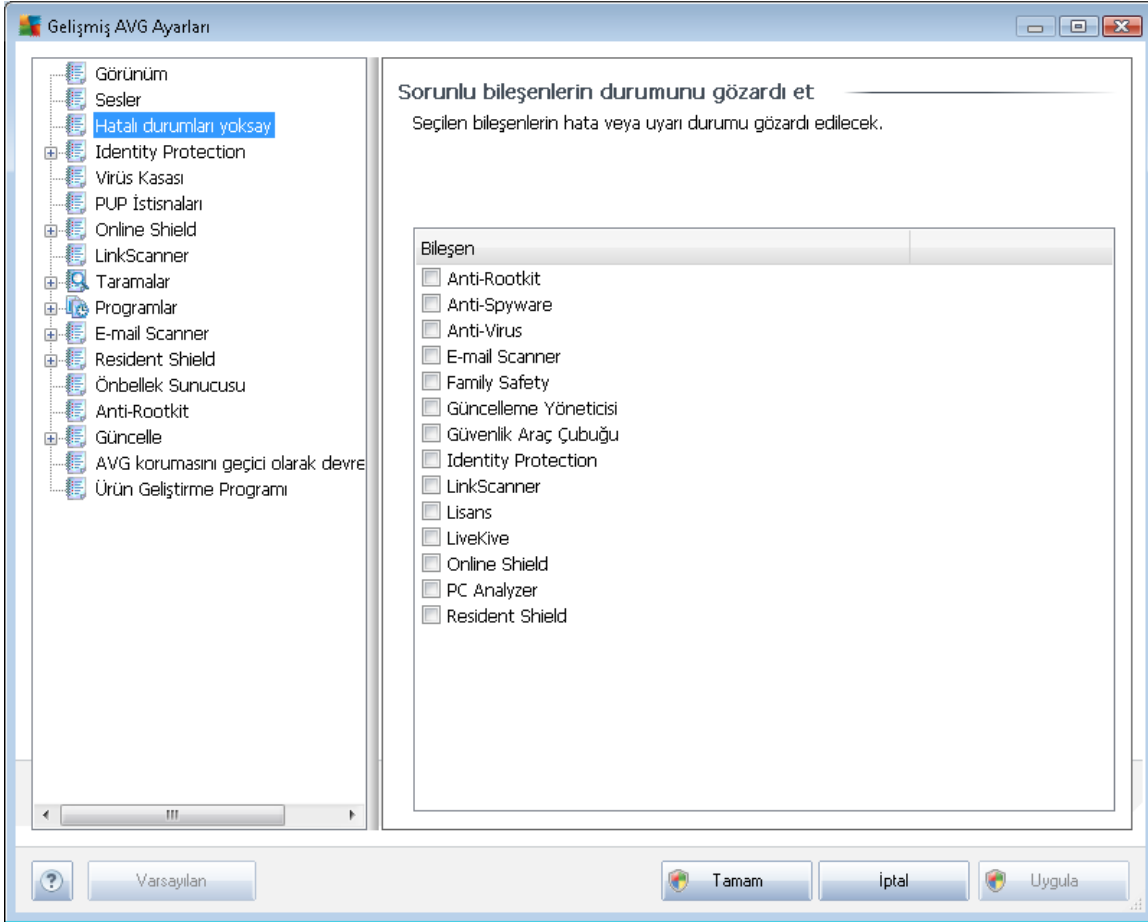


Sonra, ilgili olayı listeden seçin ve bu olaya atamak istediğiniz uygun ses için diskinize gözetin (**Gözet**). Seçili sesi dinlemek için, listede olayı vurgulayın ve **Çal** düğmesine basın. Belirli olaya atanan sesi kaldırmak için **Sil** düğmesini kullanın.

Not: Yalnızca *.wav sesleri desteklenir!

9.3. Hatalı Durumları Yoksay

Hatalı bileşenleri yok sayma koşulları 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:

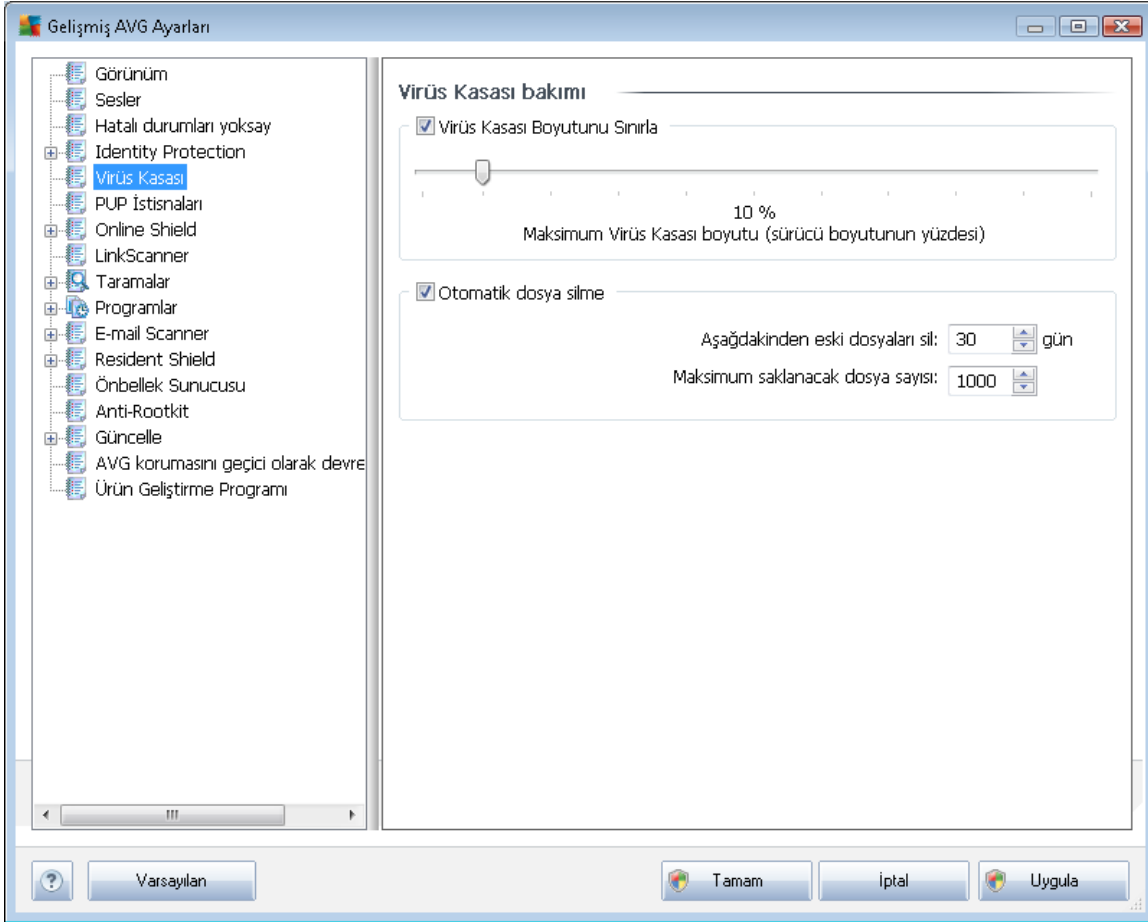
- **sistem tepsisi simgesi** - AVG'nin tüm bileşenleri doğru şekilde çalışırken simge, 4 renkli görünecektir ancak herhangi bir aksaklık olursa simgenin yanında sarı bir ünlem işareti görülür,
- AVG ana penceresinin **Güvenlik Durumu Bilgileri** bölümünde mevcut sorun açıklanır

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. **Bileşen durumunu yoksay** seçeneği, doğrudan [AVG ana penceresinin bileşenlere genel bakış](#) penceresinden de kullanılabilir.

9.4. Virüs Kasası



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

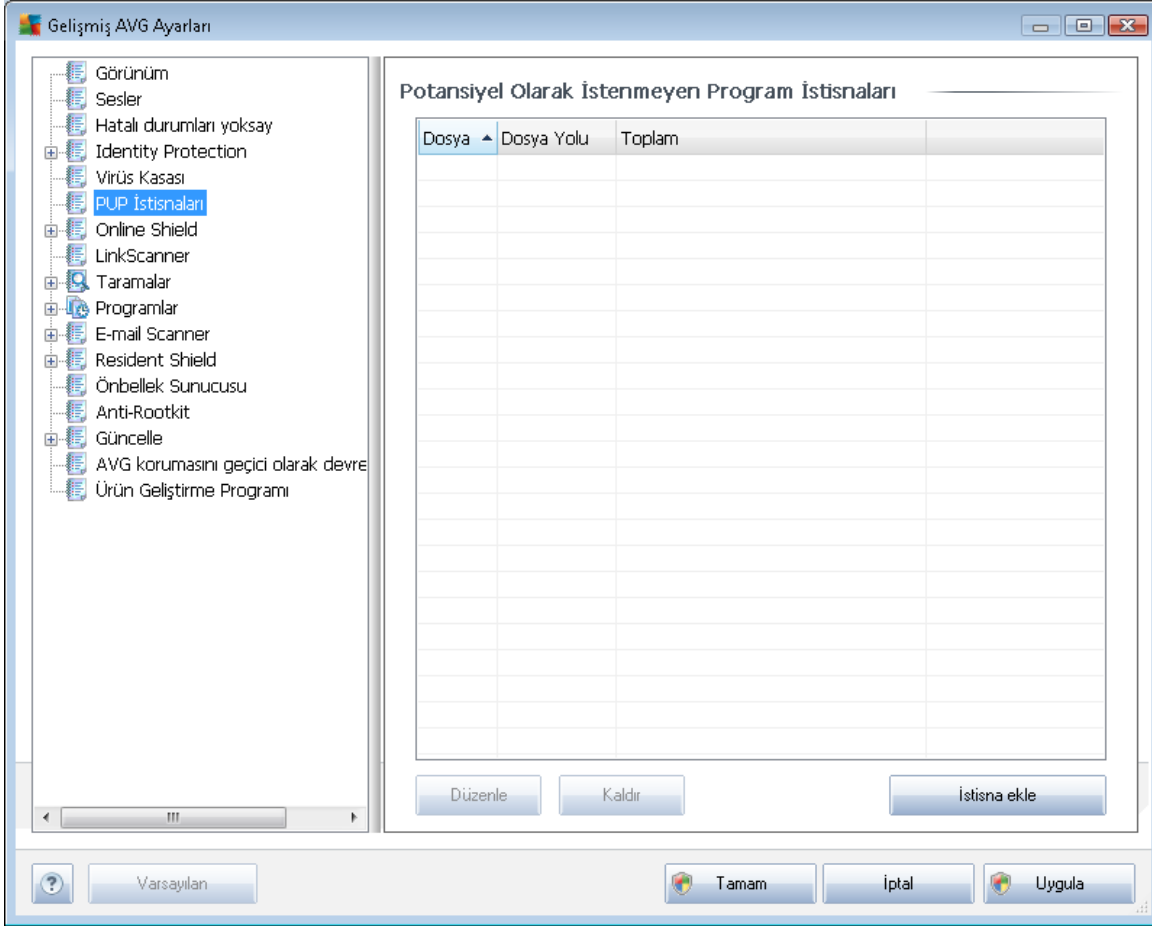
- **Virüs Kasası boyutunu sınırla** - [Virüs Kasası](#)'nın maksimum boyutu için kaydırıcıyı kullanın. Söz konusu boyut, sabit diskinizin boyutu ile doğru orantılı olacaktır.
- **Otomatik dosya silme** - bu bölümde nesnelerin [Virüs Kasasında](#) depolanacakları maksimum süreyi (... **Günden eski dosyaları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

9.5. PUP İstisnaları

AVG Anti-Virus, 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. Söz konusu reklam yazılımları AVG tarafından tespit edilip **potansiyel olarak istenmeyen program** statüsü ile rapor edilebilir. Söz konusu programın bilgisayarınızda bulunmasını istiyorsanız ilgili programı, potansiyel olarak istenmeyen program istisnası şeklinde atayabilirsiniz:

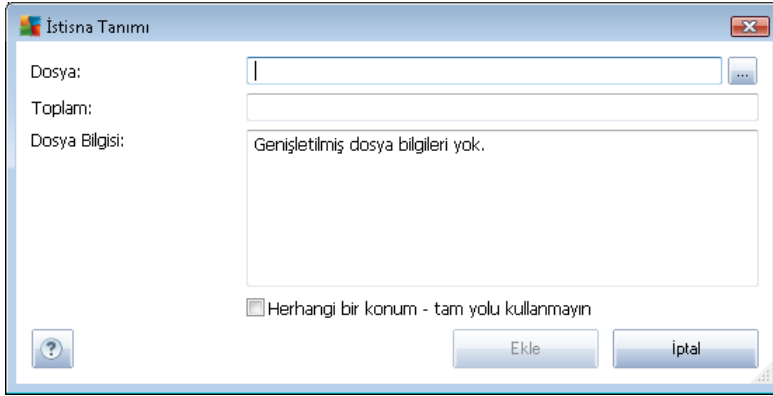


Potansiyel Olarak İstenmeyen Program İstisnaları iletişim kutusunda, potansiyel olarak istenmeyen programlardan tanımlanan ve mevcut durumda geçerli istisnalar bulunmaktadır. Listeyi düzenleyebilir, varolan öğeleri silebilir veya yeni istisnalar ekleyebilirsiniz. Aşağıdaki bilgiler her bir istisna için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

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

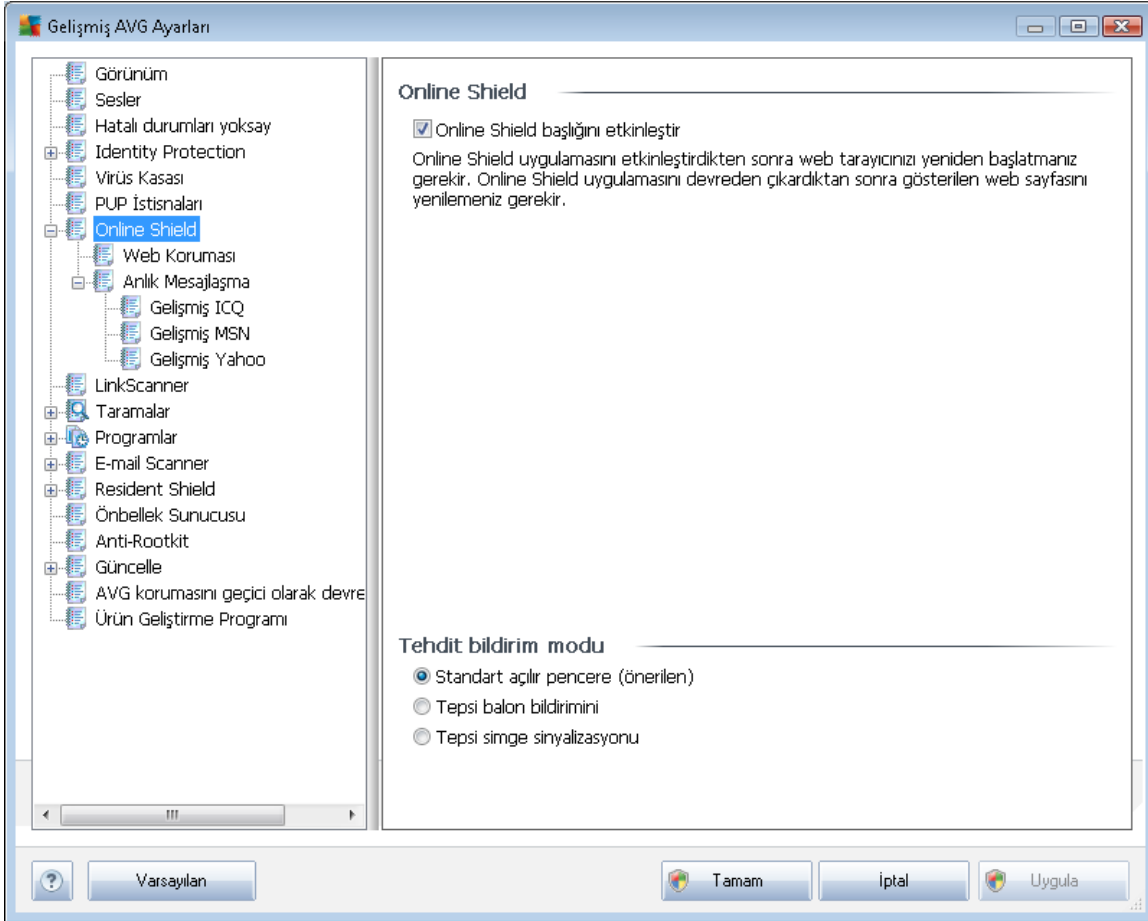
Kontrol düğmeleri

- **Düzenle** - önceden tanımlanmış olan bir istisnanın parametrelerini düzenleyebileceğiniz bir düzenleme iletişim kutusu açar (*yeni istisna tanımlama 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
- **İmza Kontrol Et** - seçilen dosyanın "özel imzasını" görüntüler. Bu sağlama, AVG'nin seçilen dosyayı diğer dosyalardan ayırmayı sağlamak üzere otomatik oluşturulan karakter dizelerinden meydana gelmektedir. 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 bulunduğuyla ilgili 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*).

9.6. Online Shield



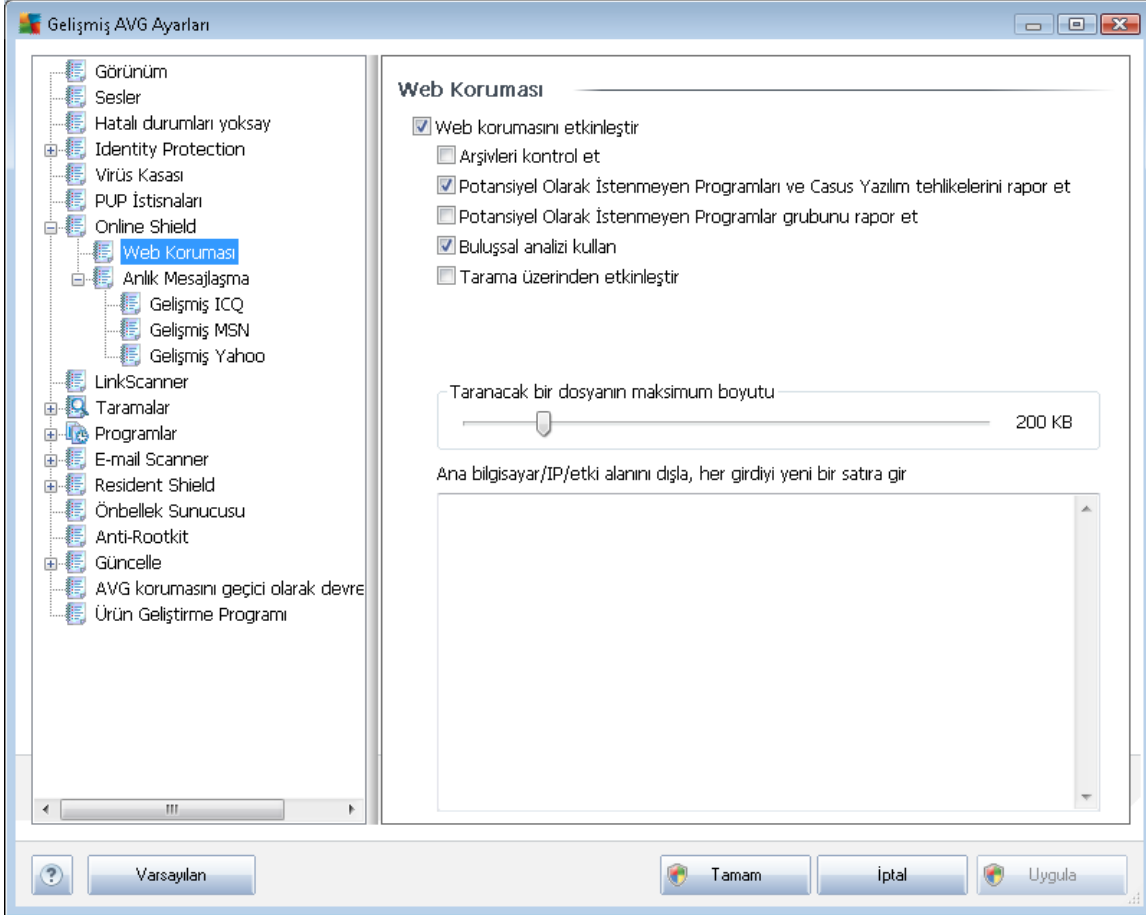
Online Shield iletişim kutusu, [Online Shield](#) bileşeninin tümünü **Online Shield'i Etkinleştir** seçeneği ile (*varsayılan olarak etkindir*) etkinleştirmenize veya devre dışı bırakmanıza olanak verir. Bu bileşenin daha fazla gelişmiş ayarını görmek için lütfen gezinti ağacında listelenen ardışık iletişim kutularına bakın:

- [Web Koruması](#)
- [Anlık Mesajlaşma](#)

Tehdit bildirim modu

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

9.6.1. Web Koruması



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

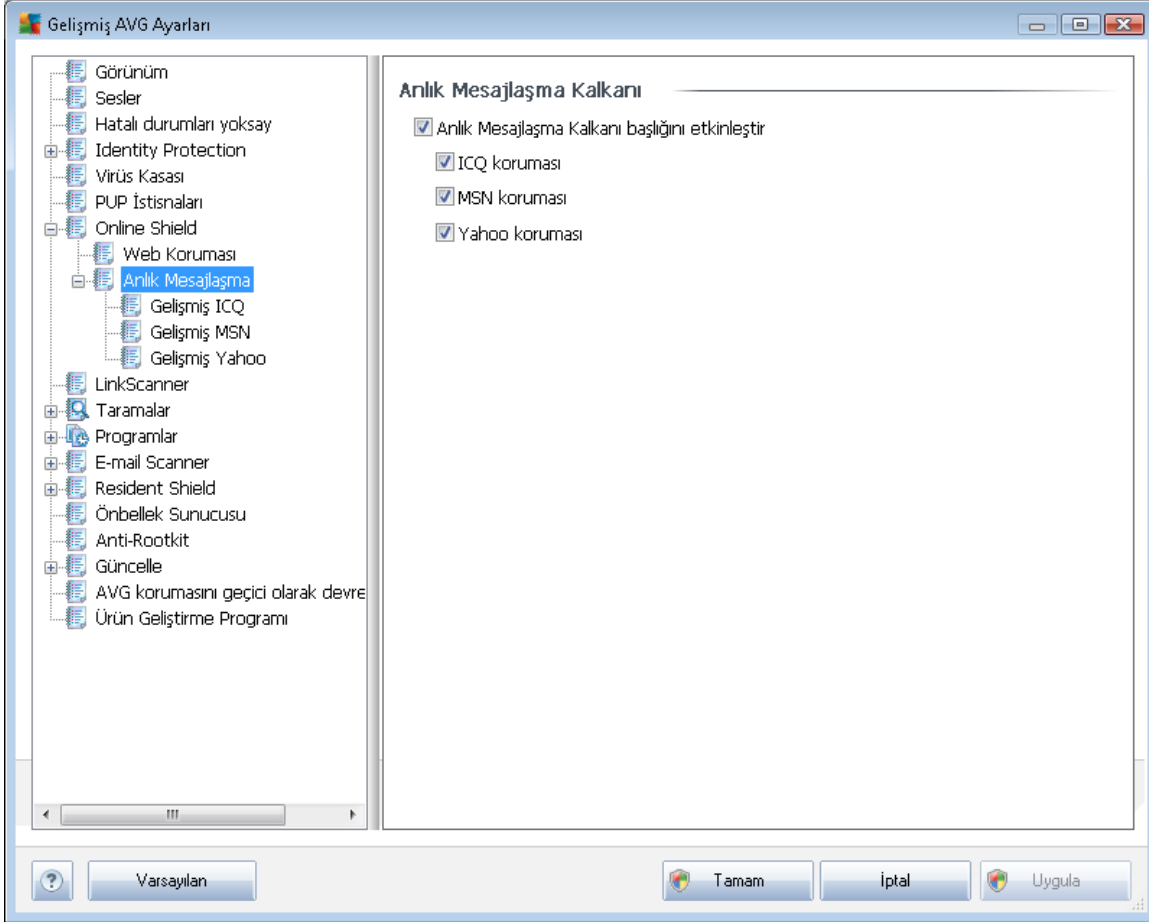
- **Web korumasını etkinleştir** - bu seçenek [Online Shield](#)'in www sayfalarının içeriğinin taranmasını gerçekleşmek gerektiğini onaylar. Bu seçeneğin etkin konumda olmasına rağmen (varsayılan olarak) söz konusu öğeleri açıp kapatabilirsiniz:
 - **Arşivleri denetle** - (varsayılanda kapalıdır): muhtemelen www sayfasında görüntülenecek arşivlerin içeriğini tarayın.
 - **Potansiyel Olarak İstenmeyen Programları ve Casus Yazılım tehlikelerini rapor et** - (varsayılan olarak açıktır): [Anti-Spyware](#) motorunu etkinleştirmek ve virüslerle birlikte casus yazılımları da kontrol etmek için işaretleyin. [Casus yazılım, şüpheli kötü amaçlı yazılım kategorisini ifade eder: genellikle bir güvenlik riskini oluşturmaya 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 kullanılabilecek programların genişletilmiş



paketinin tespit edilmesi için işaretleyin. Bu, bilgisayar güvenliğini 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 taranmasa 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.

