AVG Internet Security 2014

Kullanıcı Kılavuzu

Belge revizyonu 2014.22 (6/19/2014)

İçindekiler

1. Giriş

Bu kullanici el kitabi, **AVG Internet Security 2014** için kapsamli kullanici dokümantasyon saglar.

AVG Internet Security 2014 çevrimiçi yaptiginiz her sey için koruma katmanlari saglar. Bu, kimlik hirsizliklarindan, virüslerden ya da zararli siteleri ziyaret etmekten endise duymaniza gerek olmadigi anlamina gelir. AVG Koruyucu Bulut Teknolojisi ve AVG Topluluk Koruma Agi da dahil edilmistir; bu, en son tehdit bilgilerini topladigimiz ve en iyi korumayi aldiginizdan emin olmak için toplulugumuzla paylastigimiz anlamina gelmektedir. Gerçek zamanli korumayla alisveris ve bankacilik islemlerini güvenle yapabilir, sosyal paylasim aglarini rahatça kullanabilir ve internette güvenle gezinip arama yapabilirsiniz.

Diger bilgi kaynaklarini da kullanmak isteyebilirsiniz:

- ***Yardim dosyasi***: Dogrudan **AVG Internet Security 2014** *içindeki yardim dosyasindan erisilebilen bir Sorun giderme* bölümü mevcuttur (yardim dosyasini açmak için uygulamadaki herhangi bir iletisim kutusunda F1 tusuna basin). Bu bölüm, kullanici teknik bir sorun hakkinda profesyonel yardim aradiginda en sik karsilasilan durumlar hakkinda bir liste sunar. Lütfen sizin sorununuzu en iyi açiklayan durumu seçin ve sorunun çözümüne dair ayrintili talimatlar almak için tiklatin.

- ***AVG web sitesi Destek Merkezi***: Sorunuzun çözümünü AVG web sitesinde de (*http://www.avg.com/*) arayabilirsiniz. ***Destek Merkezi*** bölümünde hem satis sorunlari hem de teknik sorunlarla ilgili tematik olarak gruplandirilmis konular bulabilirsiniz.

- ***Sik sorulan sorular***: AVG web sitesinde (*http://www.avg.com/*) ayri ve çok ayrintili bir sik sorulan sorular bölümü de bulabilirsiniz. Bu bölüme ***Destek Merkezi / SSS'ler ve Egitimler*** menü seçeneginden erisilebilir. Burada da tüm sorular satis, teknik ve virüs kategorileri olarak organize bir sekilde siniflandirilmistir.

- ***AVG ThreatLabs***: AVG ile iliskili özel bir web sitesi (*http://www.avgthreatlabs.com/website-safety-reports/*) olarak virüs sorunlari baglaminda çevrimiçi tehditler hakkinda genel bilgiler vermek üzere hazirlanmistir. Virüs, casus yazilim silme talimatlari ve nasil güvenli kalacaginiza dair öneriler de bulabilirsiniz.

- ***Tartisma forumu***: Ayrica http://forums.avg.com adresindeki AVG kullanicilari tartisma forumunu kullanabilirsiniz.

2. AVG Yükleme Gereksinimleri

2.1. Desteklenen İşletim Sistemleri

AVG Internet Security 2014 asagidaki isletim sistemlerine sahip is istasyonlarini koruma amaçlidir:

- Windows XP Home Edition SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Vista (x86ve x64, tüm sürümleri)
- Windows 7 (x86 ve x64, tüm sürümler)
- Windows 8 (x32 ve x64)

(ve belirli isletim sistemleri için daha yeni hizmet paketleri)

***Not**: Kimlik bileseni Windows XP x64'te desteklenmez. Bu isletim sisteminde, AVG Internet Security 2014 yazilimini yalnizca IDP bileseni olmaksizin yükleyebilirsiniz.*

2.2. Minimum ve Önerilen Donanım Gereksinimleri

AVG Internet Security 2014 için minimum donanim gereksinimleri:

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

AVG Internet Security 2014 için önerilen donanim gereksinimleri:

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

3. AVG Yükleme Süreci

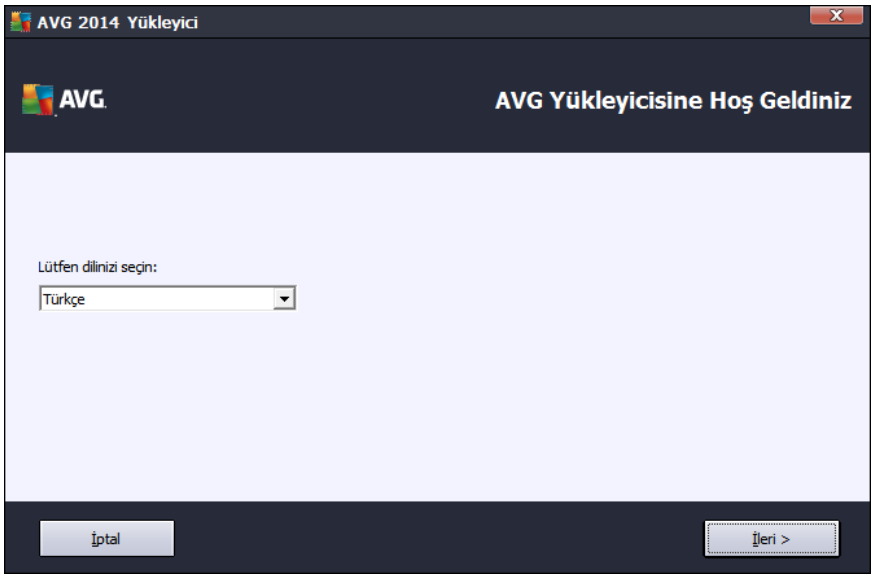
Bilgisayariniza **AVG Internet Security 2014** programini yüklemek için, en güncel yükleme dosyasini edinmeniz gerekir. **AVG Internet Security 2014** uygulamasinin dogru sürümünü yüklediginizden emin olabilmek için yükleme dosyasini AVG web sitesinden (http://www.avg.com/) indirmeniz önerilir. ***Destek Merkezi / Indirmeler*** bölümü her AVG sürümü için yükleme dosyalarina ayrintili bir genel bakis sunar.

Hangi dosyalari indirip yüklemeniz gerektiginden emin degilseniz, web sayfasinin altindaki ***Ürün seç*** hizmetini kullanmak isteyebilirsiniz. Hizmet, üç basit soruya verilen yanitlarin ardindan tam olarak ihtiyaciniz olan dosyalari tanimlar. Kisisel ihtiyaçlariniz için özellestirilmis, indirilebilir dosyalarin tam listesine yönlendirilmek için ***Devam*** dügmesine basin.

Yükleme dosyasini sabit diskinize indirme ve kaydetme islemini tamamladiktan sonra yükleme islemini baslatabilirsiniz. Yükleme, bir dizi kolay ve anlasilir iletisim kutusundan olusur. Her iletisim kutusunda yükleme sürecinin her adiminda ne yapilmasi gerektigi kisaca açiklanir. Her iletisim kutusunun ayrintili bir açiklamasi asagida sunulmustur:

3.1. Hoşgeldiniz: Dil Seçimi

Yükleme süreci ***AVG Yükleyiciye hos geldiniz*** iletisim kutusu ile baslar:

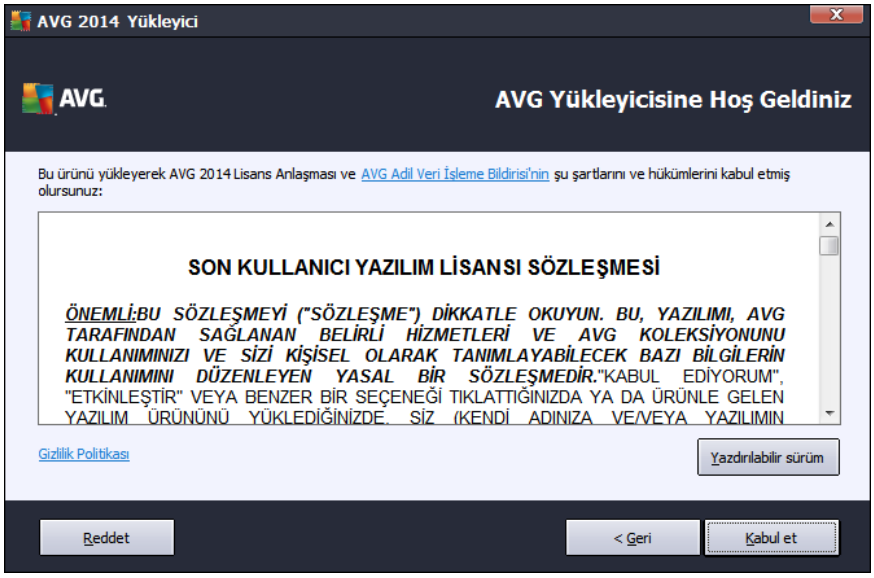


Bu iletisim kutusunda yükleme süreci için kullanilan dili seçebilirsiniz. Dil menüsünü açmak için açilir kutuyu tiklatin. Istediginiz dili seçtiginizde yükleme süreci bu dille devam eder.

Dikkat: Su anda yalnizca yükleme süreci dilini seçmektesiniz. AVG Internet Security 2014 uygulamasi seçilen dilde yüklenir ve Ingilizce her zaman otomatik olarak yüklenir. Ancak, daha fazla dil yüklemek ve AVG Internet Security 2014 uygulamasinda bu dillerden biriyle çalismak mümkündür. Özel Seçenekler adli kurulum iletisim kutularindan birinde alternatif dil seçimlerinizi onaylamaniz istenir.

3.2. Hoşgeldiniz: Lisans Sözleşmesi

AVG Kurulum'a hos geldiniz iletisim kutusu AVG lisans sözlesmesinin tam metnini içerir:



Lütfen tüm metni dikkatlice okuyun. Okudugunuzu, anladiginizi ve sözlesmeyi kabul ettiginizi onaylamak için, ***Kabul Et*** dügmesine basin. Lisans sözlesmesini kabul etmiyorsaniz ***Kabul Etmiyorum*** dügmesine basin, böylece yükleme süreci aninda iptal edilecektir.

AVG Adil Isleme Bildirimi Gizlilik Politikasi

Bu kurulum iletisim kutusu, lisans sözlesmesinin yani sira ***AVG Adil Isleme Bildirimi*** ve ***Gizlilik Politikasi*** hakkinda da daha fazla bilgi seçenegi sunar. Bahsedilen islevler iletisim kutusunda bir aktif baglanti seklinde gösterilir. Bu baglanti sizi ayrintili bilgi bulabileceginiz ilgili web sitesine götürür. Bu bildirimlerin tam metinin bulabileceginiz AVG web sitesine gitmek için (http://www.avg.com/) ilgili baglantiyi tiklatin.

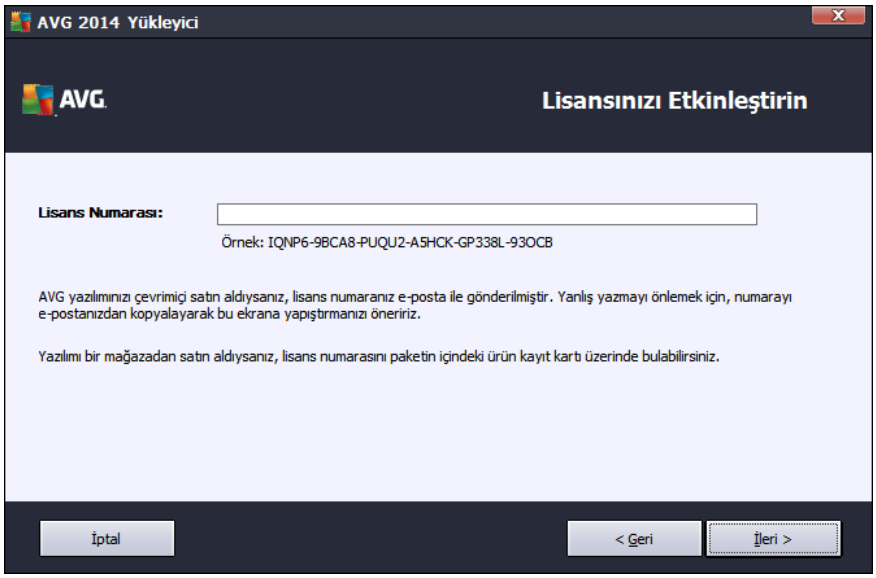
Kontrol dügmeleri

Ilk kurulum iletisim kutusunda yalnizca iki kontrol dügmesi bulunur:

- ***Yazdirilabilir sürüm*** - AVG lisans sözlesmesinin tam metninin yazdirmaya uygun biçimde düzenlendigi web arayüzünü görüntülemek için bu dügmeyi tiklatin.
- ***Reddet*** - Lisans sözlesmesini reddetmek için tiklatin. Kurulum süreci derhal sonlandirilir. **AVG Internet Security 2014** yüklenmez!
- ***Geri*** - Önceki kurulum iletisim kutusuna, bir adim geriye gitmek için tiklatin.
- ***Kabul Et*** - Lisans sözlesmesini okudugunuzu, anladiginizi ve kabul ettiginizi onaylamak için tiklatin. Yükleme devam eder ve bir sonraki kurulum iletisim kutusuna geçersiniz.

3.3. Lisansınızı etkinleştirme

Lisansinizi Etkinlestirin iletisim kutusunda, lisans numaranizi verilen metin alanina girmeniz istenir:



Lisans numarasi nereden bulunabilir

Satis numarasi, **AVG Internet Security 2014** kutusundaki CD paketinde bulunabilir. Lisans numarasi **AVG Internet Security 2014** programini çevrimiçi satin aldiktan sonra alacaginiz onay e-postasinda olacaktir. Sayilari gösterildigi gibi gitmelisiniz. Lisans numarasinin dijital formu mevcut ise (*e-postada*) girmek için kopyala ve yapistir yönteminin kullanilmasi önerilmektedir.

Kopyala ve Yapistir yöntemi nasil kullanilir

Kopyala ve Yapistir yöntemini kullanarak **AVG Internet Security 2014** lisans numarasini programa girmek, numaranin dogru biçimde girilmesini garanti altina alir. Lütfen su adimlari takip edin:

- Lisans numaranizin bulundugu e-postayi açin.
- Lisans numarasinin basinda sol fare dügmesine tiklatin, dügmeyi tutup numaranin sonuna kadar sürükleyin ve dügmeyi birakin. Numaranin vurgulanmasi gerekir.
- ***Ctrl*** tusunu basili tutun ve ***C*** tusuna basin. Bu islem numarayi kopyalar.
- Kopyalanan numarayi yapistirmak istediginiz konumu tiklatin.
- ***Ctrl*** tusunu basili tutun ve ***V*** tusuna basin. Bu islem numarayi seçilen konuma yapistirir.

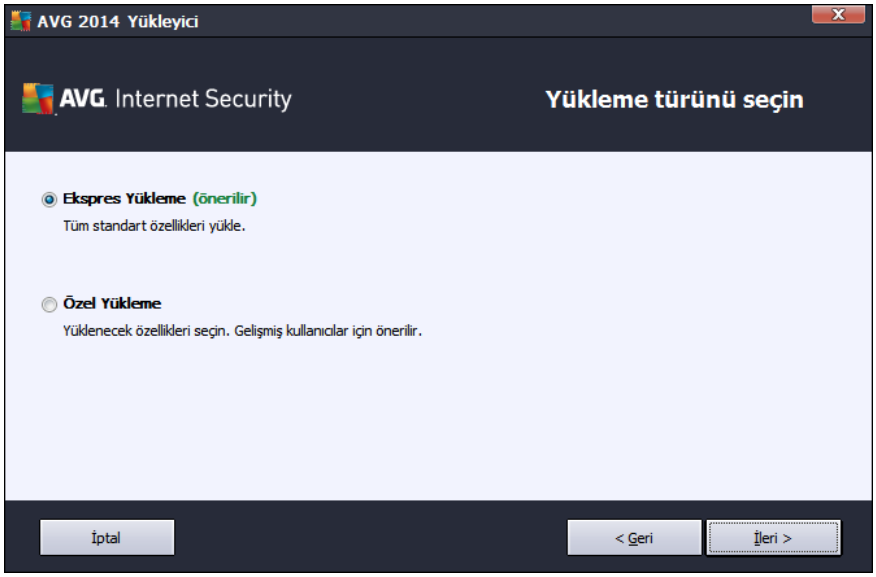
Kontrol dügmeleri

Çogu kurulum iletisim kutusunda oldugu gibi üç kontrol dügmesi mevcuttur:

- ***Iptal*** - kurulum isleminden hemen çikmak için tiklatin; **AVG Internet Security 2014** kurulmaz!
- ***Geri*** - önceki kurulum iletisim kutusuna, bir adim geriye gitmek için tiklatin.
- ***Ileri*** - kuruluma devam etmek ve bir adim ilerlemek için tiklatin.

3.4. Yükleme türünü seçin

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



Ekspres yükleme

Çogu kullanici için kesinlikle standart ***Ekspres*** yüklemenin muhafaza edilmesi önerilir. Bu yolla **AVG Internet Security 2014** programini AVG Security Toolbar da dahil olmak üzere program tedarikçisi tarafindan önceden tanimlanmis ayarlarla tam otomatik modda yüklersiniz. Bu yapilandirma, minimum kaynak kullanimi ile maksimum güvenligi bir araya getirir. Gelecekte söz konusu yapilandirmayi degistirme ihtiyaci duyarsaniz söz konusu islemi dogrudan **AVG Internet Security 2014** uygulamasindan yapabileceksiniz.

Yükleme isleminin sondaki iletisim kutusuna geçmek için ***Ileri*** dügmesine basin.

Özel yükleme

Özel Yükleme **AVG Internet Security 2014** uygulamasini standart olmayan ayarlarla kurmak için geçerli bir nedeni olan deneyimli kullanicilar tarafindan kullanilmalidir. Örn. belirli sistem gereksinimlerini karsilamak için. Bu seçenege karar verirseniz iletisim kutusunda birkaç yeni seçenek etkinlestirilir:

- ***Internet korumanizi gelistirmek için AVG Toolbar'i yükleyin*** - Varsayilan ayarlari degistirmezseniz, internette gezinirken size daha kapsamli çevrimiçi koruma saglamak için bu bilesen otomatik olarak varsayilan internet tarayiciniza yüklenir (*su anda desteklenen tarayicilar Microsoft Internet Explorer sürüm 6.0 ya da üstü ve Mozilla Firefox sürüm 3.0 ya da üstüdür*). Diger tarayicilar desteklenmez; Avant Browser gibi alternatif internet tarayicilari kullaniyorsaniz beklenmeyen davranislarla karsilasabilirsiniz.

- ***AVG Secure Search'ü varsayilan ana sayfaniz ve yeni sekme sayfaniz olarak ayarlayin ve koruyun*** - Varsayılan internet tarayıcınızı ve tarayıcının tüm sekmelerini ana sayfanız AVG Secure Search olarak ayarlanmış şekilde açmayı onaylamak için isaretli olarak birakin.

- ***AVG Secure Search'ü varsayilan arama saglayiciniz olarak ayarlayin ve koruyun*** - Çevrimiçi maksimum güvenlik için Link Scanner Sörf Kalkanı bileşeniyle sıkı bir işbirliği içinde çalışan AVG Secure Search motorunu kullanmak istediğinizi onaylamak için işaretli olarak bırakın.

- ***Hedef klasör*** - Burada, **AVG Internet Security 2014** uygulamasinin yüklenecegi konumu belirtmeniz beklenmektedir. **AVG Internet Security 2014**, varsayilan olarak iletisim kutusundaki metin alaninda belirtildigi gibi, C: sürücüsündeki program dosyalari klasörüne yüklenir. Bu konumu degistirmek istiyorsaniz, sürücü yapisini görüntülemek ve ilgili klasörü seçmek için ***Gözat*** dügmesini kullanin. Yazilim tedarikçisi tarafindan önceden ayarlanmis varsayilan hedefi geri getirmek için ***Varsayilan*** dügmesini kullanin.

Ardindan, ***Özel Seçenekler*** iletisim kutusuna gitmek için ileri dügmesine basin.

Kontrol dügmeleri

Çogu kurulum iletisim kutusunda oldugu gibi üç kontrol dügmesi mevcuttur:

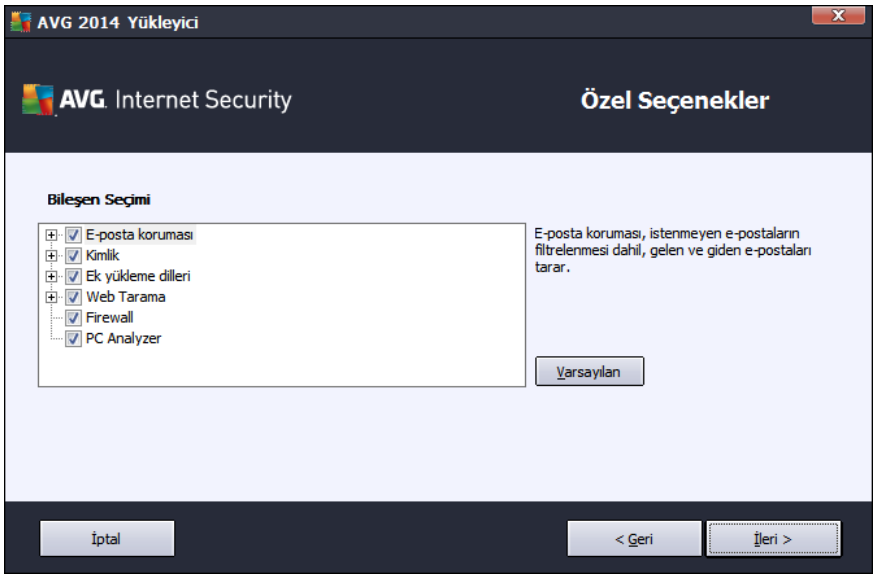
- ***Iptal*** - kurulum isleminden hemen çikmak için tiklatin; **AVG Internet Security 2014** kurulmaz!

- ***Geri*** - önceki kurulum iletisim kutusuna, bir adim geriye gitmek için tiklatin.

- ***Ileri*** - kuruluma devam etmek ve bir adim ilerlemek için tiklatin.

3.5. Özel seçenekler

Özel Seçenekler iletisim kutusu yükleme parametrelerinin ayrintili parametrelerini ayarlamaniza olanak verir:



Bilesen Seçimi bölümünde, yüklenebilecek tüm **AVG Internet Security 2014** bilesenleriyle ilgili genel bir görünüm bulunur. Varsayilan ayarlarin size uygun olmamasi halinde belirli bilesenleri kaldirabilir ya da ekleyebilirsiniz. ***Ancak, yalnizca satin aldiginiz AVG sürümü dahilinde bulunan bilesenler arasindan seçim yapabilirsiniz! Bilesen Seçimi*** listesindeki herhangi bir ögeyi vurgulayin, böylece ilgili bilesenin kisa açiklamasi bu bölümün sag tarafindan görüntülenir. Her bilesenin islevleri ile ilgili ayrintili bilgiler için, bu belgedeki Bilesen Genel Görünümü bölümüne bakin. Yazilim saticisi tarafindan önceden ayarlanmis varsayilan yapilandirmayi geri getirmek için, ***Varsayilan*** dügmesini kullanin.

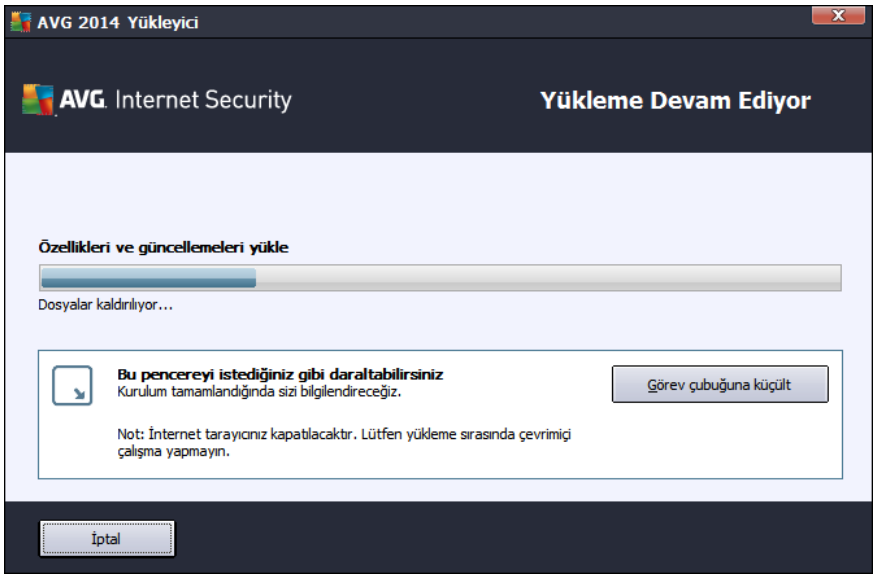
Kontrol dügmeleri

Çogu kurulum iletisim kutusunda oldugu gibi üç kontrol dügmesi mevcuttur:

- ***Iptal*** - kurulum isleminden hemen çikmak için tiklatin; **AVG Internet Security 2014** kurulmaz!
- ***Geri*** - önceki kurulum iletisim kutusuna, bir adim geriye gitmek için tiklatin.
- ***Ileri*** - kuruluma devam etmek ve bir adim ilerlemek için tiklatin.

3.6. Yükleme ilerlemesi

Yükleme Ilerlemesi iletisim kutusu yükleme sürecinin ilerleme durumu gösterir ve herhangi bir müdahale gerektirmez:



Yükleme islemi bittiginde, otomatik olarak bir sonraki iletisim kutusuna yönlendirilirsiniz.

Kontrol dügmeleri

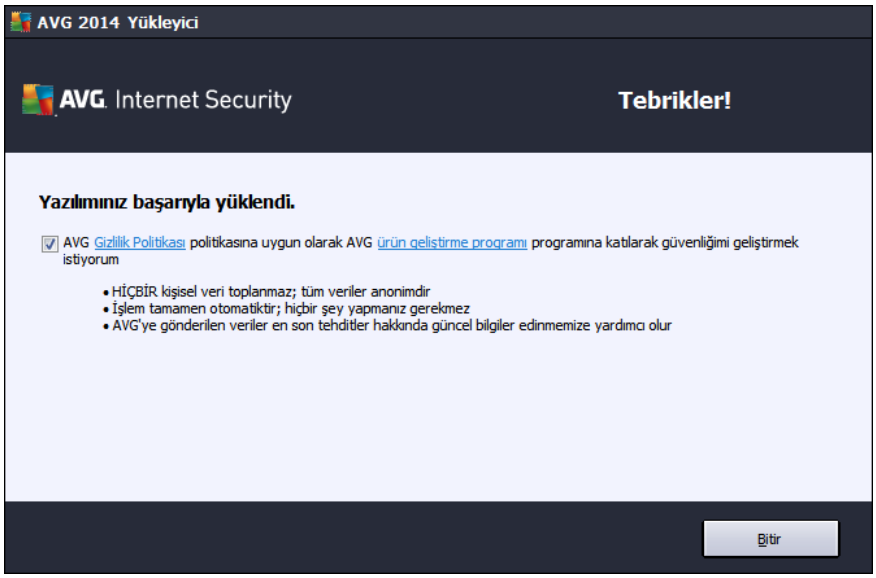
Bu iletisim kutusunda iki adet kontrol dügmesi bulunmaktadir:

- ***Minimize et*** - Yükleme islemi birkaç dakika alabilir. Bu dügmeyi tiklatarak iletisi penceresini sistem çubugunda görünen bir simge haline küçültebilirsiniz. Yükleme tamamlandiginda iletisim kutusu tekrar görüntülenir.

- ***Iptal*** - Yalnizca devam eden yükleme sürecini durdurmak istiyorsaniz bu dügmeyi kullanmalisiniz. Böyle bir durumda **AVG Internet Security 2014** uygulamasinin yüklenmeyecegini lütfen unutmayin!

3.7. Tebrikler!

Tebrikler iletisim kutusu, **AVG Internet Security 2014** yaziliminizin tam olarak yüklendigini ve yapilandirildigini onaylar:



Ürün Gelistirme Programi ve Gizlilik Politikasi

Burada, genel internet güvenligi seviyesini yükseltmek için anonim olarak bilgi toplayan ***Ürün Gelistirme Programi'na katilip katilmamayi seçebilirsiniz*** (*ayrintilar için AVG Gelismis Ayarlari / Ürün Gelistirme Programi* bölümüne bakabilirsiniz). Tüm veriler gizli olarak ve AVG Gizlilik Politikasi'na uygun olarak islenir; AVG Gizlilik Politikasi'nin tam metnini bulabileceginiz AVG web sitesine (http://www.avg.com/) gitmek için ***Gizlilik Politikasi*** baglantisini tiklatin. Kabul ediyorsaniz, lütfen seçenegi isaretli olarak birakin *(seçenek varsayilan olarak onaylidir)*.

Yükleme sürecini bitirmek için ***Bitir*** dügmesine basin.

4. Yüklemeden Sonra

4.1. Ürün kaydı

AVG Internet Security 2014 yüklemesini tamamladiktan sonra, lütfen ürününüzü çevrimiçi olarak AVG web sitesinde (*http://www.avg.com/*) kaydettirin. Kayit isleminin ardindan AVG kullanici hesabiniza erisebilecek, AVG Güncelleme bültenini alacak ve sadece kayitli kullanicilara sunulan diger hizmetlerden yararlanacaksiniz. Ürünü kaydettirmenin en kolay yolu dogrudan **AVG Internet Security 2014** kullanici arayüzünü kullanmaktir. Lütfen üstteki gezinme bölümünden / Seçenekler / Simdi kaydet ögesini seçin. AVG web sitesindeki (*http://www.avg.com/*) ***Kayit*** sayfasina yönlendirilirsiniz. Lütfen sayfadaki talimatlari izleyin.

4.2. Kullanıcı arayüzüne erişim

AVG ana iletisim kutusuna çesitli yöntemlerle ulasabilirsiniz:

- AVG sistem tepsisi sembolü'nü çift tiklatin
- Masaüstünüzdeki AVG simgesini çift tiklatin
- menüden ***Baslat / Tüm Programlar / AVG / AVG 2014***

4.3. Tüm bilgisayarın taranması

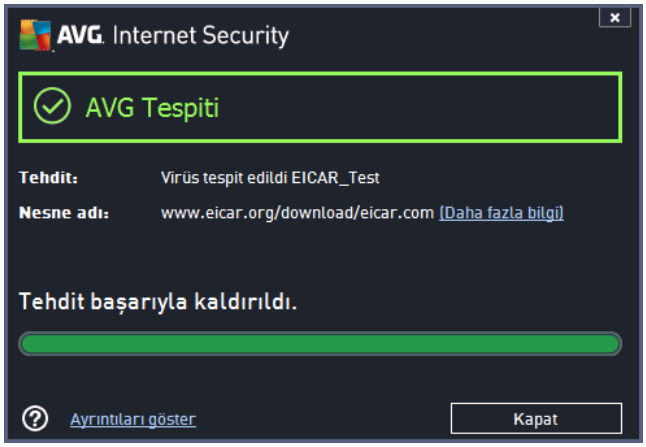
AVG Internet Security 2014 yüklemesinden önce bilgisayariniza virüs bulasmis olmasi ihtimali bulunmaktadir. Bu nedenle bilgisayarinizda virüs bulunmadigindan emin olmak için Tüm bilgisayar taramasi yapmaniz gerekmektedir. Ilk tarama uzun bir süre alabilir *(bir saat civarinda)*, ancak bilgisayarinizin herhangi bir tehdit altinda olmadigindan emin olmak için bu taramayi baslatmaniz önerilir. Tüm bilgisayar taramasi konusunda talimatlar için AVG Taramasi bölümünü inceleyin.

4.4. Eicar testi

AVG Internet Security 2014 programinin düzgün olarak yüklendigini onaylamak için EICAR testini çalistirabilirsiniz.

EICAR testi, virüslerden koruma sisteminin çalistigindan emin olmak üzere kullanilan standart ve kesinlikle güvenli bir yöntemdir. Gerçek bir virüs olmadigi için yayilmasinda sakinca yoktur ve herhangi bir virüs kodu içermemektedir. Ürünlerin çogu sanki bir virüsmüs gibi tepki verir (*ancak "EICAR-AV-Test" adi altinda rapor ederler*). EICAR virüsünü www.eicar.com adresinde bulunan EICA'in web sitesinden indirebilir ve bunun yani sira EICAR testi hakkinda tüm gerekli bilgileri edinebilirsiniz.

eicar.com dosyasini indirmeye çalisin ve sabit diskinize kaydedin. Siz test dosyasinin indirilmesini onaylar onaylamaz, **AVG Internet Security 2014** uygulamaniz uyarida bulunmaksizin buna yanit verir. Bu bildirim, AVG'nin bilgisayariniza dogru bir sekilde yüklenmis oldugunu gösterir.



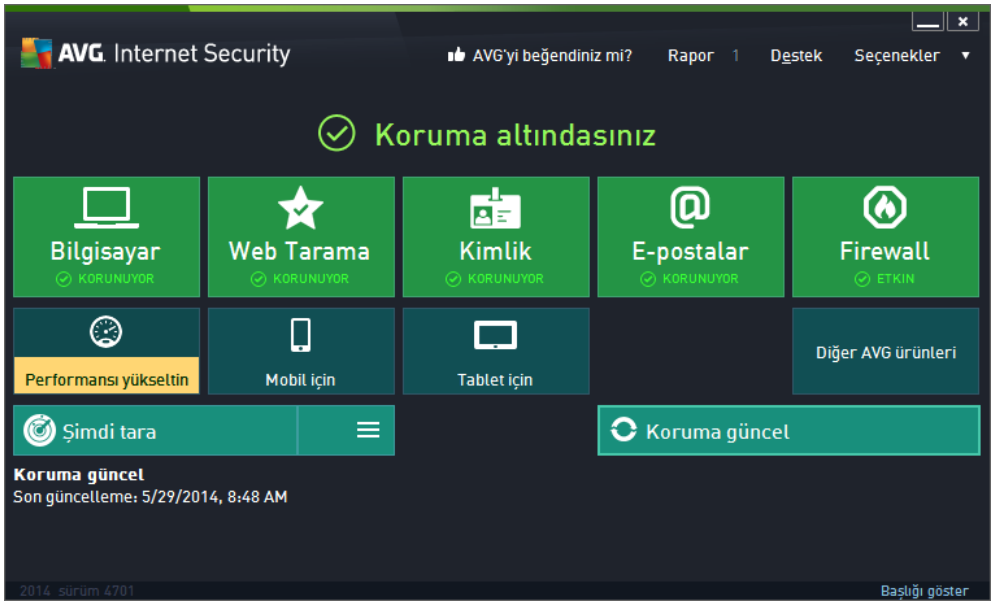
AVG'nin EICAR test dosyasini virüs olarak algilamamasi halinde program yapilandirmasini yeniden kontrol etmeniz gerekir!

4.5. AVG varsayılan yapılandırması

AVG Internet Security 2014 *varsayilan yapilandirmasi* (**yani, uygulamanin yüklemeden sonra dogru sekilde nasil ayarlanacagi**) yazilim saticisi tarafindan ayarlanabilir, böylece optimum performans elde etmek için tüm bilesenler ve islevler ayarlanabilir. ***Bunun için iyi bir nedeniniz olmadikça AVG yapilandirmasini degistirmeyin! Ayarlarda yapilacak her tür degisiklik sadece deneyimli bir kullanici tarafindan gerçeklestirilmelidir.*** Ihtiyaçlarinizi daha iyi karsilamasi açisindan AVG yapilandirmasini degistirme ihtiyaci hissederseniz AVG Gelismis Ayarlar'ina gidin: ana menü ögesi *Seçenekler/Gelismis ayarlar*'i seçin ve AVG yapilandirmasini yeni açilan AVG Gelismis Ayarlar iletisim kutusunda düzenleyin.

5. AVG Kullanıcı Arayüzü

AVG Internet Security 2014 ana pencerede açilir:



Ana pencere çok sayida bölüme ayrilir:

- ***Üst satir gezinme*** ana pencerenin üst bölümünde yan yana dizilen dört aktif baglantidan olusur *(AVG'yi begendiniz mi?, Raporlar, Destek, Seçenekler).* Ayrintilar >>
- ***Güvenlik Durumu Bilgisi*** **AVG Internet Security 2014** ürününüzün mevcut durumu hakkinda temel bilgileri saglar. Ayrintilar >>
- ***Yüklü bilesenlerin genel görünümü*** ana pencerenin orta bölümünde yatay bloklar halinde siralanir. Bilesenler ilgili bilesen simgesiyle etiketlenen açik yesil bloklar olarak görüntülenir ve bilesen durumu bilgileri belirtilir. Ayrintilar >>
- ***Uygulamalarim*** ana pencerenin alt orta bölümünde yer alir ve **AVG Internet Security 2014** ürününüzü tamamlayici nitelikteki bilgisayarinizda zaten yüklü olan veya yüklenmesi önerilen uygulamalar hakkinda genel bilgiler sunar. Ayrintilar >>
- ***Tara / Güncelle hizli baglantilari*** ana penceredeki bloklarin alt kismina yerlestirilmistir. Bu dügmeler en önemli ve en sik kullanilan AVG islevlerine aninda erisim saglar. Ayrintilar >>

AVG Internet Security 2014 ana penceresi disinda, uygulamaya erismek için kullanabileceginiz bir kontrol ögesi daha vardir:

- ***Sistem tepsisi simgesi*** monitörün sag alt kösesinde yer alir *(sistem tepsisinde)* ve **AVG Internet Security 2014** uygulamasinin mevcut durumunu gösterir. Ayrintilar >>

5.1. Üst Satır Gezinme

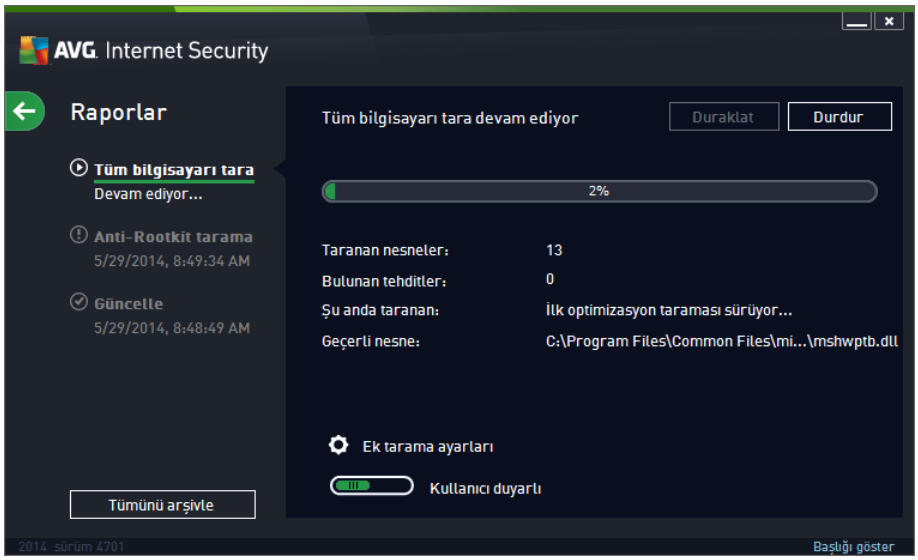
Üst satir gezinme ana menünün üst bölümünde yan yana dizilmis birkaç etkin baglantidan olusur. Gezinme bölümündeki dügmeler:

5.1.1. Facebook'ta bize katıl

Baglantiya tek sefer tiklatip AVG Facebook topluluguna baglanarak maksimum internet güvenliginiz için AVG ile ilgili en son bilgi, haber, ipucu ve kolay yollari paylasabilirsiniz.

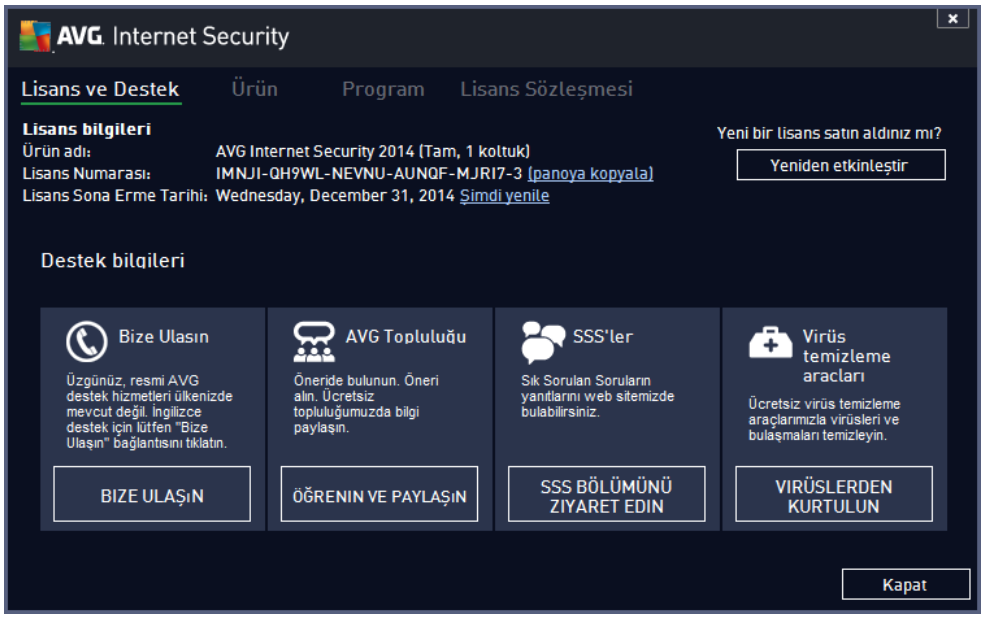
5.1.2. Raporlar

Önceden baslatilmis olan tüm taramalar ve güncelleme islemleri hakkinda genel bilgilerin yer aldigi yeni bir ***Raporlar*** iletisim kutusu açar. O anda tarama veya güncelleme çalisiyorsa, ana kullanici arayüzünün üst bölümündeki ***Raporlar*** ögesinin yaninda dönen bir daire simgesi gösterilir. Çalisan islemin ilerlemesini gösteren iletisim kutusuna gitmek için bu daireyi tiklatin:



5.1.3. Destek

AVG Internet Security 2014 uygulamasiyla ilgili tüm bilgileri bulabileceginiz dört sekmeye ayrilmis yeni bir iletisim kutusu açar:



- ***Lisans ve Destek*** - Bu sekme ürün adi, lisans numarasi ve son kullanma tarihi bilgilerini gösterir. Iletisim kutusunun alt bölümünde müsteri destek birimine ulasabileceginiz tüm iletisim bilgilerini bulabilirsiniz. Sekmede bulunan etkin baglantilar ve dügmeler:
    - *(Yeniden) Etkinlestir* - Yeni ***AVG Yazilim Etkinlestirme*** iletisim kutusunu açmak için tiklatin. Satis numaranizi *(AVG Internet Security 2014 yüklemesi sirasinda kullandiginiz)* degistirmek veya mevcut lisans numaranizi bir baskasiyla degistirmek *(örn. daha üst bir AVG ürününe yükseltme yaparken)* için ilgili alana lisans numaranizi girin.
    - *Panoya kopyala* - Lisans numarasini kopyalayip uygun alana yapistirmak için bu baglantiyi kullanin. Bu sayede lisans numarasinin dogru girildiginden emin olabilirsiniz.
    - *Simdi yenile* - **AVG Internet Security 2014** Lisans yenilemenizi uygun bir zamanda, mevcut lisansinizin süresi sona ermeden en az bir ay önce satin almanizi öneririz. Yaklasmakta olan son kullanma tarihi konusunda bilgilendirilirsiniz. Bu baglantiyi tiklatarak AVG web sitesine *(http://www.avg.com/)* giderek lisans durumunuz, son kullanma tarihi ve yenileme/yükseltme kampanyalari hakkinda ayrintili bilgi alabilirsiniz.
- ***Ürün*** - Bu sekme **AVG Internet Security 2014** ürün bilgileri, yüklü bilesenler, yüklü e-posta korumasi ve sistem bilgileri hakkinda en önemli teknik verileri gösterir.
- ***Program*** - Bu sekmede program dosyasi sürümü ve üründe kullanilan üçüncü taraflara ait kodlar hakkinda bilgi bulabilirsiniz.
- ***Lisans Sözlesmesi*** - Bu sekmede siz ve AVG Technologies arasindaki lisans

sözlesmesinin tam metni bulunur.

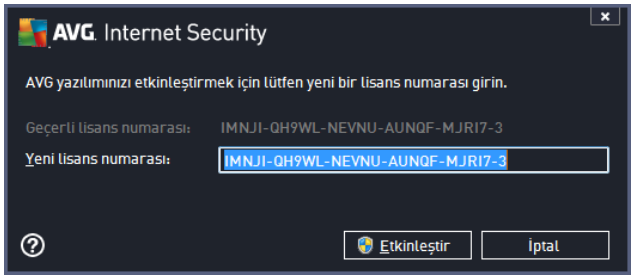
5.1.4. Seçenekler

AVG Internet Security 2014 ürününün bakim islemine ***Seçenekler*** ögesinden erisilebilir. Açilir menüyü açmak için oku tiklatin:

- ***Bilgisayari tara*** tüm bilgisayar taramasi baslatir.
- ***Seçilen klasörü tara...*** - AVG tarama arayüzüne geçer ve bilgisayarinizin dolasim agacindan taranmasini istediginiz dosya ve klasörleri seçmenizi saglar.
- ***Dosyayi tara...*** - Belirli tek bir dosya üzerinde talebe göre test yapmanizi saglar. Diskinizin agaç yapisini içeren yeni bir pencere açmak için bu seçenegi tiklatin. Istediginiz dosyayi seçin ve tarama baslatmayi onaylayin.
- ***Güncelle*** - **AVG Internet Security 2014** güncellemesini otomatik olarak baslatir.
- ***Dizinden güncelle...*** - Sabit diskinizde bulunan belirli bir dosyanin içinde yer alan güncelleme dosyalarini alarak güncelleme islemini gerçeklestirir. Öte yandan bu seçim sadece internet baglantisinin olmamasi gibi (örnegin bilgisayariniza virüs bulasmis ise ve internet baglantiniz kesildiyse; bilgisayariniz bir aga bagliysa fakat internet erisimi yok ise vb.) acil durumlarda önerilmektedir. Yeni açilan pencereden, daha önce güncelleme dosyasini depoladiginiz klasörü seçin ve güncelleme islemini baslatin.
- ***Virüs Kasasi*** - Belirli bir neden dogrultusunda AVG'nin tespit edilmis temizlenemeyen tüm bulasmalari tasidigi karantina alaninin arayüzü olan Virüs Kasasi'ni açar. Karantina altinda bulunan bulasmis dosyalar, yalitilmistir, bilgisayarinizin güvenligi garanti altindadir ve ayni anda bulasmis dosyalar ileride tamir edilebilecekleri göz önünde bulundurularak depolanir.
- ***Geçmis*** - Bazi alt menü seçenekleri sunar:
  - *Tarama sonuçlari* - Tarama sonuçlari hakkinda genel bilgilerin bulundugu bir iletisim kutusu açar.
  - *Yerlesik Kalkan tespiti* - Yerlesik Kalkan tarafindan tespit edilen tehditler hakkinda genel bilgi veren bir iletisim kutusu açar.
  - Identity Protection tespiti - *Kimlik* bileseni tarafindan tespit edilen tehditler hakkinda genel bilgi veren bir iletisim kutusu açar.
  - *E-posta Korumasi tespiti* - E-posta Korumasi bileseni tarafindan tehlikeli oldugu tespit edilen posta eklentileri hakkinda genel bilgi veren bir pencere açar.
  - *Online Shield tespitleri* - Online Shield
  - *Olay geçmisi günlügü* - Kaydedilen tüm **AVG Internet Security 2014** islemleri hakkinda genel bilgi veren bir geçmis günlügü arayüzü açar.
  - *Firewall günlügü* - Tüm Firewall islemlerinin ayrintili bilgilerinin bulundugu bir iletisim kutusu açar.
- ***Gelismis ayarlar...*** - **AVG Internet Security 2014** yapilandirmasini düzenleyebileceginiz

AVG gelismis ayarlar iletisim kutusunu açar. Genel olarak uygulamanin yazilim üreticisi tarafindan tanimlanan varsayilan ayarlarinin muhafaza edilmesi önerilir.

- ***Firewall ayarlari...*** - Firewall bileseninin gelismis yapilandirmasina iliskin bagimsiz bir pencere açar.
- ***Yardim içerikleri*** - AVG yardim dosyalarini açar.
- ***Destek alin*** - Müsteri destek merkezi sayfasinda AVG web sitesini (*http://www.avg.com/*) açar.
- ***AVG Web*** - AVG web sitesini açar (*http://www.avg.com/*).
- ***Virüsler ve Tehlikeler Hakkinda*** - Belirtilen virüs hakkinda ayrintili bilgi edinebildiginiz AVG web sitesindeki (*http://www.avg.com/*) çevrimiçi virüs ansiklopedisini açar.
- ***(Yeniden) Etkinlestir*** - Yükleme islemi sirasinda girdiginiz lisans numarasinin bulundugu etkinlestirme iletisim kutusunu açar. Bu iletisim kutusunda satis numarasini (*AVG'yi yüklerken kullandiginiz numara*) ya da eski lisans numarasini (*örn. yeni bir AVG ürününe yükseltme yaparken*) degistirmek için lisans numaranizi düzenleyebilirsiniz. **AVG Internet Security 2014** deneme sürümünü kullaniyorsaniz sonraki iki öge, ***Simdi satin al*** ve ***Etkinlestir*** olarak görünür ve programin tam sürümünü hemen satin almanizi saglar. Bir satis numarasiyla yüklenmis **AVG Internet Security 2014** için ögeler ***Kaydet*** ve ***Etkinlestir*** olarak görünür:



- ***Simdi kaydet / MyAccount*** - AVG web sitesinin (*http://www.avg.com/*) kayit sayfasina baglanti saglar. Lütfen kayit bilgilerinizi doldurun; sadece AVG ürünlerini kaydettiren müsterilerimiz ücretsiz teknik destek alabilir.
- ***AVG hakkinda*** - Satin aldiginiz lisans ve erisilebilir destek, ürün ve program bilgilerine yönelik dört sekme ile lisans sözlesmesinin tam metninin bulundugu yeni bir iletisim kutusu açar. *(Ayni iletisim kutusu ana gezinme menüsündeki Destek baglantisi yoluyla açilabilir.)*

5.2. Güvenlik Durumu Bilgisi

Güvenlik Durumu Bilgisi bölümü **AVG Internet Security 2014** ana penceresinin üst kisminda yer alir. Bu bölümde **AVG Internet Security 2014** programinizin mevcut güvenlik durumu hakkinda her zaman bilgi bulabilirsiniz. Lütfen bu bölümde betimlenmesi muhtemel simgeleri ve anlamlarini inceleyin:

- yesil simge ***AVG Internet Security 2014 uygulamasinin tamamen islevsel oldugunu belirtir***. Bilgisayariniz tamamen korunur, günceldir ve yüklü tüm bilesenler dogru çalismaktadir.

 - sari simge, ***bir ya da birden fazla bilesenin yanlis yapilandirildigini*** ve söz konusu bilesenlerin özelliklerini/ayarlarini kontrol etmeniz gerektigini gösterir. **AVG Internet Security 2014** uygulamasinda herhangi bir kritik sorun yoktur ve muhtemelen bazi nedenlerden dolayi bilesenlerden bazilarini geçici olarak kapatmayi seçmis olabilirsiniz. Hala korunuyorsunuz!. Diger bir yandan lütfen bilesenin ayarlarini inceleyin! Yanlis yapilandirilmis bilesen ana kullanici arayüzünde turuncu renkli bir uyari bandiyla gösterilir.

