



AVG Internet Security

Kullanıcı Kılavuzu

Belge revizyonu AVG.07 (25/11/2016)

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



İçindekiler

1. Giriş	3
2. AVG Yükleme Gereksinimleri	4
2.1 Desteklenen İşletim Sistemleri	4
2.2 Minimum ve Önerilen Donanım Gereksinimleri	4
3. AVG Yükleme İşlemi	5
3.1 Hoş Geldiniz!	5
3.2 Lisans numaranızı girin	6
3.3 Yükleme özelleştirme	8
3.4 AVG'yi Yükleme	9
3.5 Yükleme tamamlandı	10
4. Yüklemeden Sonra	11
4.1 Virüs veritabanı güncelleme	11
4.2 Ürün kaydı	11
4.3 Kullanıcı arayüzüne erişim	11
4.4 Tüm bilgisayarın taraması	11
4.5 Eicar testi	11
4.6 AVG varsayılan yapılandırması	12
5. AVG Kullanıcı Arayüzü	13
5.1 Üst Satır Gezinme	14
5.2 Güvenlik Durumu Bilgisi	17
5.3 Bileşen Genel Görünümü	18
5.4 Uygulamalarım	19
5.5 Tara / Hızlı Bağlantıları Güncelle	19
5.6 Sistem Tepsisi Simgesi	20
5.7 AVG Tavsiyesi	21
5.8 AVG Hızlandırıcı	21
6. AVG Bileşenleri	22
6.1 Bilgisayar Koruması	22
6.2 Web Tarama Koruması	25
6.3 Software Analyzer	27
6.4 E-posta Koruması	28
6.5 Güvenlik Duvarı	30
6.6 PC Analyzer	32
7. AVG Gelişmiş Ayarlar	34
7.1 Görünüm	34
7.2 Sesler	36
7.3 AVG korumasını geçici olarak devre dışı bırak	37
7.4 Bilgisayar Koruması	38



7.5 E-posta Tarayıcısı	42
7.6 Web Tarama Koruması	57
7.7 Software Analyzer	60
7.8 Taramalar	61
7.9 Programlar	66
7.10 Güncelleme	73
7.11 İstisnalar	77
7.12 Virüs Kasası	79
7.13 AVG Kendi Kendini Koruma	80
7.14 Gizlilik Tercihleri	80
7.15 Hata Durumunu Yoksay	82
7.16 Tavsiye - Bilinen Ağlar	83
8. Güvenlik Duvarı Ayarları	84
8.1 Genel	84
8.2 Uygulamalar	86
8.3 Dosya ve yazıcı paylaşımı	87
8.4 Gelişmiş ayarlar	88
8.5 Tanımlanan ağlar	89
8.6 Sistem hizmetleri	90
8.7 Günlükler	91
9. AVG Tarama	94
9.1 Öntanımlı taramalar	96
9.2 Windows Gezgini'nde Tarama	105
9.3 Komut satırı tarama	105
9.4 Tarama programlama	109
9.5 Tarama sonuçları	115
9.6 Tarama sonuçları ayrıntıları	116
10. AVG File Shredder	118
11. Virüs Kasası	119
12. Geçmiş	120
12.1 Tarama sonuçları	120
12.2 Yerleşik Kalkan Sonuçları	122
12.3 Identity Protection Sonuçları	124
12.4 E-posta Koruması Sonuçları	125
12.5 Online Shield Sonuçları	126
12.6 Olay Geçmişi	128
12.7 Güvenlik Duvarı günlüğü	129
13. AVG Güncellemeleri	130
14. SSS ve Teknik Destek	131



1. Giriş

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

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

Diğer bilgi kaynaklarını da kullanmak isteyebilirsiniz:

- **Yardım dosyası:** Doğrudan **AVG Internet Security** 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 tıklatın.
- **AVG web sitesi destek merkezi:** Sorununuzun çözümünü AVG web sitesinde de (<http://www.avg.com/>) arayabilirsiniz. **Destek** bölümünde hem satış hem de teknik sorunlarla ilgilenen tematik gruplar hakkında genel bilgiler, sık sorulan soruların yapılandırıldığı bir bölüm ve erişilebilir iletişim bilgilerini bulabilirsiniz.
- **AVG ThreatLabs:** AVG ile ilişkili özel bir web sitesi (<http://www.avg.com/about-viruses>) 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:** <http://community.avg.com/> adresindeki AVG kullanıcıları tartışma forumunu da kullanabilirsiniz.



2. AVG Yükleme Gereksinimleri

2.1. Desteklenen İşletim Sistemleri

AVG Internet Security aşağıdaki işletim sistemleri ile çalışan çalışma istasyonlarını koruma amaçlıdır:

- Windows XP Home Edition SP3
- Windows XP Professional SP3
- Windows Vista (tüm sürümler)
- Windows 7 (tüm sürümler)
- Windows 8 (tüm sürümler)
- Windows 10 (tüm sürümler)

(ve belirli işletim sistemleri için daha yeni hizmet paketleri)

2.2. Minimum ve Önerilen Donanım Gereksinimleri

AVG Internet Security için minimum donanım gereksinimleri:

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

AVG Internet Security için önerilen donanım gereksinimleri:

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

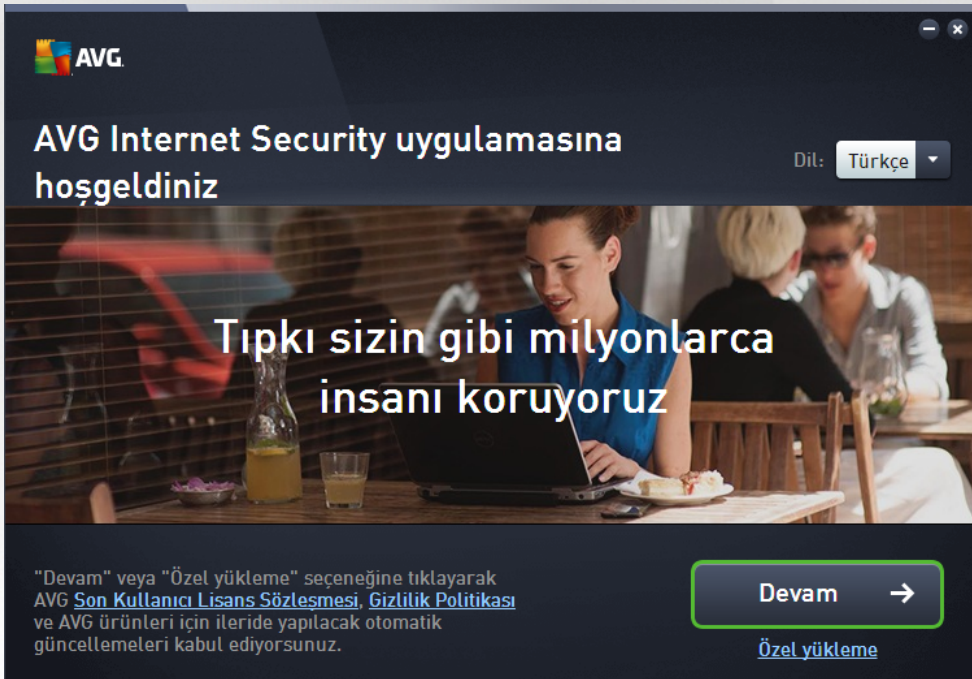


3. AVG Yükleme İşlemi

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

Yükleme işlemi **AVG Internet Security uygulamasına hoş geldiniz** iletişim kutusu ile başlar:



Dil seçimi

Bu iletişim kutusunda yükleme süreci için kullanılan dili seçebilirsiniz. Dil menüsünü açmak için **Dil** seçeneğinin yanındaki açılır kutuya tıklayın. İstediğiniz dili seçtiğinizde yükleme süreci bu dille devam eder. Uygulama da seçilen dilde çalışır ve varsayılan olarak her zaman yüklü olan İngilizceye geçme seçeneği de mevcuttur.

Son Kullanıcı Lisans Sözleşmesi ve Gizlilik Politikası

Yükleme işlemine devam etmeden önce **Son Kullanıcı Lisans Sözleşmesi** ve **Gizlilik Politikası** belgelerini incelemenizi tavsiye ederiz. Her iki belgeye de iletişim kutusunun altındaki etkin bağlantılarla erişilebilir. İlgili belgenin tam metnini gösteren yeni bir iletişim kutusu / tarayıcı penceresi açmak için bağlantılardan birine tıklayın. Lütfen yasal olarak bağlayıcı olan bu belgeleri dikkatlice okuyun. **Devam** düğmesine tıkladığınızda belgeleri kabul ettiğinizi onaylarsınız.



Yüklemeye devam et

Yüklemeye devam etmek için **Devam** düğmesine tıklayın. Sizden lisans numaranız istenecektir ve yükleme işlemi daha sonra tamamen otomatik moda çalışacaktır. Çoğu kullanıcı için **AVG Internet Security** yüklemesinde tüm ayarların program sağlayıcısı tarafından önceden tanımlandığı bu standart seçeneğin kullanılması tavsiye edilir. Bu yapılandırma, minimum kaynak kullanımı ile maksimum güvenliği bir araya getirir. Gelecekte söz konusu yapılandırmayı değiştirme ihtiyacı duyarsanız söz konusu işlemi istediğiniz zaman doğrudan uygulamadan yapabilirsiniz.

İsterseniz **Devam** düğmesinin altında yer alan bağlantıyla erişebileceğiniz **Özel yükleme** seçeneği de mevcuttur. Özel yükleme uygulamayı standart olmayan ayarlarla kurmak için geçerli bir nedeni olan (ör. belirli sistem gereksinimlerini karşılamak için) deneyimli kullanıcılar tarafından kullanılmalıdır. Özel yüklemeye karar verirsiniz lisans numaranızı girdikten sonra ayarlarınızı belirleyebileceğiniz **Yüklemenizi özelleştirin** iletişim kutusuna yönlendirilirsiniz.

3.2. Lisans numaranızı girin

Lisans numaranızı girin iletişim kutusunda, lisans numaranızı verilen metin alanına yazarak (veya kopyala ve yapıştır yönteminin kullanarak) lisansınızı etkinleştirmeniz istenir:

The screenshot shows a dark-themed window titled "Lisans numaranızı girin" (Enter your license number). At the top left is the AVG logo. Below the title bar is a back arrow and the title. A text input field is present with a placeholder text "Bunu nereden bulabilirim?". To the right of the input field is a link "Bunu nereden bulabilirim?". At the bottom right is a "Devam" button. At the bottom left, there is a link: "Lisansınız yok mu? AVG Internet Security ürününü 30 gün ücretsiz deneyin".

Lisans numaramı nereden bulabilirim?

Satış numarası **AVG Internet Security** kutunuzun içindeki CD paketinde bulunabilir. Lisans numarası **AVG Internet Security** programını çevrimiçi satın aldıktan sonra gelen onay e-postasında olacaktır. Numarayı tam olarak gösterildiği gibi girmelisiniz. Lisans numarasının dijital formu mevcut ise (e-postada) girmek için kopyala ve yapıştır yönteminin kullanılması önerilmektedir.



Kopyala ve Yapıştır yöntemi nasıl kullanılır

Kopyala ve Yapıştır yöntemini kullanarak **AVG Internet Security** 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 tıklayın, düğmeyi tutup numaranın sonuna kadar sürükleyin ve düğmeyi bırakın. Numaranın vurgulanması gerekir.
- **Ctrl** tuşunu basılı tutun ve **C** tuşuna basın. Bu işlem numarayı kopyalar.
- Kopyalanan numarayı yapıştırmak istediğiniz konumu tıklayın, yani **Lisans numaranızı girin** iletişim kutusunun metin alanını.
- **Ctrl** tuşunu basılı tutun ve **V** tuşuna basın. Bu işlem numarayı seçilen konuma yapıştırır.

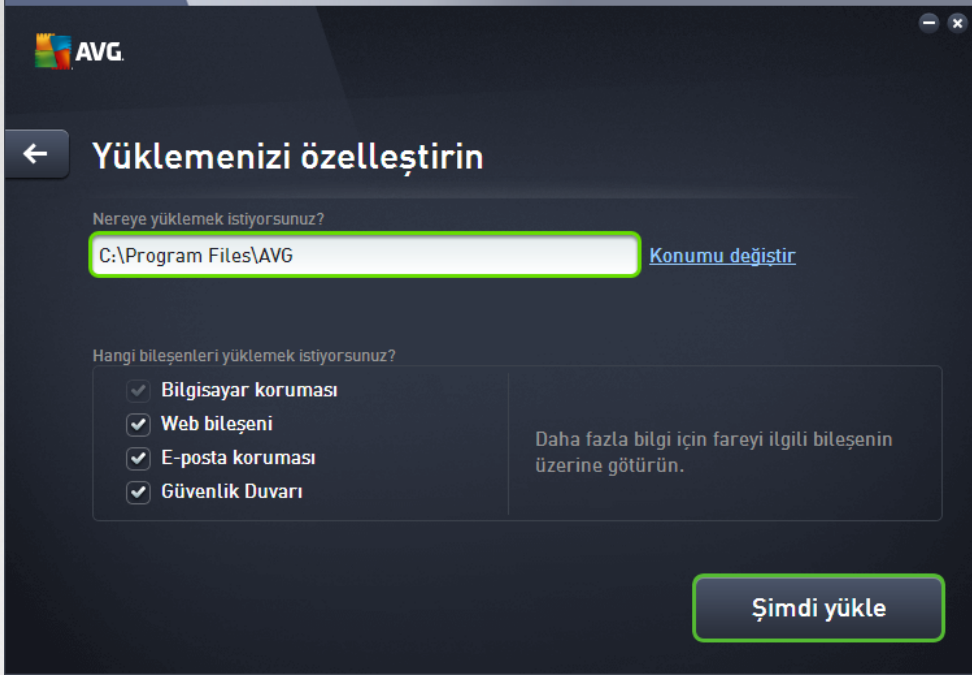
Yüklemeye devam et

İletişim kutusunun alt kısmında **Şimdi yükle** düğmesini görebilirsiniz. Düğme, lisans numaranızı girdiğinizde etkinleşir. Etkin hale geldikten sonra, yükleme işlemi başlatmak için düğmeyi tıklatmanız yeterlidir. Elinizde geçerli bir lisans numarası yoksa uygulamanın **AVG AntiVirus Free Edition** sürümünü yüklemeyi seçebilirsiniz. Ne yazık ki, ücretsiz sürümler tam profesyonel sürümde bulunan tüm işlevleri desteklemez. Dolayısıyla ayrıntılı AVG satın alma ve yükseltme bilgileri için AVG web sitesini (<http://www.avg.com/>) ziyaret etmeyi düşünebilirsiniz.



3.3. Yükleme özelleştirme

Yüklemenizi özelleştirin iletişim kutusu yükleme işleminin ayrıntılı parametrelerini ayarlamanıza olanak verir:




Nereye yüklemek istiyorsunuz?

Burada uygulamanın yüklenmesini istediğiniz yeri belirleyebilirsiniz. Metin alanındaki adres, Program Dosyaları klasörünüzdeki önerilen konumu gösterir. Başka bir konuma karar vererseniz **Konumu değiştir** bağlantısını tıklatarak diskinizin ağaç yapısında yeni bir pencere açın. Ardından, istediğiniz konuma gidin ve konumu onaylayın.

Hangi bileşenleri yüklemek istiyorsunuz?

Bu bölümde yüklenebilecek tüm bileşenlerin bir genel görünümünü sunar. Varsayılan ayarların size uygun olmaması halinde belirli bileşenleri kaldırabilirsiniz. Ancak, sadece AVG Internet Security ürününde bulunan bileşenler arasında seçim yapabilirsiniz! Bu durumun tek istisnası, yüklemeyi çıkarmayan **Bilgisayar koruması** bileşenidir. Bu bölümde herhangi bir öğeyi vurguladığınızda ilgili bileşenin kısa bir açıklaması bu bölümün sağ tarafından görüntülenir. Her bileşenin işlevleri ile ilgili ayrıntılı bilgiler için bu belgedeki [Bileşen Genel Görünümü](#) bölümüne bakın.

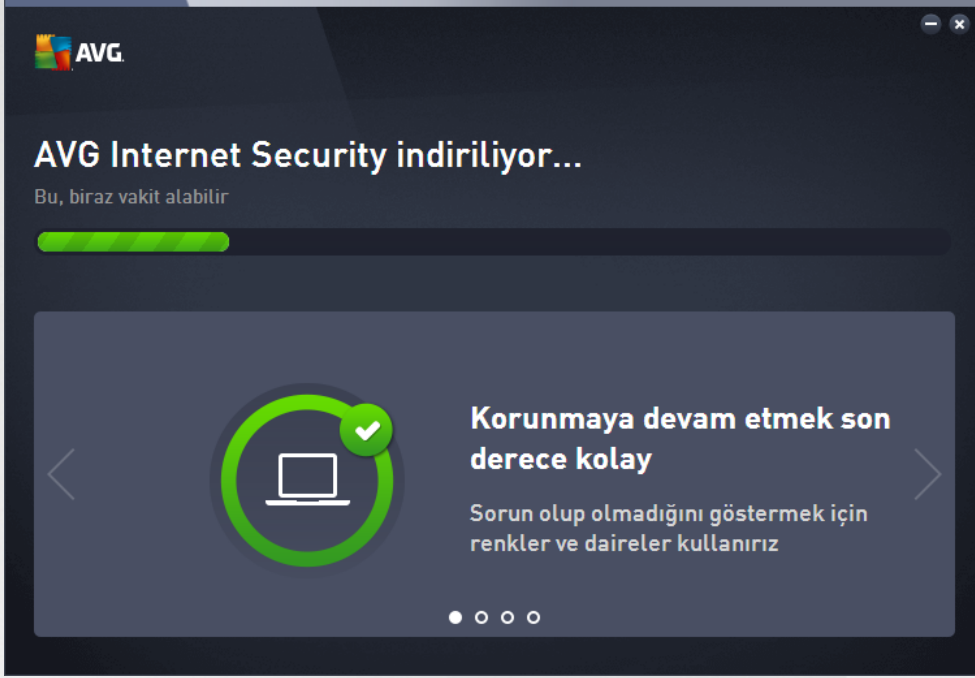
Yüklemeye devam et

Yüklemeye devam etmek için **Şimdi yükle** düğmesini tıklayın. Alternatif olarak, dil ayarlarınızı değiştirmeniz veya doğrulamanız gerekiyorsa, bu iletişim kutusunun üst tarafındaki ok düğmesini  kullanarak bir adım gerideki iletişim kutusuna gidebilirsiniz.



3.4. AVG'yi Yükleme

Önceki iletişim kutusunda yüklemeyi başlatmayı onayladıysanız yükleme işlemi tamamen otomatik modda çalışır ve herhangi bir müdahale gerektirmez:

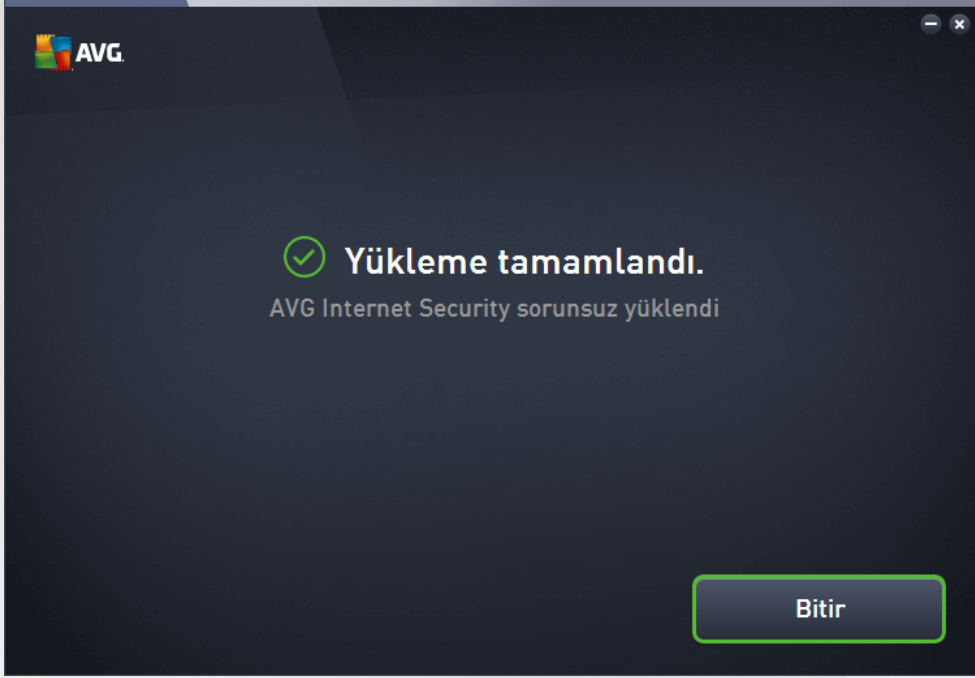


Yükleme işlemi tamamlandıktan sonra bir sonraki iletişim kutusuna otomatik olarak yönlendirilirsiniz.



3.5. Yükleme tamamlandı

Yükleme tamamlandı iletişim kutusu, AVG Internet Security ürününüzün tam olarak yüklendiğini ve yapılandırıldığını onaylar:



Yükleme işlemi tamamlamak için **Bitir** düğmesini tıklayın.



4. Yüklemeden Sonra

4.1. Virüs veritabanı güncelleme

Yüklemenin ardından (*gerekliyse, bilgisayar yeniden başlatıldıktan sonra*), **AVG Internet Security** programının virüs veritabanını ve tüm bileşenlerini otomatik olarak güncelleyerek tam çalışma düzenine geçirmesinin birkaç dakika alabileceğini lütfen unutmayın. Güncelleme işlemi çalışırken ana iletişim kutusunda görüntülenen bilgiyle durum hakkında bilgilendirilirsiniz. Lütfen güncelleme işleminin tamamlanması ve **AVG Internet Security** uygulamanızın sizi korumaya tamamen hazır hale getirilmesi için bir süre bekleyin!

4.2. Ürün kaydı

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

4.3. Kullanıcı arayüzüne erişim

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

- AVG Internet Security [sistem tepsi](#) simgesini çift tıklatın
- masaüstündeki AVG Protection simgesini çift tıklatın
- menüden *Başlat / Tüm Programlar / AVG / AVG Protection*

4.4. Tüm bilgisayarın taraması

AVG Internet Security 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.

4.5. Eicar testi

AVG Internet Security uygulamasının doğru şekilde yüklendiğinden emin olmak için EICAR testini yapabilirsiniz.

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.

eicar.com dosyasını indirmeye çalışın ve sabit diskinize kaydedin. Siz test dosyasının indirilmesini onaylar onaylamaz, **AVG Internet Security** 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!

4.6. AVG varsayılan yapılandırması

AVG Internet Security varsayılan yapılandırması (yani, uygulamanın yükledikten sonra doğru şekilde nasıl ayarlanacağı) yazılım satıcısı tarafından ayarlanabilir, böylece optimum performans elde etmek için tüm bileşenler ve işlemler ayarlanabilir. **Bunun için iyi bir nedeniniz olmadıkça AVG yapılandırmasını değiştirmeyin! Ayarlarda yapılacak her tür değişiklik sadece deneyimli bir kullanıcı tarafından gerçekleştirilmelidir.** İhtiyaçlarınızı daha iyi karşılaması açısından AVG yapılandırmasını değiştirme ihtiyacı hissederseniz [AVG Gelişmiş Ayarlar](#)'ına gidin: ana menü öğesi *Seçenekler/Gelişmiş ayarlar*'ı seçin ve AVG yapılandırmasını yeni açılan [AVG Gelişmiş Ayarlar](#) iletişim kutusunda düzenleyin.



5. AVG Kullanıcı Arayüzü

AVG Internet Security ana pencereden açılır:



Ana pencere çok sayıda bölüme ayrılır:

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

AVG Internet Security ana penceresi dışında, uygulamaya erişmek için kullanabileceğiniz bir kontrol ögesi daha vardır:

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



5.1. Üst Satır Gezinme

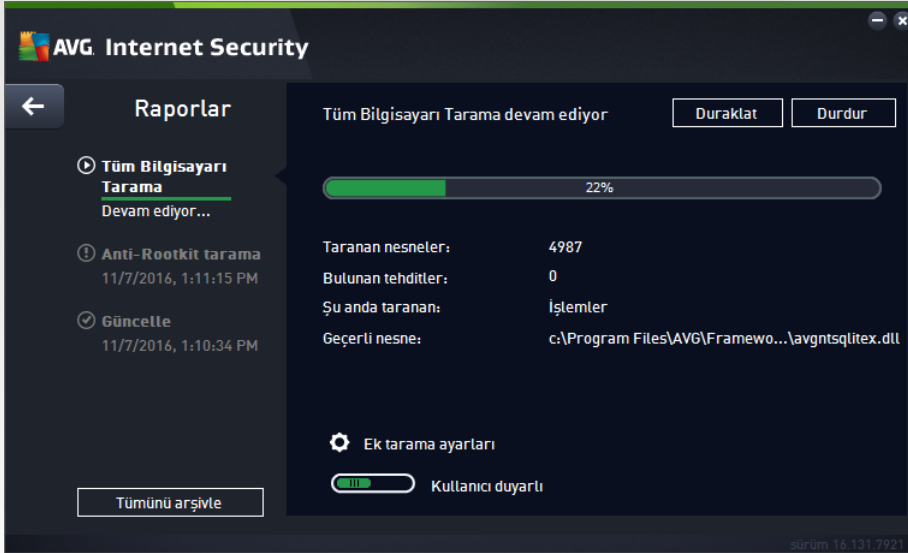
Üst satır gezinme ana menünün üst bölümünde yan yana dizilmiş birkaç etkin bağlantıdan oluşur. Gezinme bölümündeki düğmeler:

5.1.1. Diğer AVG ürünleri

Bağlantıya bir kez tıklayıp AVG web sitesine bağlanarak maksimum internet güvenliğiniz için AVG Protection ile ilgili tüm bilgileri bulabilirsiniz.

5.1.2. Raporlar

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





5.1.3. Destek

AVG Internet Security 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 bilgilerinizi bulabilirsiniz. Sekmede bulunan etkin bağlantılar ve düğmeler:
 - (Yeniden) Etkinleştir - Yeni **AVG Yazılım Etkinleştirme** iletişim kutusunu açmak için tıklayın. Satış numaranızı (AVG Internet Security yüklemesi sırasında kullandığınız) değiştirmek veya mevcut lisans numaranızı bir başkasıyla değiştirmek (ör. daha üst bir AVG ürününe yükseltme yaparken) için ilgili alana lisans numaranızı girin.
 - Panoya kopyala - Lisans numarasını kopyalayıp uygun alana yapıştırmak için bu bağlantıyı kullanın. Bu sayede lisans numarasının doğru girildiğinden emin olabilirsiniz.
 - Şimdi yenile - **AVG Internet Security** 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 tıklayıp 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 Internet Security** AV ürün bilgileri, yüklü bileşenler ve yüklü e-posta koruması hakkında en önemli teknik verileri gösterir.
- **Program** - Bu sekmede yüklü **AVG Internet Security** uygulaması hakkında ana ürün sürüm numarası ve ilgili tüm ürünlerin (ör. Zen, PC TuneUp, ...) sürüm numaraları listesi gibi ayrıntılı teknik bilgileri bulabilirsiniz. Ayrıca, bu sekme yüklü bileşenler ve belirli güvenlik bilgileri hakkında bir genel görünüm sağlar (virüs veritabanı, LinkScanner ve Anti-Spam sürüm numaraları).
- **Lisans Sözleşmesi** - Bu sekmede siz ve AVG Technologies arasındaki lisans sözleşmesinin tam metni bulunur.



5.1.4. Seçenekler

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

- **[Bilgisayarı tara](#)** seçeneği tüm bilgisayar tarama işlemi başlatır.
- **[Seçilen klasörü tara...](#)** - AVG tarama arayüzüne geçer ve bilgisayarınızın ağaç yapısından 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 tıklatın. İsteddiğiniz dosyayı seçin ve tarama başlatmayı onaylayın.
- **[Güncelle](#)** - **AVG Internet Security** güncellemesini otomatik olarak başlatır.
- **[Dizinden güncelle...](#)** - Sabit diskinizde bulunan belirli bir dosyanın içinde yer alan güncelleme dosyalarını alarak güncelleme işlemi gerçekleştirir. Öte yandan bu seçim sadece internet bağlantısının olmaması gibi (örneğin bilgisayarınıza virüs bulaşmış 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 işlemi başlatın.
- **[Virüs Kasası](#)** - AVG'nin tespit ettiği tüm bulaşmaları kaldırdığı karantina alanı olan Virüs Kasası arayüzünü açar. Karantina altında bulunan bulaşmış dosyalar yalıtılmıştır; bilgisayarınızın güvenliği garanti altındadır ve bulaşmış dosyalar da ileride tamir edilebilecekleri göz önünde bulundurularak aynı anda depolanır.
- **[Geçmiş](#)** - Bazı alt menü seçenekleri sunar:
 - **[Tarama sonuçları](#)** - Tarama sonuçları hakkında genel bilgilerin bulunduğu bir iletişim kutusu açar.
 - **[Yerleşik Kalkan Sonuçları](#)** - Yerleşik Kalkan tarafından tespit edilen tehditler hakkında genel bilgi veren bir iletişim kutusu açar.
 - **[Software Analyzer Sonuçları](#)** - Software Analyzer bileşeni tarafından tespit edilen tehditler hakkında genel bilgi veren bir iletişim kutusu açar.
 - **[E-posta Koruması Sonuçları](#)** - E-posta Koruması bileşeni tarafından tehlikeli olduğu tespit edilen posta eklentileri hakkında genel bilgi veren bir iletişim kutusu açar.
 - **[Online Shield Sonuçları](#)** - Online Shield tarafından tespit edilen tehditler hakkında genel bilgi veren bir iletişim kutusu açar.
 - **[Olay geçmişi günlüğü](#)** - Kaydedilen tüm **AVG Internet Security** işlemleri hakkında genel bilgi veren bir geçmiş günlüğü arayüzü açar.
 - **[Güvenlik Duvarı günlüğü](#)** - Tüm Güvenlik Duvarı işlemlerinin ayrıntılı bilgilerinin bulunduğu bir iletişim kutusu açar.



- **[Gelişmiş ayarlar...](#)** - **AVG Internet Security** yapılandırmasını düzenleyebileceğiniz AVG gelişmiş ayarlar iletişim kutusunu açar. Genel olarak uygulamanın yazılım üreticisi tarafından tanımlanan varsayılan ayarlarının muhafaza edilmesi önerilir.
- **[Güvenlik Duvarı ayarları...](#)** - Güvenlik Duvarı bileşeninin gelişmiş yapılandırmasına ilişkin bağımsız bir pencere açar.
- **Yardım içerikleri** - AVG yardım dosyalarını açar.
- **Destek alın** - Erişilebilir tüm iletişim ve destek bilgilerini sağlayan [destek iletişim kutusunu](#) 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 (*ör. yeni bir AVG ürününe yükseltme yaparken*) değiştirmek için lisans numaranızı düzenleyebilirsiniz. **AVG Internet Security** deneme sürümünü kullanıyorsanız sonraki iki öge, **Şimdi satın al** ve **Etkinleştir** olarak görünür ve programın tam sürümünü hemen satın almanızı sağlar. Bir satış numarasıyla yüklenmiş **AVG Internet Security** için ögeler **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 alabilecektir.
- **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 Internet Security** ana penceresinin üst kısmında bulunmaktadır. Bu bölümde **AVG Internet Security** ürününüzün mevcut güvenlik durumu hakkında bilgi bulabilirsiniz. Lütfen bu bölümde betimlenmesi muhtemel simgeleri ve anlamlarını inceleyin:



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



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

Sarı simge, bir bileşenin hata durumunu herhangi bir nedenle yoksaydığınızda da görünür. **Hata durumunu yoksay** seçeneğine [Gelişmiş ayarlar / Hata durumunu yoksay](#) yoluyla erişilebilir. Burada bileşenin hata durumunun farkında olduğunuz, ancak belirli bir neden doğrultusunda **AVG Internet**



Security 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!

Sarı simge **AVG Internet Security** uygulamanız bilgisayarın yeniden başlatılmasını gerektirdiğinde de görüntülenir (**Yeniden başlatma gerekiyor**). Lütfen bu uyarıyı dikkate alın ve bilgisayarınızı yeniden başlatın.



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

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

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

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

5.3. Bileşen Genel Görünümü

Yüklü bileşenlerin genel görünümü ana pencerenin orta bölümünde yatay bloklar halinde sıralanır. Bileşenler ilgili bileşen simgesiyle etiketlenmiş açık yeşil bloklar olarak gösterilir. Her blok korumanın geçerli 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 geçerli durumu hakkında bilgi sunar ve hangi bileşen hizmetlerinin doğru yapılandırılmadığını belirtir.

Yüklü bileşen listesi

AVG Internet Security altında **Bileşenler Genel Görünümü** bölümünde aşağıdaki bileşenler hakkında bilgi bulunur:

- **Bilgisayar** - Bu bileşen iki hizmeti kapsar: **Virüslerden Koruma Kalkanı** sisteminizdeki virüs, casus yazılım, solucan, Truva atı, istenmeyen çalıştırılabilir dosyalar veya kitaplıkları tespit eder ve sizi zararlı reklam yazılımlarına karşı korur; **Anti-Rootkit** ise uygulama, sürücü veya kitaplıklarda gizlenen tehlikeli rootkit'ler için tarama yapar. [Ayrıntılar >>](#)
- **Web Tarama** - İnternette arama ve gezinme sırasında sizi web tabanlı saldırılara karşı korur. [Ayrıntılar >>](#)



- **Yazılım** - Bileşen internette dijital varlıklarınızı yeni ve bilinmeyen tehditlere karşı sürekli olarak koruyan **Software Analyzer** hizmetini çalıştırır. [Ayrıntılar >>](#)
- **E-postalar** - Gelen e-posta mesajlarınızı istenmeyen e-postalara karşı denetler ve virüsleri, kimlik avı saldırılarını veya diğer tehditleri engeller. [Ayrıntılar >>](#)
- **Güvenlik Duvarı** - Her ağ bağlantı noktasındaki tüm iletişimleri denetleyerek sizi kötü amaçlı saldırılardan korur ve tüm sızma girişimlerini engeller. [Ayrıntılar >>](#)

Erişilebilir eylemler

- **Fareyi ilgili bileşen simgesi üzerinde hareket ettirerek** bileşen genel görünümü ekranında bileşeni seçin. Aynı anda [kullanıcı arayüzünün](#) alt kısmında bileşenin temel fonksiyonları hakkında açıklamalar görüntülenir.
- **Bileşen simgesine bir kez tıklayarak** bileşenin geçerli durumu hakkında bilgiler içeren arayüzünü açın ve bileşenin yapılandırma ve istatistik verilerine erişin.

5.4. Uygulamalarım

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

- **Mobil koruma** cep telefonunuzu virüs ve zararlı yazılımlardan koruyan bir uygulamadır. Uygulama, ayrı kalmanız durumunda akıllı telefonunuzu uzaktan izleme imkanı da sağlar.
- **PC Tuneup** uygulaması bilgisayarınızın hızının ve genel performansının nasıl iyileştirilebileceğine yönelik ayrıntılı sistem analizi ve düzeltme işlemi için gelişmiş bir araçtır.

Uygulamalarım alanındaki uygulamalar hakkında ayrıntılı bilgi için ilgili bloğu tıklayın. Bileşeni hemen indirebileceğiniz AVG web sayfasına yönlendirilirsiniz.

5.5. Tara / Hızlı Bağlantıları Güncelle

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

- **Şimdi tara** - Düğme grafik olarak iki kısma ayrılmıştır. **Şimdi tara** bağlantısını izleyerek [Tüm Bilgisayarı Tara](#) işlemini hemen başlatabilir ve ilerleme ile sonuçları otomatik olarak açılan [Raporlar](#) penceresinden izleyebilirsiniz. **Seçenekler** düğmesi **Tarama Seçenekleri** iletişim kutusunu açar; burada [zamanlanmış taramaları yönetebilir](#) ve [Tüm Bilgisayarı Tara / Belirli Dosyaları veya Klasörleri Tara](#) parametrelerini düzenleyebilirsiniz. (*Ayrıntılar için [AVG Tarama](#) bölümüne bakın*)
- **Performansı onar** - Düğme sizi bilgisayarınızın hızının ve genel performansının nasıl iyileştirilebileceğine yönelik ayrıntılı sistem analizi ve düzeltme aracı olan [PC Analyzer](#) servisine götürür.







- **Şimdi güncelle** - Ürün güncellemesini hemen başlatmak için düğmeye basın. Güncelleme sonuçları hakkında AVG sistem tepsi simgesi üzerinde beliren iletişim kutusuyla bilgilendirilirsiniz. (Ayrıntılar için [AVG Güncellemeleri](#) bölümüne bakın)

5.6. Sistem Tepsisi Simgesi

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

AVG Sistem Tepsisi Simgesi görünümü

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

AVG Sistem Tepsisi Simgesi bilgileri



AVG Sistem Tepsisi Simgesi sistem tepsi simgesinden açılan bir açılır pencere yoluyla **AVG Internet Security** programınızda o an gerçekleşen etkinlikler ve programdaki olası durum değişiklikleriyle (ör. programlı bir tarama veya güncellemenin otomatik başlatılması, Güvenlik Duvarı profil değişikliği, bir bileşenin durum değişikliği, hata durumu oluşması vb.) ilgili de bilgilendirme yapar.