9.6.2. Anlık Mesajlaşma

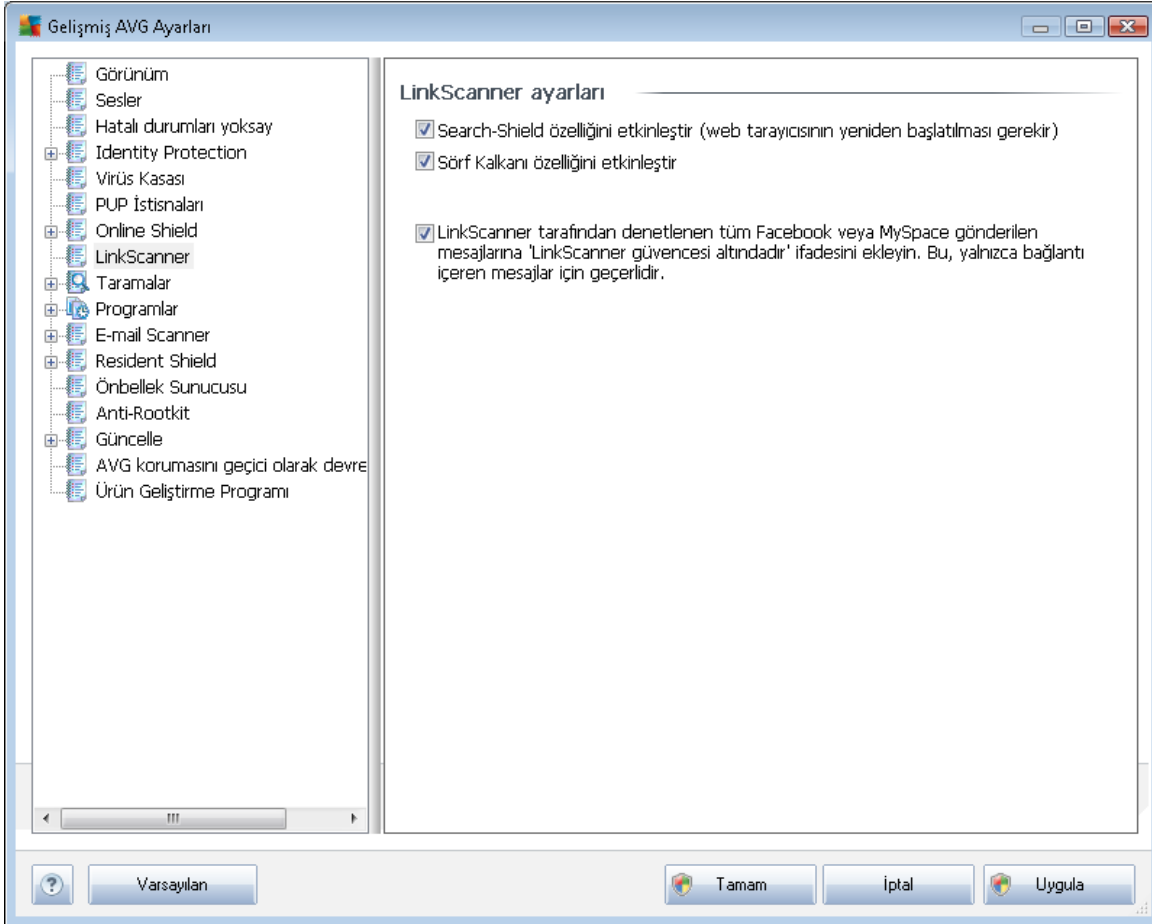


Anlık Mesajlaşma Kalkanı iletişim kutusunda anlık mesajlaşmaların taranmasına ilişkin [Online Shield](#) bileşeninin ayarlarını yapabilirsiniz. Geçerli olarak aşağıdaki üç anlık mesajlaşma programı desteklenmektedir: **ICQ**, **MSN** ve **Yahoo** - [Online Shield'in](#) çevrimiçi görüşmelerinizin virüssüz olmadığını doğrulamasını istiyorsanız ilgili öğeleri işaretleyin.

İzin verilen/engellenen kullanıcılara ilişkin ayarlar hususunda ilgili iletişim kutusunu görüntüleyebilir ya da düzenleyebilirsiniz (**Gelişmiş ICQ**, **Gelişmiş MSN**, **Gelişmiş Yahoo**) ve **Beyaz Listeyi** (sizinle iletişim kurmasına izin verilen kullanıcıların listesi) ve **Kara Listeyi** (engellenmesini istediğiniz kullanıcıların listesi) oluşturabilirsiniz.

9.7. Bağlantı Tarayıcı

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 ...** - Facebook ve MySpace'den gönderilen etkin hiper bağlantıları içeren iletilerde **Link Scanner** denetimi ile ilgili sertifikasyon bildirimi girmek istediğinizi onaylamak için bu öğeyi işaretleyin.



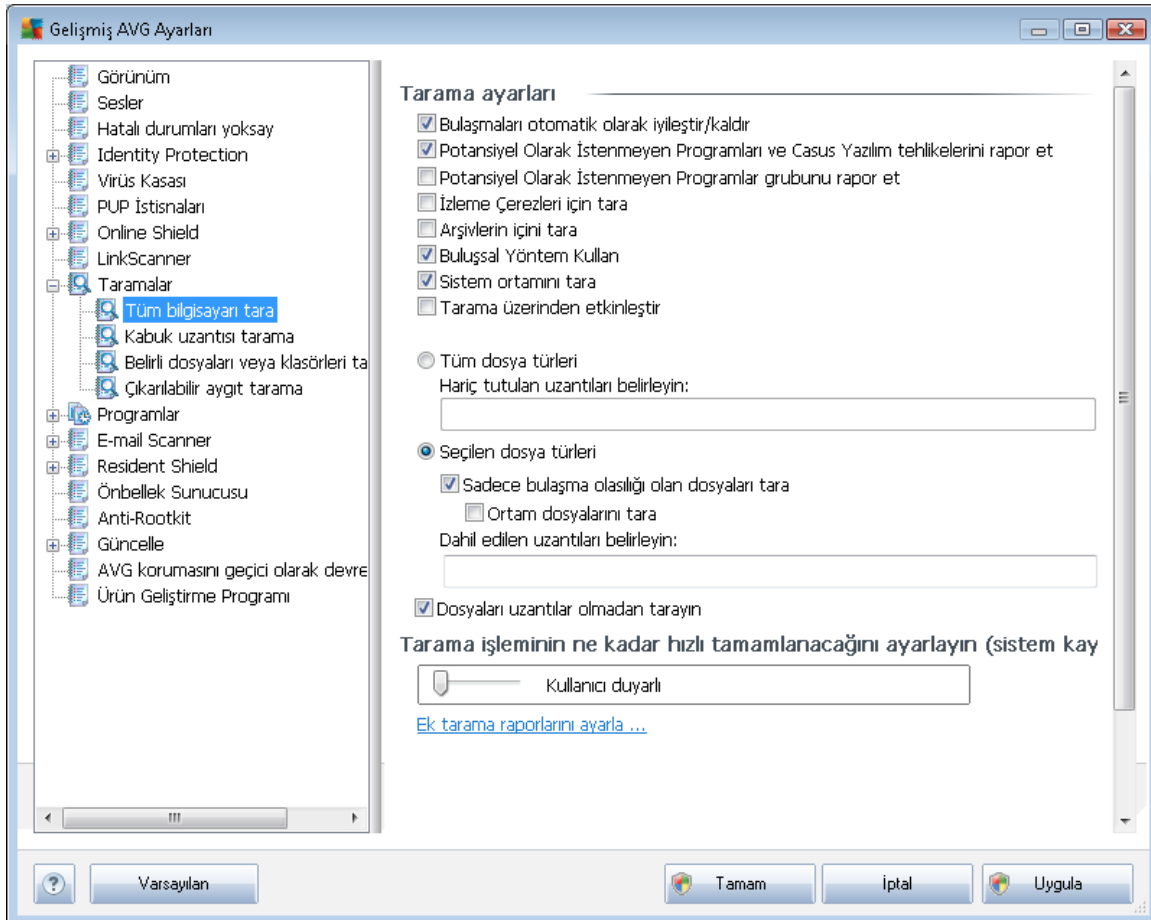
9.8. Taramalar

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 ya da Klasörlerin Taranması](#) - bilgisayarınızın seçilen alanlarının tarandığı standart öntanımlı taramadır
- [Çıkartılabilir Aygıt Taraması](#) - bilgisayarınıza bağlanan çıkartılabilir aygıtların taranması işlemidir

9.8.1. Tüm Bilgisayarı Tara

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





Tarama ayarları

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

- **Bulaşmayı otomatik olarak temizle/kaldır** (varsayılanda açıktır) - tarama sırasında virüs tanımlanırsa, 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** (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 güvenlik riski oluşturmalarına 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 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.
- **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.

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;

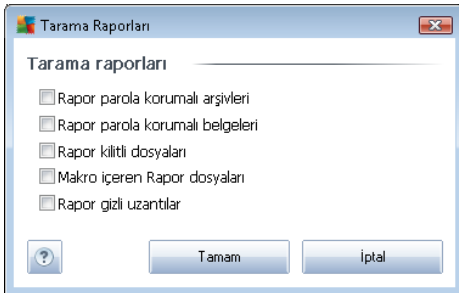
- **Seçili dosya türleri** - Yalnızca virüs bulaşabilme olasılığı olan dosyaları taramayı istediğinizi belirtebilirsiniz (*virüs bulaşmayan dosyalar taranmayacaktır, örneğin, bazı düz metin dosyaları veya bazı diğer çalıştırılmayan dosyalar*); ortam dosyaları (*video, ses dosyaları - bu onay kutusunun 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 değiştirmemeniz 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.

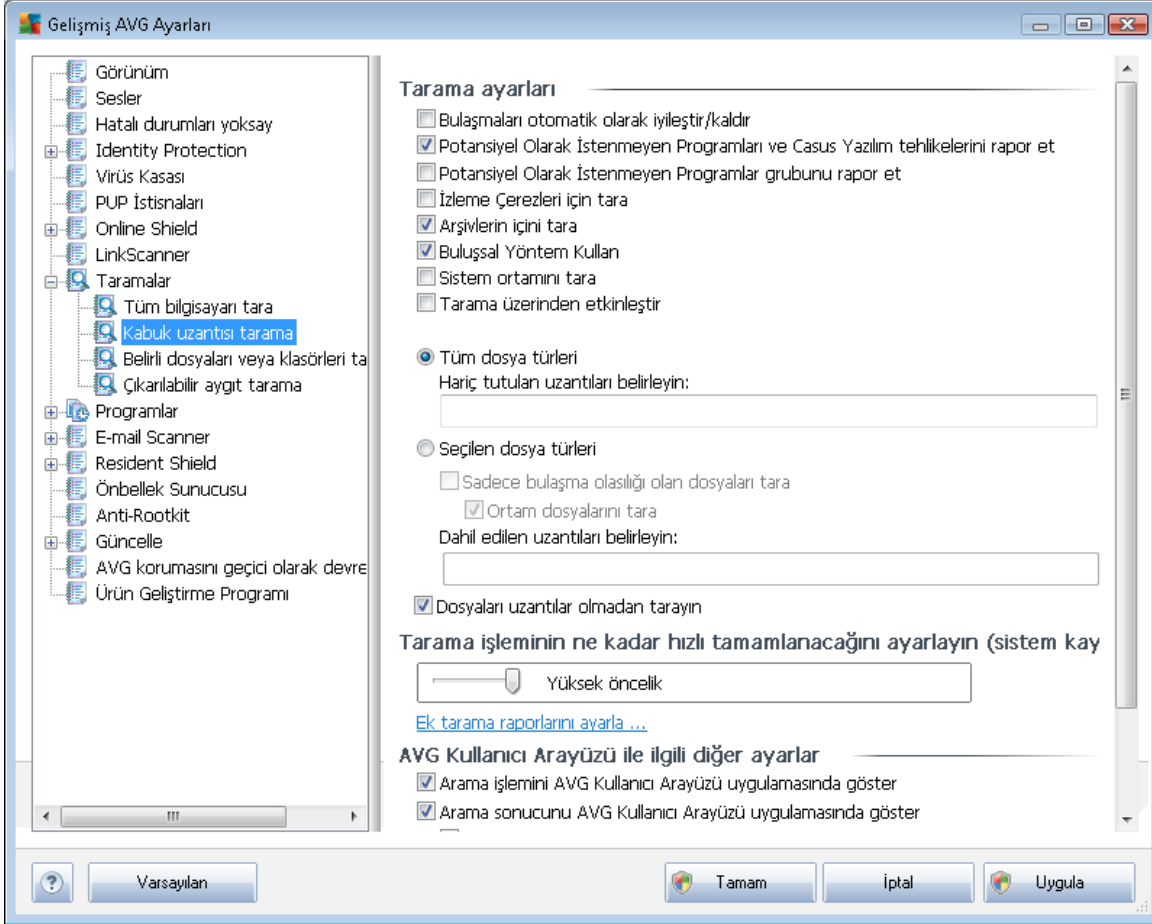
Ek tarama raporlarını ayarla...

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



9.8.2. Kabuk Uzantısı Tarama

Daha önce bahsettiğimiz [Tüm bilgisayar taraması](#) öğesine benzer olan bu öğe, **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:



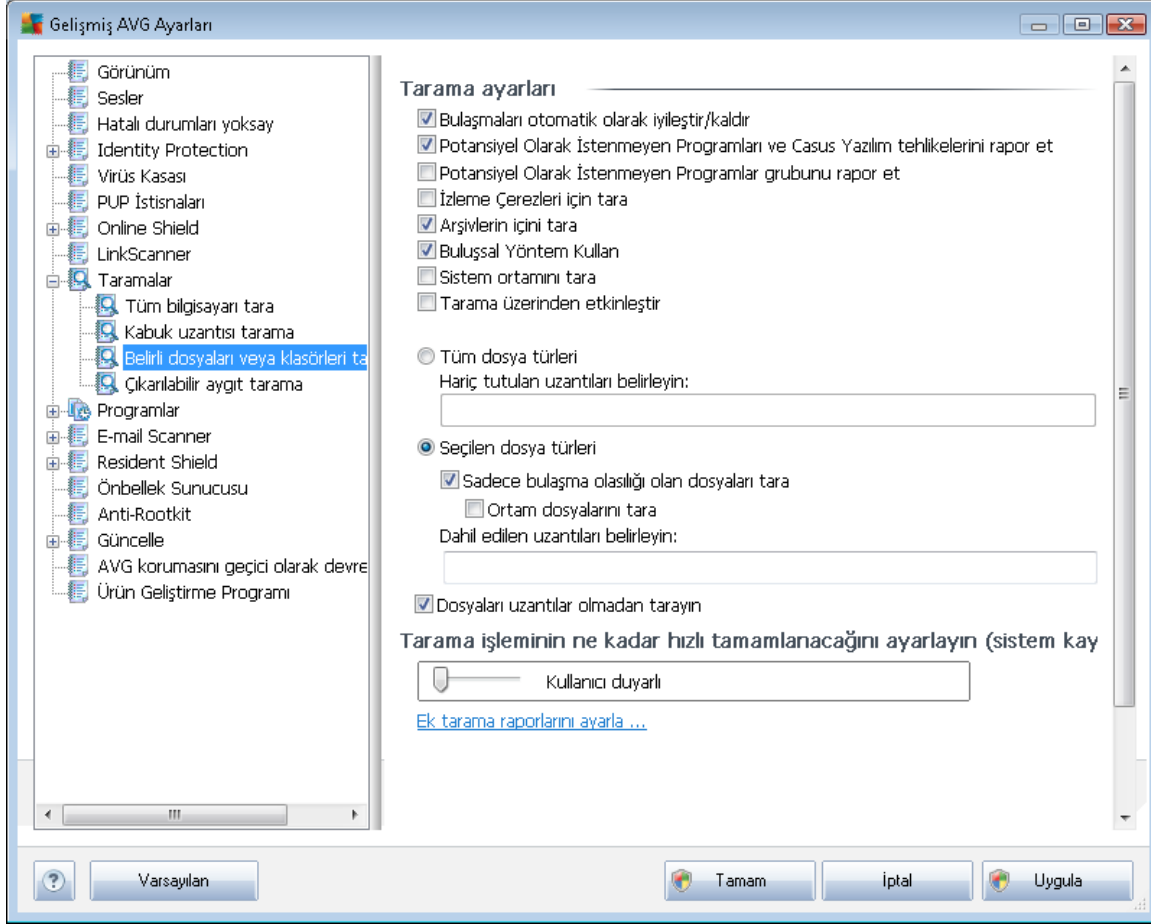
Parametre listesi, [Tüm bilgisayarı tarama](#) öğesinin parametre listesi ile aynıdır. Bununla birlikte, varsayılan ayarlar farklılık gösterebilir (örneğin, *Tüm bilgisayarın taraması işlevi arşivleri denetlemez ancak Kabuk Uzantısı Tarama başka bir işlem yaparken sistem ortamını tarama*).

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

[Tüm bilgisayarın taraması](#) iletişim kutusuyla karşılaştırıldığında, [Kabuk uzantısı tarama](#) iletişim kutusu, tarama sürecine ve tarama sonuçlarına AVG kullanıcı arayüzünden erişilebilir olmasını isteyip istemediğinizi belirtebileceğiniz [AVG Kullanıcı Arayüzü ile ilgili diğer ayarlar](#) adlı bölümü de içerir. Tarama sırasında bir bulaşma tespit edilmesi durumunda tarama sonucunun görüntülenmesi gerektiğini de tanımlayabilirsiniz.

9.8.3. Belirli Dosyaları veya Klasörleri Tara

Belirli dosyaları veya klasörleri tarama 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:

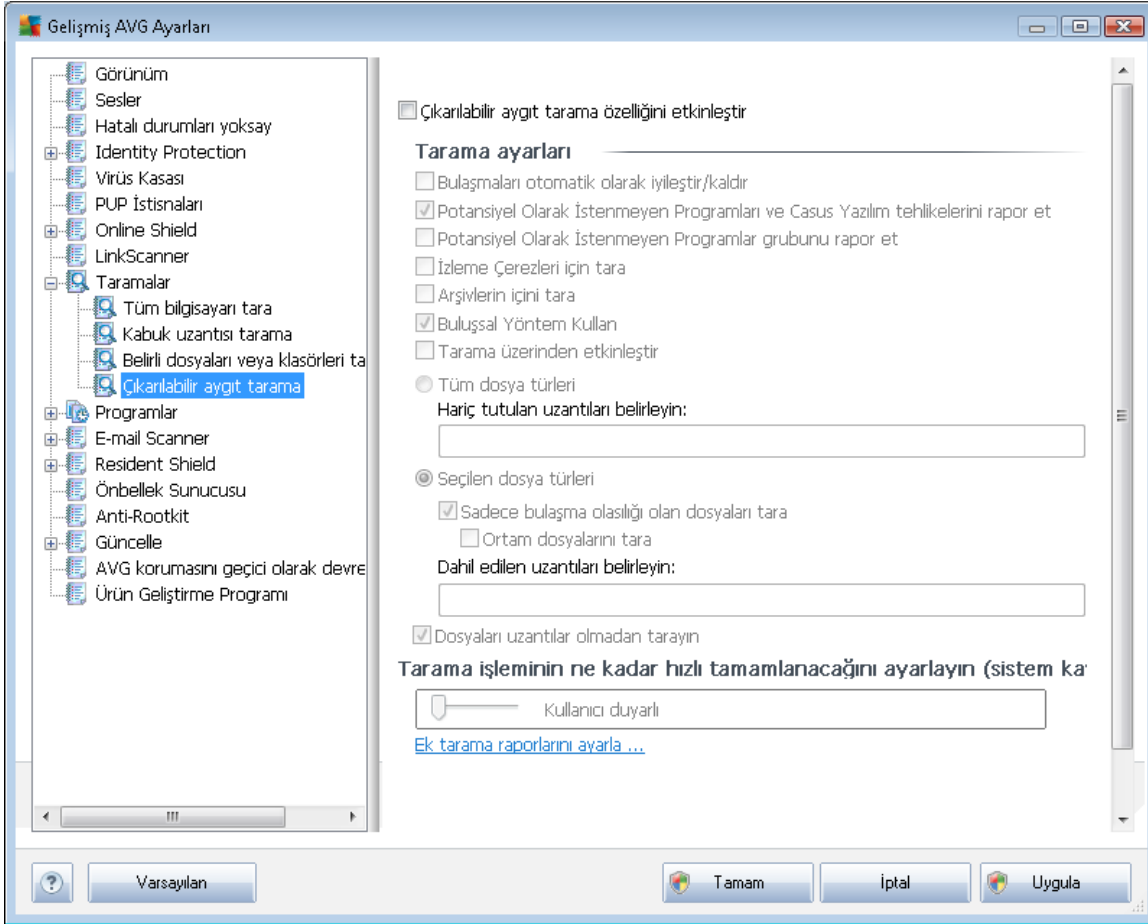


Bu yapılandırma iletişim kutusunda ayarlanan tüm parametreleri **Belirli dosya ya da klasörleri tara** ile tarama sırasında seçilen alanlar için geçerlidir!

Not: Belirli parametrelerin açıklaması için, lütfen **AVG Gelişmiş Ayarları / Taramalar / Tüm bilgisayarın taranması** bölümüne bakın.

9.8.4. Çıkarılabilir Aygıt Tarama

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



Çıkarılabilir aygıt tarama bilgisayarınıza çıkartılabilir 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 çıkartılabilir 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.

9.9. Programlar

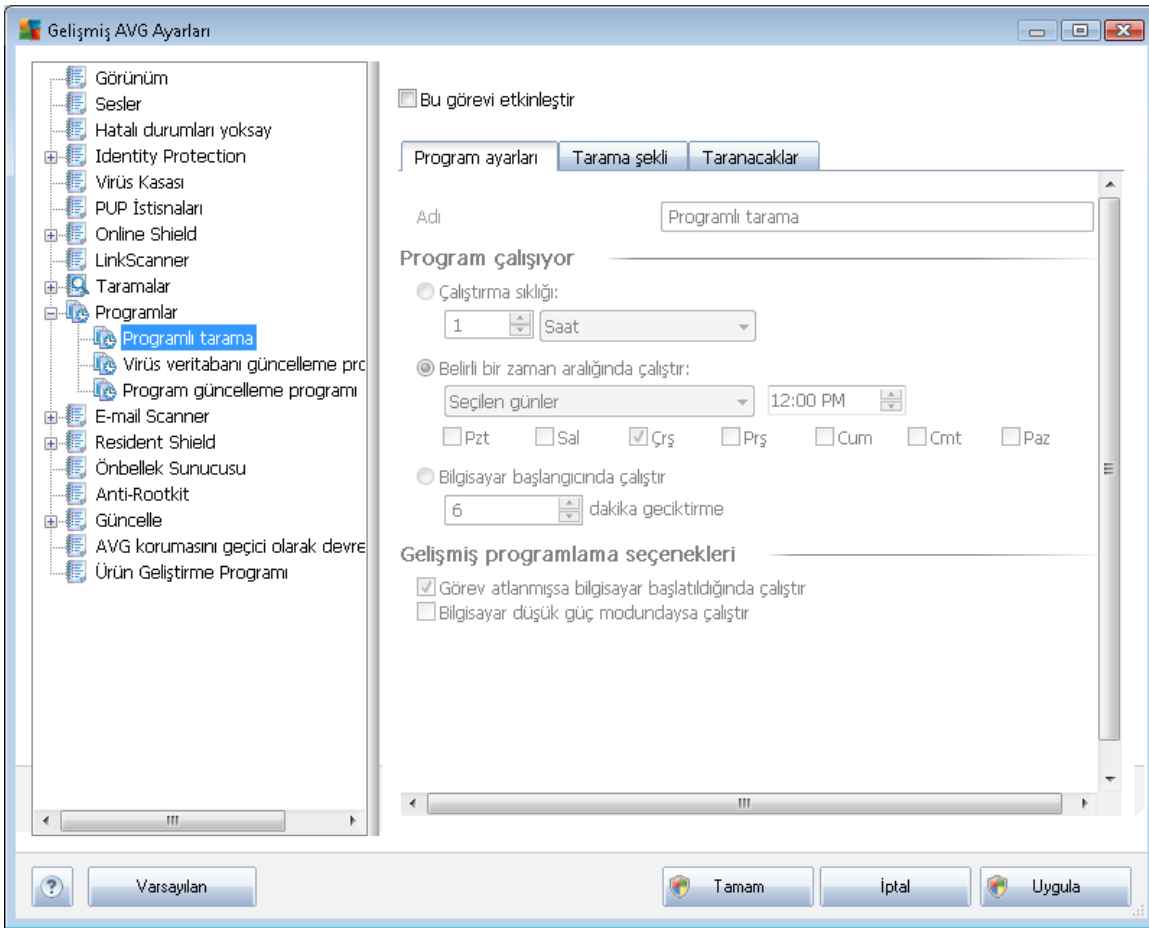
Programlar bölümünde aşağıdaki bileşenlerin öntanımlı ayarlarını düzenleyebilirsiniz:

- [Programlı tarama](#)

- [Virüs veritabanı güncelleme programı](#)
- [Program güncelleme programı](#)

9.9.1. Programlı Tarama

Üç sekmede zamanlanan tarama parametreleri düzenlenebilir (veya yeni bir zamanlama ayarlanabilir). Her sekmede **Bu görevi etkinleştir** ögesini işaretleyerek veya söz konusu öğenin 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 tıklayarak 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 taranması 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 (**Bilgisayarın başlatılmasıyla ilişkili eylem**) tanımlanabilir.

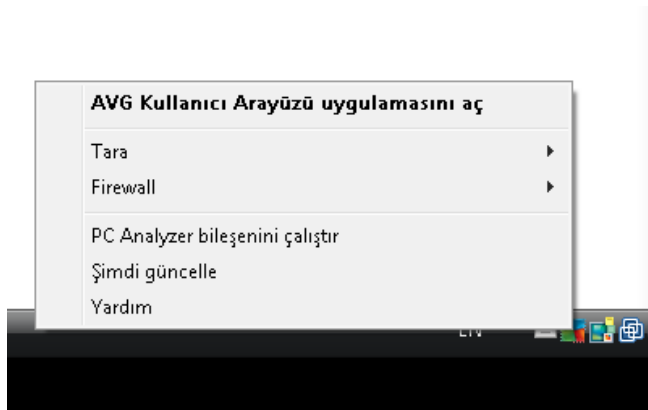
Gelişmiş programlama seçenekleri

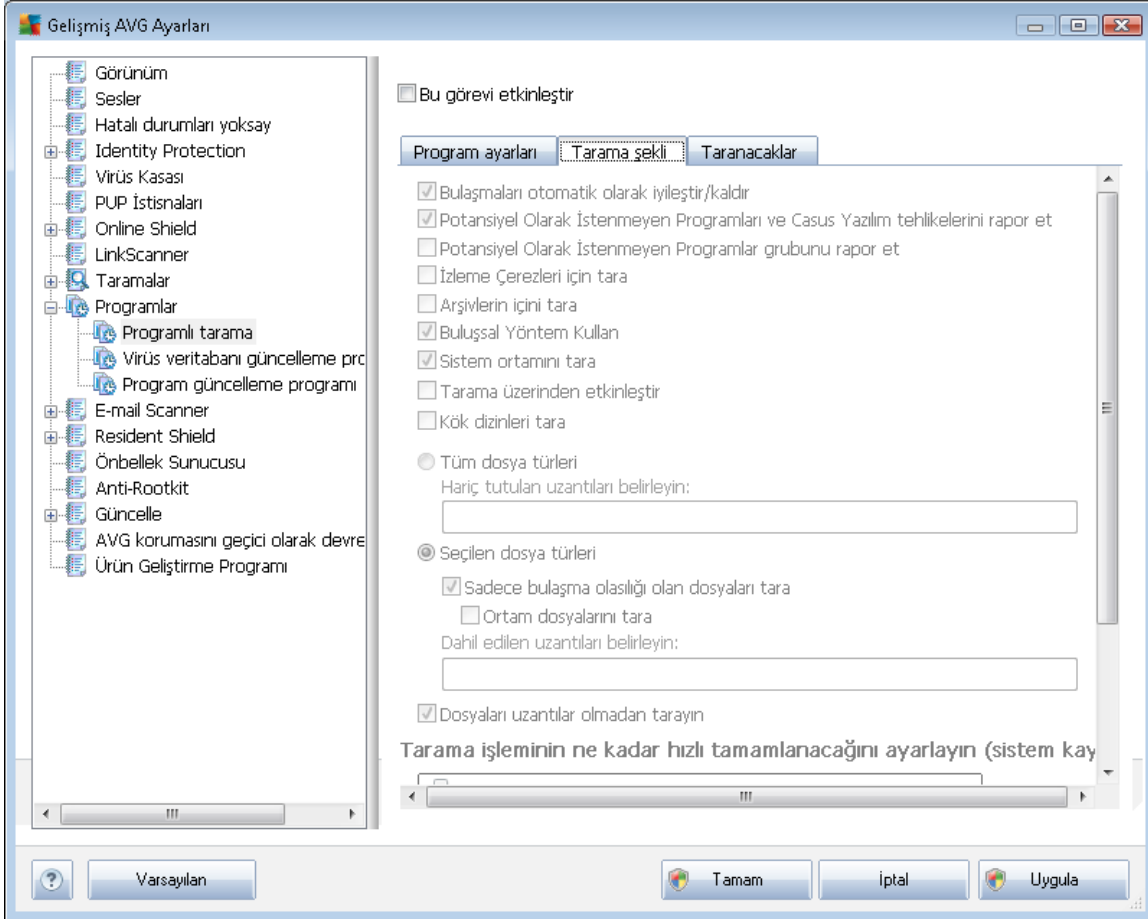
Bu bölümde, bilgisayar düşük güç modundaysa veya tamamen kapatılmışsa hangi koşullar altında taramanın başlatılması/başlatılmaması gerektiğini tanımlamanızı sağlar.

