



# AVG Internet Security 2013

## Kullanıcı Kılavuzu

### **Belge revizyonu 2013.11 (13.2.2013.)**

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

<b>1. Giriş</b>	<b>5</b>
<b>2. AVG Yükleme Gereksinimleri</b>	<b>6</b>
2.1 Desteklenen İşletim Sistemleri	6
2.2 Minimum ve Önerilen Donanım Gereksinimleri	6
<b>3. AVG Yükleme Süreci</b>	<b>7</b>
3.1 Hoşgeldiniz: Dil Seçimi	7
3.2 Hoşgeldiniz: Lisans Sözleşmesi	8
3.3 Lisansınızı etkinleştirme	9
3.4 Yükleme türünü seçin	10
3.5 Özel seçenekler	11
3.6 AVG Security Toolbar'ı Yükle	12
3.7 Yükleme ilerlemesi	13
3.8 Yükleme başarılı oldu	14
<b>4. Yüklemeden Sonra</b>	<b>15</b>
4.1 Ürün kaydı	15
4.2 Kullanıcı arayüzüne erişim	15
4.3 Tüm bilgisayarın taranması	15
4.4 Eicar testi	15
4.5 AVG varsayılan yapılandırması	16
<b>5. AVG Kullanıcı Arayüzü</b>	<b>17</b>
5.1 Üst Satır Gezinme	18
5.2 Güvenlik Durumu Bilgisi	22
5.3 Bileşen Genel Görünümü	23
5.4 Uygulamalarım	24
5.5 Tara / Hızlı Bağlantıları Güncelle	25
5.6 Sistem Tepsisi Simgesi	25
5.7 AVG Aracı	27
5.8 AVG Tavsiyesi	28
5.9 AVG Hızlandırıcı	29
<b>6. AVG Bileşenleri</b>	<b>30</b>
6.1 Bilgisayar	30
6.2 Web Tarama	31
6.3 Kimlik	33



6.4 E-postalar	35
6.5 Güvenlik Duvarı	37
6.6 Quick Tune	40
<b>7. AVG Security Toolbar</b>	<b>42</b>
<b>8. AVG Do Not Track</b>	<b>44</b>
8.1 AVG Do Not Track arayüzü	44
8.2 İzleme süreçleri hakkında bilgiler	46
8.3 İzleyici süreçlerini engelleme	46
8.4 AVG Do Not Track ayarları	47
<b>9. AVG Gelişmiş Ayarlar</b>	<b>48</b>
9.1 Görünüm	48
9.2 Sesler	51
9.3 AVG korumasını geçici olarak devre dışı bırak	52
9.4 Bilgisayar Koruması	53
9.5 E-Posta Tarayıcısı	58
9.6 Web Tarama Koruması	73
9.7 Identity Protection	76
9.8 Taramalar	77
9.9 Programlar	82
9.10 Güncelleme	91
9.11 İstisnalar	95
9.12 Virüs Kasası	97
9.13 AVG Kendi Kendini Koruma	98
9.14 Gizlilik Tercihleri	98
9.15 Hata durumunu yoksay	101
9.16 Advisor – Bilinen Ağlar	102
<b>10. Güvenlik Duvarı Ayarları</b>	<b>103</b>
10.1 Genel	103
10.2 Uygulamalar	105
10.3 Dosya ve yazıcı paylaşımı	106
10.4 Gelişmiş ayarlar	107
10.5 Tanımlanan ağlar	108
10.6 Sistem hizmetleri	109
10.7 Günlükler	110
<b>11. AVG Tarama</b>	<b>113</b>



11.1 Öntanımlı Taramalar.....	114
11.2 Windows Gezgini'nde Tarama.....	122
11.3 Komut Satırı Tarama.....	123
11.4 Tarama Programlama .....	125
11.5 Tarama Sonuçları.....	133
11.6 Tarama sonuçları ayrıntıları.....	134
<b>12. Virüs Kasası.....</b>	<b>135</b>
<b>13. Geçmiş.....</b>	<b>137</b>
13.1 Tarama sonuçları.....	137
13.2 Yerleşik Kalkan tespiti.....	138
13.3 E-posta Koruması tespiti.....	141
13.4 Online Shield tespitleri.....	142
13.5 Olay geçmişi günlüğü.....	144
13.6 Firewall günlüğü.....	145
<b>14. AVG Güncellemeleri.....</b>	<b>147</b>
14.1 Güncelleme başlatma.....	147
14.2 Güncelleme seviyeleri.....	147
<b>15. SSS ve Teknik Destek.....</b>	<b>149</b>



## 1. Giriş

Bu kullanıcı el kitabı, **AVG Internet Security 2013** için kapsamlı kullanıcı dokümantasyon sağlar.

**AVG Internet Security 2013** çevrimiçi yaptığınız her şey için koruma katmanları sağlar. Bu, kimlik hırsızlıklarından, virüslerden ya da zararlı siteleri ziyaret etmekten endişe duymanıza gerek olmadığı anlamına gelir. AVG Koruyucu Bulut Teknolojisi ve AVG Topluluk Koruma Ağı da dahil edilmiştir; bu, en son tehdit bilgilerini topladığımız ve en iyi korumayı aldığınızdan emin olmak için topluluğumuzla paylaştığımız anlamına gelmektedir. Gerçek zamanlı korumayla alışveriş ve bankacılık işlemlerini güvenle yapabilir, sosyal paylaşım ağlarını rahatça kullanabilir ve internette güvenle gezinip arama yapabilirsiniz.



## 2. AVG Yükleme Gereksinimleri

### 2.1. Desteklenen İşletim Sistemleri

**AVG Internet Security 2013** 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)
- Windows 8 (x32 ve x64)

(ve belirli işletim sistemleri için daha yeni hizmet paketleri)

**Not:** [Kimlik](#) bileşeni Windows XP x64'te desteklenmez. Bu işletim sisteminde, AVG Internet Security 2013 yazılımını yalnızca IDP bileşeni olmaksızın yükleyebilirsiniz.

### 2.2. Minimum ve Önerilen Donanım Gereksinimleri

**AVG Internet Security 2013** için minimum donanım gereksinimleri:

- Intel Pentium CPU 1,5 GHz ya da daha hızlı
- 512 MB (Windows XP) / 1024 MB (Windows Vista, Windows 7) RAM bellek
- 1,3 GB boş sabit disk alanı (*yükleme için*)

**AVG Internet Security 2013** için önerilen donanım gereksinimleri:

- Intel Pentium CPU 1,8 GHz ya da daha hızlı
- 512 MB (Windows XP) / 1024 MB (Windows Vista, Windows 7) RAM bellek
- 1,6 GB boş sabit disk alanı (*yükleme için*)



### 3. AVG Yükleme Süreci

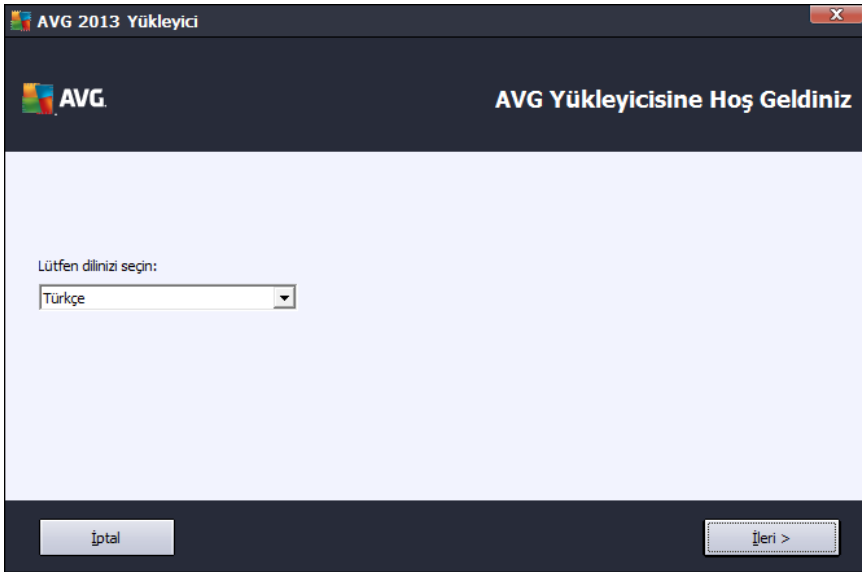
Bilgisayarınıza **AVG Internet Security 2013** programini yüklemek için, en güncel yükleme dosyasini edinmeniz gerekir. **AVG Internet Security 2013** uygulamasinin dogru sürümünü yüklediğinizden emin olabilmek için yükleme dosyasini AVG web sitesinden (<http://www.avg.com/>) indirmanız önerilir. **Destek Merkezi / İndirmeler** bölümü her AVG sürümü için yükleme dosyalarına ayrıntili bir genel bakış sunar.

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

Yükleme dosyasini sabit diskinize indirme ve kaydetme islemini tamamladıktan sonra yükleme islemini baslatabilirsiniz. Yükleme, bir dizi kolay ve anlaşılır iletişim kutusundan oluşur. Her iletişim kutusunda yükleme sürecinin her adimında ne yapılması gerektiği kısaca açıklanır. Her iletişim kutusunun ayrıntili bir açıklaması aşağıda sunulmuştur:

#### 3.1. Hoşgeldiniz: Dil Seçimi

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



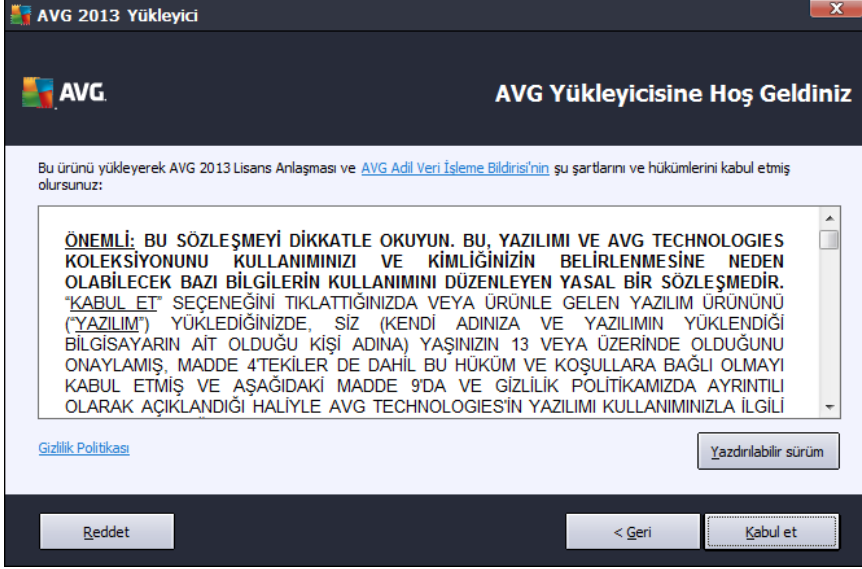
Bu iletişim kutusunda yükleme süreci için kullanılan dili seçebilirsiniz. Dil menüsünü açmak için açılır kutuyu tıklayın. İstedığınız dili seçtiğinizde yükleme süreci bu dille devam eder.

**Dikkat: Su anda yalnızca yükleme süreci dilini seçmektesiniz. AVG Internet Security 2013 uygulaması seçilen dilde yüklenir ve İngilizce her zaman otomatik olarak yüklenir. Ancak, daha fazla dil yüklemek ve AVG Internet Security 2013 uygulamasında bu dillerden biriyle çalışmak mümkündür. [Özel Seçenekler](#) adlı kurulum iletişim kutularından birinde alternatif dil seçimlerinizi onaylamanız istenir.**



### 3.2. Hoşgeldiniz: Lisans Sözleşmesi

AVG Kurulum'a hoş geldiniz iletişim kutusu AVG lisans sözleşmesinin tam metnini içerir:



Lütfen tüm metni dikkatlice okuyun. Okudugunuzu, anladiginizi ve sözleşmeyi kabul ettiginizi onaylamak için, **Kabul Et** düğmesine basın. Lisans sözleşmesini kabul etmiyorsanız **Kabul Etmiyorum** düğmesine basın, böylece yükleme süreci anında iptal edilecektir.

#### AVG Gizlilik Politikası

Bu iletişim kutusu lisans sözleşmesi dışında **AVG Adil Veri İşleme Bildirimi**, **AVG Kisiselleştirme** ve **AVG Gizlilik Politikası** hakkında da daha fazla bilgi sağlar (belirtilen tüm işlevler iletişim kutusunda aktif bir bağlantı olarak yer alır ve tıklattığınızda sizi ayrıntılı bilgilerin bulunduğu web sayfasına yönlendirir). Bu bildirimlerin tam metninin bulabileceğiniz AVG web sitesine gitmek için ( <http://www.avg.com/>) ilgili bağlantıyı tıklatin.

#### Kontrol düğmeleri

İlk kurulum iletişim kutusunda yalnızca iki kontrol düğmesi bulunur:

- **Yazdırılabilir sürüm** - AVG lisans sözleşmesinin tam metninin yazdırmaya uygun biçimde düzenlendiği web arayüzünü görüntülemek için bu düğmeyi tıklatin.
- **Reddet** - Lisans sözleşmesini reddetmek için tıklatin. Kurulum süreci derhal sonlandırılır. **AVG Internet Security 2013** yüklenmez!
- **Geri** - Önceki kurulum iletişim kutusuna, bir adım geriye gitmek için tıklatin.
- **Kabul Et** - Lisans sözleşmesini okudugunuzu, anladiginizi ve kabul ettiginizi onaylamak için tıklatin. Yükleme devam eder ve bir sonraki kurulum iletişim kutusuna geçersiniz.



### 3.3. Lisansınızı etkinleştirme

**Lisansinizi Etkinleştirin** iletişim kutusunda, lisans numaranızı verilen metin alanına girmeniz istenir:

#### Lisans numarası nereden bulunabilir

Satis numarası, **AVG Internet Security 2013** kutusundaki CD paketinde bulunabilir. Lisans numarası **AVG Internet Security 2013** 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.

#### Kopyala ve Yapıştır yöntemi nasıl kullanılır

**Kopyala ve Yapıştır** yöntemini kullanarak **AVG Internet Security 2013** lisans numarasını programa girmek, numaranın doğru biçimde girilmesini garanti altına alır. Lütfen şu adımları takip edin:

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

#### Kontrol düğmeleri

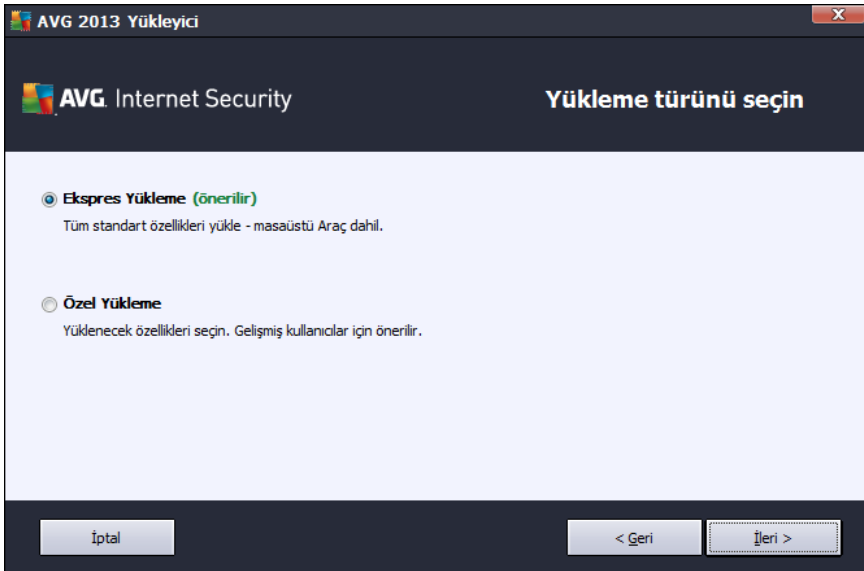


Çogu kurulum iletisim kutusunda oldugu gibi üç kontrol düğmesi mevcuttur:

- **Iptal** - kurulum isleminde hemen çıkmak için tıklatin; **AVG Internet Security 2013** kurulmaz!
- **Geri** - önceki kurulum iletisim kutusuna, bir adım geriye gitmek için tıklatin.
- **İleri** - kurulumu devam etmek ve bir adım ilerlemek için tıklatin.

### 3.4. Yükleme türünü seçin

**Yükleme türünü seçin** iletisim kutusu iki yükleme seçeneği sunar: **Ekspres Yükleme** ve **Özel Yükleme**:



#### Ekspres yükleme

Çogu kullanıcı için kesinlikle standart **Ekspres** yüklemenin muhafaza edilmesi önerilir. Bu sayede **AVG Internet Security 2013** uygulaması program sağlayıcısı tarafından önceden tanımlanmış ayarlarıyla otomatik moda yüklenir: [AVG Aracı](#), [AVG Security Toolbar](#), AVG Secure Search'nin varsayılan arama sağlayıcısı olarak yapılandırılması bu yükleme seçeneği dahilindedir. Bu yapılandırma, minimum kaynak kullanımı ile maksimum güvenliği bir araya getirir. Gelecekte söz konusu yapılandırmayı değiştirme ihtiyacı duyarsanız söz konusu işlemi doğrudan **AVG Internet Security 2013** uygulamasından yapabileceksiniz.

Yükleme işleminin sondaki iletisim kutusuna geçmek için **İleri** düğmesine basın.

#### Özel yükleme

**Özel Yükleme** **AVG Internet Security 2013** uygulamasını standart olmayan ayarlarla kurmak için geçerli bir nedeni olan deneyimli kullanıcılar tarafından kullanılmalıdır. Örn. belirli sistem



gereksinimlerini karşlamak için. Bu seçeneğe karar verirsiniz, iletişim kutusunda **Hedef Klasör** adında yeni bir iletişim kutusu görüntülenir. Bu iletişim kutusunda **AVG Internet Security 2013** uygulamasının yükleneceği yeri belirlemeniz gerekir. Varsayılan olarak, **AVG Internet Security 2013**, iletişim kutusundaki metin alanında belirtildiği gibi, C: sürücüsündeki program dosyaları klasörüne yüklenir. Bu konumu değiştirmek istiyorsanız, sürücü yapısını görüntülemek ve ilgili klasörü seçmek için **Gözet** düğmesini kullanın. Yazılım satıcısı tarafından önceden ayarlanmış varsayılan hedefi geri getirmek için, **Varsayılan** düğmesini kullanın.

Ardından, **Özel Seçenekler** iletişim kutusuna gitmek için **İleri** düğmesine basın.

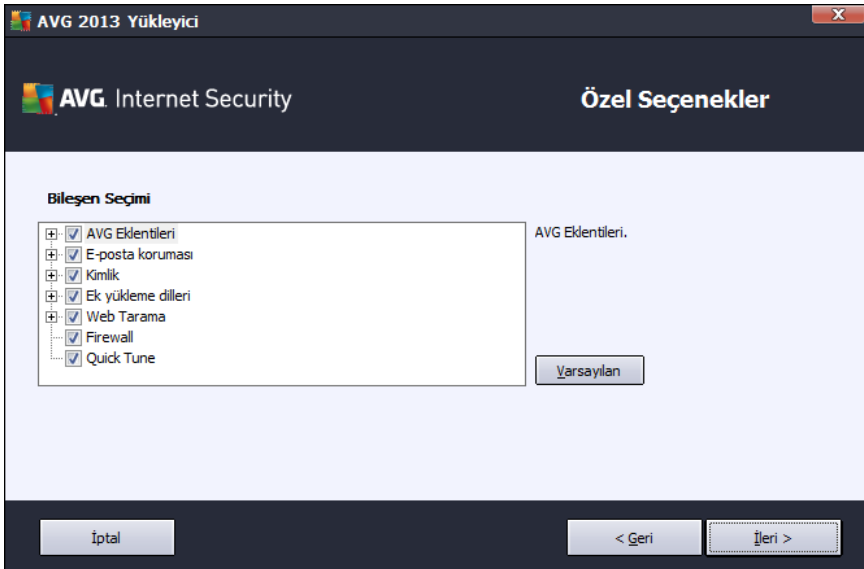
### Kontrol düğmeleri

Çoğu kurulum iletişim kutusunda olduğu gibi üç kontrol düğmesi mevcuttur:

- **İptal** - kurulum işleminden hemen çıkmak için tıklanın; **AVG Internet Security 2013** kurulmaz!
- **Geri** - önceki kurulum iletişim kutusuna, bir adım geriye gitmek için tıklanın.
- **İleri** - kurulumla devam etmek ve bir adım ilerlemek için tıklanın.

### 3.5. Özel seçenekler

**Özel Seçenekler** iletişim kutusu yükleme parametrelerinin ayrıntılı parametrelerini ayarlamanıza olanak verir:



**Bileşen Seçimi** bölümünde, yüklenebilecek tüm **AVG Internet Security 2013** 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 herhangi bir öğeyi vurgulayın, böylece ilgili bileşenin kısa açıklaması bu bölümün sağ tarafından görüntülenir. Her bileşenin işlevleri ile ilgili ayrıntılı bilgiler için, bu belgedeki [Bileşen Genel Görünümü](#) bölümüne bakın.



Yazılım satıcısı tarafından önceden ayarlanmış varsayılan yapılandırmayı geri getirmek için, **Varsayılan** düğmesini kullanın.

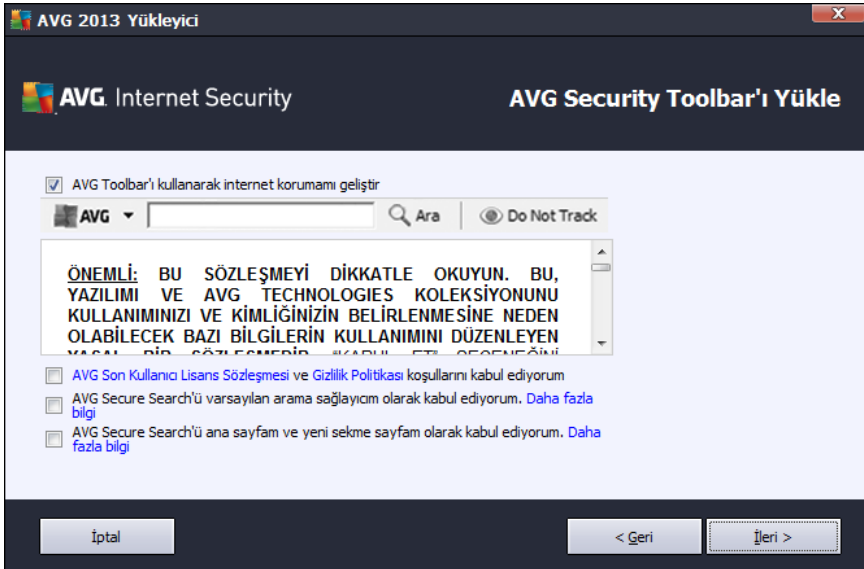
### Kontrol düğmeleri

Çogu kurulum iletişim kutusunda olduğu gibi üç kontrol düğmesi mevcuttur:

- **İptal** - kurulum işleminden hemen çıkmak için tıklatin; **AVG Internet Security 2013** kurulmaz!
- **Geri** - önceki kurulum iletişim kutusuna, bir adım geriye gitmek için tıklatin.
- **İleri** - kurulumla devam etmek ve bir adım ilerlemek için tıklatin.

### 3.6. AVG Security Toolbar'ı Yükle

**AVG Security Toolbar'ı yükle** iletişim kutusunda, [AVG Security Toolbar](#) uygulamasını yüklemek isteyip istemediğinize karar verebilirsiniz. Varsayılan ayarları değiştirmeyeniz, internette gezinirken size daha kapsamlı koruma sağlamak için bu bileşen otomatik olarak internet tarayıcınıza yüklenir ( *su anda desteklenen tarayıcılar Microsoft Internet Explorer sürüm 6.0 ya da üstü ve Mozilla Firefox sürüm 3.0 ya da üstüdür*). Su anda desteklenen internet tarayıcıları: Internet Explorer (sürüm 6.0 ve üstü) ve/veya Mozilla Firefox (sürüm 3.0 ve üstü). Diğer tarayıcılar desteklenmez (*Avant Browser gibi alternatif internet tarayıcıları kullanıyorsanız beklenmeyen davranışlarla karşılaşabilirsiniz*).



İletişim kutusunda aşağıdaki yapılandırmaya karar vermeye yönelik seçenekleriniz bulunur:

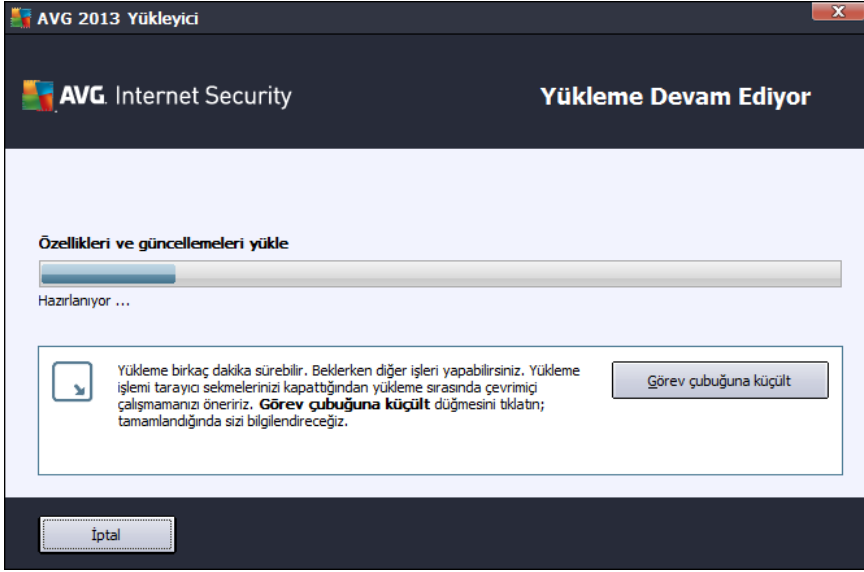
- **AVG Secure Search'ü varsayılan arama sağlayıcım olarak ayarla ve koru** - çevrimiçi maksimum güvenlik için Link Scanner Sörf Kalkanı bile eniyle sıkı bir i birli i içinde çalış an AVG Secure Search motorunu kullanmak istedi inizi onaylamak için i aretli olarak bırakın.
- **nternet korumamı geli tirmek için AVG Security Toolbar yükley** - internette gezinirken güvenli inizi en üst düzeyde tutan AVG Security Toolbar'ı yüklemek için i aretli olarak



bırakın.

### 3.7. Yükleme ilerlemesi

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



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

#### Kontrol düğmeleri

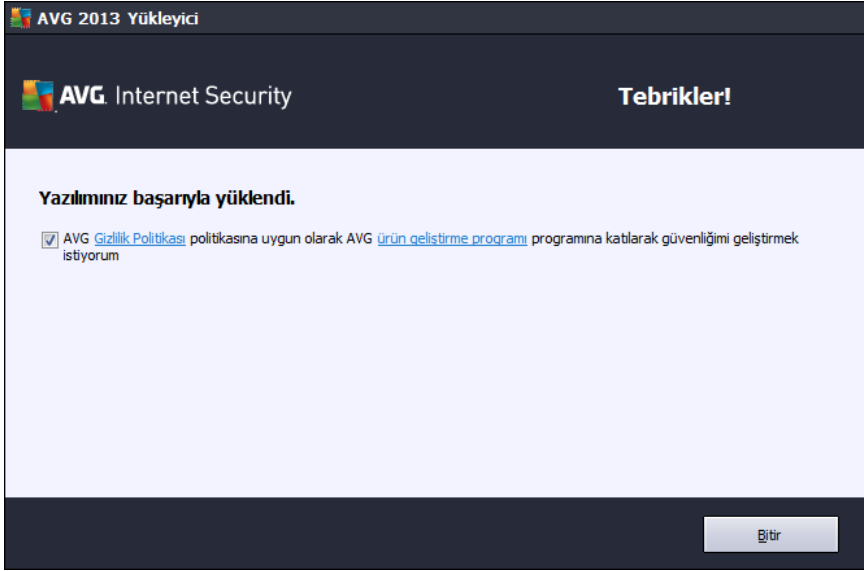
Bu iletişim kutusunda iki adet kontrol düğmesi bulunmaktadır:

- **Minimize et** - Yükleme işlemi birkaç dakika alabilir. Bu düğmeyi tıklatarak iletişim penceresini sistem çubuğunda görünen bir simge haline küçültebilirsiniz. Yükleme tamamlandığında iletişim kutusu tekrar görüntülenir.
- **İptal** - Yalnızca devam eden yükleme sürecini durdurmak istiyorsanız bu düğmeyi kullanmalısınız. Böyle bir durumda **AVG Internet Security 2013** uygulamasının yüklenmeyeceğini lütfen unutmayın!



### 3.8. Yükleme başarılı oldu

**Yükleme başarılı oldu** iletişim kutusu, **AVG Internet Security 2013** yazılımınızın tam olarak yüklendiğini ve yapılandırıldığını onaylar:



### Ürün Geliştirme Programı ve Gizlilik Politikası

Burada, genel internet güvenliği seviyesini yükseltmek için anonim olarak bilgi toplayan **Ürün Geliştirme Programı'na katılıp katılmamayı seçebilirsiniz** (ayrıntılar için [AVG Gelişmiş Ayarları / Ürün Geliştirme Programı](#) bölümüne bakabilirsiniz). Tüm veriler gizli olarak ve AVG Gizlilik Politikası'na uygun olarak işlenir; AVG Gizlilik Politikası'nın tam metnini bulabileceğiniz AVG web sitesine (<http://www.avg.com/>) gitmek için **Gizlilik Politikası** bağlantısını tıklatın. Kabul ediyorsanız, lütfen seçeneği işaretli olarak bırakın (seçenek varsayılan olarak onaylıdır).

Yükleme sürecini bitirmek için **Bitir** düğmesine basın.



## 4. Yüklemeden Sonra

### 4.1. Ürün kaydı

**AVG Internet Security 2013** yüklemesini tamamladıktan sonra, lütfen ürününüzü çevrimiçi olarak AVG web sitesinde (<http://www.avg.com/>) kaydedirin. Kayıt işleminin ardından AVG kullanıcı hesabınıza erişebileceğiniz, AVG Güncelleme bültenini alacak ve sadece kayıtlı kullanıcılara sunulan diğer hizmetlerden yararlanacaksınız. Ürünü kaydettirmenin en kolay yolu doğrudan **AVG Internet Security 2013** kullanıcı arayüzünü kullanmaktır. Lütfen [üstteki gezinme bölümünden / Seçenekler / Şimdi kaydet](#) ögesini seçin. AVG web sitesindeki (<http://www.avg.com/>) **Kayıt** sayfasına yönlendirilirsiniz. Lütfen sayfadaki talimatları izleyin.

### 4.2. Kullanıcı arayüzüne erişim

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

- [AVG sistem tepsi simgesi](#)'ni çift tıklattığınızda
- Masaüstünüzdeki AVG simgesini çift tıklattığınızda
- menüden **Baslat / Tüm Programlar / AVG / AVG 2013**

### 4.3. Tüm bilgisayarın taraması

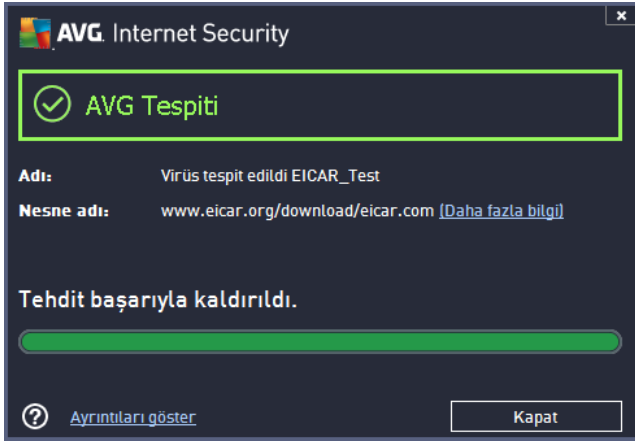
**AVG Internet Security 2013** yüklemesinden önce bilgisayarınıza virüs bulmuş olması ihtimali bulunmaktadır. Bu nedenle bilgisayarınızda virüs bulunmadığından emin olmak için [Tüm bilgisayar taraması](#) yapmanız gerekmektedir. İlk tarama uzun bir süre alabilir (*bir saat civarında*), ancak bilgisayarınızın herhangi bir tehdit altında olmadığından emin olmak için bu taramayı başlatmanız önerilir. [Tüm bilgisayar taraması](#) konusunda talimatlar için [AVG Taraması](#) bölümünü inceleyin.

### 4.4. Eicar testi

**AVG Internet Security 2013** programının düzgün olarak yüklendiğini onaylamak için EICAR testini çalıştırabilirsiniz.

EICAR testi, virüslerden koruma sisteminin 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](http://www.eicar.com) adresinde bulunan EICAR'ın web sitesinden indirebilirsiniz ve bunun yanı sıra EICAR testi hakkında tüm gerekli bilgileri edinebilirsiniz.

*www.eicar.com* dosyasını indirmeye çalışın ve sabit diskinize kaydedin. Siz test dosyasının indirilmesini onaylamaz, **AVG Internet Security 2013** uygulamanız uyarıda bulunmaksızın buna yanıt verir. Bu bildirim, AVG'nin bilgisayarınıza doğru bir şekilde yüklenmiş olduğunu gösterir.



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

#### 4.5. AVG varsayılan yapılandırması

**AVG Internet Security 2013** varsayılan yapılandırması (yani, uygulamanın yüklemesinden 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.** İhtiyaçlarınızı daha iyi karşılaması açısından AVG yapılandırmasını değiştirme ihtiyacı hissederseniz [AVG Gelişmiş Ayarlar](#)'ına gidin: ana menü öğesi *Seçenekler/Gelişmiş ayarlar*'i seçin ve AVG yapılandırmasını yeni açılan [AVG Gelişmiş Ayarlar](#) iletişim kutusunda düzenleyin.

## 5. AVG Kullanıcı Arayüzü

AVG Internet Security 2013 ana pencerede açılır:



Ana pencere çok sayıda bölüme ayrılır:

- **Üst satır gezinme** ana pencerenin üst bölümünde yan yana dizilen dört aktif bağlantıdan oluşur (*AVG'yi beğendiniz mi?*, *Raporlar*, *Destek*, *Seçenekler*). [Ayrıntılar >>](#)
- **Güvenlik Durumu Bilgisi** AVG Internet Security 2013 ürününüzün mevcut durumu hakkında temel bilgileri sağlar. [Ayrıntılar >>](#)
- **Yüklü bileşenlerin genel görünümü** ana pencerenin orta bölümünde yatay bloklar halinde sıralanır. Bileşenler ilgili bileşen simgesiyle etiketlenen açık yeşil bloklar olarak görüntülenir ve bileşen durumu bilgileri belirtilir. [Ayrıntılar >>](#)
- **Uygulamalarım** ana pencerenin alt orta bölümünde yer alır ve **AVG Internet Security 2013** ürününüzü tamamlayıcı nitelikteki bilgisayarınızda zaten yüklü olan veya yüklenmesi önerilen uygulamalar hakkında genel bilgiler sunar. [Ayrıntılar >>](#)
- **Tara / Güncelle hızlı bağlantıları** ana penceredeki blokların alt kısmına yerleştirilmiştir. Bu düğmeler en önemli ve en sık kullanılan AVG işlemlerine anında erişim sağlar. [Ayrıntılar >>](#)

AVG Internet Security 2013 ürününün ana penceresi dışında, uygulamaya erişmek için kullanabileceğiniz iki kontrol ögesi daha bulunur:

- **Sistem tepsi simgesi** monitörün sağ alt köşesinde yer alır (*sistem tepsisinde*) ve **AVG Internet Security 2013** uygulamasının mevcut durumunu gösterir. [Ayrıntılar >>](#)
- **AVG aracına** Windows kenar çubuğundan erişilir (*yalnızca Windows Vista/7/8 işletim*



sistemlerinde desteklenir) ve araç **AVG Internet Security 2013** içinde tarama ve güncelleme işlemlerine hızlı erişim sağlar. [Ayrıntılar >>](#)

## 5.1. Üst Satır Gezinme

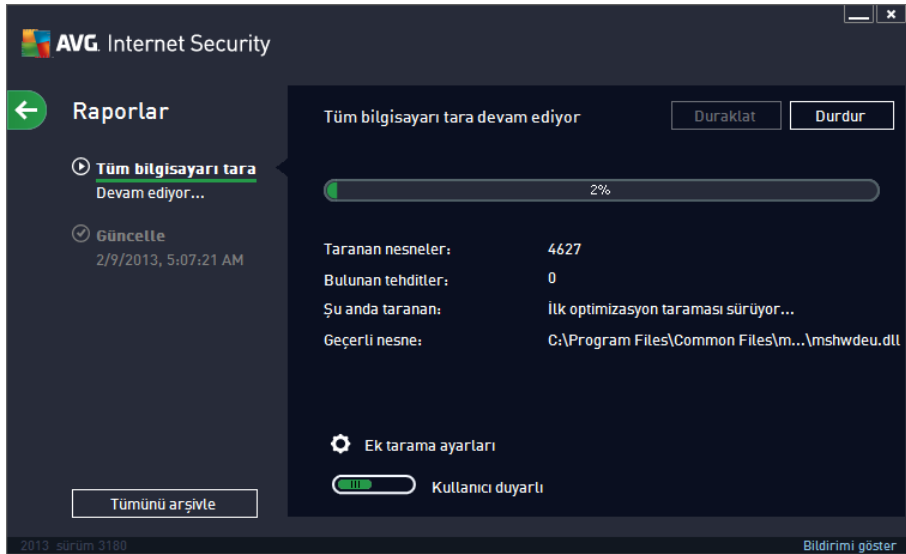
**Üst satır gezinme** ana menünün üst bölümünde yan yana dizilmiş birkaç etkin bağlantıdan oluşur. Gezinme bölümündeki düğmeler:

### 5.1.1. AVG'yi beğendiniz mi

Bağlantıyı tek sefer tıklatıp [AVG Facebook topluluğuna](#) bağlanarak maksimum internet güvenliğiniz için en son AVG bilgi, haber, ipucu ve kolay yolları paylaşabilirsiniz.

### 5.1.2. Raporlar

Önceden başlatılmış olan tüm taramalar ve güncelleme işlemleri hakkında genel bilgilerin yer aldığı yeni bir **Raporlar** iletişim kutusu açar. O anda tarama veya güncelleme çalışıyorsa, [ana kullanıcı arayüzünün](#) üst bölümündeki **Raporlar** ögesinin yanında dönen bir daire simgesi gösterilir. Çalışan işlemin ilerlemesini gösteren iletişim kutusuna gitmek için bu daireyi tıklatın:



### 5.1.3. Destek

**AVG Internet Security 2013** uygulamasıyla ilgili tüm bilgileri bulabileceğiniz dört sekmeye ayrılmış yeni bir iletişim kutusu açar:

- **Lisans ve Destek** - Bu sekme ürün adı, lisans numarası ve son kullanma tarihi bilgilerini gösterir. İletişim kutusunun alt bölümünde müşteri destek birimine ulaşabileceğiniz tüm iletişim bilgilerini bulabilirsiniz. Sekmede bulunan etkin bağlantılar ve düğmeler:
  - (Yeniden) Etkinleştir - Yeni **AVG Yazılım Etkinleştirme** iletişim kutusunu açmak için tıklatın. Satis numaranızı (AVG Internet Security 2013 yüklemesi sırasında kullandığınız) değiştirmek veya mevcut lisans numaranızı bir baskısıyla değiştirmek (örn. daha üst bir AVG ürününe yükseltme yaparken) için ilgili alana lisans numaranızı girin.



- o **Panoya kopyala** - Lisans numarasini kopyalayip uygun alana yapistirmek için bu bağlantıyı kullanin. Bu sayede lisans numarasinin dogru girildiginden emin olabilirsiniz.
- o **Simdi yenile** - **AVG Internet Security 2013** Lisans yenilemenizi uygun bir zamanda, mevcut lisansinizin süresi sona ermeden en az bir ay önce satın almanizi öneririz. Yaklaşmakta olan son kullanma tarihi konusunda bilgilendirilirsiniz. Bu bağlantıyı tıklararak AVG web sitesine (<http://www.avg.com/>) giderek lisans durumunuz, son kullanma tarihi ve yenileme/yükseltme kampanyalari hakkında ayrıntili bilgi alabilirsiniz.

**AVG Internet Security**

Lisans ve Destek Ürün Program Lisans Sözleşmesi

**Lisans bilgileri**

Ürün adı: AVG Internet Security 2013 (Tam, 1 koltuk)  
Lisans Numarası: IMNJI-QH9WL-NEVNU-AUNQF-MJRI7-3 [\[panoya kopyala\]](#)  
Lisans Sona Erme Tarihi: Wednesday, December 31, 2014 [\[Simdi yenile\]](#)

Yeni bir lisans satın aldınız mı?  
[Yeniden etkinleştir](#)

**Destek bilgileri**

**Bize e-posta gönderin**  
Daha az acil sorunlar için bize e-posta gönderin, biz de sorununuzu hemen çözmeye çalışalım.  
[BİZE E-POSTA GÖNDERİN](#)

**AVG Topluluğu**  
Öneride bulunun. Öneri alın. Ücretsiz topluluğumuzda bilgi paylaşın.  
[ÖĞRENİN VE PAYLAŞIN](#)

**SSS'ler**  
Sık Sorulan Soruların yanıtlarını web sitemizde bulabilirsiniz.  
[SSS BÖLÜMÜNÜ ZİYARET EDİN](#)

**Virüs temizleme araçları**  
Ücretsiz virüs temizleme araçlarımızla virüsleri ve bulaşmaları temizleyin.  
[VİRÜSLERDEN KURTULUN](#)

[Kapat](#)

- **Ürün** - Bu sekme **AVG Internet Security 2013** ürün bilgileri, yüklü bileşenler, yüklü e-posta koruması ve sistem bilgileri hakkında en önemli teknik verileri gösterir:

**AVG Internet Security**

Lisans ve Destek **Ürün** Program Lisans Sözleşmesi

**Ürün bilgileri**

AVG Sürümü: 2013.0.3180  
Virüs veritabanı sürümü: 3147/6086 (Wednesday, February 06, 2013, 9:24 PM)  
LinkScanner sürümü: 1500  
AVG Güvenlik Araç Çubuğu sürümü: 14.1.0.7  
Anti-Spam sürümü: 6.5.1

**Yüklenen bileşenler**  
AVG Güvenlik Araç Çubuğu, AVG Hızlandırıcı, AVG Tavsiyesi, Anti-Rootkit, Anti-Spam, Anti-Spyware, Firewall, Identity Protection, Online Shield, Quick Tune, Sörf Kalkanı, Virüslerden Koruma, Yerleşik Kalkan

**Yüklenen e-posta koruması**  
Microsoft Outlook, Kişisel E-posta Tarayıcısı

**Sistem bilgileri**

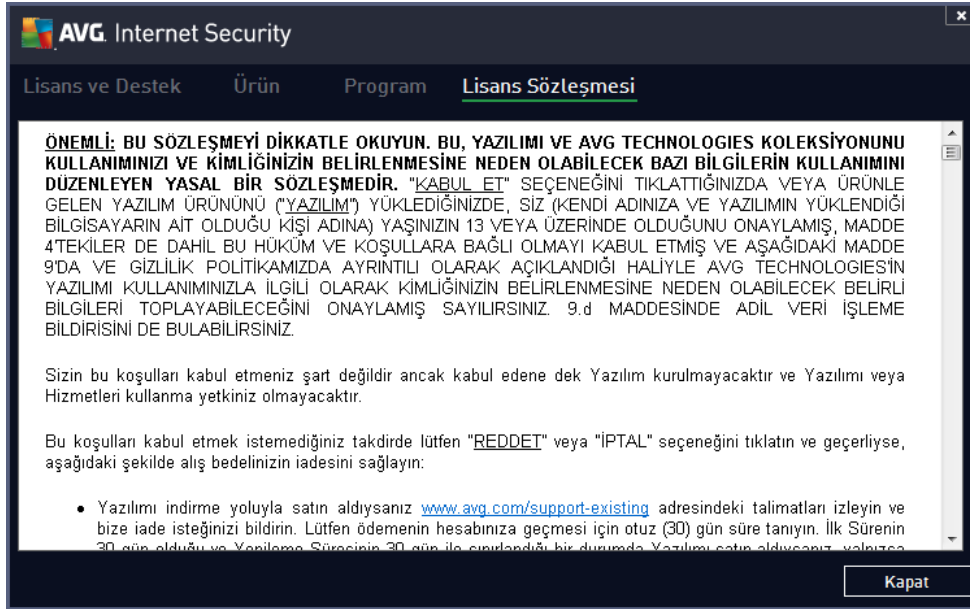
İşletim sistemi: Microsoft(R) Windows(R) Vista Ultimate Edition (32-bit) Hizmet Paketi 1  
İşlemci: Intel(R) Core(TM)2 Quad CPU Q9550 @ 2.83GHz  
Toplam / Boş bellek: 1023 / 370 MB

[Kapat](#)

- **Program** - Bu sekmede program dosyasi sürümü ve üründe kullanılan üçüncü taraflara ait kodlar hakkında bilgi bulabilirsiniz:



- **Lisans Sözleşmesi** - Bu sekmede siz ve AVG Technologies arasındaki lisans sözleşmesinin tam metni bulunur:



#### 5.1.4. Seçenekler

AVG Internet Security 2013 ürününün bakım işlemine **Seçenekler** ögesinden erişilebilir. Açılır menüyü açmak için oku tıklayın:

- **Bilgisayarı tara** tüm bilgisayar taraması baslatır.



- **[Seçilen klasörü tara...](#)** - AVG tarama arayüzüne geçer ve bilgisayarınızın dolasım ağacından taranmasını istediğiniz dosya ve klasörleri seçmenizi sağlar.
- **[Dosyayı tara...](#)** - Belirli tek bir dosya üzerinde talebe göre test yapmanızı sağlar. Diskinizin ağaç yapısını içeren yeni bir pencere açmak için bu seçeneği tıklayın. İstedığınız dosyayı seçin ve tarama başlatmayı onaylayın.
- **[Güncelle](#)** - **AVG Internet Security 2013** güncellemesini otomatik olarak başlatır.
- **[Dizinden güncelle...](#)** - Sabit diskinizde bulunan belirli bir dosyanın içinde yer alan güncelleme dosyalarını alarak güncelleme işlemi gerçekleştirir. Diğer yandan bu seçim sadece acil durumlarda önerilmektedir. Örn. internet bağlantısı olmadığı durumlarda (Örneğin bilgisayarınıza virüs bulamıyorsa ve internet bağlantınız kesildiyse; bilgisayarınız bir ağa bağlıysa fakat internet erişimi yoksa vb.). Yeni açılan pencereden, daha önce güncelleme dosyasını depoladığınız klasörü seçin ve güncelleme işlemi başlatın.
- **[Virüs Kasası](#)** - Belirli bir neden doğrultusunda AVG'nin tespit edilmiş temizlenemeyen tüm bulgularını tasıdığı karantina alanının arayüzü olan Virüs Kasası'ni açar. Karantina altında bulunan bulgular, yalıtılmıştır, bilgisayarınızın güvenliği garanti altındadır ve aynı anda bulgular ileride tamir edilebilecekleri göz önünde bulundurulurken depolanır.
- **[Geçmiş](#)** - Bazı alt menü seçenekleri sunar:
  - **[Tarama sonuçları](#)** - Tarama sonuçları hakkında genel bilgilerin bulunduğu bir iletişim kutusu açar.
  - **[Yerleşik Kalkan tespiti](#)** - Yerleşik Kalkan tarafından tespit edilen tehditler hakkında genel bilgi veren bir iletişim kutusu açar.
  - **[Identity Protection tespiti](#)** - Identity Protection tarafından tespit edilen tehditler hakkında genel bilgi veren bir iletişim kutusu açar.
  - **[E-posta Koruması tespiti](#)** - E-posta Koruması bileşeni tarafından tehlikeli olduğu tespit edilen posta eklentileri hakkında genel bilgi veren bir pencere açar.
  - **[Online Shield tespitleri](#)** - Online Shield
  - **[Olay geçmişi günlüğü](#)** - Kaydedilen tüm **AVG Internet Security 2013** işlemleri hakkında genel bilgi veren bir geçmiş günlüğü arayüzü açar.
  - **[Firewall günlüğü](#)** - Tüm Firewall işlemlerinin ayrıntılı bilgilerinin bulunduğu bir iletişim kutusu açar.
- **[Gelişmiş ayarlar...](#)** - **AVG Internet Security 2013** yapılandırmasını düzenleyebileceğiniz AVG gelişmiş ayarlar iletişim kutusunu açar. Genel olarak uygulamanın yazılım üreticisi tarafından tanımlanan varsayılan ayarlarının muhafaza edilmesi önerilir.
- **[Firewall ayarları...](#)** - Firewall bileşeninin gelişmiş yapılandırmasına ilişkin bağımsız bir pencere açar.
- **[Yardım içerikleri](#)** - AVG yardım dosyalarını açar.
- **[Destek alın](#)** - Müşteri destek merkezi sayfasında AVG web sitesini (<http://www.avg.com/>)

açar.

- **AVG Web** - AVG web sitesini (<http://www.avg.com/>) açar.
- **Virüsler ve Tehlikeler Hakkında** - Tanımlanan virüs hakkında ayrıntılı bilgi edinebildiğiniz çevrimiçi virüs ansiklopedisini açar.
- **(Yeniden) Etkinleştir** - yükleme işlemi sırasında girdiğiniz bilgilerin bulunduğu **AVG Etkinleştirme** 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 kaydet / Hesabım** - AVG web sitesinin (<http://www.avg.com/>) kayıt sayfasına bağlantı sağlar. Lütfen kayıt bilgilerinizi doldurun; sadece AVG ürünlerini kaydettiren müşterilerimiz ücretsiz teknik destek alabilecektir. Deneme sürümünü kullanıyorsanız, **AVG Internet Security 2013** sonraki iki öge, **Şimdi satın al** ve **Etkinleştir** olarak görünür ve programın tam sürümünü hemen satın almanızı sağlar. Bir-satış numarasıyla yüklenmiş **AVG Internet Security 2013** için öğeler **Kaydet** ve **Etkinleştir** olarak görünür.
- **AVG hakkında** - Satın aldığınız lisans ve erişilebilir destek, ürün ve program bilgilerine yönelik dört sekme ile lisans sözleşmesinin tam metninin bulunduğu yeni bir iletişim kutusu açar.

## 5.2. Güvenlik Durumu Bilgisi

**Güvenlik Durumu Bilgisi** bölümü **AVG Internet Security 2013** ana penceresinin üst kısmında yer alır. Bu bölümde **AVG Internet Security 2013** programınızın mevcut güvenlik durumu hakkında her zaman bilgi bulabilirsiniz. Lütfen bu bölümde betimlenmesi muhtemel simgeleri ve anlamlarını inceleyin:



- yeşil simge **AVG Internet Security 2013 uygulamasının tamamen işlevsel olduğunu belirtir**. Bilgisayarınız tamamen korunur, günceldir ve yüklü tüm bileşenler doğru çalışmaktadır.