AVG Sistem Tepsisi Simgesi yoluyla erişilebilen işlemler

AVG Sistem Tepsisi Simgesi, **AVG Internet Security kullanıcı arayüzüne** erişmek için bir hızlı bağlantı olarak da kullanılabilir; bunun için simgeyi çift tıklatmak yeterlidir. Simgeyi sağ tıklatarak aşağıdaki en önemli özelliklerden bazılarını sunan kısa bir bağlam menüsü açarsınız:

- **Aç** – [ana kullanıcı arayüzünü](#) α | μακ | ι | ν β | υ δ | □ μεν | κ | λ | λαν □ ν.
- **Şimdi Tara** - [Tüm Bilgisayarı Tara](#) ι | λ | ε | μ | ν | β | α | λ | α | τ | α | κ | ι | ν β | υ δ | □ μεν | κ | λ | λαν □ ν.



- **Koruma** (etkinleştirildi  / devre dışı bırakıldı ) - gerçek zamanlı koruma sağlayan **AVG Internet Security** bileşenlerini kapatmak için bu düğmeyi kullanın. Artık, **AVG Internet Security** ürününün ne kadar uzun süre devre dışı kalacağını belirleyebilirsiniz. Burada Güvenlik Duvarı bileşeninin kapatılıp kapatılmayacağına da karar verebilirsiniz. Düğmeye tekrar tıklayarak **AVG Internet Security** korumasını istediğiniz zaman yeniden etkinleştirebilirsiniz.

5.7. AVG Tavsiyesi

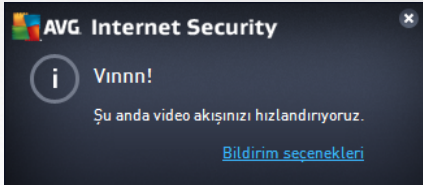
AVG Tavsiyesi bilgisayarınızı riske atabilecek sorunları tespit etmek ve durumu çözecek bir işlem önermek üzere tasarlanmıştır. **AVG Tavsiyesi** sistem tepsisi üzerinde kayan bir açılır pencere olarak görülebilir. Bu hizmet, olası **tanıdık ada sahip bilinmeyen bir ağ**ı tespit eder. Bu durum yalnızca, genellikle taşınabilir bilgisayarlar kullanıp birçok ağa bağlanan kullanıcılar için geçerlidir. Yeni, bilinmeyen bir ağ iyi bilinen, sık kullanılan bir ağla aynı ada sahipse (ör. *Ev veya BenimWifi*), karışıklık olabilir 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 ilerde tekrar rapor edilmez.

Desteklenen web tarayıcıları

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

5.8. AVG Hızlandırıcı

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





6. AVG Bileşenleri

6.1. Bilgisayar Koruması

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

- **Virüslerden Koruma** tüm dosyaları, bilgisayarın sistem alanlarını ve çıkarılabilir ortamları (*flash disk vb.*) koruyan bir tarama motoru barındırır ve bilinen virüsler için tarama yapar. Tespit edilen virüsler, harekete geçmeden engellenecek ve ardından silinecek ya da **Virüs Kasası**'nda karantinaya alınacaktır. Yerleşik koruma "arka planda" çalıştığından işlemin farkına bile varmazsınız. Virüslerden Koruma dosyaların tipik virüs özelliklerine karşı tarandığı buluşsal analiz taraması da kullanır. Bu, yeni bir virüs mevcut virüslerin tipik özelliklerinden bazılarını sahipse söz konusu Virüslerden Koruma tarayıcısının yeni ve bilinmeyen bir virüsü tespit edebileceği anlamına gelmektedir. **AVG Internet Security** 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 girişlere ve geçici internet dosyalarına karşı da tarar ve söz konusu potansiyel olarak istenmeyen nesnelere de diğer bulaşmalarla aynı şekilde düzeltmenizi sağlar.
- **Veri Kasası** içinde değerli veya hassas verileri saklayabileceğiniz sanal kasalar oluşturmanızı 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 (*Virüslerden Koruma veya Veri Kasası*) bağımsız olarak, aynıdır:

- **Etkinleştirildi / Devre dışı bırakıldı** - Düğme size hem görünüş hem de işlev olarak trafik ışıklarını hatırlatmış olabilir. İki konum arasında geçiş yapmak için tek tıklatın. Yeşil renk **Etkinleştirildi**,



yani AntiVirus güvenlik hizmetinin aktif ve tamamen çalışır durumda olduğu anlamına gelmektedir. Kırmızı renk ise **Devre dışı bırakıldı** 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 bilgisiyile olası riskler hakkında hemen uyarılırsınız. **Hizmeti mümkün olan en kısa sürede tekrar etkinleştirmeyi lütfen unutmayın!**

 **Ayarlar** - Düğmeyi tıklatarak [gelişmiş ayarlar](#) arayüzüne gidebilirsiniz. Tam olarak, ilgili iletişim kutusu açılır ve siz de burada seçilen hizmeti, yani [Virüslerden Koruma](#)'yı yapılandırabilirsiniz. Gelişmiş ayarlarda **AVG Internet Security** uygulamasındaki tüm güvenlik hizmetlerinin yapılandırmasını düzenleyebilirsiniz, ancak yapılandırma işlemi yalnızca deneyimli kullanıcılara önerilmektedir!

 **Ok** - Bileşen genel görünümünün 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 ada sahip yeni bir iletişim kutusu açmak için düğmeyi tıklatarak planladığınız kasanın parametrelerini belirleyebilirsiniz. Lütfen tüm gerekli bilgileri doldurun ve uygulamadaki talimatları izleyin:

Öncelikle, kasanın adını belirlemeniz ve güçlü bir parola oluşturmanız 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 oluştur / Parolayı yeniden yazın** - Veri kasanız için bir parola oluşturun ve parolayı ilgili metin 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** onay kutusunu işaretleyebilirsiniz (*tabii ki ekranınıza başka birinin bakmıyor olması koşuluyla*).

- **Parola ipucu** - Unutmanız durumunda size parolanızı hatırlatacak faydalı bir parola ipucu oluşturmanızı 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:

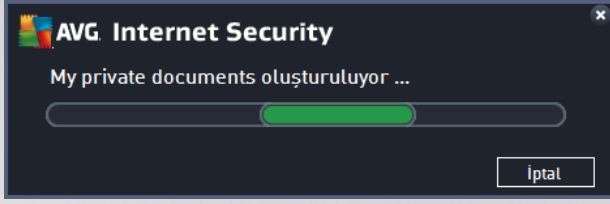


Bu iletişim kutusunun sağladığı yapılandırma seçenekleri:

- **Konum** veri kasasının fiziki olarak nereye yerleştirileceğini gösterir. Gözet düğmesiyle sabit diskinizde uygun bir konum belirleyebilir veya önceden tanımlanmış konumu (*Belgeler* klasörünüz) muhafaza edebilirsiniz. Bir veri kasası 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 kasasına 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.
- **Erişim** - bu bölümdeki onay kutuları veri kasanız için kullanışlı kısayollar oluşturmanıza olanak sağlar.

Veri kasanızı kullanma

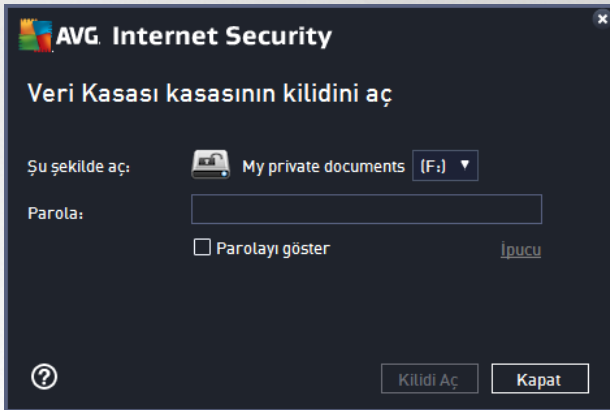
Ayarlardan memnun olduğunuzda **Kasa Oluştur** düğmesini tıklayın. Dosyalarınızı saklamak için kasanın hazır olduğunu belirten yeni bir **Veri Kasanız şimdi hazır** iletişim kutusu açılır. Artık kasa açıktır ve kasaya hemen erişebilirsiniz. Kasaya daha sonraki tüm erişim girişimlerinizde tanımlanmış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



Yeni veri kasanızı kullanabilmek için öncelikle **Şimdi Aç** düğmesini tıklatarak kasayı açmanız gerekir. Kasayı açtıktan sonra veri kasanızı 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 (*çoğunlukla sabit sürücünüze atanır*), A (*disket sürücüsü*) veya D (*DVD sürücüsü*) harflerini seçmenize izin verilmez. Bir veri kasanının kilidini her açışınızda kullanılabilir durumdaki sürücü harflerinden bir başkasını seçebileceğinizi lütfen unutmayın.

Veri kasanızın kilidini açma

Kasaya daha sonraki erişim girişiminizde tanımlamış olduğunuz parolayla kasanın kilidini açmanız istenecektir:



Metin alanında, kendinizi onaylamak için lütfen parolanızı yazın ve **Kilidi Aç** düğmesini tıklayın. Parolayı hatırlamakla ilgili yardıma ihtiyacınız varsa veri kasanızı oluştururken tanımladığınız parola ipucunu görüntülemek için İpucu'nu tıklayın. Yeni veri kasesi, veri kasanızın genel görünüm sayfasında KİLİDİ 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 tanır ve bilgisayarınıza girişini engellemek için indirme işlemini durdurur. Bu güçlü koruma, açmaya çalıştığınız web sayfalarının zararlı içeriğini engeller ve bilgisayarınıza karşıdan yüklenmesini önler. Bu özellik etkin durumdayken, tehlikeli bir site bağlantısı tıklatıldığında ya da URL'si yazıldığında otomatik olarak web sayfasını açmanız engellenir, bu sayede etkilenmeniz önlenmiş olur. Virüs bulaşmış web sayfalarını ziyaret ettiğinizde bilgisayarınıza kolayca virüs bulaşabileceğini gerçeğini hatırlamak çok önemlidir. **Online Shield'in sunucu platformlarının korunmasında kullanılması hedeflenmemiştir!**



İletişim kutusu kontrolleri

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

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

 **Ayarlar** - Düğmeyi tıklayarak [gelişmiş ayarlar](#) arayüzüne gidebilirsiniz. Tam olarak, ilgili iletişim kutusu açılır ve siz de burada [LinkScanner Sörf Kalkanı](#) veya [Online Shield](#) gibi seçtiğiniz bir hizmetin yapılandırmasını yapabilirsiniz. Gelişmiş ayarlarda **AVG Internet Security** uygulamasındaki tüm



güvenlik hizmetlerinin yapılandırmasını düzenleyebilirsiniz, ancak yapılandırma işlemi yalnızca deneyimli kullanıcılara önerilmektedir!

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

6.3. Software Analyzer

Software Analyzer bileşeni internette dijital varlıklarınızı yeni ve bilinmeyen tehditlere karşı sürekli korur:


- **Software Analyzer** zararlı yazılımlara karşı koruma hizmetidir; davranış teknolojilerini kullanarak ve yeni virüsler için ilk günden koruma sağlayarak sizi her türlü zararlı 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 (*zararlı yazılım*) çalan kimlik hırsızlığı üzerine odaklanmıştır. Bilgisayarınızda ve paylaşılan ağınızda çalışan tüm programların düzgün biçimde çalışmasını sağlar. Software Analyzer, sürekli olarak şüpheli davranışları belirleyip engeller ve tüm yeni kötü amaçlı yazılımlara karşı bilgisayarınızı korur. Software Analyzer, 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, Software Analyzer kodu [Virüs Kasası](#)'na kaldırır ve sistemde yapılan tüm değişiklikleri (*kod bulaşmaları, kayıt defteri değişiklikleri, bağlantı noktası açma vb.*) geri alır. Korunmak için tarama başlatmanız gerekmez. Bu teknoloji çok öngörülüdür, nadiren güncellemeye gereksinim duyar ve her an korur.





İletişim kutusu kontrolleri

Bu iletişim kutusunda aşağıdaki kontrolleri bulabilirsiniz:



 **Etkinleştirildi / Devre dışı bırakıldı** - Düğme size hem görünüş hem de işlev olarak trafik ışıklarını hatırlatmış olabilir. İki konum arasında geçiş yapmak için tek tıklatın. Yeşil renk **Etkinleştirildi**, yani Software Analyzer güvenlik hizmetinin aktif ve tamamen çalışır durumda olduğu anlamına gelmektedir. Kırmızı renk ise **Devre dışı bırakıldı** durumunu temsil etmektedir; yani hizmet devre dışı bırakılmıştır. Hizmeti devre dışı bırakmak için iyi bir nedeniniz yoksa tüm güvenlik yapılandırması için varsayılan ayarları kesinlikle değiştirmemenizi 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 bilgisiyle olası riskler hakkında hemen uyarılırsınız. **Hizmeti mümkün olan en kısa sürede tekrar etkinleştirmeyi lütfen unutmayın!**

 **Ayarlar** - Düğmeyi tıklayarak [gelişmiş ayarlar](#) arayüzüne gidebilirsiniz. Tam olarak, ilgili iletişim kutusu açılır ve siz de burada seçilen hizmeti, yani [Software Analyzer](#)'ı yapılandırabilirsiniz. Gelişmiş ayarlarda **AVG Internet Security** uygulamasındaki tüm güvenlik hizmetlerinin yapılandırmasını düzenleyebilirsiniz, ancak yapılandırma işlemi yalnızca deneyimli kullanıcılara önerilmektedir!

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

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

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

6.4. E-posta Koruması

E-posta Koruması bileşeni aşağıdaki iki güvenlik hizmetini kapsar: **E-posta Tarayıcısı** ve **Anti-Spam** (Anti-Spam hizmeti yalnızca Internet / Premium Security sürümlerinde erişilebilirdir).

- **E-posta Tarayıcısı**: Virüsler ve truva atları yaygın olarak e-postalar aracılığıyla yayılır. Kimlik avı ve istenmeyen postalar, e-postaları daha büyük risk kaynakları haline getirmektedir. Ücretsiz e-posta hesaplarının zararlı e-postaları alma ihtimali daha yüksek olup (*nadiren istenmeyen posta önleme teknolojisine sahip olmaları nedeniyle*) ev kullanıcıları büyük çoğunlukla söz konusu e-postaları kullanır. Bunun yanı sıra, bilmedikleri sitelerde dolaşan ve çevrimiçi formları kişisel bilgileri ile dolduran (*e-posta adresleri gibi*) ev kullanıcıları, e-posta saldırılarına sıklıkla maruz kalmaktadır. Şirketler genellikle kurumsal e-posta hesapları kullanmakta ve riskleri en aza indirmek için istenmeyen posta önleme filtrelerinden yararlanmaktadır. E-posta Koruması bileşeni, alınan veya gönderilen her e-posta iletilisini taramakla sorumludur. Bir e-postada virüs tespit edildiğinde, hemen [Virüs Kasası](#)'na kaldırır. Söz konusu bileşen belirli türde e-posta eklerine filtre uygulayabilir ve virüs bulunmayan mesajları bir onay metni ekleyebilir. **E-posta Tarayıcısının 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. Spam, müşterinin kendi isteğiyle almayı kabul ettiği yasal ticari e-posta anlamına gelmemektedir.*). 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 tespit etmek için





düzenli olarak güncellenen veritabanı kullanır. [RBL sunucularını](#) kullanmak ("bilinen istenmeyen posta göndericisi" e-posta adreslerinden oluşan genel veritabanları) ve [Beyaz listenize](#) (hiçbir zaman istenmeyen posta olarak işaretleme) ve [Kara listenize](#) (her zaman istenmeyen posta olarak işaretle) elle e-posta adresleri eklemek mümkündür.



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 şu güvenlik servisine ait olmasından bağımsız olarak işlevleri aynıdır (*E-posta Tarayıcısı* veya *Anti-Spam*):

 **Etkinleştirildi / Devre dışı bırakıldı** - Düğme size hem görünüş hem de işlev olarak trafik ışıklarını hatırlatmış olabilir. İki konum arasında geçiş yapmak için tek tıklatın. Yeşil renk **Etkinleştirildi**, yani güvenlik hizmetinin etkin ve tamamen çalışır durumda olduğu anlamına gelmektedir. Kırmızı renk ise **Devre dışı bırakıldı** durumunu temsil etmektedir; yani hizmet devre dışı bırakılmıştır. Hizmeti devre dışı bırakmak için iyi bir nedeniniz yoksa tüm güvenlik yapılandırması için varsayılan ayarları kesinlikle değiştirmemenizi 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!**

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

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



6.5. Güvenlik Duvarı

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

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

AVG Güvenlik Duvarı bileşeninin sunucu platformlarının korunmasında kullanılması hedeflenmemiştir!

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



Not: AVG Internet Security yüklemenizin ardından Güvenlik Duvarı bileşeni bilgisayarın yeniden başlatılmasını gerektirebilir. Bu durumda bileşenin iletişim kutusu yeniden başlatma gerektiği bilgisiyile birlikte görüntülenir.



Doğrudan iletişim kutusunun içinde **Şimdi yeniden başlat** düğmesini kullanabilirsiniz. Yeniden başlatmaya kadar Güvenlik Duvarı bileşeni tam olarak etkinleşmez. Ayrıca, iletişim kutusundaki tüm düzenleme seçenekleri devre dışı bırakılır. Lütfen uyarıyı dikkate alın ve bilgisayarınızı en kısa süre içinde yeniden başlatın!

Mevcut Güvenlik Duvarı modları

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

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

Not: Güvenlik Duvarı içinde de bir otomatik mod mevcuttur. Bu mod, [Bilgisayar](#) veya [Software Analyzer](#) bileşeni kapatıldığında ve bu nedenle bilgisayarınız tehditlere açık hale geldiğinde sessizce etkinleştirilir. Bu tür durumlarda, Güvenlik Duvarı yalnızca bilinen veya kesinlikle güvenli uygulamalara otomatik olarak izin verir. Diğer tüm uygulamalar için sizin karar vermeniz istenir. Bunun nedeni devre dışı bırakılan bileşenlerin boşluğunu kapatmak ve bilgisayarınızı güvende tutmaktır.

Güvenlik Duvarı'nı kesinlikle kapatmamanızı tavsiye ederiz! Bununla birlikte, ihtiyaç olması ve Güvenlik Duvarı bileşenini gerçekten devre dışı bırakmanız gerektiğinde, mevcut Güvenlik Duvarı modlarının üstündeki listeden Güvenlik Duvarı korumasını devre dışı bırakma modunu seçerek bu işlemi yapabilirsiniz.

İletişim kutusu kontrolleri

Bu iletişim kutusu Güvenlik Duvarı bileşen durumu hakkındaki temel bilgileri gösterir:

- **Güvenlik Duvarı modu** - Geçerli olarak seçili Güvenlik Duvarı modu hakkındaki bilgileri gösterir. Geçerli modu bir başka modla değiştirmek istiyorsanız, gösterilen bilginin yanındaki **Değiştir**



düğmesini kullanarak [Güvenlik Duvarı ayarları](#) arayüzüne geçebilirsiniz (*Güvenlik Duvarı profillerinin açıklamaları ve öneriler için lütfen önceki paragrafa bakın*).

- **Dosya ve yazıcı paylaşımı** - O anda dosya veya yazıcı paylaşımına (*her iki yönde de*) izin verilip verilmediği bilgisini gösterir. Dosya ve yazıcı paylaşımı Windows, ortak disk birimleri, yazıcılar, tarayıcılar ve tüm benzer cihazlarda "Paylaşılan" olarak işaretlediğiniz tüm dosyalar veya klasörler anlamına gelmektedir. Bu tür öğelerin paylaşımı yalnızca güvenli olduğu düşünülen ağlarda gerçekleştirilmelidir (*örneğin evde, işte veya okulda*). Ancak, herkese açık ağlara (*havaalanı Wi-Fi veya internet kafe ağı gibi*) bağlanıyorsanız, hiçbir şey paylaşmak istemeyebilirsiniz.
- **Şuna bağlandı** - Geçerli olarak bağlı olduğunuz ağın adıyla ilgili bilgileri gösterir. Window XP'de, ağ adı ilgili ağa ilk bağlandığınızda ağ için seçtiğiniz adlandırmaya karşılık gelir. Windows Vista ve üstü sistemlerde, ağ adı Ağ ve Paylaşım Merkezi'nden otomatik olarak alınır.
- **Varsayılanla sıfırla** - Geçerli Güvenlik Duvarı yapılandırmasının üzerine yazmak ve otomatik tespite bağlı olarak varsayılan yapılandırmaya geri dönmek için bu düğmeye basın.

İletişim kutusundaki grafik kontrolleri:



Ayarlar - İki adet seçenek sunan açılır menüye erişmek için düğmeyi tıklatın:

- **Gelişmiş ayarlar** - bu seçenek sizi tüm Güvenlik Duvarı yapılandırmasını düzenleyebileceğiniz [Güvenlik Duvarı ayarları](#) arayüzüne yönlendirir. Ancak, tüm yapılandırma işlemlerinin sadece deneyimli kullanıcılar tarafından yapılması gerektiğini unutmayın!
- **Güvenlik Duvarı korumasını kaldır** - bu seçenek işaretlenirse Güvenlik Duvarı bileşeni kaldırılır ve bu durum korumanızı zayıflatabilir. Güvenlik Duvarı bileşenini yine de kaldırmak istiyorsanız kararınızı onaylayın; bu durumda bileşen tamamen kaldırılır.



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

6.6. PC Analyzer

PC Analyzer bileşeni, bilgisayarınızın hızının ve genel performansının nasıl iyileştirilebileceğine yönelik ayrıntılı sistem analizi ve düzeltme işlemi için gelişmiş bir araçtır. Araç, [ana kullanıcı arayüzü iletişim kutusundaki Performansı onar](#) düğmesi veya [sistem tepsisindeki AVG simgesinin](#) bağlam menüsünde listelenen aynı seçenikle açılır. Bundan sonra, analiz sürecini ve sonuçlarını söz konusu tabloda doğrudan izleyebilirsiniz:



Kategorisi	Sonuçlar	Önem derecesi
Kayıt Defteri Hataları Hatalar sistem kararlılığını etkiler	114 hata bulundu Ayrıntılar...	
Önemsiz Dosyalar Bu dosyalar disk alanını doldurur	7939 hata bulundu Ayrıntılar...	
Parçalanma Disk erişim hızını düşürür	10% parçalanmış Ayrıntılar...	
Bozuk Kısayollar Gezginin tarama hızını düşürür	31 hata bulundu Ayrıntılar...	

Hataları gidermek için bir kereliğine ücretsiz yeni [AVG PC TuneUp](#) yazılımını indirin veya sınırsız Tuneup yazılımını 12 aylığına satın alın. [Şimdi onar](#)

sürüm 14.131.7921

Analiz edilebilir kategoriler: kayıt defteri hataları, önemsiz dosyalar, parçalanma ve bozuk kısayollar:

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

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

- **Analizi durdur** (analiz çalışırken görüntülenir) - bilgisayarınızın analizini hemen durdurmak için bu düğmeye basın.
- **Şimdi onar** (analiz tamamlandığında görüntülenir) - Ne yazık ki, **AVG Internet Security** içindeki PC Analyzer işlevselliği PC'nizin geçerli durum analiziyle sınırlıdır. Ancak, AVG bilgisayarınızın hızının ve genel performansının nasıl iyileştirilebileceğine yönelik ayrıntılı sistem analizi ve düzeltme işlemi için gelişmiş bir araç sağlar. Daha fazla bilgi için ilgili web sitesine yönlendirilmek üzere düğmeyi tıklayın.

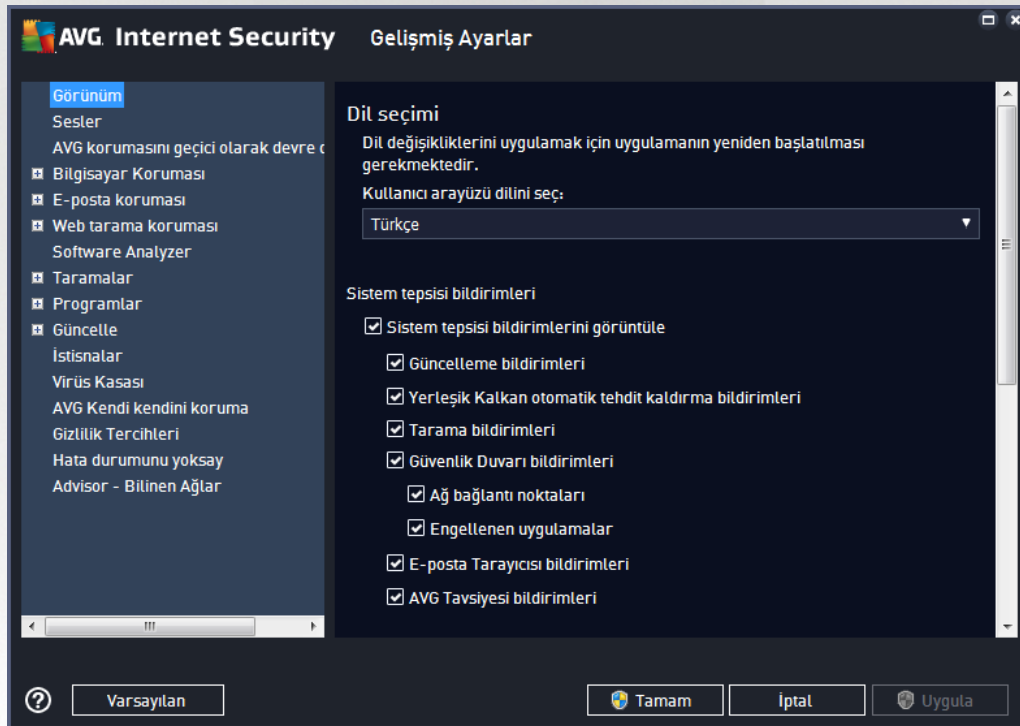


7. AVG Gelişmiş Ayarlar

AVG Internet Security 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.

7.1. Görünüm

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



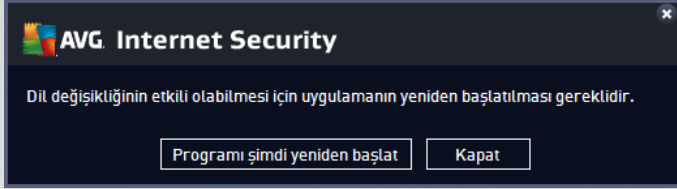
Dil seçimi

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

- Açılır menüde istediğiniz uygulama dilini seçin
- **Uygula** düğmesine (*iletişim kutusunun sağ alt tarafında*) basarak seçiminizi onaylayın
- Onaylamak için **Tamam** düğmesine basın
- Uygulamanın dilini değiştirmek için **AVG Internet Security** uygulamanın yeniden başlatılması için gerekli olan iletişim kutusunun sağ alt tarafında bulunan **Uygula** düğmesine basın



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



Sistem tepsi bildirimleri

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

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

- **Sistem tepsi bildirimlerini görüntüle** (varsayılan olarak açık) - varsayılan olarak tüm bildirimler görüntülenir. Tüm sistem bildirimleri kapatmak için bu öğenin işaretini kaldırın. Açıldığı zaman hangi bildirimlerin görüntüleneceğini de seçebilirsiniz:
 - **Güncelleme bildirimleri** (varsayılan olarak açık) - **AVG Internet Security** güncelleme işleminin başlaması, ilerleyişi ve bitişi hakkında bilgilerin görüntülenmesini isteyip istemediğinize karar verin.
 - **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 sa gösterilir*) karar verin.
 - **Tarama bildirimleri** (varsayılan olarak açık) - programlı taramaların otomatik olarak başlaması, ilerleyişi ve sonuçları hakkında bilgilerin görüntülenmesini isteyip istemediğinize karar verin.
 - **Güvenlik Duvarı bildirimleri** (varsayılan olarak açık) - Güvenlik Duvarı durum ve işlemleri hakkındaki bilgiler (ör. bileşenin etkinleştirilmesi/devre dışı bırakılması uyarıları, olası trafik engelleme vb.) görüntülemek isteyip istemediğinize karar verin. Bu öğe iki adet seçim opsiyonu daha sağlar (*her biri hakkında daha fazla bilgi için lütfen bu belgedeki [Güvenlik Duvarı](#) bölümüne bakın*):
 - **Ağ bağlantı noktaları** (varsayılan olarak kapalı) - bir ağa bağlanırken, Güvenlik Duvarı ağı bilip bilmediği ve dosya ve yazıcı paylaşımının nasıl ayarlanacağı konusunda bilgilendirme yapar.
 - **Engellenmiş uygulamalar** (varsayılan olarak açık) - ağa bilinmeyen veya şüpheli bir uygulama bağlanmaya çalışıldığında Güvenlik Duvarı girişimi engeller ve bir bildirim görüntüler. Bu bilgilendirme açısından iyidir, bu yüzden özelliği daima açık tutmanızı öneririz.



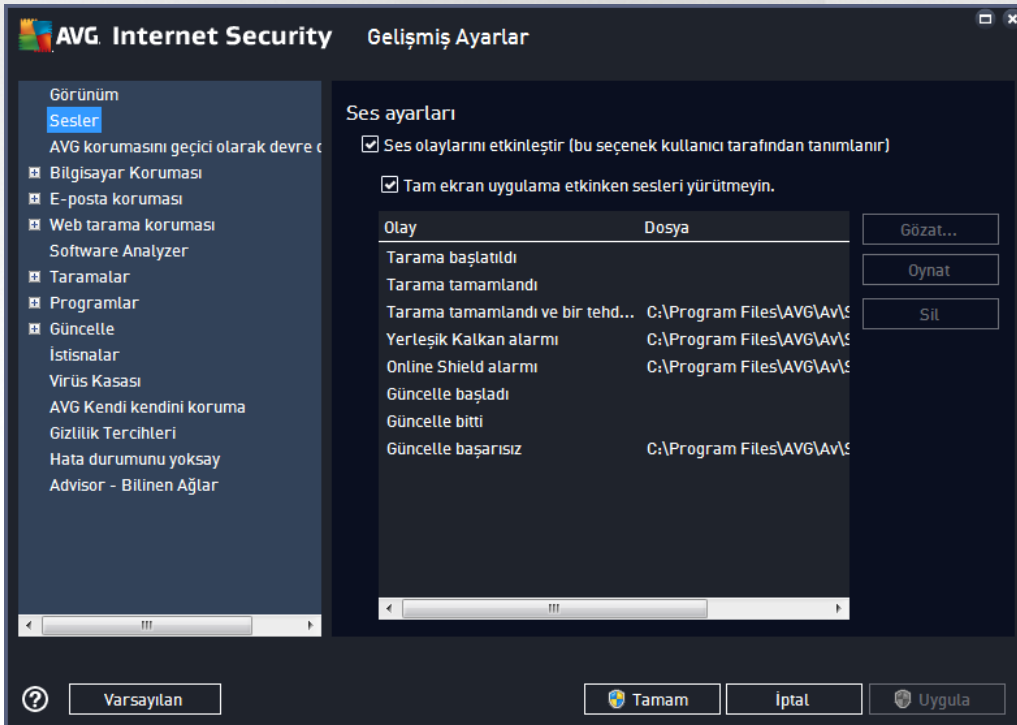
- o **E-posta Tarayıcısı bildirimleri** (varsayılan olarak açık) - gelen ve giden e-posta mesajlarının taranmasına ilişkin bildirimleri görüntülemek isteyip istemediğinize karar verin.
- o **İstatistiksel bildirimler** (varsayılan olarak açık) - düzenli istatistiksel inceleme uyarılarının sistem tepesinde görüntülenmesine izin vermek için bu seçeneği işaretli halde bırakın.
- o **AVG Tavsiyesi bildirimleri** (varsayılan olarak açık) - [AVG Tavsiyesi](#) etkinlikleri hakkındaki bilgilerin sistem tepsi panelinde görüntülenmesini isteyip istemediğinize karar verin.

Oyun modu

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

7.2. Sesler

Ses Ayarları iletişim kutusunda belirli **AVG Internet Security** işlemleri hakkında bir ses bildirimiyile bilgilendirilmek isteyip istemediğinizi belirleyebilirsiniz:



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



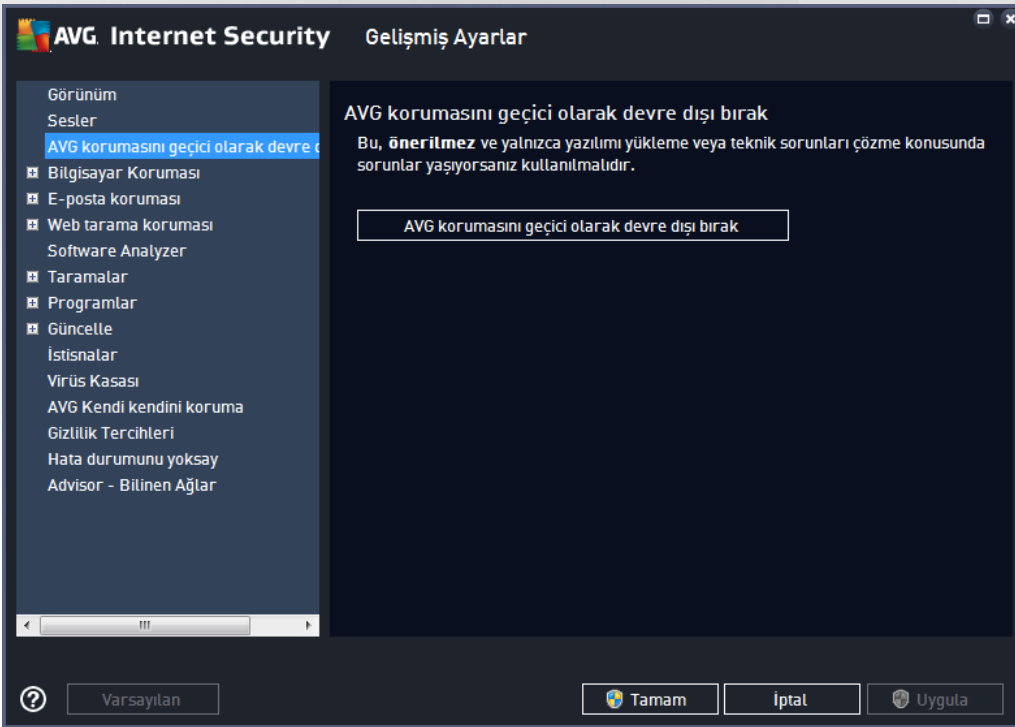
Kontrol düğmeleri

- **Gözet...** - diskinizde atamak istediğiniz ilgili ses dosyasını aramak için listeden ilgili eylem seçilmiş olarak **Gözet** düğmesini kullanın. (*Şu anda yalnızca *.wav seslerinin desteklenmekte olduğunu lütfen unutmayın!*)
- **Çal** - seçili sesi dinlemek için listede olayı vurgulayın ve **Çal** düğmesine basın.
- **Sil** - belirli olaya atanan sesi kaldırmak için **Sil** düğmesini kullanın.

7.3. AVG korumasını geçici olarak devre dışı bırak

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

Mutlaka gerekli değilse, bu seçeneği kullanmamanız gerektiğini lütfen unutmayın!