Programlanan tarama belirttiğiniz saatte başlatıldığında, [AVG sistem tepsisi simgesi](#) üzerinde açılan 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 güvenlik riski oluşturmalarına 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 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.

- **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** (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.
- **Kök dizinleri tara** (varsayılan olarak kapalıdır). Kök izin tespitini tüm bilgisayarın taranmasına eklemek için bu öğeyi işaretleyin. Rootkit tespiti işlemini [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 değiştirmemeniz önerilir. Uzantısı olmayan dosyalar şüpheli olabilir ve her zaman taranmalıdır.

Taramanın ne kadar hızlı tamamlanacağını ayarla

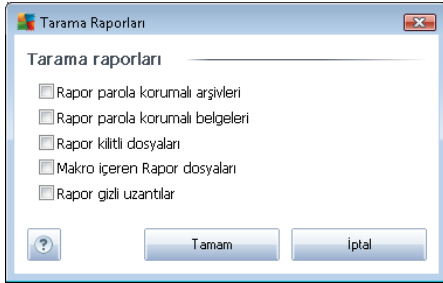
Taramanın ne kadar hızlı tamamlanacağını ayarla bölümünde, sistem kaynakları kullanımına bağlı olarak istediğiniz tarama hızını seçebilirsiniz. Bu seçenek varsayılan olarak otomatik kaynak kullanımının kullanıcıya duyarlı düzeyine ayarlanmıştır. Tarama işleminin daha hızlı ilerlemesi



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.

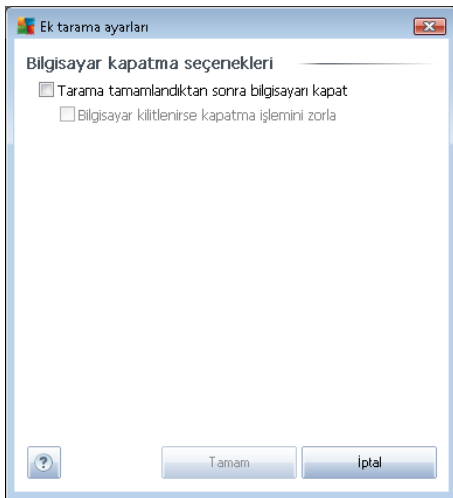
Ek tarama raporlarını ayarla

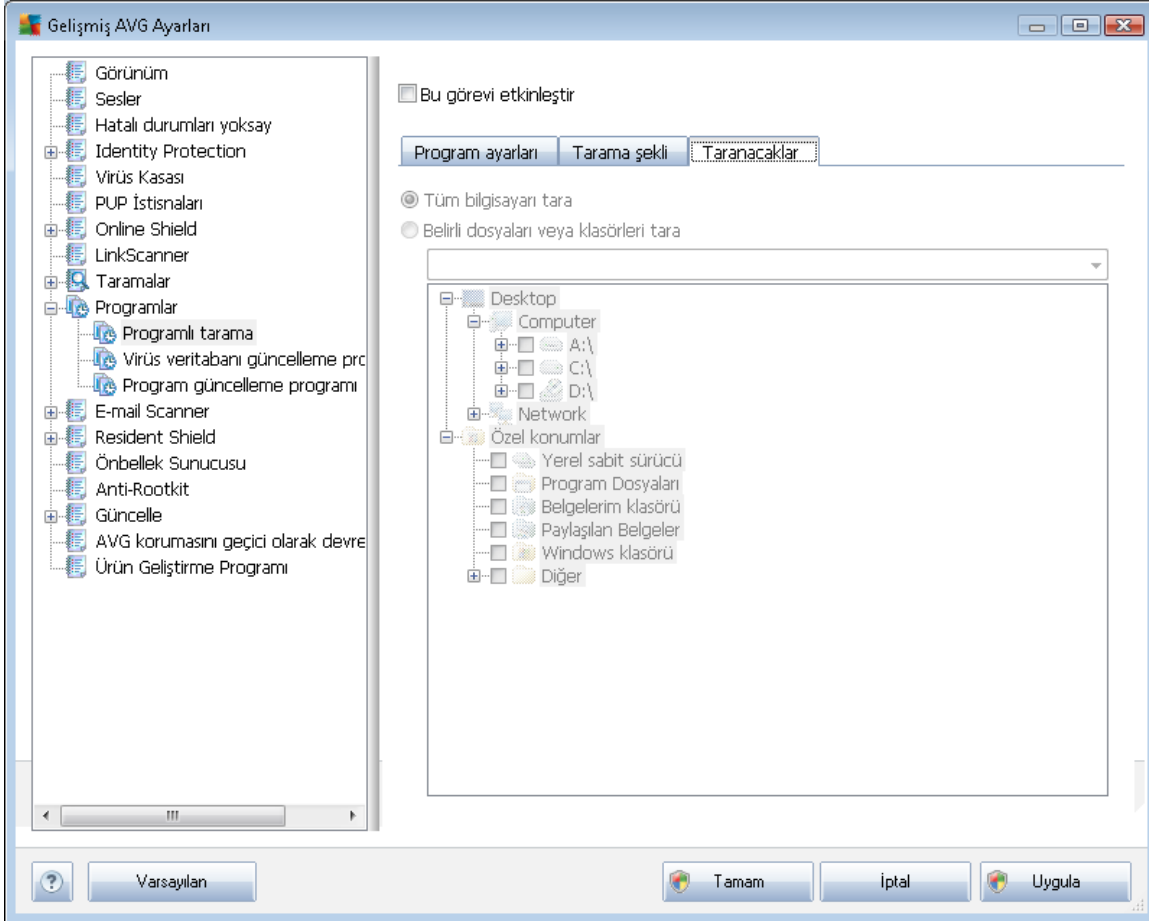
Tarama bulgularının rapor edilmesi gerekip gerekmediğini tanımlamak üzere birden fazla öğeyi ayarlayabileceğiniz **Tarama raporları** olarak adlandırılan bağımsız bir iletişim penceresi açmak için **Ek tarama raporlarını ayarla...** bağlantısını tıklayın:



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**).

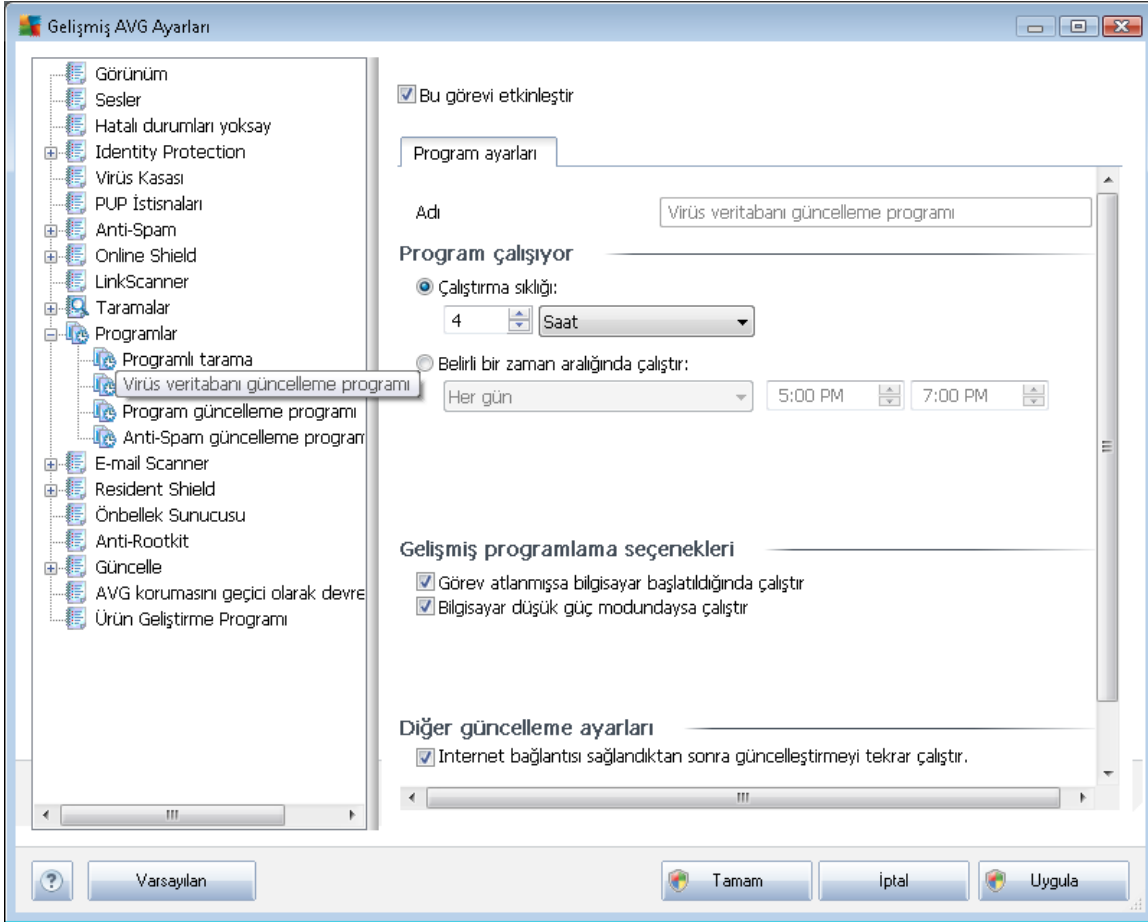




Taranacaklar sekmesinde, [tüm bilgisayarı tarama](#) veya [belirli dosya veya klasörleri taramayı](#) programlamak isteyip istemediğinizi belirleyebilirsiniz. Belirli dosya ve klasörleri taramayı seçerseniz, bu iletişim penceresinin alt kısmında görüntülenen ağaç yapısı etkinleşir ve taranacak klasörleri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

9.9.2. Virüs Veritabanı Güncelleme Programı

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



Temel virüs veritabanı güncelleme programlama işlemi **Güncelleme Yöneticisi** bileşeni kapsamında açıklanmıştır. Bu iletişim kutusunda virüs veritabanı güncelleme planı 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 virüs veritabanı 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 virüs veritabanı güncellemesinin başlatılması/başlatılmaması gerektiğini belirleyebilirsiniz.

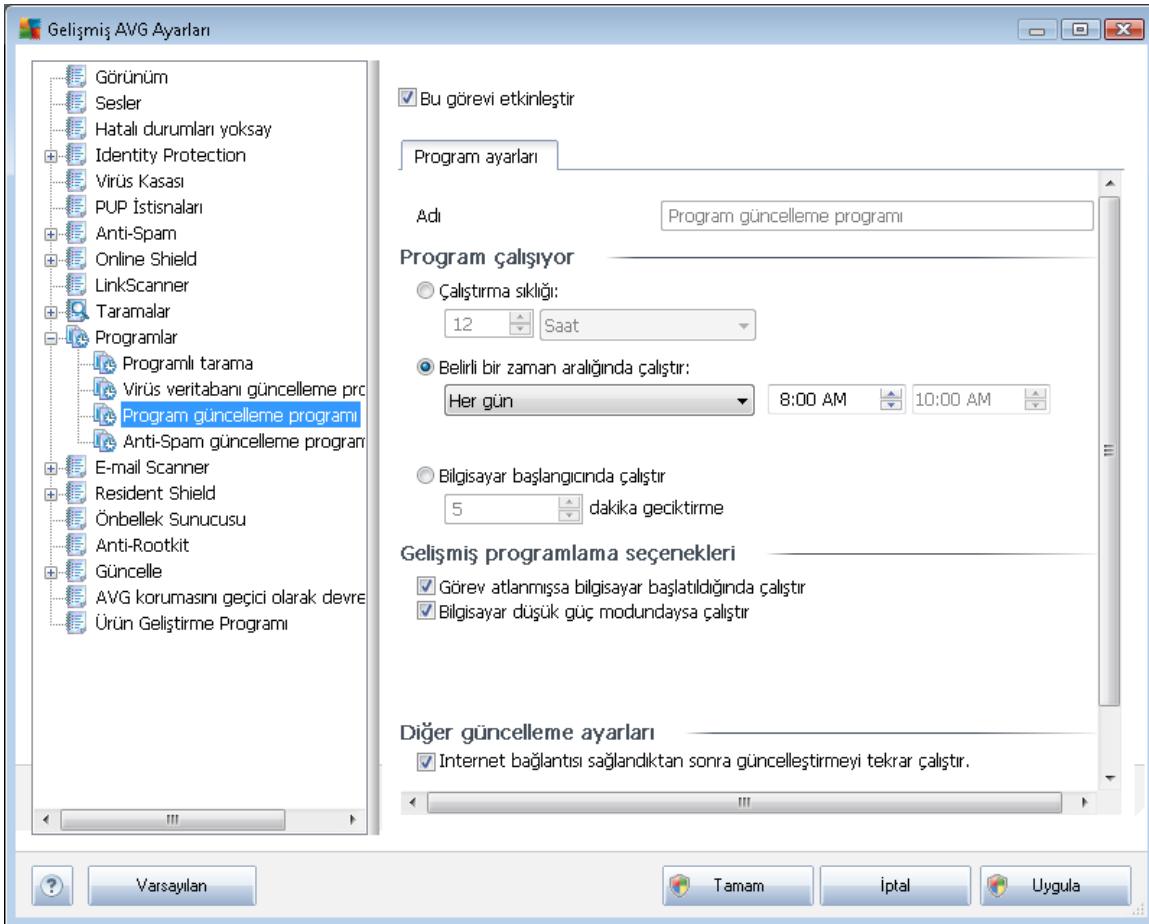
Diğer güncelleme ayarları

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.

Planlanan 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).

9.9.3. 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 alıřıyor

Burada, yeni programlanan program gncellemesinin bařlaması iin zaman aralıklarını girin. Zamanlama belirli bir srenin ardından tekrarlanan gncelleme ile (**Her ...'de bir**) ya da kesin bir tarih ve saat tanımlayarak (**Belirli bir saatte alıřtır...**) ya da (**Bilgisayar bařlangıcında**) ilgili bir programın gncellemesiyle tanımlanabilir.

Geliřmiř programlama seenekleri

Bu blmde, bilgisayar dřk g modundaysa veya tamamen kapatılmıřsa hangi kořullar altında program gncellemesinin bařlatılması/bařlatılmaması gerektiğini belirleyebilirsiniz.

Diğer gncelleme ayarları

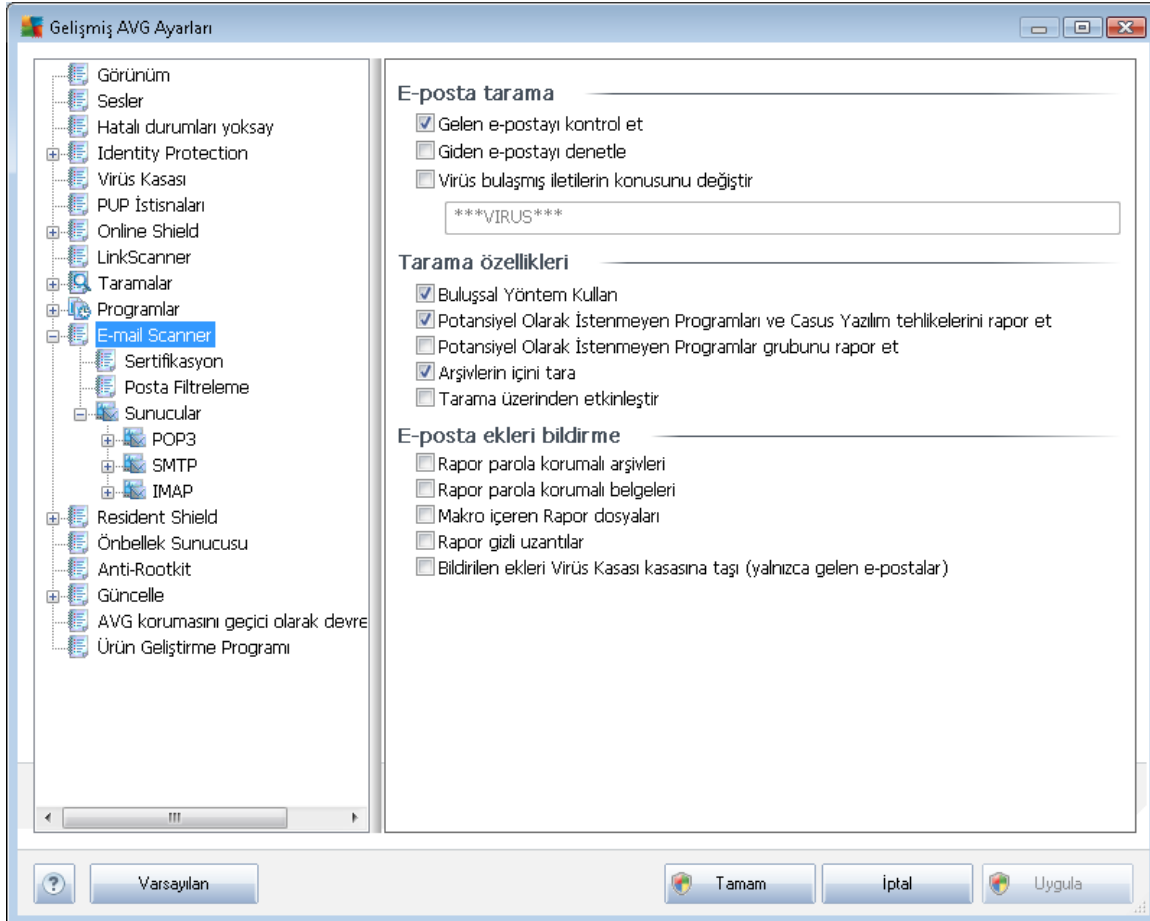
Internet baęlantısı kurulduęunda gncellemeyi yeniden alıřtır seeneğini iřaretleyerek Internet baęlantısı bozulduęunda ve gncelleme iřlemi bařarısız olduęunda, Internet baęlantısı yeniden saęlanır saęlanmaz yeniden bařlatıldıęından emin olun.

Planlanan gncelleme iřlemi sizin belirlediğiniz tarih ve saatte bařladıktan sonra [AVG sistem tepsisi simgesi](#) zerinde aılan bir aılır pencere vasıtasıyla bilgilendirileceksiniz ([Geliřmiř Ayarlar/Grnm](#) iletiřim kutusunun varsayılan yapılandırmasını deęiřtirmemiř olmanız kaydıyla).

Not: Programlanmış bir program gncellemesinin zaman akıřması oluřursa ve programlanmış tarama gerekleřirse, gncelleme iřlemi yksek nceliklidir ve tarama kesilir.

9.10. 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 filtrelenebilmesi 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 filtreleme yaparsınız; 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 oluşturmalarına 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 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.
- **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 aldığını unutmayın.

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:

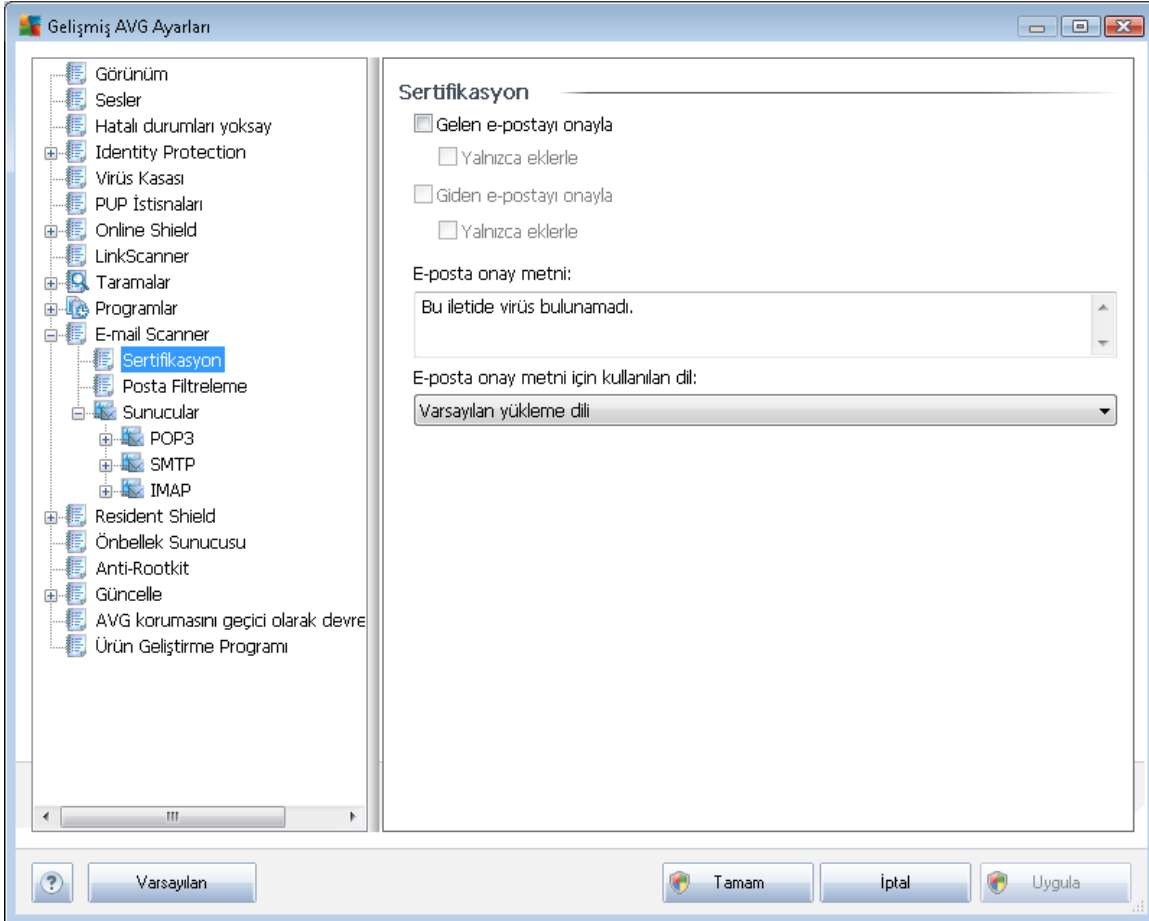
- **Parola korumalı arşivleri bildir** – parolayla korunan arşivler için (ZIP, RAR vb.) virüs taraması mümkün değildir. Bunların potansiyel olarak tehlikeli olduklarını bildirmek üzere kutuyu işaretleyin.
- **Parola korumalı belgeleri bildir** - parolayla korunan belgeler için virüs taraması mümkün değildir. 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 iletilerinin 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.

9.10.1. Sertifika

Sertifikasyon iletişim kutusunda hem gelen postanın hem de giden postanın metnini ve dilini belirleyebilirsiniz:



Sertifikasyon metni iki bölümden oluşur; kullanıcı bölümü ve sistem bölümü. Şu örneğe bakın: ilk satır kullanıcı bölümünü gösterir, geriye kalan bölüm ise otomatik olarak oluşturulur:

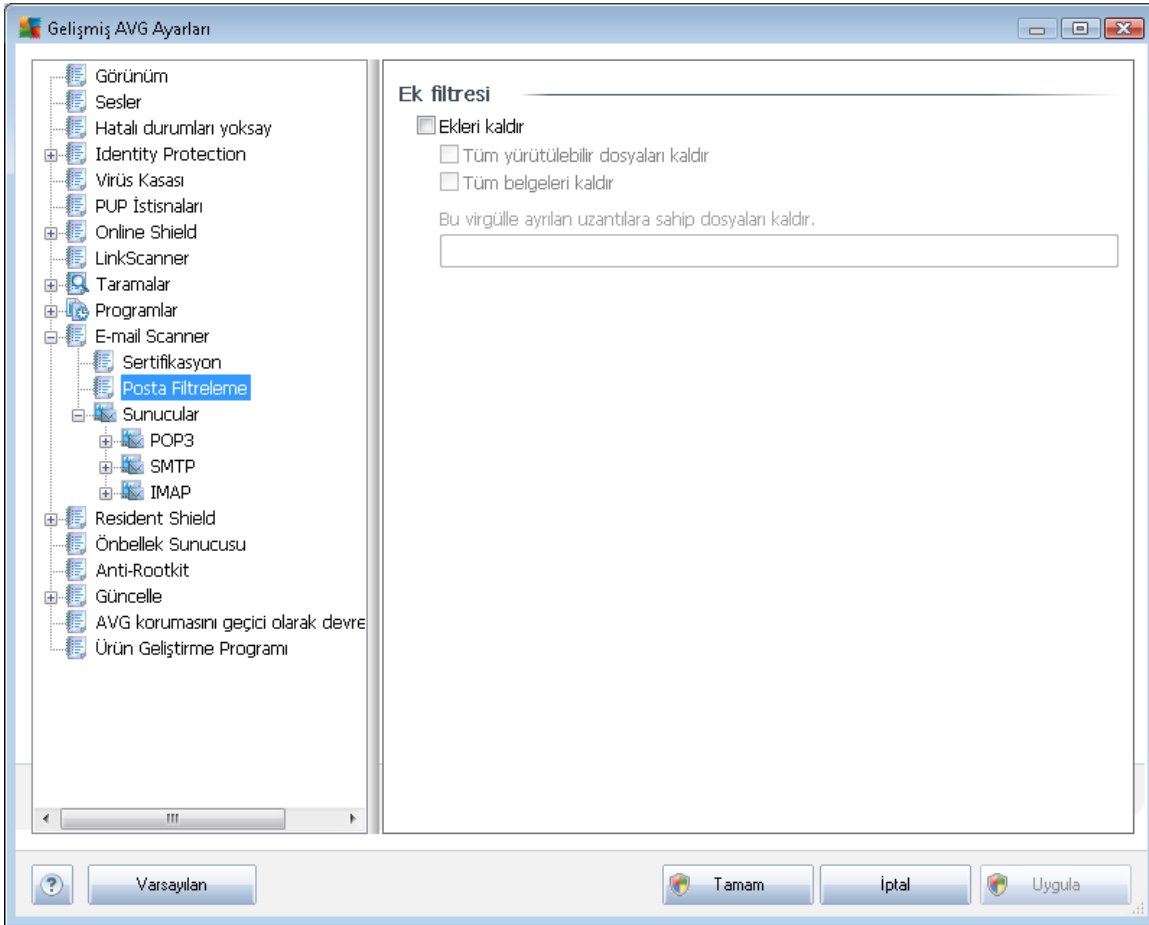
Bu iletide virüs bulunamadı.

AVG tarafından denetlendi.