- sarı simge, **bir ya da birden fazla bileşenin yanlış yapılandırıldığını** ve söz konusu bileşenlerin özelliklerini/ayarlarını kontrol etmeniz gerektiğini gösterir. **AVG Internet Security 2013** uygulamasında herhangi bir kritik sorun yoktur ve muhtemelen bazı nedenlerden dolayı bileşenlerden bazılarını geçici olarak kapatmayı seçmiş olabilirsiniz. Hala korunuyorsunuz!. Diğer bir yandan lütfen bileşenin ayarlarını inceleyin! Yanlış yapılandırılmış bileşen [ana kullanıcı arayüzünde](#) turuncu renkli bir uyarı bandıyla gösterilir.

Sarı simge, bir bileşenin hata durumunu herhangi bir nedenle yok saydığınızda da görünür. **Hata durumunu yoksay** seçeneğine [Gelişmiş ayarlar / Hata durumunu yoksay](#) yoluyla erişilebilir. Burada bileşenin hata durumunun farkında olduğunuz, ancak belirli bir neden doğrultusunda **AVG Internet Security 2013** uygulamasının bu şekilde çalışmasını ve bu konuda uyarılmak istemediğinizi belirtme seçeneğiniz vardır. Özel durumlar için bu seçeneği kullanmanız gerekebilir ancak en kısa zamanda **Hata durumunu yoksay** seçeneğini devre dışı bırakmanız önerilir!

Ya da, sarı simge **AVG Internet Security 2013** ürününüz bilgisayar yeniden başlatması gerektirdiğinde de görüntülenir (**Yeniden başlatma gerekiyor**). Lütfen bu uyarıyı dikkate alın



ve bilgisayarınızı yeniden başlatın.



- turuncu simge **AVG Internet Security 2013 uygulamasının kritik durumda olduğunu belirtir!** Bir veya daha fazla bileşen düzgün çalışmıyor ve **AVG Internet Security 2013** uygulaması bilgisayarınızı koruyamıyordu. Lütfen rapor edilen sorunu çözmek için gerekli ilgiyi gösterin! Hatayı kendi başınıza çözemiyorsanız [AVG teknik destek](#) ekibi ile iletişim kurun.

**AVG Internet Security 2013 uygulamasının en verimli performansı ayarlayamaması durumunda, Düzeltmek için tıklattığınız yeni bir düğme (alternatif olarak, sorun birden fazla bileşenle ilgiliyse, Tümünü düzeltmek için tıklattığınız düğmesi) görüntülenir. Düğmeye basarak programı otomatik olarak kontrol etme ve yapılandırma işlemini başlatın. Bu özellik, AVG Internet Security 2013 uygulamasını en verimli performansa ayarlamanın ve maksimum güvenlik düzeyine ulaşmanın kolay bir yoludur!**

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

**Not:** AVG Internet Security 2013 durum bilgilerine istediğiniz zaman [sistem tepsi simgesinden](#) de ulaşabilirsiniz.

### 5.3. Bileşen Genel Görünümü

**Yüklü bileşenlerin genel görünümü** [ana pencerenin](#) orta bölümünde yatay bloklar halinde sıralanır. Bileşenler ilgili bileşen simgesiyle etiketlenmiş açık yeşil bloklar olarak gösterilir. Her blok korumanın mevcut durumu hakkında bilgiler sağlar. Bileşen doğru yapılandırılmış ve tam olarak çalışıyorsa, bilgiler yeşil renkli harflerle gösterilir. Bileşen durdurulursa, işlevi sınırlı hale gelirse veya bileşen hata durumundaysa, turuncu renkli bir metin alanında gösterilen bir uyarı metniyle bilgilendirilirsiniz. **İlgili bileşen ayarlarına kesinlikle dikkat etmeniz tavsiye edilir!**

Fareyi bileşenin üzerine getirerek [ana pencerenin](#) altında kısa bir metin görüntüleyebilirsiniz. Metinde bileşenin işlevselliğine dair temel giriş bilgileri bulunur. Ayrıca, bileşenin mevcut durumu hakkında bilgi sunar ve hangi bileşen hizmetlerinin doğru yapılandırılmadığını belirtir.

#### Yüklü bileşen listesi

**AVG Internet Security 2013** içinde, **Bileşen Genel Görünümü** kısmi aşağıdaki bileşenler hakkında bilgiler içerir:

- **Bilgisayar** - Bu bileşen iki hizmeti kapsar: **Virüslerden Koruma Kalkanı** sisteminizdeki virüs, casus yazılım, solucan, truva atı, istenmeyen çalıştırılabilir dosyalar veya kitaplıkları tespit eder sizi zararlı reklam yazılımlarına karşı korur; **Anti-Rootkit** ise uygulama, sürücü veya kitaplıklarda gizlenen tehlikeli kök kullanıcı takımları için tarama yapar. [Ayrıntılar >>](#)
- **Web Tarama** - İnternette arama ve gezinme sırasında sizi web tabanlı saldırılara karşı korur. [Ayrıntılar >>](#)
- **Identity** - Bileşen **Identity Shield** hizmeti internette dijital varlıklarınızı yeni ve bilinmeyen tehditlere karşı sürekli olarak korur. [Ayrıntılar >>](#)



- **E-postalar** - Gelen e-posta mesajlarınızı istenmeyen e-postalara karşı denetler ve virüsleri, kimlik avı saldırılarını veya diğer tehditleri engeller. [Ayrıntılar >>](#)
- **Firewall** - Her ağ bağlantı noktasındaki tüm iletişimleri denetleyerek sizi kötü amaçlı saldırılardan korur ve tüm sızma girişimlerini engeller. [Ayrıntılar >>](#)

### Erisilebilir eylemler

- **Bileşen genel görünümü ekranında bileşeni seçmek için fareyi ilgili bileşen simgesi üzerinde hareket ettirin.** Aynı anda [kullanıcı arayüzünün](#) kısmında bileşenin temel fonksiyonları hakkında açıklamalar görüntülenir.
- **Bileşen simgesini tek tıklayarak** bileşenin mevcut durumu hakkında bilgiler içeren arayüzünü açın ve bileşenin yapılandırma ve istatistik verilerine erişin.

## 5.4. Uygulamalarım

**Uygulamalarım** alanında (*bileşenler grubunun altındaki yeşil bloklar satırı*) bilgisayarınızda zaten yüklü olan veya yüklenmesi önerilen ilave AVG uygulamaları hakkında genel bilgiler bulabilirsiniz. Bloklar kosullu olarak görüntülenir ve aşağıdaki uygulamalardan herhangi birini temsil edebilir:

- **Mobil koruma** cep telefonunuzu virüs ve zararlı yazılımlardan koruyan bir uygulamadır. Uygulama, ayrı kalmanız durumunda akıllı telefonunuzu uzaktan izleme imkanı da sağlar.
- **LiveKive** güvenli sunuculara çevrimiçi veri yedeklemesi yapmak için hazırlanmıştır. LiveKive tüm dosyalarınızı, fotoğraflarınızı ve müzik dosyalarınızı güvenli bir yerde yedekleyerek bunları ailenizle ve arkadaşlarınızla paylaşmanıza ve iPhone ve Android cihazları da dahil olmak üzere söz konusu dosyalara web etkinliği olan tüm cihazlardan erişmenize olanak sağlar.
- **Family Safety** çocuklarınızın uygunsuz web sitelerine, medya içeriklerine ve çevrimiçi aramalara karşı korunmasına yardımcı olur ve çevrimiçi faaliyetleriyle ilgili size rapor sağlar. AVG Family Safety çocuklarınızın sohbet odaları ve sosyal paylaşım sitelerindeki etkinliklerini izlemek için tuz wurusu teknolojisi kullanır. Çocukların istismarında kullanıldığı bilinen kelimeler, ifadeler ve cümleler algılasa, SMS veya e-posta yoluyla sizi anında bilgilendirir. Uygulama aracılığıyla çocuklarınızdan her biri için uygun koruma düzeyi ayarlayabilir ve benzersiz girişler aracılığıyla onları ayrı ayrı gözlemleyebilirsiniz.
- **PC Tuneup** uygulaması bilgisayarınızın hızının ve genel performansının nasıl iyileştirilebileceğine yönelik ayrıntılı sistem analizi ve düzeltme işlemi için gelişmiş bir araçtır.
- **MultiMi** tüm e-posta ve sosyal hesaplarınızı tek bir güvenli alanda birleştirerek aile ve arkadaşlarınızla iletişim kurmayı, internette gezinmeyi, fotoğraf, video ve dosya paylaşmayı çok daha kolay hale getirir. MultiMi, görüntülediğiniz web sayfalarındaki bağlantıların ardındaki web sayfalarını analiz edip bunların güvenli olduğundan emin olarak sizi sayıları sürekli olarak artan tehditlerden koruyan LinkScanner hizmetini de barındırır.
- **AVG Toolbar**'na doğrudan internet tarayıcınızdan erişebilirsiniz; bu uygulama internette gezinirken size maksimum koruma sağlar.

**Uygulamalarım** alanındaki uygulamalar hakkında ayrıntılı bilgi için ilgili blogu tıklatin. Bileseni hemen indirebileceğiniz AVG web sayfasına yönlendirilirsiniz.

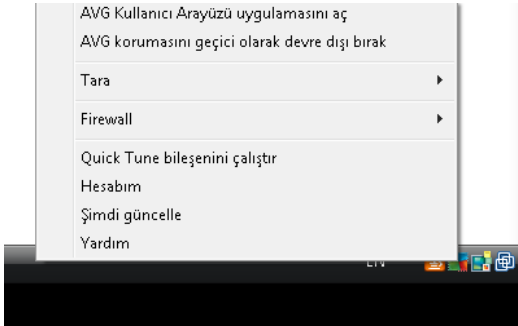
## 5.5. Tara / Hızlı Bağlantıları Güncelle

**Hızlı bağlantılar** AVG Internet Security 2013 [kullanıcı arayüzünün alt bölümündeki düğmelerde yer alır](#). Bu bağlantılar tarama ve güncelleme gibi en önemli ve en sık kullanılan uygulama özelliklerine anında erişebilmenizi sağlar. Hızlı bağlantılara kullanıcı arayüzündeki tüm iletişim kutularından erişilebilir:



- **Şimdi tara** - Düğme grafik olarak iki kısma ayrılmıştır. **Şimdi tara** bağlantısını izleyerek [Tüm Bilgisayarı Tara](#) işlemini hemen başlatabilir ve ilerleme ile sonuçları otomatik olarak açılan [Raporlar](#) penceresinden izleyebilirsiniz. **Seçenekler** düğmesi **Tarama Seçenekleri** iletişim kutusunu açar; burada [zamanlanmış taramaları yönetebilir](#) ve [Tüm Bilgisayarı Tara / Belirli Dosyaları veya Klasörleri Tara](#) parametrelerini düzenleyebilirsiniz. (Ayrıntılar için [AVG Tarama](#) bölümüne bakın)
- **Şimdi güncelle** - Ürün güncellemesini hemen başlatmak için düğmeye basın. Güncelleme sonuçları hakkında AVG sistem tepsisi simgesi üzerinde beliren iletişim kutusuyla bilgilendirilirsiniz. (Ayrıntılar için [AVG Güncellemeleri](#) bölümüne bakın)

## 5.6. Sistem Tepsisi Simgesi

**AVG Sistem Tepsisi Simgesi** (Windows görev çubuğunuzda, ekranınızın sol alt köşesinde) **AVG Internet Security 2013 uygulamanızın mevcut durumunu gösterir**. **AVG Internet Security 2013 kullanıcı arayüzü** ana penceresinin açık ya da kapalı olduğu önemli olmaksızın devamlı olarak sistem tepsinizde bulunur:





### AVG Sistem Tepsisi Simgesi görünümü

-  Tam renkli ve başka öğe bulunmayan simge tüm **AVG Internet Security 2013** bileşenlerinin etkin ve tamamen çalışır durumda olduğunu gösterir. Ancak, simge bileşenlerden biri tam çalışır durumda olmasa da (kullanıcı [bilesen durumunu yoksaymaya](#) karar verdiğinde) bu şekilde görünebilir. (Bilesenin durumunu yoksayma seçeneğini onaylayarak, [bilesenin hata durumunun](#) farkında olduğunuzu, ancak kimi nedenlerle durumun böyle kalmasını ve durum hakkında uyarı almak istemediğinizi ifade edersiniz.)
-  Üzerinde ünlem isareti bulunan simge bir bileşenin (veya daha fazla bileşenin) [hata durumunda](#) olduğunu gösterir. Bu tip uyarılara mutlaka dikkat edin ve düzgün ayarlanmamış bileşenin yapılandırma sorununu gidermeye çalışın. Bileşen yapılandırması değişikliklerini



gerçekleştirebilmek için sistem tepsisi simgesini çift tıklatarak [uygulamanın kullanıcı arayüzünü](#) açın. Hangi bileşenin [hata durumunda](#) olduğuyla ilgili ayrıntılı bilgi için lütfen [güvenlik durumu bilgisi](#) bölümüne bakın.

-  Sistem tepsisi tam renkli olarak yanıp sönen ve dönen bir ışıkla da görünebilir. Bu grafik gösterim o anda baslatılan bir güncelleme işlemi işaret eder.
-  Tam renkli ve ok işaretli simge ise **AVG Internet Security 2013** taramalarından birinin o anda çalışmakta olduğunu gösterir.

### AVG Sistem Tepsisi Simgesi bilgileri

**AVG Sistem Tepsisi Simgesi** sizi sistem tepsisi simgesi hizasından açılan bir pencere aracılığıyla **AVG Internet Security 2013** uygulamanızda o an gerçekleşen işlemler ve programdaki olası durum değişiklikleri hakkında da bilgilendirir (örn. *programlanan tarama ya da güncellemenin otomatik olarak baslatılması, Firewall profil değişikliği, bir bileşenin durum değişikliği, hata durumu oluşumu, ...*).

### AVG Sistem Tepsisi Simgesi yoluyla erişilebilen işlemler

**AVG Sistem Tepsisi Simgesi**, **AVG Internet Security 2013** [kullanıcı arayüzüne](#) erişmek için bir hızlı bağlantı olarak da kullanılabilir; bunun için simgeyi çift tıklamak yeterlidir. Simgeyi sağ tıklatarak aşağıdaki seçenekleri sunan kısa bir bağlam menüsü açarsınız:

- **AVG Kullanıcı Arayüzünü Aç - AVG Internet Security 2013** [kullanıcı arayüzünüz](#) açmak için tıklayın.
- **AVG korumasını geçici olarak devre dışı bırak** - bu seçenek **AVG Internet Security 2013** tarafından sağlanan tüm korumayı tek seferde kapatmanızı sağlar. Mutlaka gerekli değilse, bu seçeneği kullanmamanız gerektiğini lütfen unutmayın! Çoğu durumda, yeni yazılımı veya sürücülerini yüklemeyi önce ve hatta yükleyici veya yazılım sihirbazı yükleme işlemi sırasında istenmeyen kesintilerin olmamasını sağlamak için çalışan program ve uygulamaların kapatılmasını önerse bile **AVG Internet Security 2013** uygulamasını devre dışı bırakmak gerekmez. **AVG Internet Security 2013** uygulamasını geçici olarak devre dışı bırakmanız gerekirse, işinizi bitirdikten sonra yeniden etkinleştirmeniz gerekir. Virüslerden korunma yazılımınız devre dışı bırakılmıyken internete veya bir ağa bağlanırsanız, bilgisayarınız saldırılara açık durumda olur..
- **Tarama** - [önceden tanımlanan taramalar](#) ([Tüm Bilgisayarı Tara](#) ve [Belirli Dosyaları veya Klasörleri Tara](#)) bağlam menüsünü açmak ve gerekli taramayı seçmek için tıklayın; tarama hemen baslatılacaktır.
- **Çalışan taramalar ...** - bu öğe yalnızca bilgisayarınızda o anda çalışan bir tarama olması durumunda görüntülenir. Bunun ardından, bu tarama için taramanın önceliğini ayarlayabilir, alternatif olarak çalışan taramayı durdurabilir veya duraklatabilirsiniz. Su işlemlere de erişilebilir: *Tüm taramalar için öncelikli ayarla, Tüm taramaları duraklat veya Tüm taramaları durdur.*
- **PC Analyzer'i çalıştır** - PC Analyzer bileşenini başlatmak için tıklayın.



- **Hesabim** - Abonelik ürünlerinizi yönetebileceğiniz, ilave koruma satın alabileceğiniz, yükleme dosyalarını indirebileceğiniz, geçmiş sipariş ve faturalarınızı kontrol edebileceğiniz ve kişisel bilgilerinizi yönetebileceğiniz Hesabim ana sayfasını açar.
- **Simdi Güncelle** - anında [güncelleme işlemi başlatır](#).
- **Yardım** - başlangıç sayfasında yardım dosyasını açar.

## 5.7. AVG Aracı

**AVG aracı** i Windows masaüstünde görüntülenir (*Windows Kenar Çubuğu*). Bu uygulama yalnızca Windows Vista ve Windows 7/8 işletim sistemlerinde desteklenir. **AVG aracı** en önemli **AVG Internet Security 2013** işlemlerine, yani [taramaya](#) ve [güncellemeye](#) hemen erişim sağlar:



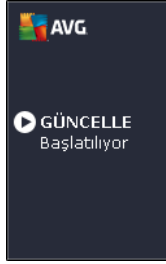
### AVG araç kontrolleri



Gerek olması durumunda, AVG aracı bir tarama veya güncellemeyi hemen başlatabilmenizi sağlar; ayrıca popüler sosyal paylaşım ağlarına hızlı bağlantılar ve hızlı arama seçenekleri de sunar:

- **Simdi tara - tüm bilgisayarın taranmasını** doğrudan başlatmak için [Simdi tara](#) bağlantısını tıklatın. Tarama ilerlemesini aracın 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 basurun. Bu iletişim kutusu, **Ayrıntıları göster** seçeneği aracılığıyla doğrudan araç üzerinden açılabilir (*ilgili tarama sonuçları Kenar çubuğu aracı taraması*) altında listelenir.



- **Simdi güncelle** - güncellemesini doğrudan araç içerisinde başlatmak için **Simdi güncelle** AVG Internet Security 2013 bağlantısını tıklatın:

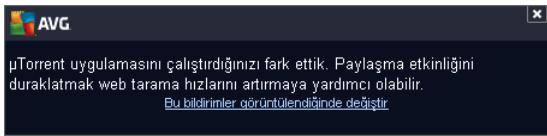


- **Twitter bağlantısı**  - Twitter'da gönderilen en son AVG yayınlarının genel görünümünü sunan yeni bir **AVG aracı** arayüzü açar. İnternet tarayicinizi yeni bir pencerede açmak için, **AVG Twitter yayınlarının tümünü görüntüle** bağlantısını izleyin, böylece doğrudan Twitter web sitesine, özellikle de AVG ile ilgili haberler için atanan sayfaya yönlendirilirsiniz.
- **Facebook bağlantısı**  - internet tarayicinizi Facebook web sitesinde, özellikle de **AVG topluluğu** sayfasında açar.
- **Arama kutusu** - bir anahtar kelime yazın ve varsayılan web tarayicinizde yeni açılan bir pencerede arama sonuçlarını hemen alın.

## 5.8. AVG Tavsiyesi

**AVG Tavsiyesi** bilgisayarınızı yavaşlatabilecek veya riske atabilecek sorunları tespit etmek ve durumu çözecek bir işlem önermek üzere tasarlanmıştır. Bilgisayarda ani bir yavaşlama yaşarsanız (*internet tarama, genel performans*), sorunun kaynağı ve dolayısıyla çözüm yolu genellikle çok net değildir. Bu durumda yardıma **AVG Tavsiyesi** yetisir. Sorunun ne olabileceği ve çözüm önerilerine yönelik bir bilgilendirmeyi sistem tepsisinde gösterir. **AVG Tavsiyesi** bilgisayarınızdaki çalışan tüm işlemleri olası sorunlara karşı sürekli izler ve sorunları engellemeye yönelik ipuçları önerir.

**AVG Tavsiyesi** sistem tepsisi üzerinde beliren bir açılır pencere olarak görülebilir:



**AVG Tavsiyesi** özellikle aşağıdaki durumları izler:

- **O anda açık web tarayıcılarının durumu.** Web tarayıcıları belleği asırı yükleyebilir, özellikle de belirli bir süre birden fazla sekme veya pencere açılmışsa, ve çok fazla sistem kaynağı tüketir (örn. bilgisayarınızı yavaşlatır). Böyle bir durumda web tarayıcısının yeniden başlatılması genellikle işe yarar.
- **Esler Arası bağlantıları çalıştırma.** Dosya paylaşımı için P2P protokolü kullanıldıktan sonra, bağlantı bazen etkin kalarak belirli miktarda bant genişliğini kullanır. Bunun sonucunda web taramasında yavaşlama görebilirsiniz.
- **Tanidik ada sahip bilinmeyen ağ.** Bu durum yalnızca, genellikle taşınabilir bilgisayarlar kullanıp birçok ağa bağlanan kullanıcılar için geçerlidir. Yeni, bilinmeyen bir ağ iyi bilinen, sık kullanılan bir ağla aynı ada sahipse (örn. Ev veya Wifi), karışıklık meydana gelebilir ve yanlışlıkla hiç bilinmeyen ve muhtemelen güvenli olmayan bir ağa bağlanabilirsiniz. **AVG**



**Tavsiyesi** bilinen adın aslında yeni bir ağa ait olduğu uyarısıyla bu durumu engelleyebilir. Tabii ki, bilinmeyen ağın güvenli olduğuna karar verirseniz, bunu bir **AVG Tavsiyesi** bilinen ağlar listesine kaydedebilirsiniz, böylece ağ ileride tekrar rapor edilmez.

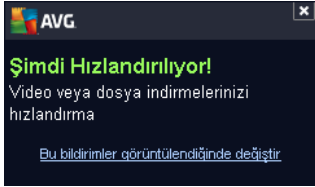
Bu durumların her birinde, **AVG Advisor** gerçekleştirebilecek olası sorunlar hakkında sizi uyarır ve çakışan işlem veya uygulamanın adını ve simgesini gösterir. Ayrıca, **AVG Advisor** olası sorunları engellemek için yapılması gerekenler hakkında önerilerde bulunur.

### Desteklenen web tarayıcıları

Özelligin çalıştığı web tarayıcıları: Internet Explorer, Chrome, Firefox, Opera, Safari.

## 5.9. AVG Hızlandırıcı

**AVG Accelerator** daha düzgün çevrimiçi video oynatmaya izin verir ve ilave indirmeleri daha kolay hale getirir. Video hızlandırma işlemi çalışırken sistem tepsisi açılır penceresi ile bilgilendirilirsiniz.





## 6. AVG Bileşenleri

### 6.1. Bilgisayar

**Bilgisayar** bileşeni iki temel güvenlik hizmetini kapsar: **Virüslerden Koruma** ve **Anti-Rootkit**.


- **Virüslerden Koruma** tüm dosyaları, bilgisayarın sistem alanlarını ve çıkarılabilir ortamları (*flash disk vb.*) koruyan bir tarama motoru barındırır. ve bilinen virüslere karşı tarama yapar. Tespit edilen virüsler, harekete geçmeden engellenecek ve ardından silinecek ya da [Virüs Kasası](#)'nda karantinaya alınacaktır. Yerleşik koruma "arkaplanda" çalıştığından işlemin farkına bile varmazsınız. Virüslerden Koruma dosyaların tipik virüs özelliklerine karşı tarandığı bulusal analiz taraması da kullanır. Bu, yeni bir virüs mevcut virüslerin tipik özelliklerinden bazılarını sahipse Virüslerden Koruma bileşeninin yeni ve bilinmeyen bir virüsü tespit edebileceği anlamına gelmektedir. **AVG Internet Security 2013** sistem içinde potansiyel olarak istenmeyen statüsündeki çalıştırılabilir uygulamalar ve DLL kitaplıklarını da analiz ve tespit eder (*çeşitli türlerde casus yazılım, reklam yazılımı vb.*). Virüslerden Koruma buna ek olarak, sistem kayıt defterinizi şüpheli girdilere ve geçici internet dosyalarına karşı da tarar ve söz konusu potansiyel olarak istenmeyen nesnelere de diğer buluşmalarla aynı şekilde tedavi etmenizi sağlar.
- **Anti-Rootkit** tehlikeli kök dizinleri, diğer bir deyişle bilgisayarınızdaki tehlikeli yazılımları gizleyen program ve teknolojileri etkili bir biçimde tespit edip silen özel bir araçtır. Kök dizin, sistem yöneticisinin izni olmaksızın yasal olmayan şekilde bilgisayar sisteminin kontrolünü ele almak için tasarlanmış bir programdır. Anti-Rootkit öntanımlı kurallar setine göre kök dizinleri algılayabilir. Anti-Rootkit bir kök dizini bulduğunda, bu kök dizinde mutlaka virüs olduğu anlamına gelmez. Bazen kök dizinler sürücülerde kullanılır ya da doğru uygulamaların bir parçası olabilir.





### İletişim kutusu kontrolleri





İletişim kutusunun iki bölümü arasında geçiş yapmak için ilgili hizmet panelinde herhangi bir yeri tıklatabilirsiniz. Bu durumda panel açık mavi bir tonda vurgulanır. İletişim kutusunun her iki bölümünde de aşağıdaki kontrolleri bulabilirsiniz. Bu veya su güvenlik servisine ait olmasından bağımsız olarak işlevleri aynıdır (*Virüslerden Koruma* veya *Anti-Rootkit*):

 **Etkin / Devre dışı** - Düğme size hem görünüş hem de işlev olarak trafik işiklerini hatırlatmış olabilir. İki konum arasında geçiş yapmak için tek tıklatın. Yeşil renk **Etkin**, yani Virüslerden Koruma güvenlik hizmetinin aktif ve tamamen çalışır durumda olduğu anlamına gelmektedir. Kırmızı renk ise **Devre dışı** durumunu temsil etmektedir; yani hizmet devre dışı bırakılmıştır. Hizmeti devre dışı bırakmak için iyi bir nedeniniz yoksa, tüm güvenlik yapılandırması için varsayılan ayarları kesinlikle değiştirmenizi öneririz. Varsayılan ayarlar uygulama için en iyi performansı ve sizin için de maksimum güvenliği sağlar. Belirli bir nedenle hizmeti devre dışı bırakmak istiyorsanız, kırmızı renkli **Uyarı** işareti ve o anda tam olarak korunmadığınız bilgisayarı olası riskler hakkında hemen uyarılırsınız. **Hizmeti mümkün olan en kısa sürede tekrar etkinleştirmeyi lütfen unutmayın!**

 **Ayarlar** - Düğmeyi tıklatarak [gelmiş ayarlar](#) arayüzüne gidebilirsiniz. Tam olarak, ilgili iletişim kutusu açılır ve siz de burada [Virüslerden Koruma](#) veya [Anti-Rootkit](#) gibi seçtiğiniz bir hizmetin yapılandırmasını yapabilirsiniz. Gelişmiş ayarlarda **AVG Internet Security 2013** uygulamasındaki tüm güvenlik hizmetlerinin yapılandırmasını düzenleyebilirsiniz, ancak yapılandırma işlemi yalnızca deneyimli kullanıcılara önerilmektedir!

 **İstatistikler** - Düğmeyi tıklatarak AVG web sitesinde özel olarak hazırlanmış bir sayfaya gidebilirsiniz (<http://www.avg.com/>). Bu sayfada belirli bir zaman diliminde ve toplam olarak bilgisayarınızda gerçekleştirilen tüm **AVG Internet Security 2013** etkinliklerine ayrıntılı bir istatistiksel genel bakış bulabilirsiniz.

 **Ayrıntılar** - Düğmeyi tıklattığınızda vurgulanan hizmetin kısa bir açıklaması iletişim kutusunun alt kısmında görüntülenir.

 - Bileşen genel bilgilerinin bulunduğu [ana kullanıcı arayüzüne](#) dönmek için iletişim kutusunun sol üst kısmında bulunan yeşil oku kullanın.

Anti-Rootkit bölümünde, bağımsız bir kök dizin taramasını doğrudan başlatabileceğiniz bir **Kök dizinleri tara** düğmesi de bulabilirsiniz (*ancak, kök dizin taraması [Tüm bilgisayar taraması](#) dahilinde gerçekleştirilen bir işlemdir*).

## 6.2. Web Tarama

**Web tarama koruması** iki hizmetten oluşur: **LinkScanner Sörf Kalkanı** ve **Online Shield**:

- **LinkScanner Sörf Kalkanı** 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 Sörf Kalkanı sunucu platformları korumasında kullanılmak için tasarlanmamıştır!**
- **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 tanıyıp ve bilgisayarınıza girişini engellemek için indirme işlemini durdurur. Bu güçlü koruma, açmaya çalıştığınız web sayfalarının kötü amaçlı içeriğini engeller ve bilgisayarınıza karsıdan 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. Virüs bulmuş web sayfalarını ziyaret ettiğinizde bilgisayarınıza kolayca virüs bulabileceğini gerçeğini hatırlamak çok önemlidir. **Online Shield'in sunucu platformlarının korunmasında kullanılması hedeflenmemiştir!**



## İletişim kutusu kontrolleri


İletişim kutusunun iki bölümü arasında geçiş yapmak için ilgili hizmet panelinde herhangi bir yeri tıklatabilirsiniz. Bu durumda panel açık mavi bir tonda vurgulanır. İletişim kutusunun her iki bölümünde de aşağıdaki kontrolleri bulabilirsiniz. Bu veya su güvenlik servisine ait olmasından bağımsız olarak işlevleri aynıdır (*LinkScanner Sörf Kalkanı* veya *Online Shield*):


 **Etkin / Devre dışı** - Düğme size hem görünüş hem de işlev olarak trafik işiklerini hatırlatmış olabilir. İki konum arasında geçiş yapmak için tek tıklatın. Yeşil renk **Etkin**, yani LinkScanner Sörf Kalkanı / Online Shield güvenlik hizmetinin aktif ve tamamen çalışır durumda olduğu anlamına gelmektedir. Kırmızı renk ise **Devre dışı** durumunu temsil etmektedir; yani hizmet devre dışı bırakılmıştır. Hizmeti devre dışı bırakmak için iyi bir nedeniniz yoksa, tüm güvenlik yapılandırması için varsayılan ayarları kesinlikle değiştirmenizi öneririz. Varsayılan ayarlar uygulama için en iyi performansı ve sizin için de maksimum güvenliği sağlar. Belirli bir nedenle hizmeti devre dışı bırakmak istiyorsanız, kırmızı renkli **Uyarı** isareti ve o anda tam olarak korunmadığınız bilgisayarı olası riskler hakkında hemen uyarılırsınız. **Hizmeti mümkün olan en kısa sürede tekrar etkinleştirmeyi lütfen unutmayın!**


 **Ayarlar** - Düğmeyi tıklatarak [gelmiş ayarlar](#) arayüzüne gidebilirsiniz. Tam olarak, ilgili iletişim kutusu açılır ve siz de burada [LinkScanner Sörf Kalkanı](#) veya [Online Shield](#) gibi



seçtiğiniz bir hizmetin yapılandırmasını yapabilirsiniz. Gelişmiş ayarlarda **AVG Internet Security 2013** uygulamasındaki tüm güvenlik hizmetlerinin yapılandırmasını düzenleyebilirsiniz, ancak yapılandırma işlemi yalnızca deneyimli kullanıcılara önerilmektedir!

 **İstatistikler** - Düğmeyi tıklatarak AVG web sitesinde özel olarak hazırlanmış bir sayfaya gidebilirsiniz (<http://www.avg.com/>). Bu sayfada belirli bir zaman diliminde ve toplam olarak bilgisayarınızda gerçekleştirilen tüm **AVG Internet Security 2013** etkinliklerine ayrıntılı bir istatistiksel genel bakış bulabilirsiniz.

 **Ayrıntılar** - Düğmeyi tıklattığınızda vurgulanan hizmetin kısa bir açıklaması iletişim kutusunun alt kısmında görüntülenir.

 - Bileşen genel bilgilerinin bulunduğu [ana kullanıcı arayüzüne](#) dönmek için iletişim kutusunun sol üst kısmında bulunan yeşil oku kullanın.

### 6.3. Kimlik


**Identity protection** bileşeni **Identity Shield** hizmeti internette dijital varlıklarınızı yeni ve bilinmeyen tehditlere karşı sürekli olarak korur:


- **Identity Protection** kötü amaçlı yazılımlara karşı koruma hizmetidir, davranış teknolojilerini kullanarak ve yeni virüsler için ilk günden koruma sağlayarak sizi her türlü kötü amaçlı yazılımlardan (*casus yazılım, robotlar, kimlik hırsızlığı...*) korur. Identity Protection, PC'nizdeki parolalarınızı, banka hesabı ayrıntılarınızı, kredi kartı numaralarınızı ve diğer kişisel dijital bilgilerinizi tüm kötü amaçlı yazılımlarla (*kötü amaçlı yazılım*) çalan kimlik hırsızlığı üzerine odaklanmıştır. Bilgisayarınızda ve paylaşılan ağınızda çalışan tüm programların düzgün biçimde çalışmasını sağlar. Identity Protection, sürekli olarak şüpheli davranışları belirleyip engeller ve tüm yeni kötü amaçlı yazılımlara karşı bilgisayarınızı korur. Identity Protection, yeni ve hatta bilinmeyen tehlikelere karşı bilgisayarınıza gerçek zamanlı bir koruma sağlar. Tüm işlemleri (*gizli olanlar da dahil*) ve *285 üzerinde farklı davranış modelini izler ve sisteminizle ilgili kötü amaçlı herhangi bir durum meydana gelip gelmediğini belirleyebilir*. Bu nedenle, virüs veritabanında henüz açıklanmamış tehditleri bile açığa çıkarabilir. Bilgisayarınıza bilinmeyen bir kod gelirse söz konusu kod kötü amaçlı davranışlara karşı hemen gözlenir ve izlenir. Dosyanın kötü amaçlı olduğu tespit edilirse, Identity Protection kodu **Virüs Kasası**'na kaldırır ve sistemde yapılan tüm değişiklikleri (*kod bulaşmaları, kayıt defteri değişiklikleri, bağlantı noktası açma vb.*) geri alır. Korunmak için tarama başlatmanız gerekmez. Bu teknoloji çok öngörülüdür, nadiren güncellemeye gereksinim duyar ve her an korur.





## İletişim kutusu kontrolleri

İletişim kutusunda bulabileceğiniz kontroller:

 **Etkin / Devre dışı** - Düğme size hem görünüş hem de işlev olarak trafik isiklerini hatırlatmış olabilir. İki konum arasında geçiş yapmak için tek tıklatın. Yeşil renk **Etkin**, yani Identity Protection güvenlik hizmetinin aktif ve tamamen çalışır durumda olduğu anlamına gelmektedir. Kırmızı renk ise **Devre dışı** durumunu temsil etmektedir; yani hizmet devre dışı bırakılmıştır. Hizmeti devre dışı bırakmak için iyi bir nedeniniz yoksa, tüm güvenlik yapılandırması için varsayılan ayarları kesinlikle değiştirmenizi öneririz. Varsayılan ayarlar uygulama için en iyi performansı ve sizin için de maksimum güvenliği sağlar. Belirli bir nedenle hizmeti devre dışı bırakmak istiyorsanız, kırmızı renkli **Uyarı** isareti ve o anda tam olarak korunmadığınız bilgisıyla olası riskler hakkında hemen uyarılırsınız. **Hizmeti mümkün olan en kısa sürede tekrar etkinleştirmeyi lütfen unutmayın!**

 **Ayarlar** - Düğmeyi tıklatarak [gelişmiş ayarlar](#) arayüzüne gidebilirsiniz. Tam olarak, ilgili iletişim kutusu açılır ve siz de burada [Identity Protection](#) gibi seçtiğiniz bir hizmetin yapılandırmasını yapabilirsiniz. Gelişmiş ayarlarda **AVG Internet Security 2013** uygulamasındaki tüm güvenlik hizmetlerinin yapılandırmasını düzenleyebilirsiniz, ancak yapılandırma işlemi yalnızca deneyimli kullanıcılara önerilmektedir!

 **Ayrıntılar** - Düğmeyi tıklattığınızda vurgulanan hizmetin kısa bir açıklaması iletişim kutusunun alt kısmında görüntülenir.

 - Bilesen genel bilgilerinin bulunduğu [ana kullanıcı arayüzüne](#) dönmek için iletişim kutusunun sol üst kısmında bulunan yeşil oku kullanın.

Ne yazık ki, **AVG Internet Security 2013** uygulamasında Identity Alert hizmeti yer almamaktadır. Bu koruma türünü kullanmak istiyorsanız, **Etkinleştirme için Yükselt** düğmesini kullanarak Identity Alert lisansı satın alabileceğiniz web sayfasına gidebilirsiniz.



AVG Premium Security sürümlerinde dahi Identity Alert hizmetinin su anda yalnızca ABD, Birleşik Krallık, Kanada ve İrlanda bölgelerinde sunulduğunu lütfen aklınızda bulundurun.

## 6.4. E-postalar


**E-posta koruması** bileşeni iki güvenlik hizmetini kapsar: **E-posta Tarayıcısı** ve **Anti-Spam**:

- **E-posta Tarayıcısı**: Virüsler ve truva atları yaygın olarak e-postalar aracılığıyla yayılır. Kimlik avı 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 teknolojilerine sahip olmaları nedeniyle*) ev kullanıcıları büyük çoğunlukla söz konusu e-postaları kullanır. Bunun yanı sıra, bilmedikleri sitelerde dolan 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 anti-spam filtrelerinden yararlanmaktadır. E-posta Koruması bileşeni, alınan veya gönderilen her e-posta iletilisini taramakla sorumludur. Bir e-postada virüs tespit edildiğinde, hemen [Virüs Kasası](#)'na kaldırır. Söz konusu bileşen belirli türde e-posta eklerini filtreleyebilir ve virüs bulunmayan iletilere bir onay metni ekleyebilir. **E-posta Tarayıcısı'nın sunucu platformlarında kullanılması hedeflenmemiştir!**
- **Anti-Spam** gelen tüm e-posta mesajlarını kontrol eder ve istenmeyen e-postaları spam olarak işaretler (*Spam, ürün veya hizmet reklamı yapmak amacıyla bir kerede çok sayıda e-posta adresine toplu olarak gönderilen ve kullanıcıların posta kutularını dolduran istenmeyen e-postalardır. İstenmeyen posta, müşterinin kendi isteğiyle almayı kabul ettiği yasal ticari e-posta anlamına gelmez..* Anti-Spam özel metin dizesi ekleyerek e-postanın konusunu değiştirebilir (*istenmeyen posta olarak tanımlanır*). Böylece, e-posta istemcinize göre e-postalarınızı filtreleyebilirsiniz. Anti-Spam bileşeni, her e-posta iletilisini işlemek için çeşitli analiz yöntemleri kullanır ve istenmeyen e-postaları karşı mümkün olan en üst seviyede koruma sağlar. Anti-Spam istenmeyen postayı algılamak için düzenli olarak güncellenen veritabanı kullanır. [RBL sunucularını](#) ("*bilinen istenmeyen posta göndericisi*") e-posta adreslerinden oluşan genel veritabanları kullanmak ve [Beyaz listenize](#) (*hiçbir zaman spam olarak işaretleme*) ve [Kara listenize](#) (*her zaman spam olarak işaretleme*) manuel olarak e-posta adresleri eklemek de mümkündür.





## İletişim kutusu kontrolleri

İletişim kutusunun iki bölümü arasında geçiş yapmak için ilgili hizmet panelinde herhangi bir yeri tıklatabilirsiniz. Bu durumda panel açık mavi bir tonda vurgulanır. İletişim kutusunun her iki bölümünde de aşağıdaki kontrolleri bulabilirsiniz. Bu veya su güvenlik servisine ait olmasından bağımsız olarak işlevleri aynıdır (*E-posta Tarayıcısı* veya *Anti-Spam*):

 **Etkin / Devre dışı** - Düğme size hem görünüş hem de işlev olarak trafik ışıklarını hatırlatmış olabilir. İki konum arasında geçiş yapmak için tek tıklatın. Yeşil renk **Etkin**, yani güvenlik hizmetinin aktif ve tamamen çalışır durumda olduğu anlamına gelmektedir. Kırmızı renk ise **Devre dışı** durumunu temsil etmektedir; yani hizmet devre dışı bırakılmıştır. Hizmeti devre dışı bırakmak için iyi bir nedeniniz yoksa, tüm güvenlik yapılandırması için varsayılan ayarları kesinlikle değiştirmenizi öneririz. Varsayılan ayarlar uygulama için en iyi performansı ve sizin için de maksimum güvenliği sağlar. Belirli bir nedenle hizmeti devre dışı bırakmak istiyorsanız, kırmızı renkli **Uyarı** işareti ve o anda tam olarak korunmadığınız bilgisıyla olası riskler hakkında hemen uyarılırsınız. **Hizmeti mümkün olan en kısa sürede tekrar etkinleştirmeyi lütfen unutmayın!**


E-posta Tarayıcısı bölümünde iki adet "trafik ışığı" düğmesi görebilirsiniz. Bu sayede E-posta Tarayıcısı'nın gelen, giden veya hem gelen hem de giden mesajları tarayıp taramamasını ayrı ayrı belirleyebilirsiniz. Varsayılan olarak, tarama gelen e-postalar için açık, ancak bulasma riski düşük olduğundan giden postalar için kapalıdır.


 **Ayarlar** - Düğmeyi tıklatarak [gelişmiş ayarlar](#) arayüzüne gidebilirsiniz. Tam olarak, ilgili iletişim kutusu açılır ve siz de burada [E-posta Tarayıcısı](#) veya [Anti-Spam](#) gibi seçtiğiniz bir hizmetin yapılandırmasını yapabilirsiniz. Gelişmiş ayarlarda **AVG Internet Security 2013** uygulamasındaki tüm güvenlik hizmetlerinin yapılandırmasını düzenleyebilirsiniz, ancak yapılandırma işlemi yalnızca deneyimli kullanıcılara önerilmektedir!

 **İstatistikler** - Düğmeyi tıklatarak AVG web sitesinde özel olarak hazırlanmış bir sayfaya gidebilirsiniz (<http://www.avg.com/>). Bu sayfada belirli bir zaman diliminde ve toplam olarak



bilgisayarınızda gerçekleştirilen tüm **AVG Internet Security 2013** etkinliklerine ayrıntılı bir istatistiksel genel bakış bulabilirsiniz.

 **Ayrıntılar** - Düğmeyi tıklattığınızda vurgulanan hizmetin kısa bir açıklaması iletişim kutusunun alt kısmında görüntülenir.

 - Bileşen genel bilgilerinin bulunduğu [ana kullanıcı arayüzüne](#) dönmek için iletişim kutusunun sol üst kısmında bulunan yeşil oku kullanın.

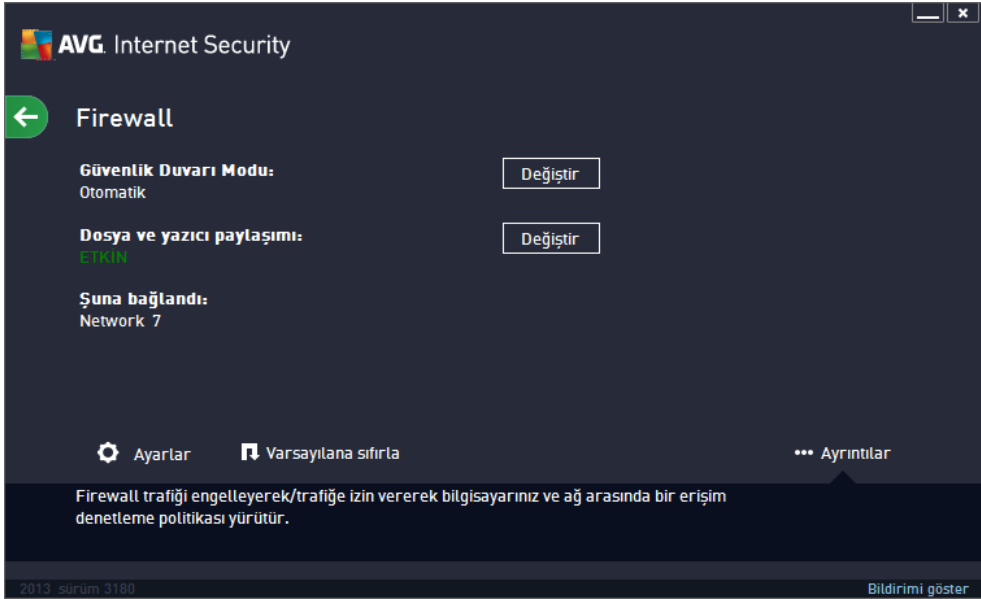
## 6.5. Güvenlik Duvarı

**Firewall**, trafiği engellemek/izin vermek suretiyle iki ya da daha fazla ağ arasında gerçekleşen erişimi kontrol eden bir sistemdir. Firewall dahili ağı *disarıdan (genellikle internetten)* kaynaklanan saldırılara karşı koruyan bir dizi kural içerir ve ağ bağlantı noktalarının her birinde gerçekleşen iletişimi kontrol eder. İletişim tanımlanan kurallar doğrultusunda değerlendirilir ve ardından söz konusu işleme izni verilir ya da engellenir. Firewall sisteme yetkisiz girilmeye çalışıldığını tespit ederse söz konusu teşebbüsü "engeller" ve söz konusu kişinin bilgisayarınıza erişimini engeller. Firewall, tanımlı yazılım uygulamaları için ve tanımlanan bağlantı yuvaları üzerinden dahili/harici iletişime (*her iki yönde, giriş ve çıkış*) izin vermek ya da engellemek üzere yapılandırılır. Örneğin, güvenlik duvarı, Microsoft Explorer kullanılarak sadece içeri ve dışarı veri akışına izin verecek şekilde de yapılandırılabilir. Diğer web tarayıcıları tarafından web verilerini aktarmaya yönelik teşebbüsler engellenecektir. Kişisel açıdan tanımlanabilir verilerin sizin izniniz olmaksızın bilgisayarınızdan gönderilmesini engeller. Bilgisayarın internet ya da yerel ağ üzerinden diğer bilgisayarlarla yaptığı veri değişimini kontrol eder. Firewall kurumlarda ağa bağlı diğer bilgisayarları tek bir bilgisayar tarafından ortaya konan saldırılara karşı da korur.

**AVG Internet Security 2013** uygulamasında **Firewall** bilgisayarındaki her ağ bağlantı noktasının trafiğini kontrol eder. Firewall, tanımlanan kurallara bağlı olarak hem bilgisayarınızda çalışan (*ve internet/yerel ağ yoluyla bağlanmak isteyen*) uygulamaları hem de bilgisayarınıza bağlanmayı deneyerek dışarıdan bilgisayarınıza girmeye çalışan uygulamaları değerlendirir. Firewall bu uygulamaların her biri için ağ bağlantı noktaları üzerinde iletişime izin verir ya da iletişimi yasaklar. Varsayılan olarak, uygulama bilinmiyorsa (*diğer bir deyişle, Firewall kuralları tanımlanmamış*), Firewall iletişim girişimine izin vermek veya girişimi engellemek isteyip istemediğinizi soracaktır.

**AVG Firewall bileşeninin sunucu platformlarının korunmasında kullanılması hedeflenmemiştir!**

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



## Mevcut Firewall modları

Firewall, bilgisayarınızın bir alanda bulunmasına, bağımsız bir bilgisayar veya bir dizüstü bilgisayar olmasına bağlı olarak özel güvenlik kuralları tanımlamanıza olanak tanır. Bu seçeneklerin her biri için farklı bir koruma seviyesi gerekir ve bu seviyeler de ilgili modların kapsamındadır. Kısaca, Firewall modu Firewall bileşeni için özel bir yapılandırma ve bu şekilde önceden tanımlanmış çok sayıda yapılandırmayı kullanabilirsiniz.

- **Otomatik** - Bu modda Firewall tüm ağ trafiğini otomatik olarak denetler. Hiçbir karar için onayınız istenmez. Firewall bilinen tüm uygulamalarla bağlantıya izin verir ve aynı zamanda uygulamaya her zaman bağlanabilmesi için bir kural oluşturulur. Firewall, diğer uygulamalar için uygulamanın davranışına bağlı olarak uygulamaya yönelik izin veya engelleme kararı verir. Ancak, böyle durumlarda kural oluşturulmaz ve uygulama her bağlanmaya çalışıldığında kontrol edilir. Otomatik mod arka planda dikkat çekmeden çalışır ve çoğu kullanıcı için önerilen moddur.
- **İnteraktif** - bilgisayarınızda gelen ve giden tüm ağ trafiğini tam olarak kontrol etmek istiyorsanız bu mod kullanışlıdır. Firewall trafiği sizin için izler ve tüm iletişim ve veri aktarım girişimlerinden sizi haberdar ederek girişimi uygun gördüğünüz biçimde engelleme veya izin vermenizi sağlar. Yalnızca ileri düzey kullanıcılar için önerilir.
- **İnternet erişimini engelle** - internet bağlantısı tamamen engellenir, internete erişemezsiniz ve dışarıdan hiç kimse de bilgisayarınıza erişemez. Yalnızca özel ve kısa süreli kullanım içindir.
- **Güvenlik duvarı korumasını kapat** - Firewall korumasının devre dışı bırakılması bilgisayarınızda gelen ve giden tüm trafiğe izin verir. Sonuç olarak, bilgisayarınız hacker saldırılarına açık hale gelir. Lütfen bu seçeneği kullanırken çok dikkatli olun.

Not: Firewall içinde de bir otomatik mod mevcuttur. Bu mod, [Bilgisayar](#) veya [Identity protection](#) bileşeni kapatıldığında ve bu nedenle bilgisayarınız tehditlere açık hale geldiğinde sessizce etkinleştirilir. Bu tür durumlarda, Firewall yalnızca bilinen veya kesinlikle güvenli uygulamalara



otomatik olarak izin verir. Diğer tüm uygulamalar için sizin karar vermeniz istenir. Bunun nedeni devre dışı bırakılan bileşenlerin boşluğunu kapatmak ve bilgisayarınızı güvende tutmaktır.