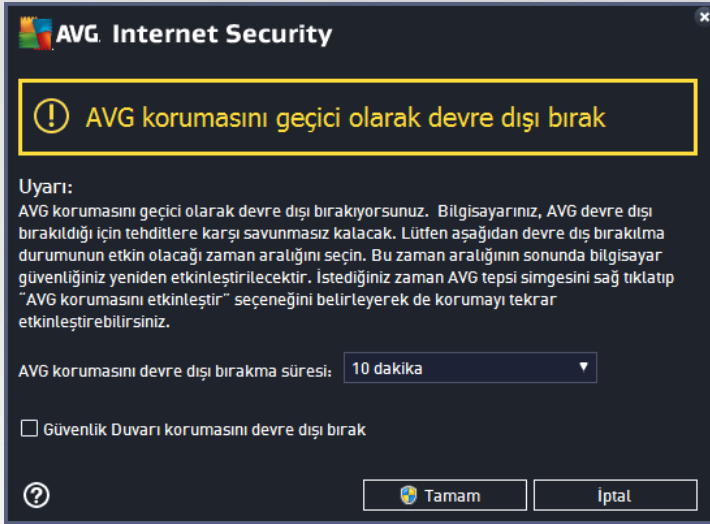


Çoğu durumda, **yeni yazılımı veya sürücülerini yüklemeyen** önce ve hatta yükleyici veya yazılım sihirbazı yükleme işlemi sırasında istenmeyen kesintilerin olmamasını sağlamak için çalışan program ve uygulamaların kapatılmasını önerse bile **AVG Internet Security** uygulamasını devre dışı bırakmak gerekmez.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



AVG koruması geçici olarak nasıl devre dışı bırakılır

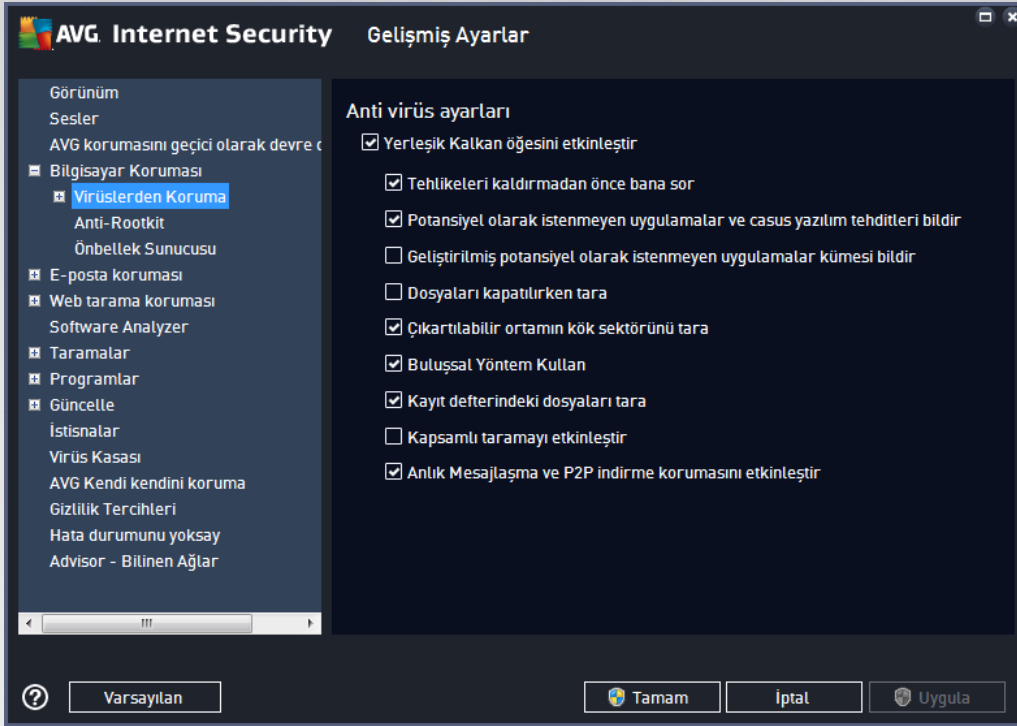
AVG korumasını geçici olarak devre dışı bırak onay kutusunu işaretleyin ve **Uygula** düğmesine basarak seçiminizi onaylayın. Yeni açılan **AVG korumasını geçici olarak devre dışı bırak** iletişim kutusunda **AVG Internet Security** uygulamanızı ne kadar süreyle devre dışı bırakmak istediğinizi belirleyin. 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. **Güvenlik Duvarı** bileşenini ayrı olarak devre dışı bırakma seçeneği **AVG korumasını geçici olarak devre dışı bırak** iletişim kutusunda yer alır. **Güvenlik Duvarı korumasını devre dışı bırak** kutusunu işaretleyerek bu işlemi gerçekleştirebilirsiniz.



7.4. Bilgisayar Koruması

7.4.1. Virüslerden Koruma

Virüslerden Koruma, **Yerleşik 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*).



Yerleşik Kalkan Ayarları iletişim kutusunda yerleşik korumayı **Yerleşik Kalkan'ı etkinleştir** öğesini işaretleyerek ya da işaretini kaldırarak etkinleştirebilir ya da devre dışı bırakabilirsiniz (*bu seçenek varsayılan olarak açıktır*). Ayrıca yerleşik korumanın hangi özelliklerinin etkinleştirileceğini seçebilirsiniz:

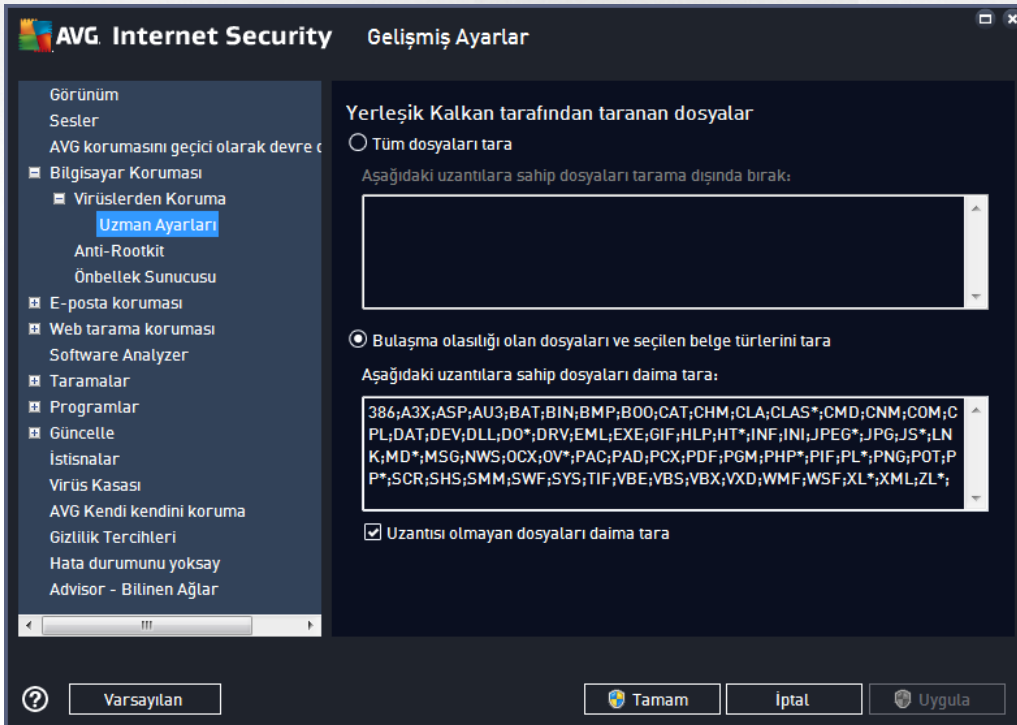
- **Tehlikeleri kaldırmadan önce bana sor** (*varsayılan olarak açık*) - Yerleşik Kalkan'ın hiçbir işlemi otomatik olarak yapmaması; bunun yerine, tespit edilen tehdidi ne yapacağınıza karar vermeniz için göstermesini sağlamak amacıyla işaretleyin. Kutuyu işaretlemeyeniz **AVG Internet Security** bulaşmayı otomatik olarak temizler; bu mümkün değilse nesne [Virüs Kasası](#)'na taşınır.
- **Potansiyel olarak istenmeyen uygulamalar ve casus yazılım tehditlerini bildir** (*varsayılan olarak açık*) - virüslerin yanı sıra casus yazılımları da taramak için işaretleyin. Casus yazılım, şüpheli zararlı 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 uygulamalar geliştirilmiş grubunu bildir** (*varsayılan olarak kapalı*) - casus yazılımların, yani doğrudan üreticiden alındığında 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.
- **Dosyaları kapatılırken tara** (*varsayılan olarak kapalı*) - işlem sonunda tarama, AVG'nin etkin nesnelere (ör. uygulamalar, belgeler vb.) hem açılırken hem de kapatılırken taradığından emin olmanızı sağlar. Bu özellik bilgisayarınızı bazı karmaşık virüs türlerine karşı korumanıza yardımcı olur.
- **Çıkarılabilir ortamın kök sektörünü tara** (*varsayılan olarak açık*) - takılı USB flaş disklerin, harici disk sürücülerinin ve diğer çıkarılabilir ortamların kök sektörlerini tehditlere karşı taramak için işaretleyin.



- **Buluşsal Yöntem Kullan** (varsayılan olarak açık) - buluşsal analiz, tespit işlemi sırasında kullanılır (taranan nesnenin yönergelerinin sanal bilgisayar ortamında dinamik olarak canlandırılması).
- **Kayıt defterindeki dosyaları tara** (varsayılan olarak açık) - bilinen bulaşmanın sonraki bilgisayar başlangıcında çalıştırılmasını önlemek için, başlangıç kayıt defterine eklenmiş tüm çalıştırılabilir dosyaları AVG'nin taradığını bu parametre tanımlar.
- **Kapsamlı taramayı etkinleştir** (varsayılan olarak kapalı) - belirli durumlarda (çok acil bir durum olduğunda) olası tehdit barındıran tüm nesnelerin derinlemesine 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 vb.) ve Eşler 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.

Not: Windows 10 işletim sistemi üzerinde AVG yüklüyse listede **Daha kapsamlı yazılım taraması için Windows Zararlı Yazılım Koruma Taraması Arayüzünü Etkinleştir** olarak adlandırılan bir seçenek de mevcuttur. Bu özellik, Windows işletim sisteminin ve AVG yazılımının zararlı yazılım kodlarını ortaya çıkarmada daha yakın bir işbirliği içerisinde bulunmalarını sağlarken, korumayı daha güvenilir bir hale getirip hatalı uyarıların sayısını azaltarak virüs korumasının geliştirilmesini sağlar.

Yerleşik Kalkan Tarafından Taranan Dosyalar iletişim kutusunda hangi dosyaların taranacağını yapılandırmak mümkündür (belirli dosya uzantılarına göre):



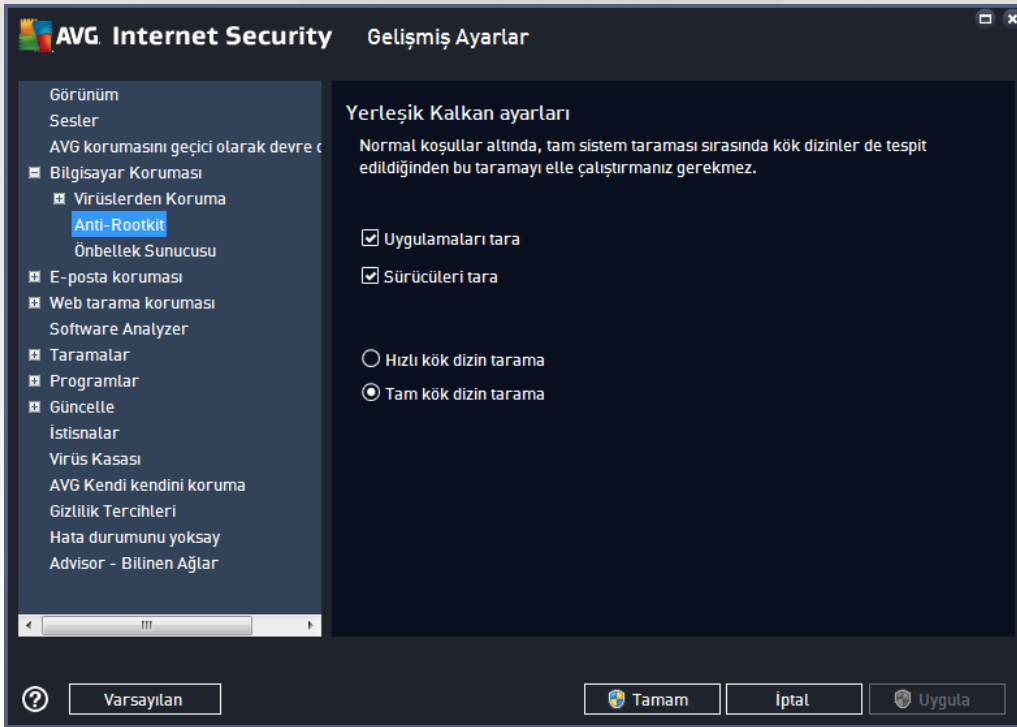


Tüm dosyaları tara veya yalnızca **Bulaşma olasılığı olan dosyaları ve seçilen belge türlerini tara** seçimi yapmak için ilgili onay kutusunu işaretleyin. Taramayı hızlandırmak ve aynı zamanda maksimum koruma düzeyi sağlamak için varsayılan ayarları korumanızı öneririz. Bu sayede yalnızca virüs bulaşabilecek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

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

7.4.2. 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 işlemdir:



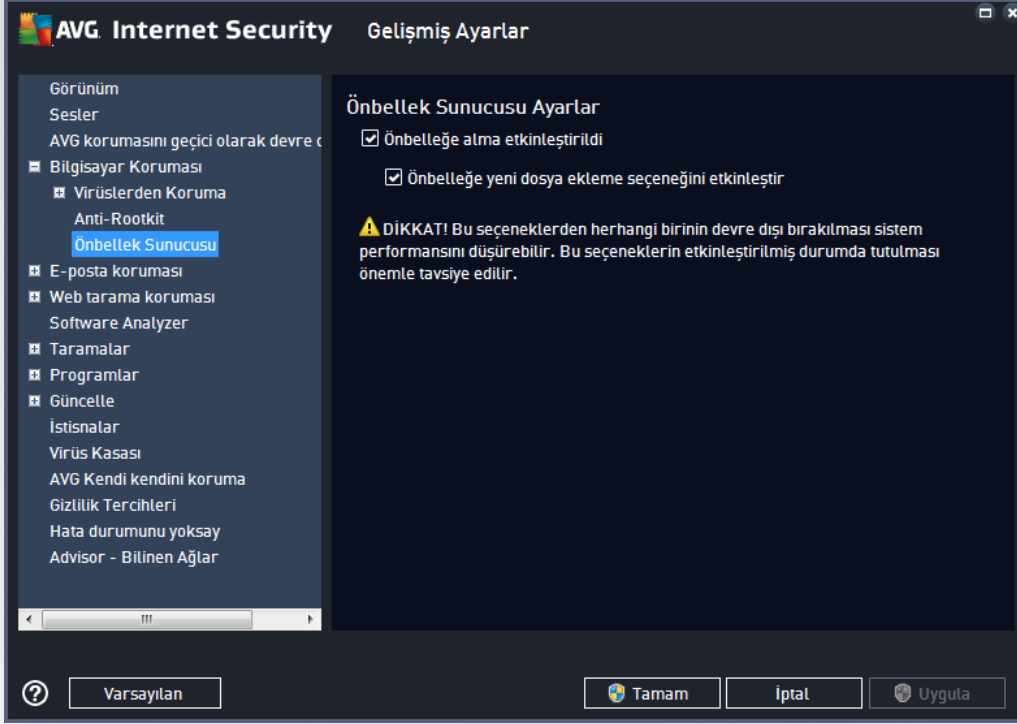
Tarama uygulamaları ve **Tarama sürücülerini** anti-rootkit taramasına nelerin dahil edileceğini ayrıntılı şekilde belirlemenize olanak tanır. Bu ayarlar gelişmiş kullanıcılara yöneliktir; tüm seçenekleri açık konumda muhafaza etmenizi öneririz. Rootkit tarama modunu da seçebilirsiniz:

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



7.4.3. Önbellek Sunucusu

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



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

Önbellek Sunucusu Ayarları iletişim kutusu aşağıdaki yapılandırma seçeneklerini sunar:

- **Önbelleğe alma etkinleştirildi** (*varsayılan olarak açık*) - **Önbellek Sunucusu**'nu kapatmak için kutunun işareti kaldırın ve önbellek belleğini boşaltın. Kullanılan her dosya öncelikle virüslere ve casus yazılımlara karşı taranacağından, taramanın yavaşlayabileceğini ve bilgisayarın genel performansının düşebileceğini unutmayın.
- **Önbelleğe yeni dosya ekleme seçeneğini etkinleştir** (*varsayılan olarak açık*) - önbelleğe daha fazla dosya eklenmesini durdurmak için kutunun işaretini kaldırın. Zaten önbelleğe alınmış dosyalar, önbelleğe alma işlemi tamamen kapatılana kadar veya bir sonraki virüs veritabanı güncellemesine kadar saklanır ve kullanılır.

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.

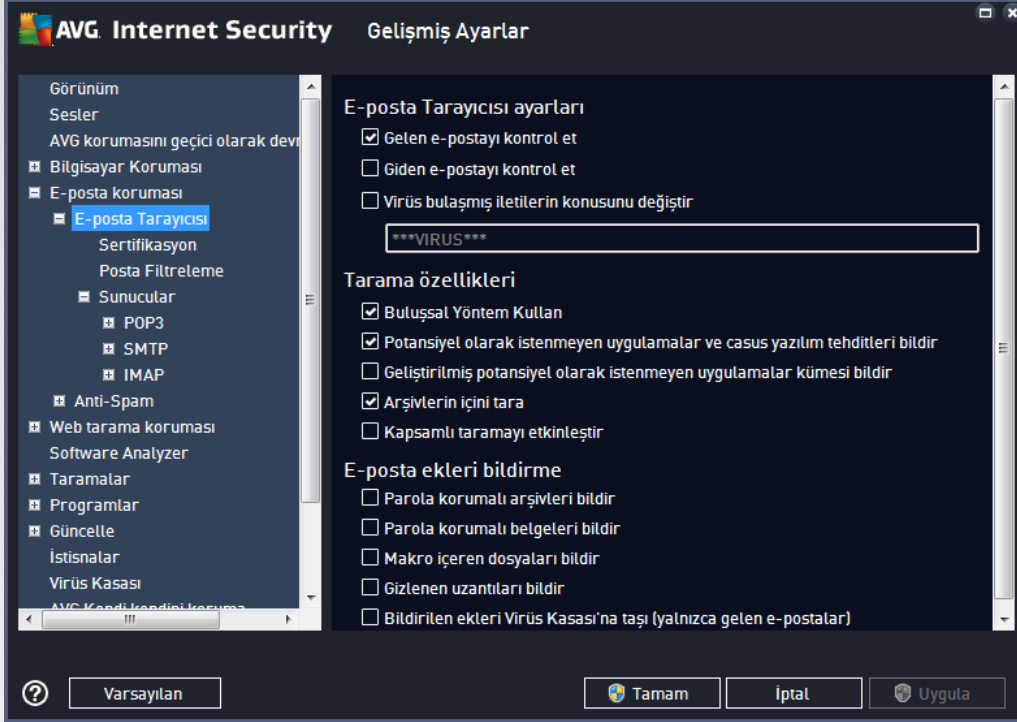
7.5. E-posta Tarayıcısı

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



7.5.1. 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 kontrol et** (*varsayılan olarak açık*) - e-posta istemcinize gelen tüm e-postaları tarama seçeneğini açmak/kapatmak için işaretleyin
- **Giden e-postayı kontrol et** (*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 mesajının 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 mesajının "Konu" alanına eklenecektir. Varsayılan değer *****VIRUS***** olarak belirlenmiştir ve bu değeri korumanızı öneririz.

Tarama özellikleri

Bu bölümde, e-posta iletilerinin nasıl taranacağını belirleyebilirsiniz:

- **Buluşsal Yöntem Kullan** (*varsayılan olarak açık*) - e-posta mesajlarını tararken buluşsal tespit yöntemi kullanmak için işaretleyin. Bu seçenek açık olduğunda, e-posta eklerini yalnızca uzantıya göre filtreleyemezsiniz; ekin gerçek içeriği de göz önünde bulundurulur. Filtreleme işlemi [Posta Filtreleme](#) iletişim kutusundan ayarlanabilir.



- **Potansiyel Olarak İstenmeyen Uygulamalar ve Casus Yazılım tehditlerini bildir** (varsayılan olarak açık) - virüslerin yanı sıra casus yazılımları da taramak için işaretleyin. Casus yazılım, şüpheli zararlı 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 İstenmeyen Uygulamalar geliştirilmiş grubunu bildir** (varsayılan olarak kapalı) - Casus yazılımların, yani doğrudan üreticiden alındığında 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.
- **Arşivlerin içeriğini tara** (varsayılan olarak açık) - e-posta mesajlarına 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 aldığı unutulmamalıdır.

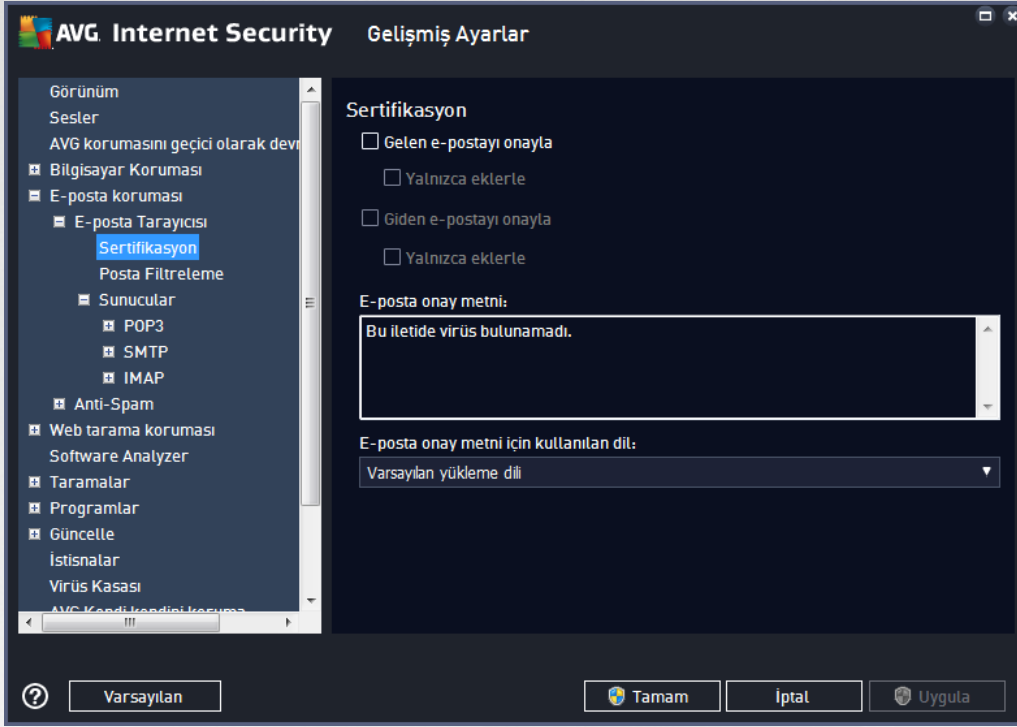
E-posta eklerini bildirme

Bu bölümde, potansiyel olarak tehlikeli ve şüpheli olan dosyalar için ek raporlar ayarlayabilirsiniz. Lütfen bir uyarı iletişim kutusu görüntülenmeyeceğini unutmayın. Yalnızca e-posta mesajının 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 yönergeler içerebilir. Makro içeren dosyaların şüpheli olarak bildirilmesini sağlamak için kutuyu işaretleyebilirsiniz.
- **Gizlenen uzantıları bildir** - gizli uzantılar şüpheli bir çalıştırılabilir dosyayı (ör. "birşey.txt.exe") zararsız bir düz metin dosyası gibi (ör. "birşey.txt") gösterebilir; bunları potansiyel olarak tehlikeli olarak bildirmek için kutuyu işaretleyin.
- **Rapor edilen ekleri Virüs Kasası'na taşı** - taranan e-posta iletilisinin 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.

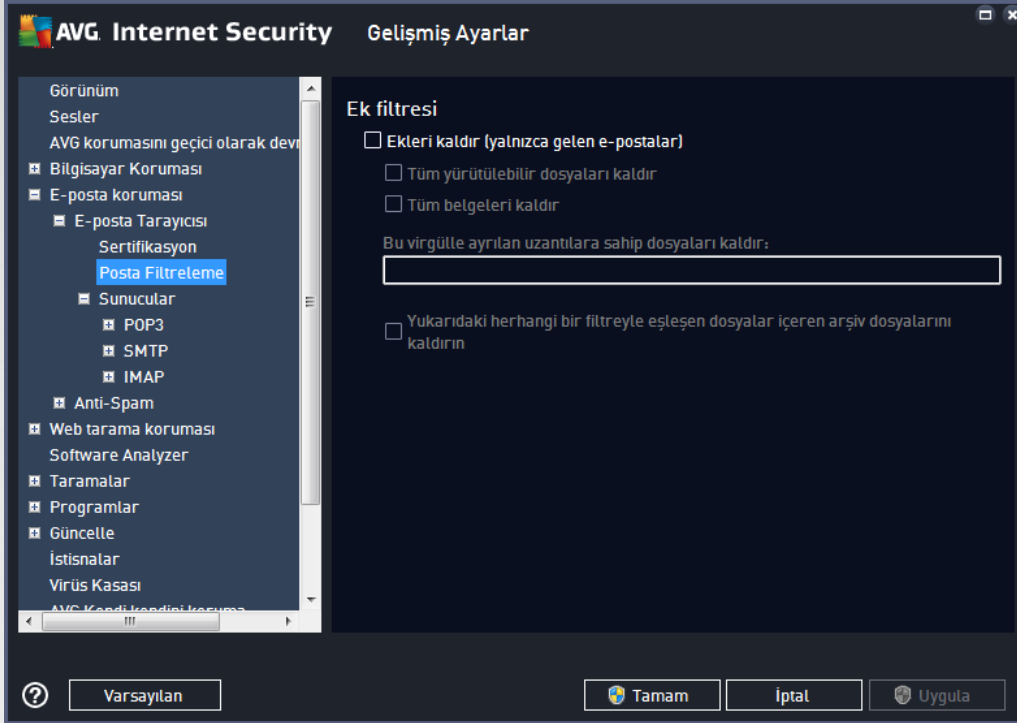


Sertifikasyon iletişim kutusunda gelen (**Gelen e-postayı onayla**) ve/veya giden e-postaları onaylamaya (**Giden e-postayı onayla**) veya onaylamamaya karar vermek için çeşitli onay kutularını işaretleyebilirsiniz. Bu seçeneklerin her biri için **Yalnızca eklerle** parametresini işaretleyip onayın yalnızca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



Varsayılan olarak, onay mesajı şunun gibi temel bilgiler içerir: *Bu mesajda 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 mesajda virüs bulunamadı*) hangi dilde görüntüleneceğini de belirleyebilirsiniz.

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



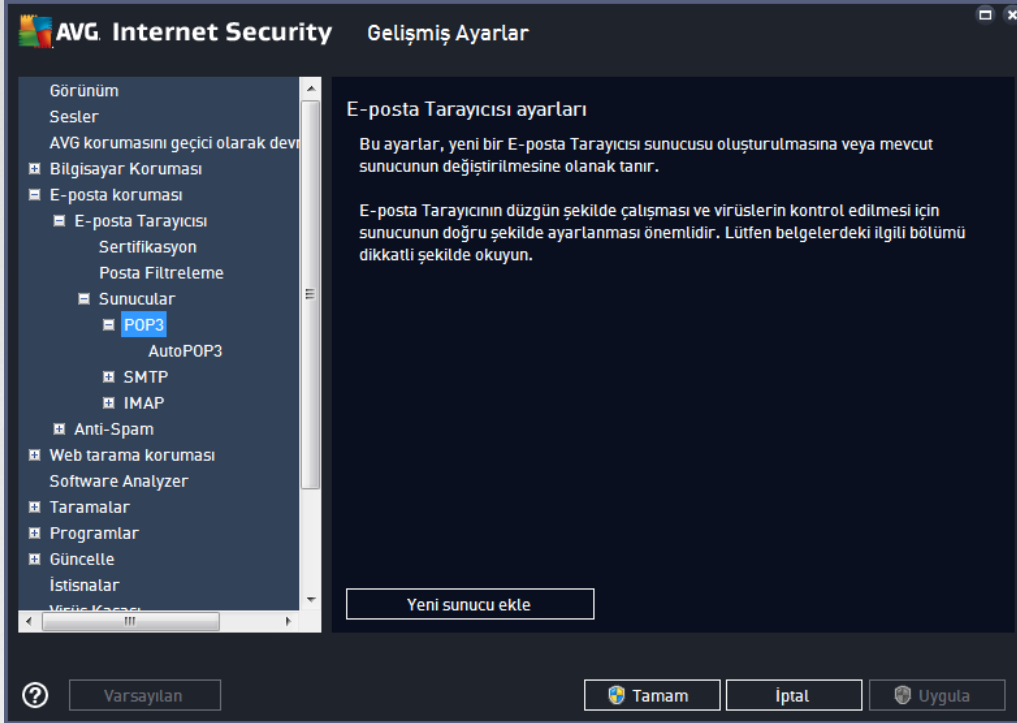
Ek filtresi iletişim kutusu, e-posta mesajlarının eklerinin taranmasına ilişkin parametreleri ayarlayabilmenizi sağlar. Varsayılan olarak **Eklenileri sil** seçeneği kapalıdır. Etkinleştirmeye karar verirsiniz tüm e-posta mesajlarının eklentileri, bulaşmış nesne ya da potansiyel olarak tehlikeli nesne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

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

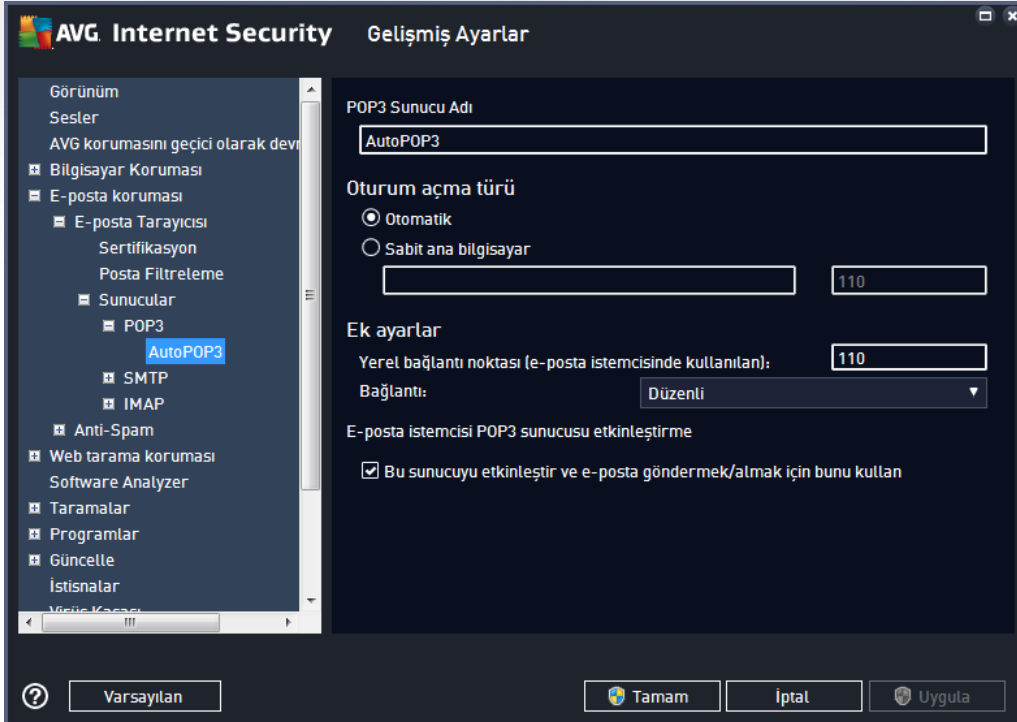
Sunucular bölümünde [E-posta Tarayıcısı](#) sunucularının parametrelerini düzenleyebilirsiniz:

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

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

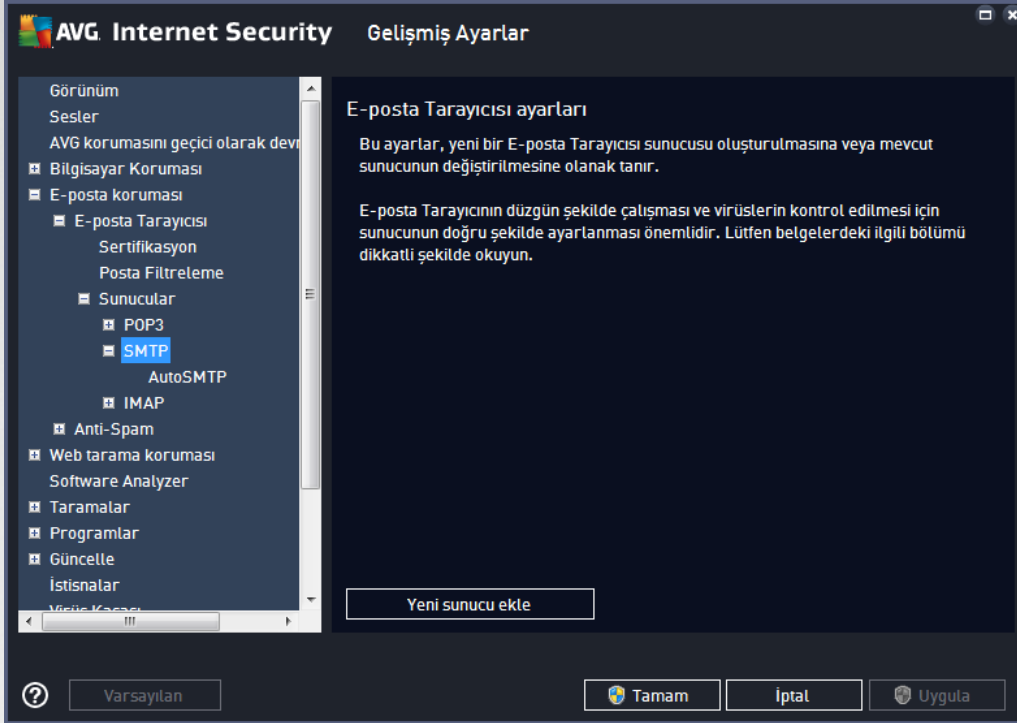


Bu iletişim kutusunda gelen postalar için POP3 protokolünü kullanarak yeni bir [E-posta Tarayıcısı](#) sunucusu kurabilirsiniz:

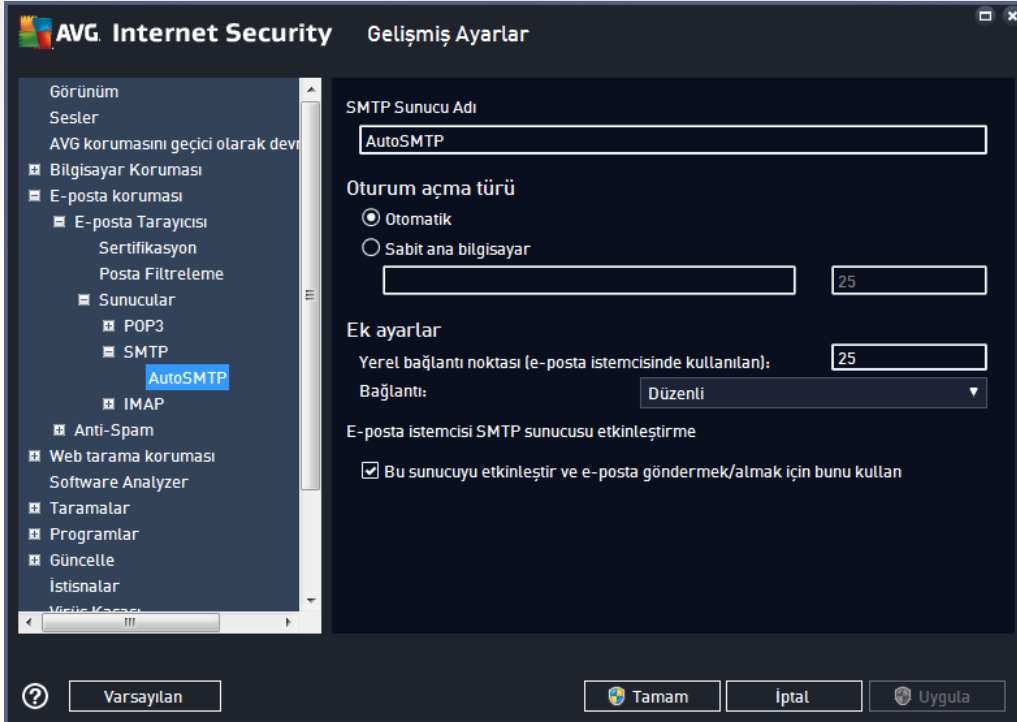




- **POP3 Sunucusunun Adı** - bu alanda yeni eklenen sunucuların adını belirtebilirsiniz (*bir POP3 sunucusu eklemek için sol menü ağacının POP3 ögesinin üzerinde sağ fare düğmesini tıklayın*).
- **Oturum açma tipi** - gelen postalar için kullanılan posta sunucularının belirlenmesi sırasında kullanılan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

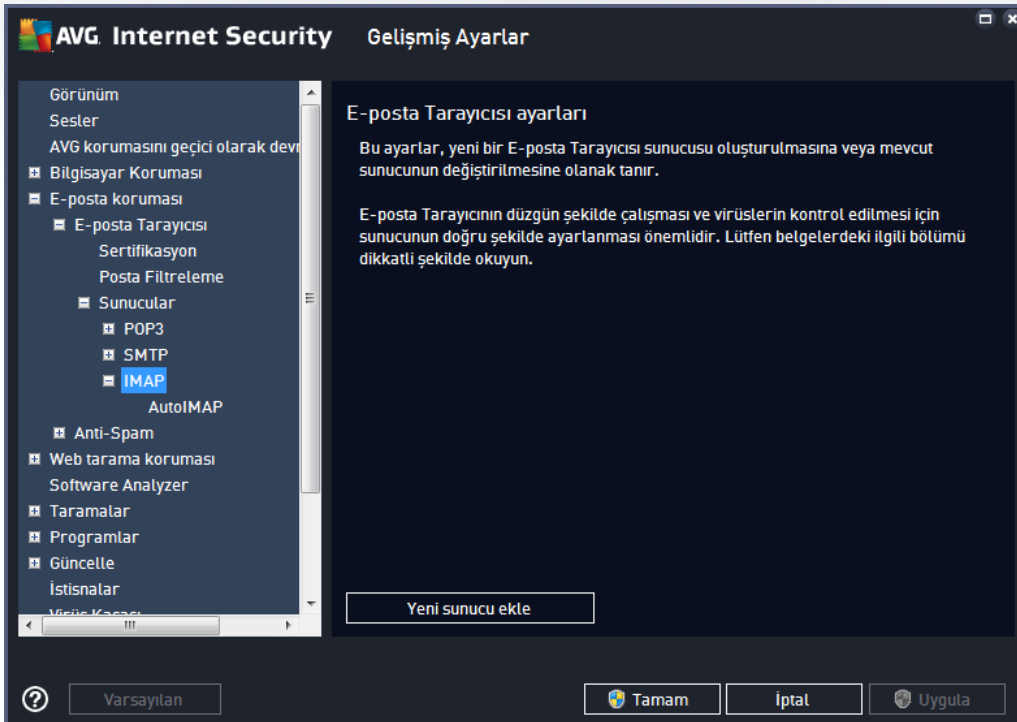


Bu iletişim kutusunda giden postalar için SMTP protokolünü kullanarak yeni bir [E-posta Tarayıcısı](#) sunucusu kurabilirsiniz:



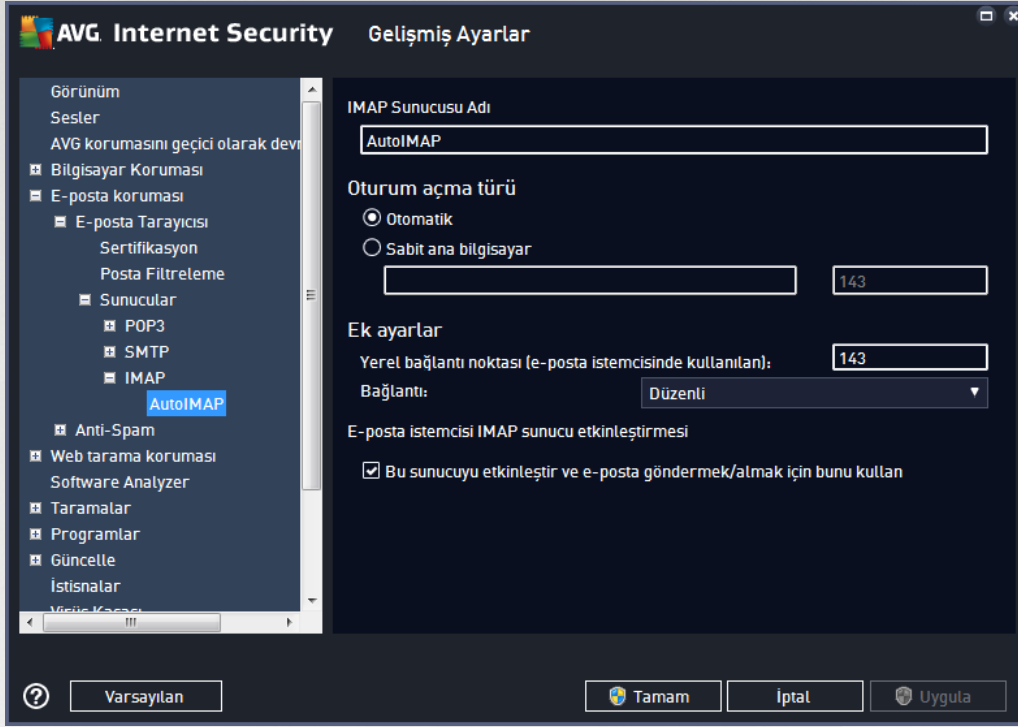


- **SMTP Sunucusunun Adı** - bu alanda yeni eklenen sunucuların adını belirtebilirsiniz (*bir SMTP sunucusu eklemek için sol menü ağacının SMTP öğesinin üzerinde sağ fare düğmesini tıklayın*). Otomatik olarak oluşturulan "AutoSMTP" sunucuları için bu alan devre dışı bırakılmıştır.
- **Oturum Açma Tipi** - 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 (*örneğin, 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 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:

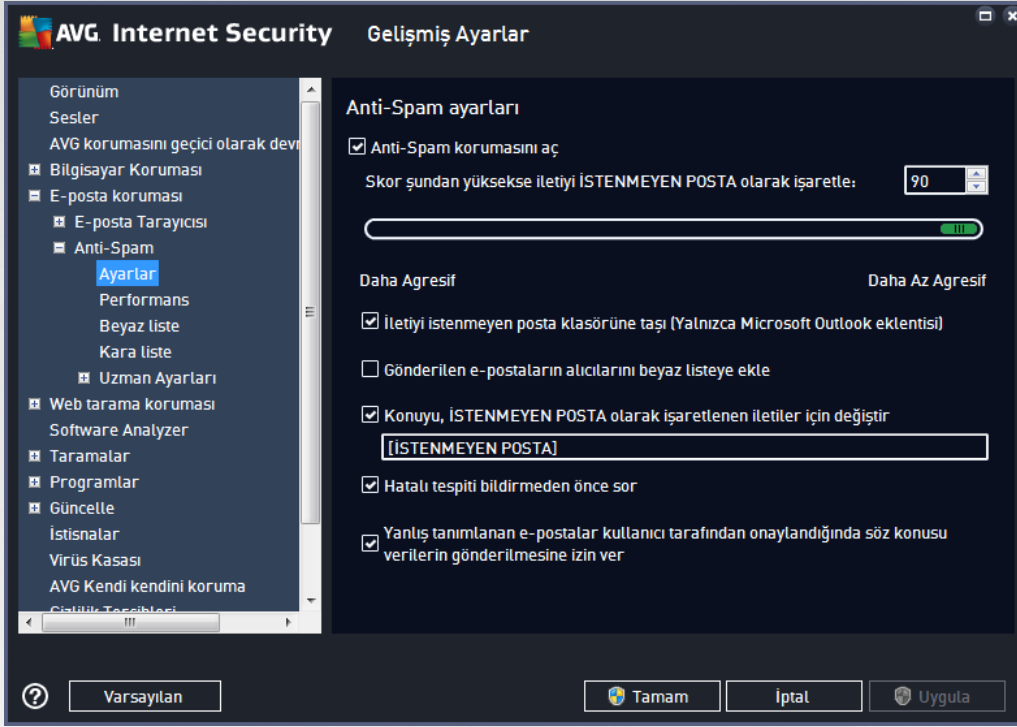


- **IMAP Sunucusunun Adı** - bu alanda yeni eklenen sunucuların adını belirtebilirsiniz (bir IMAP sunucusu eklemek için sol menü ağacının IMAP ögesinin üzerinde sağ fare düğmesini tıklayın).
- **Oturum Açma Tipi** - giden postalar için kullanılan posta sunucusunu belirleme yöntemini tanımlar:
 - **Otomatik** - 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.
 - **Bağlantı** - bu açılır 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.

7.5.2. Anti-Spam



Anti-Spam Ayarları iletişim kutusunda **Anti-Spam korumasını aç** onay kutusunu işaretleyerek veya bu kutunun işaretini kaldırarak e-posta iletişiminin anti-spam taramasına izin verebilir ya da taramayı engelleyebilirsiniz. Bu seçenek varsayılan olarak açıktır ve geçerli bir neden olmadıkça her zaman bu yapılandırmayı korumanız önerilir.

Daha sonra, daha fazla ya da daha az agresif değerlendirme ölçütleri de seçebilirsiniz. **Anti-Spam** filtresi, çeşitli dinamik tarama teknikleri sayesinde mesajlardan her birine (*başka bir deyişle, mesajın içeriğinin İSTENMEYEN POSTA'ya ne kadar yakın olduğunu belirlemek üzere*) bir puan verir. **Puan şundan yüksekse iletiyi istenmeyen posta olarak işaretle** ayarını, değeri girerek ya da kaydırma çubuğunu sola veya sağa hareket ettirerek ayarlayabilirsiniz.

Değerlerin aralığı 50 ile 90 arasındadır. Burada puan eşiği hakkında genel bilgi verilmektedir:

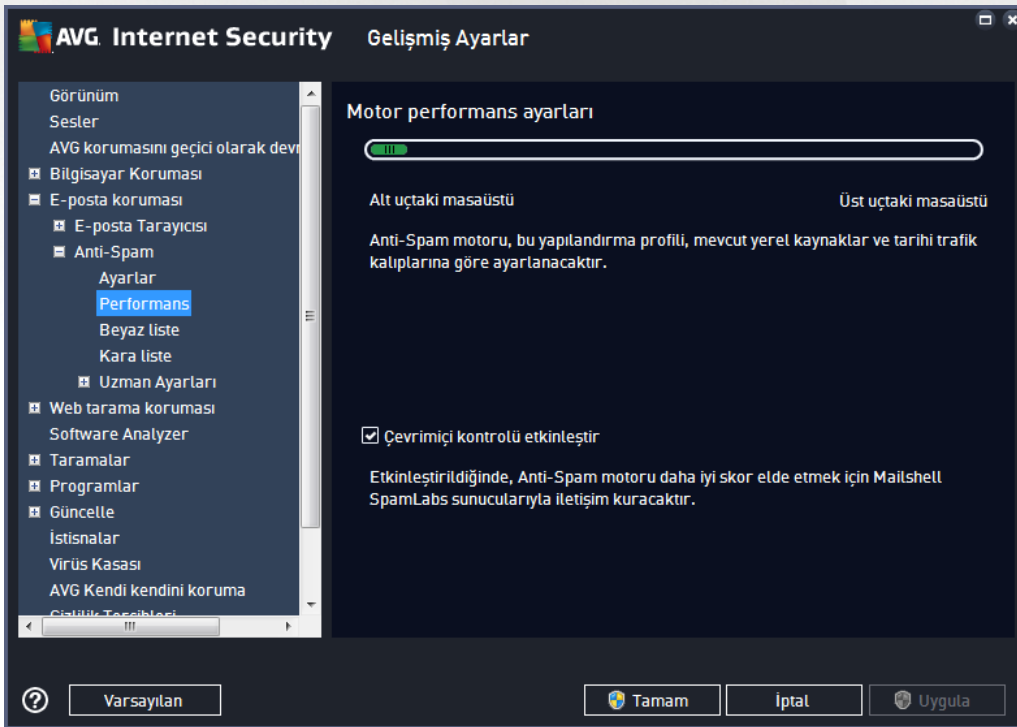
- **Değer 80-90** - istenmeyen posta olması muhtemel e-posta mesajları filtrelenecektir. İstenmeyen posta olmayan bazı postalar yanlışlıkla istenmeyen posta şeklinde etiketlenebilir.
- **Değer 60-79** - oldukça etkili bir yapılandırma olarak değerlendirilir. İstenmeyen posta olması muhtemel e-posta mesajları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



Anti-Spam ayarları iletişim kutusunda, tespit edilen istenmeyen e-posta mesajlarına ne yapılacağını da belirleyebilirsiniz:

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

Motor Performans Ayarları iletişim kutusu, (solda bulunan gezinme alanında **Performans** ögesi altında bağlantısı verilen) **Anti-Spam** bileşenin performans ayarlarını sunar:



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

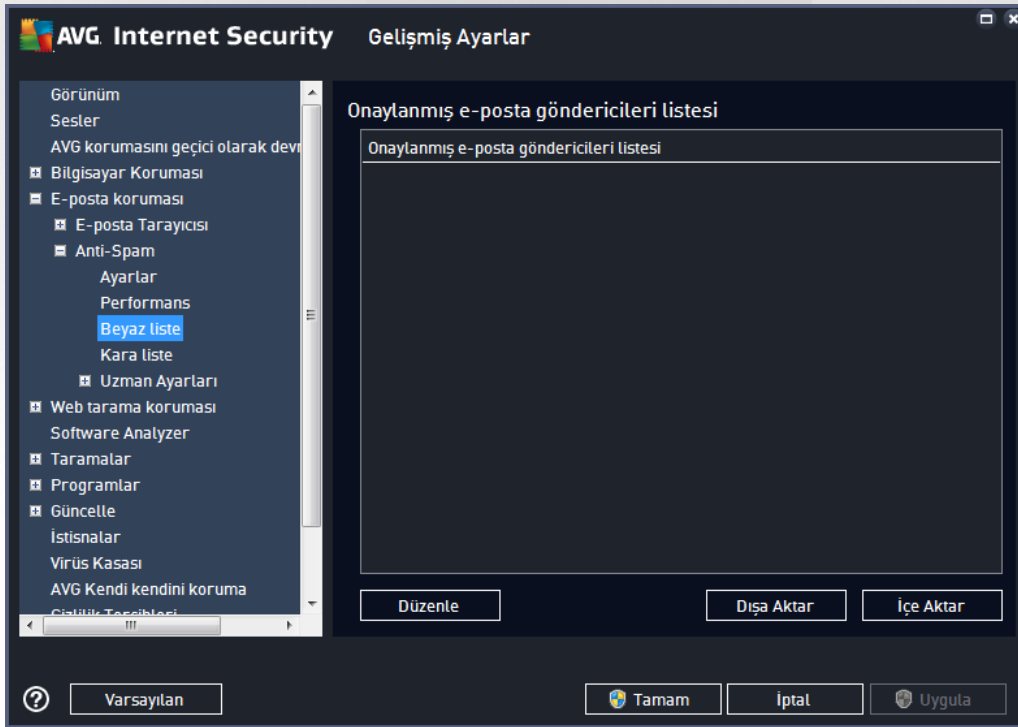


- **Alt uç masaüstü** - tarama işlemi sırasında istenmeyen postaların tespit edilmesi için herhangi bir kural kullanılmayacaktır. Tanımlama için sadece eğitim verileri kullanılacaktır. Bu mod, bilgisayar donanımlarınız çok eski değilse genel kullanım için önerilmemektedir.
- **Üst uç masaüstü** - bu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

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

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

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



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

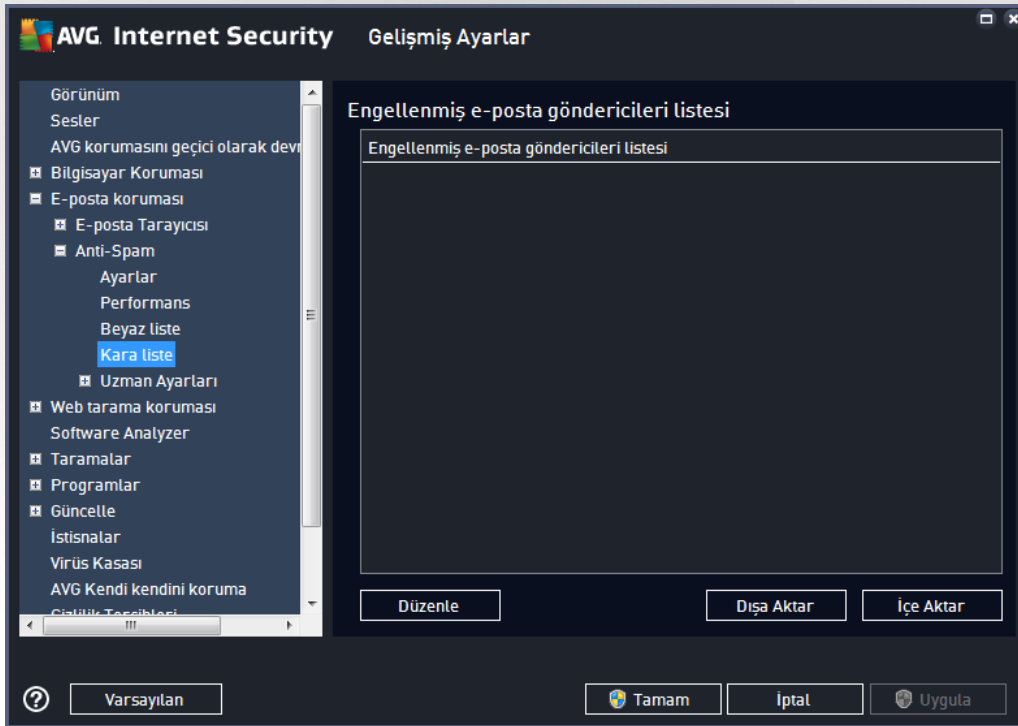
Kontrol düğmeleri



Şu kontrol düğmeleri bulunur:

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

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



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

Kontrol düğmeleri

Şu kontrol düğmeleri bulunur:



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

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

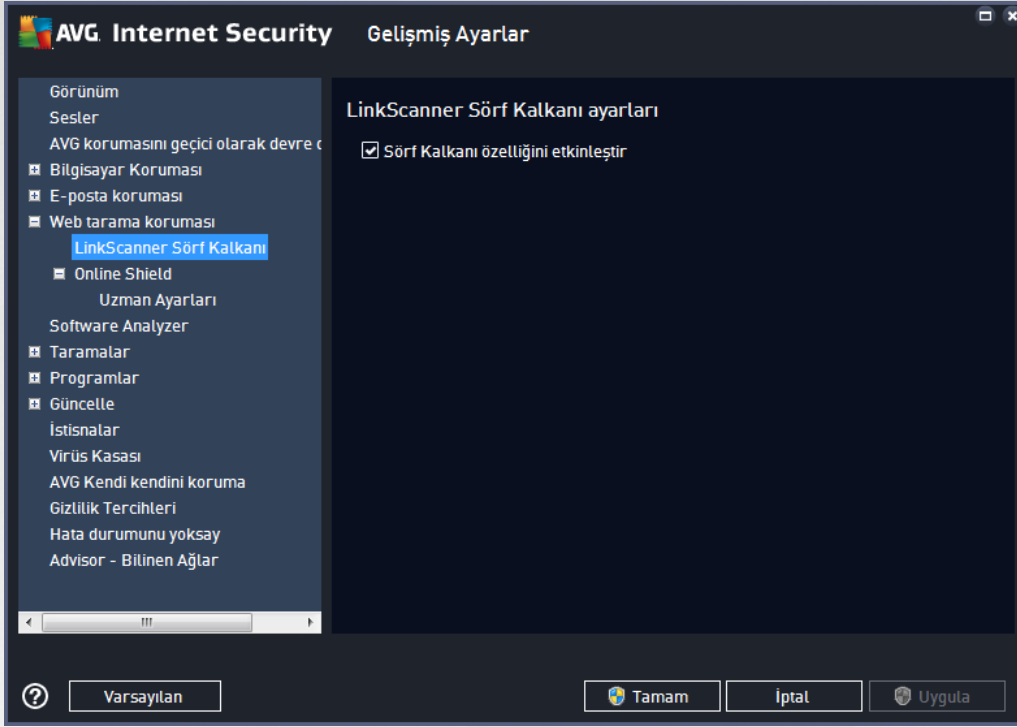
Anti-Spam yapılandırmasını gelişmiş seviyede değiştirmeniz gerektiğini düşünüyorsanız lütfen kullanıcı arayüzünde belirtilen talimatları izleyin. Genel olarak, her iletişim kutusunda düzenleyebileceğiniz spesifik bir özellik bulursunuz. Özelliğin açıklaması mutlaka iletişim kutusunun içinde yer alır.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

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



7.6. Web Tarama Koruması

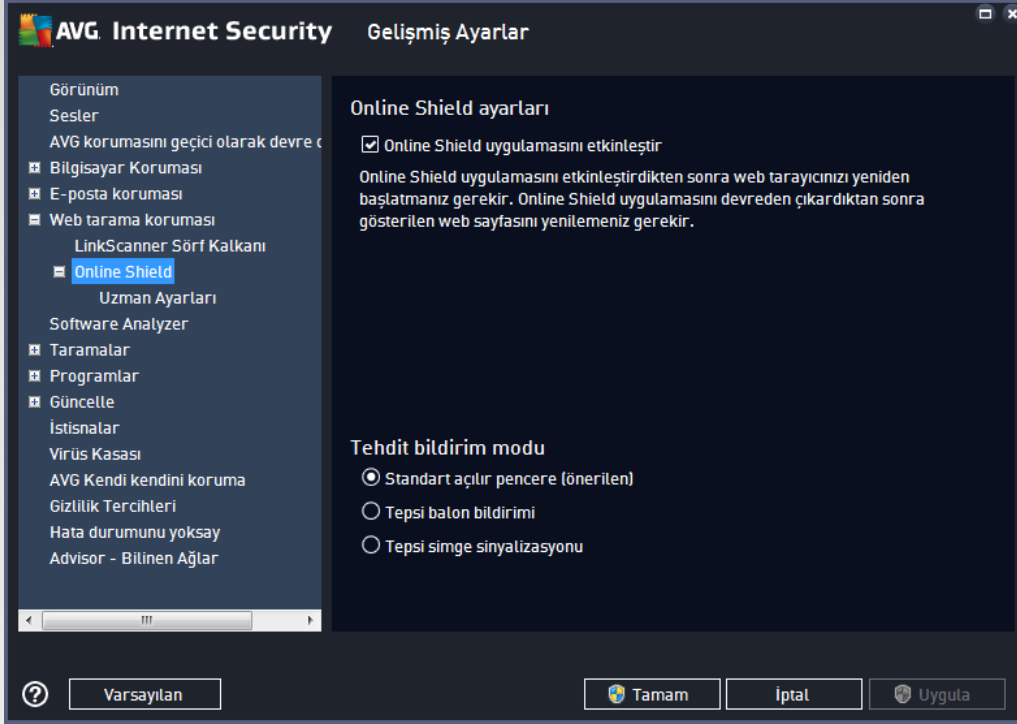
LinkScanner ayarları iletişim kutusunda aşağıdaki özellikleri işaretleyebilir veya bunların işaretlerini kaldırabilirsiniz:



- **Sörf Kalkanı özelliğini etkinleştir** - (varsayılan olarak açık): erişim sağlandığı anda güvenlik açığı olan web sitelerine karşı (gerçek zamanlı) koruma sağlamak için etkinleştirin. Bilinen zararlı site bağlantıları ve güvenlik açığından yararlanan içerikler, kullanıcı bir web tarayıcısı (ya da HTTP kullanan diğer bir program) aracılığıyla erişim sağladığında engellenir.

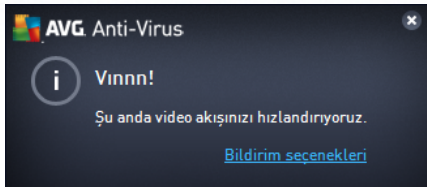


7.6.1. Online Shield



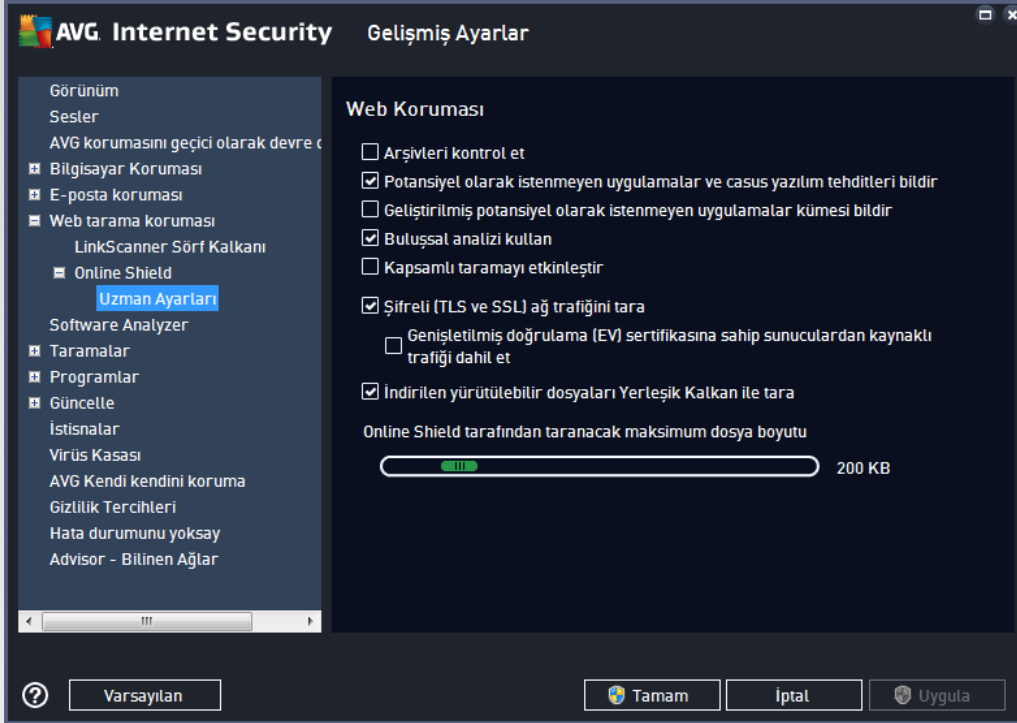
Online Shield iletişim kutusu şu seçenekleri sunar:

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



Tehdit bildirim modu

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



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

- **Arşivleri kontrol et** - (varsayılan olarak kapalı): Görüntülenecek www sayfasında bulunması muhtemel arşivlerin içeriğini tarayın.
- **Potansiyel olarak istenmeyen uygulamalar ve casus yazılım tehditlerini bildir** - (varsayılan olarak açık): virüslerin yanı sıra casus yazılımları da taramak için işaretleyin. Casus yazılım, şüpheli zararlı 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 uygulamalar geliştirilmiş grubunu bildir** - (varsayılan olarak kapalı): Casus yazılımların, yani doğrudan üreticiden alındığında 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.
- **Buluşsal yöntem kullan** - (varsayılan olarak açık): görüntülenecek web sitesinin içeriği buluşsal analiz yöntemi kullanılarak taranır (taranan nesnenin yönergelerinin sanal bir bilgisayar ortamında dinamik olarak canlandırılması).
- **Kapsamlı taramayı etkinleştir** - (varsayılan olarak kapalı): 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.



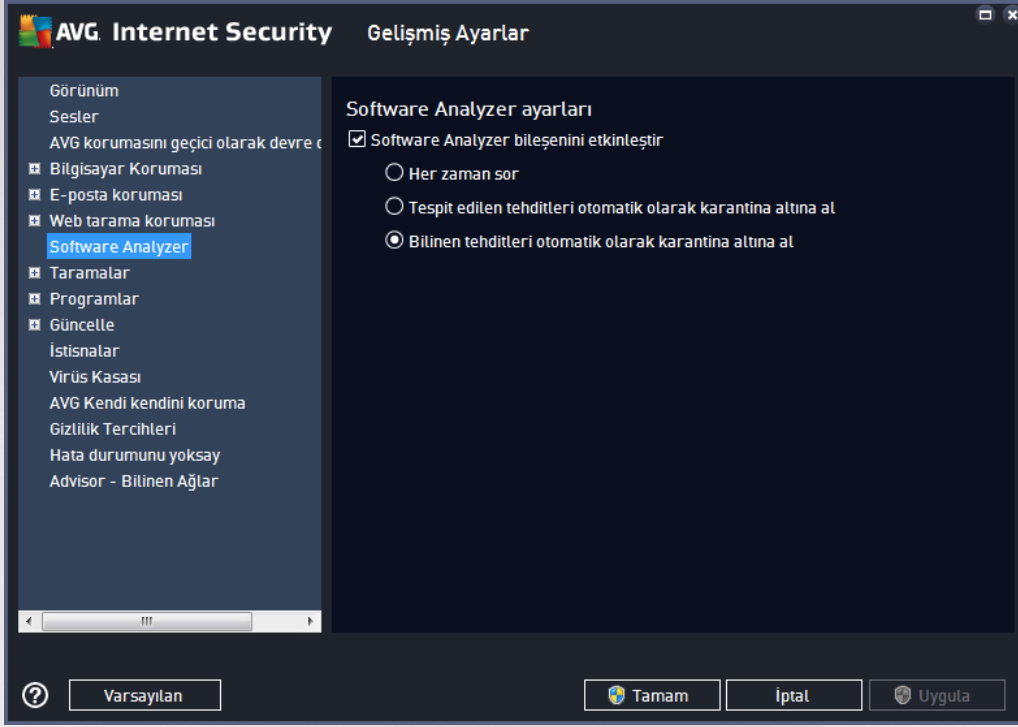
- **Şifreli (TLS ve SSL) ağ trafiğini tara** - (varsayılan olarak açık): AVG'nin tüm şifreli ağ trafiğini, yani güvenlik protokolleri (SSL ve onun yeni sürümü TLS) üzerindeki bağlantıları da taramasına izin vermek için seçeneği işaretli bırakın. Bu tarama HTTPS kullanan web siteleri ve TLS/SSL kullanan e-posta istemci bağlantıları için geçerlidir. Güvenlik altına alınan trafiğin şifresi çözülür, zararlı yazılımlara karşı taranır ve bilgisayarınıza güvenli biçimde teslim edilmek üzere tekrar şifrelenir. Bu seçenekte **Genişletilmiş doğrulama (EV) sertifikasına sahip sunuculardan kaynaklı trafiği dahil etme** ve Genişletilmiş Doğrulama Sertifikası olan sunuculardan kaynaklı şifreli ağ trafiğini de tarama tercihinde bulunabilirsiniz. EV sertifikası yayınlamak sertifika yetkilisinin kapsamlı doğrulama sürecini gerektirir, dolayısıyla bu sertifika altında işletilen web siteleri çok daha güvenlidir (*zararlı yazılım dağıtma ihtimalleri daha azdır*). Bu nedenle, EV sertifikalı sunucu trafiğinin taranmamasını tercih edebilirsiniz ve bu da şifreli iletişimi biraz daha hızlandırır.
- **İndirilen yürütülebilir dosyaları Yerleşik Kalkan ile tara** - (varsayılan olarak açık): indirilmelerinin ardından yürütülebilir dosyaları (*tipik dosya uzantıları: exe, bat, com*) tarar. Yerleşik kalkan bilgisayarınıza zararlı herhangi bir kodun ulaşmaması için dosyaları indirilmeden önce tarar. Ancak, bu tarama **Taranacak dosyanın maksimum parça boyutu** ile sınırlandırılmıştır (bu iletişim kutusunda bir sonraki öğeye 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 işaretli 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, bulaşmış olması halinde **Yerleşik Kalkan** tarafından tespit edilecektir.

7.7. Software Analyzer

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

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



Software Analyzer bileşenini etkinleştir (varsayılan olarak açık) - [Kimlik](#) bileşenini kapatmak için işaretini kaldırın. **Zorunlu olmadıkça, bu işareti kesinlikle kaldırmamanızı tavsiye ederiz!** Software Analyzer etkinleştirildiğinde, bir tehlike algılandığında ne yapacağınızı belirtebilirsiniz:

- **Her zaman sor** - bir tehdit tespit edildiğinde, çalıştırmak istediğiniz hiçbir uygulamanın kaldırılmaması için tehdidin karantinaya alınması gerekip gerekmediği size sorulacaktır.
- **Tespit edilen tehditleri otomatik olarak karantina altına al** - tespit edilen tüm olası tehditlerin [Virüs Kasası](#) güvenilir alanına hemen taşınmasını istediğinizi belirtmek için bu onay kutusunu işaretleyin. Varsayılan ayarlarda, bir tehdit tespit edildiğinde, çalıştırmak istediğiniz hiçbir uygulamanın kaldırılmaması için size uygulamanın karantinaya alınması gerekip gerekmediği sorulacaktır.
- **Bilinen tehditleri otomatik olarak karantina altına al** (varsayılan olarak açık) - zararlı yazılım olasılığı tespit edilen tüm uygulamaların otomatik olarak ve hemen [Virüs Kasası](#)'na taşınmasını istiyorsanız bu öğeyi işaretli bırakın.

7.8. Taramalar

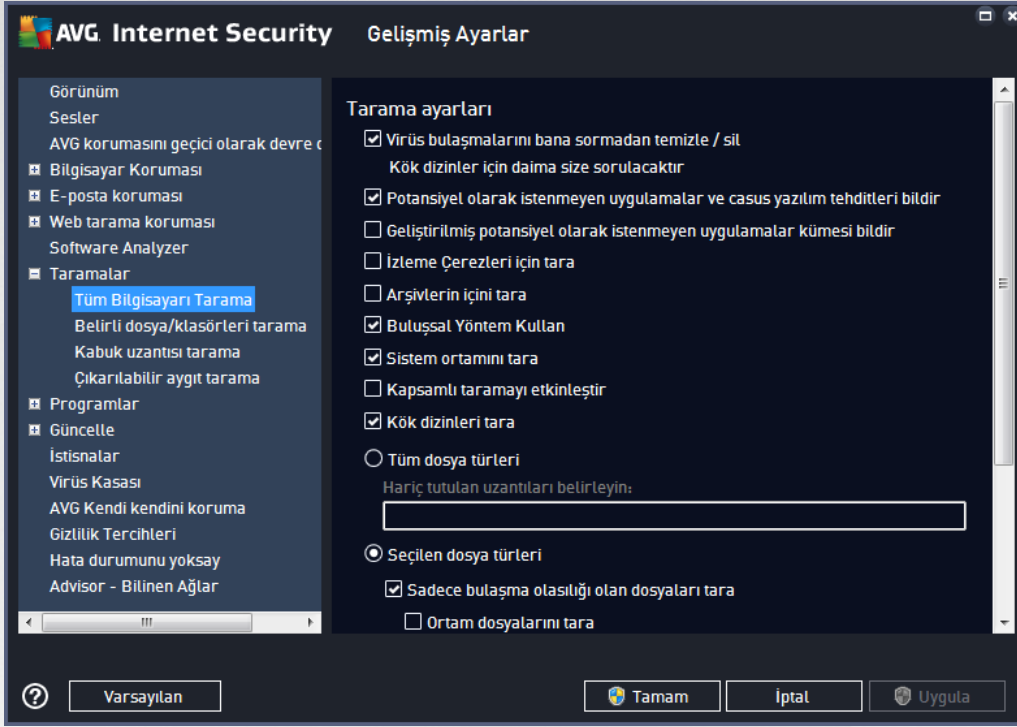
Gelişmiş tarama ayarları, yazılım geliştiricisi tarafından tanımlanan belirli tarama türlerine ilişkin dört kategoriye bölünmüştür:

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



7.8.1. Tüm Bilgisayar Taraması

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



Tarama ayarları

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

- **Bulaşmayı bana sormadan temizle / kaldır** (varsayılan olarak açık) - tarama sırasında virüs tespit edildiğinde, çözümü varsa otomatik olarak temizlenir. Bulaşmış dosya otomatik olarak temizlenemezse bulaşmış nesne [Virüs Kasası](#)'na taşınır.
- **Potansiyel olarak istenmeyen uygulamalar ve casus yazılım tehditlerini bildir** (varsayılan olarak açık) - virüslerin yanı sıra casus yazılımları da taramak için işaretleyin. Casus yazılım, şüpheli zararlı 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 uygulamalar geliştirilmiş grubunu bildir** (varsayılan olarak kapalı) - casus yazılımların, yani doğrudan üreticiden alındığında 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 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).



- **Arşivlerin içini tara** (varsayılan olarak kapalı) - bu parametre tarama işleminin ZIP, RAR vb. arşiv dosyalarının içinde saklanan tüm dosyaları denetlemesi gerektiğini belirtir.
- **Buluşsal yöntem kullan** (varsayılan olarak açık): Buluşsal 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.
- **Kapsamlı taramayı etkinleştir** (varsayılan olarak kapalı) - 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** (varsayılan olarak açık) - [Anti-Rootkit](#) taraması bilgisayarınızı olası rootkit'lere, yani bilgisayarınızda zararlı etkinlik içerebilecek programlar ve teknolojilere karşı tarar. Bir rootkit tespit edilmesi bilgisayarınızda mutlaka bulaşma olduğu anlamına gelmez. Bazı durumlarda, belirli sürücüler veya normal uygulamaların bölümleri yanlışlıkla rootkit olarak tespit edilebilir.

Tarama için dosya türlerini de belirlemeniz gerekir

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

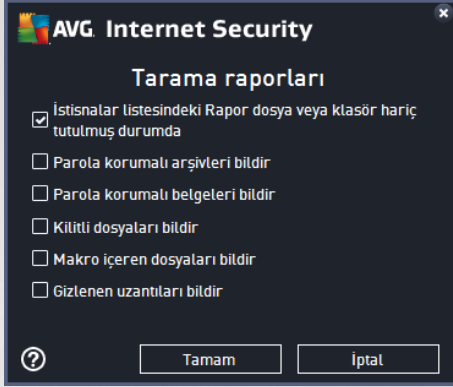
Taramanın ne kadar hızlı tamamlanacağını ayarla

Taramanın ne kadar hızlı tamamlanacağını ayarla bölümünde, sistem kaynakları kullanımına bağlı olarak istediğiniz tarama hızını seçebilirsiniz. Bu seçenek varsayılan olarak otomatik kaynak kullanımının *kullanıcıya duyarlı* seviyesine 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 açık, ancak kimse tarafından kullanılmadığı sırada seçilebilir). Öte yandan, tarama süresini uzatarak sistem kaynaklarının kullanımını azaltabilirsiniz.

Ek tarama raporlarını ayarla...

