



AVG AntiVirus 2014

Kullanıcı Kılavuzu

Belge revizyonu 2014.21 (6/11/2014)

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

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

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

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

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

İçindekiler

| | |
|--|-----------|
| 1. Giriş | 5 |
| 2. AVG Yükleme Gereksinimleri | 6 |
| 2.1 Desteklenen İşletim Sistemleri | 6 |
| 2.2 Minimum ve Önerilen Donanım Gereksinimleri | 6 |
| 3. AVG Yükleme Süreci | 7 |
| 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 | 12 |
| 3.6 Yükleme ilerlemesi | 13 |
| 3.7 Tebrikler! | 14 |
| 4. Yüklemeden Sonra | 15 |
| 4.1 Ürün kaydı | 15 |
| 4.2 Kullanıcı arayüzüne erişim | 15 |
| 4.3 Tüm bilgisayarın taraması | 15 |
| 4.4 Eicar testi | 15 |
| 4.5 AVG varsayılan yapılandırması | 16 |
| 5. AVG Kullanıcı Arayüzü | 17 |
| 5.1 Üst Satır Gezinme | 18 |
| 5.2 Güvenlik Durumu Bilgisi | 21 |
| 5.3 Bileşen Genel Görünümü | 22 |
| 5.4 Uygulamalarım | 23 |
| 5.5 Tara / Hızlı Bağlantıları Güncelle | 24 |
| 5.6 Sistem Tepsisi Simgesi | 24 |
| 5.7 AVG Tavsiyesi | 26 |
| 5.8 AVG Hızlandırıcı | 27 |
| 6. AVG Bileşenleri | 28 |
| 6.1 Bilgisayar Koruması | 28 |
| 6.2 Web Tarama Koruması | 33 |
| 6.3 Identity Protection | 34 |
| 6.4 E-posta Koruması | 36 |
| 6.5 Quick Tune bileşeni | 38 |

| | |
|---|------------|
| 7. AVG Security Toolbar | 40 |
| 8. AVG Do Not Track | 43 |
| 8.1 AVG Do Not Track arayüzü | 43 |
| 8.2 İzleme süreçleri hakkında bilgiler | 45 |
| 8.3 İzleyici süreçlerini engelleme | 45 |
| 8.4 AVG Do Not Track ayarları | 46 |
| 9. AVG Gelişmiş Ayarlar | 47 |
| 9.1 Görünüm | 47 |
| 9.2 Sesler | 49 |
| 9.3 AVG korumasını geçici olarak devre dışı bırak | 50 |
| 9.4 Bilgisayar Koruması | 51 |
| 9.5 E-Posta Tarayıcısı | 56 |
| 9.6 Web Tarama Koruması | 66 |
| 9.7 Identity Protection | 69 |
| 9.8 Taramalar | 70 |
| 9.9 Programlar | 76 |
| 9.10 Güncelleme | 84 |
| 9.11 İstisnalar | 88 |
| 9.12 Virüs Kasası | 90 |
| 9.13 AVG Kendi Kendini Koruma | 91 |
| 9.14 Gizlilik Tercihleri | 91 |
| 9.15 Hata Durumunu Yoksay | 94 |
| 9.16 Advisor - Bilinen Ağlar | 95 |
| 10. AVG Tarama | 96 |
| 10.1 Öntanımlı Taramalar | 98 |
| 10.2 Windows Gezgini'nde Tarama | 107 |
| 10.3 Komut Satırı Tarama | 107 |
| 10.4 Tarama Programlama | 110 |
| 10.5 Tarama Sonuçları | 118 |
| 10.6 Tarama sonuçları ayrıntıları | 119 |
| 11. AVG File Shredder | 120 |
| 12. Virüs Kasası | 121 |
| 13. Geçmiş | 123 |
| 13.1 Tarama sonuçları | 123 |



| | |
|---|------------|
| 13.2 Yerleşik Kalkan Sonuçları..... | 124 |
| 13.3 Identity Protection Sonuçları..... | 127 |
| 13.4 E-posta Koruması Sonuçları..... | 128 |
| 13.5 Online Shield Sonuçları..... | 129 |
| 13.6 Olay Geçmişi..... | 131 |
| 14. AVG Güncellemeleri..... | 132 |
| 14.1 Güncelleme başlatma..... | 132 |
| 14.2 Güncelleme seviyeleri..... | 132 |
| 15. SSS ve Teknik Destek..... | 134 |

1. Giriş

Bu kullanıcı el kitabı, **AVG AntiVirus** için kapsamlı kullanıcı dokümantasyon sağlar.

AVG AntiVirus günümüzün en gelişmiş tehditlerine karşı gerçek zamanlı koruma sağlar. Gerçek zamanlı koruma sayesinde güvenle sohbet edip dosya indirebilir veya paylaşabilirsiniz; kesilme sıkıntısı yaşamadan oyun oynayıp video izleyebilirsiniz; emniyetli şekilde dosya indirip paylaşabilir ve mesaj gönderebilirsiniz; sosyal paylaşım ağlarını rahatça kullanabilir ve internette güvenli biçimde gezinip arama yapabilirsiniz.

Diğer bilgi kaynaklarını da kullanmak isteyebilirsiniz:

- **Yardım dosyası:** Doğrudan **AVG AntiVirus** içindeki yardım dosyasından erişilebilen bir *Sorun giderme* bölümü mevcuttur (yardım dosyasını açmak için uygulamadaki herhangi bir iletişim kutusunda F1 tuşuna 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 tıklayın.
- **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'ler ve Eğitimler** menü seçeneğinden erişilebilir. Burada da tüm sorular satış, teknik ve virüs kategorileri olarak organize bir şekilde sınıflandırılmıştır.
- **AVG ThreatLabs:** AVG ile ilişkili özel bir web sitesi (<http://www.avgthreatlabs.com/website-safety-reports/>) olarak virüs sorunları bağlamında çevrimiçi tehditler hakkında genel bilgiler vermek üzere hazırlanmıştır. 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.



2. AVG Yükleme Gereksinimleri

2.1. Desteklenen İşletim Sistemleri

AVG AntiVirus 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 AntiVirus yazılımını yalnızca IDP bileşeni olmaksızın yükleyebilirsiniz.

2.2. Minimum ve Önerilen Donanım Gereksinimleri

AVG AntiVirus 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 AntiVirus 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

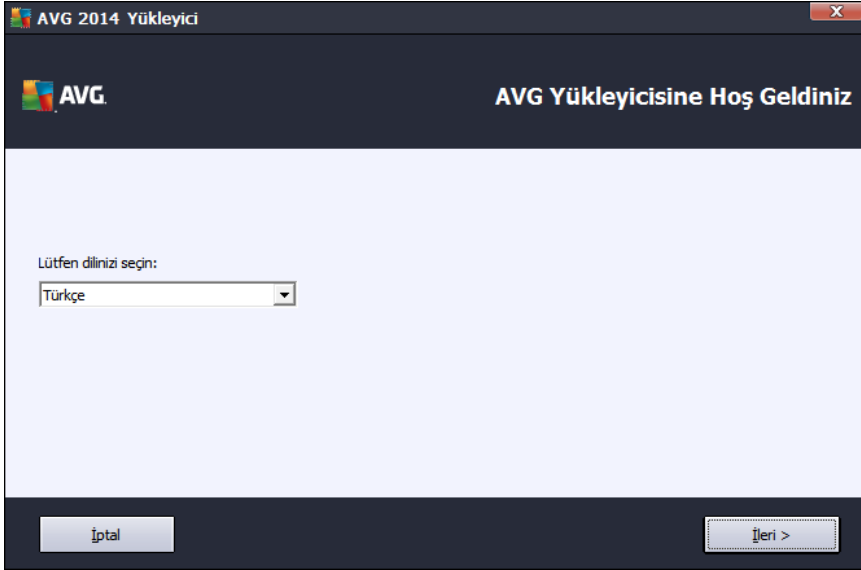
Bilgisayarınıza **AVG AntiVirus** programını yüklemek için, en güncel yükleme dosyasını edinmeniz gerekir. **AVG AntiVirus** uygulamasının doğru sürümünü yüklediğinizden emin olabilmek için yükleme dosyasını AVG web sitesinden (<http://www.avg.com/>) indirmeniz önerilir. **Destek Merkezi / İndirmeler**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

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

Yükleme dosyasını sabit diskinize indirme ve kaydetme işlemini tamamladıktan sonra yükleme işlemini başlatabilirsiniz. Yükleme, bir dizi kolay ve anlaşılır iletişim kutusundan oluşur. Her iletişim kutusunda yükleme sürecinin her adımında ne yapılması gerektiği kısaca açıklanır. Her iletişim kutusunun ayrıntılı bir açıklaması aşağıda sunulmuştur:

3.1. Hoş geldiniz: Dil Seçimi

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

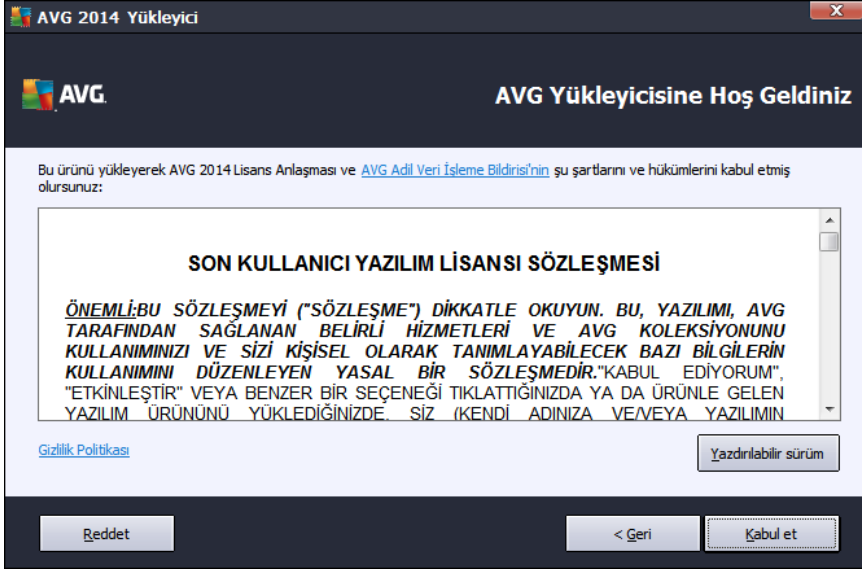


Bu iletişim kutusunda yükleme süreci için kullanılan dili seçebilirsiniz. Dil menüsünü açmak için açılır kutuyu tıklayın. İstedığınız dili seçtiğinizde yükleme süreci bu dille devam eder.

Dikkat: *Su anda yalnızca yükleme süreci dilini seçmektesiniz. AVG AntiVirus uygulaması seçilen dilde yüklenir ve İngilizce her zaman otomatik olarak yüklenir. Ancak, daha fazla dil yüklemek ve AVG AntiVirus 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, anladığınızı ve sözleşmeyi kabul ettiğinizi onaylamak için, **Kabul Et** düğmesine basın. Lisans sözleşmesini kabul etmiyorsanız **Kabul Etmiyorum** düğmesine basın, böylece yükleme süreci anında iptal edilecektir.

AVG Adil İşleme Bildirimi Gizlilik Politikası

Bu kurulum iletişim kutusu, lisans sözleşmesinin yanı sıra **AVG Adil İşleme Bildirimi** ve **Gizlilik Politikası** hakkında da daha fazla bilgi seçeneği sunar. Bahsedilen işlemler iletişim kutusunda bir aktif bağlantı şeklinde gösterilir. Bu bağlantı sizi ayrıntılı bilgi bulabileceğiniz ilgili web sitesine götürür. Bu bildirimlerin tam metninin bulabileceğiniz AVG web sitesine gitmek için (<http://www.avg.com/>) ilgili bağlantıyı tıklattın.

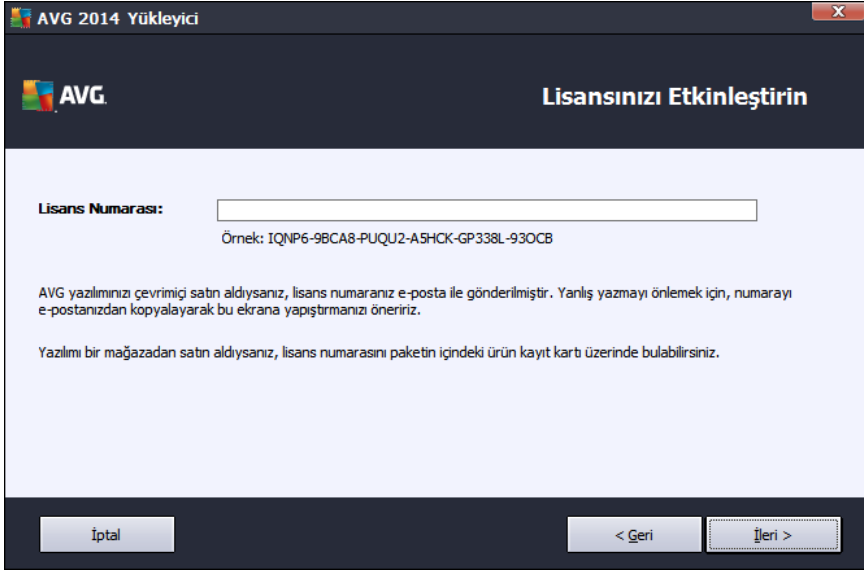
Kontrol düğmeleri

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 tıklattın.
- **Reddet** - Lisans sözleşmesini reddetmek için tıklattın. Kurulum süreci derhal sonlandırılır. **AVG AntiVirus** yüklenmez!
- **Geri** - Önceki kurulum iletişim kutusuna, bir adım geriye gitmek için tıklattın.
- **Kabul Et** - Lisans sözleşmesini okudugunuzu, anladığınızı ve kabul ettiğinizi onaylamak için tıklattın. 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 AntiVirus** kutusundaki CD paketinde bulunabilir. Lisans numarası **AVG AntiVirus** 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 AntiVirus** 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** tusunu basılı tutun ve **C** tusuna basın. Bu işlem numarayı kopyalar.
- Kopyalanan numarayı yapıştırmak istediğiniz konumu tıklattığınız.
- **Ctrl** tusunu basılı tutun ve **V** tusuna basın. Bu işlem numarayı seçilen konuma yapıştırır.



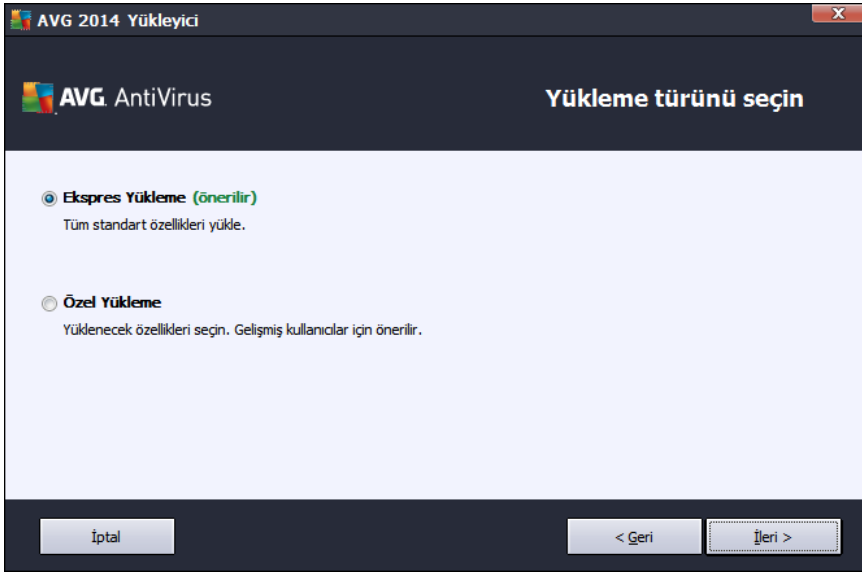
Kontrol düğmeleri

Çogu kurulum iletişim kutusunda olduğu gibi üç kontrol düğmesi mevcuttur:

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

3.4. Yükleme türünü seçin

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



Ekspres yükleme

Çogu kullanıcı için kesinlikle standart **Ekspres** yüklemenin muhafaza edilmesi önerilir. Bu yolla **AVG AntiVirus** programını [AVG Security Toolbar](#) da dahil olmak üzere program tedarikçisi tarafından önceden tanımlanmış ayarlarla tam otomatik moda yüklersiniz. Bu yapılandırma, minimum kaynak kullanımı ile maksimum güvenliği bir araya getirir. Gelecekte söz konusu yapılandırmayı değiştirme ihtiyacı duyarsanız söz konusu işlemi doğrudan **AVG AntiVirus** uygulamasından yapabileceksiniz.

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

Özel yükleme

Özel Yükleme **AVG AntiVirus** uygulamasını standart olmayan ayarlarla kurmak için geçerli bir



nedeni olan deneyimli kullanıcılar tarafından kullanılmalıdır. Örn. belirli sistem gereksinimlerini karşılamak için. Bu seçeneğe karar verirken iletişim kutusunda birkaç yeni seçenek etkinleştirilir:

- **İnternet korumanızı geliştirmek için AVG Toolbar'i yükleyin** - Varsayılan ayarları değiştirmeyeniz, internette gezinirken size daha kapsamlı çevrimiçi koruma sağlamak için bu bileşen otomatik olarak varsayılan 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*). Diğer tarayıcılar desteklenmez; Avant Browser gibi alternatif internet tarayıcıları kullanıyorsanız beklenmeyen davranışlarla karşılaşabilirsiniz.
- **AVG Secure Search'ü varsayılan ana sayfanız ve yeni sekme sayfanız olarak ayarlayın ve koruyun** - Varsayılan internet tarayıcınızı ve tarayıcının tüm sekmelerini ana sayfanız AVG Secure Search olarak ayarlanmı ekilde açmayı onaylamak için işaretli olarak bırakın.
- **AVG Secure Search'ü varsayılan arama sağlayıcınız olarak ayarlayın ve koruyun** - 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.
- **Hedef klasör** - Burada, **AVG AntiVirus** uygulamasının yükleneceği konumu belirtmeniz beklenmektedir. **AVG AntiVirus**, varsayılan olarak 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 tedarikçisi tarafından önceden ayarlanmış varsayılan hedefi geri getirmek için **Varsayılan** düğmesini kullanın.

Ardından, **Özel Seçenekler** iletişim kutusuna gitmek için [İleri](#) düğmesine basın.

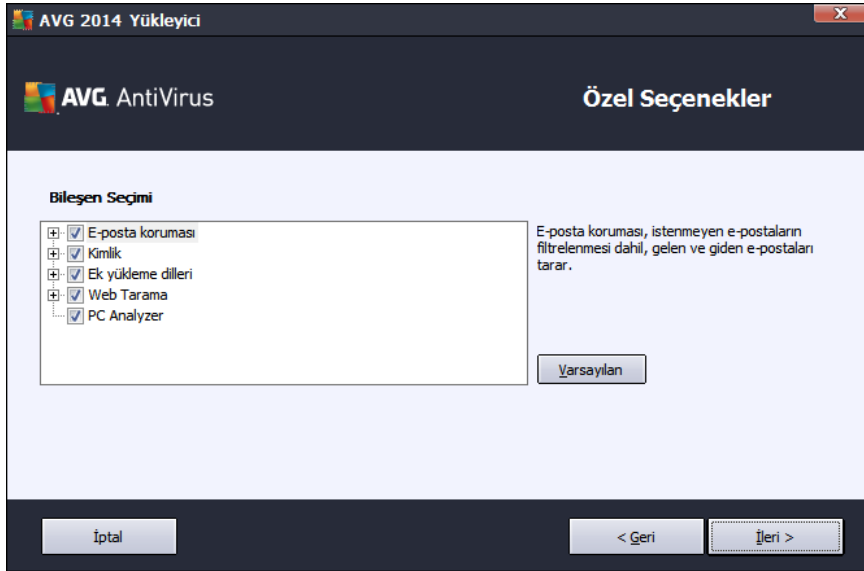
Kontrol düğmeleri

Çogu kurulum iletişim kutusunda olduğu gibi üç kontrol düğmesi mevcuttur:

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

3.5. Özel seçenekler

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



Bileşen Seçimi bölümünde, yüklenebilecek tüm **AVG AntiVirus** 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.

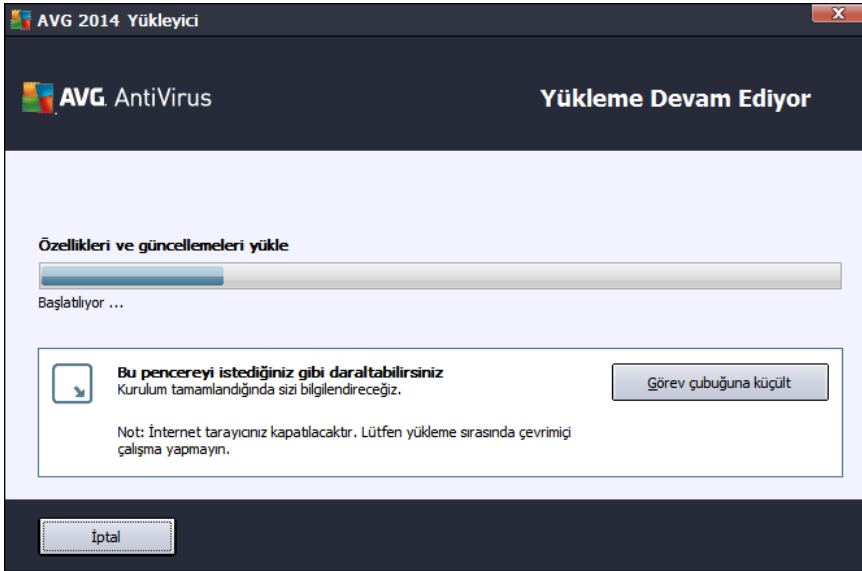
Kontrol düğmeleri

Çoğu kurulum iletişim kutusunda olduğu gibi üç kontrol düğmesi mevcuttur:

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

3.6. Yükleme ilerlemesi

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



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

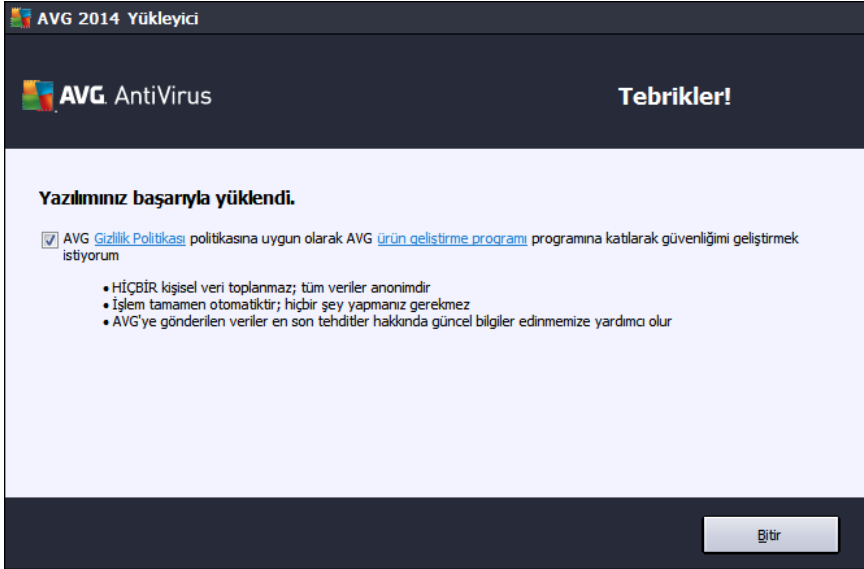
Kontrol düğmeleri

Bu iletişim kutusunda iki adet kontrol düğmesi bulunmaktadır:

- **Minimize et** - Yükleme işlemi birkaç dakika alabilir. Bu düğmeyi tıklatarak iletişim kutusunu 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 AntiVirus** uygulamasının yüklenmeyeceğini lütfen unutmayın!

3.7. Tebrikler!

Tebrikler iletilim kutusu, **AVG AntiVirus** 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 AntiVirus yüklemesini tamamladıktan sonra, lütfen ürününüzü çevrimiçi olarak AVG web sitesinde (<http://www.avg.com/>) kaydettirin. Kayıt işleminin ardından AVG kullanıcı hesabınıza erişebilecek, AVG Güncelleme bültenini alacak ve sadece kayıtlı kullanıcılara sunulan diğer hizmetlerden yararlanacaksınız. Ürünü kaydettirmenin en kolay yolu doğrudan **AVG AntiVirus** kullanıcı arayüzünü kullanmaktır. Lütfen [üstteki gezinme bölümünden / Seçenekler / Simdi 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 2014**

4.3. Tüm bilgisayarın taraması

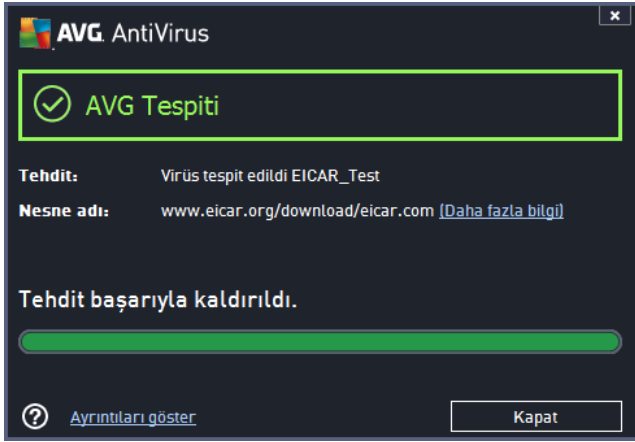
AVG AntiVirus yüklemesinden önce bilgisayarınıza virüs bulaşmış olması ihtimali bulunmaktadır. Bu nedenle bilgisayarınızda virüs bulunmadığından emin olmak için [Tüm bilgisayar taraması](#) yapmanız gerekmektedir. İlk tarama uzun bir süre alabilir (*bir saat civarında*), ancak bilgisayarınızın herhangi 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 AntiVirus 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 adresinde bulunan EICAR'ın web sitesinden indirebilir 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 AntiVirus** uygulamanız uyarıda bulunmazsınız buna yanıt verir. Bu bildirim, AVG'nin bilgisayarınıza doğru bir şekilde yüklenmiş olduğunu gösterir.



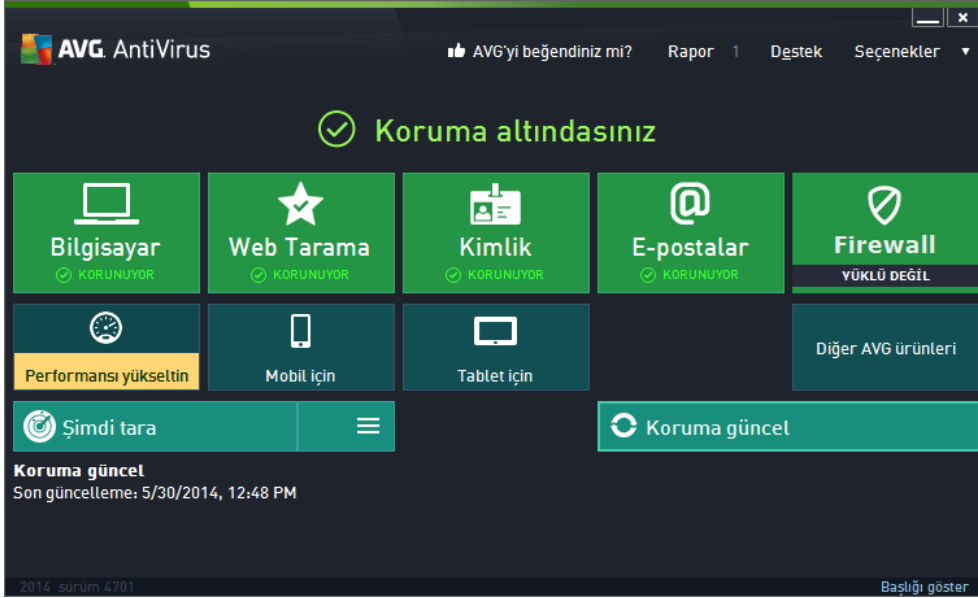
AVG'nin EICAR test dosyasını virüs olarak algılamaması halinde program yapılandırmasını yeniden kontrol etmeniz gerekir!

4.5. AVG varsayılan yapılandırması

AVG AntiVirus varsayılan yapılandırması (yani, uygulamanın yükledikten sonra doğru şekilde nasıl ayarlanacağı) yazılım satıcısı tarafından ayarlanabilir, böylece optimum performans elde etmek için tüm bileşenler ve işlevler ayarlanabilir. **Bunun için iyi bir nedeniniz olmadıkça AVG yapılandırmasını değiştirmeyin! Ayarlarda yapılacak her tür değişiklik sadece deneyimli bir kullanıcı tarafından gerçekleştirilmelidir.** 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 AntiVirus 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 AntiVirus 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 AntiVirus** 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 AntiVirus ana penceresi dışında, uygulamaya erişmek için kullanabileceğiniz bir kontrol öğesi daha vardır:

- **Sistem tepsisi simgesi** monitörün sağ alt köşesinde yer alır (*sistem tepsisinde*) ve **AVG AntiVirus** uygulamasının mevcut durumunu gösterir. [Ayrıntılar >>](#)

5.1. Üst Satır Gezinme

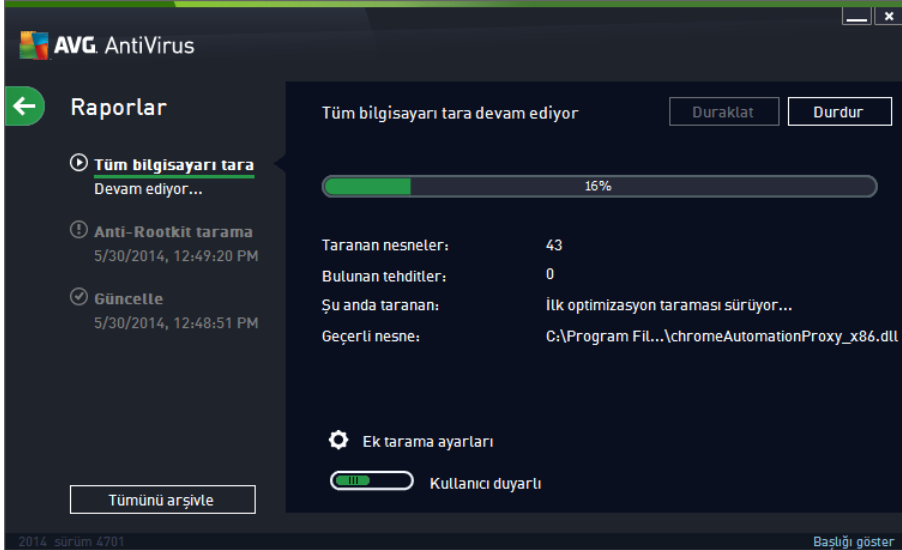
Üst satır gezinme ana menünün üst bölümünde yan yana dizilmiş birkaç etkin bağlantıdan oluşur. Gezinme bölümündeki düğmeler:

5.1.1. Facebook'ta bize katıl

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

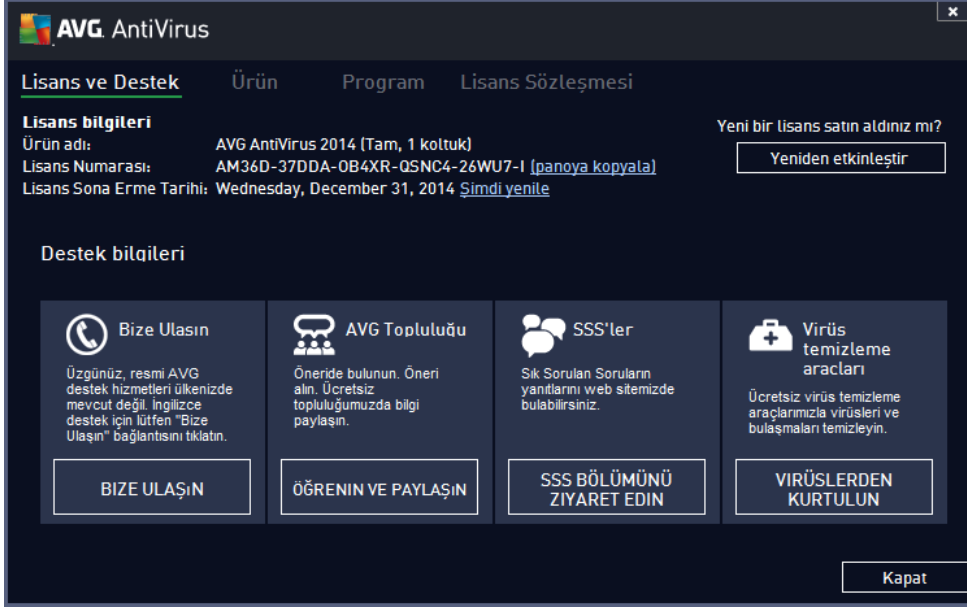
5.1.2. Raporlar

Önceden baslatılmış 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 tıklatin:



5.1.3. Destek

AVG AntiVirus uygulamasıyla ilgili tüm bilgileri bulabileceğiniz dört sekmeye ayrılmış yeni bir iletişim kutusu açar:



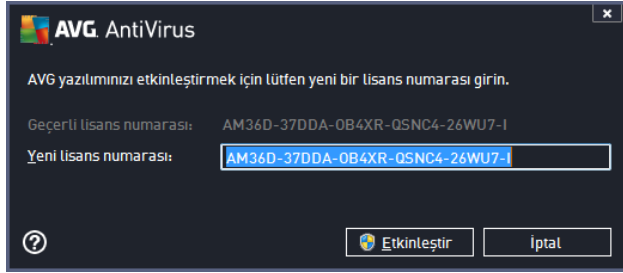
- **Lisans ve Destek** - Bu sekme ürün adı, lisans numarası ve son kullanma tarihi bilgilerini gösterir. İletişim kutusunun alt bölümünde müşteri destek birimine ulaşabileceğiniz tüm iletişim bilgilerini bulabilirsiniz. Sekmede bulunan etkin bağlantılar ve düğmeler:
 - *(Yeniden) Etkinleştir* - Yeni **AVG Yazılım Etkinleştirme** iletişim kutusunu açmak için tıklanın. Satis numaranızı (*AVG AntiVirus 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.
 - *Panoya kopyala* - Lisans numarasını kopyalayip uygun alana yapıştırmak için bu bağlantıyı kullanın. Bu sayede lisans numarasının doğru girildiğinden emin olabilirsiniz.
 - *Simdi yenile* - **AVG AntiVirus** Lisans yenilemenizi uygun bir zamanda, mevcut lisansınızın süresi sona ermeden en az bir ay önce satın almanızı 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 kampanyaları hakkında ayrıntılı bilgi alabilirsiniz.
- **Ürün** - Bu sekme **AVG AntiVirus** ürün bilgileri, yüklü bileşenler, yüklü e-posta koruması ve sistem bilgileri hakkında en önemli teknik verileri gösterir.
- **Program** - Bu sekmede program dosyası 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 AntiVirus ürününün bakım işlemine **Seçenekler** ögesinden erişilebilir. Açılır menüyü açmak için oku tıklatin:

- [Bilgisayari tara](#) tüm bilgisayar taramasi baslatir.
- [Seçilen klasörü tara...](#) - AVG tarama arayüzüne geçer ve bilgisayarınızın dolasımdan 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 tıklatin. İstedığınız dosyayı seçin ve tarama baslatmayı onaylayın.
- [Güncelle](#) - **AVG AntiVirus** güncellemesini otomatik olarak baslatir.
- [Dizinden güncelle...](#) - Sabit diskinizde bulunan belirli bir dosyanın içinde yer alan güncelleme dosyalarını alarak güncelleme işlemini gerçekleştirir. Öte yandan bu seçim sadece internet bağlantısının olmaması gibi (örneğin bilgisayarınıza virüs bulmuş ise ve internet bağlantınız kesildiyse; bilgisayarınız bir ağa bağlıysa fakat internet erişimi yok ise vb.) acil durumlarda önerilmektedir. Yeni açılan pencereden, daha önce güncelleme dosyasını depoladığınız klasörü seçin ve güncelleme işlemini baslatın.
- [Virüs Kasası](#) - Belirli bir neden doğrultusunda AVG'nin tespit edilmiş temizlenemeyen tüm buluşmaları tasıdığı karantina alanının arayüzü olan Virüs Kasası'ni açar. Karantina altında bulunan buluşmuş dosyalar, yalıtılmıştır, bilgisayarınızın güvenliği garanti altındadır ve aynı anda buluşmuş dosyalar ileride tamir edilebilecekleri göz önünde bulundurularak depolanır.
- [Geçmiş](#) - Bazı alt menü seçenekleri sunar:
 - [Tarama sonuçları](#) - Tarama sonuçları hakkında genel bilgilerin bulunduğu bir iletişim kutusu açar.
 - [Yerlesik Kalkan tespiti](#) - Yerlesik Kalkan tarafından tespit edilen tehditler hakkında genel bilgi veren bir iletişim kutusu açar.
 - [Identity Protection tespiti](#) - *Kimlik* bileşeni 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 AntiVirus** işlemleri hakkında genel bilgi veren bir geçmiş günlüğü arayüzü açar.
- [Gelişmiş ayarlar...](#) - **AVG AntiVirus** yapılandırmasını düzenleyebileceğiniz AVG gelişmiş ayarlar iletişim kutusunu açar. Genel olarak uygulamanın yazılım üreticisi tarafından tanımlanan varsayılan ayarlarınınin muhafaza edilmesi önerilir.
- [Yardım içerikleri](#) - AVG yardım dosyalarını açar.