## İletişim kutusu kontrolleri


Bu iletişim kutusu Firewall bileşen durumu hakkındaki temel bilgileri gösterir:


- **Güvenlik Duvarı Modu** - Geçerli olarak seçili Firewall modu hakkındaki bilgileri gösterir. Geçerli modu bir başka moda değiştirmek istiyorsanız, gösterilen bilginin yanındaki **Değiştir** düğmesini kullanarak [Firewall ayarları](#) arayüzüne geçebilirsiniz (*Firewall profillerinin açıklamaları ve öneriler için lütfen önceki paragrafta bakın*).
- **Dosya ve yazıcı paylaşımı** - O anda dosya veya yazıcı paylaşımına (*her iki yönde de*) izin verip verilmediği bilgisini gösterir. Dosya ve yazıcı paylaşımı Windows, ortak disk birimleri, yazıcılar, tarayıcılar ve tüm benzer cihazlarda "Paylaşılan" olarak işaretlediğiniz tüm dosyalar veya klasörler anlamına gelmektedir. Bu tür öğelerin paylaşımı yalnızca güvenli olduğu düşünülen ağlarda gerçekleştirilmelidir (*örneğin evde, iste veya okulda*). Ancak, herkese açık ağlara (*havaalanı Wi-Fi veya internet kafe ağı gibi*) bağlanıyorsanız, hiçbir şey paylaşmak istemeyebilirsiniz.
- **Suna bağlandı** - Geçerli olarak bağlı olduğunuz ağın adıyla ilgili bilgileri gösterir. Windows XP'de, ağ adı ilgili ağa ilk bağlandığınızda ağ için seçtiğiniz adlandırmaya karşılık gelir. Windows Vista ve üstü sistemlerde, ağ adı Ağ ve Paylaşım Merkezi'nden otomatik olarak alınır.


İletişim kutusunun kontrolleri:

**Değiştir** - Bu düğme ilgili parametrenin durumunu değiştirmenizi sağlar. Değiştirme işleminin ayrıntıları için lütfen yukarıdaki paragrafta ilgili parametrenin açıklamasına bakın.

 **Ayarlar** - Bu düğmeyi tıklayarak [Firewall ayarları](#) arayüzüne geçip tüm Firewall yapılandırmasını düzenleyebilirsiniz. Tüm yapılandırma işlemleri, sadece deneyimli kullanıcılar tarafından yapılmalıdır.

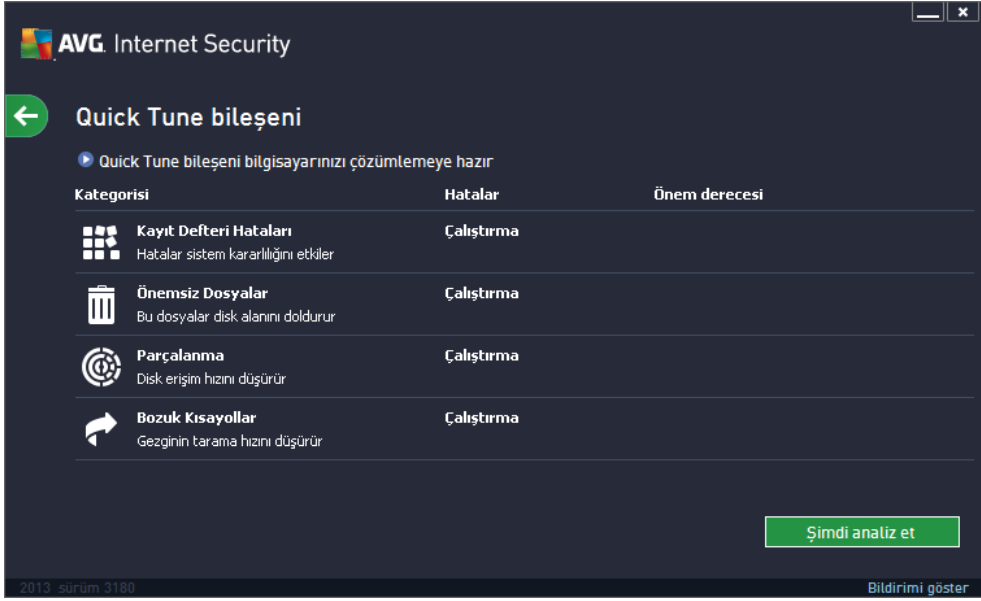
 **Varsayılanla sıfırla** - Geçerli Firewall yapılandırmasının üzerine yazmak ve otomatik tespite bağlı olarak varsayılan yapılandırmaya geri dönmek için bu düğmeye basın.

 **Ayrıntılar** - Düğmeyi tıklattığınızda vurgulanan hizmetin kısa bir açıklaması iletişim kutusunun alt kısmında görüntülenir.

 - Bileşen genel bilgilerinin bulunduğu [ana kullanıcı arayüzüne](#) dönmek için iletişim kutusunun sol üst kısmında bulunan yeşil oku kullanın.

## 6.6. Quick Tune

**Quick Tune** bileşeni, bilgisayarınızın hızının ve genel performansının nasıl iyileştirilebileceğine yönelik ayrıntılı sistem analizi ve düzeltme işlemi için gelişmiş bir araçtır:



Su kategoriler analiz edilebilir ve onarılabilir: kayıt defteri hataları, istenmeyen dosyalar, parçalama ve bozuk kısayollar:

- **Kayıt Defteri Hataları** bilgisayarınızı yavaşlatıyor olması veya hata mesajlarının görüntülenmesine neden olması muhtemel Windows Kayıt Defteri'ndeki hataların sayısını verir.
- **İstenmeyen Dosyalar** disk alanınızı kullanan ve silinebilecek dosyaların sayısını verir. Normal olarak, bunlar çeşitli türlerde geçici dosyalar ve Geri Dönüşüm Kutusundaki dosyalar olabilir.
- **Bölümlendirme**, bölümlendirilmiş, başka bir deyişle, fiziksel diskin farklı parçalarına dağıtılmış dosyaların sabit diskteki yüzdesini hesaplar.
- **Bozuk kısayollar** artık çalışmayan ve var olmayan konumlara yönlendiren vs. kısayolları bulur.

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



The screenshot shows the AVG Internet Security Quick Tune bileşeni window. The window title is "AVG. Internet Security". The main heading is "Quick Tune bileşeni". Below the heading, there is a green checkmark icon and the text "Quick Tune bileşeni incelemeyi tamamladı". The window displays a table with three columns: "Kategori", "Hatalar", and "Önem derecesi". The table contains four rows of data:

Kategori	Hatalar	Önem derecesi
 <b>Kayıt Defteri Hataları</b> Hatalar sistem kararlılığını etkiler	<b>103 hata bulundu</b> <a href="#">Ayrıntılar...</a>	
 <b>Önemsiz Dosyalar</b> Bu dosyalar disk alanını doldurur	<b>448 hata bulundu</b> <a href="#">Ayrıntılar...</a>	
 <b>Parçalanma</b> Disk erişim hızını düşürür	<b>13% parçalanmış</b> <a href="#">Ayrıntılar...</a>	
 <b>Bozuk Kısayollar</b> Gezginin tarama hızını düşürür	<b>21 hata bulundu</b> <a href="#">Ayrıntılar...</a>	

At the bottom right of the window, there is a green button labeled "Şimdi onar". At the bottom left, it says "2013 sürüm 3180". At the bottom right, it says "Bildirim göster".

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

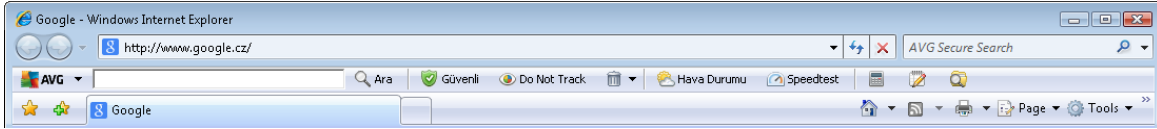
### Kontrol düğmeleri

- **Şimdi analiz et** (analiz başlamadan önce görüntülenir) - bilgisayarınızın analiz işlemini hemen başlatmak için bu düğmeye basın
- **Şimdi onar** (analiz sona erdiğinde görüntülenir) - bulunan tüm hataları onarmak için düğmeye basın. Düzeltme işlemi bittiginde sonuçla ilgili bir genel görünüm alırsınız.
- **İptal** - analizin çalışmasını durdurmak veya analiz tamamlandıktan sonra varsayılan [AVG ana iletişim kutusuna](#) (bileşenler genel görünümüne) geri dönmek için bu düğmeye basın



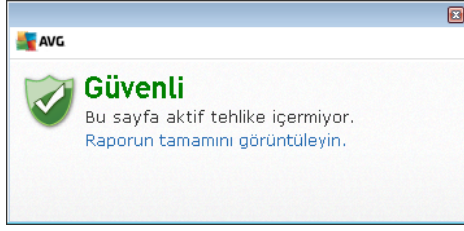
## 7. AVG Security Toolbar

**AVG Security Toolbar**, LinkScanner Sörf Kalkanı bileşeni ile siki bir entegrasyon içinde çalışan bir araçtır ve internet taramaları sırasında güvenliğinizi en üst düzeyde sağlar. **AVG Internet Security 2013** içinde **AVG Security Toolbar** kurulumu isteğe bağlıdır; [kurulum işlemi](#) sırasında bileşenin kurulup kurulmayacağına karar vermeniz istenir. **AVG Security Toolbar** internet tarayıcınızdan doğrudan kullanılabilir. Su anda desteklenen internet tarayıcıları: Internet Explorer (sürüm 6.0 üstü), ve/veya Mozilla Firefox (sürüm 3.0 ve üstü). Diğer tarayıcılar desteklenmez (*Avant Browser gibi alternatif internet tarayıcıları kullanıyorsanız beklenmeyen davranışlarla karşılaşabilirsiniz*).



**AVG Security Toolbar**'nin içerdiği öğeler:

- **Açılır menülü AVG logosu:**
  - **Geçerli Tehdit Düzeyi** - web'de geçerli tehdit seviyesinin grafik görünümünü içeren virüs laboratuvarı web sayfasını açar.
  - **AVG Tehlike Laboratuvarları** - çeşitli web sitelerinin güvenliği ve geçerli tehlike düzeyi hakkında çevrimiçi bilgi alabileceğiniz **AVG Tehlike Laboratuvarı** web sitesini açar (<http://www.avgthreatlabs.com>).
  - **Toolbar Yardımı** - tüm **AVG Security Toolbar** işlemlerini kapsayan çevrimiçi yardımı açar.
  - **Ürün Geribildirimi Gönder** - **AVG Security Toolbar** hakkında görüşlerinizi bildirebileceğiniz bir form içeren bir web sayfası açar.
  - **AVG Security Toolbar'nu kaldır** - **AVG Security Toolbar**'nu desteklenen web tarayıcılarının her birinde nasıl devre dışı bırakabileceğinizde dair ayrıntılı talimat içeren bir web sayfası açar.
  - **Hakkında...** - yüklü **AVG Security Toolbar** sürümü hakkında bilgilerin yer aldığı yeni bir pencere açar.
- **Arama alanı** - görüntülenen tüm arama sonuçları yüzde yüz güvenli olduğundan, kesin biçimde güvenli ve rahat olmak için internet aramalarında **AVG Security Toolbar**'nu kullanın. Anahtar sözcük veya ifadeyi arama alanına girin ve **Ara** düğmesine (veya **Enter tusuna**) basın.
- **Site Güvenliği** - bu düğme ziyaret etmekte olduğunuz sayfanın mevcut güvenlik düzeyi hakkında bilgi sağlayan yeni bir iletişim kutusu açar (*Su anda güvenli*). Bu kısa açıklama genişletilebilir ve sayfaya ilgili güvenlik aktiviteleri hakkında tüm detaylar doğrudan tarayıcı penceresinde görülebilir (*Raporun tamamını görüntüle*):



- **Do Not Track** - DNT servisi çevrimiçi etkinliklerinizi izleyen web sitelerini belirlemenize yardımcı olur ve size bunlara izin verme veya bunları engelleme seçeneği sunar. [Ayrıntılar >>](#)
- **Sil** - 'çöp kutusu' düğmesi tarama, indirme ve çevrimiçi formlarla ilgili bilgileri seçerek silmek için bir açılır menü sunar; isterseniz tüm arama geçmişinizi tek seferde de silebilirsiniz.
- **Hava** - düğme, yaşadığınız yerin o gün ve sonraki iki günü kapsayan hava durumu hakkında bilgi sağlayan yeni bir iletişim kutusu açar. Bilgiler her 3-6 saatte bir düzenli olarak güncellenir. İletişim kutusunda istediğiniz konumu el ile seçebilir ve sıcaklık değerlerinin Celsius veya Fahrenheit cinsinden gösterilmesini tercih edebilirsiniz.



- **Facebook** - Bu düğme doğrudan [AVG Security Toolbar](#) içinden **Facebook** sosyal paylaşım ağına bağlanabilmenizi sağlar.
- **Hız testi** - Bu düğme sizi internet bağlantınızın kalitesini (*ping*) ve indirme/yükleme hızını doğrulayabileceğiniz çevrimiçi bir uygulamaya yönlendirir.
- Su uygulamalara hızlı erişim için kısayol düğmeleri: **Hesap Makinesi, Not Defteri, Windows Explorer.**



## 8. AVG Do Not Track


**AVG Do Not Track** çevrimiçi etkinlikleriniz hakkında bilgi toplayan web siteleri hakkında sizi bilgilendirir. [AVG Security Toolbar](#)'in bir parçası olan **AVG Do Not Track** özelliği etkinlikleriniz hakkında veri toplayan web siteleri veya reklamcileri gösterir ve size bunları engelleme veya bunlara izin verme seçeneği sunar.

- **AVG Do Not Track** her servis için gizlilik politikası hakkında ek bilgilerin yanı sıra varsa ilgili servisin dışında kalmak için doğrudan bir bağlantı da sunar.
- **AVG Do Not Track** sizi izlemesini istemediğiniz siteler hakkında otomatik bilgilendirme için [W3C DNT protokolünü](#) de destekler. Bu bilgilendirme otomatik olarak etkindir, ancak istenildiğinde değiştirilebilir.
- **AVG Do Not Track** uygulaması şu [sartlar ve hükümler](#) altında sağlanır.
- **AVG Do Not Track** varsayılan olarak etkindir, ancak istenildiğinde kolayca devre dışı bırakılabilir. Talimatları bulabileceğiniz SSS makalesi: [AVG Do Not Track özelliğini devre dışı bırakma](#).
- **AVG Do Not Track** hakkında daha fazla bilgi için lütfen [web sitemizi](#) ziyaret edin.

Su anda, **AVG Do Not Track** özelliği işlevsel olarak Mozilla Firefox, Chrome ve Internet Explorer tarayıcılarında destekleniyor.

### 8.1. AVG Do Not Track arayüzü

Çevrimiçi olarak, **AVG Do Not Track** herhangi bir veri toplama faaliyeti tespit edilir edilmez sizi uyarır. Böyle bir durumda, [AVG Security Toolbar](#) üzerinde yer alan **AVG Do Not Track** simgesi görünümünü değiştirir; simgenin yanında tespit edilen veri toplama servislerinin sayısını gösteren

küçük bir sayı görünür:  Aşağıdaki iletişim kutusunu görüntülemek için simgeyi tıklattığınızda:



Tespit edilen tüm veri toplama servisleri **Bu sayfadaki izleyiciler** bilgi ekranında listelenir. **AVG Do Not Track** tarafından tanınan üç tür bilgi toplama etkinliği vardır:

- **Web Analytics** (varsayılan olarak izin verilir): İlgili web sitelerinin performans ve deneyimini geliştirmek için kullanılan servisler. Bu kategoride Google Analytics, Omniture veya Yahoo Analytics gibi servisleri bulabilirsiniz. Web sitesi istenildiği şekilde çalışmayabileceğinden web analytics servislerini engellememenizi öneririz.
- **Ad Networks** (bazıları varsayılan olarak engellenir): İçerik tabanlı reklamlar yerine size özel reklamlar sunmak için birden fazla sitede çevrimiçi etkinlikleriniz hakkında doğrudan veya dolaylı olarak bilgi toplayan ve paylaşan servislerdir. Bu durum ilgili Ad networks öğesinin web sitesindeki gizlilik politikasına göre belirlenir. Bazı ad networks öğeleri varsayılan olarak engellenir.
- **Social Buttons** (varsayılan olarak izin verilir): Sosyal ağ deneyimini geliştirmek için tasarlanmış öğeler. Social buttons öğeleri ziyaret ettiğiniz siteye sosyal ağlardan sunulur. Oturumunuz açıkken çevrimiçi etkinlikleriniz hakkında bilgi toplayabilirler. Social buttons örnekleri: Facebook Sosyal Eklentileri, Twitter Düğmesi, Google +1.

**Not:** Web sitesinin arka planında çalışan servislere bağlı olarak, AVG Do Not Track iletişim kutusunda yukarıda açıklanan üç bölümden bazıları yer almayabilir.

### İletişim kutusu kontrolleri

- **İzleme nedir?** - İzleme prensipleri hakkında ayrıntılı açıklamalar ve belirli izleme türlerinin tarifini içeren bir web sayfasına yönlendirilmek için iletişim kutusunun üst bölümünde yer alan bu bağlantıyı tıklanın.

- **Tümünü Engelle** - Hiçbir veri toplama faaliyeti istemiyorsanız iletişim kutusunun altındaki bu düğmeyi tıklattın (*ayrıntılar için [İzleme işlemlerini engelleme](#) bölümüne bakın*).
- **Do Not Track ayarları** - Çeşitli **AVG Do Not Track** parametrelerinin yapılandırma ayarlarını yapabileceğiniz bir web sayfasına yönlendirilmek için iletişim kutusunun alt bölümündeki bu bağlantıyı tıklattın (*ayrıntılı bilgi için [AVG Do Not Track ayarları](#) bölümüne bakın*).

## 8.2. İzleme süreçleri hakkında bilgiler


Tespit edilen veri toplama servislerinin listesi yalnızca ilgili servisin adını gösterir. İlgili servise izin verme veya engelleme yönünde bilinçli bir tercih yapmak için daha fazla bilgiye ihtiyacınız vardır. Fare imlecini ilgili liste öğesinin üzerine getirin. Servis hakkında detaylı bilgileri içeren bir bilgi balonu görüntülenir. Servisin kişisel verilerinizi mi yoksa başka verileri mi topladığı, verilerin diğer üçüncü taraflarla paylaşılıp paylaşılmadığı ve toplanan verilerin ileride kullanılmak üzere saklanıp saklanmadığı gibi konular hakkında bilgi sahibi olursunuz:




Bilgi balonunun alt bölümünde, tespit edilen ilgili servisin web sitesinde gizlilik politikasına yönlendiren bir **Gizlilik Politikası** bağlantısı bulunur.

## 8.3. İzleyici süreçlerini engelleme

Tüm Ad Networks / Social Buttons / Web Analytics listesiyle istediğiniz servislerin engellenmesini kontrol etme seçeneğine sahip olursunuz. İki seçenektten birini tercih edebilirsiniz:

- **Tümünü Engelle** - Hiçbir veri toplama faaliyeti istemiyorsanız iletişim kutusunun altındaki bu düğmeyi tıklattın. (*Ancak, bu işlemin servisin çalıştığı ilgili web sitesinin işlevlerini bozabileceğine dikkat edin!*)
-  - Tespit edilen servislerin tamamını bir seferde engellemek istemiyorsanız, servislerin engellenmesine veya bunlara izin verilmesine tek tek karar verebilirsiniz. Tespit edilen

sistemlerden bazılarının çalışmasına izin verebilirsiniz (örn. *Web Analytics*): Bu sistemler toplanan verileri kendi web sitelerinin optimizasyonu için kullanır ve böylece tüm kullanıcılar için internet ortamının geliştirilmesine yardımcı olur. Ancak, aynı zamanda Ad Networks olarak sınıflandırılan tüm veri toplama faaliyetlerini engelleyebilirsiniz. Veri toplama engellemenin (servis adı çarpi ile işaretlenir) veya veri toplama için yeniden izin vermek için ilgili servisin yanındaki  simgesini tıklayın.

## 8.4. AVG Do Not Track ayarları

**Do Not Track Seçenekleri** iletişim kutusunun sunduğu yapılandırma seçenekleri:



- **Do Not Track etkin** - Varsayılan olarak DNT servisi etkindir (AÇIK). Hizmeti devre dışı bırakmak için anahtarı KAPALI konumuna getirin.
- İletişim kutusunun orta bölümünde Ad Networks olarak sınıflandırılacak bilinen veri toplama servislerinin bir listesinin yer aldığı bir kutu görebilirsiniz. **Do Not Track** varsayılan olarak Ad Networks servislerinin bir kısmını otomatik olarak engeller ve geri kalanların engellenmesi veya bunlara izin verilmesi sizin seçiminize kalır. Bunun için listenin altındaki **Tümünü Engelle** düğmesini tıklaymanız yeterlidir. Bunun yerine, yapılan tüm ayar değişikliklerini iptal etmek ve orijinal yapılandırmaya geri dönmek için **Varsayılan** düğmesini kullanabilirsiniz.
- **Web siteleri bildirimini ...** - Bu bölümde **İzlenmek istemediğim web siteleri hakkında bilgilendir** seçeneğini açabilir veya kapatabilirsiniz (varsayılan olarak açıktır). **Do Not Track** özelliğinin sizi izlemesini istemediğiniz veri toplama servisleri hakkında bilgilendirmesini istiyorsanız bu seçeneği işaretli olarak bırakın.

## 9. AVG Gelişmiş Ayarlar

**AVG Internet Security 2013** 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 kutusunun pencerenin sağ kısmında görüntülemek için yapılandırmasını (*ya da belirli bir parçasını*) değiştirmek istediğiniz bileşeni seçin.

### 9.1. Görünüm

Menü ağacının ilk ögesi olan **Görünüm**, **AVG Internet Security 2013** [kullanıcı arayüzünün](#) genel ayarlarına ilişkindir ve uygulama davranışı için bazı temel seçenekleri sağlar:



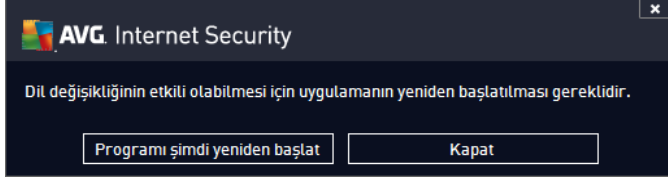
#### Dil seçimi

**Dil seçimi** bölümünde açılır menüden istediğiniz dili seçebilirsiniz. Seçilen dil **AVG Internet Security 2013** [kullanıcı arayüzünün](#) tamamı için kullanılır. Aşağı açılır menü yükleme işlemi sırasında yüklenmesini istediğiniz dilleri ve İngilizceyi sunar (*İngilizce daima varsayılan olarak yüklenir*). **AVG Internet Security 2013** uygulamasını başka bir dile geçirmek için yeniden başlatmanız gerekir. Lütfen şu adımları takip edin:

- Aşağı açılır menüde istediğiniz uygulama dilini seçin
- **Uygula** düğmesine (*iletişim kutusunun sağ alt tarafında*) basarak seçiminizi onaylayın
- Onaylamak için **Tamam** düğmesine basın
- Uygulamanın dilini değiştirmek için **AVG Internet Security 2013**



- Programın yeniden başlatılmasını onaylamak için **Programı şimdi yeniden başlat** düğmesine basın ve dil değişikliğinin gerçekleşmesi için bir saniye bekleyin:



### Sistem tepsi bildirimleri

Bu bölümde **AVG Internet Security 2013** uygulama durumu hakkında sistem tepsisi üzerinde beliren bildirimleri kaldırabilirsiniz. Varsayılan olarak, sistem bildirimlerinin görüntülenmesine izin verilir. Bu yapılandırmayı kesinlikle muhafaza etmeniz önerilir! Sistem bildirimleri örneğin tarama veya güncelleme işlemi başlatma ya da bir **AVG Internet Security 2013** bileşeni durum değişikliği hakkında bilgi verir. Bu bildirimlere kesinlikle dikkat etmeniz gerekir!

Ancak, belirli bir neden dolayısıyla bu yolla bilgilendirilmek istemiyorsanız ya da sadece belirli bildirimlerin görüntülenmesini istiyorsanız (*belirli AVG Internet Security 2013 bileşenlerine ilişkin*) tercihlerinizi aşağıdaki seçenekleri işaretleyerek ya da işaretlemeyerek tanımlayabilir ve belirleyebilirsiniz:

- **Sistem tepsi bildirimlerini görüntüle** ( varsayılan olarak açık) - varsayılan olarak tüm bildirimler görüntülenir. Tüm sistem bildirimleri kapatmak için bu öğenin işaretini kaldırın. Açıldığı zaman hangi bildirimlerin görüntüleneceğini seçebilirsiniz:



- **Güncelleme bildirimleri** (varsayılan olarak açık) - **AVG Internet Security 2013**



güncelleme isleminin başlamasi, ilerleyisi ve bitisi hakkında bilgilerin görüntülenmesini isteyip istemediginize karar verin.

- o **Bilesen degisiklik bildirimleri** (varsayilan olarak kapali) - bilesenlerin etkin olup olmadigi ya da olasi sorunlari hakkında bildirimlerin görüntülenmesini isteyip istemediginize karar verin. Bir bilesenin hata durumu rapor edilirken bu fonksiyon, [sistem tepsisi simgesinin](#) herhangi bir **AVG Internet Security 2013** bileseninde meydana gelen sorunu rapor ederken kullandigi bilgilendirici fonksiyonuna esdegerdir.
- o **Yerlesik Kalkan otomatik tehdit kaldırma bildirimleri**(varsayilan olarak açık) - dosya kaydetme, kopyalama ve açma islemleriyle ilgili bilgilerin görüntülenmesine veya gizlenmesine (bu yapılandırma yalnızca Yerlesik Kalkan otomatik temizleme seçeneği açık sagösterilir) karar verin.
- o **Tarama bildirimleri** (varsayilan olarak açık) - programli taramaların otomatik olarak başlamasi, ilerleyisi ve sonuçlari hakkında bilgilerin görüntülenmesini isteyip istemediginize karar verin.
- o **Firewall bildirimleri** (varsayilan olarak açık) - Firewall durum ve islemleri hakkında, örneğin bilesenin etkinlestirilmesi/devre disi bırakılması uyarilari, olasi trafik engelleme vb. hakkında bilgilerin görüntülenip görüntülenmeyecegine karar verin. Bu öge iki adet seçim seçeneği daha saglar (her biri hakkında daha fazla bilgi için lütfen bu belgedeki [Firewall](#) bölümüne bakın):
  - **Ag baglantı noktaları** (varsayilan olarak kapali) - bir aga bağlanırken, Firewall ağı bilip bilmediği ve dosya ve yazıcı paylaşımının nasıl ayarlanacağı konusunda bilgilendirme yapar.
  - **Engellenmiş uygulamalar** (varsayilan olarak açık) - aga bilinmeyen veya şüpheli bir uygulama bağlanmaya çalıştığında Firewall girişini engeller ve bir bildirim görüntüler. Bu bilgilendirme açısından iyidir, bu yüzden özelliği daima açık tutmanızı öneririz.
- o **E-posta Tarayicisi bildirimleri** (varsayilan olarak açık) - gelen ve giden e-posta mesajlarının taranmasına ilişkin bildirimleri görüntülemek isteyip istemediginize karar verin.
- o **Istatistiksel bildirimler** (varsayilan olarak açık) - düzenli istatistiksel inceleme uyarılarının sistem tepsisinde görüntülenmesine izin vermek için bu seçeneği isaretili halde bırakın.
- o **AVG Hizlandirici bildirimleri** (varsayilan olarak açık) - **AVG Hizlandirici** etkinlikleri hakkındaki bilgilerin görüntülenmesini isteyip istemediginize karar verin. **AVG Hizlandirici** hizmetidaha düzgün çevrimiçi video oynatmaya izin verir ve ilave indirmeleri daha kolay hale getirir.
- o **Baslatma zamanini gelistirme bildirimleri** (varsayilan olarak kapali) - bilgisayarınızın baslatma zamanının geliştirilmesi hakkında bilgilendirilmek isteyip istemediginize karar verin.
- o **AVG Tavsiyesi bildirimleri** (varsayilan olarak açık) - [AVG Tavsiyesi](#) etkinlikleri hakkındaki bilgilerin sistem tepsisi panelinde görüntülenmesini isteyip istemediginize



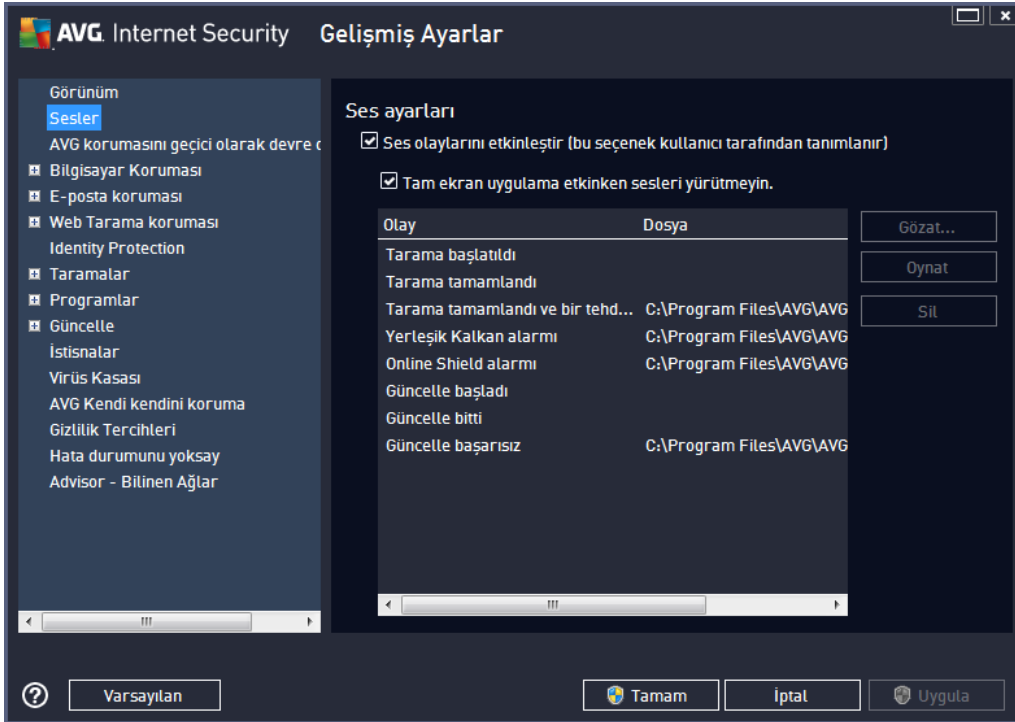
karar verin.

## Oyun modu

Bu AVG islevi, tüm AVG bilgi balonlarının (örn. programlanmış bir tarama baslatıldığında gösterilir) rahatsız edici olabileceği (uygulamayı küçültebilir veya grafiklerini bozabilir) tam ekran uygulamaları için tasarlanmıştır. Bu durumu önlemek için, **Tam ekran uygulaması çalıştırılırken oyun modunu etkinleştir** seçeneğini işaretli bırakın (varsayılan ayar).

## 9.2. Sesler

**Sesler** iletişim kutusu içinde, belirli **AVG Internet Security 2013** eylemleri hakkında bir ses bildiriminiyle bilgilendirilmek isteyip istemediğinizi belirleyebilirsiniz:



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

## Kontrol düğmeleri

- **Gözet** - diskinizde atamak istediğiniz ilgili ses dosyasını aramak için, listeden ilgili eylem seçilmiş olarak **Gözet** düğmesini kullanın. (Su anda yalnızca \*.wav seslerinin desteklenmekte olduğunu lütfen unutmayın!)

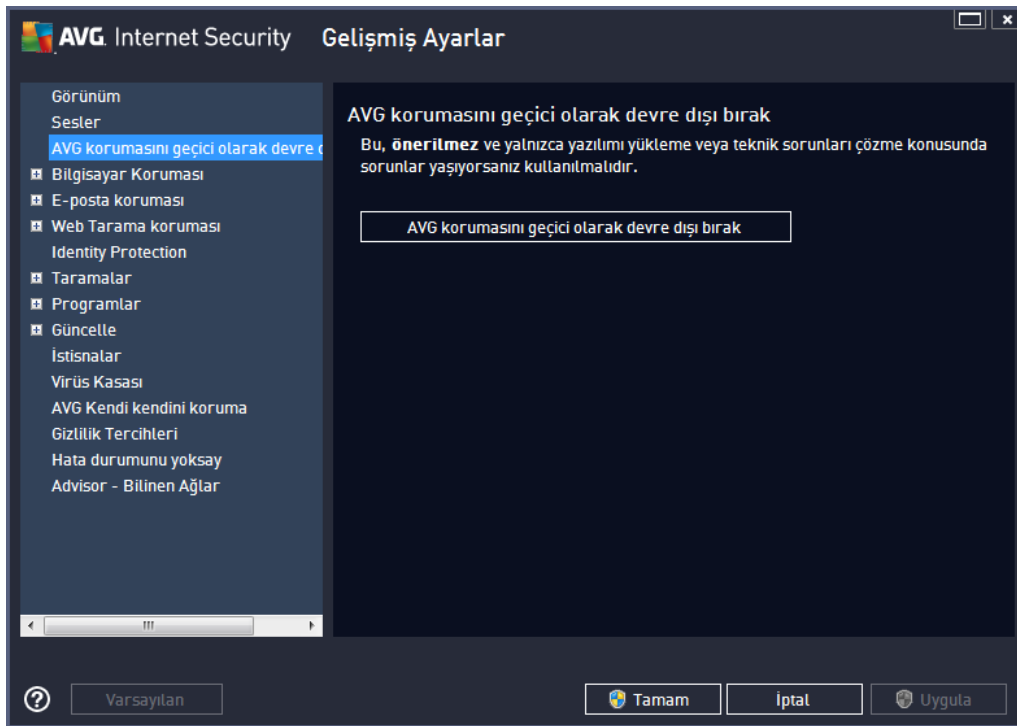


- **Çal** - seçili sesi dinlemek için, listede olayı vurgulayın ve **Çal** düğmesine basın.
- **Sil** - belirli olaya atanan sesi kaldırmak için **Sil** düğmesini kullanın.

### 9.3. AVG korumasını geçici olarak devre dışı bırak

**AVG korumasını geçici olarak devre dışı bırak** iletişim kutusunda, **AVG Internet Security 2013** yazılımınız tarafından güvende tutulan tüm korumayı bir seferde kapatma seçeneğiniz vardır.

**Mutlaka gerekli değilse, bu seçeneği kullanmamanız gerektiğini lütfen unutmayın!**



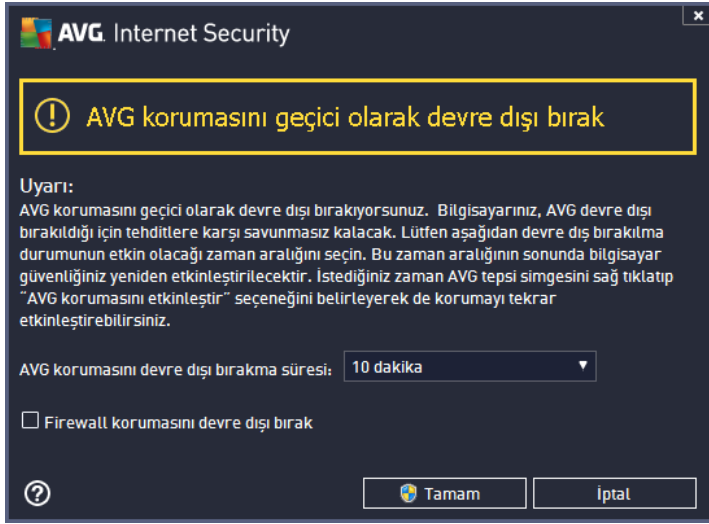
Çoğu durumda, yeni yazılımı veya sürücülerini yüklemeyen önce ve hatta yükleyici veya yazılım sihirbazı yükleme işlemi sırasında istenmeyen kesintilerin olmamasını sağlamak için çalışan program ve uygulamaların kapatılmasını önerse bile **AVG Internet Security 2013** uygulamasını devre dışı bırakmak **gerekmez**. Yükleme sırasında gerçekten sorunlar yaşıyorsanız, öncelikle yerleşik korumayı devre dışı bırakmayı deneyin (*Yerleşik Kalkan'ı etkinleştir*). **AVG Internet Security 2013** uygulamasını geçici olarak devre dışı bırakmanız gerekirse, işinizi bitirdikten sonra yeniden etkinleştirmeniz gerekir. Virüslerden korunma yazılımınız devre dışı bırakılmıyken internete veya bir ağa bağlanırsanız, bilgisayarınız saldırılara açık durumda olur.

#### **AVG korumasını geçici olarak nasıl devre dışı bırakılır**

**AVG korumasını geçici olarak devre dışı bırak** onay kutusunu işaretleyin ve **Uygula** düğmesine basarak seçiminizi onaylayın. Yeni açılan **AVG korumasını geçici olarak devre dışı bırak** iletişim kutusunda **AVG Internet Security 2013** uygulamanızı ne kadar süreyle devre dışı bırakmak istediğinizi belirleyin. Koruma, varsayılan olarak 10 dakika süreyle kapatılır. Bu süre, yeni bir yazılım



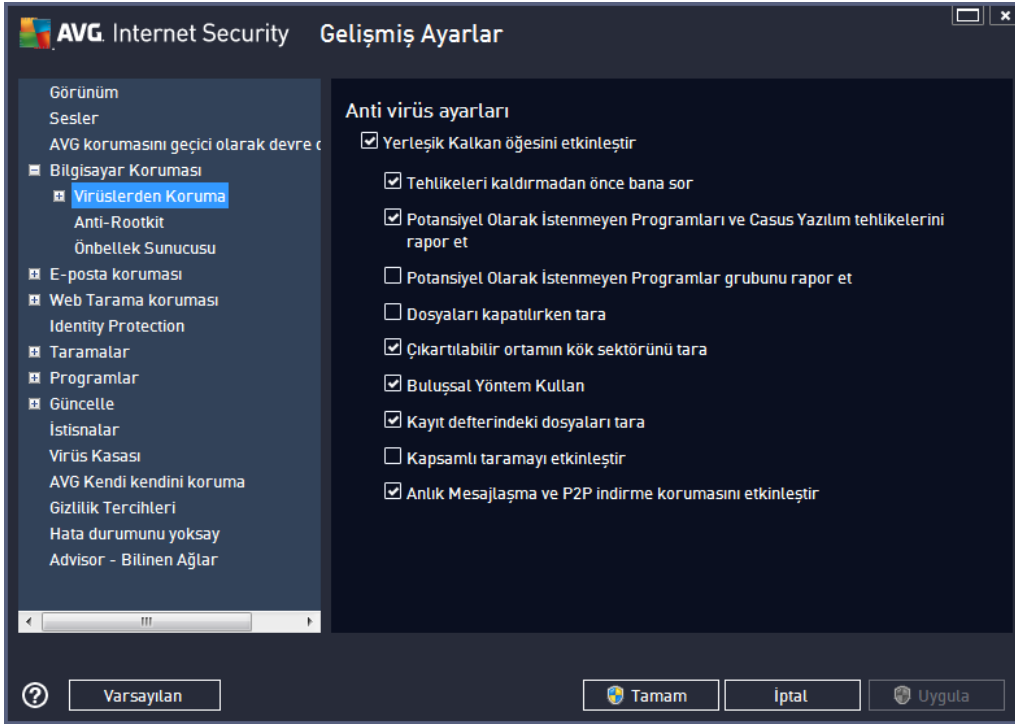
yükleme gibi herhangi bir işlem için yeterli olacaktır. Daha uzun bir süre de belirleyebilirsiniz, ancak kesinlikle gerekli değilse bu seçeneği kullanmanız önerilmez. Daha sonra, devre dışı bırakılan tüm bileşenler yeniden etkinleştirilir. AVG korumasını en uzun süreyle bir sonraki bilgisayar başlatmasına kadar devre dışı bırakabilirsiniz. **Firewall** bileşenini ayrı olarak devre dışı bırakma seçeneği **AVG korumasını geçici olarak devre dışı bırak** iletişim kutusunda yer alır. **Firewall korumasını devre dışı bırak** kutusunu işaretleyerek bu işlemi gerçekleştirebilirsiniz.



## 9.4. Bilgisayar Koruması

### 9.4.1. Virüslerden Koruma

**Virüslerden Koruma**, **Yerlesik Kalkan** ile birlikte bilgisayarınızı bilinen tüm virüs, casus yazılım ve zararlı yazılımlara karşı sürekli olarak korur (*uyuyan veya aktif hale geçmemiş, yani indirilmiş ancak henüz etkin hale geçmemiş zararlı yazılımlar da dahil*).



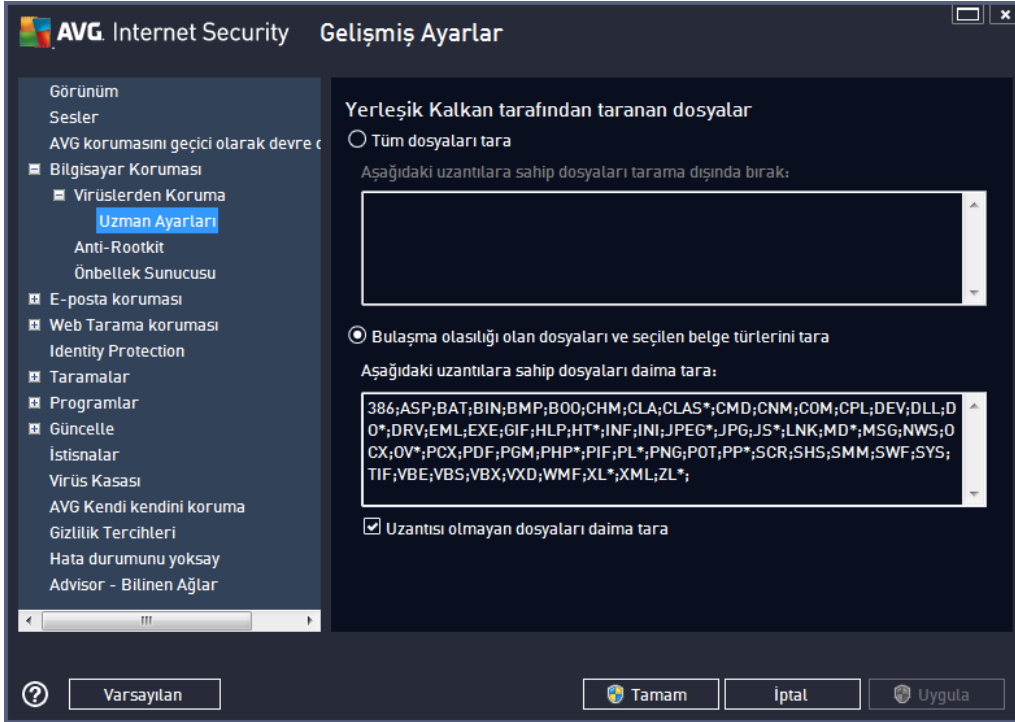
**Yerlesik Kalkan ayarları** iletişim kutusunda yerlesik kalkan korumasini **Yerlesik Kalkan'i etkinlestir** ögesini isaretleyerek ya da isaretini kaldırarak etkinlestirebilir ya da devre disi bırakabilirsiniz (*bu seçenek varsayılan olarak açıktır*). Ayrıca yerlesik kalkanin hangi özelliklerinin etkinlestirileceğini seçebilirsiniz:

- **Tehlikeleri kaldırmadan önce bana sor** (*varsayılan olarak açık*) - Yerlesik Kalkan'in hiçbir işlemi otomatik olarak yapmaması; bunun yerine, tespit edilen tehlikeyi ne yapacağınıza karar vermeniz için göstermesini sağlamak için isaretleyin. Kutuyu isaretlemezseniz, **AVG Internet Security 2013** bulasmayı otomatik olarak temizler; bu mümkün değilse nesne [Virüs Kasası](#)'na tasınır.
- **Potansiyel Olarak İstenmeyen Programları ve Casus Yazılım tehlikelerini rapor et** (*varsayılan olarak açık*) - virüslerin yanı sıra casus yazılımları da taramak için isaretleyin. Casus yazılım, süpheli 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 öneririz.
- **Potansiyel Olarak İstenmeyen Programlar grubunu rapor et** (*varsayılan olarak kapalı*) - casus yazılımların, yani doğrudan üreticiden alınan tamamen zararsız olan, ancak daha sonra kötüye kullanılacak programların genişletilmiş paketinin tespit edilmesi için isaretleyin. Bu, bilgisayarınızın güvenliğini daha da artıran ek bir önlemdir, ancak yasal programları da engelleyebildiğinden varsayılan olarak kapalıdır.
- **Dosyaları kapatılırken tara** (*varsayılan olarak kapalı*) - işlem sonunda tarama, AVG'nin etkin nesnelere hem açılırken hem de kapatılırken taradığından emin olmanızı sağlar. Bunun yanı sıra bu özellik, bilgisayarınızı karmaşık virüslere karşı korumanıza da yardımcı olur.
- **Çıkartılabilir ortamın kök sektörünü tara** (*varsayılan olarak açık*)



- **Bulussal Yöntem Kullan** (varsayılan olarak açık) - bulussal analiz, tespit etme işlemi sırasında kullanılır (taranan nesnenin komutlarının sanal bilgisayar ortamında dinamik olarak canlandırılması).
- **Kayıt defterindeki dosyaları tara** (varsayılan olarak açık) - bilinen buluşmanın sonraki bilgisayar başlangıcında çalıştırılmasını önlemek için, başlangıç kayıtlarına eklenmiş tüm çalıştırılabilir dosyaları AVG tarafından bu parametre belirtilir.
- **Kapsamlı taramayı etkinleştir** (varsayılan olarak kapalı) - belirli durumlarda (çok acil bir durum olduğunda) nesnelerin derinlemesine islenme olasılığını denetleyecek çok hassas algoritmaları etkinleştirmek için bu seçeneği işaretleyebilirsiniz. Ancak, bu yöntemin çok fazla zaman aldığını unutmayın.
- **Anlık Mesajlaşma korumasını ve P2P indirme korumasını etkinleştir** (varsayılan olarak açık) - anlık mesajlaşma iletişimi (örneğin AIM, Yahoo!, ICQ, Skype, MSN Messenger, ...) ve Esler Arası ağlar içinde indirilen verilerin (sunucuya gerek olmaksızın istemciler arasında doğrudan bağlantı sağlayan ağlar; genellikle müzik dosyalarının paylaşımı için kullanılır ve potansiyel olarak tehlikelidir) virüssüz olduğunu doğrulamak istiyorsanız bu öğeyi işaretleyin.

**Yerleşik Kalkan tarafından taranan dosyalar** iletişim kutusunda hangi dosyaların taranacağını yapılandırılabilir (belirli dosya uzantılarına göre):



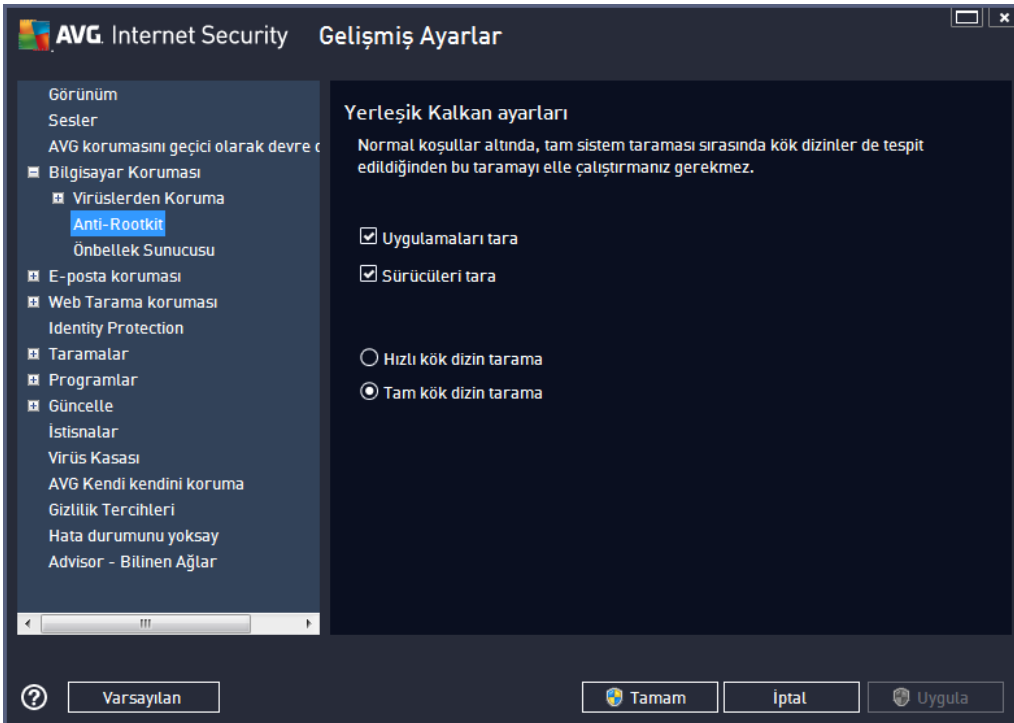
**Tüm dosyaları tara** veya yalnızca **Bulaşma olasılığı olan dosyaları ve seçilen belge türlerini tara** seçimi yapmak için ilgili onay kutusunu işaretleyin. Taramayı hızlandırmak ve aynı zamanda maksimum koruma düzeyi sağlamak için varsayılan ayarları korumanızı öneririz. Bu sayede yalnızca virüs bulabilecek dosyalar taranır. İletişim kutusunun ilgili bölümünde taramaya dahil edilen

dosyaları tanımlayan düzenlenebilir bir uzanti listesi bulabilirsiniz.

Uzantisi olmayan ve bilinmeyen biçimdeki dosyaların da Yerleşik Kalkan ile taranmasını sağlamak için **Uzantisi olmayan dosyaları daima tara** (varsayılan olarak açıktır) seçeneğini işaretleyin. Uzantisi olmayan dosyalar şüpheli dosyalar olduğundan, bu özelliği her zaman açık tutmanızı öneririz.