Sari simge, bir bilesenin hata durumunu herhangi bir nedenle yok saydiginizda da görünür. ***Hata durumunu yoksay*** seçenegine Gelismis ayarlar / Hata durumunu yoksay yoluyla erisilebilir. Burada bilesenin hata durumunun farkinda oldugunuz, ancak belirli bir neden dogrultusunda **AVG Internet Security 2014** uygulamasinin bu sekilde çalismasini ve bu konuda uyarilmak istemediginizi belirtme seçeneginiz vardir. Özel durumlar için bu seçenegi kullanmaniz gerekebilir ancak en kisa zamanda ***Hata durumunu yoksay*** seçenegini devre disi birakmaniz önerilir!

Ya da, sari simge **AVG Internet Security 2014** ürününüz bilgisayar yeniden baslatmasi gerektirdiginde de görüntülenir (***Yeniden baslatma gerekiyor***). Lütfen bu uyariyi dikkate alin ve bilgisayarinizi yeniden baslatin.

 - turuncu simge ***AVG Internet Security 2014 uygulamasinin kritik durumda oldugunu belirtir***! Bir veya daha fazla bilesen düzgün çalismiyor ve **AVG Internet Security 2014** uygulamasi bilgisayarinizi koruyamiyordur. Lütfen rapor edilen sorunu çözmek için gerekli ilgiyi gösterin! Hatayi kendi basiniza çözemiyorsaniz AVG teknik destek ekibi ile iletisim kurun.

AVG Internet Security 2014 uygulamasinin en verimli performansi ayarlayamamasi durumunda, Düzeltmek için tiklatin adli yeni bir dügme (alternatif olarak, sorun birden fazla bilesenle ilgiliyse, Tümünü düzeltmek için tiklatin dügmesi) görüntülenir. Dügmeye basarak programi otomatik olarak kontrol etme ve yapilandirma islemini baslatin. Bu özellik, AVG Internet Security 2014 uygulamasini en verimli performansa ayarlamanin ve maksimum güvenlik düzeyine ulasmanin kolay bir yoludur!

Güvenlik Durumu Bilgisi fonksiyonuna gereken özeni göstermeniz ve herhangi bir sorunun rapor edilmesi halinde aninda sorunu çözmeye çalismaniz önerilmektedir. Aksi takdirde bilgisayariniz risk altinda olacaktir!

Not: *AVG Internet Security 2014 durum bilgilerine istediginiz zaman sistem tepsisi simgesinden de ulasabilirsiniz.*

5.3. Bileşen Genel Görünümü

Yüklü bilesenlerin genel görünümü ana pencerenin orta bölümünde yatay bloklar halinde siralanir. Bilesenler ilgili bilesen simgesiyle etiketlenmis açik yesil bloklar olarak gösterilir. Her blok korumanin mevcut durumu hakkinda bilgiler saglar. Bilesen dogru yapilandirilmis ve tam olarak çalisiyorsa, bilgiler yesil renkli harflerle gösterilir. Bilesen durdurulursa, islevi sinirli hale gelirse veya bilesen hata durumundaysa, turuncu renkli bir metin alaninda gösterilen bir uyari metniyle bilgilendirilirsiniz. ***Ilgili bilesen ayarlarina kesinlikle dikkat etmeniz tavsiye edilir!***

Fareyi bilesenin üzerine getirerek ana pencerenin altinda kisa bir metin görüntüleyebilirsiniz. Metinde bilesenin islevselligine dair temel giris bilgileri bulunur. Ayrica, bilesenin mevcut durumu hakkinda bilgi sunar ve hangi bilesen hizmetlerinin dogru yapilandirilmadigini belirtir.

Yüklü bilesen listesi

AVG Internet Security 2014 içinde, ***Bilesen Genel Görünümü*** kismi asagidaki bilesenler hakkinda bilgiler içerir:

- ***Bilgisayar*** - Bu bilesen iki hizmeti kapsar: ***AntiVirus Shield*** sisteminizdeki virüs, casus yazilim, solucan, truva ati, istenmeyen çalistirilabilir dosyalar veya kitapliklari tespit eder sizi zararli reklam yazilimlarina karsi korur; ***Anti-Rootkit*** ise uygulama, sürücü veya kitapliklarda gizlenen tehlikeli kök dizinler için tarama yapar. Ayrintilar >>
- ***Web Tarama*** - Internette arama ve gezinme sirasinda sizi web tabanli saldirilara karsi korur. Ayrintilar >>
- ***Identity*** - Bilesen internette dijital varliklarinizi yeni ve bilinmeyen tehditlere karsi sürekli olarak koruyan ***Identity Shield*** hizmetini çalistirir. Ayrintilar >>
- ***E-postalar*** - Gelen e-posta mesajlarinizi istenmeyen e-postalara karsi denetler ve virüsleri, kimlik avi saldirilarini veya diger tehditleri engeller. Ayrintilar >>
- ***Firewall*** - Her ag baglanti noktasindaki tüm iletisimleri denetleyerek sizi kötü amaçli saldirilardan korur ve tüm sizma girisimlerini engeller. Ayrintilar >>

Erisilebilir eylemler

- ***Bilesen genel görünümü ekraninda bileseni seçmek için fareyi ilgili bilesen simgesi üzerinde hareket ettirin***. Ayni anda kullanici arayüzünün kisminda bilesenin temel fonksiyonlari hakkinda açiklamalar görüntülenir.
- ***Bilesen simgesini tek tiklatarak*** bilesenin mevcut durumu hakkinda bilgiler içeren arayüzünü açin ve bilesenin yapilandirma ve istatistik verilerine erisin.

5.4. Uygulamalarım

Uygulamalarim alaninda *(bilesenler grubunun altindaki yesil bloklar satiri)* bilgisayarinizda zaten yüklü olan veya yüklenmesi önerilen ilave AVG uygulamalari hakkinda genel bilgiler bulabilirsiniz. Bloklar kosullu olarak görüntülenir ve asagidaki uygulamalardan herhangi birini temsil edebilir:

- ***Mobil koruma*** cep telefonunuzu virüs ve zararli yazilimlardan koruyan bir uygulamadir. Uygulama, ayri kalmaniz durumunda akilli telefonunuzu uzaktan izleme imkani da saglar.
- ***LiveKive*** güvenlikli sunuculara çevrimiçi veri yedeklemesi yapmak için hazirlanmistir. LiveKive tüm dosyalarinizi, fotograflarinizi ve müzik dosyalarinizi güvenli bir yerde yedekleyerek bunlari ailenizle ve arkadaslarinizla paylasmaniza ve iPhone ve Android cihazlari da dahil olmak üzere söz konusu dosyalara web etkinligi olan tüm cihazlardan erismenize olanak saglar.
- ***Family Safety*** çocuklarinizin uygunsuz web sitelerine, medya içeriklerine ve çevrimiçi aramalara karsi korunmasina yardimci olur ve çevrimiçi faaliyetleriyle ilgili size rapor saglar. AVG Family Safety çocuklarinizin sohbet odalari ve sosyal paylasim sitelerindeki etkinliklerini izlemek için tus vurusu teknolojisi kullanir. Çocuklarin istismarinda kullanildigi

bilinen kelimeler, ifadeler ve cümleler algilarsa, SMS veya e-posta yoluyla sizi aninda bilgilendirir. Uygulama araciligiyla çocuklarinizdan her biri için uygun koruma düzeyi ayarlayabilir ve benzersiz girisler araciligiyla onlari ayri ayri gözlemleyebilirsiniz.

- ***PC Tuneup*** uygulamasi bilgisayarinizin hizinin ve genel performansinin nasil iyilestirilebilecegine yönelik ayrintili sistem analizi ve düzeltme islemi için gelismis bir araçtir.

- ***MultiMi*** tüm e-posta ve sosyal hesaplarinizi tek bir güvenli alanda birlestirerek aile ve arkadaslarinizla iletisim kurmayi, internette gezinmeyi, fotograf, video ve dosya paylasmayi çok daha kolay hale getirir. MultiMi, görüntülediginiz web sayfalarindaki baglantilarin ardindaki web sayfalarini analiz edip bunlarin güvenli oldugundan emin olarak sizi sayilari sürekli olarak artan tehditlerden koruyan LinkScanner hizmetini de barindirir.

- ***AVG Toolbar***'na dogrudan internet tarayicinizdan erisebilirsiniz; bu uygulama internette gezinirken size maksimum koruma saglar.

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

5.5. Tara / Hızlı Bağlantıları Güncelle

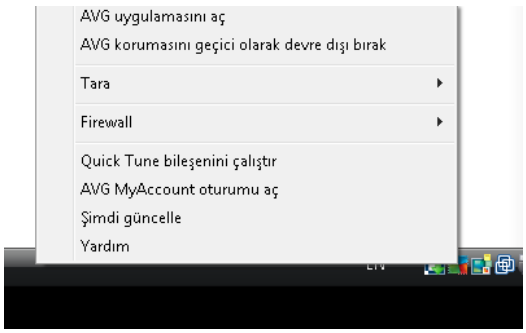
Hizli baglantilar **AVG Internet Security 2014** kullanici arayüzünün alt bölümündeki dügmelerde yer alir. Bu baglantilar tarama ve güncelleme gibi en önemli ve en sik kullanilan uygulama özelliklerine aninda erisebilmenizi saglar. Hizli baglantilara kullanici arayüzündeki tüm iletisim kutularindan erisilebilir:

- ***Simdi tara*** - Dügme grafik olarak iki kisma ayrilmistir. ***Simdi tara*** baglantisini izleyerek Tüm Bilgisayari Tara islemini hemen baslatabilir ve ilerleme ile sonuçlari otomatik olarak açilan Raporlar penceresinden izleyebilirsiniz. ***Seçenekler*** dügmesi ***Tarama Seçenekleri*** iletisim kutusunu açar; burada zamanlanmis taramalari yönetebilir ve Tüm Bilgisayari Tara / Belirli Dosyalari veya Klasörleri Tara parametrelerini düzenleyebilirsiniz. *(Ayrintilar için AVG Tarama bölümüne bakin)*

- ***Simdi güncelle*** - Ürün güncellemesini hemen baslatmak için dügmeye basin. Güncelleme sonuçlari hakkinda AVG sistem tepsisi simgesi üzerinde beliren iletisim kutusuyla bilgilendirilirsiniz. *(Ayrintilar için AVG Güncellemeleri bölümüne bakin)*

5.6. Sistem Tepsisi Simgesi

AVG Sistem Tepsisi Simgesi *(Windows görev çubugunuzda, ekraninizin sol alt kösesinde)* **AVG Internet Security 2014** uygulamanizin mevcut durumunu gösterir. **AVG Internet Security 2014** kullanici arayüzü ana penceresinin açik ya da kapali oldugu önemli olmaksizin devamli olarak sistem tepsinizde bulunur:



AVG Sistem Tepsisi Simgesi görünümü

- Tam renkli ve baska öge bulunmayan simge tüm **AVG Internet Security 2014** bilesenlerinin etkin ve tamamen çalisir durumda oldugunu gösterir. Ancak, simge bilesenlerden biri tam çalisir durumda olmasa da (kullanici bilesen durumunu yoksaymaya karar verdiginde) bu sekilde görünebilir. *(Bilesenin durumunu yoksayma seçenegini onaylayarak, bilesenin hata durumunun farkinda oldugunuzu, ancak kimi nedenlerle durumun böyle kalmasini ve durum hakkinda uyari almak istemediginizi ifade edersiniz.)*

- Üzerinde ünlem isareti bulunan simge bir bilesenin *(veya daha fazla bilesenin)* hata durumunda oldugunu gösterir. Bu tip uyarilara mutlaka dikkat edin ve düzgün ayarlanmamis bilesenin yapilandirma sorununu gidermeye çalisin. Bilesen yapilandirmasi degisikliklerini gerçeklestirebilmek için sistem tepsisi simgesini çift tiklatarak uygulamanin kullanici arayüzünü açin. Hangi bilesenin hata durumunda olduguyla ilgili ayrintili bilgi için lütfen güvenlik durumu bilgisi bölümüne bakin.

- Sistem tepsisi tam renkli olarak yanip sönen ve dönen bir isikla da görünebilir. Bu grafik gösterim o anda baslatilan bir güncelleme islemini isaret eder.

- Tam renkli ve ok isaretli simge ise **AVG Internet Security 2014** taramalarindan birinin o anda çalismakta oldugunu gösterir.

AVG Sistem Tepsisi Simgesi bilgileri

AVG Sistem Tepsisi Simgesi sizi sistem tepsisi simgesi hizasindan açilan bir pencere araciligiyla **AVG Internet Security 2014** uygulamanizda o an gerçeklesen islemler ve programdaki olasi durum degisiklikleri hakkinda da bilgilendirir (*örn. programlanan tarama ya da güncellemenin otomatik olarak baslatilmasi, Firewall profil degisikligi, bir bilesenin durum degisikligi, hata durumu olusumu, ...*).

AVG Sistem Tepsisi Simgesi yoluyla erisilebilen islemler

AVG Sistem Tepsisi Simgesi, **AVG Internet Security 2014** kullanici arayüzüne erismek için bir hizli baglanti olarak da kullanilabilir; bunun için simgeyi çift tiklatmak yeterlidir. Simgeyi sag tiklatarak asagidaki seçenekleri sunan kisa bir baglam menüsü açarsiniz:

- ***AVG'yi Aç*** - **AVG Internet Security 2014** kullanici arayüzünü açmak için tiklatin.

- ***AVG korumasini geçici olarak devre disi birak*** - bu seçenek **AVG Internet Security 2014** tarafindan saglanan tüm korumayi tek seferde kapatmanizi saglar. Mutlaka gerekli degilse, bu seçenegi kullanmamaniz gerektigini lütfen unutmayin! Çogu durumda, yeni yazilimi veya sürücüleri yüklemeden önce ve hatta yükleyici veya yazilim sihirbazi yükleme islemi sirasinda istenmeyen kesintilerin olmamasini saglamak için çalisan program ve uygulamalarin kapatilmasini önerse bile **AVG Internet Security 2014** uygulamasini devre disi birakmak gerekmez. **AVG Internet Security 2014** uygulamasini geçici olarak devre disi birakmaniz gerekirse, isinizi bitirdikten sonra yeniden etkinlestirmeniz gerekir. Virüslerden korunma yaziliminiz devre disi birakilmisken Internete veya bir aga baglanirsaniz, bilgisayariniz saldirilara açik durumda olur.

- ***Tarama*** - önceden tanimlanan taramalar (*Tüm Bilgisayari Tara* ve *Belirli Dosyalari veya Klasörleri Tara*) baglam menüsünü açmak ve gerekli taramayi seçmek için tiklatin; tarama hemen baslatilacaktir.

- ***Çalisan taramalar ...*** - bu öge yalnizca bilgisayarinizda o anda çalisan bir tarama olmasi durumunda görüntülenir. Bunun ardindan, bu tarama için taramanin önceligini ayarlayabilir, alternatif olarak çalisan taramayi durdurabilir veya duraklatabilirsiniz. Su islemlere de erisilebilir: *Tüm taramalar için önceligi ayarla, Tüm taramalari duraklat* veya *Tüm taramalari durdur*.

- ***Quick Tune bilesenini çalistir*** - Quick Tune bilesenini baslatmak için tiklatin.

- ***AVG MyAccount oturumu aç*** - Abonelik ürünlerinizi yönetebileceginiz, ilave koruma satin alabileceginiz, yükleme dosyalarini indirebileceginiz, geçmis siparis ve faturalarinizi kontrol edebileceginiz ve kisisel bilgilerinizi yönetebileceginiz MyAccount ana sayfasini açar.

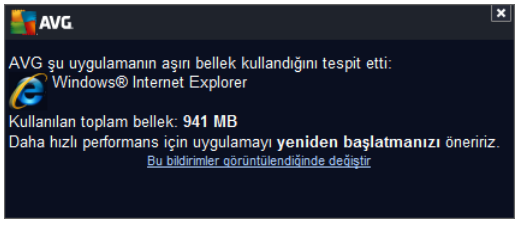
- ***Simdi Güncelle*** - aninda güncelleme islemini baslatir.

- ***Yardim*** - baslangiç sayfasinda yardim dosyasini açar.

5.7. AVG Tavsiyesi

AVG Tavsiyesi bilgisayarinizi yavaslatabilecek veya riske atabilecek sorunlari tespit etmek ve durumu çözecek bir islem önermek üzere tasarlanmistir. Bilgisayarda ani bir yavaslama yasarsaniz *(internet tarama, genel performans)*, sorunun kaynagi ve dolayisiyla çözüm yolu genellikle çok net degildir. Bu durumda yardima ***AVG Tavsiyesi*** yetisir: Sorunun ne olabilecegi ve çözüm önerilerine yönelik bir bilgilendirmeyi sistem tepsisinde gösterir. ***AVG Tavsiyesi*** bilgisayarinizdaki çalisan tüm islemleri olasi sorunlara karsi sürekli izler ve sorunlari engellemeye yönelik ipuçlari önerir.

AVG Tavsiyesi sistem tepsisi üzerinde beliren bir açilir pencere olarak görülebilir:



AVG Tavsiyesi özellikle asagidaki durumlari izler:

- ***O anda açik web tarayicilarinin durumu***. Web tarayicilari bellegi asiri yükleyebilir,

özellikle de belirli bir süre birden fazla sekme veya pencere açilmissa, ve çok fazla sistem kaynagi tüketir (örn. bilgisayarinizi yavaslatir). Böyle bir durumda web tarayicisinin yeniden baslatilmasi genellikle ise yarar.

- ***Esler Arasi baglantilari çalistirma***. Dosya paylasimi için P2P protokolü kullanildiktan sonra, baglanti bazen etkin kalarak belirli miktarda bant genisliginizi kullanir. Bunun sonucunda web taramasinda yavaslama görebilirsiniz.

- ***Tanidik ada sahip bilinmeyen ag***. Bu durum yalnizca, genellikle tasinabilir bilgisayarlar kullanip birçok aga baglanan kullanicilar için geçerlidir: Yeni, bilinmeyen bir ag iyi bilinen, sik kullanilan bir agla ayni ada sahipse *(örn. Ev veya Wifi)*, karisiklik meydana gelebilir ve yanlislikla hiç bilinmeyen ve muhtemelen güvenli olmayan bir aga baglanabilirsiniz. ***AVG Tavsiyesi*** bilinen adin aslinda yeni bir aga ait oldugu uyarisiyla bu durumu engelleyebilir. Tabii ki, bilinmeyen agin güvenli olduguna karar verirseniz, bunu bir ***AVG Tavsiyesi*** bilinen aglar listesine kaydedebilirsiniz, böylece ag ilerde tekrar rapor edilmez.

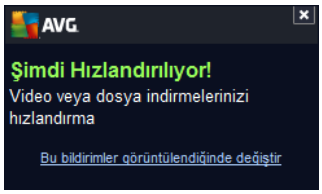
Bu durumlarin her birinde, ***AVG Advisor*** gerçeklesebilecek olasi sorunlar hakkinda sizi uyarir ve çakisan islem veya uygulamanin adini ve simgesini gösterir. Ayrica, ***AVG Advisor*** olasi sorunlari engellemek için yapilmasi gerekenler hakkinda önerilerde bulunur.

Desteklenen web tarayicilari

Özelligin çalistigi web tarayicilari: Internet Explorer, Chrome, Firefox, Opera, Safari.

5.8. AVG Hızlandırıcı

AVG Accelerator daha düzgün çevrimiçi video oynatmaya izin verir ve ilave indirmeleri daha kolay hale getirir. Video hizlandirma islemi çalisirken sistem tepsisi açilir penceresi ile bilgilendirilirsiniz.



6. AVG Bileşenleri

6.1. Bilgisayar Koruması

Bilgisayar bileseni iki temel güvenlik hizmetini kapsar: ***Virüslerden Koruma*** ve ***Veri Kasasi***:

- ***AntiVirus*** tüm dosyalari, bilgisayarin sistem alanlarini ve çikarilabilir ortamlari *(flash disk vb.) koruyan bir tarama motoru barindirir.* ve bilinen virüslere karsi tarama yapar. Tespit edilen virüsler, harekete geçmeden engellenecek ve ardindan silinecek ya da Virüs Kasasi 'nda karantinaya alinacaktir. Yerlesik koruma "arkaplanda" çalistigindan islemin farkina bile varmazsiniz. AntiVirus dosyalarin tipik virüs özelliklerine karsi tarandigi bulussal analiz taramasi da kullanir. Bu, yeni bir virüs mevcut virüslerin tipik özelliklerinden bazilarina sahipse söz konusu AntiVirus tarayicisinin yeni ve bilinmeyen bir virüsü tespit edebilecegi anlamina gelmektedir. **AVG Internet Security 2014** sistem içinde potansiyel olarak istenmeyen statüsündeki çalistirilabilir uygulamalar ve DLL kitapliklarini da analiz ve tespit eder *(çesitli türlerde casus yazilim, reklam yazilimi vb.)*. Virüslerden Koruma buna ek olarak, sistem kayit defterinizi süpheli girdilere ve geçici internet dosyalarina karsi da tarar ve söz konusu potansiyel olarak istenmeyen nesneleri de diger bulasmalarla ayni sekilde düzeltmenizi saglar.

- ***Veri Kasasi*** degerli veya hassas verileri saklamak için güvenli sanal kasalar olusturmaniza olanak saglar. Veri Kasasi içerikleri sifrelenir ve sizin seçtiginiz bir parola ile korunur; bu sayede yetkisi olmayan hiç kimse bunlara erisemez.

Iletisim kutusu kontrolleri

Iletisim kutusunun iki bölümü arasinda geçis yapmak için ilgili hizmet panelinde herhangi bir yeri tiklatabilirsiniz. Bu durumda panel açik mavi bir tonda vurgulanir. Iletisim kutusunun her iki bölümünde de asagidaki kontrolleri bulabilirsiniz. Bölümlerin islevselligi, ait olduklari güvenlik servisinden bagimsiz olarak, aynidir *(Virüslerden Koruma veya Dosya Kasalari)*:

 ***Etkin / Devre disi*** - Dügme size hem görünüs hem de islev olarak trafik isiklarini hatirlatmis olabilir. Iki konum arasinda geçis yapmak için tek tiklatin. Yesil renk ***Etkin***, yani AntiVirus güvenlik hizmetinin aktif ve tamamen çalisir durumda oldugu anlamina gelmektedir. Kirmizi renk ise ***Devre disi*** durumunu temsil etmektedir; yani hizmet devre disi birakilmistir. Hizmeti devre disi birakmak için iyi bir nedeniniz yoksa, tüm güvenlik yapilandirmasi için varsayilan ayarlari kesinlikle degistirmemenizi öneririz. Varsayilan ayarlar uygulama için en iyi performansi ve sizin için de maksimum güvenligi saglar. Belirli bir nedenle hizmeti devre disi birakmak istiyorsaniz, kirmizi renkli ***Uyari*** isareti ve o anda tam olarak korunmadiginiz bilgisiyle olasi riskler hakkinda hemen uyarilirsiniz. ***Hizmeti mümkün olan en kisa sürede tekrar etkinlestirmeyi lütfen unutmayin!***

 ***Ayarlar*** - Dügmeyi tiklatarak gelismis ayarlar arayüzüne gidebilirsiniz. Tam olarak, ilgili iletisim kutusu açilir ve siz de burada seçilen hizmeti, yani Virüslerden Koruma'yi yapilandirabilirsiniz. Gelismis ayarlarda **AVG Internet Security 2014** uygulamasindaki tüm güvenlik hizmetlerinin yapilandirmasini düzenleyebilirsiniz, ancak yapilandirma islemi yalnizca deneyimli kullanicilara önerilmektedir!

 ***Istatistikler*** - Dügmeyi tiklatarak AVG web sitesinde özel olarak hazirlanmis bir sayfaya gidebilirsiniz (*http://www.avg.com/*). Bu sayfada belirli bir zaman diliminde ve toplam olarak bilgisayarinizda gerçeklestirilen tüm **AVG Internet Security 2014** etkinliklerine ayrintili bir istatistiksel genel bakis bulabilirsiniz.

 ***Ayrintilar*** - Dügmeyi tiklattiginizda vurgulanan hizmetin kisa bir açiklamasi iletisim kutusunun alt kisminda görüntülenir.

 - Bilesen genel bilgilerinin bulundugu ana kullanici arayüzüne dönmek için iletisim kutusunun sol üst kisminda bulunan yesil oku kullanin.

Veri kasanizi olusturma

Bilgisayar Koruması iletisim kutusunun ***Veri Kasasi*** bölümünde ***Kasanizi Olusturun*** dügmesini bulabilirsiniz. Ayni ada sahip yeni bir iletisim kutusu açmak için dügmeyi tiklatarak planladiginiz kasanin parametrelerini belirleyebilirsiniz. Lütfen tüm gerekli bilgileri doldurun ve uygulamadaki yönergeleri izleyin:

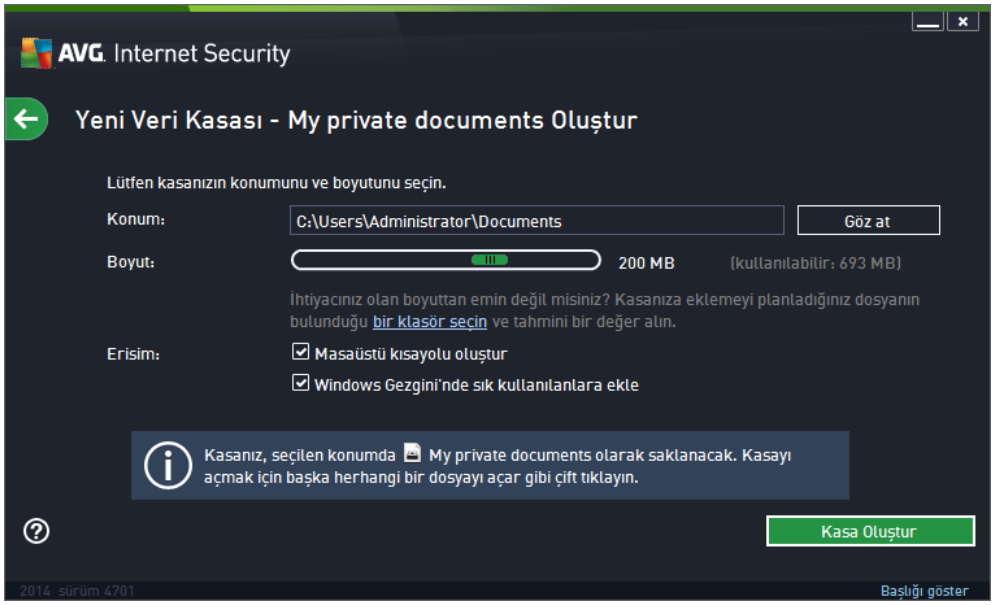
Öncelikle, kasanin adini belirlemeniz ve güçlü bir parola olusturmaniz gerekir:

- ***Kasa adi*** - Yeni bir veri kasasi olusturmak için öncelikle taniyabileceginiz uygun bir kasa adi seçmeniz gerekir. Bilgisayari diger aile fertleri ile paylasiyorsaniz kasa içeriklerini gösteren bir ifadenin yani sira adinizi da ekleyebilirsiniz: *Babanin e-postalari* gibi.

- ***Parola olustur / Parolayi yeniden yazin*** - Veri kasaniz için bir parola olusturun ve parolayi ilgili metin alanlarina yazin. Parolanizin zayif mi *(özel yazilim araçlariyla kirilmasi görece kolay)* yoksa güçlü mü oldugu sag taraftaki grafik göstergede belirtilir. En azindan orta kuvvette bir parola seçmenizi tavsiye ederiz. Büyük harfler, sayilar ve nokta, tire vb. baska karakterler ekleyerek parolanizi daha güçlü hale getirebilirsiniz. Parolanizi istediginiz sekilde yazdiginizdan emin olmak istiyorsaniz ***Parolayi göster*** kutusunu *isaretleyebilirsiniz (tabii ki ekraniniza baska birinin bakmiyor olmasi kosuluyla)*.

- ***Parola ipucu*** - Unutmaniz durumunda size parolanizi hatirlatacak faydali bir parola ipucu olusturmanizi da kesinlikle tavsiye ederiz. Veri Kasasi'nin yalnizca parola ile erisime izin vererek dosyalarinizi güvenli tutmak üzere tasarlanmis oldugunu lütfen unutmayin; bu durumun geçici bir çözümü yoktur ve parolayi unutursaniz Veri Kasasi'na erisemezsiniz!

Metin alanlarindaki tüm zorunlu verileri belirlediyseniz bir sonraki adima geçmek için ***Ileri*** dügmesini tiklatin:



Bu iletisim kutusunun sagladigi yapilandirma seçenekleri:

- ***Konum*** veri kasasinin fiziki olarak nereye yerlestirilecegini gösterir. Gözat dügmesiyle sabit diskinizde uygun bir konum belirleyebilir veya önceden tanimlanmis konumu (*Belgeler* klasörünüz) muhafaza edebilirsiniz. Bir veri kasasi olusturduktan sonra bu kasanin konumunu degistiremeyeceginizi lütfen unutmayin.

- ***Boyut*** - veri kasanizin boyutunu önceden tanimlayarak disk üzerinde gerekli alanin tahsis edilmesini saglayabilirsiniz. Ayarlanacak deger ne çok küçük *(ihtiyaçlariniz için yetersiz)*, ne de çok büyük *(gereksiz yere çok fazla disk alani kaplayacak nitelikte)* olmalidir. Veri kasasina ne koymak istediginizi biliyorsaniz tüm dosyalari tek bir klasöre yerlestirebilir ve ardindan ***Bir klasör seç*** baglantisini kullanarak toplam boyutu otomatik olarak hesaplayabilirsiniz. Ancak, boyut daha sonra ihtiyaçlariniz dogrultusunda degistirilebilir.

- ***Erisim*** - bu bölümdeki onay kutulari veri kasaniz için kullanisli kisayollar olusturmaniza olanak saglar.

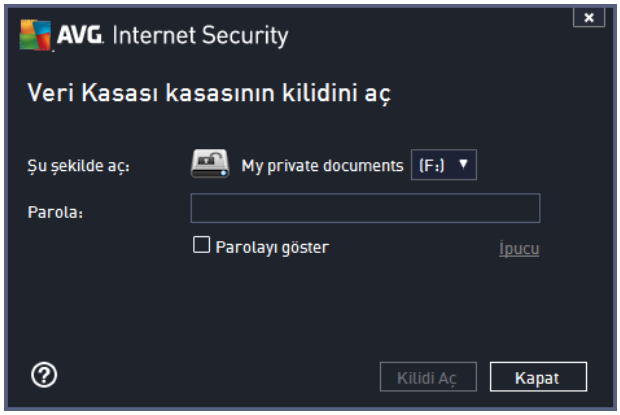
Veri kasanizi kullanma

Ayarlardan memnun oldugunuzda ***Kasa Olustur*** dügmesini tiklatin. Dosyalarinizi saklamak için kasanin hazir oldugunu belirten yeni bir ***Veri Kasaniz simdi hazir*** iletisim kutusu açilir. Artik kasa açiktir ve kasaya hemen erisebilirsiniz. Kasaya daha sonraki tüm erisim girisimlerinizde tanimlamis oldugunuz parolayla kasanin kilidini açmaniz istenecektir:

Yeni veri kasanizi kullanabilmek için öncelikle ***Simdi Aç*** dügmesini tiklatarak kasayi açmaniz gerekir. Kasayi açtiktan sonra veri kasasi bilgisayarinizda yeni bir sanal disk olarak görünür. Lütfen kasaya açilir menüden seçtiginiz bir harfi atayin (*yalnizca o anda bos olan diskler arasindan seçim yapmaniza izin verilir*). Genel olarak, C *(çogunlukla sabit sürücünüze atanir)*, A *(disket sürücüsü)* veya D *(DVD sürücüsü)* harflerini seçmenize izin verilmez. Bir veri kasasinin kilidini her açisinizda kullanilabilir durumdaki sürücü harflerinden bir baskasini seçebileceginizi lütfen unutmayin.

Veri kasanizin kilidini açma

Kasaya daha sonraki erisim girisiminizde tanimlamis oldugunuz parolayla kasanin kilidini açmaniz istenecektir:



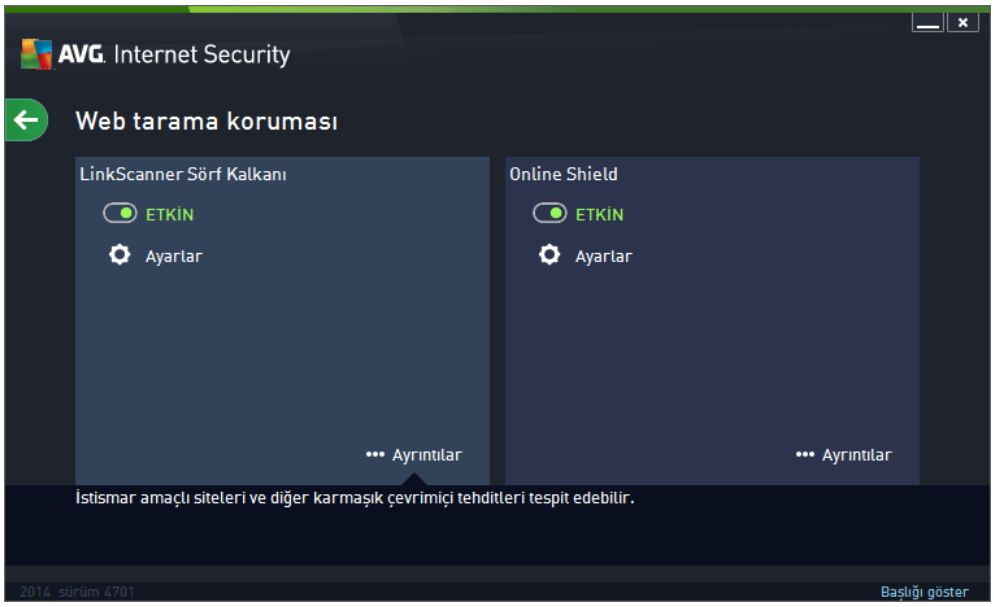
Metin alaninda, kendinizi onaylamak için lütfen parolanizi yazin ve ***Kilidi Aç*** dügmesini tiklatin. Parolayi hatirlamakla ilgili yardima ihtiyaciniz varsa veri kasasini olustururken tanimladiginiz parola ipucunu görüntülemek için ***Ipucu***'nu tiklatin. Yeni veri kasasi, veri kasalarinizin genel görünüm sayfasinda KILIDI AÇIK olarak görünür ve gerektigi sekilde kasaya dosya ekleyebilir veya kasadan dosya silebilirsiniz.

6.2. Web Tarama Koruması

Web Tarama Korumasi iki hizmetten olusur: ***LinkScanner Sörf Kalkani*** ve ***Online Shield***:

- ***LinkScanner Sörf Kalkani*** sizi web üzerinde "günden güne" artan tehditlere karsi korur. Bu tehditler idari web sitelerinden, taninmis markalarin web sitelerinden tutun, küçük isletmelerin web sitelerine kadar her tür web sitesinde gizlenmis olabilir. LinkScanner görüntülemekte oldugunuz web sitesinde bulunan tüm baglantilarin arkasindaki web sayfalarini analiz ederek ve siz söz konusu baglantiyi tiklamak üzereyken o anda güvenli olup olmadigindan emin olarak sizi korur. ***LinkScanner Sörf Kalkani sunucu platformlari korumasinda kullanilmak için tasarlanmamistir!***

- ***Online Shield***, ziyaret ettiginiz web sitelerinin içerigini (muhtemel dosyalar da dahil olmak üzere), hatta henüz web tarayicinizda görünmeden ya da bilgisayariniza indirilmeden önce tarayan gerçek zamanli bir koruma yöntemidir. Online Shield, ziyaret ettiginiz sayfanin tehlikeli javascript içerdigini tespit ederse, sayfanin görüntülenmesini engeller. Buna ek olarak bir sayfada bulunan zararli yazilimi tanir ve bilgisayariniza girisini engellemek için indirme islemini durdurur. Bu güçlü koruma, açmaya çalistiginiz web sayfalarinin kötü amaçli içerigini engeller ve bilgisayariniza karsidan yüklenmesini önler. Bu özellik etkin durumdayken, tehlikeli bir site baglantisi tiklatildiginda ya da URL'si yazildiginda otomatik olarak web sayfasini açmaniz engellenir, bu sayede etkilenmeniz önlenmis olur. Virüs bulasmis web sayfalarini ziyaret ettiginizde bilgisayariniza kolayca virüs bulasabilecegini gerçegini hatirlamak çok önemlidir. ***Online Shield'in sunucu platformlarinin korunmasinda kullanilmasi hedeflenmemistir!***



Iletisim kutusu kontrolleri

Iletisim kutusunun iki bölümü arasinda geçis yapmak için ilgili hizmet panelinde herhangi bir yeri tiklatabilirsiniz. Bu durumda panel açik mavi bir tonda vurgulanir. Iletisim kutusunun her iki bölümünde de asagidaki kontrolleri bulabilirsiniz. Bu veya su güvenlik servisine ait olmasindan bagimsiz olarak islevleri aynidir *(LinkScanner Sörf Kalkani veya Online Shield)*:

 ***Etkin / Devre disi*** - Dügme size hem görünüs hem de islev olarak trafik isiklarini hatirlatmis olabilir. Iki konum arasinda geçis yapmak için tek tiklatin. Yesil renk ***Etkin***, yani LinkScanner Sörf Kalkani / Online Shield güvenlik hizmetinin aktif ve tamamen çalisir durumda oldugu anlamina gelmektedir. Kirmizi renk ise ***Devre disi*** durumunu temsil etmektedir; yani hizmet devre disi birakilmistir. Hizmeti devre disi birakmak için iyi bir nedeniniz yoksa, tüm güvenlik yapilandirmasi için varsayilan ayarlari kesinlikle degistirmemenizi öneririz. Varsayilan ayarlar uygulama için en iyi performansi ve sizin için de maksimum güvenligi saglar. Belirli bir nedenle hizmeti devre disi birakmak istiyorsaniz, kirmizi renkli ***Uyari*** isareti ve o anda tam olarak korunmadiginiz bilgisiyle olasi riskler hakkinda hemen uyarilirsiniz. ***Hizmeti mümkün olan en kisa sürede tekrar etkinlestirmeyi lütfen unutmayin!***

 ***Ayarlar*** - Dügmeyi tiklatarak gelismis ayarlar arayüzüne gidebilirsiniz. Tam olarak, ilgili iletisim kutusu açilir ve siz de burada LinkScanner Sörf Kalkani veya Online Shield gibi seçtiginiz bir hizmetin yapilandirmasini yapabilirsiniz. Gelismis ayarlarda **AVG Internet Security 2014** uygulamasindaki tüm güvenlik hizmetlerinin yapilandirmasini düzenleyebilirsiniz, ancak yapilandirma islemi yalnizca deneyimli kullanicilara önerilmektedir!

 ***Ayrintilar*** - Dügmeyi tiklattiginizda vurgulanan hizmetin kisa bir açiklamasi iletisim kutusunun alt kisminda görüntülenir.

 - Bilesen genel bilgilerinin bulundugu ana kullanici arayüzüne dönmek için iletisim kutusunun sol üst kisminda bulunan yesil oku kullanin.

6.3. Identity Protection

Identity Protection bileseni internette dijital varliklarinizi yeni ve bilinmeyen tehditlere karsi sürekli olarak koruyan ***Identity Shield*** hizmetini çalistirir:

- ***Identity Protection*** kötü amaçli yazilimlara karsi koruma hizmetidir, davranis teknolojilerini kullanarak ve yeni virüsler için ilk günden koruma saglayarak sizi her türlü kötü amaçli yazilimlardan (*casus yazilim, robotlar, kimlik hirsizligi...*) korur. Identity Protection, PC'nizdeki parolalarinizi, banka hesabi ayrintilarinizi, kredi karti numaralarinizi ve diger kisisel dijital bilgilerinizi tüm kötü amaçli yazilimlarla *(kötü amaçli yazilim)* çalan kimlik hirsizligi üzerine odaklanmistir. Bilgisayarinizda ve paylasilan aginizda çalisan tüm programlarin düzgün biçimde çalismasini saglar. Identity Protection, sürekli olarak süpheli davranislari belirleyip engeller ve tüm yeni kötü amaçli yazilimlara karsi bilgisayarinizi korur. Identity Protection, yeni ve hatta bilinmeyen tehlikelere karsi bilgisayariniza gerçek zamanli bir koruma saglar. Tüm islemleri *(gizli olanlar da dahil) ve 285 üzerinde farkli davranis modelini izler ve sisteminizle ilgili kötü amaçli herhangi bir durum meydana gelip gelmedigini belirleyebilir.* Bu nedenle, virüs veritabaninda henüz açiklanmamis tehditleri bile açiga çikarabilir. Bilgisayariniza bilinmeyen bir kod gelirse söz konusu kod kötü amaçli davranislara karsi hemen gözlenir ve izlenir. Dosyanin kötü amaçli oldugu tespit edilirse, Identity Protection kodu Virüs Kasasi'na kaldirir ve sistemde yapilan tüm degisiklikleri *(kod bulasmalari, kayit defteri degisiklikleri, baglanti noktasi açma vb.) geri alir.* Korunmak için tarama baslatmaniz gerekmez. Bu teknoloji çok öngörülüdür, nadiren güncellemeye gereksinim duyar ve her an korur.

Iletisim kutusu kontrolleri

Iletisim kutusunda bulabileceginiz kontroller:

Etkin / Devre disi - Dügme size hem görünüs hem de islev olarak trafik isiklarini hatirlatmis olabilir. Iki konum arasinda geçis yapmak için tek tiklatin. Yesil renk ***Etkin***, yani Identity Protection güvenlik hizmetinin aktif ve tamamen çalisir durumda oldugu anlamina gelmektedir. Kirmizi renk ise ***Devre disi*** durumunu temsil etmektedir; yani hizmet devre disi birakilmistir. Hizmeti devre disi birakmak için iyi bir nedeniniz yoksa, tüm güvenlik yapilandirmasi için varsayilan ayarlari kesinlikle degistirmemenizi öneririz. Varsayilan ayarlar uygulama için en iyi performansi ve sizin için de maksimum güvenligi saglar. Belirli bir nedenle hizmeti devre disi birakmak istiyorsaniz, kirmizi renkli ***Uyari*** isareti ve o anda tam olarak korunmadiginiz bilgisiyle olasi riskler hakkinda hemen uyarilirsiniz. ***Hizmeti mümkün olan en kisa sürede tekrar etkinlestirmeyi lütfen unutmayin!***

Ayarlar - Dügmeyi tiklatarak gelismis ayarlar arayüzüne gidebilirsiniz. Tam olarak, ilgili iletisim kutusu açilir ve siz de burada Identity Protection gibi seçtiginiz bir hizmetin yapilandirmasini yapabilirsiniz. Gelismis ayarlarda **AVG Internet Security 2014** uygulamasindaki tüm güvenlik hizmetlerinin yapilandirmasini düzenleyebilirsiniz, ancak yapilandirma islemi yalnizca deneyimli kullanicilara önerilmektedir!

Ayrintilar - Dügmeyi tiklattiginizda vurgulanan hizmetin kisa bir açiklamasi iletisim kutusunun alt kisminda görüntülenir.

- Bilesen genel bilgilerinin bulundugu ana kullanici arayüzüne dönmek için iletisim kutusunun sol üst kisminda bulunan yesil oku kullanin.

Ne yazik ki, **AVG Internet Security 2014** uygulamasinda Identity Alert hizmeti yer almamaktadir. Bu koruma türünü kullanmak istiyorsaniz, ***Etkinlestirme Için Yükselt*** dügmesini kullanarak Identity Alert lisansi satin alabileceginiz web sayfasina gidebilirsiniz.

AVG Premium Security sürümlerinde dahi Identity Alert hizmetinin su anda yalnizca ABD, Birlesik Krallik, Kanada ve Irlanda bölgelerinde sunuldugunu lütfen aklinizda bulundurun.

6.4. E-posta Koruması

E-posta Korumasi bileseni iki güvenlik hizmetini kapsar: ***E-posta Tarayicisi*** ve ***Anti-Spam***:

- ***E-posta Tarayicisi***: Virüsler ve truva atlari yaygin olarak e-postalar araciligiyla yayilir. Kimlik avi ve istenmeyen postalar, e-postalari daha büyük risk kaynaklari haline getirmektedir. Ücretsiz e-posta hesaplarinin zararli e-postalari alma ihtimali daha yüksek olup *(nadiren istenmeyen posta önleme teknolojisine sahip olmalari nedeniyle)* ev kullanicilari büyük çogunlukla söz konusu e-postalari kullanir. Bunun yani sira, bilmedikleri sitelerde dolasan ve çevrimiçi formlari kisisel bilgileri ile dolduran *(e-posta adresleri gibi)* ev kullanicilari, e-posta saldirilarina siklikla maruz kalmaktadir. Sirketler genellikle kurumsal e-posta hesaplari kullanmakta ve riskleri en aza indirmek için anti-spam filtrelerinden yararlanmaktadir. E-posta Korumasi bileseni, alinan veya gönderilen her e-posta iletisini taramakla sorumludur. Bir e-postada virüs tespit edildiginde, hemen Virüs Kasasi'na kaldirir. Söz konusu bilesen belirli türde e-posta eklerini filtreleyebilir ve virüs bulunmayan iletilere bir onay metni ekleyebilir. ***E-posta Tarayicisi'nin sunucu platformlarinda kullanilmasi hedeflenmemistir!***

- ***Anti-Spam*** gelen tüm e-posta mesajlarini kontrol eder ve istenmeyen e-postalari spam olarak isaretler *(Spam, ürün veya hizmet reklami yapmak amaciyla bir kerede çok sayida e-posta adresine toplu olarak gönderilen ve kullanicilarin posta kutularini dolduran istenmeyen e-postalardir. Istenmeyen posta, müsterinin kendi istegiyle almayi kabul ettigi yasal ticari e-posta anlamina gelmez.*. Anti-Spam özel metin dizesi ekleyerek e-postanin konusunu degistirebilir *(istenmeyen posta olarak tanimlanir)*. Böylece, e-posta istemcinize göre e-postalarinizi filtreleyebilirsiniz. Anti-Spam bileseni, her e-posta iletisini islemek için çesitli analiz yöntemleri kullanir ve istenmeyen e-postalari karsi mümkün olan en üst seviyede koruma saglar. Anti-Spam istenmeyen postayi algilamak için düzenli olarak güncellenen veritabani kullanir. RBL sunucularini *("bilinen istenmeyen posta göndericisi" e-posta adreslerinden olusan genel veritabanlari)* kullanmak ve Beyaz listenize *(hiçbir zaman spam olarak isaretleme)* ve Kara listenize *(her zaman spam olarak isaretle)* manuel olarak e-posta adresleri eklemek de mümkündür.

Iletisim kutusu kontrolleri

Iletisim kutusunun iki bölümü arasinda geçis yapmak için ilgili hizmet panelinde herhangi bir yeri tiklatabilirsiniz. Bu durumda panel açik mavi bir tonda vurgulanir. Iletisim kutusunun her iki bölümünde de asagidaki kontrolleri bulabilirsiniz. Bu veya su güvenlik servisine ait olmasindan bagimsiz olarak islevleri aynidir *(E-posta Tarayicisi veya Anti-Spam)*:

Etkin / Devre disi - Dügme size hem görünüs hem de islev olarak trafik isiklarini hatirlatmis olabilir. Iki konum arasinda geçis yapmak için tek tiklatin. Yesil renk ***Etkin***, yani güvenlik hizmetinin aktif ve tamamen çalisir durumda oldugu anlamina gelmektedir. Kirmizi renk ise ***Devre disi*** durumunu temsil etmektedir; yani hizmet devre disi birakilmistir. Hizmeti devre disi birakmak için iyi bir nedeniniz yoksa, tüm güvenlik yapilandirmasi için varsayilan ayarlari kesinlikle degistirmemenizi öneririz. Varsayilan ayarlar uygulama için en iyi performansi ve sizin için de maksimum güvenligi saglar. Belirli bir nedenle hizmeti devre disi birakmak istiyorsaniz, kirmizi renkli ***Uyari*** isareti ve o anda tam olarak korunmadiginiz bilgisiyle olasi riskler hakkinda hemen uyarilirsiniz. ***Hizmeti mümkün olan en kisa sürede tekrar etkinlestirmeyi lütfen unutmayin!***

E-posta Tarayicisi bölümünde iki adet "trafik isigi" dügmesi görebilirsiniz. Bu sayede E-posta Tarayicisi'nin gelen, giden veya hem gelen hem de giden mesajlari tarayip taramamasini ayri ayri belirleyebilirsiniz. Varsayilan olarak, tarama gelen e-postalar için açik, ancak bulasma riski düsük oldugundan giden postalar için kapalidir.

Ayarlar - Dügmeyi tiklatarak gelismis ayarlar arayüzüne gidebilirsiniz. Tam olarak, ilgili iletisim kutusu açilir ve siz de burada E-posta Tarayicisi veya Anti-Spam gibi seçtiginiz bir hizmetin yapilandirmasini yapabilirsiniz. Gelismis ayarlarda **AVG Internet Security 2014** uygulamasindaki tüm güvenlik hizmetlerinin yapilandirmasini düzenleyebilirsiniz, ancak yapilandirma islemi yalnizca deneyimli kullanicilara önerilmektedir!

Istatistikler - Dügmeyi tiklatarak AVG web sitesinde özel olarak hazirlanmis bir sayfaya gidebilirsiniz (http://www.avg.com/). Bu sayfada belirli bir zaman diliminde ve toplam olarak

bilgisayarinizda gerçeklestirilen tüm **AVG Internet Security 2014** etkinliklerine ayrintili bir istatistiksel genel bakis bulabilirsiniz.

 ***Ayrintilar*** - Dügmeyi tiklattiginizda vurgulanan hizmetin kisa bir açiklamasi iletisim kutusunun alt kisminda görüntülenir.

 - Bilesen genel bilgilerinin bulundugu ana kullanici arayüzüne dönmek için iletisim kutusunun sol üst kisminda bulunan yesil oku kullanin.

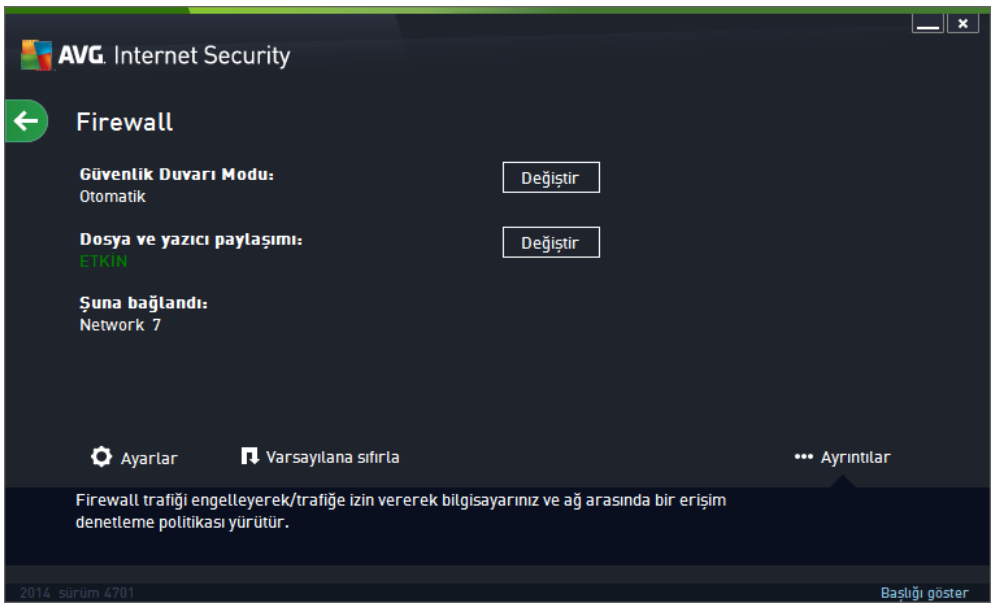
6.5. Firewall

Firewall, trafigi engellemek/izin vermek suretiyle iki ya da daha fazla ag arasinda gerçeklesen erisimi kontrol eden bir sistemdir. Firewall dahili agi *disaridan (genellikle internetten)* kaynaklanan saldirilara karsi koruyan bir dizi kural içerir ve ag baglanti noktalarinin her birinde gerçeklesen iletisimi kontrol eder. Iletisim tanimlanan kurallar dogrultusunda degerlendirilir ve ardindan söz konusu isleme izni verilir ya da engellenir. Firewall sisteme yetkisiz girilmeye çalisildigini tespit ederse söz konusu tesebbüsü "engeller" ve söz konusu kisinin bilgisayariniza erisimini engeller. Firewall, tanimli yazilim uygulamalari için ve tanimlanan baglanti yuvalari üzerinden dahili/harici iletisime *(her iki yönde, giris ve çikis)* izin vermek ya da engellemek üzere yapilandirilir. Örnegin, güvenlik duvari, Microsoft Explorer kullanilarak sadece içeri ve disari veri akisina izin verecek sekilde de yapilandirilabilir. Diger web tarayicilari tarafindan web verilerini aktarmaya yönelik tesebbüsler engellenecektir. Kisisel açidan tanimlanabilir verilerin sizin izniniz olmaksizin bilgisayarinizdan gönderilmesini engeller. Bilgisayarin internet ya da yerel ag üzerinden diger bilgisayarlarla yaptigi veri degisimini kontrol eder. Firewall kurumlarda aga bagli diger bilgisayarlari tek bir bilgisayar tarafindan ortaya konan saldirilara karsi da korur.