- **Destek alın** - Müsteri destek merkezi sayfasında AVG web sitesini (<http://www.avg.com/>) açar.
- **AVG Web** - AVG web sitesini açar (<http://www.avg.com/>).
- **Virüsler ve Tehlikeler Hakkında** - Belirtilen virüs hakkında ayrıntılı bilgi edinebildiğiniz AVG web sitesindeki (<http://www.avg.com/>) çevrimiçi virüs ansiklopedisini açar.
- **(Yeniden) Etkinleştir** - Yükleme işlemi sırasında girdiğiniz lisans numarasının bulunduğu etkinleştirme iletişim kutusunu açar. Bu iletişim kutusunda satış numarasını (AVG'yi yüklerken kullandığınız numara) ya da eski lisans numarasını (örn. yeni bir AVG ürününe yükseltme yaparken) değiştirmek için lisans numaranızı düzenleyebilirsiniz. **AVG AntiVirus** deneme sürümünü kullanıyorsanız sonraki iki öğe, **Şimdi satın al** ve **Etkinleştir** olarak görünür ve programın tam sürümünü hemen satın almanızı sağlar. Bir satış numarasıyla yüklenmiş **AVG AntiVirus** için öğeler **Kaydet** ve **Etkinleştir** olarak görünür:



- **Şimdi kaydet / MyAccount** - AVG web sitesinin (<http://www.avg.com/>) kayıt sayfasına bağlantı sağlar. Lütfen kayıt bilgilerinizi doldurun; sadece AVG ürünlerini kaydettiren müşterilerimiz ücretsiz teknik destek alabilir.
- **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. (Aynı iletişim kutusu ana gezinme menüsündeki [Destek](#) bağlantısı yoluyla açılabilir.)

5.2. Güvenlik Durumu Bilgisi

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



- yeşil simge **AVG AntiVirus 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 AntiVirus** 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



erisilebilir. Burada bileşenin hata durumunun farkında olduğunuz, ancak belirli bir neden doğrultusunda **AVG AntiVirus** 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 AntiVirus** ürününüz bilgisayar yeniden başlatması gerektirdiğinde de görüntülenir (**Yeniden başlatma gerekiyor**). Lütfen bu uyarıyı dikkate alın ve bilgisayarınızı yeniden başlatın.



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

AVG AntiVirus 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 AntiVirus 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 AntiVirus durum bilgilerine istediğiniz zaman [sistem tepsisi 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 AntiVirus içinde, **Bileşen Genel Görünümü** kısmi aşağıdaki bileşenler hakkında bilgiler içerir:

- **Bilgisayar** - Bu bileşen iki hizmeti kapsar: **AntiVirus Shield** 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 dizinler için tarama yapar. [Ayrıntılar >>](#)

- **Web Tarama** - Internette arama ve gezinme sirasinda sizi web tabanli saldirilara karsi korur. [Ayrıntılar >>](#)
- **Identity** - Bilesen internette dijital varliklarinizi yeni ve bilinmeyen tehditlere karsi sürekli olarak koruyan **Identity Shield** hizmetini çalistirir. [Ayrıntılar >>](#)
- **E-postalar** - Gelen e-posta mesajlarinizi istenmeyen e-postalara karsi denetler ve virüsleri, kimlik avi saldirilarini veya diger tehditleri engeller. [Ayrıntılar >>](#)

Erisilebilir eylemler

- **Bilesen genel görünümü ekranında bileseni seçmek için fareyi ilgili bilesen simgesi üzerinde hareket ettirin.** Aynı anda [kullanıcı arayüzünün](#) kısmında bilesenin temel fonksiyonlari hakkında açıklamalar görüntülenir.
- **Bilesen simgesini tek tıklatarak** bilesenin mevcut durumu hakkında bilgiler içeren arayüzünü açın ve bilesenin yapılandırma ve istatistik verilerine erisin.

5.4. Uygulamalarım

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

- **Mobil koruma** cep telefonunuzu virüs ve zararlı yazılımlardan koruyan bir uygulamadır. Uygulama, ayrı kalmaniz durumunda akıllı telefonunuzu uzaktan izleme imkanı da saglar.
- **LiveKive** güvenli sunuculara çevrimiçi veri yedeklemesi yapmak için hazırlanmıştır. LiveKive tüm dosyalarınızı, fotoğraflarınızı ve müzik dosyalarınızı güvenli bir yerde yedekleyerek bunlari ailenizle ve arkadaşlarınızla paylaşmaniza ve iPhone ve Android cihazlari da dahil olmak üzere söz konusu dosyalara web etkinligi olan tüm cihazlardan erismenize olanak saglar.
- **Family Safety** çocuklarınızın uygunsuz web sitelerine, medya içeriklerine ve çevrimiçi aramalara karsi korunmasına yardımcı olur ve çevrimiçi faaliyetleriyle ilgili size rapor saglar. AVG Family Safety çocuklarınızın sohbet odalari ve sosyal paylaşım sitelerindeki etkinliklerini izlemek için tuz wurusu teknolojisi kullanır. Çocukların istismarında kullanildigi bilinen kelimeler, ifadeler ve cümleler algılarsa, SMS veya e-posta yoluyla sizi anında bilgilendirir. Uygulama araciligıyla çocuklarınızdan her biri için uygun koruma düzeyi ayarlayabilir ve benzersiz girişler araciligıyla onlari ayrı ayrı gözlemleyebilirsiniz.
- **PC Tuneup** uygulaması bilgisayarınızın hizinin ve genel performansının nasıl iyileştirilebilecegine yönelik ayrıntılı sistem analizi ve düzeltme islemi 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 dogrudan internet tarayicinizdan erisebilirsiniz; bu uygulama internette gezinirken size maksimum koruma saglar.

Uygulamalarim alanindaki uygulamalar hakkında ayrintili bilgi için ilgili blogu tiklatin. Bileseni hemen indirebileceginiz AVG web sayfasina yönlendirilirsiniz.

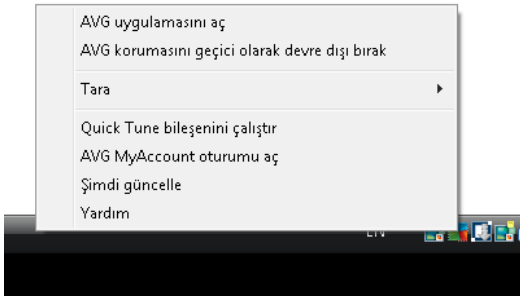
5.5. Tara / Hızlı Bağlantıları Güncelle

Hızlı bağlantılar AVG AntiVirus [kullanici arayüzünün](#) alt bölümündeki düğmelerde yer alır. Bu bağlantılar tarama ve güncelleme gibi en önemli ve en sık kullanılan uygulama özelliklerine anında erisebilmenizi saglar. Hızlı bağlantılara kullanici arayüzündeki tüm iletişim kutularından erisebilir:



- **Simdi tara** - Düğme grafik olarak iki kisma ayrılmıştır. **Simdi tara** bağlantısını izleyerek [Tüm Bilgisayari Tara](#) islemini hemen baslatabilir ve ilerleme ile sonuçlari otomatik olarak açılan [Raporlar](#) penceresinden izleyebilirsiniz. **Seçenekler** düğmesi **Tarama Seçenekleri** iletişim kutusunu açar; burada [zamanlanmış taramalari yönetebilir](#) ve [Tüm Bilgisayari Tara / Belirli Dosyalari veya Klasörleri Tara](#) parametrelerini düzenleyebilirsiniz. (Ayrıntilar için [AVG Tarama](#) bölümüne bakın)
- **Simdi güncelle** - Ürün güncellemesini hemen baslatmak için düğmeye basın. Güncelleme sonuçlari hakkında AVG sistem tepsi simgesi üzerinde beliren iletişim kutusuyla bilgilendirilirsiniz. (Ayrıntilar için [AVG Güncellemeleri](#) bölümüne bakın)

5.6. Sistem Tepsisi Simgesi



AVG Sistem Tepsisi Simgesi (Windows görev çubugunuzda, ekraninizin sol alt kösesinde) **AVG AntiVirus** uygulamanizin mevcut durumunu gösterir. **AVG AntiVirus** [kullanici arayüzü](#) ana penceresinin açık ya da kapali oldugu önemli olmaksizin devamlı olarak sistem tepsinizde bulunur:



AVG Sistem Tepsisi Simgesi görünümü

-  Tam renkli ve baska öge bulunmayan simge tüm **AVG AntiVirus** bileşenlerinin etkin ve tamamen çalışır durumda olduğunu gösterir. Ancak, simge bileşenlerden biri tam çalışır durumda olmasa da (kullanici [bilesen durumunu yoksaymaya](#) karar verdiginde) bu şekilde görünebilir. (Bilesenin durumunu yoksayma seçenegini onaylayarak, [bilesenin hata durumununun](#) farkında olduğunuzu, ancak kimi nedenlerle durumun böyle kalmasını ve durum hakkında uyarı almak istemediginizi 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 başlatılan bir güncelleme işlemi işaret eder.
-  Tam renkli ve ok işaretli simge ise **AVG AntiVirus** taramalarından birinin o anda çalışmakta olduğunu gösterir.

AVG Sistem Tepsisi Simgesi bilgileri

AVG Sistem Tepsisi Simgesi sizi sistem tepsisi simgesi üzerinden açılan bir pencere aracılığıyla **AVG AntiVirus** uygulamanızda o an gerçekleşen işlemler ve programdaki olası durum değişiklikleri hakkında da bilgilendirir (örn. *programlanan tarama ya da güncelleme otomatik olarak başlatılması, bir bileşenin durum değişikliği, hata durumu oluşumu, ...*).

AVG Sistem Tepsisi Simgesi yoluyla erişilebilen işlemler

AVG Sistem Tepsisi Simgesi, **AVG AntiVirus** [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:

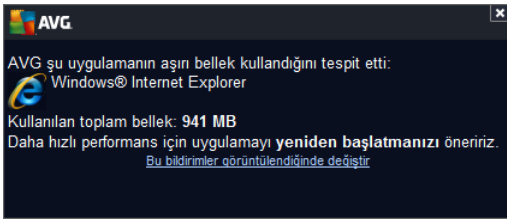
- **AVG'yi Aç - AVG AntiVirus** [kullanıcı arayüzünü](#) açmak için tıklanın.
- **AVG korumasını geçici olarak devre dışı bırak** - bu seçenek **AVG AntiVirus** tarafından sağlanan tüm korumayı tek seferde kapatmanızı sağlar. Mutlaka gerekli değilse, bu seçeneği kullanmamanız gerektiğini lütfen unutmayın! Çoğu durumda, yeni yazılımı veya sürücülerini yüklemeye önce ve hatta yükleyici veya yazılım sihirbazı yükleme işlemi sırasında istenmeyen kesintilerin olmamasını sağlamak için çalışan program ve uygulamaların kapatılmasını önerse bile **AVG AntiVirus** uygulamasını devre dışı bırakmak gerekmez. **AVG AntiVirus** uygulamasını geçici olarak devre dışı bırakmanız gerekirse, işinizi bitirdikten sonra yeniden etkinleştirmeniz gerekir. Virüslerden korunma yazılımınız devre dışı bırakılmıyken İnternete 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 tıklanın; tarama hemen başlatılacaktır.
- **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.*
- **Quick Tune bileşenini çalıştır** - [Quick Tune](#) bileşenini başlatmak için tıklanın.

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

5.7. 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 aşırı 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.
- **Tanıdık 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 verirsiniz, 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.

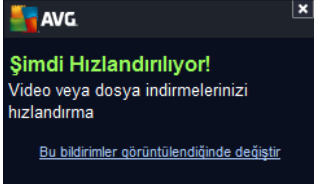
Desteklenen web tarayıcıları



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

5.8. AVG Hızlandırıcı

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

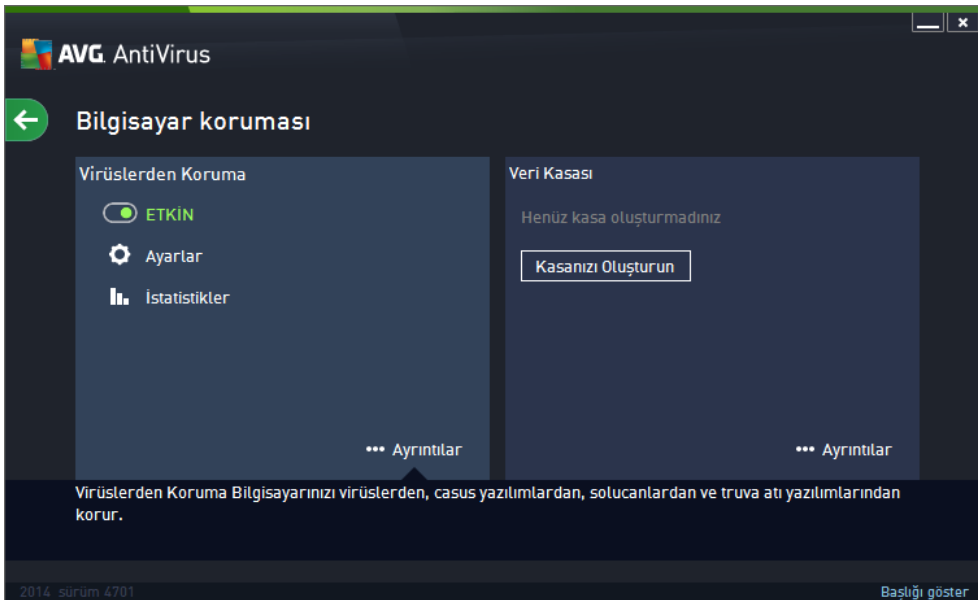


6. AVG Bileşenleri

6.1. Bilgisayar Koruması


Bilgisayar bileşeni iki temel güvenlik hizmetini kapsar: **Virüslerden Koruma** ve **Veri Kasası**:


- **AntiVirus** 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. AntiVirus dosyaların tipik virüs özelliklerine karşı tarandığı buluşsal analiz taraması da kullanır. Bu, yeni bir virüs mevcut virüslerin tipik özelliklerinden bazılarında sahipse söz konusu AntiVirus tarayıcısının yeni ve bilinmeyen bir virüsü tespit edebileceği anlamına gelmektedir. **AVG AntiVirus** 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 düzeltmenizi sağlar.
- **Veri Kasası** değerli veya hassas verileri saklamak için güvenli sanal kasa oluşturmaya olanak sağlar. Veri Kasası içerikleri şifrelenir ve sizin seçtiğiniz bir parola ile korunur; bu sayede yetkisi olmayan hiç kimse bunlara erişemez.





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. Bölümlerin işlevselliği, ait oldukları güvenlik servisinden bağımsız olarak, aynıdır (*Virüslerden Koruma veya Dosya Kasaları*):

 **Etkin / Devre dışı** - Düğme size hem görünüş hem de islev olarak trafik isiklerini hatırlatmış olabilir. İki konum arasında geçiş yapmak için tek tıklatin. Yeşil renk **Etkin**, yani AntiVirus 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 bilgisiyle 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 seçilen hizmeti, yani [Virüslerden Koruma](#)'yı yapılandırabilirsiniz. Gelmiş ayarlarda **AVG AntiVirus** 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 AntiVirus** 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.

Veri kasanızı oluşturma

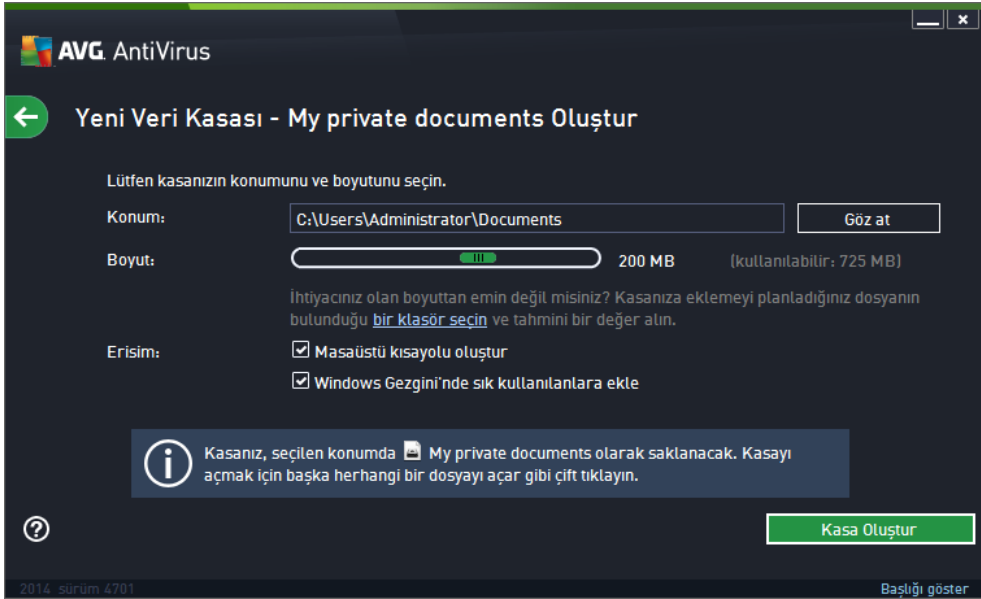
Bilgisayar Koruması iletişim kutusunun **Veri Kasası** bölümünde **Kasanızı Oluşturun** düğmesini bulabilirsiniz. Aynı anda sahip yeni bir iletişim kutusu açmak için düğmeyi tıklatarak planladığınız kasanın parametrelerini belirleyebilirsiniz. Lütfen tüm gerekli bilgileri doldurun ve uygulamadaki yönergeleri izleyin:



Öncelikle, kasanın adını belirlemeniz ve güçlü bir parola oluşturmamız gerekir:

- **Kasa adı** - Yeni bir veri kasası oluşturmak için öncelikle tanıyabileceğiniz uygun bir kasa adı seçmeniz gerekir. Bilgisayarı diğer aile fertleri ile paylaşıyorsanız kasa içeriklerini gösteren bir ifadenin yanı sıra adınızı da ekleyebilirsiniz: *Babanın e-postaları* gibi.
- **Parola oluşturun / Parolayı yeniden yazın** - Veri kasanız için bir parola oluşturun ve parolayı ilgili alanlarına yazın. Parolanızın zayıf mı (*özel yazılım araçlarıyla kırılması görece kolay*) yoksa güçlü mü olduğu sağ taraftaki grafik göstergede belirtilir. En azından orta kuvvette bir parola seçmenizi tavsiye ederiz. Büyük harfler, sayılar ve nokta, tire vb. başka karakterler ekleyerek parolanızı daha güçlü hale getirebilirsiniz. Parolanızı istediğiniz şekilde yazdığınızdan emin olmak istiyorsanız **Parolayı göster** kutusunu *isaretleyebilirsiniz* (*tabii ki ekranınıza başka birinin bakmıyor olması koşuluyla*).
- **Parola ipucu** - Unutmanız durumunda size parolanızı hatırlatacak faydalı bir parola ipucu oluşturmamız da kesinlikle tavsiye ederiz. Veri Kasası'nın yalnızca parola ile erişime izin vererek dosyalarınızı güvenli tutmak üzere tasarlanmış olduğunu lütfen unutmayın; bu durumun geçici bir çözümü yoktur ve parolayı unutursanız Veri Kasası'na erişemezsiniz!

Metin alanlarındaki tüm zorunlu verileri belirlediyseniz bir sonraki adıma geçmek için **İleri** düğmesini tıklayın:



Bu iletişim kutusunun sağladığı yapılandırma seçenekleri:

- **Konum** veri kasanının fiziki olarak nereye yerleştirileceğini gösterir. Gözet düğmesiyle sabit diskinizde uygun bir konum belirleyebilir veya önceden tanımlanmış konumu (*Belgeler* klasörünüz) muhafaza edebilirsiniz. Bir veri kasesi oluşturduktan sonra bu kasanın konumunu değiştiremeyeceğinizi lütfen unutmayın.
- **Boyut** - veri kasanızın boyutunu önceden tanımlayarak disk üzerinde gerekli alanın tahsis edilmesini sağlayabilirsiniz. Ayarlanacak değer ne çok küçük (*ihtiyaçlarınız için yetersiz*), ne de çok büyük (*gereksiz yere çok fazla disk alanı kaplayacak nitelikte*) olmalıdır. Veri kasesine ne koymak istediğinizi biliyorsanız tüm dosyaları tek bir klasöre yerleştirebilir ve ardından **Bir klasör seç** bağlantısını kullanarak toplam boyutu otomatik olarak hesaplayabilirsiniz. Ancak, boyut daha sonra ihtiyaçlarınız doğrultusunda değiştirilebilir.
- **Erisim** - bu bölümdeki onay kutuları veri kasanız için kullanışlı kısayollar oluşturmanıza olanak sağlar.

Veri kasanızı kullanma

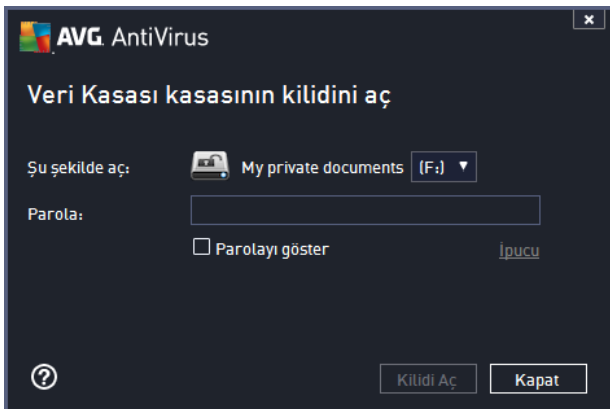
Ayarlardan memnun olduğunuzda **Kasa Oluştur** düğmesini tıklatın. Dosyalarınızı saklamak için kasanın hazır olduğunu belirten yeni bir **Veri Kasanız şimdi hazır** iletişim kutusu açılır. Artık kasa açıktır ve kasaya hemen erişebilirsiniz. Kasaya daha sonraki tüm erişim girişimlerinizde tanımladığınız parolayla kasanın kilidini açmanız istenecektir:



Yeni veri kasanizi kullanabilmek için öncelikle **Şimdi Aç** düğmesini tiktatarak kasayı açmanız gerekir. Kasayı açtıktan sonra veri kasanizi bilgisayarınızda yeni bir sanal disk olarak görünür. Lütfen kasaya açılır menüden seçtiğiniz bir harfi atayın (*yalnızca o anda boş olan diskler arasından seçim yapmanıza izin verilir*). Genel olarak, C (*çogunlukla sabit sürücünüze atanır*), A (*disket sürücüsü*) veya D (*DVD sürücüsü*) harflerini seçmenize izin verilmez. Bir veri kasaninin kilidini her açışınızda kullanılabilir durumdaki sürücü harflerinden bir baskasını seçebileceğinizi lütfen unutmayın.

Veri kasanizin kilidini açma

Kasaya daha sonraki erişim girişiminizde tanımladığınız parolayla kasanin kilidini açmanız istenecektir:



Metin alanında, kendinizi onaylamak için lütfen parolanizi yazın ve **Kilidi Aç** düğmesini tiktatın. Parolayı hatırlamakla ilgili yardıma ihtiyacınız varsa veri kasanini oluşturunken tanımladığınız parola ipucunu görüntülemek için **İpucu**'nu tiktatın. Yeni veri kasanizi, veri kasanizinin genel görünüm sayfasında KILIDI AÇIK olarak görünür ve gerektiği şekilde kasaya dosya ekleyebilir veya kasadan dosya silebilirsiniz.

6.2. Web Tarama Koruması


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 tanımlar 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 geçeceğini 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 ışıklarını 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. Gelmiş ayarlarda **AVG AntiVirus** 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.

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

6.3. Identity Protection


Identity Protection bileşeni internette dijital varlıklarınızı yeni ve bilinmeyen tehditlere karşı sürekli olarak koruyan **Identity Shield** hizmetini çalıştırır:


- **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 bulasmaları, 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 [gelmiş ayarlar](#) arayüzüne gidebilirsiniz. Tam olarak, ilgili iletişim kutusu açılır ve siz de burada [Identity Protection](#) gibi seçtiğiniz bir hizmetin yapılandırmasını yapabilirsiniz. Gelmiş ayarlarda **AVG AntiVirus** 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 AntiVirus** 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, Birlesik Krallik, Kanada ve Irlanda bölgelerinde sunulduğunu lütfen aklınızda bulundurun.

6.4. E-posta Koruması


E-posta Koruması bileşeni iki güvenlik hizmetini kapsar: **E-posta Tarayicisi** ve **Anti-Spam**:

- **E-posta Tarayicisi**: 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 teknolojisine 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 Tarayicisi'nin 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 [gelismis 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 AntiVirus** 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

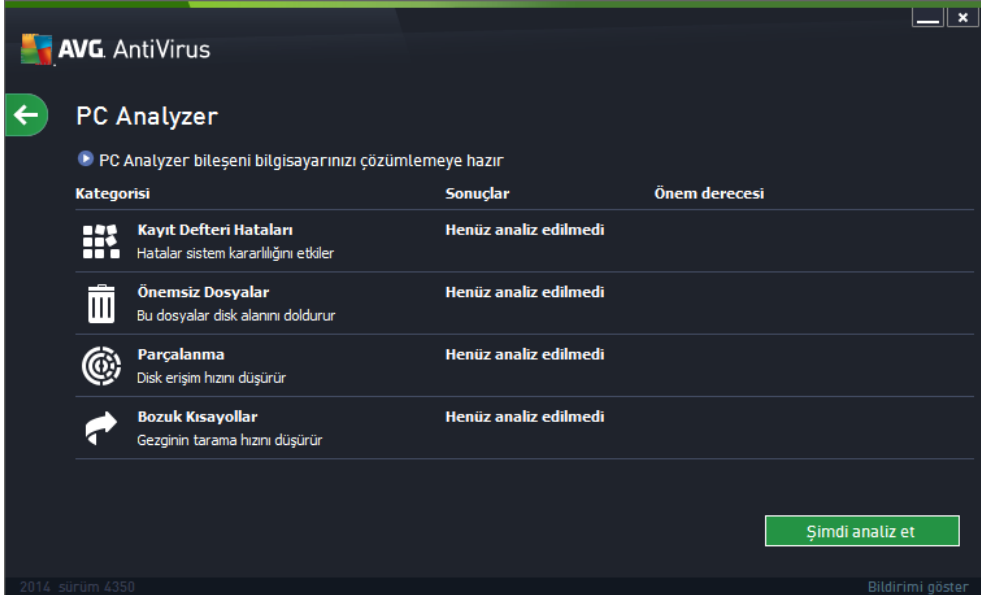
bilgisayarınızda gerçekleştirilen tüm **AVG AntiVirus** etkinliklerine ayrıntılı bir istatistiksel genel bakış bulabilirsiniz.

☰ **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. Quick Tune bileşeni

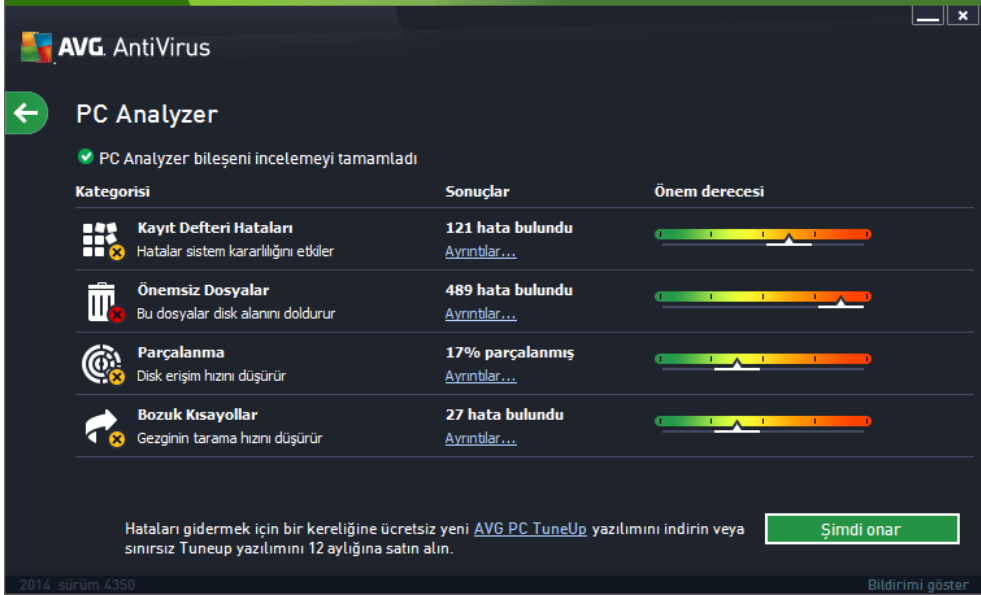
Quick Tune bileşeni, bilgisayarınızın hızının ve genel performansının nasıl iyileştirilebileceğine yönelik ayrıntılı sistem analizi ve düzeltme işlemi için tasarlanmış gelişmiş bir araçtır. Bu bileşen [ana kullanıcı arayüzünde](#) **Performansı Yükseltin** ögesinden açılır:



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:



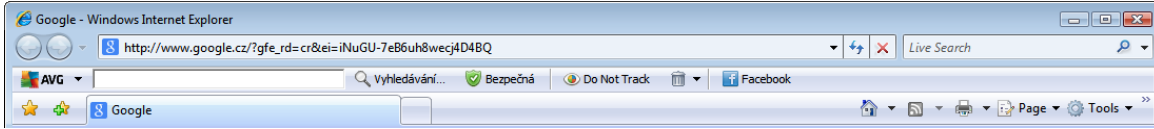
Sonuçlar genel görünümü, tespit edilen sistem sorunlarının sayısını, test edilen ilgili kategorilere göre verir. Analiz sonuçları **Önem Düzeyi** sütununda bir eksen üzerinde grafiksel olarak da görüntülenecektir.