## 9.4.2. Anti-Rootkit

**Anti-Rootkit ayarları** iletişim kutusunda **Anti-Rootkit** hizmetinin yapılandırmasını ve anti-rootkit taramasının belirli parametrelerini düzenleyebilirsiniz. Anti-rootkit taraması [Tüm Bilgisayar Taraması](#) dahilindeki varsayılan bir işlemidir:

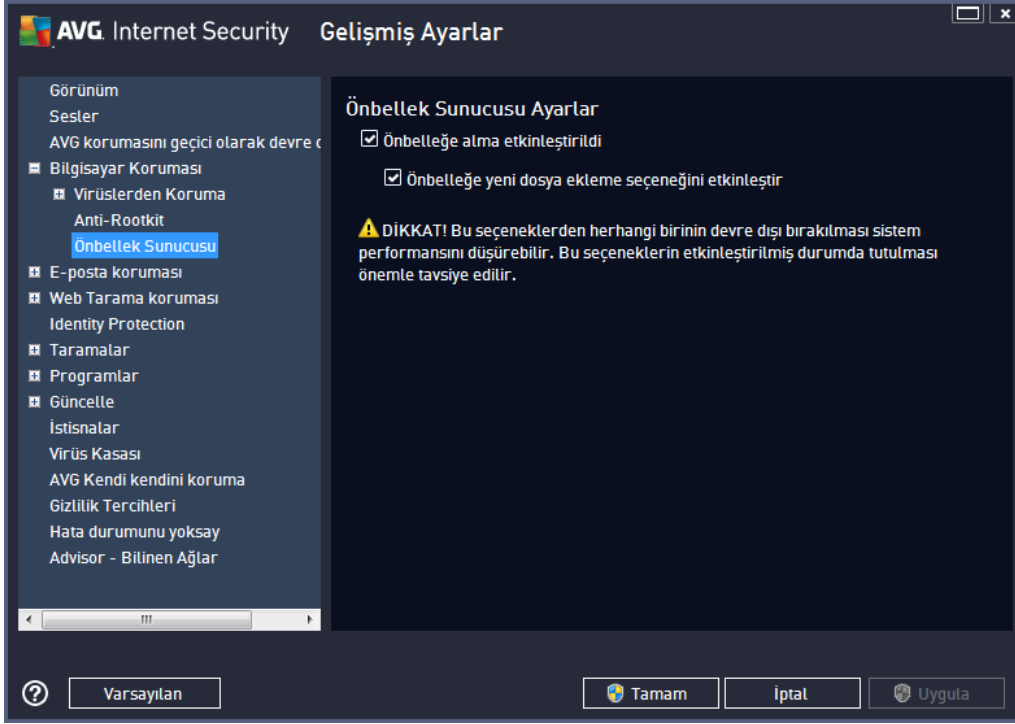


**Tarama uygulamaları** ve **Tarama sürücülerini** anti-rootkit taramasına nelerin dahil edileceğini ayrıntılı şekilde belirlemenize olanak tanır. Bu ayarlar gelişmiş kullanıcılara yöneliktir; tüm seçenekleri açık konumda muhafaza etmenizi öneririz. Rootkit tarama modunu da seçebilirsiniz:

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

### 9.4.3. Önbellek Sunucusu

**Önbellek Sunucusu Ayarları** iletişim kutusu tüm **AVG Internet Security 2013** tarama türlerini hızlandırmak için tasarlanan önbellek sunucusu sürecini isaret eder:



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

**Önbellek Sunucusu Ayarları** iletişim kutusu aşağıdaki yapılandırma seçeneklerini sunar:

- **Önbelleğe alma etkin** (*varsayılan olarak açıktır*) - **Önbellek Sunucusu**'nu kapatmak için kutunun isareti 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 isaretini kaldırın. Önceden önbelleğe alınmış her dosya korunacak ve önbelleğe alma tamamen kapatılincaya kadar veya virüs veritabanının bir sonraki güncellenmesine kadar kullanılacaktır.

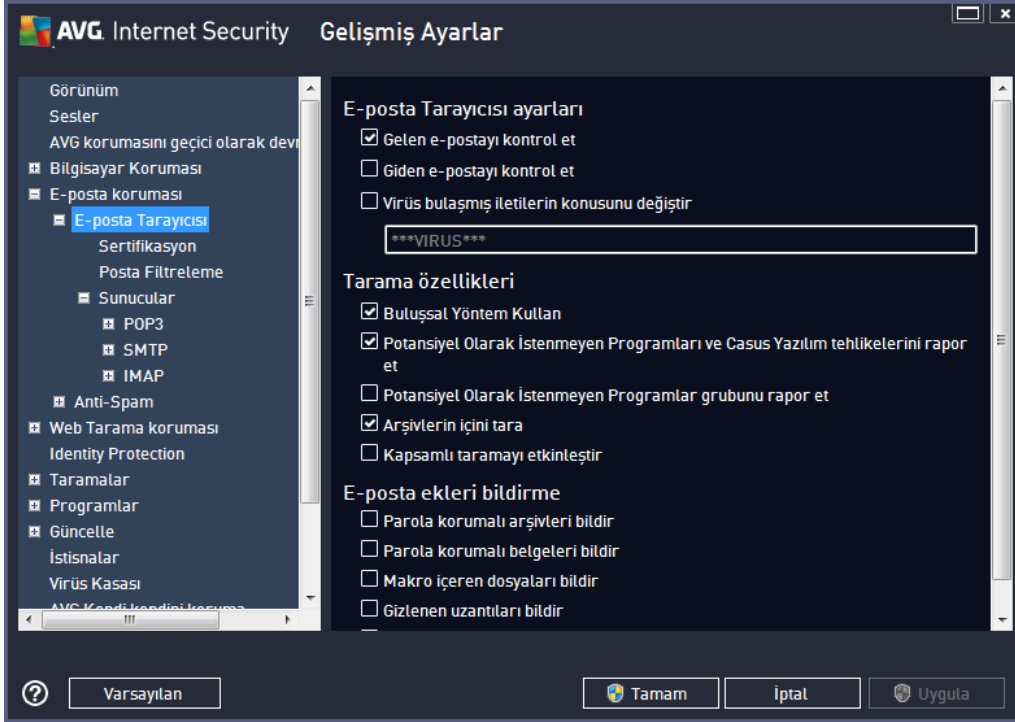
**Önbellek sunucusunu kapatmak için iyi bir nedeniniz yoksa, kesinlikle varsayılan ayarları muhafaza etmenizi ve seçeneğin açık kalmasını öneririz! Aksi durumda, sistem hızı ve performansında ciddi bir düşüş görebilirsiniz.**

## 9.5. E-Posta Tarayıcısı

Bu bölümde [E-posta Tarayıcısı](#) ve [Anti-Spam](#) için ayrıntılı yapılandırmalar düzenleyebilirsiniz:

### 9.5.1. E-Posta Tarayıcısı

*E-Posta Tarayıcısı* iletişim kutusu üç bölüme ayrılmıştır:



### E-posta tarama

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

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

### Tarama özellikleri

Bu bölümde, e-posta iletilerinin nasıl taranacağını belirleyebilirsiniz:

- **Bulussal Yöntem Kullan** (varsayılan olarak açık) - e-posta iletilerini tararken bulussal tespit yöntemi kullanmak için işaretleyin. Bu seçenek açık olduğunda, e-posta eklerini yalnızca uzantıya göre filtrelemezsiniz; ekin gerçek içeriği de göz önünde bulundurulur. Filtreleme işlemi [Posta Filtreleme](#) iletişim kutusundan ayarlanabilir.
- **Potansiyel Olarak İstenmeyen Programları ve Casus Yazılım tehditlerini rapor et** (varsayılan olarak açık) - virüslerin yani sıra casus yazılımları da taramak 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 öneririz.
- **Potansiyel Olarak İstenmeyen Programlar gelişmiş grubunu rapor et** (varsayılan olarak kapalı) - casus yazılımların, yani doğrudan üreticiden alınan tamamen zararsız olan, ancak daha sonra kötüye kullanılacak programların genişletilmiş paketlerinin tespit edilmesi için işaretleyin. Bu, bilgisayar güvenliğinizi daha da artıran ek bir önlemdir, ancak yasal programları da engelleyebilir ve bu yüzden varsayılan olarak kapalıdır.
- **Arsivlerin içeriğini tara** (varsayılan olarak açık) - e-posta iletilerine eklenen arşivlerin içeriklerini taramak için işaretleyin.
- **Kapsamlı taramayı etkinleştir** (varsayılan olarak kapalı) - belirli durumlarda (örneğin, bilgisayarınıza virüs bulaştığından veya saldırı olduğundan 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.

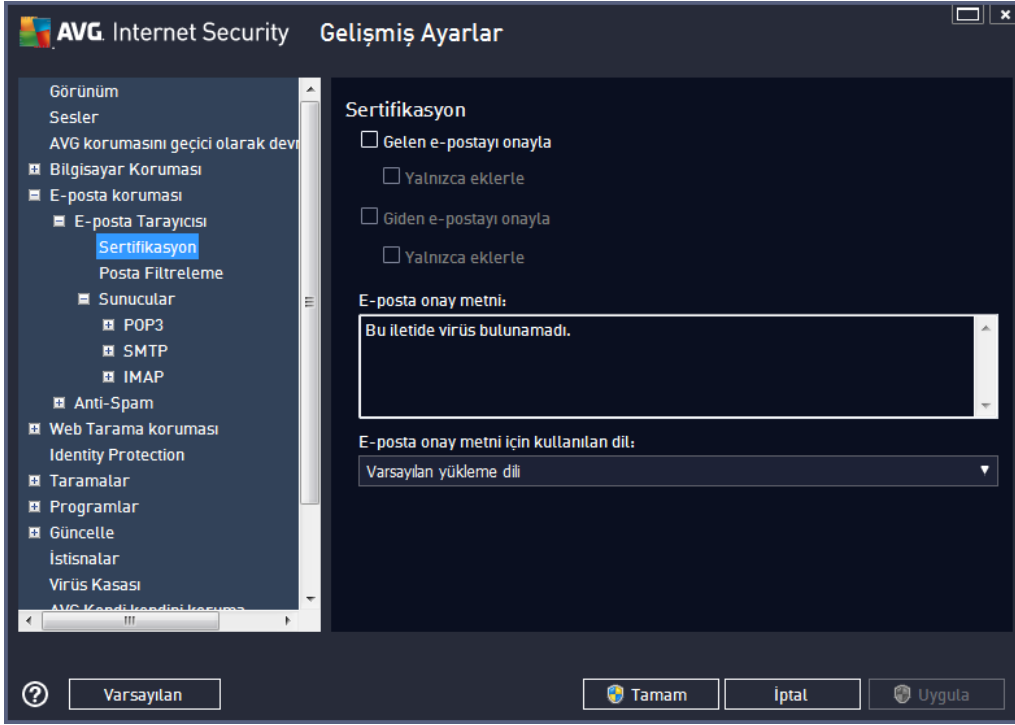
## E-posta ekleri bildirme

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 raporların tümü [E-posta Koruması tespiti](#) iletişim kutusunda listelenir:

- **Parola korumalı arşivleri bildir** - parolayla korunan arşivler (ZIP, RAR vb.) virüs için taranamaz; bunların potansiyel olarak tehlikeli olduklarını bildirmek için kutuyu işaretleyin.
- **Parola korumalı belgeleri bildir** - parolayla korunan belgeler virüs için taranamaz; bunların potansiyel olarak tehlikeli olduklarını bildirmek için 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. "birsey.txt.exe") zararsız bir düz metin dosyası gibi (örn. "birsey.txt") gösterebilir; bunları potansiyel olarak tehlikeli olarak bildirmek için kutuyu işaretleyin.
- **Rapor edilen ekleri Virüs Kasasına tasi** - taranan e-posta iletilerinin ekinde gizli bir eklenti tespit edildiğinde parola korumalı arşivler, parola korumalı belgeler, makro içeren dosyalar ve/veya gizli uzantılı dosyalar hakkında e-posta vasıtasıyla bilgilendirilmek isteyip istemediğinizi belirtin. Tarama işlemi sırasında bu tür bir mesaj tespit edilirse tespit edilen bulaşmış nesnenin [Virüs Kasası](#)'na taşınmasını isteyip istemediğinizi belirtin.

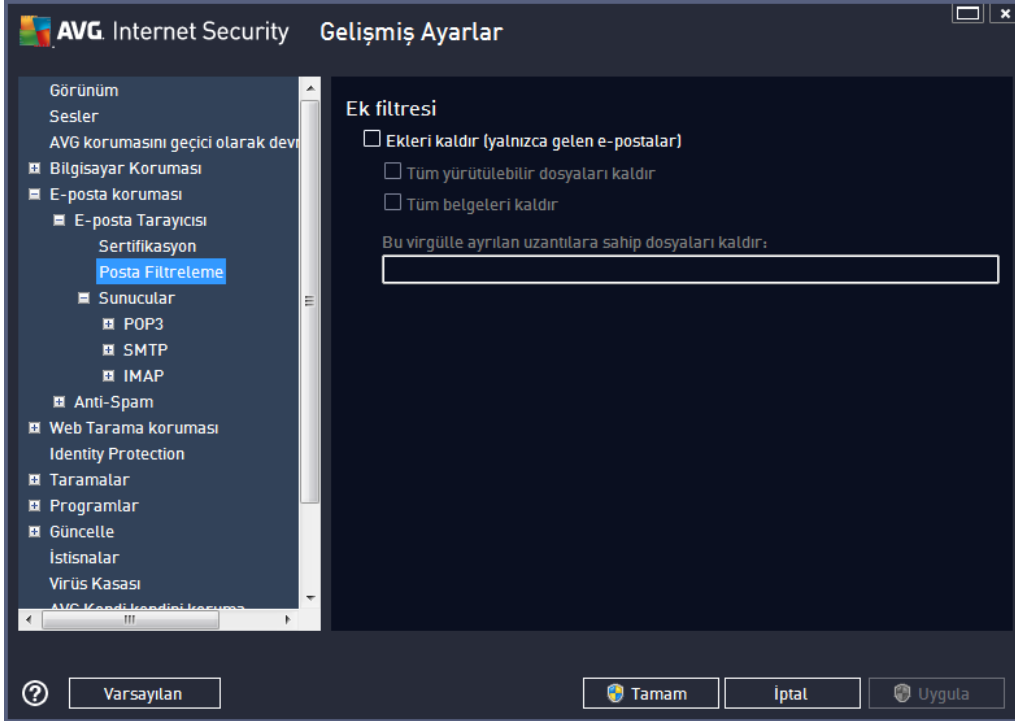


**Sertifika** iletişim kutusunda gelen (**Gelen e-postayı onayla**) ve/veya giden e-postaları onaylamaya (**Giden e-postayı onayla**) veya onaylamamaya karar vermek için çeşitli onay kutularını işaretleyebilirsiniz. Bu seçeneklerin her biri için **Yalnızca ekleri olanlar** parametresini işaretleyip onayın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



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

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



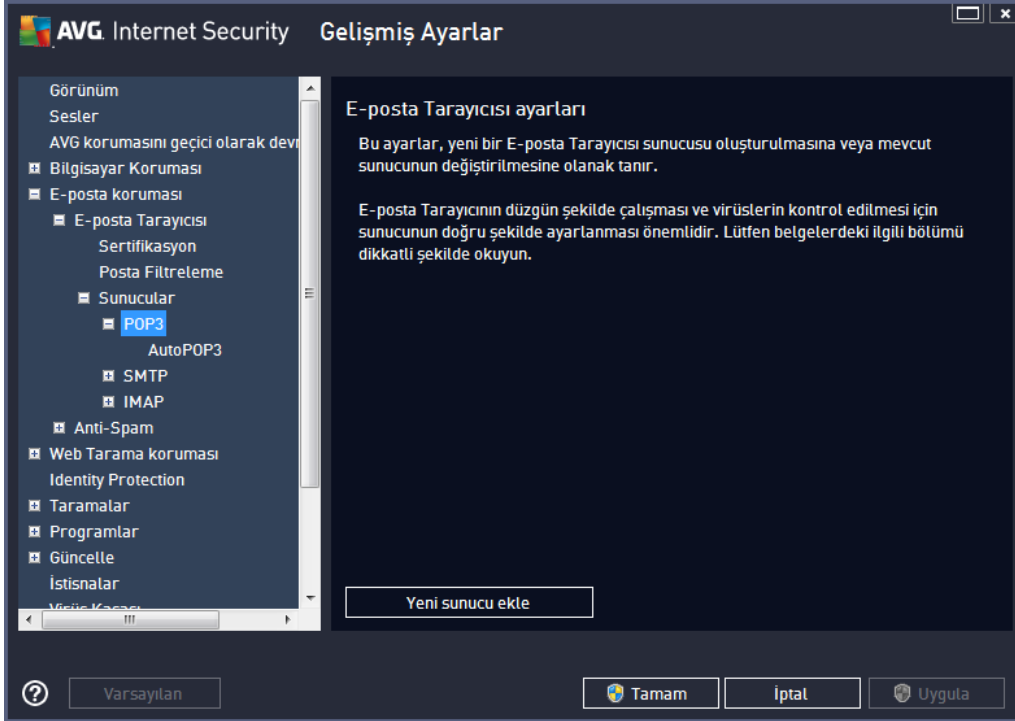
**Ek filtresi** iletişim kutusu, e-posta mesajlarının eklerinin taranmasına ilişkin parametreleri ayarlayabilmenizi sağlar. Varsayılan olarak **Eklenmeleri sil** seçeneği kapalıdır. Etkinleştirmeye karar verirsiniz tüm e-posta mesajlarının eklentileri, bulasmis nesne ya da potansiyel olarak tehlikeli 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 su uzantılara sahip dosyaları kaldır** - Tanımlanan uzantılara sahip tüm dosyalar kaldırılacaktır

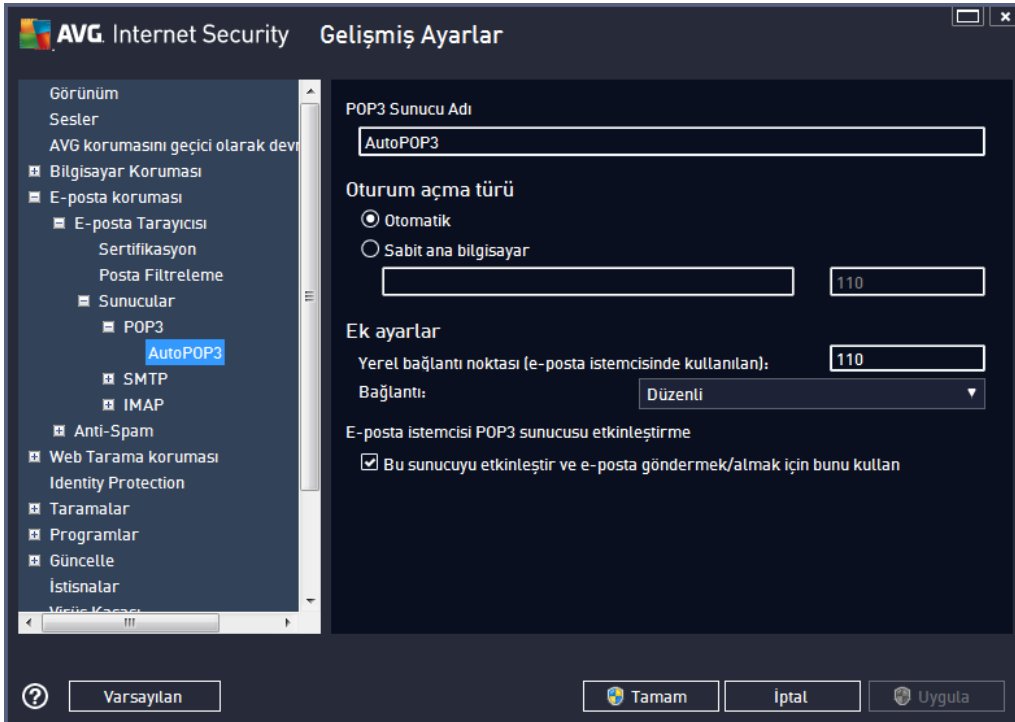
**Sunucular** bölümünde [E-posta Tarayıcısı](#) sunucularının parametrelerini düzenleyebilirsiniz:

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

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



Bu iletişim kutusunda gelen postalar için POP3 protokolünü kullanarak yeni bir [E-posta Tarayıcısı](#) sunucusu kurabilirsiniz:

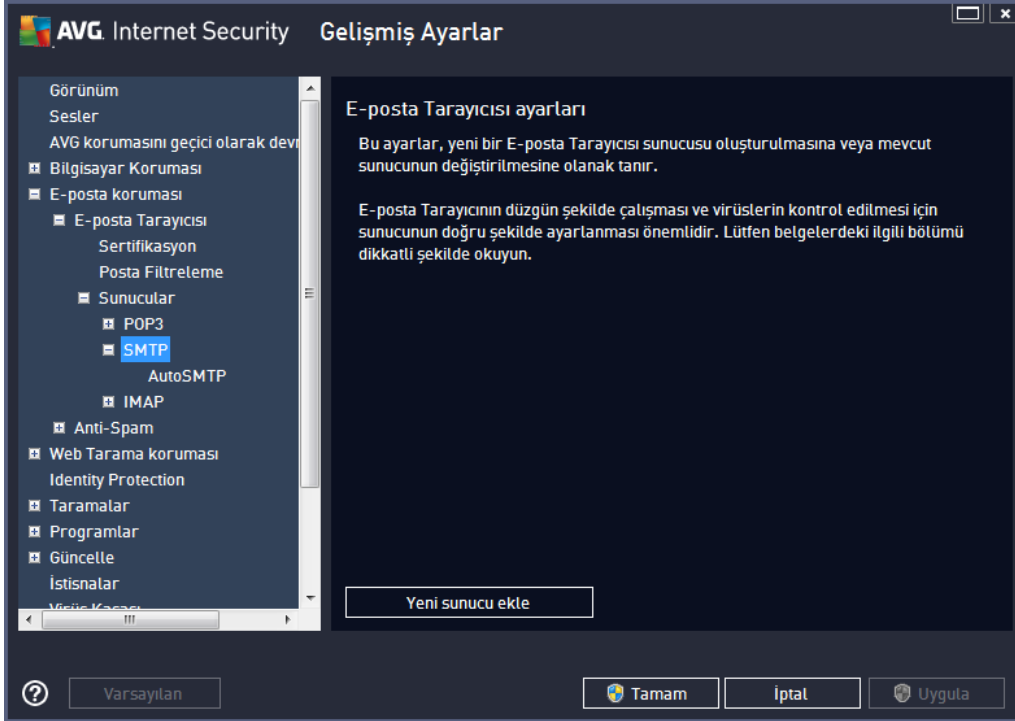


- **POP3 Sunucusunun Adı** - bu alanda yeni eklenen sunucuların adını belirtebilirsiniz (bir

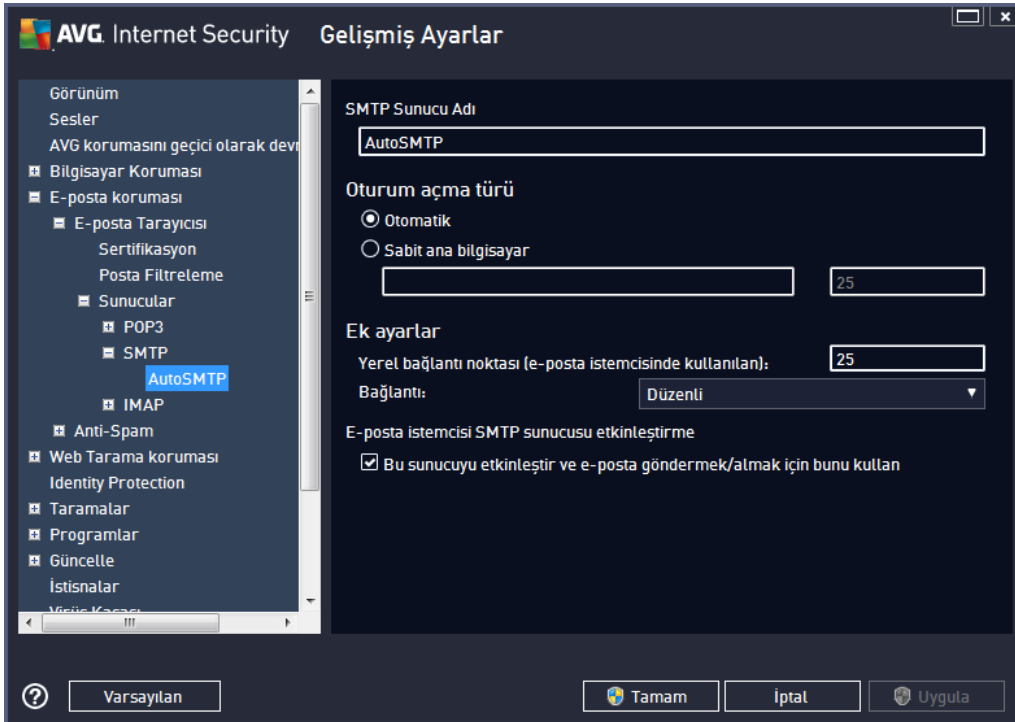


POP3 sunucusu eklemek için, sol menü ağacının POP3 ögesinin üzerinde sağ fare düğmesini tıklatin). Otomatik olarak oluşturulan "AutoPOP3" sunucuları için bu alan devre dışı bırakılmıştır.

- **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 veya işaretini kaldırın.



Bu iletişim kutusunda giden postalar için SMTP protokolünü kullanarak yeni bir [E-posta Tarayıcısı](#) sunucusu kurabilirsiniz:

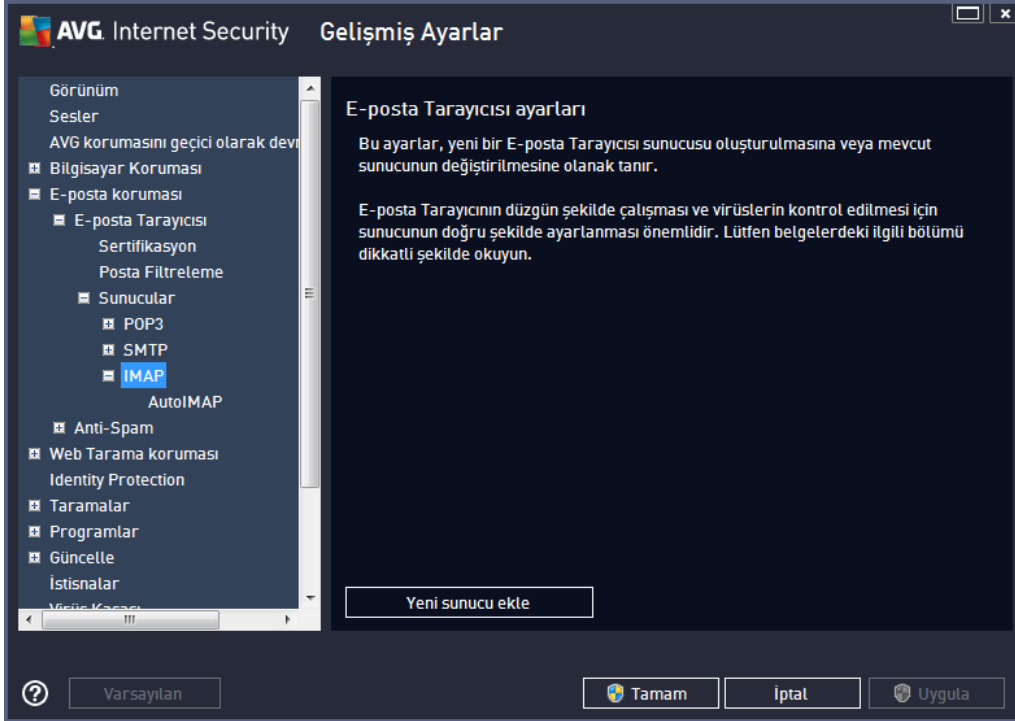


- **SMTP Sunucusunun Adı** - bu alanda yeni eklenen sunucuların adını belirtebilirsiniz (*bir*

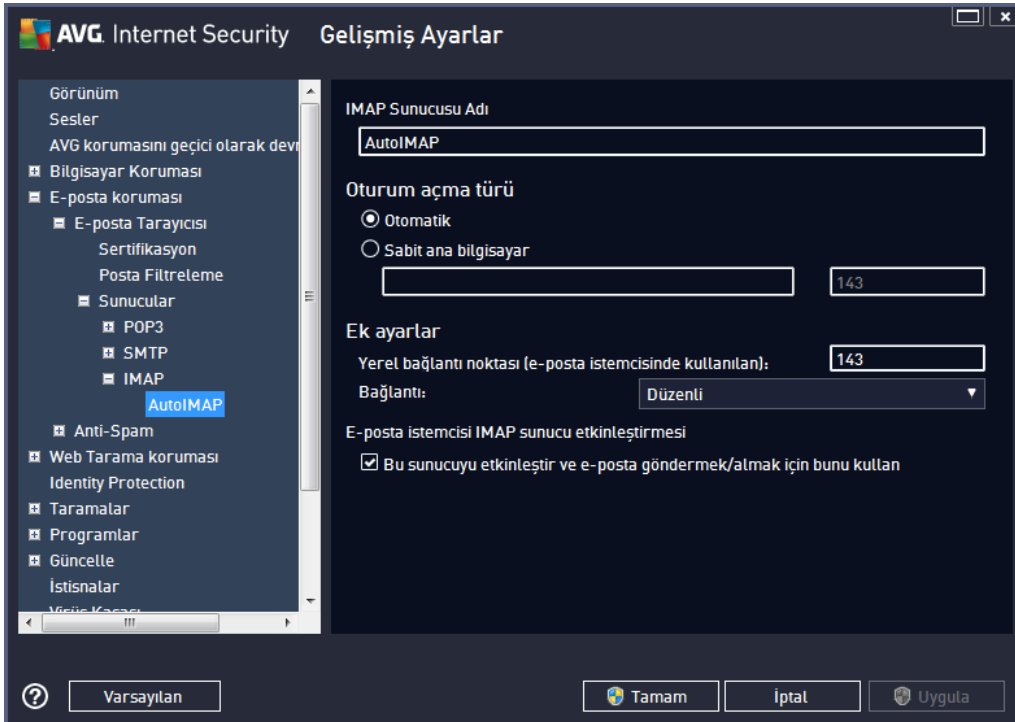


SMTP sunucusu eklemek için, sol menü ağacının SMTP ögesinin üzerinde sağ fare düğmesini tıklatin). Otomatik olarak oluşturulan "AutoSMTP" sunucuları için bu alan devre dışı bırakılmıştır.

- **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.
- **Diger 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.
  - **Baglanti** - 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 veya kutunun işaretini kaldırın



Bu iletişim kutusunda giden postalar için IMAP protokolünü kullanarak yeni bir [E-posta Tarayıcısı](#) sunucusu kurabilirsiniz:



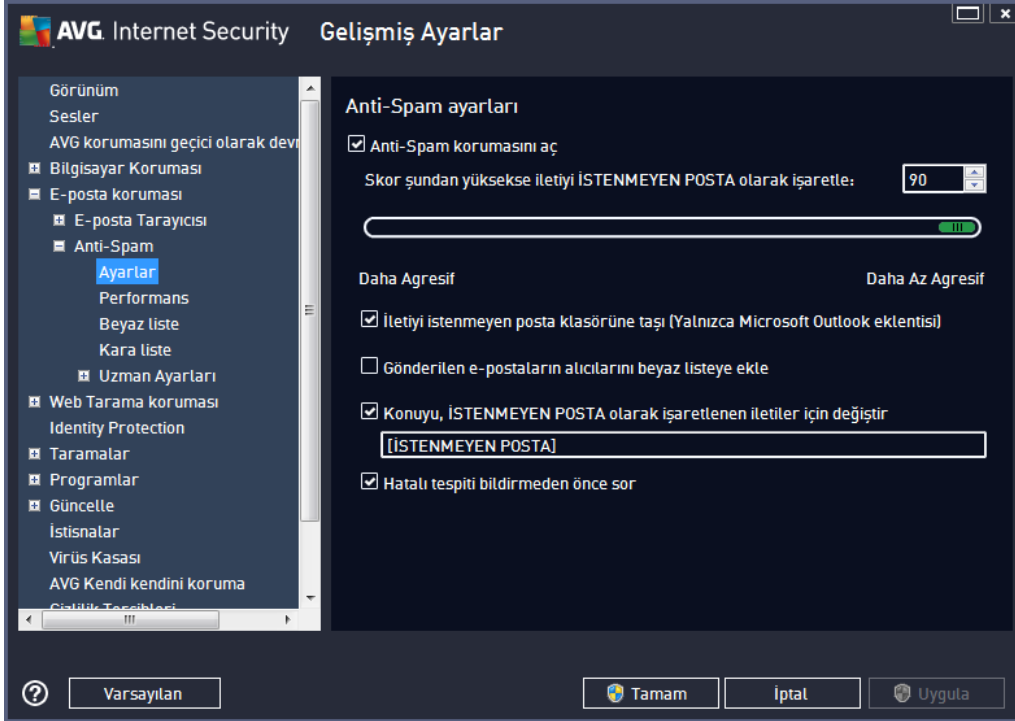
- **IMAP Sunucusunun Adı** - bu alanda yeni eklenen sunucuların adını belirtebilirsiniz (bir



IMAP sunucusu eklemek için, sol menü ağacının IMAP ögesinin üzerinde sağ fare düğmesini tıklayın). Otomatik olarak oluşturulan "AutoIMAP" sunucuları 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.
- **Diger 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.
  - **Baglantı** - bu açılır aşağı menüden, kullanılacak bağlantı türünü belirtebilirsiniz (normal/SSL/SSL varsayılan). Bir SSL bağlantısını 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 veya kutunun işaretini kaldırın

## 9.5.2. Anti-Spam



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

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

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

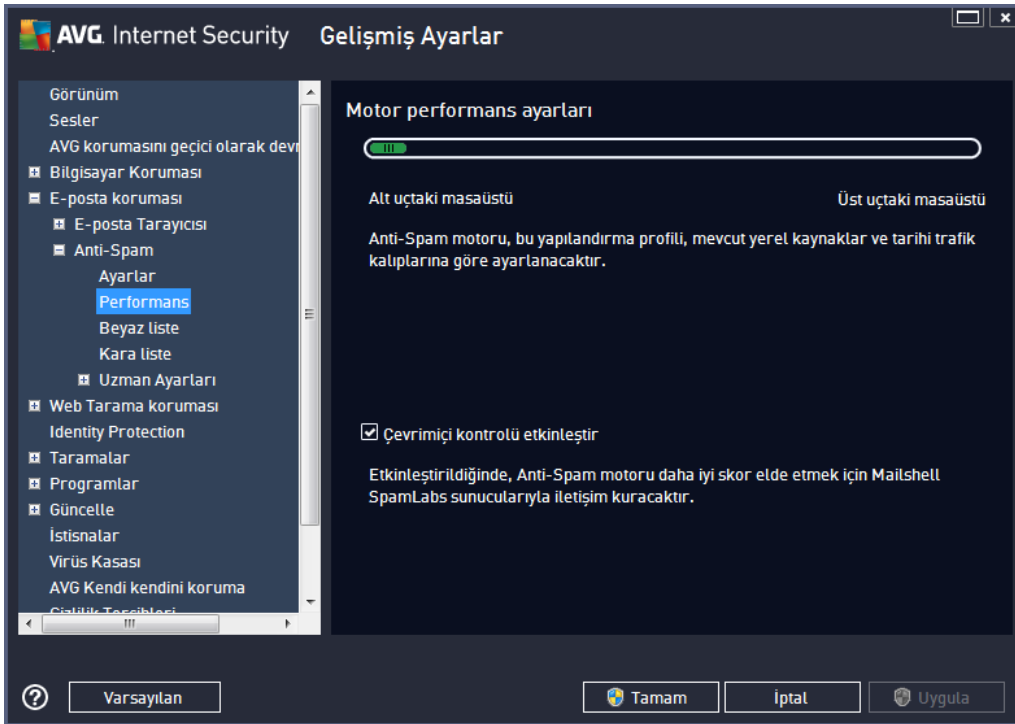
- **Değer 80-90** - istenmeyen posta olması muhtemel e-posta iletileri filtrelenecektir. İstenmeyen posta olmayan bazı postalar yanlışlıkla istenmeyen posta şeklinde etiketlenebilir.
- **Değer 60-79** - oldukça etkili bir yapılandırma olarak değerlendirilir. Olası istenmeyen posta iletileri filtrelenir, ancak istenmeyen posta olmayan bazı iletiler de yakalanabilir.
- **Değer 50-59** - çok etkili yapılandırma. İstenmeyen posta olmayan e-posta iletilerinin de gerçek istenmeyen posta iletileri ile birlikte yakalanma ihtimali çok yüksektir. Bu esik aralığı normal kullanım için önerilmez.

**Anti-Spam ayarları** iletisim kutusunda, tespit edilen istenmeyen postalara ne yapılacağını da belirleyebilirsiniz:



- **İletiyi istenmeyen posta klasörüne taşı** (yalnızca Microsoft Outlook eklentisi) - algılanan istenmeyen mesajların, otomatik olarak MS Outlook e-posta istemcinizin önemsiz posta klasörüne taşınmasını istiyorsanız bu onay kutusunu işaretleyin. Su anda, özellik diğer posta istemcilerinde desteklenmiyor.
- **Gönderilen e-postaların göndericilerini beyaz listeye** ekle - gönderilen e-postaların göndericilerinin tümüne güvendiğinizi onaylamak ve söz konusu kişilerin e-posta hesaplarından gönderilen e-postaların daima alınmasını istediğinizi teyit etmek için bu kutuyu işaretleyin.
- **Konuyu, İSTENMEYEN POSTA olarak işaretlenen iletiler için değiştir** - istenmeyen posta olarak işaretlenmiş e-postaların konu alanına belirli bir kelime ya da ibarenin yazılmasını istiyorsanız bu onay kutusunu işaretleyin; istenen metin, etkinleştirilen metin alanına yazılabilir.
- **Hatali tespiti bildirmeden önce sor** - yükleme süreci sırasında [Gizlilik Tercihleri](#) projesine katılmayı kabul ettiğinizde sağlanır. Kabul ettiyseniz, tespit edilen tehditlerin AVG'ye bildirilmesine izin verirsiniz. Rapor otomatik olarak oluşturulur. Ancak, gerçekten istenmeyen posta olarak sınıflandırılması gerekip gerekmediğinden emin olmak için, tespit edilen istenmeyen posta AVG'ye bildirilmeden önce sorulmasını istediğinizi onaylamak için bu onay kutusunu işaretleyebilirsiniz.

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



Tarama performans seviyesini **Alt uç masaüstü** / **Üst uç masaüstü** modları arasında yapılandırmak için çubuğu sola ya da sağa kaydırın.

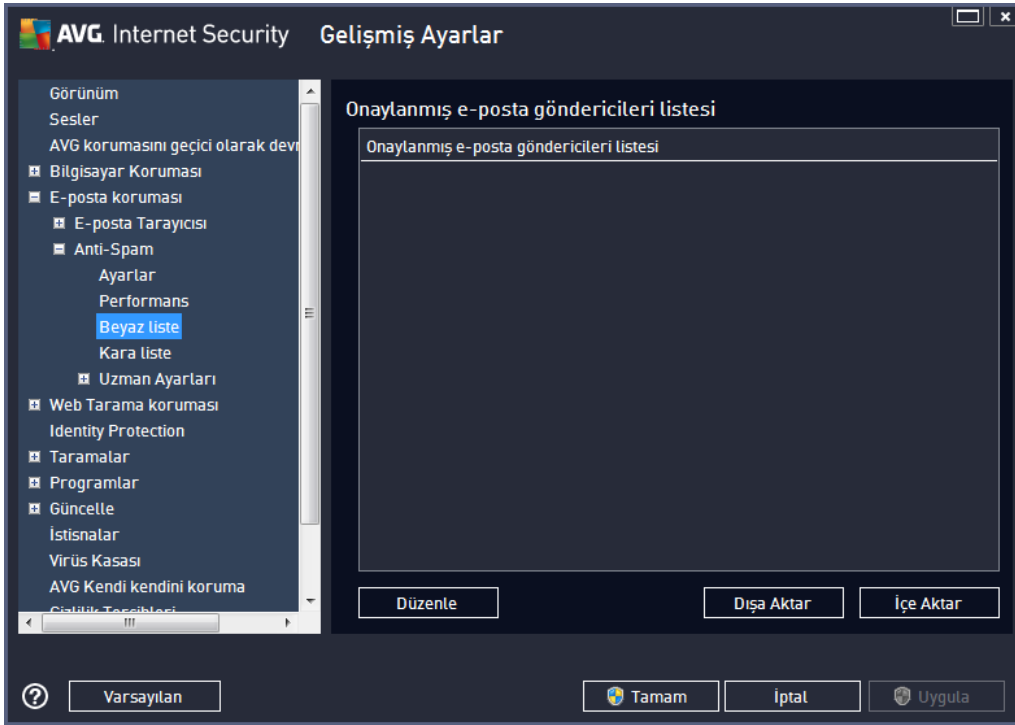


- **Alt uç masaüstü** - tarama işlemi sırasında istenmeyen postaların tespit edilmesi için herhangi bir kural kullanılmayacaktır. Tanımlama için sadece eğitim verileri kullanılacaktır. Bu mod, bilgisayar donanımlarınız çok eski değil ise genel kullanım için önerilmemektedir.
- **Üst uç masaüstü** - bu mod büyük miktarda bellek tüketir. Tarama işlemi sırasında istenmeyen postaları ayırt etmek için şu özellikler kullanılacaktır: kurallar ve istenmeyen posta veritabanı önbelleği, temel ve gelişmiş kurallar, istenmeyen postayı gönderenin IP adresi ve gönderici veritabanları.

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

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

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



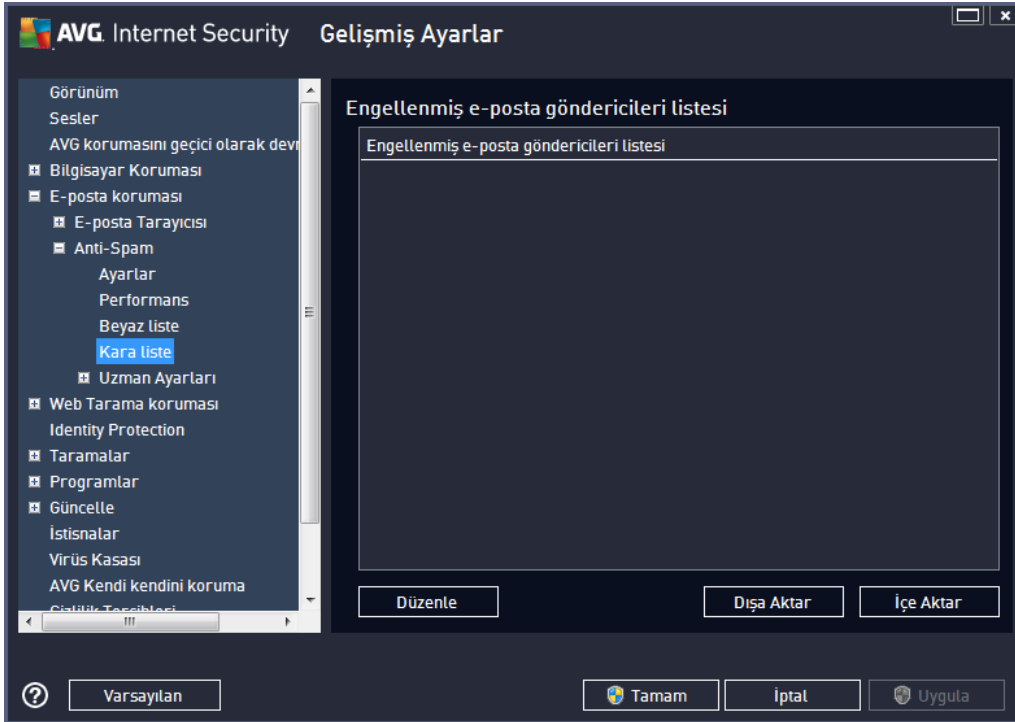
Düzenleme arayüzünde asla istenmeyen posta (istenmeyen posta) göndermeyecek göndericilerden oluşan bir liste düzenleyebilirsiniz. Bunun yanı sıra istenmeyen mesaj göndermediğini bildiğiniz tüm etki alanı adlarını içeren (örn. avg.com) bir liste de oluşturabilirsiniz. Söz konusu gönderici ve/veya etki alanı adı listelerini tamamladıktan sonra aşağıdaki yöntemlerden biriyle girebilirsiniz: e-posta adresini doğrudan girerek ya da tüm adres listesini bir kerede içe aktararak.

## Kontrol düğmeleri

Su kontrol düğmeleri bulunur:

- **Düzenle** - adres listesini manüel olarak doldurabileceğiniz iletişim kutusunu açmak için bu düğmeye basın (*bunun yani sıra kopyala ve yapıştır* yöntemini de kullanabilirsiniz). Satir basına bir öge ekleyin (*gönderen, etki alanı adı*).
- **Disa Aktar** - Kayitlari belli bir amaçla disa aktarmaya karar verirseniz, bu düğmeye basarak disa aktarabilirsiniz. Tüm kayitlar temel metin dosyasina kaydedilecektir.
- **İçe aktar** - hazirladiginiz e-posta adreslerinin/alan adlarinin bulunduđu bir metin dosyasina sahipseniz, bu düğmeyi seçerek kolayca içe aktarabilirsiniz. Dosya içeriğinin her satir için yalnızca bir öge (*adres, alan adı*) içermesi gerekir.

**Kara liste** ögesi iletileri her zaman istenmeyen posta olarak isaretlenecek engellenmiş gönderici e-posta adresleri ve alan adlarının genel bir listesinin bulunduğu bir iletişim kutusu açar.



Düzenleme arayüzünde, istenmeyen ileti (*istenmeyen posta*) göndermesini beklediğiniz göndericilerin bir listesini oluşturabilirsiniz. Ayrıca istenmeyen mesajlar beklediğiniz veya aldığınız tam alana adlarının (*örn. spammingcompany.com*) bir listesini oluşturabilirsiniz. Listelenen adreslerden/alan adlarından gelecek tüm e-postalar istenmeyen posta olarak tanımlanacaktır. Söz konusu gönderici ve/veya etki alanı listelerini tamamladıktan sonra aşağıdaki yöntemlerden biriyle girebilirsiniz: e-posta adresini doğrudan girerek ya da tüm adres listesini bir kerede içe aktararak.



## Kontrol düğmeleri

Su kontrol düğmeleri bulunur:

- **Düzenle** - adres listesini manüel olarak doldurabileceğiniz iletişim kutusunu açmak için bu düğmeye basın (*bunun yani sıra kopyala ve yapıştır* yöntemini de kullanabilirsiniz). Satır başına bir öge ekleyin (*gönderen, etki alanı adı*).
- **Disa Aktar** - Kayıtları belli bir amaçla disa aktarmaya karar verirsiniz, bu düğmeye basarak disa aktarabilirsiniz. Tüm kayıtlar düz bir metin dosyasına kaydedilecektir.
- **İçe aktar** - mevcut durumda hazırlamış olduğunuz bir gönderici / barındırma adı listesi varsa bu düğmeye basarak söz konusu dosyayı içe aktarabilirsiniz.

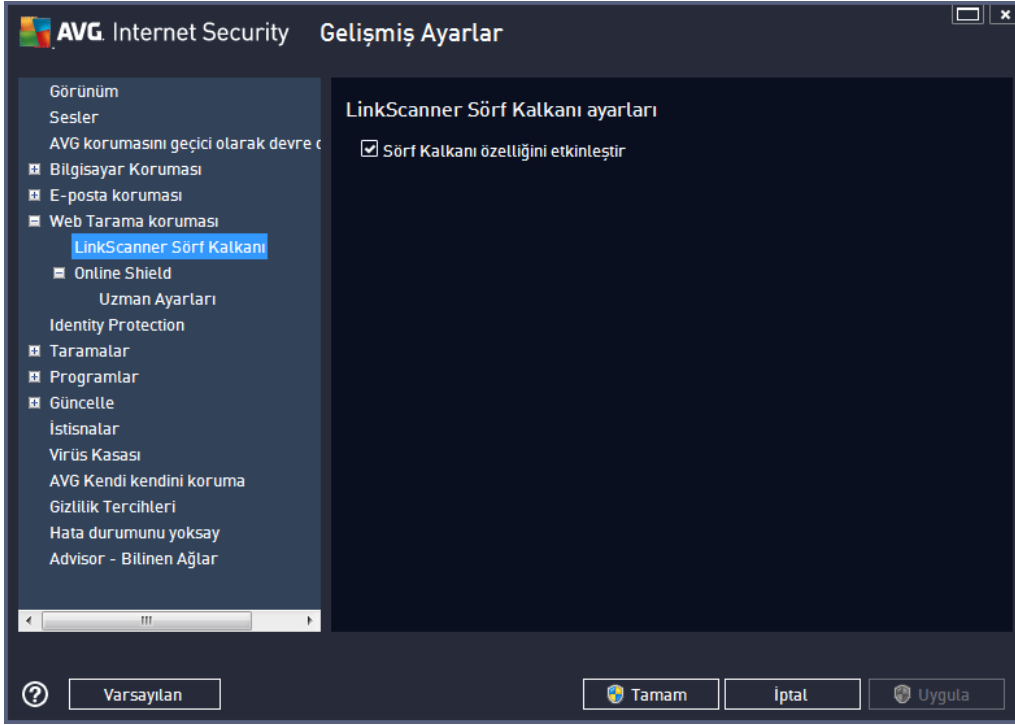
**Uzman Ayarları bölümü Anti-Spam özelliğine ilişkin kapsamlı ayar ve seçenekler sunar. Bu ayarlar özellikle deneyimli kullanıcılar, genel olarak e-posta sunucuları için en iyi korumayı sağlamak üzere istenmeyen postalardan korunmayı yapılandırmaya gereksinim duyan ağ yöneticileri için tasarlanmıştır. Bu nedenle, her bir iletişim kutusu için ayrıca yardım sunulmamaktadır. Ancak, ilgili her seçenek için kullanıcı arayüzünde doğrudan kısa bir açıklama bulunmaktadır. Spamcatcher (MailShell Inc.) uygulamasının gelişmiş ayarlarıyla ilgili bilgileriniz yeterli değilse, kesinlikle hiçbir ayarı değiştirmemenizi öneririz. Uygun olmayan her değişiklik performansın düşmesine veya bileşenin hatalı çalışmasına neden olabilir.**

Anti-Spam yapılandırmasını gelişmiş seviyede değiştirmeniz gerektiğini düşünüyorsanız lütfen kullanıcı arayüzünde belirtilen talimatları izleyin. Genel olarak, her iletişim kutusunda düzenleyebileceğiniz spesifik bir özellik bulursunuz. Özelliğin açıklaması mutlaka iletişim kutusunun içinde yer alır. Düzenleyebileceğiniz parametreler:

- **Filtreleme** - dil listesi, ülke listesi, onaylanan IP'ler, engellenen IP'ler, engellenen ülkeler, engellenen karakter setleri, sahte göndericiler
- **RBL** - RBL sunucuları, çoklu eşleşme, esik, zaman asimi, maksimum IP'ler
- **İnternet bağlantısı** - zaman asimi, proxy sunucusu, proxy kimlik doğrulaması

## 9.6. Web Tarama Koruması

**LinkScanner ayarları** iletişim kutusunda aşağıdaki özellikleri işaretleyebilir veya bunların işaretlerini kaldırabilirsiniz:



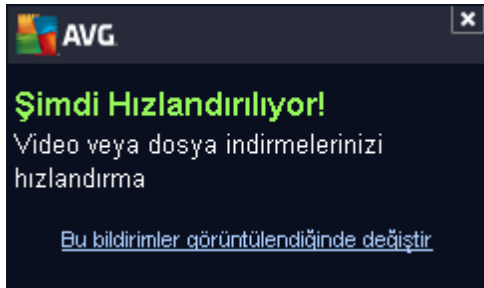
- **Sörf Kalkanı özelliğini etkinleştir** - (varsayılan olarak açık): erişim sağlandığı anda güvenlik açığı olan web sitelerine karşı (gerçek zamanlı) koruma sağlamak için etkinleştirin. Bilinen kötü amaçlı site bağlantıları ve güvenlik açığından yararlanan içerikler, kullanıcı bir web tarayıcısı (ya da HTTP kullanan diğer bir program) aracılığıyla erişim sağlandığında engellenir.
- **'LinkScanner Tarafından Korunmaktadır' ibaresi ekle...** - (varsayılan olarak kapalı): Facebook ve MySpace sosyal paylaşım ağlarından gönderilen etkin hiper bağlantıları içeren iletilerde Link Scanner denetimi ile ilgili sertifikasyon bildirimini girmek istediğinizi onaylamak için bu öğeyi işaretleyin.