Sürüm: x.y.zz / Virüs Veritabanı : xx.y.z - Yayınlanma Tarihi: 12/9/2010

Ya gelen ya da giden e-posta iletilerinin sertifikasyonunu kullanmaya karar vererseniz, bu iletişim kutusunda sertifikasyon metninin kullanıcı bölümünde (**E-posta sertifikasyon metni**) tam olarak ne yazacağını da belirtebilir ve sertifikasyonun otomatik olarak oluşturulan sistem bölümünde hangi dilin kullanılması gerektiğini seçebilirsiniz (**E-posta sertifikasyon metni için kullanılan dil**).

9.10.2. Posta Filtreleme

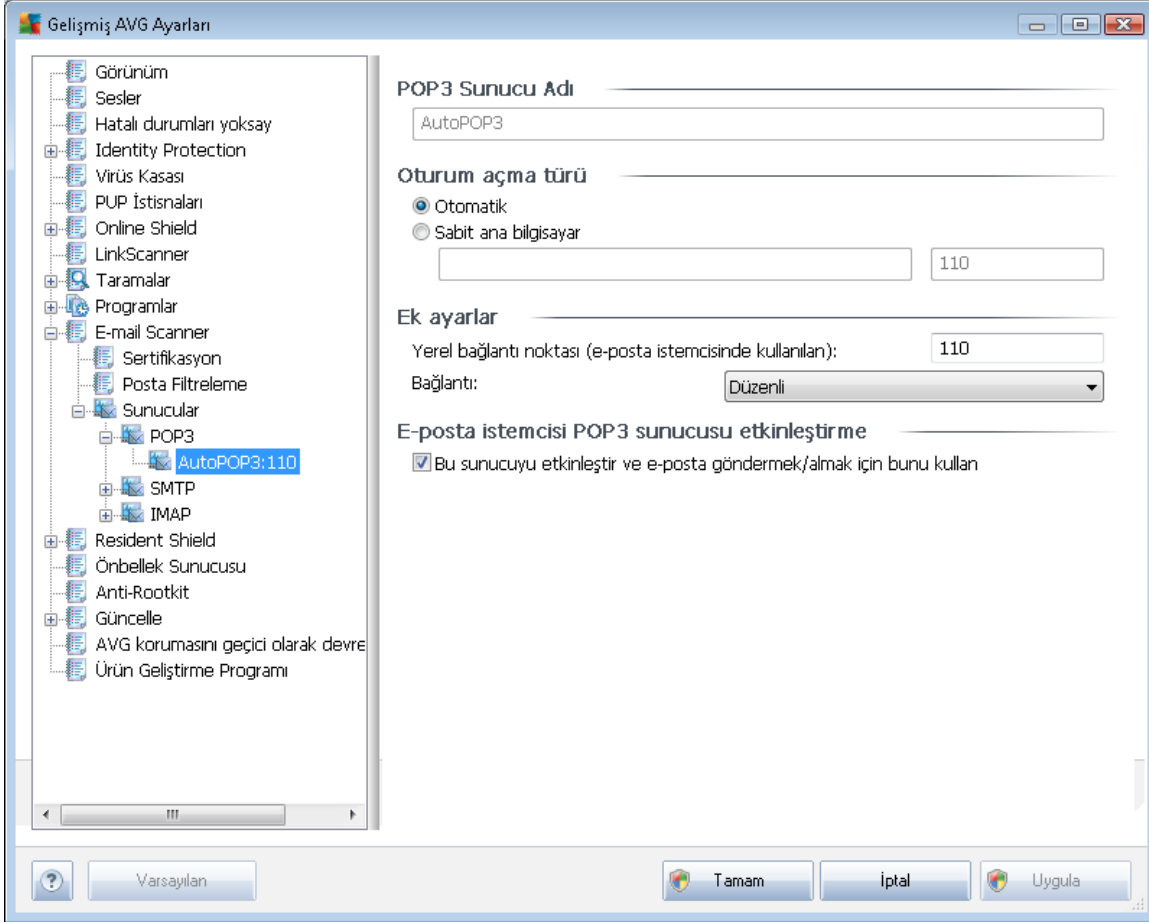


Ek filtresi iletişim kutusu, e-posta mesajlarının eklerinin taranmasına ilişkin parametreleri ayarlayabilmenizi sağlar. Varsayılan olarak **Eklentileri sil** seçeneği kapalıdır. Etkinleştirmeye karar vererseniz tüm e-posta mesajlarının eklentileri, bulaşmış nesne ya da potansiyel olarak tehlikeli nesne 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

9.10.3. Sunucular

Sunucular bölümünde [E-posta Tarayıcısı](#) bileşeninin sunucu parametrelerini değiştirebilir ya da **Yeni sunucu ekle** düğmesini kullanarak yeni sunucu yapılandırabilirsiniz.



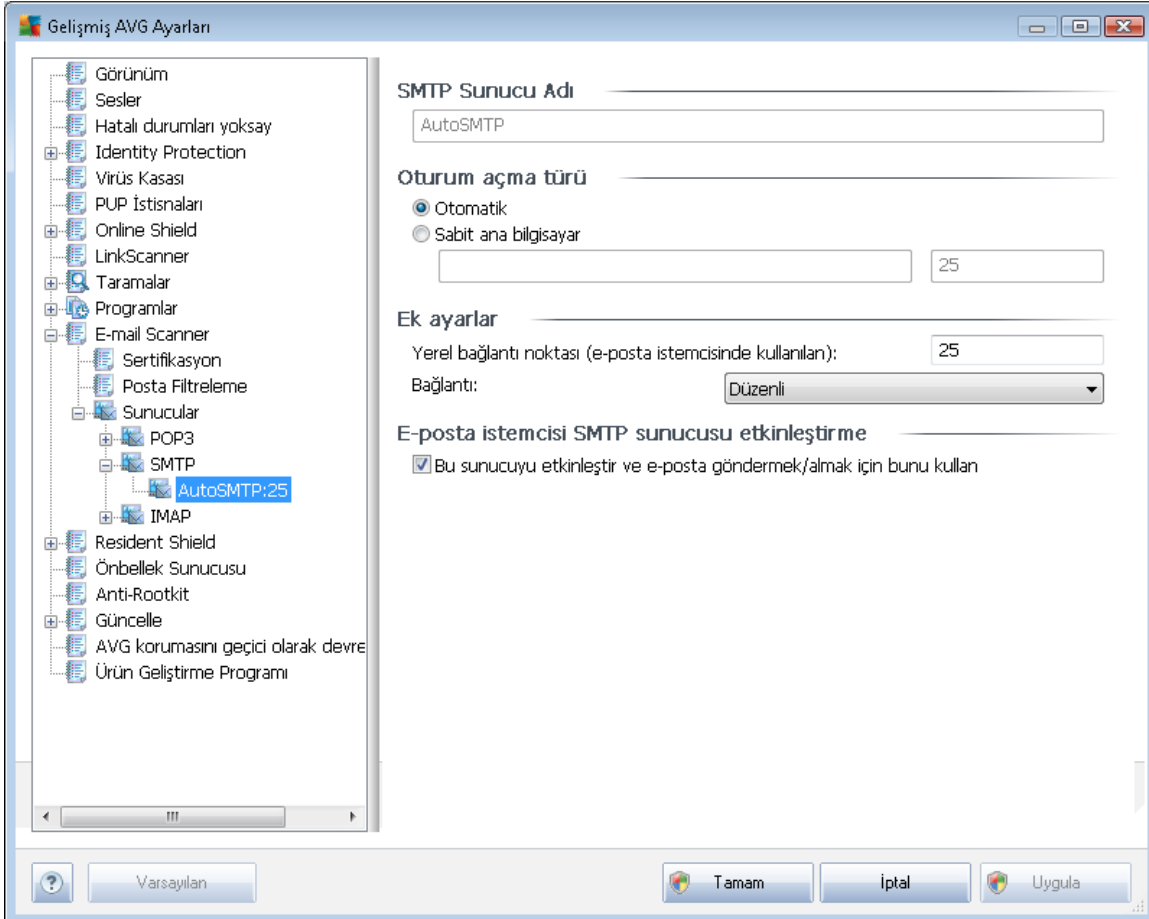
(**Sunucular** / **POP3** ile açılan) bu iletişim kutusunda, gelen postalar için POP3 protokolü kullanarak yeni bir [E-posta Tarayıcısı](#) sunucusu kurabilirsiniz:

- **POP3 Sunucusunun Adı** - bu alanda yeni eklenen sunucuların adını belirtebilirsiniz (*bir POP3 sunucusu eklemek için, sol menü ağacının POP3 öğesinin 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 ayırıcı olarak iki nokta üst üste kullanarak sunucu adının arkasına yazabilirsiniz (*örn. smtp.acme.com:8200*). POP3 iletişimi için standart bağlantı noktası 110'dur.

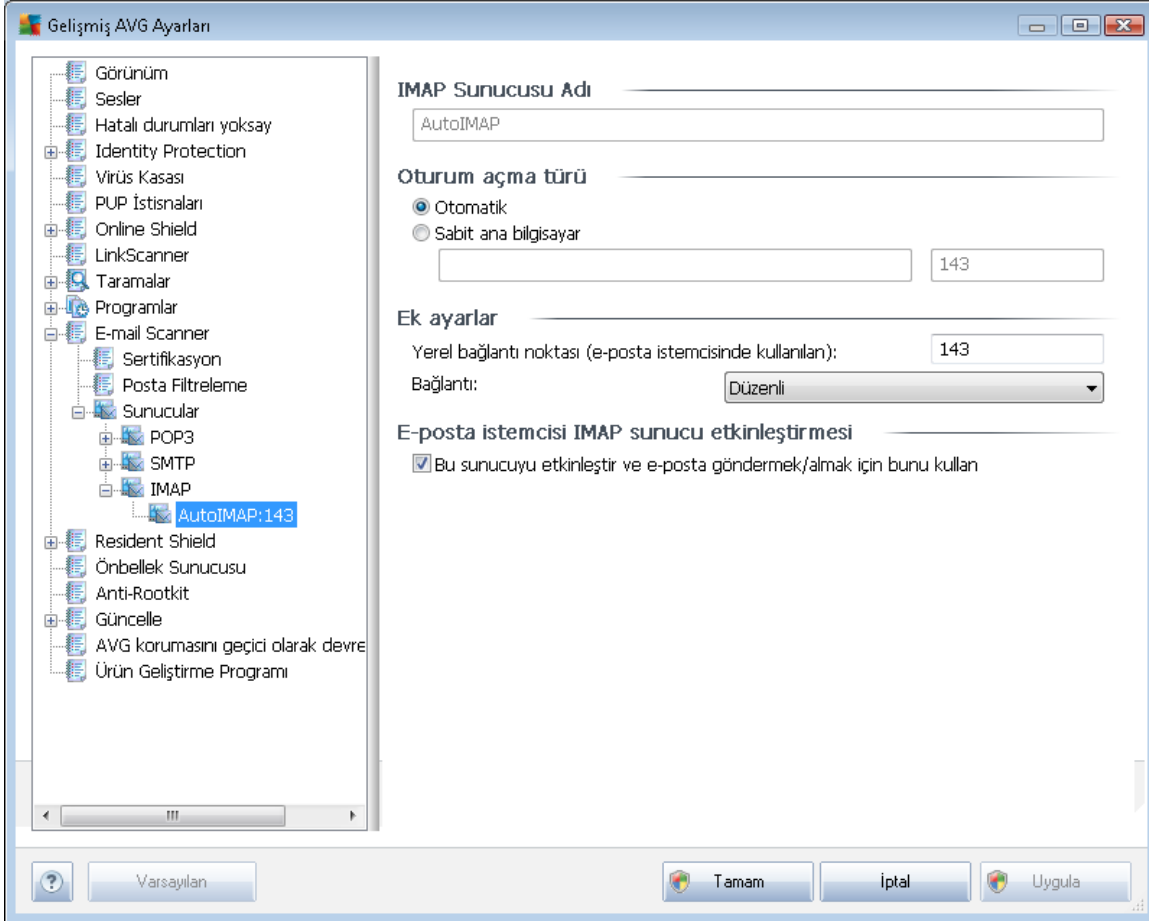
- **Diğer ayarlar** - daha ayrıntılı parametreleri belirler:
 - **Yerel bağlantı noktası** - Posta uygulamanızın iletişim kurması beklenen bağlantı noktasını belirler. Posta uygulamanızda, bu bağlantı noktasını POP3 iletişimi bağlantı noktası olarak belirtmeniz gerekir.
 - **Bağlantı** - kullanılacak 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 ögesinin 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

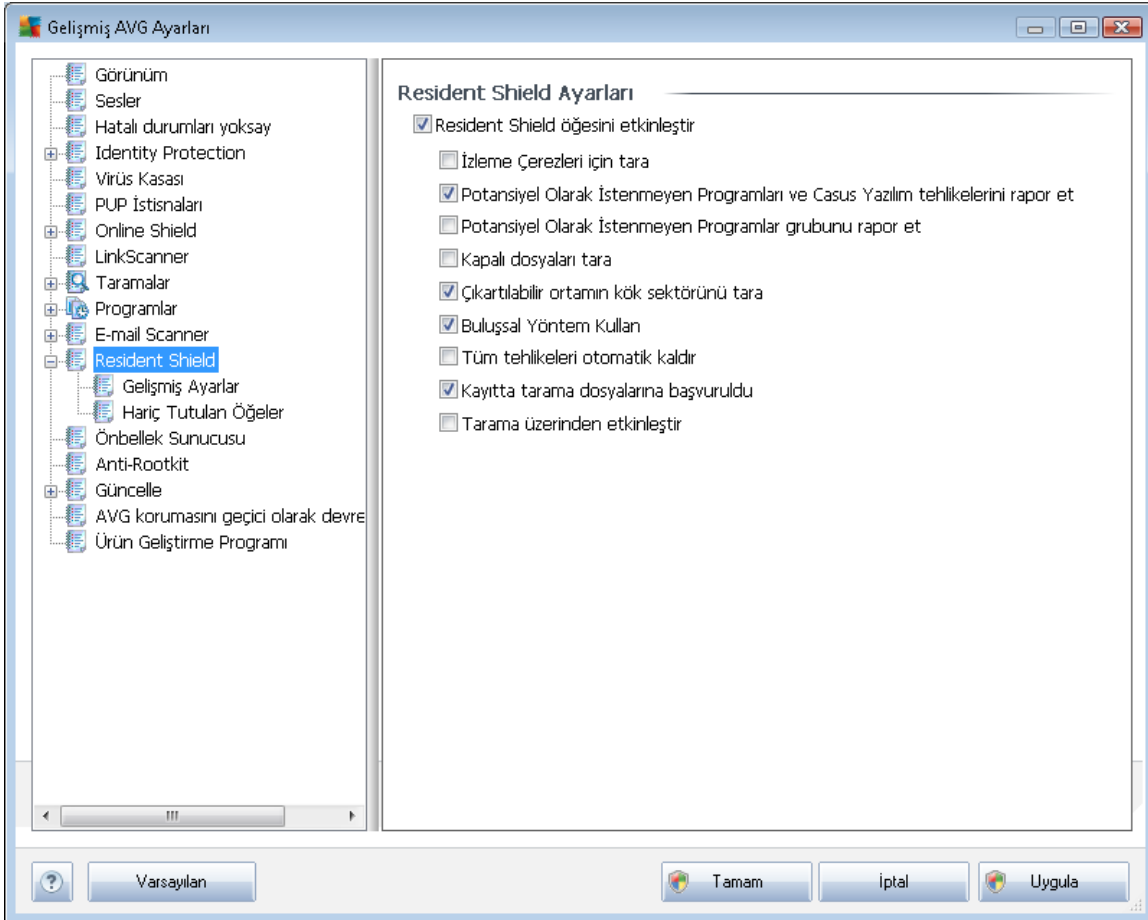


bağlantı noktası 143'tür.

- **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

9.11. Yerleşik Kalkan

Yerleşik Kalkan bileşeni, dosya ve klasörlerinizi çevrimiçi ortamda virüslere, casus yazılımlar ve diğer kötü amaçlı yazılımlara karşı korur.



Yerleşik Kalkan Ayarları iletişim kutusunda **Yerleşik Kalkan** korumasını **Yerleşik Kalkanı**

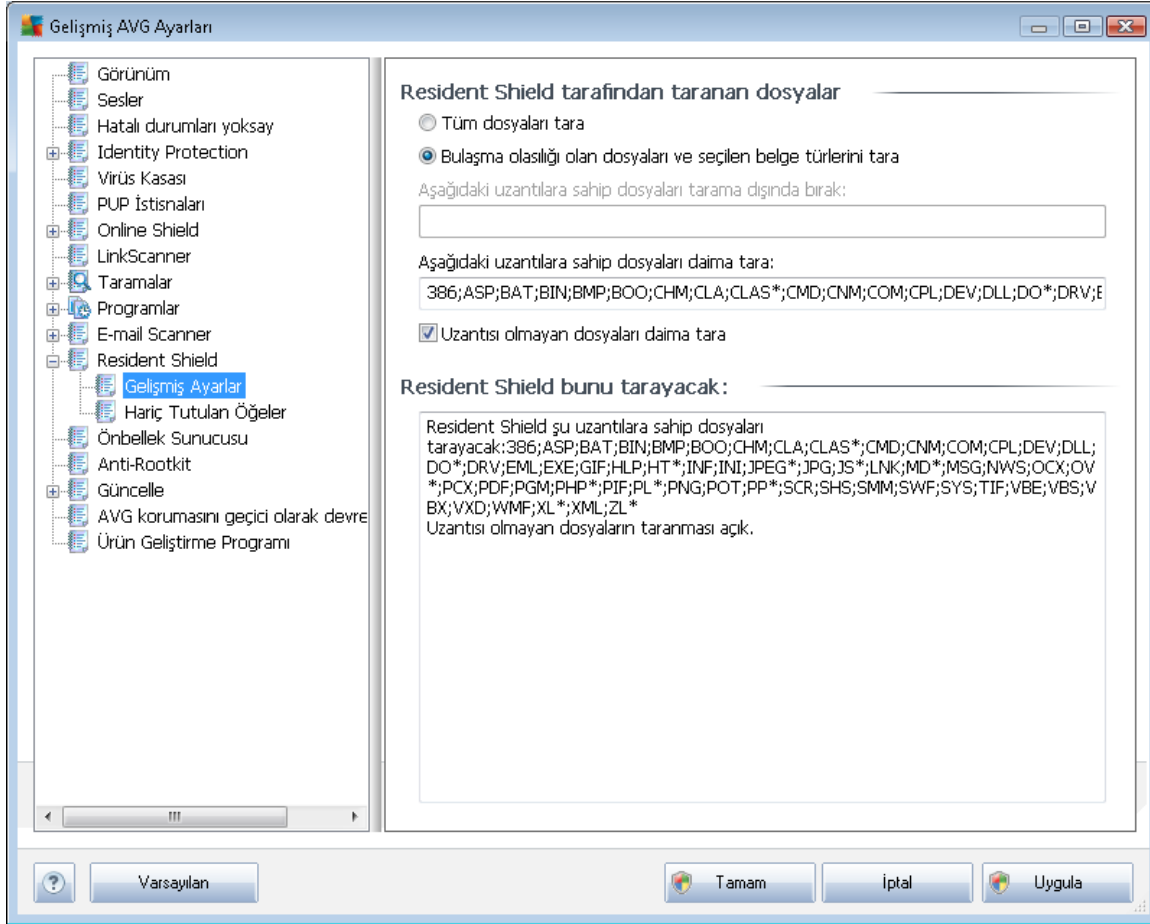


Etkinleştiröğesini işaretleyerek ya da işaretini kaldırarak etkinleştirebilir ya da devre dışı bırakabilirsiniz (*bu seçenek varsayılan olarak açıktır*). Buna ek olarak [Yerleşik Kalkanın](#) hangi özelliklerinin etkinleştirileceğini de seçebilirsiniz:

- **Tanımlama bilgilerini izlemek için tara** (*varsayılanda kapalıdır*) - 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 tehlikelerini rapor et** - (*varsayılan olarak açıktır*): [Anti-Spyware](#) motorunu etkinleştirmek ve virüslerle birlikte casus yazılımları da kontrol etmek için işaretleyin. [Casus yazılım, şüpheli kötü amaçlı yazılım kategorisini ifade eder: genellikle bir güvenlik riskini oluşturmaya 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 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** (*varsayılanda kapalıdır*) - işlem sonunda tarama, AVG'nin etkin nesneleri 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** - (*varsayılanda açıktır*) [buluşsal analiz](#), tespit etme işlemi sırasında kullanılır (*taranan nesne'nin komutlarının sanal bilgisayar ortamında dinamik olarak canlandırılması*)
- **Tüm tehditleri otomatik olarak kaldır** (*varsayılan olarak kapalıdır*) - tespit edilen tüm bulaşmalar, bir temizleme işlemi mevcutsa iyileştirilir ve temizlenemeyen tüm bulaşmalar kaldırılır.
- **Kayıt defterindeki dosyaları tara** (*varsayılanda açıktır*) - bilinen bulaşmanın sonraki bilgisayar başlangıcında çalıştırılmasını önlemek için, başlangıç kayıt defterine eklenmiş tüm çalıştırılabilir dosyaları AVG tarar.
- **Kapsamlı taramayı etkinleştir** (*varsayılanda kapalıdır*) - belirli durumlarda (*çok acil bir durum olduğunda*) nesnelerin derinlemesine işleme olasılığını denetleyecek çok hassas algoritmaları etkinleştirmek için bu seçeneği işaretleyebilirsiniz. Ancak, bu yöntemin çok fazla zaman aldığını unutmayın.

9.11.1. Gelişmiş Ayarlar

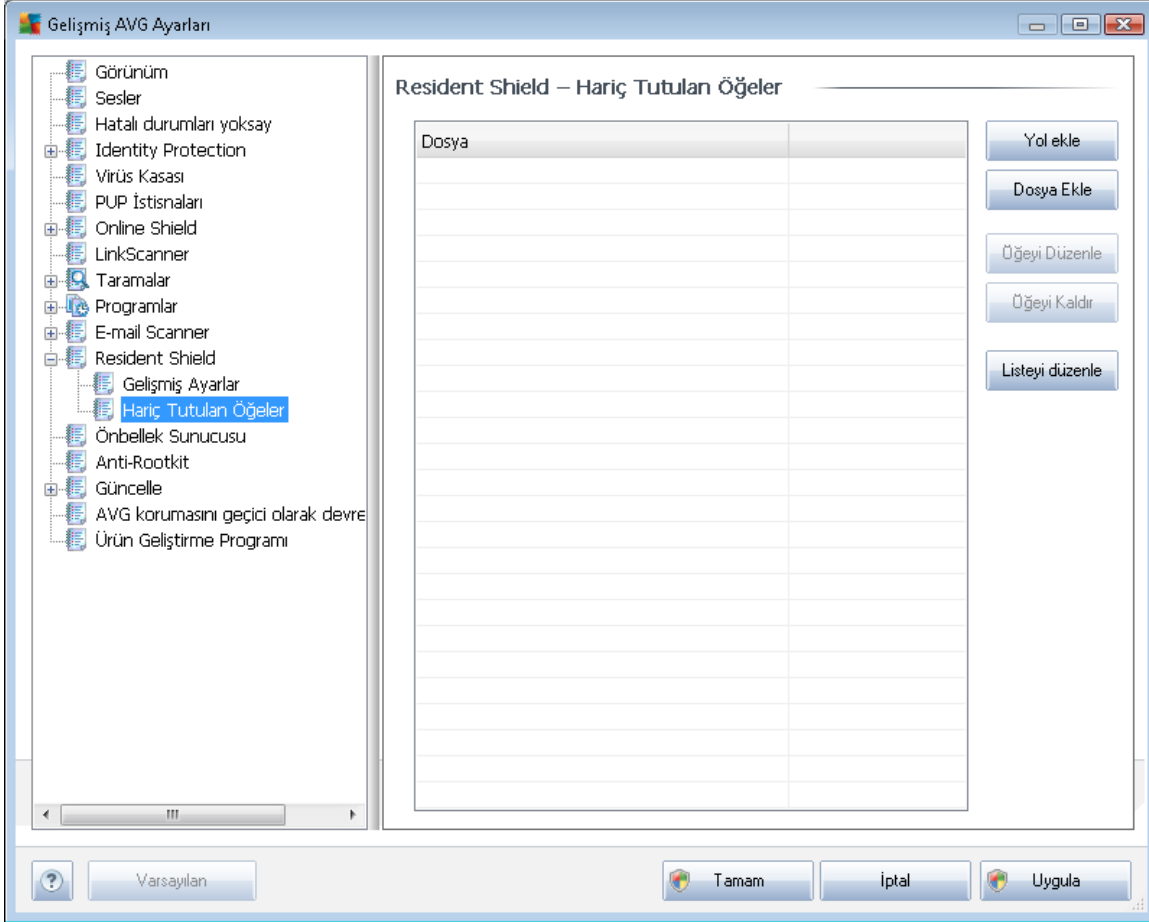
Yerleşik Kalkan tarafından taranan dosyalar penceresinde taranan dosyaların yapılandırılması mümkündür (belirli dosya uzantılarına göre):



Tüm dosyaların mı yoksa sadece bulaşmış dosyaların mı taranacağına karar verin - Bunun ardından tarama işlemi sırasında hariç tutulacak dosyaları tanımlayan dosya uzantısı listesini de seçebilirsiniz, bunun yanı sıra her ne şart altında olursa olsun taranmasını istediğiniz dosyaları tanımlayan dosya uzantılarını gösteren bir liste de oluşturabilirsiniz.

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

9.11.2. Hariç tutulan öğeler



Yerleşik Kalkan - Hariç Tutulan Öğeler iletişim kutusu [Yerleşik Kalkan](#) taraması sırasında hariç tutulması gereken klasörleri seçebilmenizi sağlar.