AVG Internet Security 2014 uygulamasinda ***Firewall*** bilgisayarinizdaki her ag baglanti noktasinin trafigini kontrol eder. Firewall, tanimlanan kurallara bagli olarak hem bilgisayarinizda çalisan *(ve internet/yerel ag yoluyla baglanmak isteyen)* uygulamalari hem de bilgisayariniza baglanmayi deneyerek disaridan bilgisayariniza girmeye çalisan uygulamalari degerlendirir. Firewall bu uygulamalarin her biri için ag baglanti noktalari üzerinde iletisime izin verir ya da iletisimi yasaklar. Varsayilan olarak, uygulama bilinmiyorsa *(diger bir degisle, Firewall kurallari tanimlanmamissa)*, Firewall iletisim girisimine izin vermek veya girisimi engellemek isteyip istemediginizi soracaktir.

AVG Firewall bileseninin sunucu platformlarinin korunmasinda kullanilmasi hedeflenmemistir!

Öneri: *Genellikle tek bir bilgisayarda birden fazla güvenlik duvari kullanilmasi önerilmez. Birden fazla güvenlik duvari kullanirsaniz bilgisayarin güvenligi gelistirilemez. Bu iki uygulama arasinda bazi çakismalarin olusmasi mümkündür. Bu yüzden bilgisayarinizda yalnizca bir güvenlik duvari kullanmaniz ve diger tümünün etkinligini kaldirmaniz önerilir, böylece olasi çakismalar ve bununla ilgili sorunlar ortadan kaldirilir.*



Not: *AVG Internet Security 2014 yüklemenizin ardindan Firewall bileseni bilgisayarin yeniden baslatilmasini gerektirebilir. Bu durumda bilesenin iletisim kutusu yeniden baslatma gerektigi bilgisiyle birlikte görüntülenir. Dogrudan iletisim kutusunun içinde* ***Simdi yeniden baslat*** *dügmesini kullanabilirsiniz. Yeniden baslatmaya kadar Firewall bileseni tam olarak etkinlesmez. Ayrica, iletisim kutusundaki tüm düzenleme seçenekleri devre disi birakilir. Lütfen uyariyi dikkate alin ve bilgisayarinizi en kisa süre içinde yeniden baslatin!*

Mevcut Firewall modlari

Firewall, bilgisayarinizin bir alanda bulunmasina, bagimsiz bir bilgisayar veya bir dizüstü bilgisayar olmasina bagli olarak özel güvenlik kurallari tanimlamaniza olanak tanir. Bu seçeneklerin her biri için farkli bir koruma seviyesi gerekir ve bu seviyeler de ilgili modlarin kapsamindadir. Kisaca, Firewall modu Firewall bileseni için özel bir yapilandirmadir ve bu sekilde önceden tanimlanmis çok sayida yapilandirmayi kullanabilirsiniz.

- ***Otomatik*** - Firewall, bu modda tüm ag trafigini otomatik olarak denetler. Hiçbir karar için onayiniz istenmez. Firewall bilinen tüm uygulamalarla baglantiya izin verir ve ayni zamanda uygulamaya her zaman baglanabilmesi için bir kural olusturulur. Firewall, diger uygulamalar için uygulamanin davranisina bagli olarak uygulamaya yönelik izin veya engelleme kararini verir. Ancak, böyle durumlarda kural olusturulmaz ve uygulama her baglanmaya çalistiginda kontrol edilir. Otomatik mod arka planda dikkat çekmeden çalisir ve çogu kullanici için önerilen moddur.

- ***Interaktif*** - bilgisayarinizda gelen ve giden tüm ag trafigini tam olarak kontrol etmek istiyorsaniz bu mod kullanislidir. Firewall trafigi sizin için izler ve tüm iletisim ve veri aktarim girisimlerinden sizi haberdar ederek girisimi uygun gördügünüz biçimde engellemenizi veya izin vermenizi saglar. Yalnizca ileri düzey kullanicilar için önerilir.

- ***Internet erisimini engelle*** - internet baglantisi tamamen engellenir, internete erisemezsiniz ve disaridan hiç kimse de bilgisayariniza erisemez. Yalnizca özel ve kisa süreli kullanim içindir.

- ***Firewall korumasini kapat (önerilmez)*** - Firewall korumasinin devre disi birakilmasi bilgisayarinizda gelen ve giden tüm trafige izin verir. Sonuç olarak, bilgisayariniz hacker saldirilarina açik hale gelir. Lütfen bu seçenegi kullanirken çok dikkatli olun.

Not: Firewall içinde de bir otomatik mod mevcuttur. Bu mod, Bilgisayar veya Identity protection bileseni kapatildiginda ve bu nedenle bilgisayariniz tehditlere açik hale geldiginde sessizce etkinlestirilir. Bu tür durumlarda, Firewall yalnizca bilinen veya kesinlikle güvenli uygulamalara otomatik olarak izin verir. Diger tüm uygulamalar için sizin karar vermeniz istenir. Bunun nedeni devre disi birakilan bilesenlerin boslugunu kapatmak ve bilgisayarinizi güvende tutmaktir.

Iletisim kutusu kontrolleri

Bu iletisim kutusu Firewall bilesen durumu hakkindaki temel bilgileri gösterir:

- ***Güvenlik Duvari Modu*** - Geçerli olarak seçili Firewall modu hakkindaki bilgileri gösterir. Geçerli modu bir baska modla degistirmek istiyorsaniz, gösterilen bilginin yanindaki ***Degistir*** dügmesini kullanarak Firewall ayarlari arayüzüne geçebilirsiniz *(Firewall profillerinin açiklamalari ve öneriler için lütfen önceki paragrafa bakin)*.

- ***Dosya ve yazici paylasimi*** - O anda dosya veya yazici paylasimina *(her iki yönde de)* izin verilip verilmedigi bilgisini gösterir. Dosya ve yazici paylasimi Windows, ortak disk birimleri, yazicilar, tarayicilar ve tüm benzer cihazlarda "Paylasilan" olarak isaretlediginiz tüm dosyalar veya klasörler anlamina gelmektedir. Bu tür ögelerin paylasimi yalnizca güvenli oldugu düsünülen aglarda gerçeklestirilmelidir *(örnegin evde, iste veya okulda)*. Ancak, herkese açik aglara *(havaalani Wi-Fi veya internet kafe agi gibi)* baglaniyorsaniz, hiçbir sey paylasmak istemeyebilirsiniz.

- ***Suna baglandi*** - Geçerli olarak bagli oldugunuz agin adiyla ilgili bilgileri gösterir. Window XP'de, ag adi ilgili aga ilk baglandiginizda ag için seçtiginiz adlandirmaya karsilik gelir. Windows Vista ve üstü sistemlerde, ag adi Ag ve Paylasim Merkezi'nden otomatik olarak alinir.

Iletisim kutusunun kontrolleri:

Degistir - Bu dügme ilgili parametrenin durumunu degistirmenizi saglar. Degistirme isleminin ayrintilari için lütfen yukaridaki paragrafta ilgili parametrenin açiklamasina bakin.

 ***Ayarlar*** - Bu dügmeyi tiklatarak Firewall ayarlari arayüzüne geçip tüm Firewall yapilandirmasini düzenleyebilirsiniz. Tüm yapilandirma islemleri, sadece deneyimli kullanicilar tarafindan yapilmalidir.

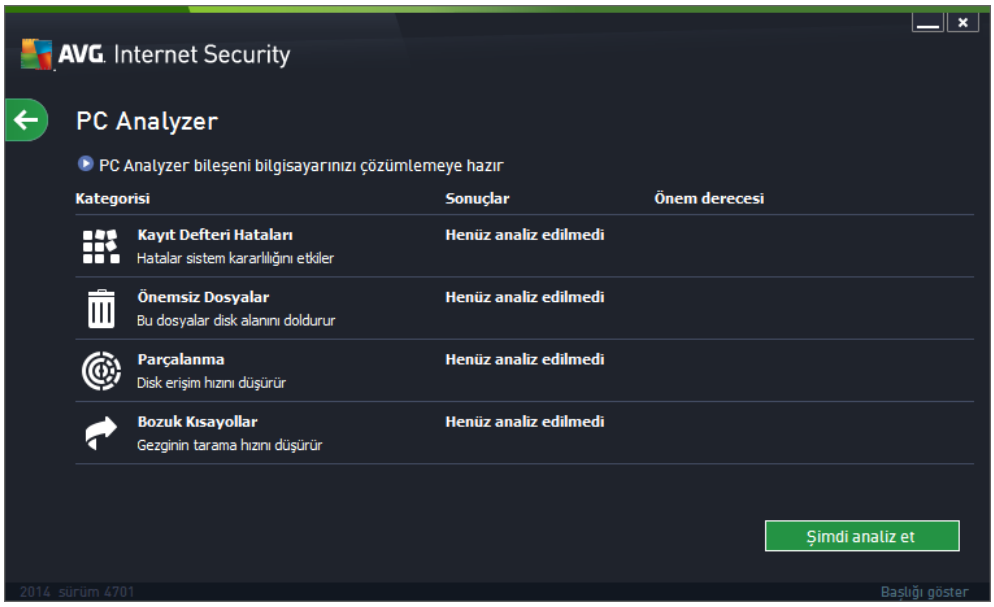
 ***Varsayilana sifirla*** - Geçerli Firewall yapilandirmasinin üzerine yazmak ve otomatik tespite bagli olarak varsayilan yapilandirmaya geri dönmek için bu dügmeye basin.

 ***Ayrintilar*** - Dügmeyi tiklattiginizda vurgulanan hizmetin kisa bir açiklamasi iletisim kutusunun alt kisminda görüntülenir.

 - Bilesen genel bilgilerinin bulundugu ana kullanici arayüzüne dönmek için iletisim kutusunun sol üst kisminda bulunan yesil oku kullanin.

6.6. Quick Tune bileşeni

Quick Tune bileseni, bilgisayarinizin hizinin ve genel performansinin nasil iyilestirilebilecegine yönelik ayrintili sistem analizi ve düzeltme islemi için tasarlanmis gelismis bir araçtir. Bu bilesen ana kullanici arayüzünde ***Performansi Yükseltin*** ögesinden açilir:



Su kategoriler analiz edilebilir ve onarilabilir: kayit defteri hatalari, istenmeyen dosyalar, parçalama ve bozuk kisayollar:

- ***Kayit Defteri Hatalari*** bilgisayarinizi yavaslatiyor olmasi veya hata mesajlarinin görüntülenmesine neden olmasi muhtemel Windows Kayit Defteri'ndeki hatalarin sayisini verir.
- ***Istenmeyen Dosyalar*** disk alaninizi kullanan ve silinebilecek dosyalarin sayisini verir. Normal olarak, bunlar çesitli türlerde geçici dosyalar ve Geri Dönüsüm Kutusundaki dosyalar olabilir.
- ***Bölümlendirme***, bölümlendirilmis, baska bir deyisle, fiziksel diskin farkli parçalarina dagitilmis dosyalarin sabit diskteki yüzdesini hesaplar.
- ***Bozuk kisayollar*** artik çalismayan ve var olmayan konumlara yönlendiren vs. kisayollari bulur.

Sisteminizi analiz etmeye baslamak için, ***Simdi analiz et*** dügmesine basin. Bundan sonra, analiz sürecini ve sonuçlarini söz konusu tabloda dogrudan izleyebilirsiniz:

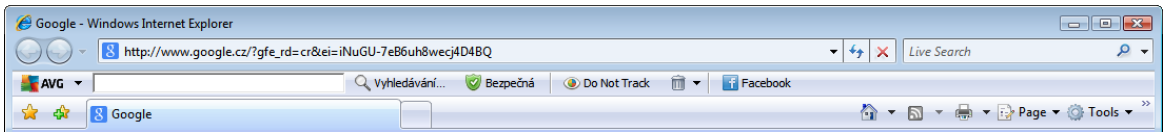
Sonuçlar genel görünümü, tespit edilen sistem sorunlarinin sayisini, test edilen ilgili kategorilere göre verir. Analiz sonuçlari ***Önem Düzeyi*** sütununda bir eksen üzerinde grafiksel olarak da görüntülenecektir.

Kontrol dügmeleri

- ***Simdi analiz et*** (*analiz baslamadan önce görüntülenir*) - bilgisayarinizin analiz islemini hemen baslatmak için bu dügmeye basin.
- ***Simdi onar*** *(analiz sona erdiginde görüntülenir*) - bulunan tüm hatalari onarmak için dügmeye basin. Düzeltme islemi bittiginde sonuçla ilgili bir genel görünüm alirsiniz.
- ***Iptal*** - analizin çalismasini durdurmak veya analiz tamamlandiktan sonra varsayilan AVG ana iletisim kutusuna (*bilesenler genel görünümüne*) geri dönmek için bu dügmeye basin.

7. AVG Security Toolbar

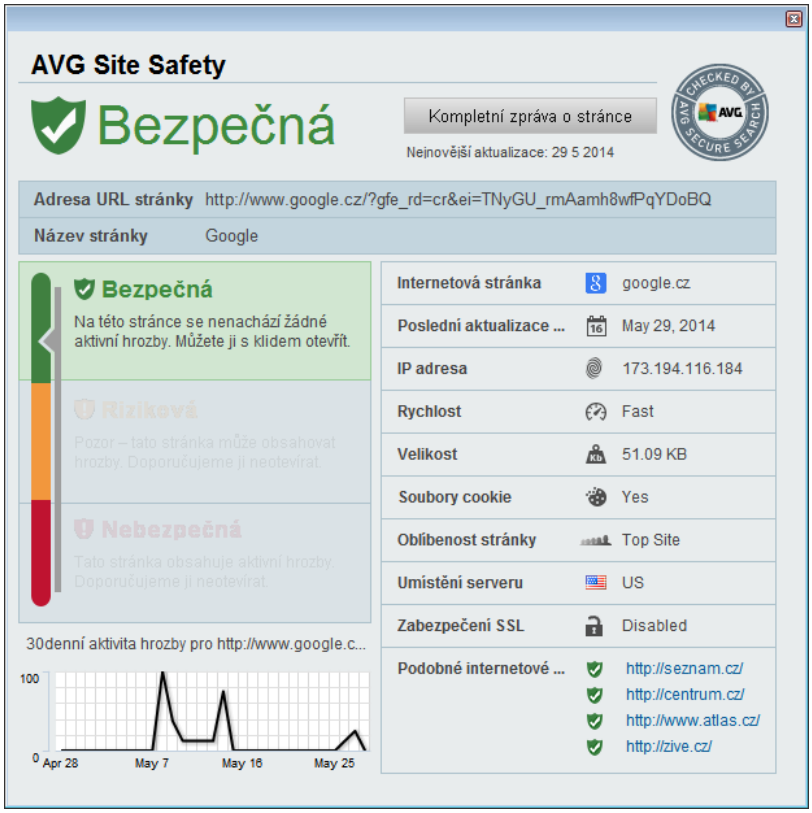
AVG Security Toolbar, LinkScanner Sörf Kalkani bileseni ile siki bir entegrasyon içinde çalisan bir araçtir ve internet taramalari sirasinda güvenliginizi en üst düzeyde saglar. **AVG Internet Security 2014** içinde ***AVG Security Toolbar*** kurulumu istege baglidir; kurulum islemi sirasinda bilesenin kurulup kurulmayacagina karar vermeniz istenir. ***AVG Security Toolbar*** internet tarayicinizdan dogrudan kullanilabilir. Su anda desteklenen internet tarayicilari: Internet Explorer (*sürüm 6.0 ve üstü*) ve/veya Mozilla Firefox (*sürüm 3.0 ve üstü*). Diger tarayicilar desteklenmez *(Avant Browser gibi alternatif internet tarayicilari kullaniyorsaniz beklenmeyen davranislarla karsilasabilirsiniz).*



AVG Security Toolbar'nun içerdigi ögeler:

- ***Açilir menülü AVG logosu***:
    - ***Geçerli Tehdit Düzeyi*** - web'de geçerli tehdit seviyesinin grafik görünümünü içeren virüs laboratuari web sayfasini açar.
    - ***AVG Tehlike Laboratuarlari*** - çesitli web sitelerinin güvenligi ve geçerli tehlike düzeyi hakkinda çevrimiçi bilgi alabileceginiz ***AVG Tehlike Laboratuari*** web sitesini açar (*http://www.avgthreatlabs.com*).
    - ***Toolbar Yardimi*** - tüm ***AVG Security Toolbar*** islevlerini kapsayan çevrimiçi yardimi açar.
    - ***Ürün Geribildirimi Gönder*** - ***AVG Security Toolbar*** hakkinda görüslerinizi bildirebileceginiz bir form içeren bir web sayfasi açar.
    - ***Son Kullanici Lisans Sözlesmesi*** - **AVG Internet Security 2014** kullaniminizla ilgili lisans sözlesmesinin tam metninin yer aldigi AVG web sitesi sayfasini açar.
    - ***Gizlilik Politikasi*** - AVG Gizlilik Politikasi'nin tam metnini bulabileceginiz AVG web sitesi sayfasini açar.
    - ***AVG Security Toolbar'nu kaldir*** - ***AVG Security Toolbar***'nu desteklenen web tarayicilarinin her birinde nasil devre disi birakabileceginize dair ayrintili talimat içeren bir web sayfasi açar.
    - ***Hakkinda...*** - yüklü ***AVG Security Toolbar*** sürümü hakkinda bilgilerin yer aldigi yeni bir pencere açar.
- ***Arama alani*** - görüntülenen tüm arama sonuçlari yüzde yüz güvenli oldugundan, kesin biçimde güvenli ve rahat olmak için internet aramalarinda ***AVG Security Toolbar***'nu kullanin. Anahtar sözcük veya ifadeyi arama alanina girin ve ***Ara*** dügmesine *(veya Enter tusuna)* basin.
- ***Site Güvenligi*** - bu dügme ziyaret etmekte oldugunuz sayfanin mevcut tehdit seviyesi (*Güvenli*) hakkinda bilgi saglayan yeni bir iletisim kutusu açar. Bu kisa açiklama genisletilebilir ve sayfayla ilgili güvenlik aktiviteleri hakkinda tüm ayrintilar dogrudan tarayici

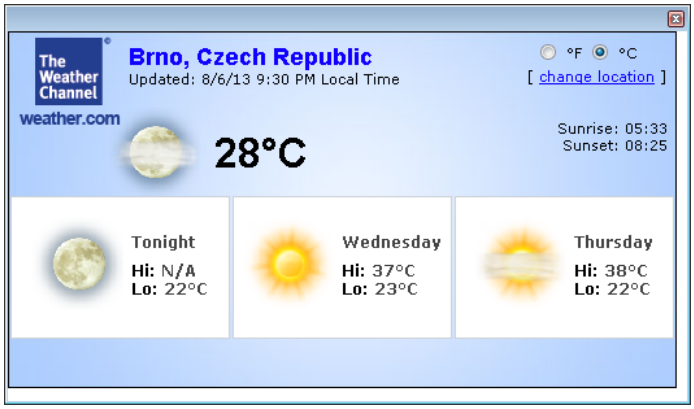
penceresinde görüntülenebilir (*Tam Web Sitesi Raporu*):



- ***Do Not Track*** - DNT servisi çevrimiçi etkinliklerinizi izleyen web sitelerini belirlemenize yardimci olur ve size bunlara izin verme veya bunlari engelleme seçenegi sunar. Ayrintilar >>

- ***Sil*** - 'çöp kutusu' dügmesi tarama, indirme ve çevrimiçi formlarla ilgili bilgileri seçerek silmek için bir açilir menü sunar; isterseniz tüm arama geçmisinizi tek seferde de silebilirsiniz.

- ***Hava*** - dügme, yasadiginiz yerin o gün ve sonraki iki günü kapsayan hava durumu hakkinda bilgi saglayan yeni bir iletisim kutusu açar. Bilgiler her 3-6 saatte bir düzenli olarak güncellenir. Iletisim kutusunda istediginiz konumu el ile seçebilir ve sicaklik degerlerinin Celsius veya Fahrenheit cinsinden gösterilmesini tercih edebilirsiniz.



- ***Facebook*** - Bu dügme dogrudan AVG Security Toolbar içinden ***Facebook*** sosyal paylasim agina baglanabilmenizi saglar.

- Su uygulamalara hizli erisim için kisayol dügmeleri: ***Hesap Makinesi***, ***Not Defteri***, ***Windows Explorer***.

8. AVG Do Not Track

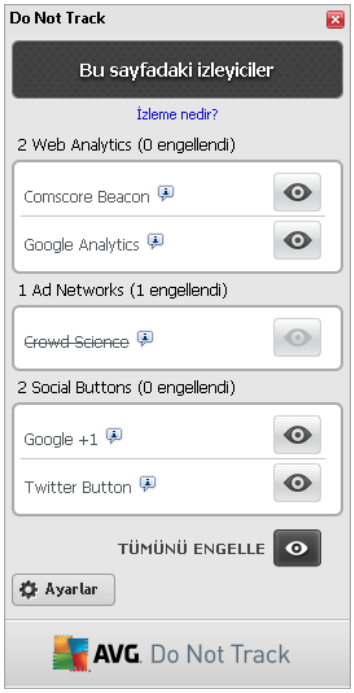
AVG Do Not Track çevrimiçi etkinlikleriniz hakkinda bilgi toplayan web siteleri hakkinda sizi bilgilendirir. AVG Security Toolbar'in bir parçasi olan ***AVG Do Not Track*** özelligi etkinlikleriniz hakkinda veri toplayan web siteleri veya reklamcilari gösterir ve size bunlari engelleme veya bunlara izin verme seçenegi sunar.

- ***AVG Do Not Track*** her servis için gizlilik politikasi hakkinda ek bilgilerin yani sira varsa ilgili servisin disinda kalmak için dogrudan bir baglanti da sunar.
- ***AVG Do Not Track*** sizi izlemesini istemediginiz siteler hakkinda otomatik bilgilendirme için W3C DNT protokolünü de destekler. Bu bilgilendirme otomatik olarak etkindir, ancak istenildiginde degistirilebilir.
- ***AVG Do Not Track*** uygulamasi su sartlar ve hükümler altinda saglanir.
- ***AVG Do Not Track*** varsayilan olarak etkindir, ancak istenildiginde kolayca devre disi birakilabilir. Talimatlari bulabileceginiz SSS makalesi: AVG Do Not Track özelligini devre disi birakma.
- ***AVG Do Not Track*** hakkinda daha fazla bilgi için lütfen web sitemizi ziyaret edin.

Su anda, ***AVG Do Not Track*** özelligi islevsel olarak Mozilla Firefox, Chrome ve Internet Explorer tarayicilarinda destekleniyor.

8.1. AVG Do Not Track arayüzü

Çevrimiçiyken, ***AVG Do Not Track*** herhangi bir veri toplama faaliyeti tespit edilir edilmez sizi uyarir. Böyle bir durumda, AVG Security Toolbar üzerinde yer alan ***AVG Do Not Track*** simgesi görünümünü degistirir; simgenin yaninda tespit edilen veri toplama servislerinin sayisini gösteren küçük bir sayi görünür:  Asagidaki iletisim kutusunu görüntülemek için simgeyi tiklatin:



Tespit edilen tüm veri toplama servisleri ***Bu sayfadaki izleyiciler*** bilgi ekraninda listelenir. ***AVG Do Not Track*** tarafindan taninan üç tür bilgi toplama etkinligi vardir:

- ***Web Analytics*** *(varsayilan olarak izin verilir):* Ilgili web sitelerinin performans ve deneyimini gelistirmek için kullanilan servisler. Bu kategoride Google Analytics, Omniture veya Yahoo Analytics gibi servisleri bulabilirsiniz. Web sitesi istenildigi sekilde çalismayabileceginden web analytics servislerini engellememenizi öneririz.

- ***Ad Networks*** *(bazilari varsayilan olarak engellenir):* Içerik tabanli reklamlar yerine size özel reklamlar sunmak için birden fazla sitede çevrimiçi etkinlikleriniz hakkinda dogrudan veya dolayli olarak bilgi toplayan ve paylasan servislerdir. Bu durum ilgili Ad networks ögesinin web sitesindeki gizlilik politikasina göre belirlenir. Bazi ad networks ögeleri varsayilan olarak engellenir.

- ***Social Buttons*** *(varsayilan olarak izin verilir):* Sosyal ag deneyimini gelistirmek için tasarlanmis ögeler. Social buttons ögeleri ziyaret ettiginiz siteye sosyal aglardan sunulur. Oturumunuz açikken çevrimiçi etkinlikleriniz hakkinda bilgi toplayabilirler. Social buttons örnekleri: Facebook Social Eklentileri, Twitter Dügmesi, Google +1.

Not: *Web sitesinin arka planinda çalisan servislere bagli olarak, AVG Do Not Track iletisim kutusunda yukarida açiklanan üç bölümden bazilari yer almayabilir.*

Iletisim kutusu kontrolleri

- ***Izleme nedir?*** - Izleme prensipleri hakkinda ayrintili açiklamalar ve belirli izleme türlerinin tarifini içeren bir web sayfasina yönlendirilmek için iletisim kutusunun üst bölümünde yer alan bu baglantiyi tiklatin.

- ***Tümünü Engelle*** - Hiçbir veri toplama faaliyeti istemiyorsaniz iletisim kutusunun altindaki

bu dügmeyi tiklatin *(ayrintilar için Izleme islemlerini engelleme bölümüne bakin).*

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

8.2. İzleme süreçleri hakkında bilgiler

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

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

8.3. İzleyici süreçlerini engelleme

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

- ***Tümünü Engelle*** - Hiçbir veri toplama faaliyeti istemiyorsaniz iletisim kutusunun altindaki bu dügmeyi tiklatin. *(Ancak, bu islemin servisin çalistigi ilgili web sitesinin islevlerini bozabilecegine dikkat edin!)*

-  - Tespit edilen servislerin tamamini bir seferde engellemek istemiyorsaniz, servislerin engellenmesine veya bunlara izin verilmesine tek tek karar verebilirsiniz. Tespit edilen sistemlerden bazilarinin çalismasina izin verebilirsiniz *(örn. Web Analytics):* Bu sistemler toplanan verileri kendi web sitelerinin optimizasyonu için kullanir ve böylece tüm kullanicilar

için internet ortaminin gelistirilmesine yardimci olur. Ancak, ayni zamanda Ad Networks olarak siniflandirilan tüm veri toplama faaliyetlerini engelleyebilirsiniz. Veri toplamayi engellemek *(servis adi çarpi ile isaretlenir)* veya veri toplamaya yeniden izin vermek için ilgili servisin yanindaki simgesini tiklatin.

8.4. AVG Do Not Track ayarları

Do Not Track Seçenekleri iletisim kutusunun sundugu yapilandirma seçenekleri:

- ***Do Not Track etkin*** - Varsayilan olarak DNT servisi etkindir *(AÇIK)*. Hizmeti devre disi birakmak için anahtari KAPALI konumuna getirin.

- Iletisim kutusunun orta bölümünde Ad Networks olarak siniflandirilabilecek bilinen veri toplama servislerinin bir listesinin yer aldigi bir kutu görebilirsiniz. ***Do Not Track*** varsayilan olarak Ad Networks servislerinin bir kismini otomatik olarak engeller ve geri kalanlarin engellenmesi veya bunlara izin verilmesi sizin seçiminize kalir. Bunun için listenin altindaki ***Tümünü Engelle*** dügmesini tiklatmaniz yeterlidir. Bunun yerine, yapilan tüm ayar degisikliklerini iptal etmek ve orijinal yapilandirmaya geri dönmek için ***Varsayilan*** dügmesini kullanabilirsiniz.

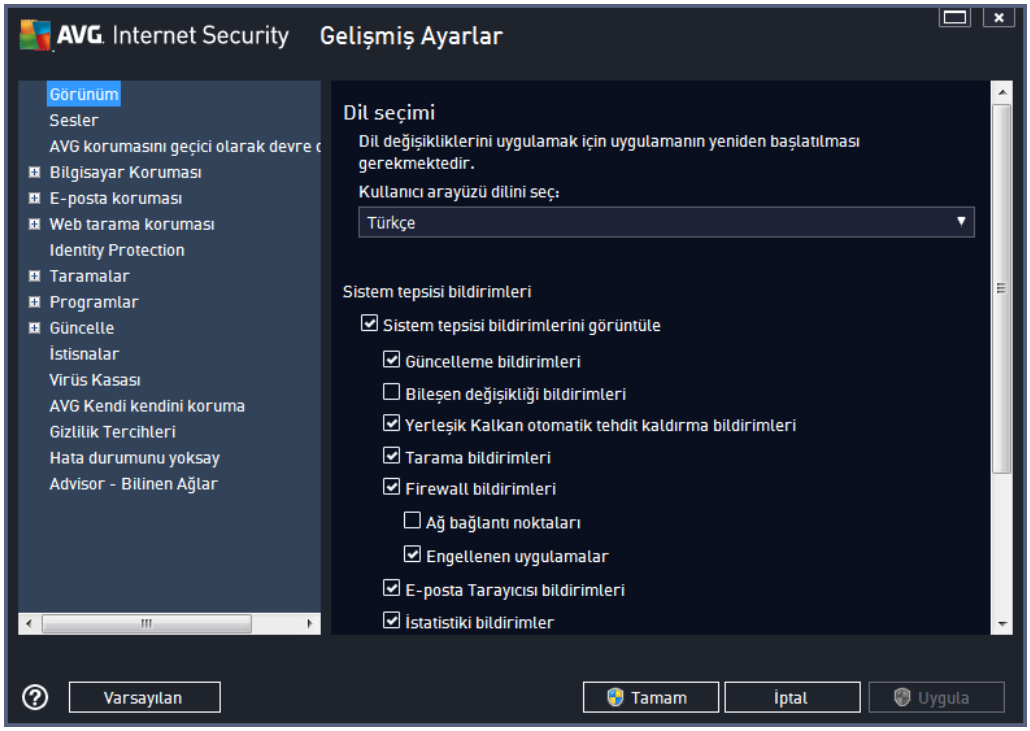
- ***Web siteleri bildirimi ...*** - Bu bölümde ***Izlenmek istemedigim web siteleri hakkinda bilgilendir*** seçenegini açabilir veya kapatabilirsiniz*(varsayilan olarak açiktir).* ***Do Not Track*** özelliginin sizi izlemesini istemediginiz veri toplama servisleri hakkinda bilgilendirmesini istiyorsaniz bu seçenegi isaretli olarak birakin.

9. AVG Gelişmiş Ayarlar

AVG Internet Security 2014 Gelismis yapilandirma iletisim kutusu ***Gelismis AVG Ayarlari*** adli yeni bir pencerede açilir. Pencere iki bölüme ayrilir: sol tarafta program yapilandirma seçeneklerini gösteren agaç tipli menü bulunmaktadir. Iletisim kutusunun pencerenin sag kisminda görüntülemek için yapilandirmasini (*ya da belirli bir parçasini*) degistirmek istediginiz bileseni seçin.

9.1. Görünüm

Menü agacinin ilk ögesi olan ***Görünüm***, **AVG Internet Security 2014** kullanici arayüzünün genel ayarlarina iliskindir ve uygulama davranisi için bazi temel seçenekleri saglar:

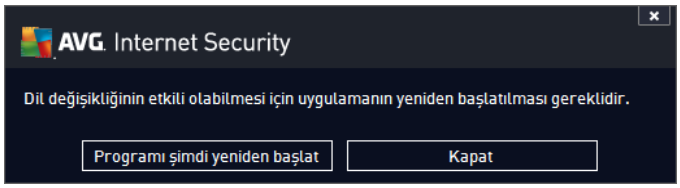


Dil seçimi

Dil seçimi bölümünde açilir menüden istediginiz dili seçebilirsiniz. Seçilen dil **AVG Internet Security 2014** kullanici arayüzünün tamami için kullanilir. Asagi açilir menü yükleme islemi sirasinda yüklenmesini istediginiz dilleri ve Ingilizceyi sunar (*Ingilizce daima varsayilan olarak yüklenir*). **AVG Internet Security 2014** uygulamasini baska bir dile geçirmek için yeniden baslatmaniz gerekir. Lütfen su adimlari takip edin:

- Asagi açilir menüde istediginiz uygulama dilini seçin
- ***Uygula*** dügmesine *(iletisim kutusunun sag alt tarafinda) basarak seçiminizi onaylayin*
- Onaylamak için ***Tamam*** dügmesine basin
- Uygulamanin dilini degistirmek için **AVG Internet Security 2014**

- Programin yeniden baslatilmasini onaylamak için ***AVG'yi simdi yeniden baslat*** dügmesine basin ve dil degisikliginin gerçeklesmesi için bir saniye bekleyin:



Sistem tepsisi bildirimleri

Bu bölümde **AVG Internet Security 2014** uygulama durumu hakkinda sistem tepsisi üzerinde beliren bildirimleri kaldirabilirsiniz. Varsayilan olarak, sistem bildirimlerinin görüntülenmesine izin verilir. Bu yapilandirmayi kesinlikle muhafaza etmeniz önerilir! Sistem bildirimleri örnegin tarama veya güncelleme islemi baslatma ya da bir **AVG Internet Security 2014** bileseni durum degisikligi hakkinda bilgi verir. Bu bildirimlere kesinlikle dikkat etmeniz gerekir!

Ancak, belirli bir neden dolayisiyla bu yolla bilgilendirilmek istemiyorsaniz ya da sadece belirli bildirimlerin görüntülenmesini istiyorsaniz *(belirli AVG Internet Security 2014 bilesenlerine iliskin)* tercihlerinizi asagidaki seçenekleri isaretleyerek ya da isaretlemeyerek tanimlayabilir ve belirleyebilirsiniz:

- ***Sistem tepsisi bildirimlerini görüntüle*** *(varsayilan olarak açik)* - varsayilan olarak tüm bildirimler görüntülenir. Tüm sistem bildirimleri kapatmak için bu ögenin isaretini kaldirin. Açildigi zaman hangi bildirimlerin görüntülenecegini seçebilirsiniz:
  - ***Güncelleme bildirimleri*** *(varsayilan olarak açik)* - **AVG Internet Security 2014** güncelleme isleminin baslamasi, ilerleyisi ve bitisi hakkinda bilgilerin görüntülenmesini isteyip istemediginize karar verin.
  - ***Bilesen degisiklik bildirimleri*** *(varsayilan olarak kapali)* - bilesenlerin etkin olup olmadigi ya da olasi sorunlari hakkinda bildirimlerin görüntülenmesini isteyip istemediginize karar verin. Bir bilesenin hata durumu rapor edilirken bu fonksiyon, sistem tepsisi simgesinin herhangi bir **AVG Internet Security 2014** bileseninde meydana gelen sorunu rapor ederken kullandigi bilgilendirici fonksiyonuna esdegerdir.
  - ***Yerlesik Kalkan otomatik tehdit kaldirma bildirimleri*** *(varsayilan olarak açik)* - dosya kaydetme, kopyalama ve açma islemleriyle ilgili bilgilerin görüntülenmesine veya gizlenmesine (*bu yapilandirma yalnizca Yerlesik Kalkan otomatik temizleme seçenegi açiksa*gösterilir) karar verin.
  - ***Tarama bildirimleri*** *(varsayilan olarak açik)* - programli taramalarin otomatik olarak baslamasi, ilerleyisi ve sonuçlari hakkinda bilgilerin görüntülenmesini isteyip istemediginize karar verin.
  - ***Firewall bildirimleri*** *(varsayilan olarak açik)* - Firewall durum ve islemleri hakkinda, örnegin bilesenin etkinlestirilmesi/devre disi birakilmasi uyarilari, olasi trafik engelleme vb. hakkinda bilgilerin görüntülenip görüntülenmeyecegine karar verin. Bu öge iki adet seçim seçenegi daha saglar *(her biri hakkinda daha fazla bilgi için lütfen bu belgedeki Firewall bölümüne bakin)*:

- ***Ag baglanti noktalari*** *(varsayilan olarak kapali)* - bir aga baglanirken, Firewall agi bilip bilmedigi ve dosya ve yazici paylasiminin nasil ayarlanacagi konusunda bilgilendirme yapar.

- ***Engellenmis uygulamalar*** *(varsayilan olarak açik)* - aga bilinmeyen veya süpheli bir uygulama baglanmaya çalistiginda Firewall girisimi engeller ve bir bildirim görüntüler. Bu bilgilenmeniz açisindan iyidir, bu yüzden özelligi daima açik tutmanizi öneririz.

- ***E-posta Tarayicisi*** ***bildirimleri*** *(varsayilan olarak açik)* - gelen ve giden e-posta mesajlarinin taranmasina iliskin bildirimleri görüntülemek isteyip istemediginize karar verin.

- ***Istatistiksel bildirimler*** *(varsayilan olarak açik)* - düzenli istatistiksel inceleme uyarilarinin sistem tepsisinde görüntülenmesine izin vermek için bu seçenegi isaretli halde birakin.

- ***AVG Hizlandirici bildirimleri*** *(varsayilan olarak açik)* - ***AVG Hizlandirici*** etkinlikleri hakkindaki bilgilerin görüntülenmesini isteyip istemediginize karar verin. ***AVG Hizlandirici*** hizmetidaha düzgün çevrimiçi video oynatmaya izin verir ve ilave indirmeleri daha kolay hale getirir.

- ***Baslatma zamanini gelistirme bildirimleri*** *(varsayilan olarak kapali)* - bilgisayarinizin baslatma zamaninin gelistirilmesi hakkinda bilgilendirilmek isteyip istemediginize karar verin.

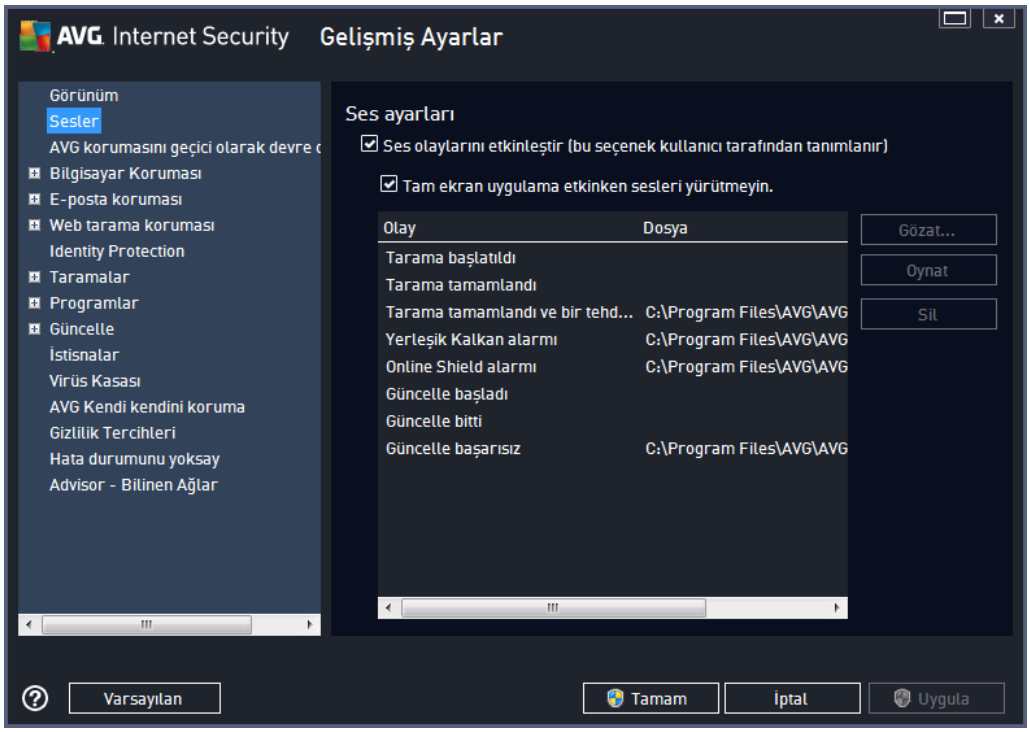
- ***AVG Tavsiyesi bildirimleri*** *(varsayilan olarak açik)* - AVG Tavsiyesi etkinlikleri hakkindaki bilgilerin sistem tepsisi panelinde görüntülenmesini isteyip istemediginize karar verin.

Oyun modu

Bu AVG islevi, tüm AVG bilgi balonlarinin (*örn. programlanmis bir tarama baslatildiginda gösterilir*) rahatsiz edici olabilecegi (*uygulamayi küçültebilir veya grafiklerini bozabilir*) tam ekran uygulamalari için tasarlanmistir. Bu durumu önlemek için, ***Tam ekran uygulamasi çalistirilirken oyun modunu etkinlestir*** seçenegini isaretli birakin (*varsayilan ayar*).

9.2. Sesler

Ses Ayarlari iletisim kutusunda belirli **AVG Internet Security 2014** islemleri hakkinda bir ses bildirimiyle bilgilendirilmek isteyip istemediginizi belirleyebilirsiniz:



Bu ayarlar yalnizca mevcut kullanici hesabi için geçerlidir. Bu nedenle bilgisayar üzerindeki kullanicilarin her birine ait ses ayarlari vardir. Sesli bildirime izin vermek istiyorsaniz, ilgili tüm eylemler listesini etkinlestirmek için ***Sesli uyarilari etkinlestir*** seçenegini isaretli birakin (*seçenek varsayilan olarak açiktir*). Ayrica, rahatsiz edici olabilecekleri durumlarda sesli bildirimleri kapatmak için ***Tam ekran uygulama etkinken sesleri yürütme*** seçenegini isaretlemek isteyebilirsiniz *(ayrica bu belgedeki Gelismis Ayarlar/Görünüm bölümünün Oyun modu kismina bakin)*.

Kontrol dügmeleri

- ***Gözat...*** - diskinizde atamak istediginiz ilgili ses dosyasini aramak için, listeden ilgili eylem seçilmis olarak ***Gözat*** dügmesini kullanin. *(Su anda yalnizca *.wav seslerinin desteklenmekte oldugunu lütfen unutmayin!)*

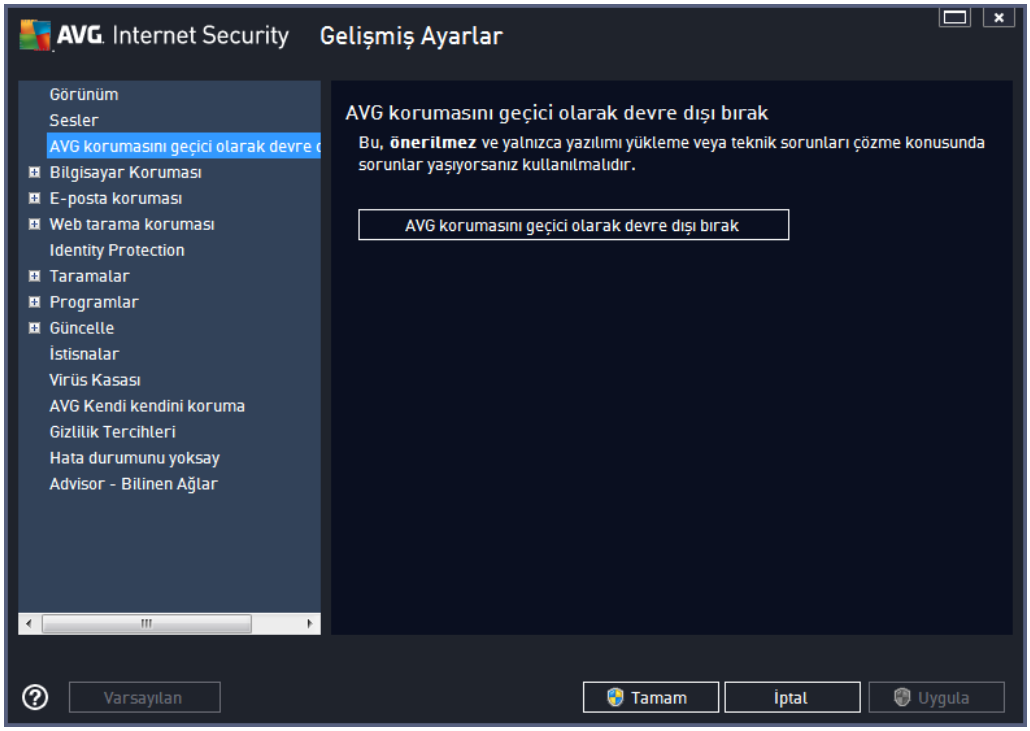
- ***Çal*** - seçili sesi dinlemek için, listede olayi vurgulayin ve ***Çal*** dügmesine basin.

- ***Sil*** - belirli olaya atanan sesi kaldirmak için ***Sil*** dügmesini kullanin.

9.3. AVG korumasını geçici olarak devre dışı bırak

AVG korumasini geçici olarak devre disi birak iletisim kutusunda, **AVG Internet Security 2014** yaziliminiz tarafindan güvende tutulan tüm korumayi bir seferde kapatma seçeneginiz vardir.

Mutlaka gerekli degilse, bu seçenegi kullanmamaniz gerektigini lütfen unutmayin!

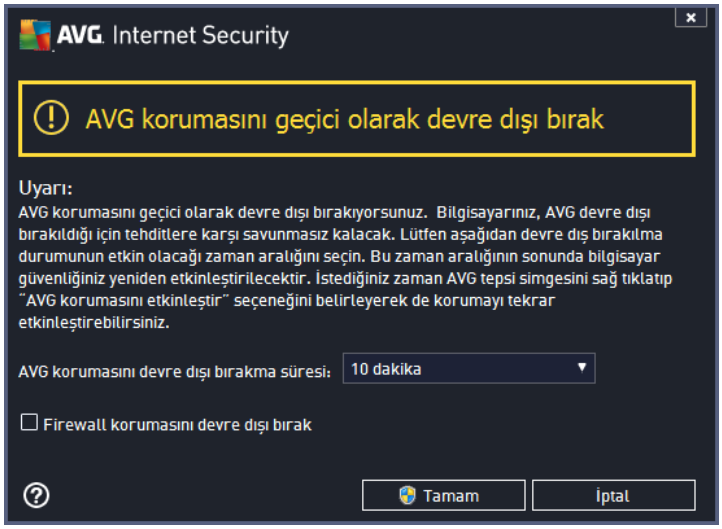


Çogu durumda, yeni yazilimi veya sürücüleri yüklemeden önce ve hatta yükleyici veya yazilim sihirbazi yükleme islemi sirasinda istenmeyen kesintilerin olmamasini saglamak için çalisan program ve uygulamalarin kapatilmasini önerse bile **AVG Internet Security 2014** uygulamasini devre disi birakmak ***gerekmez***. Yükleme sirasinda gerçekten sorunlar yasiyorsaniz, öncelikle yerlesik korumayi devre disi birakmayi deneyin (*Yerlesik Kalkan'i etkinlestir*). **AVG Internet Security 2014** uygulamasini geçici olarak devre disi birakmaniz gerekirse, isinizi bitirdikten sonra yeniden etkinlestirmeniz gerekir. Virüslerden korunma yaziliminiz devre disi birakilmisken internete veya bir aga baglanirsaniz, bilgisayariniz saldirilara açik durumda olur.

AVG korumasi geçici olarak nasil devre disi birakilir

AVG korumasini geçici olarak devre disi birak onay kutusunu isaretleyin ve ***Uygula*** dügmesine basarak seçiminizi onaylayin. Yeni açilan ***AVG korumasini geçici olarak devre disi birak*** iletisim kutusunda **AVG Internet Security 2014** uygulamanizi ne kadar süreyle devre disi birakmak istediginizi belirleyin. Koruma, varsayilan olarak 10 dakika süreyle kapatilir. Bu süre, yeni bir yazilim yükleme gibi herhangi bir islem için yeterli olacaktir. Daha uzun bir süre de belirleyebilirsiniz, ancak kesinlikle gerekli degilse bu seçenegi kullanmaniz önerilmez. Daha sonra, devre disi birakilan tüm bilesenler yeniden etkinlestirilir. AVG korumasini en uzun süreyle bir sonraki bilgisayar baslatmasina kadar devre disi birakabilirsiniz. ***Firewall*** bilesenini ayri olarak devre disi birakma seçenegi ***AVG***

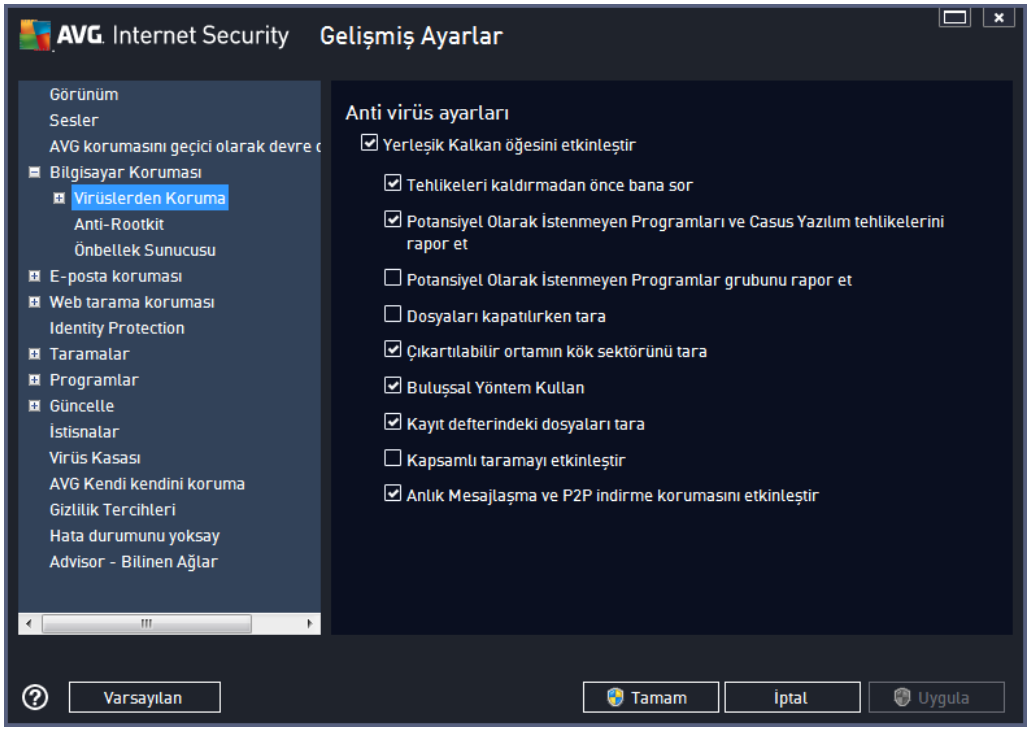
korumasini geçici olarak devre disi birak iletisim kutusunda yer alir. ***Firewall korumasini devre disi birak*** kutusunu isaretleyerek bu islemi gerçeklestirebilirsiniz.