### 9.6.1. Online Shield



**Online Shield** iletişim kutusu şu seçenekleri sunar:

- **Online Shield'i etkinleştir** (varsayılan olarak açık) - **Online Shield** hizmetinin tamamını etkinleştirir/devre dışı bırakır. Diğer **Online Shield** gelişmiş ayarları için lütfen [Web Koruması](#) adındaki sonraki iletişim kutusuna geçin.
- **AVG Hızlandırıcı ürününü etkinleştir** (varsayılan olarak açık) - AVG Hızlandırıcı hizmetini etkinleştirin veya devre dışı bırakın. AVG Hızlandırıcı daha düzgün çevrimiçi video oynatmaya izin verir ve ilave indirmeleri daha kolay hale getirir. Video hızlandırma işlemi çalışırken sistem tepsi açılır penceresi ile bilgilendirilirsiniz:



#### Tehdit bildirim modu

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



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

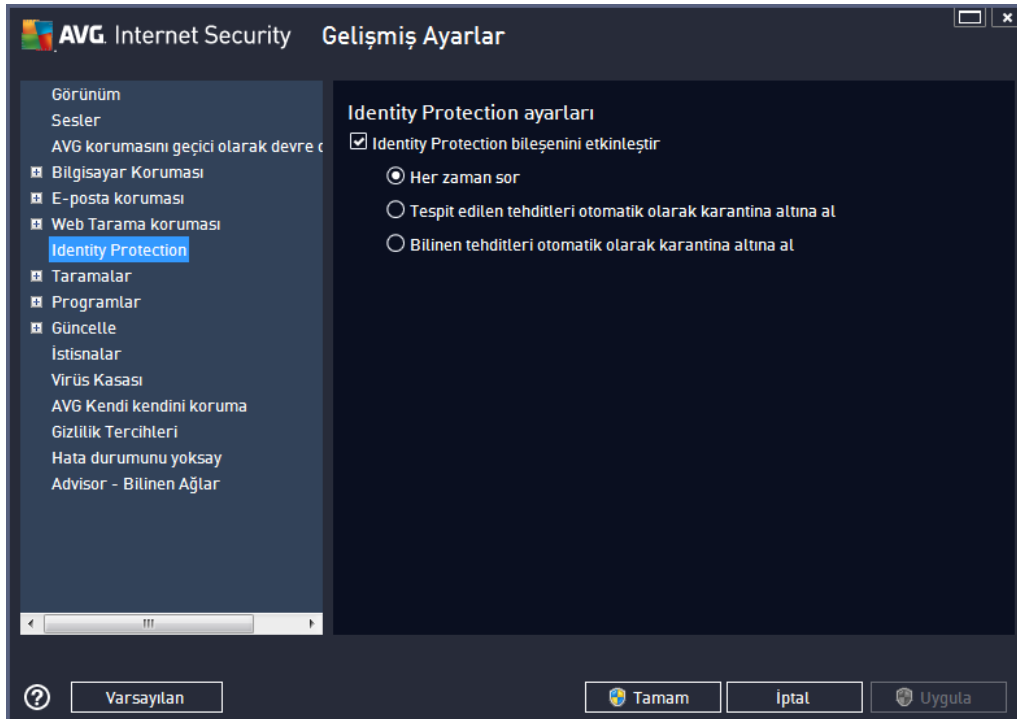
- **Web korumasını etkinleştir** - bu seçenek **Online Shield** bileşeninin www sayfalarının içeriğinin taranmasını gerçekleştirmesi gerektiğini onaylar. Bu seçenek açık olduğunda (*varsayılan olarak açık*), şu öğeleri de açabilir veya kapatabilirsiniz:
  - **Arsivleri denetle** - (*varsayılan olarak kapalı*): görüntülenecek www sayfasında bulunması muhtemel arşivlerin içeriğini tarayın.
  - **Potansiyel Olarak İstenmeyen Programları ve Casus Yazılım tehlikelerini rapor et** - (*varsayılan olarak açık*): Virüslerin yanı sıra casus yazılımları da taramak 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 öneririz.
  - **Potansiyel Olarak İstenmeyen Programlar gelişmiş grubunu rapor et** - (*varsayılan olarak kapalı*): 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.
  - **Bulussal analiz yöntemini kullan** - (*varsayılan olarak açık*): görüntülenecek web sitesinin içeriği bulussal analiz yöntemi kullanılarak taranır (*taranan nesnenin komutlarının sanal bir bilgisayar ortamında dinamik olarak canlandırılması*).

- o **Kapsamli taramayi etkinlestir** (varsayilan olarak kapali) - belirli durumlarda (bilgisayarınıza bulasma olmasından süpheleniyorsanız) yalnızca emin olmak üzere bilgisayarınızın bulasma olması çok zor olan alanlarını bile tarayan en kapsamlı tarama algoritmalarını etkinleştirmek için bu seçeneği işaretleyebilirsiniz. Ancak, bu yöntemin çok fazla zaman aldığını unutmayın.
- o **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, bulasmış olması halinde **Yerlesik Kalkan** tarafından tespit edilecektir.
- o **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 girebilirsiniz. Bu nedenle, bu işlemi yapmadan önce web sitesinin içeriğinin zararlı olmadığından emin olmanız gerekir.

## 9.7. Identity Protection

**Identity Protection** davranışsal teknolojiler ve yeni virüslere karşı sıfır gün koruması kullanarak sizi tüm kötü amaçlı yazılımlardan (casus yazılım, robotlar, kimlik hırsızlığı, ...) koruyan bir kötü amaçlı yazılımlara karşı koruma bileşenidir (bileşenlerin işlevleri hakkında ayrıntılı bilgi için lütfen [Identity](#) bölümüne bakın).

**Identity Protection ayarları**iletisim kutusu [Identity Protection](#) bileşeninin temel özelliklerini açmanızı/kapatmanızı sağlar:





**Identity Protection bileşenini etkinleştir** (varsayılan olarak açık) - [Identity](#) bileşenini kapatmak için işaretleyin.

**Zorunlu olmadıkça, bu işareti kaldırmamanızı önemle tavsiye ederiz!**

Identity Protection etkinleştirildiğinde, bir tehlike algılandığında ne yapacağınızı belirtebilirsiniz:

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

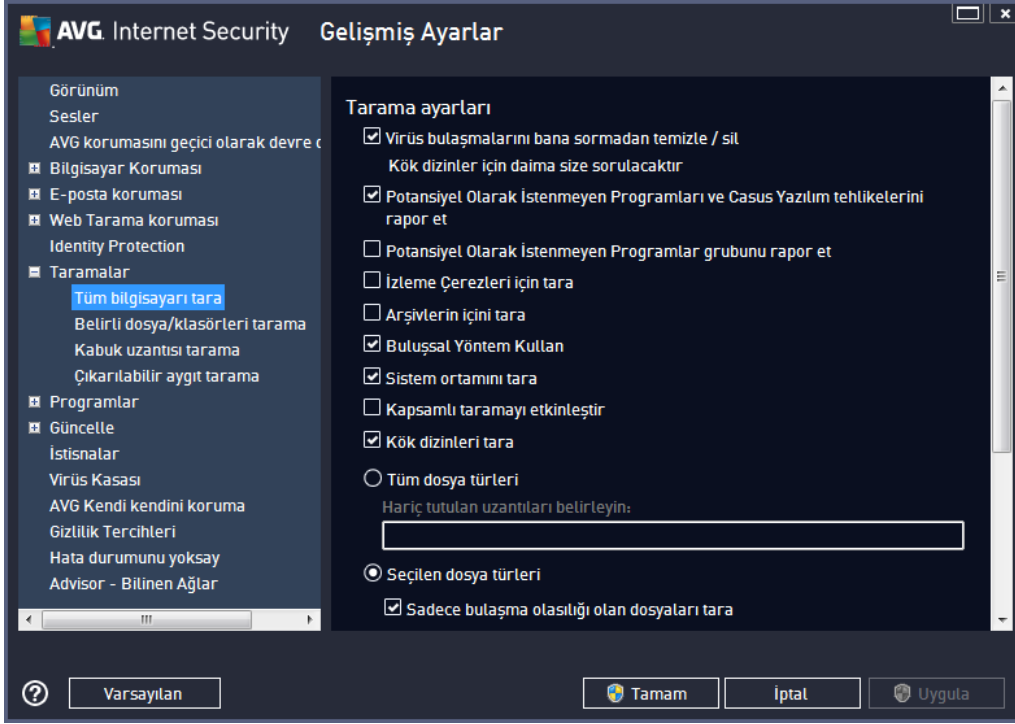
## 9.8. Taramalar

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

- [Tüm bilgisayarın taraması](#) - tüm bilgisayarın standart öntanımlı taramasıdır
- [Kabuk uzanti taraması](#) - seçilen nesnenin doğrudan Windows Gezgini ortamında taraması işlemidir
- [Belirli dosya veya klasörleri tarama](#) - bilgisayarınızın seçilen alanlarının tarandığı standart öntanımlı taramadır
- [Çıkartılabilir aygıt taraması](#) - bilgisayarınıza bağlanan çıkartılabilir aygıtların taraması işlemidir

### 9.8.1. Tüm bilgisayar taraması

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



### Tarama ayarları

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

- **Bulaşmayı bana sormadan temizle / kaldır** (varsayılan olarak açık) - Tarama sırasında virüs tanımlanırsa, bir giderme yazılımı mevcutsa otomatik olarak temizlenir. Bulaşmış dosya otomatik olarak temizlenemezse, bulaşmış nesne [Virüs Kasası](#)'na tasınır.
- **Potansiyel Olarak İstenmeyen Programları ve Casus Yazılım tehditlerini rapor et** (varsayılan olarak açık) - virüslerin yanı sıra casus yazılımları da taramak için isaretleyin. Casus yazılım, süpheli 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 öneririz.
- **Potansiyel Olarak İstenmeyen Programlar gelişmiş grubunu rapor et** (varsayılan olarak kapalı) - casus yazılımların, yani doğrudan üreticiden alınan tamamen zararsız olan, ancak daha sonra kötüye kullanılacak programların genişletilmiş paketinin tespit edilmesi için isaretleyin. Bu, bilgisayar güvenliğinizi daha da artıran ek bir önlemdir, ancak yasal programları da engelleyebilir ve bu yüzden varsayılan olarak kapalıdır.
- **İzleme Çerezleri için tara** (varsayılan olarak kapalı) - bu parametre, tespit edilmesi istenen çerezleri tanımlar; (HTTP çerezleri kimlik doğrulaması, izleme ve kullanıcılar hakkındaki



site tercihleri veya elektronik alisveris sepetlerinin ierigi gibi belirli bilgilerin korunmasi iin kullanilir)

- **Arsivleri tara** (varsayilan olarak kapali) - bu parametre, ZIP, RAR vb. arshiv dosyalarinin iinde sikistirilmis dosyalarin bile taranmasini saglar.
- **Bulussal Analiz Yöntemlerini Kullan** (varsayilan olarak aiktir) - bulussal analiz yöntemi ( taranan nesnenin komutlarinin sanal bir bilgisayar ortaminda dinamik olarak canlandırılması ) tarama sirasinda kullanılacak virüs tespiti yöntemlerinden biridir.
- **Sistem ortamini tara** (varsayilan olarak aiktir) - tarama islemi, bilgisayarinizin sistem alanlarini da kontrol edecektir.
- **Kapsamli taramayi etkinlestir** (varsayilan olarak kapali) - belirli durumlarda (bilgisayarınıza bulasma olmasindan süpheleniyorsanız) yalnızca emin olmak üzere bilgisayarınızın bulasma olması çok zor olan alanlarını bile tarayan en kapsamlı tarama algoritmalarını etkinlestirmek iin bu seçeneği isaretleyebilirsiniz. Ancak, bu yöntemin çok fazla zaman aldığını unutmayın.
- **Rootkit'leri tara** (varsayilan olarak aik) - [Anti-Rootkit](#) taramasi bilgisayarınızı olasi rootkit'lere, örneğin bilgisayarınızda kötü amaçlı etkinlik ierebilecek programlar ve teknolojilere karsi tarar. Bir kök dizin algilanirsa, bu, bilgisayarınızda mutlaka virüs olduğu anlamına gelmez. Bazı durumlarda, belirli sürücüler veya normal uygulamaların bölümleri kök dizin olarak yanlış algılanabilir.

Ayrıca tarama iin dosya türlerini de belirlemeniz gerekir

- **Tüm dosya türleri** , virgülle ayrılmis (kaydedilirken virgüller noktali virgüle dönüşür) dosya uzantıları listesi saglayarak taramadan hari tutulacakların taranmaması iin tanımlama olasılığı saglar;
- **Seili dosya türleri** - yalnızca virüs bulasabilme olasılığı olan dosyaları taramayı istediğinizi belirtebilirsiniz (virüs bulasamayan dosyalar taranmayacaktır, örneğin, bazı düz metin dosyaları veya bazı diğeri alistirilamayan dosyalar); ortam dosyaları (video, ses dosyaları - bu onay kutusunun isaretini kaldırırsanız, bu dosyalar genellikle çok büyük olduğundan ve virüs bulasma olasılıkları çok az olduğundan tarama süresini daha da azaltır). Tekrar, her zaman taranması gereken dosyaları uzantılarına göre belirtebilirsiniz.
- Isteğe baėlı olarak, **Uzantıları olmayan dosyaları taramaya** da karar verebilirsiniz ve bu seçenek varsayilan olarak aiktir ve gerçekten bir nedeniniz yoksa deėistirmemeniz önerilir. Uzantısı olmayan dosyalar süpheli olabilir ve her zaman taranmalıdır.

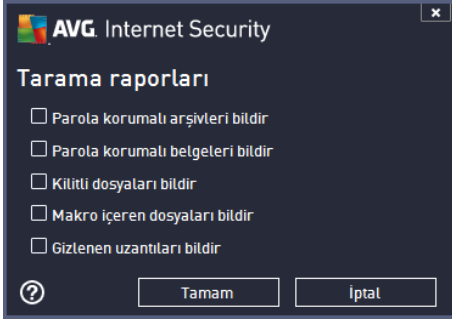
## Taramanın ne kadar hızlı tamamlanacağını ayarla

**Taramanın ne kadar hızlı tamamlanacağını ayarla** bölümünde, sistem kaynakları kullanımına baėlı olarak istediğiniz tarama hızını seçebilirsiniz. Bu seçenek varsayilan olarak otomatik kaynak kullanımının *kullanıcıya duyarlı* düzeyine ayarlanmıştır. Tarama işleminin daha hızlı ilerlemesini istiyorsanız tarama işleminin daha kısa sürecektir fakat tarama işleminin sırasında sistem kaynakları oldukça yüklü bir şekilde kullanılacak ve bilgisayar üzerindeki diğeri işlemleri yavaşlatacaktır (bu seçenek bilgisayarınız aikken kullanılmadığı sırada seçilebilir). Öte yandan, tarama süresini uzatarak sistem kaynaklarının kullanımını azaltabilirsiniz.



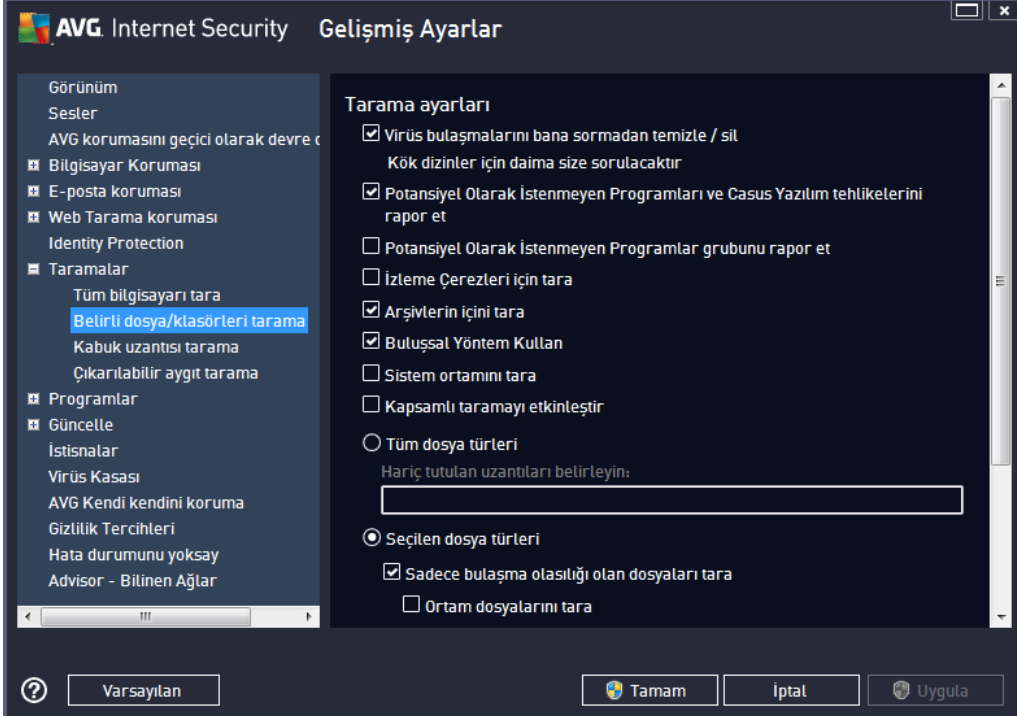
### Ek tarama raporlarını ayarla...

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



### 9.8.2. Belirli dosya/klasörleri tarama

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

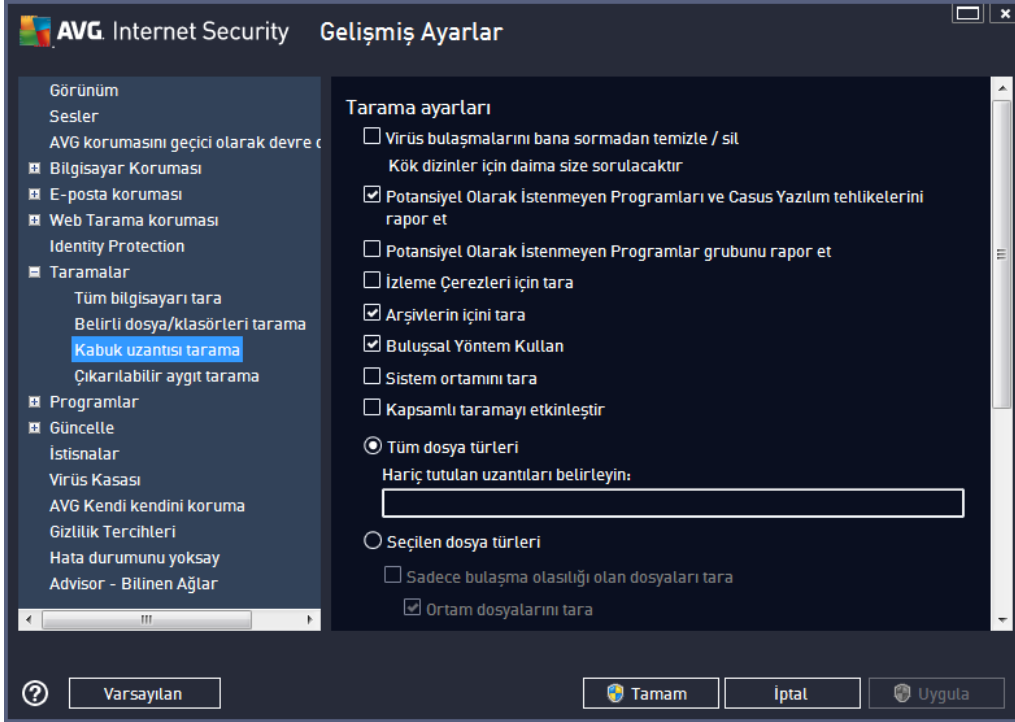


Bu yapılandırma iletişim kutusunda ayarlanan tüm parametreleri [Belirli dosya ya da klasörleri tara](#) ile tarama sırasında seçilen alanlar için geçerlidir!

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

### 9.8.3. Kabuk uzantısı tarama

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



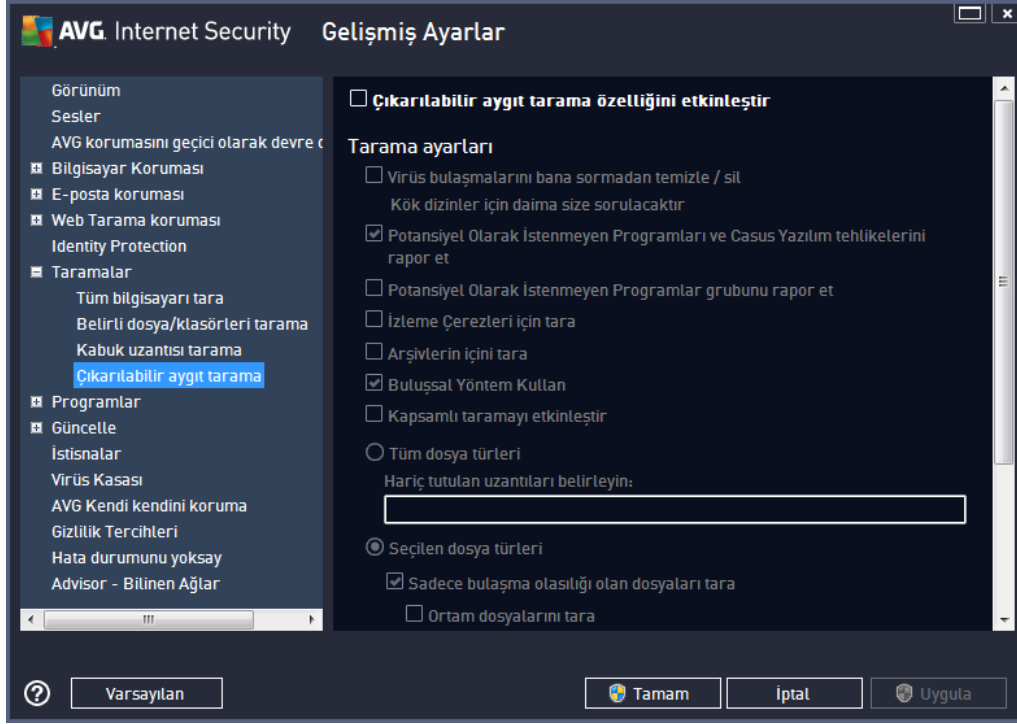
Parametre listesi, [Tüm bilgisayari tarama](#) ögesinin parametre listesi ile aynıdır. Bununla birlikte, varsayılan ayarlar farklılık gösterebilir (*örneğin, Tüm bilgisayarın taraması islevi arşivleri denetlemez ancak sistem ortamını denetler; Kabuk Uzantısı Tarama'da ise durum tam tersidir*).

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

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

#### 9.8.4. Çıkarılabilir aygıt tarama

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



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

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

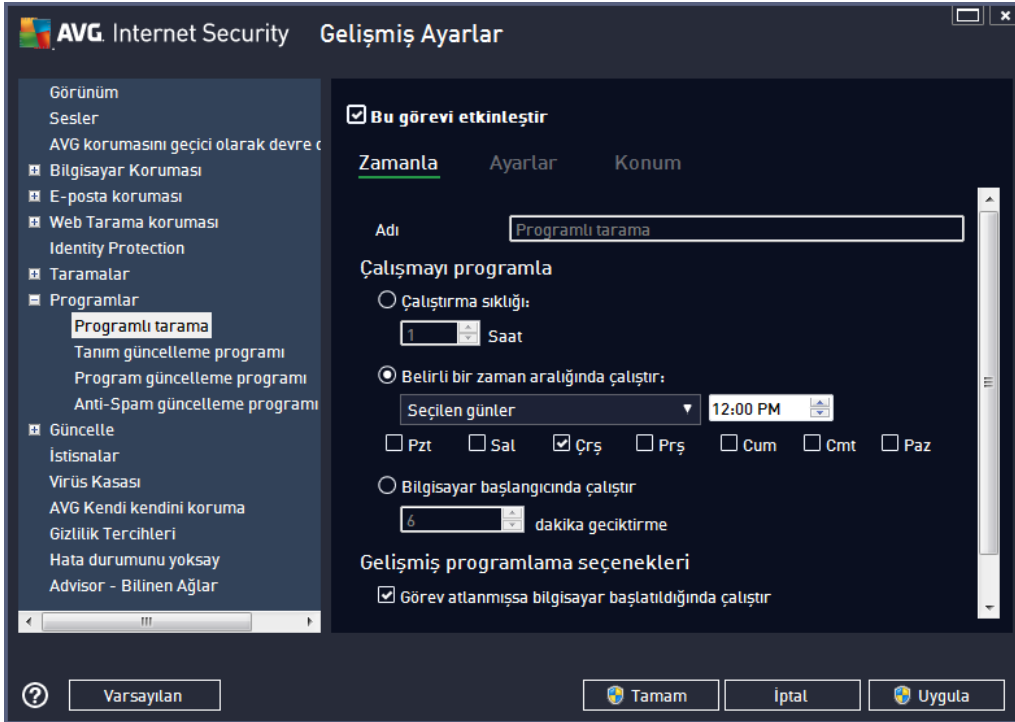
#### 9.9. Programlar

**Programlar** bölümünde aşağıdaki bileşenlerin öntanımlı ayarlarını düzenleyebilirsiniz:

- [Zamanlanan tarama](#)
- [Tanım güncelleme programı](#)
- [Program güncelleme programı](#)
- [Anti-Spam güncelleme programı](#)

### 9.9.1. Programlanmış Tarama

Planlanan tarama parametreleri üç sekmeden düzenlenebilir (*ya da yeni bir zamanlama ayarlanabilir*). Her sekmede **Bu görevi etkinleştir** ögesini isaretleyerek veya söz konusu ögenin isaretini kaldırarak zamanlanan testi geçici olarak devre dışı bırakabilir ve gerektiğinde yeniden açabilirsiniz:



**Ad** adındaki metin alanı (*tüm varsayılan zamanlamalar için devre dışı bırakılmıdır*) bu zamanlamaya program satıcısı tarafından atanan adı gösterir. Yeni eklenen zamanlamalar için (*sol gezinti ağacındayken Taramayı programla* ögesi üzerinde *sağ tıklatarak* yeni bir zamanlama ekleyebilirsiniz) kendi adınızı belirtebilirsiniz ve bu durumda metin alanı düzenleme için açılacaktır. Programladığınız taramaları diğerlerinden kolaylıkla ayırabilmek için her zaman taramalarınıza kısa, açıklayıcı adlar vermeye çalışın.

**Örnek:** Taramayı "Yeni Tarama" veya "Taramam" adıyla adlandırmanız uygun değildir çünkü bu adlar, taramanın fiilen neyi kontrol ettiğini açıklamaz. Diğer bir yandan "Sistem alanı taraması" vb. 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:

#### Çalışmayı programla

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



tanımlanarak (**Bilgisayar başlangıcında çalıştır**) tanımlanabilir.

### Gelişmiş zamanlama seçenekleri

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

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.



**Ayarlar** 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 yapılandırmayı olduğu gibi muhafaza etmeniz önerilir.**

- **Bulasmayı bana sormadan temizle / kaldır** (varsayılan olarak açık): Tarama sırasında virüs tanımlanırsa, bir giderme yazılımı mevcutsa otomatik olarak temizlenir. Bulasmis dosya otomatik olarak temizlenemezse, bulasmis nesne [Virüs Kasası](#)'na tasınır.
- **Potansiyel Olarak İstenmeyen Programları ve Casus Yazılım tehditlerini rapor et** (varsayılan olarak açık): virüslerin yanı sıra casus yazılımları da taramak için işaretleyin. Casus yazılım, şüpheli kötü amaçlı yazılım kategorisini ifade eder: genellikle bir güvenlik



riskini olusturmasına ragmen bu programlardan bazilari bilerek yuklenebilir. Bilgisayarinizin guvenligini artirdigindan, bu ozelligi etkin durumda tutmanizi öneririz.

- **Potansiyel Olarak Istenmeyen Programlar gelismis grubunu rapor et** (varsayilan olarak kapali): casus yazilimlarin, yani dogrudan ureticiden alinan tamamen zararsiz olan, ancak daha sonra kötüye kullanilabilecek programlarin genisletilmis paketinin tespit edilmesi için isaretleyin. Bu, bilgisayar guvenliginizi daha da artiran ek bir önlemdir, ancak yasal programlari da engelleyebilir ve bu yüzden varsayilan olarak kapalıdır.
- **Izleme Çerezleri için tara** (varsayilan olarak kapali): bu parametre, tarama sirasinda tespit edilmesi istenen çerezleri tanimlar (*HTTP çerezleri kimlik dogrulaması, izleme ve kullanıcılar hakkındaki site tercihleri veya elektronik alisveris sepetlerinin içeriği gibi belirli bilgilerin korunması için kullanılır*).
- **Arsivleri tara** - (varsayilan olarak kapali): bu parametre, tarama isleminin ZIP, RAR gibi belirli bir arşiv türü ile sikistirilmiş olsa bile tüm dosyaların taranması gerektigini belirtir.
- **Bulussal Analiz Yöntemlerini Kullan** - (varsayilan olarak açıktır). Bulussal analiz yöntemi (*taranan nesnenin komutlarının sanal bir bilgisayar ortamında dinamik olarak canlandırılması*) tarama sirasinda kullanılacak virüs tespiti yöntemlerinden biridir.
- **Sistem ortamını tara** - (varsayilan olarak açıktır). Tarama islemi, bilgisayarınızın sistem alanlarını da kontrol edecektir.
- **Kapsamli taramayı etkinleştir** (varsayilan olarak kapali) belirli durumlarda (*bilgisayarınıza bulasma olmasından şüpheleniliyorsa*) yalnızca emin olmak üzere bilgisayarınızın bulasma olması çok zor olan alanlarını bile tarayan en kapsamli tarama algoritmalarını etkinleştirmek için bu seçeneği isaretleyebilirsiniz. Ancak, bu yöntemin çok fazla zaman aldığını unutmayın.
- **Kök dizinleri tara** (varsayilan olarak açık): Anti-Rootkit taraması bilgisayarınızı olası rootkitlere, örneğin bilgisayarınızda kötü amaçlı etkinlik içerebilecek programlar ve teknolojilere karşı tarar. Bir kök dizin algılanırsa, bu, bilgisayarınızda mutlaka virüs olduğu anlamına gelmez. Bazı durumlarda, belirli sürücüler veya normal uygulamaların bölümleri kök dizin olarak yanlış algılanabilir.

Ayrıca tarama için dosya türlerini de belirlemeniz gerekir

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

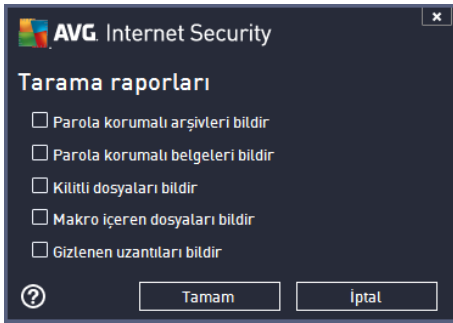


### Taramanın ne kadar hızlı tamamlanacağını ayarla

Bu bölümde ayrıca istenen tarama hızını, sistemin kaynak kullanımına bağlı olarak belirleyebilirsiniz. Varsayılan olarak, bu seçenek otomatik kaynak kullanımının *kullanıcıya duyarlı* seviyesine ayarlıdır. Tarama işleminin daha hızlı ilerlemesini istiyorsanız tarama işlemi daha kısa sürecektir fakat tarama işlemi sırasında sistem kaynakları oldukça yüklü bir şekilde kullanılacak ve bilgisayar üzerindeki diğer işlemleri yavaşlatacaktır (*bu seçenek bilgisayarınız açıkken kullanılmadığı sırada seçilebilir*). Öte yandan, tarama süresini uzatarak sistem kaynaklarının kullanımını azaltabilirsiniz.

### Ek tarama raporlarını ayarla

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



### Bilgisayar kapatma seçenekleri

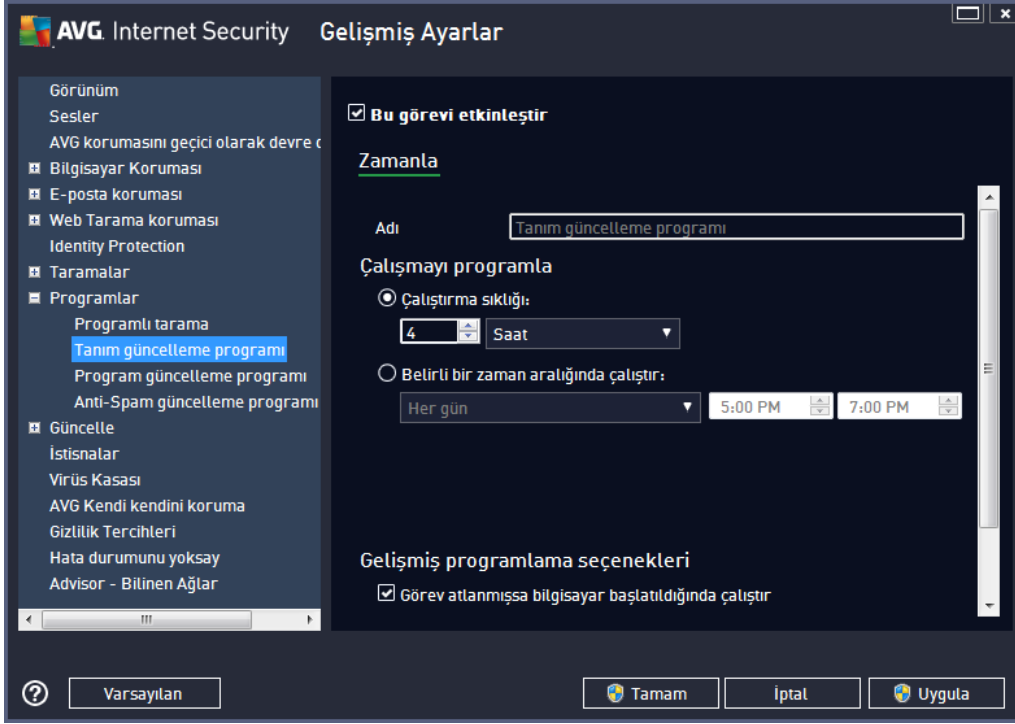
**Bilgisayar kapatma seçenekleri** bölümünde çalışan tarama işlemi bittiginde bilgisayarın otomatik olarak kapatılması gerekip gerekmediğine karar verebilirsiniz. Bu seçeneği seçerseniz (**Tarama bittikten sonra bilgisayarı kapat**) bilgisayar mevcut durumda kilitli olsa bile bilgisayarın kapatılmasını sağlayan bir seçeneğin bulunduğu bir pencere açılacaktır (**Bilgisayar kilitliyse bilgisayarı kapanmaya zorla**).



**Konum** sekmesinde, [tüm bilgisayarı tarama](#) veya [belirli dosya veya klasörleri taramayı](#) programlamak isteyip istemediğinizi tanımlayabilirsiniz. Belirli dosya ve klasörleri taramayı seçerseniz, bu iletişim kutusunun alt kısmında görüntülenen ağaç yapısı etkinlesir ve taranacak klasörleri seçebilirsiniz.

## 9.9.2. Tanım güncelleme programı

**Gerçekten gerekliyse Bu görevi etkinleştir** ögesinin isaretini kaldırarak zamanlanmış tanımları geçici olarak devre dışı bırakabilir ve daha sonra tekrar açabilirsiniz:



Bu iletişim kutusunda tanım güncelleme zamanlaması parametrelerinden bazılarını ayrıntılarıyla yapılandırabilirsiniz. **Ad** adındaki metin alanı (*tüm varsayılan zamanlamalar için devre dışı bırakılmıdır*) bu zamanlamaya program satıcısı tarafından atanan adı gösterir.

### Programlı çalıştırma

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

### Gelişmiş programlama seçenekleri

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

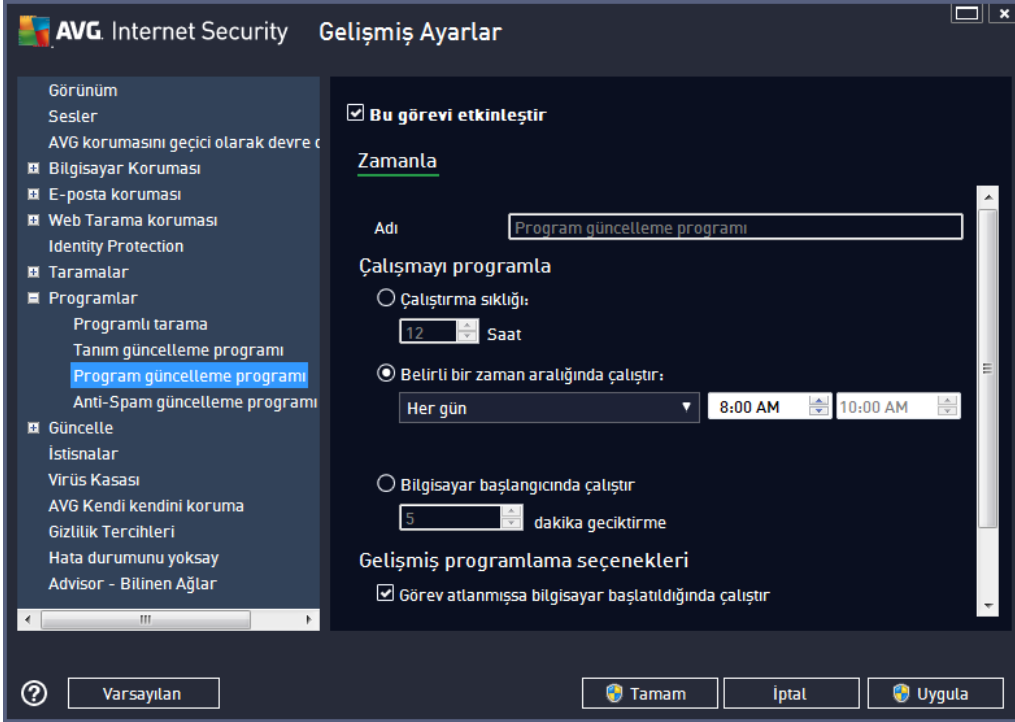
### Diğer güncelleme ayarları

Son olarak, **İnternet bağlantısı kurulduğunda güncellemeyi yeniden çalıştır** seçeneğini işaretleyerek internet bağlantısı kesildiğinde ve güncelleme işlemi başarısız olduğunda, internet bağlantısı yeniden sağlanır sağlanmaz yeniden başlatılmasını sağlayın. 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 gerekiyorsa Bu görevi etkinleştir** öğesinin işaretini kaldırarak zamanlanmış programı geçici olarak devre dışı bırakabilir ve daha sonra tekrar açabilirsiniz:



**Ad** adındaki metin alanı (*tüm varsayılan zamanlamalar için devre dışı bırakılmıdır*) bu zamanlamaya program satıcısı tarafından atanan adı gösterir.

#### Çalışmayı programla

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

#### Gelişmiş programlama seçenekleri

Bu bölümde, bilgisayar düşük güç modundaydı ya da tamamen kapatılmışsa hangi koşullar altında program güncellemesinin başlatılması/baslatılmaması gerektiğini belirleyebilirsiniz.

#### Diğer güncelleme ayarları

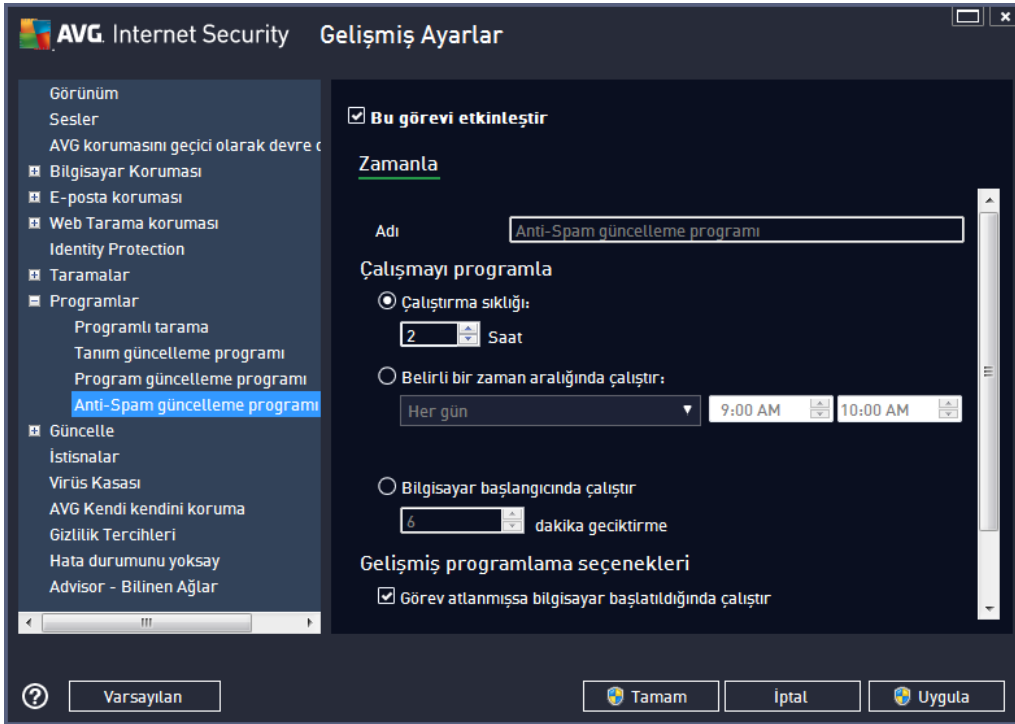


**Internet bağlantısı kurulduğunda güncellemeyi yeniden çalıştır** seçeneğini işaretleyerek internet bağlantısı kesildiğinde ve güncelleme işlemi başarısız olduğunda, internet bağlantısı yeniden sağlanır sağlanmaz yeniden başlatılmasını sağlayın. Planlanan güncelleme işlemi sizin belirlediğiniz tarih 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).

**Not:** Programlanmış bir program güncellemesinin zaman çakışması olursa ve programlı tarama gerçekleşirse, güncelleme işlemi yüksek önceliklidir ve tarama kesilir.

#### 9.9.4. Anti-Spam Güncelleme Zamanlaması

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



Bu iletişim kutusunda güncelleme zamanlaması parametrelerinden bazılarını ayrıntılarıyla yapılandırabilirsiniz. **Ad** adındaki metin alanı (*tüm varsayılan zamanlamalar için devre dışı bırakılmıştır*) bu zamanlamaya program satıcısı tarafından atanan adı gösterir.

#### Programlı çalıştırma

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

#### Gelişmiş program seçenekleri



Bu bölümde, bilgisayar düşük güç modundaydı veya tamamen kapatılmışsa hangi koşullar altında Anti-Spam güncellemesinin baslatılması/baslatılmaması gerektiğini belirleyebilirsiniz.

### Diger güncelleme ayarlari

**Internet bağlantısı kurulduğunda güncellemeyi yeniden çalıştır** seçeneğini işaretleyerek internet bağlantısı kesildiğinde ve Anti-Spam güncelleme işlemi başarısız olduğunda, internet bağlantısı yeniden sağlanır sağlanmaz yeniden baslatılmasını sağlayın.

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

## 9.10. Güncelleme

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



### Dosya güncelleme zamanı

Bu bölümde, güncelleme işlemi bilgisayarınızın yeniden baslatılmasını gerektiriyorsa, üç seçenek arasından birini belirleyebilirsiniz. Güncellenmenin tamamlanması işlemi, bilgisayarınızın bir sonraki yeniden baslatılma sürecine zamanlanabilir veya yeniden baslatma işlemi hemen yapabilirsiniz:

- **Kullanıcıdan onay iste** (varsayılan) - [güncelleme işleminin](#) tamamlanması için gereken bilgisayarın yeniden baslatılması süreci için onayınız istenir



- **Hemen yeniden baslat** - [güncelleme islemi](#) tamamlanir tamamlanmaz onayiniz istenmeden bilgisayarınız yeniden baslatilacaktir
- **Bilgisayarın bir sonraki yeniden baslatilmasında tamamla** - [güncelleme isleminin](#) tamamlanması bilgisayarın bir sonraki yeniden baslatilmasına kadar ertelenir. Lütfen bu seçeneğin yalnızca bilgisayarın düzenli olarak (en azından günde bir kez) yeniden baslatildigini bilmeniz halinde önerildigini unutmayın!

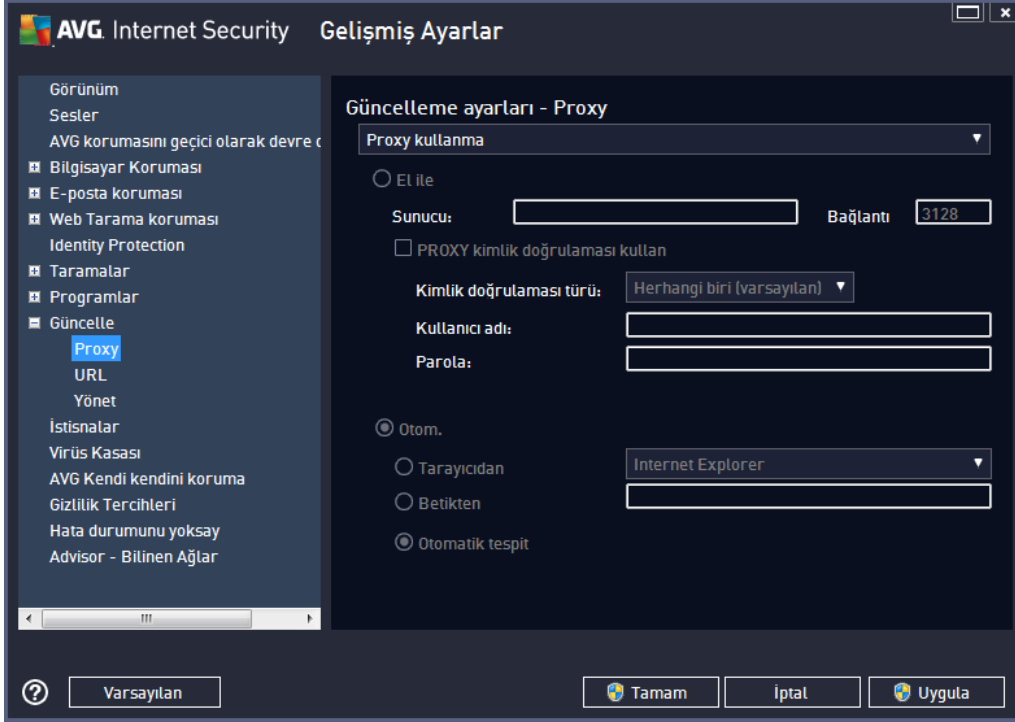
### Güncelleme sonrası bellek tarama

Basariyla tamamlanan her güncelleme sonrasında yeni bir bellek taraması baslatmak istediginizi belirtmek için bu onay kutusunu isaretleyin. En son indirilen güncelleme yeni virüs tanımlarını içerebilir ve bunlar taramaya hemen uygulanir.

### Ek güncelleme seçenekleri

- **Her program güncellemesinden sonra sistem geri yükleme noktası olustur** - AVG programının güncelleme islemi başlamadan önce her seferinde geri yükleme noktası olusturulur Güncelleme isleminin başarısız olması ve işletim sisteminizin çökmesi halinde işletim sisteminizi bu noktaya geri döndürebilirsiniz. Bu seçeneğe Baslat / Tüm Programlar / Donatılar / Sistem araçları / Sistem Geri Yükleme yoluyla erisebilirsiniz fakat değişikliklerin sadece uzman kullanıcılar tarafından yapılması önerilmektedir! Bu fonksiyonu kullanmak istiyorsanız bu kutucuğu isaretleyin.
- **DNS güncellemesini kullan** (varsayılan olarak açık) - bu öğe isaretlendiğinde güncelleme islemi baslatildığında **AVG Internet Security 2013** en yeni veritabanı sürümüyle ve DNS sunucusundaki en yeni program sürümüyle ilgili bilgileri arar. Yalnızca en küçük, kesin olarak gerekli güncelleme dosyaları indirilir ve uygulanir. 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 açık) - güncelleme isleminin 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 isaretleyin.