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 AntiVirus** 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 ve 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 içerdigi öğeler:

- **Açılır menü** AVĞ logosu:
 - **Geçerli Tehdit Düzeyi** - web'de geçerli tehdit seviyesinin grafik görünümünü içeren virüs laboratuari web sayfasını açar.
 - **AVG Tehlike Laboratuvarları** - çeşitli web sitelerinin güvenliği ve geçerli tehlike düzeyi hakkında çevrimiçi bilgi alabileceğiniz **AVG Tehlike Laboratuari** web sitesini açar (<http://www.avgthreatlabs.com>).
 - **Toolbar Yardımı** - tüm **AVG Security Toolbar** işlemlerini kapsayan çevrimiçi yardımı açar.
 - **Ürün Geribildirim Gönder** - **AVG Security Toolbar** hakkında görüşlerinizi bildirebileceğiniz bir form içeren bir web sayfasını açar.
 - **Son Kullanıcı Lisans Sözleşmesi** - **AVG AntiVirus** kullanımınızla ilgili lisans sözleşmesinin tam metninin yer aldığı AVĞ web sitesi sayfasını açar.
 - **Gizlilik Politikası** - AVĞ Gizlilik Politikası'nın tam metnini bulabileceğiniz AVĞ web sitesi sayfasını açar.
 - **AVG Security Toolbar'nu kaldır** - **AVG Security Toolbar**'nu desteklenen web tarayıcılarının her birinde nasıl devre dışı bırakabileceğinizle dair ayrıntılı talimat içeren bir web sayfasını 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 tehdit seviyesi (*Güvenli*) hakkında bilgi sağlayan yeni bir iletişim kutusu açar. Bu kısa açıklama genişletilebilir ve sayfayla ilgili güvenlik aktiviteleri hakkında tüm ayrıntılar doğrudan tarayıcı

penceresinde görüntülenebilir (*Tam Web Sitesi Raporu*):



AVG Site Safety

Bezpečná (Safe)

Kompletní zpráva o stránce
Nejnovější aktualizace: 29.5.2014

Adresa URL stránky: http://www.google.cz/?gfe_rd=cr&ei=TNYGU_rmAamh8wfPqYDoBQ

Název stránky: Google

Bezpečná
Na této stránce se nenachází žádné aktivní hrozby. Můžete ji s klidem otevřít.

Riziková
Pozor – tato stránka může obsahovat hrozby. Doporučujeme ji neotevírat.

Nebezpečná
Tato stránka obsahuje aktivní hrozby. Doporučujeme ji neotevírat.

30denní aktivita hrozb pro <http://www.google.cz>

100
0
Apr 28 May 7 May 16 May 25

| | |
|--------------------------|--|
| Internetová stránka | google.cz |
| Poslední aktualizace ... | May 29, 2014 |
| IP adresa | 173.194.116.184 |
| Rychlost | Fast |
| Velikost | 51.09 KB |
| Soubory cookie | Yes |
| Obľíbenost stránky | Top Site |
| Umístění serveru | US |
| Zabezpečení SSL | Disabled |
| Podobné internetové ... | http://seznam.cz/ http://centrum.cz/ http://www.atlas.cz/ http://zive.cz/ |

- **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.



The Weather Channel
weather.com

Brno, Czech Republic
Updated: 8/6/13 9:30 PM Local Time [[change location](#)]

28°C
Sunrise: 05:33
Sunset: 08:25

| | | |
|--------------------------------|-----------------------------------|----------------------------------|
| Tonight Hi: N/A Lo: 22°C | Wednesday Hi: 37°C Lo: 23°C | Thursday Hi: 38°C Lo: 22°C |
|--------------------------------|-----------------------------------|----------------------------------|



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

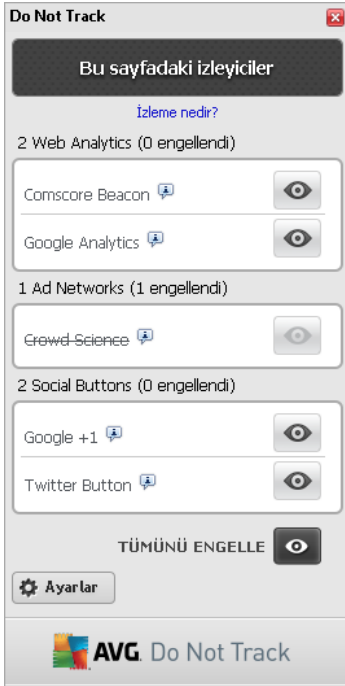
- **AVG Do Not Track** her servis için gizlilik politikası hakkında ek bilgilerin yanı sıra varsa ilgili servisin dışında kalmak için doğrudan bir bağlantı da sunar.
- **AVG Do Not Track** sizi izlemesini istemediğiniz siteler hakkında otomatik bilgilendirme için [W3C DNT protokolünü](#) de destekler. 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

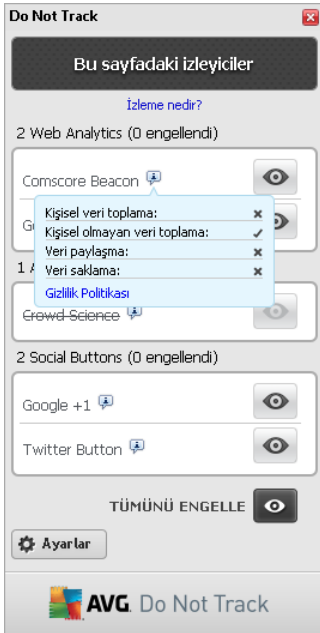
- **İzleme nedir?** - İzleme prensipleri hakkında ayrıntılı açıklamalar ve belirli izleme türlerinin tarifini içeren bir web sayfasına yönlendirilmek için iletişim kutusunun üst bölümünde yer alan bu bağlantıyı tıklanın.
- **Tümünü Engelle** - Hiçbir veri toplama faaliyeti istemiyorsanız iletişim kutusunun altındaki

bu düğmeyi tıklatin (*ayrintilar için [Izleme islemlerini engelleme](#) bölümüne bakin*).

- **Do Not Track ayarlari** - Çesitli **AVG Do Not Track** parametrelerinin yapilandirma ayarlarini yapabileceginiz bir web sayfasina yönlendirilmek için iletisim kutusunun alt bölümündeki bu baglantiyi tıklatin (*ayrintili bilgi için [AVG Do Not Track ayarlari](#) bölümüne bakin*)

8.2. İzleme süreçleri hakkında bilgiler


Tespit edilen veri toplama servislerinin listesi yalnızca ilgili servisin adini gösterir. İlgili servise izin verme veya engelleme yönünde bilinçli bir tercih yapmak için daha fazla bilgiye ihtiyaciniz vardır. Fare imlecini ilgili liste ögesinin üzerine getirin. Servis hakkında detayli bilgileri içeren bir bilgi balonu görüntülenir. Servisin kisisel verilerinizi mi yoksa baska verileri mi topladigi, verilerin diger üçüncü taraflarla paylasilip paylasilmadigi ve toplanan verilerin ileride kullanilmak üzere saklanip saklanmadigi gibi konular hakkında bilgi sahibi olursunuz:




Bilgi balonunun alt bölümünde, tespit edilen ilgili servisin web sitesinde gizlilik politikasina yönlendiren bir **Gizlilik Politikasi** baglantisi bulunur.

8.3. İzleyici süreçlerini engelleme

Tüm Ad Networks / Social Buttons / Web Analytics listesiyle istediginiz servislerin engellenmesini kontrol etme seçenegine sahip olursunuz. İki seçenekten birini tercih edebilirsiniz:

- **Tümünü Engelle** - Hiçbir veri toplama faaliyeti istemiyorsanız iletisim kutusunun altındaki bu düğmeyi tıklatin. (*Ancak, bu islemin servisin çalıştigi ilgili web sitesinin islevlerini bozabileceğine dikkat edin!*)
-  - Tespit edilen servislerin tamamini bir seferde engellemek istemiyorsanız, servislerin engellenmesine veya bunlara izin verilmesine tek tek karar verebilirsiniz. Tespit edilen sistemlerden bazilarinin çalışmasına izin verebilirsiniz (*örn. Web Analytics*): Bu sistemler toplanan verileri kendi web sitelerinin optimizasyonu için kullanir ve böylece tüm kullanıcılar

için internet ortamının geliştirilmesine yardımcı olur. Ancak, aynı zamanda Ad Networks olarak sınıflandırılan tüm veri toplama faaliyetlerini engelleyebilirsiniz. Veri toplamayı engellemek (*servis adi çarpi ile isaretlenir*) veya veri toplamaya 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:



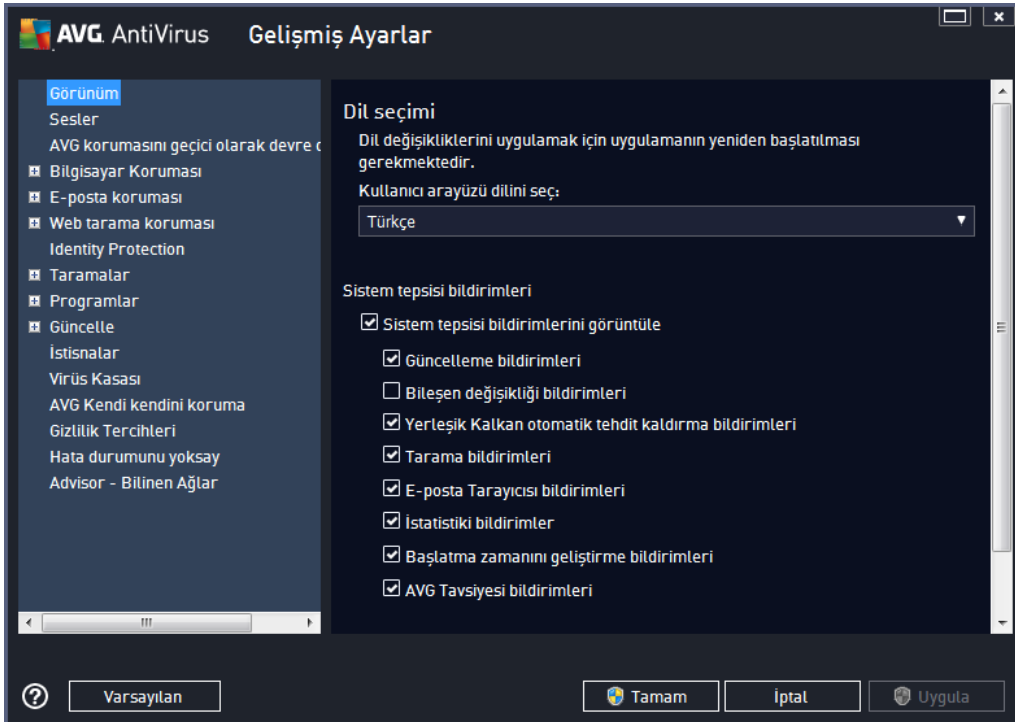
- **Do Not Track etkin** - Varsayılan olarak DNT servisi etkindir (*AÇIK*). Hizmeti devre dışı bırakmak için anahtarı *KAPALI* konumuna getirin.
- İletişim kutusunun orta bölümünde Ad Networks olarak sınıflandırılacak bilinen veri toplama servislerinin bir listesinin yer aldığı bir kutu görebilirsiniz. **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 AntiVirus 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 AntiVirus kullanıcı arayüzünün** genel ayarlarına iliskindir ve uygulama davranışı için bazı temel seçenekleri sağlar:

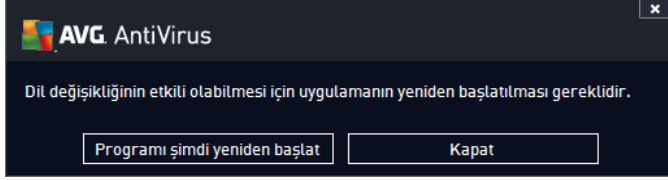


Dil seçimi

Dil seçimi bölümünde açılır menüden istediğiniz dili seçebilirsiniz. Seçilen dil **AVG AntiVirus kullanıcı arayüzünün** tamamı için kullanılır. Aşağı açılır menü yükleme işlemi sırasında yüklenmesini istediğiniz dilleri ve İngilizceyi sunar (*İngilizce daima varsayılan olarak yüklenir*). **AVG AntiVirus** 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 AntiVirus**
- Programın yeniden başlatılmasını onaylamak için **AVG'yi şimdi yeniden başlat** düğmesine

basın ve dil değişikliğinin gerçekleşmesi için bir saniye bekleyin:



Sistem tepsisi bildirimleri

Bu bölümde **AVG AntiVirus** 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 AntiVirus** 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 AntiVirus bileşenlerine ilişkin*) tercihlerinizi aşağıdaki seçenekleri işaretleyerek ya da işaretlemeyerek tanımlayabilir ve belirleyebilirsiniz:

- **Sistem tepsisi 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 AntiVirus** güncelleme işleminin başlaması, ilerleyisi ve bitisi hakkında bilgilerin görüntülenmesini isteyip istemediğinize karar verin.
 - **Bileşen değişiklik bildirimleri** (*varsayılan olarak kapalı*) - bileşenlerin etkin olup olmadığı ya da olası sorunları hakkında bildirimlerin görüntülenmesini isteyip istemediğinize karar verin. Bir bileşenin hata durumu rapor edilirken bu fonksiyon, [sistem tepsisi simgesinin](#) herhangi bir **AVG AntiVirus** bileşeninde meydana gelen sorunu rapor ederken kullandığı bilgilendirici fonksiyonuna esdeğerdir.
 - **Yerleşik Kalkan otomatik tehdit kaldırma bildirimleri** (*varsayılan olarak açık*) - dosya kaydetme, kopyalama ve açma işlemleriyle ilgili bilgilerin görüntülenmesine veya gizlenmesine (*bu yapılandırma yalnızca Yerleşik Kalkan otomatik temizleme seçeneği açık olduğunda*) karar verin.
 - **Tarama bildirimleri** (*varsayılan olarak açık*) - programlı taramaların otomatik olarak başlaması, ilerleyisi ve sonuçları hakkında bilgilerin görüntülenmesini isteyip istemediğinize karar verin.
 - **E-posta Tarayıcısı bildirimleri** (*varsayılan olarak açık*) - gelen ve giden e-posta mesajlarının taranmasına ilişkin bildirimleri görüntülemek isteyip istemediğinize karar verin.
 - **İstatistiksel bildirimler** (*varsayılan olarak açık*) - düzenli istatistiksel inceleme uyarılarının sistem tepsisinde görüntülenmesine izin vermek için bu seçeneği işaretli halde bırakın.

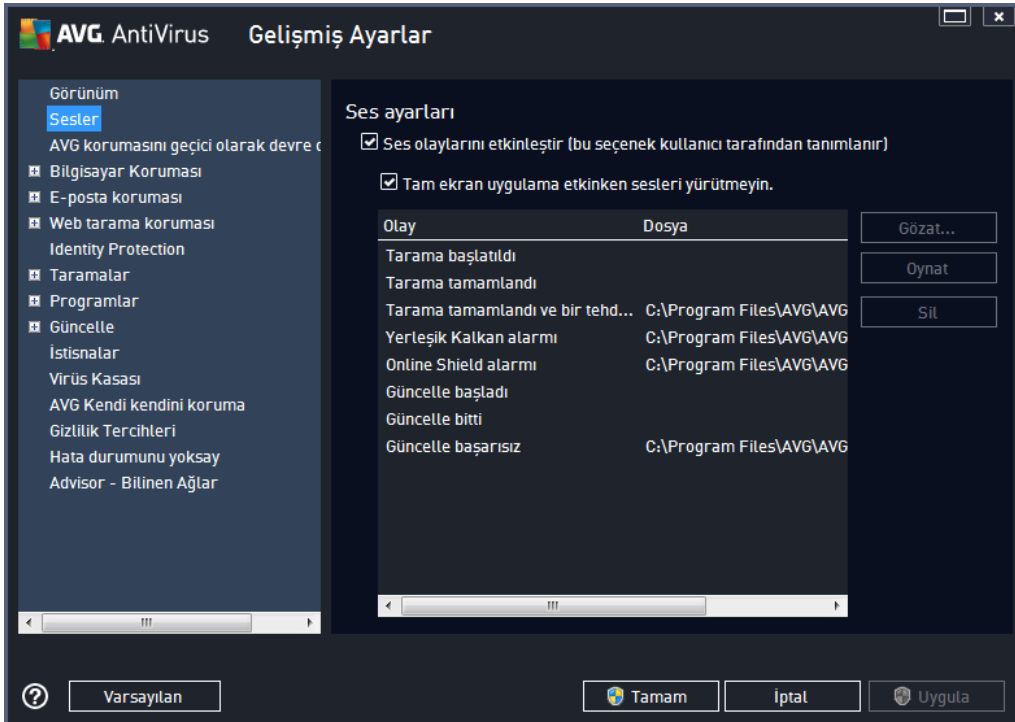
- o **Baslatma zamanini gelistirme bildirimleri** (varsayilan olarak kapali) - bilgisayarinizin baslatma zamaninin gelistirilmesi hakkında bilgilendirilmek isteyip istemediginize karar verin.
- o **AVG Tavsiyesi bildirimleri** (varsayilan olarak acik) - [AVG Tavsiyesi](#) etkinlikleri hakkındaki bilgilerin 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 (varsayilan ayar).

9.2. Sesler

Ses Ayarları iletişim kutusunda belirli **AVG AntiVirus** işlemleri hakkında bir ses bildiriyle bilgilendirilmek isteyip istemediğinizi belirleyebilirsiniz:



Bu ayarlar yalnızca mevcut kullanıcı hesabı için geçerlidir. Bu nedenle bilgisayar üzerindeki kullanıcıların her birine ait ses ayarları vardır. Sesli bildiriye izin vermek istiyorsanız, ilgili tüm eylemler listesini etkinleştirmek için **Sesli uyarıları etkinleştir** seçeneğini işaretli bırakın (seçenek varsayilan 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).

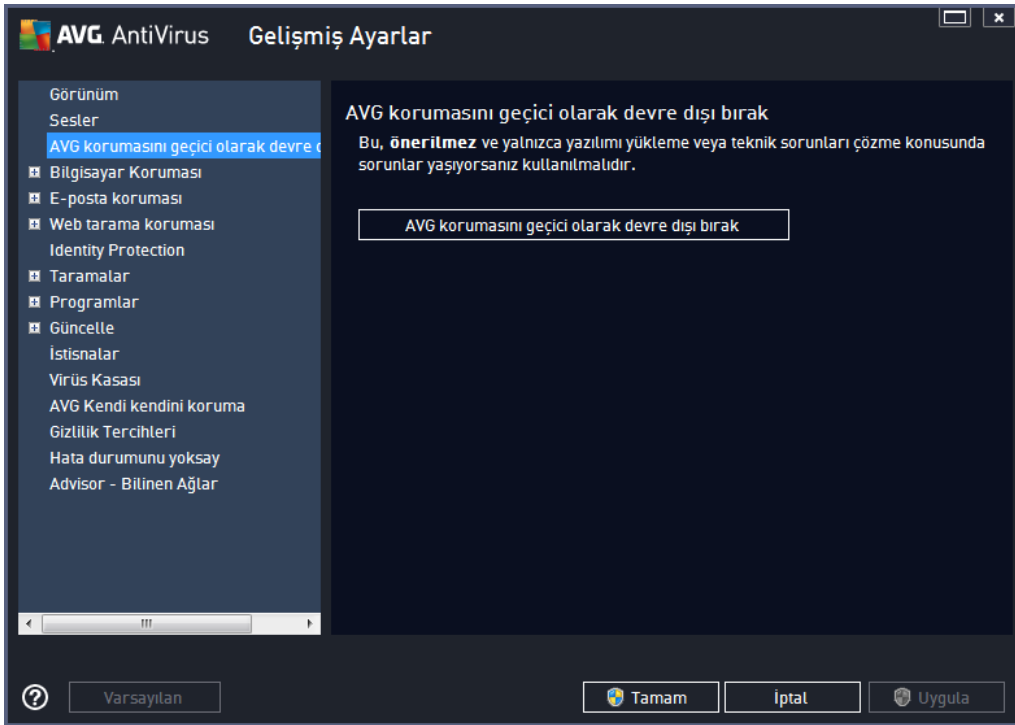
Kontrol düğmeleri

- **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 AntiVirus** yazılımınız tarafından güvende tutulan tüm korumayı bir seferde kapatma seçeneğiniz vardır.

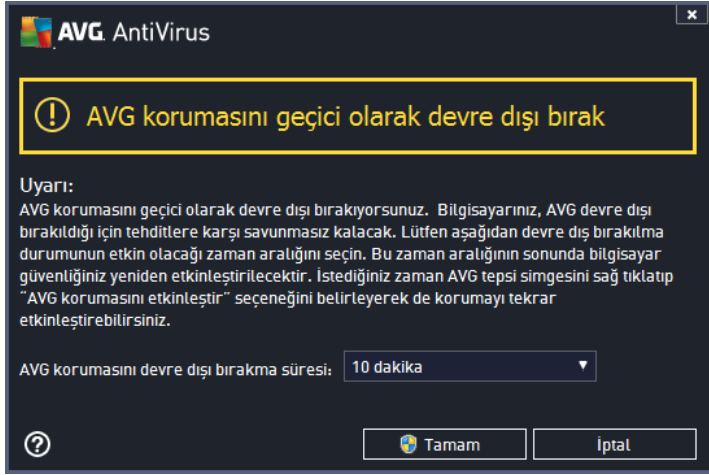
Mutlaka gerekli değilse, bu seçeneği kullanmamanız gerektiğini lütfen unutmayın!



Çoğu durumda, yeni yazılımı veya sürücülerini yüklemeye başlamadan önce ve hatta yükleyici veya yazılımı sihirbazı yükleme işlemi sırasında istenmeyen kesintilerin olmamasını sağlamak için çalışan program ve uygulamaların kapatılmasını önerse bile **AVG AntiVirus** uygulamasını devre dışı bırakmak **gerekmez**. Yükleme sırasında gerçekten sorunlar yaşıyorsanız, öncelikle yerleşik korumayı devre dışı bırakmayı deneyin (*Yerleşik Kalkanı etkinleştir*). **AVG AntiVirus** 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 koruması geçici olarak nasıl devre dışı bırakılır

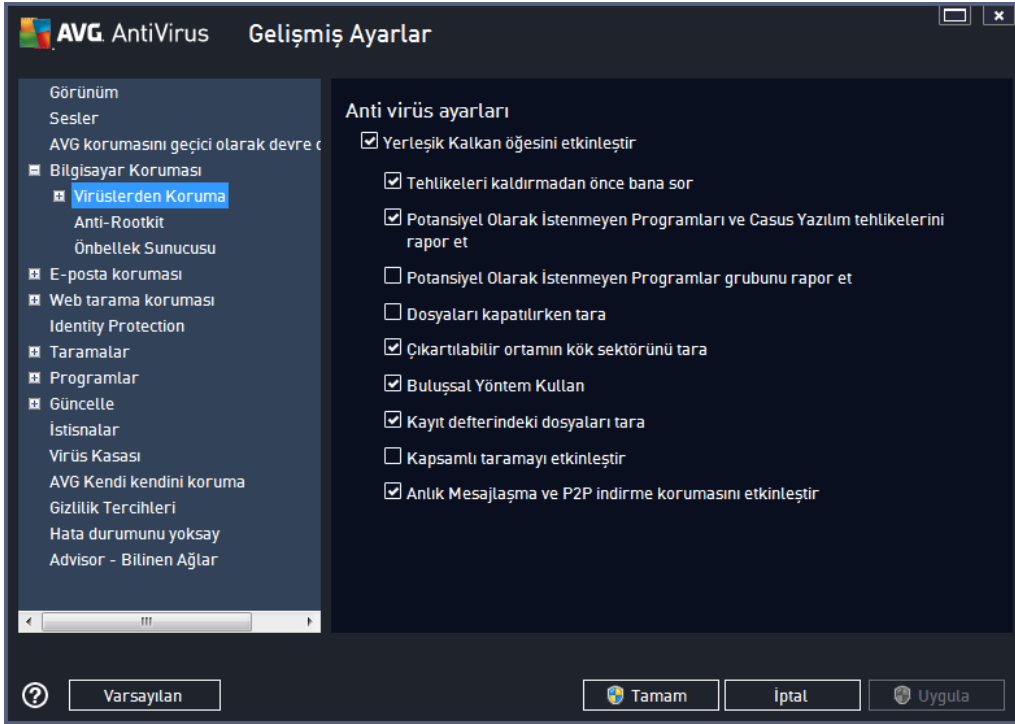
AVG korumasını geçici olarak devre dışı bırak onay kutusunu işaretleyin ve **Uygula** düğmesine basarak seçiminizi onaylayın. Yeni açılan **AVG korumasını geçici olarak devre dışı bırak** iletişim kutusunda **AVG AntiVirus** uygulamanızı ne kadar süreyle devre dışı bırakmak istediğinizi belirleyin. Koruma, 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.



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*).

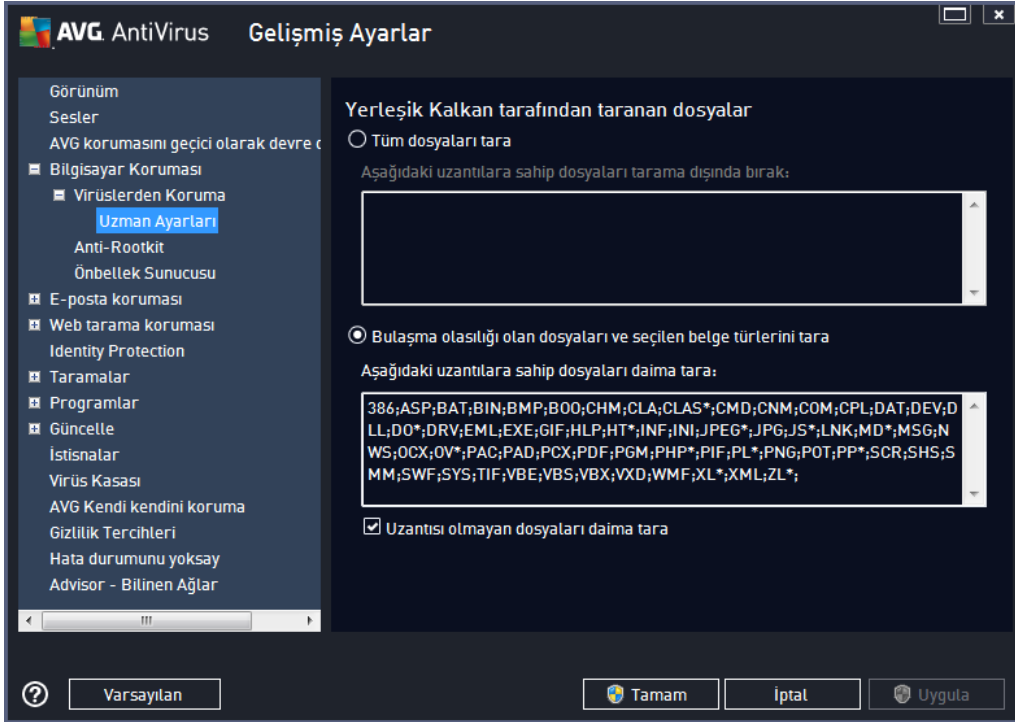


Yerlesik Kalkan ayarları iletişim kutusunda yerlesik kalkan korumasini **Yerlesik Kalkan'i etkinlestir** ögesini isaretleyerek ya da isaretini kaldırarak etkinlestirebilir ya da devre disi bırakabilirsiniz (*bu seçenek varsayılan olarak açıktır*). Ayrıca yerlesik kalkanin hangi özelliklerinin etkinlestirileceğini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



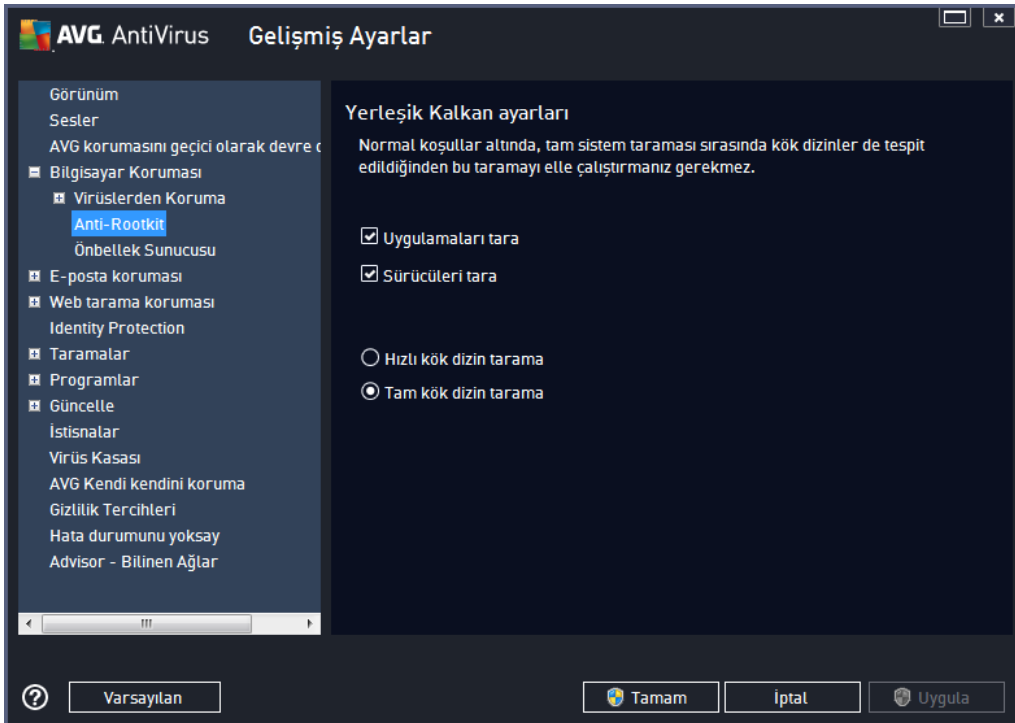
Tüm dosyaları tara veya yalnızca **Bulasma olasılığı olan dosyaları ve seçilen belge türlerini tara** seçimi yapmak için ilgili onay kutusunu işaretleyin. Taramayı hızlandırmak ve aynı zamanda maksimum koruma düzeyi sağlamak için varsayılan ayarları korumanızı öneririz. Bu sayede yalnızca virüs bulabilecek 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:

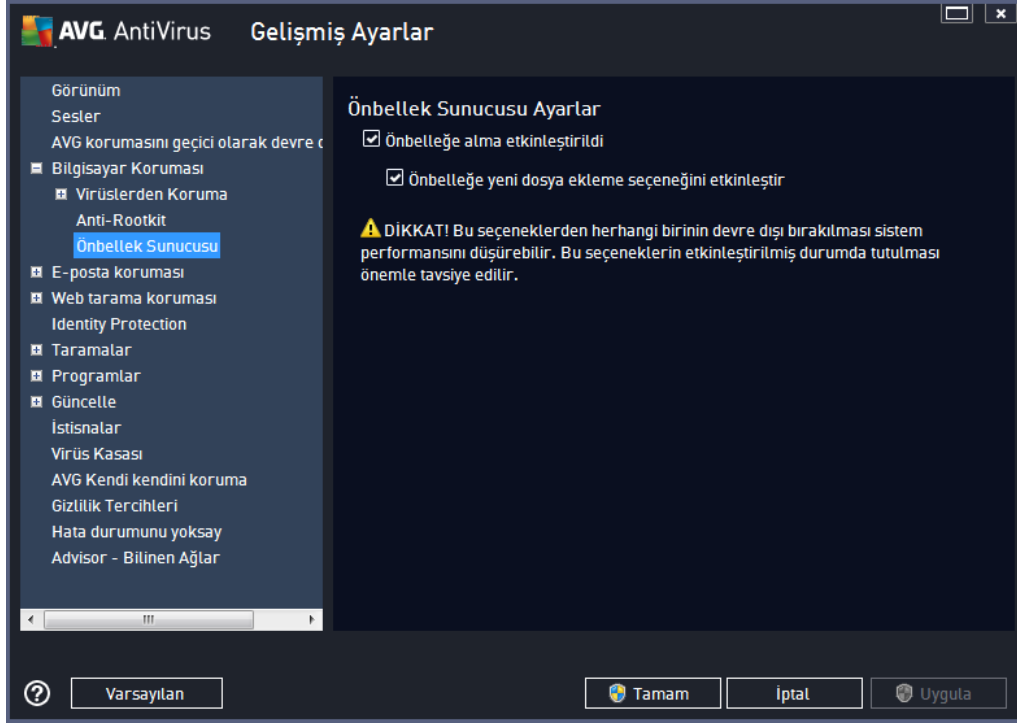


Tarama uygulamaları ve **Tarama sürücülerini** anti-rootkit taramasına nelerin dahil edileceğini ayrıntılı şekilde belirlemenize olanak tanır. Bu ayarlar gelişmiş kullanıcılara yöneliktir; tüm seçenekleri açık konumda muhafaza etmenizi öneririz. Rootkit tarama modunu da seçebilirsiniz:

- **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 AntiVirus** 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 kapatılıncaya kadar veya virüs veritabanının bir sonraki güncellenmesine kadar kullanılacaktır.