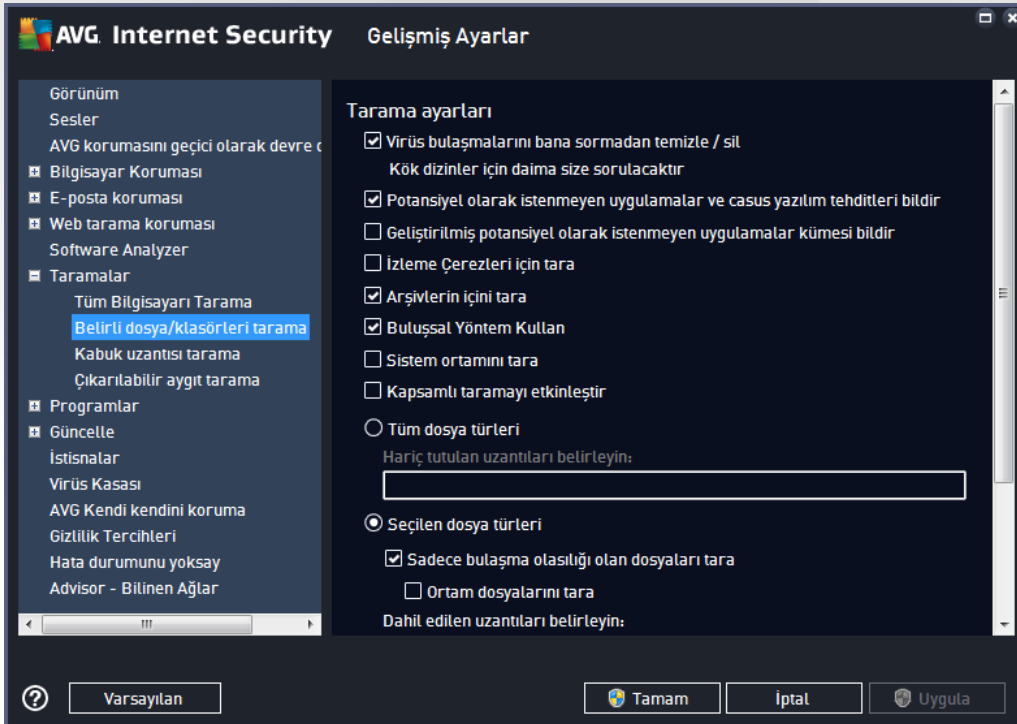


Ek tarama raporlarını ayarla ... bağlantısını tıklatarak tarama bulgularının rapor edilmesi gerekip gerekmediğini tanımlamak üzere birden fazla öğeyi ayarlayabileceğiniz **Tarama raporları** olarak adlandırılan bağımsız bir iletişim kutusu açın:



7.8.2. Belirli dosya/klasörleri tarama

Belirli Dosyaları veya Klasörleri Tara işlevinin düzenleme arayüzü [Tüm Bilgisayarı Tara](#) işlevinin düzenleme iletişim kutusu ile neredeyse aynıdır; fakat [Tüm Bilgisayarı Tara](#) işlevinin varsayılan ayarları daha kesindir:



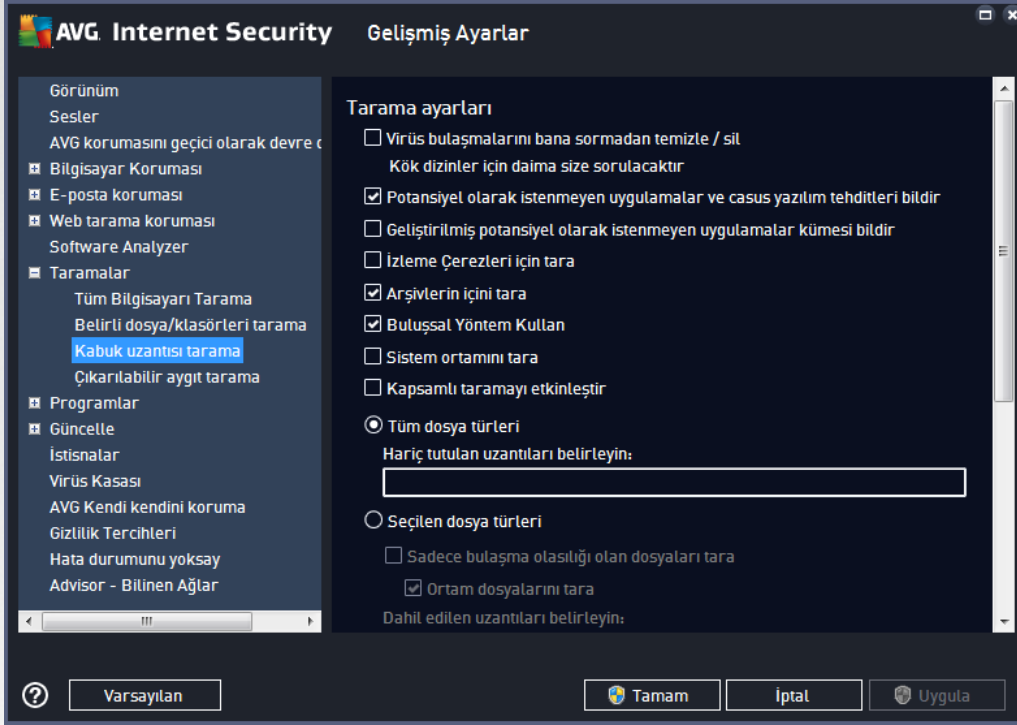
Bu yapılandırma iletişim kutusunda ayarlanan tüm parametreler [Belirli Dosyaları veya Klasörleri Tara](#) işlemi ile tarama sırasında seçilen alanlar için geçerlidir!

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



7.8.3. Kabuk Uzantısı Tarama

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



Düzenleme seçenekleri [Tüm Bilgisayar Taraması](#) için mevcut olanlarla neredeyse 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*).

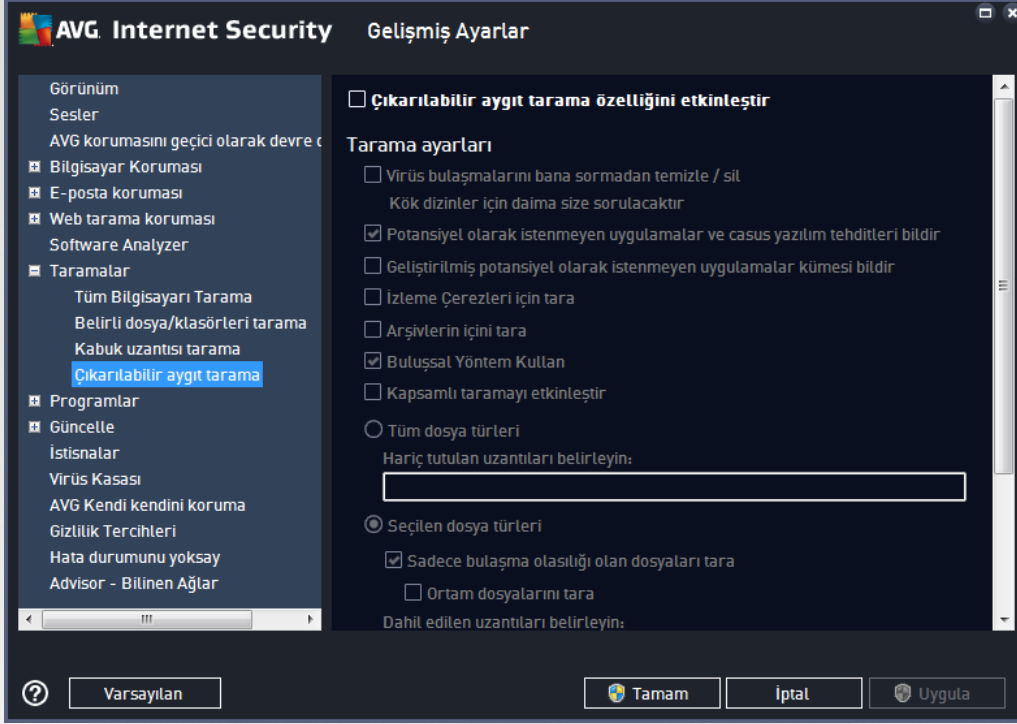
Not: Belirli parametrelerin açıklaması için lütfen [AVG Gelişmiş Ayarları / Taramalar / Tüm Bilgisayarı Tara](#) bölümüne bakın.

[Tüm Bilgisayarı Tara](#) iletişim kutusuyla karşılaştırıldığında **Kabuk Uzantısı Tarama** iletişim kutusu, tarama sürecinde ve tarama sonuçlarında AVG kullanıcı arayüzünden erişilebilir olmasını isteyip istemediğinizi belirleyebileceğiniz **Tarama ilerlemesi ve sonuçlarının gösterilmesi** adlı bölümü de içerir. Tarama sonucunun yalnızca tarama sırasında bir bulaşma tespit edilmesi durumunda görüntülenmesi gerektiğini de belirleyebilirsiniz.



7.8.4. 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 başlıca bulaşma kaynaklarından biri olduğu için söz konusu çıkartılabilir aygıtların potansiyel tehditlere karşı taranması hayati önem taşımaktadır. Bu tarama özelliğinin istendiği zaman otomatik olarak başlatılacak şekilde hazır bulundurulması için **Çıkarılabilir aygıt taramayı etkinleştir** seçeneğini işaretleyin.

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

7.9. Programlar

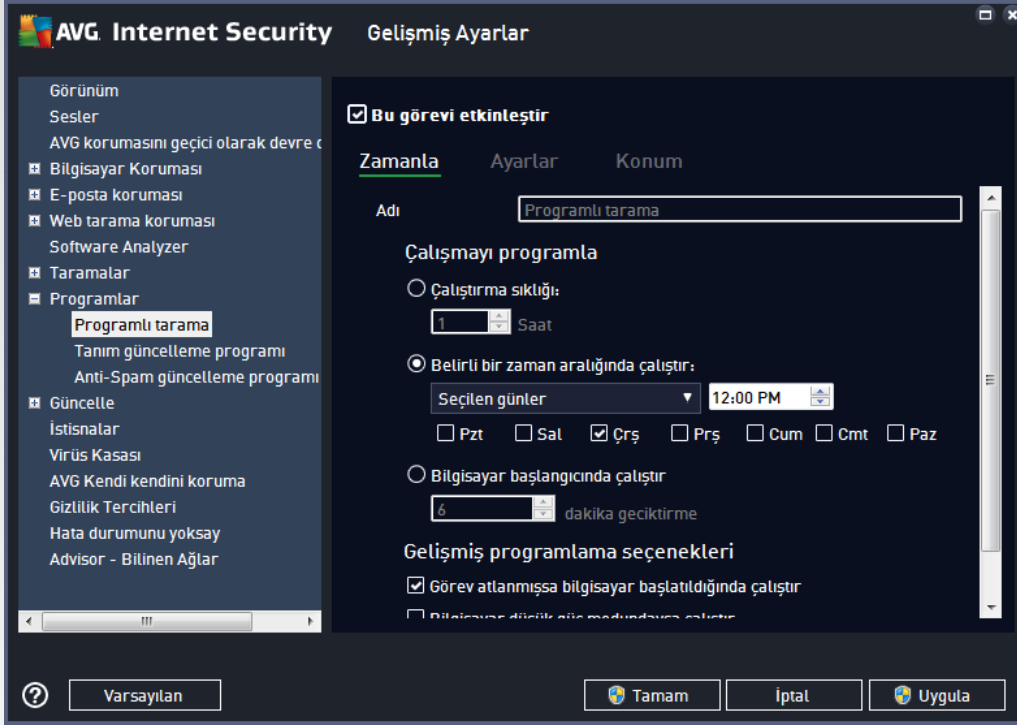
Programlar bölümünde aşağıdaki bileşenlerin öntanımlı ayarlarını düzenleyebilirsiniz:

- [Programlı Tarama](#)
- [Tanım Güncelleme Programı](#)
- Program Güncelleme Programı
- [Anti-Spam Güncelleme Programı](#)



7.9.1. Programlı Tarama

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



Ad adındaki metin alanı (*tüm varsayılan zamanlamalar için devre dışı bırakılmıştır*) bu zamanlamaya program satıcısı tarafından atanan adı gösterir. Yeni eklenen zamanlamalar için (*sol gezinti ağacındayken **Programlı tarama** ögesi üzerinde sağ tıklatarak* yeni bir zamanlama ekleyebilirsiniz) kendi adınızı belirtebilirsiniz ve bu durumda metin alanı düzenleme için açılacaktır. Programladığınız taramaları diğerlerinden kolaylıkla ayırtabilmek 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. Öte yandan iyi bir açıklayıcı ada örnek olarak "Sistem alanı taraması" vb. gösterilebilir. Ayrıca taramanın adında bu taramanın tüm bilgisayarda mı yoksa sadece seçilen dosyalar veya klasörlerde mi gerçekleştirildiğini belirtmek de gerekir; kendi taramalarınız her zaman belirli bir [seçilen dosyalar veya klasörlerin taraması](#) sürümü olacaktır.

Bu iletişim kutusunda taramanın aşağıdaki parametrelerini de tanımlayabilirsiniz:

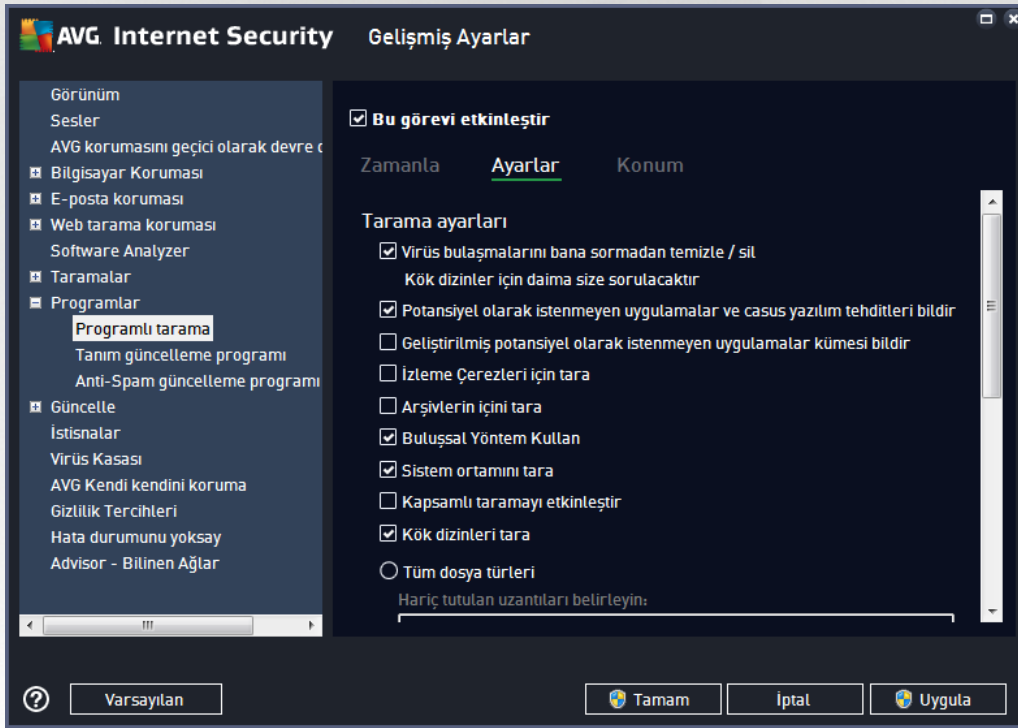
Çalışmayı programla

Burada, yeni programlanan tarama başlatması için zaman aralıkları belirtebilirsiniz. Zamanlama belirli bir sürenin ardından tekrarlanan tarama başlatması ile (**Çalıştırma sıklığı**) ya da kesin bir tarih ve saat tanımlanarak (**Belirli saatlerde çalıştır**), veya tarama başlatmayla ilişkilendirilmesi gereken bir olay tanımlanarak (**Bilgisayar başlangıcında çalıştır**) tanımlanabilir.



Gelişmiş programlama seçenekleri

- **Görev atlanmıyssa bilgisayar başlatıldığında çalıştır** – taramayı belirli bir zamanda çalışmak üzere programlıyorsanız, bu seçenek taramanın bilgisayarın kapalı olduğu zamana programlanması durumunda sonradan gerçekleştirilmesini sağlar.
- **Bilgisayar düşük güç modundayyssa çalıştır** – bilgisayar, programlı tarihte pille çalışıyor olsa da tarama gerçekleştirilmelidir.



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.**

- **Virüs bulaşmasını bana sormadan temizle / sil** (varsayılan olarak açık): Tarama sırasında bir virüs tespit edildiğinde, çözümü varsa otomatik olarak temizlenebilir. Bulaşmış dosya otomatik olarak temizlenemezse bulaşmış nesne [Virüs Kasası](#)'na taşınır.
- **Potansiyel olarak istenmeyen uygulamalar ve casus yazılım tehditlerini bildir** (varsayılan olarak açık): virüslerin yanı sıra casus yazılımları da taramak için işaretleyin. Casus yazılım, şüpheli zararlı 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 uygulamalar geliştirilmiş grubunu bildir** (varsayılan olarak kapalı): Casus yazılımların, yani doğrudan üreticiden alındığında tamamen zararsız olan, ancak daha sonra kötüye kullanılacak programların genişletilmiş paketlerinin tespit edilmesi için işaretleyin. Bu,



bilgisayar güvenliğini 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*).
- **Arşivlerin içeriğini tara** (varsayılan olarak kapalı): Bu parametre, tarama işleminde ZIP, RAR vb. bir arşiv ile saklanmış olsa bile tüm dosyaların taranması gerektiğini belirtir.
- **Buluşsal yöntem kullan** (varsayılan olarak açık): Buluşsal 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.
- **Kapsamlı taramayı etkinleştir** (varsayılan olarak kapalı) belirli durumlarda (*bilgisayarınıza bulaşma olmasından şüpheleniliyorsa*) yalnızca emin olmak üzere, bilgisayarınızın bulaşma olması çok zor olan alanlarını bile tarayan, en kapsamlı tarama algoritmalarını etkinleştirmek için bu seçeneği işaretleyebilirsiniz. Ancak, bu yöntemin çok fazla zaman aldığını unutmayın.
- **Rootkit'leri tara** (varsayılan olarak açık): Anti-Rootkit taraması bilgisayarınızı olası rootkit'lere karşı (bilgisayarınızdaki zararlı yazılım etkinliği içerebilecek programlar ve teknolojiler açısından) tarar. Bir rootkit tespit edilmesi bilgisayarınızda mutlaka bulaşma olduğu anlamına gelmez. Bazı durumlarda, belirli sürücüler veya normal uygulamaların bölümleri yanlışlıkla rootkit olarak tespit edilebilir.

Tarama için dosya türlerini de belirlemeniz gerekir

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

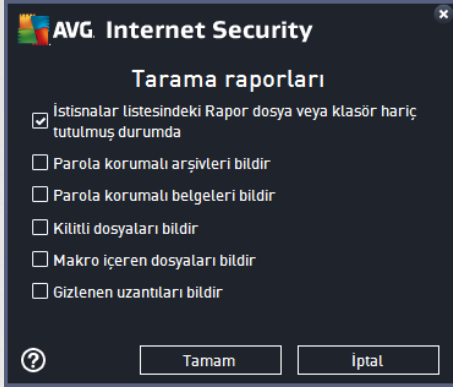
Taramanın ne kadar hızlı tamamlanacağını ayarla

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 açık, ancak kimse tarafından kullanılmadığı sırada seçilebilir*). Öte yandan, tarama süresini uzatarak sistem kaynaklarının kullanımını azaltabilirsiniz.



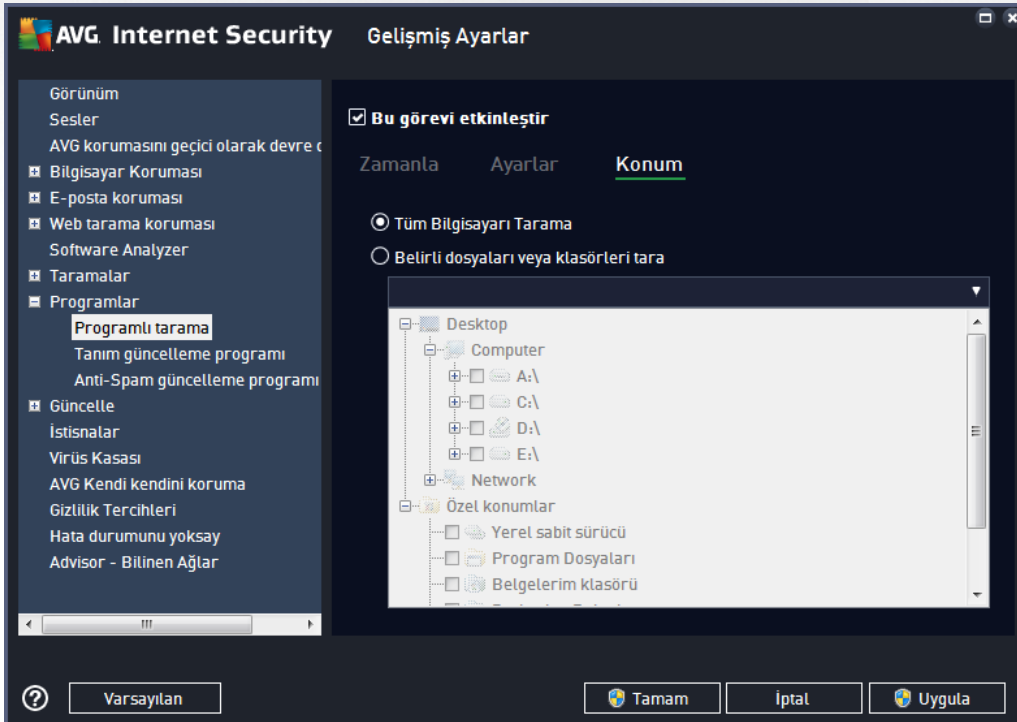
Ek tarama raporlarını ayarla

Ek tarama raporlarını ayarla ... bağlantısını tıklatarak tarama bulgularının rapor edilmesi gerekip gerekmediğini tanımlamak üzere birden fazla öğeyi ayarlayabileceğiniz **Tarama raporları** olarak adlandırılan bağımsız bir iletişim kutusu açın:



Bilgisayar kapatma seçenekleri

Bilgisayar kapatma seçenekleri bölümünde çalışan tarama işlemi bittiğinde bilgisayarın otomatik olarak kapatılması gerekip gerekmediğine karar verebilirsiniz. Bu seçeneği işaretlerseniz (**Tarama tamamlandıktan sonra bilgisayarı kapat**) bilgisayar geçerli durumda kilitli olsa bile bilgisayarın kapatılmasını sağlayan bir seçeneğin bulunduğu bir pencere açılacaktır (**Bilgisayar kilitlenirse kapatma işlemi zorla**).

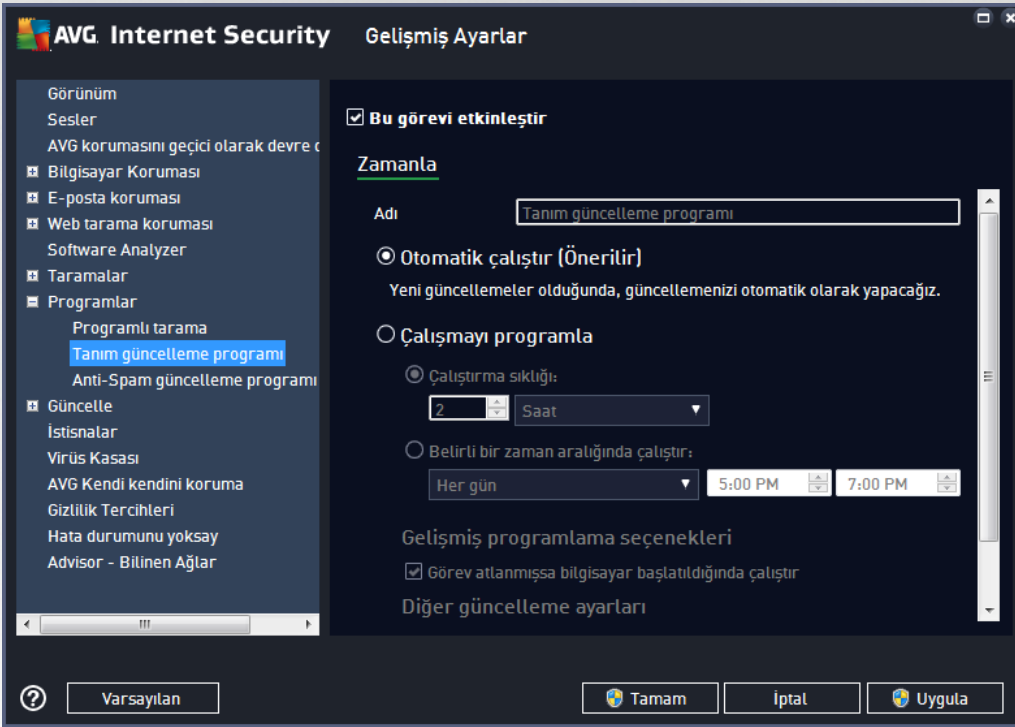




Konum sekmesinde, [tüm bilgisayar tarama](#) veya [belirli dosya veya klasörleri taramayı](#) programlamak isteyip istemediğinizi tanımlayabilirsiniz. Belirli dosya ve klasörleri taramayı seçerseniz, bu iletişim kutusunun alt kısmında görüntülenen ağaç yapısı etkinleşir ve taranacak klasörleri seçebilirsiniz.

7.9.2. Tanım Güncelleme Programı

Gerçekten gerekliyse Bu görevi etkinleştir öğesinin işaretini 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 bırakılmıştır*) bu zamanlamaya program satıcısı tarafından atanan adı gösterir.

Çalışmayı programla

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 elle ayarlayabilir ve yeni programlanan tanım güncelleme başlatmaları için zaman aralıkları belirleyebilirsiniz. Zamanlama belirli bir sürenin ardından tekrarlanan güncelleme başlatması ile (**Çalıştırma sıklığı**) ya da kesin bir tarih ve saat (**Belirli saatlerde çalıştır**) tanımlanarak tanımlanabilir.

Gelişmiş programlama seçenekleri

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

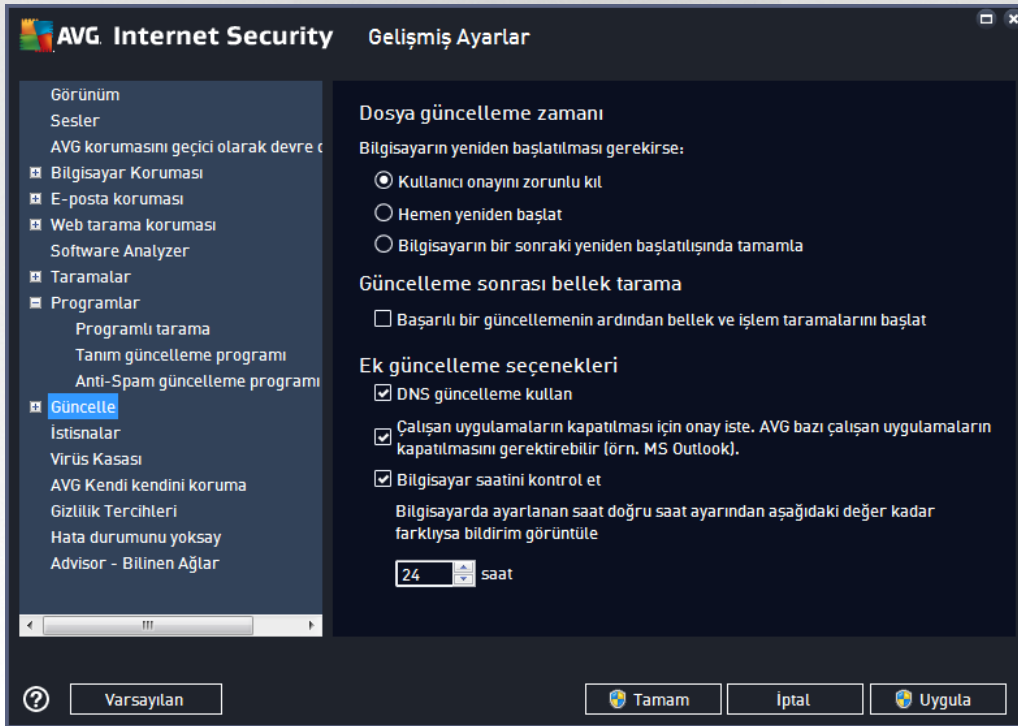


Diğer güncelleme ayarları

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

7.9.3. Anti-Spam Güncelleme Programı

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



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

Çalışmayı programla

Burada, yeni programlanan Anti-Spam güncellemesinin başlaması için zaman aralığı girin. Zamanlama belirli bir sürenin ardından tekrarlanan Anti-Spam güncelleme başlatması ile (**Çalıştırma sıklığı**) ya da kesin bir tarih ve saat tanımlanarak (**Belirli saatlerde çalıştır**) veya güncelleme başlatmayla ilişkilendirilmesi gereken bir olay tanımlanarak (**Bilgisayar başlangıcında çalıştır**) tanımlanabilir.

Gelişmiş programlama seçenekleri



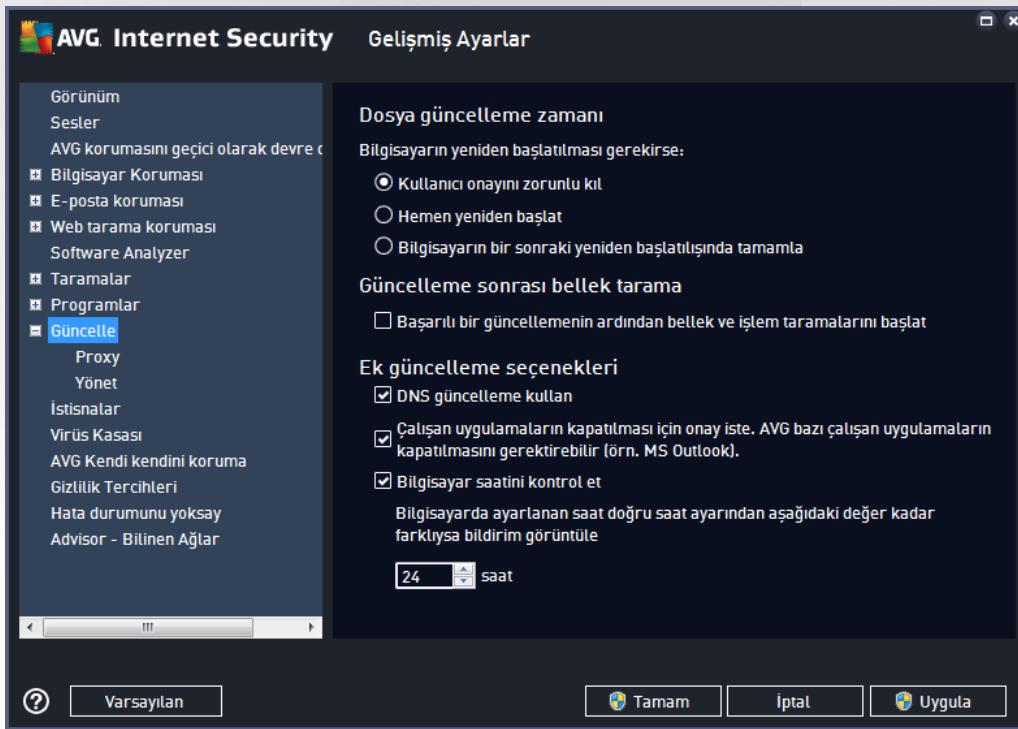
Bu bölümde, bilgisayar düşük güç modundaydı veya tamamen kapatılmışsa hangi koşullar altında Anti-Spam güncellemesinin başlatılması/başlatılmaması gerektiğini belirleyebilirsiniz.

Diğer güncelleme ayarları

İnternet bağlantısı kurulduğunda güncellemeyi yeniden çalıştır seçeneğini işaretleyerek internet bağlantısı kesildiğinde ve Anti-Spam güncelleme işlemi başarısız olduğunda, internet bağlantısı yeniden sağlanırsa sağlanmaz yeniden başlatılmasını sağlayın. Planlanan tarama işlemi sizin belirlediğiniz tarih ve saatte başladıktan sonra [AVG sistem tepsi simgesi](#) üzerinde açılan bir açılır pencere vasıtasıyla bilgilendirileceksiniz ([Gelişmiş Ayarlar/Görünüm](#) iletişim kutusunun varsayılan yapılandırmasını değiştirmemiş olmanız kaydıyla).

7.10. Güncelleme

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



Dosya güncelleme zamanı

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

- **Kullanıcıdan onay iste** (varsayılan) - **güncelleme** işleminin tamamlanması için gereken bilgisayarın yeniden başlatılması süreci için onayınız istenir



- **Hemen yeniden başlat - güncelleme** işlemi tamamlanır tamamlanmaz onayınız istenmeden bilgisayarınız yeniden başlatılacaktır
- **Bilgisayarın bir sonraki yeniden başlatılmasında tamamla - güncelleme** işleminin tamamlanması bilgisayarın bir sonraki yeniden başlatılmasına kadar ertelenir. Lütfen bu seçeneğin yalnızca bilgisayarın düzenli olarak (en azından günde bir kez) yeniden başlatıldığını bilmeniz halinde önerildiğini unutmayın!

Güncelleme sonrası bellek tarama

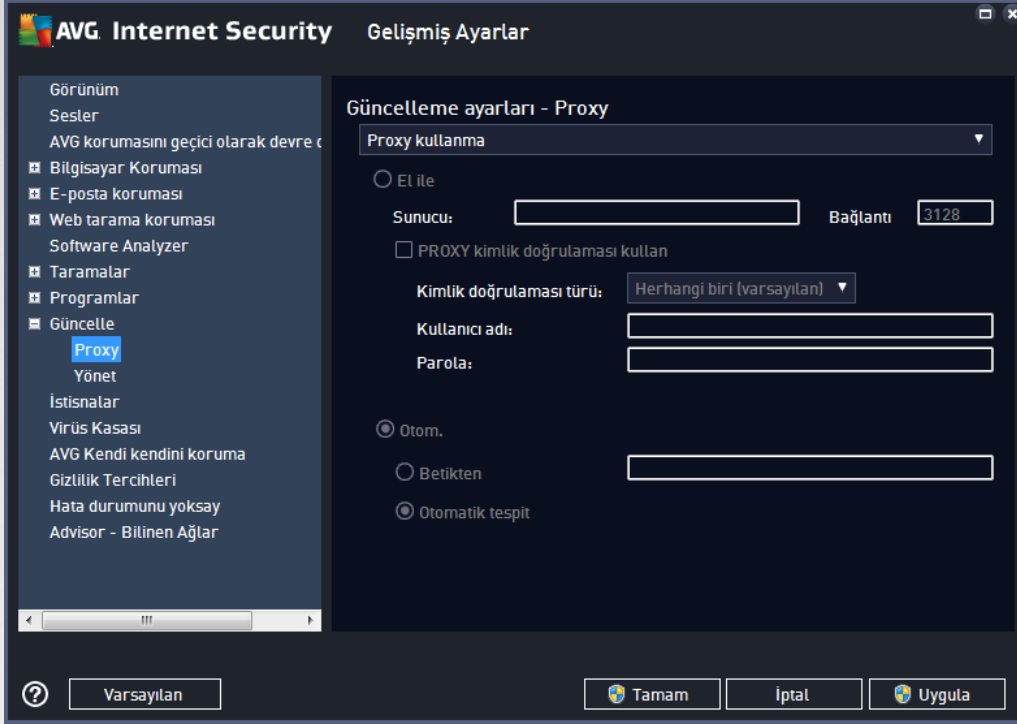
Başarıyla tamamlanan her güncelleme sonrasında yeni bir bellek taraması başlatmak istediğinizi belirtmek için bu onay kutusunu işaretleyin. En son indirilen güncelleme yeni virüs tanımlarını içerebilir ve bunlar taramaya hemen uygulanır.

Ek güncelleme seçenekleri

- **Her program güncellemesi sırasında yeni sistem geri alma noktası oluştur** (varsayılan olarak açık) - her AVG program güncelleme işlemi başlamadan önce bir sistem geri yükleme noktası oluşturulur. Güncelleme işleminin başarısız olması ve işletim sisteminizin çökmesi halinde işletim sisteminizi bu noktaya geri döndürebilirsiniz. Bu seçeneğe Başlat / Tüm Programlar / Donatılar / Sistem araçları / Sistem Geri Yükleme yoluyla erişebilirsiniz fakat değişikliklerin sadece uzman kullanıcılar tarafından yapılması önerilmektedir! Bu fonksiyonu kullanmak istiyorsanız bu onay kutusunu işaretleyin.
- **DNS güncelleme kullan** (varsayılan olarak açık) - bu öge işaretlendiğinde güncelleme işlemi başlatıldığında **AVG Internet Security** en yeni veritabanı sürümüyle ve DNS sunucusundaki en yeni program sürümüyle ilgili bilgileri arar. Yalnızca en küçük, kesin olarak gerekli güncelleme dosyaları indirilir ve uygulanır. Bu şekilde, indirilen toplam veri miktarı en düşük seviyede tutulur ve güncelleme süreci daha hızlı bir şekilde gerçekleştirilir.
- **Çalışan uygulamaları kapatmak için onay iste** (varsayılan olarak açık) - o anda çalışmakta olan uygulamaların izniniz olmaksızın kapatılmamasını sağlar (gerekirse güncelleme işleminin sonlandırılması için).
- **Bilgisayar saatini kontrol et** (varsayılan olarak açık) - bilgisayar saati ile doğru saat arasındaki fark belirlenen süreden uzun olduğunda bilgilendirilmek istediğinizi belirtmek için bu seçeneği işaretleyin.



7.10.1. Proxy



Proxy sunucusu, internete daha güvenli bir şekilde bağlanmanızı sağlayan bağımsız bir sunucu ya da bilgisayarınızda çalışan bir hizmet programıdır. Belirlenen ağ kuralları doğrultusunda, internete 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 manüel ya da otomatik olarak yapılandırılabilir.