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

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

#### Manüel yapılandırma

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

- **Sunucu** - sunucunun IP adresini ya da sunucunun adını girin
- **Bağlantı Noktası** - İnternet erişimine açık bağlantı noktasının numarasını girin (*varsayılan olarak bu değer 3128 olarak atanmıştır fakat istediğiniz doğrultusunda değiştirebilirsiniz - emin değilseniz lütfen ağ yöneticiniz ile irtibat kurun*)



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

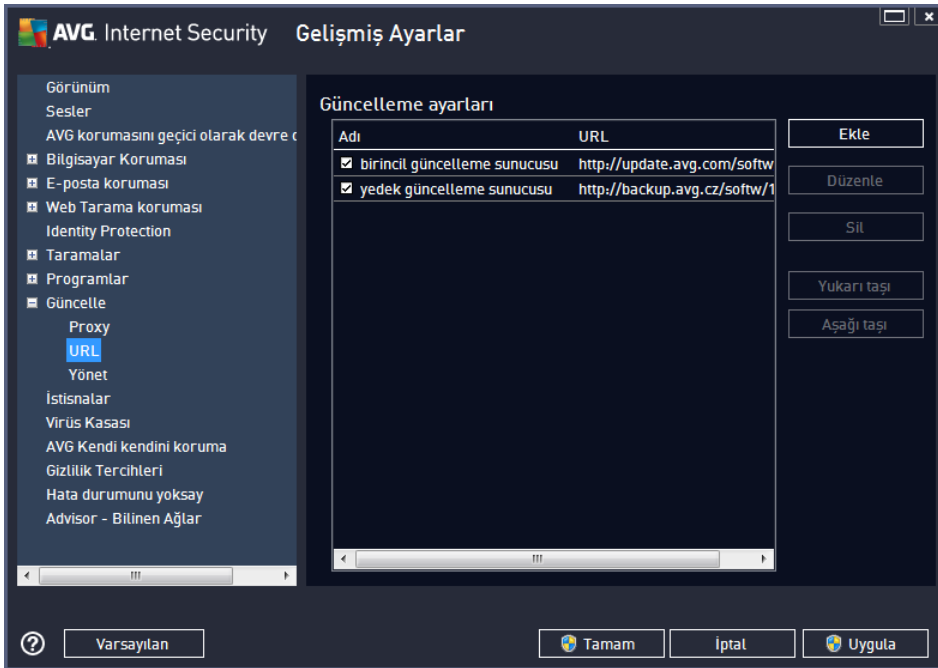
### Otomatik yapılandırma

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

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

### 9.10.2. URL

**URL** iletişim kutusunda güncelleme dosyalarının indirilebileceği bir dizi İnternet adresi bulunur:



### Kontrol düğmeleri

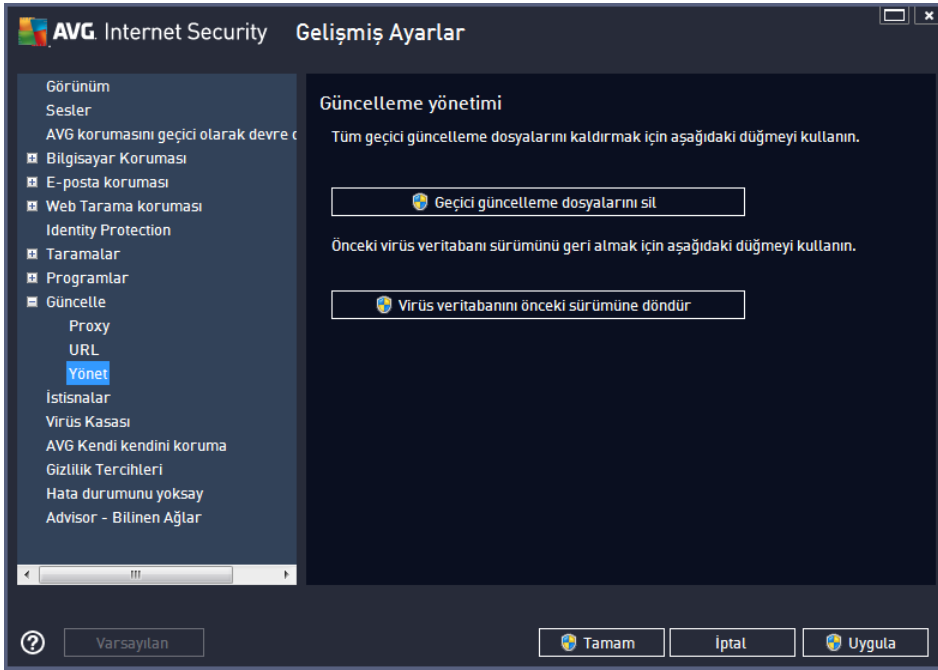
Liste ve liste öğeleri aşağıdaki kontrol düğmeleri kullanılarak düzenlenebilir:

- **Ekle** - Listenize yeni bir URL eklemek için kullanacağınız iletişim kutusunu açar
- **Düzenle** - seçilen URL parametrelerini düzenleyebileceğiniz iletişim kutusunu açar

- **Sil** - seçilen URL'yi listeden seçer
- **Yukari Tasi** - seçilen URL'yi listede bir sıra yukari tasir
- **Asagi Tasi** - seçilen URL'yi listede bir sıra asagi tasir

### 9.10.3. Yönetme

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

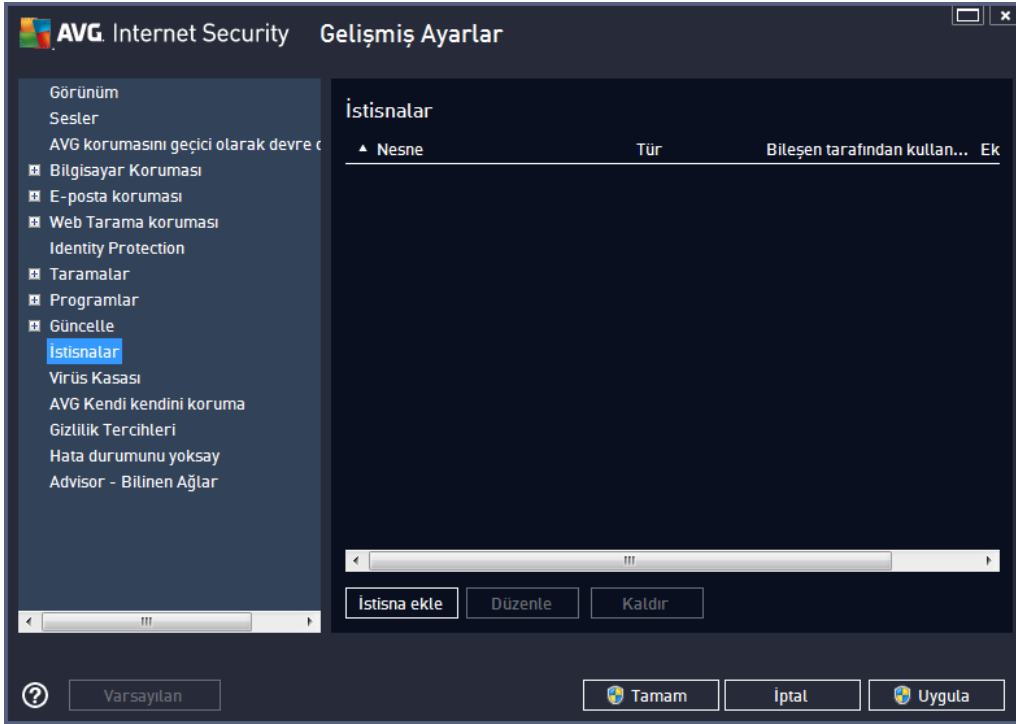


- **Geçici güncelleme dosyalarını sil** - tüm gereksiz güncelleme dosyalarını sabit diskinizden silmek için bu düğmeye basın (*öntanimli olarak söz konusu dosyalar 30 gün boyunca saklanir*)
- **Virüs veritabanını bir önceki sürüme döndür** - en güncel virüs veritabanını sabit diskinizden silmek ve daha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

### 9.11. İstisnalar

**İstisnalar** iletişim kutusunda istisnalar, yani **AVG Internet Security 2013** uygulamasının yok sayacağı öğeler tanımlayabilirsiniz. AVG bir program veya dosyayı sürekli biçimde tehdit olarak tespit ediyorsa veya güvenli bir web sitesini tehlikeli olarak engelliyorsa, bir istisna tanımlamanız gerekir. Bu tür dosya veya web sitelerini istisna listesine eklediğinizde AVG bunları artık rapor etmez veya engellemez.

**Lütfen ilgili dosya, program veya web sitesinin kesinlikle güvenli olduğundan daima emin olun!**

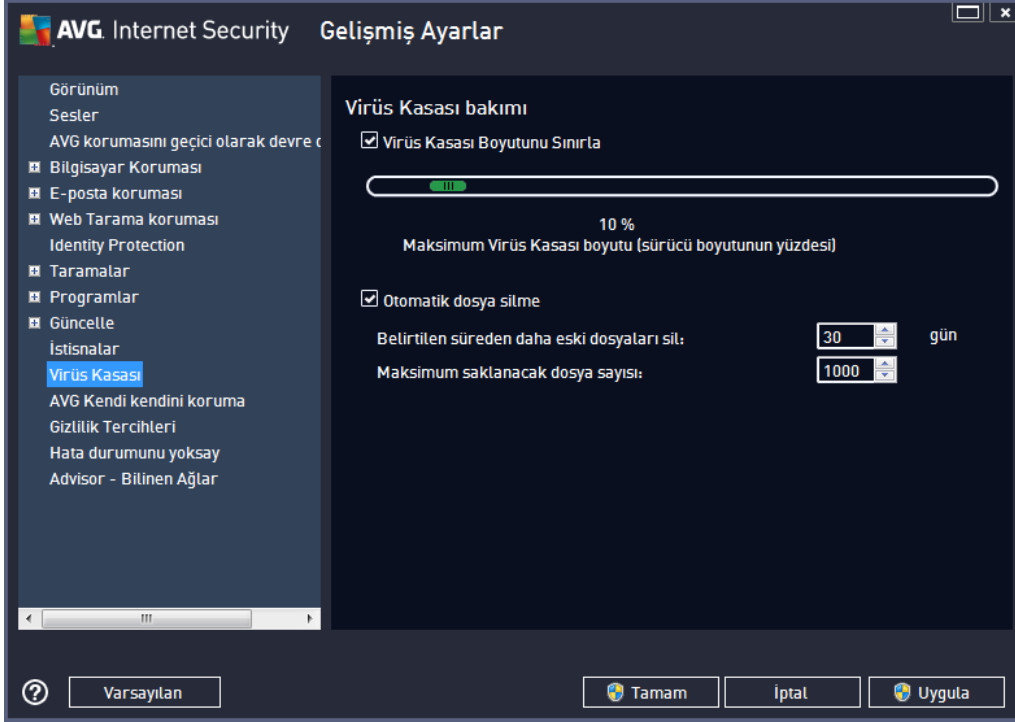


İletişim kutusundaki tabloda, daha önce tanımlanan istisnalar varsa, bunların bir listesi görüntülenir. Her öğenin yanında bir onay kutusu bulunur. Onay kutusu işaretliyse istisna etkindir. İşaretsizse, istisna tanımlanmıştır ancak simdiye kadar kullanılmamıştır. Sütun başlığını tıklayarak, izin verilen öğeleri ilgili kritere göre sıralayabilirsiniz.

### Kontrol düğmeleri

- **İstisna ekle** - AVG taramasının dışında tutulacak bir öğe belirleyebileceğiniz yeni bir iletişim kutusu açmak için tıklayın. Önce, nesnenin türünü (dosya, klasör veya URL) belirlemeniz gerekir. Ardından ilgili nesnenin yolunu diskinizden bulmanız veya URL'yi yazmanız gerekir. Son olarak, hangi AVG özelliklerinin seçilen nesneyi yok sayacağını seçebilirsiniz (*Yerleşik Kalkan, Identity, Scan, Anti-Rootkit*).
- **Düzenle** - Bu düğme ancak bazı istisnalar tanımlanmış ve tabloda listelenmişse etkin olur. Bu durumda seçilen bir istisna için düzenleme iletişim kutusunu açmak ve istisnanın parametrelerini yapılandırmak için bu düğmeyi kullanabilirsiniz.
- **Kaldır** - Bu düğmeyi önceden tanımlanmış bir istisnayı iptal etmek için kullanın. İstisnaları tek tek kaldırabilir veya listeden bir istisnalar blogunu vurgulayıp tanımlanan istisnaları kaldırabilirsiniz. İstisna kaldırıldığında ilgili dosya, klasör veya URL AVG tarafından yeniden kontrol edilir. Dosya veya klasörün kendisi değil, yalnızca istisna kaldırılır!

## 9.12. Virüs Kasası

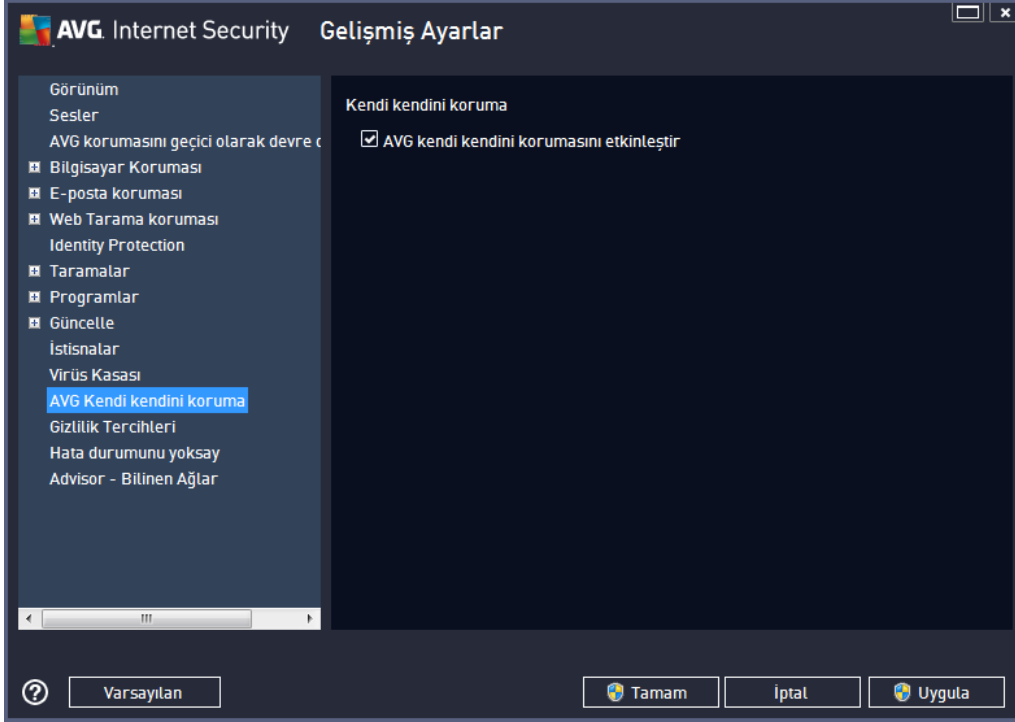


**Virüs Kasası bakımı** iletişim kutusu, [Virüs Kasası](#)'nda depolanan nesnelerin yönetimi hususunda çeşitli parametreleri tanımlayabilmenizi sağlar:

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



### 9.13. AVG Kendi Kendini Koruma

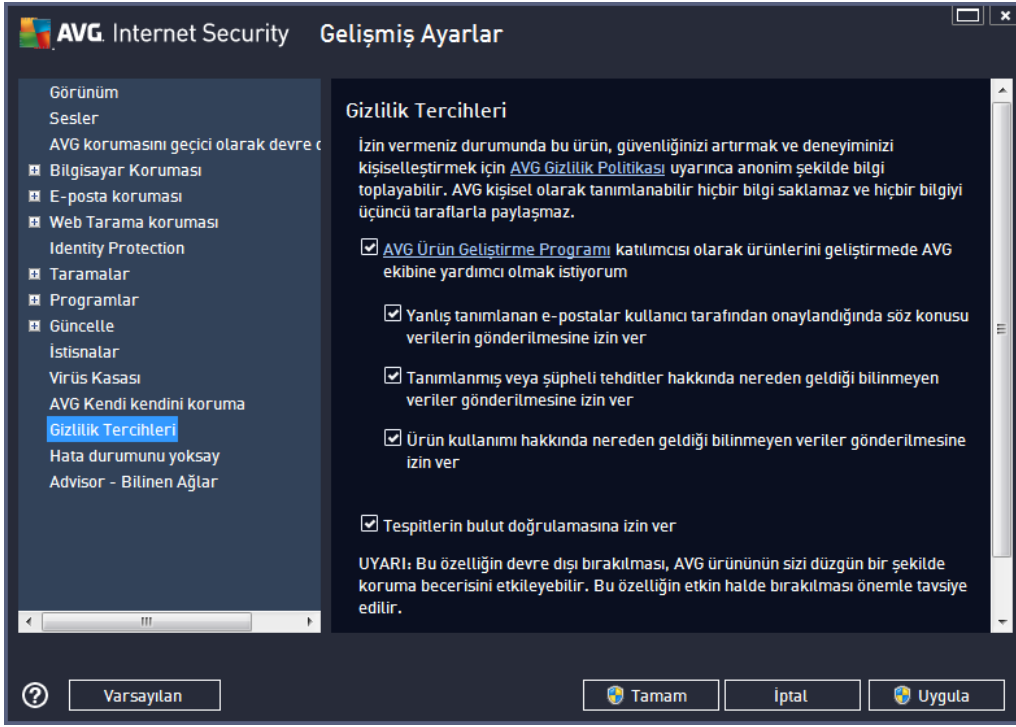


**AVG Kendi Kendini Koruma** , **AVG Internet Security 2013** yazılımının kendi işlem, dosya, kayıt defteri anahtarlarını ve sürücülerini değiştirilmekten ve devre dışı bırakılmaktan korur. Bu tür bir koruma sunmanın ana nedeni gelişkin tehditlerin önce virüslerden koruma yazılımını devre dışı bırakıp ardından bilgisayarınıza kolayca zarar verebilmesidir.

***Bu özelliği açık tutmanızı öneririz!***

### 9.14. Gizlilik Tercihleri

**Gizlilik Tercihleri** iletişim kutusu, sizi AVG ürün geliştirmesine katılmaya ve toplam internet güvenliği seviyesini artırmaya davet eder. Katiliminiz, dünyanın her tarafındaki katılımcılardan en son tehditlere ilişkin güncel bilgileri toplamamıza ve koruma özelliklerini herkes için geliştirmemize yardımcı olacaktır. Raporlama otomatik olarak yapılır, yani sizin için hiçbir rahatsızlık yaratmaz. Raporlarda hiçbir kişisel bilgi yer almaz. Tespit edilen tehditlerin rapor edilmesi isteğe bağlıdır, ancak, bu seçeneği açık bırakmanızı rica ediyoruz. Böylece hem siz hem de diğer AVG kullanıcıları için korumayı geliştirmeye devam edebiliriz.



İletişim kutusundaki mevcut ayarlama seçenekleri:

- **AVG Ürün Geliştirme Programı'na katılarak AVG'nin ürünlerini geliştirmesine yardımcı olmak istiyorum** (varsayılan olarak açık) - AVG Internet Security 2013 ürününü daha da geliştirmemize yardımcı olmak istiyorsanız onay kutusunu işaretli tutun. Bu şekilde, karşılaşılan tüm tehditler AVG'ye bildirilir ve böylece biz tüm dünyadan kötü amaçlı yazılımlarla ilgili güncel bilgileri toplayarak korumayı herkes için geliştirebiliriz. Raporlama işlemi otomatik olarak gerçekleştirilir. Bu nedenle sizi hiçbir şekilde rahatsız etmez ve raporlar kişisel bilgilerinizi içermez.
  - **Kullanıcı onayı üzerine yanlış tanımlanan e-posta hakkında veri gönderilmesine izin ver** (varsayılan olarak açık) - yanlış bir şekilde istenmeyen posta olarak tanımlanan e-postalar veya Anti-Spam hizmeti tarafından algılanmayan istenmeyen postalar hakkında bilgi gönderin. Bu tür bilgiler gönderilirken onayınız istenir.
  - **Algılanan veya şüpheli tehditler hakkında anonim veriler gönderilmesine izin ver** (varsayılan olarak açık) - tüm şüpheli veya olumlu bir şekilde tehlikeli kod veya davranış modeli hakkında bilgi gönderin (bilgisayarınızda algılanan virüs, casus yazılım veya erişmeye çalıştığınız kötü amaçlı web sitesi olabilir) .
  - **Ürün kullanımı hakkında anonim bilgi gönderilmesine izin ver** (varsayılan olarak açık) - algılama sayısı, yapılan taramalar, başarılı veya başarısız güncellemeler gibi uygulama kullanımı hakkında temel istatistikler gönderin.
- **Algılamaların bulut doğrulamasına izin ver** (varsayılan olarak açık) – hatalı pozitif sonuçları ayıklamak için algılanan tehditler gerçekten virüs bulaşması içerip içermediklerinin belirlenmesi amacıyla denetlenir.
- **AVG Personalization özelliğini açarak AVG'nin deneyimini kişiselleştirmesini istiyorum** -



bu özellik bilgisayarınızda yüklü program ve uygulamaların davranışını anonim olarak analiz eder. AVG bu analizi değerlendirerek ihtiyaçlarınıza en uygun hizmetleri sunarak güvenliğinizi en üst düzeye çıkarır.

### En yaygın tehditler

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:

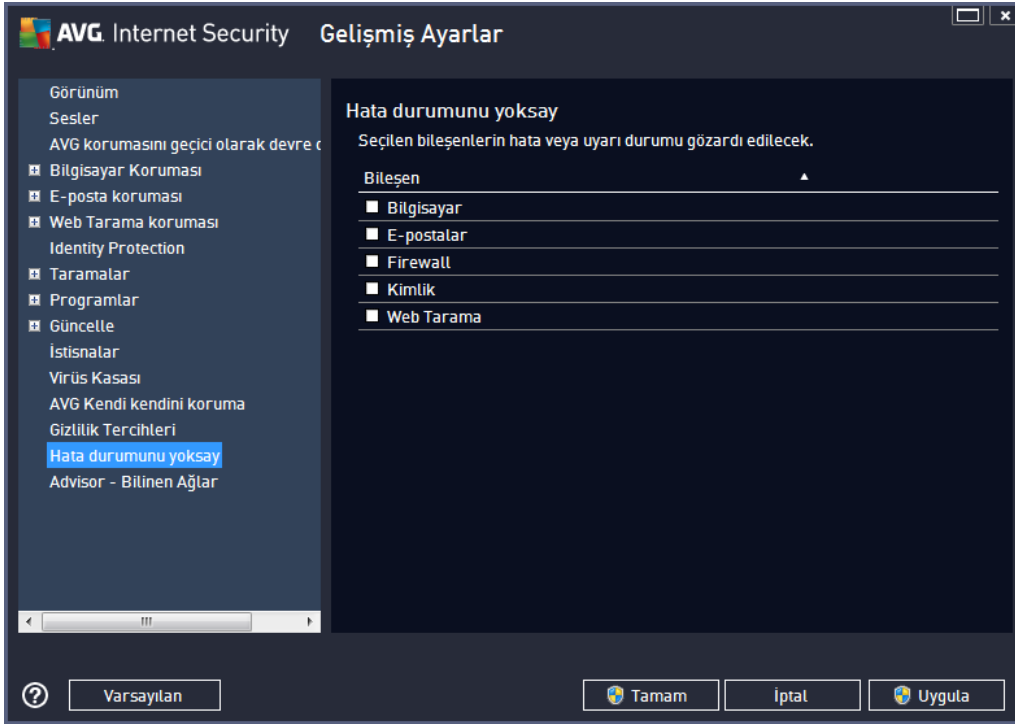
- **Virüs**, kendi kendini kopyalayan ve yayılan zararlı bir koddur ve genellikle zarar olusana kadar fark edilmez. Bazı virüsler ciddi bir tehdit oluşturur, dosyaları siler veya istediği şekilde değiştirir. Bazı virüsler ise görünüşte zararsız olan müzik çalma gibi işlemler yapar. Ancak, temel olarak 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, "tasıyıcı" nesneye gerek duymayan bir virüs alt kategorisidir; genellikle e-posta yoluyla kendini diğer bilgisayarlara gönderir ve e-posta sunucuları ve ağ sistemlerinde asiri 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 tasarlanırlar. Can sıkıcıdır ancak geçekte 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 geçmişsiniz 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 e-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 üzere aldatıcı e-posta iletilerini kullanır.
- **Kötü amaçlı web siteleri**, bilgisayarınıza bilerek kötü amaçlı yazılım yükleyen sitelerdir. Saldırıya uğrayan siteler de aynı işi yapar ancak bunlar kötü amaçlı ziyaretçiler tarafından zarar verilen yasal web siteleridir.



**AVG Internet Security 2013 sizi farklı türlerdeki tüm bu tehditlerden korumak için özel bileşenler içerir. Bu bileşenlerin kısa bir açıklaması için lütfen [Bileşen Genel Görünümü](#) bölümüne bakın.**

## 9.15. Hata durumunu yoksay

**Hata durumunu yoksay** iletişim kutusunda, bilgilendirilmek istemediğiniz bileşenleri seçebilirsiniz:



Varsayılan olarak listede herhangi bir bileşen seçilmemiştir. Bileşenlerden herhangi biri hata verirse 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

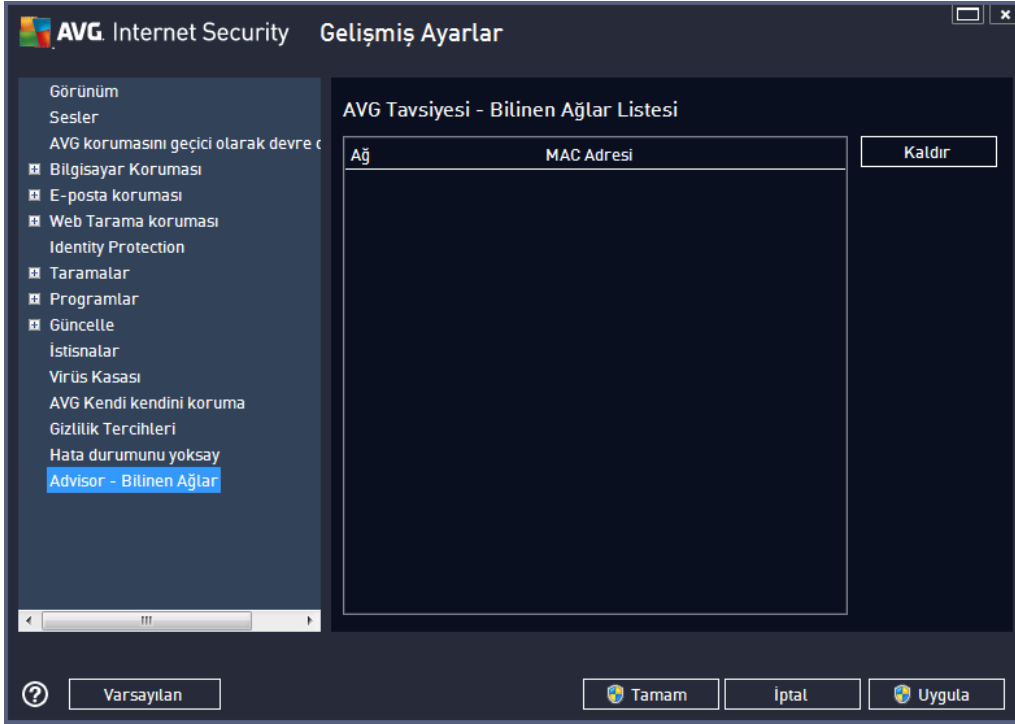
Belirli bir nedenle bileşenlerden birini geçici olarak kapatmanız gereken bir durum olabilir. **Bu önerilmez, tüm bileşenleri sürekli olarak açık ve varsayılan yapılandırılmada tutmanız gerekir**, ancak böyle bir durum meydana gelebilir. Bu durumda sistem tepsisi simgesi, otomatik olarak bileşenin hata durumunda olduğunu 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, **Hata durumunu yoksay** iletişim kutusunda hata durumunda olan (ya da kapatılmış) bileşenleri seçebilirsiniz ve söz konusu durum hakkında bilgilendirilmek istemeyebilirsiniz. Onaylamak için **Tamam** düğmesine basın.

## 9.16. Advisor – Bilinen Ağlar

[AVG Advisor](#) bağlandığınız ağları izleyen ve yeni bir ağ bulunduğunda (*daha önce kullanılan bir ağ adına sahip olduğundan karışıklığa neden olabilecek bir ağ*) sizi bilgilendiren ve ağın güvenli olduğuna karar verirsiniz, bunları listeye de kaydedebilirsiniz (*Bilinmeyen bir ağ tespit edildiğinde sistem tepsi üzerinde hareket eden AVG Tavsiyesi tepsi bildiriminde sağlanan bağlantı yoluyla. Ayrıntılar için lütfen [AVG Tavsiyesi](#) hakkındaki bölüme bakın.*). [AVG Tavsiyesi](#) bu işlemin ardından ağın benzersiz özneliklerini hatırlar (*özellikle de MAC adresini*) ve bir dahaki sefere bildirim göstermez. Bağlandığınız her ağ otomatik olarak bilinen ağ olarak değerlendirilir ve listeye eklenir. **Kaldır** düğmesine basarak herhangi bir girişi silebilirsiniz; bu durumda ilgili ağ tekrar bilinmeyen ve muhtemelen güvensiz ağ olarak değerlendirilir.

Bu iletişim kutusunda hangi ağların bilinen olarak sınıflandırıldığını kontrol edebilirsiniz:



**Not:** AVG Tavsiyesi'ndeki bilinen ağlar özelliği Windows XP 64 bit sürümünde desteklenmez.



## 10. Güvenlik Duvarı Ayarları

[Firewall](#) yapılandırması, çeşitli iletişim kutularında bileşenin gelişmiş parametrelerini yapılandırabileceğiniz yeni bir pencere açar. Firewall yapılandırması bileşenin gelişmiş parametrelerini birkaç farklı yapılandırma iletişim kutusunda düzenleyebileceğiniz yeni bir pencerede açılır. Yapılandırma temel modda veya uzman modunda görüntülenebilir. Yapılandırma penceresine ilk girdiğinizde temel mod su parametrelerin düzenleme seçenekleriyle açılır:

- [Genel](#)
- [Uygulamalar](#)
- [Dosya ve Yazıcı Paylaşımı](#)

İletişim kutusunun altında **Uzman modu** düğmesini bulabilirsiniz. Düğmeye basarak çok daha gelişmiş Firewall yapılandırma seçeneklerinin yer aldığı iletişim kutusunu açabilirsiniz:

- [Gelişmiş ayarlar](#)
- [Tanımlanan aklar](#)
- [Sistem hizmetleri](#)
- [Günlükler](#)

**Ancak, yazılım satıcısı tüm AVG Internet Security 2013 bileşenlerini optimum performans sağlayacak şekilde ayarlamıştır. Bunun için iyi bir nedeniniz olmadıkça varsayılan yapılandırmayı değiştirmeyin. Ayarlarda yapılacak her tür değişiklik sadece deneyimli bir kullanıcı tarafından gerçekleştirilmelidir!**

### 10.1. Genel

**Genel bilgiler** iletişim kutusu mevcut Firewall modları hakkında genel bilgiler sunar. Firewall modunun geçerli seçimi menüden başka bir mod seçilerek değiştirilebilir.

**Ancak, yazılım satıcısı tüm AVG Internet Security 2013 bileşenlerini optimum performans sağlayacak şekilde ayarlamıştır. Bunun için iyi bir nedeniniz olmadıkça varsayılan yapılandırmayı değiştirmeyin. Ayarlarda yapılacak her tür değişiklik sadece deneyimli bir kullanıcı tarafından gerçekleştirilmelidir!**



Firewall, bilgisayarınızın bir alanda bulunmasına, bağımsız bir bilgisayar veya bir dizüstü bilgisayar olmasına bağlı olarak özel güvenlik kuralları tanımlamanıza olanak tanır. Bu seçeneklerin her biri için farklı bir koruma seviyesi gerekir ve bu seviyeler de ilgili modların kapsamındadır. Kısaca, Firewall modu Firewall bileşeni için özel bir yapılandırma değildir ve bu şekilde önceden tanımlanmış çok sayıda yapılandırmayı kullanabilirsiniz:

- **Otomatik** - Bu modda Firewall tüm ağ trafiğini otomatik olarak denetler. Hiçbir karar için onayınız istenmez. Firewall bilinen tüm uygulamalarla bağlantıya izin verir ve aynı zamanda uygulamaya her zaman bağlanabilmesi için bir kural oluşturulur. Firewall, diğer uygulamalar için uygulamanın davranışına bağlı olarak uygulamaya yönelik izin veya engelleme kararını verir. Ancak, böyle durumlarda kural oluşturulmaz ve uygulama her bağlanmaya çalıştığında kontrol edilir. **Otomatik mod arka planda dikkat çekmeden çalışır ve çoğu kullanıcı için önerilen moddur.**
- **İnteraktif** - bilgisayarınızda gelen ve giden tüm ağ trafiğini tam olarak kontrol etmek istiyorsanız bu mod kullanışlıdır. Firewall trafiği sizin için izler ve tüm iletişim ve veri aktarım girişimlerinden sizi haberdar ederek girişimi uygun gördüğünüz biçimde engellenizi veya izin vermenizi sağlar. Yalnızca ileri düzey kullanıcılar için önerilir.
- **İnternet erişimini engelle** - internet bağlantısı tamamen engellenir, internete erişemezsiniz ve dışarıdan hiç kimse de bilgisayarınıza erişemez. Yalnızca özel ve kısa süreli kullanım içindir.
- **Güvenlik duvarı korumasını kapat** - Firewall korumasının devre dışı bırakılması bilgisayarınızda gelen ve giden tüm trafige izin verir. Sonuç olarak, bilgisayarınız hacker saldırılarına açık hale gelir. Lütfen bu seçeneği kullanırken çok dikkatli olun.

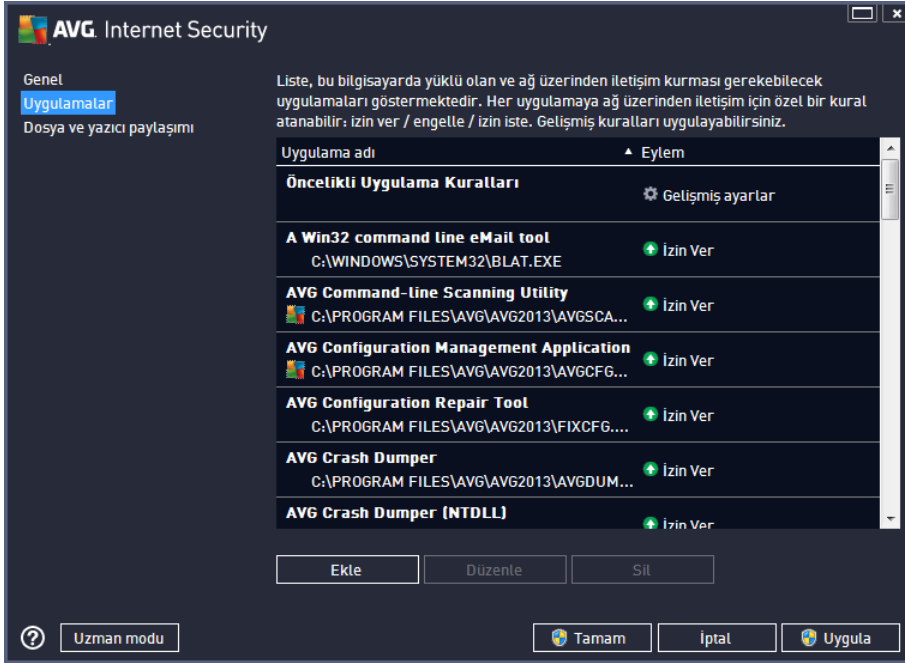
Not: Firewall içinde de bir otomatik mod mevcuttur. Bu mod, [Bilgisayar](#) veya [Identity protection](#) bileşeni kapatıldığında ve bu nedenle bilgisayarınız tehditlere açık hale geldiğinde sessizce etkinleştirilir. Bu tür durumlarda, Firewall yalnızca bilinen veya kesinlikle güvenli uygulamalara otomatik olarak izin verir. Diğer tüm uygulamalar için sizin karar vermeniz istenir. Bunun nedeni



devre dışı bırakılan bileşenlerin boşluğunu kapatmak ve bilgisayarınızı güvende tutmaktır.

## 10.2. Uygulamalar

**Uygulama** iletişim kutusu, ağ üzerinden o ana kadar iletişim kurmaya çalışan tüm uygulamaları ve ilgili işlem için atanan eylemlerin simgelerini listeler:



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

- - tüm ağlar için iletişime izin ver
- - iletişimi engelle
- - gelişmiş ayarlar tanımlandı

**Yalnızca önceden yüklü olan uygulamaların tespit edilebildiğini unutmayın. Varsayılan olarak, yeni uygulama ağ üzerinden ilk defa bağlanmaya çalıştığında, [güvenli veritabanlarına](#) göre Firewall onun için otomatik olarak bir kural oluşturacak veya iletişime izin vermek mi yoksa engellemek mi istediğinizi soracaktır. İkinci durumda, yanıtınızı kalıcı bir kural olarak kaydedebileceksiniz (daha sonra bu iletişim kutusunda listelenecek).**

Elbette, yeni uygulama için hemen kural tanımlayabilirsiniz. Bu iletişim kutusunda, **Ekle** seçeneğine basın ve uygulama bilgilerini girin.

Listede, uygulamaların dışında iki özel öğe vardır. **Öncelikli Uygulama Kuralları** (listenin üst kısmında) tercihe bağlıdır ve her zaman tek bir uygulamanın kurallarından önce uygulanır. **Diğer Uygulama Kuralları** (listenin alt kısmında bulunur) örneğin bilinmeyen veya tanımlanmayan bir uygulama için özel uygulama kuralları uygulanmadığında "son örnek" olarak kullanılır. Böyle bir uygulama ağ üzerinden iletişim kurmaya çalıştığında baslatılacak işlemi seçin: Engelle (iletişim her zaman engellenir), İzin ver (tüm ağlar üzerinden iletişime izin verilir), Sor (iletişime yönelik izin verme



veya engelleme tercihi size bırakılır). **Bu öğelerin genel uygulamalardan farklı ayar seçenekleri bulunur ve bunlar yalnızca deneyimli kullanıcılara yöneliktir. Ayarları değiştirmemenizi önemle öneririz!**

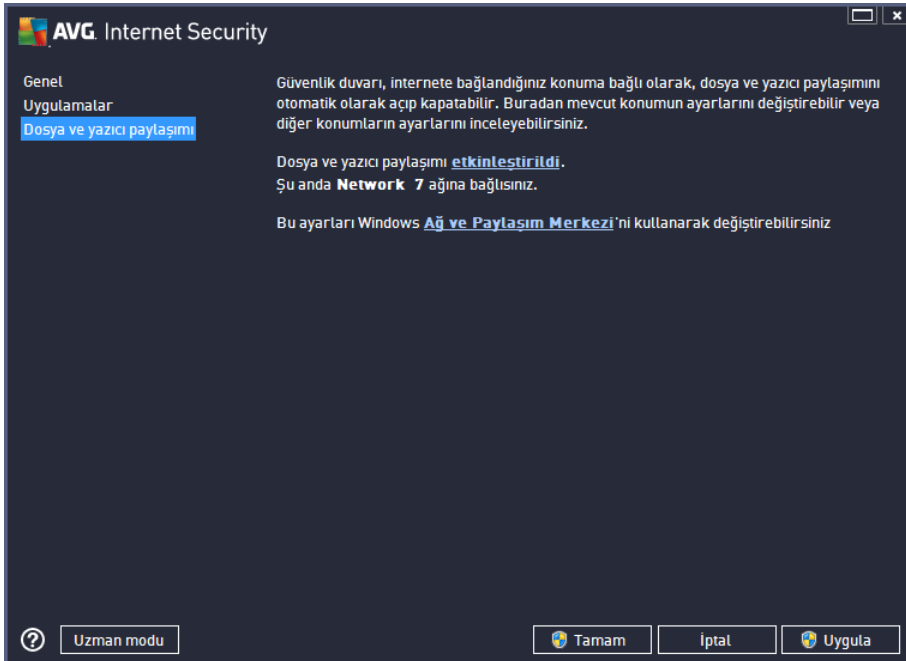
### Kontrol düğmeleri

Liste, aşağıdaki denetim düğmeleri kullanılarak düzenlenebilir:

- **Ekle** - yeni uygulama kurallarını tanımlamak için boş bir iletişim kutusu açar.
- **Düzenle** - var olan bir uygulamanın kural kümesinin düzenlenmesi için sağlanan verilerle aynı iletişim kutusunu açar.
- **Sil** - seçilen uygulamayı listeden siler.

### 10.3. Dosya ve yazıcı paylaşımı

Dosya ve yazıcı paylaşımı Windows, ortak disk birimleri, yazıcılar, tarayıcılar ve tüm benzer cihazlarda "Paylaşılan" olarak işaretlediğiniz tüm dosyalar veya klasörler anlamına gelmektedir. Bu tür öğelerin paylaşımı yalnızca güvenli olduğu düşünülen ağlarda gerçekleştirilmelidir (*örneğin evde, ıste veya okulda*). Ancak, herkese açık ağlara (*havaalanı Wi-Fi veya internet kafe gibi*) bağlanıyorsanız, hiçbir şey paylaşmak istemeyebilirsiniz. AVG Firewall paylaşımı kolayca engelleyip izin verebilir ve daha önce ziyaret ettiğiniz ağlarla ilgili seçiminizi kaydetmenizi sağlar.

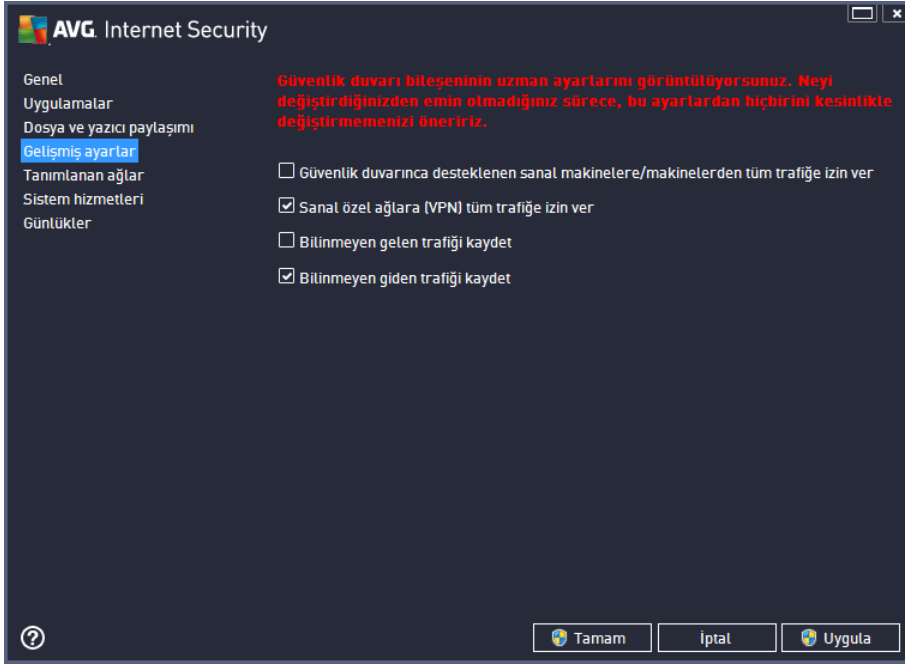


**Dosya ve Yazıcı Paylaşımı** iletişim kutusunda dosya ve yazıcı paylaşımı ve o anda bağlı olan ağların yapılandırmasını düzenleyebilirsiniz. Window XP'de, ağ adı ilgili ağa ilk bağlandığınızda ağ için seçtiğiniz adlandırmaya karşılık gelir. Windows Vista ve üstü sistemlerde, ağ adı Ağ ve Paylaşım Merkezi'nden otomatik olarak alınır.



## 10.4. Gelişmiş ayarlar

**Gelişmiş ayarlar iletişim kutusundaki tüm düzenleme seçenekleri YALNIZCA DENEYİMLİ KULLANICILAR için tasarlanmıştır!**

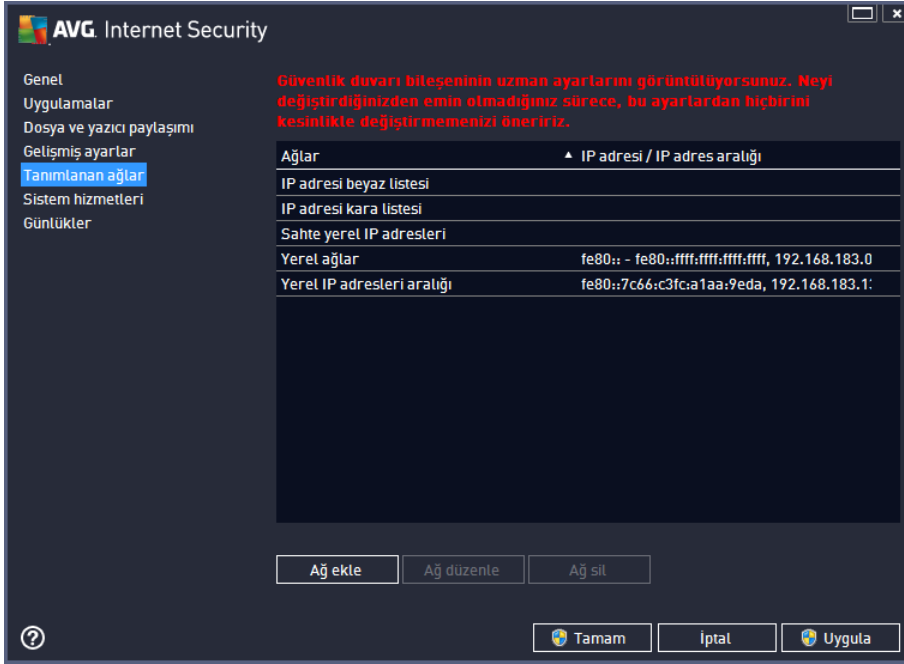


**Gelişmiş ayarlar** iletişim kutusu aşağıdaki Firewall parametrelerini etkinleştirmenizi veya devre dışı bırakmanızı sağlar:

- **Güvenlik duvarınca desteklenen sanal makinelere/makinelerden tüm trafiğe izin ver** - VMware gibi sanal makinelerde ağ bağlantısı için destek.
- **Sanal özel ağlara (VPN) tüm trafiğe izin ver** - VPN bağlantıları (uzak bilgisayarları bağlamak için kullanılır) için destek.
- **Bilinmeyen gelen/giden trafiği günlük dosyasına kaydet** - bilinmeyen uygulamalardan kaynaklanan tüm iletişim girişimleri (gelen/giden) [Firewall günlüğü](#) dosyasında kaydedilir.

## 10.5. Tanımlanan ağlar

**Tanımlanan ağlar iletişim kutusundaki tüm düzenleme seçenekleri YALNIZCA DENEYİMLİ KULLANICILAR için tasarlanmıştır!**

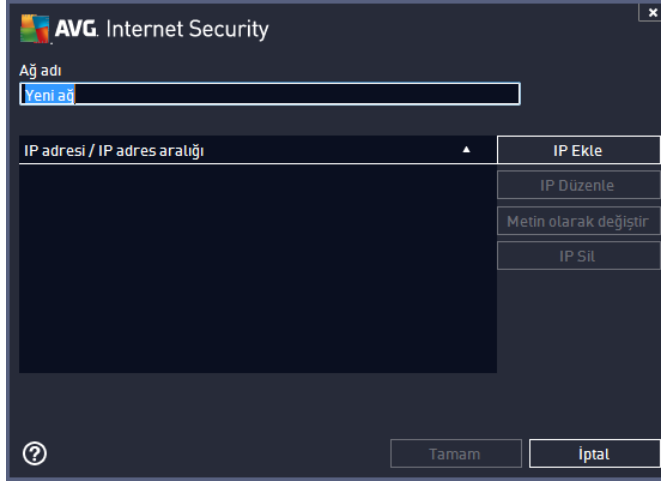


**Tanımlanan ağlar** iletişim kutusunda bilgisayarınızın bağlı olduğu ağlar görüntülenir. Liste algılanan her ağla ilgili aşağıdaki bilgileri sağlar:

- **Ağlar** - bilgisayarın bağlı olduğu tüm ağların adlarını listeler.
- **IP adresi aralığı** - her ağ otomatik olarak tespit edilir ve IP adresi aralığı formunda belirtilir.

### Kontrol düğmeleri

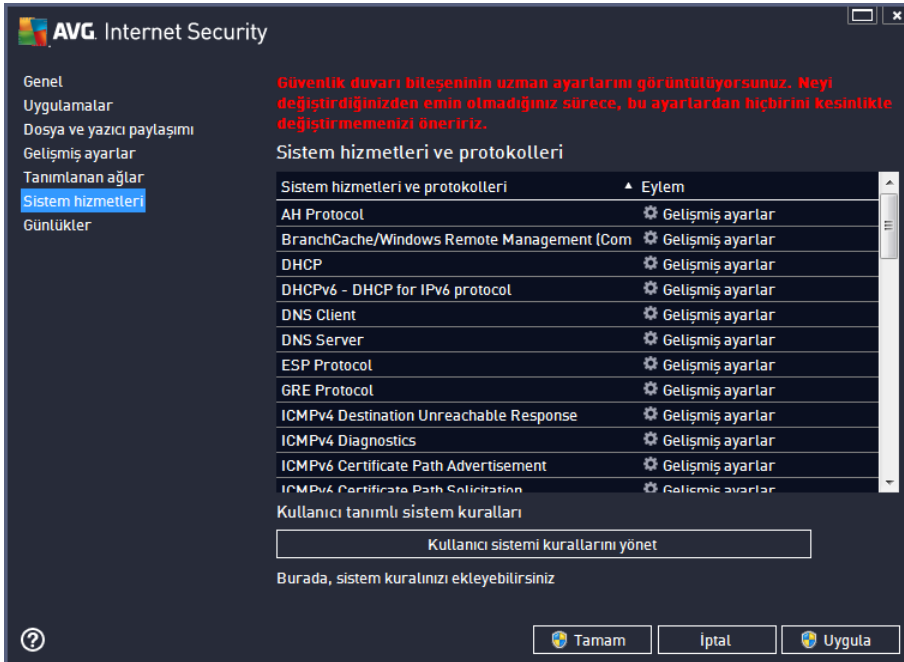
- **Ağ ekle** - yeni tanımlanan ağın parametrelerini düzenleyebileceğiniz yeni bir iletişim penceresi açar; örneğin **Ağ adı** girmek ve **IP adresi aralığı** belirlemek için:



- **Agi düzenle** - mevcut durumda tanımlanmış ağın parametrelerini düzenleyebileceğiniz **Ag özellikleri** iletişim kutusunu açar (yukarı bakınız) (bu pencere yeni ağ ekleme penceresi ile aynıdır, bir önceki paragrafta verilen açıklamaları okuyunuz).
- **Agi sil**, seçilen ağ ile ilgili referansı ağ listesinden siler.

## 10.6. Sistem hizmetleri

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



**Sistem hizmetleri ve protokolleri** iletişim kutusu, ağ üzerinden iletişim kurulması gerekebilecek Windows standart sistem servisleri ve protokollerini listeler. Grafik aşağıdaki sütunları içerir:

- **Sistem hizmeti ve protokolleri** - Bu sütun ilgili sistem hizmetinin adını gösterir.