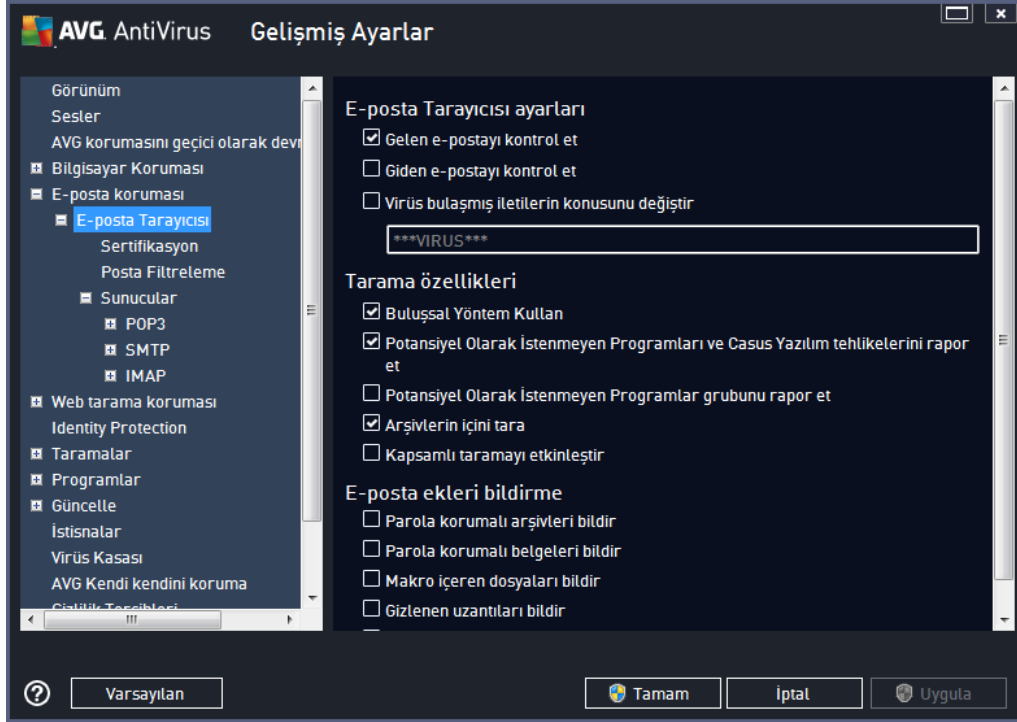
Önbellek sunucusunu kapatmak için iyi bir nedeniniz yoksa, kesinlikle varsayılan ayarları muhafaza etmenizi ve seçeneğin açık kalmasını öneririz! Aksi durumda, sistem hızı ve performansında ciddi bir düşüş görebilirsiniz.

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:

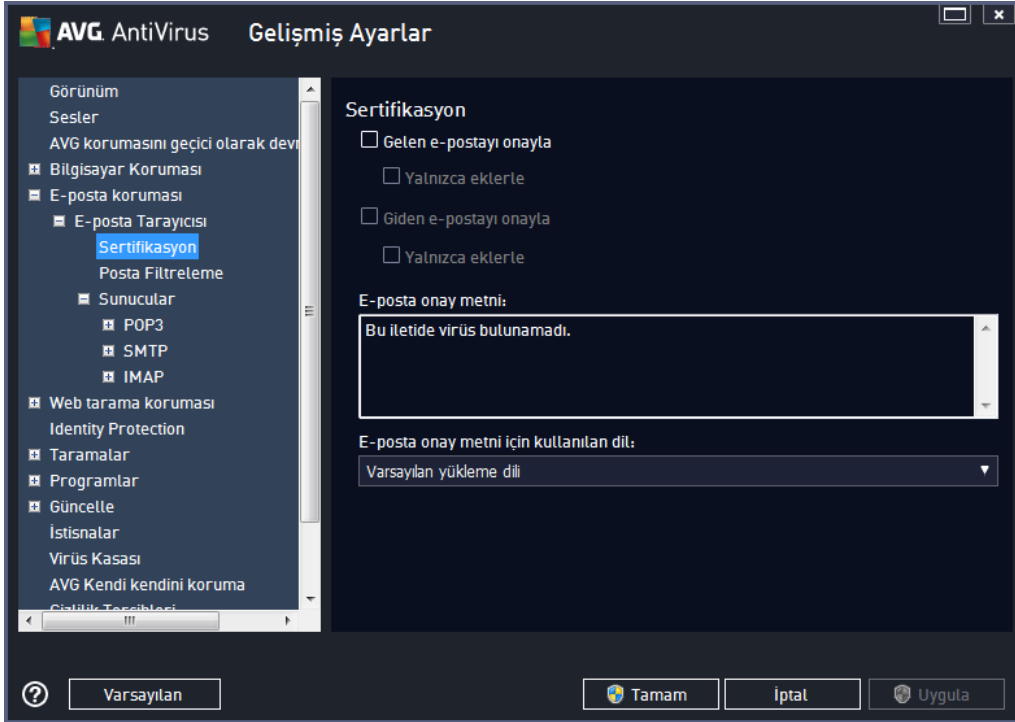
- **Bulussal Yöntem Kullan** (varsayılan olarak açık) - e-posta iletilerini tararken bulussal tespit yöntemi kullanmak için işaretleyin. Bu seçenek açık olduğunda, e-posta eklerini yalnızca uzantıya göre filtrelemezsiniz; ekin gerçek içeriği de göz önünde bulundurulur. Filtreleme işlemi [Posta Filtreleme](#) 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:

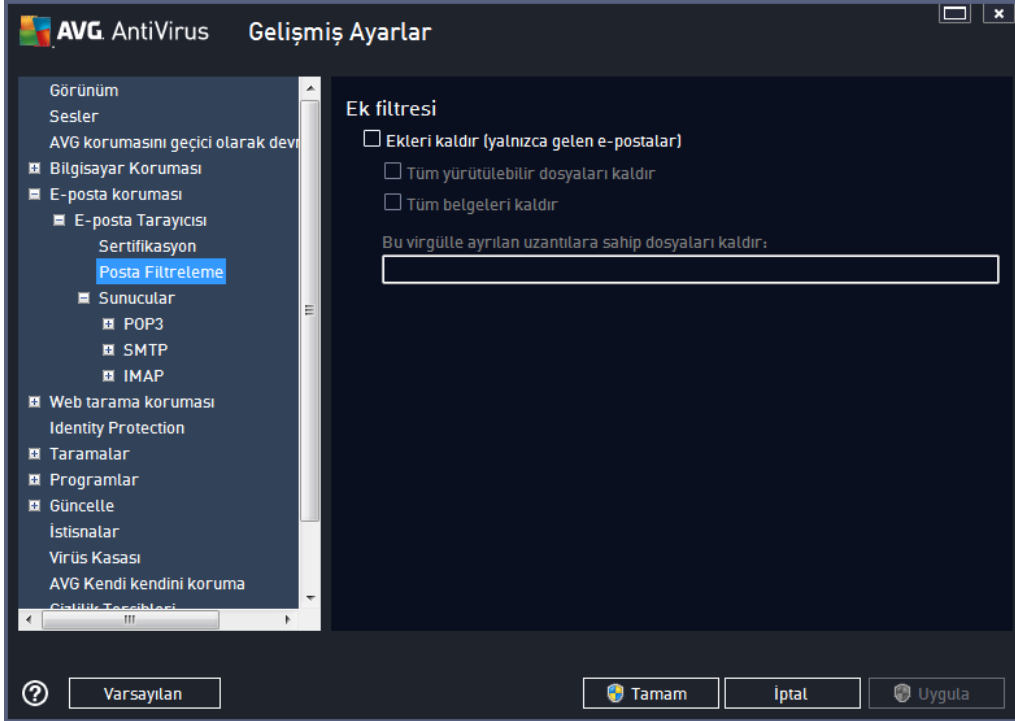
- **Parola korumalı arşivleri bildir** - parolayla korunan arşivler (ZIP, RAR vb.) virüslere karşı taranamaz; bunların potansiyel olarak tehlikeli olduklarını bildirmek için kutuyu işaretleyin.
- **Parola korumalı belgeleri bildir** - parolayla korunan belgeler virüslere karşı taranamaz; bunların potansiyel 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!*



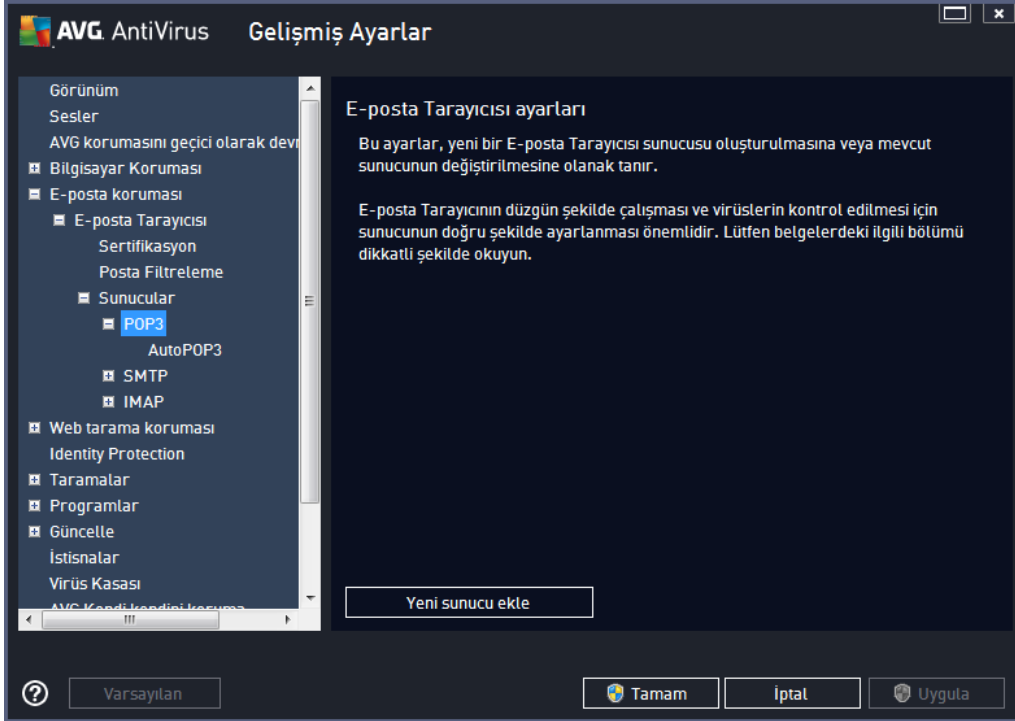
Ek filtresi iletişim kutusu, e-posta mesajlarının eklerinin taranmasına ilişkin parametreleri ayarlayabilmenizi sağlar. Varsayılan olarak **Eklenileri sil** seçeneği kapalıdır. Etkinleştirmeye karar verirsiniz tüm e-posta mesajlarının eklentileri, bulasız nesne ya da potansiyel olarak tehlikeli nesne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

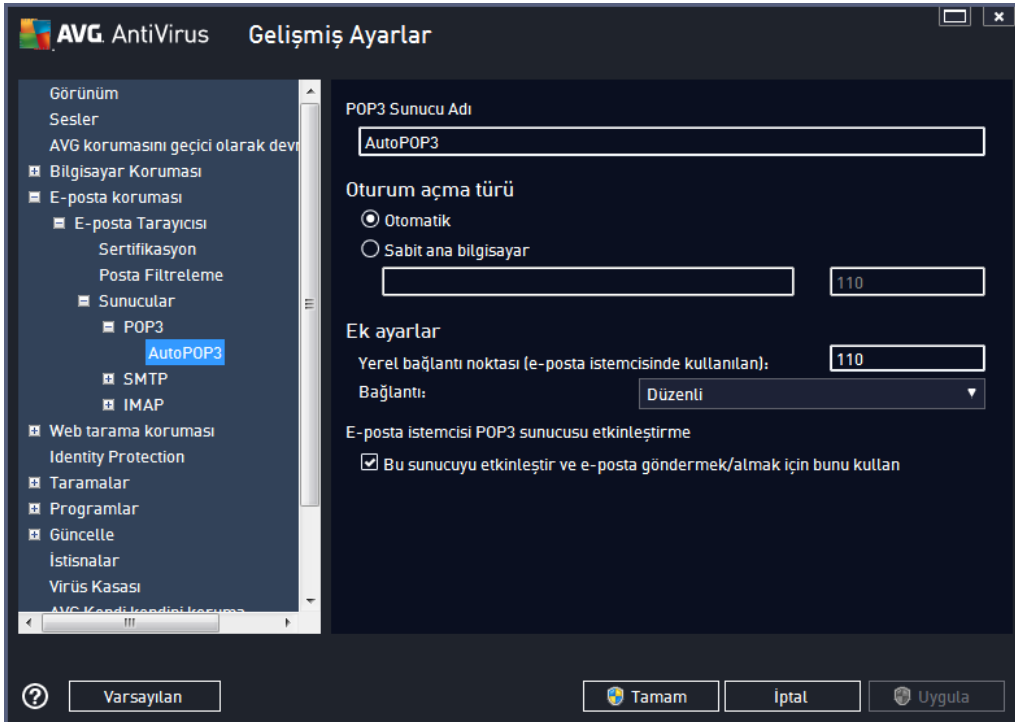
Sunucular bölümünde [E-posta Tarayıcısı](#) sunucularının parametrelerini düzenleyebilirsiniz:

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

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



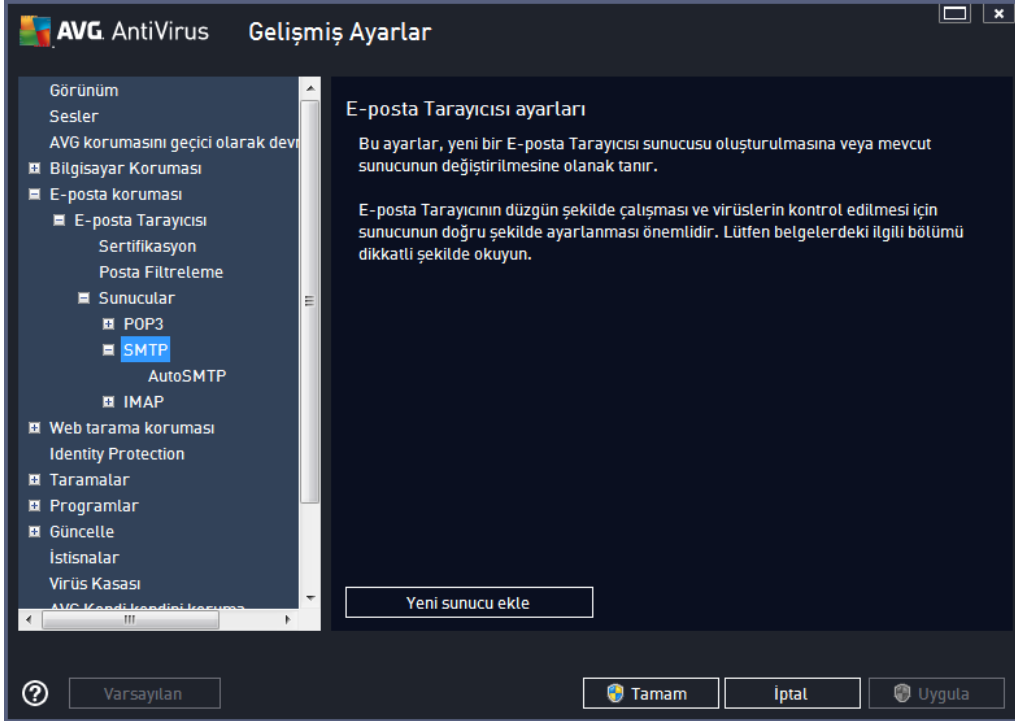
Bu iletişim kutusunda gelen postalar için POP3 protokolünü kullanarak yeni bir [E-posta Tarayıcısı](#) sunucusu kurabilirsiniz:



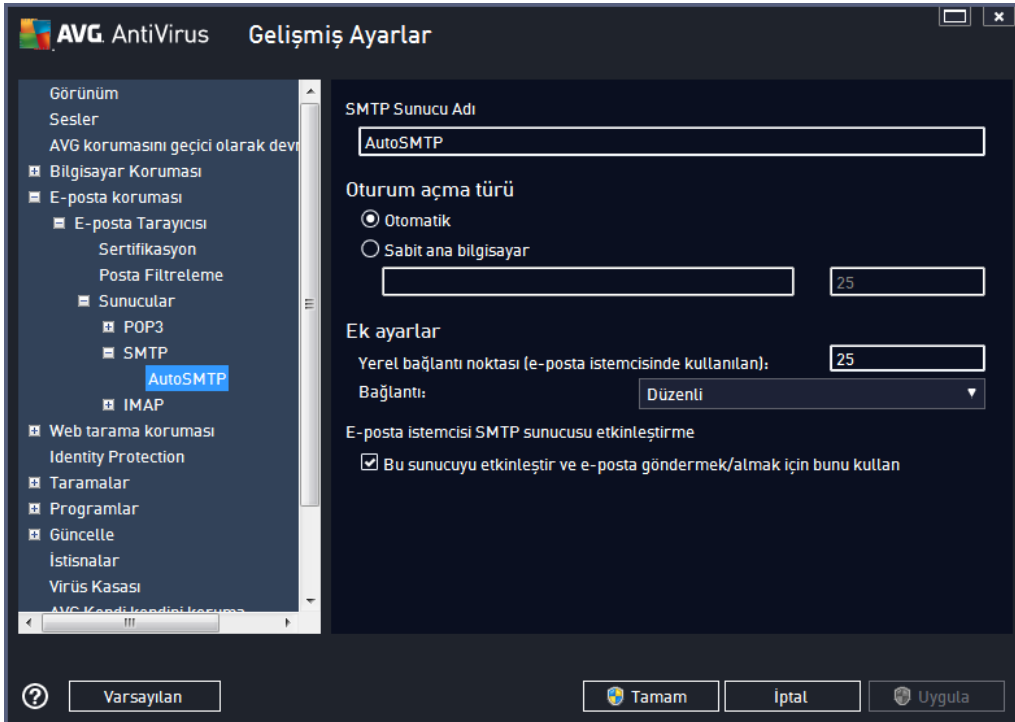
- **POP3 Sunucusunun Adı** - bu alanda yeni eklenen sunucuların adını belirtebilirsiniz (bir

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 sunucusunu belirleme yöntemini 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 İstemcisi POP3 Sunucusunu Etkinleştirme** - belirtilen POP3 sunucusunu etkinleştirmek veya devre dışı bırakmak için bu öğeyi işaretleyin veya öğenin işaretini kaldırın.



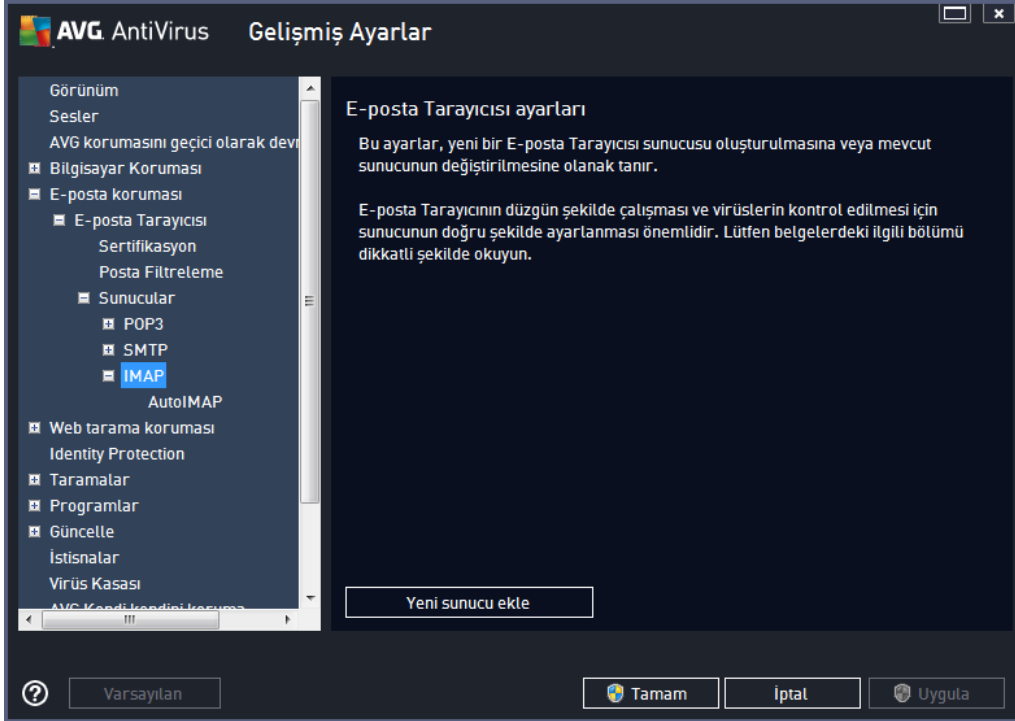
Bu iletişim kutusunda giden postalar için SMTP protokolünü kullanarak yeni bir [E-posta Tarayıcısı](#) sunucusu kurabilirsiniz:



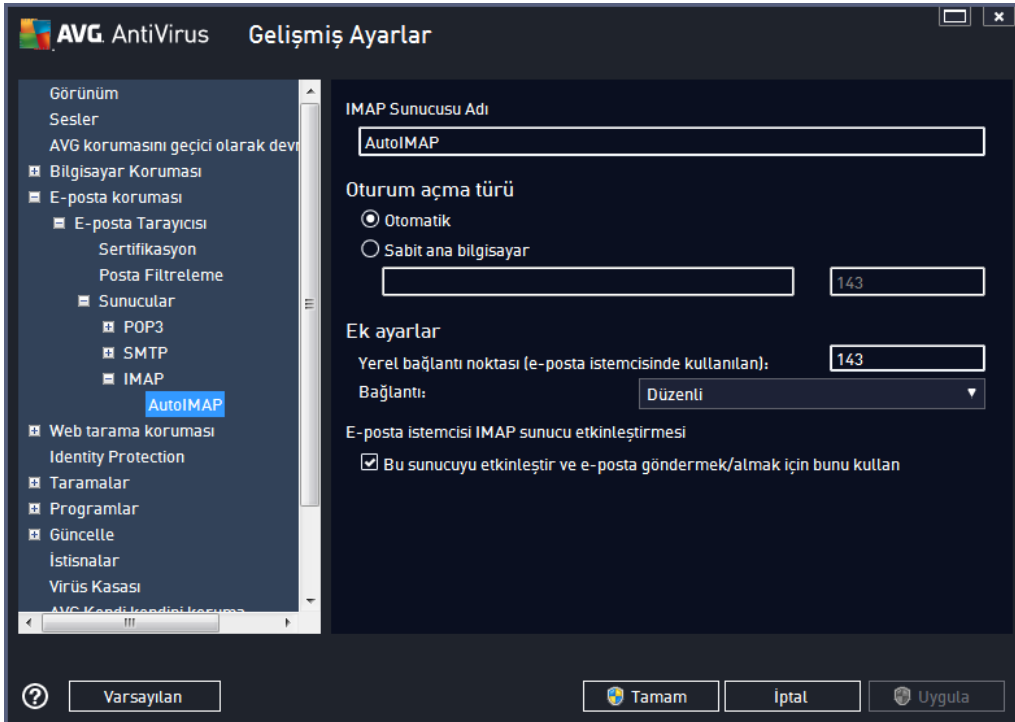
- **SMTP Sunucusunun Adı** - bu alanda yeni eklenen sunucuların adını belirtebilirsiniz (*bir*

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

- **Oturum Açma Tipi** - giden postalar için kullanılan posta sunucusunu belirleme yöntemini 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. Ad için, IP adresinin yanı sıra (örneğin, 123.45.67.89) etki alanı adı da (örneğin, smtp.acme.com) kullanabilirsiniz. *Posta sunucusu standart olmayan bir bağlantı noktası kullanıyorsa, bu bağlantı noktasını ayırıcı olarak iki nokta üst üste kullanarak sunucu adının arkasına girebilirsiniz (örn. smtp.acme.com:8200). SMTP iletişimi için standart bağlantı noktası 25'tir.*
- **Diğer Ayarlar** - daha ayrıntılı parametreleri belirler:
 - **Yerel bağlantı noktası** - Posta uygulamanızın iletişim kurması beklenen bağlantı noktasını belirler. Posta uygulamanızda, bu bağlantı noktasını SMTP iletişimi bağlantı noktası olarak belirtmeniz gerekir.
 - **Bağlantı** - bu açılır aşağı menüden, kullanılacak bağlantı türünü belirtebilirsiniz (*normal/SSL/SSL varsayılan*). SSL bağlantıyı tercih ederseniz, gönderilen veri, üçüncü bir taraf tarafından izlenme riski olmayacak şekilde şifrelenir. Bu özellik, yalnızca hedef posta sunucusu tarafından desteklendiğinde kullanılabilir.
- **E-posta İstemcisi SMTP Sunucusunu Etkinleştirme** - 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:



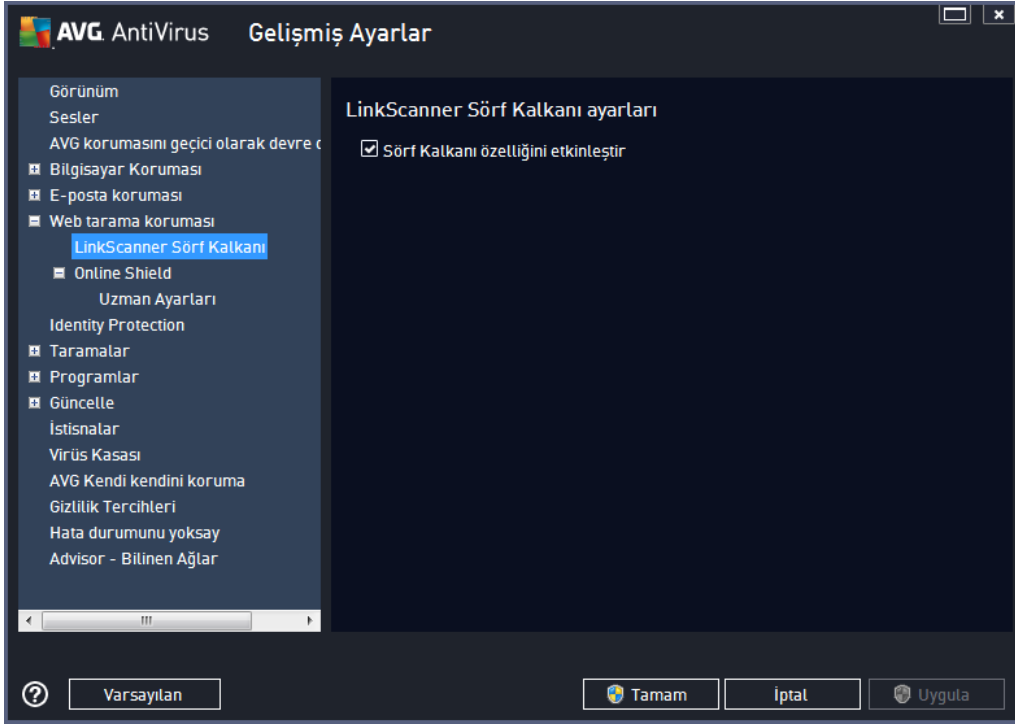
- **IMAP Sunucusunun Adı** - bu alanda yeni eklenen sunucuların adını belirtebilirsiniz (bir

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 sunucusunu belirleme yöntemini 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. Ad için, IP adresinin yanı sıra (örneğin, 123.45.67.89) etki alanı adı da (örneğin, smtp.acme.com) kullanabilirsiniz. Posta sunucusu standart olmayan bir bağlantı noktası kullanıyorsa, bu bağlantı noktasını ayırıcı olarak iki nokta üst üste kullanarak sunucu adının arkasına yazabilirsiniz (örneğin, smtp.acme.com:8200). IMAP iletişiminin standart bağlantı noktası 143'tür.
- **Diğer Ayarlar** - daha ayrıntılı parametreleri belirler:
 - **Kullanılan 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 İstemcisi IMAP Sunucusunu Etkinleştirme** - yukarıda belirtilen IMAP sunucusunu etkinleştirmek/devre dışı bırakmak için bu kutuyu işaretleyin veya kutunun işaretini kaldırın

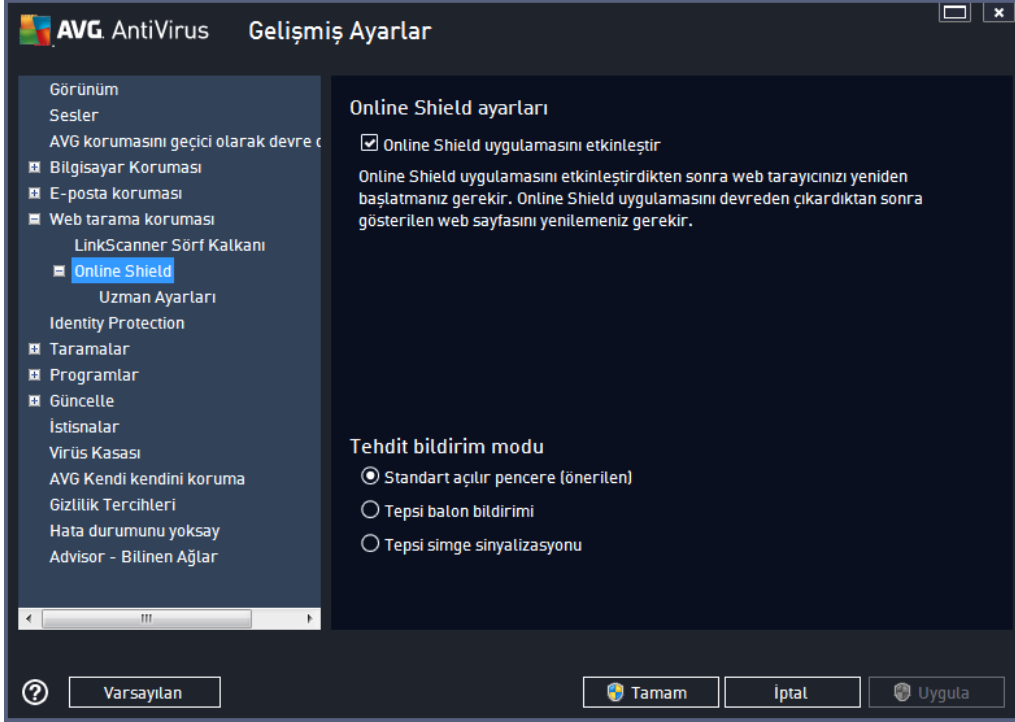
9.6. Web Tarama Koruması

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 bağlantıları içeren iletilerde LinkScanner denetimi ile ilgili sertifikasyon bildirimini girmek istediğinizi onaylamak için bu öğeyi işaretleyin.

9.6.1. Online Shield

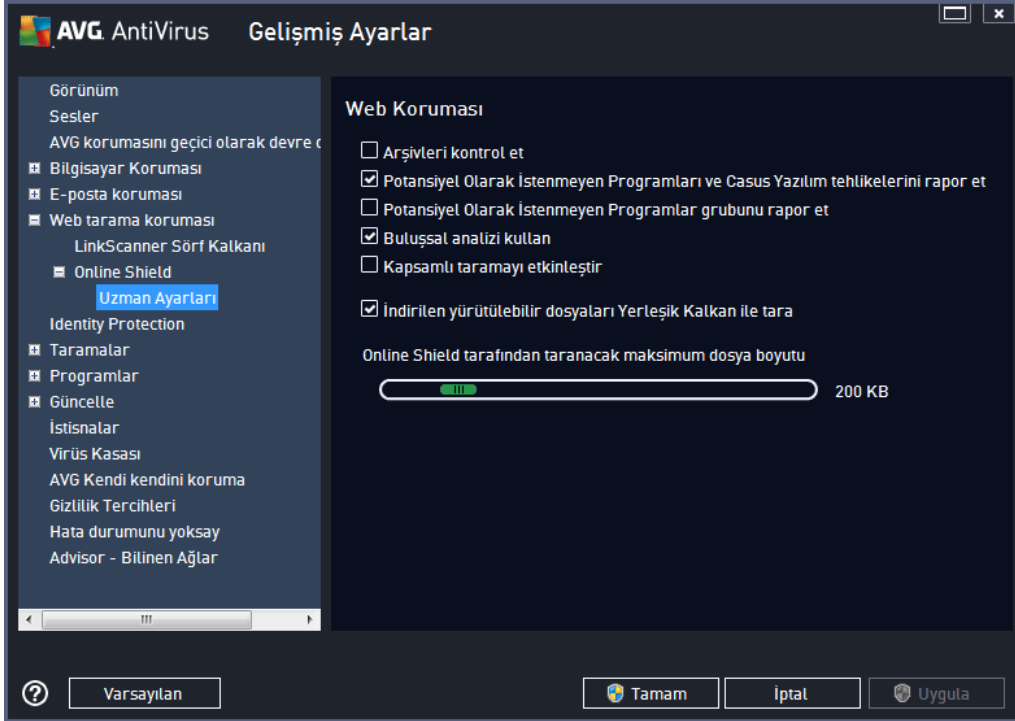


Online Shield iletişim kutusu su seçenekleri sunar:

- **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.