Manüel yapılandırma

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

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



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

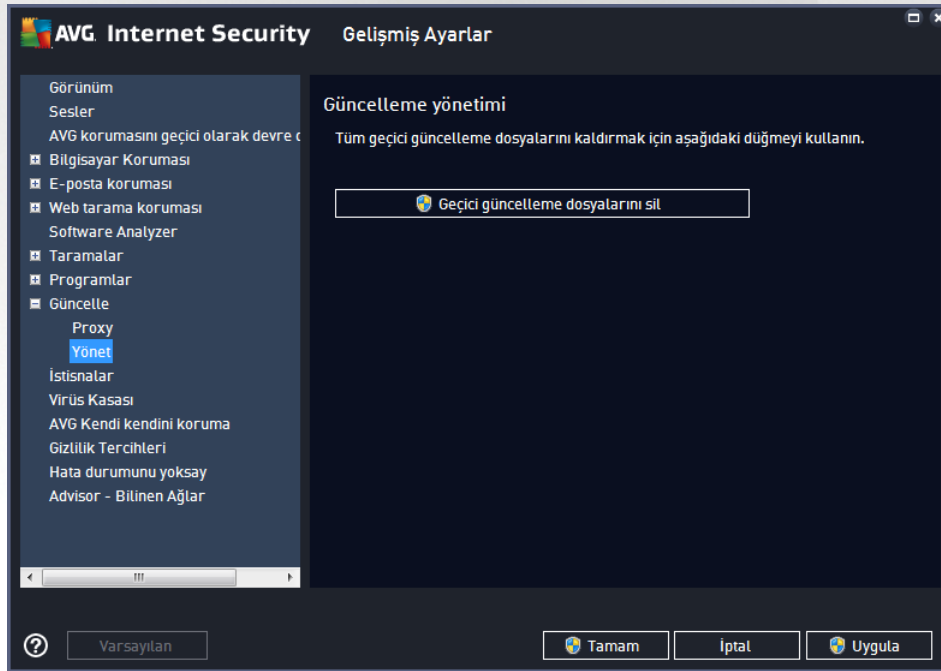
Otomatik yapılandırma

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

- **Tarayıcıdan** - yapılandırma varsayılan internet 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

7.10.2. Yönetme

Güncelleme Yönetimi iletişim kutusu, iki adet düğme vasıtasıyla erişilebilen iki seçenek sunmaktadır:



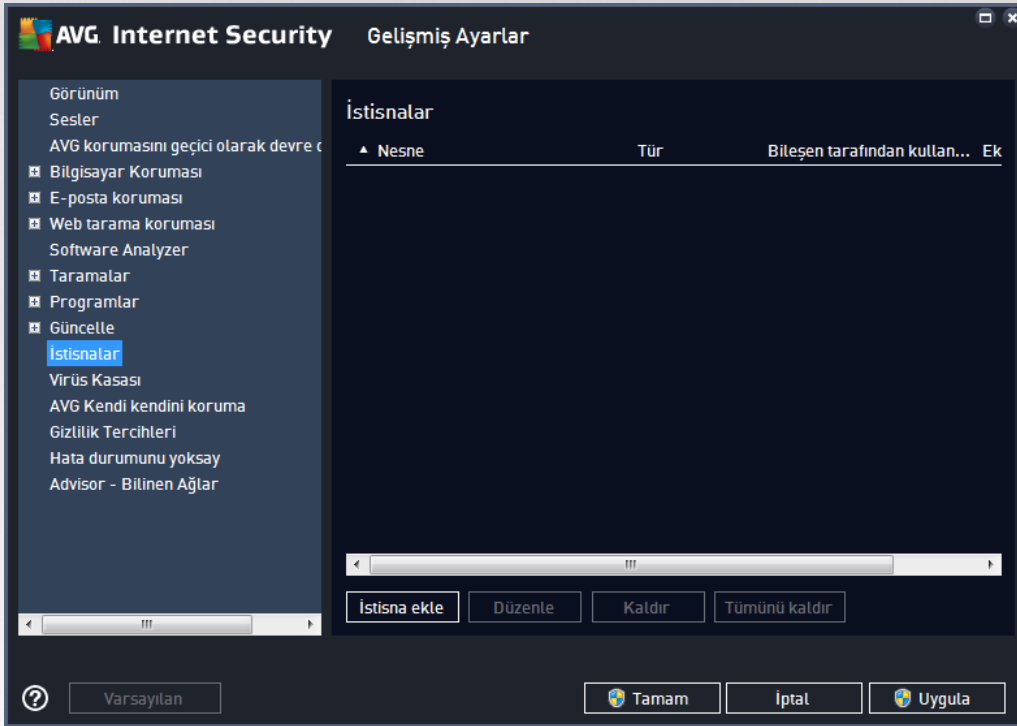
- **Geçici güncelleme dosyalarını sil** - tüm gereksiz güncelleme dosyalarını sabit diskinizden silmek için bu düğmeye basın (*varsayılan olarak söz konusu dosyalar 30 gün boyunca saklanır*)
- **Virüs veritabanını önceki sürümüne döndür** - en güncel virüs veritabanını sabit diskinizden silmek ve daha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



7.11. İstisnalar

İstisnalar iletişim kutusunda istisnalar, yani **AVG Internet Security** uygulamasının yoksayacağı 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.

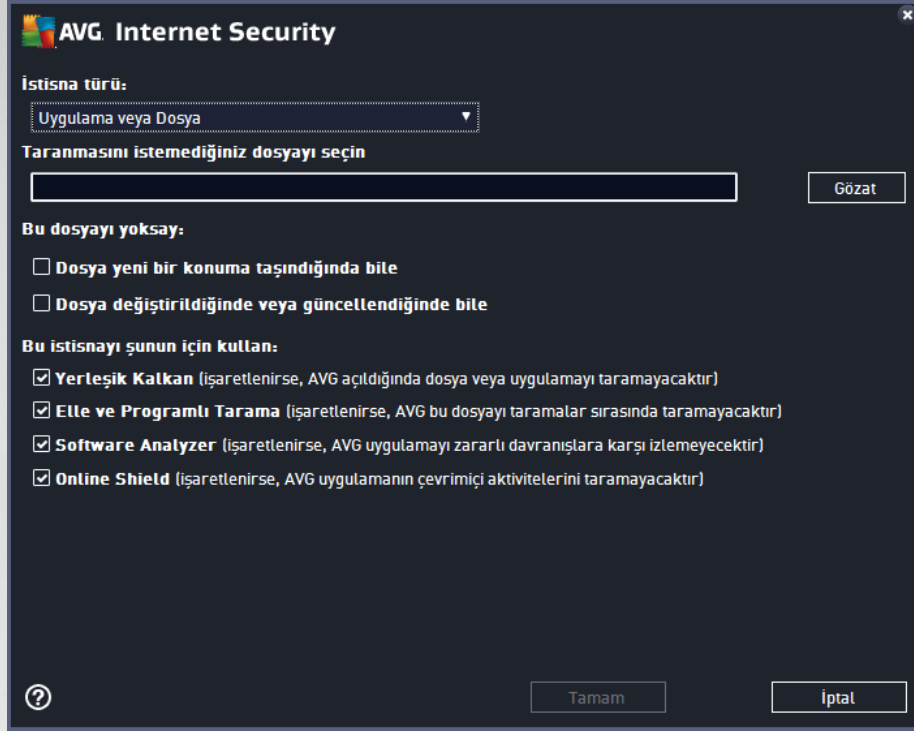
Lütfen ilgili dosya, program veya web sitesinin kesinlikle güvenli olduğundan daima emin olun!



İletişim kutusundaki tabloda, daha önce tanımlanan istisnalar varsa bunların bir listesi görüntülenir. Her öğenin yanında bir onay kutusu bulunur. Onay kutusu işaretliyse istisna etkindir. İşaretli değilse istisna tanımlanmıştır, ancak şimdilik kullanılmamaktadır. Sütun başlığını tıklatarak, izin verilen öğeleri ilgili kritere göre sıralayabilirsiniz.

Kontrol düğmeleri

- **İstisna ekle** - AVG taramasının dışında tutulacak bir öğe belirleyebileceğiniz yeni bir iletişim kutusu açmak için tıklanın:

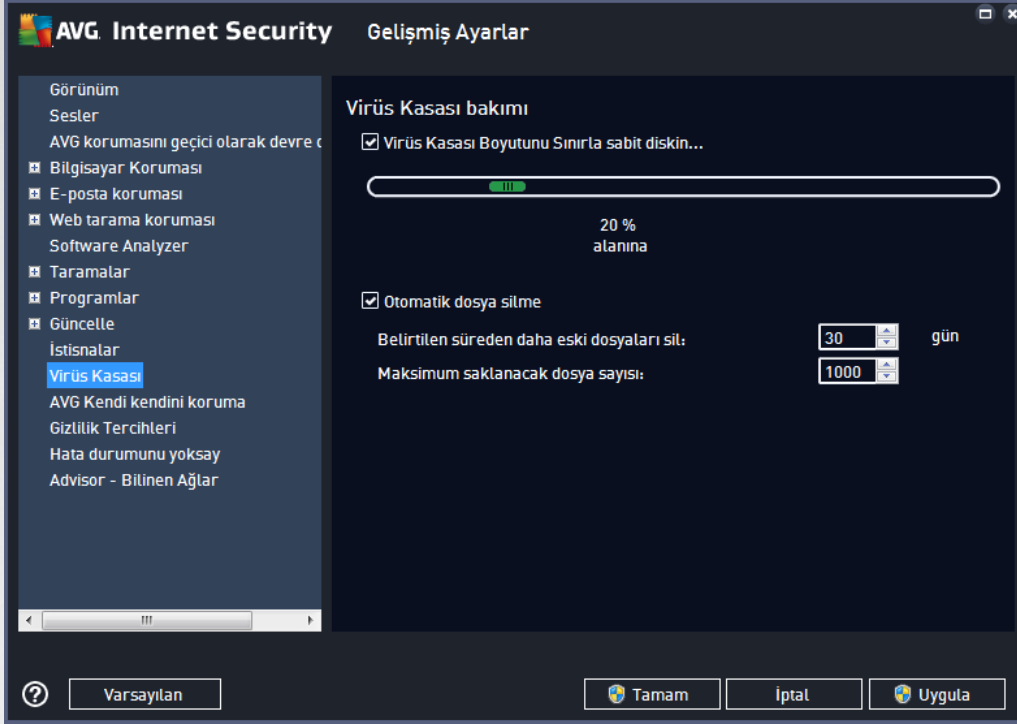


Önce, nesnenin türünü, yani nesnenin bir uygulama mı yoksa dosya, klasör, URL veya sertifika mı olduğunu belirlemeniz gerekir. Ardından ilgili nesnenin yolunu diskinizden bulmanız veya URL'yi yazmanız gerekir. Son olarak, hangi AVG özelliklerinin (*Yerleşik Kalkan*, *Elle ve Programlı Tarama*, *Software Analyzer*, *Online Shield* ve *Windows Zararlı Yazılım Tarama Arayüzü*) seçilen nesneyi yoksayacağını seçebilirsiniz.

- **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 iptal edildiğinde ilgili dosya, klasör veya URL AVG tarafından yeniden kontrol edilir. Dosya veya klasörün kendisi değil, yalnızca istisna kaldırılır!
- **Tümünü kaldır** - Listedeki tüm tanımlı istisnaları silmek için bu düğmeyi kullanın.



7.12. Virüs Kasası

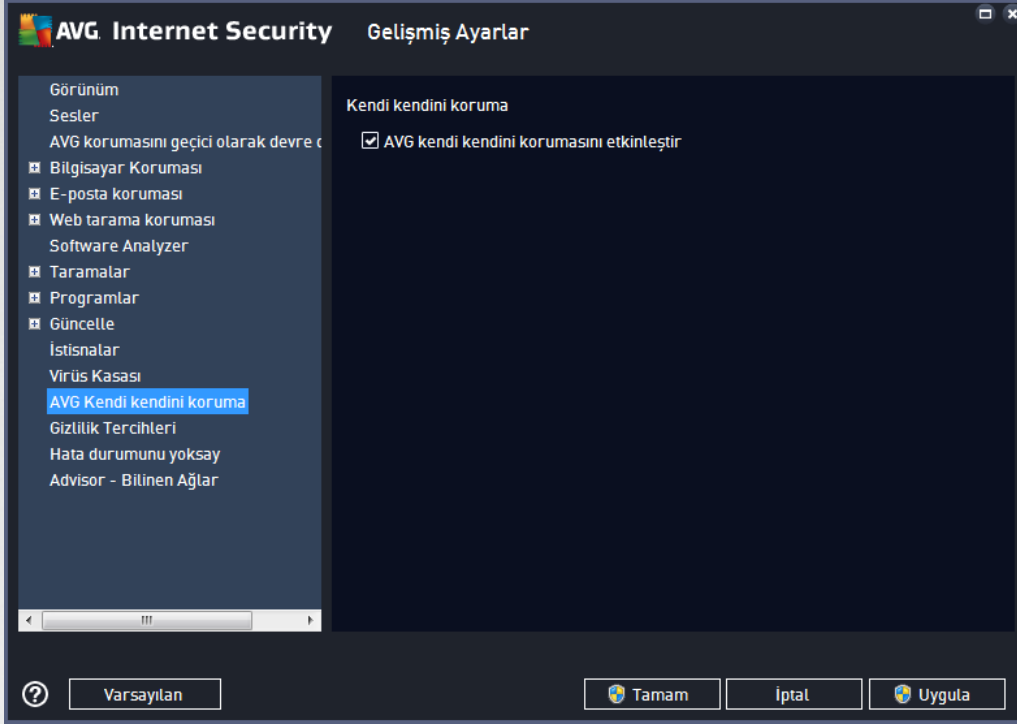


Virüs Kasası Bakımı iletişim kutusu, [Virüs Kasası](#)'nda saklanan nesnelerin yönetimiyle ilgili çeşitli parametreleri tanımlayabilmenizi sağlar:

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



7.13. AVG Kendi Kendini Koruma

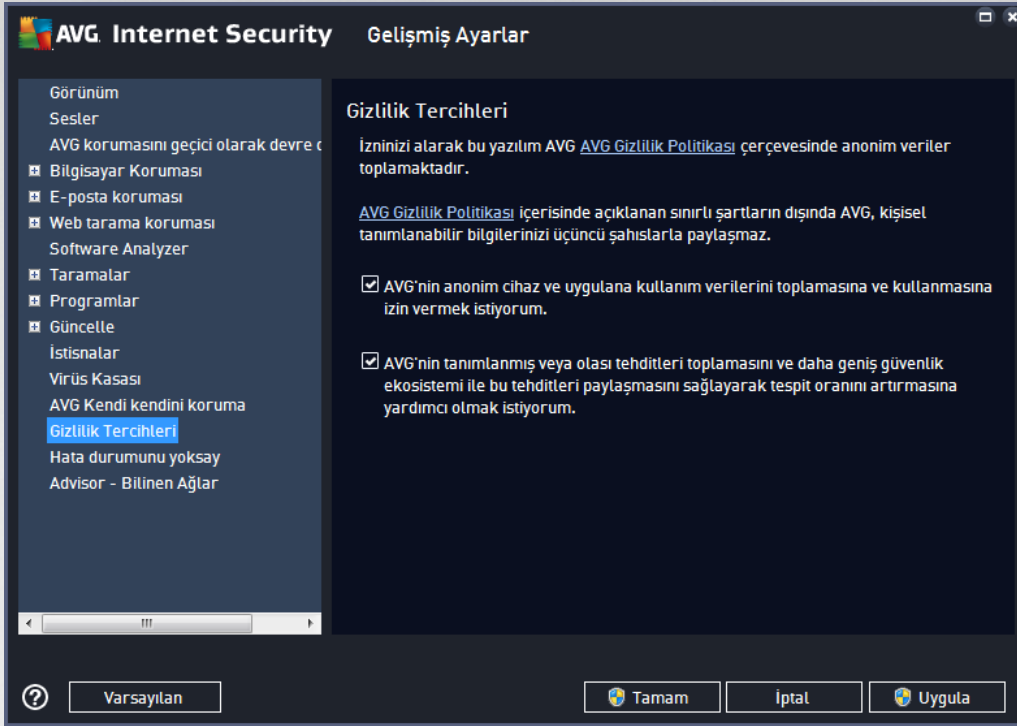


AVG Kendi Kendini Koruma, AVG Internet Security programının kendi işlem, dosya, kayıt defteri anahtarlarını ve sürücülerini değiştirilmekten ve devre dışı bırakılmaktan korur. Bu tür bir koruma sunmanın ana nedeni gelişkin tehditlerin önce virüs koruma yazılımını devre dışı bırakıp ardından bilgisayarınıza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

Bu özelliği açık tutmanızı öneririz!

7.14. Gizlilik Tercihleri

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



İletişim kutusundaki mevcut ayarlama seçenekleri:

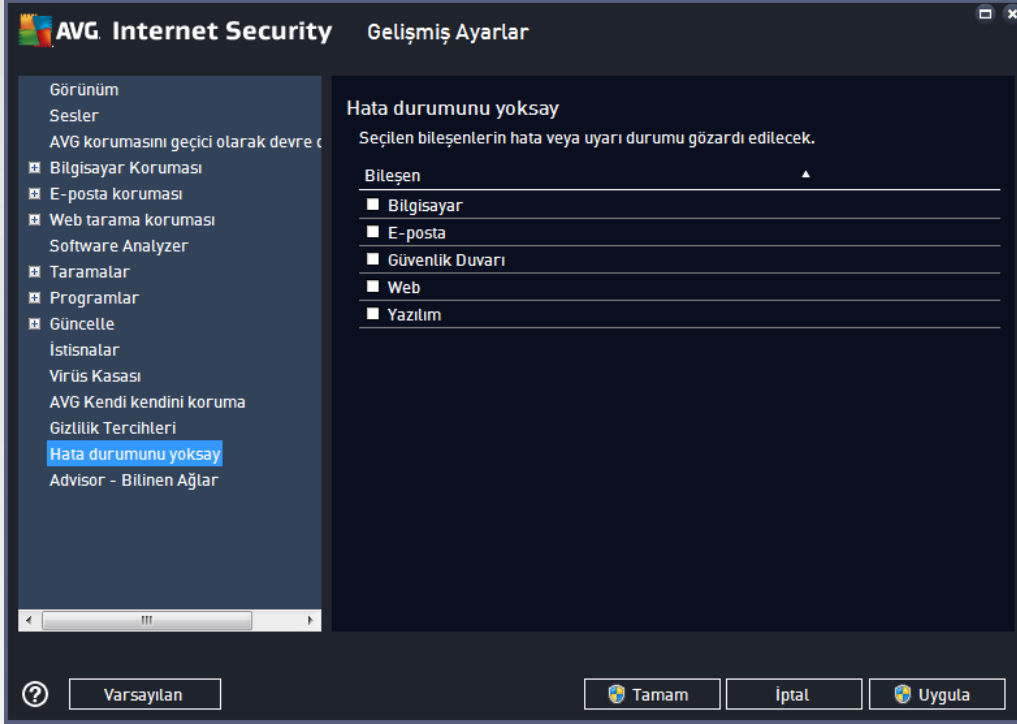
- **AVG Ürün Geliştirme Programı'na katılarak AVG'nin ürünlerini geliştirmesine yardımcı olmak istiyorum** (varsayılan olarak açık) - AVG Internet Security ürününü daha da geliştirmemize yardımcı olmak istiyorsanız onay kutusunu işaretli tutun. Bu şekilde, karşılaşılan tüm tehditler AVG'ye bildirilir 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.
- **Belirlenen veya şüpheli tehditler hakkında anonim veriler gönderilmesine izin ver** (varsayılan olarak açık) - tüm şüpheli veya gerçekten tehlikeli kod veya davranış modeli hakkında bilgi gönderin (bilgisayarınızda tespit edilen virüs, casus yazılım veya erişmeye çalıştığınız zararlı 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.
- **Tespitlerin bulut doğrulamasına izin ver** (varsayılan olarak açık) - hatalı pozitif sonuçları ayıklamak için tespit edilen tehditler gerçekten virüs bulaşması 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.

7.15. Hata Durumunu Yoksay

Hata durumunu yoksay iletişim kutusunda, bilgilendirilmek istemediğiniz bileşenleri seçebilirsiniz:



Varsayılan olarak listede herhangi bir bileşen seçilmemiştir. Bileşenlerden herhangi biri hata verirse aşağıdaki yöntemlerden biri vasıtasıyla uyarılacaksınız demektir:

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

Belirli bir nedenle bileşenlerden birini geçici olarak kapatmanız gereken bir durum olabilir. **Bu önerilmez, tüm bileşenleri sürekli olarak açık ve varsayılan yapılandırılmada tutmanız gerekir**, ancak böyle bir durum meydana gelebilir. Bu durumda sistem tepsisi simgesi, otomatik olarak bileşenin hata durumunda olduğunu bildirir. Ancak bu durumda gerçek bir hatadan söz edemeyiz çünkü hatayı siz başlatmışsınızdır ve potansiyel riskin farkında olmalısınız. Aynı zamanda, simge gri renkli görüntüledikten sonra daha sonra meydana gelecek hataları rapor edemez.

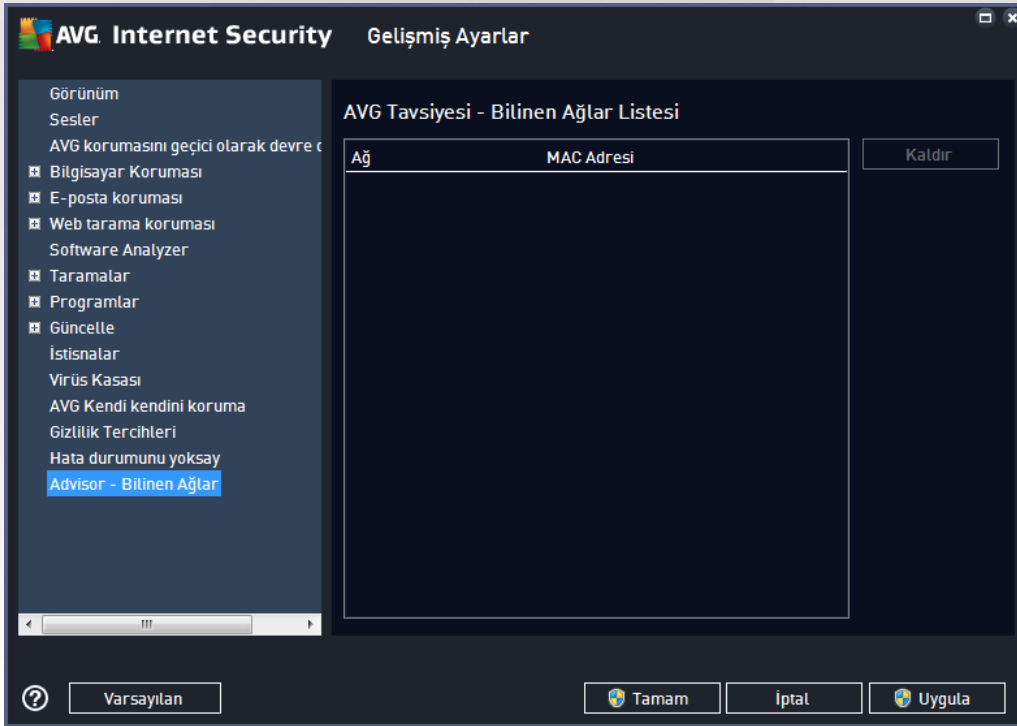
Bu durumda, **Hata durumunu yoksay** iletişim kutusunda hata durumunda olan (ya da kapatılmış) bileşenleri seçebilirsiniz ve söz konusu durum hakkında bilgilendirilmek istemeyebilirsiniz. Onaylamak için **Tamam** düğmesine basın.



7.16. Tavsiye - Bilinen Ağlar

[AVG Tavsiyesi](#) 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 güvenliğini kontrol etmenizi öneren bir özelliğe sahiptir. Yeni ağların bağlanmak için güvenli olduğuna karar vererseniz, 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 özniteliklerini 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.



8. Güvenlik Duvarı Ayarları

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

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

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

- [Gelişmiş Ayarlar](#)
- [Tanımlanan Ağlar](#)
- [Sistem Hizmetleri](#)
- [Günlükler](#)

8.1. Genel

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

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



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

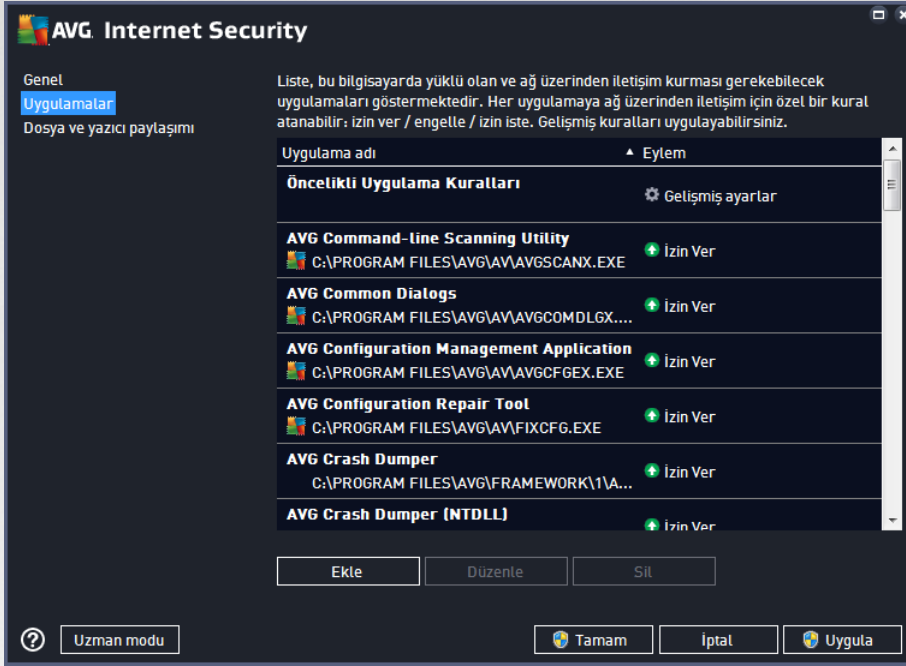
- **Otomatik** - Güvenlik Duvarı, bu modda tüm ağ trafiğini otomatik olarak denetler. Hiçbir karar için onayınız istenmez. Güvenlik Duvarı bilinen tüm uygulamalarla bağlantıya izin verir ve aynı zamanda uygulamaya her zaman bağlanabilmesi için bir kural oluşturulur. Güvenlik Duvarı, diğer uygulamalar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

Not: Güvenlik Duvarı içinde de bir otomatik mod mevcuttur. Bu mod, [Bilgisayar](#) veya [Software Analyzer](#) bileşeni kapatıldığında ve bu nedenle bilgisayarınız tehditlere açık hale geldiğinde sessizce etkinleştirilir. Bu tür durumlarda, Güvenlik Duvarı yalnızca bilinen veya kesinlikle güvenli uygulamalara otomatik olarak izin verir. Diğer tüm uygulamalar için sizin karar vermeniz istenir. Bunun nedeni devre dışı bırakılan bileşenlerin boşluğunu kapatmak ve bilgisayarınızı güvende tutmaktır.



8.2. Uygulamalar

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



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

- - tüm ağlar için iletişime izin verme
- - iletişimi engelleme
- - gelişmiş ayarları tanımlama

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

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

Listede, uygulamaların dışında iki özel öge vardır. **Öncelikli Uygulama Kuralları** (listenin üst kısmında) tercihe bağlıdır ve her zaman tek bir uygulamanın kurallarından önce uygulanır. **Diğer Uygulama Kuralları** (listenin alt kısmında bulunur) örneğin bilinmeyen veya tanımlanmayan bir uygulama için özel uygulama kuralları uygulanmadığında "son örnek" olarak kullanılır. Bu tür bir uygulama ağ üzerinden iletişim kurmaya çalıştığında tetiklenmesi gereken eylemi seçin: Engelle (iletişim her zaman engellenir), İzin ver (tüm ağlar üzerinden iletişime izin verilir), Sor (iletişime yönelik izin verme veya engelleme tercihi size bırakılır). **Bu öğelerin genel uygulamalardan farklı ayar seçenekleri bulunur ve bunlar yalnızca deneyimli kullanıcılara yöneliktir. Ayarları değiştirmemenizi önemle öneririz!**



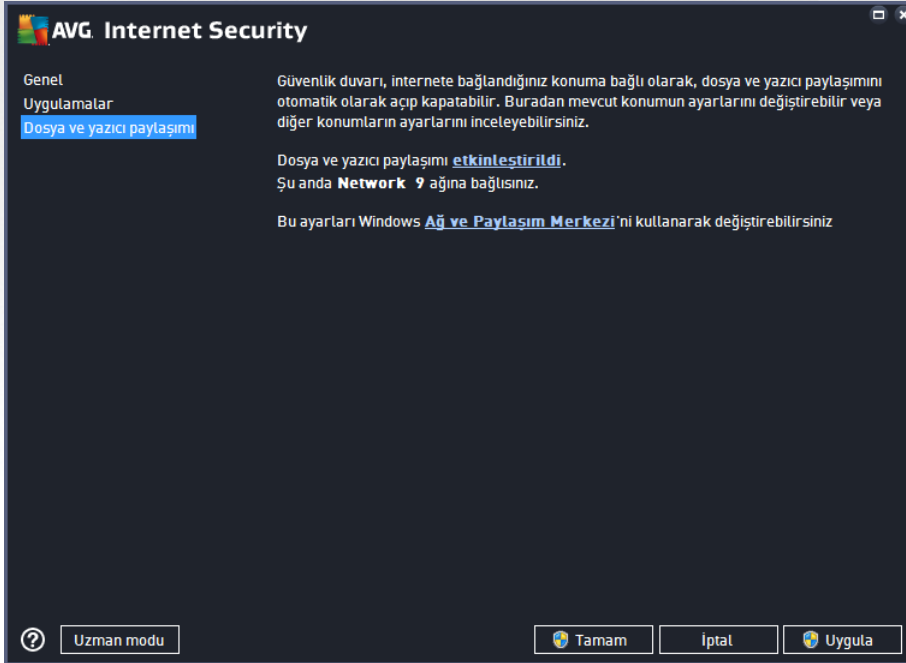
Kontrol düğmeleri

Liste, aşağıdaki denetim düğmeleri kullanılarak düzenlenebilir:

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

8.3. Dosya ve yazıcı paylaşımı

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

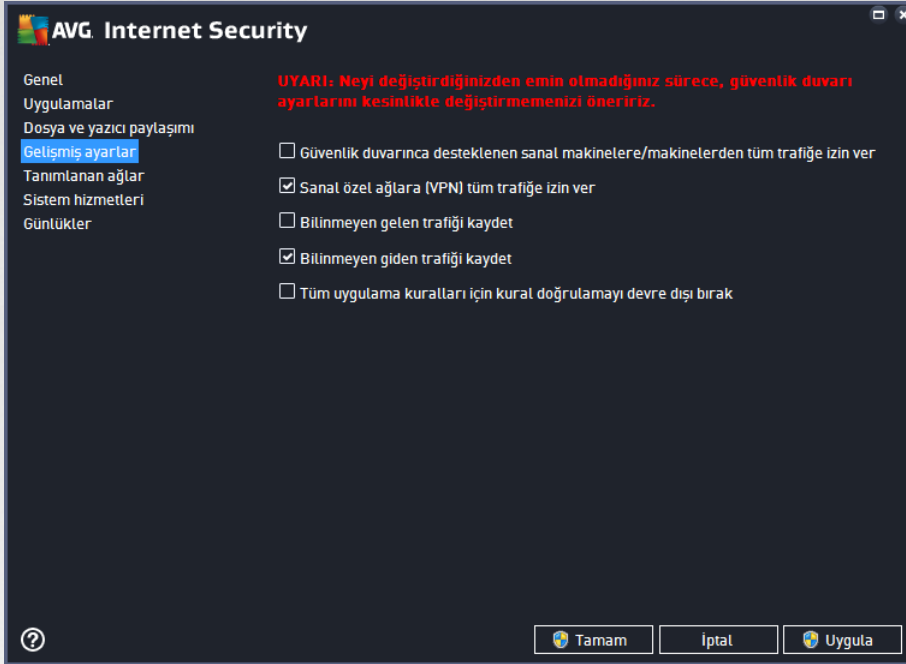


Dosya ve Yazıcı Paylaşımı iletişim kutusunda dosya ve yazıcı paylaşımı ve o anda bağlı olan ağların yapılandırmasını düzenleyebilirsiniz. Window XP'de, ağ adı ilgili ağa ilk bağlandığınızda ağ için seçtiğiniz adlandırmaya karşılık gelir. Windows Vista ve üstü sistemlerde, ağ adı Ağ ve Paylaşım Merkezi'nden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



8.4. Gelişmiş ayarlar

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



Gelişmiş ayarlar iletişim kutusu aşağıdaki Güvenlik Duvarı parametrelerini etkinleştirmenizi veya devre dışı bırakmanızı sağlar:

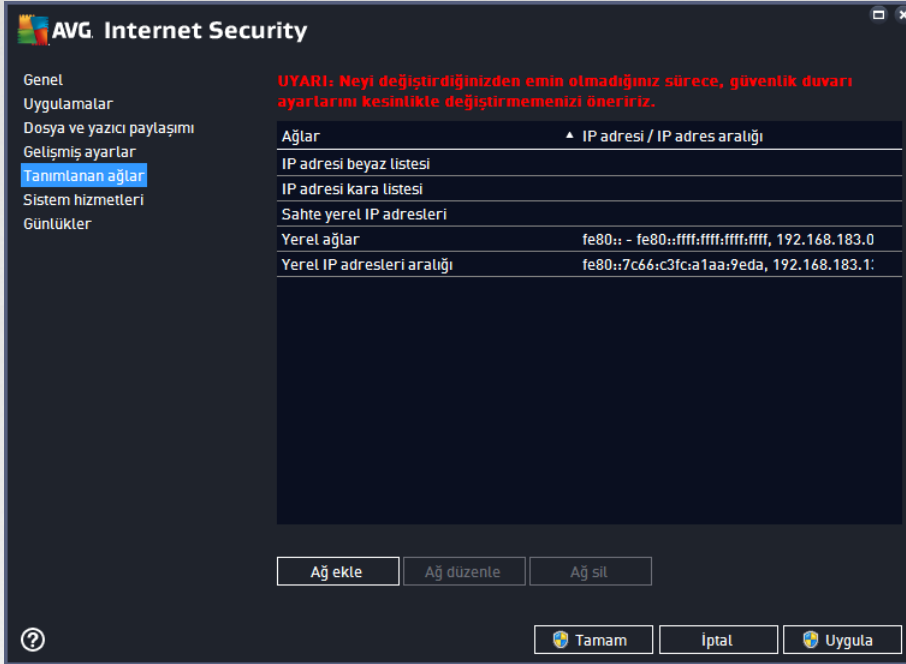
- **Güvenlik duvarınca desteklenen sanal makinelere/makinelerden tüm trafiğe izin ver** - VMware gibi sanal makinelerde ağ bağlantısı için destek.
- **Sanal özel ağlara (VPN) tüm trafiğe izin ver** - VPN bağlantıları (*uzak bilgisayarları bağlamak için kullanılır*) için destek.
- **Bilinmeyen gelen/giden trafiği günlük dosyasına kaydet** - bilinmeyen uygulamalardan kaynaklanan tüm iletişim girişimleri (*gelen/giden*) [Güvenlik Duvarı günlüğüne](#) kaydedilir.
- **Tüm uygulama kuralları için kural doğrulamayı devre dışı bırak** - Güvenlik Duvarı sürekli olarak her uygulama kuralı kapsamındaki tüm dosyaları izler. İkili dosyada bir değişiklik gerçekleştiğinde, Güvenlik Duvarı bir kez daha standart yöntemle, yani sertifikasını doğrulayarak, [güvenilir uygulamalar veritabanında](#) arayarak vb. bir yolla uygulamanın güvenilirliğini onaylamaya çalışır. Uygulama güvenli olarak değerlendirilmezse Güvenlik Duvarı uygulama için [seçilen moda](#) göre işlem yapar:
 - Güvenlik Duvarı **Otomatik mod**'da çalışıyorsa uygulamaya varsayılan olarak izin verilir;
 - Güvenlik Duvarı **Etkileşimli mod**'da çalışıyorsa uygulama engellenir ve kullanıcıya uygulama için nasıl bir işlem yapılmasını istediğini soran bir iletişim kutusu görüntülenir.

Belirli bir uygulamaya yönelik olarak nasıl işlem yapılacağıyla ilgili istenen süreç [Uygulamalar](#) iletişim kutusunda her uygulama için ayrı ayrı tanımlanabilir.