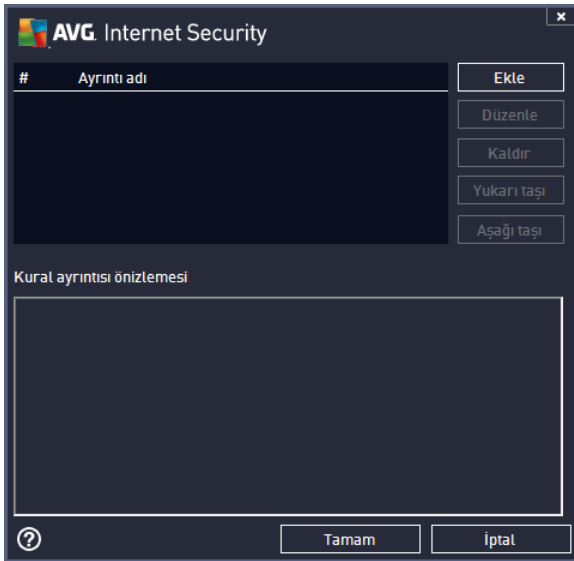


- **Eylem** - Bu sütun atanan eylemin simgesini görüntüler:
  - Tüm ağlar için iletişime izin ver
  - İletisimi engelle

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

### Kullanıcı tanımlı sistem kuralları

Kendi sistem hizmeti kuralınızı tanımlamak üzere yeni bir iletişim kutusu açmak için (*asagıdaki resme bakın*), **Kullanıcı sistemi kurallarını yönet** düğmesine basın. Sistem hizmetleri ve protokolleri listesindeki mevcut öğelerden herhangi birinin yapılandırmasını düzenlemeye karar vererseniz aynı iletişim kutusu açılır. Bu iletişim kutusunun üst kısmı geçerli olarak düzenlenen sistem kuralının tüm ayrıntılarının genel bir görünümünü görüntüler, alt kısım seçili ayrıntıyı gösterir. İlgili düğmeyle bir ayrıntılar kuralı düzenlenebilir, eklenebilir veya silinebilir:



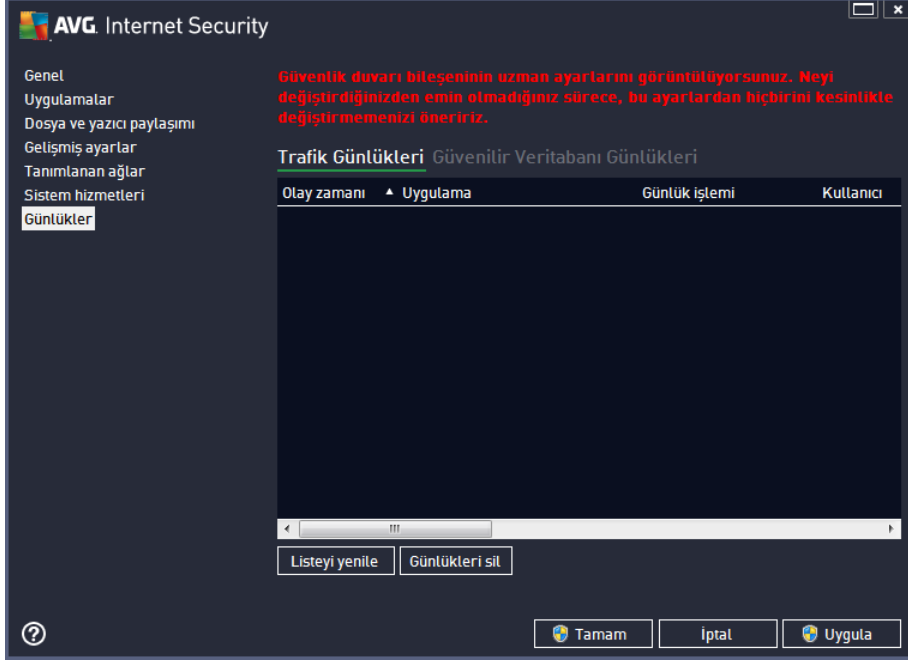
**Ayrıntı kuralı ayarlarının gelişmiş ayarlar olduğunu ve Firewall yapılandırması üzerinde tam denetime sahip olması gereken ağ yöneticilerine yönelik tasarlandığını lütfen unutmayın. İletişim protokolleri türleri, ağ bağlantı noktası numaraları, IP adresi tanımları vb. hakkında bilginiz yoksa, lütfen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

## 10.7. Günlükler

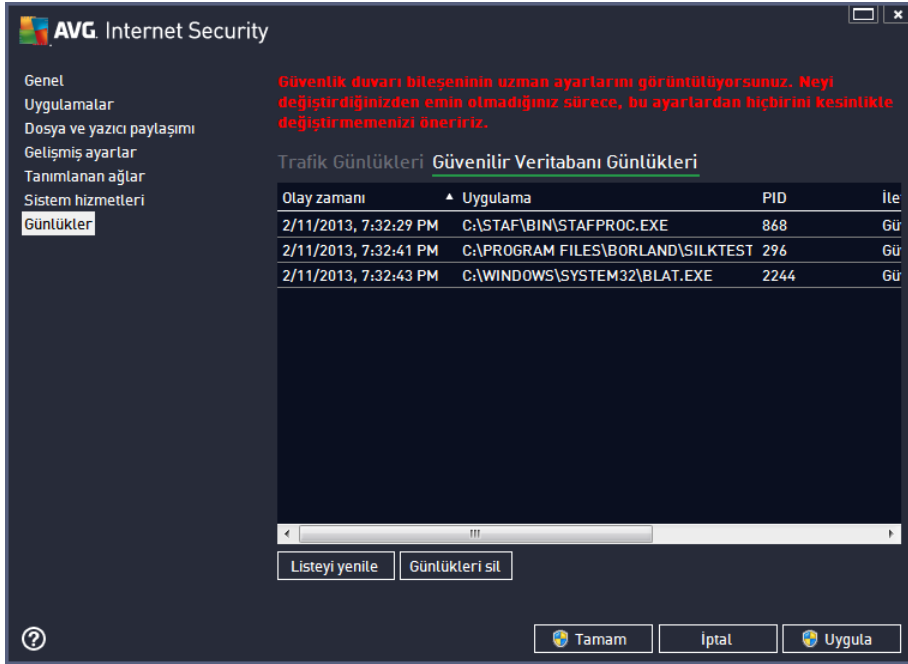
**Günlükler iletişim kutusundaki tüm düzenleme seçenekleri YALNIZCA DENEYİMLİ KULLANICILAR için tasarlanmıştır!**

**Günlükler** iletişim kutusu, kaydedilen tüm Firewall eylemlerini ve etkinliklerini ilgili parametrelerin ayrıntılı tanımları ile birlikte iki sekmede görüntüleyebilmenizi sağlar.

- **Trafik Günlükleri** - Bu sekme ağına bağlanmaya çalışan tüm uygulamaların etkinlikleri hakkındaki bilgileri sunar. Her öğe için olay zamanı, uygulama adı, ilgili günlük işlemi, kullanıcı adı, PID, trafik yönü, protokol türü, uzak ve yerel bağlantı noktalarının numaralarıyla yerel ve uzak IP adresleri hakkındaki bilgileri bulabilirsiniz.



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



AVG Internet Security

Genel  
Uygulamalar  
Dosya ve yazıcı paylaşımı  
Gelişmiş ayarlar  
Tanımlanan ağlar  
Sistem hizmetleri  
**Günlükler**

Güvenlik duvarı bileşeninin uzman ayarlarını görüntüyorsunuz. Neyi değiştirdiğinizden emin olmadığımız sürece, bu ayarlardan hiçbirini kesinlikle değiştirmenizi öneririz.

Trafik Günlükleri **Güvenilir Veritabanı Günlükleri**

Olay zamanı	Uygulama	PID	İle
2/11/2013, 7:32:29 PM	C:\STAF\BIN\STAFPROC.EXE	868	Gü
2/11/2013, 7:32:41 PM	C:\PROGRAM FILES\BORLAND\SILKTEST	296	Gü
2/11/2013, 7:32:43 PM	C:\WINDOWS\SYSTEM32\BLAT.EXE	2244	Gü

Listeyi yenile Günlükleri sil

Tamam İptal Uygula


### Kontrol düğmeleri

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

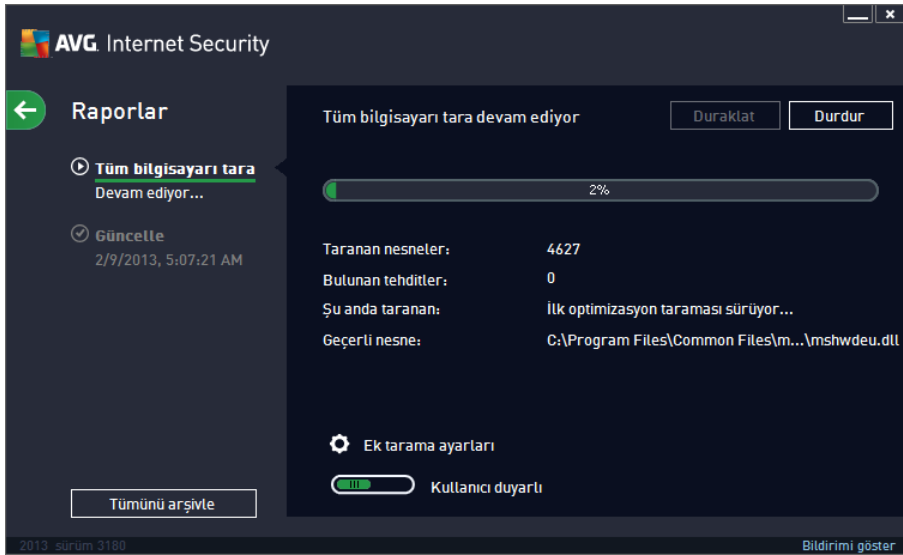
## 11. AVG Tarama

Varsayılan olarak, **AVG Internet Security 2013** ilk taramadan sonra olduğu gibi hiçbir taramayı çalıştırmaz (*sizin baslatmanız istenir*), her zaman korumada olan **AVG Internet Security 2013** ürününün yerleşik bileşenleri ile mükemmel olarak korunuyor olmanız ve hiçbir kötü amaçlı yazılımın bilgisayarınıza hiçbir surette girmesine izin vermemeniz gerekir. Elbette belirli aralıklarda çalıştırılacak bir [tarama planlayabilir](#) veya bir taramayı gereksinimlerinize göre el ile baslatabilirsiniz.

AVG tarama arayüzüne [ana kullanıcı arayüzünden](#) grafik olarak iki bölüme ayrılmış düğme

aracılığıyla erişilebilir: 

- **Simdi Tara** - [Tüm Bilgisayarı Tara](#) işlemini hemen başlatmak için düğmeye basın; ilerleme ve sonuçları otomatik olarak açılan [Raporlar](#) penceresinden izleyin:



- **Seçenekler** - Bu düğmeyi seçerek (*grafik olarak yeşil bir alanda üç yatay çizgi olarak görünür*) **Tarama Seçenekleri** iletişim kutusunu açıp burada [zamanlanmış taramaları yönetebilir](#) ve [Tüm Bilgisayarı Tara](#) / [Belirli Dosyaları veya Klasörleri Tara](#) parametrelerini düzenleyebilirsiniz:



**Tarama Seçenekleri** iletişim kutusunda üç ana tarama yapılandırması bölümü görebilirsiniz:

- **Zaman. taramaları yönet** - [Tüm tarama zamanlamalarının genel görünümünü içeren yeni bir iletişim kutusu](#) açmak için bu seçeneği tıklayın. Kendi taramalarınızı tanımlamadan önce, listede yalnızca yazılım sağlayıcısı tarafından önceden tanımlanmış tek bir zamanlanmış tarama görebilirsiniz. Tarama varsayılan olarak kapatılmıştır. Taramayı açmak için sağ tıklayın ve bağlam menüsünden *Görevi etkinleştir*'i seçin. Zamanlanmış tarama etkinleştirildiğinde *Tarama zaman. düzenle* düğmesiyle [taramanın yapılandırmasını düzenleyebilirsiniz](#). Kendi istediğiniz yeni bir tarama zamanlaması oluşturmak için *Tarama zaman. ekle* düğmesini de tıklatabilirsiniz.
- **Tüm bilgisayarı tara / Ayarlar** - Düğme iki kısma ayrılmıştır. Tüm bilgisayarınızın taramasını hemen başlatmak için *Tüm bilgisayarı tara* seçeneğini tıklayın (*tüm bilgisayar taramasıyla ilgili ayrıntılar için lütfen [Öntanımlı taramalar / Tüm bilgisayarı tarama](#) başlıklı bölüme bakın*). Altındaki *Ayarlar* bölümünü tıklarsanız [tüm bilgisayar taramasının yapılandırma iletişim kutusunu](#) açarsınız.
- **Belirli dosyaları veya klasörleri tara / Ayarlar** - Bu düğme de iki kısma ayrılmıştır. Bilgisayarınızda seçtiğiniz alanların taramasını hemen başlatmak için *Belirli dosyaları veya klasörleri tara* seçeneğini tıklayın (*belirli dosya ve klasörlerin taramasıyla ilgili ayrıntılar için lütfen [Öntanımlı taramalar / Belirli dosyaları veya klasörleri tarama](#) başlıklı bölüme bakın*). Altındaki *Ayarlar* bölümünü tıklarsanız [belirli dosya veya klasör taramasının yapılandırma iletişim kutusunu](#) açarsınız.

## 11.1. Öntanımlı Taramalar

**AVG Internet Security 2013** programının ana özelliklerinden biri istek üzerine taramadır. İsteğe bağlı taramalar, muhtemel bir virüs hakkında şüpheye düştüğünüz an bilgisayarınızın istediğiniz zamanda yapabileceğiniz taramalardır. Kısacası, bilgisayarınızda virüs olduğunu düşünmeseniz bile söz konusu taramaların düzenli aralıklarla yapılması önerilmektedir.

**AVG Internet Security 2013** içinde, yazılım satıcısının önceden tanımladığı aşağıdaki tarama türlerini bulacaksınız:

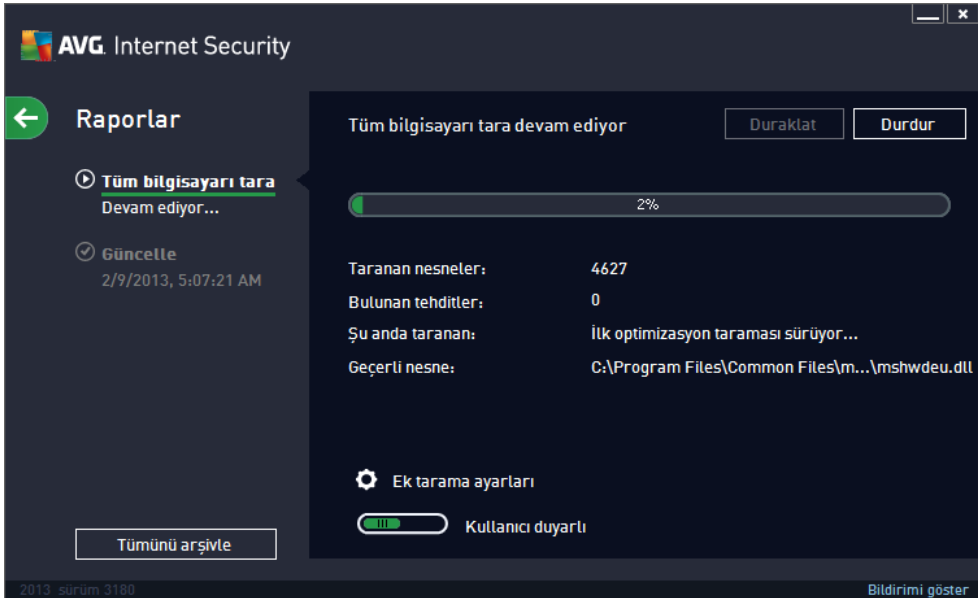


### 11.1.1. Tüm bilgisayarı tara

**Tüm bilgisayarı tara** tüm bilgisayarı muhtemel bulasmalara ve/veya potansiyel olarak istenmeyen programlara karşı tarar. Bu tarama, bilgisayarınızın tüm sabit disklerini tarayacak, virüsleri tespit edecek ve temizleyecek ya da tespit edilen bulasmayı [Virüs Kasası](#)'na taşıyacaktır. Bilgisayarın tümü haftada en az bir defa taranmalıdır.

#### Tarama baslatma

**Tüm bilgisayarı tara** işlemi doğrudan [ana kullanıcı arayüzünden](#) **Şimdi tara** düğmesi tıklanarak başlatılabilir. Bu tür tarama için başka bir yapılandırma yapmaya gerek yoktur; tarama hemen başlar. **Tüm bilgisayarı tarama devam ediyor** iletişim kutusunda (*ekran resmine bakın*) ilerlemeyi ve sonuçları izleyebilirsiniz. Tarama işlemi gerekirse geçici olarak kesintiye uğratabilir (**Duraklat**) ya da iptal edilebilir (**Durdur**).



#### Tarama yapılandırması düzenleme

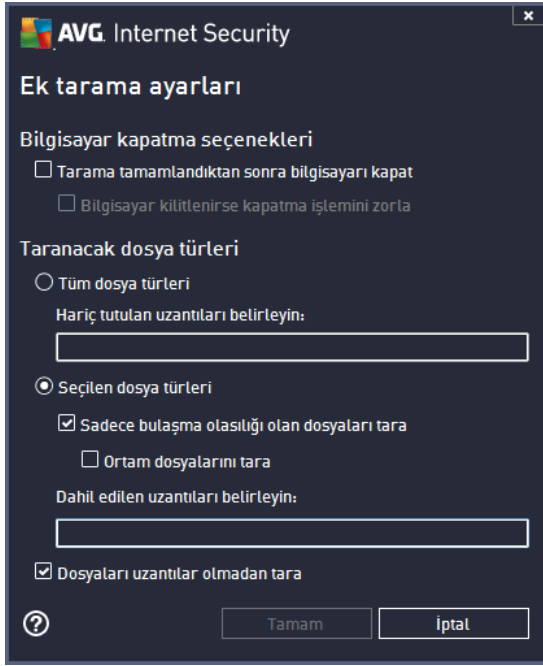
**Tüm bilgisayarı tara** yapılandırmasını **Tüm bilgisayarı tara - Ayarlar** iletişim kutusunda düzenleyebilirsiniz (*iletişim kutusuna* [Tarama seçenekleri](#) iletişim kutusundaki **Tüm bilgisayarı tara** işleminin **Ayarlar bağlantısından** erişilebilir). **Değiştirmek için geçerli bir nedeniniz olmadığı müddetçe varsayılan ayarları korumanız önerilir!**



Tarama parametreleri listesindeki belirli parametreleri isteginiz doğrultusunda açip kapatabilirsiniz:

- **Bulasmayı bana sormadan temizle / kaldır** (varsayılan olarak açık) - Tarama sırasında virüs tanımlanırsa, bir giderme yazılımı mevcutsa otomatik olarak temizlenir. Bulasmis dosya otomatik olarak temizlenemezse, bulasmis nesne [Virüs Kasası](#)'na tasınir.
- **Potansiyel Olarak İstenmeyen Programları ve Casus Yazılım tehditlerini rapor et** (varsayılan olarak açık) - Virüslerin yani sıra casus yazılımları da taramak için işaretleyin. Casus yazılım, süpheli kötü amaçlı yazılım kategorisini ifade eder: genellikle bir güvenlik riskini olusturmasına ragmen bu programlardan bazilari bilerek yüklenebilir. Bilgisayarınızın güvenliğini artirdigidandan, bu özelligi etkin durumda tutmanizi öneririz.
- **Potansiyel Olarak İstenmeyen Programlar gelismis grubunu rapor et** (varsayılan olarak kapali) - Casus yazılımların, yani dogrudan üreticiden alınan tamamen zararsız olan, ancak daha sonra kötüye kullanılabilcek programların genişletilmiş paketlerinin 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 Çerezleri için tara** (varsayılan olarak kapali) - Bu parametre, tespit edilmesi istenen çerezleri tanımlar; (HTTP çerezleri kimlik doğrulaması, izleme ve kullanıcılar hakkındaki site tercihleri veya elektronik alışveriş sepetlerinin içeriği gibi belirli bilgilerin korunması için kullanılır).
- **Arsivleri tara** (varsayılan olarak kapali) - Bu parametre, ZIP, RAR vb. arşiv dosyalarının içinde sıkıştırılmış dosyaların bile taranmasını sağlar.
- **Bulussal Analiz Yöntemlerini Kullan** (varsayılan olarak açık) - Bulussal analiz yöntemi (taranan nesnenin komutlarının sanal bir bilgisayar ortamında dinamik olarak canlandırılması) tarama sırasında kullanılacak virüs tespiti yöntemlerinden biridir.
- **Sistem ortamını tara** (varsayılan olarak açık) - Tarama işlemi, bilgisayarınızın sistem alanlarını da kontrol edecektir.

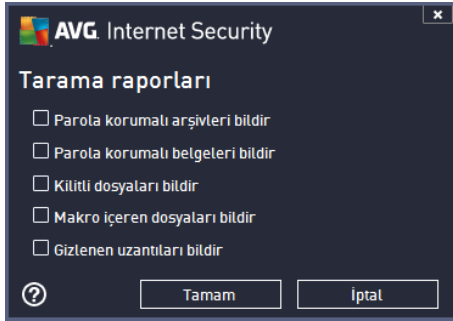
- **Kapsamli taramayi etkinlestir** (varsayilan olarak kapali) - Belirli durumlarda (bilgisayarınıza bulaşma olmasından şüpheleniyorsanız) yalnızca emin olmak üzere bilgisayarınızın bulaşma olması çok zor olan alanlarını bile tarayan en kapsamlı tarama algoritmalarını etkinleştirmek için bu seçeneği işaretleyebilirsiniz. Ancak, bu yöntemin çok fazla zaman aldığını unutmayın.
- **Ek tarama ayarları** - Bağlantı, şu parametreleri belirtebileceğiniz yeni bir Ek tarama ayarları iletişim kutusu açar:



- o **Bilgisayar kapatma seçenekleri** - Çalışan tarama işlemi bittiğinde bilgisayarın otomatik olarak kapatılması gerekir gerekmedikçe 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**).
- o **Taranacak dosya türleri** - taranacak dosya türleriyle ilgili aşağıdaki tercihlerden birini yapmanız gerekir:
  - **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 deđistirmemeniz önerilir. Uzantisi olmayan dosyalar süpheli olabilir ve her zaman taranmalıdır.

- **Taramanın ne kadar hızlı tamamlanacağını ayarlayın** - tarama sürecinin önceliđini deđistirmek için kaydırma çubugunu kullanabilirsiniz. Varsayılan olarak, bu seçenek otomatik kaynak kullanımının *kullanıcıya duyarlı* seviyesine ayarlıdır. Alternatif olarak, sistem kaynakları kullanımını minimize etmek için tarama işlemini yavaşlatabilir ( *bilgisayarda çalışmanız gerektiđi ancak taramanın ne kadar sürdüđünü önemsemediđiniz durumlar için uygundur*) veya sistem kaynaklarını daha yoğun kullanmak suretiyle daha hızlı bir şekilde (örn., *bilgisayar geçici bir süreyle kullanılmadığında*) çalıştırabilirsiniz.
- **Tarama raporu oluşturun** - bağlantı üzerinden **Tarama Raporları** isimli bir iletişim kutusu açılır ve buradan ne tip buluntuların rapor edileceđiniz seçebilirsiniz:



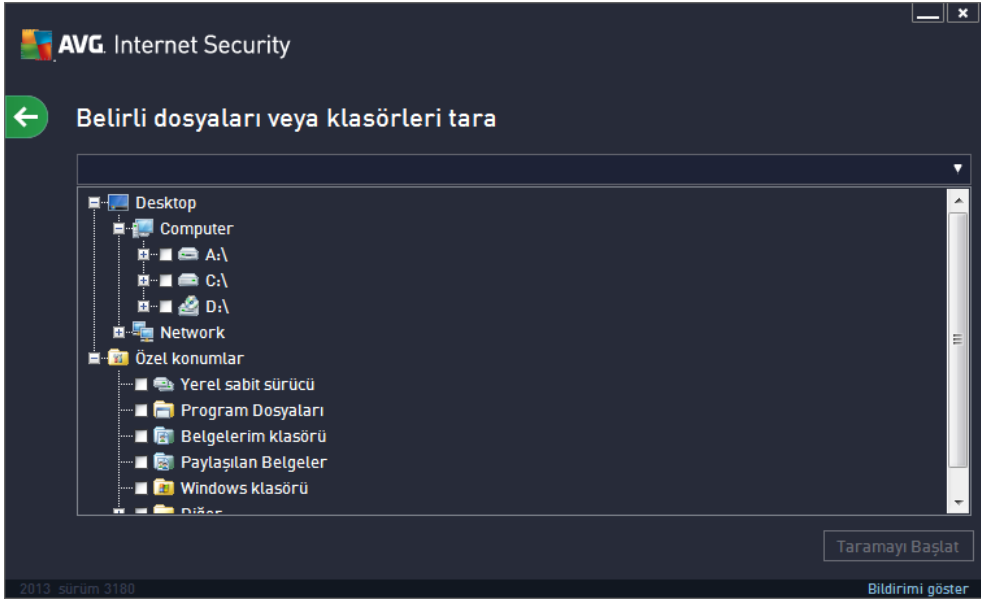
**Uyari:** Bu tarama parametreleri, yeni tanımlanan taramanın parametreleri ile aynıdır - [AVG Taraması / Tarama zamanlama / Tarama Tipi](#) bölümünde açıklanmış olduğu doğrultuda. **Tüm bilgisayarı tara** fonksiyonunun varsayılan yapılandırmasını deđistirmeye karar verirseniz yeni ayarlarınızı, belirli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

### 11.1.2. Belirli dosyaları veya klasörleri tara

**Belirli dosyaları veya klasörleri tara** - bilgisayarınızın sadece taranması için seçtiđiniz 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.

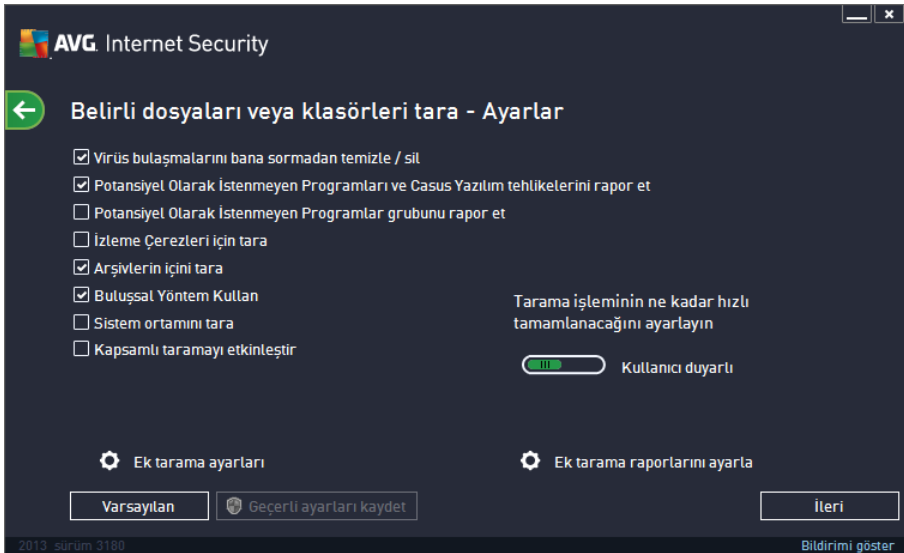
#### Tarama başlatma

**Belirli dosyaları veya klasörleri tara** işlemi doğrudan [Tarama seçenekleri](#) iletişim kutusundaki **Belirli dosyaları veya klasörleri tara** düğmesi tıklanarak başlatılabilir. Yeni bir **Tarama için belirli dosya ve klasörleri seçin** iletişim kutusu açılır. Bilgisayarınızın ağaç görünümünden taranmasını istediđiniz 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 seçenek 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 bilgisayarı tara](#) işlemi ile aynıdır.



## Tarama yapılandırması düzenleme

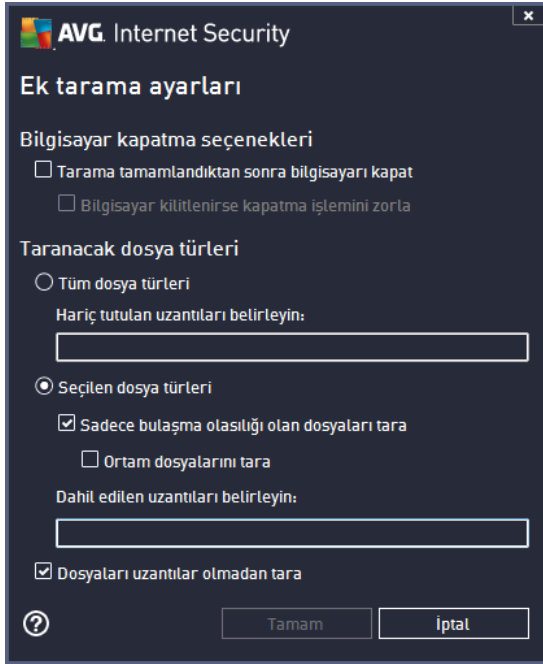
**Belirli dosyaları veya klasörleri tara** yapılandırmasını **Belirli dosyaları veya klasörleri tara - Ayarlar** iletişim kutusunda düzenleyebilirsiniz (*iletilim kutusuna [Tarama seçenekleri](#) iletişim kutusundaki Belirli dosyaları veya klasörleri tara seçeneğinde yer alan Ayarlar bağlantısından erişilebilir*). **Değiştirmek için geçerli bir nedeniniz olmadığı müddetçe varsayılan ayarları korumanız önerilir!**



Tarama parametreleri listesinde parametreleri ihtiyaçlarınıza uygun olarak açabilir / kapatabilirsiniz:

- **Bulasmayı bana sormadan temizle / kaldır** (varsayılan olarak açı): Tarama sırasında virüs tanımlanırsa, bir giderme yazılımı mevcutsa otomatik olarak temizlenir. Bulasmis dosya otomatik olarak temizlenemezse, bulasmis nesne [Virüs Kasası](#)'na taşınır.

- **Potansiyel Olarak İstenmeyen Programları ve Casus Yazılım tehditlerini rapor et** (varsayılan olarak açık): Virüslerin yani sira casus yazılımları da taramak için isaretleyin. 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 öneririz.
- **Potansiyel Olarak İstenmeyen Programlar gelişmiş grubunu rapor et** (varsayılan olarak kapalı): Casus yazılımların, yani doğrudan üreticiden alınan tamamen zararsız olan, ancak daha sonra kötüye kullanılacak programların genişletilmiş paketlerinin tespit edilmesi için isaretleyin. Bu, bilgisayar güvenliğinizi daha da artıran ek bir önlemdir, ancak yasal programları da engelleyebilir ve bu yüzden varsayılan olarak kapalıdır.
- **İzleme Çerezleri için tara** (varsayılan olarak kapalı): Bu parametre, tespit edilmesi istenen çerezleri tanımlar; (HTTP çerezleri kimlik doğrulaması, izleme ve kullanıcılar hakkındaki site tercihleri veya elektronik alışveriş sepetlerinin içeriği gibi belirli bilgilerin korunması için kullanılır).
- **Arsivleri tara** (varsayılan olarak açık): Bu parametre, ZIP, RAR vb. arşiv dosyalarının içinde sıkıştırılmış dosyaların bile taranmasını sağlar.
- **Bulussal Analiz Yöntemlerini Kullan** (varsayılan olarak açık): Bulussal analiz yöntemi (taranan nesnenin komutlarının sanal bir bilgisayar ortamında dinamik olarak canlandırılması) tarama sırasında kullanılacak virüs tespiti yöntemlerinden biridir.
- **Sistem ortamını tara** (varsayılan olarak kapalı): Tarama işlemi, bilgisayarınızın sistem alanlarını da kontrol edecektir.
- **Kapsamli taramayı etkinleştir** (varsayılan olarak kapalı): Belirli durumlarda (bilgisayarınıza bulasma olmasından şüpheleniyorsanız) yalnızca emin olmak üzere bilgisayarınızın bulasma olması çok zor olan alanlarını bile tarayan en kapsamlı tarama algoritmalarını etkinleştirmek için bu seçeneği isaretleyebilirsiniz. Ancak, bu yöntemin çok fazla zaman aldığını unutmayın.
- **Ek tarama ayarları** - Bağlantı, şu parametreleri belirtebileceğiniz yeni bir **Ek tarama ayarları** iletişim kutusu açar:

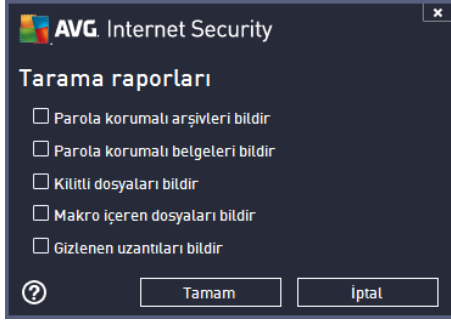


- **Bilgisayar kapatma seçenekleri** - Çalışan tarama işlemi bittğinde bilgisayarın otomatik olarak kapatılması gerekip gerekmediğine karar verir. Bu seçeneği seçerseniz (**Tarama bittikten sonra bilgisayarı kapat**) bilgisayar mevcut durumda kilitli olsa bile bilgisayarın kapatılmasını sağlayan bir seçeneğin bulunduğu bir pencere açılacaktır (**Bilgisayar kilitliyse bilgisayarı kapanmaya zorla**).
- **Taranacak dosya türleri** - taranacak dosya türleriyle ilgili aşağıdaki tercihlerden birini yapmanız gerekir:
  - **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. Varsayılan olarak, bu seçenek otomatik kaynak kullanımının *kullanıcıya duyarlı* seviyesine 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 yavaş kullanmak suretiyle daha hızlı



bir şekilde (ör., bilgisayar geçici bir süreyle kullanılmadığında) çalıştırabilirsiniz.

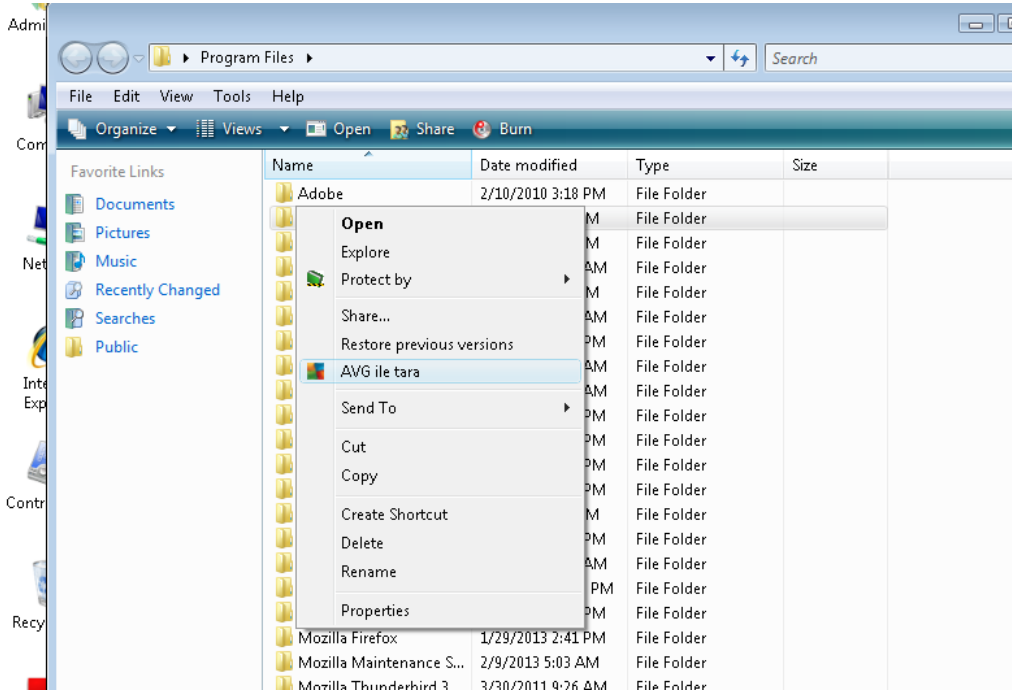
- **Tarama raporu oluşturun** - bağlantı üzerinden **Tarama Raporları** isimli yeni bir iletişim kutusu açılır ve buradan ne tip potansiyel bulguların rapor edileceğini seçebilirsiniz:



**Uyarı:** Bu tarama parametreleri, yeni tanımlanan taramanın parametreleri ile aynıdır - [AVG Taraması / Tarama zamanlama / Tarama Tipi](#) bölümünde açıklandığı doğrultuda. **Belirli dosya veya klasörleri tara** fonksiyonunun varsayılan yapılandırmasını değiştirmeye karar verirseniz 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 sablon görevi görecek (tüm özelleştirilmiş taramalar. Seçilen dosya ya da klasörleri tara fonksiyonunun mevcut yapılandırmasına dayanmaktadır).

## 11.2. Windows Gezgini'nde Tarama

Bilgisayarın tümünde ya da seçilen bölümlerinde gerçekleştirilen öntanımlı taramaların yanı sıra **AVG Internet Security 2013**, 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 istediginiz dosyayi (ya da klasörü) seçin
- Baglam menüsünü açmak için nesneye farenizle sag tiklatin
- **ile Tara** seçeneğini seçerek dosyanin AVG tarafından taranmasını saglayin **AVG Internet Security 2013**

### 11.3. Komut Satırı Tarama

**AVG Internet Security 2013** içinde, taramayı komut satirından çalıştırma seçeneği vardır. Bu seçeneği, sunucularda ya da bilgisayar yeniden başlatıldıktan sonra otomatik olarak çalıştırılacak komut metinlerinin oluşturulması sırasında kullanabilirsiniz. Komut satirında AVG'nin grafik kullanıcı arayüzünde sunulan parametrelerden daha fazlasını kullanarak tarama işlemini gerçekleştirebilirsiniz.

AVG taramasını komut satirından 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 yani sıra bir de tire işareti ile ayrılmalıdır
- Parametrelerden biri için belirli bir değer verilmesi gerekiyorsa (örneğin **/scan** parametresi taramak üzere bilgisayarınızın seçilen alanları hakkında bilgi talep eder ve sizin de seçilen bölüme ilişkin veri yolunu tam olarak sağlamanız gerekir). Değerler noktali 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 taraması gerektiğini belirlemek için kullanılan **/SCAN** parametresidir. Seçenekler hakkında daha ayrıntılı açıklama almak için [komut satiri parametrelerine genel bakis](#) bölümüne bakın.

Tarama işlemini başlatmak için **Enter** tusuna basın. Tarama sırasında işlemi **Ctrl+C** veya **Ctrl+Pause** tuslarını kullanarak durdurabilirsiniz.

#### Grafik arayüzünden başlatılan CMD taraması

Bilgisayarınızı Windows Güvenli Modda çalıştırdığınız zaman komut satiri taramasını grafik kullanıcı



arayüzünden baslatma seçeneğiniz de bulunmaktadır. Taramanın kendisi komut satirından baslatılacaktır, **Komut Satiri Olusturucu** iletisim kutusu, en yaygin tarama parametrelerini konforlu grafik arayüzünde görüntüler.

Söz konusu iletisim kutusuna sadece Windows Güvenli Moddan ulasilabildiginden iletisim kutusu hakkında ayrintili bilgi almak için dogrudan iletisim kutusundan açilan yardım dosyasini inceleyin.

### 11.3.1. CMD Tarama Parametreleri

Komut satiri taramada kullanilabilecek parametrelerin listesi:

- /SCAN [Belirli dosya ya da klasörleri tara](#) /SCAN=yol;yol (örn. /SCAN=C:\;D:\)
- /COMP [Tüm bilgisayari tara](#)
- /HEUR Bulussal analiz kullan
- /EXCLUDE Tarama isleminde dizin yolu veya dosyalari hariç tut
- /@ Komut dosyasi /dosya adi/
- /EXT Bu uzantilari tara / örneğin EXT=EXE,DLL/
- /NOEXT Bu uzantilari tarama / örneğin NOEXT=JPG/
- /ARC ArsiMeri tara
- /CLEAN Otomatik olarak temizle
- /TRASH Bulasan dosyalari [Virüs Kasasi](#)
- /QT Hizli test
- /LOG Bir tarama sonucu dosyasi olustur
- /MACROW Makrolari rapor et
- /PWDW Parola ile korunan dosyalari rapor et
- /ARCBOMBSW ArsiV bombalarini rapor et (*tekrar tekrar sikistirilan arsiVler*)
- /IGNLOCKED Kilitli dosyalari yoksay
- /REPORT Dosyaya /dosya adina/ rapor et
- /REPAPPEND Rapor dosyasina ekle
- /REPOK Bulasmamis dosyalari Tamam olarak rapor et
- /NOBREAK CTRL-BREAK ile islemin kesilmesine izin verme
- /BOOT MBR/BOOT kontrolünü etkinlestir

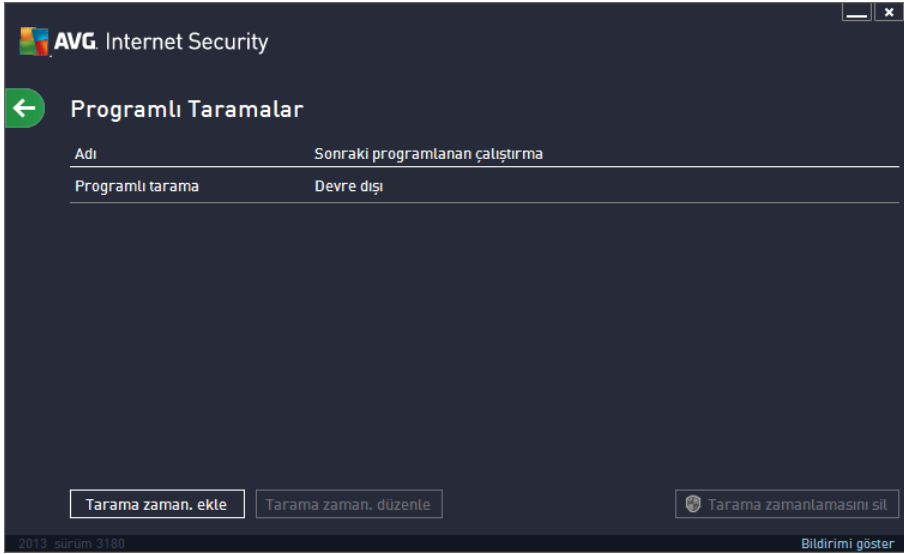


- /PROC Aktif islemleri tara
- /PUP Potansiyel olarak istenmeyen programlari rapor et
- /PUPEXT Potansiyel olarak istenmeyen programlar grubunu rapor et
- /REG Kayit defterini tara
- /COO Çerezleri tara
- /? Bu konuyla ilgili yardimi görüntüle
- /HELP Bu konuyla ilgili yardimi görüntüle
- /PRIORITY Tarama önceligini belirle /Düşük, Oto, Yüksek/ (bkz. [Gelismiş ayarlar / Taramalar](#))
- /SHUTDOWN Tarama tamamlandıktan sonra bilgisayari kapat
- /FORCESHUTDOWN Tarama tamamlandıktan sonra bilgisayari kapatmayı zorla
- /ADS Alternatif Veri Akislarini Tara (yalnızca NTFS)
- /HIDDEN Gizli uzantili dosyalari rapor et
- /INFECTABLEONLY Yalnızca bulasabilir uzantiya sahip dosyalari tara
- /THOROUGHSCAN Kapsamli taramayi etkinlestir
- /CLOUDCHECK Hatali tespitler açısından denetle
- /ARCBOMBSW Yeniden sikistirilmiş arşiv dosyalarini rapor et

#### 11.4. Tarama Programlama


**AVG Internet Security 2013** ile isteginiz dogrultusunda tarama yapmanin (*örneğin bilgisayarınıza virüs bulastigindan şüphelenirseniz*) yani sıra zamanlanan bir plan dogrultusunda da tarama yapabilirsiniz. Taramaların bir program dogrultusunda yapılması önerilmektedir: bu şekilde, bilgisayarınızın virüs bulması ihtimaline karşı korundugundan emin olursunuz ve ne zaman tarama yapmanız gerektiği konusunda endişelenmenize gerek kalmaz. [Tüm bilgisayar taraması](#) islemini en az haftada bir kez düzenli olarak baslatmanız gerekir. Diğer yandan, yapabiliyorsanız programli taramanın varsayılan yapılandırmasında ayarlandığı gibi tüm bilgisayar taramasını günlük olarak yapın. Bilgisayarınız "daima açık" ise taramaları çalışma saatlerinden sonra gerçekleştirilecek şekilde programlayabilirsiniz. Bilgisayarınızı arada sırada kapatıyorsanız taramayı, taramaları [görev yerine getirilemediginde bilgisayarın başlaması ile baslat](#) şeklinde programlayın.

Tarama zamanlaması [Tarama seçenekleri](#) iletişim kutusundaki **Zamanlanmış taramayı yönet** düğmesiyle erişilebilen **Zamanlanmış taramalar** iletişim kutusunda oluşturulabilir / düzenlenebilir. Yeni **Zamanlanmış Tarama** iletişim kutusunda geçerli olarak zamanlanmış olan tüm taramaların genel görünümünü görebilirsiniz:



Kendi taramalarınızı tanımlamadan önce, listede yalnızca yazılım sağlayıcısı tarafından önceden tanımlanmış tek bir zamanlanmış tarama görebilirsiniz. Tarama varsayılan olarak kapatılmıştır. Taramayı açmak için sağ tıklatın ve bağlam menüsünden **Görevi etkinleştir**i seçin. Zamanlanmış tarama etkinleştirildiğinde **Tarama zaman. düzenle** düğmesiyle [taramanın yapılandırmasını düzenleyebilirsiniz](#). Kendi istediğiniz yeni bir tarama zamanlaması oluşturmak için **Tarama zaman. ekle** düğmesini de tıklatabilirsiniz. Planlanan tarama parametreleri üç sekmeden düzenlenebilir ( *ya da yeni bir zamanlama ayarlanabilir*):

- [Zamanla](#)
- [Ayarlar](#)
- [Konum](#)

Her sekmede "trafik ışığı" düğmesini kullanarak  zamanlanan testi geçici olarak devre dışı bırakabilir ve gerek duyduğunuzda tekrar açabilirsiniz:

### 11.4.1. Zamanla




**Zamanla** sekmesinin üst bölümünde geçerli olarak tanımlanmış tarama zamanlaması için ad belirleyebileceğiniz metin alanını bulabilirsiniz. Programladığınız taramaları diğerlerinden kolaylıkla ayırabilmek için her zaman taramalarınıza kısa, açıklayıcı adlar vermeye çalışın. Örneğin, Taramayı "Yeni Tarama" veya "Taramam" adıyla adlandırmanız uygun değildir çünkü bu adlar, taramanın fiilen neyi kontrol ettiğini açıklamaz. Diğer bir yandan "Sistem alanı taraması" vb. oldukça açıklayıcı bir isim olacaktır.

Bu iletişim kutusunda taramanın aşağıdaki parametrelerini de tanımlayabilirsiniz:

- **Çalışmayı programla** - 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 başlatılmasında çalıştır*) tanımlanabilir.
- **Gelişmiş planlama seçenekleri** - Bu bölümde, bilgisayar düşük güç modundayken veya tamamen kapatılmışsa hangi koşullar altında taramanın başlatılması/baslatılmaması gerektiğini belirleyebilirsiniz. Programlanan tarama belirttiğiniz saatte başlatıldığında, [AVG sistem tepsi simgesi](#) üzerinde bir açılır pencere ile bu konuda bilgilendirileceksiniz. Bunun ardından yeni bir [AVG sistem tepsi 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.

#### İletişim kutusundaki kontroller

- **Kaydet** - Bu sekmede veya bu iletişim kutusunun başka herhangi bir sekmesinde gerçekleştirdiğiniz tüm değişiklikleri kaydeder ve [Zamanlanmış taramalar](#) genel görünümüne geri döner. Bu nedenle tüm sekmelerdeki test parametrelerini yapılandırmak istiyorsanız gereksinimlerinizin tamamını belirledikten sonra bunları kaydetmek için düğmeye basın.

-  - [Zamanlanmış taramalar](#) genel görünümüne dönmek için sol üst kısımdaki yeşil oku kullanın.

## 11.4.2. Ayarlar



**Ayarlar** sekmesinin üst bölümünde geçerli olarak tanımlanmış tarama zamanlaması için ad belirleyebileceğiniz metin alanını bulabilirsiniz. Programladığınız taramaları diğerlerinden kolaylıkla ayırabilmek için her zaman taramalarınıza kısa, açıklayıcı adlar vermeye çalışın. Örneğin, Taramayı "Yeni Tarama" veya "Taramam" adıyla adlandırmanız uygun değildir çünkü bu adlar, taramanın fiilen neyi kontrol ettiğini açıklamaz. Diğer bir yandan "Sistem alanı taraması" vb. oldukça açıklayıcı bir isim olacaktır.

**Ayarlar** sekmesinde, isteğe bağlı olarak açılıp/kapatılabilen tarama parametrelerine ilişkin bir liste bulabilirsiniz. **Söz konusu ayarları değiştirmek açısından geçerli bir nedeniniz yoksa öntanımlı yapılandırmayı olduğu gibi muhafaza etmeniz önerilir.**

- **Bulaşmayı bana sormadan temizle / kaldır** (varsayılan olarak açık): Tarama sırasında virüs tanımlanırsa, bir giderme yazılımı mevcutsa otomatik olarak temizlenir. Bulaşmış dosya otomatik olarak temizlenemezse, bulaşmış nesne [Virüs Kasası](#)'na tasınır.
- **Potansiyel Olarak İstenmeyen Programları ve Casus Yazılım tehditlerini rapor et** (varsayılan olarak açık): virüslerin yani sıra casus yazılımları da taramak 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 öneririz.
- **Potansiyel Olarak İstenmeyen Programlar gelişmiş grubunu rapor et** (varsayılan olarak kapalı): 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 Çerezleri için tara** (varsayılan olarak kapalı): bu parametre, tarama sırasında tespit



edilmesi istenen çerezleri tanımlar (*HTTP çerezleri kimlik doğrulaması, izleme ve kullanıcılar hakkındaki site tercihleri veya elektronik alışveriş sepetlerinin içeriği gibi belirli bilgilerin korunması için kullanılır*).

- **Arsivleri tara** - (*varsayılan olarak kapalı*): bu parametre, tarama işleminin ZIP, RAR gibi belirli bir arşiv türü ile sıkıştırılmış olsa bile tüm dosyaların taranması gerektiğini belirtir.
- **Bulussal Analiz Yöntemlerini Kullan** - (*varsayılan olarak açıktır*). Bulussal 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 kapalı*) 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.
- **Kök dizinleri tara** (*varsayılan olarak açık*): Anti-Rootkit taraması bilgisayarınızı olası rootkitlere, örneğin bilgisayarınızda kötü amaçlı etkinlik içerebilecek programlar ve teknolojilere karşı tarar. Bir kök dizin algılanırsa, bu, bilgisayarınızda mutlaka virüs olduğu anlamına gelmez. Bazı durumlarda, belirli sürücüler veya normal uygulamaların bölümleri kök dizin olarak yanlış algılanabilir.

## Ek tarama ayarları

Bağlantı, şu parametreleri belirtebileceğiniz yeni bir **Ek Tarama Ayarları** iletişim kutusu açar:

The screenshot shows the 'Ek tarama ayarları' (Advanced Scan Settings) dialog box in AVG Internet Security. The dialog is titled 'AVG. Internet Security' and has a close button in the top right corner. It contains the following sections and options:

- Bilgisayar kapatma seçenekleri**
  - Tarama tamamlandıktan sonra bilgisayarı kapat
  - Bilgisayar kilitlenirse kapatma işlemini zorla
- Taranacak dosya türleri**
  - Tüm dosya türleri
  - Hariç tutulan uzantıları belirleyin:
  - Seçilen dosya türleri
    - Sadece bulaşma olasılığı olan dosyaları tara
    - Ortam dosyalarını tara
  - Dahil edilen uzantıları belirleyin:
  - Dosyaları uzantılar olmadan tara

At the bottom, there is a help icon (question mark), a 'Tamam' (OK) button, and an 'İptal' (Cancel) button.