Tehdit bildirim modu

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



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

- **Arsivleri denetle** - (varsayılan olarak kapalı): Görüntülenecek www sayfasında bulunması muhtemel arşivlerin içeriğini tarayın.
- **Potansiyel olarak istenmeyen programları ve casus yazılım tehlikelerini rapor et** - (varsayılan olarak açık): Virüslerin yanı sıra casus yazılımların da taranmasını etkinleştirmek için işaretleyin. 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 istenmeyen programlar gelişmiş grubunu rapor et** - (varsayılan olarak kapalı): Casus yazılımların, yani doğrudan üreticiden alınan ve 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 yöntem kulan** - (varsayılan olarak açık): Görüntülenecek sayfanın içeriği bulussal analiz yöntemi kullanılarak taranır (*taranan nesnenin komutlarının sanal bir bilgisayar ortamında dinamik olarak canlandırılması*).
- **Kapsamlı taramayı etkinleştir** - (varsayılan olarak kapalı): Belirli durumlarda (*bilgisayarınıza bulaşma olmasından süpheleniyorsanız*) yalnızca emin olmak amacıyla 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.

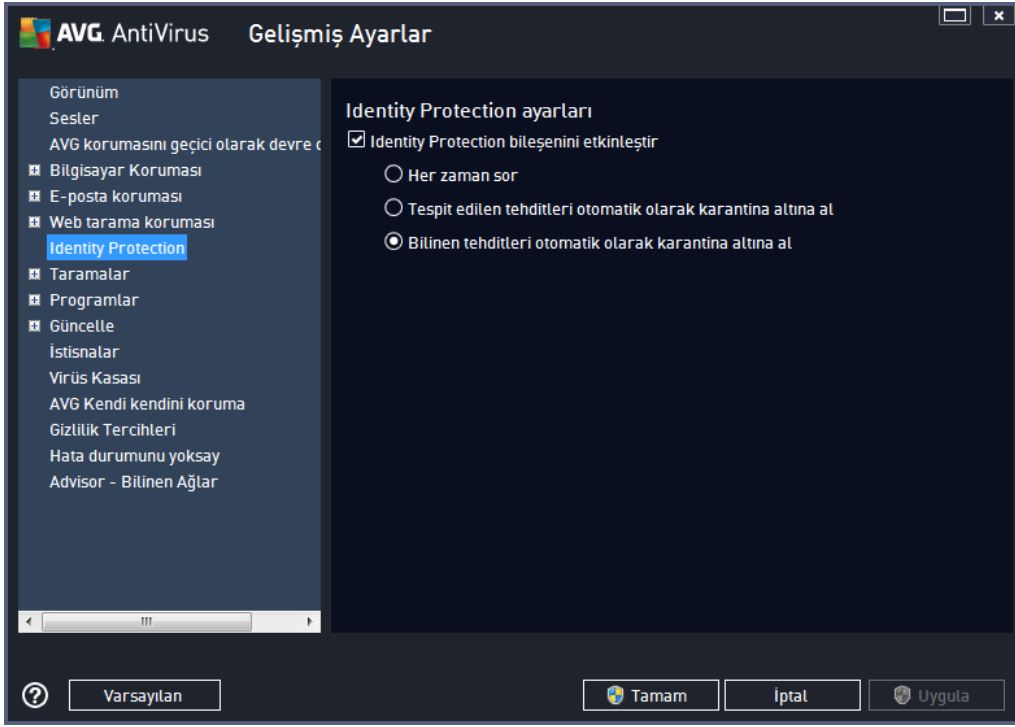
- o **İndirilen yürütülebilir dosyaları Yerlesik Kalkan ile tara** - (varsayılan olarak açık): Yürütülebilir dosyaları (*genellikle exe, bat, com uzantılı dosyalar*) indirilmelerinden ardından tarayın. Yerlesik kalkan bilgisayarınıza zararlı herhangi bir kodun ulaşmaması için dosyaları indirilmeden önce tarar. Ancak, bu tarama **Taranacak dosyanın maksimum parça boyutu** ile sınırlanmıştır (bu iletişim kutusunda bir sonraki ögeye bakın). Bu nedenle büyük dosyalar parça parça taranır ve yürütülebilir dosyaların çoğu da büyük dosyadır. Yürütülebilir dosyalar bilgisayarınızda pek çok görevi gerçekleştirebilir; bu nedenle bu dosyaların %100 güvenli olması hayati önemdedir. Bu güvenlik hem dosyanın indirilmeden önce parça parça taranmasıyla hem de indirme tamamlandıktan sonra bütün olarak taranmasıyla sağlanabilir. Bu seçeneği isretli bırakmanızı tavsiye ederiz. Bu seçeneği devre dışı bıraksanız bile, potansiyel olarak tehlikeli tüm kodlar AVG tarafından bulunacağı için rahat olabilirsiniz. Yalnızca genellikle yürütülebilir dosyayı bir bütün olarak değerlendiremeyeceği için bazı yanlış tespitler yapabilir.

İletişim kutusunun altındaki kaydırıcı **Taranacak maksimum dosya bölümü büyüklüğü**nü tanımlamanızı sağlar; dahil edilen dosyalar görüntülenen sayfada mevcutsa bunları bilgisayarınıza indirmeden önce de dosya 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, bulmuş olması halinde **Yerlesik Kalkan** tarafından tespit edilecektir.

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



Identity Protection bileşenini etkinleştir (varsayılan olarak açık) - **Identity** bileşenini kapatmak için işaretini kaldırın.

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 gerekir ve 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 gerekir ve 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:

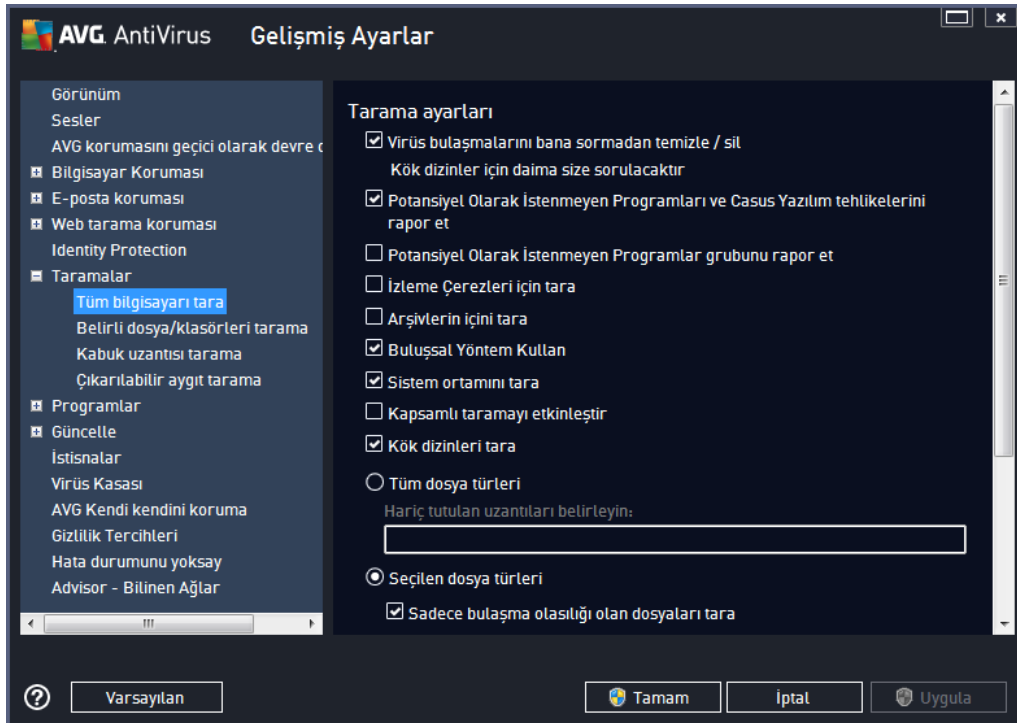
- **Tüm bilgisayarın taraması** - tüm bilgisayarın standart öntanımlı taramasıdır
- **Belirli dosya veya klasörleri tarama** - bilgisayarınızın seçilen alanlarının tarandığı standart

öntanımlı taramadır

- [Kabuk uzanti taraması](#) - seçilen nesnenin doğrudan Windows Gezgini ortamında taranması işlemidir
- [Çıkarılabilir aygıt taraması](#) - bilgisayarınıza bağlanan çıkarılabilir aygıtların taranması 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:

- **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 istenmeyen 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 istenmeyen programlar gelişmiş grubunu rapor et** (varsayılan olarak kapalı) - Casus yazılımların, yani doğrudan üreticiden alındığında 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 çerezlerin tespit edilmesi gerektiğini belirtir (*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 vb. arşiv dosyalarının içinde saklanan tüm dosyaları denetlemesi gerektiğini belirtir.
- **Bulussal yöntem kullan** (varsayılan olarak açık) - bulussal analiz (*taranan nesnenin yönergelerinin sanal bir bilgisayar ortamında dinamik olarak canlandırılması*) tarama sırasında kullanılacak virüs tespit 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 bulasma olmasından şüpheleniyorsanız*) 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.
- **Rootkit'leri tara** (varsayılan olarak açık) - [Anti-Rootkit](#) taraması bilgisayarınızı olası rootkit'lere, 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 noktalı 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 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 dehistirmemeniz önerilir. Uzantısı olmayan dosyalar şüpheli olabilir ve her zaman taranmalıdır.

Taramanın ne kadar hızlı tamamlanacağını ayarla

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

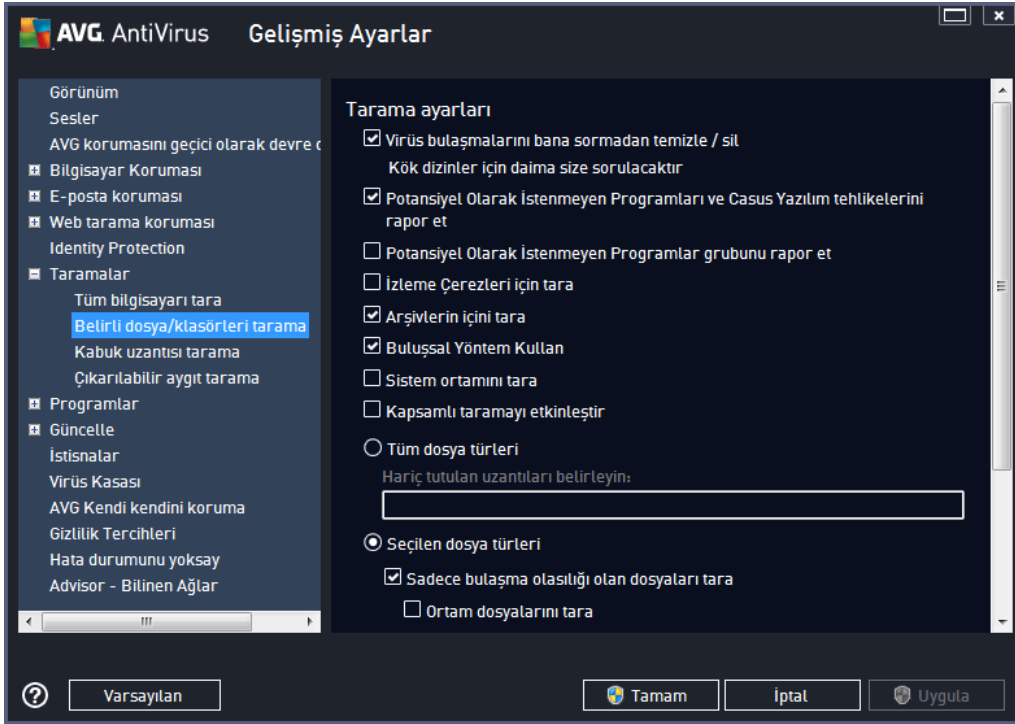
Ek tarama raporlarını ayarla...

Diğer 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 Bilgisayarı Tara](#) işlevinin düzenleme iletişim kutusu ile aynıdır. Tüm yapılandırma seçenekleri aynıdır; fakat [Tüm Bilgisayarı Tara](#) işlevinin varsayılan ayarları daha kesindir:

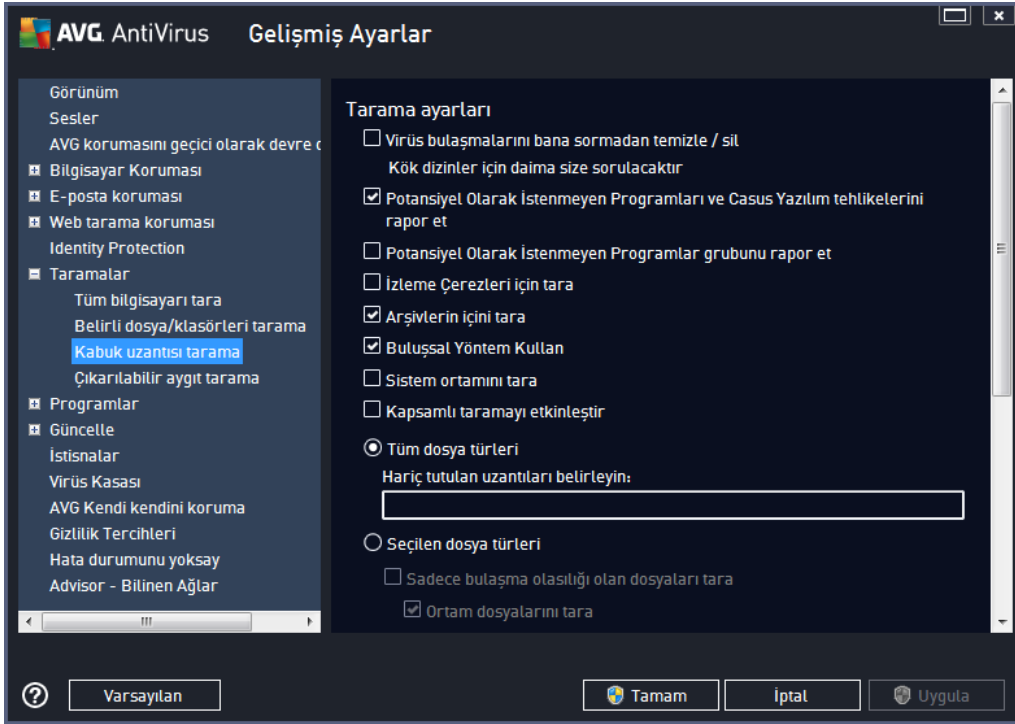


Bu yapılandırma iletişim kutusunda ayarlanan tüm parametreler [Belirli Dosyaları veya Klasörleri Tara](#) işlemi ile tarama sırasında seçilen alanlar için geçerlidir!

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

9.8.3. Kabuk Uzantısı Tarama

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



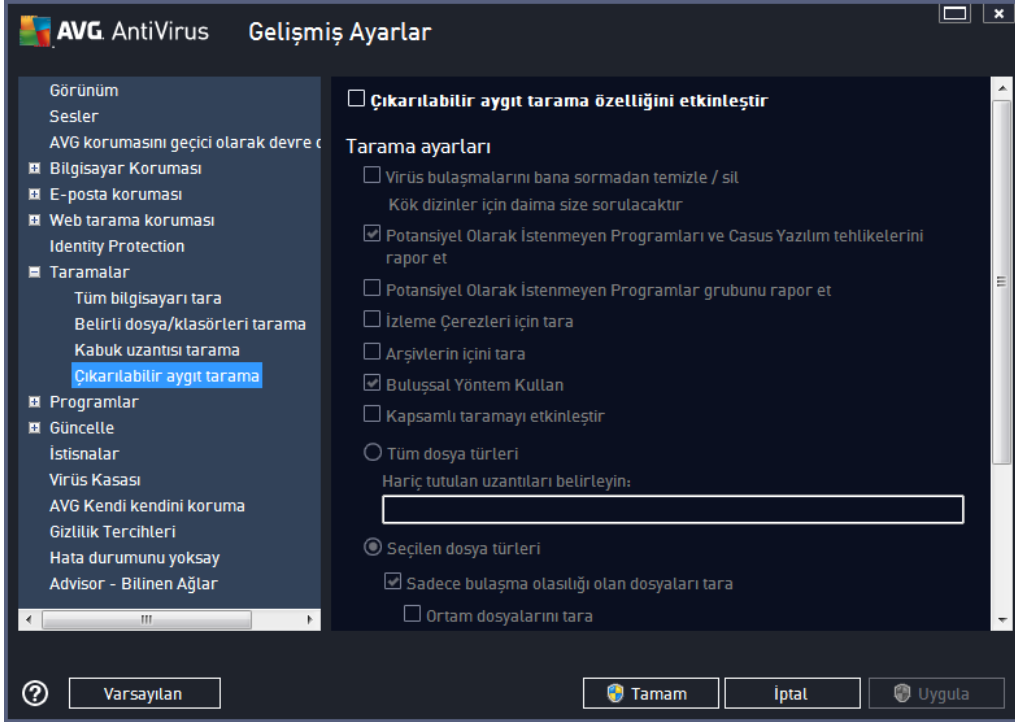
Parametre listesi, [Tüm Bilgisayarı Tara](#) ögesinin parametre listesi ile aynıdır. Bununla birlikte, varsayılan ayarlar farklılık gösterebilir (*örneğin, Tüm Bilgisayarı Tara işlevi arşivleri denetlemediği halde sistem ortamını denetler; Kabuk Uzantısı Tarama'da ise durum tam tersidir*).

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

[Tüm Bilgisayarı Tara](#) 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 sonucunun yalnızca tarama sırasında bir bulaşma tespit edilmesi durumunda görüntülenmesi gerektiğini de belirleyebilirsiniz.

9.8.4. Çıkarılabilir Aygıt Tarama

Çıkarılabilir Aygıt Tarama düzenleme arayüzü de [Tüm Bilgisayarı Tara](#) düzenleme iletişim kutusuna çok benzerdir:



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

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

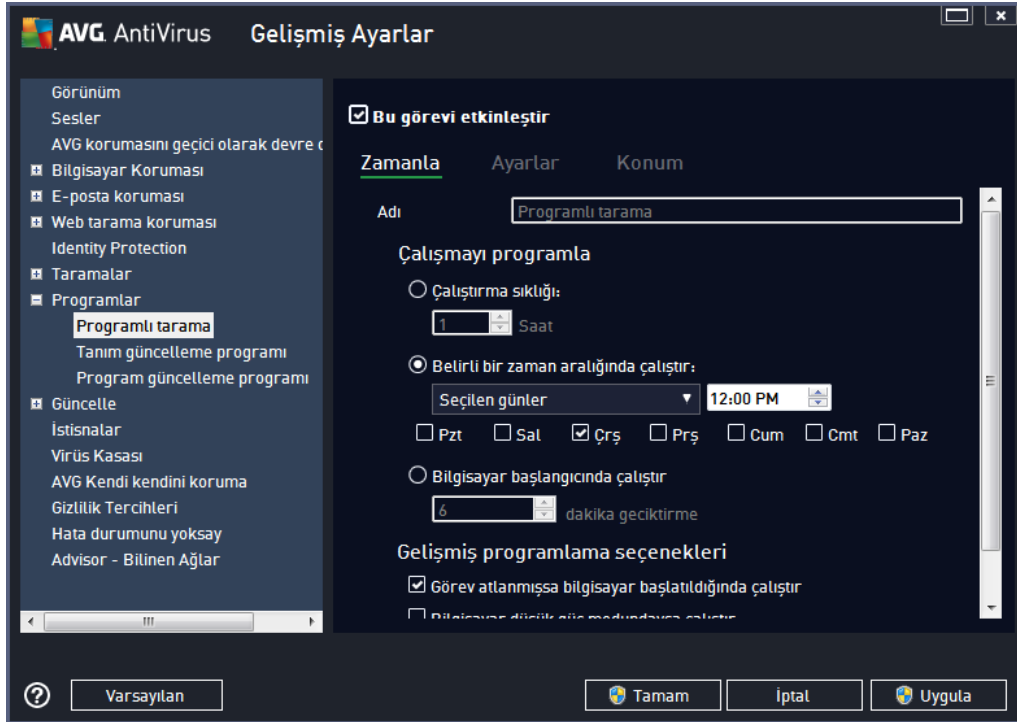
9.9. Programlar

Programlar bölümünde aşağıdaki bileşenlerin öntanımlı ayarlarını düzenleyebilirsiniz:

- [Programlanmış Tarama](#)
- [Tanım güncelleme programı](#)
- [Program Güncelleme Planı](#)

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

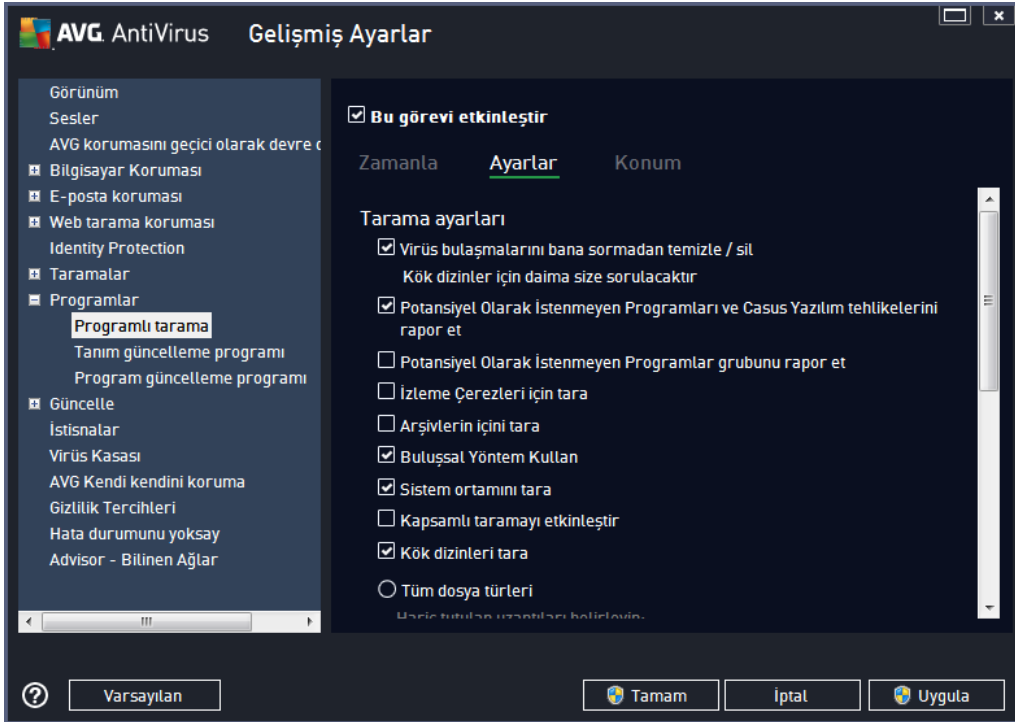
Burada, yeni programlanan tarama başlatması için zaman aralıkları belirtebilirsiniz. Zamanlama belirli bir sürenin ardından tekrarlanan tarama başlatması ile (**Her ...'de bir**) ya da kesin bir tarih ve saat tanımlayarak (**Belirli bir zaman aralığında çalıştır ...**), veya tarama başlangıcıyla ilgili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

- **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 istenmeyen 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 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 üreticiden alindiginda 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 kapalidir.
- **izleme çerezleri için tara** (varsayilan olarak kapali): Bu parametre tarama sirasinda çerezlerin tespit edilmesi gerektigini belirtir (*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 isleminde ZIP, RAR vb. bir arşiv ile saklanmış olsa bile tüm dosyaların taranması gerektigini belirtir.
- **Bulussal yöntem kullan** (varsayilan olarak açık): Bulussal analiz (*taranan nesnenin yönergelerinin sanal bir bilgisayar ortamında dinamik olarak canlandırılması*) tarama sirasinda kullanılacak virüs tespit yöntemlerinden biridir.
- **Sistem ortamini tara** (varsayilan olarak açık): 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

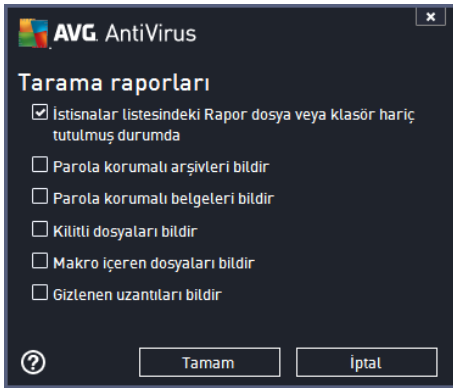
- **Tüm dosya türleri**, virgülle ayrılmış (*kaydedilirken virgüller noktalı virgüle dönüşür*) dosya uzantıları listesi sağlayarak taramadan hariç tutulacakların taranmaması için tanımlama seçeneği ile.
- **Seçili dosya türleri** - yalnızca virüs bulasabilme olasılığı olan dosyaları taramayı istediğinizi 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.
- İsteğe 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.

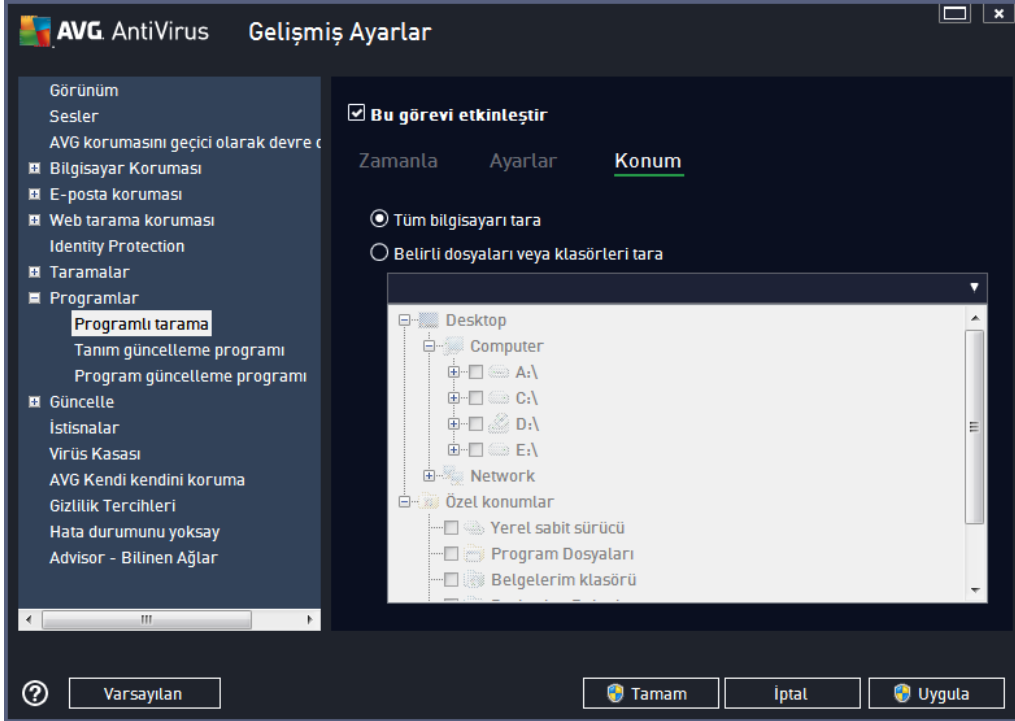
Ek tarama raporlarını ayarla

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

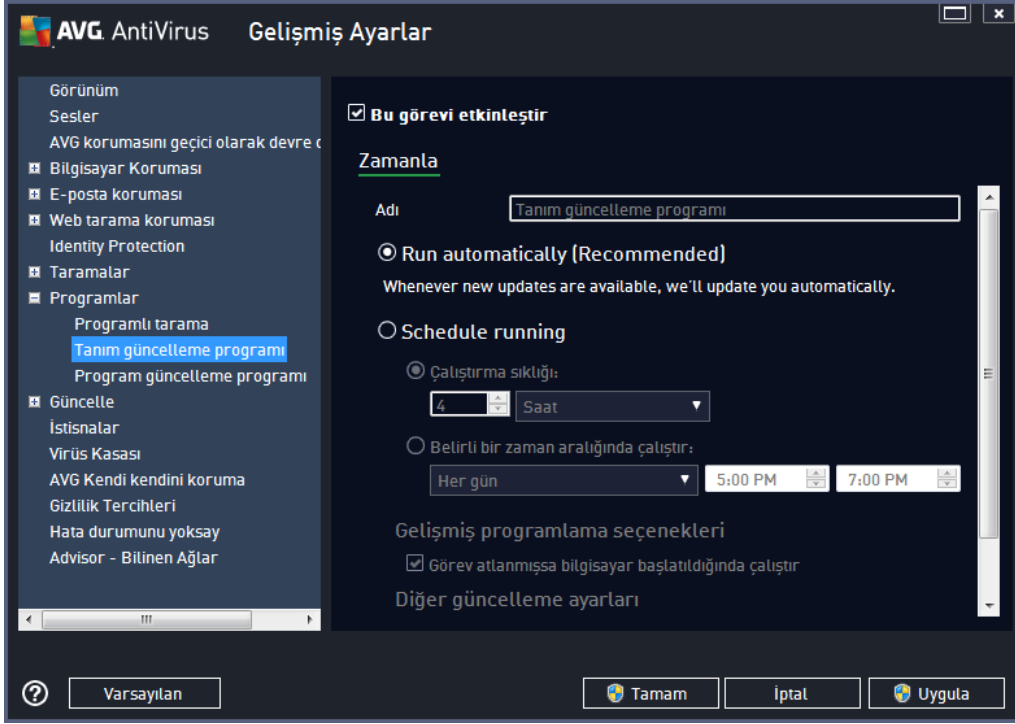
Bilgisayar kapatma seçenekleri bölümünde çalışan tarama işlemi bittiginde bilgisayarın otomatik olarak kapatılması gerekip gerekmediğine karar verebilirsiniz. Bu seçeneği seçerseniz (**Tarama bittikten sonra bilgisayarı kapat**) bilgisayar mevcut durumda kilitli olsa bile bilgisayarın kapatılmasını sağlayan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

Varsayılan olarak, yeni bir virüs tanım güncellenmesi yayınlanır yayınlanmaz görev otomatik olarak başlatılır (**Otomatik olarak çalıştır**). Değiştirmek için iyi bir nedeniniz yoksa bu yapılandırmayı muhafaza etmenizi tavsiye ederiz! Ardından, görev başlatmayı manuel olarak ayarlayabilir ve yeni programlanan tanım güncelleme başlatmaları için zaman aralıkları belirleyebilirsiniz. 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.

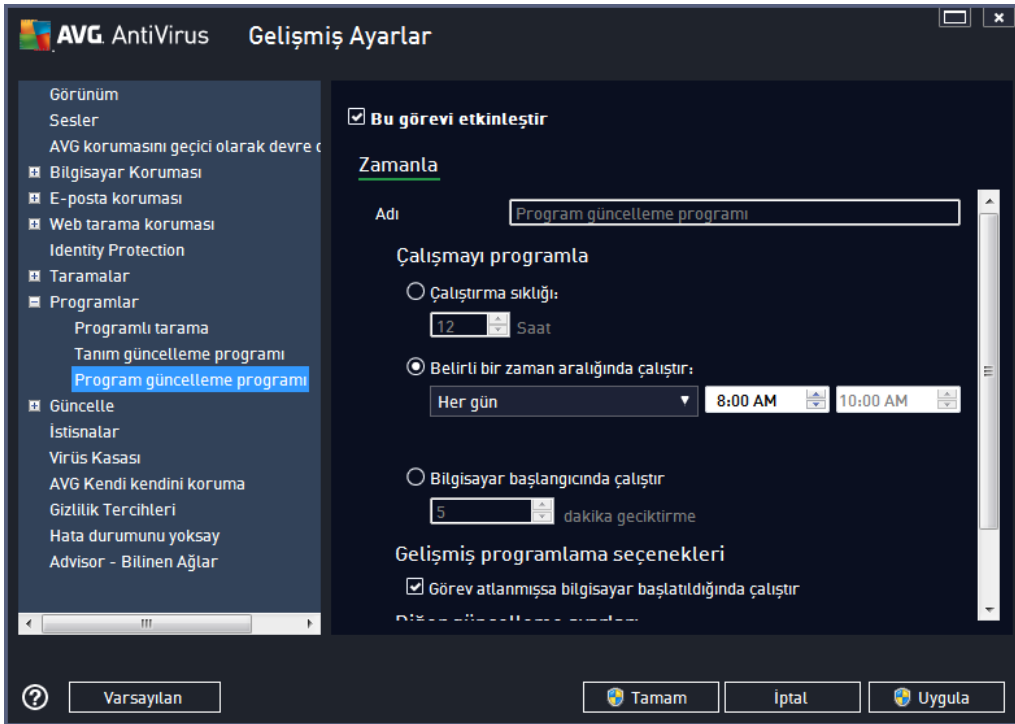
Diğer güncelleme ayarları

Son olarak, **İnternet bağlantısı kurulduğunda güncellemeyi yeniden çalıştır** seçeneğini

isaretleyerek 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.