9.4. Bilgisayar Koruması

9.4.1. Virüslerden Koruma

Virüslerden Koruma, ***Yerlesik Kalkan*** ile birlikte bilgisayarinizi bilinen tüm virüs, casus yazilim ve zararli yazilimlara karsi sürekli olarak korur *(uyuyan veya aktif hale geçmemis, yani indirilmis ancak henüz etkin hale geçmemis zararli yazilimlar da dahil)*.



Yerlesik Kalkan ayarlari iletisim kutusunda yerlesik kalkan korumasini ***Yerlesik Kalkan'i etkinlestir*** ögesini isaretleyerek ya da isaretini kaldirarak etkinlestirebilir ya da devre disi birakabilirsiniz (*bu seçenek varsayilan olarak açiktir*). Ayrica yerlesik kalkanin hangi özelliklerinin etkinlestirilecegini seçebilirsiniz:

- ***Tehlikeleri kaldirmadan önce bana sor*** (*varsayilan olarak açik*) - Yerlesik Kalkan'in hiçbir islemi otomatik olarak yapmamasi; bunun yerine, tespit edilen tehlikeyi ne yapacaginiza karar vermeniz için göstermesini saglamak için isaretleyin. Kutuyu isaretlemezseniz, **AVG Internet Security 2014** bulasmayi otomatik olarak temizler; bu mümkün degilse nesne Virüs Kasasi'na tasinir.

- ***Potansiyel Olarak Istenmeyen Programlari ve Casus Yazilim tehlikelerini rapor et*** (*varsayilan olarak açik*) - virüslerin yani sira casus yazilimlari da taramak için isaretleyin. Casus yazilim, süpheli kötü amaçli yazilim kategorisini ifade eder: genellikle bir güvenlik riskini olusturmasina ragmen bu programlardan bazilari bilerek yüklenebilir. Bilgisayarinizin güvenligini artirdigindan, bu özelligi etkin durumda tutmanizi öneririz.

- ***Potansiyel Olarak Istenmeyen Programlar grubunu rapor et*** (*varsayilan olarak kapali*) - casus yazilimlarin, yani dogrudan üreticiden alinan tamamen zararsiz olan, ancak daha sonra kötüye kullanilabilecek programlarin genisletilmis paketinin tespit edilmesi için isaretleyin. Bu, bilgisayarinizin güvenligini daha da artiran ek bir önlemdir, ancak yasal programlari da engelleyebildiginden varsayilan olarak kapalidir.

- ***Dosyalari kapatilirken tara*** (*varsayilan olarak kapali*) - islem sonunda tarama, AVG'nin etkin nesneleri hem açilirlarken hem da kapatilirlarken taradigindan emin olmanizi saglar. Bunun yani sira bu özellik, bilgisayarinizi karmasik virüslere karsi korumaniza da yardimci olur.

- ***Çikartilabilir ortamin kök sektörünü tara*** (*varsayilan olarak açik*)

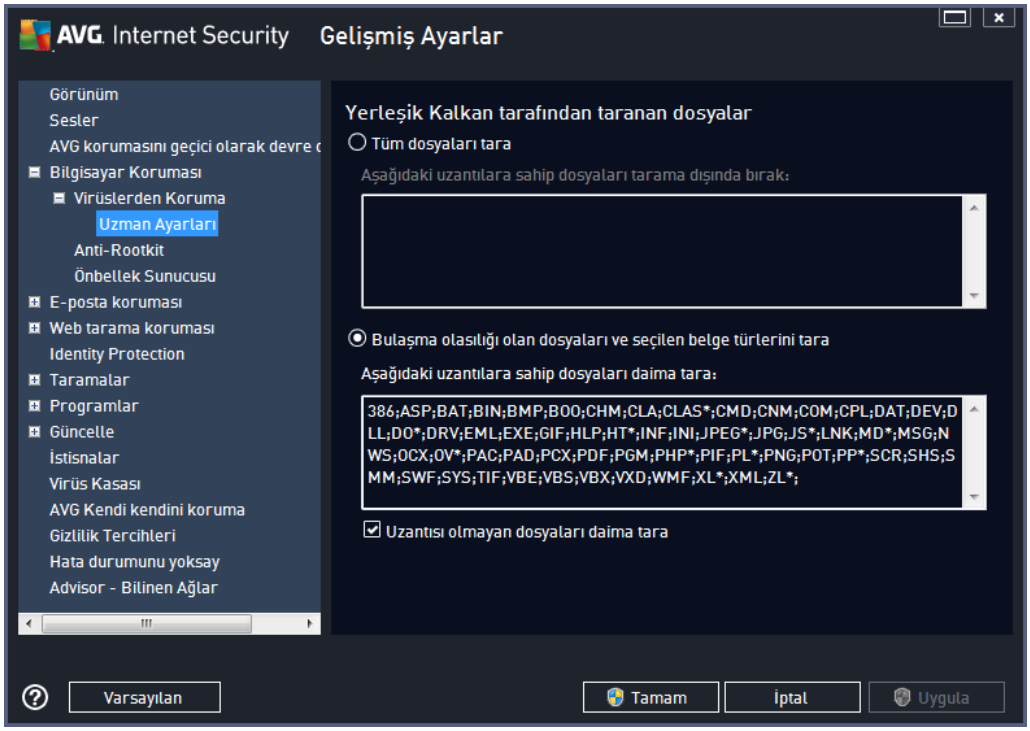
- ***Bulussal Yöntem Kullan*** (*varsayilan olarak açik*) - bulussal analiz, tespit etme islemi sirasinda kullanilir (*taranan nesnenin komutlarinin sanal bilgisayar ortaminda dinamik olarak canlandirilmasi*).

- ***Kayit defterindeki dosyalari tara*** (*varsayilan olarak açik*) - bilinen bulasmanin sonraki bilgisayar baslangicinda çalistirilmasini önlemek için, baslangiç kayit defterine eklenmis tüm çalistirilabilir dosyalari AVG taradigini bu parametre belirtir.

- ***Kapsamli taramayi etkinlestir*** (*varsayilan olarak kapali*) - belirli durumlarda (*çok acil bir durum oldugunda*) nesnelerin derinlemesine islenme olasiligini denetleyecek çok hassas algoritmalari etkinlestirmek için bu seçenegi isaretleyebilirsiniz. Ancak, bu yöntemin çok fazla zaman aldigini unutmayin.

- ***Anlik Mesajlasma korumasini ve P2P indirme korumasini etkinlestir*** (*varsayilan olarak açik*) - anlik mesajlasma iletisimi (*örnegin AIM, Yahoo!, ICQ, Skype, MSN Messenger, ...*) ve Esler Arasi aglar içinde indirilen verilerin *(sunucuya gerek olmaksizin istemciler arasinda dogrudan baglanti saglayan aglar; genellikle müzik dosyalarinin paylasimi için kullanilir ve potansiyel olarak tehlikelidir)* virüssüz oldugunu dogrulamak istiyorsaniz bu ögeyi isaretleyin.

Yerlesik Kalkan Tarafindan Taranan Dosyalar iletisim kutusunda hangi dosyalarin taranacagini yapilandirmak mümkündür (*belirli dosya uzantilarina göre*):



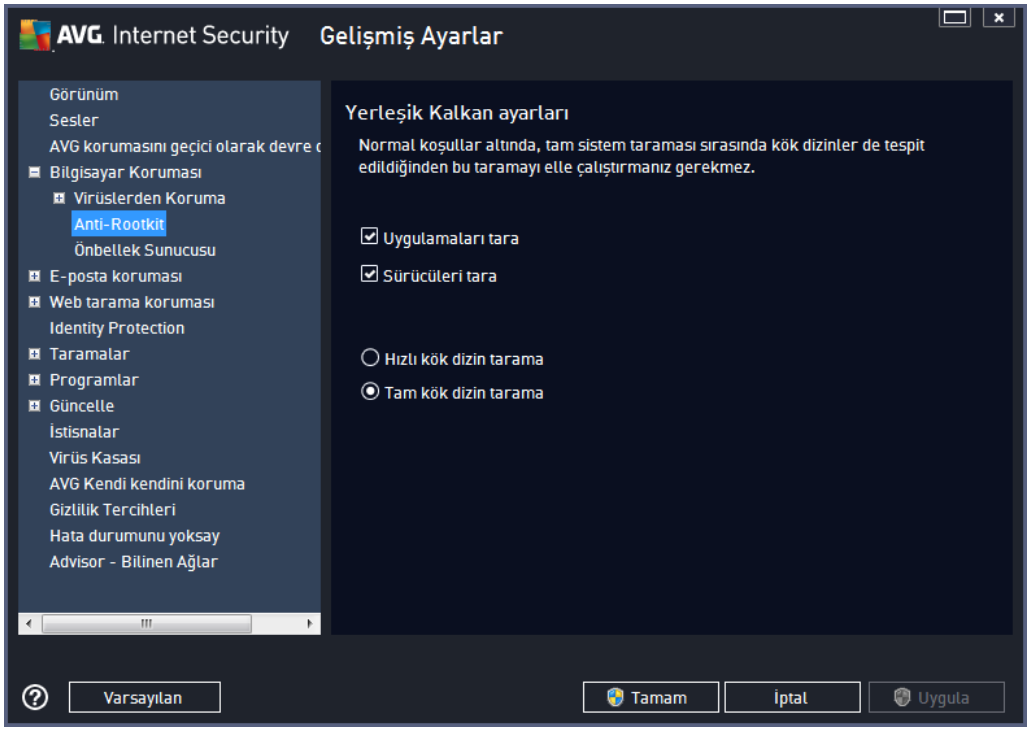
Tüm dosyalari tara veya yalnizca ***Bulasma olasiligi olan dosyalari ve seçilen belge türlerini tara*** seçimi yapmak için ilgili onay kutusunu isaretleyin. Taramayi hizlandirmak ve ayni zamanda maksimum koruma düzeyi saglamak için varsayilan ayarlari korumanizi öneririz. Bu sayede yalnizca virüs bulasabilecek dosyalar taranir. Iletisim kutusunun ilgili bölümünde taramaya dahil edilen

dosyalari tanimlayan düzenlenebilir bir uzanti listesi bulabilirsiniz.

Uzantisi olmayan ve bilinmeyen biçimdeki dosyalarin da Yerlesik Kalkan ile taranmasini saglamak için ***Uzantisi olmayan dosyalari daima tara*** (*varsayilan olarak açiktir*) seçenegini isaretleyin. Uzantisi olmayan dosyalar süpheli dosyalar oldugundan, bu özelligi her zaman açik tutmanizi öneririz.

9.4.2. Anti-Rootkit

Anti-Rootkit Ayarlari iletisim kutusunda ***Anti-Rootkit*** hizmetinin yapilandirmasini ve anti-rootkit taramasinin belirli parametrelerini düzenleyebilirsiniz. Anti-rootkit taramasi Tüm Bilgisayar Taramasi dahilindeki varsayilan bir islemdir:

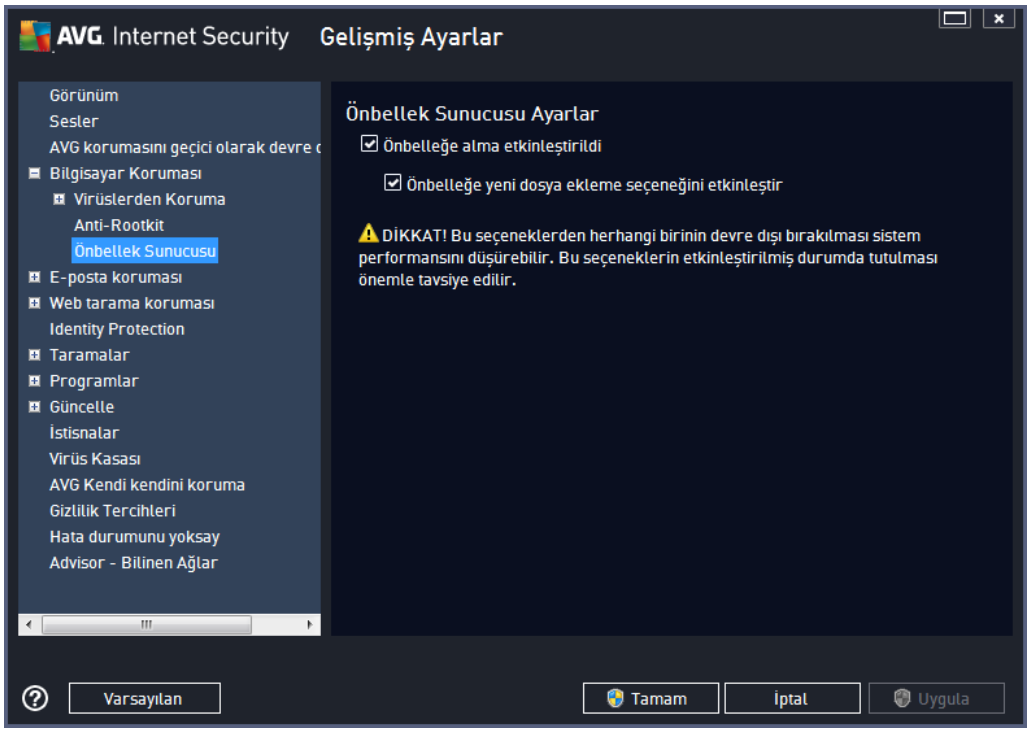


Tarama uygulamalari ve ***Tarama sürücüleri*** anti-rootkit taramasina nelerin dahil edilecegini ayrintili sekilde belirlemenize olanak tanir. Bu ayarlar gelismis kullanicilara yöneliktir; tüm seçenekleri açik konumda muhafaza etmenizi öneririz. Rootkit tarama modunu da seçebilirsiniz:

- ***Hizli kök dizin tarama*** - çalisan tüm islemleri, yüklü sürücüleri ve sistem klasörlerini (*genellikle c:\Windows*) tarar
- ***Tam kök dizin tarama*** - çalisan tüm islemleri, yüklü sürücüleri, sistem klasörünü (*genellikle c:\Windows*), ayrica tüm yerel diskleri (*flash disk dahil, ancak disket/CD sürücüleri hariç*) tarar

9.4.3. Önbellek Sunucusu

Önbellek Sunucusu Ayarlari iletisim kutusu tüm **AVG Internet Security 2014** tarama türlerini hizlandirmak için tasarlanan önbellek sunucusu sürecini isaret eder:



Önbellek sunucusu güvenilir dosyalarin bilgilerini toplar ve saklar (*bir dosya güvenilir bir kaynak tarafindan dijital imza ile imzalandiginda güvenilir sayilir*). Böylece bu dosyalar otomatik olarak güvenli varsayilir ve yeniden taranmalarina gerek duyulmaz; bu nedenle tarama sirasinda bu dosyalar atlanir.

Önbellek Sunucusu Ayarlari iletisim kutusu asagidaki yapilandirma seçeneklerini sunar:

- ***Önbellege alma etkin*** (*varsayilan olarak açiktir*) - ***Önbellek Sunucusu***'nu kapatmak için kutunun isareti kaldirin ve önbellek bellegini bosaltin. Lütfen, kullanimdaki her bir dosya virüs ve casus yazilim için ilk kez taranacagindan taramanin yavas olabilecegini ve bilgisayarinizin genel performansinin azalacagini unutmayin.

- ***Önbellege yeni dosyalarin eklenmesini etkinlestir*** (*varsayilan olarak açiktir*) - önbellege daha fazla dosya eklenmesini durdurmak için kutunun isaretini kaldirin. Önceden önbellege alinmis her dosya korunacak ve önbellege alma tamamen kapatilincaya kadar veya virüs veritabaninin bir sonraki güncellenmesine kadar kullanilacaktir.

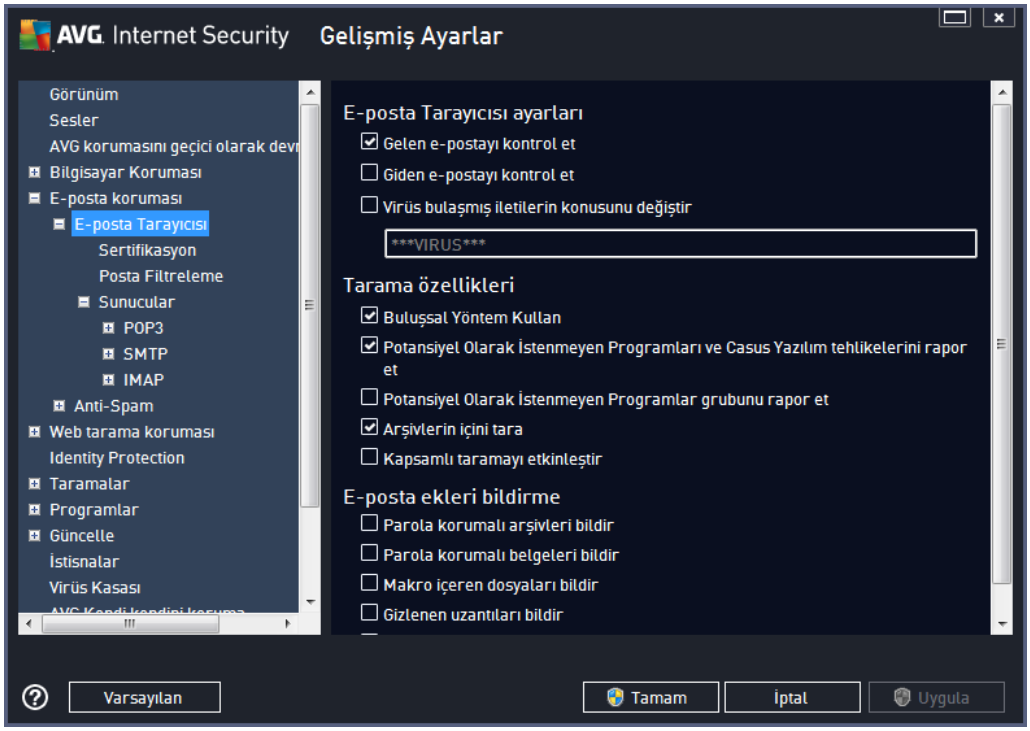
Önbellek sunucusunu kapatmak için iyi bir nedeniniz yoksa, kesinlikle varsayilan ayarlari muhafaza etmenizi ve seçenegin açik kalmasini öneririz! Aksi durumda, sistem hizi ve performansinda ciddi bir düsüs görebilirsiniz.

9.5. E-Posta Tarayıcısı

Bu bölümde E-posta Tarayicisi ve Anti-Spam için ayrintili yapilandirmalar düzenleyebilirsiniz:

9.5.1. E-Posta Tarayıcısı

E-Posta Tarayicisi iletisim kutusu üç bölüme ayrilmistir:



E-posta tarama

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

- ***Gelen e-postayi denetle*** (*varsayilan olarak açik*) - e-posta istemcinize gelen tüm e-postalari tarama seçenegini açmak/kapatmak için isaretleyin
- ***Giden e-postayi denetle*** (*varsayilan olarak kapali*) - hesabinizdan gönderilen tüm e-postalari tarama seçenegini açmak/kapatmak için isaretleyin
- ***Virüs bulasmis iletilerin konusunu degistir*** (*varsayilan olarak kapali*) - taranan e-posta iletisinin bulasmis olarak tespit edilmesi durumunda size bildirilmesini istiyorsaniz, bu ögeyi isaretleyin ve metin alanina istediginiz metni yazin. Ardindan bu metin, daha kolay tanimlanmasi ve filtrelenmesi için tespit edilen her e-posta iletisinin "Konu" alanina eklenecektir. Varsayilan deger ***VIRUS*** olarak belirlenmistir ve bu degeri korumanizi öneririz.

Tarama özellikleri

Bu bölümde, e-posta iletilerinin nasil taranacagini belirleyebilirsiniz:

- ***Bulussal Yöntem Kullan*** (*varsayilan olarak açik*) - e-posta iletilerini tararken bulussal tespit yöntemi kullanmak için isaretleyin. Bu seçenek açik oldugunda, e-posta eklerini yalnizca uzantiya göre filtrelemezsiniz; ekin gerçek içerigi de göz önünde bulundurulur. Filtreleme islemi Posta Filtreleme iletisim kutusundan ayarlanabilir.

- ***Potansiyel Olarak Istenmeyen Programlari ve Casus Yazilim tehditlerini rapor et*** (*varsayilan olarak açik*) - virüslerin yani sira casus yazilimlari da taramak için isaretleyin. Casus yazilim, süpheli kötü amaçli yazilim kategorisini ifade eder: genellikle bir güvenlik riskini olusturmasina ragmen bu programlardan bazilari bilerek yüklenebilir. Bilgisayarinizin güvenligini artirdigindan, bu özelligi etkin durumda tutmanizi öneririz.

- ***Potansiyel Olarak Istenmeyen Programlar gelismis grubunu rapor et*** (varsayilan olarak kapali) - casus yazilimlarin, yani dogrudan üreticiden alinan tamamen zararsiz olan, ancak daha sonra kötüye kullanilabilecek programlarin genisletilmis paketlerinin tespit edilmesi için isaretleyin. Bu, bilgisayar güvenliginizi daha da artiran ek bir önlemdir, ancak yasal programlari da engelleyebilir ve bu yüzden varsayilan olarak kapalidir.

- ***Arsivlerin içini tara*** (*varsayilan olarak açik*) - e-posta iletilerine eklenen arsivlerin içeriklerini taramak için isaretleyin.

- ***Kapsamli taramayi etkinlestir*** (*varsayilan olarak kapali*) - belirli durumlarda (*örnegin, bilgisayariniza virüs bulastigindan veya saldiri oldugundan süpheleniliyorsa*) yalnizca emin olmak üzere bilgisayarinizin bulasma olmasi çok zor olan alanlarini bile tarayan en kapsamli tarama algoritmalarini etkinlestirmek için bu seçenegi isaretleyebilirsiniz. Ancak, bu yöntemin çok fazla zaman aldigini unutmayin.

E-posta ekleri bildirme

Bu bölümde, potansiyel olarak tehlikeli ve süpheli olan dosyalar için ek raporlar ayarlayabilirsiniz. Lütfen bir uyari iletisim kutusu görüntülenmeyecegini unutmayin. Yalnizca e-posta iletisinin sonuna bir onay metni eklenir ve bu tür raporlarin tümü E-posta Korumasi tespiti iletisim kutusunda listelenir:

- ***Parola korumali arsivleri bildir*** - parolayla korunan arsivler (*ZIP, RAR vb.*) virüslere karsi taranamaz; bunlarin potansiyel olarak tehlikeli olduklarini bildirmek için kutuyu isaretleyin.

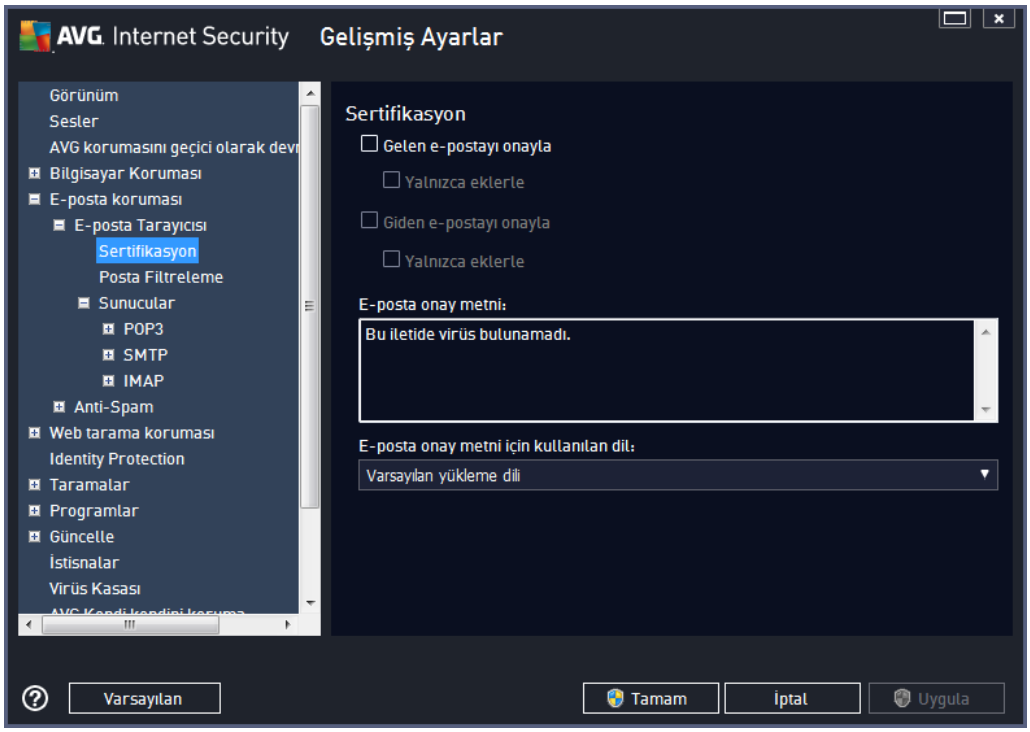
- ***Parola korumali belgeleri bildir*** - parolayla korunan belgeler virüslere karsi taranamaz; bunlarin potansiyel olarak tehlikeli olduklarini bildirmek için kutuyu isaretleyin.

- ***Makro içeren dosyalari bildir*** - Makro, bazi görevlerin kullanici için daha kolay hale getirilmesini amaçlayan önceden tanimlanmis adimlar dizisidir (*MS Word makrolari yaygin olarak bilinir*). Makro, potansiyel olarak tehlikeli talimatlar içerebilir. Makro içeren dosyalarin süpheli olarak bildirilmesini saglamak için kutuyu isaretleyebilirsiniz.

- ***Gizlenen uzantilari bildir*** - gizli uzantilar süpheli bir çalistirilabilir dosyayi (örn. "birsey.txt.exe") zararsiz bir düz metin dosyasi gibi (örn. "birsey.txt") gösterebilir; bunlari potansiyel olarak tehlikeli olarak bildirmek için kutuyu isaretleyin.

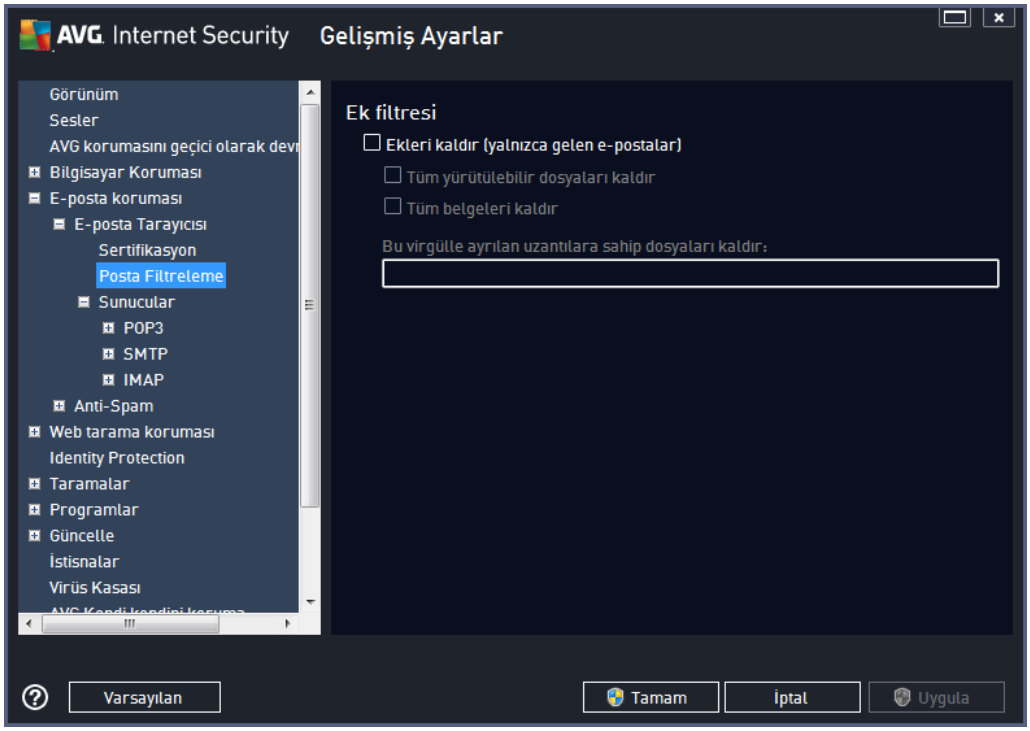
- ***Rapor edilen ekleri Virüs Kasasina tasi*** - taranan e-posta iletisinin ekinde gizli bir eklenti tespit edildiginde parola korumali arsivler, parola korumali belgeler, makro içeren dosyalar ve/veya gizli uzantili dosyalar hakkinda e-posta vasitasiyla bilgilendirilmek isteyip istemediginizi belirtin. Tarama islemi sirasinda bu tür bir mesaj tespit edilirse tespit edilen bulasmis nesnenin Virüs Kasasi'na tasinmasini isteyip istemediginizi belirtin.

Sertifika iletisim kutusunda gelen (***Gelen e-postayi onayla***) ve/veya giden e-postalari onaylamaya (***Giden e-postayi onayla***) veya onaylamamaya karar vermek için çesitli onay kutularini isaretleyebilirsiniz. Bu seçeneklerin her biri için ***Yalnizca ekleri olanlar*** parametresini isaretleyip onayin yalnizca ekleri olan e-postalara eklenmesini saglayabilirsiniz:



Varsayilan olarak, onay mesaji sunun gibi temel bilgiler içerir:*Bu iletide virüs bulunamadi.* Ancak, bu bilgiler ihtiyaçlariniza göre artirilabilir veya degistirilebilir: ***E-posta onay metni*** alanina istediginiz onay metnini yazin. ***E-posta onay metni için kullanilan dil*** bölümünde onayin otomatik olarak olusturulan kisminin (*Bu iletide virüs bulunamadi*) hangi dilde görüntülenecegini de belirleyebilirsiniz.

Not: *Istenen dilde yalnizca varsayilan metnin görüntülenecegine ve özellestirilmis metninizin otomatik olarak çevrilmeyecegine dikkat edin!*



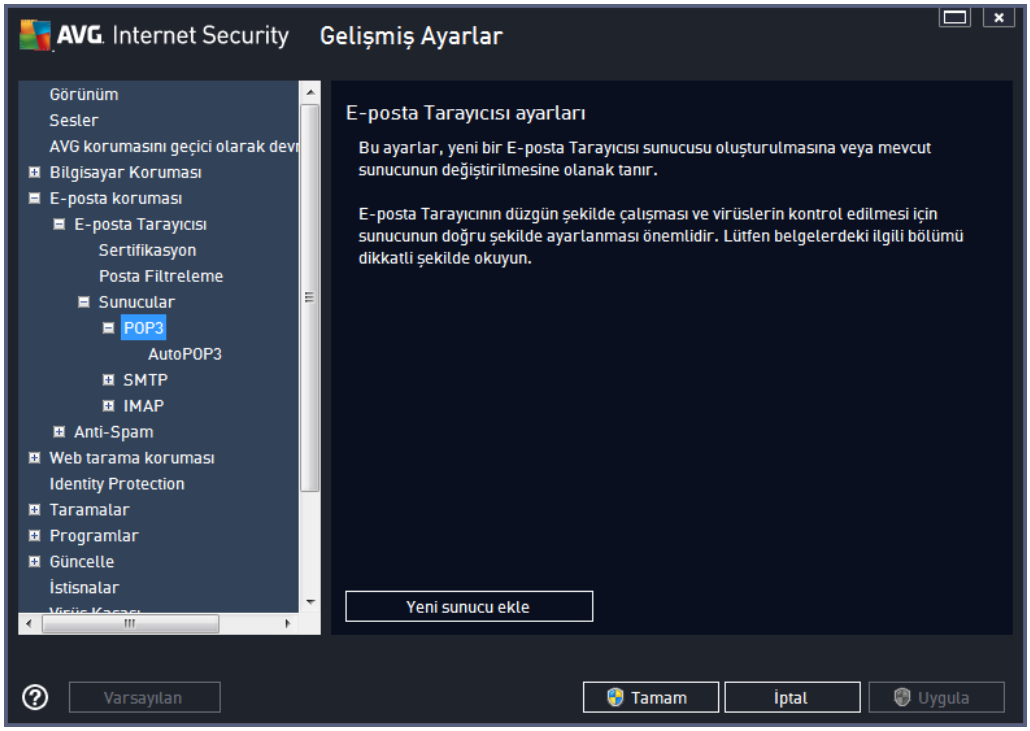
Ek filtresi iletisim kutusu, e-posta mesajlarinin eklerinin taranmasina iliskin parametreleri ayarlayabilmenizi saglar.Varsayilan olarak ***Eklentileri sil*** seçenegi kapalidir. Etkinlestirmeye karar verirseniz tüm e-posta mesajlarinin eklentileri, bulasmis nesne ya da potansiyel olarak tehlikeli nesne olarak algilanacak ve silinecektir. Belirli ek türlerinin silinmesini istiyorsaniz ilgili seçenegi seçin:

- ***Tüm çalistirilabilir dosyalari sil*** - tüm *.exe dosyalari silinecektir
- ***Tüm belgeleri kaldir*** - tüm *.doc, *.docx, *.xls, *.xlsx dosyalari silinecektir
- ***Virgülle ayrilmis su uzantilara sahip dosyalari kaldir*** - Tanimlanan uzantilara sahip tüm dosyalar kaldirilacaktir

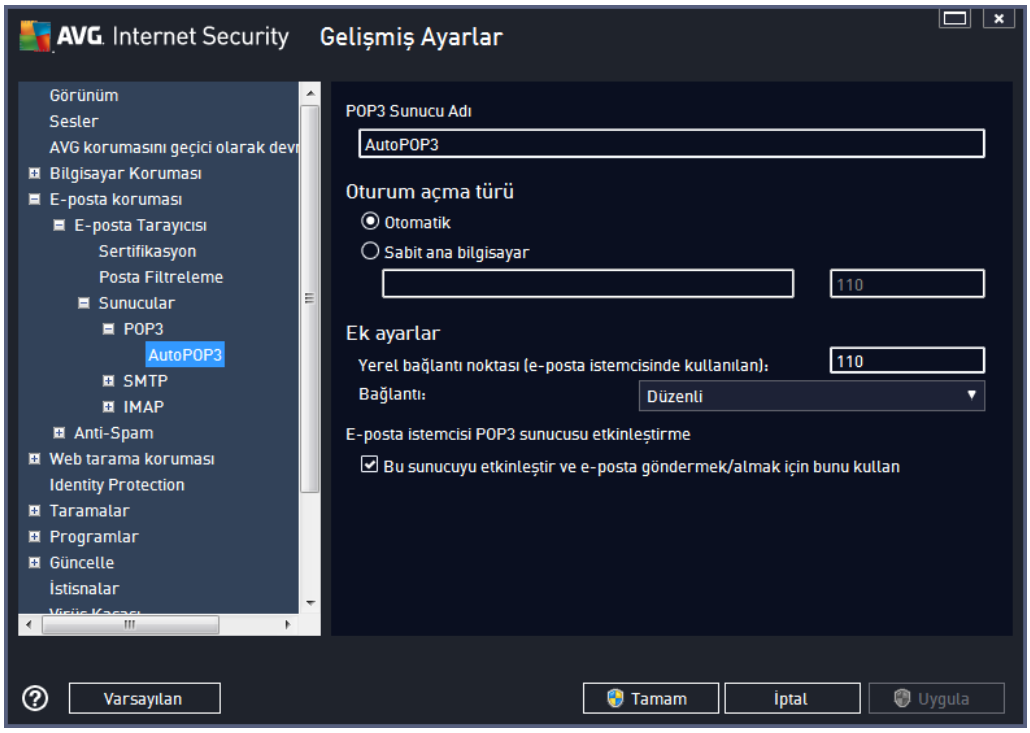
Sunucular bölümünde E-posta Tarayicisi sunucularinin parametrelerini düzenleyebilirsiniz:

- POP3 sunucusu
- SMTP sunucusu
- IMAP sunucusu

Ayrica, ***Yeni sunucu ekle*** dügmesiyle gelen ve giden postalar için yeni sunucular tanimlayabilirsiniz.



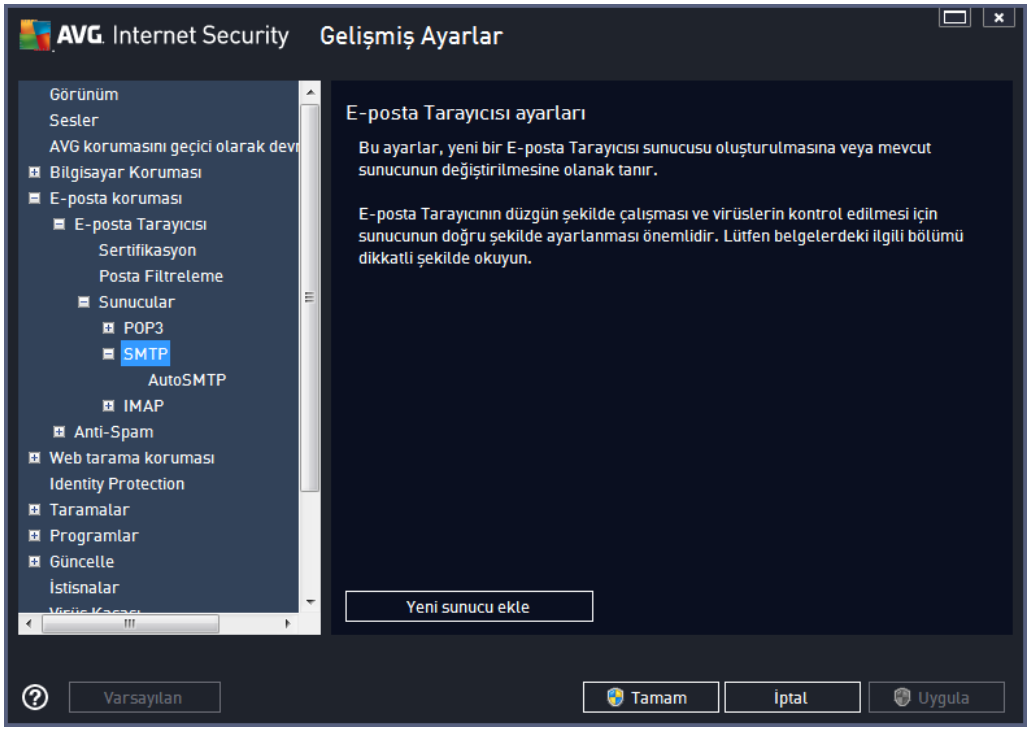
Bu iletisim kutusunda gelen postalar için POP3 protokolünü kullanarak yeni bir E-posta Tarayicisi sunucusu kurabilirsiniz:



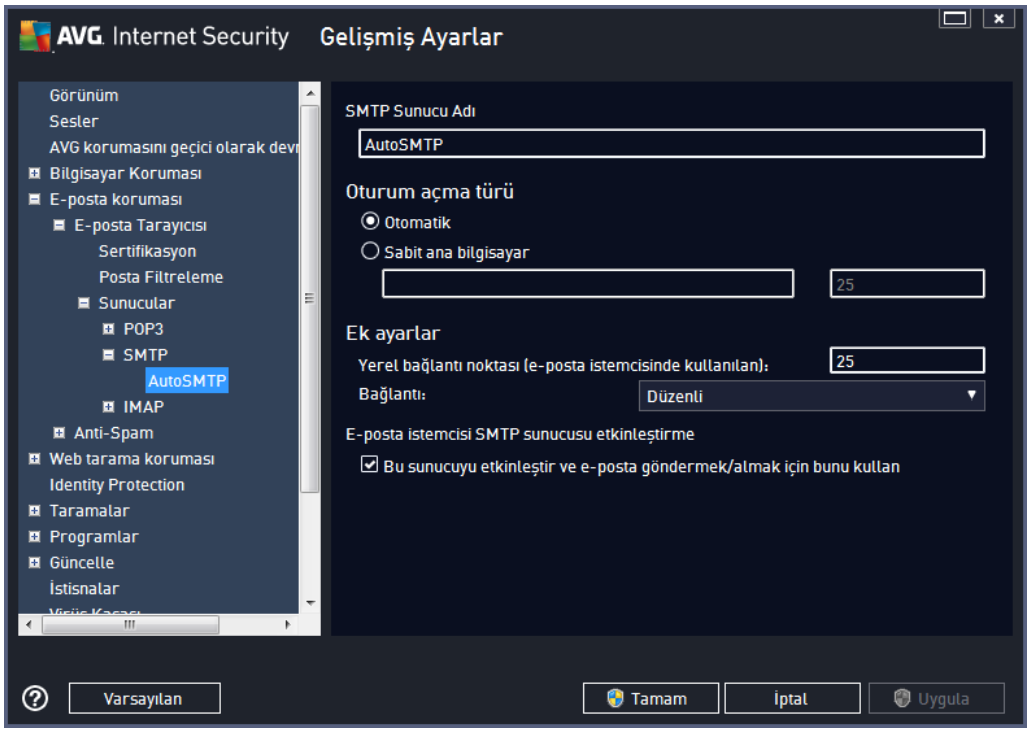
- ***POP3 Sunucusunun Adi*** - bu alanda yeni eklenen sunucularin adini belirtebilirsiniz (*bir*

POP3 sunucusu eklemek için, sol menü agacinin POP3 ögesinin üzerinde sag fare dügmesini tiklatin). Otomatik olarak olusturulan "AutoPOP3" sunuculari için bu alan devre disi birakilmistir.

- ***Oturum Açma Tipi*** - gelen postalar için kullanilan posta sunucusunu belirleme yöntemini tanimlar:
    - ***Otomatik*** - oturum açma islemi, e-posta istemcinizin ayarlarina göre otomatik olarak gerçeklestirilir.
    - ***Sabit ana bilgisayar*** - bu durumda, program her zaman burada belirtilen sunucuyu kullanir. Lütfen posta sunucunuzun adresini veya adini belirtin. Oturum açma adi degismez. Ad için, IP adresinin yani sira (*örnegin, 123.45.67.89*) etki alani adi da (*örnegin, pop.acme.com*) kullanabilirsiniz. Posta sunucusu standart olmayan bir baglanti noktasi kullaniyorsa, bu baglanti noktasini ayirici olarak iki nokta üst üste kullanarak sunucu adinin arkasina yazabilirsiniz (*örn. smtp.acme.com:8200*). POP3 iletisimi için standart baglanti noktasi 110'dur.
- ***Diger Ayarlar*** - daha ayrintili parametreleri belirler:
    - ***Yerel baglanti noktasi*** - Posta uygulamanizin iletisim kurmasi beklenen baglanti noktasini belirler. Posta uygulamanizda, bu baglanti noktasini POP3 iletisimi baglanti noktasi olarak belirtmeniz gerekir.
    - ***Baglanti*** - *kullanilacak baglanti türünü asagi açilir menüden belirtebilirsiniz (normal/ SSL/SSL varsayilan*). SSL baglantiyi tercih ederseniz, gönderilen veri, üçüncü bir taraf tarafindan izlenme riski olmayacak sekilde sifrelenir. Bu özellik de, yalnizca hedef posta sunucusu tarafindan desteklendiginde kullanilabilir.
- ***E-posta Istemcisi POP3 Sunucusunu Etkinlestirme*** - belirtilen POP3 sunucusunu etkinlestirmek veya devre disi birakmak için bu ögeyi isaretleyin veya ögenin isaretini kaldirin.



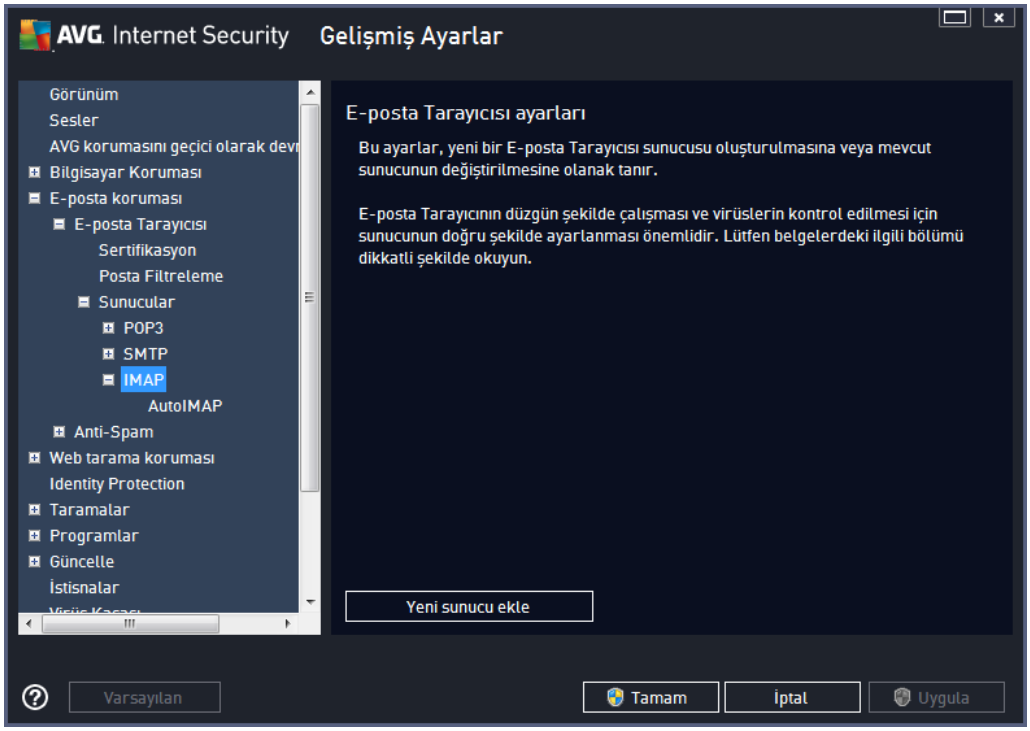
Bu iletisim kutusunda giden postalar için SMTP protokolünü kullanarak yeni bir E-posta Tarayicisi sunucusu kurabilirsiniz:



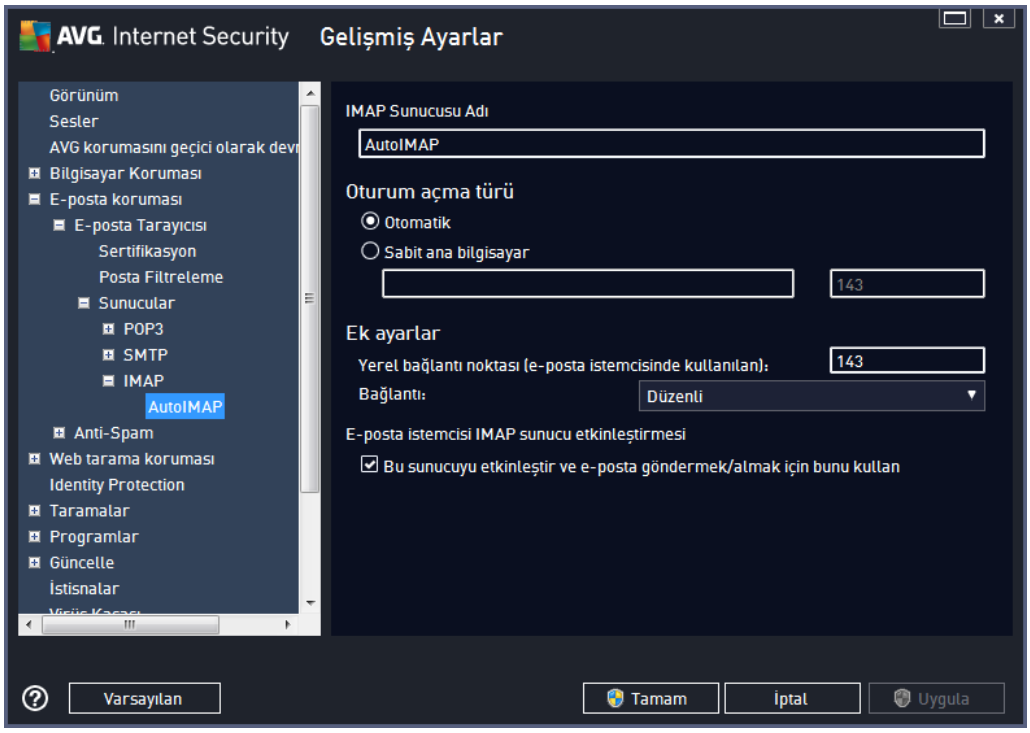
- ***SMTP Sunucusunun Adi*** - bu alanda yeni eklenen sunucularin adini belirtebilirsiniz (*bir*

SMTP sunucusu eklemek için, sol menü agacinin SMTP ögesinin üzerinde sag fare dügmesini tiklatin). Otomatik olarak olusturulan "AutoSMTP" sunuculari için bu alan devre disi birakilmistir.

- ***Oturum Açma Tipi*** - giden postalar için kullanilan posta sunucusunu belirleme yöntemini tanimlar:
    - ***Otomatik*** - oturum açma islemi, e-posta istemcinizin ayarlarina göre otomatik olarak gerçeklestirilir.
    - ***Sabit ana bilgisayar*** - bu durumda, program her zaman burada belirtilen sunucuyu kullanir. Lütfen posta sunucunuzun adresini veya adini belirtin. Ad için, IP adresinin yani sira (*örnegin, 123.45.67.89*) etki alani adi da (*örnegin, smtp.acme.com*) kullanabilirsiniz. *Posta sunucusu standart olmayan bir baglanti noktasi kullaniyorsa, bu baglanti noktasini ayirici olarak iki nokta üst üste kullanarak sunucu adinin arkasina girebilirsiniz (örn. smtp.acme.com:8200*). SMTP iletisimi için standart baglanti noktasi 25'tir.
- ***Diger Ayarlar*** - daha ayrintili parametreleri belirler:
    - ***Yerel baglanti noktasi*** - Posta uygulamanizin iletisim kurmasi beklenen baglanti noktasini belirler. Posta uygulamanizda, bu baglanti noktasini SMTP iletisimi baglanti noktasi olarak belirtmeniz gerekir.
    - ***Baglanti*** - bu açilir asagi menüden, kullanilacak baglanti türünü belirtebilirsiniz (*normal/SSL/SSL varsayilan*). SSL baglantiyi tercih ederseniz, gönderilen veri, üçüncü bir taraf tarafindan izlenme riski olmayacak sekilde sifrelenir. Bu özellik, yalnizca hedef posta sunucusu tarafindan desteklendiginde kullanilabilir.
- ***E-posta Istemcisi SMTP Sunucusunu Etkinlestirme*** - yukarida belirtilen SMTP sunucusunu etkinlestirmek/devre disi birakmak için bu kutuyu isaretleyin veya kutunun isaretini kaldirin



Bu iletisim kutusunda giden postalar için IMAP protokolünü kullanarak yeni bir E-posta Tarayicisi sunucusu kurabilirsiniz:

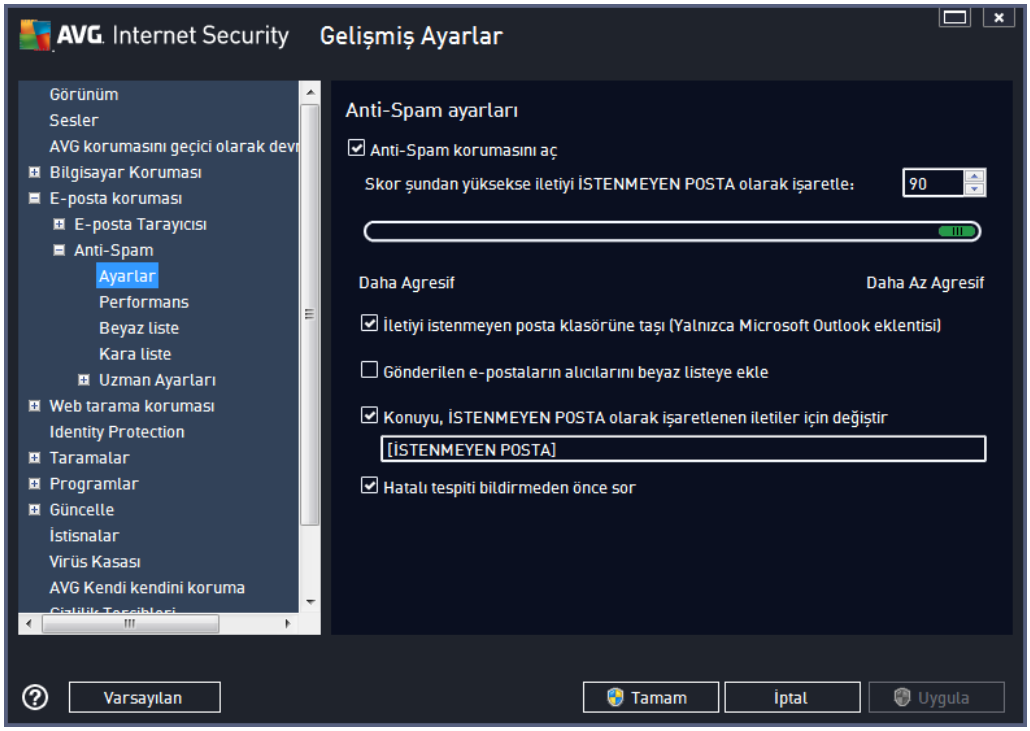


- ***IMAP Sunucusunun Adi*** - bu alanda yeni eklenen sunucularin adini belirtebilirsiniz (*bir*

IMAP sunucusu eklemek için, sol menü agacinin IMAP ögesinin üzerinde sag fare dügmesini tiklatin). Otomatik olarak olusturulan "AutoIMAP" sunuculari için bu alan devre disi birakilmistir.