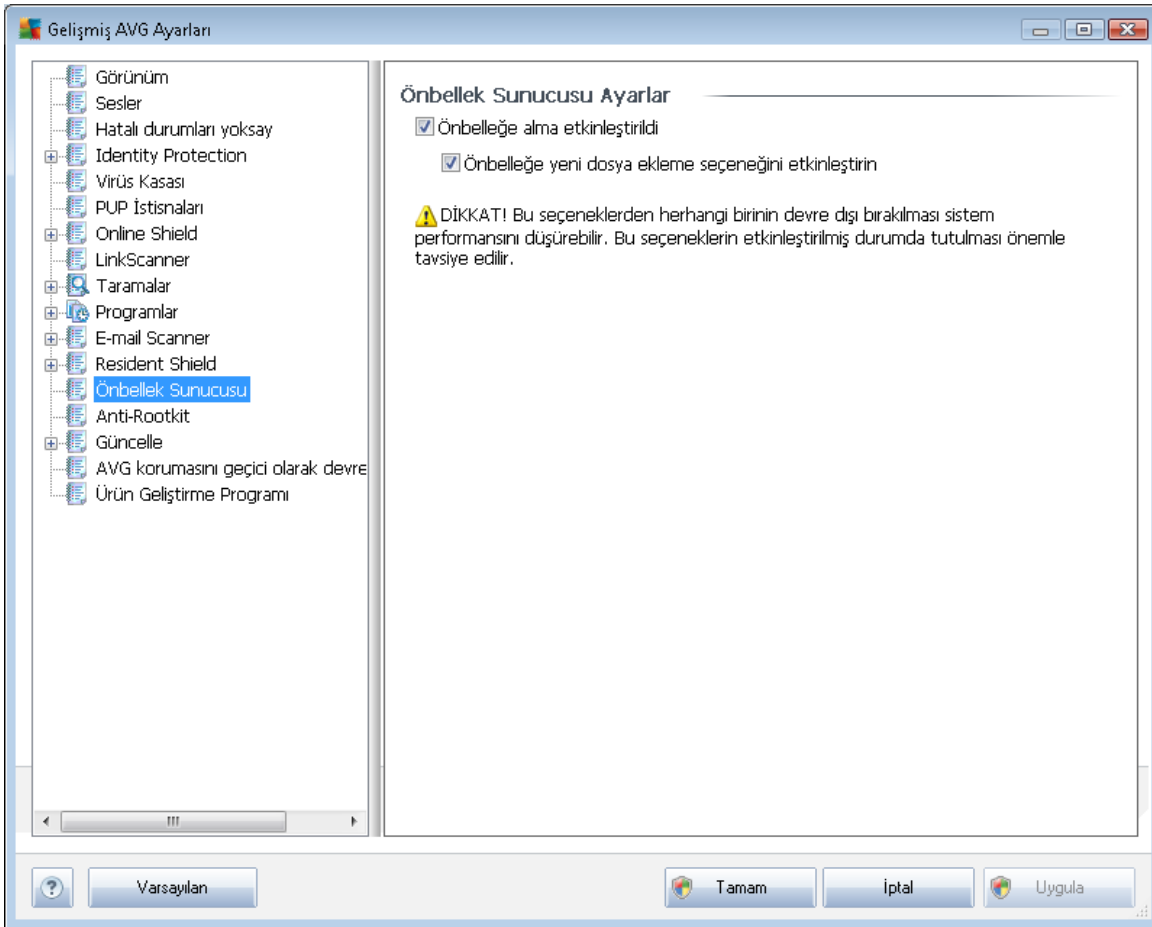
Bu gerekli değilse, hiçbir öğeyi hariç tutmamanızı önemle öneririz!

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

9.12. Önbellek Sunucusu

Önbellek Sunucusu, herhangi bir taramayı hızlandırmak için tasarlanmış bir işlemdir (*istek üzerine tarama, programlanmış tüm bilgisayarı tarama, Yerleşik Kalkan taraması*). Güvenilir dosyaların bilgilerini toplar ve saklar (*dijital imzalı sistem dosyaları vb.*): Bu dosyalar, daha sonra güvenli olarak ele alınır ve tarama sırasında atlanır.



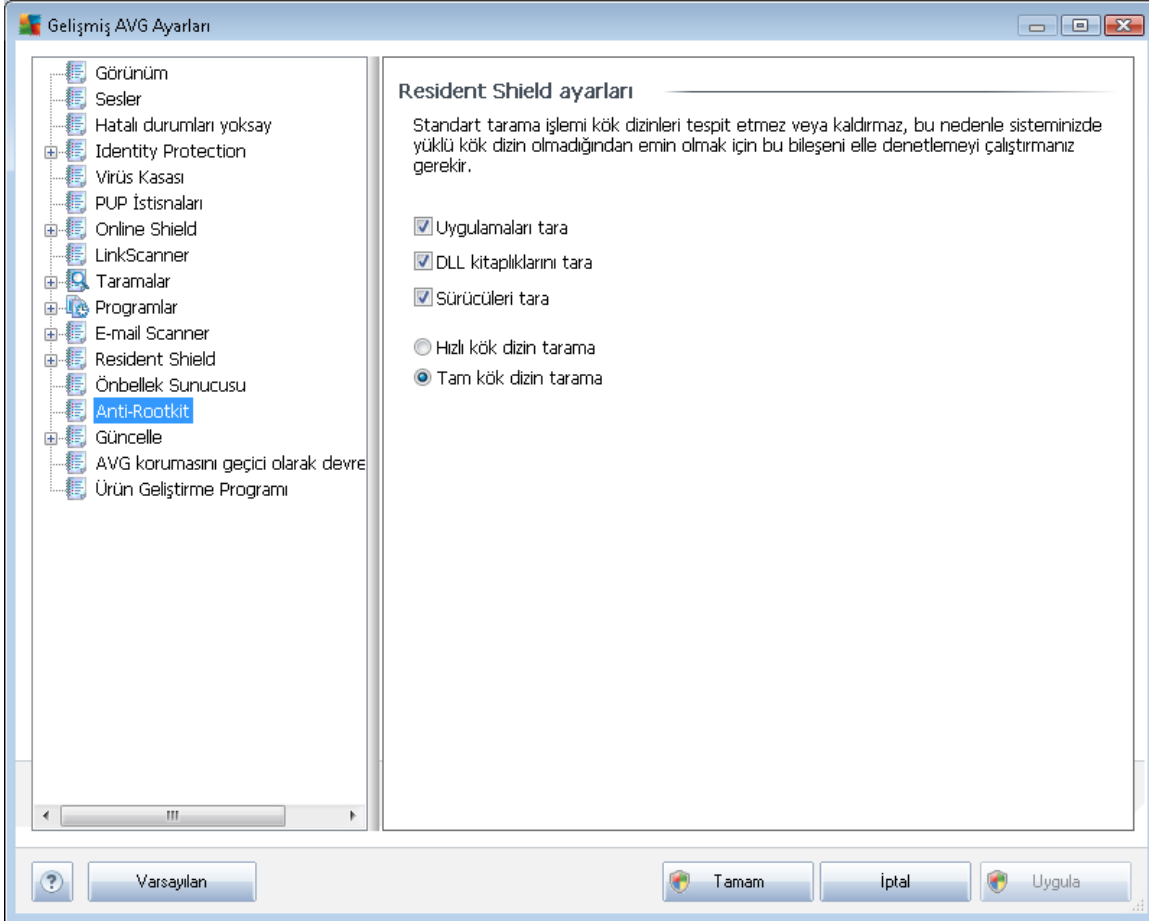
Ayarlar iletişim kutusu iki seçenek sunar:

- **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 taranacağından 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.



9.13. Kök Kullanıcı Takımlarına Karşı Koruma (Anti-Rootkit)

Bu iletişim kutusunda [Anti-Rootkit](#) bileşenlerinin yapılandırmasını düzenleyebilirsiniz:



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

Taranmasını istediğiniz nesneleri belirlemek üzere ilgili kutuları işaretleyin:

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

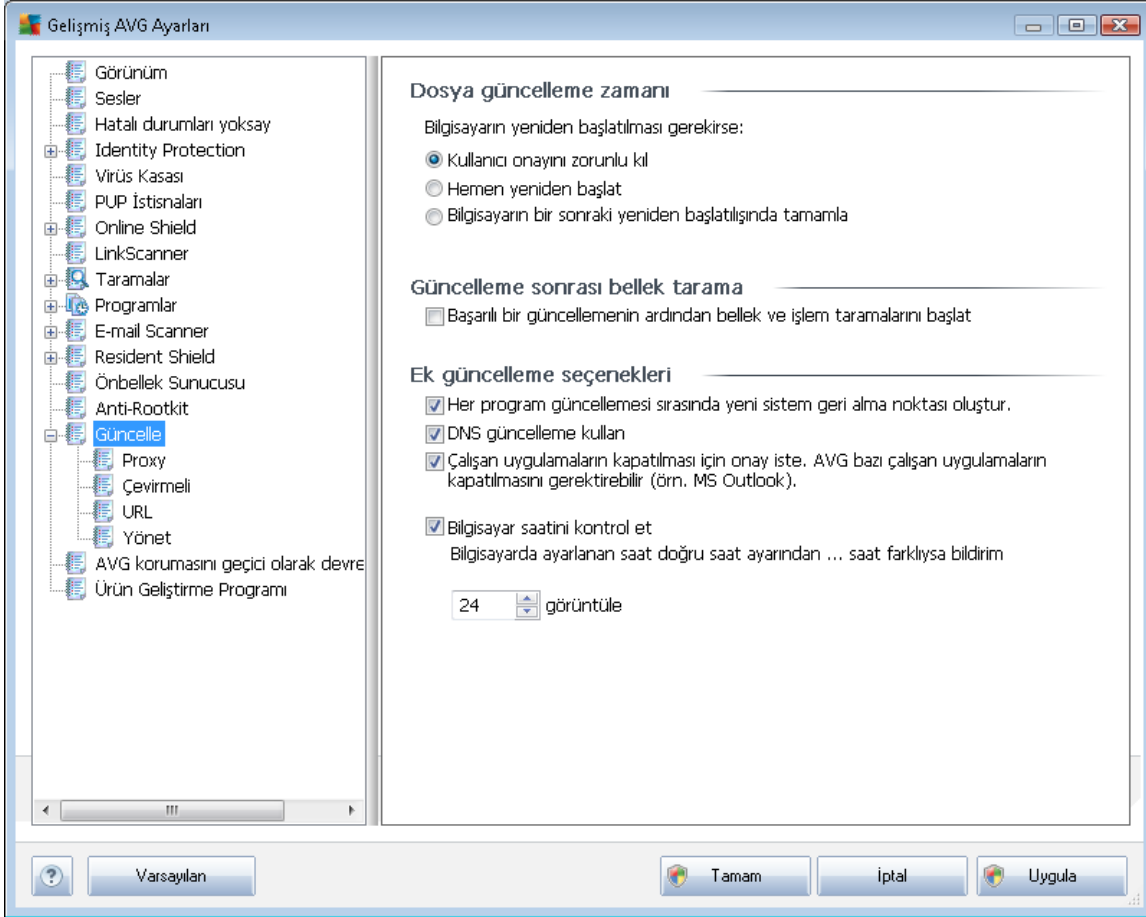
Bunun ardından kök kullanıcı tarama modunu da seçebilirsiniz:

- **Hızlı kök dizin tarama** - çalışan tüm işlemleri, yüklü sürücüler ve sistem klasörlerini (genellikle c:\Windows) tarar
- **Tam kök dizin tarama** - çalışan tüm işlemleri, yüklü sürücüler, sistem klasörünü (



genellikle c:\Windows), ayrıca tüm yerel diskleri (flash disk dahil, ancak disket/CD sürücülerini hariç) tarar

9.14. 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](#)
- **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!

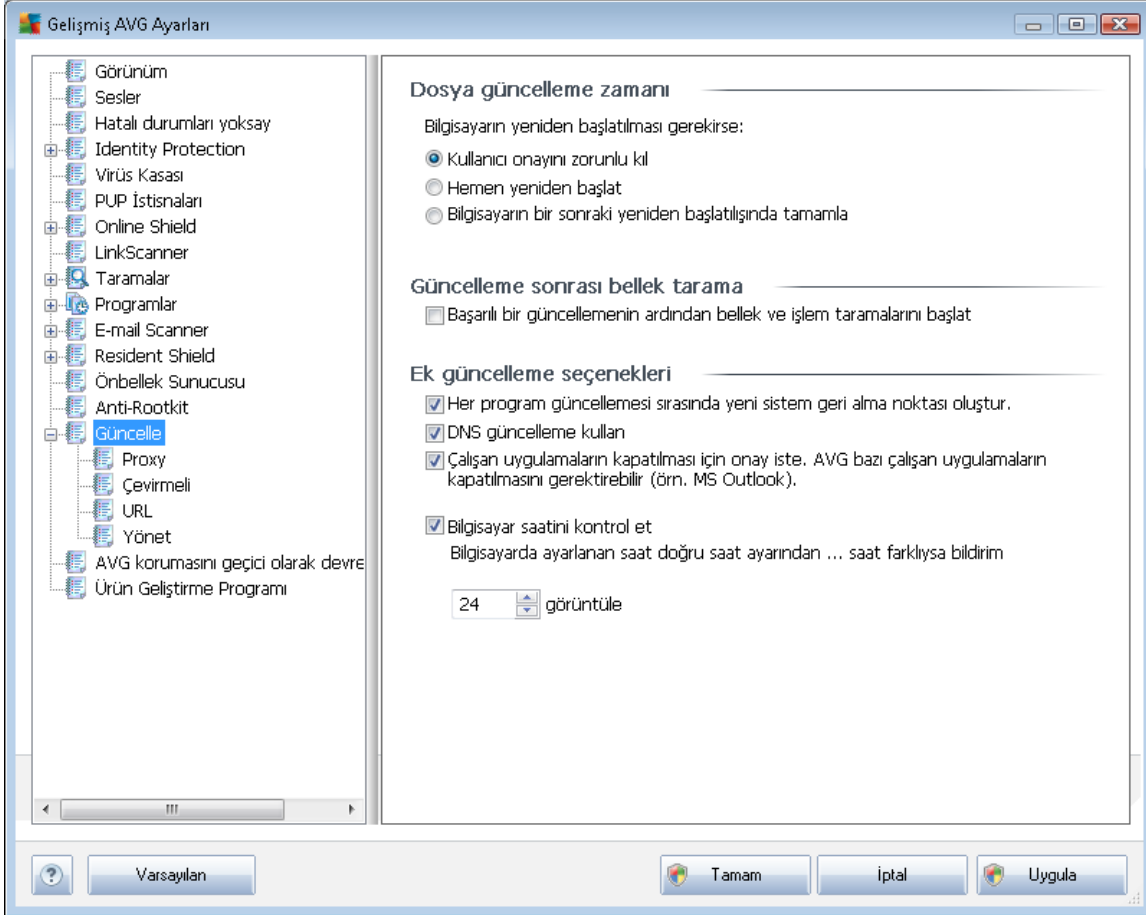
Güncelleme sonrası bellek tarama

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 Anti-Virus** 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.

9.14.1. 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 sunucusu 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**



seeneęini iřaretleyin) ařaęıdaki bilgileri girmeniz gerekir:

- **Sunucu**– sunucunun IP adresini ya da sunucunun adını girin
- **Baęlantı Noktası**– İnternet erişimine açık baęlantı noktasının numarasını girin (*varsayılan olarak bu deęer 3128 olarak atanmıřtır fakat isteęiniz doęrultusunda deęiřtirebilirsiniz – emin deęilseniz lütfen aę yöneticiniz ile irtibat kurun*)

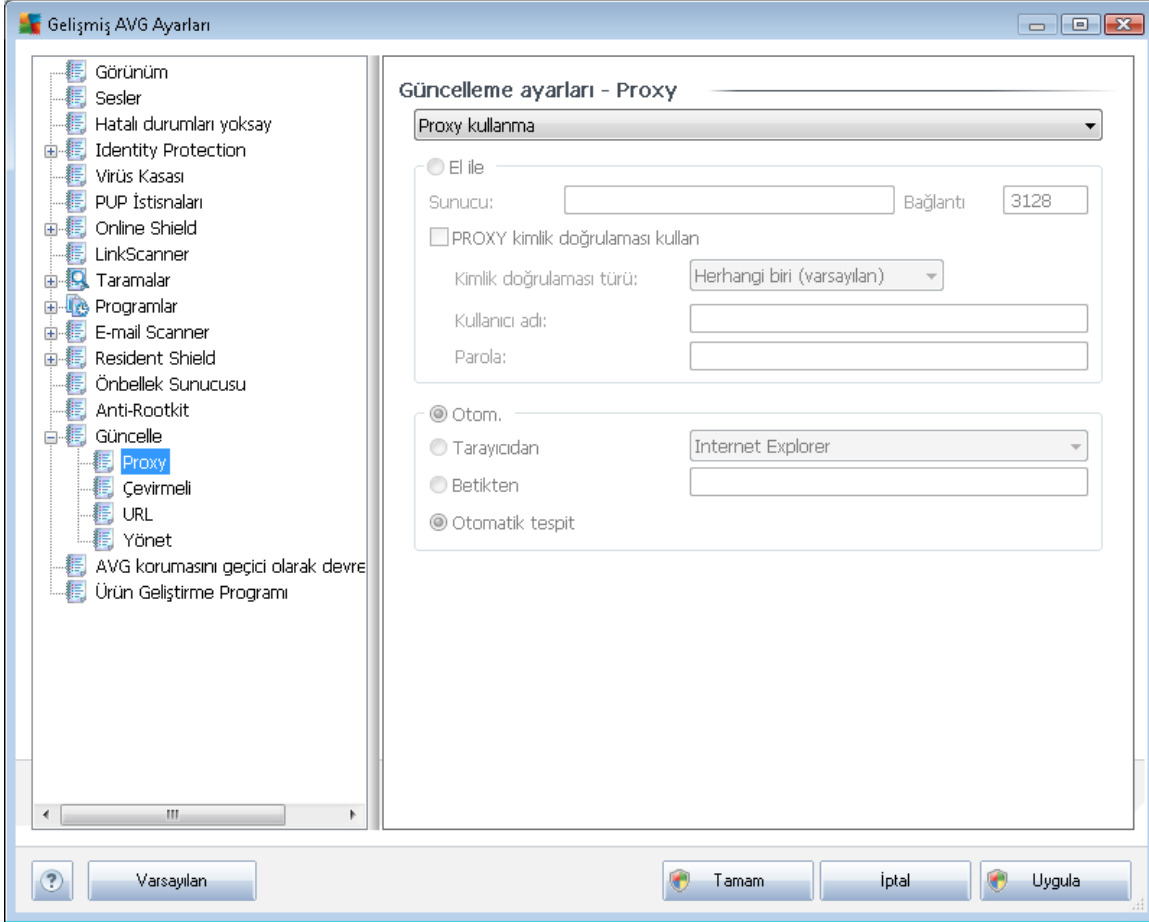
Proxy sunucusunda her kullanıcı için farklı kurallar yapılandırılabilir. Proxy sunucunuz bu řekilde yapılandırılmıř ise proxy sunucusu üzerinden yapılan İnternet baęlantınıza iliřkin kullanıcı adı ve parolanızı onaylamak için **PROXY kimlik doęrulamasını kullan** seeneęini iřaretleyin.

Otomatik yapılandırma

Otomatik yapılandırmayı seerseniz (*ilgili iletiřim kutusunu etkinleřtirmek için Oto seeneęini iřaretleyin*) ardından proxy yapılandırmasının nereden alınacaęını belirleyin:

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

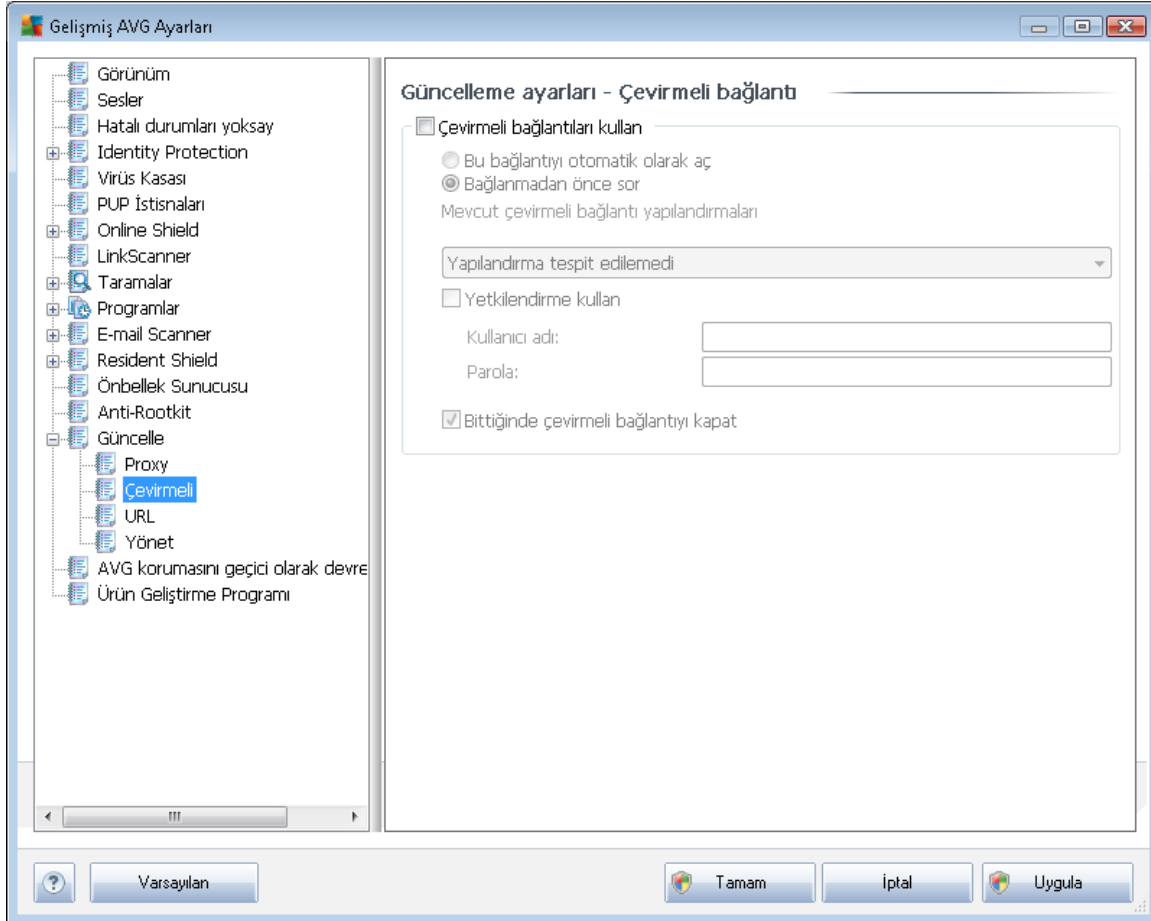
9.14.2. Çevirmeli



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

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

9.14.3. URL

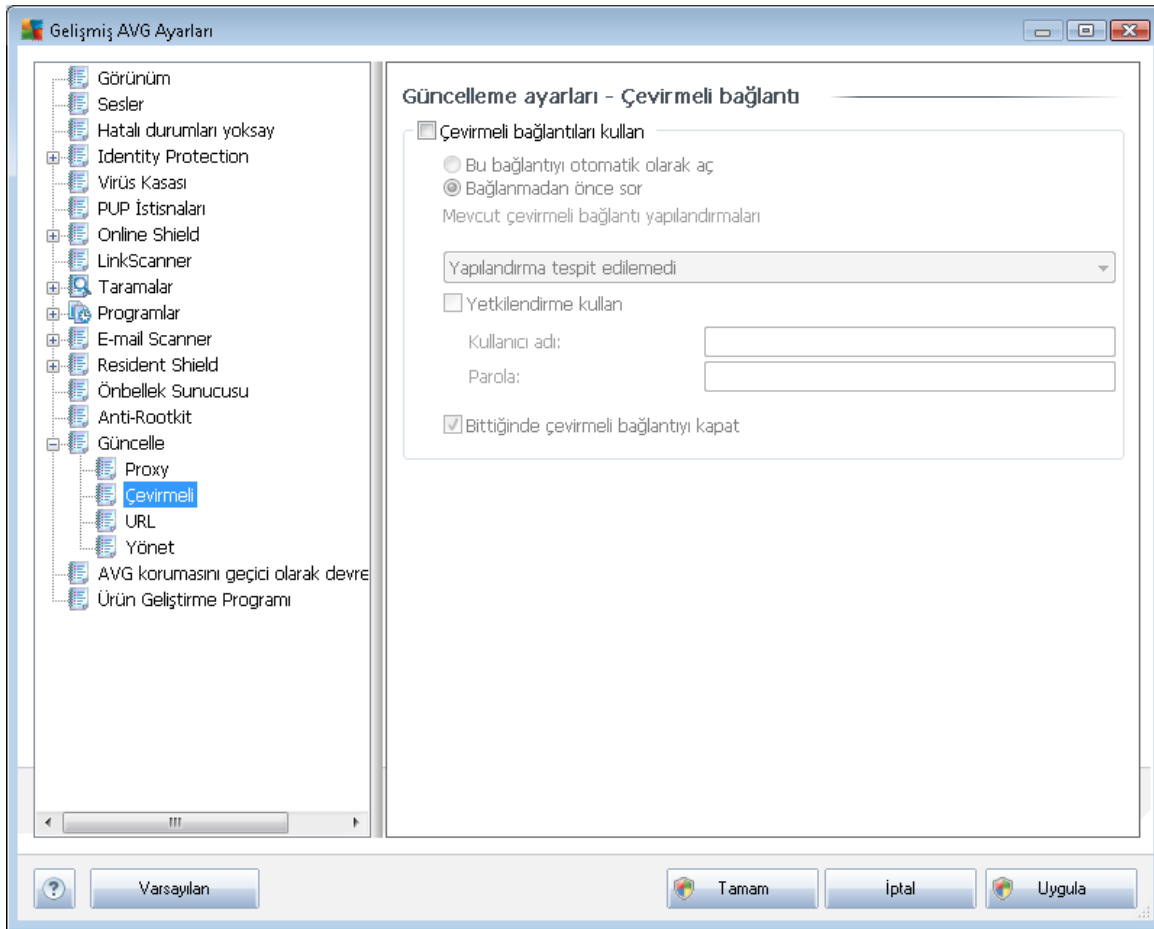


URL iletişim kutusunda güncelleme dosyalarının indirilebileceği bir dizi Internet adresi bulunur. Liste ve liste öğeleri aşağıdaki kontrol düğmeleri kullanılarak düzenlenebilir:

- **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

9.14.4. Yönetme

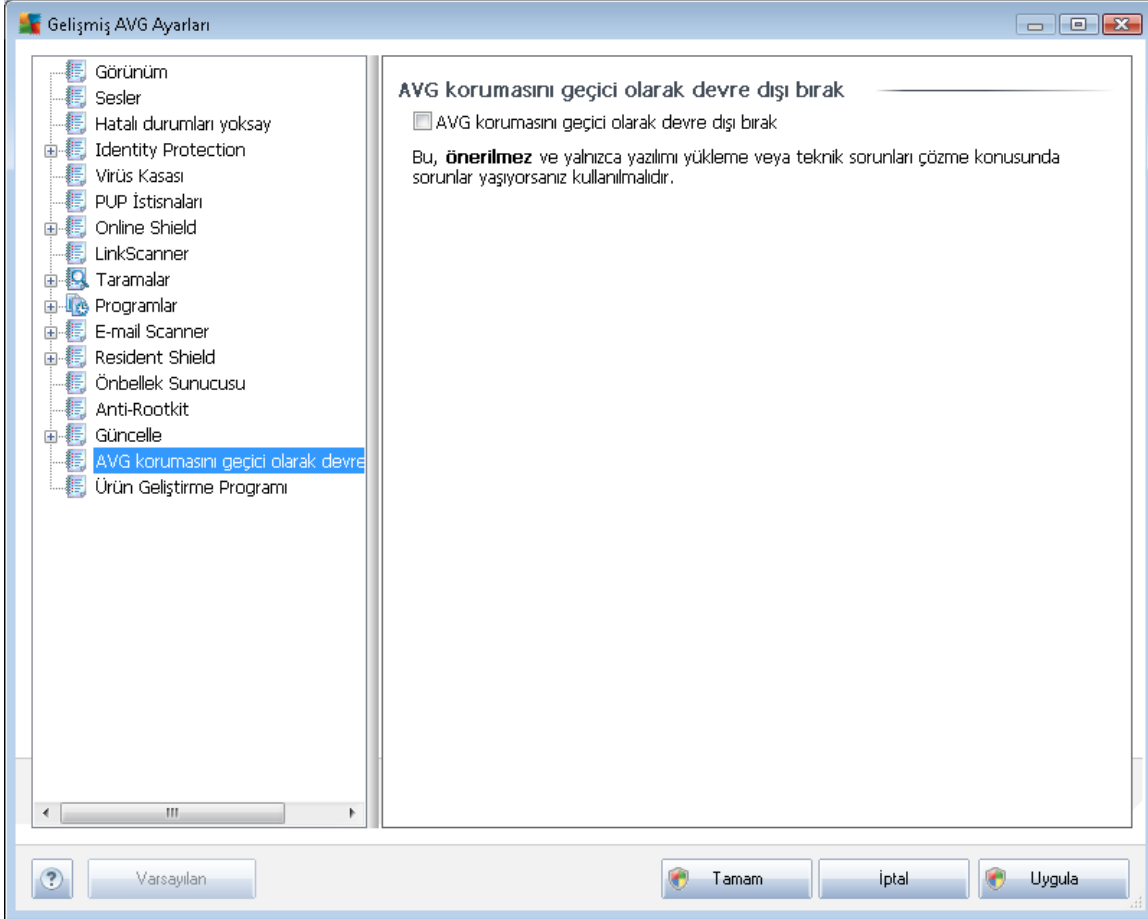
Yönet iletişim penceresi, iki adet düğme ile ulaşılabilen iki seçenek sunmaktadır:



- **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*)



9.15. AVG korumasını geçici olarak devre dışı bırak



AVG korumasını geçici olarak devre dışı bırak iletişim kutusunda, **AVG Anti-Virus** 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 yüklemekten önce ve hatta yükleyici veya yazılım sihirbazı yükleme işlemi sırasında istenmeyen kesintilerin olmamasını sağlamak için çalışan program ve uygulamaların kapatılmasını önerse bile AVG'yi devre dışı bırakmak **gerekmez**. Yükleme sırasında gerçekten sorun yaşıyorsanız, öncelikle [Yerleşik Kalkan](#) bileşenini devre dışı bırakmayı deneyin. AVG'yi geçici olarak devre dışı bırakmanız gerekiyorsa, işleminizi tamamladıktan sonra AVG'yi en kısa zamanda tekrar etkinleştirmeniz gerekir. Virüslerden korunma yazılımınız devre dışı bırakılmışken İnternete veya bir ağa bağlanırsanız, bilgisayarınız saldırılara açık durumda olur.