- **Bilgisayar kapatma seçenekleri** - Çalışan tarama işlemi bittiginde bilgisayarın otomatik olarak kapatılması gerekip gerekmediğine karar verir. Bu seçeneği onaylarsanız (*Tarama*



*bittikten sonra bilgisayari kapat) bilgisayar mevcut durumda kilitli olsa bile bilgisayarın kapatilmasini saglayan bir seçenegin bulunduđu bir pencere açilacaktır (Bilgisayar kilitliyse bilgisayari kapanmaya zorla).*

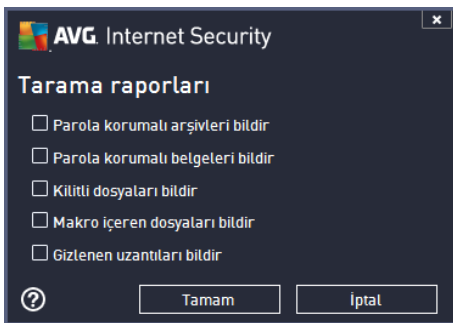
- **Taranacak dosya türleri** - taranacak dosya türleriyle ilgili asagidaki tercihlerden birini yapmanız gerekir:
  - **Tüm dosya türleri** taranmaması gereken virgülle ayrılmış dosya uzantılarının listesini saglayarak taramada istisnaları tanımlama seçeneğiyle;
  - **Seçili dosya türleri** - yalnızca virüs bulasabilme olasılığı olan dosyaları taramayı istediğinizi belirtebilirsiniz (*virüs bulasamayan 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 bulasma 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 süpheli olabilir ve her zaman taranmalıdır.

### Taramanın ne kadar hızlı tamamlanacağını ayarla


Bu bölümde ayrıca istenen tarama hızını, sistemin kaynak kullanımına bağlı olarak belirleyebilirsiniz. Varsayılan olarak, bu seçenek otomatik kaynak kullanımının *kullanıcıya duyarlı* seviyesine ayarlıdır. Tarama işleminin daha hızlı ilerlemesini istiyorsanız tarama işlemi daha kısa sürecektir fakat tarama işlemi sırasında sistem kaynakları oldukça yüklü bir şekilde kullanılacak ve bilgisayar üzerindeki diğer işlemleri yavaşlatacaktır (*bu seçenek bilgisayarınız açıkken kullanılmadığı sırada seçilebilir*). Öte yandan, tarama süresini uzatarak sistem kaynaklarının kullanımını azaltabilirsiniz.

### Ek tarama raporlarını ayarla

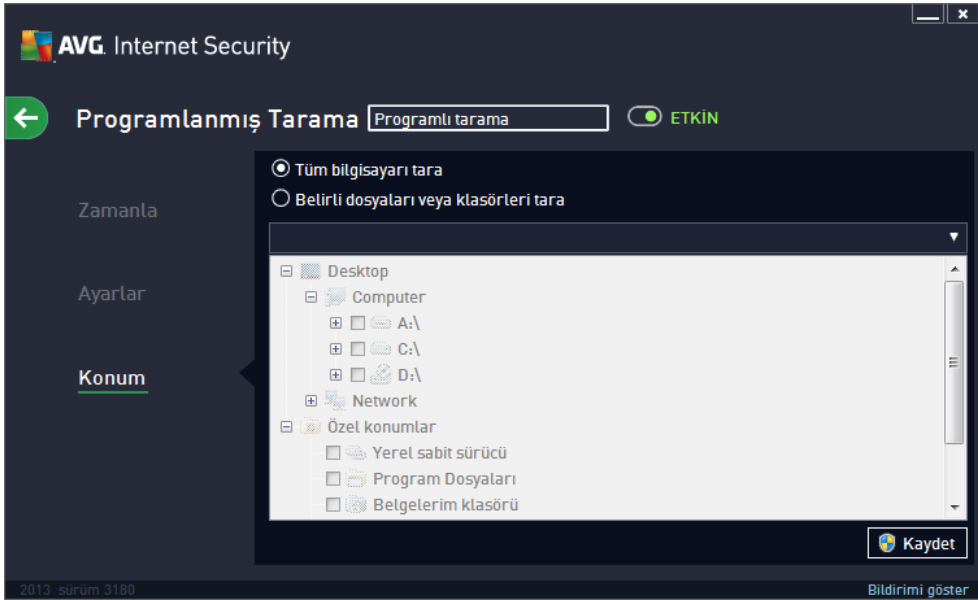
Tarama bulgularının rapor edilmesi gerekip gerekmediğini tanımlamak üzere birden fazla öğeyi ayarlayabileceğiniz **Tarama raporları** olarak adlandırılan bağımsız bir iletişim penceresi açmak için **Ek tarama raporlarını ayarla...** bağlantısını tıklayın:



### İletişim kutusundaki kontroller

- **Kaydet** - Bu sekmede veya bu iletişim kutusunun başka herhangi bir sekmesinde gerçekleştirdiğiniz tüm değişiklikleri kaydeder ve [Zamanlanmış taramalar](#) genel görünümüne geri döner. Bu nedenle tüm sekmelerdeki test parametrelerini yapılandırmak istiyorsanız gereksinimlerinizin tamamını belirledikten sonra bunları kaydetmek için düğmeye basın.
-  - [Zamanlanmış taramalar](#) genel görünümüne dönmek için sol üst kısımdaki yeşil oku kullanın.

### 11.4.3. Konum



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

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


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



- **Belgelerim klasörü**

- *Win XP için:* C:\Documents and Settings\Default User\Belgelerim\
  - *Windows Vista/7 için:* C:\Users\user\Documents\
    - *Windows Vista/7 için:* C:\Users\Public\Documents\
      - *Windows klasörü* - C:\Windows\
        - **Diger**
          - *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*)

## **İletişim kutusundaki kontroller**

- **Kaydet** - Bu sekmede veya bu iletişim kutusunun başka herhangi bir sekmesinde gerçekleştirdiğiniz tüm değişiklikleri kaydeder ve [Zamanlanmış taramalar](#) genel görünümüne geri döner. Bu nedenle tüm sekmelerdeki test parametrelerini yapılandırmak istiyorsanız gereksinimlerinizin tamamını belirledikten sonra bunları kaydetmek için düğmeye basın.
-  - [Zamanlanmış taramalar](#) genel görünümüne dönmek için sol üst kısımdaki yeşil oku kullanın.







## 11.5. Tarama Sonuçları



The screenshot shows the AVG Internet Security interface. The window title is "AVG Internet Security". The main heading is "Tarama sonuçları genel görünümü". Below this is a table with the following columns: "Adı", "Başlangıç za...", "Bitiş zamanı", "Test edilen ne...", "Bulaşmalar", and "Yüksek". The table contains one row with the following data: "Tüm bilgisayarı tara", "2/9/2013, 5:08", "2/9/2013, 5:09", "4649", "0", and "0". At the bottom of the window, there are buttons for "Ayrıntıları göster" and "Sonucu sil".

Adı	Başlangıç za...	Bitiş zamanı	Test edilen ne...	Bulaşmalar	Yüksek
Tüm bilgisayarı tara	2/9/2013, 5:08	2/9/2013, 5:09	4649	0	0

**Tarama sonuçları genel görünümü** iletişim kutusu o ana kadar gerçekleştirilmiş tüm taramaların sonuçlarını listeler. Tabloda her tarama sonucuna ilişkin olarak şu bilgiler bulunur:


- **Simge** - İlk sütunda taramanın durumunu açıklayan bir bilgi simgesi gösterilir:
  -  Bulaşma bulunmadı, tarama tamamlandı
  -  Bulaşma bulunmadı, tarama tamamlanmadan yarıda kesildi
  -  Bulaşma bulundu ve iyileştirilmedi, tarama tamamlandı
  -  Bulaşma bulundu ve temizlenmedi, tarama tamamlanmadan yarıda kesildi
  -  Bulaşmalar bulundu ve tümü iyileştirildi veya kaldırıldı, tarama tamamlandı
  -  Bulaşmalar bulundu ve tümü temizlendi veya kaldırıldı, tarama tamamlanmadan yarıda kesildi
- **Ad** - Bu sütun ilgili taramanın adını gösterir. Bu ya iki [öntanımlı taramadan](#) biridir ya da sizin kendi [zamanlanmış taramanızdır](#).
- **Başlangıç zamanı** - Taramanın başlatıldığı tarih ve saati verir.
- **Bitiş zamanı** - Taramanın tamamlandığı, duraklatıldığı veya kesildiği tarih ve saati verir.
- **Test edilen nesnelere** - Taranan toplam nesne sayısını gösterir.
- **Bulaşmalar** - Kaldırılan/bulunan toplam bulaşma sayısını verir.
- **Yüksek / Orta / Düşük** - Sonraki üç sütun sırasıyla bulunan yüksek, orta ve düşük öncelikli bulaşma sayısını verir.

- **Rootkitler** - Tarama sırasında bulunan toplam [rootkit](#) sayısını gösterir.

### İletişim kutusu kontrolleri

**Ayrıntıları göster** - Seçilen bir tarama hakkındaki ayrıntılı bilgileri görmek [için bu düğmeyi tıklatin](#) (yukarıdaki tabloda vurgulanır).

**Sonuçları sil** - Seçilen bir tarama sonucunu tablodan kaldırmak için bu düğmeyi tıklatin.

 - Bileşen genel bilgilerinin bulunduğu [ana kullanıcı arayüzüne](#) dönmek için iletişim kutusunun sol üst kısmında bulunan yeşil oku kullanın.

### 11.6. Tarama sonuçları ayrıntıları

Seçilen bir tarama sonucunun ayrıntılı bilgilerini açmak için [Tarama sonuçları genel görünümü](#) iletişim kutusundan erişilebilen **Ayrıntıları göster** düğmesini tıklatin. Aynı iletişim kutusu arayüzünde ilgili tarama sonucu hakkında ayrıntılı bilgilerin açıklandığı bölüme yönlendirilirsiniz. Bilgiler üç sekmede gösterilir:

- **Özet** - Bu sekme tarama hakkındaki temel bilgileri sunar: Taramanın başarıyla tamamlanıp tamamlanmadığı, tehdit tespit edilip edilmediği ve tespit edilenlere ne olduğu.
- **Ayrıntılar** - Bu sekme tespit edilen tüm tespitlerin ayrıntıları da dahil olmak üzere tarama hakkındaki tüm bilgileri gösterir. Genel görünümü dosyaya aktar ayrıntıları .csv dosyası olarak kaydetmenize olanak tanır.
- **Tespitler** - Bu sekme ancak tarama sırasında tehdit tespit edilmişse görüntülenir ve tehditler hakkında ayrıntılı bilgiler sunar:

• **Düşük önem derecesi:** bilgiler veya uyarılar, gerçek tehditler değildir. Genellikle makro içeren belgeler, parola ile korunan belgeler veya arşivler, kilitli dosyalar vb.

• **Orta önem derecesi:** genellikle PUP (potansiyel olarak istenmeyen programlar, reklam yazılımı gibi) veya izleme çerezleri

• **Yüksek önem derecesi:** virüsler, Truva atları, açiktan yararlanma girişimleri vb. ciddi tehditler. Ayrıca Bulussal Yöntem tespit yöntemi tarafından tespit edilen nesnelere, virüs veritabanında henüz tanımlanmamış tehditler gibi.

## 12. Virüs Kasası



**Virüs Kasası** AVG taramaları sırasında tespit edilen şüpheli/bulasmış nesnelere yönetilmesi için güvenli bir ortamdır. Tarama sırasında bulasmış bir nesne tespit edildikten sonra AVG, söz konusu bulaşmayı otomatik olarak temizleyemiyorsa şüpheli nesne hakkında ne yapmak istediğiniz sorulur. Önerilen çözüm, nesneyi daha sonra ilgilenmek üzere **Virüs Kasasına** tasimaktır. **Virüs Kasası**ni 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 bulasmış nesnelere hakkında genel bilgi içerir:

- **Saklama tarihi** - Şüpheli dosyanın tespit edildiği ve Virüs Kasası'na kaldırıldığı tarih ve saati gösterir.
- **Önem seviyesi** - [Identity](#) bileşenini **AVG Internet Security 2013** uygulamanıza yüklemeye karar verdiğinizde, ilgili bulgunun önem seviyesinin grafik bir tanımı dört seviyeli bir ölçekte kusursuz bir şekilde (*üç yeşil nokta*) çok tehlikeli seviyesine kadar (*üç kırmızı nokta*) dört seviyeli bir ölçekte grafik olarak gösterimi ve bulaşma türü hakkındaki bilgiler (*bulaşma seviyesine bağlı olarak - listelenen tüm nesnelere virüs bulaşmıştır veya bulaşma olasılığı vardır*) bu bölümde gösterilir.
- **Tespit Adı** - Tespit edilen bulaşmanın adını çevrimiçi [virüs ansiklopedisine](#) göre belirtir.
- **Kaynak** - İlgili tehdidi hangi **AVG Internet Security 2013** bileşeninin tespit ettiğini belirtir.
- **Mesajlar** - Çok nadiren, bu sütunda ilgili tehdit hakkında ayrıntılı açıklamalar sunan notlar gösterilebilir.



## Kontrol düğmeleri

**Virüs Kasası** arayüzünden ulaşabileceğiniz kontrol düğmeleri şunlardır:

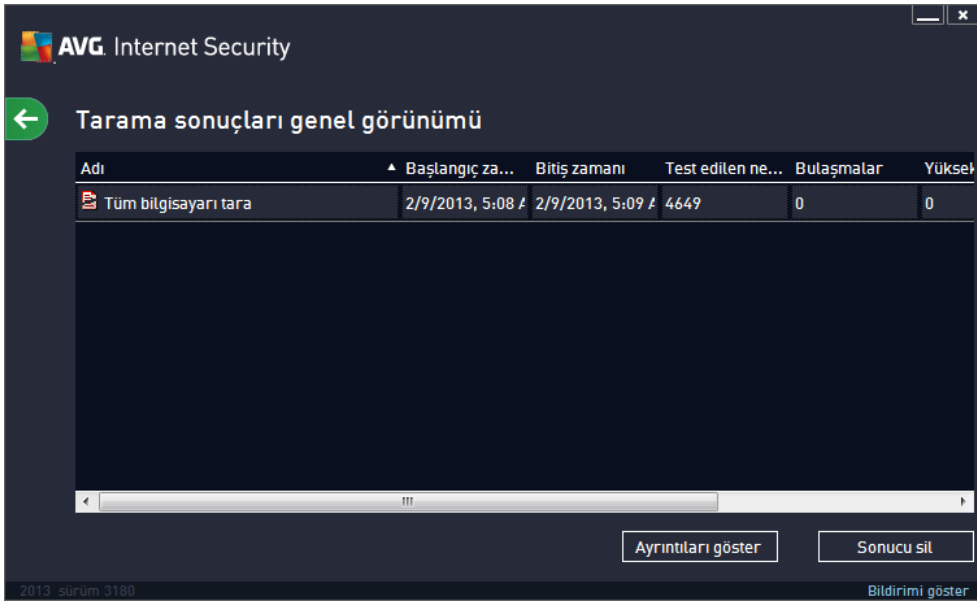
- **Geri Yükle** - bulasmis dosyayı sabit diskinizdeki orijinal konumuna geri yükler.
- **Farkli Geri Yükle** - bulasmis dosyayı seçili klasöre tasir.
- **Ayrıntılar** - **Virüs Kasası**'nda karantinaya alınan tehdit hakkında ayrıntili bilgi için listede seçili öğeyi vurgulayın ve **Ayrıntılar** düğmesini tıklatarak tespit edilen tehdidin açıklamasını içeren yeni bir iletişim kutusu açın.
- **Sil** - bulasmis dosyayı **Virüs Kasası**'ndan tamamen ve geri döndürülemez şekilde siler.
- **Kasayı Bosalt** - **Virüs Kasası** içeriğini tamamen temizler. Dosyaları **Virüs Kasası**'ndan kaldırdığınızda, bu dosyalar diskten geri alınmayacak biçimde kaldırılır (**Geri Dönüşüm Kutusu'na tasınmaz**).


## 13. Geçmiş

**Geçmiş** bölümü tüm geçmiş olaylarla ilgili bilgileri içerir(güncellemeler, taramalar, tespitler vb.) ve bu olaylar hakkında rapor verir. Bu bölüme [ana kullanıcı arayüzündeki Seçenekler / Geçmiş](#) öğeleri yoluyla erişilebilir. Kaydedilen olayların tüm geçmişi şu bölümlere ayrılmıştır:

- [Tarama sonuçları](#)
- [Yerlesik Kalkan tespiti](#)
- [E-posta Koruması tespiti](#)
- [Online Shield tespitleri](#)
- [Olay geçmişi günlüğü](#)
- [Firewall günlüğü](#)


### 13.1. Tarama sonuçları




Adı	Başlangıç za...	Bitiş zamanı	Test edilen ne...	Bulaşmalar	Yüksek
 Tüm bilgisayarları tarama	2/9/2013, 5:08	2/9/2013, 5:09	4649	0	0


**Tarama sonuçları genel görünümü** iletişim kutusuna **AVG Internet Security 2013** ana penceresinin üst satırındaki gezinme bölümünden **Seçenekler / Geçmiş / Tarama sonuçları** menü öğesi yoluyla erişilebilir. İletişim kutusunda, daha önce baslatılan 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 bulasmanın tespit edildiğini ancak bulasmanın nesnenin otomatik olarak silindiğini gösterir

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


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

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

- **Baslangıç zamanı** - taramanın başlatıldığı tarih ve saati gösterir.
- **Bitiş zamanı** - taramanın bittiği tarih ve saati gösterir.
- **Taranan nesnelere** - tarama sırasında kontrol edilen nesne sayısıdır
- **Bulasmalar** - tespit edilen / silinenvirüs bulasma sayısı
- **Yüksek / Orta / Düşük** - bu sütunlar kaldırılan/bulunan toplam bulasma sayısını sırasıyla yüksek, orta ve düşük önem seviyesine göre gösterir
- **Bilgi** - tarama işlemine ve sonucuna ilişkin bilgiler (*genellikle işlemin tamamlanmasının ya da kesilmesinin hemen ardından görüntülenir*)
- **Kök dizinler** - algılanan [kök dizinlerin](#)

### Kontrol düğmeleri

**Tarama sonuçlarına genel bakış** penceresindeki kontrol düğmeleri şunlardır:

- **Ayrıntıları göster** - seçili taramada ayrıntılı verileri görüntülemek için [Tarama sonuçları](#) iletişim kutusuna geçmek için basın
- **Sonucu sil** - seçili öğeyi tarama sonuçlarına genel bakıştan silmek için basın
-  - varsayılan [AVG ana iletişim kutusuna](#) (*bilesen genel görünümü*) geri dönmek için bu iletişim kutusunun sol üst kısmındaki oku kullanın

### 13.2. Yerleşik Kalkan tespiti

**Yerleşik Kalkan** hizmeti [Bilgisayar](#) bileşenin bir parçasıdır ve kopyalanan, açılan veya kaydedilen dosyaları tarar. Herhangi bir virüs ya da bir tehlike tespit edildiği zaman aşağıdaki iletişim kutusu ile anında uyarılırsınız:

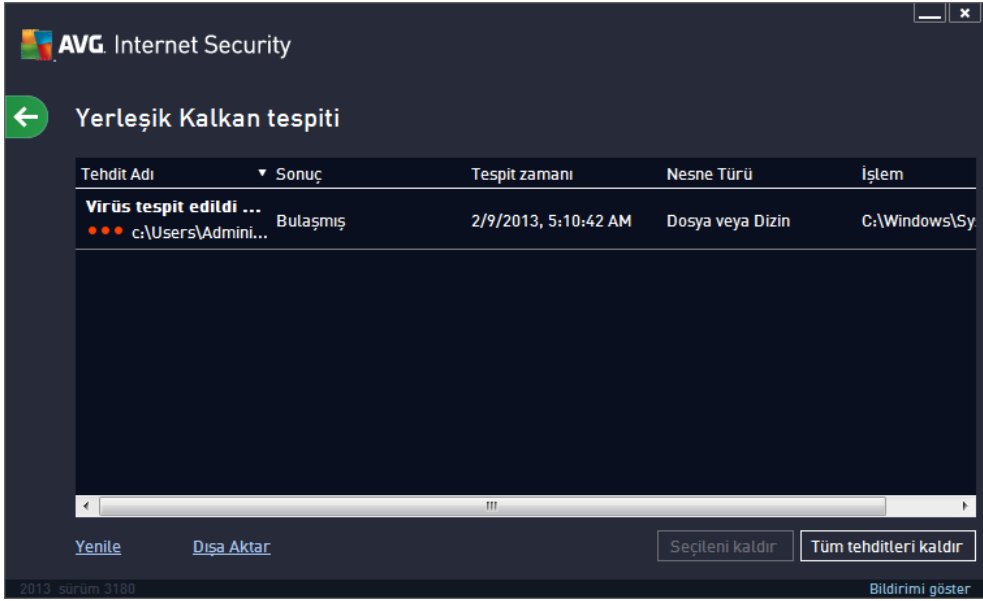


Bu uyarı iletişim kutusunda tespit edilen ve virüs bulasmis olarak atanan nesne hakkında daha fazla bilgi (*Ad*) ve ilgili bulasma hakkında bazı açıklamalar (*Açıklama*) bulabilirsiniz. [Ayrıntıları göster](#) bağlantısı, sizi tespit edilen bulasma hakkında ayrıntılı bilgi bulabileceğiniz (biliniyorsa) çevrimiçi virüs ansiklopedisine yönlendirir. İletişim kutusunda, tespit edilen tehdide yönelik olarak kullanabileceğiniz çözümler hakkında genel bilgiler de bulabilirsiniz. Alternatiflerden birin önerilen olarak etiketlenir: **Beni Korum (önerilir). Yapabiliyorsanız, her zaman bu seçeneği kullanın!**

**Not:** Tespit edilen nesnenin büyüklüğü, Virüs Kasası'ndaki boş alan sinirini asabilir. Bu durumda, bulasmis nesneyi Virüs Kasası'na tasimaya çalıştığınızda size bu sorun hakkında bilgi veren bir uyarı iletisi görüntülenir. Ancak Virüs Kasası boyutu degistirilebilir. Sabit diskinizin gerçek boyutunun uyarlanabilir yüzdesi olarak tanımlanır. Virüs Kasanizin boyutunu arttırmak için, 'Virüs Kasası boyutunu sınırlandır' seçeneği aracılığıyla [AVG Gelismis Ayarlardaki Virüs Kasası](#) iletişim kutusuna gidin.

İletişim kutusunun alt kısmında **Ayrıntıları göster** bağlantısını bulabilirsiniz. Bağlantıyı tıklatarak bulasma tespit edildiğinde çalışan işlem ve işlemin tanımlanması hakkında ayrıntılı bilgilerin bulunduğu yeni bir pencere açabilirsiniz.


Yerlesik Kalkan tespitlerinin tamamının listesine **Yerlesik Kalkan tespiti** iletişim kutusundan erişilebilir. Bu iletişim kutusuna **AVG Internet Security 2013 ana penceresinin** üst bölümünde yer alan **Seçenekler / Geçmiş / Yerlesik Kalkan tespiti** menü ögesi yoluyla erişilebilir. İletişim kutusu yerlesik kalkan tarafından tespit edilip tehlikeli olduğu görülen ve temizlenen ya da [Virüs Kasası](#)'na tasinan nesnelere hakkında genel bilgi vermektedir.



Tespit edilen tüm nesnelere için aşağıdaki bilgiler verilir:

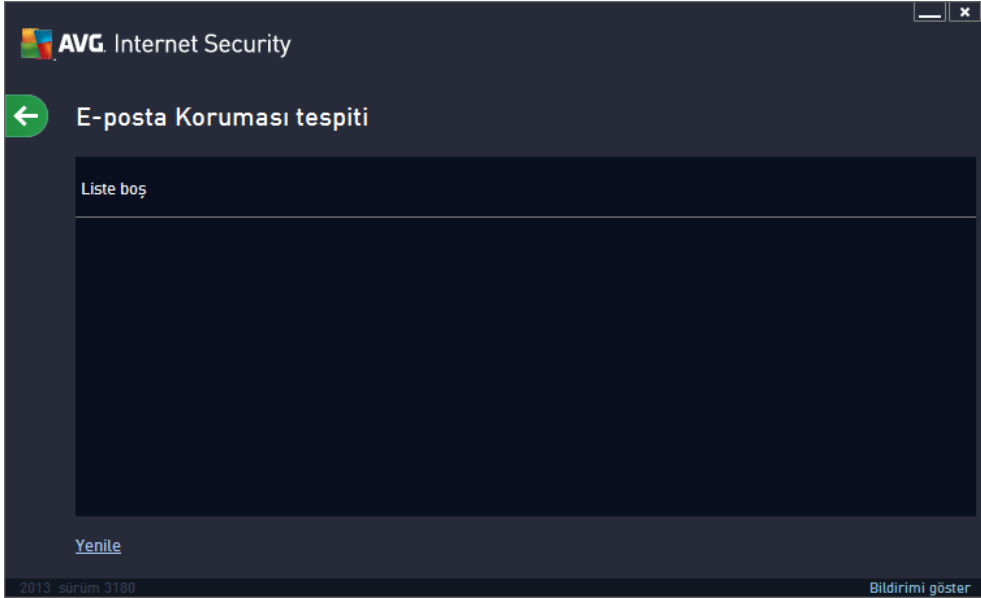
- **Tespit adı** - tespit edilen nesnenin adı (*muhtemelen adı da*) ve konumu
- **Sonuç** - tespit edilen nesne ile gerçekleştirilen eylem
- **Algılama zamanı** - Tehlikenin algılandığı ve engellendiği tarih ve saat
- **Nesne Türü** - tespit edilen nesnenin türü
- **İşlem** - tespit edilmesi amacıyla potansiyel tehlike taşıyan nesneyi uyararak işlem nedir

### Kontrol düğmeleri

- **Yenile - Online Shield**
- **Dışa aktar** - tespit edilen tüm nesnelere bir dosyada dışa aktarın
- **Seçileni kaldır** - listeden seçilen kayıtları vurgulayabilir ve bu düğmeyi kullanarak yalnızca bu seçilen öğeleri silebilirsiniz
- **Tüm tehditleri kaldır** - iletişim kutusunda listelenen tüm kayıtları silmek için bu düğmeyi kullanın
-  - varsayılan [AVG ana iletişim kutusuna](#) (*bilesen genel görünümü*) geri dönmek için bu iletişim kutusunun sol üst kısmındaki oku kullanın

### 13.3. E-posta Koruması tespiti

**E-posta Koruması tespiti** iletişim kutusuna **AVG Internet Security 2013** ana penceresinin üst satır gezinme menüsünün **Seçenekler / Geçmiş / E-posta Koruması tespiti** ögesi yoluyla erişilebilir.




İletişim kutusunda [E-postalar](#) bileşenin tespit ettiği tüm bulguların listesi bulunur. Tespit edilen tüm nesnelere için aşağıdaki bilgiler verilir:

- **Tespit adı** - tespit edilen nesnenin açıklaması (*muhtemelen adı da*) ve kaynağı
- **Sonuç** - tespit edilen nesne ile gerçekleştirilen eylem
- **Algılama zamanı** - Şüpheli nesnenin algılandığı tarih ve saat
- **Nesne Türü** - tespit edilen nesnenin türü
- **İşlem** - tespit edilmesi amacıyla potansiyel tehlike taşıyan nesneyi uyararak işlem nedir

İletişim penceresinin alt kısmında, listenin altında yukarıda listelenen tespit edilen nesnelere toplam sayısı hakkında bilgi bulabilirsiniz. Ayrıca, tespit edilen nesnelere listesini ayrı bir dosyaya dışarı aktarabilirsiniz (**Listeyi dosyaya aktar**) ve tespit edilen nesnelere hakkındaki tüm girişleri silebilirsiniz (**Listeyi temizle**).

#### Kontrol düğmeleri

**E-posta Tarayıcısı tespiti** arayüzünde bulunan kontrol düğmeleri şunlardır:

- **Listeyi yenile** - Algılanan tehlikelerin listesini günceller.
-  - varsayılan [AVG ana iletişim kutusuna](#) (bileşenin genel görünümü) geri dönmek için bu iletişim kutusunun sol üst kısmındaki oku kullanın



### 13.4. Online Shield tespitleri

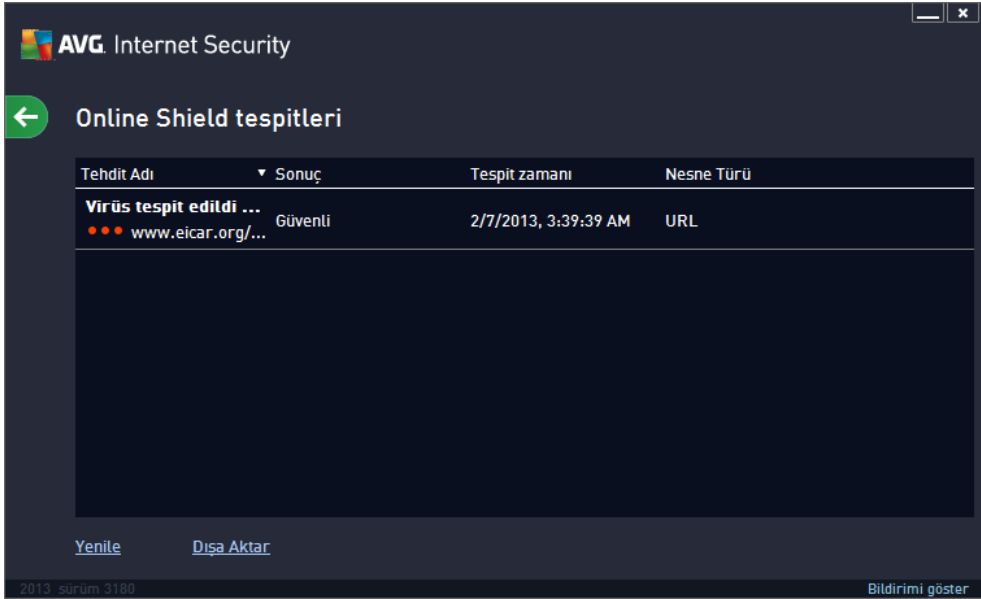
**Online Shield** ziyaret ettiğiniz web sitelerinin içeriklerini ve sitelerin içindeki muhtemel dosyaları, ilgili web sitesi henüz tarayıcınızda görünmeden ya da bilgisayarınıza indirmeden tarar. Bir tehdit tespit edilirse aşağıdaki iletişim kutusu vasıtasıyla hemen uyarılırsınız:



Bu uyarı iletişim kutusunda tespit edilen ve virüs bulasmis olarak atanan nesne hakkında daha fazla bilgi (*Aç*) ve ilgili bulasma hakkında bazı açıklamalar (*Açıklama*) bulabilirsiniz. [Ayrıntıları göster](#) bağlantısı, sizi tespit edilen bulasma hakkında ayrıntılı bilgi bulabileceğiniz (biliniyorsa) çevrimiçi virüs ansiklopedisine yönlendirir. İletişim kutusundan aşağıdaki kontrol öğeleri bulunur:

- **Ayrıntıları göster** - bulasma tespit edildiğinde çalışan işlem ve işlemin tanımı ile ilgili bilgileri bulabileceğiniz yeni bir açılır pencere açmak için bu bağlantıyı tıklatin.
- **Kapat** - uyarı iletişim kutusunu kapatmak için bu düğmeyi tıklatin.

Süphemli web sayfası açılmaz ve tehlike tespiti **Online Shield tespitleri** listesinde kaydedilir. Bu tespit edilen tehditler genel görünümüne **AVG Internet Security 2013** ana penceresinin üst bölümünde yer alan **Seçenekler / Geçmiş / Online Shield** tespiti menü öğesi yoluyla erişilebilir.




The screenshot shows the AVG Internet Security interface. The title bar reads "AVG Internet Security". The main window is titled "Online Shield tespitleri" (Online Shield detections). Below the title, there is a table with the following columns: "Tehdit Adı" (Threat Name), "Sonuç" (Result), "Tespit zamanı" (Detection Time), and "Nesne Türü" (Object Type). The table contains one entry: "Virüs tespit edildi ..." (Virus detected ...) with a result of "Güvenli" (Safe), a detection time of "2/7/2013, 3:39:39 AM", and an object type of "URL". The URL is "www.eicar.org/...". At the bottom of the window, there are buttons for "Yenile" (Refresh) and "Dışa Aktar" (Export). The status bar at the bottom left shows "2013 sürüm 3180" and the bottom right shows "Bildirimi göster" (Show report).

Tehdit Adı	Sonuç	Tespit zamanı	Nesne Türü
Virüs tespit edildi ... www.eicar.org/...	Güvenli	2/7/2013, 3:39:39 AM	URL

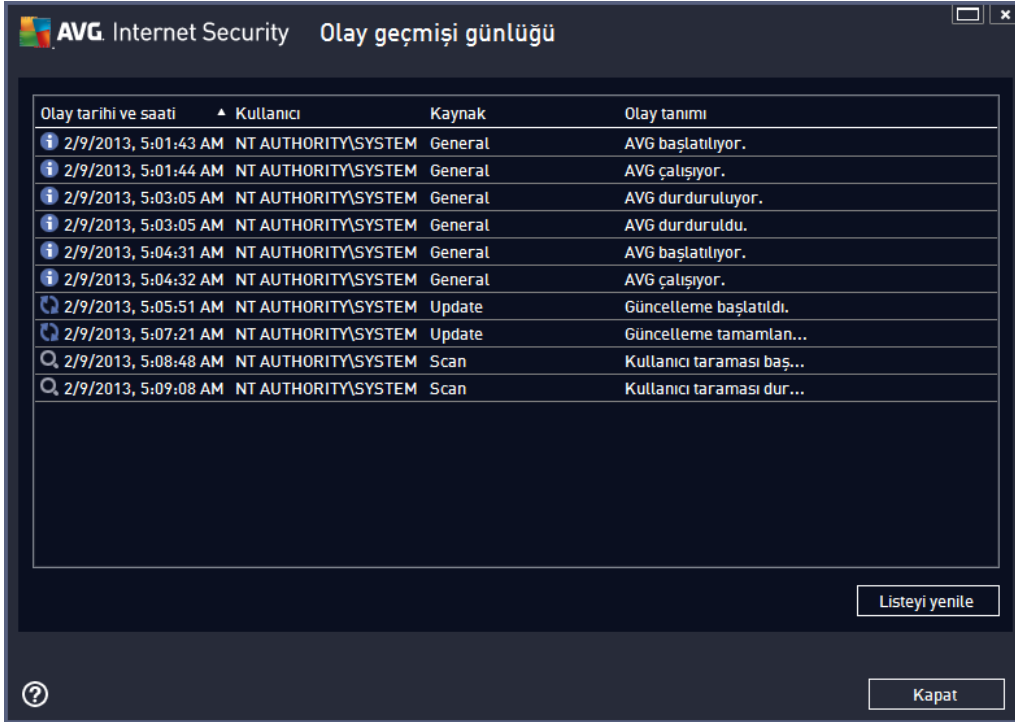
Tespit edilen tüm nesnelere için aşağıdaki bilgiler verilir:

- **Tespit adı** - tespit edilen nesnenin açıklaması (*muhtemelen adı da*) ve kaynağı (*web sayfası*)
- **Sonuç** - tespit edilen nesne ile gerçekleştirilen işlem
- **Algılama zamanı** - Tehlikenin algılandığı ve engellendiği tarih ve saat
- **Nesne Türü** - tespit edilen nesnenin türü
- **İşlem** - tespit edilmesi amacıyla potansiyel tehlike taşıyan nesneyi uyararak işlem nedir

### Kontrol düğmeleri

- **Yenile - Online Shield**
- **Disa aktar** - tespit edilen tüm nesnelere bir dosyada dışa aktarın
-  - varsayılan [AVG ana iletişim kutusuna](#) (*bilesen genel görünümü*) geri dönmek için bu iletişim kutusunun sol üst kısmındaki oku kullanın

### 13.5. Olay gemiři gnlg



The screenshot shows the AVG Internet Security 'Olay gemiři gnlg' (Event History) window. It displays a table of events with columns for 'Olay tarihi ve saati' (Event date and time), 'Kullanıcı' (User), 'Kaynak' (Source), and 'Olay tanımı' (Event description). The events listed are:

Olay tarihi ve saati	Kullanıcı	Kaynak	Olay tanımı
2/9/2013, 5:01:43 AM	NT AUTHORITY\SYSTEM	General	AVG bařlatılıyor.
2/9/2013, 5:01:44 AM	NT AUTHORITY\SYSTEM	General	AVG alıřıyor.
2/9/2013, 5:03:05 AM	NT AUTHORITY\SYSTEM	General	AVG durduruluyor.
2/9/2013, 5:03:05 AM	NT AUTHORITY\SYSTEM	General	AVG durduruldu.
2/9/2013, 5:04:31 AM	NT AUTHORITY\SYSTEM	General	AVG bařlatılıyor.
2/9/2013, 5:04:32 AM	NT AUTHORITY\SYSTEM	General	AVG alıřıyor.
2/9/2013, 5:05:51 AM	NT AUTHORITY\SYSTEM	Update	Gncelleme bařlatıldı.
2/9/2013, 5:07:21 AM	NT AUTHORITY\SYSTEM	Update	Gncelleme tamamlan...
2/9/2013, 5:08:48 AM	NT AUTHORITY\SYSTEM	Scan	Kullanıcı taraması bař...
2/9/2013, 5:09:08 AM	NT AUTHORITY\SYSTEM	Scan	Kullanıcı taraması dur...

At the bottom of the window, there are two buttons: 'Listeyi yenile' (Refresh list) and 'Kapat' (Close).

**Olay gemiři gnlg** iletisim kutusuna **AVG Internet Security 2013** ana penceresinin st satirindeki gezinme blmnden **Seenekler / Gemiř / Olay gemiři gnlg** men gesi yoluyla erisilebilir. Bu iletisim kutusunda, **AVG Internet Security 2013** uygulamasinin alıřmasi sirasinda olusan nemli olaylarin bir zetini bulabilirsiniz. Bu iletisim kutusunun kayitlarini sagladığı olay trleri: AVG uygulaması gncellemeleri hakkında bilgiler; tarama baslangici, sonu veya durdurulmasi hakkında bilgiler(*otomatik olarak gereklestirilen testler de dahil*); virs tespitiyle baglantili olaylar hakkında gereklestigi konumu da ieren bilgiler (*yerlesik kalkan veya [tarama](#) kaynakli*) ve diger nemli olaylar.

Her olay iin su bilgiler listelenir:

- **Olay tarihi ve saati** olayin gereklestigi kesin tarihi ve zamani belirtir.
- **Kullanıcı** olayin gereklestigi sirada oturum amis olan kullanicinin adini gsterir.
- **Kaynak**, kaynak bileşeni veya AVG sisteminin olayi tetikleyen blm hakkında bilgi verir.
- **Olay tanimi**, tam olarak ne oldugu hakkında kısa bir aıklama saglar.

#### Kontrol dgmeleri

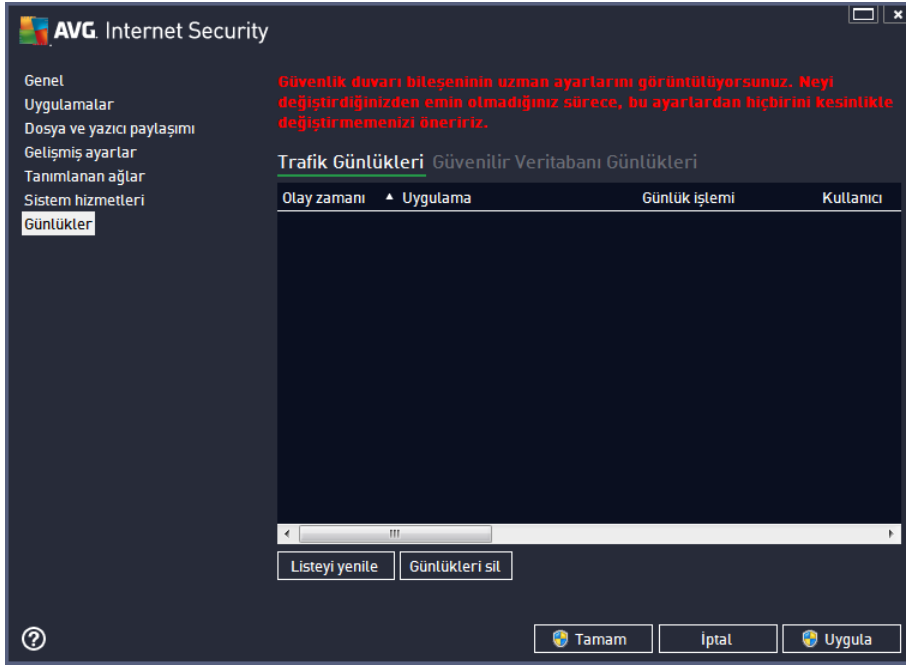
- **Listeyi yenile** - olaylar listesindeki tm girisleri gncellemek iin bu dgmeye basin
- **Kapat** - **AVG Internet Security 2013** ana penceresine dnmek iin bu dgmeyi tiklatin

## 13.6. Firewall günlüğü

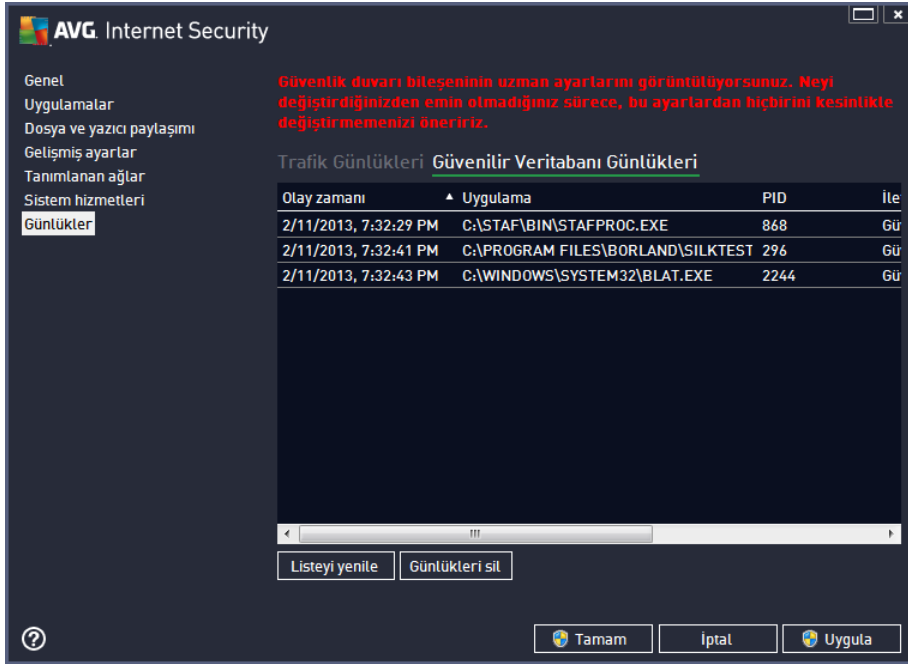
**Bu iletişim kutusu uzman düzeyinde yapılandırma için tasarlanmıştır ve yapacağınız değişiklikten kesinlikle emin değilseniz hiçbir ayarı değiştirmemenizi tavsiye ederiz!**

**Günlükler** iletişim kutusu, kaydedilen tüm Firewall eylemlerini ve etkinliklerini ilgili parametrelerin ayrıntılı tanımları ile birlikte iki sekmede görüntüleyebilmenizi sağlar.

- **Trafik Günlükleri** - Bu sekme ağa bağlanmaya çalışan tüm uygulamaların etkinlikleri hakkındaki bilgileri sunar. Her öge için olay zamanı, uygulama adı, ilgili günlük işlemi, kullanıcı adı, PID, trafik yönü, protokol türü, uzak ve yerel bağlantı noktalarının numaralarıyla yerel ve uzak IP adresleri hakkındaki bilgileri bulabilirsiniz.



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



AVG Internet Security

Genel  
Uygulamalar  
Dosya ve yazıcı paylaşımı  
Gelişmiş ayarlar  
Tanımlanan ağlar  
Sistem hizmetleri  
**Günlükler**

Güvenlik duvarı bileşeninin uzman ayarlarını görüntüyorsunuz. Neyi değiştirdiğinizden emin olmadığımız sürece, bu ayarlardan hiçbirini kesinlikle değiştirmenizi öneririz.

Trafik Günlükleri **Güvenilir Veritabanı Günlükleri**

Olay zamanı	Uygulama	PID	İle
2/11/2013, 7:32:29 PM	C:\STAF\BIN\STAFPROC.EXE	868	Gü
2/11/2013, 7:32:41 PM	C:\PROGRAM FILES\BORLAND\SILKTEST	296	Gü
2/11/2013, 7:32:43 PM	C:\WINDOWS\SYSTEM32\BLAT.EXE	2244	Gü

Listeyi yenile Günlükleri sil

Tamam İptal Uygula

### Kontrol düğmeleri

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



## 14. AVG Güncellemeleri

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

Yeni ortaya çıkan tehditler ve bunların yayılma hızı dikkate alındığında **AVG Internet Security 2013** ürününüzü düzenli olarak güncellemek hayati bir öneme sahiptir. En iyi çözüm, otomatik güncellenen yapılandırıldığı program varsayılan ayarlarına güvenmektir. **AVG Internet Security 2013** ürününüzün virüs veritabanı güncel değilse, programın en yeni tehditleri tespit edemeyeceğini lütfen unutmayın!

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

### 14.1. Güncelleme başlatma

Mümkün olan en yüksek güvenliği sağlamak için, **AVG Internet Security 2013** varsayılan olarak her dört saatte bir yeni virüs veritabanı güncellemeleri kontrol etmeye ayarlanmıştır. AVG güncellemeleri belirli bir takvime göre değil yeni tehditlerin miktarı ve ciddiyetine göre yayınlandığından, bu kontrol AVG virüs veritabanınızın sürekli güncel tutulması açısından çok önemlidir.

Yeni güncelleme dosyalarını hemen kontrol etmek istiyorsanız, ana kullanıcı arayüzündeki [Şimdi güncelle](#) hızlı bağlantısını kullanın. Bu bağlantıya her zaman herhangi bir [kullanıcı arayüzü](#) iletişim kutusundan ulaşabilirsiniz. Güncellemeyi başlatmanızın ardından AVG, yeni güncelleme dosyaları olup olmadığını doğrular. Varsa, **AVG Internet Security 2013** güncellemeleri indirmeye başlar ve güncelleme işlemini kendisi başlatır. Güncelleme sonuçları hakkında AVG sistem tepsisi simgesi üzerinde beliren iletişim kutusuyla bilgilendirilirsiniz.

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

- [Tanim güncelleme programi](#)
- [Program güncelleme programi](#)
- [Anti-Spam güncelleme programi](#)

### 14.2. Güncelleme seviyeleri

**AVG Internet Security 2013** seçilebilecek iki güncelleme düzeyi sunar:

- **Tanim güncellemeleri** güvenilir virüslerden koruma, istenmeyen posta önleme ve kötü amaçlı yazılımlara karşı koruma için gerekli değişiklikleri içerir. Genellikle kodu değiştirmez ve yalnızca tanımlama veritabanını günceller. Bu güncelleme sunulur sunulmaz yüklenmelidir.



- **Program gncellemesi** esitli program deęisikliklerini, onarımları ve iyilestirmeleri ierir.

Bir [gncelleme programlarken](#), her iki gncelleme dzeyi iin de belirli parametreler tanımlamak mmkndr:

- [Tanım gncelleme programı](#)
- [Program gncelleme programı](#)

**Not:** Zamanlanmış bir program gncellemesinin zaman akışması olursa ve zamanlanmış tarama gerekleşirse, gncelleme işlemi yksek nceliklidir ve tarama kesilir.

## 15. SSS ve Teknik Destek

AVG Internet Security 2013 uygulamanızın satışıyla ilgili veya teknik sorunlarınız olması durumunda yardım için birçok yol mevcuttur. Lütfen aşağıdaki seçeneklerden birini seçin:

- **Destek Alın:** Doğrudan AVG uygulaması içinden AVG web sitesindeki (<http://www.avg.com/>) özel bir müşteri destek sayfasına erişebilirsiniz. AVG web sitesindeki destek seçeneklerine erişmek için **Yardım / Destek Alın** ana menü öğesini seçin. Devam etmek için lütfen web sayfasındaki talimatları izleyin.
- **Destek (ana menü bağlantısı):** AVG uygulama menüsünde (ana kullanıcı arayüzünün en üstünde) yardım bulmaya çalışırken ihtiyacınız olabilecek tüm bilgileri içeren yeni bir iletişim kutusu açan **Destek** bağlantısı bulunur. İletişim kutusunda kurulu AVG programınız ( *program / veritabanı sürümü*) ile ilgili temel bilgiler, lisans ayrıntıları ve hızlı destek bağlantıları listesi bulunur:



- **Yardım dosyasında sorun giderme:** Doğrudan **AVG Internet Security 2013** içindeki yardım dosyasından erişilebilen yeni bir **Sorun giderme** bölümü mevcuttur (*yardım dosyasını açmak için uygulamadaki herhangi bir pencerede F1 tusuna basın*). Bu bölüm, kullanıcı teknik bir sorun hakkında profesyonel yardım aradığında en sık karşılaşılan durumlar hakkında bir liste sunar. Lütfen sizin sorununuzu en iyi açıklayan durumu seçin ve sorunun çözümüne dair ayrıntılı talimatlar almak için tıklattın.
- **AVG web sitesi Destek Merkezi:** Sorunuzun çözümünü AVG web sitesinde de (<http://www.avg.com/>) arayabilirsiniz. **Destek Merkezi** bölümünde hem satış sorunları hem de teknik sorunlarla ilgili tematik olarak gruplandırılmış konular bulabilirsiniz.
- **Sık sorulan sorular:** AVG web sitesinde (<http://www.avg.com/>) ayrı ve çok ayrıntılı bir sık sorulan sorular bölümü de bulabilirsiniz. Bu bölüme **Destek Merkezi / SSS** menü seçeneğinden erişilebilir. Burada da tüm sorular satış, teknik ve virüs kategorileri şeklinde sınıflandırılmıştır.
- **Virüsler ve tehlikeler hakkında:** Virüs sorunlarına ayrılmış özel bir AVG web sitesi (<http://www.avg.com/>)



www.avg.com/) bölümü (*web sayfasına ana menüdeki Yardım / Virüsler ve Tehlikeler Hakkında seçeneginden erişilebilir*). Çevrimiçi tehlikeler hakkında sınıflandırılmış bilgiler sunan bir sayfaya girmek için menüde **Destek Merkezi / Virüsler ve tehlikeler hakkında** ögesini tıklatin. Virüs, casus yazılım silme talimatları ve nasıl güvenli kalacağınıza dair öneriler de bulabilirsiniz.

- **Tartışma forumu:** Ayrıca <http://forums.avg.com> adresindeki AVG kullanıcıları tartışma forumunu kullanabilirsiniz.