8.5. Tanımlanan ağlar

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

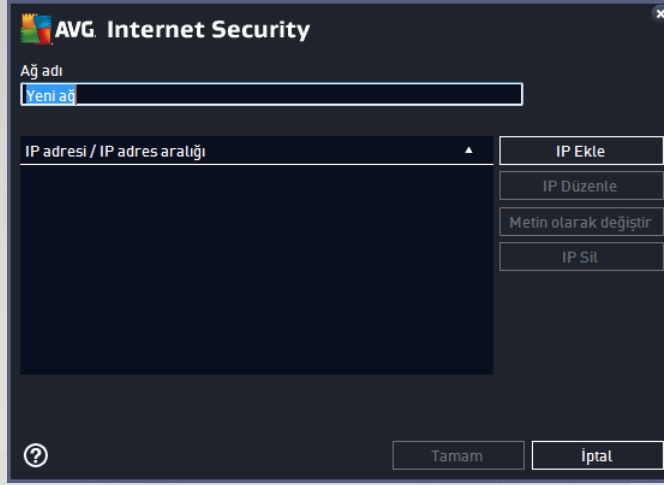


Tanımlanan ağlar iletişim kutusunda bilgisayarınızın bağlı olduğu ağlar görüntülenir. Liste tespit edilen her ağla ilgili aşağıdaki bilgileri sağlar:

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

Kontrol düğmeleri

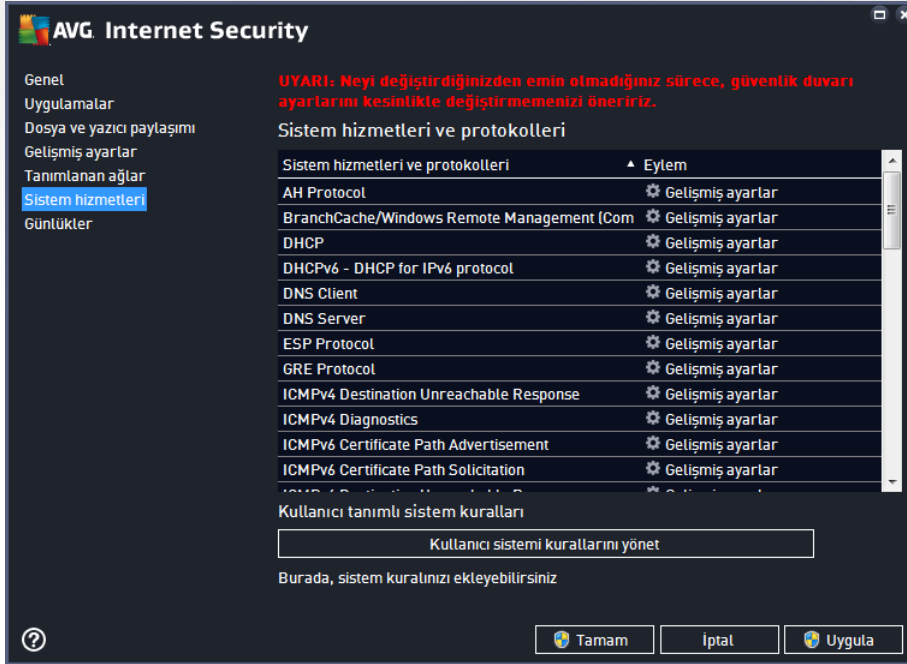
- **Ağ ekle** - yeni tanımlanan ağın parametrelerini düzenleyebileceğiniz yeni bir iletişim penceresi açar; yani **Ağ adı** girmek ve **IP adresi aralığı** belirlemek için:



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

8.6. Sistem hizmetleri

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



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

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



- **Eylem** - Bu sütun atanan eylemin simgesini görüntüler:

- Tüm ağlar için iletişime izin ver
- İletişimi engelle

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

Kullanıcı tanımlı sistem kuralları

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



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

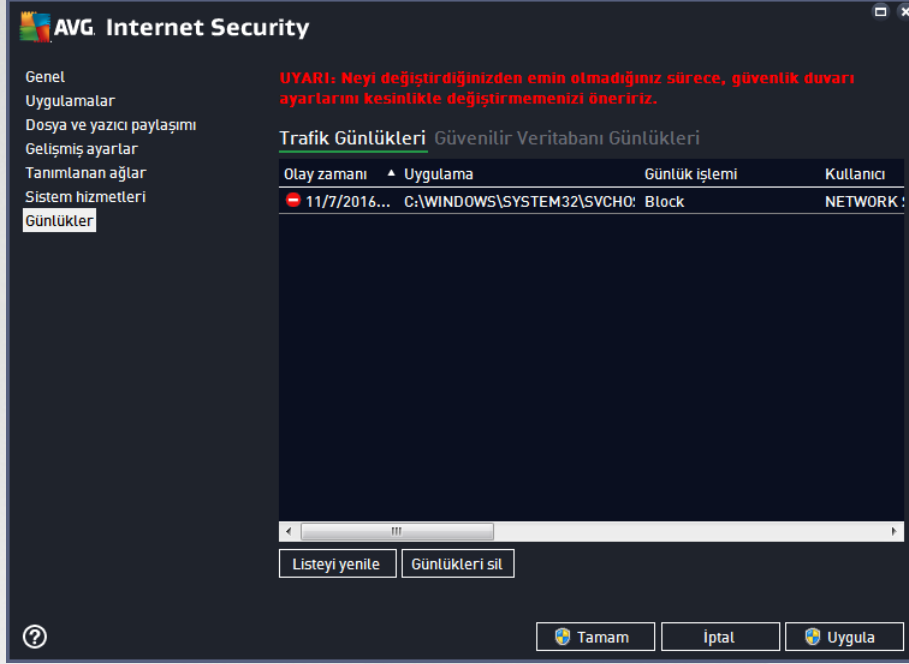
8.7. Günlükler

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

Günlükler iletişim kutusu, kaydedilen tüm Güvenlik Duvarı eylemlerini ve etkinliklerini ilgili parametrelerin ayrıntılı tanımları ile birlikte iki sekmede görüntüleyebilenizi sağlar:



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



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



AVG Internet Security

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

UYARI: Neyi değiştirdiğinizden emin olmadığımız sürece, güvenlik duvarı ayarlarınızı kesinlikle değiştirmenizi öneririz.

Trafik Günlükleri **Güvenilir Veritabanı Günlükleri**

Olay zamanı	Uygulama	PID	İle
11/7/2016, 1:09:11 PM	C:\PROGRAM FILES\INTERNET EXPLORE	5032	Gü
11/7/2016, 1:09:19 PM	C:\STAF\BIN\STAFPROC.EXE	2276	Gü
11/7/2016, 1:09:33 PM	C:\PROGRAM FILES\SILK\SILKTEST\AGE	2364	Gü
11/7/2016, 1:18:12 PM	C:\WINDOWS\EHOME\MCUPDATE.EXE	6004	Gü

Listeyi yenile Günlükleri sil

Tamam İptal Uygula

Kontrol düğmeleri


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



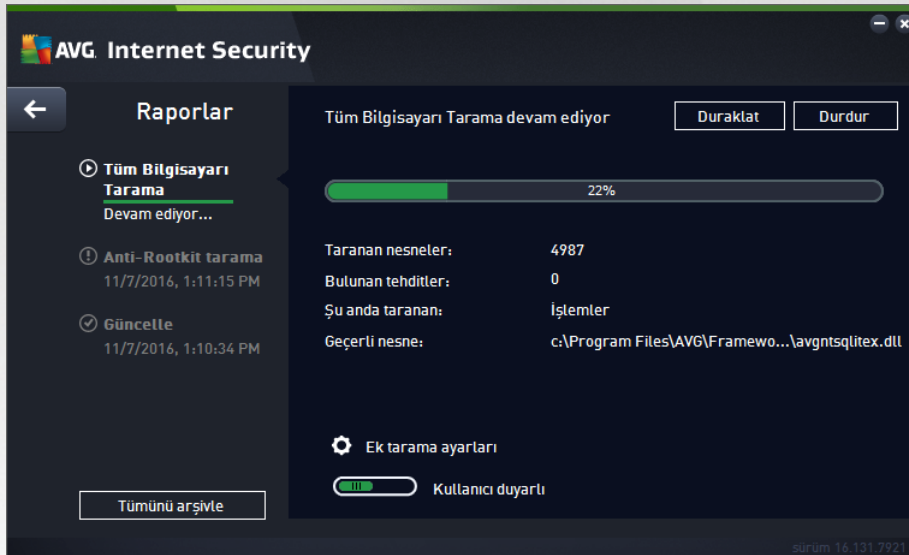
9. AVG Tarama

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

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

erişilebilir: 

- **Şimdi 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:

- **Zamanlanmış 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 programlı tarama görebilirsiniz. Tarama varsayılan olarak kapatılmıştır. Taramayı açmak için sağ tıklayın ve bağlam menüsünden *Görevi etkinleştir*'i seçin. Programlı tarama etkinleştirildiğinde *Tarama zamanlamasını düzenle* düğmesiyle [taramanın yapılandırmasını düzenleyebilirsiniz](#). Kendi istediğiniz yeni bir tarama zamanlaması oluşturmak için *Tarama zamanlaması 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 tarama](#) başlıklı bölüme bakın*). *Ayarlar* bölümünü tıklarızsanız [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 (*seçilen dosya ve klasörlerin taranmasıyla ilgili ayrıntılar için lütfen [Öntanımlı taramalar / Belirli dosyaları veya klasörleri tarama](#) başlıklı bölüme bakın*). *Ayarlar* bölümünü tıklarızsanız [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 tarama](#) adlı ilgili bölüme bakın*). *Ayarlar* bölümünü tıklarızsanız [rootkit taramasının yapılandırma iletişim kutusunu](#) açarsınız.



9.1. Öntanımlı taramalar

Başlıca **AVG Internet Security** özelliklerinden biri isteğe bağlı taramalardır. İsteğe bağlı taramalar, muhtemel bir virüs hakkında şüpheye düştüğünüz an bilgisayarınızın istediğiniz kısmında istediğiniz zaman yapabileceğiniz taramalardır. Kısacası, bilgisayarınızda virüs olduğunu düşünmeseniz bile söz konusu taramaların düzenli aralıklarla yapılması önerilmektedir.

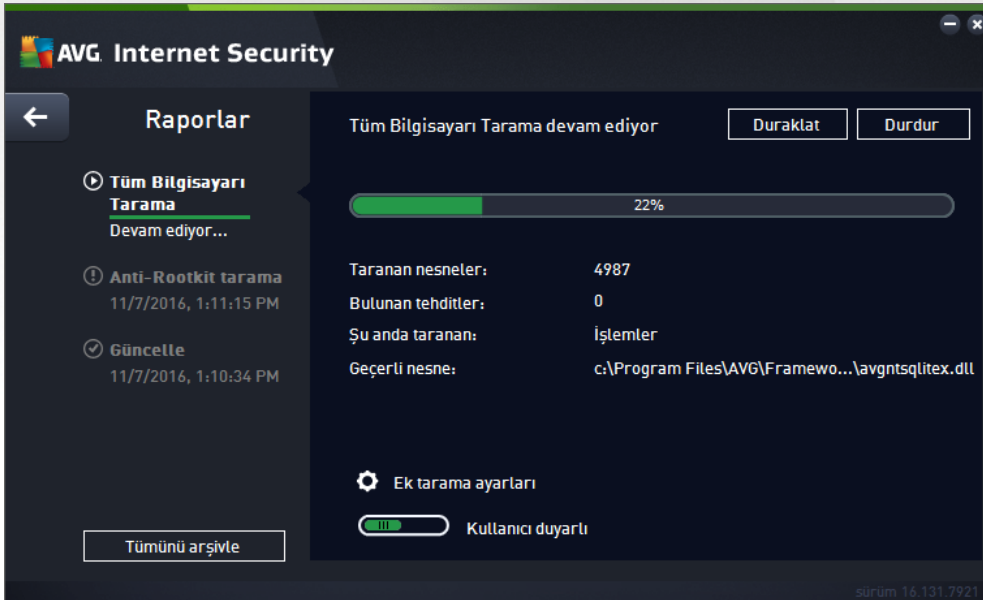
AVG Internet Security içinde, yazılım satıcısının önceden tanımladığı aşağıdaki tarama türlerini bulacaksınız:

9.1.1. Tüm bilgisayarı tara

Tüm bilgisayarı tara tüm bilgisayarı muhtemel bulaşmalara ve/veya potansiyel olarak istenmeyen uygulamalara karşı tarar. Bu tarama, bilgisayarınızın tüm sabit disklerini tarayacak, virüsleri tespit edecek ve temizleyecek ya da tespit edilen bulaşmayı **Virüs Kasası**'na taşıyacaktır. Bilgisayarın tümü haftada en az bir defa taranmalıdır.

Tarama başlatma

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



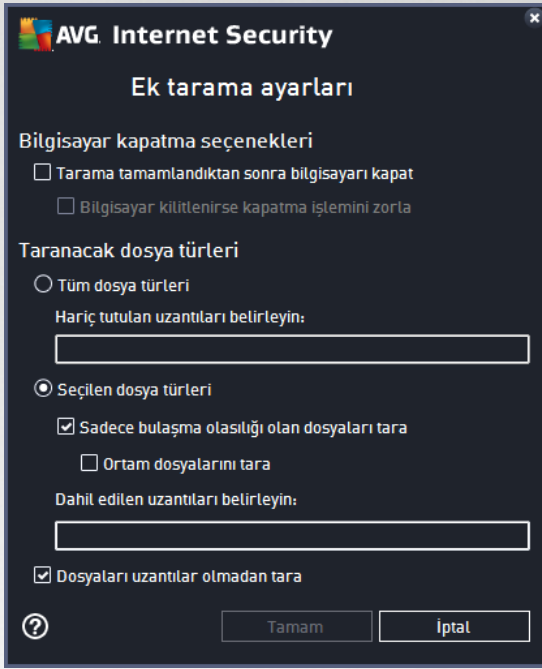
Tarama parametreleri listesindeki belirli parametreleri isteğiniz doğrultusunda açıp kapatabilirsiniz:

- **Bulaşmayı bana sormadan temizle / kaldır** (varsayılan olarak açık) - Tarama sırasında virüs tespit edildiğinde, çözüm varsa otomatik olarak temizlenir. Bulaşmış dosya otomatik olarak temizlenemezse bulaşmış nesne [Virüs Kasası](#)'na taşınır.
- **Potansiyel olarak istenmeyen uygulamalar ve casus yazılım tehditlerini bildir** (varsayılan olarak açık) - Virüslerin yanı sıra casus yazılımları da taramak için işaretleyin. Casus yazılım, şüpheli zararlı 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 uygulamalar geliştirilmiş grubunu bildir** (varsayılan olarak kapalı) - Casus yazılımların, yani doğrudan üreticiden alındığında 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 kullanıcılar hakkındaki site tercihleri veya elektronik alışveriş sepetlerinin içeriği gibi belirli bilgilerin doğrulanması, izlenmesi ve muhafaza edilmesi için kullanılır).
- **Arşivlerin içini tara** (varsayılan olarak kapalı) - Bu parametre ZIP, RAR vb. arşiv dosyalarının içinde saklanan tüm dosyaların taranmasını sağlar.
- **Buluşsal yöntem kullan** (varsayılan olarak açık) - Buluşsal 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.
- **Kapsamlı taramayı etkinleştir** (varsayılan olarak kapalı) - 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.

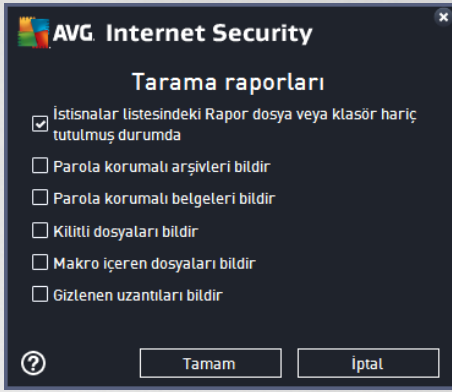
- **Rootkit'leri tara** (varsayılan olarak açık): tüm bilgisayar taramasına anti-rootkit taramasını dahil eder. [Anti-rootkit taraması](#) ayrı olarak da başlatılabilir.
- **Ek tarama ayarları** - bağlantı, şu parametreleri belirtebileceğiniz yeni bir Ek tarama ayarları iletişim kutusu açar:



- **Bilgisayar kapatma seçenekleri** - çalışan tarama işlemi bittiğinde bilgisayarın otomatik olarak kapatılması gerekip gerekmediğine karar verir. Bu seçeneği işaretlerseniz (**Tarama tamamlandıktan sonra bilgisayarı kapat**) bilgisayar geçerli durumda kilitli olsa bile bilgisayarın kapatılmasını sağlayan bir seçeneğin bulunduğu bir pencere açılacaktır (**Bilgisayar kilitletirse kapatma işlemini 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.
 - **Seçilen dosya türleri** - yalnızca virüs bulaşma olasılığı olan dosyaları taramayı istediğinizi belirtebilirsiniz (*virüs bulaşmayan dosyalar taranmayacaktır, örneğin, bazı düz metin dosyaları veya çalıştırılmayan bazı başka 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** karar verebilirsiniz; bu seçenek varsayılan olarak açıktır ve gerçekten bir nedeniniz yoksa değiştirmeniz önerilir. Uzantısı olmayan dosyalar şüpheli olabilir ve her zaman taranmalıdır.



- **Taramanın ne kadar hızlı tamamlanacağını ayarlayın** - tarama sürecinin önceliğini değiştirmek için kaydırma çubuğunu kullanabilirsiniz. Varsayılan olarak, bu seçenek otomatik kaynak kullanımının kullanıcıya duyarlı seviyesine ayarlıdır. Buna alternatif olarak, sistem kaynakları kullanımını minimize etmek için tarama işlemini daha yavaş (*bilgisayarda çalışmanız gerektiği ve taramanın ne kadar sürdüğünü önemsemediğiniz durumlar için uygundur*) ya da sistem kaynaklarını oldukça yoğun kullanarak daha hızlı (*ör. bilgisayarı geçici olarak kimse kullanmayacak ise*) gerçekleştirebilirsiniz.
- **Ek tarama raporlarını ayarla** - bağlantı üzerinden **Tarama Raporları** isimli bir iletişim kutusu açılır ve buradan ne tip buluntuların rapor edileceğini seçebilirsiniz:



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

9.1.2. Belirli dosyaları veya klasörleri tara

Belirli Dosyaları veya Klasörleri Tara - bilgisayarınızın sadece taraması 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. **Taramak için belirli dosya ve klasörleri seçin** adında yeni bir iletişim kutusu açılır. Bilgisayarınızın ağaç görünümünden taramasını 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 taramaması gibi bir seçenek de vardır. Bunu yapabilmek için otomatik olarak oluşturulan yolun başına "-" işareti koyun (*ekran görüntüsüne bakın*). 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 (*iletişim 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!**

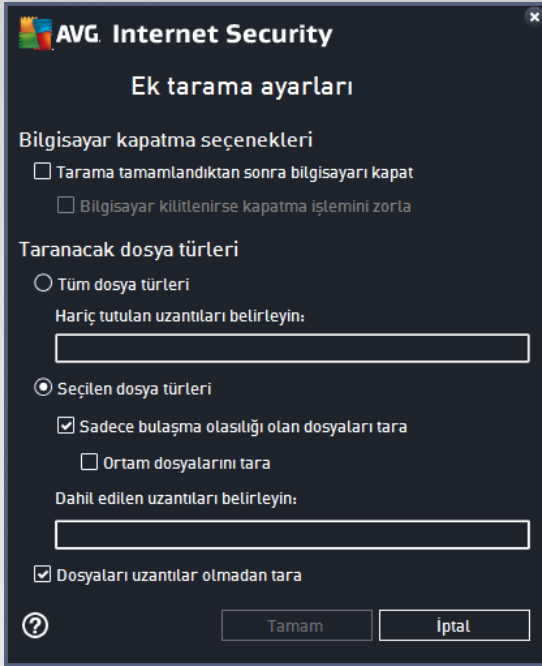


Tarama parametreleri listesinde parametreleri ihtiyaçlarınıza uygun olarak açabilir / kapatabilirsiniz:

- **Virüs bulaşmasını bana sormadan temizle / sil** (varsayılan olarak açık): Tarama sırasında bir virüs tespit edildiğinde, çözümü varsa otomatik olarak temizlenebilir. Bulaşmış dosya otomatik olarak temizlenemezse bulaşmış nesne [Virüs Kasası](#)'na taşınır.



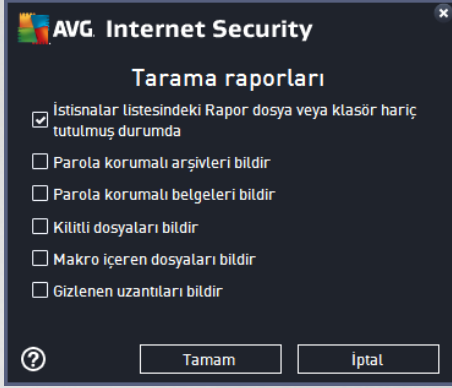
- **Potansiyel olarak istenmeyen uygulamalar ve casus yazılım tehditlerini bildir** (varsayılan olarak açık): Virüslerin yanı sıra casus yazılımları da taramak için işaretleyin. Casus yazılım, şüpheli zararlı yazılım kategorisini ifade eder: genellikle bir güvenlik riskini oluşturmasına rağmen bu programlardan bazıları bilerek yüklenebilir. Bilgisayarınızın güvenliğini artırdığından, bu özelliği etkin durumda tutmanızı öneririz.
- **Potansiyel olarak istenmeyen uygulamalar geliştirilmiş grubunu bildir** (varsayılan olarak kapalı): Casus yazılımların, yani doğrudan üreticiden alındığında 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 kullanıcılar hakkındaki site tercihleri veya elektronik alışveriş sepetlerinin içeriği gibi belirli bilgilerin doğrulanması, izlenmesi ve muhafaza edilmesi için kullanılır*).
- **Arşivlerin içeriğini tara** (varsayılan olarak açık): Bu parametre ZIP, RAR vb. arşiv dosyalarının içinde saklanan tüm dosyaların taranmasını sağlar.
- **Buluşsal Yöntem Kullan** (varsayılan olarak açık): Buluşsal analiz (*taranan nesnenin yönergelerinin sanal bir bilgisayar ortamında dinamik olarak canlandırılması*) tarama sırasında kullanılacak virüs tespiti yöntemlerinden birisidir.
- **Sistem ortamını tara** (varsayılan olarak kapalı): Tarama bilgisayarınızın sistem alanlarını da kontrol edecektir.
- **Kapsamlı taramayı etkinleştir** (varsayılan olarak kapalı): Belirli durumlarda (*bilgisayarınıza bulaşma olmasından şüpheleniyorsanız*) yalnızca emin olmak üzere, bilgisayarınızın bulaşma olması çok zor olan alanlarını bile tarayan, en kapsamlı tarama algoritmalarını etkinleştirmek için bu seçeneği işaretleyebilirsiniz. Ancak, bu yöntemin çok fazla zaman aldığını unutmayın.
- **Ek tarama ayarları** - Bağlantı, şu parametreleri belirtebileceğiniz yeni bir **Ek tarama ayarları** iletişim kutusu açar:



- **Bilgisayar kapatma seçenekleri** - çalışan tarama işlemi bittiğinde bilgisayarın otomatik olarak kapatılması gerekip gerekmediğine karar verir. Bu seçeneği işaretlerseniz (**Tarama tamamlandıktan sonra bilgisayarı kapat**) bilgisayar geçerli durumda kilitli olsa bile bilgisayarın kapatılmasını sağlayan bir seçeneğin bulunduğu bir pencere açılacaktır (**Bilgisayar kilitletirse kapatma işlemini 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;
 - **Seçilen dosya türleri** - yalnızca virüs bulaşma olasılığı olan dosyaları taramayı istediğinizi belirtebilirsiniz (*virüs bulaşmayan dosyalar taranmayacaktır, örneğin, bazı düz metin dosyaları veya çalıştırılmayan bazı başka 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** karar verebilirsiniz; bu seçenek varsayılan olarak açıktır ve gerçekten bir nedeniniz yoksa değiştirmeniz önerilir. Uzantısı olmayan dosyalar şüpheli olabilir ve her zaman taranmalıdır.
- **Taramanın ne kadar hızlı tamamlanacağını ayarlayın** - tarama sürecinin önceliğini değiştirmek için kaydırma çubuğunu kullanabilirsiniz. Varsayılan olarak, bu seçenek otomatik kaynak kullanımının kullanıcıya duyarlı seviyesine ayarlıdır. Buna alternatif olarak, sistem kaynakları kullanımını minimize etmek için tarama işlemini daha yavaş (*bilgisayarda çalışmanız gerektiği ve taramanın ne kadar sürdüğünü önemsemediğiniz durumlar için uygundur*) ya da sistem kaynaklarını oldukça yoğun kullanarak daha hızlı (*ör. bilgisayarı geçici olarak kimse kullanmayacak ise*) gerçekleştirebilirsiniz.



- **Ek tarama raporlarını ayarla** - bağlantı üzerinden **Tarama Raporları** isimli yeni bir iletişim kutusu açılır ve buradan ne tip potansiyel bulguların rapor edileceğini seçebilirsiniz:



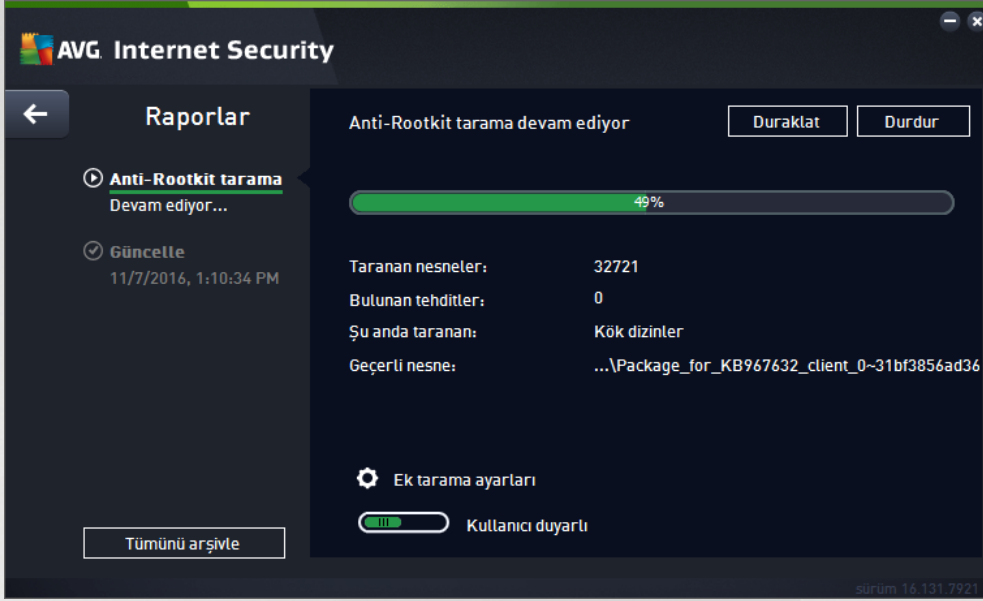
Uyarı: Bu tarama ayarları, yeni tanımlanan taramanın parametreleri ile aynıdır - [AVG Taraması / Tarama zamanlama / Tarama Tipi](#) bölümünde açıklandığı doğrultuda. **Belirli dosyaları veya klasörleri tara** işlevinin varsayılan yapılandırmasını değiştirmeye karar vererseniz yeni ayarlarınızı, belirli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

9.1.3. 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 bulaşma olduğu anlamına gelmez. Rootkit'ler bazen sürücülerde kullanılır ya da doğru uygulamaların bir parçası olabilir.

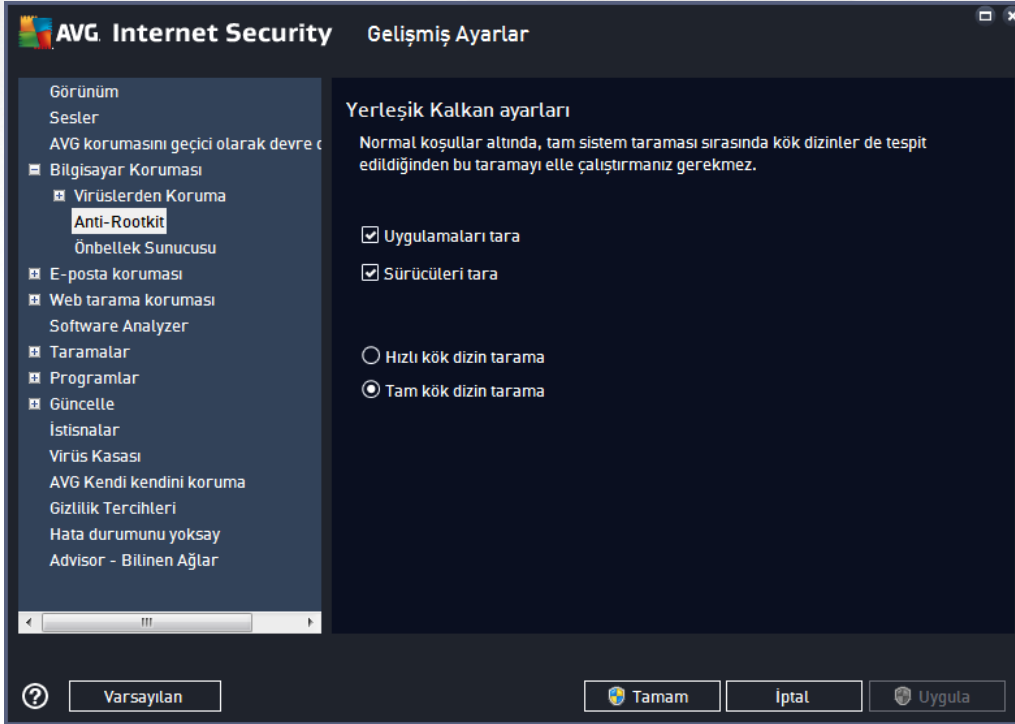
Tarama başlatma

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 (*iletişim kutusuna [Tarama seçenekleri](#) iletişim kutusundaki Bilgisayarda rootkit'leri tara işleminin Ayarlar bağlantısından erişilebilir*). **Değiştirmek için geçerli bir nedeniniz olmadığı müddetçe varsayılan ayarları korumanız önerilir!**



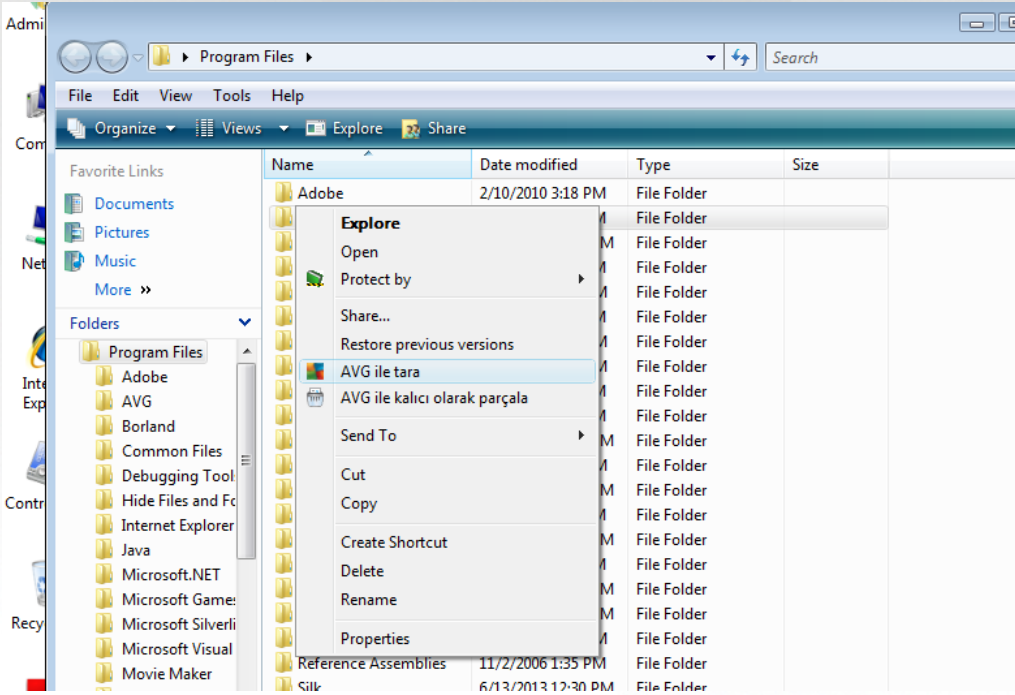


Tarama uygulamaları ve **Tarama sürücülerini** anti-rootkit taramasına nelerin dahil edileceğini ayrıntılı şekilde belirlemenize olanak tanır. Bu ayarlar gelişmiş kullanıcılara yöneliktir; tüm seçenekleri açık konumda muhafaza etmenizi öneririz. Rootkit tarama modunu da seçebilirsiniz:

- **Hızlı rootkit tarama** - çalışan tüm işlemleri, tüm yüklü sürücülerini ve ayrıca sistem klasörünü (genellikle c:\Windows) tarar
- **Tam rootkit tarama** - çalışan tüm işlemler, tüm yüklü sürücüler ve sistem klasörünün (genellikle c:\Windows) yanı sıra tüm yerel diskleri (flash disk dahil, ancak disket/CD sürücülerini hariç) tarar

9.2. Windows Gezgininde Tarama

Bilgisayarın tümünde ya da seçilen bölümlerinde gerçekleştirilen öntanımlı taramaların yanı sıra **AVG Internet Security**, doğrudan Windows Gezgininde 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 Gezgininde 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 Internet Security**

9.3. Komut satırı tarama

AVG Internet Security uygulamasında tarama işleminin komut satırından gerçekleştirilmesine yönelik bir seçenek bulunmaktadır. 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:

- **avgscanx** 32 bit işletim sistemi için
- **avgscana** 64 bit işletim sistemi için

9.3.1. Komut sözdizimi

Komut söz dizimi aşağıdaki gibidir:

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

9.3.2. Tarama parametreleri

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

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

9.3.3. Grafik arayüzünden çalıştırılan CMD taraması

Bilgisayarınızı Windows Güvenli Modda çalıştırdığınız zaman komut satırı taramasını grafik kullanıcı arayüzünden başlatma seçeneğiniz de bulunmaktadır:





Güvenli Modda tarama işleminin kendisi komut satırından başlatılır. Bu iletişim kutusu yalnızca rahat grafik arayüzünde tarama parametrelerini belirlemenize olanak tanır.

Önce bilgisayarınızın taranmasını istediğiniz alanlarını seçin. Önceden tanımlanmış [Tüm Bilgisayarı Tara](#) veya [Seçilen klasörleri veya dosyaları tara](#) seçeneklerinden birini seçebilirsiniz. Üçüncü seçenek olan **Hızlı tarama** ise, bilgisayarınızın başlatılması için gerekli tüm kritik alanları inceleyen Güvenli Modda kullanılmak için tasarlanmış belirli bir tarama başlatır.

Bir sonraki bölümdeki tarama ayarları ayrıntılı tarama parametreleri belirlemenizi sağlar. Tüm ayarlar varsayılan olarak işaretlidir; bu ayarları korumanızı ve özel bir nedeniniz olmadığı sürece bir parametrenin seçimini kaldırmamanızı tavsiye ederiz:

- **"Potansiyel olarak istenmeyen programları" tara** - virüslerin yanı sıra casus yazılımların da taranması
- **Alternatif Veri Akışlarını Tara (yalnızca NTFS için)** - NTFS Alternatif Veri Akışlarının, yani özellikle zararlı kodlar içeren verileri gizlemek amacıyla saldırganlar tarafından kötüye kullanılacak olan bir Windows özelliğinin taranması
- **Bulaşmaları otomatik olarak temizle veya kaldır** - tüm olası tespitlerle ilgilenilir ve bunlar otomatik olarak bilgisayarınızdan temizlenir veya kaldırılır
- **Aktif işlemleri tara** - bilgisayarınızın belleğine yüklenmiş işlemlerin ve uygulamaların taranması
- **Kayıt defterini tara** - Windows kayıt defterinin taranması
- **Ana Önyükleme Kaydı kontrolünü etkinleştir** - Bölüm tablosu ve Önyükleme kesiminin taranması

Son olarak, bu iletişim kutusunun alt bölümünde tarama raporunun dosya adını ve türünü belirtebilirsiniz.