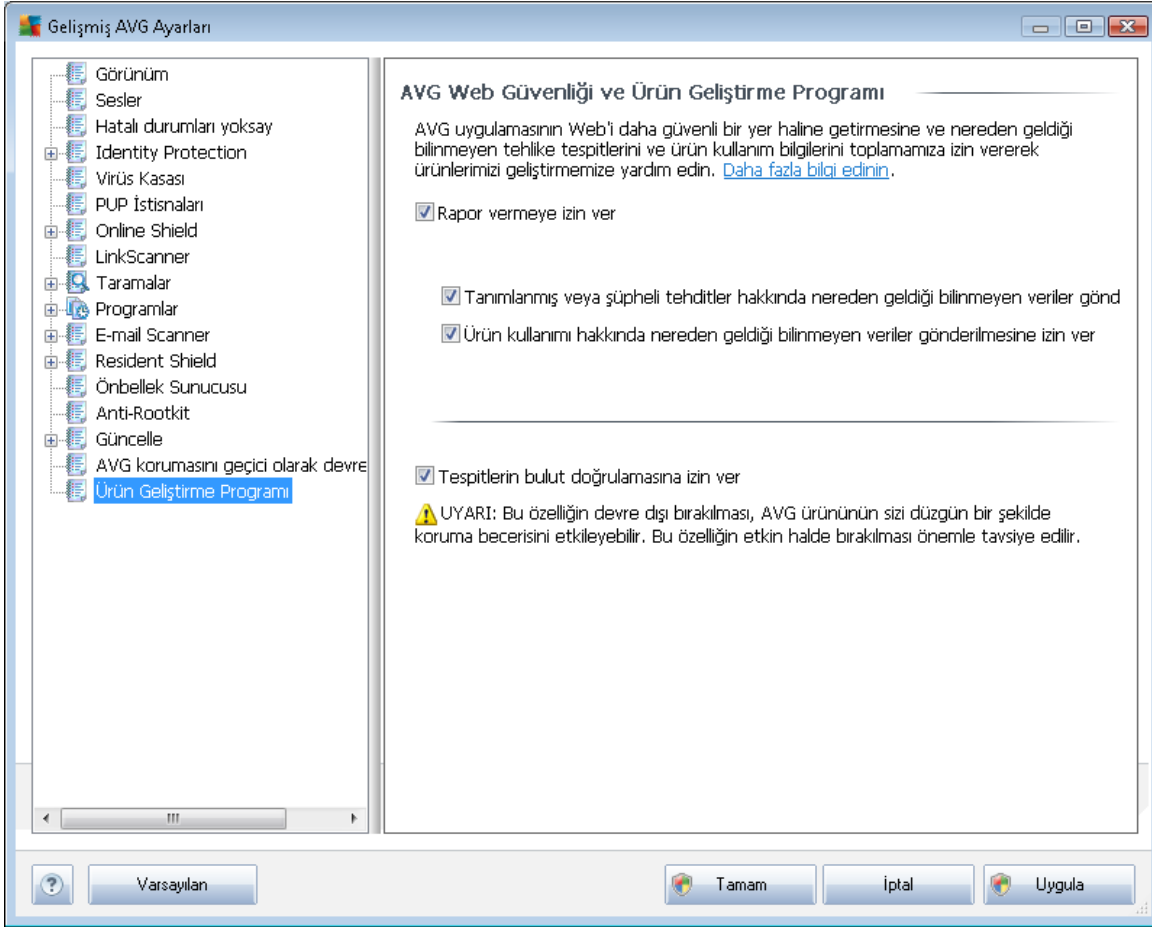
9.16. Ürün Geliştirme Programı

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. **Raporlamaya izin ver** seçeneği, tespit edilen tehditlerin AVG'ye bildirilmesini etkinleştirmek içindir. 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 ayrıca raporlarda kişisel bilgileriniz bulunmaz. Tespit edilen tehditlerin bildirilmesi isteğe bağlıdır, ancak bu özelliği açmanız bizim için gerçekten önemlidir. Bu şekilde siz ve diğer AVG kullanıcıları için korumamızı geliştirmemize yardımcı olursunuz.



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



sunucularında ve ağı 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 yazılımlarıdır. 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, uyarıda 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.

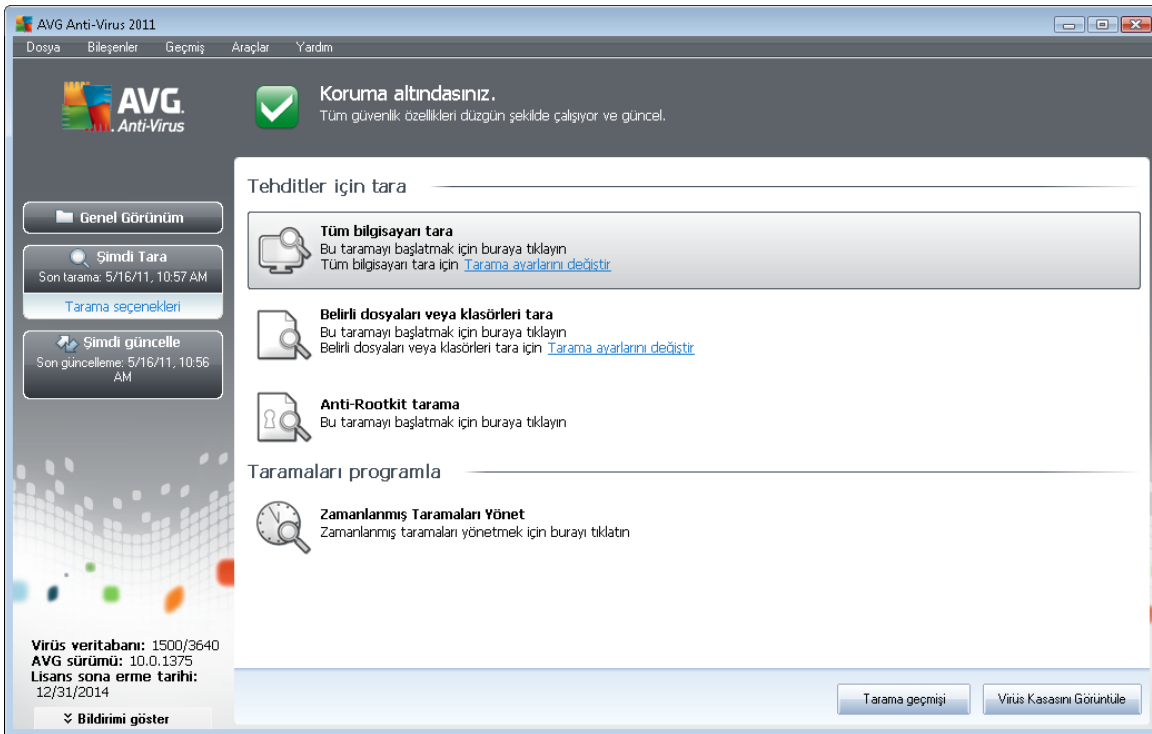
Sizi bu farklı türlerdeki tüm tehditlere karşı korumak için AVG aşağıdaki özel bileşenleri içerir:

- **[Anti-Virus](#)**, bilgisayarınızı virüslerden korur.
- **[Anti-Spyware](#)**, bilgisayarınızı casus yazılımlara karşı korur.
- **[Online Shield](#)**, internette gezinirken sizi hem virüslere hem de casus yazılımlara karşı korur.
- **[LinkScanner](#)**, sizi bu bölümde açıklanan diğer çevrimiçi tehditlere karşı korur.

10. AVG Tarama

Tarama, **AVG Anti-Virus** işlevinin önemli bir parçasıdır. Talebe uygun taramalar yapabilir ya da istediğiniz zamanlarda [periyodik taramalar planlayabilirsiniz](#).

10.1. Tarama Arayüzü



AVG tarama arayüzüne [Tarama seçenekleri](#) [hızlı bağlantısı](#) aracılığıyla erişilebilir. **Tehditleri tarama** 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 tarama](#)
 - [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.

10.2. Öntanımlı Taramalar

AVG Anti-Virus 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.

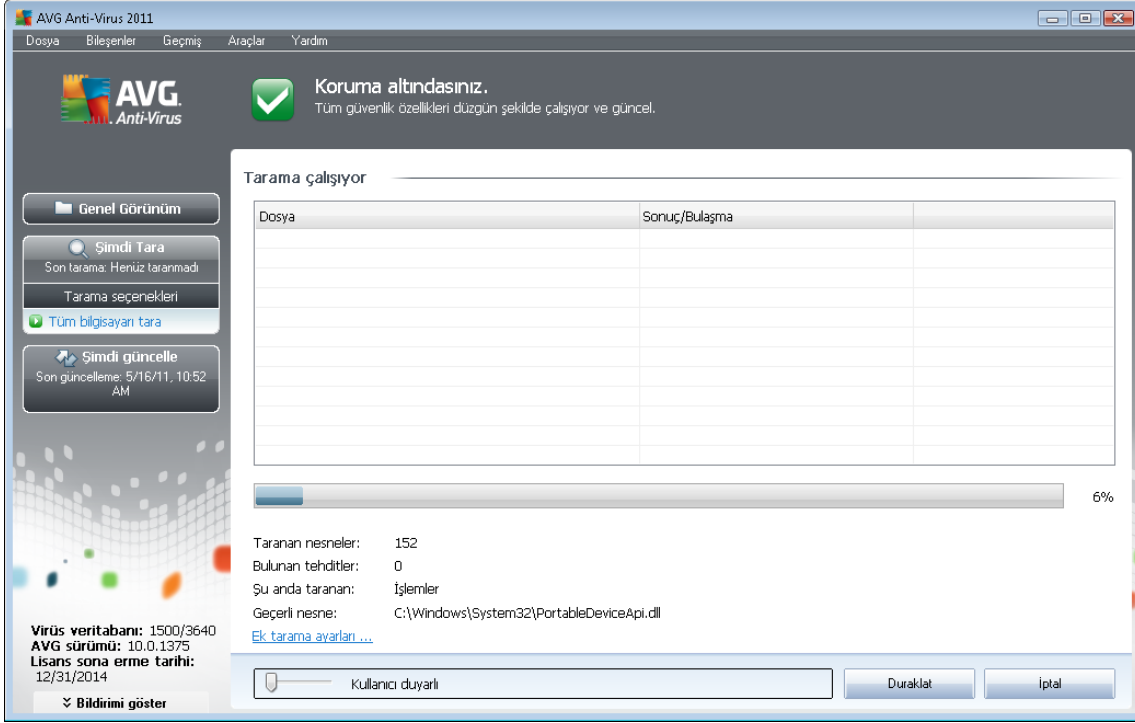
AVG Anti-Virus içinde, yazılım satıcısının önceden tanımladığı aşağıdaki tarama türlerini bulacaksınız:

10.2.1. 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.

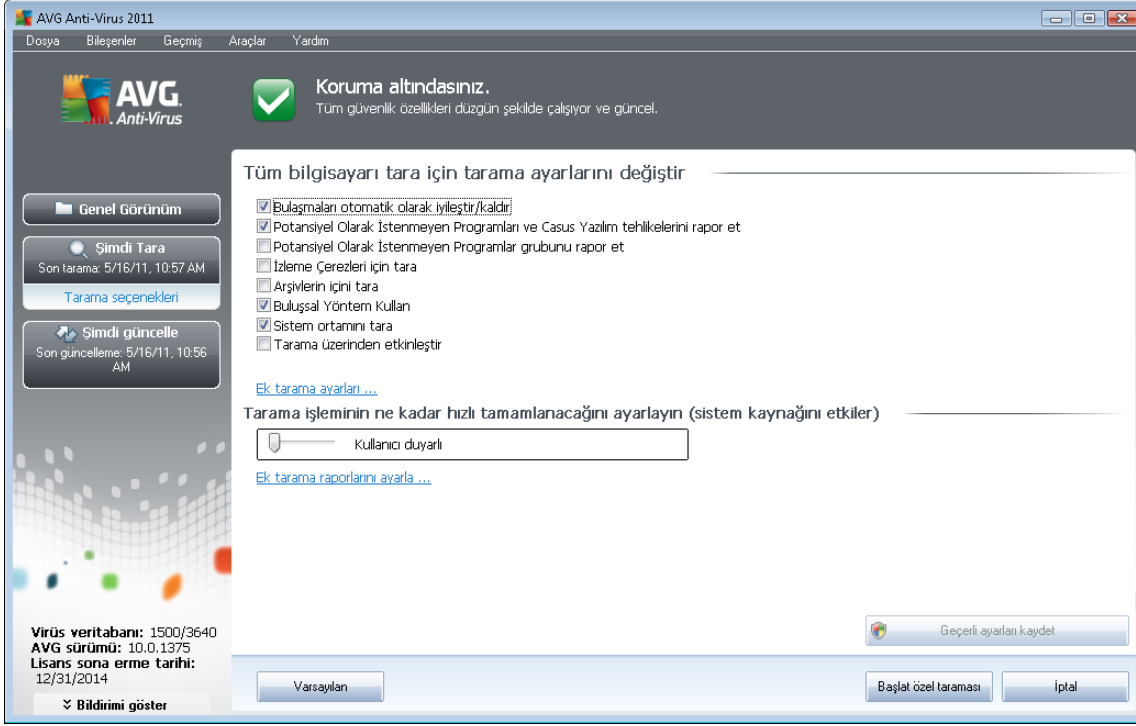
Tarama başlatma

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**).



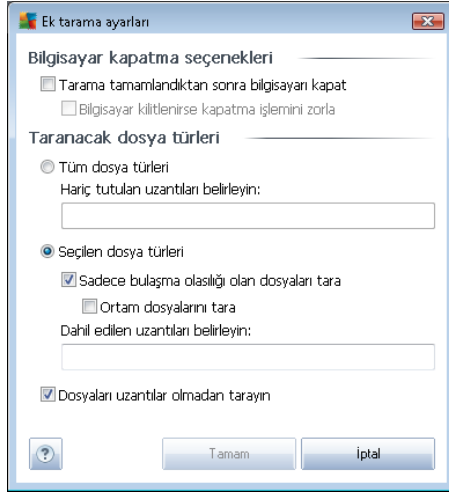
Tarama yapılandırması düzenleme

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 güvenlik riski oluşturmalarına 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 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.
 - **İzleme Tanımlama Bilgilerini Tarama** (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:

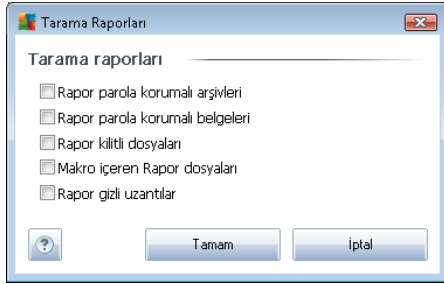


- **Bilgisayar kapatma seçenekleri** - Çalışan tarama işlemi bittiğinde bilgisayarın otomatik olarak kapatılması gerekip gerekmediğine karar verir. Bu seçeneği seçerseniz (**Tarama bittikten sonra bilgisayarı kapat**) bilgisayar mevcut durumda kilitli olsa bile bilgisayarın kapatılmasını sağlayan bir seçeneğin bulunduğu bir pencere açılacaktır (**Bilgisayar kilitliyse bilgisayarı kapanmaya zorla**).
- **Tarama için dosya türlerini tanımla** - Nelerin taranmasını istediğine 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 oluşturun** - 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 vererseniz yeni ayarlarınızı, belirli dosya ya da klasörlerin taranması için kullanılacak varsayılan yapılandırma olarak atayabilirsiniz.

10.2.2. 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

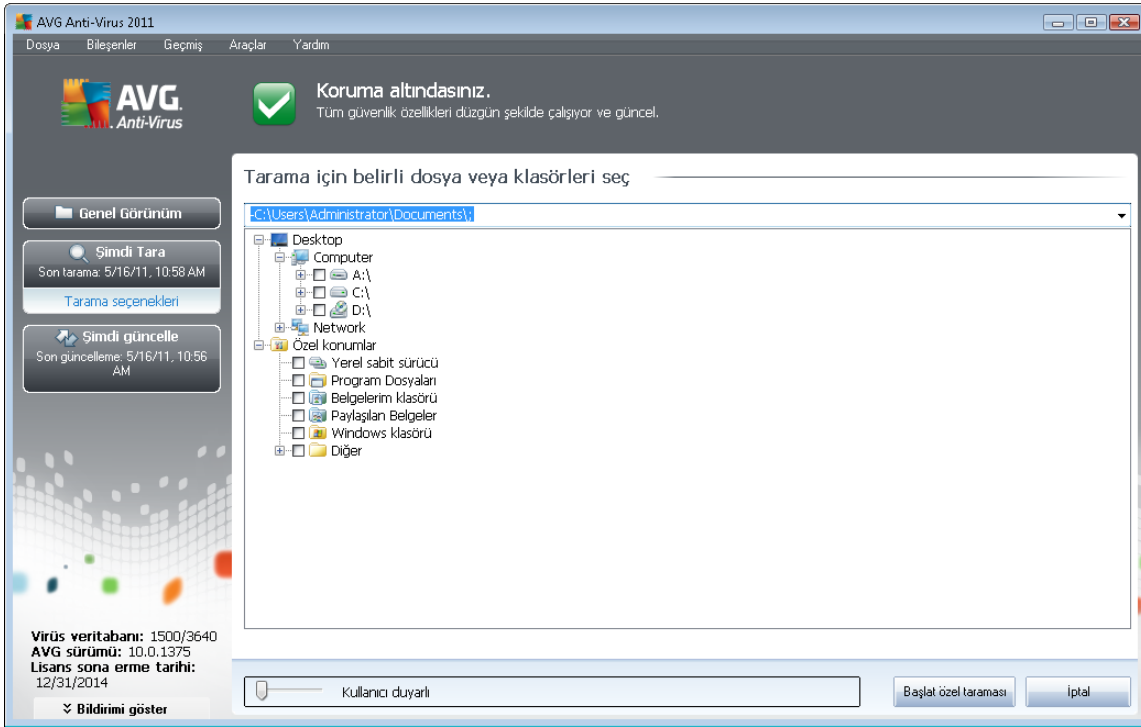
Belirli dosya ve klasörleri tara işlevi, tarama simgesi tıklanarak doğrudan [tarama arayüzünden](#) başlatılabilir. Yeni bir **Taramak için belirli dosya ve klasörleri seçin** iletişim kutusu açılır. Bilgisayarınızın ağaç görünümünden taranmasını istediğiniz klasörleri seçin. Seçilen klasörlerin her birine giden yol, otomatik olarak oluşturulacak ve iletişim kutusunun üst kısmındaki metin alanında



görüntülenecektir.

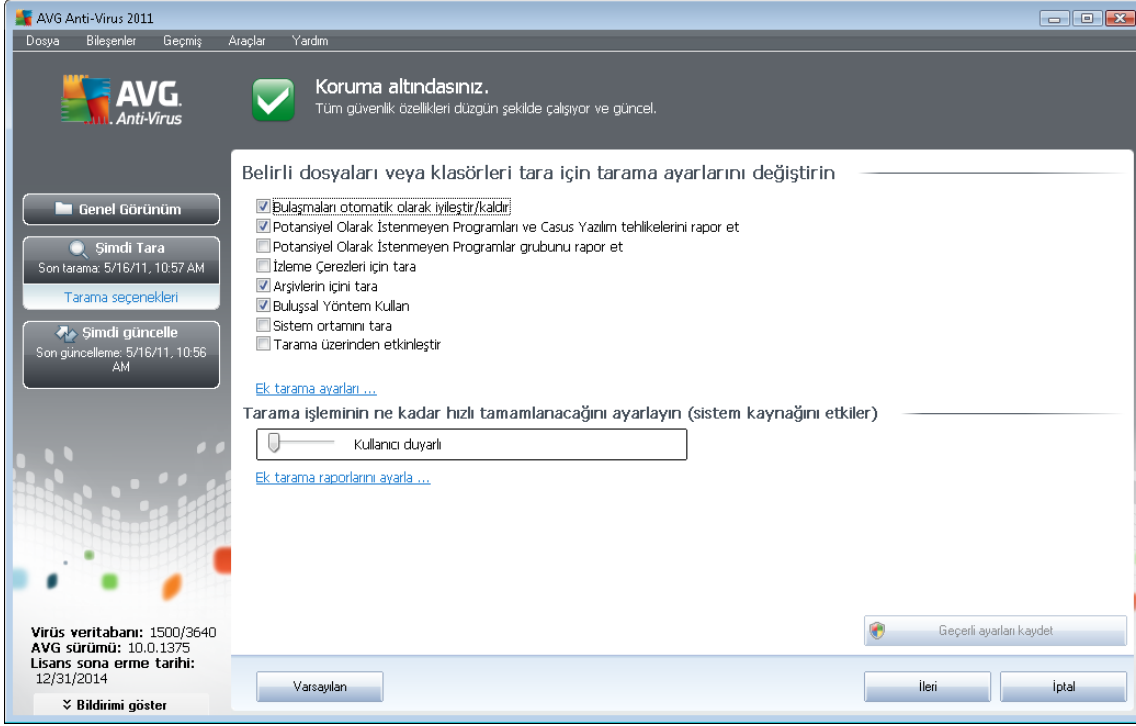
Belirli bir klasör taranırken içinde bulunan klasörlerin taranmaması gibi bir ihtimal de vardır. Bunu yapabilmek için otomatik olarak oluşturulan yolun başına "-" işareti koyun (*ekran görüntülerini inceleyin*). Klasörün tümünü tarama dışında tutmak için "!" parametresini kullanın.

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



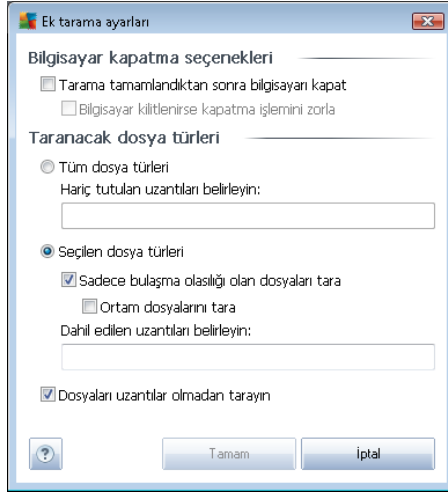
Tarama yapılandırması düzenleme

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 güvenlik riski oluşturmalarına 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 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.
 - **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:

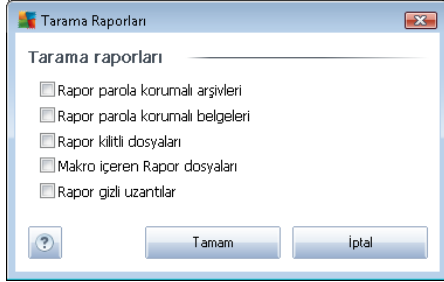


- **Bilgisayar kapatma seçenekleri** - Çalışan tarama işlemi bittiğinde bilgisayarın otomatik olarak kapatılması gerekip gerekmediğine karar verir. Bu seçeneği seçerseniz (**Tarama bittikten sonra bilgisayarı kapat**) bilgisayar mevcut durumda kilitli olsa bile bilgisayarın kapatılmasını sağlayan bir seçeneğin bulunduğu bir pencere açılacaktır (**Bilgisayar kilitliyse bilgisayarı kapanmaya zorla**).
- **Tarama için dosya türlerini tanımla** - 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 oluşturma** - 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 tarama 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 görecek tir (tüm özelleştirilmiş taramalar, Seçilen dosya ya da klasörleri tarama fonksiyonunun mevcut yapılandırmasına dayanmaktadır).**

10.2.3. Anti-Rootkit Tarama

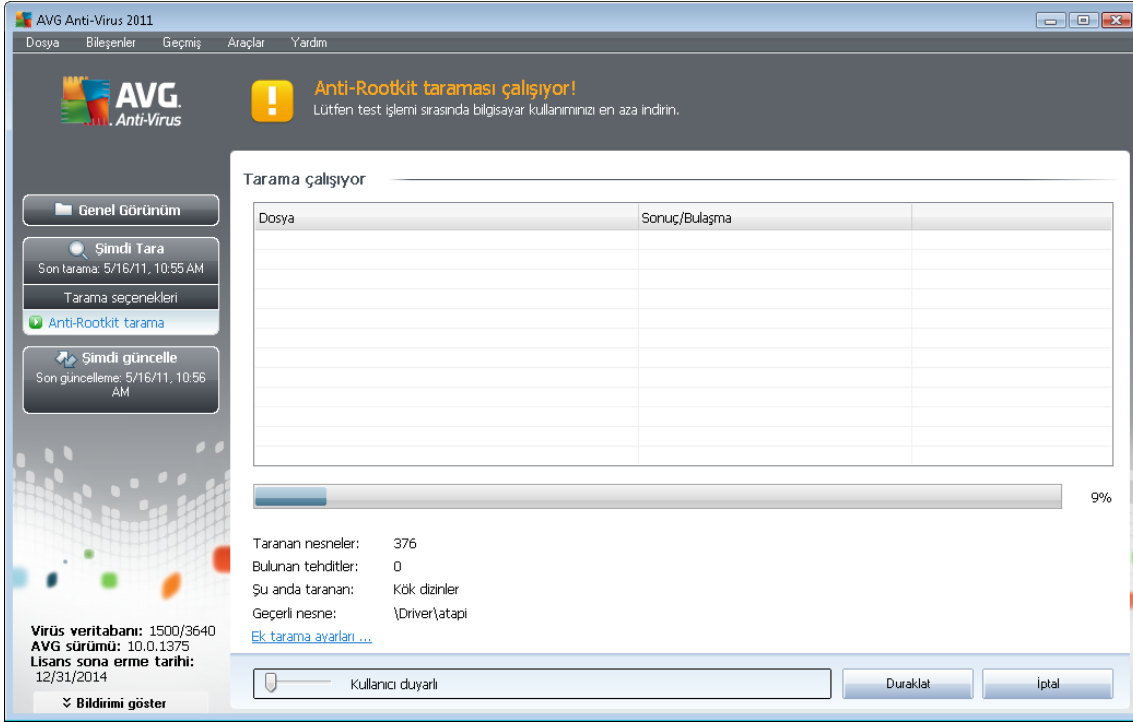
Anti-Rootkit tarama, bilgisayarınızı olası kök dizine karşı (bilgisayarınızdaki kötü amaçlı yazılım etkinliği içerebilecek programlar ve teknolojiler) açısından tarama. Bir rootkit algılanırsa, bu, bilgisayarınızda mutlaka virüs olduğu anlamına gelmez. Bazı durumlarda, belirli sürücüler veya normal uygulamaların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



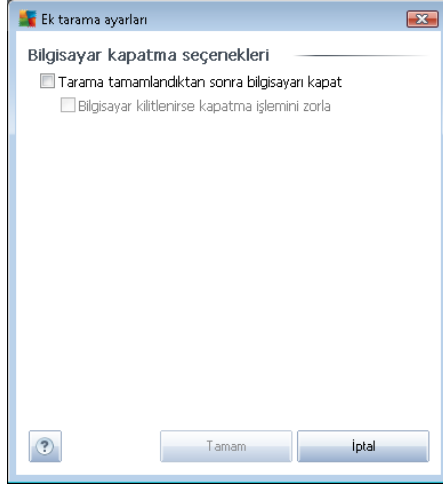
kutusunda **hemen başlayacaktır** (ekran görüntüsüne bakın). Tarama işlemi gerekirse geçici olarak kesintiye uğratılabilir (**Duraklat**) ya da iptal edilebilir (**Durdur**).