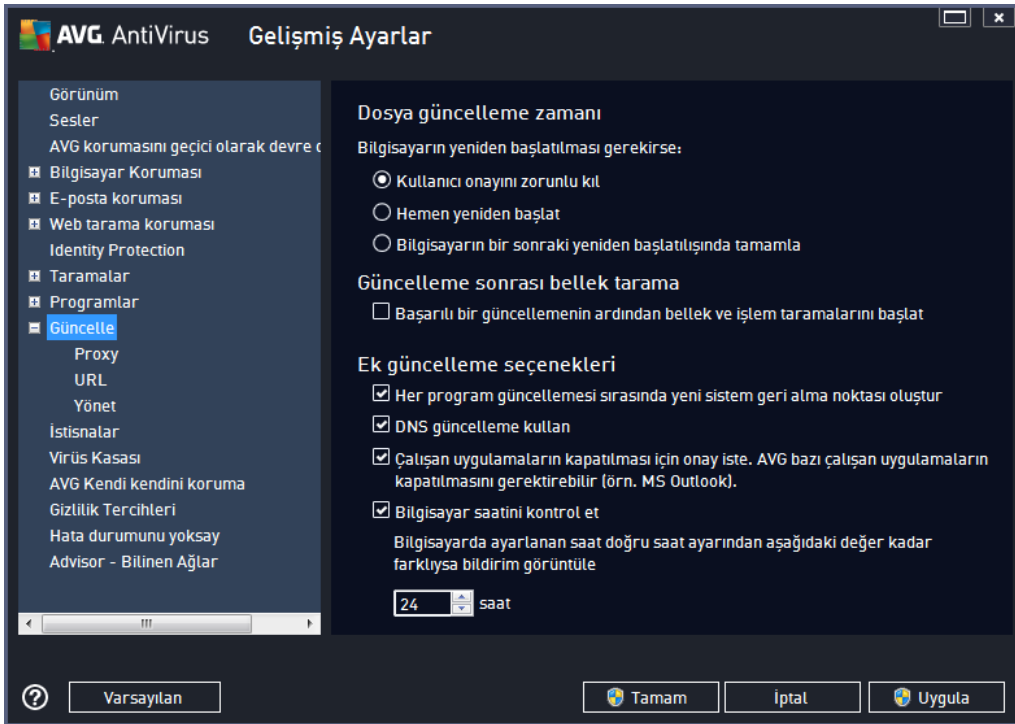
Diger gncelleme ayarları

Internet bağlantısı kurulduğunda gncellemeyi yeniden alistir seenegini isaretleyerek internet bağlantısı kesildiğinde ve gncelleme işlemi başarısız olduğunda, internet bağlantısı yeniden sağlanır sağlanmaz yeniden başlatılmasını sağlayın. Planlanan gncelleme 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: Zamanlaması önceden yapılmış bir program gncellemesi ile taramanın zamanlamalarının akışması durumunda gncelleme işlemi daha yüksek önceliğe sahiptir ve tarama işlemine ara verilir. Böyle bir durumda akışma hakkında bilgilendirilirsiniz.

9.10. Gncelleme

Gncelle navigasyonu ögesi, [AVG gncellemesine](#) ilişkin genel parametreleri belirleyebileceğiniz yeni bir iletişim kutusu açar:



Dosya gncelleme zamanı

Bu bölümde, gncelleme işlemi bilgisayarınızın yeniden başlatılmasını gerektiriyorsa, üç seenek arasından birini belirleyebilirsiniz. Güncellenenin tamamlanması işlemi, bilgisayarınızın bir sonraki yeniden başlatılma sürecine zamanlanabilir veya yeniden başlatma işlemi hemen yapılabilir:

- **Kullanıcıdan onay iste (varsayılan)** - [gncelleme işleminin](#) tamamlanması için gereken bilgisayarın yeniden başlatılması süreci için onayınız istenir

- **Hemen yeniden baslat** - [güncelleme islemi](#) tamamlanir tamamlanmaz onayiniz istenmeden bilgisayarınız yeniden baslatilacaktır
- **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!

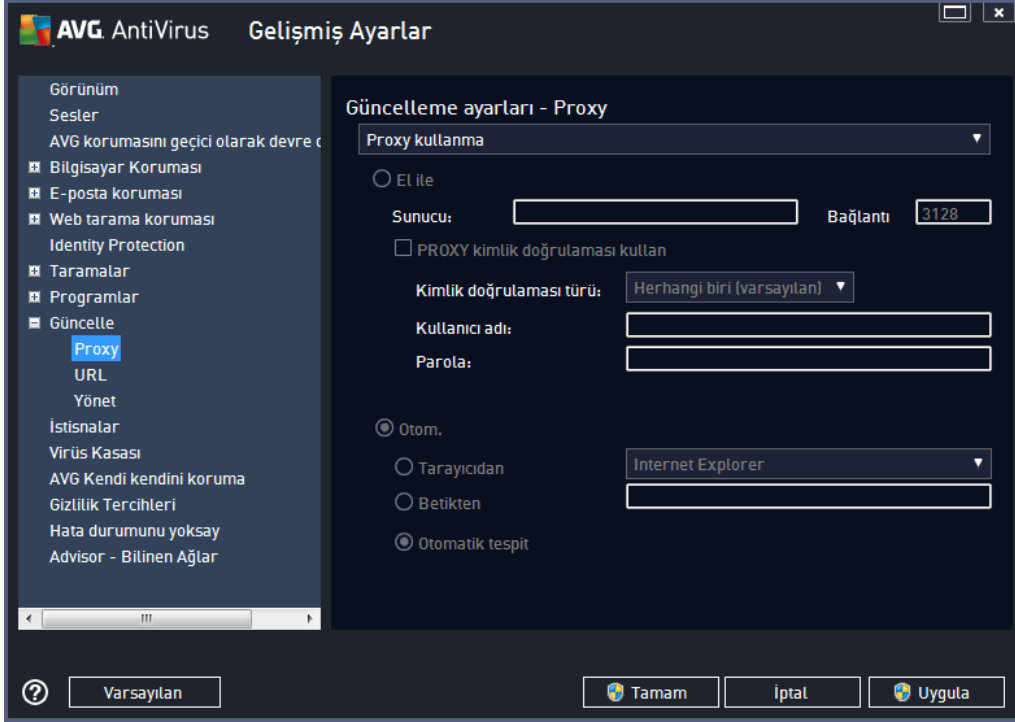
Güncelleme sonrası bellek tarama

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 güncellemesi sırasında yeni sistem geri alma noktası oluşturun** (varsayılan olarak açık) - her AVG program güncelleme islemi başlamadan önce bir sistem geri yükleme noktası oluşturulur. 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 erişebilirsiniz 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 baslatıldığında **AVG AntiVirus** 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) - o anda çalışmakta olan uygulamaların izniniz olmaksızın kapatılmamasını sağlar (gerekirse güncelleme isleminin sonlandırılması için).
- **Bilgisayar saatini kontrol et** (varsayılan olarak açık) - bilgisayar saati ile doğru saat arasındaki fark belirlenen süreden uzun olduğunda bilgilendirilmek istediginizi belirtmek için 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.

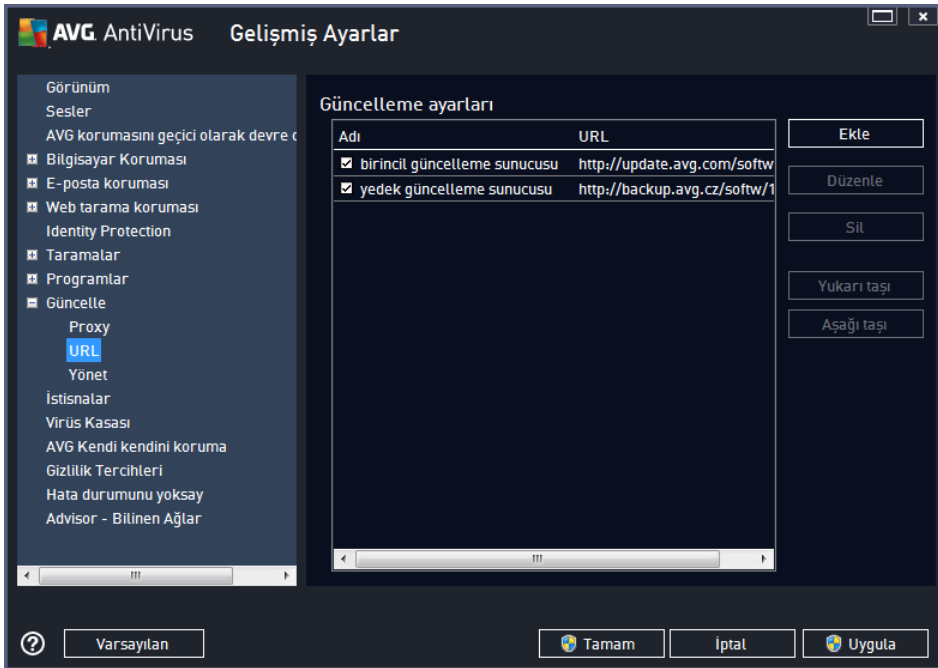
Otomatik yapılandırma

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

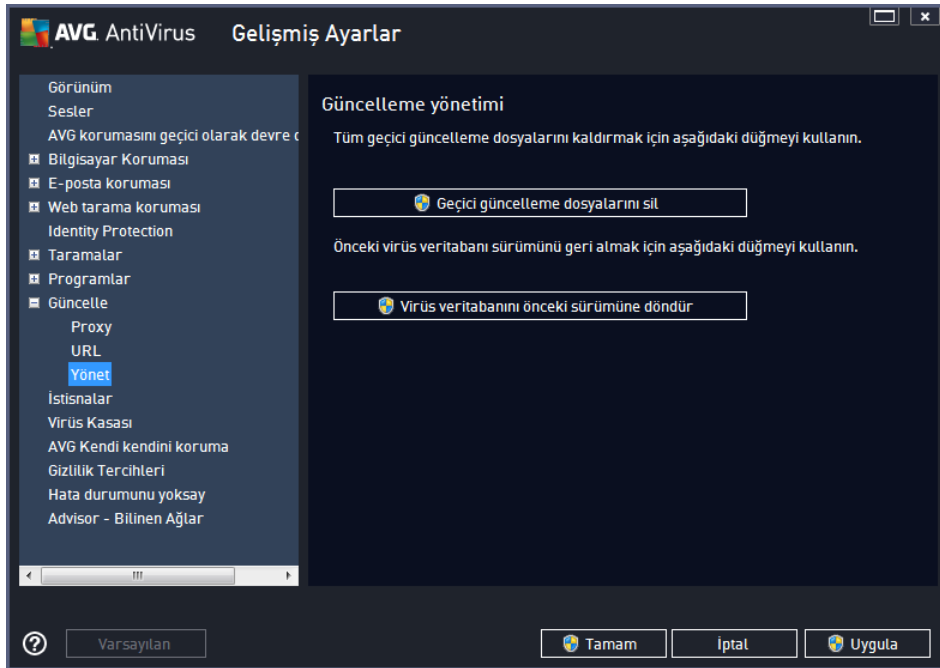
Liste ve liste öğeleri aşağıdaki kontrol düğmeleri kullanılarak düzenlenebilir:

- **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 vasıtasıyla erişilebilen iki seçenek sunmaktadır:

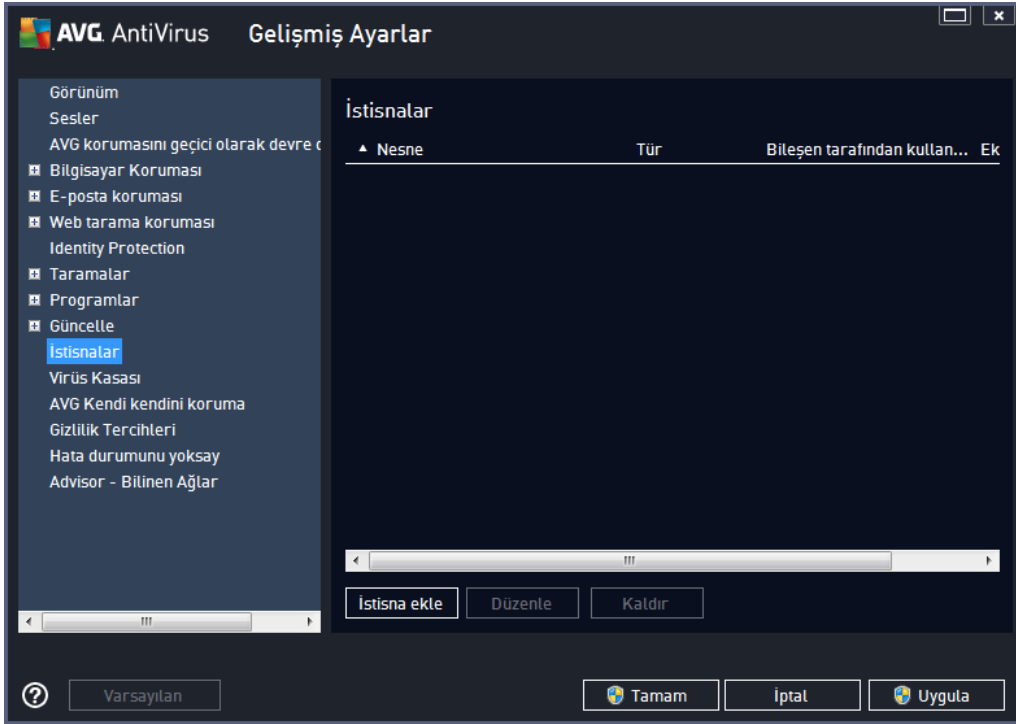


- **Geçici güncelleme dosyalarını sil** - tüm gereksiz güncelleme dosyalarını sabit diskinizden silmek için bu düğmeye basın (*varsayılan olarak söz konusu dosyalar 30 gün boyunca saklanır*)
- **Virüs veritabanını bir önceki sürüme döndür** - en güncel virüs veritabanını sabit diskinizden silmek ve daha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

9.11. İstisnalar

İstisnalar iletişim kutusunda istisnalar, yani **AVG AntiVirus** 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!

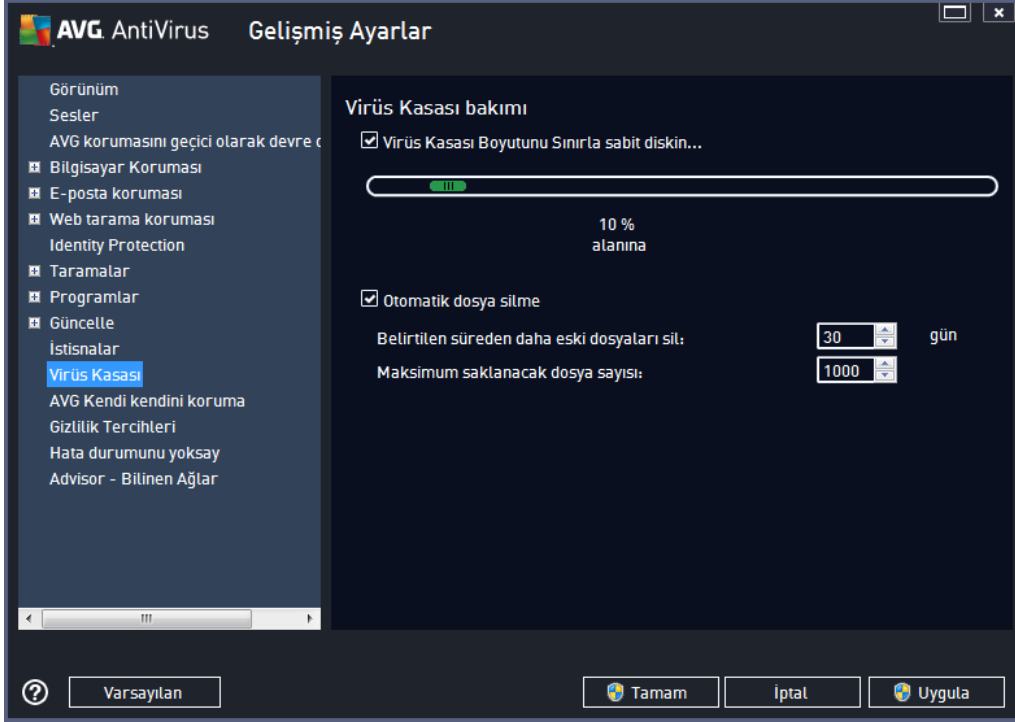


İletişim kutusundaki tabloda, daha önce tanımlanan istisnalar varsa, bunların bir listesi görüntülenir. Her öğenin yanında bir onay kutusu bulunur. Onay kutusu işaretliyse istisna etkindir. İşaretsizse, istisna tanımlanmıştır ancak simdiye kadar kullanılmamıştır. Sütun başlığını tıklayarak, izin verilen 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 bloğunu vurgulayıp tanımlanan istisnaları kaldırabilirsiniz. İstisna kaldırıldığında ilgili dosya, klasör veya URL AVG tarafından yeniden kontrol edilir. Dosya veya klasörün kendisi değil, yalnızca istisna kaldırılır!

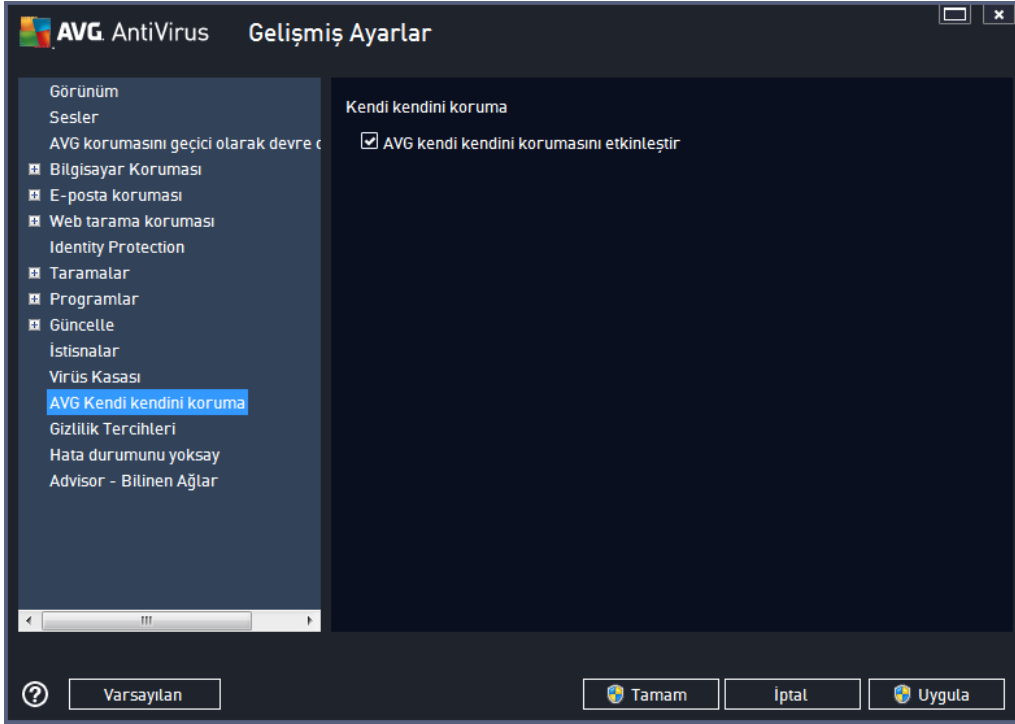
9.12. Virüs Kasası



Virüs Kasası Bakımı iletişim kutusu, [Virüs Kasası](#)'nda saklanan nesnelerin yönetimiyle ilgili çeşitli parametreleri tanımlayabilmenizi sağlar:

- **Virüs Kasası Boyutunu Sınırla** - [Virüs Kasası](#)'nin maksimum boyutunu ayarlamak için kaydırıcıyı kullanın. Bu boyut, sabit diskinizin boyutu ile orantili olarak belirlenir.
- **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

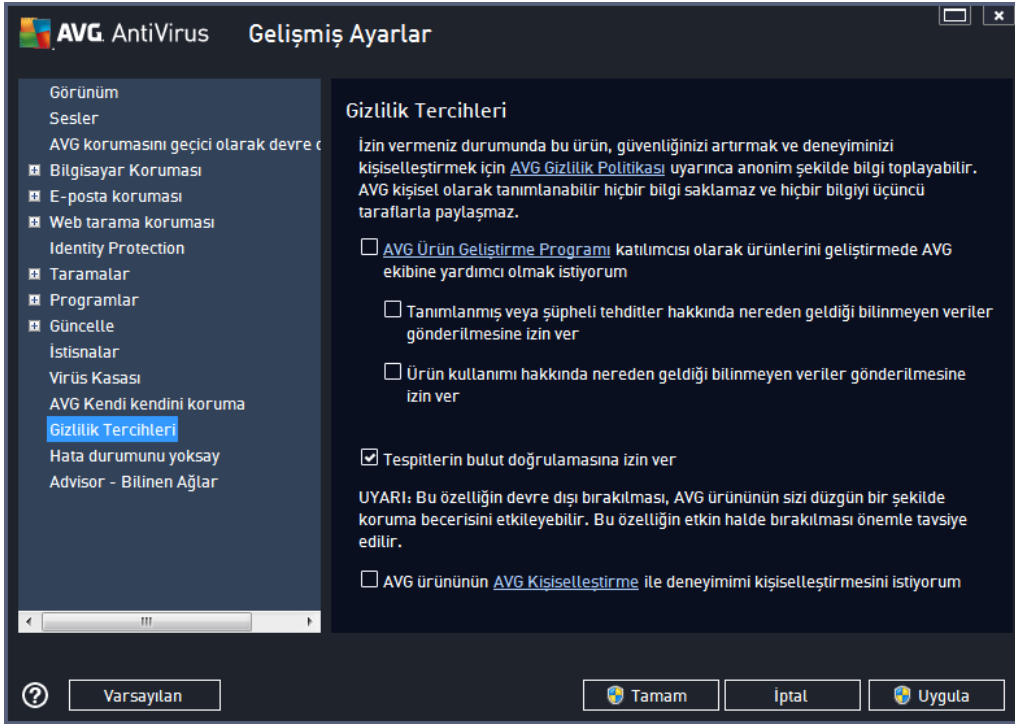


AVG Kendi Kendini Koruma, AVG AntiVirus yazılımının kendi işlem, dosya, kayıt defteri anahtarlarını ve sürücülerini değiştirilmekten ve devre dışı bırakılmaktan korur. Bu tür bir koruma sunmanın ana nedeni geliskin tehditlerin önce virüs koruma yazılımını devre dışı bırakıp ardından bilgisayarınıza kolayca 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 AntiVirus 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 tespit edilmeyen 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 tespit edilen virüs, casus yazılım veya erişmeye çalıştığınız kötü amaçlı web sitesi olabilir).
 - **Ürün kullanımı hakkında anonim bilgi gönderilmesine izin ver** (varsayılan olarak açık) - tespit 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 tespit edilen tehditler gerçekten virüs bulması içerip içermediklerinin belirlenmesi amacıyla denetlenir.

- **AVG Personalization özelliğini açarak AVG'nin deneyimini kişiselleştirmesini istiyorum** (varsayılan olarak kapalı) - 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:

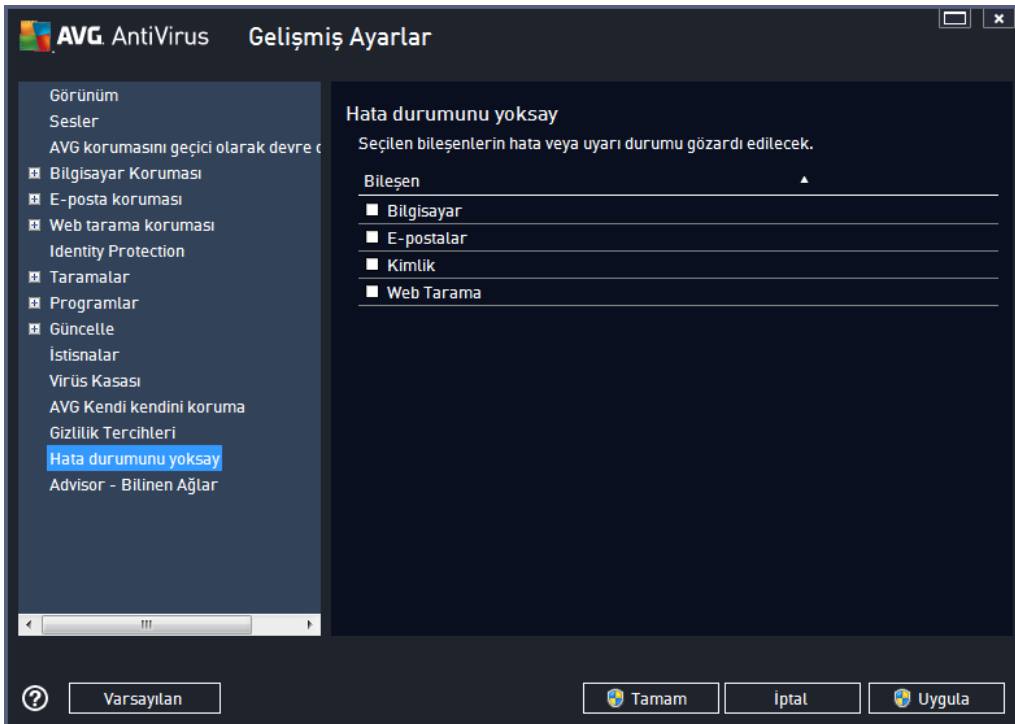
- **Virüs**, kendi kendini kopyalayan ve yayılan zararlı bir koddur ve genellikle zarar olusana kadar fark edilmez. Bazı virüsler ciddi bir tehdit oluşturur, dosyaları siler veya istediği şekilde değiştirir. Bazı virüsler ise görünüşte zararsız olan müzik çalma gibi işlemler yapar. Ancak, tüm virüsler 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, "tasiyici" 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 zararlı kategorisinde (*zararlı 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 AntiVirus 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 tepsi 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

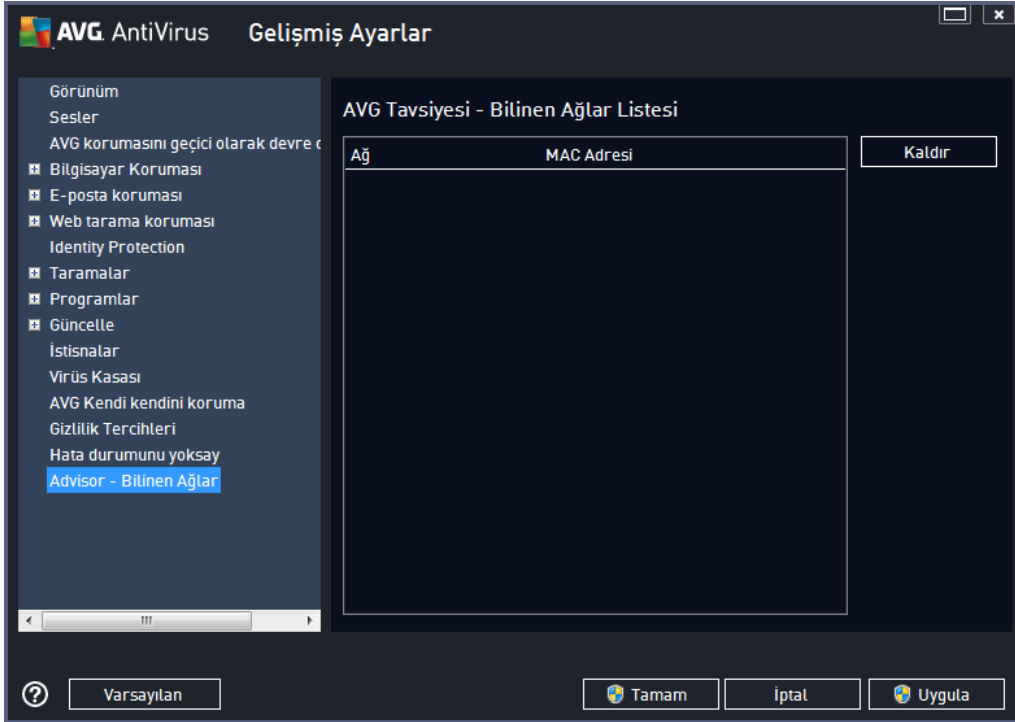
Belirli bir nedenle bileşenlerden birini geçici olarak kapatmanız gereken bir durum olabilir. **Bu önerilmez, tüm bileşenleri sürekli olarak açık ve varsayılan yapılandırılmada tutmanız gerekir**, ancak böyle bir durum meydana gelebilir. Bu durumda sistem tepsi simgesi, otomatik olarak bileşenin hata durumunda olduğunu bildirir. Ancak bu durumda gerçek bir hatadan söz edemeyiz çünkü hatayı siz baslatmışsınız 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.

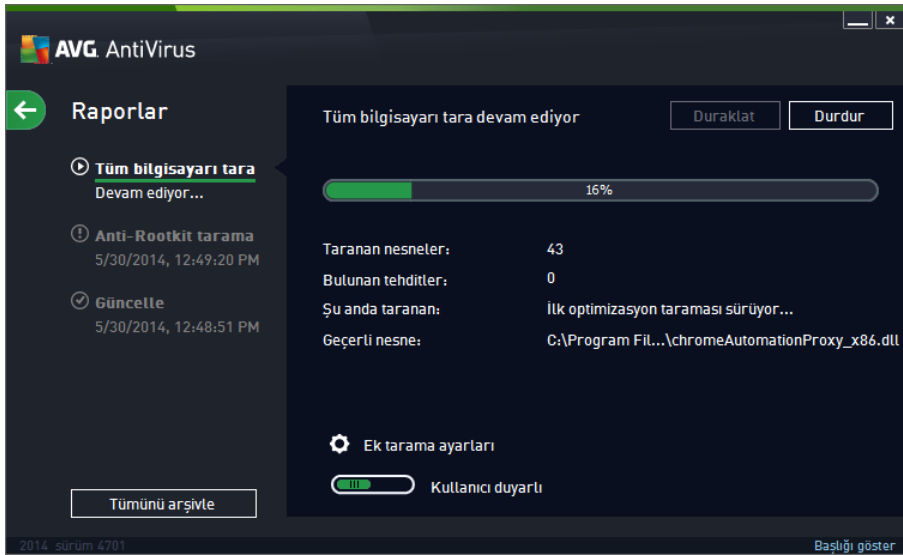
10. AVG Tarama

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

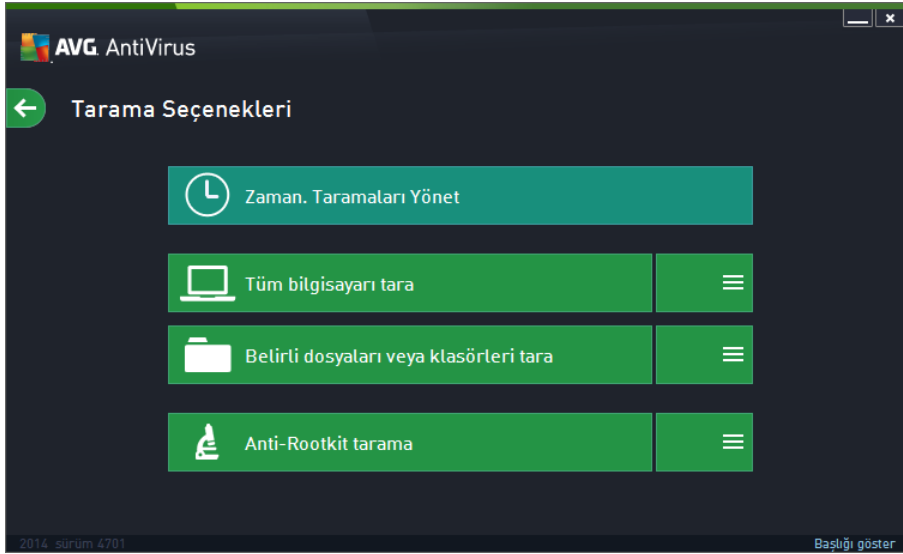
AVG tarama arayüzüne [ana kullanıcı arayüzünden](#) grafik olarak iki bölüme ayrılmış düğme

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 taranmasını hemen başlatmak için *Tüm bilgisayarı tara* seçeneğini tıklayın (*tüm bilgisayar taramasıyla ilgili ayrıntılar için lütfen [Öntanımlı taramalar / Tüm bilgisayarı tara](#) başlıklı bölüme bakın*). *Ayarlar* bölümünü tıklarsanız [tüm bilgisayarı tarama işleminin yapılandırma iletişim kutusunu](#) açarsınız.
- **Belirli dosyaları veya klasörleri tara / Ayarlar** - Bu düğme de iki kısma ayrılmıştır. Bilgisayarınızda seçtiğiniz alanların taranmasını hemen başlatmak için *Belirli dosyaları veya klasörleri tara* seçeneğini tıklayın (*belirli dosya ve klasörlerin taranmasıyla ilgili ayrıntılar için lütfen [Öntanımlı taramalar / Belirli dosyaları veya klasörleri tara](#) başlıklı bölüme bakın*). *Ayarlar* bölümünü tıklarsanız [belirli dosyaları veya klasörleri tarama işleminin yapılandırma iletişim kutusunu](#) açarsınız.
- **Bilgisayarda rootkit'leri tara / Ayarlar** - Düğmenin *Bilgisayarda rootkit'leri tara* olarak etiketlenen soldaki bölümü hemen anti-rootkit taramasını başlatır (*rootkit taraması hakkındaki ayrıntılar için lütfen [Öntanımlı Taramalar / Bilgisayarda rootkit'leri tara](#) adlı ilgili bölüme bakın*). *Ayarlar* bölümünü tıklarsanız [rootkit taramasının yapılandırma iletişim kutusunu](#) açarsınız.