- ***Oturum Açma Tipi*** - giden postalar için kullanilan posta sunucusunu belirleme yöntemini tanimlar:
    - ***Otomatik*** - oturum açma islemi, e-posta istemcinizin ayarlarina göre otomatik olarak gerçeklestirilir.
    - ***Sabit ana bilgisayar*** - bu durumda, program her zaman burada belirtilen sunucuyu kullanir. Lütfen posta sunucunuzun adresini veya adini belirtin. Ad için, IP adresinin yani sira (*örnegin, 123.45.67.89*) etki alani adi da (*örnegin, smtp.acme.com*) kullanabilirsiniz. Posta sunucusu standart olmayan bir baglanti noktasi kullaniyorsa, bu baglanti noktasini ayirici olarak iki nokta üst üste kullanarak sunucu adinin arkasina yazabilirsiniz (*örnegin, smtp.acme.com:8200*). IMAP iletisiminin standart baglanti noktasi 143'tür.
- ***Diger Ayarlar*** - daha ayrintili parametreleri belirler:
    - ***Kullanilan yerel baglanti noktasi*** - posta uygulamanizin iletisim kurmasi beklenen baglanti noktasini belirler. Bundan sonra, posta uygulamanizda, bu baglanti noktasini IMAP iletisimi baglanti noktasi olarak belirtmeniz gerekir.
    - ***Baglanti*** - bu açilir asagi menüden, kullanilacak baglanti türünü belirtebilirsiniz (*normal/SSL/SSL varsayilan*). Bir SSL baglantisini tercih ederseniz, gönderilen veri, üçüncü bir taraf tarafindan izlenme riski olmayacak sekilde sifrelenir. Bu özellik, yalnizca hedef posta sunucusu tarafindan desteklendiginde kullanilabilir.
- ***E-posta Istemcisi IMAP Sunucusunu Etkinlestirme*** - yukarida belirtilen IMAP sunucusunu etkinlestirmek/devre disi birakmak için bu kutuyu isaretleyin veya kutunun isaretini kaldirin

9.5.2. Anti-Spam



Anti-Spam Ayarlari iletisim kutusunda ***Anti-Spam korumasini aç*** onay kutusunu isaretleyerek veya bu kutunun isaretini kaldirarak e-posta iletisiminin anti-spam taramasina izin verebilir ya da taramayi engelleyebilirsiniz. Bu seçenek varsayilan olarak açiktir ve geçerli bir neden olmadikça her zaman bu yapilandirmayi korumaniz önerilir.

Sonra, daha fazla ya da daha az agresif degerlendirme ölçütleri de seçebilirsiniz. ***Istenmeyen Posta Önleme*** filtresi, çesitli dinamik tarama teknikleri sayesinde mesajlardan her birine bir puan verir (*mesajin içeriginin ISTENMEYEN POSTA'ya ne kadar yakin oldugunu belirlemek üzere*). Deger girerek ya da kaydirma çubugunu saga ya da sola hareket ettirerek (*deger araligi 50 ile 90 arasindadir*) ***Skor sundan yüksekse iletiyi ISTENMEYEN POSTA olarak isaretle*** ögesini ayarlayabilirsiniz.

Genel olarak egisi 50 ila 90 arasinda bir degere ayarlamanizi veya gerçekten emin degilseniz 90 olarak ayarlamanizi öneririz. Burada puan esigi hakkinda genel bilgi verilmektedir:

- ***Deger 80-90*** - istenmeyen posta olmasi muhtemel e-posta mesajlari filtrelenecektir. Istenmeyen posta olmayan bazi postalar yanlislikla istenmeyen posta seklinde etiketlenebilir.
- ***Deger 60-79*** - oldukça etkili bir yapilandirma olarak degerlendirilir. Istenmeyen posta olmasi muhtemel e-posta mesajlari filtrelenecektir. Istenmeyen posta olmayan mesajlarin da yakalanma ihtimali vardir.
- ***Deger 50-59*** - çok etkili yapilandirma. Istenmeyen posta olmayan e-posta iletilerinin de gerçek istenmeyen posta iletileri ile birlikte yakalanma ihtimali çok yüksektir. ***Bu esik araligi normal kullanim için önerilmez.***

Anti-Spam ayarlari iletisim kutusunda, tespit edilen istenmeyen postalara ne yapilacagini da

belirleyebilirsiniz:

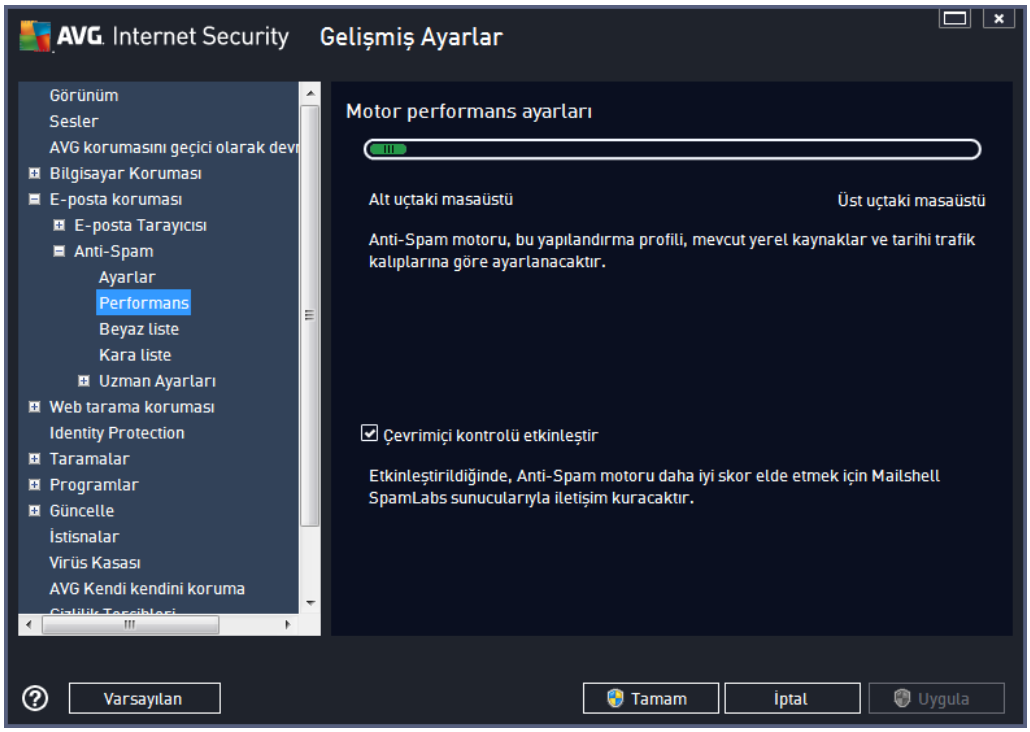
- ***Iletiyi istenmeyen posta klasörüne tasi*** *(yalnizca Microsoft Outlook eklentisi)* - algilanan istenmeyen mesajlarin, otomatik olarak MS Outlook e-posta istemcinizin önemsiz posta klasörüne tasinmasini istiyorsaniz bu onay kutusunu isaretleyin. Su anda, özellik diger posta istemcilerinde desteklenmiyor.

- ***Gönderilen e-postalarin göndericilerini beyaz listeye*** ekle - gönderilen e-postalarin göndericilerinin tümüne güvendiginizi onaylamak ve söz konusu kisilerin e-posta hesaplarindan gönderilen e-postalarin daima alinmasini istediginizi teyit etmek için bu kutuyu isaretleyin.

- ***Konuyu, ISTENMEYEN POSTA olarak isaretlenen iletiler için degistir*** - istenmeyen posta olarak isaretlenmis e-postalarin konu alanina belirli bir kelime ya da ibarenin yazilmasini istiyorsaniz bu onay kutusunu isaretleyin; istenen metin, etkinlestirilen metin alanina yazilabilir.

- ***Hatali tespiti bildirmeden önce sor*** - yükleme islemi sirasinda Gizlilik Tercihleri projesine katilmayi kabul etmeniz kosuluyla. Kabul ettiyseniz, tespit edilen tehditlerin AVG'ye bildirilmesine izin verirsiniz. Rapor otomatik olarak olusturulur. Ancak, gerçekten istenmeyen posta olarak siniflandirilmasi gerekip gerekmediginden emin olmak için, tespit edilen istenmeyen posta AVG'ye bildirilmeden önce sorulmasini istediginizi onaylamak için bu onay kutusunu isaretleyebilirsiniz.

Motor Performans Ayarlari iletisim kutusu, (*solda bulunan gezinme alaninda* ***Performans*** *ögesi altinda baglantisi verilen*) ***Anti-Spam*** bileseninin performans ayarlarini sunar:



Tarama performans seviyesini ***Alt uç masaüstü*** / ***Üst uç masaüstü*** modlari arasinda degistirmek için

çubugu sola ya da saga kaydirin.

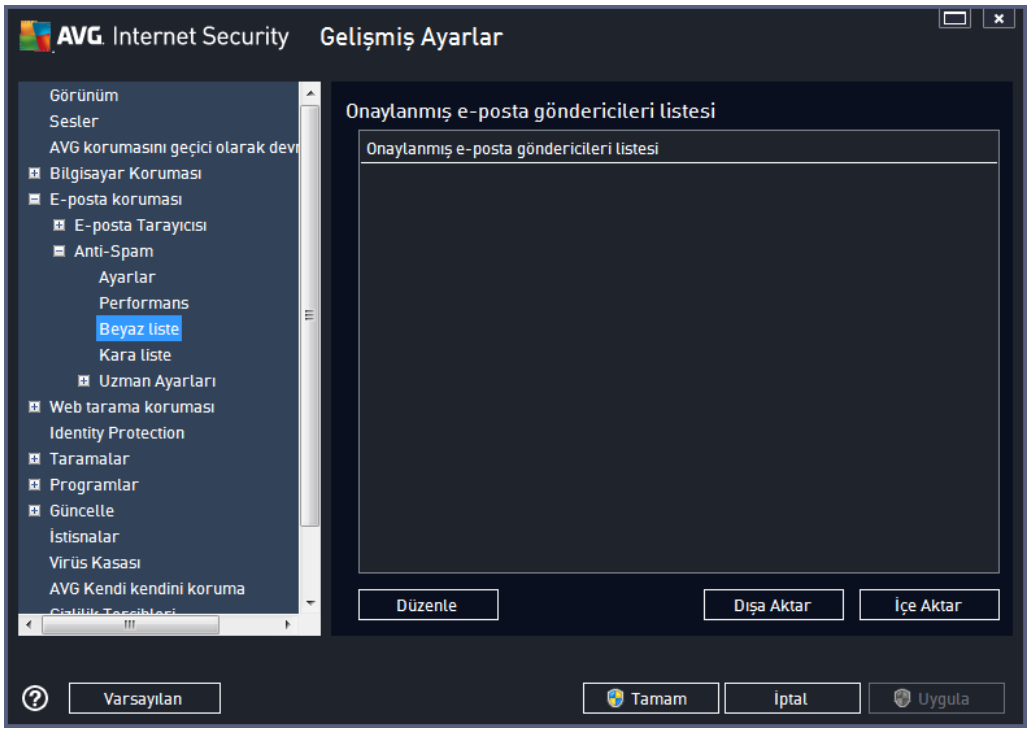
- ***Alt uç masaüstü*** - tarama islemi sirasinda istenmeyen postalarin tespit edilmesi için herhangi bir kural kullanilmayacaktir. Tanimlama için sadece egitim verileri kullanilacaktir. Bu mod, bilgisayar donanimlariniz çok eski degil ise genel kullanim için önerilmemektedir.

- ***Üst uç masaüstü*** - bu mod büyük miktarda bellek tüketir. Tarama islemi sirasinda istenmeyen postalari ayirt etmek için su özellikler kullanilacaktir: kurallar ve istenmeyen posta veritabani önbellegi, temel ve gelismis kurallar, istenmeyen postayi gönderenin IP adresi ve gönderici veritabanlari.

Çevrimiçi taramayi etkinlestir ögesi varsayilan olarak açiktir. Ana sunucular ile iletisim kurmak vasitasiyla istenmeyen postalarin daha hassas sekilde tespit edilmesini saglar. Diger bir deyisle, taranan veriler çevrimiçi Ana veritabanlari ile karsilastirilacaktir.

Genellikle öntanimli ayarlari kullanmaniz ve ancak geçerli bir nedeniniz varsa söz konusu ayarlari degistirmeniz önerilir. Yapilandirma sadece uzman kullanicilar tarafindan degistirilmelidir!

Beyaz Liste ögesi, mesajlari hiçbir zaman istenmeyen posta olarak algilanmayacak olan onaylanan gönderen e-posta adresleri ve etki alani adlarinin genel bir listesini içeren ***Onaylanmis e-posta gönderenleri listesi*** adli bir iletisim kutusu açar.



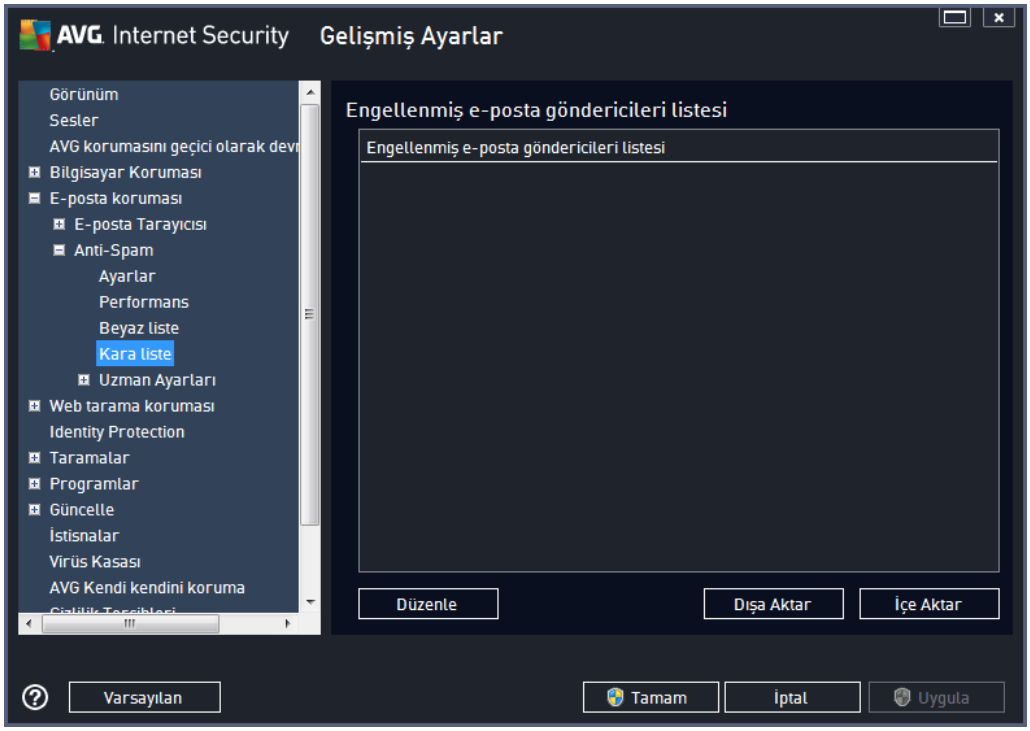
Düzenleme arayüzünde asla istenmeyen posta (istenmeyen posta) göndermeyecek göndericilerden olusan bir liste düzenleyebilirsiniz. Bunun yani sira istenmeyen mesaj göndermedigini bildiginiz tüm etki alani adlarini içeren (*örn. avg.com*) bir liste de olusturabilirsiniz. Söz konusu gönderici ve barindirma adi listelerini tamamladiktan sonra asagidaki yöntemlerden biriyle girebilirsiniz: e-posta adresini dogrudan girerek ya da tüm adres listesini bir kerede içe aktararak.

Kontrol dügmeleri

Su kontrol dügmeleri bulunur:

- ***Düzenle*** - adres listesini manüel olarak doldurabileceginiz iletisim kutusunu açmak için bu dügmeye basin (*bunun yani sira kopyala ve yapistir* yöntemini de kullanabilirsiniz). Satir basina bir öge ekleyin (*gönderen, etki alani adi*).
- ***Disa Aktar*** - Kayitlari belli bir amaçla disa aktarmaya karar verirseniz, bu dügmeye basarak disa aktarabilirsiniz. Tüm kayitlar temel metin dosyasina kaydedilecektir.
- ***Içe aktar*** - hazirladiginiz e-posta adreslerinin/alan adlarinin bulundugu bir metin dosyasina sahipseniz, bu dügmeyi seçerek kolayca içe aktarabilirsiniz. Dosya içeriginin her satir için yalnizca bir öge (*adres, alan adi*) içermesi gerekir.

Kara liste ögesi engellenmis gönderici e-posta adresleri ve iletileri her zaman gereksiz posta olarak isaretlenecek alan adlarinin global bir listesinin bulundugu bir iletisim kutusu açar.



Düzenleme arayüzünde, istenmeyen ileti *(istenmeyen posta)* göndermesini beklediginiz göndericilerin bir listesini olusturabilirsiniz. Ayrica istenmeyen mesajlar beklediginiz veya aldiginiz tam alana adlarinin (*örn. spammingcompany.com*) bir listesini olusturabilirsiniz. Listelenen adreslerden/alan adlarindan gelecek tüm e-postalar istenmeyen posta olarak tanimlanacaktir. Söz konusu gönderici ve/veya etki alani adi listelerini tamamladiktan sonra asagidaki yöntemlerden biriyle girebilirsiniz: e-posta adresini dogrudan girerek ya da tüm adres listesini bir kerede içe aktararak.

Kontrol dügmeleri

Su kontrol dügmeleri bulunur:

- ***Düzenle*** - adres listesini manüel olarak doldurabileceginiz iletisim kutusunu açmak için bu dügmeye basin (*bunun yani sira kopyala ve yapistir* yöntemini de kullanabilirsiniz). Satir basina bir öge ekleyin (*gönderen, etki alani adi*).
- ***Disa Aktar*** - Kayitlari belli bir amaçla disa aktarmaya karar verirseniz, bu dügmeye basarak disa aktarabilirsiniz. Tüm kayitlar düz bir metin dosyasina kaydedilecektir.
- ***Içe aktar*** - mevcut durumda hazirlamis oldugunuz bir gönderici / barindirma adi listesi varsa bu dügmeye basarak söz konusu dosyayi içe aktarabilirsiniz.

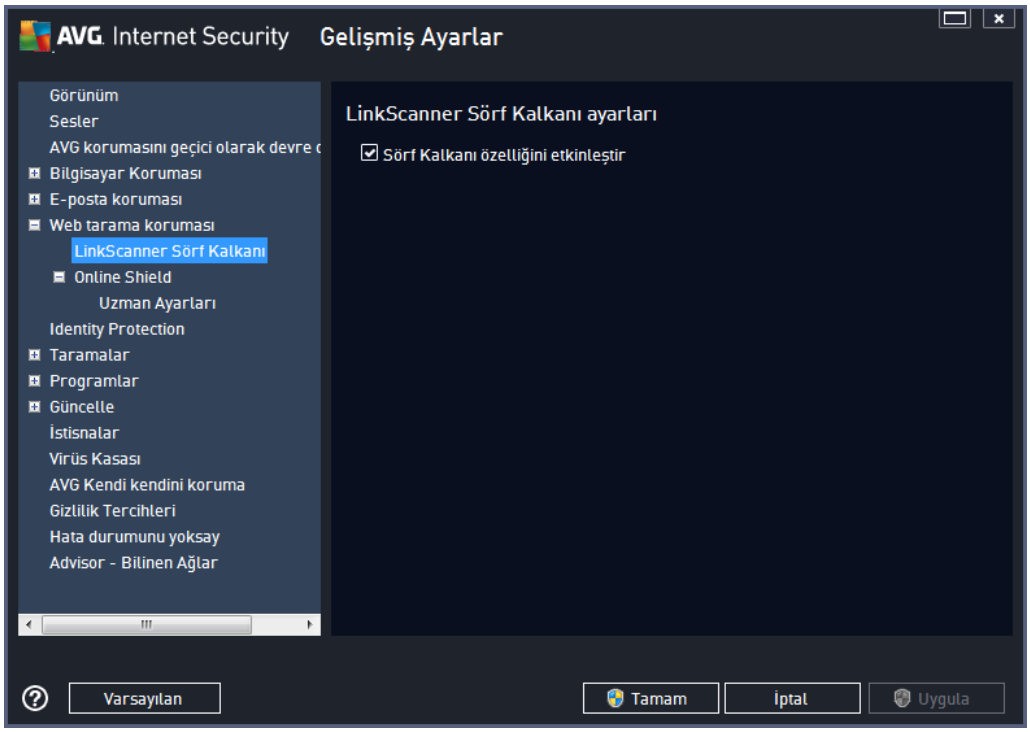
Uzman Ayarlari bölümü Anti-Spam özelligine iliskin kapsamli ayar ve seçenekler sunar. Bu ayarlar özellikle deneyimli kullanicilar, genel olarak e-posta sunuculari için en iyi korumayi saglamak üzere istenmeyen postalardan korunmayi yapilandirmaya gereksinim duyan ag yöneticileri için tasarlanmistir. Bu nedenle, her bir iletisim kutusu için ayrica yardim sunulmamaktadir. Ancak, ilgili her seçenek için kullanici arayüzünde dogrudan kisa bir açiklama bulunmaktadir. Spamcatcher (MailShell Inc.) uygulamasinin gelismis ayarlariyla ilgili bilgileriniz yeterli degilse, kesinlikle hiçbir ayari degistirmemenizi öneririz. Uygun olmayan her degisiklik performansin düsmesine veya bilesenin hatali çalismasina neden olabilir.

Anti-Spam yapilandirmasini gelismis seviyede degistirmeniz gerektigini düsünüyorsaniz lütfen kullanici arayüzünde belirtilen talimatlari izleyin. Genel olarak, her iletisim kutusunda düzenleyebileceginiz spesifik bir özellik bulursunuz. Özelligin açiklamasi mutlaka iletisim kutusunun içinde yer alir. Düzenleyebileceginiz parametreler:

- ***Filtreleme*** - dil listesi, ülke listesi, onaylanan IP'ler, engellenen IP'ler, engellenen ülkeler, engellenen karakter setleri, sahte göndericiler
- ***RBL*** - RBL sunuculari, çoklu eslesme, esik, zaman asimi, maksimum IP'ler
- ***Internet baglantisi*** - zaman asimi, proxy sunucusu, proxy kimlik dogrulamasi

9.6. Web Tarama Koruması

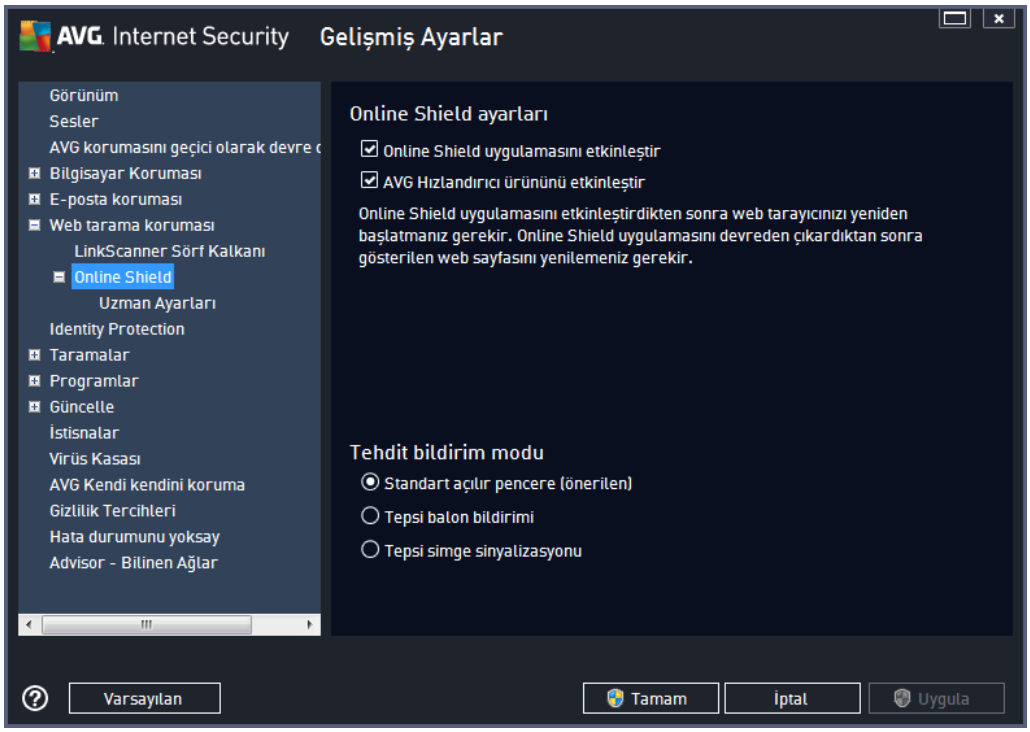
LinkScanner ayarlari iletisim kutusunda asagidaki özellikleri isaretleyebilir veya bunlarin isaretlerini kaldirabilirsiniz:



- ***Sörf Kalkani özelligini etkinlestir*** - (*varsayilan olarak açik*): erisim saglandigi anda güvenlik açigi olan web sitelerine karsi (*gerçek zamanli*) koruma saglamak için etkinlestirin. Bilinen kötü amaçli site baglantilari ve güvenlik açigindan yararlanan içerikler, kullanici bir web tarayicisi (*ya da HTTP kullanan diger bir program*) araciligiyla erisim sagladiginda engellenir.

- ***'LinkScanner Tarafindan Korunmaktadir' ibaresi ekle...*** - (*varsayilan olarak kapali*): Facebook ve MySpace sosyal paylasim aglarindan gönderilen etkin baglantilari içeren iletilerde LinkScanner denetimi ile ilgili sertifikasyon bildirimi girmek istediginizi onaylamak için bu ögeyi isaretleyin.

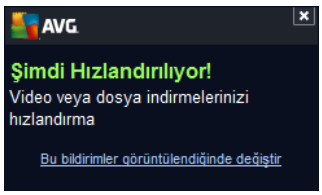
9.6.1. Online Shield



Online Shield iletisim kutusu su seçenekleri sunar:

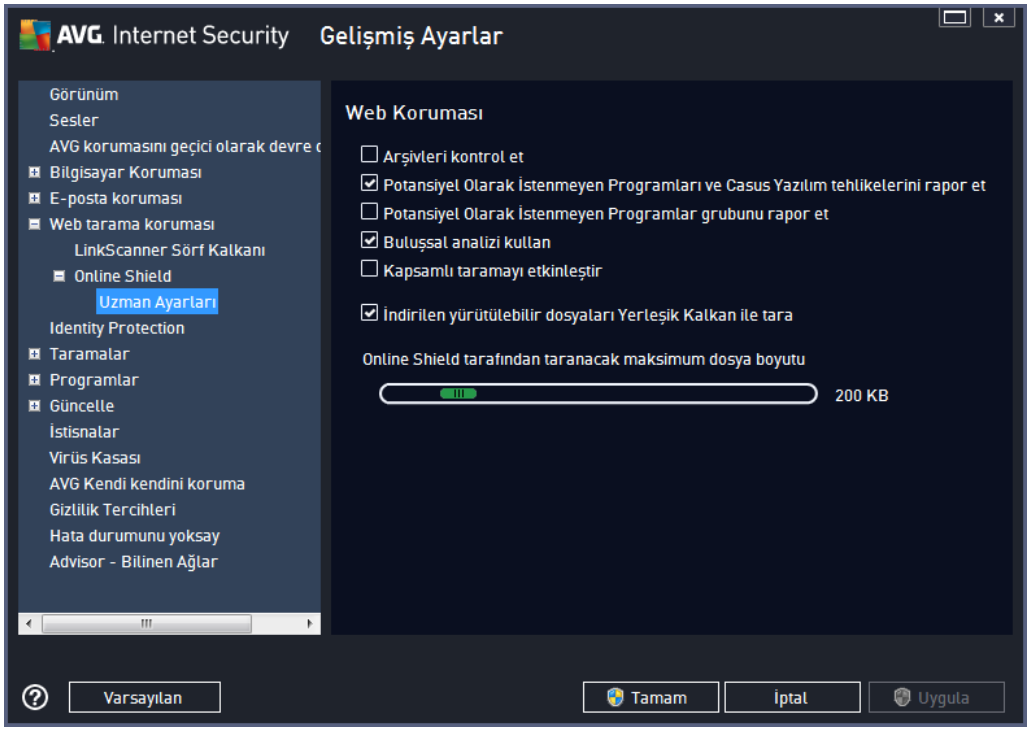
- ***Online Shield'i etkinlestir*** *(varsayilan olarak açik)* - ***Online Shield*** hizmetinin tamamini etkinlestirir/devre disi birakir. Diger ***Online Shield*** gelismis ayarlari için lütfen Web Koruması adindaki sonraki iletisim kutusuna geçin.

- ***AVG Hizlandirici ürününü etkinlestir*** *(varsayilan olarak açik)* - AVG Hizlandirici hizmetini etkinlestirin veya devre disi birakin. AVG Hizlandirici daha düzgün çevrimiçi video oynatmaya izin verir ve ilave indirmeleri daha kolay hale getirir. Video hizlandirma islemi çalisirken sistem tepsisi açilir penceresi ile bilgilendirilirsiniz:



Tehdit bildirim modu

Iletisim kutusunun alt kisminda algilanmasi muhtemel tehdit hakkinda hangi yöntemle bilgilendirilmek istediginizi seçin: standart açilir iletisim kutusuyla, tepsi balon bildirimiyle ya da tepsi simgesi bilgileriyle.



Web Korumasi - web sitelerinin içeriginin taranmasina iliskin bilesen yapilandirmasini düzenleyebilirsiniz. Düzenleme arayüzü ile asagidaki temel seçenekleri yapilandirabilirsiniz:

- ***Arsivleri denetle*** - (*varsayilan olarak kapali*): Görüntülenecek www sayfasinda bulunmasi muhtemel arsivlerin içerigini tarayin.
- ***Potansiyel olarak istenmeyen programlari ve casus yazilim tehlikelerini rapor et*** - (*varsayilan olarak açik*): Virüslerin yani sira casus yazilimlarin da taranmasini etkinlestirmek için isaretleyin. Casus yazilim, süpheli kötü amaçli yazilim kategorisini ifade eder: genellikle bir güvenlik riskini olusturmasina ragmen bu programlardan bazilari bilerek yüklenebilir. Bilgisayarinizin güvenligini artirdigindan, bu özelligi etkin durumda tutmanizi öneririz.
- ***Potansiyel olarak istenmeyen programlar gelismis grubunu rapor et*** - (*varsayilan olarak kapali*): Casus yazilimlarin, yani dogrudan üreticiden alinan ve tamamen zararsiz olan, ancak daha sonra kötüye kullanilabilecek programlarin genisletilmis paketinin tespit edilmesi için isaretleyin. Bu, bilgisayar güvenliginizi daha da artiran ek bir önlemdir, ancak yasal programlari da engelleyebilir ve bu yüzden varsayilan olarak kapalidir.
- ***Bulussal yöntem kulan*** - (*varsayilan olarak açik*): Görüntülenecek sayfanin içerigi bulussal analiz yöntemi kullanilarak taranir (*taranan nesnenin komutlarinin sanal bir bilgisayar ortaminda dinamik olarak canlandirilmasi*).
- ***Kapsamli taramayi etkinlestir*** - (*varsayilan olarak kapali*): Belirli durumlarda (*bilgisayariniza bulasma olmasindan süpheleniyorsaniz*) yalnizca emin olmak amaciyla bilgisayarinizin bulasma olmasi çok zor olan alanlarini bile tarayan en kapsamli tarama algoritmalarini etkinlestirmek için bu seçenegi isaretleyebilirsiniz.

Ancak, bu yöntemin çok fazla zaman aldigini unutmayin.

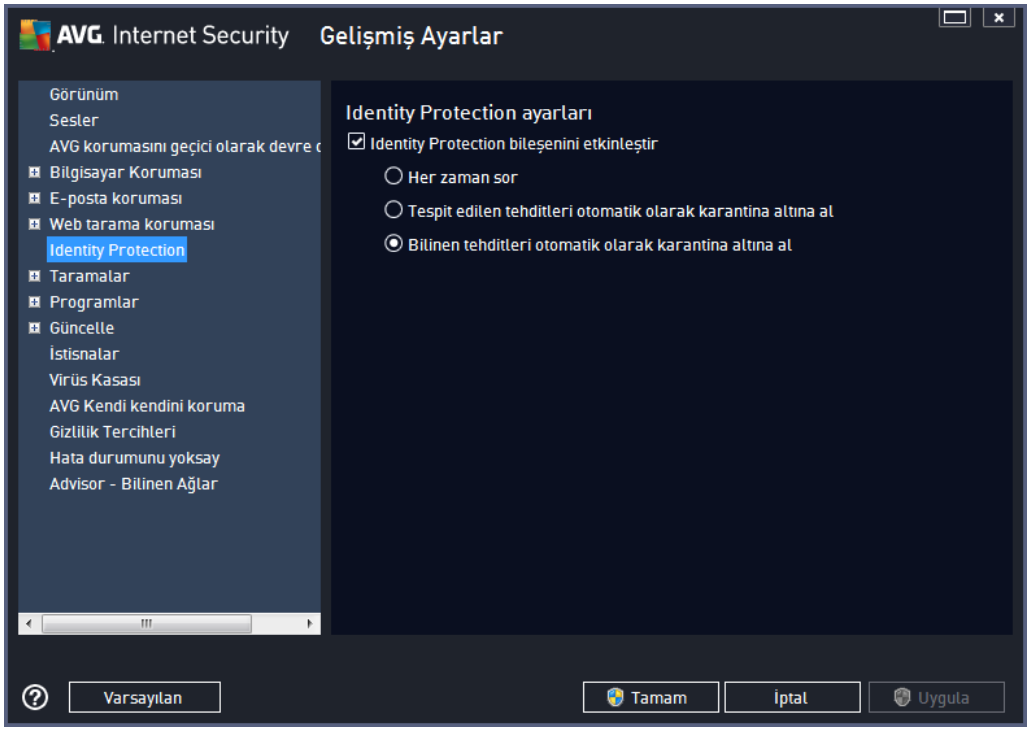
- ***Indirilen yürütülebilir dosyalari Yerlesik Kalkan ile tara*** - (*varsayilan olarak açik*): Yürütülebilir dosyalari *(genellikle exe, bat, com uzantili dosyalar)* indirilmelerinin ardindan tarayin. Yerlesik kalkan bilgisayariniza zararli herhangi bir kodun ulasmamasi için dosyalari indirilmeden önce tarar. Ancak, bu tarama ***Taranacak dosyanin maksimum parça boyutu*** ile sinirlandirilmistir (bu iletisim kutusunda bir sonraki ögeye bakin). Bu nedenle büyük dosyalar parça parça taranir ve yürütülebilir dosyalarin çogu da büyük dosyadir. Yürütülebilir dosyalar bilgisayarinizda pek çok görevi gerçeklestirebilir; bu nedenle bu dosyalarin %100 güvenli olmasi hayati önemdedir. Bu güvenlik hem dosyanin indirilmeden önce parça parça taranmasiyla hem de indirme tamamlandiktan sonra bütün olarak taranmasiyla saglanabilir. Bu seçenegi isaretli birakmanizi tavsiye ederiz. Bu seçenegi devre disi biraksaniz bile, potansiyel olarak tehlikeli tüm kodlar AVG tarafindan bulunacagi için rahat olabilirsiniz. Yalnizca genellikle yürütülebilir dosyayi bir bütün olarak degerlendiremeyecegi için bazi yanlis tespitler yapabilir.

Iletisim kutusunun altindaki kaydirici ***Taranacak maksimum dosya bölümü büyüklügü***'nü tanimlamanizi saglar; dahil edilen dosyalar görüntülenen sayfada mevcutsa bunlari bilgisayariniza indirmeden önce de dosya içeriklerini tarayabilirsiniz. Ancak, büyük dosyalarin taranmasi zaman alabilir ve web sayfasinin indirilmesi de önemli ölçüde yavaslayabilir. ***Online Shield*** ile taranacak dosyanin maksimum boyutunu belirlemek için kaydirma çubugunu kullanabilirsiniz. Indirilen dosya belirtilen dosya boyutundan daha büyük olsa ve buna bagli olarak Online Shield ile taranmasa bile korunmaya devam edersiniz: Dosya, bulasmis olmasi halinde ***Yerlesik Kalkan*** tarafindan tespit edilecektir.

9.7. Identity Protection

Identity Protection davranissal teknolojiler ve yeni virüslere karsi sifir gün korumasi kullanarak sizi tüm kötü amaçli yazilimlardan (*casus yazilim, robotlar, kimlik hirsizligi, ...*) koruyan bir kötü amaçli yazilimlara karsi koruma bilesenidir *(bilesenlerin islevleri hakkinda ayrintili bilgi için lütfen Identity bölümüne bakin*).

Identity Protection ayarlari iletisim kutusu Identity Protection bileseninin temel özelliklerini açmanizi/kapatmanizi saglar:



Identity Protection bilesenini etkinlestir (*varsayilan olarak açik*) - Identity bilesenini kapatmak için isaretini kaldirin.

Zorunlu olmadikça, bu isareti kaldirmamanizi önemle tavsiye ederiz!

Identity Protection etkinlestirildiginde, bir tehlike algilandiginda ne yapacaginizi belirtebilirsiniz:

- ***Her zaman sor*** (*varsayilan olarak açik*) - bir tehlike algilandiginda, çalistirmak istediginiz bir uygulamanin kaldirilmamasindan emin olmak için karantinaya alinmasi gerekip gerekmedigi size sorulacaktir.
- ***Algilanan tehlikeleri otomatik olarak karantinaya al*** - algilanan tüm olasi tehlikelerin Virüs Kasasi güvenilir alanina hemen tasinmasini istediginizi belirtmek için bu onay kutusunu isaretleyin. Varsayilan ayarlarda, bir tehlike algilandiginda, çalistirmak istediginiz hiçbir uygulamanin kaldirilmamasi için size uygulamanin karantinaya alinmasi gerekip gerekmedigi sorulacaktir.
- ***Bilinen tehlikeleri otomatik olarak karantinaya al*** - kötü amaçli yazilim olasiligi algilanan tüm uygulamalarin otomatik olarak ve hemen Virüs Kasasi'na alinmasini istiyorsaniz bu ögeyi isaretli birakin.

9.8. Taramalar

Gelismis tarama ayarlari, yazilim gelistiricisi tarafindan tanimlanan belirli tarama türlerine iliskin dört kategoriye bölünmüstür:

- Tüm bilgisayarin taranmasi - tüm bilgisayarin standart öntanimli taramasidir
- Belirli dosya veya klasörleri tarama - bilgisayarinizin seçilen alanlarinin tarandigi standart

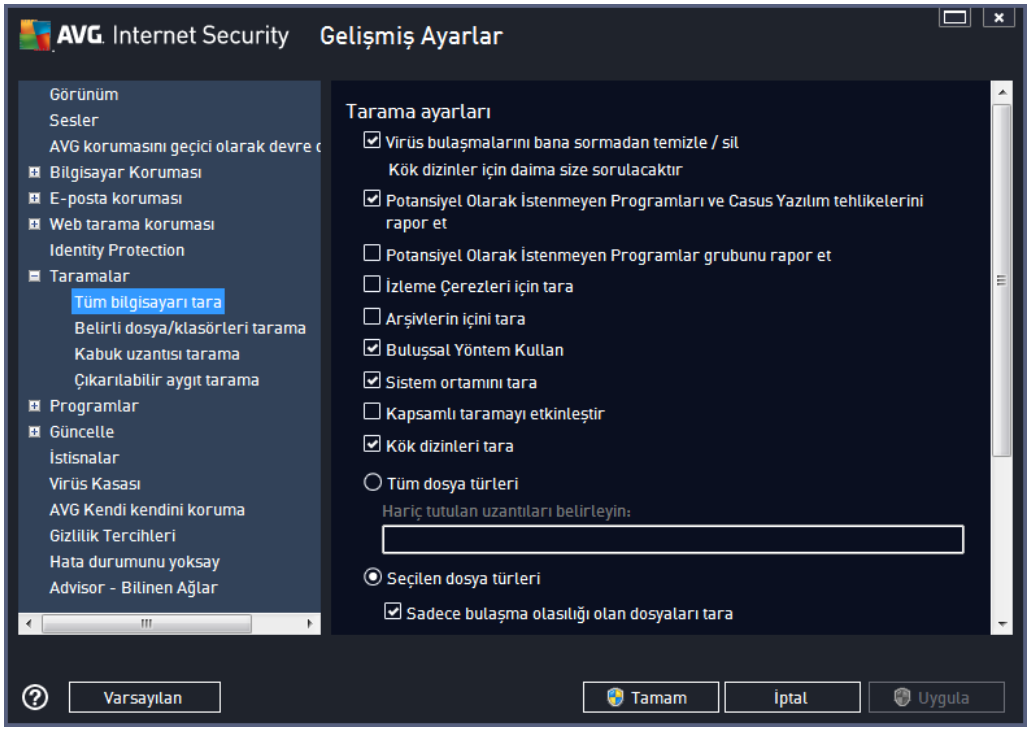
öntanimli taramadir

- Kabuk uzanti taramasi - seçilen nesnenin dogrudan Windows Gezgini ortaminda taranmasi islemidir

- Çikartilabilir aygit taramasi - bilgisayariniza baglanan çikartilabilir aygitlarin taranmasi islemidir

9.8.1. Tüm Bilgisayar Taraması

Tüm Bilgisayari Tara seçenegi, yazilim saticisi tarafindan belirlenmis varsayilan tarama yöntemlerinden birinin parametrelerini düzenleyebilmenize olanak tanir, Tüm Bilgisayari Tara:



Tarama ayarlari

Tarama Ayarlari bölümünde istege bagli olarak açilip kapatilabilecek tarama parametreleri listelenmistir:

- ***Bulasmayi bana sormadan temizle / kaldir*** (*varsayilan olarak açik*) - Tarama sirasinda virüs tanimlanirsa, bir giderme yazilimi mevcutsa otomatik olarak temizlenir. Bulasmis dosya otomatik olarak temizlenemezse, bulasmis nesne Virüs Kasasi'na tasinir.

- ***Potansiyel olarak istenmeyen programlari ve casus yazilim tehlikelerini rapor et*** (*varsayilan olarak açik*) - virüslerin yani sira casus yazilimlari da taramak için isaretleyin. Casus yazilim, süpheli kötü amaçli yazilim kategorisini ifade eder: genellikle bir güvenlik riskini olusturmasina ragmen bu programlardan bazilari bilerek yüklenebilir. Bilgisayarinizin güvenligini artirdigindan, bu özelligi etkin durumda tutmanizi öneririz.

- ***Potansiyel olarak istenmeyen programlar gelismis grubunu rapor et*** (*varsayilan olarak kapali*) - Casus yazilimlarin, yani dogrudan üreticiden alindiginda tamamen zararsiz olan, ancak daha sonra kötüye kullanilabilecek programlarin genisletilmis paketinin tespit edilmesi için isaretleyin. Bu, bilgisayar güvenliginizi daha da artiran ek bir önlemdir, ancak yasal programlari da engelleyebilir ve bu yüzden varsayilan olarak kapalidir.

- ***Izleme çerezleri için tara*** (*varsayilan olarak kapali*) - bu parametre tarama sirasinda çerezlerin tespit edilmesi gerektigini belirtir (*HTTP çerezleri kimlik dogrulamasi, izleme ve kullanicilar hakkindaki site tercihleri veya elektronik alisveris sepetlerinin içerigi gibi belirli bilgilerin korunmasi için kullanilir*).

- ***Arsivleri tara*** (*varsayilan olarak kapali*) - bu parametre tarama isleminin ZIP, RAR vb. arsiv dosyalarinin içinde saklanan tüm dosyalari denetlemesi gerektigini belirtir.

- ***Bulussal yöntem kullan*** (*varsayilan olarak açik*) - bulussal analiz (*taranan nesnenin yönergelerinin sanal bir bilgisayar ortaminda dinamik olarak canlandirilmasi*) tarama sirasinda kullanilacak virüs tespit yöntemlerinden biridir.

- ***Sistem ortamini tara*** (*varsayilan olarak açiktir*) - tarama islemi, bilgisayarinizin sistem alanlarini da kontrol edecektir.

- ***Kapsamli taramayi etkinlestir*** (*varsayilan olarak kapali*) - belirli durumlarda (*bilgisayariniza bulasma olmasindan süpheleniyorsaniz*) yalnizca emin olmak üzere bilgisayarinizin bulasma olmasi çok zor olan alanlarini bile tarayan en kapsamli tarama algoritmalarini etkinlestirmek için bu seçenegi isaretleyebilirsiniz. Ancak, bu yöntemin çok fazla zaman aldigini unutmayin.

- ***Rootkit'leri tara*** (*varsayilan olarak açik*) - Anti-Rootkit taramasi bilgisayarinizi olasi rootkit'lere, örnegin bilgisayarinizda kötü amaçli etkinlik içerebilecek programlar ve teknolojilere karsi tarar. Bir kök dizin algilanirsa, bu, bilgisayarinizda mutlaka virüs oldugu anlamina gelmez. Bazi durumlarda, belirli sürücüler veya normal uygulamalarin bölümleri kök dizin olarak yanlis algilanabilir.

Ayrica tarama için dosya türlerini de belirlemeniz gerekir

- ***Tüm dosya türleri***, virgülle ayrilmis (*kaydedilirken virgüller noktali virgüle dönüsür*) dosya uzantilari listesi saglayarak taramadan hariç tutulacaklarin taranmamasi için tanimlama olasiligi saglar;

- ***Seçili dosya türleri*** - yalnizca virüs bulasabilme olasiligi olan dosyalari taramayi istediginizi belirtebilirsiniz (*virüs bulasamayan dosyalar taranmayacaktir, örnegin, bazi düz metin dosyalari veya bazi diger çalistirilamayan dosyalar*); ortam dosyalari (*video, ses dosyalari - bu onay kutusunun isaretini kaldirirsaniz, bu dosyalar genellikle çok büyük oldugundan ve virüs bulasma olasiliklari çok az oldugundan tarama süresini daha da azaltir*). Tekrar, her zaman taranmasi gereken dosyalari uzantilarina göre belirtebilirsiniz.

- Istege bagli olarak, ***Uzantilari olmayan dosyalari taramaya*** da karar verebilirsiniz ve bu seçenek varsayilan olarak açiktir ve gerçekten bir nedeniniz yoksa degistirmemeniz önerilir. Uzantisi olmayan dosyalar süpheli olabilir ve her zaman taranmalidir.

Taramanin ne kadar hizli tamamlanacagini ayarla

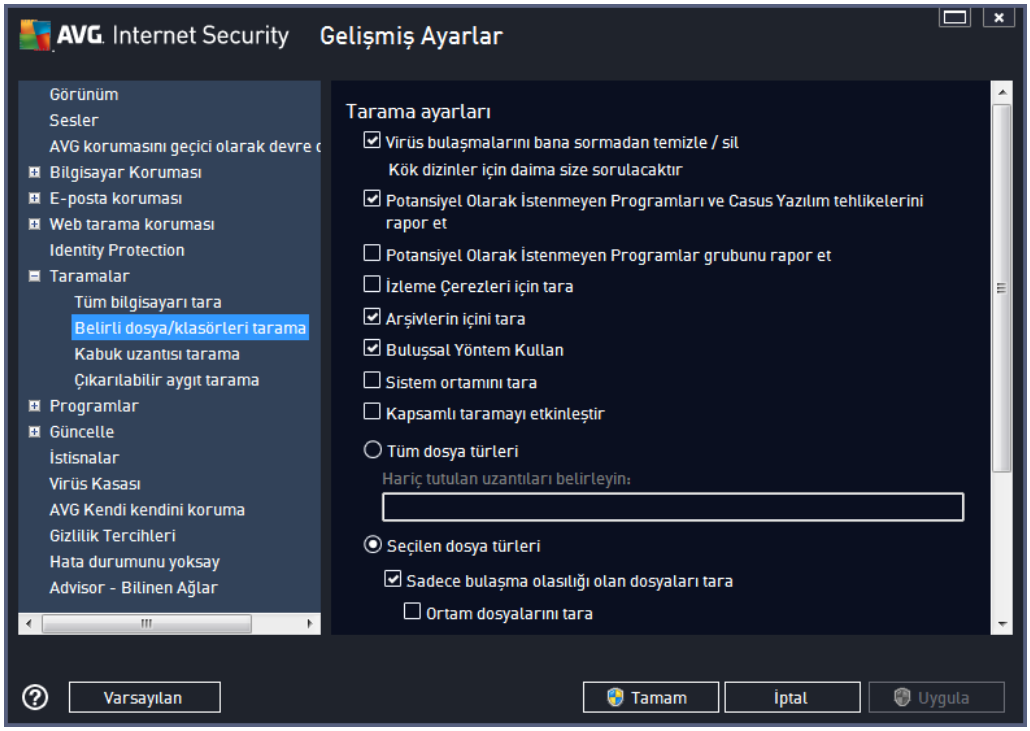
Taramanin ne kadar hizli tamamlanacagini ayarla bölümünde, sistem kaynaklari kullanimina bagli olarak istediginiz tarama hizini seçebilirsiniz. Bu seçenek varsayilan olarak otomatik kaynak kullaniminin *kullaniciya duyarli* düzeyine ayarlanmistir. Tarama isleminin daha hizli ilerlemesini istiyorsaniz tarama islemi daha kisa sürecektir fakat tarama islemi sirasinda sistem kaynaklari oldukça yüklü bir sekilde kullanilacak ve bilgisayar üzerindeki diger islemleri yavaslatacaktir (*bu seçenek bilgisayariniz açikken kullanilmadigi sirada seçilebilir*). Öte yandan, tarama süresini uzatarak sistem kaynaklarinin kullanimini azaltabilirsiniz.

Ek tarama raporlarini ayarla...