Tarama yapılandırması düzenleme

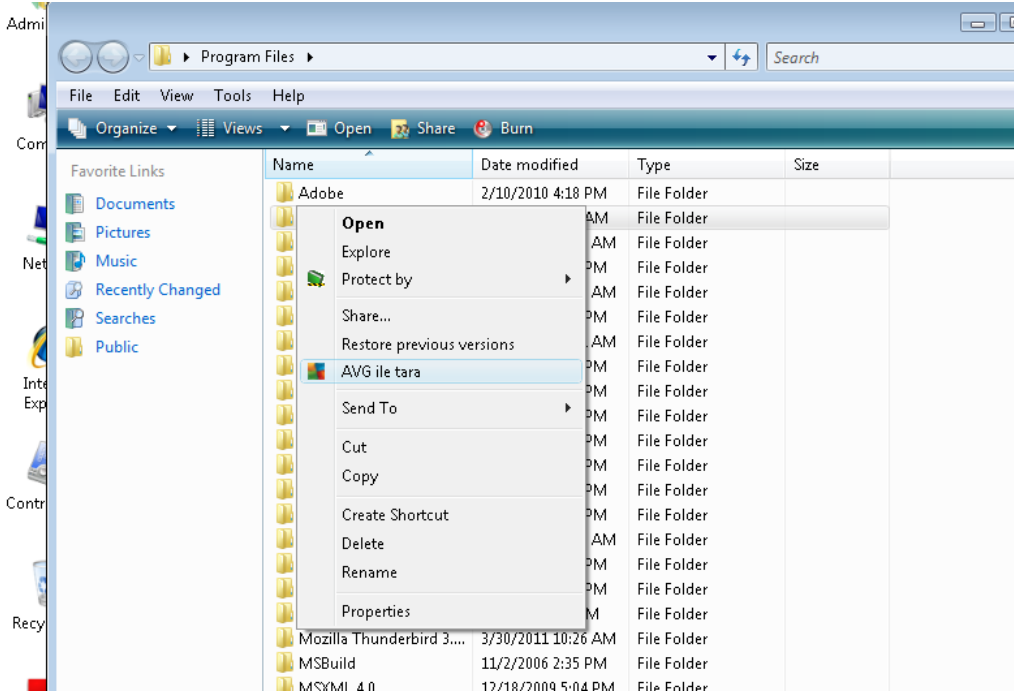
Anti-Rootkit tarama varsayılan ayarlarda her zaman başlatılır ve tarama parametrelerinin düzenlenmesine yalnızca [AVG Gelişmiş Ayarları/Anti-Rootkit](#) iletişim kutusundan erişilebilir. Tarama arayüzünde, şu yapılandırma kullanılabilir (ancak yalnızca tarama çalışırken):

- **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 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 kilitlenirse kapatmaya zorla**):



10.3. Windows Gezgini'nde Tarama

Bilgisayarın tümünde ya da seçilen bölümlerinde gerçekleştirilen öntanımlı taramaların yanı sıra **AVG Anti-Virus**, doğrudan Windows Gezgini ortamında bulunan belirli nesnelerin hızlı bir şekilde taranmasını 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 farenizle sağ tıklayın
- **AVG ile Tara** seçeneğini seçerek dosyanın AVG tarafından taranmasını sağlayın



10.4. Komut Satırı Tarama

AVG Anti-Virus 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.

10.4.1. 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 dizin 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** Arşivleri 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



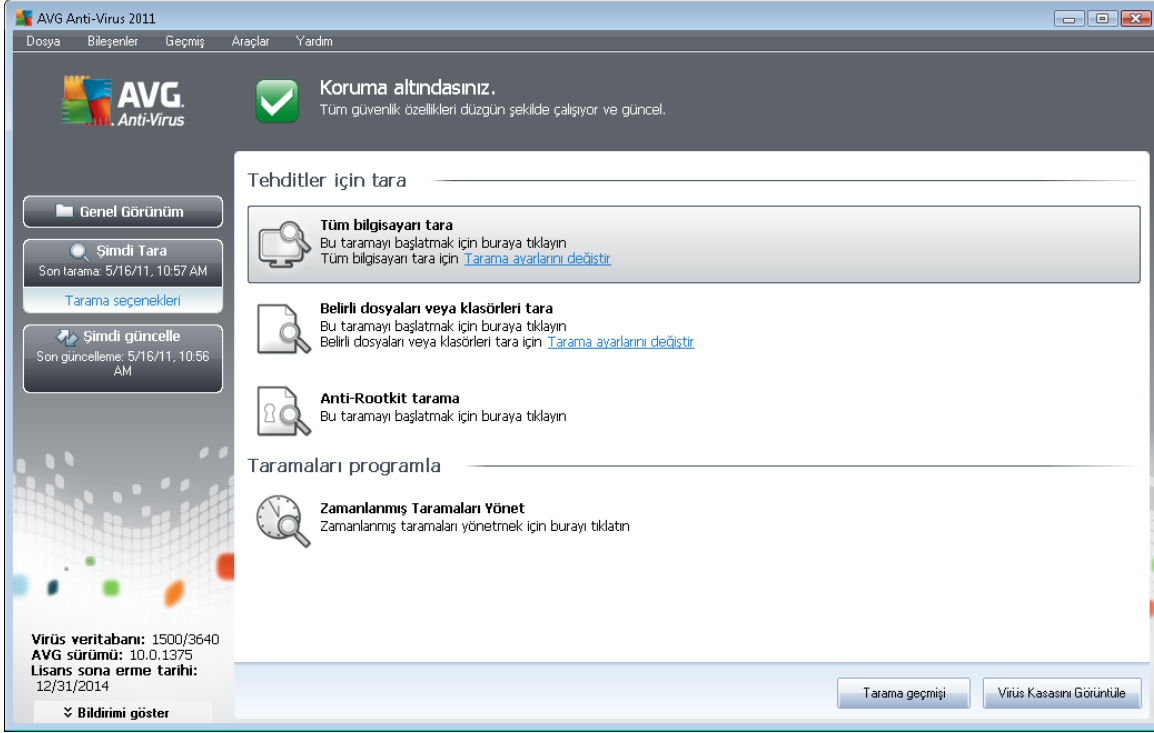
- **/HELP** Bu konuyla ilgili yardımı görüntüle
- **/PRIORITY** Tarama önceliğini belirle /Düşük, Oto, Yüksek/ (Bkz [Gelişmiş ayarlar / Taramalar](#))
- **/SHUTDOWN** Tarama tamamlandıktan sonra bilgisayarı kapat
- **/FORCESHUTDOWN** Tarama tamamlandıktan sonra bilgisayarı kapatmayı zorla
- **/ADS**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

10.5. Tarama Planlama

AVG Anti-Virus 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.

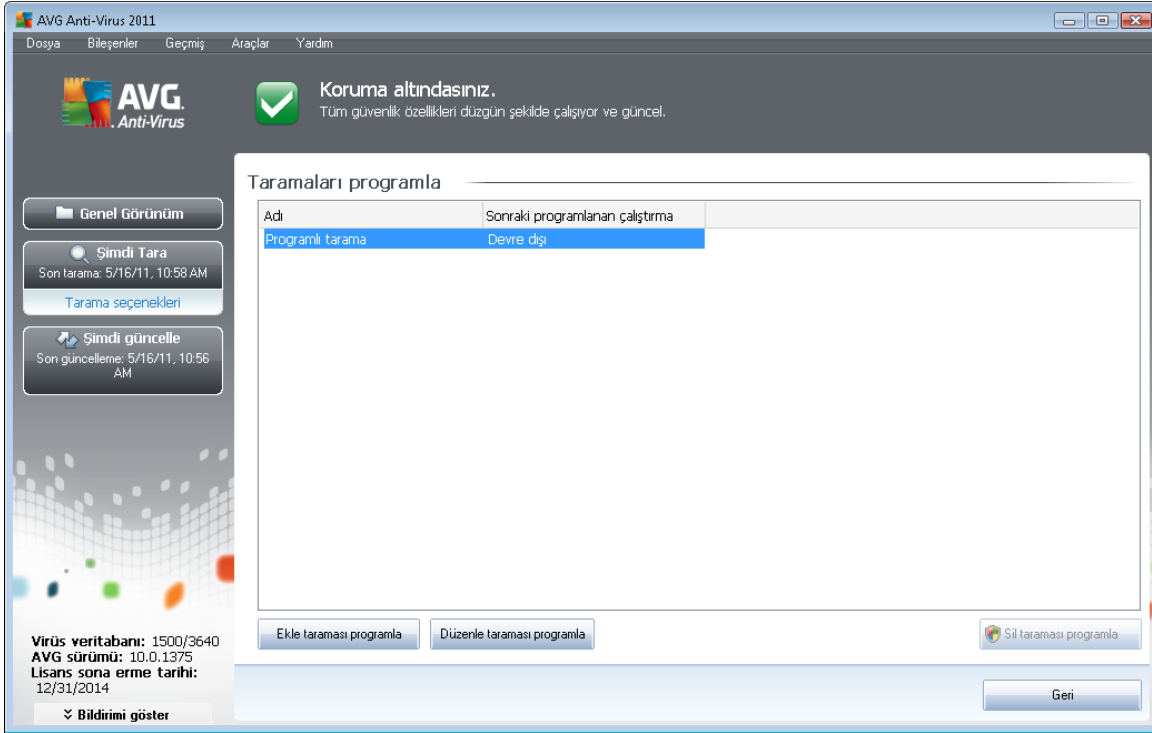
[Tüm bilgisayar taraması](#)'nı en az haftada bir kez düzenli olarak başlatmanız gerekir. Diğer bir yandan, mümkün olması halinde programlı taramanın varsayılan yapılandırılmasında ayarlandığı gibi tüm bilgisayar taramasını günlük olarak yapın. Bilgisayarınız "daima açık" ise taramaları çalışma saatlerinden 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:

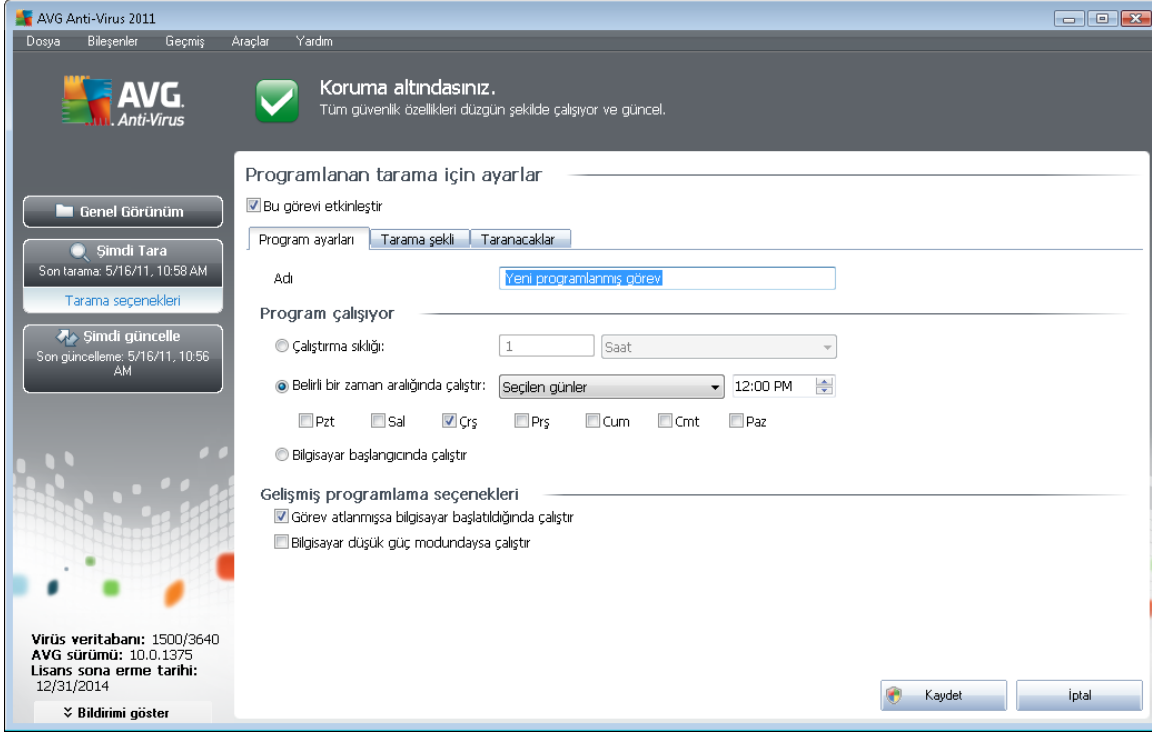


Şu kontrol düğmelerini kullanarak taramaları düzenleyebilir/ekleyebilirsiniz:

- **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](#)

10.5.1. 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 ayırmak 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.

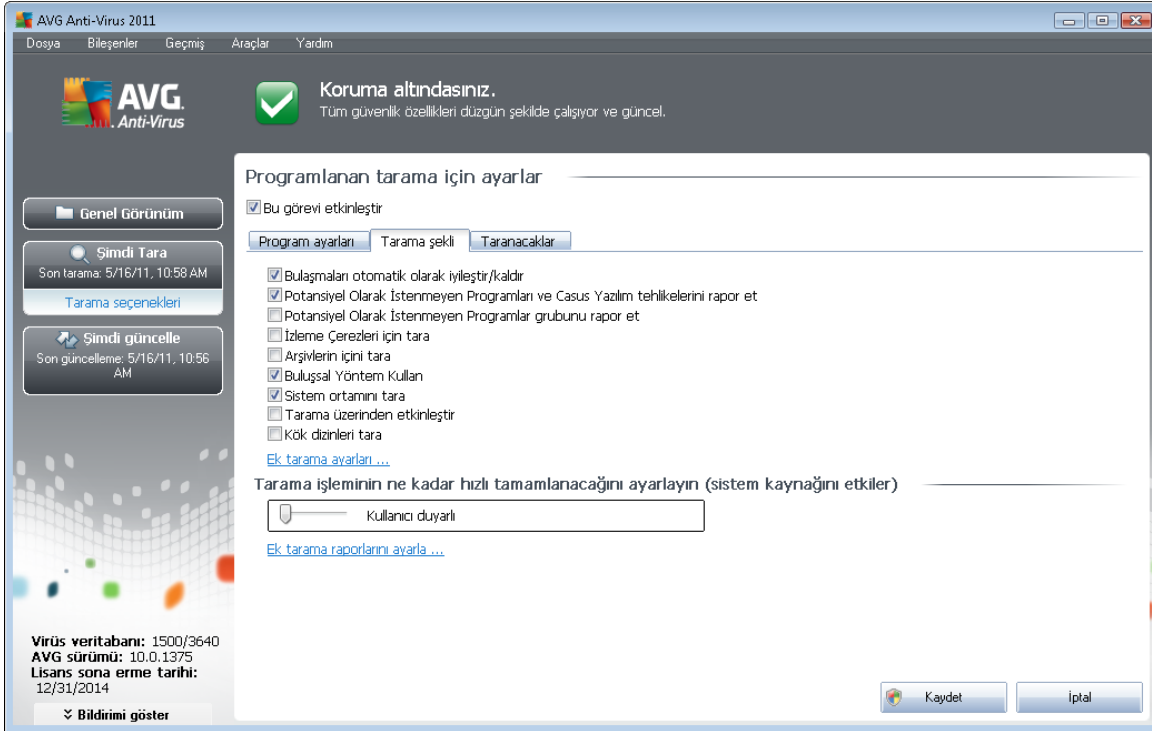
Programlı tarama iletişim kutusuna dair ayarların kontrol düğmeleri



Programlı tarama ayarları iletişim kutusunun üç sekmesinde (**Programlama ayarları**, **Tarama şekli** ve **Taranacaklar**) iki kontrol düğmesi bulunmaktadır 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](#).

10.5.2. 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:

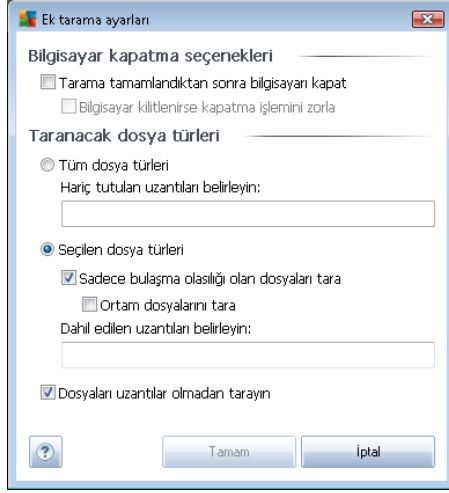
- **Bulaşmayı otomatik olarak temizle/kaldır** (varsayılanda açıktır): Tarama sırasında virüs tanımlanırsa, bir giderme yazılımı mevcutsa otomatik olarak temizlenir. Etkilenen dosyanın otomatik olarak silinmiyor olması halinde ya da bu seçeneği kapatmayı seçerseniz bir virüs tespit edildiğinde bilgilendirileceksiniz ve tespit edilen bulaşma hakkında ne yapılacağına karar vermek zorunda kalacaksınız. Önerilen işlem, bulaşmış dosyayı [Virüs Kasesine](#) 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 güvenlik riski oluşturmaya rağmen bu programlardan bazıları bilerek yüklenebilir. Bilgisayarınızın güvenliğini artırdığından, bu özelliği etkin durumda tutmanızı öneriyoruz.

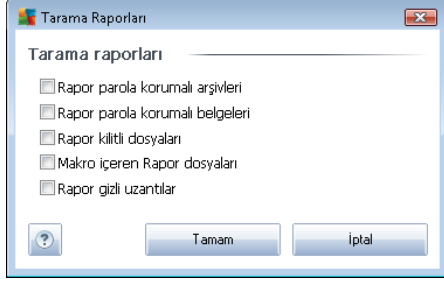
- **Potansiyel Olarak İstenmeyen Programlar gelişmiş grubunu rapor et** (varsayılanda *kapalıdır*) - bu parametre [casus yazılımların](#), yani doğrudan üreticiden alınan tamamen zararsız olan, ancak daha sonra kötüye kullanılacak programların genişletilmiş paketinin tespit edilmesi için işaretleyin. 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 aldığını unutmayın.

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 türlerini tanımla** - Nelerin taranmasını istediğine 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 değiştirmeniz 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 oluşturun** - bağlantı üzerinden **Tarama Raporları** isimli bir iletişim kutusu açılır ve buradan ne tip buluntuların rapor edileceğini seçebilirsiniz:



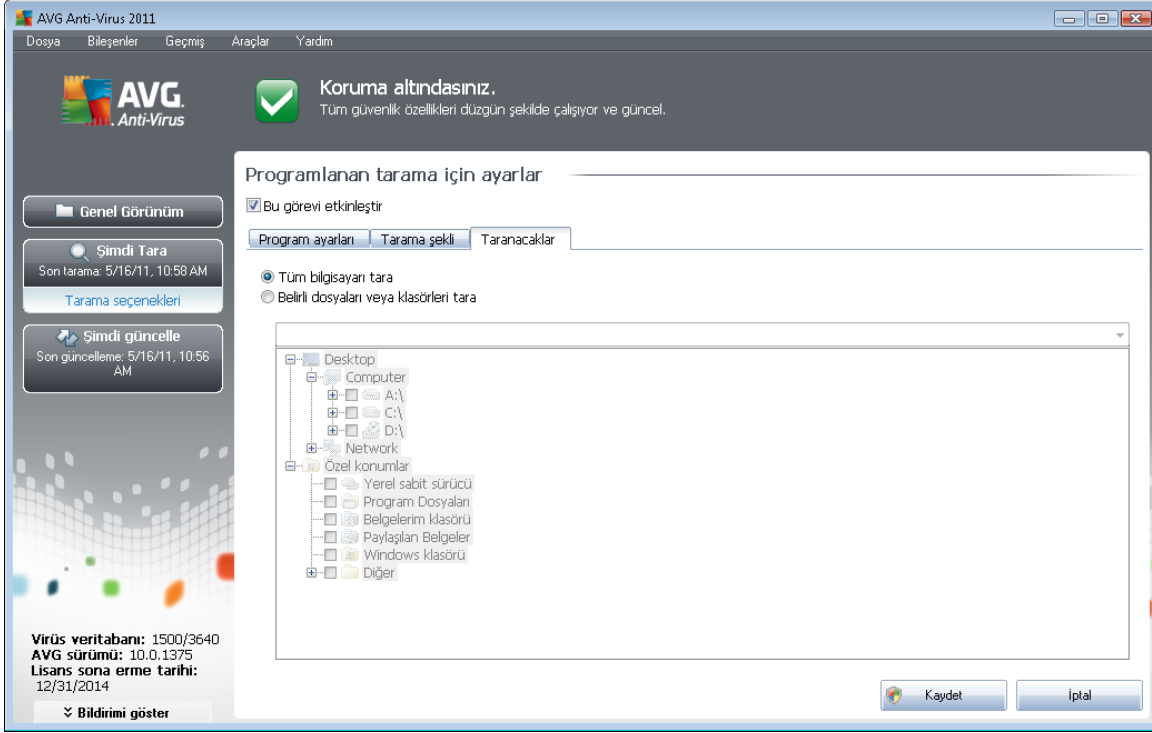
Not: Tarama yapılandırması varsayılan olarak optimum performansta gerçekleşecek şekilde ayarlanmıştır. Tarama ayarlarını değiştirmek için geçerli bir nedeniniz yoksa mevcut yapılandırmayı muhafaza etmeniz önerilmektedir. Yapılandırma, sadece deneyimli kullanıcılar tarafından değiştirilmelidir. Tarama yapılandırma hakkında daha fazla seçenek görmek için **Dosya / Gelişmiş ayarlar** sistem menüsünden ulaşabileceğiniz [Gelişmiş ayarlar](#) iletişim kutusunu açın.

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](#).

10.5.3. 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 sürüler
- **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**

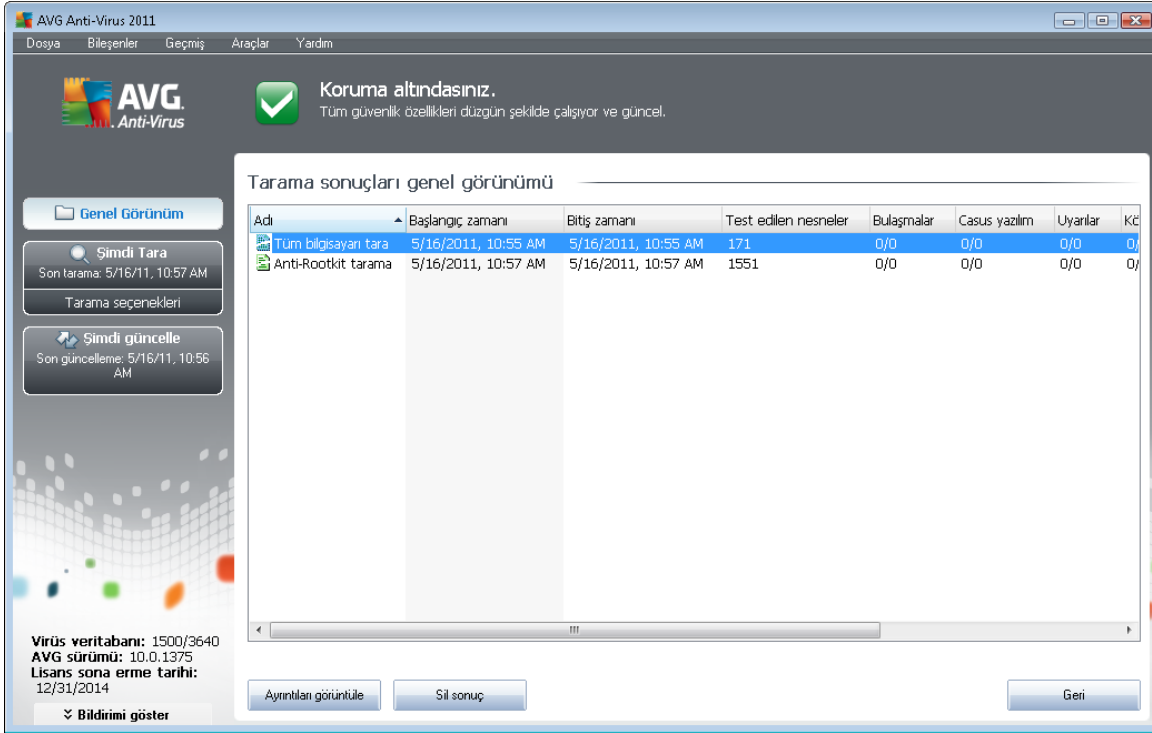
- Sistem sürücüsü - işletim sisteminin yüklü olduğu sabit sürücü (genellikle C:)
- Sistem klasörü - C:\Windows\System32\
- Geçici Dosyalar klasörü - C:\Documents and Settings\User\Local\ (Windows XP) veya C:\Users\user\AppData\Local\Temp\ (Windows Vista/7)
- Geçici İnternet Dosyaları - C:\Documents and Settings\User\Local Settings\Geçici İnternet Dosyaları\ (Windows XP) veya C:\Users\user\AppData\Local\Microsoft\Windows\Geçici İnternet Dosyaları (Windows Vista/7)

Programlı tarama iletişim kutusuna dair ayarların kontrol düğmeleri

Programlı tarama ayarları iletişim kutusunun üç sekmesinde (**Programlama ayarları**, **Tarama şekli** ve **Taranacaklar**) iki kontrol düğmesi bulunmaktadır 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](#).