10.1. Öntanımlı Taramalar

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

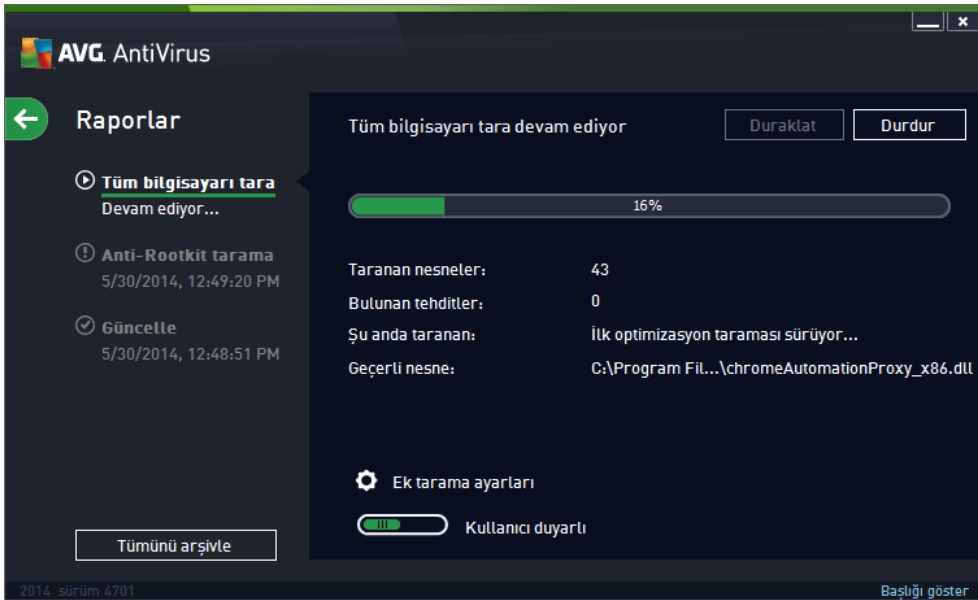
AVG AntiVirus içinde, yazılım satıcısının önceden tanımladığı aşağıdaki tarama türlerini bulacaksınız:

10.1.1. 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 tasiyacaktır. Bilgisayarın tümü haftada en az bir defa taranmalıdır.

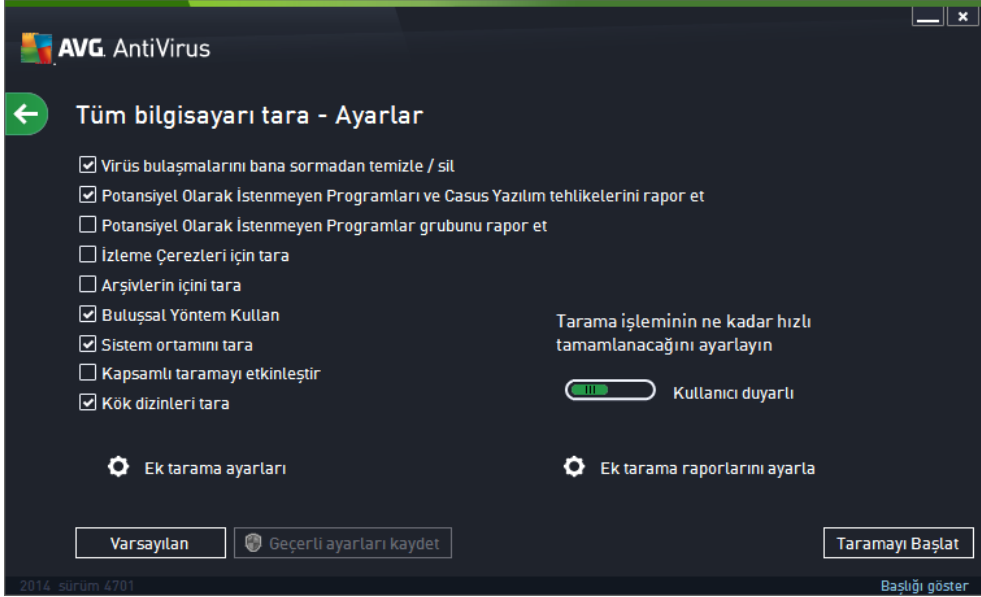
Tarama başlatma

Tüm bilgisayarı tara işlemi doğrudan [ana kullanıcı arayüzünden](#) **Simdi 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 uğratılabilir (**Duraklat**) ya da iptal edilebilir (**Durdur**).



Tarama yapılandırması düzenleme

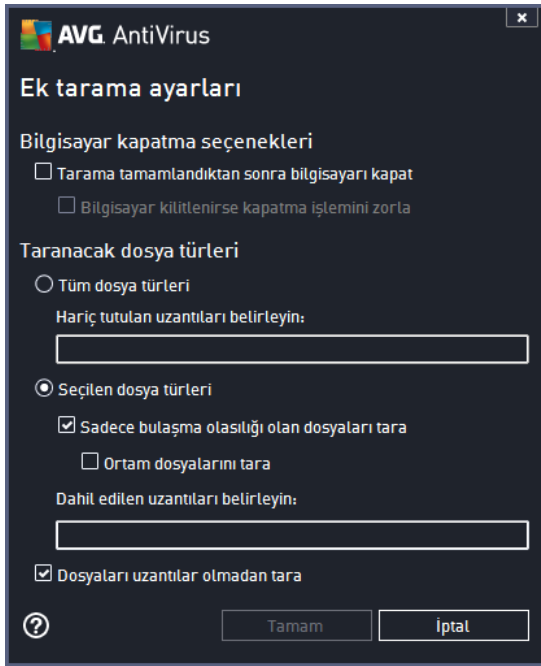
Tüm bilgisayarı tara yapılandırmasını **Tüm bilgisayarı tara - Ayarlar** iletişim kutusunda düzenleyebilirsiniz (*iletişim kutusuna [Tarama seçenekleri](#) iletişim kutusundaki Tüm bilgisayarı tara işleminin Ayarlar bağlantısından erişilebilir*). **Değiştirmek için geçerli bir nedeniniz olmadığı müddetçe 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 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 olusturmasına 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.
- **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).
- **Arşivleri tara** (varsayılan olarak kapalı) - 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.
- **Rootkit'leri tara** (varsayilan olarak açık): tüm bilgisayar taramasına anti-rootkit taramasını dahil eder. [Anti-rootkit taraması](#) ayrı olarak da başlatılabilir.
- **Ek tarama ayarları** - bağlantı, şu parametreleri belirtebileceğiniz yeni bir Ek tarama ayarları iletişim kutusu açar:



- **Bilgisayar kapatma seçenekleri** - Çalışan tarama işlemi bittiginde bilgisayarın otomatik olarak kapatılması gerekir gerekmedigine karar verir. Bu seçeneği seçerseniz (**Tarama bittikten sonra bilgisayarı kapat**) bilgisayar mevcut durumda kilitleli olsa bile bilgisayarın kapatılmasını sağlayan bir seçeneğin bulunduğu bir pencere açılacaktır (**Bilgisayar kilitletirse 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.

➤ Isteğe 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 süpheli 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 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 edileceğini seçebilirsiniz:



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

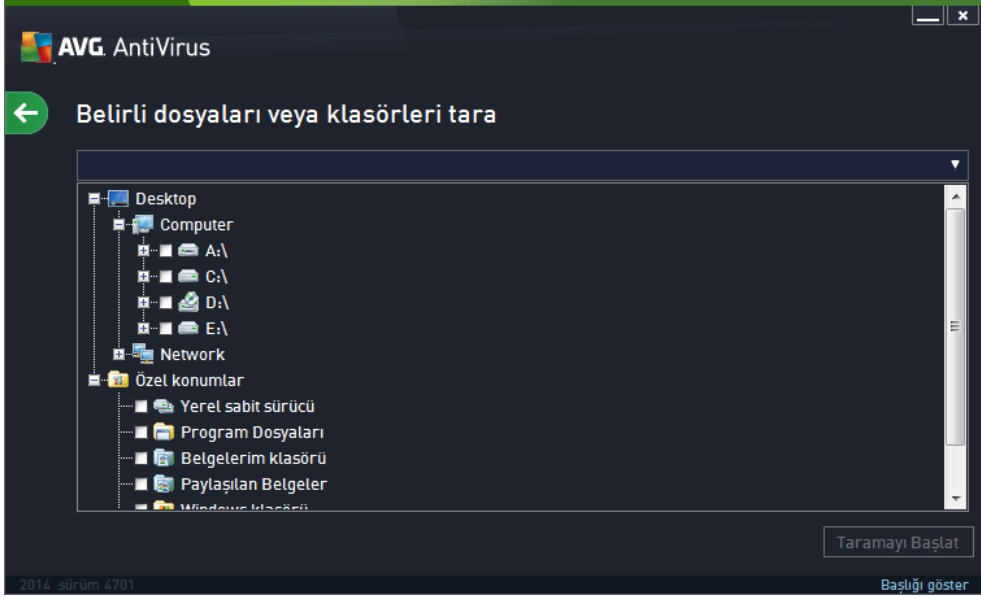
10.1.2. Belirli dosyaları veya klasörleri tara

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

Tarama başlatma

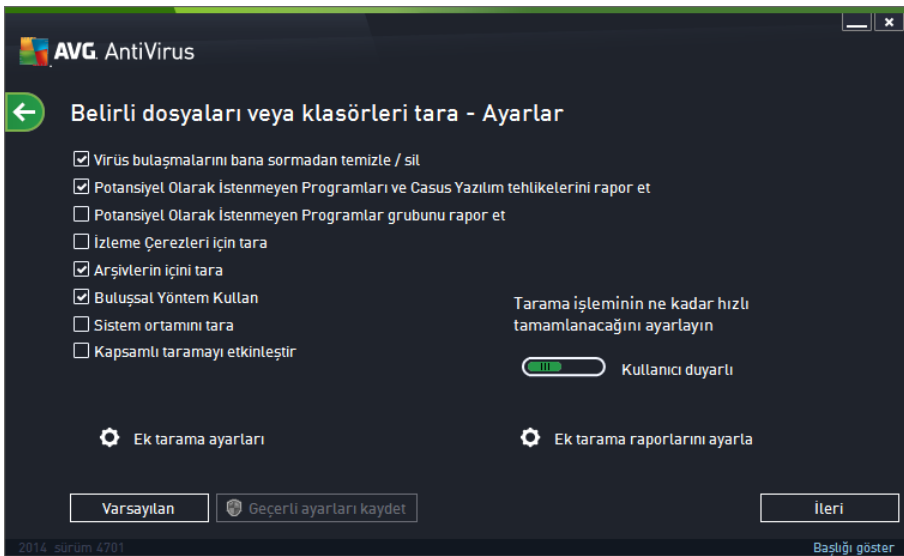
Belirli dosyaları veya klasörleri tara işlemi doğrudan [Tarama seçenekleri](#) iletişim kutusundaki **Belirli dosyaları veya klasörleri tara** düğmesi tıklanarak başlatılabilir. Yeni bir **Tarama için belirli dosya ve klasörleri seçin** iletişim kutusu açılır. Bilgisayarınızın ağaç görünümünden taranmasını istediğiniz klasörleri seçin. Seçilen klasörlerin her birine giden yol, otomatik olarak oluşturulacak ve iletişim kutusunun üst kısmındaki metin alanında görüntülenecektir. Belirli bir klasör taranırken içinde bulunan klasörlerin taranmaması gibi bir seçenek de vardır. Bunu yapabilmek için otomatik olarak oluşturulan yolun başına "-" isareti 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!**

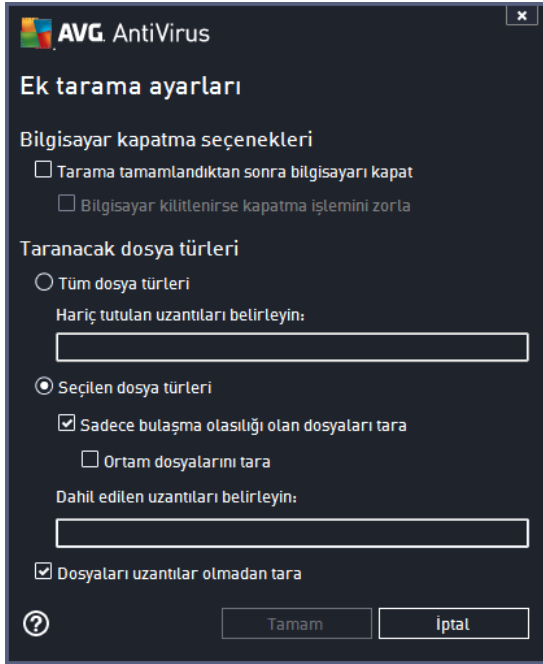


Tarama parametreleri listesinde parametreleri ihtiyaçlarınıza uygun olarak açabilir / kapatabilirsiniz:

- **Bulasmayı bana sormadan temizle / kaldır** (varsayılan olarak açılı): 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 yani sira 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.
- **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.
- **Kapsamlı 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 işaretleyebilirsiniz. Ancak, bu yöntemin çok fazla zaman aldığını unutmayın.
- **Ek tarama ayarları** - Bağlantı, su parametreleri belirtebileceğiniz yeni bir **Ek tarama ayarları** iletişim kutusu açar:



- **Bilgisayar kapatma seçenekleri** - Çalışan tarama işlemi bittiginde 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 süpheli 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 işlemini 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:



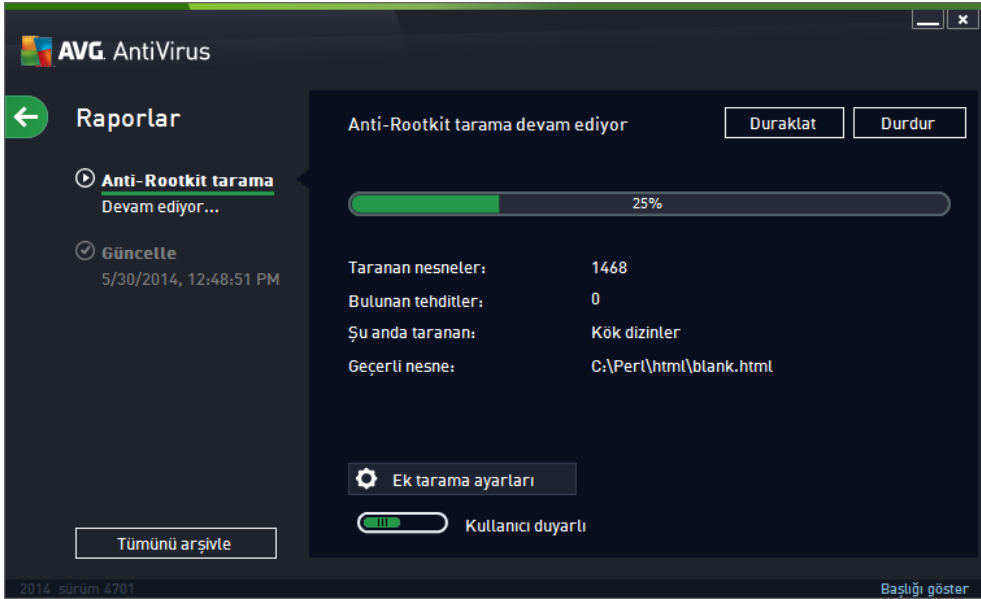
Uyarı: Bu tarama parametreleri, yeni tanımlanan taramanın parametreleri ile aynıdır - [AVG Taraması / Tarama zamanlama / Tarama Tipi](#) bölümünde açıklandığı doğrultuda. **Belirli dosya veya klasörleri tara** fonksiyonunun varsayılan yapılandırmasını değiştirmeye karar vererseniz yeni ayarlarınızı,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

10.1.3. Bilgisayarda rootkit'leri tara

Bilgisayarda rootkit'leri tara tehlikeli rootkit'leri, diğer bir deyişle bilgisayarınızdaki tehlikeli yazılımların varlığını gizleyen program ve teknolojileri tespit edip etkili bir biçimde silen özel bir araçtır. Rootkit, bir bilgisayar sisteminin kontrolünü, sistem sahiplerinin ve yasal yöneticilerinin izni olmaksızın ele geçirmek için tasarlanmış bir programdır. Tarama işlemi öntanımlı bir kurallar setine göre rootkit'leri tespit edebilir. Bir rootkit bulunması kesin olarak bir bulasma olduğu anlamına gelmez. Rootkit'ler bazen sürücülerde kullanılır ya da doğru uygulamaların bir parçası olabilir.

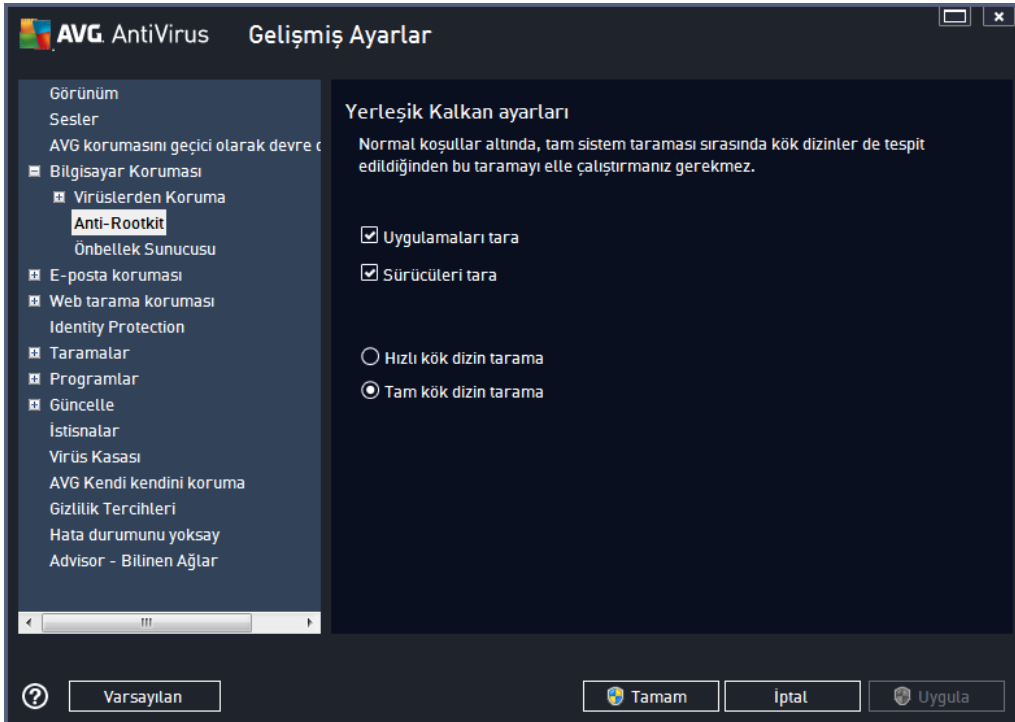
Tarama başlatma

Bilgisayarda rootkit'leri tara işlemi [Tarama seçenekleri](#) iletişim kutusunda **Bilgisayarda rootkit'leri tara** düğmesine basılarak doğrudan başlatılabilir. **Anti-rootkit taraması devam ediyor** adlı yeni bir iletişim kutusu açılarak başlatılan taramanın ilerlemesini gösterir:



Tarama yapılandırması düzenleme

Anti-Rootkit tarama yapılandırmasını **Anti-Rootkit Ayarları** iletişim kutusunda düzenleyebilirsiniz (iletilim kutusuna [Tarama seçenekleri](#) iletişim kutusundaki *Bilgisayarı rootkit'lere karşı tara* işleminin *Ayarlar bağlantısından erişilebilir*). **Değiştirmek için geçerli bir nedeniniz olmadığı müddetçe varsayılan ayarları korumanız önerilir!**



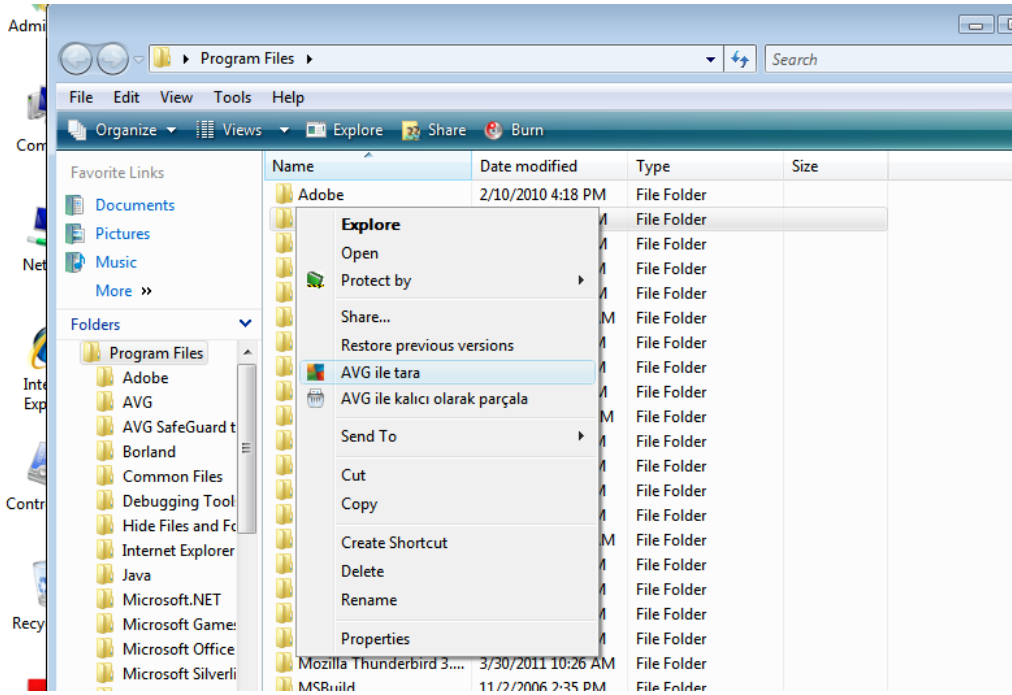
Tarama uygulamaları ve Tarama sürücülerini anti-rootkit taramasına nelerin dahil edileceğini ayrıntılı

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) tarama
- **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) tarama

10.2. Windows Gezgini'nde Tarama

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



- Windows Gezgini'nde taramak istediğiniz dosyayı (ya da klasörü) seçin
- Bağlam menüsünü açmak için nesneye fare ile sağ tıklayın
- **AVG ile Tara** seçeneğini seçerek dosyanın AVG tarafından taramasını sağlayın **AVG AntiVirus**

10.3. Komut Satırı Tarama

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



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

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

Komut sözdizimi

Komut söz dizimi aşağıdaki gibidir:

- **Tam bilgisayar taraması yapılırken avgscanx /parametre ...** Örn. **avgscanx /comp**
- **avgscanx /parameter /parameter ..** Birden fazla parametre kullanıldığı zaman bunlar bir sıra halinde dizilmeli ve bir boşluğun 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 satırı parametrelerine genel bakış](#) 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 satırı taramasını grafik kullanıcı arayüzünden başlatma seçeneğiniz de bulunmaktadır. Taramanın kendisi komut satırından başlatılacaktır, **Komut Satırı Olusturucu** iletişim kutusu, en yaygın tarama parametrelerini konforlu grafik arayüzünde görüntüler.

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

10.3.1. CMD Tarama Parametreleri

Komut satırı taramada kullanılacak parametrelerin listesi:

- **/SCAN** [Belirli dosya ya da klasörleri tara](#) /SCAN=yol;yol (örn. /SCAN=C:\;D:\)
- **/COMP** [Tüm bilgisayarı 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 Arşivleri tara
- /CLEAN Otomatik olarak temizle
- /TRASH Bulanan dosyalari [Virüs Kasası](#)
- /QT Hızlı test
- /LOG Bir tarama sonucu dosyasi oluşturun
- /MACROW Makrolari rapor et
- /PWDW Parola ile korunan dosyalari rapor et
- /ARCBOMBSW Arşiv bombalarını rapor et (*tekrar tekrar sıkıştırılan arşivler*)
- /IGNLOCKED Kilitli dosyalari yoksay
- /REPORT Dosyaya /dosya adına/ rapor et
- /REPAPPEND Rapor dosyasına ekle
- /REPOK Bulanmamış dosyalari Tamam olarak rapor et
- /NOBREAK CTRL-BREAK ile islemin kesilmesine izin verme
- /BOOT MBR/BOOT kontrolünü etkinleştir
- /PROC Aktif işlemleri tara
- /PUP Potansiyel olarak istenmeyen programlari rapor et
- /PUPEXT Potansiyel olarak istenmeyen programlar grubunu rapor et
- /REG Kayıt defterini tara
- /COO Çerezleri tara
- /? Bu konuyla ilgili yardımı görüntüle
- /HELP Bu konuyla ilgili yardımı görüntüle
- /PRIORITY Tarama önceliğini belirle /Düşük, Orta, Yüksek/ (bkz. [Gelişmiş ayarlar](#) /

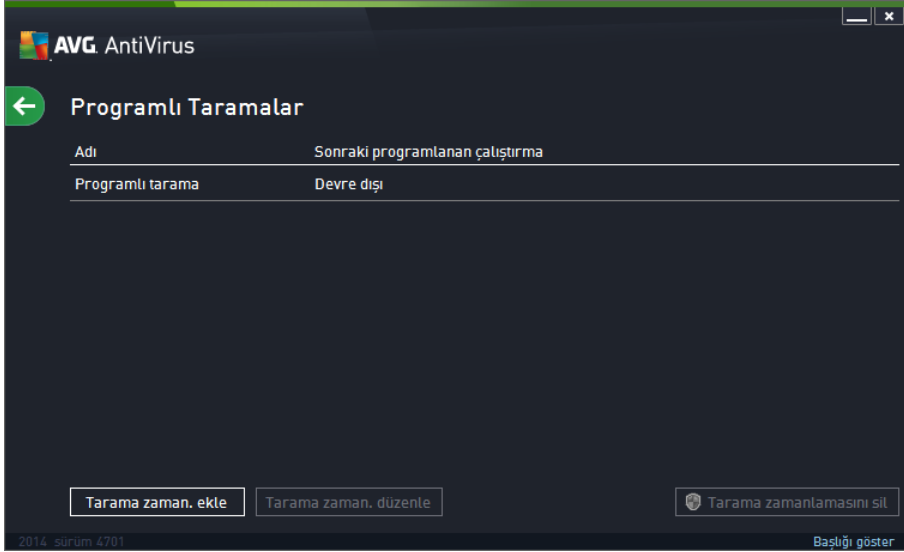
Taramalar)

- /SHUTDOWN Tarama tamamlandıktan sonra bilgisayarı kapat
- /FORCESHUTDOWN Tarama tamamlandıktan sonra bilgisayarı kapatmayı zorla
- /ADS Alternatif Veri Akislerini Tara (*yalnızca NTFS*)
- /HIDDEN Gizli uzantılı dosyaları rapor et
- /INFECTABLEONLY Yalnızca bulaşabilir uzantıya sahip dosyaları tara
- /THOROUGHSCAN Kapsamlı taramayı etkinleştir
- /CLOUDCHECK Hatalı tespitler açısından denetle
- /ARCBOMBSW Yeniden sıkıştırılmış arşiv dosyalarını rapor et

10.4. Tarama Programlama


AVG AntiVirus ile isteginiz doğrultusunda tarama yapmanın (*örneğin bilgisayarınıza virüs bulduğundan şüphelenirseniz*) yani sıra zamanlanan bir plan doğrultusunda da tarama yapabilirsiniz. Taramaların bir program doğrultusunda yapılması önerilmektedir: bu şekilde, bilgisayarınızın virüs bulaşması ihtimaline karşı korunduğundan emin olursunuz ve ne zaman tarama yapmanız gerektiği konusunda endişelenmenize gerek kalmaz. [Tüm bilgisayar taraması](#) işlemini en az haftada bir kez düzenli olarak başlatmanız gerekir. Diğer yandan, yapabiliyorsanız programlı taramanın varsayılan yapılandırmasında ayarlandığı gibi tüm bilgisayar taramasını günlük olarak yapın. Bilgisayarınız "daima açık" ise taramaları çalışma saatlerinden sonra gerçekleştirilecek şekilde programlayabilirsiniz. Bilgisayarınızı arada sırada kapatıyorsanız taramayı, taramaları [görev yerine getirilemediğinde bilgisayarın başlaması ile başlat](#) şeklinde programlayın.

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:

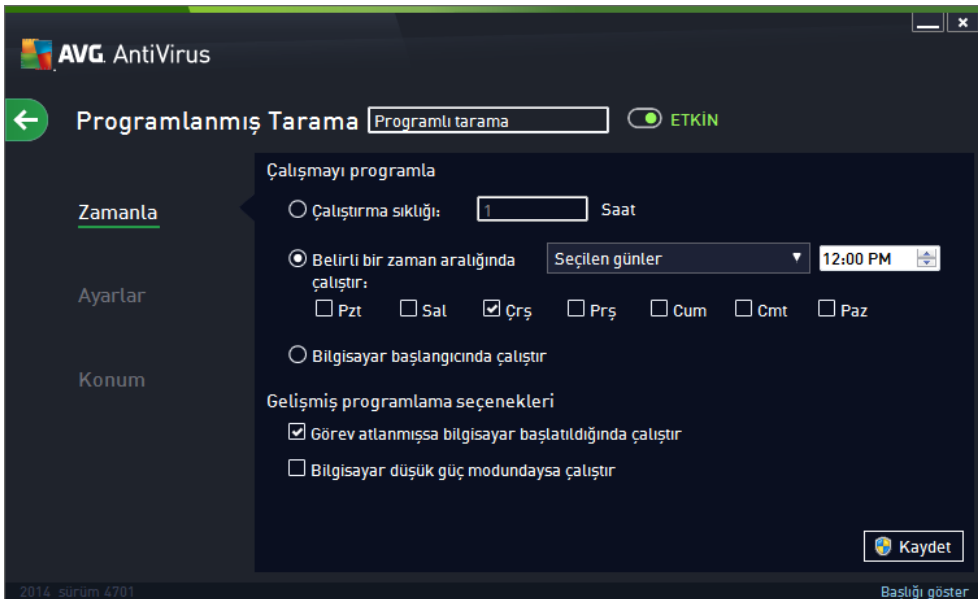


İletişim kutusunda kendi taramalarınızı belirleyebilirsiniz. Kendi istediğiniz yeni bir tarama zamanlaması oluşturmak için **Tarama zamanlaması ekle** düğmesini tıklatın. Planlanan tarama parametreleri üç sekmeden düzenlenebilir (*ya da yeni bir zamanlama ayarlanabilir*):

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

Her sekmede "trafik isigi" düğmesini kullanarak  zamanlaması belirlenen testi geçici olarak devre dışı bırakabilir ve gerek duyduğunuzda tekrar açabilirsiniz.

10.4.1. 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.

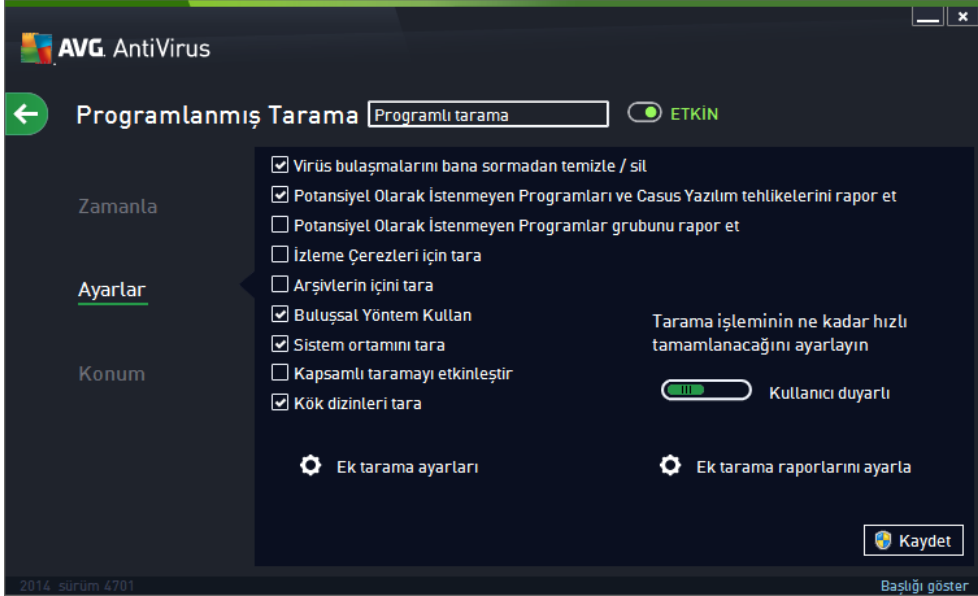
Bu iletişim kutusunda taramanın aşağıdaki parametrelerini de tanımlayabilirsiniz:

- **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 modundaydı 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.

10.4.2. Ayarlar



Ayarlar sekmesinin üst bölümünde geçerli olarak tanımlanmış tarama zamanlaması için ad belirleyebileceğiniz alan 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.