Diger tarama raporlarini belirle... baglantisina tiklayarak hangi tarama bulgularinin rapor edilecegine iliskin seçimleri yapabileceginiz ***Tarama raporlari*** iletisim kutusu penceresini açabilirsiniz:

9.8.2. Belirli dosya/klasörleri tarama

Belirli Dosyalari veya Klasörleri Tara islevinin düzenleme arayüzü Tüm Bilgisayari Tara islevinin düzenleme iletisim kutusu ile aynidir. Tüm yapilandirma seçenekleri aynidir; fakat Tüm Bilgisayari Tara islevinin varsayilan ayarlari daha kesindir:

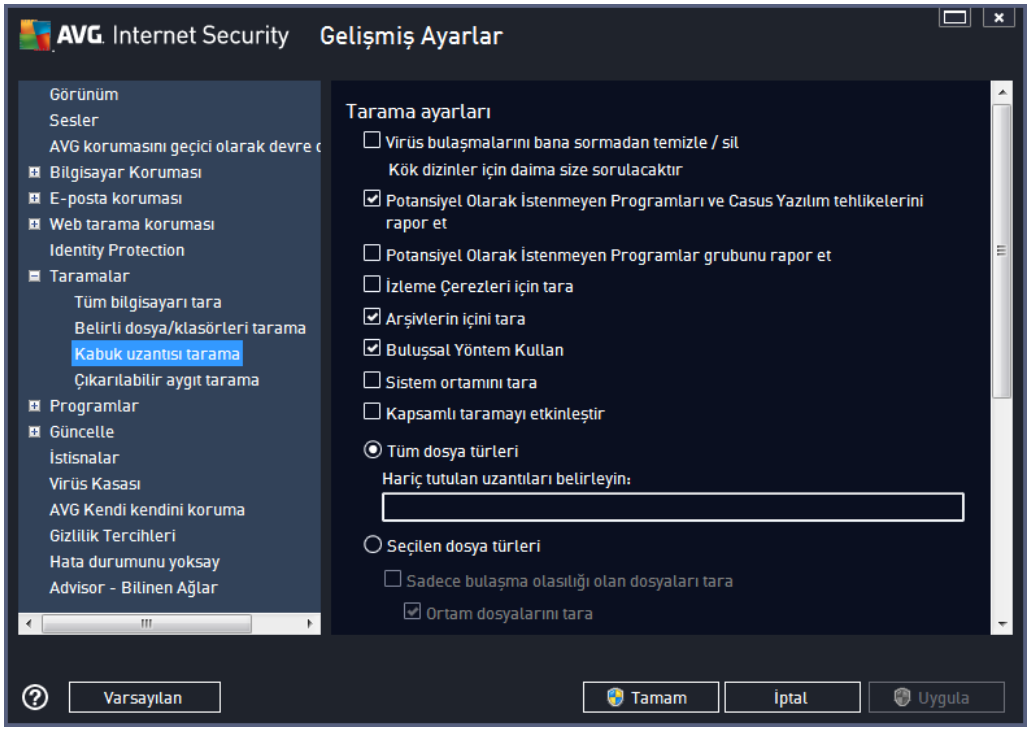


Bu yapilandirma iletisim kutusunda ayarlanan tüm parametreler Belirli Dosyalari veya Klasörleri Tara islemi ile tarama sirasinda seçilen alanlar için geçerlidir!

Not: *Belirli parametrelerin açiklamasi için lütfen AVG Gelismis Ayarlari / Taramalar / Tüm Bilgisayari Tara bölümüne bakin.*

9.8.3. Kabuk Uzantısı Tarama

Daha önce bahsettigimiz Tüm Bilgisayari Tara ögesine benzer olan bu öge, ***Kabuk Uzantisi Tarama*** olarak adlandirilir ve taramayi düzenlemek için yazilim saticisi tarafindan önceden tanimlanmis birkaç seçenek de sunar. Bu sefer, yapilandirma dogrudan Windows Gezgini üzerinden baslatilan belirli nesnelerin taranmasi esasina dayanmaktadir (*kabuk uzantisi*), Windows Gezgini'nde Tarama bölümüne bakin:



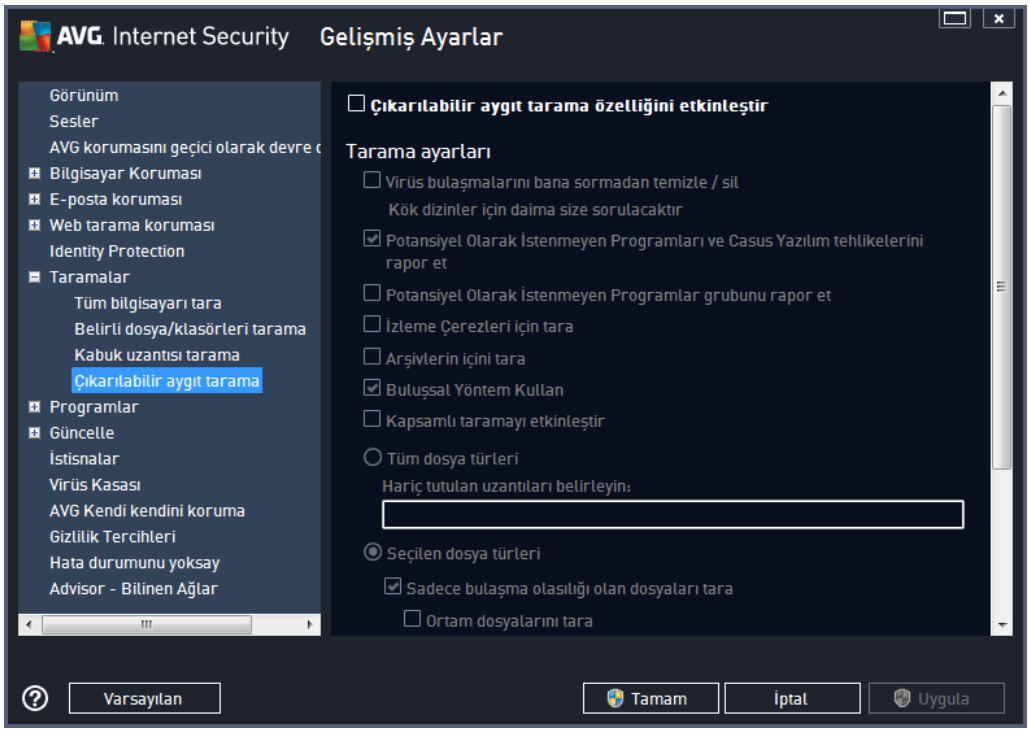
Parametre listesi, Tüm Bilgisayari Tara ögesinin parametre listesi ile aynidir. Bununla birlikte, varsayilan ayarlar farklilik gösterebilir (*örnegin, Tüm Bilgisayari Tara islevi arsivleri denetlemedigi halde sistem ortamini denetler; Kabuk Uzantisi Tarama'da ise durum tam tersidir*).

Not: *Belirli parametrelerin açiklamasi için lütfen AVG Gelismis Ayarlari / Taramalar / Tüm Bilgisayari Tara bölümüne bakin.*

Tüm Bilgisayari Tara iletisim kutusuyla karsilastirildiginda ***Kabuk Uzantisi Tarama*** iletisim kutusu, tarama sürecinde ve tarama sonuçlarinda AVG kullanici arayüzünden erisilebilir olmasini isteyip istemediginizi belirleyebileceginiz ***AVG Kullanici Arayüzü ile ilgili diger ayarlar*** adli bölümü de içerir. Tarama sonucunun yalnizca tarama sirasinda bir bulasma tespit edilmesi durumunda görüntülenmesi gerektigini de belirleyebilirsiniz.

9.8.4. Çıkarılabilir Aygıt Tarama

Çikarilabilir Aygit Tarama düzenleme arayüzü de Tüm Bilgisayari Tara düzenleme iletisim kutusuna çok benzerdir:



Çikarilabilir Aygit Tarama islemi bilgisayariniza çikarilabilir bir aygit taktiginiz anda otomatik olarak baslar. Varsayilan olarak bu tarama islemi kapalidir. Diger bir yandan baslica bulasma kaynaklarindan biri oldugu için söz konusu çikartilabilir aygitlarin potansiyel tehditlere karsi taranmasi hayati önem tasimaktadir. Bu tarama özelliginin istendigi zaman otomatik olarak baslatilacak sekilde hazir bulundurulmasi için ***Çikartilabilir aygit taramayi etkinlestir*** seçenegini isaretleyin.

Not: *Belirli parametrelerin açiklamasi için lütfen AVG Gelismis Ayarlari / Taramalar / Tüm Bilgisayari Tara bölümüne bakin.*

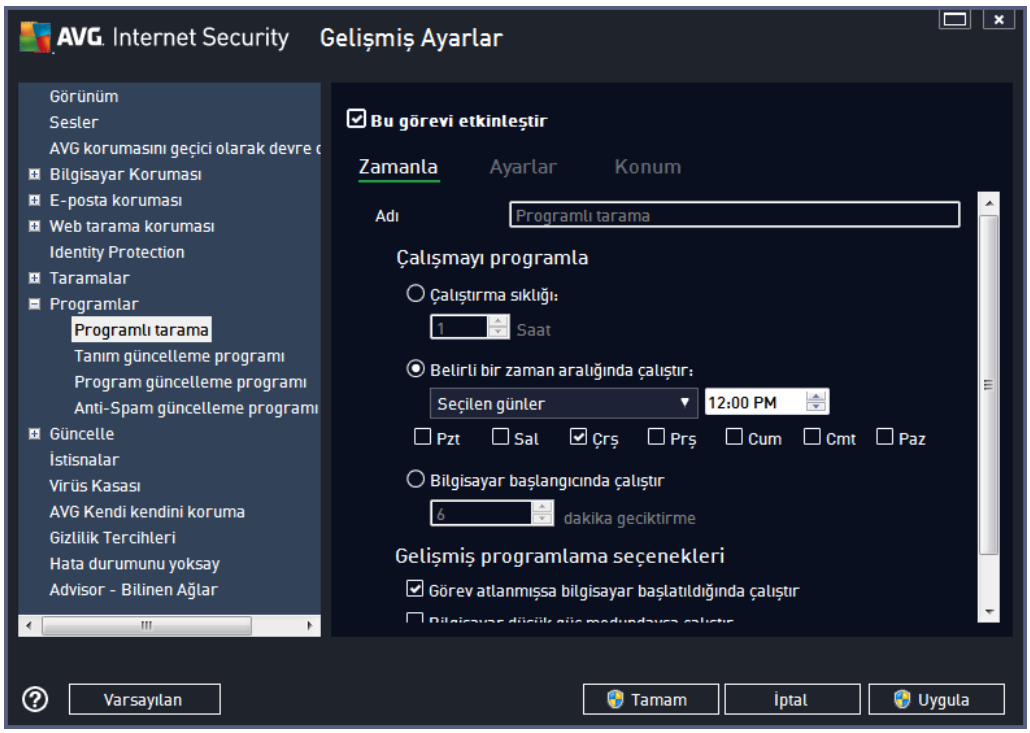
9.9. Programlar

Programlar bölümünde asagidaki bilesenlerin öntanimli ayarlarini düzenleyebilirsiniz:

- Programlanmis Tarama
- Tanim güncelleme programi
- Program Güncelleme Plani
- Anti-Spam Güncelleme Zamanlamasi

9.9.1. Programlanmış Tarama

Planlanan tarama parametreleri üç sekmeden düzenlenebilir (*ya da yeni bir zamanlama ayarlanabilir*). Her sekmede ***Bu görevi etkinlestir*** ögesini isaretleyerek veya söz konusu ögenin isaretini kaldirarak zamanlanan testi geçici olarak devre disi birakabilir ve gerektiginde yeniden açabilirsiniz:



Ad adindaki metin alani (*tüm varsayilan zamanlamalar için devre disi birakilmistir*) bu zamanlamaya program saticisi tarafindan atanan adi gösterir. Yeni eklenen zamanlamalar için (*sol gezinti agacindayken* ***Taramayi programla*** *ögesi üzerinde sag tiklatarak* yeni bir zamanlama ekleyebilirsiniz) kendi adinizi belirtebilirsiniz ve bu durumda metin alani düzenleme için açilacaktir. Programladiginiz taramalari digerlerinden kolaylikla ayirabilmek için her zaman taramalariniza kisa, açiklayici adlar vermeye çalisin.

Örnek: *Taramayi "Yeni Tarama" veya "Taramam" adiyla adlandirmaniz uygun degildir çünkü bu adlar, taramanin fiilen neyi kontrol ettigini açiklamaz. Diger bir yandan "Sistem alani taramasi" vb. oldukça açiklayici bir isim olacaktir. Ayrica, taramanin adinda söz konusu taramanin tam bilgisayar taramasi ya da sadece seçilen dosya ya da klasörlerin taranmasi olup olmadigini belirtmenize gerek yoktur - taramalariniz [seçilen dosya ya da klasörleri tara](#) islevinin farkli sekillerinden ibaret olacaktir.*

Bu iletisim kutusunda taramanin asagidaki parametrelerini de tanimlayabilirsiniz:

Çalismayi programla

Burada, yeni programlanan tarama baslatmasi için zaman araliklari belirtebilirsiniz. Zamanlama belirli bir sürenin ardindan tekrarlanan tarama baslatmasi ile (***Her ...'de bir***) ya da kesin bir tarih ve saat tanimlayarak (***Belirli bir zaman araliginda çalistir ...***), veya tarama baslangiciyla ilgili bir olay

tanimlanarak (***Bilgisayar baslangicinda çalistir***) tanimlanabilir.

Gelismis zamanlama seçenekleri

Bu bölümde, bilgisayar düsük güç modundaysa veya tamamen kapatilmissa hangi kosullar altinda taramanin baslatilmasi/baslatilmamasi gerektigini tanimlamanizi saglar. Programlanan tarama belirttiginiz saatte baslatildiginda, AVG sistem tepsisi simgesi üzerinde beliren bir açilir pencereyle bu konuda bilgilendirilirsiniz.

Bunun ardindan yeni bir AVG sistem tepsisi simgesi görüntülenir (*üzerinde beyaz bir ok bulunur ve tamamen renklidir*) ve programlanan taramanin basladigini bildirir. Çalisan taramayi duraklatmaya hatta durdurmaya karar verebileceginiz ve o anda çalismakta olan taramanin önceligini degistirebileceginiz baglam menüsü açmak için, çalisan taramayi sag tiklatin.

Ayarlar sekmesinde, istege bagli olarak açilip/kapatilabilen tarama parametrelerine iliskin bir liste bulabilirsiniz. Varsayilan olarak birçok parametre devreye sokulur ve islevsellik de tarama sirasinda uygulanacaktir. ***Söz konusu ayarlari degistirmek açisindan geçerli bir nedeniniz yoksa öntanimli yapilandirmayi oldugu gibi muhafaza etmeniz önerilir***:

- ***Bulasmayi bana sormadan temizle / kaldir*** *(varsayilan olarak açik):* Tarama sirasinda virüs tanimlanirsa, bir giderme yazilimi mevcutsa otomatik olarak temizlenir. Bulasmis dosya otomatik olarak temizlenemezse, bulasmis nesne Virüs Kasasi'na tasinir.

- ***Potansiyel olarak istenmeyen programlari ve casus yazilim tehlikelerini rapor et*** *(varsayilan olarak açik):* Virüslerin yani sira casus yazilimlari da taramak için isaretleyin. Casus yazilim, süpheli kötü amaçli yazilim kategorisini ifade eder: genellikle bir güvenlik

riskini olusturmasina ragmen bu programlardan bazilari bilerek yüklenebilir. Bilgisayarinizin güvenligini artirdigindan, bu özelligi etkin durumda tutmanizi öneririz.

- ***Potansiyel olarak istenmeyen programlar gelismis grubunu rapor et*** (*varsayilan olarak kapali*): Casus yazilimlarin, yani dogrudan üreticiden alindiginda tamamen zararsiz olan, ancak daha sonra kötüye kullanilabilecek programlarin genisletilmis paketinin tespit edilmesi için isaretleyin. Bu, bilgisayar güvenliginizi daha da artiran ek bir önlemdir, ancak yasal programlari da engelleyebilir ve bu yüzden varsayilan olarak kapalidir.

- ***Izleme çerezleri için tara*** (*varsayilan olarak kapali*): Bu parametre tarama sirasinda çerezlerin tespit edilmesi gerektigini belirtir (*HTTP çerezleri kimlik dogrulamasi, izleme ve kullanicilar hakkindaki site tercihleri veya elektronik alisveris sepetlerinin içerigi gibi belirli bilgilerin korunmasi için kullanilir*).

- ***Arsivleri tara*** (*varsayilan olarak kapali*): Bu parametre, tarama isleminde ZIP, RAR vb. bir arsiv ile saklanmis olsa bile tüm dosyalarin taranmasi gerektigini belirtir.

- ***Bulussal yöntem kullan*** (*varsayilan olarak açik*): Bulussal analiz (*taranan nesnenin yönergelerinin sanal bir bilgisayar ortaminda dinamik olarak canlandirilmasi*) tarama sirasinda kullanilacak virüs tespit yöntemlerinden biridir.

- ***Sistem ortamini tara*** (*varsayilan olarak açik*): Tarama islemi, bilgisayarinizin sistem alanlarini da kontrol edecektir.

- ***Kapsamli taramayi etkinlestir*** (*varsayilan olarak kapali*) belirli durumlarda (*bilgisayariniza bulasma olmasindan süpheleniliyorsa*) yalnizca emin olmak üzere bilgisayarinizin bulasma olmasi çok zor olan alanlarini bile tarayan en kapsamli tarama algoritmalarini etkinlestirmek için bu seçenegi isaretleyebilirsiniz. Ancak, bu yöntemin çok fazla zaman aldigini unutmayin.

- ***Kök dizinleri tara*** *(varsayilan olarak açik):* Anti-Rootkit taramasi bilgisayarinizi olasi rootkitlere, örnegin bilgisayarinizda kötü amaçli etkinlik içerebilecek programlar ve teknolojilere karsi tarar. Bir kök dizin algilanirsa, bu, bilgisayarinizda mutlaka virüs oldugu anlamina gelmez. Bazi durumlarda, belirli sürücüler veya normal uygulamalarin bölümleri kök dizin olarak yanlis algilanabilir.

Ayrica tarama için dosya türlerini de belirlemeniz gerekir

- ***Tüm dosya türleri***, virgülle ayrilmis (*kaydedilirken virgüller noktali virgüle dönüsür*) dosya uzantilari listesi saglayarak taramadan hariç tutulacaklarin taranmamasi için tanimlama seçenegi ile.

- ***Seçili dosya türleri*** - yalnizca virüs bulasabilme olasiligi olan dosyalari taramayi istediginizi belirtebilirsiniz (*virüs bulasamayan dosyalar taranmayacaktir, örnegin, bazi düz metin dosyalari veya bazi diger çalistirilamayan dosyalar*); ortam dosyalari (*video, ses dosyalari - bu onay kutusunun isaretini kaldirirsaniz, bu dosyalar genellikle çok büyük oldugundan ve virüs bulasma olasiliklari çok az oldugundan tarama süresini daha da azaltir*). Tekrar, her zaman taranmasi gereken dosyalari uzantilarina göre belirtebilirsiniz.

- Istege bagli olarak, ***Uzantilari olmayan dosyalari taramaya*** da karar verebilirsiniz ve bu seçenek varsayilan olarak açiktir ve gerçekten bir nedeniniz yoksa degistirmemeniz önerilir. Uzantisi olmayan dosyalar süpheli olabilir ve her zaman taranmalidir.

Taramanin ne kadar hizli tamamlanacagini ayarla

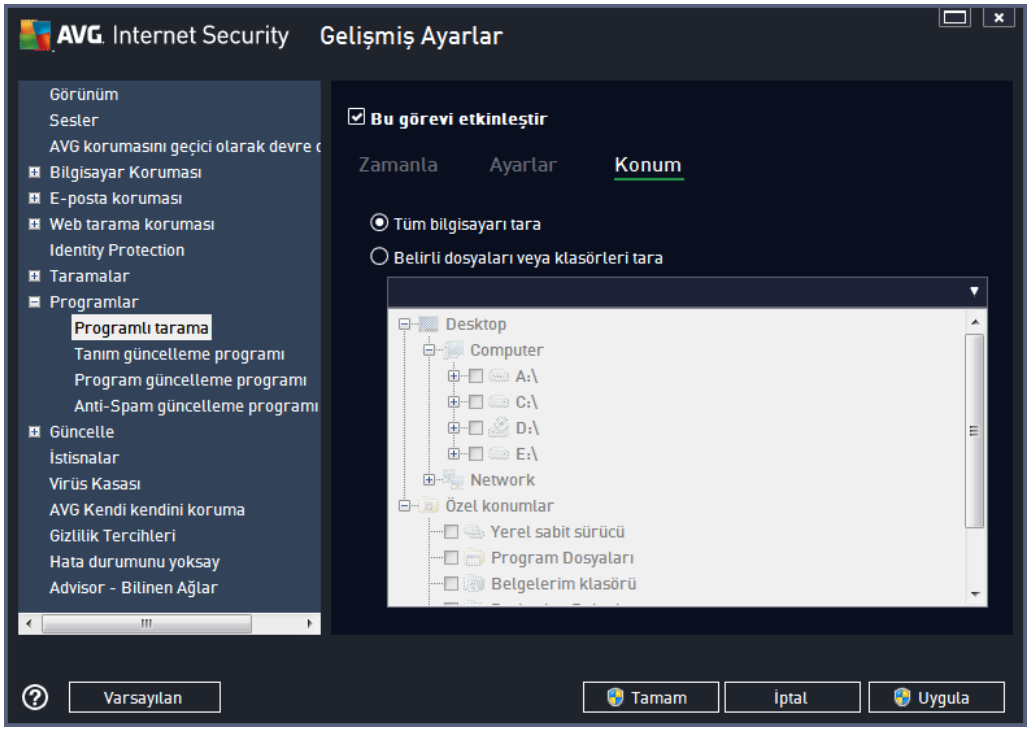
Bu bölümde ayrica istenen tarama hizini, sistemin kaynak kullanimina bagli olarak belirleyebilirsiniz. Varsayilan olarak, bu seçenek otomatik kaynak kullaniminin *kullaniciya duyarli* seviyesine ayarlidir. Tarama isleminin daha hizli ilerlemesini istiyorsaniz tarama islemi daha kisa sürecektir fakat tarama islemi sirasinda sistem kaynaklari oldukça yüklü bir sekilde kullanilacak ve bilgisayar üzerindeki diger islemleri yavaslatacaktir (*bu seçenek bilgisayariniz açikken kullanilmadigi sirada seçilebilir*). Öte yandan, tarama süresini uzatarak sistem kaynaklarinin kullanimini azaltabilirsiniz.

Ek tarama raporlarini ayarla

Tarama bulgularinin rapor edilmesi gerekip gerekmedigini tanimlamak üzere birden fazla ögeyi ayarlayabileceginiz ***Tarama raporlari*** olarak adlandirilan bagimsiz bir iletisim penceresi açmak için ***Ek tarama raporlarini ayarla...*** baglantisini tiklatin:

Bilgisayar kapatma seçenekleri

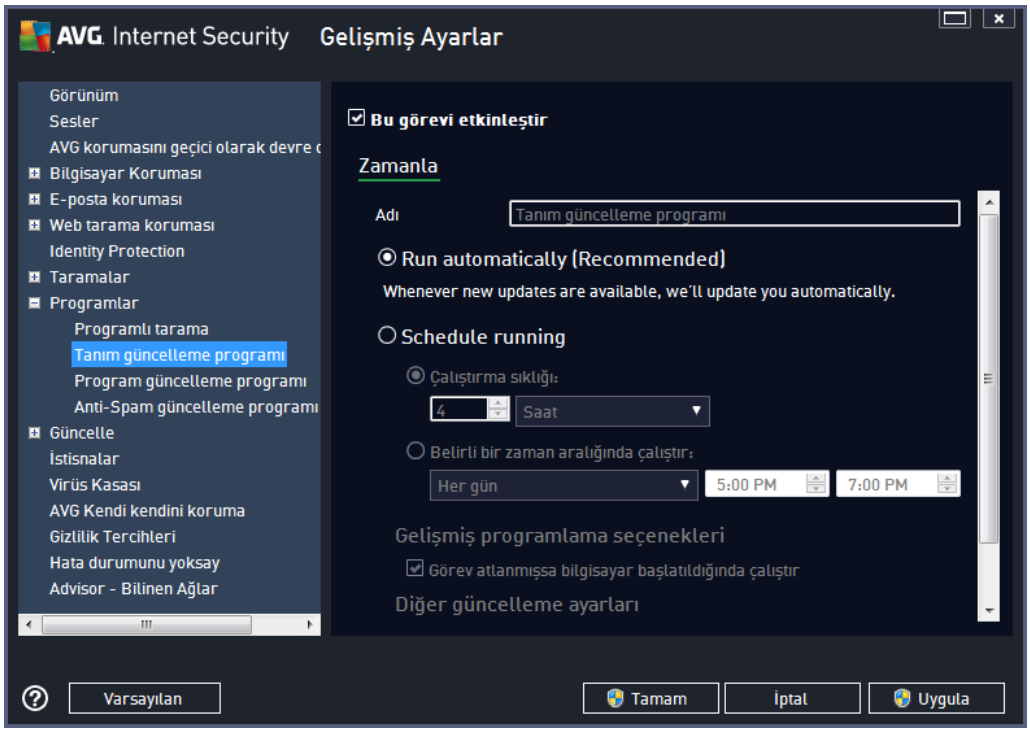
Bilgisayar kapatma seçenekleri bölümünde çalisan tarama islemi bittiginde bilgisayarin otomatik olarak kapatilmasi gerekip gerekmedigine karar verebilirsiniz. Bu seçenegi seçerseniz (***Tarama bittikten sonra bilgisayari kapat***) bilgisayar mevcut durumda kilitli olsa bile bilgisayarin kapatilmasini saglayan bir seçenegin bulundugu bir pencere açilacaktir (***Bilgisayar kilitliyse bilgisayari kapanmaya zorla***).



Konum sekmesinde, tüm bilgisayari tarama veya belirli dosya veya klasörleri taramayi programlamak isteyip istemediginizi tanimlayabilirsiniz. Belirli dosya ve klasörleri taramayi seçerseniz, bu iletisim kutusunun alt kisminda görüntülenen agaç yapisi etkinlesir ve taranacak klasörleri seçebilirsiniz.

9.9.2. Tanım güncelleme programı

Gerçekten gerekliyse Bu görevi etkinlestir ögesinin isaretini kaldirarak zamanlanmis tanimlari geçici olarak devre disi birakabilir ve daha sonra tekrar açabilirsiniz:



Bu iletisim kutusunda tanim güncelleme zamanlamasi parametrelerinden bazilarini ayrintilariyla yapilandirabilirsiniz. ***Ad*** adindaki metin alani (*tüm varsayilan zamanlamalar için devre disi birakilmistir*) bu zamanlamaya program saticisi tarafindan atanan adi gösterir.

Programli çalistirma

Varsayilan olarak, yeni bir virüs tanim güncellenmesi yayinlanir yayinlanmaz görev otomatik olarak baslatilir (***Otomatik olarak çalistir***). Degistirmek için iyi bir nedeniniz yoksa bu yapilandirmayi muhafaza etmenizi tavsiye ederiz! Ardindan, görev baslatmayi manuel olarak ayarlayabilir ve yeni programlanan tanim güncelleme baslatmalari için zaman araliklari belirleyebilirsiniz. Zamanlama, belirli bir süreden sonra (***Çalistirma sikligi...***) tekrarlanan güncelleme baslatmasi olarak veya belirli bir tarih ve saat (***Belirli bir saatte çalistir...***) tanimlanarak tanimlanabilir.

Gelismis programlama seçenekleri

Bu bölümde, bilgisayar düsük güç modundaysa veya tamamen kapatilmissa hangi kosullar altinda tanim güncellemesinin baslatilmasi/baslatilmamasi gerektigini belirleyebilirsiniz.

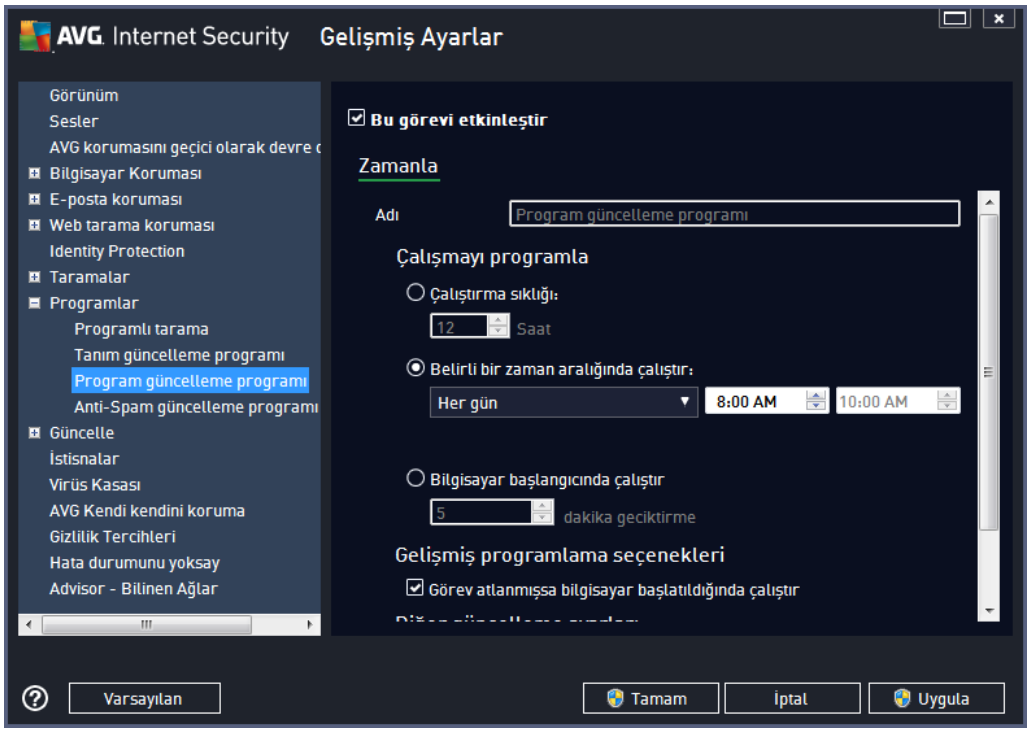
Diger güncelleme ayarlari

Son olarak, ***Internet baglantisi kuruldugunda güncellemeyi yeniden çalistir*** seçenegini

isaretleyerek internet baglantisi kesildiginde ve güncelleme islemi basarisiz oldugunda, internet baglantisi yeniden saglanir saglanmaz yeniden baslatilmasini saglayin. Planlanan güncelleme islemi sizin belirlediginiz tarih ve saatte basladiktan sonra AVG sistem tepsisi simgesi üzerinde açilan bir açilir pencere vasitasiyla bilgilendirileceksiniz (*Gelismis Ayarlar/Görünüm iletisim kutusunun varsayilan yapilandirmasini degistirmemis olmaniz kaydiyla)*.

9.9.3. Program Güncelleme Planı

Gerçekten gerekliyse Bu görevi etkinlestir ögesinin isaretini kaldirarak zamanlanmis programi geçici olarak devre disi birakabilir ve daha sonra tekrar açabilirsiniz:



Ad adindaki metin alani (*tüm varsayilan zamanlamalar için devre disi birakilmistir*) bu zamanlamaya program saticisi tarafindan atanan adi gösterir.

Çalismayi programla

Burada, yeni programlanan program güncellemesinin baslamasi için zaman araliklarini girin. Zamanlama belirli bir sürenin ardindan tekrarlanan güncelleme ile (***Her ...'de bir***) ya da kesin bir tarih ve saat tanimlayarak (***Belirli bir saatte çalistir...***) ya da (***Bilgisayar baslangicinda***) ilgili bir programin güncellemesiyle tanimlanabilir.

Gelismis programlama seçenekleri

Bu bölümde, bilgisayar düsük güç modundaysa veya tamamen kapatilmissa hangi kosullar altinda program güncellemesinin baslatilmasi/baslatilmamasi gerektigini belirleyebilirsiniz.

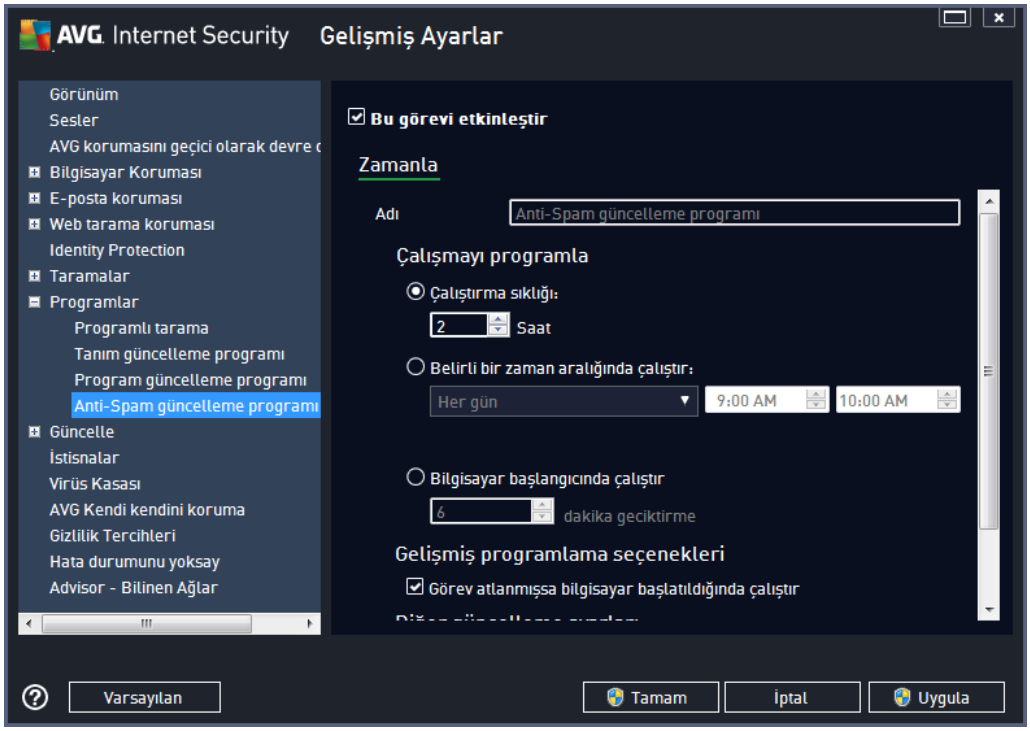
Diger güncelleme ayarlari

Internet baglantisi kuruldugunda güncellemeyi yeniden çalistir seçenegini isaretleyerek internet baglantisi kesildiginde ve güncelleme islemi basarisiz oldugunda, internet baglantisi yeniden saglanir saglanmaz yeniden baslatilmasini saglayin. Planlanan güncelleme islemi sizin belirlediginiz tarih ve saatte basladiktan sonra AVG sistem tepsisi simgesi üzerinde açilan bir açilir pencere vasitasiyla bilgilendirileceksiniz (*Gelismis Ayarlar/Görünüm iletisim kutusunun varsayilan yapilandirmasini degistirmemis olmaniz kaydiyla)*.

Not: *Zamanlamasi önceden yapilmis bir program güncellemesi ile taramanin zamanlamalarinin çakismasi durumunda güncelleme islemi daha yüksek öncelige sahiptir ve tarama islemine ara verilir. Böyle bir durumda çakisma hakkinda bilgilendirilirsiniz.*

9.9.4. Anti-Spam Güncelleme Zamanlamasi

Gerçekten gerekliyse, ***Bu görevi etkinlestir*** ögesinin isaretini kaldirarak zamanlanmis Anti-Spam güncellemesini geçici olarak devre disi birakabilir ve daha sonra tekrar açabilirsiniz:



Bu iletisim kutusunda güncelleme zamanlamasi parametrelerinden bazilarini ayrintilariyla yapilandirabilirsiniz. ***Ad*** adindaki metin alani (*tüm varsayilan zamanlamalar için devre disi birakilmistir*) bu zamanlamaya program saticisi tarafindan atanan adi gösterir.

Programli çalistirma

Burada, yeni programlanan Anti-Spam güncellemesinin baslamasi için zaman araligi girin. Zamanlama belirli bir sürenin ardindan tekrarlanan Anti-Spam güncellemesi ile (***Her ...'de bir***) ya da kesin bir tarih ve saat tanimlayarak (***Belirli zaman araliklariyla çalistir***) ya da (***Bilgisayar***

baslangicinda) ilgili bir programin güncellemesiyle tanimlanabilir.

Gelismis program seçenekleri

Bu bölümde, bilgisayar düsük güç modundaysa veya tamamen kapatilmissa hangi kosullar altinda Anti-Spam güncellemesinin baslatilmasi/baslatilmamasi gerektigini belirleyebilirsiniz.

Diger güncelleme ayarlari

Internet baglantisi kuruldugunda güncellemeyi yeniden çalistir seçenegini isaretleyerek internet baglantisi kesildiginde ve Anti-Spam güncelleme islemi basarisiz oldugunda, internet baglantisi yeniden saglanir saglanmaz yeniden baslatilmasini saglayin.

Planlanan tarama islemi sizin belirlediginiz tarih ve saatte basladiktan sonra AVG sistem tepsisi simgesi üzerinde açilan bir açilir pencere vasitasiyla bilgilendirileceksiniz (*Gelismis Ayarlar/Görünüm iletisim kutusunun varsayilan yapilandirmasini degistirmemis olmaniz kaydiyla).*

9.10. Güncelleme

Güncelle navigasyonu ögesi, AVG güncellemesine iliskin genel parametreleri belirleyebileceginiz yeni bir iletisim kutusu açar:

Dosya güncelleme zamani

Bu bölümde, güncelleme islemi bilgisayarinizin yeniden baslatilmasini gerektiriyorsa, üç seçenek

arasindan birini belirleyebilirsiniz. Güncellemenin tamamlanmasi islemi, bilgisayarinizin bir sonraki yeniden baslatilma sürecine zamanlanabilir veya yeniden baslatma islemini hemen yapabilirsiniz:

- ***Kullanicidan onay iste*** *(varsayilan)* - güncelleme isleminin tamamlanmasi için gereken bilgisayarin yeniden baslatilmasi süreci için onayiniz istenir
- ***Hemen yeniden baslat*** - güncelleme islemi tamamlanir tamamlanmaz onayiniz istenmeden bilgisayariniz yeniden baslatilacaktir
- ***Bilgisayarin bir sonraki yeniden baslatilmasinda tamamla*** - güncelleme isleminin tamamlanmasi bilgisayarin bir sonraki yeniden baslatilmasina kadar ertelenir. Lütfen bu seçenegin yalnizca bilgisayarin düzenli olarak (en azindan günde bir kez) yeniden baslatildigini bilmeniz halinde önerildigini unutmayin!

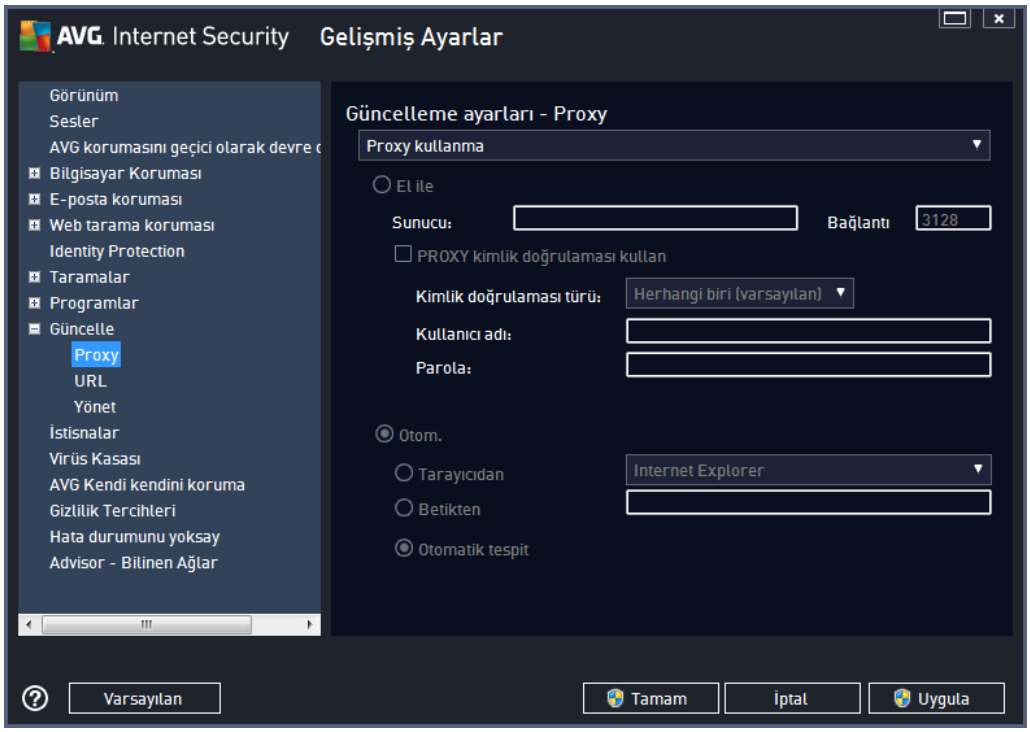
Güncelleme sonrasi bellek tarama

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

Ek güncelleme seçenekleri

- ***Her program güncellemesi sirasinda yeni sistem geri alma noktasi olustur*** (*varsayilan olarak açik*) - her AVG program güncelleme islemi baslamadan önce bir sistem geri yükleme noktasi olusturulur. Güncelleme isleminin basarisiz olmasi ve isletim sisteminizin çökmesi halinde isletim sisteminizi bu noktaya geri döndürebilirsiniz. Bu seçenege Baslat / Tüm Programlar / Donatilar / Sistem araçlari / Sistem Geri Yükleme yoluyla erisebilirsiniz fakat degisikliklerin sadece uzman kullanicilar tarafindan yapilmasi önerilmektedir! Bu fonksiyonu kullanmak istiyorsaniz bu kutucugu isaretleyin.
- ***DNS güncellemesini kullan*** (*varsayilan olarak açik*) - bu öge isaretlendiginde güncelleme islemi baslatildiginda **AVG Internet Security 2014** en yeni veritabani sürümüyle ve DNS sunucusundaki en yeni program sürümüyle ilgili bilgileri arar. Yalnizca en küçük, kesin olarak gerekli güncelleme dosyalari indirilir ve uygulanir. Bu sekilde, indirilen toplam veri miktari en düsük seviyede tutulur ve güncelleme süreci daha hizli bir sekilde gerçeklestirilir.
- ***Çalisan uygulamalari kapatmak için onay iste*** (*varsayilan olarak açik*) - o anda çalismakta olan uygulamalarin izniniz olmaksizin kapatilmamasini saglar (gerekirse güncelleme isleminin sonlandirilmasi için).
- ***Bilgisayar saatini kontrol et*** (*varsayilan olarak açik*) - bilgisayar saati ile dogru saat arasindaki fark belirlenen süreden uzun oldugunda bilgilendirilmek istediginizi belirtmek için bu seçenegi isaretleyin.

9.10.1. Proxy



Proxy sunucusu, Internet'e daha güvenli bir sekilde baglanmanizi saglayan bagimsiz bir sunucu ya da bilgisayarinizda çalisan bir hizmet programidir. Belirlenen ag kurallari dogrultusunda, Internet'e dogrudan ya da bir proxy sunucusu üzerinden ulasabilirsiniz; ayni anda her iki isleme de izin verilir. Bunun ardindan ***Güncelleme ayarlari - Proxy*** iletisim kutusunun ilk ögesinden asagidaki seçimleri yapmaniz gerekmektedir:

- ***Proxy kullanma*** - varsayilan ayarlar
- ***Proxy kullan***
- ***Proxy kullanarak baglanmayi dene; basarisiz olursa dogrudan baglan***

Proxy sunucusu kullanan herhangi bir seçenegi seçerseniz daha ayrintili bilgi girmeniz istenecektir. Sunucu ayarlari manüel ya da otomatik olarak yapilandirilabilir.

Manüel yapilandirma

Manüel yapilandirmayi seçerseniz (ilgili iletisim kutusu bölümünü etkinlestirmek için ***Manüel*** *seçenegini isaretleyin*) asagidaki bilgileri girmeniz gerekir:

- ***Sunucu*** - sunucunun IP adresini ya da sunucunun adini girin
- ***Baglanti Noktasi*** - internet erisimine açik baglanti noktasinin numarasini girin (*varsayilan olarak bu deger 3128 olarak atanmistir fakat isteginiz dogrultusunda degistirebilirsiniz; emin degilseniz lütfen ag yöneticiniz ile irtibat kurun*)

Proxy sunucusunda her kullanici için farkli kurallar yapilandirilabilir. Proxy sunucunuz bu sekilde yapilandirilmis ise proxy sunucusu üzerinden yapilan Internet baglantiniza iliskin kullanici adi ve parolanizi onaylamak için ***PROXY kimlik dogrulamasini kullan*** seçenegini isaretleyin.

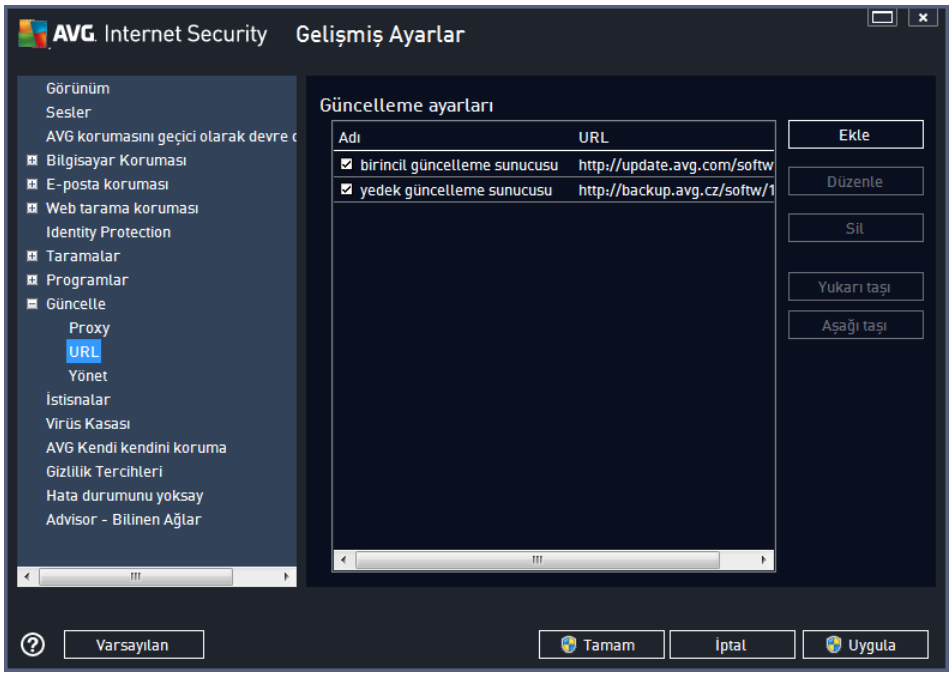
Otomatik yapilandirma

Otomatik yapilandirmayi seçerseniz (*ilgili iletisim kutusunu etkinlestirmek için **Oto** seçenegini isaretleyin*) ardindan proxy yapilandirmasinin nereden alinacagini belirleyin:

- ***Tarayicidan*** - yapilandirma varsayilan internet tarayicinizdan okunacaktir
- ***Komut satirindan*** - yapilandirma, proxy adresine dönme fonksiyonu olan indirilmis bir komut satirindan okunacaktir
- ***Otomatik Tespit Et*** - yapilandirma otomatik olarak dogrudan proxy sunucusundan tespit edilecektir

9.10.2. URL

URL iletisim kutusunda güncelleme dosyalarinin indirilebilecegi bir dizi internet adresi bulunur:



Kontrol dügmeleri

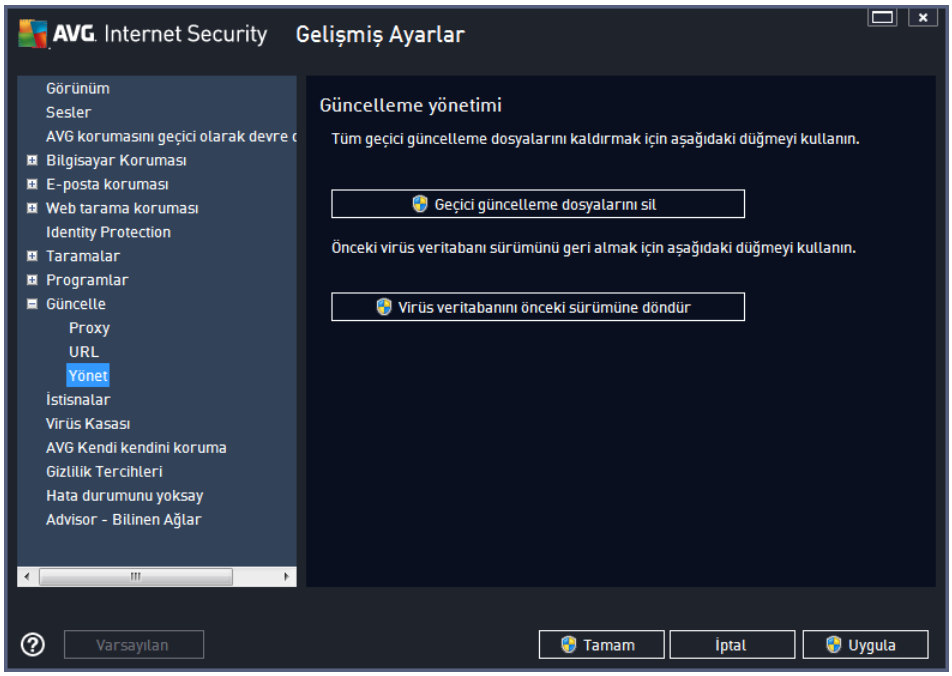
Liste ve liste ögeleri asagidaki kontrol dügmeleri kullanilarak düzenlenebilir:

- ***Ekle*** - listenize yeni bir URL eklemek için kullanacaginiz iletisim kutusunu açar
- ***Düzenle*** - seçilen URL parametrelerini düzenleyebileceginiz iletisim kutusunu açar

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

9.10.3. Yönetme

Güncelleme Yönetimi iletisim kutusu, iki adet dügme vasitasiyla erisilebilen iki seçenek sunmaktadir:

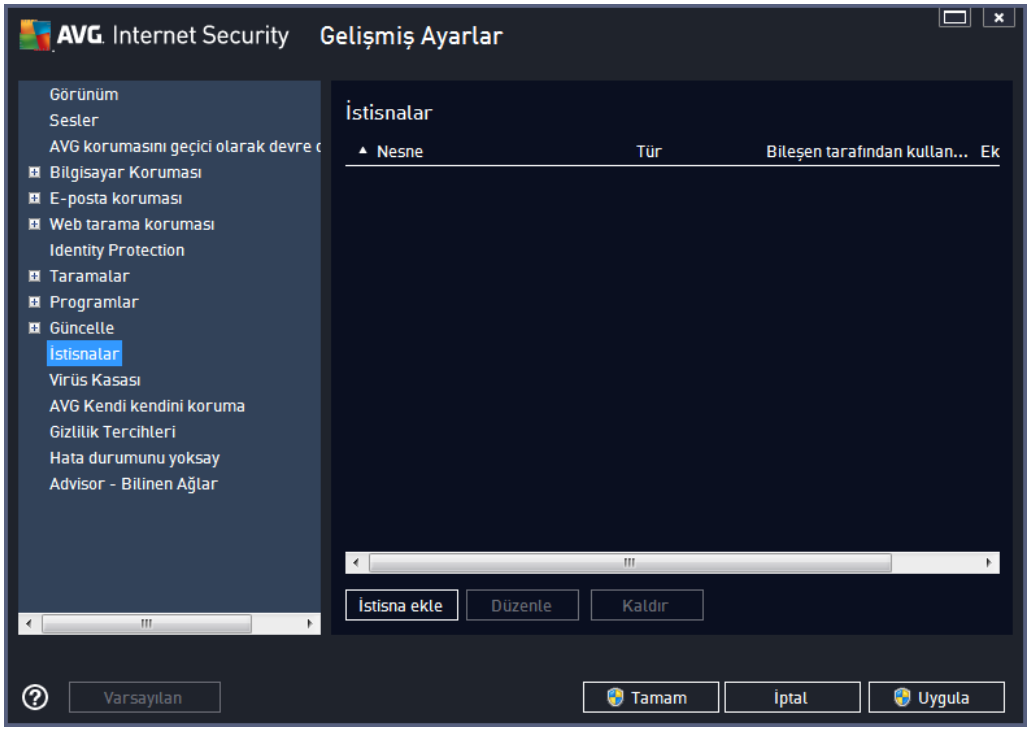


- ***Geçici güncelleme dosyalarini sil*** - tüm gereksiz güncelleme dosyalarini sabit diskinizden silmek için bu dügmeye basin (*varsayilan olarak söz konusu dosyalar 30 gün boyunca saklanir*)
- ***Virüs veritabanini bir önceki sürüme döndür*** - en güncel virüs veritabanini sabit diskinizden silmek ve daha önce kaydedilmis sürüme dönmek için bu dügmeye basin (*yeni virüs tabani sürümü, bir sonraki güncellemenin bir parçasi olacaktir*)

9.11. İstisnalar

Istisnalar iletisim kutusunda istisnalar, yani **AVG Internet Security 2014** uygulamasinin yok sayacagi ögeler tanimlayabilirsiniz. AVG bir program veya dosyayi sürekli biçimde tehdit olarak tespit ediyorsa veya güvenli bir web sitesini tehlikeli olarak engelliyorsa, bir istisna tanimlamaniz gerekir. Bu tür dosya veya web sitelerini istisna listesine eklediginizde AVG bunlari artik rapor etmez veya engellemez.