10.6. Tarama Sonuçları Genel Görünümü



Tarama sonuçlarına genel bakış penceresine, [AVG tarama arayüzünde Tarama geçmiş](#) 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 nesneler** - tarama sırasında kontrol edilen nesne sayısıdır
- **Bulaşmalar** - tespit edilen / silinen [virüs bulaşması](#) sayısı
- **Casus yazılım** - tespit edilen / silinen [casus yazılım](#) sayısı
- **Uyarılar** - algılanan [şüpheli nesnelerin](#)
- **Kök dizinler** - algılanan [kök dizinlerin](#)
- **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](#)

10.7. 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.

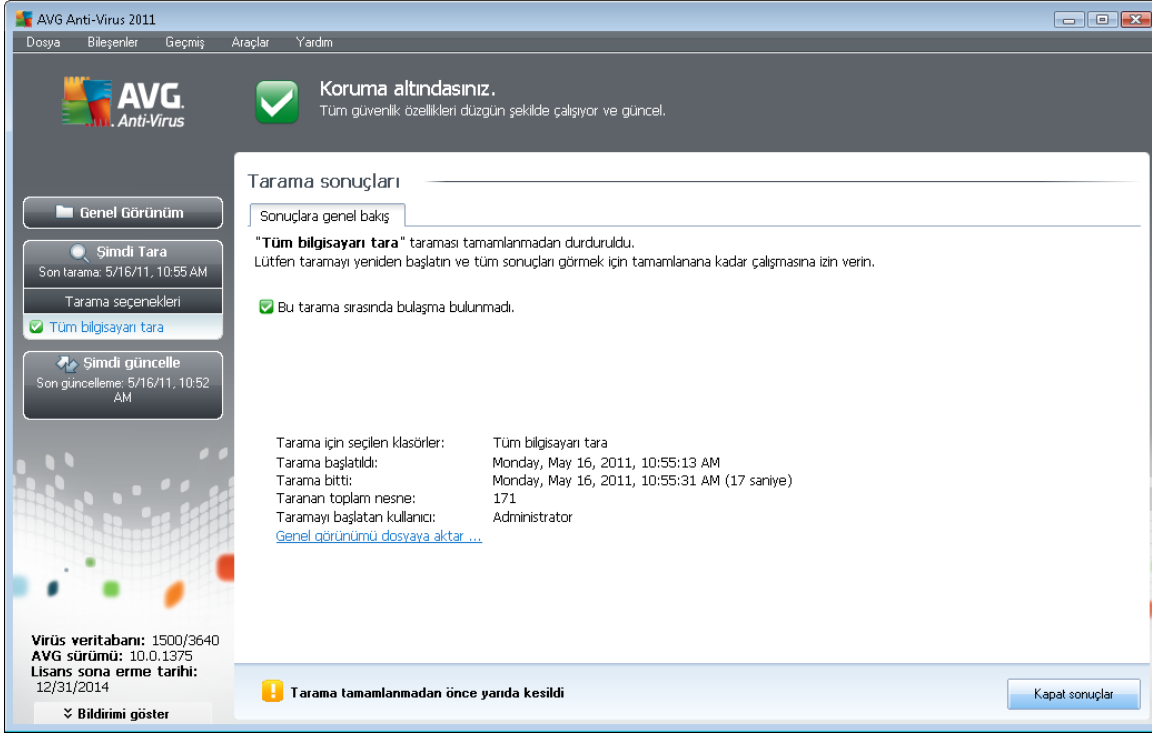
İletişim penceresi çok sayıda sekme ayrılır:

- **Sonuçlara Genel Bakış** - bu sekme daima görüntülenir ve tarama işlemi tanımayan istatistiki veriler 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 nesneler hakkında bilgi de bulacaksınız (örn. parola korumalı



arşivler).

10.7.1. Sonuçlara Genel Bakış Sekmesi



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

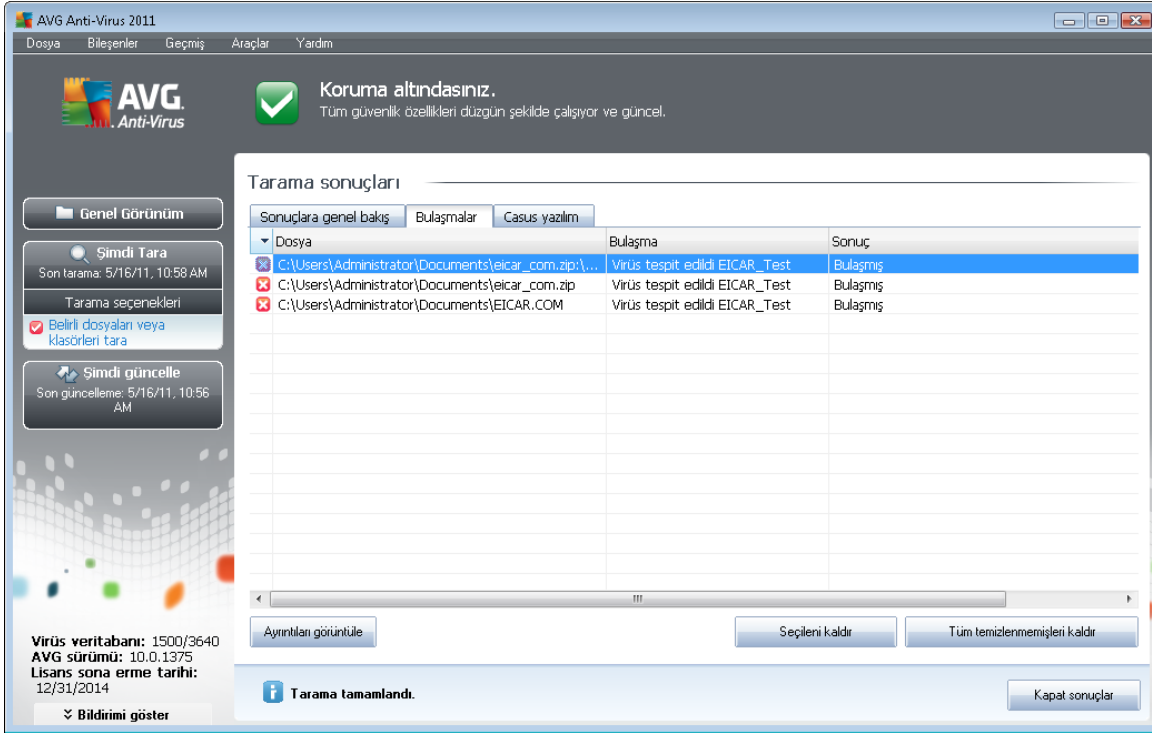
- tespit edilen [virüs bulaşmaları](#) / [casus yazılım](#)
- silinen [virüs bulaşmaları](#) / [casus yazılım](#)
- kaldırılmayan ya da temizlenemeyen [virüs bulaşması](#) / [casus yazılım](#) sayısı

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.

10.7.2. Bulaşma Sekmesi



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

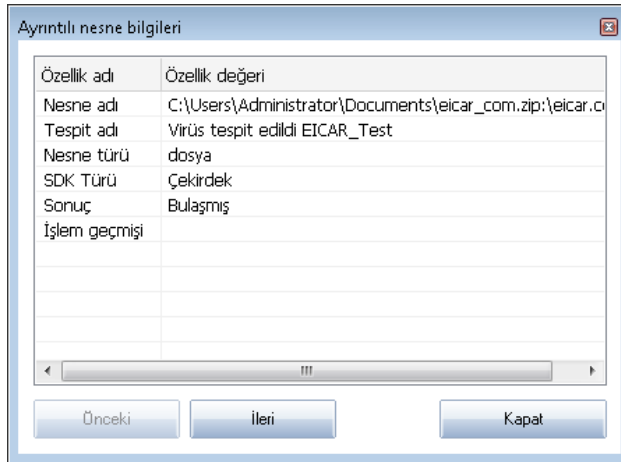
- **Dosya** - bulaşmış nesnenin orijinal konumunun tam dizin yolu
- **Bulaşmalar** - tespit edilen [virüs](#)ün adı (belirli virüs türleri hakkında ayrıntılı bilgi almak için lütfen çevrimiçi [Virüs Ansiklopedisine](#) danışın)
- **Sonuç** - tarama sırasında tespit edilen bulaşmış nesnenin mevcut durumunu 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 istisnaları](#) iletişim kutusundan 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:

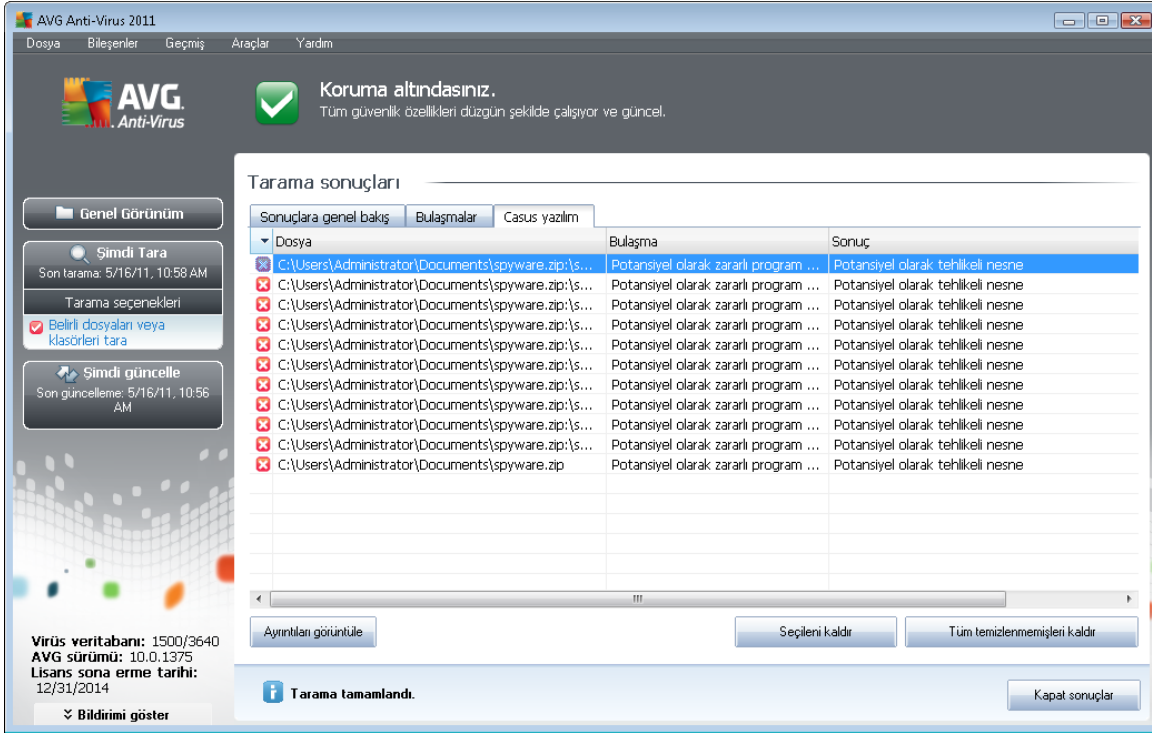
- **Ayrıntıları görüntüle** - düğme Ayrıntılı nesne bilgileri adlı yeni bir iletişim kutusu penceresi açar:



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.

- **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

10.7.3. Casus Yazılım Sekmesi



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

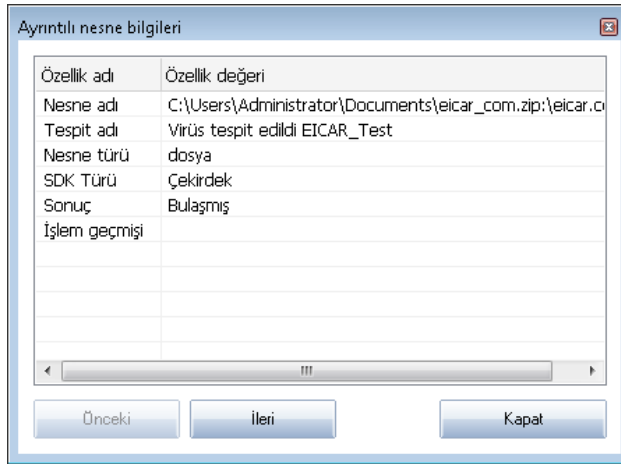
- **Dosya** - bulaşmış nesnenin orijinal konumunun tam dizin yolu
- **Bulaşmalar** - tespit edilen [casus yazılımın adıdır](#) (belirli virüs türleri hakkında ayrıntılı bilgi almak için lütfen çevrimiçi [Virüs Ansiklopedisi](#)'ne başvurun)
- **Sonuç** - tarama sırasında tespit edilen nesnenin mevcut 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 istisnaları](#) iletişim kutusundan 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.

- **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

10.7.4. Uyarılar Sekmesi

Uyarılar sekmesinde, tarama sırasında tespit edilip "şüpheli duyulan" nesneler (*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. AVG testi tarafından sadece Uyarılar tespit edildiyse herhangi bir işlem yapmanıza gerek kalmaz.

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'niz, zararlı olabileceğinden şüphelendiğiniz gizli bir dosya rapor ederse, [AVG Virüs Kasası](#)'na 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.

10.7.5. 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. Rootkit, 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.

10.7.6. 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 taraması, bulaşmayan fakat şüpheli olan dosyaları tespit edebilir. Bu dosyalar [Uyarı](#) veya **Bilgi** olarak rapor edilir.

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

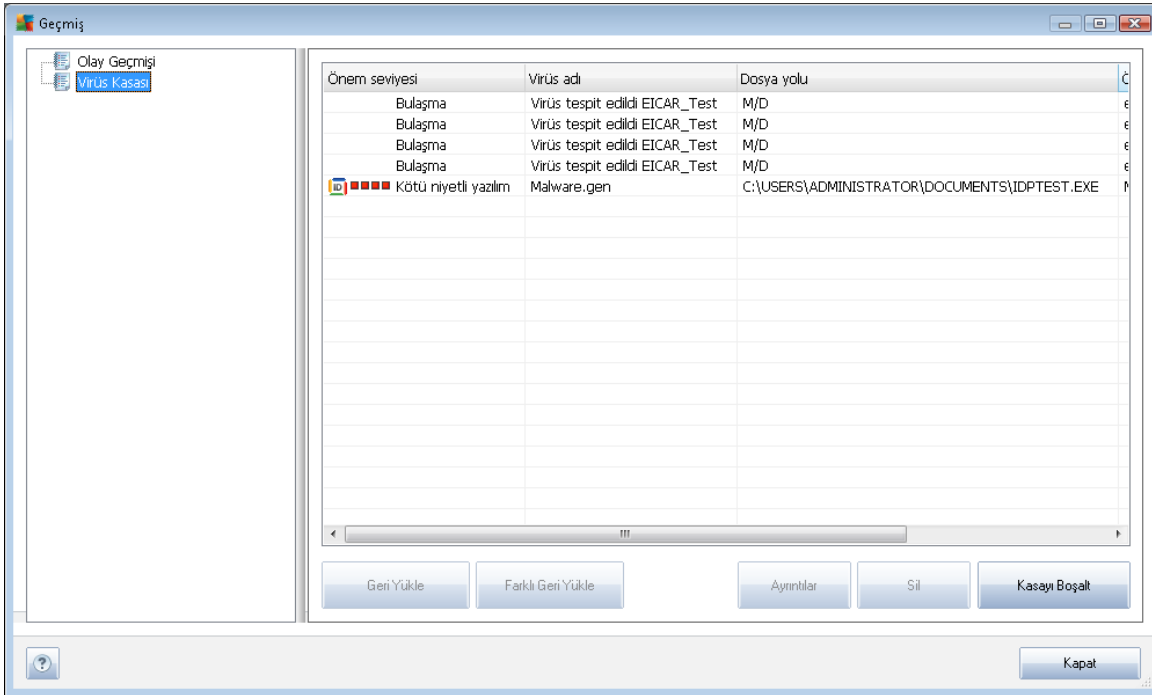
- **Çalışma zamanı pakettli** - Dosya, dosyanın taranmasını önleme çabası olarak



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 (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 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) AVG bu durumu rapor eder. Bazı durumlarda virüsler, sistemde fark edilmemek için standart sistem işlemlerinin adını alır.
- **Kilitli dosya** - Rapor edilen dosya kilitli, bu yüzden AVG tarafından taranamıyor. Bu, genellikle bir dosyanın sistem tarafından kullanılmakta olduğu anlamına gelir (örn. *takas dosyası*).

10.8. 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 Kasası'na** 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 oluştuyorsa, bu dosyayı analize gönderebilir veya orijinal konumuna geri yükleyebilirsiniz.

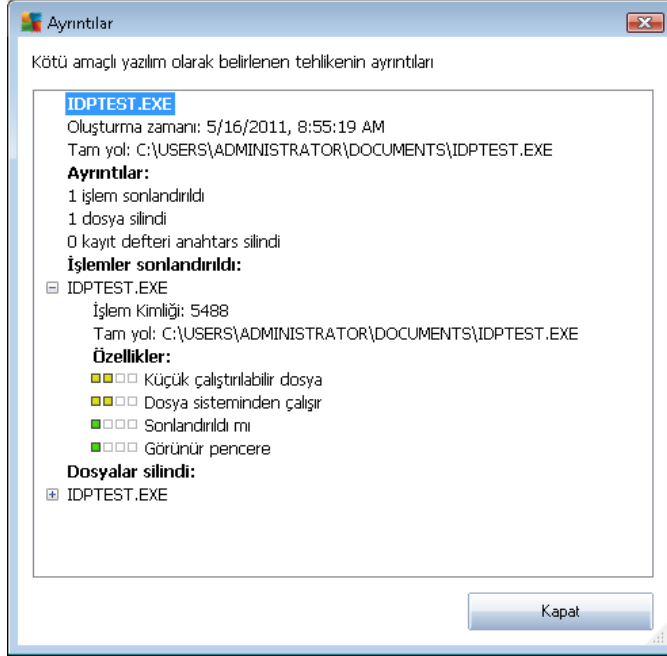
Virüs Kasası arayüzü, yeni bir pencerede açılır ve karantina altındaki bulaşmış nesneler hakkında genel bilgi içerir:

- **Önem Düzeyi** - **AVG Anti-Virus** uygulamanızın içine [Kimlik Koruma](#) bileşenini yüklemeye karar verdiğinizde, ilgili tehdidin önem seviyesinin grafik bir tanımı dört seviyeli bir ölçekte kusursuz bir şekilde (■□□□) çok tehlikeli seviyesine kadar (■ ■ ■ ■) ve bulaşma türü hakkında bilgi (*bulaşma seviyesine göre bu kısımda sağlanır - 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 nesneler, tarama işlemi sırasında AVG tarafından verilen standart isim ile etiketlenmiştir. Nesnenin bilinmeyen farklı bir adı olması halinde (Öm. *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 dönüştürülemeyecek 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*).



11. AVG Güncellemeleri

Yeni bulunan tüm virüslerin mümkün olduğunca çabuk algılanabilmesi için AVG'nizi güncel tutmak çok önemlidir.

AVG güncellemeleri herhangi bir sabit plana göre yayınlanmadığı ancak yeni tehditlerin miktarına veya önem düzeyine göre yayınlandığı için, yeni güncellemeleri en az günde bir kez, hatta daha sık denetlemeniz önerilir. Yalnızca bu şekilde **AVG Anti-Virus** ürününüzün gün boyunca da güncel olduğundan emin olabilirsiniz.

11.1. Güncelleme Seviyeleri

AVG, arasından seçim yapabileceğiniz iki güncelleme seviyesi sunmaktadır:

- **Tanım güncellemeleri** güvenilir virüsten koruma için gerekli değişiklikleri içerir. Genellikle kodu değiştirmez ve yalnızca tanımlama veritabanını günceller. Bu güncelleme sunulur sunulmaz yüklenmelidir.
- **Program güncellemeleri** çeşitli program değişikliklerini, onarımlarını ve gelişimlerini içerir.

[Bir güncelleme programlanırken](#) indirme ve uygulanma açısından öncelik sırasını seçmek mümkündür.

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

11.2. Güncelleme Türleri

İki güncelleme türü arasında seçim yapabilirsiniz:

- **İsteğe Bağlı Güncelleme** ihtiyacınız olduğu durumlarda hemen gerçekleştirilebilecek AVG güncellemesidir.
- **Programlanan güncelleme** - AVG menüsünden [bir güncelleme planı programlayabilirsiniz](#). Programlı güncelleme, yapılandırma ayarlarınıza bağlı olarak periyodik olarak gerçekleştirilir. Belirli bir konumda yeni güncelleme dosyaları bulunur bulunmaz doğrudan İnternet'ten ya da ağ dizininden indirilirler. Yeni güncelleme dosyası yoksa herhangi bir işlem yapılmaz.

11.3. Güncelleme İşlemi

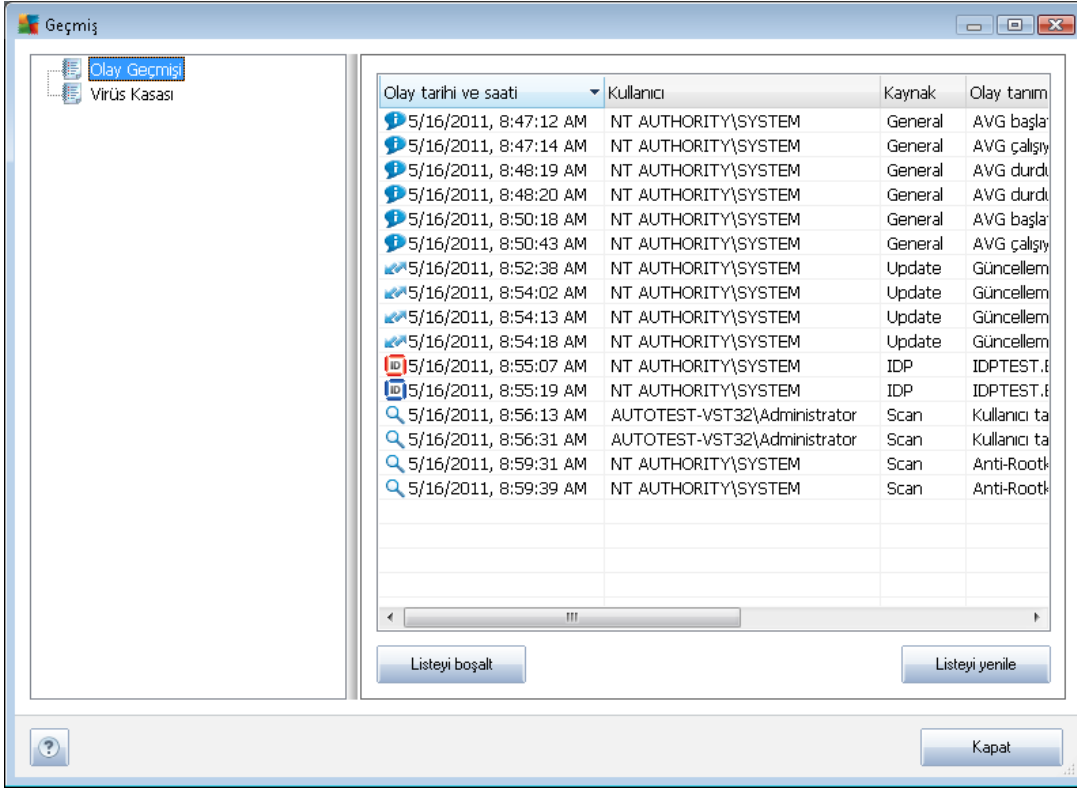
Güncelleme işlemi **Şimdi Güncelle** [hızlı bağlantısına](#) tıklanarak istenilen anda başlatılabilir. Bu bağlantıya bütün [AVG Kullanıcı Arayüzü](#) pencerelerinden ulaşabilirsiniz. Diğer bir yandan [Güncelleme yöneticisi](#) bileşeninden düzenlenebilen güncelleme programlarında planlanan güncellemelerin düzenli olarak yapılması önerilmektedir.

Güncellemeye başladıktan sonra AVG, yeni güncelleme dosyasının olup olmadığını aramaya başlayacaktır. Varsa AVG indirme işlemine başlat ve güncelleme işlemini otomatik olarak başlatır. Güncelleme işlemi sırasında güncelleme işleminin ilerleyişinin yanı sıra ilgili istatistiki parametreleri de görüntüleyebileceğiniz **Güncelleme** arayüzüne yeniden yönlendirileceksiniz (*güncelleme dosyasının boyutu, alınan veriler, indirme hızı, kalan süre...*).



Not: 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. Bu seçeneğe Başlat/Tüm Programlar bilgisayarınızın günde an az bir kere açıldığından emin olduğunuz durumlarda önerilir/Donatılar /Sistem Araçları /Sistem Geri Yükleme menüsünden erişebilirsiniz fakat değişikliklerin sadece uzman kullanıcılar tarafından yapılması önerilmektedir.

12. Olay Geçmişi



Geçmiş iletişim kutusuna [sistem menüsü](#) üzerinden **Geçmiş/Olay Geçmişi Günlüğü** ögesi aracılığıyla ulaşabilirsiniz. Bu iletişim kutusunda, **AVG Anti-Virus** 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 *otomatik olarak gerçekleştirilen taramalar dahil olmak üzere*)
- Olay konumu da dahil olmak üzere virüs tespitine bağlı olaylar ([Yerleşik Kalkan](#) veya [tarama](#) ile)
- Diğer önemli olaylar

Her olay için, şu bilgiler listelenir:

- **Olay tarihi ve saati**, olayın meydana geldiği kesin tarih ve saati gösterir.
- **Kullanıcı**, olayı kimin başlattığını belirtir
- **Kaynak**, kaynak bileşenin veya AVG sisteminin olayı tetikleyen bölümünü belirtir



- ***Olay açıklaması***, tam olarak ne olduğu hakkında kısa bir açıklama sağlar

Kontrol düğmeleri

- ***Listeyi temizle*** - etkinlik listesindeki tüm girişleri siler
- ***Listeyi yenile*** - etkinlik listesindeki tüm girişleri günceller



13. SSS ve Teknik Destek

İşletmenizde ya da teknik açıdan AVG ile herhangi bir sorun yaşıyorsanız lütfen, AVG web sitesinin (<http://www.avg.com/>) [SSS](#) bölümüne bakın.

Bu şekilde yardım alamazsanız teknik destek bölümüne e-posta ile başvurun. Lütfen **Yardım/Çevrimiçi yardım al** sistem menüsünden ulaşabileceğiniz iletişim formunu kullanın.