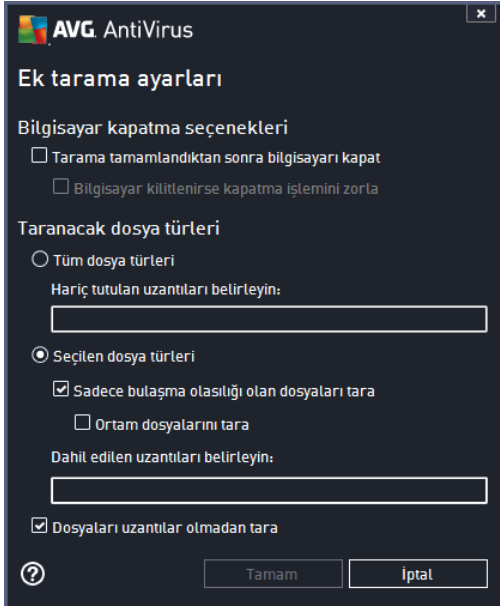
Ayarlar sekmesinde, isteğe bağlı olarak açılıp/kapatılabilen tarama parametrelerine ilişkin bir liste bulabilirsiniz. **Söz konusu ayarları değiştirmek açısından geçerli bir nedeniniz yoksa öntanımlı yapılandırmayı olduğu gibi muhafaza etmeniz önerilir.**

- **Bulaşmayı bana sormadan temizle / kaldır (varsayılan olarak açık):** Tarama sırasında virüs tanımlanırsa, bir giderme yazılımı mevcutsa otomatik olarak temizlenir. Bulmuş dosya otomatik olarak temizlenemezse, bulmuş nesne [Virüs Kasası](#)'na taşınır.
- **Potansiyel olarak istenmeyen 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 oluşturmasına rağmen bu programlardan bazıları bilerek yüklenebilir. Bilgisayarınızın güvenliğini artırdığından, bu özelliği etkin durumda tutmanızı öneririz.
- **Potansiyel olarak istenmeyen programlar gelişmiş grubunu rapor et (varsayılan olarak kapalı):** Casus yazılımların, yani doğrudan üreticiden alındığında 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 çerezlerin tespit edilmesi gerektiğini belirtir (*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 işleminde ZIP, RAR vb. bir arşiv ile saklanmış olsa bile tüm dosyaların taranması gerektiğini belirtir.
- **Bulussal yöntem kullan** (varsayılan olarak açık): Bulussal analiz (taranan nesnenin yönergelerinin sanal bir bilgisayar ortamında dinamik olarak canlandırılması) tarama sırasında kullanılacak virüs tespit yöntemlerinden biridir.
- **Sistem ortamını tara** (varsayılan olarak açık): Tarama işlemi, bilgisayarınızın sistem alanlarını da kontrol edecektir.
- **Kapsamli 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:



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

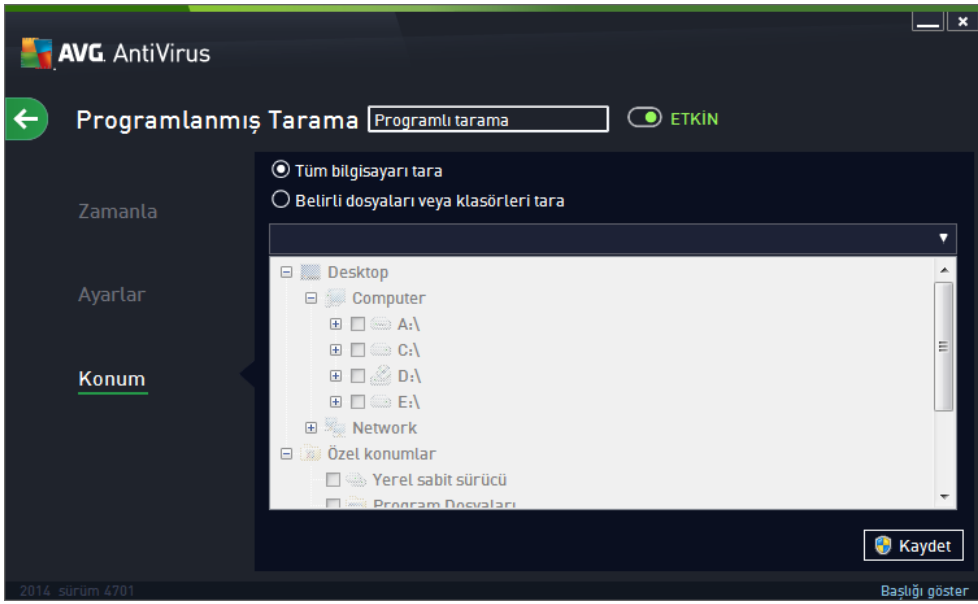
Tarama bulgularının rapor edilmesi gerekip gerekmediğini tanımlamak üzere birden fazla öğeyi ayarlayabileceğiniz **Tarama raporları** olarak adlandırılan bağımsız bir iletişim penceresi açmak için **Ek tarama raporlarını ayarla...** bağlantısını tıklayın:



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.

10.4.3. 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 isaretini tıklatarak öğeleri genişletin*). İlgili kutuları işaretleyerek birden fazla klasör seçebilirsiniz. Seçilen klasörler, iletişim kutusunun üstünde bulunan metin alanında görüntülenir. Açılır menü seçilen tarama geçmişini daha sonra kullanılmak üzere saklar. Alternatif olarak, istediğiniz klasörün tam yolunu elle girebilirsiniz (*birden fazla yol girerseniz, bunları ekstra boşluk bırakmadan noktalı virgülle ayırmanız gerekir*).


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

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

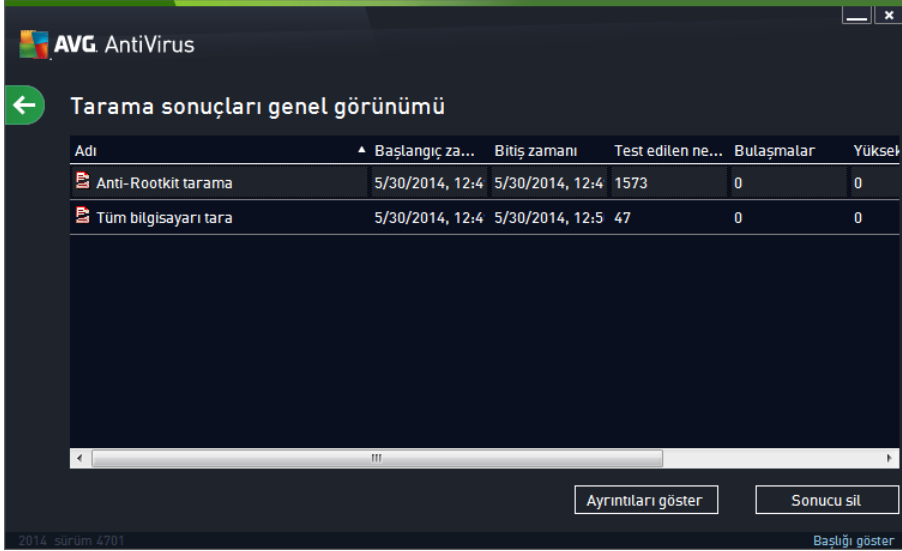


- *Win XP için:* C:\Documents and Settings\Default User\Belgelerim\
- *Windows Vista/7 için:* C:\Users\user\Documents\
- **Paylaşılan Belgeler**
 - *Win XP için:* C:\Documents and Settings\All Users\Documents\
 - *Windows Vista/7 için:* C:\Users\Public\Documents\
- **Windows klasörü** - C:\Windows\
- **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.

10.5. Tarama Sonuçları









The screenshot shows the AVG AntiVirus interface with the title 'Tarama sonuçları genel görünümü'. It displays a table with the following data:

| Adı | Başlangıç za... | Bitiş zamanı | Test edilen ne... | Bulaşmalar | Yüksek |
|----------------------|-----------------|-----------------|-------------------|------------|--------|
| Anti-Rootkit tarama | 5/30/2014, 12:4 | 5/30/2014, 12:4 | 1573 | 0 | 0 |
| Tüm bilgisayarı tara | 5/30/2014, 12:4 | 5/30/2014, 12:5 | 47 | 0 | 0 |

Buttons at the bottom include 'Ayrıntıları göster' and 'Sonucu sil'. The status bar at the bottom left shows '2014, sürüm 4701' and the bottom right shows 'Başlığı göster'.

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** - Taramanın 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.


10.6. 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:

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

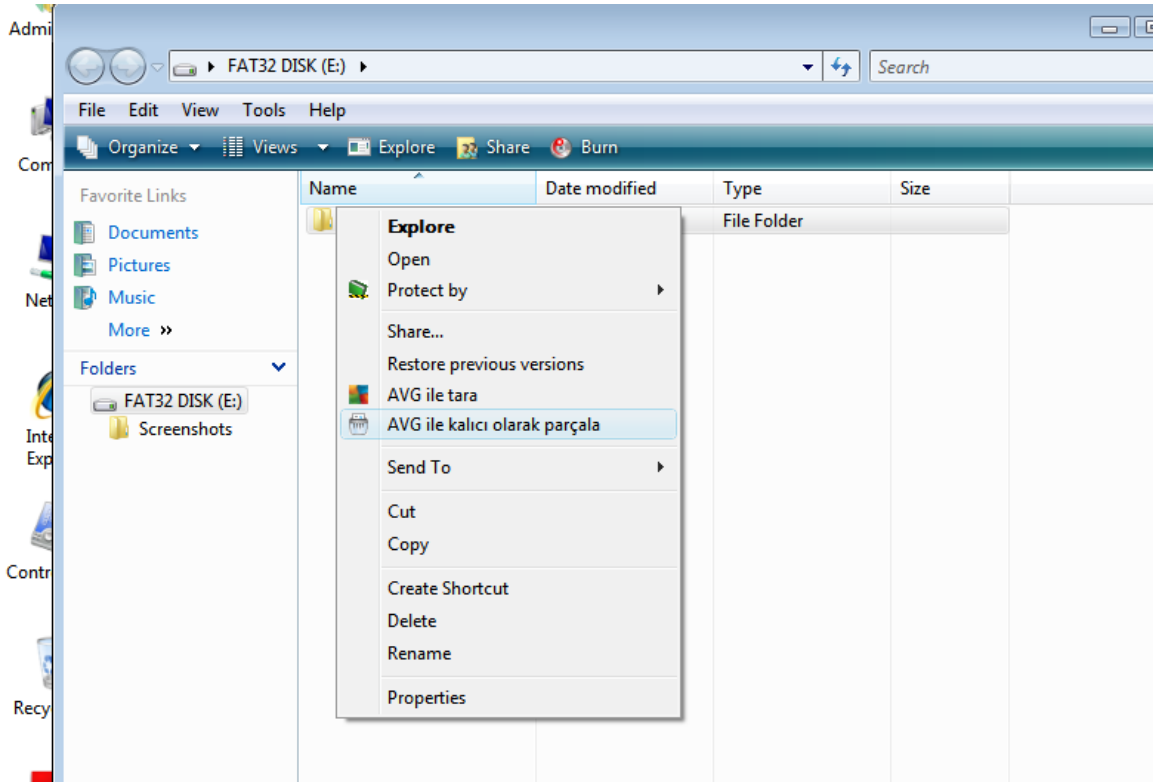
 **Orta önem derecesi:** genellikle PUP (potansiyel olarak istenmeyen programlar, reklam yazılımı gibi) veya izleme çerezleri

 **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.

11. AVG File Shredder

AVG File Shredder dosyaları tamamen güvenli biçimde silmek (yani kurtarma amaçlı tasarlanmış gelişmiş yazılım araçlarıyla bile kurtarma ihtimali olmayacak biçimde silmek) üzere tasarlanmıştır.

Bir dosya veya klasörü parçalamak için dosyayı/klasörü bir dosya yöneticisinde (*Windows Explorer, Total Commander, ...*) sağ tıklatın ve bağlam menüsünden **AVG ile kalıcı olarak parçala**'yi seçin. Geri Dönüşüm Kutusu içindeki dosyalar da parçalanabilir. Belirli bir konumdaki (*örneğin CD-ROM*) belirli bir dosya güvenilir biçimde parçalanamıyorsa bu konuda bilgilendirilirsiniz veya bağlam menüsündeki seçenek tamamen kullanılmaz olur.



Lütfen her zaman aklınızda tutun: Parçaladığınız bir dosya artık sonsuza dek yok olur.

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:

- **Ekleme Tarihi** - Şüpheli dosyanın tespit edildiği ve Virüs Kasası'na kaldırıldığı tarih ve saati gösterir.
- **Önem seviyesi** - [Kimlik](#) bileşenini **AVG AntiVirus** yazılımınıza yüklemeye karar verdiğinizde, ilgili bulgunun önem seviyesi, sakıncasız (*üç yeşil nokta*) ile çok tehlikeli (*üç kırmızı nokta*) arasında değişen dört seviyeli bir ölçekte grafik olarak bu bölümde gösterilir; bulaşma türü hakkındaki bilgiler (*bulaşma seviyesine bağlı olarak - listelenen tüm nesnelere virüs bulaşmıştır veya bulaşma olasılığı vardır*) de gösterilir.
- **Tehdit Adı** - Tespit edilen bulaşmanın adını çevrimiçi [virüs ansiklopedisine](#) göre belirtir.
- **Kaynak** - İlgili tehdidi hangi **AVG AntiVirus** bileşeninin tespit ettiğini belirtir.
- **Mesaj** - Çok nadiren, bu sütunda ilgili tehdit hakkında ayrıntılı açıklamalar sunan notlar gösterilebilir.

Kontrol düğmeleri



Virüs Kasası arayüzünden ulaşabileceğiniz kontrol düğmeleri şunlardır:

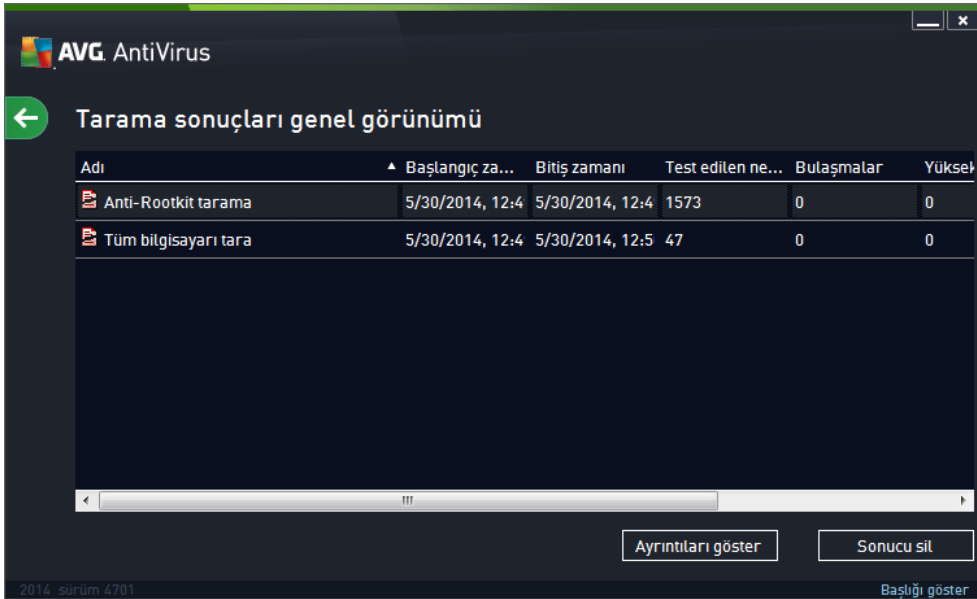
- **Geri Yükle** - bulasmis dosyayı sabit diskinizdeki orijinal konumuna geri yükler.
- **Farklı Geri Yükle** - bulasmis dosyayı seçili klasöre tasir.
- **Ayrıntılar** - **Virüs Kasası**nda karantinaya alınan tehdit hakkında ayrıntılı bilgi için listede seçili öğeyi vurgulayın ve **Ayrıntılar** düğmesini 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](#)


13.1. Tarama sonuçları



| Adı | Başlangıç za... | Bitiş zamanı | Test edilen ne... | Bulaşmalar | Yüksek |
|----------------------|-----------------|-----------------|-------------------|------------|--------|
| Anti-Rootkit tarama | 5/30/2014, 12:4 | 5/30/2014, 12:4 | 1573 | 0 | 0 |
| Tüm bilgisayarı tara | 5/30/2014, 12:4 | 5/30/2014, 12:5 | 47 | 0 | 0 |


Tarama sonuçları genel görünümü iletişim kutusuna **AVG AntiVirus** 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 bulaşmanın tespit edildiğini ancak bulaşmış

nesnenin otomatik olarak silindigini gösterir

 - kirmizi simge tarama sirasinda bir bulasmanin tespit edildigini, ancak bulasmis nesnenin silinemedigini gösterir!


Simgeler bütün halinde ya da yarisi kesilmis olabilir - bütün halindeki simge, tarama isleminin dogru sekilde tamamlandigini ve bitirildigini gösterirken yarisi kesilmis simge, taramanın iptal edildigini ya da kesildigini 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 baslatıldığı tarih ve saati gösterir.
- **Bitiş zamanı** - taramanın bittiği tarih ve saati gösterir.
- **Taranan nesnelere** - tarama sırasında kontrol edilen nesne sayısidir
- **Bulasmalar** - tespit edilen / silinenvirüs bulasma sayisi
- **Yüksek / Orta** - bu sütunlar kaldırılan/bulunan toplam bulasma sayisini sirasiyla yüksek ve orta önem seviyesine göre gösterir
- **Bilgi** - tarama islemine ve sonucuna iliskin bilgiler (*genellikle islemin tamamlanmasinin 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 Sonuçları

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:

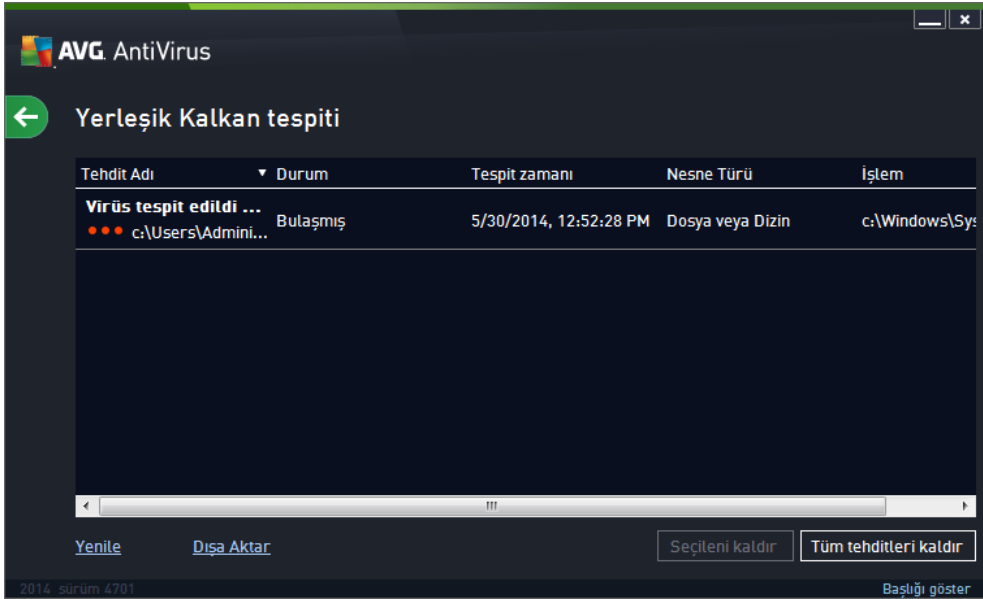


Bu uyarı iletişim kutusunda tespit edilen ve virüs bulasmis olarak atanan nesne hakkında daha fazla bilgi (*Tehdit*) ve ilgili bulasma hakkında bazı açıklamalar (*Açıklama*) bulabilirsiniz. [Ayrıntıları göster](#) bağlantısı, sizi tespit edilen bulasma hakkında ayrıntılı bilgi bulabileceğiniz (biliniyorsa) 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 değiştirilebilir. Sabit diskinizin gerçek boyutunun uyarlanabilir yüzdesi olarak tanımlanır. Virüs Kasasının 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 AntiVirus 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:

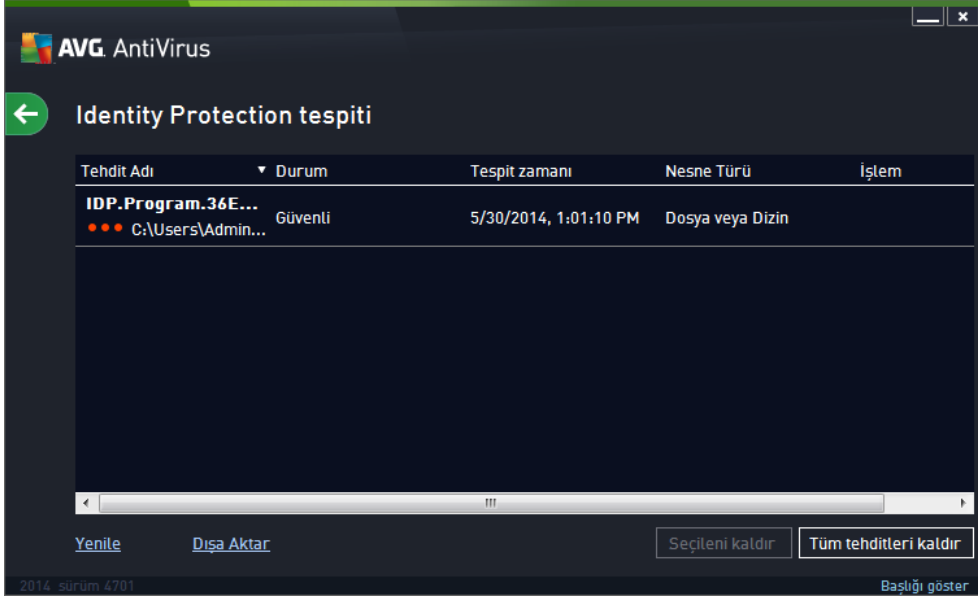
- **Tespit Adı** - tespit edilen nesnenin açıklaması (*muhtemelen adı da*) ve konumu
- **Sonuç** - tespit edilen nesne ile gerçekleştirilen eylem
- **Tespit Zamanı** - tehdidin tespit edildiği ve engellendiği tarih ve saat
- **Nesne Türü** - tespit edilen nesnenin türü
- **İşlem** - tespit edilmesi amacıyla potansiyel tehlike taşıyan nesneyi uyararak işlem nedir

Kontrol düğmeleri

- **Yenile - Online Shield**
- **Disa aktar** - tespit edilen tüm nesnelere bir dosyada disa aktarın
- **Seçilene 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. Identity Protection Sonuçları

Identity Protection Sonuçları iletişim kutusuna **AVG AntiVirus ana penceresinin üst satirındaki gezinme bölümünden Seçenekler / Geçmiş / Identity Protection Sonuçları** menü ögesi yoluyla erişilebilir.




İletişim kutusunda [Identity Protection](#) bileşenin tespit ettiği tüm bulguların listesi bulunur. Tespit edilen tüm nesnelere ilişkin aşağıdaki bilgiler verilir:

- **Tehdit Adı** - tespit edilen nesnenin açıklaması (*muhtemelen adı da*) ve kaynağı
- **Sonuç** - tespit edilen nesne için yapılan işlem
- **Tespit Zamanı** - şüpheli nesnenin tespit edildiği 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 dışa aktarabilirsiniz (**Listeyi dosyaya aktar**) ve tespit edilen nesnelere hakkındaki tüm girişleri silebilirsiniz (**Listeyi temizle**).

Kontrol düğmeleri

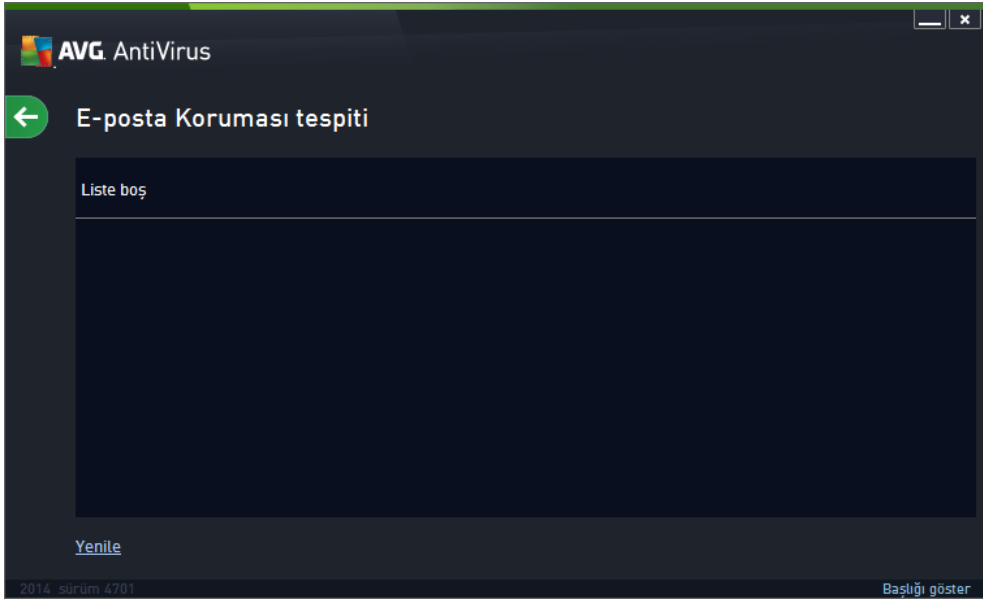
Identity Protection Sonuçları arayüzünde bulunan kontrol düğmeleri şunlardır:

- **Listeyi yenile** - Tespit edilen tehlikelerin listesini günceller
-  - Varsayılan [AVG ana iletişim kutusuna](#) (*bileşen genel görünümü*) geri dönmek için bu

iletisim kutusunun sol üst kısmındaki oku kullanın

13.4. E-posta Koruması Sonuçları

E-posta Koruması Sonuçları iletisim kutusuna **AVG AntiVirus** ana penceresinin üst satırındaki gezinme bölümünden **Seçenekler / Geçmiş / E-posta Koruması Sonuçları** menü öğesi yoluyla erişilebilir.



iletisim kutusunda [E-posta Tarayicisi](#) 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

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

Kontrol düğmeleri

E-posta Tarayicisi algılama arayüzünde bulunan kontrol düğmeleri şunlardır:

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

-  - Varsayılan [AVG ana iletişim kutusuna](#) (bilesen genel görünümü) geri dönmek için bu iletişim kutusunun sol üst kısmındaki oku kullanın

13.5. Online Shield Sonuçları

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 bulaşmış olarak atanan nesne hakkında daha fazla bilgi (*Tehdit*) ve ilgili bulaşma hakkında bazı açıklamalar (*Nesne adı*) bulabilirsiniz. [Daha fazla bilgi](#) bağlantısı, sizi tespit edilen bulaşma hakkında ayrıntılı bilgi (biliniyorsa) bulabileceğiniz çevrimiçi virüs ansiklopedisine yönlendirir. İletişim kutusundan aşağıdaki kontrol öğeleri bulunur:

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


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



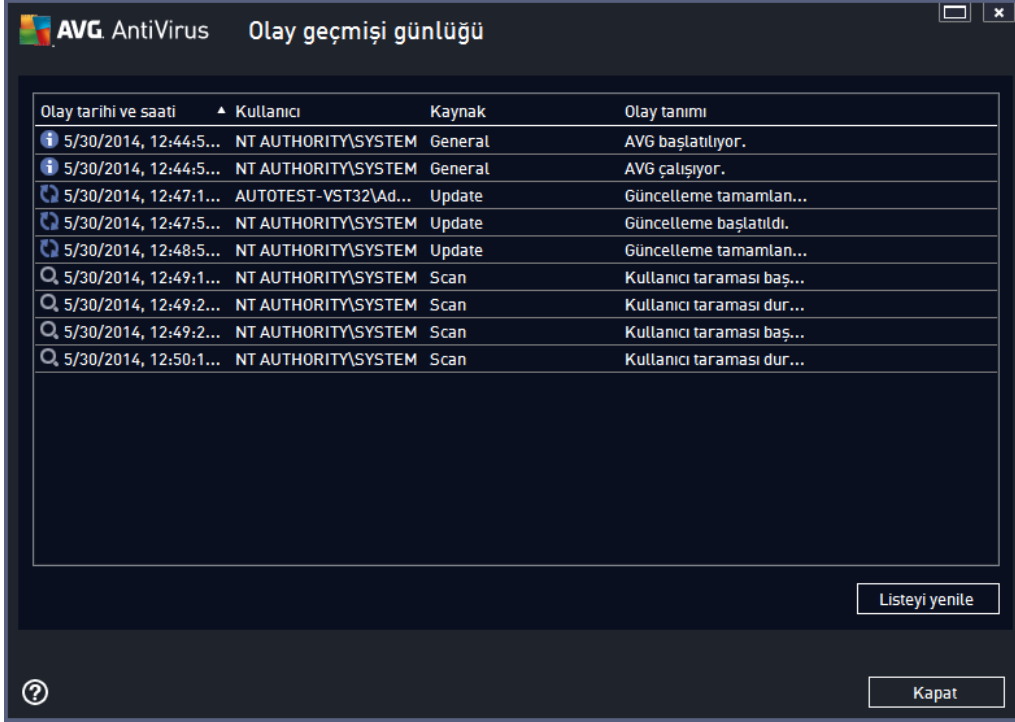
Tespit edilen tüm nesnelere için aşağıdaki bilgiler verilir:

- **Tehdit Adı** - tespit edilen nesnenin açıklaması (*muhtemelen adı da*) ve kaynağı (*web sayfası*)
- **Sonuç** - tespit edilen nesne ile gerçekleştirilen işlem
- **Tespit Zamanı** - tehdidin tespit edildiği 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
-  - varsayılan [AVG ana iletişim kutusuna](#) (*bilesen genel görünümü*) geri dönmek için bu iletişim kutusunun sol üst kısmındaki oku kullanın

13.6. Olay Geçmiş



Olay geçmişi iletişim kutusuna **AVG AntiVirus ana penceresinin üst satirindeki gezinme bölümünden Seçenekler / Geçmiş / Olay Geçmiş** menü ögesi yoluyla erişilebilir. Bu iletişim kutusunda, **AVG AntiVirus** uygulamasının çalışması sırasında oluşan önemli olayların bir özeti bulabilirsiniz. Bu iletişim kutusunun kayıtlarını sağladığı olay türleri: AVG uygulaması güncellemeleri hakkında bilgiler; tarama başlangıcı, sonu veya durdurulması hakkında bilgiler(*otomatik olarak gerçekleştirilen testler de dahil*); virüs tespitiyle bağlantılı olaylar hakkında gerçekleştiği konumu da içeren bilgiler (*yerleşik kalkan veya [tarama](#) kaynaklı*) ve diğer önemli olaylar.

Her olay için şu bilgiler listelenir:

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

Kontrol düğmeleri

- **Listeyi yenile** - olaylar listesindeki tüm girişleri güncellemek için bu düğmeye basın
- **Kapat** - **AVG AntiVirus** ana penceresine dönmek için bu düğmeyi tıklayın

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 AntiVirus** ürününüzü düzenli olarak güncellemek hayati bir öneme sahiptir. En iyi çözüm, otomatik güncellenmenin yapılandırıldığı program varsayılan ayarlarına güvenmektir. **AVG AntiVirus** 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 AntiVirus** 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 AntiVirus** güncellemeleri indirmeye başlar ve güncelleme işlemini kendisi başlatır. Güncelleme sonuçları hakkında AVG sistem tepsisi simgesi üzerinde belirgin 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](#)

14.2. Güncelleme seviyeleri

AVG AntiVirus seçilebilecek iki güncelleme düzeyi sunar:

- **Tanim güncellemeleri** güvenilir virüs koruması için gerekli değişiklikleri içerir. Genellikle kodu değiştirmez ve yalnızca tanımlama veritabanını günceller. Bu güncelleme sunulur sunulmaz yüklenmelidir.
- **Program güncellemesi** çeşitli program değişikliklerini, onarımları ve iyileştirmeleri içerir.

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



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

Not: Zamanlamasi önceden yapilmis bir program güncellemesi ile taramanın çakismasi durumunda güncelleme islemi daha yüksek öncelige sahiptir ve tarama islemine ara verilir. Böyle bir durum ortaya çikarsa çakisma hakkında bilgilendirilirsiniz.

15. SSS ve Teknik Destek

AVG AntiVirus 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 ile ilgili temel bilgiler (program / veritabanı sürümü), lisans ayrıntıları ve hızlı destek bağlantıları listesi bulunur.
- **Yardım dosyasında sorun giderme:** Doğrudan **AVG AntiVirus 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 tıklanın.
- **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'ler ve Eğitimler** menü seçeneğinden erişilebilir. Burada da tüm sorular satış, teknik ve virüs kategorileri olarak organize bir şekilde sınıflandırılmıştır.
- **AVG ThreatLabs:** AVG ile ilişkili özel bir web sitesi (<http://www.avgthreatlabs.com/website-safety-reports/>) olarak virüs sorunları bağlamında çevrimiçi tehditler hakkında genel bilgiler vermek üzere hazırlanmıştır. 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.