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



Iletisim kutusundaki tabloda, daha önce tanimlanan istisnalar varsa, bunlarin bir listesi görüntülenir. Her ögenin yaninda bir onay kutusu bulunur. Onay kutusu isaretliyse istisna etkindir. Isaretli degilse, istisna tanimlanmistir ancak simdilik kullanilmamaktadir. Sütun basligini tiklatarak, izin verilen ögeleri ilgili kritere göre siralayabilirsiniz.

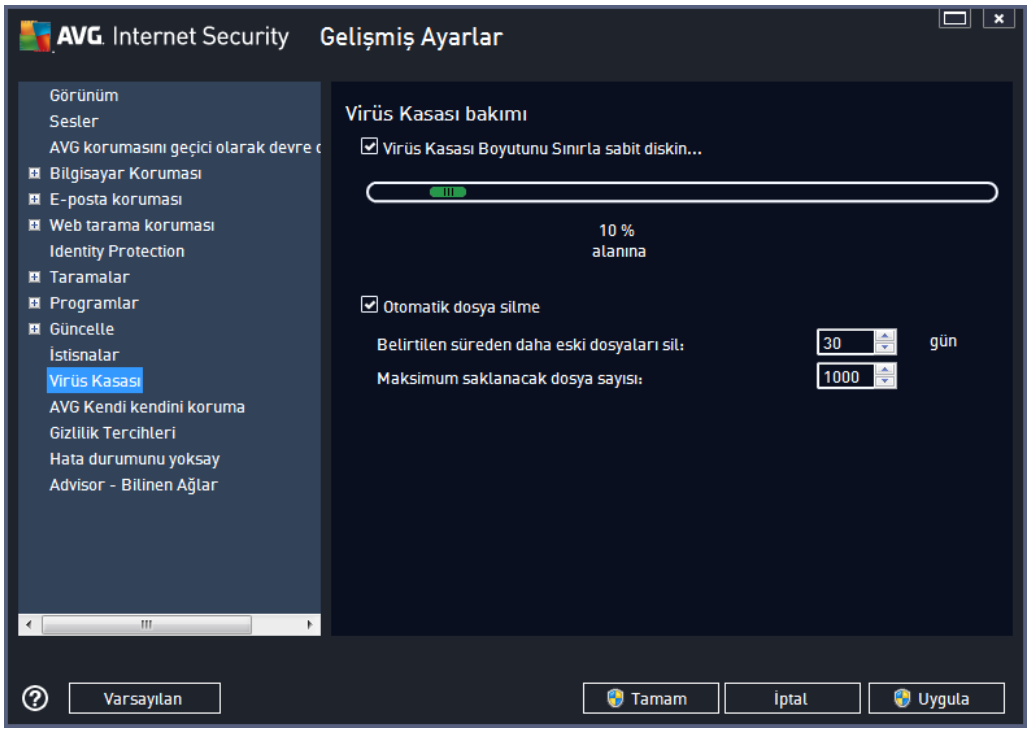
Kontrol dügmeleri

- ***Istisna ekle*** - AVG taramasinin disinda tutulacak bir öge belirleyebileceginiz yeni bir iletisim kutusu açmak için tiklatin. Önce, nesnenin türünü (dosya, klasör veya URL) belirlemeniz istenir. Ardindan ilgili nesnenin yolunu diskinizden bulmaniz veya URL'yi yazmaniz gerekir. Son olarak, hangi AVG özelliklerinin seçilen nesneyi yok sayacagini seçebilirsiniz *(Yerlesik Kalkan, Identity, Scan, Anti-Rootkit)*.

- ***Düzenle*** - Bu dügme ancak bazi istisnalar tanimlanmis ve tabloda listelenmisse etkin olur. Bu durumda seçilen bir istisna için düzenleme iletisim kutusunu açmak ve istisnanin parametrelerini yapilandirmak için bu dügmeyi kullanabilirsiniz.

- ***Kaldir*** - Bu dügmeyi önceden tanimlanmis bir istisnayi iptal etmek için kullanin. Istisnalari tek tek kaldirabilir veya listeden bir istisnalar blogunu vurgulayip tanimlanan istisnalari kaldirabilirsiniz. Istisna kaldirildiginda ilgili dosya, klasör veya URL AVG tarafindan yeniden kontrol edilir. Dosya veya klasörün kendisi degil, yalnizca istisna kaldirilir!

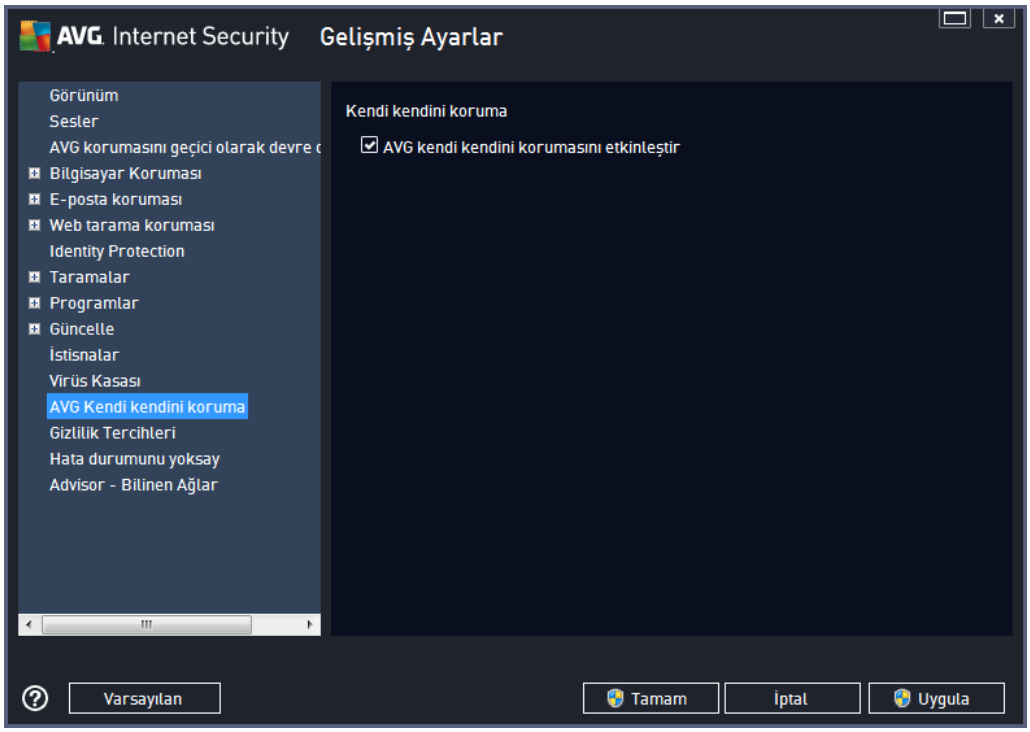
9.12. Virüs Kasası



Virüs Kasasi Bakimi iletisim kutusu, Virüs Kasasi'nda saklanan nesnelerin yönetimiyle ilgili çesitli parametreleri tanimlayabilmenizi saglar:

- ***Virüs Kasasi Boyutunu Sinirla*** - Virüs Kasasi'nin maksimum boyutunu ayarlamak için kaydiriciyi kullanin. Bu boyut, sabit diskinizin boyutu ile orantili olarak belirlenir.
- ***Otomatik dosya silme*** - bu bölümde nesnelerin Virüs Kasasi'nda depolanacaklari maksimum süreyi (***... Günden eski dosyalari sil***), Virüs Kasasi'nda depolanacak maksimum dosya sayisini (***Depolanacak maksimum dosya sayisi***) belirleyebilirsiniz.

9.13. AVG Kendi Kendini Koruma

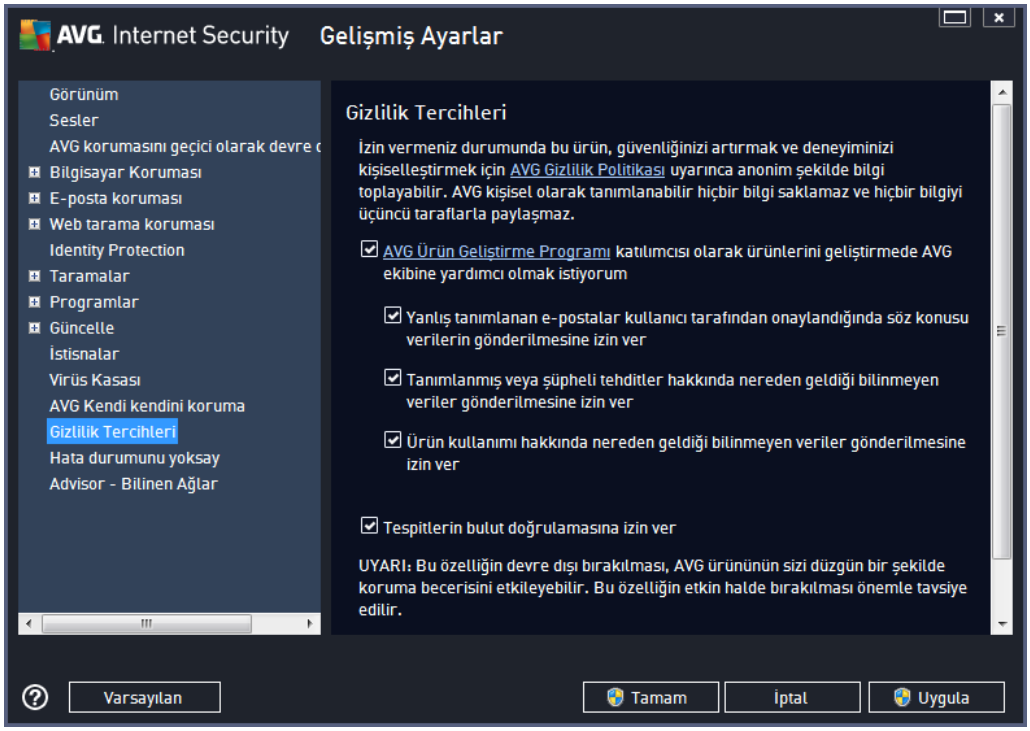


AVG Kendi Kendini Koruma , **AVG Internet Security 2014** yaziliminin kendi islem, dosya, kayit defteri anahtarlarini ve sürücülerini degistirilmekten ve devre disi birakilmaktan korur. Bu tür bir koruma sunmanin ana nedeni geliskin tehditlerin önce virüs koruma yazilimini devre disi birakip ardindan bilgisayariniza kolayca zarar verebilmesidir.

Bu özelligi açik tutmanizi öneririz!

9.14. Gizlilik Tercihleri

Gizlilik Tercihleri iletisim kutusu, sizi AVG ürün gelistirmesine katilmaya ve toplam internet güvenligi seviyesini artirmaya davet eder. Katiliminiz, dünyanin her tarafindaki katilimcilardan en son tehditlere iliskin güncel bilgileri toplamamiza ve koruma özelliklerini herkes için gelistirmemize yardimci olacaktir. Raporlama otomatik olarak yapilir, yani sizin için hiçbir rahatsizlik yaratmaz. Raporlarda hiçbir kisisel bilgi yer almaz. Tespit edilen tehditlerin rapor edilmesi istege baglidir, ancak, bu seçenegi açik birakmanizi rica ediyoruz. Böylece hem siz hem de diger AVG kullanicilari için korumayi gelistirmeye devam edebiliriz.



Iletisim kutusundaki mevcut ayarlama seçenekleri:

- ***AVG Ürün Gelistirme Programi'na katilarak AVG'nin ürünlerini gelistirmesine yardimci olmak istiyorum*** *(varsayilan olarak açik)* - **AVG Internet Security 2014** ürününü daha da gelistirmemize yardimci olmak istiyorsaniz onay kutusunu isaretli tutun. Bu sekilde, karsilasilan tüm tehditler AVG'ye bildirilir ve böylece biz tüm dünyadan kötü amaçli yazilimlarla ilgili güncel bilgileri toplayarak korumayi herkes için gelistirebiliriz. Raporlama islemi otomatik olarak gerçeklestirilir. Bu nedenle sizi hiçbir sekilde rahatsiz etmez ve raporlar kisisel bilgilerinizi içermez.
    - ***Kullanici onayi üzerine yanlis tanimlanan e-posta hakkinda veri gönderilmesine izin ver*** *(varsayilan olarak açik)* - yanlis bir sekilde istenmeyen posta olarak tanimlanan e-postalar veya Anti-Spam hizmeti tarafindan tespit edilmeyen istenmeyen postalar hakkinda bilgi gönderin. Bu tür bilgiler gönderilirken onayiniz istenir.
    - ***Algilanan veya süpheli tehditler hakkinda anonim veriler gönderilmesine izin ver*** *(varsayilan olarak açik)* - tüm süpheli veya olumlu bir sekilde tehlikeli kod veya davranis modeli hakkinda bilgi gönderin *(bilgisayarinizda tespit edilen virüs, casus yazilim veya erismeye çalistiginiz kötü amaçli web sitesi olabilir)*.
    - ***Ürün kullanimi hakkinda anonim bilgi gönderilmesine izin ver*** *(varsayilan olarak açik)* - tespit sayisi, yapilan taramalar, basarili veya basarisiz güncellemeler gibi uygulama kullanimi hakkinda temel istatistikler gönderin.
- ***Algilamalarin bulut dogrulamasina izin ver*** *(varsayilan olarak açik)* - hatali pozitif sonuçlari ayiklamak için tespit edilen tehditler gerçekten virüs bulasmasi içerip içermediklerinin belirlenmesi amaciyla denetlenir.

- ***AVG Personalization özelligini açarak AVG'nin deneyimimi kisisellestirmesini istiyorum*** *(varsayilan olarak kapali)* - bu özellik bilgisayarinizda yüklü program ve uygulamalarin davranisini anonim olarak analiz eder. AVG bu analizi degerlendirerek ihtiyaçlariniza en uygun hizmetleri sunarak güvenliginizi en üst düzeye çikarir.

En yaygin tehditler

Günümüzde, normal virüslerin disinda çok fazla tehdit bulunmaktadir. Kötü amaçli yazilimlarin ve tehlikeli web sitelerinin yazarlari çok yenilikçidir ve yeni tehdit türleri oldukça sik ortaya çikar, bunlarin oldukça büyük bir çogunlugu ise Internet üzerindedir. Bu tehditlerin en yaygin olanlari sunlardir:

- ***Virüs***, kendi kendini kopyalayan ve yayilan zararli bir koddur ve genellikle zarar olusana kadar fark edilmez. Bazi virüsler ciddi bir tehdit olusturur, dosyalari siler veya istedigi sekilde degistirir. Bazi virüsler ise görünüste zararsiz olan müzik çalma gibi islemler yapar. Ancak, tüm virüsler temel olarak sahip olduklari çogalma özelligi nedeniyle tehlikelidir; en basit virüs bile bilgisayarinizin tüm bellegini bir anda ele geçirebilir ve bilgisayarin çökmesine neden olur.

- ***Solucan***, normal virüsün aksine, "tasiyici" nesneye gerek duymayan bir virüs alt kategorisidir; genellikle e-posta yoluyla kendini diger bilgisayarlara gönderir ve e-posta sunuculari ve ag sistemlerinde asiri yüklenmeye neden olur.

- ***Casus yazilim***, genellikle zararli kategorisinde (*zararli yazilim = virüsler de dahil tüm kötü amaçli yazilimlar*) yer alan programlardir (genellikle Truva atlaridir). Bu tür yazilimlarin amaci kisisel bilgileri, sifreleri, kredi karti numaralarini çalmak veya bir bilgisayarin içine sizarak saldirganin bilgisayari uzaktan yönetmesini saglamaktir. Elbette, bunlarin hepsi bilgisayar sahibinin izni veya bilgisi olmadan yapilir.

- ***Potansiyel olarak istenmeyen programlar***, tehlikeli olabilecek ancak bilgisayariniz için mutlaka tehlikeli olmasi gerekmeyen bir casus yazilim türüdür. Özel bir PUP örnegi reklam yazilimlaridir. Bu yazilimlar, genellikle açilir pencerelerde reklam görüntülemek üzere tasarlanir. Can sikicidir ancak gerçekte zararli degildir.

- ***Izleme çerezleri*** de bir casus yazilim türü olarak degerlendirilebilir. Bu küçük dosyalar web tarayicisinda saklandigindan ve tekrar ziyaret ettiginizde "ana" web sitesine otomatik olarak gönderildiginden, tarama geçmisiniz ve benzer diger bilgiler gibi verileri içerebilir.

- ***Güvenlik açigi yazilimi***, isletim sistemindeki, Internet tarayicisindaki veya gerekli diger programlardaki bir açiktan faydalanan kötü amaçli bir koddur.

- ***Kimlik Avi***, kendilerini güvenilir veya taninmis kurulus gibi göstererek hassas kisisel verileri elde etme girisimidir. Genel olarak, potansiyel kurbanlara, örnegin banka hesabi bilgilerini güncellemelerini isteyen toplu e-postalarla ulasilir. Bunu yapmak için, kisilerden verilen baglantiyi ziyaret etmeleri istenir. Bu baglanti sahte bir banka web sitesine yönlendirir.

- ***Aldatmaca (Hoax)*** tehlikeli, uyarida bulunan veya yalnizca rahatsiz edici ve gereksiz bilgiler içeren toplu e-postalardir. Yukaridaki tehditlerin çogu, yayilmak üzere aldatici e-posta iletilerini kullanir.

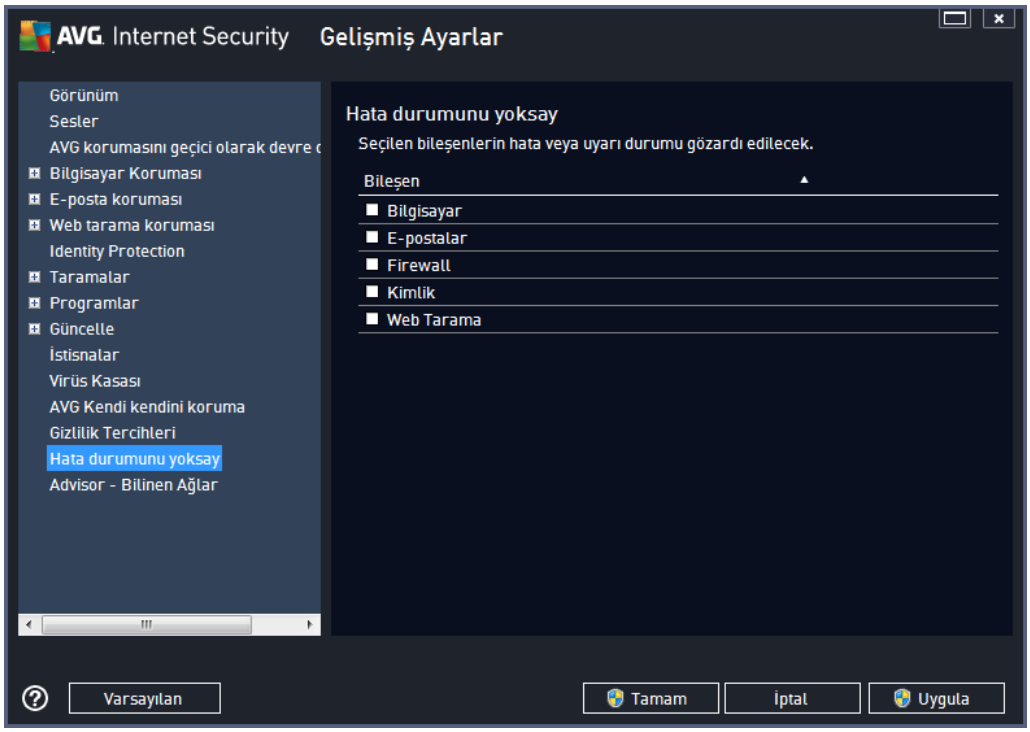
- ***Kötü amaçli web siteleri***, bilgisayariniza bilerek kötü amaçli yazilim yükleyen sitelerdir. Saldiriya ugrayan siteler de aynisini yapar ancak bunlar kötü amaçli ziyaretçiler tarafindan

zarar verilen yasal web siteleridir.

AVG Internet Security 2014 sizi farkli türlerdeki tüm bu tehditlerden korumak için özel bilesenler içerir. Bu bilesenlerin kisa bir açiklamasi için lütfen Bilesen Genel Görünümü bölümüne bakin.

9.15. Hata Durumunu Yoksay

Hata durumunu yoksay iletisim kutusunda, bilgilendirilmek istemediginiz bilesenleri seçebilirsiniz:



Varsayilan olarak listede herhangi bir bilesen seçilmemistir. Bilesenlerden herhangi biri hata verirse asagidaki yöntemlerden biri vasitasiyla uyarilacaksiniz demektir:

- sistem tepsisi simgesi - AVG'nin tüm bilesenleri dogru sekilde çalisirken simge, 4 renkli görünecektir ancak herhangi bir aksaklik olusursa simgenin yaninda sari bir ünlem isareti görülür,
- AVG ana penceresinin Güvenlik Durumu Bilgileri bölümünde mevcut sorun açiklanir

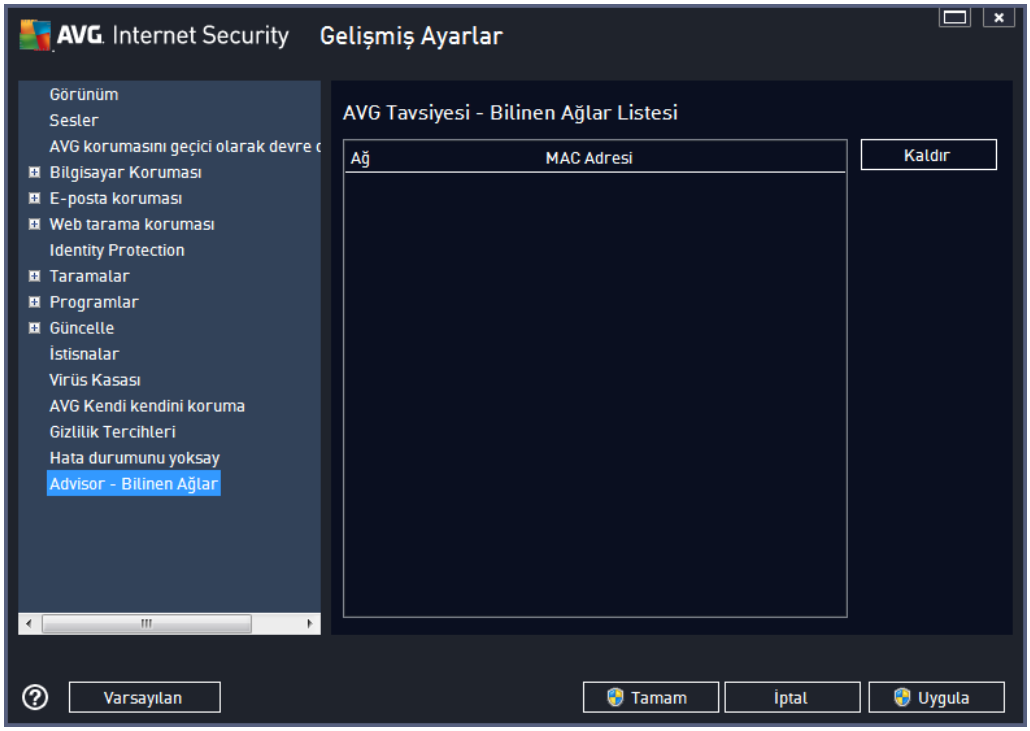
Belirli bir nedenle bilesenlerden birini geçici olarak kapatmaniz gereken bir durum olabilir. ***Bu önerilmez, tüm bilesenleri sürekli olarak açik ve varsayilan yapilandirmada tutmaniz gerekir***, ancak böyle bir durum meydana gelebilir. Bu durumda sistem tepsisi simgesi, otomatik olarak bilesenin hata durumunda oldugunu bildirir. Ancak bu durumda gerçek bir hatadan söz edemeyiz çünkü hatayi siz baslatmissinizdir ve potansiyel riskin farkinda olmalisiniz. Ayni zamanda, simge gri renkli görüntülendikten sonra daha sonra meydana gelecek hatalari rapor edemez.

Bu durumda, ***Hata durumunu yoksay*** iletisim kutusunda hata durumunda olan (*ya da kapatilmis*) bilesenleri seçebilirsiniz ve söz konusu durum hakkinda bilgilendirilmek istemeyebilirsiniz. Onaylamak için ***Tamam*** dügmesine basin.

9.16. Advisor - Bilinen Ağlar

AVG Advisor baglandiginiz aglari izleyen ve yeni bir ag bulundugunda *(daha önce kullanilan bir ag adina sahip oldugundan karisikliga neden olabilecek bir ag)* sizi bilgilendiren ve agin güvenligini kontrol etmenizi öneren bir özellige sahiptir. Yeni aglarin baglanmak için güvenli olduguna karar verirseniz, bunlari listeye de kaydedebilirsiniz *(Bilinmeyen bir ag tespit edildiginde sistem tepsisi üzerinde hareket eden AVG Tavsiyesi tepsi bildiriminde saglanan baglanti yoluyla. Ayrintilar için lütfen AVG Tavsiyesi hakkindaki bölüme bakin.)*. AVG Tavsiyesi bu islemin ardindan agin benzersiz özniteliklerini hatirlar *(özellikle de MAC adresini)* ve bir dahaki sefere bildirim göstermez. Baglandiginiz her ag otomatik olarak bilinen ag olarak degerlendirilir ve listeye eklenir. ***Kaldir*** dügmesine basarak herhangi bir girisi silebilirsiniz; bu durumda ilgili ag tekrar bilinmeyen ve muhtemelen güvensiz ag olarak degerlendirilir.

Bu iletisim kutusunda hangi aglarin bilinen olarak siniflandirildigini kontrol edebilirsiniz:



Not: *AVG Tavsiyesi'ndeki bilinen aglar özelligi Windows XP 64 bit sürümünde desteklenmez.*

10. Güvenlik Duvarı Ayarları

Firewall yapilandirmasi, çesitli iletisim kutularinda bilesenin gelismis parametrelerini yapilandirabileceginiz yeni bir pencere açar. Firewall yapilandirmasi bilesenin gelismis parametrelerini birkaç farkli yapilandirma iletisim kutusunda düzenleyebileceginiz yeni bir pencerede açilir. Yapilandirma temel modda veya uzman modunda görüntülenebilir. Yapilandirma penceresine ilk girdiginizde temel mod su parametrelerin düzenleme seçenekleriyle açilir:

- Genel
- Uygulamalar
- Dosya ve Yazici Paylasimi

Iletisim kutusunun altinda ***Uzman modu*** dügmesini bulabilirsiniz. Dügmeye basarak çok daha gelismis Firewall yapilandirma seçeneklerinin yer aldigi iletisim kutusunu açabilirsiniz:

- Gelismis ayarlar
- Tanimlanan aglar
- Sistem hizmetleri
- Günlükler

Ancak, yazilim saticisi tüm AVG Internet Security 2014 bilesenlerini optimum performans saglayacak sekilde ayarlamistir. Bunun için iyi bir nedeniniz olmadikça varsayilan yapilandirmayi degistirmeyin. Ayarlarda yapilacak her tür degisiklik sadece deneyimli bir kullanici tarafindan gerçeklestirilmelidir!

10.1. Genel

Genel bilgiler iletisim kutusu mevcut Firewall modlari hakkinda genel bilgiler sunar. Firewall modunun geçerli seçimi menüden baska bir mod seçilerek degistirilebilir.

Ancak, yazilim saticisi tüm AVG Internet Security 2014 bilesenlerini optimum performans saglayacak sekilde ayarlamistir. Bunun için iyi bir nedeniniz olmadikça varsayilan yapilandirmayi degistirmeyin. Ayarlarda yapilacak her tür degisiklik sadece deneyimli bir kullanici tarafindan gerçeklestirilmelidir!

Firewall, bilgisayarinizin bir alanda bulunmasina, bagimsiz bir bilgisayar veya bir dizüstü bilgisayar olmasina bagli olarak özel güvenlik kurallari tanimlamaniza olanak tanir. Bu seçeneklerin her biri için farkli bir koruma seviyesi gerekir ve bu seviyeler de ilgili modlarin kapsamindadir. Kisaca, Firewall modu Firewall bileseni için özel bir yapilandirmadir ve bu sekilde önceden tanimlanmis çok sayida yapilandirmayi kullanabilirsiniz:

- ***Otomatik*** - Firewall, bu modda tüm ag trafigini otomatik olarak denetler. Hiçbir karar için onayiniz istenmez. Firewall bilinen tüm uygulamalarla baglantiya izin verir ve ayni zamanda uygulamaya her zaman baglanabilmesi için bir kural olusturulur. Firewall, diger uygulamalar için uygulamanin davranisina bagli olarak uygulamaya yönelik izin veya engelleme kararini verir. Ancak, böyle durumlarda kural olusturulmaz ve uygulama her baglanmaya çalistiginda kontrol edilir. ***Otomatik mod arka planda dikkat çekmeden çalisir ve çogu kullanici için önerilen moddur.***

- ***Interaktif*** - bilgisayarinizda gelen ve giden tüm ag trafigini tam olarak kontrol etmek istiyorsaniz bu mod kullanislidir. Firewall trafigi sizin için izler ve tüm iletisim ve veri aktarim girisimlerinden sizi haberdar ederek girisimi uygun gördügünüz biçimde engellemenizi veya izin vermenizi saglar. Yalnizca ileri düzey kullanicilar için önerilir.

- ***Internet erisimini engelle*** - internet baglantisi tamamen engellenir, internete erisemezsiniz ve disaridan hiç kimse de bilgisayariniza erisemez. Yalnizca özel ve kisa süreli kullanim içindir.

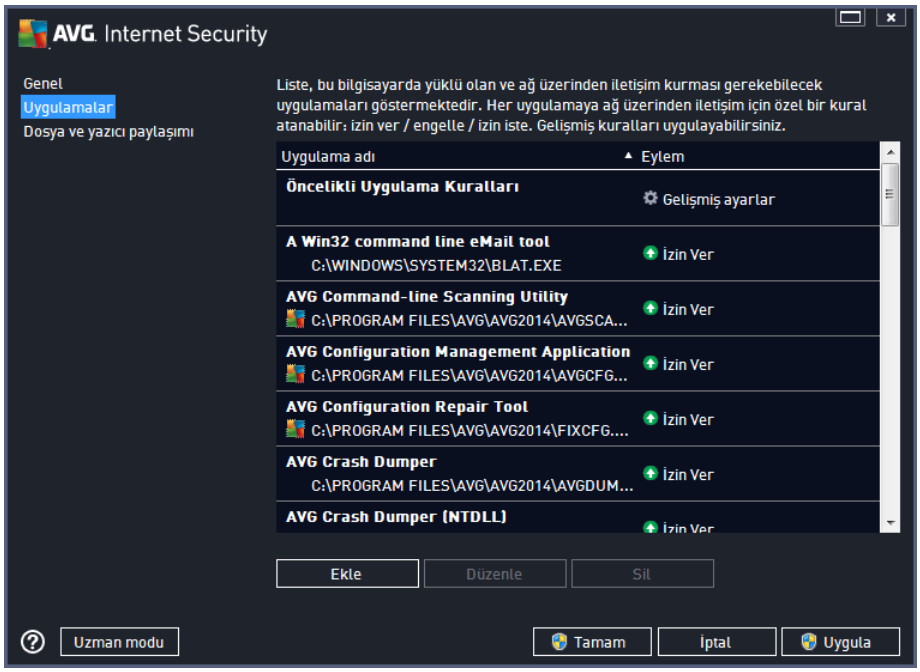
- ***Güvenlik duvari korumasini kapat*** - Firewall korumasinin devre disi birakilmasi bilgisayarinizda gelen ve giden tüm trafige izin verir. Sonuç olarak, bilgisayariniz hacker saldirilarina açik hale gelir. Lütfen bu seçenegi kullanirken çok dikkatli olun.

Not: Firewall içinde de bir otomatik mod mevcuttur. Bu mod, Bilgisayar veya Identity protection bileseni kapatildiginda ve bu nedenle bilgisayariniz tehditlere açik hale geldiginde sessizce etkinlestirilir. Bu tür durumlarda, Firewall yalnizca bilinen veya kesinlikle güvenli uygulamalara otomatik olarak izin verir. Diger tüm uygulamalar için sizin karar vermeniz istenir. Bunun nedeni

devre disi birakilan bilesenlerin boslugunu kapatmak ve bilgisayarinizi güvende tutmaktir.

10.2. Uygulamalar

Uygulama iletisim kutusu, ag üzerinden o ana kadar iletisim kurmaya çalisan tüm uygulamalari ve ilgili islem için atanan eylemlerin simgelerini listeler:



Uygulama listesi'ndeki uygulamalar, bilgisayarinizda tespit edilenlerdir (*ve atanan ilgili islemlerdir*). Kullanilabilir islem türleri:

- - tüm aglar için iletisime izin ver
- - iletisimi engelle
- - gelismis ayarlar tanimlandi

Yalnizca önceden yüklü olan uygulamalarin tespit edilebildigini unutmayin. Varsayilan olarak, yeni uygulama ag üzerinden ilk defa baglanmaya çalistiginda, güvenli veritabanlarina göre Firewall onun için otomatik olarak bir kural olusturacak veya iletisime izin vermek mi yoksa engellemek mi istediginizi soracaktir. Ikinci durumda, yanitinizi kalici bir kural olarak kaydedebileceksiniz (daha sonra bu iletisim kutusunda listelenecek).

Elbette, yeni uygulama için hemen kural tanimlayabilirisiniz. Bu iletisim kutusunda, ***Ekle*** seçenegine basin ve uygulama bilgilerini girin.

Listede, uygulamalarin disinda iki özel öge vardir. ***Öncelikli Uygulama Kurallari*** (*listenin üst kisminda*) tercihe baglidir ve her zaman tek bir uygulamanin kurallarindan önce uygulanir. ***Diger Uygulama Kurallari*** (*listenin alt kisminda bulunur*) örnegin bilinmeyen veya tanimlanmayan bir uygulama için özel uygulama kurallari uygulanmadiginda "son örnek" olarak kullanilir. Böyle bir uygulama ag üzerinden iletisim kurmaya çalistiginda baslatilacak islemi seçin: Engelle *(iletisim her zaman engellenir)*, Izin ver *(tüm aglar üzerinden iletisime izin verilir)*, Sor *(iletisime yönelik izin verme*

veya engelleme tercihi size birakilir). ***Bu ögelerin genel uygulamalardan farkli ayar seçenekleri bulunur ve bunlar yalnizca deneyimli kullanicilara yöneliktir. Ayarlari degistirmemenizi önemle öneririz!***

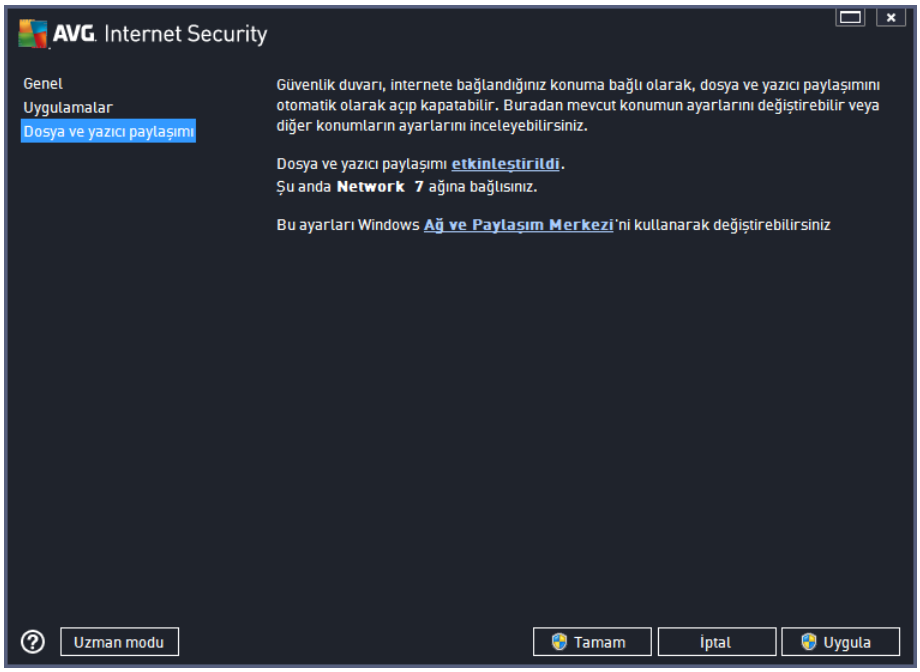
Kontrol dügmeleri

Liste, asagidaki denetim dügmeleri kullanilarak düzenlenebilir:

- ***Ekle*** - yeni uygulama kurallarini tanimlamak için bos bir iletisim kutusu açar.
- ***Düzenle*** - var olan bir uygulamanin kural kümesinin düzenlenmesi için saglanan verilerle ayni iletisim kutusunu açar.
- ***Sil*** - seçilen uygulamayi listeden siler.

10.3. Dosya ve yazıcı paylaşımı

Dosya ve yazici paylasimi Windows, ortak disk birimleri, yazicilar, tarayicilar ve tüm benzer cihazlarda "Paylasilan" olarak isaretlediginiz tüm dosyalar veya klasörler anlamina gelmektedir. Bu tür ögelerin paylasimi yalnizca güvenli oldugu düsünülen aglarda gerçeklestirilmelidir *(örnegin evde, iste veya okulda)*. Ancak, herkese açik aglara *(havaalani Wi-Fi veya internet kafe agi gibi)* baglaniyorsaniz, hiçbir sey paylasmak istemeyebilirsiniz. AVG Firewall paylasimi kolayca engelleyip izin verebilir ve daha önce ziyaret ettiginiz aglarla ilgili seçiminizi kaydetmenizi saglar.



Dosya ve Yazici Paylasimi iletisim kutusunda dosya ve yazici paylasimi ve o anda bagli olan aglarin yapilandirmasini düzenleyebilirsiniz. Window XP'de, ag adi ilgili aga ilk baglandiginizda ag için seçtiginiz adlandirmaya karsilik gelir. Windows Vista ve üstü sistemlerde, ag adi Ag ve Paylasim Merkezi'nden otomatik olarak alinir.

10.4. Gelişmiş ayarlar

Gelismis ayarlar iletisim kutusundaki tüm düzenleme seçenekleri YALNIZCA DENEYIMLI KULLANICILAR için tasarlanmistir!

Gelismis ayarlar iletisim kutusu asagidaki Firewall parametrelerini etkinlestirmenizi veya devre disi birakmanizi saglar:

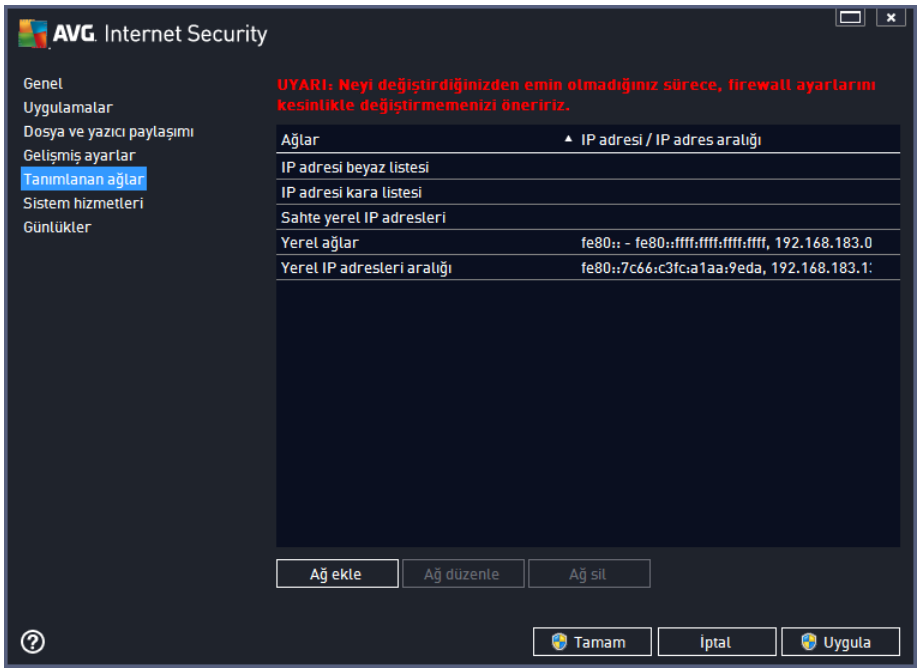
- ***Firewall tarafindan desteklenen sanal makinelere/makinelerden tüm trafige izin ver*** - VMWare gibi sanal makinelerde ag baglantisi için destek.
- ***Sanal özel aglara (VPN) tüm trafige izin ver*** - VPN baglantilari *(uzak bilgisayarlari baglamak için kullanilir)* için destek.
- ***Bilinmeyen gelen/giden trafigi günlük dosyasina kaydet*** - bilinmeyen uygulamalardan kaynaklanan tüm iletisim girisimleri*(gelen/giden)* Firewall günlügü dosyasinda kaydedilir.
- ***Tüm uygulama kurallari için kural dogrulamayi devre disi birak*** - Firewall sürekli olarak her uygulama kurali kapsamindaki tüm dosyalari izler. Ikili dosyada bir degisiklik gerçeklestiginde, Firewall bir kez daha standart yöntemle, yani sertifikasini dogrulayarak, güvenilir uygulamalar veritabaninda arayarak vb. bir yolla uygulamanin güvenilirligini onaylamaya çalisir. Uygulama güvenli olarak degerlendirilmezse Firewall uygulama için seçilen moda göre islem yapar:
    - Firewall ***Otomatik mod***'da çalisiyorsa uygulamaya varsayilan olarak izin verilir;
    - Firewall ***Etkilesimli mod***'da çalisiyorsa uygulama engellenir ve kullaniciya uygulama için nasil bir islem yapilmasini istedigini soran bir iletisim kutusu görüntülenir.

Belirli bir uygulamaya yönelik olarak nasil islem yapilacagiyla ilgili istenen süreç Uygulamalar

iletisim kutusunda her uygulama için ayri ayri tanimlanabilir.

10.5. Tanımlanan ağlar

Tanimlanan aglar iletisim kutusundaki tüm düzenleme seçenekleri YALNIZCA DENEYIMLI KULLANICILAR için tasarlanmistir!

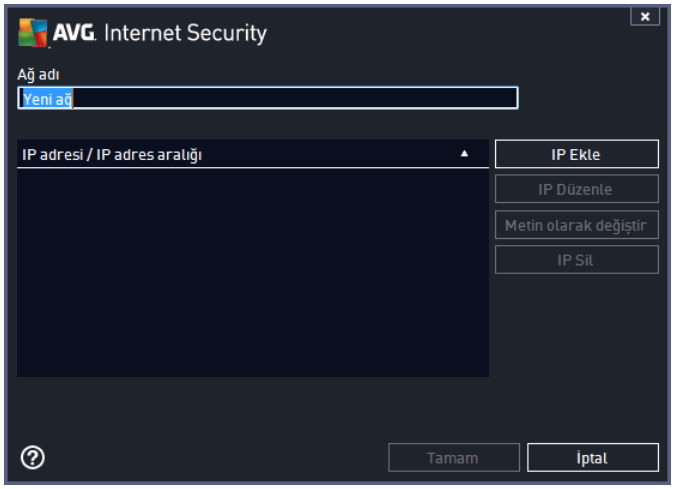


Tanimlanan aglar iletisim kutusunda bilgisayarinizin bagli oldugu aglar görüntülenir. Liste algilanan her agla ilgili asagidaki bilgileri saglar:

- ***Aglar*** - bilgisayarin bagli oldugu tüm aglarin adlarini listeler.
- ***IP adresi araligi*** - her ag otomatik olarak tespit edilir ve IP adresi araligi formunda belirtilir.

Kontrol dügmeleri

- ***Ag ekle*** - yeni tanimlanan agin parametrelerini düzenleyebileceginiz yeni bir iletisim penceresi açar; örnegin ***Ag adi*** girmek ve ***IP adresi araligi*** belirlemek için:

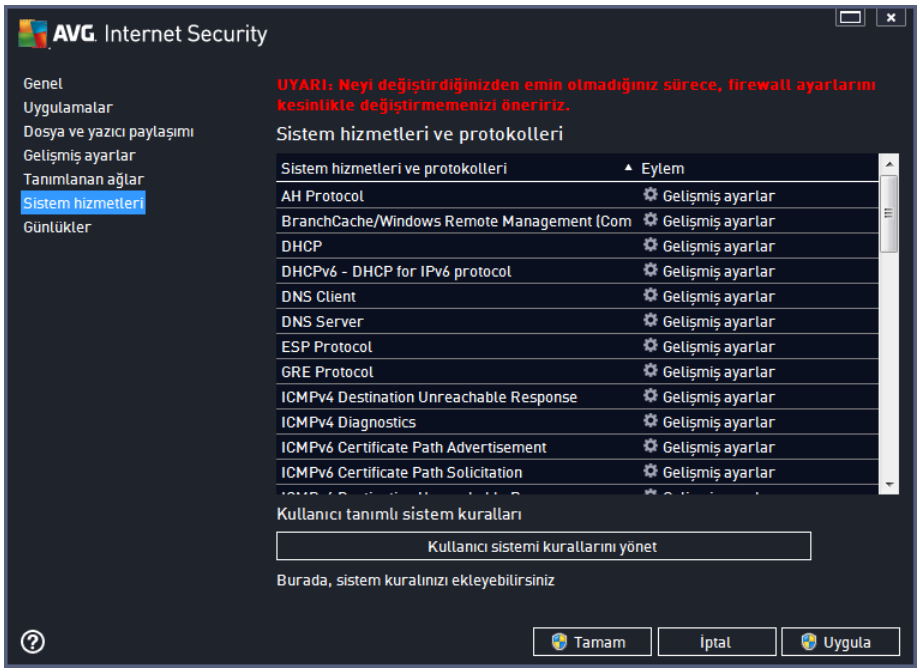


- ***Agi düzenle*** - mevcut durumda tanimlanmis agin parametrelerini düzenleyebileceginiz ***Ag özellikleri*** iletisim kutusunu açar (*yukari bakiniz*) (*bu pencere yeni ag ekleme penceresi ile aynidir, bir önceki paragrafta verilen açiklamalari okuyunuz*).

- ***Agi sil***, seçilen ag ile ilgili referansi ag listesinden siler.

10.6. Sistem hizmetleri

Sistem hizmetleri ve protokolleri iletisim kutusu içinde yapilacak tüm düzeltmeler YALNIZCA DENEYIMLI KULLANICILAR içindir!



Sistem hizmetleri ve protokolleri iletisim kutusu, ag üzerinden iletisim kurulmasi gerekebilen Windows standart sistem servisleri ve protokollerini listeler. Grafik asagidaki sütunlari içerir:

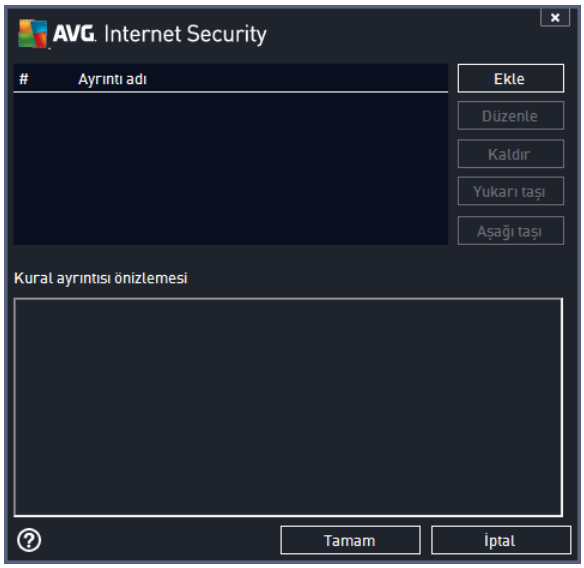
- ***Sistem hizmeti ve protokolleri*** - Bu sütun ilgili sistem hizmetinin adini gösterir.

- ***Eylem*** - Bu sütun atanan eylemin simgesini görüntüler:
    - o Tüm aglar için iletisime izin ver
    - o İletisimi engelle

Listedeki ögelerin ayarlarini düzenlemek için (*atanan eylemler de dahil* olmak üzere), ögeyi sag tiklatin ve ***Düzenle***'yi seçin. ***Ancak, sistem kurallarinin düzenlenmesi yalnizca gelismis kullanicilar tarafindan yapilmalidir ve kesinlikle sistem kurallarini düzenlememeniz önerilir!***

Kullanici tanimli sistem kurallari

Kendi sistem hizmeti kuralinizi tanimlamak üzere yeni bir iletisim kutusu açmak için (*asagidaki resme bakin*), ***Kullanici sistemi kurallarini yönet*** dügmesine basin. Sistem hizmetleri ve protokolleri listesindeki mevcut ögelerden herhangi birinin yapilandirmasini düzenlemeye karar verirseniz ayni iletisim kutusu açilir. Bu iletisim kutusunun üst kismi geçerli olarak düzenlenen sistem kuralinin tüm ayrintilarinin genel bir görünümünü görüntüler, alt kisim seçili ayrintiyi gösterir. Ilgili dügmeyle bir ayrintilar kurali düzenlenebilir, eklenebilir veya silinebilir:



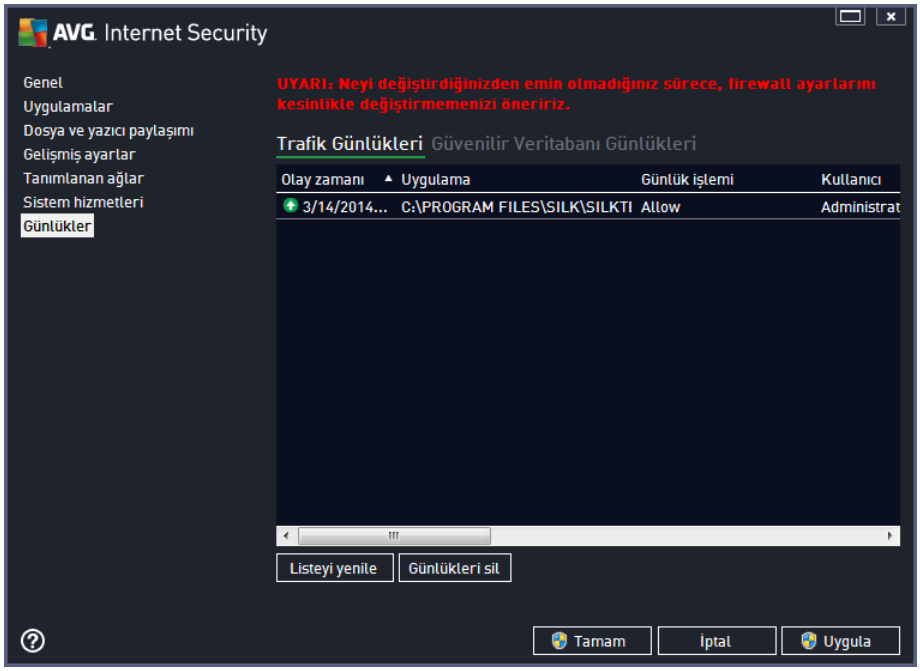
Ayrinti kurali ayarlarinin gelismis ayarlar oldugunu ve Firewall yapilandirmasi üzerinde tam denetime sahip olmasi gereken ag yöneticilerine yönelik tasarlandigini lütfen unutmayin. Iletisim protokolleri türleri, ag baglanti noktasi numaralari, IP adresi tanimlari vb. hakkinda bilginiz yoksa, lütfen bu ayarlari degistirmeyin! Yapilandirmayi gerçekten degistirmeniz gerekiyorsa, belirli ayrintilar için lütfen ilgili iletisim kutusunun yardim dosyalarina basvurun.