9.3.4. CMD tarama parametreleri

Komut satırı taramada kullanılacak parametrelerin listesi:

- **/?** Bu konuyla ilgili yardımı görüntüle
- **/@** Komut dosyası /dosya adı/
- **/ADS** Alternatif Veri Akışlarını Tara (*yalnızca NTFS only*)
- **/ARC** Arşivleri tara
- **/ARCBOMBSW** Yeniden sıkıştırılmış arşiv dosyalarını bildir
- **/ARCBOMBSW** Arşiv bombalarını bildir (*tekrar tekrar sıkıştırılan arşivler*)
- **/BOOT** MBR/BOOT kontrolünü etkinleştir
- **/BOOTPATH** Hızlı Tarama başlat
- **/CLEAN** Otomatik olarak temizle
- **/CLOUDCHECK** Hatalı tespitler açısından denetle



- /COMP [Tüm bilgisayarı tara](#)
- /COO Çerezleri tara
- /EXCLUDE Tarama işleminden dizin yolu veya dosyaları hariç tut
- /EXT Bu uzantıları tara (örneğin, EXT=EXE,DLL)
- /FORCESHUTDOWN Tarama tamamlandıktan sonra bilgisayarı kapatmayı zorla
- /HELP Bu konuyla ilgili yardımı görüntüle
- /HEUR Buluşsal analiz kullan
- /HIDDEN Gizli uzantılı dosyaları bildir
- /IGNLOCKED Kilitli dosyaları yoksay
- /INFECTABLEONLY Yalnızca bulaşabilir uzantıya sahip dosyaları tara
- /LOG Bir tarama sonucu dosyası oluştur
- /MACROW Makroları bildir
- /NOBREAK CTRL-BREAK ile işlemin kesilmesine izin verme
- /NOEXT Bu uzantıları tarama (örneğin, NOEXT=JPG)
- /PRIORITY Tarama önceliğini belirle (Düşük, Otomatik, Yüksek - bkz. [Gelişmiş ayarlar / Taramalar](#))
- /PROC Etkin işlemleri tara
- /PUP Potansiyel olarak istenmeyen uygulamaları bildir
- /PUPEXT Potansiyel olarak istenmeyen uygulamalar geliştirilmiş grubunu bildir
- /PWDW Parola korumalı dosyaları bildir
- /QT Hızlı test
- /REG Kayıt defterini tara
- /REPAPPEND Rapor dosyasına ekle
- /REPOK Bulaşmamış dosyaları Tamam olarak rapor et
- /REPORT Dosyaya rapor et (dosya adı)
- /SCAN [Belirli dosya ya da klasörleri tara](#) (SCAN=yol;yol - örneğin, /SCAN=C:\;D:\)
- /SHUTDOWN Tarama tamamlandıktan sonra bilgisayarı kapat

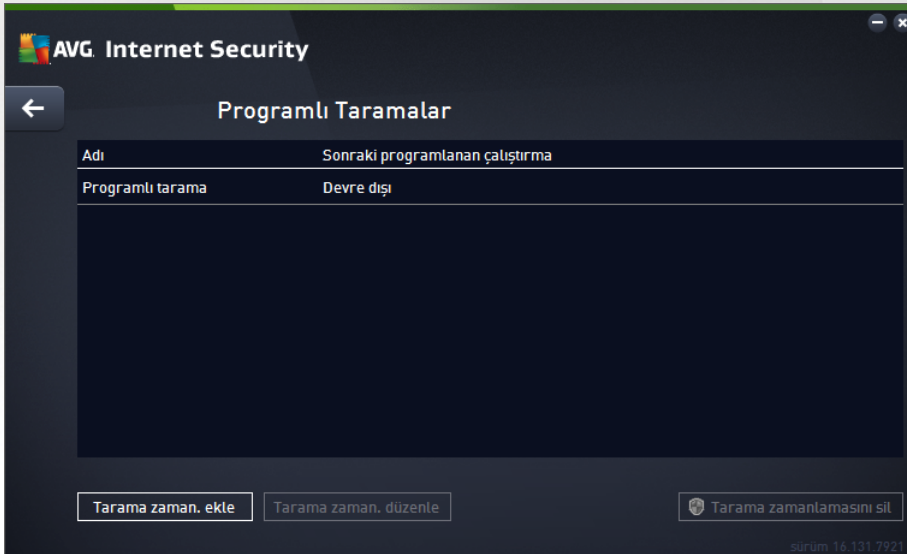


- /THOROUGHSCAN Kapsamlı taramayı etkinleştir
- /TRASH Bulaşan dosyaları [Virüs Kasası](#)na taşı

9.4. Tarama programlama


AVG Internet Security ile isteğiniz doğrultusunda tarama yapmanın (örneğin bilgisayarınıza virüs bulaştığından şüphelenirseniz) yanı 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 tara](#) işlemini en az haftada bir kez düzenli olarak başlatmanız gerekir. Diğer bir yandan, mümkün olması halinde programlı tarama varsayılan yapılandırmasında ayarlandığı gibi tüm bilgisayar taramasını günlük olarak gerçekleştirin. 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 **Programlı taramalar** iletişim kutusunda oluşturulabilir / düzenlenebilir. Yeni **Programlı Tarama** iletişim kutusunda geçerli olarak programlanmış olan tüm taramaların genel görünümünü görebilirsiniz:



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

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

Her sekmede "trafik ışığı" düğmesinin  konumunu değiştirerek zamanlanan testi geçici olarak devre dışı bırakabilir ve gerektiğinde yeniden açabilirsiniz.



9.4.1. Zamanla



Programla 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 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 (*Çalıştırma sıklığı ...*) ya da kesin bir tarih ve saat tanımlanarak (*Belirli saatlerde çalıştır*) veya tarama başlatmayla ilişkilendirilmesi gereken bir olay tanımlanarak (*Bilgisayar başlangıcında çalıştır*) tanımlanabilir.
- **Gelişmiş programlama seçenekleri** - Bu bölümde, bilgisayar düşük güç modundaydı veya tamamen kapatılmışsa hangi koşullar altında taramanın başlatılması/başlatılmaması gerektiğini belirleyebilirsiniz. Programlanan tarama belirttiğiniz saatte başlatıldığında, [AVG sistem tepsi simgesi](#) üzerinde açılan 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 [Programlı taramalar](#) genel görünümüne döner. Bu nedenle, tüm sekmelerdeki test parametrelerini yapılandırmak istiyorsanız gereksinimlerinizin tamamını belirledikten sonra bunları kaydetmek için düğmeye basın.



- - [Programlı taramalar](#) genel görünümüne dönmek için iletişim kutusunun sol üst bölümündeki yeşil oku kullanın.

9.4.2. Ayarlar



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

- **Virüs bulaşmasını bana sormadan temizle / sil** (varsayılan olarak açık): Tarama sırasında bir virüs tespit edildiğinde, çözümü varsa otomatik olarak temizlenebilir. Bulaşmış dosya otomatik olarak temizlenemezse bulaşmış nesne [Virüs Kasası](#)'na taşınır.
- **Potansiyel olarak istenmeyen uygulamalar ve casus yazılım tehditlerini bildir** (varsayılan olarak açık): virüslerin yanı sıra casus yazılımları da taramak için işaretleyin. Casus yazılım, şüpheli zararlı 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 uygulamalar geliştirilmiş grubunu bildir** (varsayılan olarak kapalı): Casus yazılımların, yani doğrudan üreticiden alındığında 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 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*).



- **Arşivlerin içini tara** (varsayılan olarak kapalı): Bu parametre, tarama işleminde ZIP, RAR vb. bir arşiv ile saklanmış olsa bile tüm dosyaların taranması gerektiğini belirtir.
- **Buluşsal yöntem kullan** (varsayılan olarak açık): Buluşsal 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.
- **Kapsamlı taramayı etkinleştir** (varsayılan olarak kapalı) belirli durumlarda (bilgisayarınıza bulaşma olmasından şüpheleniliyorsa) yalnızca emin olmak üzere, bilgisayarınızın bulaşma olması çok zor olan alanlarını bile tarayan, en kapsamlı tarama algoritmalarını etkinleştirmek için bu seçeneği işaretleyebilirsiniz. Ancak, bu yöntemin çok fazla zaman aldığını unutmayın.
- **Rootkit'leri tara** (varsayılan olarak açık): Anti-Rootkit taraması bilgisayarınızı olası rootkit'lere karşı (bilgisayarınızdaki zararlı yazılım etkinliği içerebilecek programlar ve teknolojiler açısından) tarar. Bir rootkit tespit edilmesi bilgisayarınızda mutlaka bulaşma olduğu anlamına gelmez. Bazı durumlarda, belirli sürücüler veya normal uygulamaların bölümleri yanlışlıkla rootkit olarak tespit edilebilir.

Ek tarama ayarları

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

The screenshot shows the 'Ek tarama ayarları' (Advanced Scan Settings) dialog box in AVG Internet Security. The dialog is titled 'AVG. Internet Security' and 'Ek tarama ayarları'. It contains the following settings:

- Bilgisayar kapatma seçenekleri**
 - Tarama tamamlandıktan sonra bilgisayarı kapat
 - Bilgisayar kilitletirse kapatma işlemini zorla
- Taranacak dosya türleri**
 - Tüm dosya türleri
 - Hariç tutulan uzantıları belirteyin: [Empty text box]
 - Seçilen dosya türleri
 - Sadece bulaşma olasılığı olan dosyaları tara
 - Ortam dosyalarını tara
 - Dahil edilen uzantıları belirteyin: [Empty text box]
 - Dosyaları uzantılar olmadan tara

At the bottom, there is a help icon (?), a 'Tamam' button, and an 'İptal' button.

- **Bilgisayar kapatma seçenekleri** - çalışan tarama işlemi bittiğinde bilgisayarın otomatik olarak kapatılması gerekip gerekmediğine karar verin. Bu seçeneği seçerseniz (*Tarama tamamlandıktan sonra bilgisayarı kapat*) bilgisayar geçerli durumda kilitli olsa bile bilgisayarın kapatılmasını sağlayan bir seçeneğin bulunduğu bir pencere açılacaktır (*Bilgisayar kilitletirse kapatma işlemini zorla*).
- **Taranacak dosya türleri** - taranacak dosya türleriyle ilgili aşağıdaki tercihlerden birini de yapmanız gerekir:



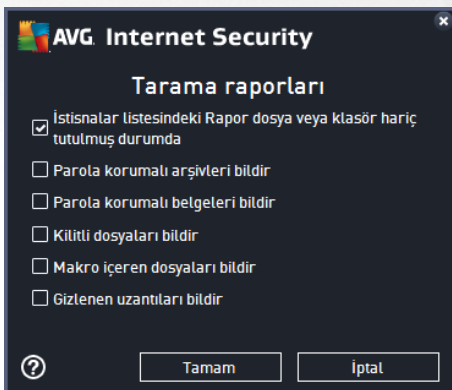
- **Tüm dosya türleri** taranmaması gereken virgülle ayrılmış dosya uzantılarının listesini sağlayarak taramada istisnaları tanımlama seçeneğiyle.
- **Seçilen dosya türleri** - yalnızca virüs bulaşma olasılığı olan dosyaları taramayı istediğinizi belirtebilirsiniz (*virüs bulaşmayan dosyalar taranmayacaktır, örneğin, bazı düz metin dosyaları veya çalıştırılmayan bazı başka dosyalar*); ortam dosyaları (*video, ses dosyaları - bu onay kutusunun işaretini kaldırırsanız, bu dosyalar genellikle çok büyük olduğundan ve virüs bulaşma olasılıkları çok az olduğundan tarama süresini daha da azaltır*). Tekrar, her zaman taranması gereken dosyaları uzantılarına göre belirtebilirsiniz.
- İsteğe bağlı olarak, **Uzantıları olmayan dosyaları taramaya** da karar verebilirsiniz ve bu seçenek varsayılan olarak açıktır ve gerçekten bir nedeniniz yoksa değiştirmemeniz önerilir. Uzantısı olmayan dosyalar şüpheli olabilir ve her zaman taranmalıdır.

Taramanın ne kadar hızlı tamamlanacağını ayarla

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 açık, ancak kimse tarafından kullanılmadığı sırada seçilebilir*). Öte yandan, tarama süresini uzatarak sistem kaynaklarının kullanımını azaltabilirsiniz.

Ek tarama raporlarını ayarla

Ek tarama raporlarını ayarla ... bağlantısını tıklatarak tarama bulgularının rapor edilmesi gerekip gerekmediğini tanımlamak üzere birden fazla öğeyi ayarlayabileceğiniz **Tarama raporları** olarak adlandırılan bağımsız bir iletişim kutusu açın:



İletişim kutusundaki kontroller

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



- - [Programlı taramalar](#) genel görünümüne dönmek için iletişim kutusunun sol üst bölümündeki yeşil oku kullanın.

9.4.3. Konum



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

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

- **Yerel sabit sürücüler** - bilgisayarınızdaki tüm sabit sürücüler
- **Program dosyaları**
 - C:\Program Dosyaları\
 - 64 bit'lik sürümde C:\Program Dosyaları (x86)
- **Belgelerim klasörü**
 - Win XP için: C:\Documents and Settings\Varsayılan Kullanıcı\Belgelerim\
 - Windows Vista/7 için: C:\Kullanıcılar\kullanıcı\Belgeler\
- **Paylaşılan Belgeler**



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

İletişim kutusundaki kontroller

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

9.5. Tarama sonuçları

Adı	Başlangıç za...	Bitiş zamanı	Test edilen ne...	Bulaşmalar	Yükse
Anti-Rootkit tarama	11/7/2016, 1:11	11/7/2016, 1:11	32974	0	0
Tüm Bilgisayarı Tarama	11/7/2016, 1:11	11/7/2016, 1:11	5160	0	0

Ayrıntıları göster Sonucu sil

sürüm 16.131.7921

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
 - Bulaşmalar bulundu ve temizlenmedi, tarama tamamlandı
 - Bulaşmalar bulundu ve temizlenmedi, tarama tamamlanmadan yarıda kesildi
 - Bulaşmalar bulundu ve tümü temizlendi 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 [programlı taramanızdır](#).
- **Başlangıç zamanı** - Taramanın başlatıldığı tarih ve saati verir.
- **Bitiş zamanı** - Taramanın tamamlandığı, duraklatıldığı veya kesildiği tarih ve saati verir.
- **Test edilen nesnelere** - Taranan toplam nesne sayısını gösterir.
- **Bulaşmalar** - Kaldırılan/bulunan toplam bulaşma sayısını verir.
- **Yüksek / Orta / Düşük** - Sonraki üç sütun sırasıyla bulunan yüksek, orta ve düşük öncelikli bulaşma sayısını verir.
- **Rootkit'ler** - Tarama sırasında bulunan toplam [rootkit](#) sayısını gösterir.

İletişim kutusu kontrolleri

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

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

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

9.6. Tarama sonuçları ayrıntıları

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

- **Özet** - Sekme, tarama hakkındaki temel bilgileri sunar: Taramanın başarıyla tamamlanıp tamamlanmadığı, tehdit bulunup bulunmadığı ve bulunanlara ne olduğu.



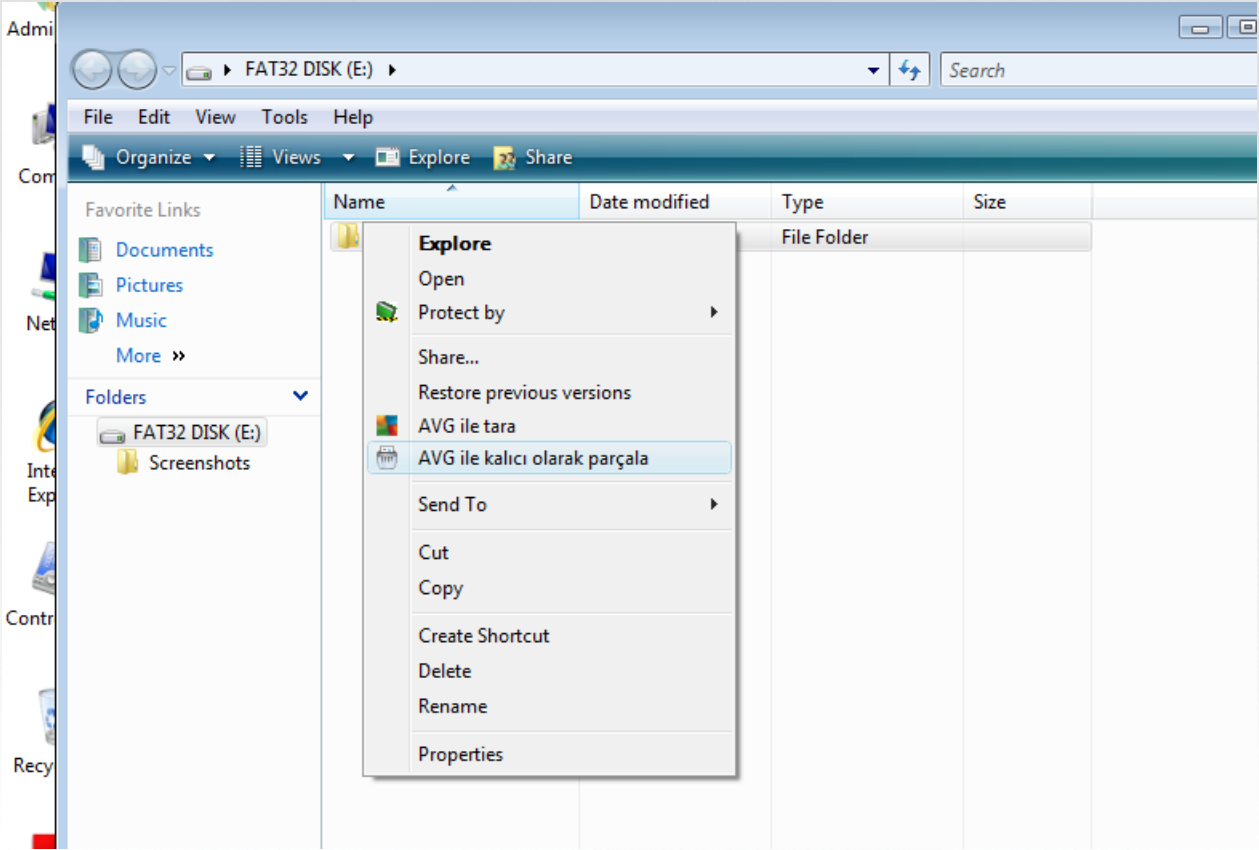
- **Ayrıntılar** - Bu sekme tespit edilen tüm tehditlerin ayrıntıları da dahil olmak üzere tarama hakkındaki tüm bilgileri gösterir. Genel görünümü dosyaya aktarma özelliği ayrıntıları .csv dosyası olarak kaydetmenize olanak tanır.
- **Tespitler** - Bu sekme ancak tarama sırasında tehdit tespit edilmişse 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 potansiyel olarak istenmeyen uygulama (*reklam yazılımı gibi*) veya izleme çerezleri
 - **Yüksek önem derecesi:** virüsler, Truva atları, açıktan yararlanma girişimleri vb. ciddi tehditler. Ayrıca Buluşsal tespit yöntemi tarafından tespit edilen nesnelere, virüs veritabanında henüz tanımlanmamış tehditler gibi.



10. 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**'yı 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.



11. Virüs Kasası

Virüs Kasası AVG taramaları sırasında tespit edilen şüpheli/bulaşmış nesnelere için güvenli bir ortamdır. Tarama sırasında bulaşmış bir nesne tespit edildikten sonra AVG, söz konusu bulaşmayı otomatik olarak temizleyemiyorsa şüpheli nesne hakkında ne yapmak istediğiniz sorulur. Önerilen çözüm, nesneyi daha sonra ilgilenmek üzere **Virüs Kasası**'na taşımaktır. **Virüs Kasası**'nın ana amacı silinen bir dosyayı belirli bir süre için saklamasıdır, böylece dosyayı orijinal konumunda artık istemediğinizden emin olabilirsiniz. Dosyanın yokluğu sorun oluşturuyorsa, bu dosyayı analize gönderebilir veya orijinal konumuna geri yükleyebilirsiniz.

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

- **Ekleme Tarihi** - Şüpheli dosyanın tespit edildiği ve Virüs Kasası'na kaldırıldığı tarih ve saati gösterir.
- **Tehdit - AVG Internet Security** yazılımınıza [Software Analyzer](#) bileşenini yüklemeye karar vermeniz durumunda, bulgunun önem derecesini gösteren bir grafik tanımlama bu bölümde gösterilir: kusursuzdan (*üç yeşil nokta*) çok tehlikeliye (*üç kırmızı nokta*) kadar. Bulaşma türü ve orijinal konumu hakkında da bilgi bulabilirsiniz. *Daha fazla bilgi* bağlantısı sizi [çevrimiçi virüs ansiklopedisinde](#) tespit edilen tehdit hakkında ayrıntılı bilgiler sağlayan bir sayfaya yönlendirir.
- **Kaynak** - İlgili tehdidi hangi **AVG Internet Security** bileşeninin tespit ettiğini belirtir.
- **Bildirimler** - Çok nadiren, bu sütunda ilgili tehdit hakkında ayrıntılı açıklamalar sunan notlar gösterilebilir.

Kontrol düğmeleri

Virüs Kasası arayüzünden ulaşabileceğiniz kontrol düğmeleri şunlardır:

- **Geri Yükle** - bulaşmış dosyayı sabit diskinizdeki orijinal konumuna geri yükler.
- **Farklı geri yükle** - bulaşmış dosyayı seçilen klasöre taşır.
- **Analize gönder** - düğme yalnızca yukarıdaki tespitler listesindeki bir nesneyi vurguladığınızda etkin hale gelir. Böyle bir durumda, tespit edilen nesneyi ayrıntılı analiz için AVG virüs laboratuvarlarına gönderme seçeneğini kullanabilirsiniz. Lütfen, bu özelliğin öncelikli olarak hatalı tespitleri (yani AVG tarafından bulaşmış veya şüpheli olarak tespit edilen; ancak sizin zararsız olduğunu düşündüğünüz dosyaları) göndermek için kullanıldığını unutmayın.
- **Ayrıntılar** - **Virüs Kasası**'nda karantinaya alınan tehdit hakkında ayrıntılı bilgi için listede seçili öğeyi vurgulayın ve **Ayrıntılar** düğmesini tıklayarak tespit edilen tehdidin açıklamasını içeren yeni bir iletişim kutusu açın.
- **Sil** - bulaşmış dosyayı **Virüs Kasası**'ndan tamamen ve geri döndürülemez şekilde siler.
- **Kasayı Boşalt** - **Virüs Kasası** içeriğini tamamen temizler. Dosyaları **Virüs Kasası**'ndan kaldırdığınızda, bu dosyalar diskten geri alınmayacak biçimde kaldırılır (*Geri Dönüşüm Kutusu'na taşınmaz*).



12. Geçmiş

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

- [Tarama Sonuçları](#)
- [Yerleşik Kalkan Sonuçları](#)
- [E-posta Koruması Sonuçları](#)
- [Online Shield Sonuçları](#)
- [Olay Geçmişi](#)
- [Güvenlik Duvarı Günlüğü](#)

12.1. Tarama sonuçları




The screenshot shows the AVG Internet Security interface. The title bar reads "AVG Internet Security". The main window title is "Tarama sonuçları genel görünümü". Below the title bar is a table with the following columns: "Adı", "Başlangıç za...", "Bitiş zamanı", "Test edilen ne...", "Bulaşmalar", and "Yükse". The table contains two rows of scan results:


Adı	Başlangıç za...	Bitiş zamanı	Test edilen ne...	Bulaşmalar	Yükse
Anti-Rootkit tarama	11/7/2016, 1:11	11/7/2016, 1:11	32974	0	0
Tüm Bilgisayarı Tarama	11/7/2016, 1:11	11/7/2016, 1:11	5160	0	0

At the bottom of the window, there are two buttons: "Ayrıntıları göster" and "Sonucu sil". The version number "sürüm 16.131.7921" is visible in the bottom right corner.


Tarama sonuçları genel görünümü iletişim kutusuna **AVG Internet Security** ana penceresinin **üst satırındaki gezinme bölümünden Seçenekler / Geçmiş / Tarama sonuçları** menü öğesi yoluyla erişilebilir. İletişim kutusunda, daha önce başlatılan tüm taramalar ve sonuçları hakkında bilgi bulunmaktadır:

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

 - yeşil simge tarama sırasında herhangi bir bulaşmanın tespit edilemediğini gösterir.

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



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


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

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

- **Başlangıç zamanı** - taramanın başlatıldığı tarih ve saati gösterir
- **Bitiş zamanı** - taramanın bittiği tarih ve saati gösterir
- **Test edilen nesnelere** - tarama sırasında kontrol edilen nesne sayısıdır
- **Bulaşmalar** - tespit edilen / silinen virüs bulaşması sayısı
- **Yüksek / Orta** - bu sütunlar kaldırılan/bulunan toplam bulaşma sayısını sırasıyla yüksek ve orta önem seviyesine göre gösterir
- **Bilgi** - tarama işlemine ve sonucuna ilişkin bilgiler (*genellikle işlemin tamamlanmasının ya da kesilmesinin hemen ardından görüntülenir*)
- **Rootkit'ler** - tespit edilen [rootkit'lerin](#) sayısı

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 sonuçları genel görünümünden silmek için basın
-  - varsayılan [AVG ana iletişim kutusuna](#) (*bileşen genel görünümü*) dönmek için bu iletişim kutusunun sol üst kısmındaki oku kullanın



12.2. Yerleşik Kalkan Sonuçları

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



Bu uyarı iletişim kutusunda tespit edilen ve virüs bulaşmış olarak atanan nesne hakkında daha fazla bilgi (*Tehdit*) ve ilgili bulaşma hakkında bazı açıklamalar (*Açıklama*) bulabilirsiniz. *Daha fazla bilgi* bağlantısı sizi [çevrimiçi virüs ansiklopedisinde](#) tespit edilen tehdit hakkında ayrıntılı bilgiler sağlayan (bu tehditler biliniyorsa) bir sayfaya yönlendirir. İletişim kutusunda, tespit edilen tehdide yönelik olarak kullanabileceğiniz çözümler hakkında genel bilgiler de bulabilirsiniz. Alternatiflerden biri önerilen olarak etiketlenir: **Beni Korum (önerilir)**. **Yapabiliyorsanız, her zaman bu seçeneği kullanın!**

Not: *Tespit edilen nesnenin boyutunun Virüs Kasası'ndaki ücretsiz alan sınırını aşması olasıdır. Bu durumda, bulaşmış nesneyi Virüs Kasası'na taşımaya çalıştığınızda size bu sorun hakkında bilgi veren bir uyarı mesajı 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 Gelişmiş Ayarlar](#)'daki [Virüs Kasası](#) iletişim kutusuna gidin.*

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

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



Tespit edilen tüm nesnelere için aşağıdaki bilgiler verilir:

- **Tespit Adı** - tespit edilen nesnenin açıklaması (*muhtemelen adı da*) ve konumu. *Daha fazla bilgi* bağlantısı sizi [çevrimiçi virüs ansiklopedisinde](#) tespit edilen tehdit hakkında ayrıntılı bilgiler sağlayan bir sayfaya yönlendirir.
- **Durum** - tespit edilen nesne için yapılan 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 getirmek için gerçekleştirilen işlem

Kontrol düğmeleri

- **Yenile - Online Shield** $\tau\alpha\rho\alpha\phi\iota\nu\delta\alpha\nu$ tespit edilen bulgular listesini $\gamma\eta\chi\epsilon\lambda\lambda\epsilon\rho$
- **Dışa aktar** - tespit edilen tüm nesnelere bir dosyada dışa aktarın
- **Seçileni kaldır** - listeden seçilen kayıtları vurgulayabilir ve bu düğmeyi kullanarak yalnızca bu seçilen öğeleri silebilirsiniz
- **Tüm tehditleri kaldır** - iletişim kutusunda listelenen tüm kayıtları silmek için bu düğmeyi kullanın
- **←** - varsayılan [AVG ana iletişim kutusuna](#) (*bileşen genel görünümü*) dönmek için bu iletişim kutusunun sol üst kısmındaki oku kullanın



12.3. Identity Protection Sonuçları

Software Analyzer Sonuçları iletişim kutusuna **AVG Internet Security** ana penceresinin üst satırındaki gezinme bölümünden **Seçenekler / Geçmiş / Software Analyzer Sonuçları** menü öğesi yoluyla erişilebilir.



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

- **Tehdit Adı** - tespit edilen nesnenin açıklaması (*muhtemelen adı da*) ve konumu. *Daha fazla bilgi* bağlantısı sizi [çevrimiçi virüs ansiklopedisinde](#) tespit edilen tehdit hakkında ayrıntılı bilgiler sağlayan bir sayfaya yönlendirir.
- **Durum** - tespit edilen nesne için yapılan 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 getirmek için gerçekleştirilen işlem

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

Kontrol düğmeleri

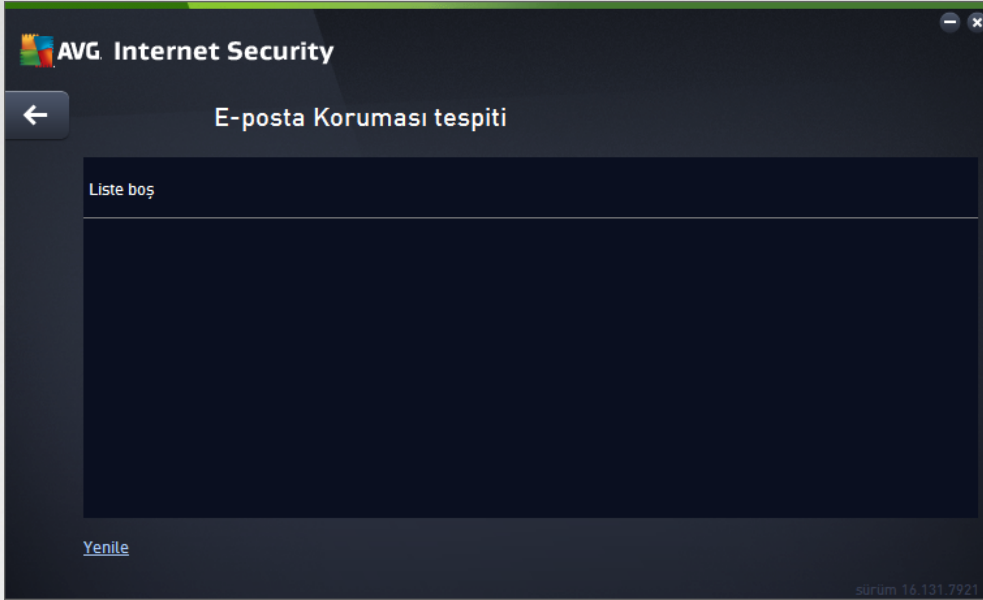
Software Analyzer Sonuçları arayüzünde bulunan kontrol düğmeleri şunlardır:

- **Listeyi yenile** - tespit edilen tehditlerin listesini günceller
- **←** - varsayılan [AVG ana iletişim kutusuna](#) (*bileşen genel görünümü*) dönmek için bu iletişim kutusunun sol üst kısmındaki oku kullanın



12.4. E-posta Koruması Sonuçları

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



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

- **Tespit adı** - tespit edilen nesnenin açıklaması (*muhtemelen adı da*) ve kaynağı
- **Sonuç** - tespit edilen nesne için yapılan işlem
- **Tespit zamanı** - Şüpheli nesnenin tespit tarih ve saat
- **Nesne Türü** - tespit edilen nesnenin türü
- **İşlem** - tespit edilmesi amacıyla potansiyel tehlike taşıyan nesneyi getirmek için gerçekleştirilen işlem

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

Kontrol düğmeleri

E-posta Tarayıcısı tespiti arayüzünde bulunan kontrol düğmeleri şunlardır:

- **Listeyi yenile** - tespit edilen tehditlerin listesini günceller
- **←** - varsayılan [AVG ana iletişim kutusuna](#) (*bileşen genel görünümü*) dönmek için bu iletişim kutusunun sol üst kısmındaki oku kullanın



12.5. 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.

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



Tespit edilen tüm nesnelere için aşağıdaki bilgiler verilir:

- **Tehdit Adı** - tespit edilen nesnenin açıklaması (*muhtemelen adı da*) ve kaynağı (*web sayfası*); *Daha fazla bilgi* bağlantısı sizi [çevrimiçi virüs ansiklopedisinde](#) tespit edilen tehdit hakkında ayrıntılı bilgiler sağlayan bir sayfaya yönlendirir.
- **Durum** - tespit edilen nesne için yapılan işlem
- **Tespit Zamanı** - tehdidin tespit edildiği ve engellendiği tarih ve saat
- **Nesne Türü** - tespit edilen nesnenin türü

Kontrol düğmeleri

- **Yenile** - **Online Shield** tarafından tespit edilen bulgular listesini yenile
- **Dışa aktar** - tespit edilen tüm nesnelere bir dosyada dışa aktarın
- - varsayılan [AVG ana iletişim kutusuna](#) (*bileşen genel görünümü*) dönmek için bu iletişim kutusunun sol üst kısmındaki oku kullanın



12.6. Olay Geçmişi

Olay tarihi ve saati	Kullanıcı	Kaynak	Olay tanımı
11/7/2016, 1:04:39 ...	NT AUTHORITY\SYSTEM	General	AVG başlatılıyor.
11/7/2016, 1:04:39 ...	NT AUTHORITY\SYSTEM	General	AVG çalışıyor.
11/7/2016, 1:04:54 ...	AUTOTEST-VST32\Ad...	Update	Güncelleme tamamlan...
11/7/2016, 1:04:55 ...	NT AUTHORITY\SYSTEM	Update	Güncelleme başlatıldı.
11/7/2016, 1:06:17 ...	NT AUTHORITY\SYSTEM	Update	Güncelleme tamamlan...
11/7/2016, 1:07:07 ...	NT AUTHORITY\SYSTEM	General	AVG durduruluyor.
11/7/2016, 1:07:07 ...	NT AUTHORITY\SYSTEM	General	AVG durduruldu.
11/7/2016, 1:08:15 ...	NT AUTHORITY\SYSTEM	General	AVG başlatılıyor.
11/7/2016, 1:08:16 ...	NT AUTHORITY\SYSTEM	General	AVG çalışıyor.
11/7/2016, 1:10:05 ...	NT AUTHORITY\SYSTEM	Update	Güncelleme başlatıldı.
11/7/2016, 1:10:34 ...	NT AUTHORITY\SYSTEM	Update	Güncelleme tamamlan...
11/7/2016, 1:11:08 ...	NT AUTHORITY\SYSTEM	Scan	Kullanıcı taraması baş...
11/7/2016, 1:11:15 ...	NT AUTHORITY\SYSTEM	Scan	Kullanıcı taraması dur...
11/7/2016, 1:11:17 ...	NT AUTHORITY\SYSTEM	Scan	Kullanıcı taraması baş...
11/7/2016, 1:11:35 ...	NT AUTHORITY\SYSTEM	Scan	Kullanıcı taraması dur...

Listeyi yenile

Kapat

Olay geçmişi iletişim kutusuna **AVG Internet Security** ana penceresinin üst satırındaki gezinme bölümünden **Seçenekler / Geçmiş / Olay Geçmişi** menü öğesi yoluyla erişilebilir. Bu iletişim penceresinde **AVG Internet Security** etkinliği sırasında oluşan önemli olaylara ilişkin kısa bir özet 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 Internet Security** ana penceresine dönmek için bu düğmeye basın

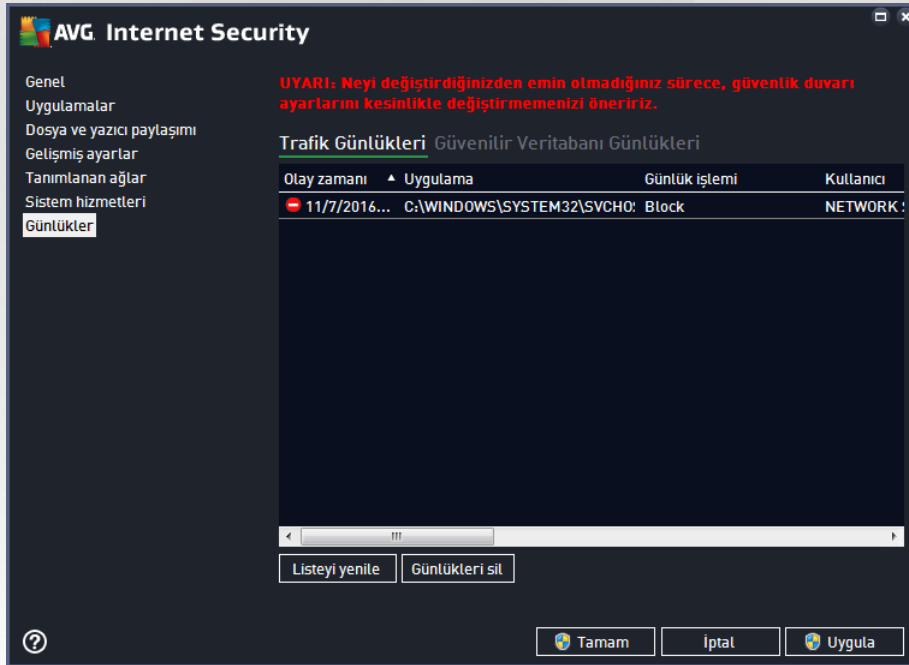


12.7. Güvenlik Duvarı günlüğü

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

Günlükler iletişim kutusu, kaydedilen tüm Güvenlik Duvarı eylemlerini ve etkinliklerini ilgili parametrelerin ayrıntılı tanımları ile birlikte iki sekmede görüntüleyebilmenizi sağlar:

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



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

Kontrol düğmeleri

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



13. 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 zararlı yazılımlar ve yeni bilgisayar saldırıları gerçekleştirilmektedir. Bu nedenle yazılım geliştiricileri, tespit edilen güvenlik açıklarını kapatmak üzere devamlı olarak güncellemeler ve güvenlik paketleri yayınlamaktadır. Yeni ortaya çıkan tehditler ve bunların yayılma hızı dikkate alındığında **AVG Internet Security** ürününüzü düzenli olarak güncellemek hayati bir öneme sahiptir. En iyi çözüm, otomatik güncellenmenin yapılandırıldığı program varsayılan ayarlarına güvenmektir. **AVG Internet Security** ürününüzün virüs veritabanı güncel değilse programın en yeni tehditleri tespit edemeyeceğini lütfen unutmayın!

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

Mümkün olan en yüksek güvenliği sağlamak için **AVG Internet Security** varsayılan olarak her dört saatte bir yeni virüs veritabanı güncellemelerini 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. AVG, güncellemeyi başlatmanızın ardından yeni güncelleme dosyaları olup olmadığını doğrular. Varsa, **AVG Internet Security** güncellemeleri indirmeye başlar ve güncelleme işlemini kendisi başlatır. Güncelleme sonuçları hakkında AVG sistem tepsisi simgesi üzerinde beliren iletişim kutusuyla bilgilendirilirsiniz.

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

- [Tanım güncelleme programı](#)
- [Anti-Spam güncelleme programı](#)



14. SSS ve Teknik Destek

AVG Internet Security 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 Internet Security** içindeki yardım dosyasından erişilebilen yeni bir **Sorun giderme** bölümü mevcuttur (*yardım dosyasını açmak için uygulamadaki herhangi bir pencerede 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 tıklatın.
- **AVG web sitesi destek merkezi:** Sorununuzun çözümünü AVG web sitesinde de (<http://www.avg.com/>) arayabilirsiniz. **Destek** bölümünde hem satış hem de teknik sorunlarla ilgilenen tematik gruplar hakkında genel bilgiler, sık sorulan soruların yapılandırıldığı bir bölüm ve erişilebilir iletişim bilgilerini bulabilirsiniz.
- **AVG ThreatLabs:** AVG ile ilişkili özel bir web sitesi (<http://www.avg.com/about-viruses>) 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:** <http://community.avg.com/> adresindeki AVG kullanıcıları tartışma forumunu da kullanabilirsiniz.