10.7. Günlükler

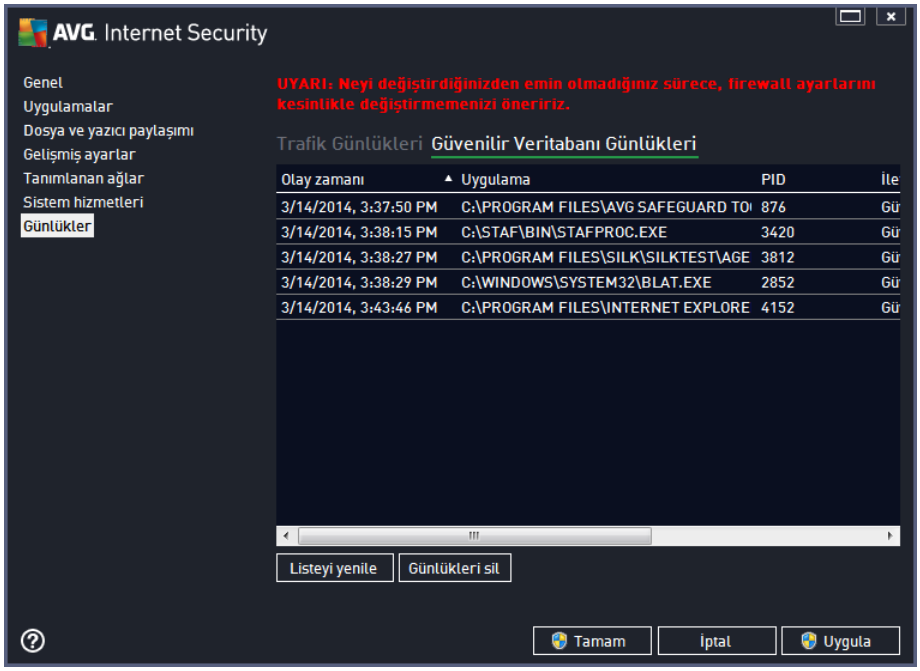
Günlükler iletisim kutusundaki tüm düzenleme seçenekleri YALNIZCA DENEYIMLI KULLANICILAR için tasarlanmistir!

Günlükler iletisim kutusu, kaydedilen tüm Firewall eylemlerini ve etkinliklerini ilgili parametrelerin ayrintili tanimlari ile birlikte iki sekmede görüntüleyebilmenizi saglar.

- ***Trafik Günlükleri*** - Bu sekme aga baglanmaya çalisan tüm uygulamalarin etkinlikleri hakkindaki bilgileri sunar. Her öge için olay zamani, uygulama adi, ilgili günlük islemi, kullanici adi, PID, trafik yönü, protokol türü, uzak ve yerel baglanti noktalarinin numaralariyla yerel ve uzak IP adresleri hakkindaki bilgileri bulabilirsiniz.



- ***Güvenilir Veritabani Günlükleri*** - *Güvenilir veritabani*, her zaman çevrimiçi iletisime izin verebilen sertifikali ve güvenilir uygulamalar hakkinda bilgi toplayan AVG dahili veritabanidir. Yeni bir uygulama aga ilk baglanmaya çalistiginda (*diger bir deyisle, bu uygulama için henüz güvenlik duvari kurali belirtilmediginde*), ilgili uygulama için ag iletisimine izin verilip verilmeyecegini ögrenmek önemlidir. Ilk önce, AVG *Güvenilir veritabanini* arar ve uygulama listelenmisse otomatik olarak aga erisim izni verir. Ancak bundan sonra, veritabaninda uygulama hakkinda mevcut bilgi yoksa, uygulamanin aga erismesine izin vermek isteyip istemediginiz tek bir iletisim kutusuyla size sorulur.



Kontrol dügmeleri

- ***Listeyi yenile*** - kaydedilen tüm parametreler seçilen davranis özelliklerine göre düzenlenebilir: kronolojik olarak (*tarihler*) ya da alfabetik olarak (*diger sütunlarda*) sadece ilgili sütun basligini tiklatin. O anda görüntülenen bilgileri yenilemek için ***Listeyi yenile*** dügmesini kullanin.

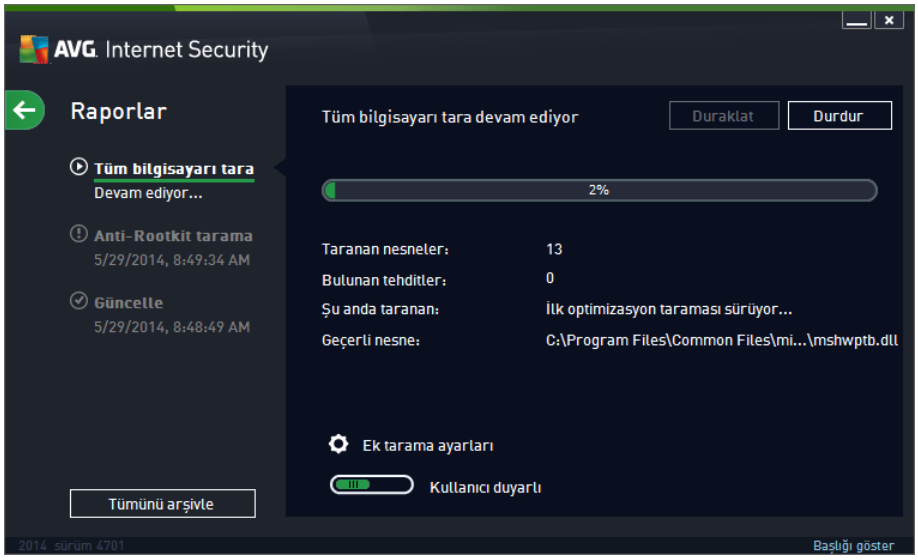
- ***Günlükleri sil*** - tablodaki tüm girisleri silmek için basin.

11. AVG Tarama

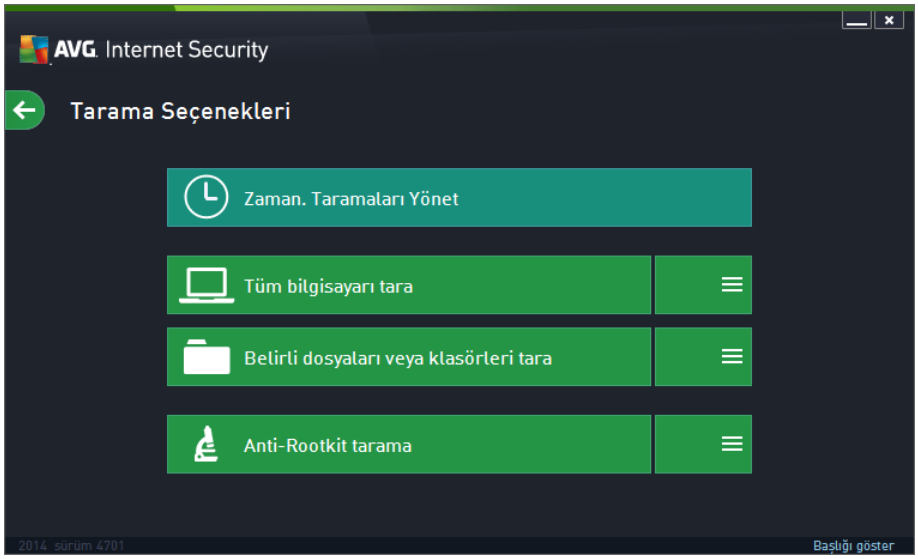
Varsayilan olarak, **AVG Internet Security 2014** ilk taramadan sonra oldugu gibi hiçbir taramayi çalistirmaz *(sizin baslatmaniz istenir)*, her zaman korumada olan **AVG Internet Security 2014** ürününün yerlesik bilesenleri ile mükemmel olarak korunuyor olmaniz ve hiçbir kötü amaçli yazilimin bilgisayariniza hiçbir surette girmesine izin vermemeniz gerekir. Elbette belirli araliklarda çalistirilacak bir tarama planlayabilir veya bir taramayi gereksinimlerinize göre el ile baslatabilirsiniz.

AVG tarama arayüzüne ana kullanici arayüzünden grafik olarak iki bölüme ayrilmis dügme araciligiyla erisilebilir: 

- ***Simdi Tara*** - Tüm Bilgisayari Tara islemini hemen baslatmak için dügmeye basin; ilerleme ve sonuçlari otomatik olarak açilan Raporlar penceresinden izleyin:



- ***Seçenekler*** - Bu dügmeyi seçerek *(grafik olarak yesil bir alanda üç yatay çizgi olarak görünür)* ***Tarama Seçenekleri*** iletisim kutusunu açip burada zamanlanmis taramalari yönetebilir ve Tüm Bilgisayari Tara / Belirli Dosyalari veya Klasörleri Tara parametrelerini düzenleyebilirsiniz:



Tarama Seçenekleri iletisim kutusunda üç ana tarama yapilandirmasi bölümü görebilirsiniz:

- ***Zaman. taramalari yönet*** - Tüm tarama zamanlamalarinin genel görünümünü içeren yeni bir iletisim kutusu açmak için bu seçenegi tiklatin. Kendi taramalarinizi tanimlamadan önce, listede yalnizca yazilim saglayicisi tarafindan önceden tanimlanmis tek bir zamanlanmis tarama görebilirsiniz. Tarama varsayilan olarak kapatilmistir. Taramayi açmak için sag tiklatin ve baglam menüsünden *Görevi etkinlestir*'i seçin. Zamanlanmis tarama etkinlestirildiginde *Tarama zaman. düzenle* dügmesiyle taramanin yapilandirmasini düzenleyebilirsiniz. Kendi istediginiz yeni bir tarama zamanlamasi olusturmak için *Tarama zaman. ekle* dügmesini de tiklatabilirsiniz.

- ***Tüm bilgisayari tara / Ayarlar*** - Dügme iki kisma ayrilmistir. Tüm bilgisayarinizin taranmasini hemen baslatmak için *Tüm bilgisayari tara* seçenegini tiklatin *(tüm bilgisayar taramasiyla ilgili ayrintilar için lütfen Öntanimli taramalar / Tüm bilgisayari tarama baslikli bölüme bakin). Ayarlar* bölümünü tiklatirsaniz tüm bilgisayari tarama isleminin yapilandirma iletisim kutusunu açarsiniz.

- ***Belirli dosyalari veya klasörleri tara / Ayarlar*** - Bu dügme de iki kisma ayrilmistir. Bilgisayarinizda seçtiginin alanlarin taranmasini hemen baslatmak için *Belirli dosyalari veya klasörleri tara* seçenegini tiklatin *(belirli dosya ve klasörlerin taranmasiyla ilgili ayrintilar için lütfen Öntanimli taramalar / Belirli dosyalari veya klasörleri tarama baslikli bölüme bakin). Ayarlar* bölümünü tiklatirsaniz belirli dosyalari veya klasörleri tarama isleminin yapilandirma iletisim kutusunu açarsiniz.

- ***Bilgisayarda rootkit'leri tara / Ayarlar*** - Dügmenin *Bilgisayarda rootkit'leri tara* olarak etiketlenen soldaki bölümü hemen anti-rootkit taramasini baslatir *(rootkit taramasi hakkindaki ayrintilar için lütfen Öntanimli Taramalar / Bilgisayarda rootkit'leri tara adli ilgili bölüme bakin). Ayarlar* bölümünü tiklatirsaniz rootkit taramasinin yapilandirma iletisim kutusunu açarsiniz.

11.1. Öntanımlı Taramalar

AVG Internet Security 2014 programinin ana özelliklerinden biri istek üzerine taramadir. Istege bagli taramalar, muhtemel bir virüs hakkinda süpheye düstügünüz an bilgisayarinizin istediginiz kisminda istediginiz zaman yapabileceginiz taramalardir. Kisacasi, bilgisayarinizda virüs oldugunu düsünmeseniz bile söz konusu taramalarin düzenli araliklarla yapilmasi önerilmektedir.

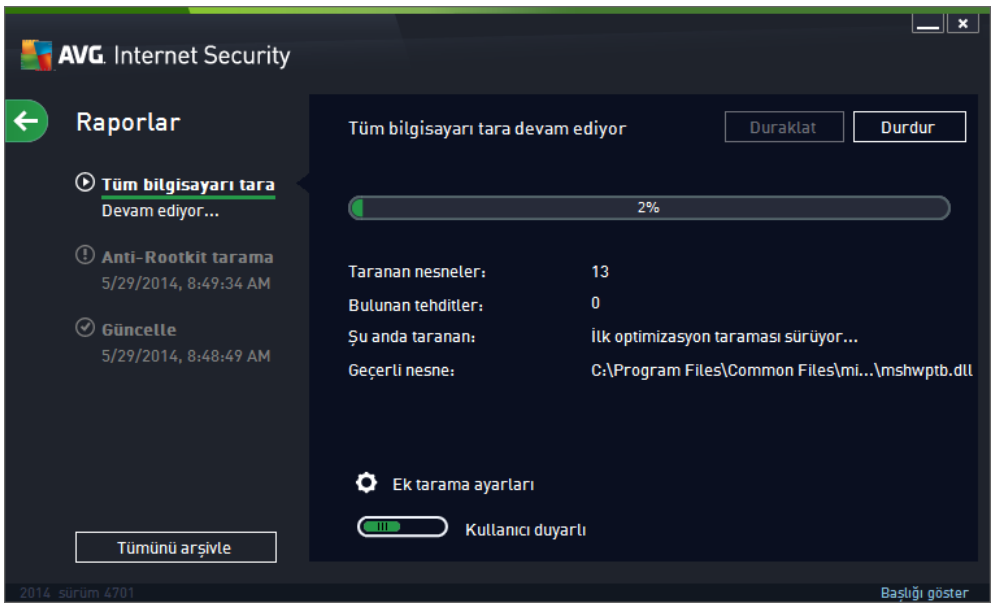
AVG Internet Security 2014 içinde, yazilim saticisinin önceden tanimladigi asagidaki tarama türlerini bulacaksiniz:

11.1.1. Tüm bilgisayarı tara

Tüm bilgisayari tara tüm bilgisayari muhtemel bulasmalara ve/veya potansiyel olarak istenmeyen programlara karsi tarar. Bu tarama, bilgisayarinizin tüm sabit disklerini tarayacak, virüsleri tespit edecek ve temizleyecek ya da tespit edilen bulasmayi Virüs Kasasi'na tasiyacaktir. Bilgisayarin tümü haftada en az bir defa taranmalidir.

Tarama baslatma

Tüm bilgisayari tara islemi dogrudan ana kullanici arayüzünden ***Simdi tara*** dügmesi tiklatilarak baslatilabilir. Bu tür tarama için baska bir yapilandirma yapmaya gerek yoktur; tarama hemen baslar. ***Tüm bilgisayari tarama devam ediyor*** iletisim kutusunda (*ekran resmine bakin*) ilerlemeyi ve sonuçlari izleyebilirsiniz. Tarama islemi gerekirse geçici olarak kesintiye ugratilabilir (***Duraklat***) ya da iptal edilebilir (***Durdur***).



Tarama yapilandirmasi düzenleme

Tüm bilgisayari tara yapilandirmasini ***Tüm bilgisayari tara - Ayarlar*** iletisim kutusunda düzenleyebilirsiniz *(iletisim kutusuna Tarama seçenekleri iletisim kutusundaki Tüm bilgisayari tara isleminin Ayarlar baglantisindan erisilebilir).* ***Degistirmek için geçerli bir nedeniniz olmadigi müddetçe varsayilan ayarlari korumaniz önerilir!***

Tarama parametreleri listesindeki belirli parametreleri isteginiz dogrultusunda açip kapatabilirsiniz:

- ***Bulasmayi bana sormadan temizle / kaldir*** *(varsayilan olarak açik)* - Tarama sirasinda virüs tanimlanirsa, bir giderme yazilimi mevcutsa otomatik olarak temizlenir. Bulasmis dosya otomatik olarak temizlenemezse, bulasmis nesne Virüs Kasasi'na tasinir.

- ***Potansiyel Olarak Istenmeyen Programlari ve Casus Yazilim tehditlerini rapor et*** *(varsayilan olarak açik)* - Virüslerin yani sira casus yazilimlari da taramak için isaretleyin. Casus yazilim, süpheli kötü amaçli yazilim kategorisini ifade eder: genellikle bir güvenlik riskini olusturmasina ragmen bu programlardan bazilari bilerek yüklenebilir. Bilgisayarinizin güvenligini artirdigindan, bu özelligi etkin durumda tutmanizi öneririz.

- ***Potansiyel Olarak Istenmeyen Programlar gelismis grubunu rapor et*** *(varsayilan olarak kapali)* - Casus yazilimlarin, yani dogrudan üreticiden alinan tamamen zararsiz olan, ancak daha sonra kötüye kullanilabilecek programlarin genisletilmis paketlerinin tespit edilmesi için isaretleyin. Bu, bilgisayar güvenliginizi daha da artiran ek bir önlemdir, ancak yasal programlari da engelleyebilir ve bu yüzden varsayilan olarak kapalidir.

- ***Izleme Çerezleri için tara*** *(varsayilan olarak kapali)* - Bu parametre, tespit edilmesi istenen çerezleri tanimlar; *(HTTP çerezleri kimlik dogrulamasi, izleme ve kullanicilar hakkindaki site tercihleri veya elektronik alisveris sepetlerinin içerigi gibi belirli bilgilerin korunmasi için kullanilir)*.

- ***Arsivleri tara*** *(varsayilan olarak kapali)* - Bu parametre, ZIP, RAR vb. arsiv dosyalarinin içinde sikistirilmis dosyalarin bile taranmasini saglar.

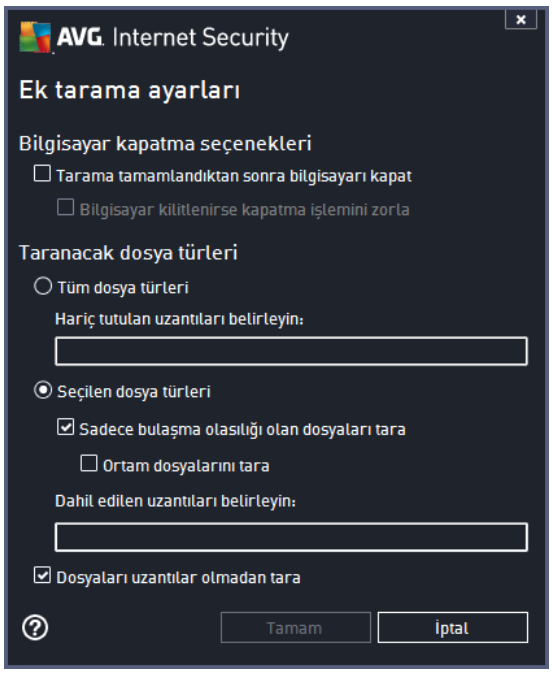
- ***Bulussal Analiz Yöntemlerini Kullan*** *(varsayilan olarak açik)* - Bulussal analiz yöntemi *(taranan nesnenin komutlarinin sanal bir bilgisayar ortaminda dinamik olarak canlandirilmasi)* tarama sirasinda kullanilacak virüs tespiti yöntemlerinden biridir.

- ***Sistem ortamini tara*** *(varsayilan olarak açik)* - Tarama islemi, bilgisayarinizin sistem alanlarini da kontrol edecektir.

- ***Kapsamli taramayi etkinlestir*** *(varsayilan olarak kapali)* - Belirli durumlarda *(bilgisayariniza bulasma olmasindan süpheleniyorsaniz)* yalnizca emin olmak üzere bilgisayarinizin bulasma olmasi çok zor olan alanlarini bile tarayan en kapsamli tarama algoritmalarini etkinlestirmek için bu seçenegi isaretleyebilirsiniz. Ancak, bu yöntemin çok fazla zaman aldigini unutmayin.

- ***Rootkit'leri tara*** *(varsayilan olarak açik)*: tüm bilgisayar taramasina anti-rootkit taramasini dahil eder. Anti-rootkit taramasi ayri olarak da baslatilabilir.

- ***Ek tarama ayarlari*** - baglanti, su parametreleri belirtebileceginiz yeni bir Ek tarama ayarlari iletisim kutusu açar:



  - ***Bilgisayar kapatma seçenekleri*** - Çalisan tarama islemi bittiginde bilgisayarin otomatik olarak kapatilmasi gerekip gerekmedigine karar verir. Bu seçenegi seçerseniz (***Tarama bittikten sonra bilgisayari kapat***) bilgisayar mevcut durumda kilitli olsa bile bilgisayarin kapatilmasini saglayan bir seçenegin bulundugu bir pencere açilacaktir (***Bilgisayar kilitliyse bilgisayari kapanmaya zorla***).

  - ***Taranacak dosya türleri*** - taranacak dosya türleriyle ilgili asagidaki tercihlerden birini yapmaniz gerekir:

    - ***Tüm dosya türleri*** taranmamasi gereken virgülle ayrilmis dosya uzantilarinin listesini saglayarak taramada istisnalari tanimlama seçenegiyle;

    - ***Seçili dosya türleri*** - yalnizca virüs bulasabilme olasiligi olan dosyalari taramayi istediginizi belirtebilirsiniz (*virüs bulasamayan dosyalar taranmayacaktir, örnegin, bazi düz metin dosyalari veya bazi diger çalistirilamayan dosyalar*); ortam dosyalari (*video, ses dosyalari - bu onay kutusunun isaretini kaldirirsaniz, bu dosyalar genellikle çok büyük oldugundan ve virüs bulasma olasiliklari çok az oldugundan tarama süresini daha da azaltir*). Tekrar, her zaman taranmasi gereken dosyalari uzantilarina göre belirtebilirsiniz.

➢ Istege bagli olarak, ***Uzantilari olmayan dosyalari taramaya*** da karar verebilirsiniz ve bu seçenek varsayilan olarak açiktir ve gerçekten bir nedeniniz yoksa degistirmemeniz önerilir. Uzantisi olmayan dosyalar süpheli olabilir ve her zaman taranmalidir.

- ***Taramanin ne kadar hizli tamamlanacagini ayarlayin*** - tarama sürecinin önceligini degistirmek için kaydirma çubugunu kullanabilirsiniz. Varsayilan olarak, bu seçenek otomatik kaynak kullaniminin *kullaniciya duyarli* seviyesine ayarlidir. Alternatif olarak, sistem kaynaklari kullanimini minimize etmek için tarama islemini yavaslatabilir (*bilgisayarda çalismaniz gerektigi ancak taramanin ne kadar sürdügünü önemsemediginiz durumlar için uygundur*) veya sistem kaynaklarini daha yogun kullanmak suretiyle daha hizli bir sekilde (*örn., bilgisayar geçici bir süreyle kullanilmadiginda*) çalistirabilirsiniz.

- ***Tarama raporu olustur*** - baglanti üzerinden ***Tarama Raporlari*** isimli bir iletisim kutusu açilir ve buradan ne tip bulunturlarin rapor edileceginiz seçebilirsiniz:

Uyari: *Bu tarama parametreleri, yeni tanimlanan taramanin parametreleri ile aynidir - AVG Taramasi / Tarama zamanlama / Tarama Tipi bölümünde açiklandigi dogrultuda.* ***Tüm bilgisayari tara*** *fonksiyonunun varsayilan yapilandirmasini degistirmeye karar verirseniz yeni ayarlarinizi, belirli dosya ya da klasörlerin taranmasi için kullanilacak varsayilan yapilandirma olarak atayabilirsiniz.*

11.1.2. Belirli dosyaları veya klasörleri tara

Belirli Dosyalari veya Klasörleri Tara - bilgisayarinizin sadece taranmasi için seçtiginiz alanlarini tarar (*seçilen klasörler, sabit diskler, disket sürücüleri, CD'ler vb.*). Virüs tespiti ve temizlenmesi sirasinda tarama islemi, tüm bilgisayar taramasi ile aynidir. Bulunan virüsler temizlenir ya da Virüs Kasasi'na tasinir. Belirli dosyalari veya klasörleri tara islevi, kendi testlerinizi ve gereksinimlerinize bagli olarak bunlarin programlamasini ayarlamak için kullanilabilir.

Tarama baslatma

Belirli dosyalari veya klasörleri tara islemi dogrudan Tarama seçenekleri iletisim kutusundaki **Belirli dosyalari veya klasörleri tara** dügmesi tiklatilarak baslatilabilir. Yeni bir ***Taramak için belirli dosya ve klasörleri seçin*** iletisim kutusu açilir. Bilgisayarinizin agaç görünümünden taranmasini istediginiz klasörleri seçin. Seçilen klasörlerin her birine giden yol, otomatik olarak olusturulacak ve iletisim kutusunun üst kismindaki metin alaninda görüntülenecektir. Belirli bir klasör taranirken içinde bulunan klasörlerin taranmamasi gibi bir seçenek de vardir. Bunu yapabilmek için otomatik olarak olusturulan yolun basina "**-**" isareti koyun (*ekran görüntülerini inceleyin*). Klasörün tümünü tarama disinda tutmak için "!" parametresini kullanin. Son olarak, taramayi baslatabilmek

için ***Taramayi baslat*** dügmesine basin. Tarama isleminin kendisi temel olarak Tüm bilgisayari tara islemi ile aynidir.

Tarama yapilandirmasi düzenleme

Belirli Dosyalari veya Klasörleri Tara yapilandirmasini ***Belirli Dosyalari veya Klasörleri Tara - Ayarlar*** iletisim kutusunda düzenleyebilirsiniz*(iletisim kutusuna Tarama seçenekleri iletisim kutusundaki Belirli dosyalari veya klasörleri tara seçeneginde yer alan Ayarlar baglantisindan erisilebilir).* ***Degistirmek için geçerli bir nedeniniz olmadigi müddetçe varsayilan ayarlari korumaniz önerilir!***

Tarama parametreleri listesinde parametreleri ihtiyaçlariniza uygun olarak açabilir / kapatabilirsiniz:

- ***Bulasmayi bana sormadan temizle / kaldir*** *(varsayilan olarak açi)*: Tarama sirasinda virüs

tanimlanirsa, bir giderme yazilimi mevcutsa otomatik olarak temizlenir. Bulasmis dosya otomatik olarak temizlenemezse, bulasmis nesne Virüs Kasasi'na tasinir.

- ***Potansiyel Olarak Istenmeyen Programlari ve Casus Yazilim tehditlerini rapor et*** *(varsayilan olarak açik)*: Virüslerin yani sira casus yazilimlari da taramak için isaretleyin. Casus yazilim, süpheli kötü amaçli yazilim kategorisini ifade eder: genellikle bir güvenlik riskini olusturmasina ragmen bu programlardan bazilari bilerek yüklenebilir. Bilgisayarinizin güvenligini artirdigindan, bu özelligi etkin durumda tutmanizi öneririz.

- ***Potansiyel Olarak Istenmeyen Programlar gelismis grubunu rapor et*** *(varsayilan olarak kapali)*: Casus yazilimlarin, yani dogrudan üreticiden alinan tamamen zararsiz olan, ancak daha sonra kötüye kullanilabilecek programlarin genisletilmis paketlerinin tespit edilmesi için isaretleyin. Bu, bilgisayar güvenliginizi daha da artiran ek bir önlemdir, ancak yasal programlari da engelleyebilir ve bu yüzden varsayilan olarak kapalidir.

- ***Izleme Çerezleri için tara*** *(varsayilan olarak kapali)*: Bu parametre, tespit edilmesi istenen çerezleri tanimlar; *(HTTP çerezleri kimlik dogrulamasi, izleme ve kullanicilar hakkindaki site tercihleri veya elektronik alisveris sepetlerinin içerigi gibi belirli bilgilerin korunmasi için kullanilir)*.

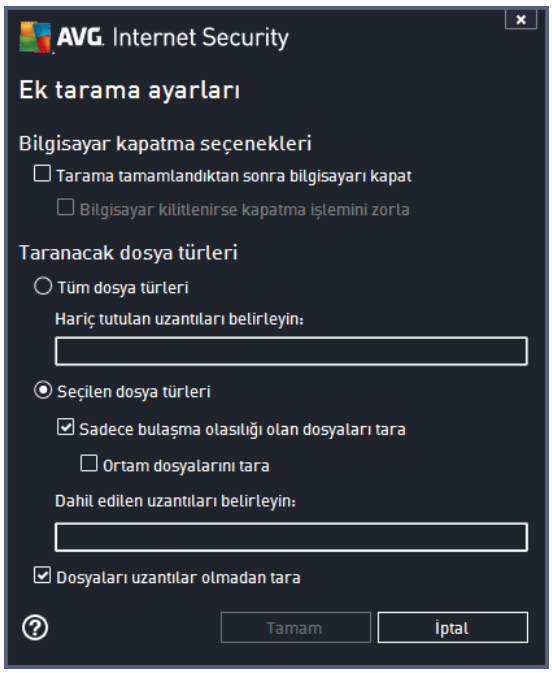
- ***Arsivleri tara*** *(varsayilan olarak açik)*: Bu parametre, ZIP, RAR vb. arsiv dosyalarinin içinde sikistirilmis dosyalarin bile taranmasini saglar.

- ***Bulussal Analiz Yöntemlerini Kullan*** *(varsayilan olarak açik)*: Bulussal analiz yöntemi *(taranan nesnenin komutlarinin sanal bir bilgisayar ortaminda dinamik olarak canlandirilmasi)* tarama sirasinda kullanilacak virüs tespiti yöntemlerinden biridir.

- ***Sistem ortamini tara*** *(varsayilan olarak kapali)*: Tarama islemi, bilgisayarinizin sistem alanlarini da kontrol edecektir.

- ***Kapsamli taramayi etkinlestir*** *(varsayilan olarak kapali)*: Belirli durumlarda*(bilgisayariniza bulasma olmasindan süpheleniyorsaniz)* yalnizca emin olmak üzere bilgisayarinizin bulasma olmasi çok zor olan alanlarini bile tarayan en kapsamli tarama algoritmalarini etkinlestirmek için bu seçenegi isaretleyebilirsiniz. Ancak, bu yöntemin çok fazla zaman aldigini unutmayin.

- ***Ek tarama ayarlari*** - Baglanti, su parametreleri belirtebileceginiz yeni bir ***Ek tarama ayarlari*** iletisim kutusu açar:



- ***Bilgisayar kapatma seçenekleri*** - Çalisan tarama islemi bittiginde bilgisayarin otomatik olarak kapatilmasi gerekip gerekmedigine karar verir. Bu seçenegi seçerseniz (***Tarama bittikten sonra bilgisayari kapat***) bilgisayar mevcut durumda kilitli olsa bile bilgisayarin kapatilmasini saglayan bir seçenegin bulundugu bir pencere açilacaktir (***Bilgisayar kilitliyse bilgisayari kapanmaya zorla***).

- ***Taranacak dosya türleri*** - taranacak dosya türleriyle ilgili asagidaki tercihlerden birini yapmaniz gerekir:

  - ***Tüm dosya türleri*** taranmamasi gereken virgülle ayrilmis dosya uzantilarinin listesini saglayarak taramada istisnalari tanimlama seçenegiyle;

  - ***Seçili dosya türleri*** - yalnizca virüs bulasabilme olasiligi olan dosyalari taramayi istediginizi belirtebilirsiniz (*virüs bulasamayan dosyalar taranmayacaktir, örnegin, bazi düz metin dosyalari veya bazi diger çalistirilamayan dosyalar*); ortam dosyalari (*video, ses dosyalari - bu onay kutusunun isaretini kaldirirsaniz, bu dosyalar genellikle çok büyük oldugundan ve virüs bulasma olasiliklari çok az oldugundan tarama süresini daha da azaltir*). Tekrar, her zaman taranmasi gereken dosyalari uzantilarina göre belirtebilirsiniz.

  - Istege bagli olarak, ***Uzantilari olmayan dosyalari taramaya*** da karar verebilirsiniz ve bu seçenek varsayilan olarak açiktir ve gerçekten bir nedeniniz yoksa degistirmemeniz önerilir. Uzantisi olmayan dosyalar süpheli olabilir ve her zaman taranmalidir.

- ***Taramanin ne kadar hizli tamamlanacagini ayarlayin*** - tarama sürecinin önceligini degistirmek için kaydirma çubugunu kullanabilirsiniz. Varsayilan olarak, bu seçenek otomatik kaynak kullaniminin *kullaniciya duyarli* seviyesine ayarlidir. Alternatif olarak, sistem kaynaklari kullanimini minimize etmek için tarama islemini yavaslatabilir (*bilgisayarda çalismaniz gerektigi ancak taramanin ne kadar sürdügünü önemsemediginiz durumlar için uygundur*) veya sistem kaynaklarini daha yogun kullanmak suretiyle daha hizli

bir sekilde (*ör., bilgisayar geçici bir süreyle kullanilmadiginda*) çalistirabilirsiniz.

- ***Tarama raporu olustur*** - baglanti üzerinden ***Tarama Raporlari*** isimli yeni bir iletisim kutusu açilir ve buradan ne tip potansiyel bulgularin rapor edilecegini seçebilirsiniz:

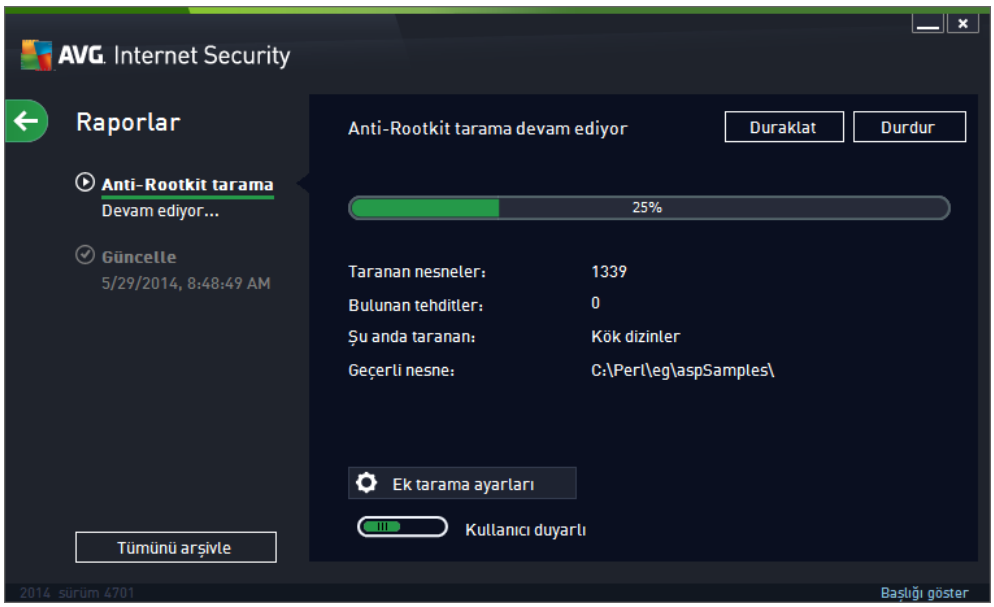
Uyari: *Bu tarama parametreleri, yeni tanimlanan taramanin parametreleri ile aynidir - AVG Taramasi / Tarama zamanlama / Tarama Tipi bölümünde açiklandigi dogrultuda.* ***Belirli dosya veya klasörleri tara*** *fonksiyonunun varsayilan yapilandirmasini degistirmeye karar verirseniz yeni ayarlarinizi, belirli dosya ya da klasörlerin taranmasi için kullanilacak varsayilan yapilandirma olarak atayabilirsiniz. Buna ek olarak söz konusu yapilandirma tüm yeni programli taramalariniz için sablon görevi görecektir (tüm özellestirilmis taramalar, Seçilen dosya ya da klasörleri tara fonksiyonunun mevcut yapilandirmasina dayanmaktadir).*

11.1.3. Bilgisayarda rootkit'leri tara

Bilgisayarda rootkit'leri tara tehlikeli rootkit'leri, diger bir deyisle bilgisayarinizdaki tehlikeli yazilimlarin varligini gizleyen program ve teknolojileri tespit edip etkili bir biçimde silen özel bir araçtir. Rootkit, bir bilgisayar sisteminin kontrolünü, sistem sahiplerinin ve yasal yöneticilerinin izni olmaksizin ele geçirmek için tasarlanmis bir programdir. Tarama islemi öntanimli bir kurallar setine göre rootkit'leri tespit edebilir. Bir rootkit bulunmasi kesin olarak bir bulasma oldugu anlamina gelmez. Rootkit'ler bazen sürücülerde kullanilir ya da dogru uygulamalarin bir parçasi olabilir.

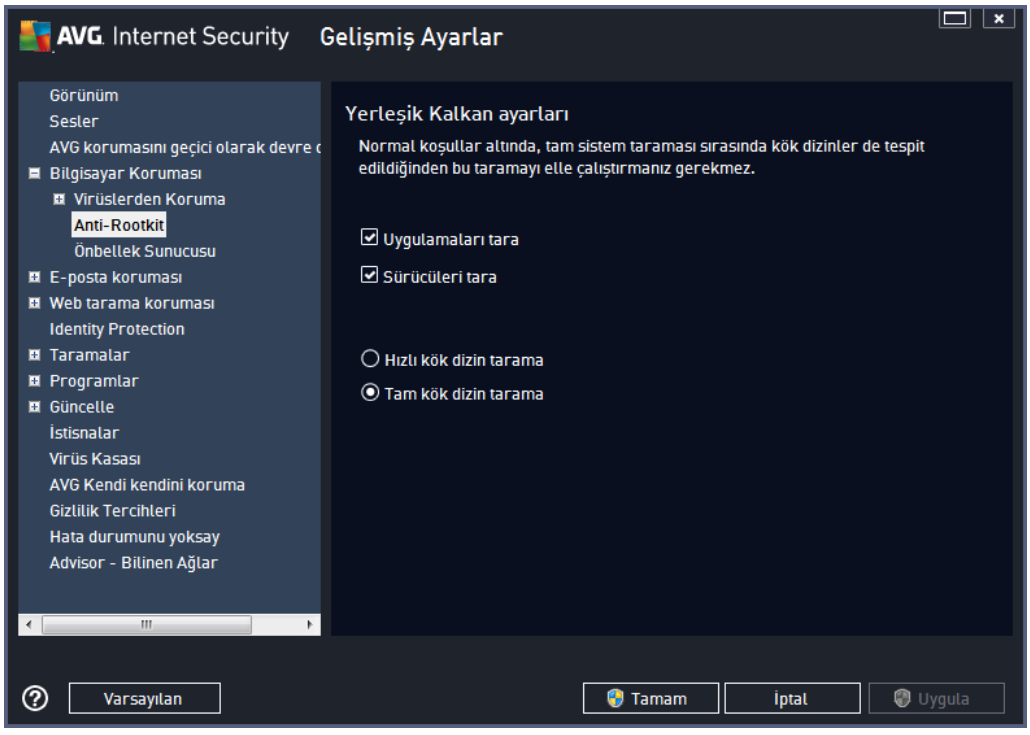
Tarama baslatma

Bilgisayarda rootkit'leri tara islemi Tarama seçenekleri iletisim kutusunda ***Bilgisayarda rootkit'leri tara*** dügmesine basilarak dogrudan baslatilabilir. ***Anti-rootkit taramasi devam ediyor*** adli yeni bir iletisim kutusu açilarak baslatilan taramanin ilerlemesini gösterir:



Tarama yapilandirmasi düzenleme

Anti-Rootkit tarama yapilandirmasini ***Anti-Rootkit Ayarlari*** iletisim kutusunda düzenleyebilirsiniz *(iletisim kutusuna Tarama seçenekleri iletisim kutusundaki Bilgisayari rootkit'lere karsi tara isleminin Ayarlar baglantisindan erisilebilir).* ***Degistirmek için geçerli bir nedeniniz olmadigi müddetçe varsayilan ayarlari korumaniz önerilir!***



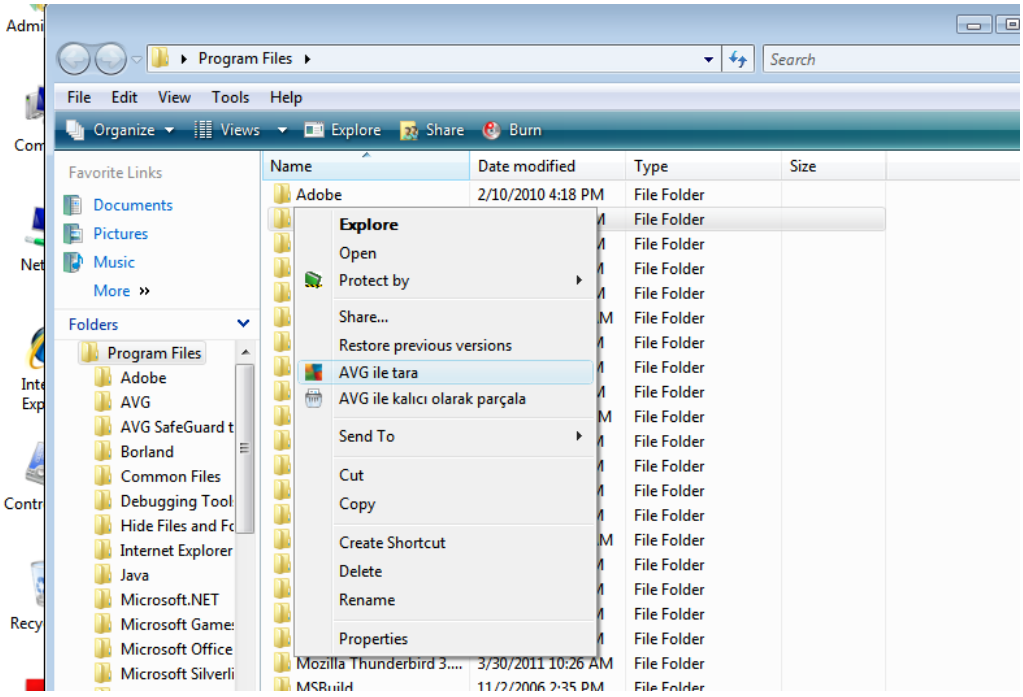
Tarama uygulamalari ve ***Tarama sürücüleri*** anti-rootkit taramasina nelerin dahil edilecegini ayrintili

sekilde belirlemenize olanak tanir. Bu ayarlar gelismis kullanicilara yöneliktir; tüm seçenekleri açik konumda muhafaza etmenizi öneririz. Rootkit tarama modunu da seçebilirsiniz:

- ***Hizli kök dizin tarama*** - çalisan tüm islemleri, yüklü sürücüleri ve sistem klasörlerini (*genellikle c:\Windows*) tarar
- ***Tam kök dizin tarama*** - çalisan tüm islemleri, yüklü sürücüleri, sistem klasörünü (*genellikle c:\Windows*), ayrica tüm yerel diskleri (*flash disk dahil, ancak disket/CD sürücüleri hariç*) tarar

11.2. Windows Gezgini'nde Tarama

Bilgisayarin tümünde ya da seçilen bölümlerinde gerçeklestirilen öntanimli taramalarin yani sira **AVG Internet Security 2014**, dogrudan Windows Gezgini ortaminda bulunan belirli nesnelerin hizli bir sekilde taranmasini da saglamaktadir. Bilinmeyen bir dosyayi açmak istiyor fakat içeriginden emin olamiyorsaniz istege bagli olarak tarayabilirsiniz. Bu adimlari takip edin:



- Windows Gezgini'nde taramak istediginiz dosyayi *(ya da klasörü)* seçin
- Baglam menüsünü açmak için nesneye farenizle sag tiklatin
- ***AVG ile Tara*** seçenegini seçerek dosyanin AVG tarafindan taranmasini saglayin **AVG Internet Security 2014**

11.3. Komut Satırı Tarama

AVG Internet Security 2014 içinde, taramayi komut satirindan çalistirma seçenegi vardir. Bu seçenegi, sunucularda ya da bilgisayar yeniden baslatildiktan sonra otomatik olarak çalistirilacak komut metinlerinin olusturulmasi sirasinda kullanabilirsiniz. Komut satirinda AVG'nin grafik kullanici arayüzünde sunulan parametrelerden daha fazlasini kullanarak tarama islemini gerçeklestirebilirsiniz.

AVG taramasini komut satirindan çalistirmak için AVG'nin yüklendigi klasörde asagidaki komutu çalistirin:

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

Komut sözdizimi

Komut söz dizimi asagidaki gibidir:

- ***Tam bilgisayar taramasi yapilirken avgscanx /parametre*** ... Örn. ***avgscanx /comp***
- ***avgscanx /parameter /parameter*** .. Birden fazla parametre kullanildigi zaman bunlar bir sira halinde dizilmeli ve bir boslugun yani sira bir de tire isareti ile ayrilmalidir
- Parametrelerden biri için belirli bir deger verilmesi gerekiyorsa (örnegin ***/scan*** parametresi taranmak üzere bilgisayarinizin seçilen alanlari hakkinda bilgi talep eder ve sizin de seçilen bölüme iliskin veri yolunu tam olarak saglamaniz gerekir). Degerler noktali virgül ile birbirinden ayrilir. Örn: ***avgscanx /scan=C:\;D:***

Tarama parametreleri

Mevcut parametrelerin tam görünümümü görüntülemek için, /? parametresi ile birlikte ilgili komutu yazin. ya da /HELP (örn. ***avgscanx /?***). Zorunlu olan tek parametre, bilgisayarin hangi alanlarinin taranmasi gerektigini belirlemek için kullanilan /SCAN parametresidir. Seçenekler hakkinda daha ayrintili açiklama almak için komut satiri parametrelerine genel bakis bölümüne bakin.

Tarama islemini baslatmak için ***Enter*** tusuna basin. Tarama sirasinda islemi ***Ctrl+C*** veya ***Ctrl+Pause*** tuslarini kullanarak durdurabilirsiniz.

Grafik arayüzünden baslatilan CMD taramasi

Bilgisayarinizi Windows Güvenli Modda çalistirdiginiz zaman komut satiri taramasini grafik kullanici arayüzünden baslatma seçeneginiz de bulunmaktadir. Taramanin kendisi komut satirindan baslatilacaktir, ***Komut Satiri Olusturucu*** iletisim kutusu, en yaygin tarama parametrelerini konforlu grafik arayüzünde görüntüler.

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

11.3.1. CMD Tarama Parametreleri

Komut satiri taramada kullanilabilecek parametrelerin listesi:

- /SCAN Belirli dosya ya da klasörleri tara /SCAN=yol;yol *(örn. /SCAN=C:\;D:\)*
- /COMP Tüm bilgisayari tara

- /HEUR Bulussal analiz kullan
- /EXCLUDE Tarama isleminden dizin yolu veya dosyalari hariç tut
- /@ Komut dosyasi /dosya adi/
- /EXT Bu uzantilari tara / örnegin EXT=EXE,DLL/
- /NOEXT Bu uzantilari tarama / örnegin NOEXT=JPG/
- /ARC Arsivleri tara
- /CLEAN Otomatik olarak temizle
- /TRASH Bulasan dosyalari Virüs Kasasi
- /QT Hizli test
- /LOG Bir tarama sonucu dosyasi olustur
- /MACROW Makrolari rapor et
- /PWDW Parola ile korunan dosyalari rapor et
- /ARCBOMBSW Arsiv bombalarini rapor et*(tekrar tekrar sikistirilan arsivler)*
- /IGNLOCKED Kilitli dosyalari yoksay
- /REPORT Dosyaya /dosya adina/ rapor et
- /REPAPPEND Rapor dosyasina ekle
- /REPOK Bulasmamis dosyalari Tamam olarak rapor et
- /NOBREAK CTRL-BREAK ile islemin kesilmesine izin verme
- /BOOT MBR/BOOT kontrolünü etkinlestir
- /PROC Aktif islemleri tara
- /PUP Potansiyel olarak istenmeyen programlari rapor et
- /PUPEXT Potansiyel olarak istenmeyen programlar grubunu rapor et
- /REG Kayit defterini tara
- /COO Çerezleri tara
- /? Bu konuyla ilgili yardimi görüntüle
- /HELP Bu konuyla ilgili yardimi görüntüle
- /PRIORITY Tarama önceligini belirle /Düsük, Oto, Yüksek/ *(bkz. Gelismis ayarlar /*

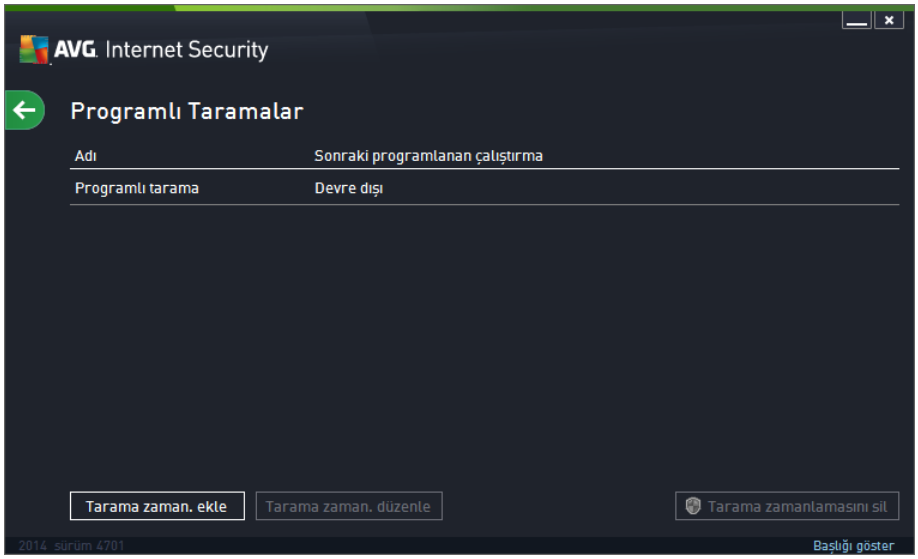
Taramalar)

- /SHUTDOWN Tarama tamamlandiktan sonra bilgisayari kapat
- /FORCESHUTDOWN Tarama tamamlandiktan sonra bilgisayari kapatmayi zorla
- /ADS Alternatif Veri Akislarini Tara *(yalnizca NTFS)*
- /HIDDEN Gizli uzantili dosyalari rapor et
- /INFECTABLEONLY Yalnizca bulasabilir uzantiya sahip dosyalari tara
- /THOROUGHSCAN Kapsamli taramayi etkinlestir
- /CLOUDCHECK Hatali tespitler açisindan denetle
- /ARCBOMBSW Yeniden sikistirilmis arsiv dosyalarini rapor et

11.4. Tarama Programlama

AVG Internet Security 2014 ile isteginiz dogrultusunda tarama yapmanin *(örnegin bilgisayariniza virüs bulastigindan süphelenirseniz)* yani sira zamanlanan bir plan dogrultusunda da tarama yapabilirsiniz. Taramalarin bir program dogrultusunda yapilmasi önerilmektedir: bu sekilde, bilgisayarinizin virüs bulasmasi ihtimaline karsi korundugundan emin olursunuz ve ne zaman tarama yapmaniz gerektigi konusunda endiselenmenize gerek kalmaz. Tüm bilgisayar taramasi islemini en az haftada bir kez düzenli olarak baslatmaniz gerekir. Diger yandan, yapabiliyorsaniz programli taramanin varsayilan yapilandirmasinda ayarlandigi gibi tüm bilgisayar taramasini günlük olarak yapin. Bilgisayariniz "daima açik" ise taramalari çalisma saatlerinden sonra gerçeklestirilecek sekilde programlayabilirsiniz. Bilgisayarinizi arada sirada kapatiyorsaniz taramayi, taramalari görev yerine getirilemediginde bilgisayarin baslamasi ile baslat seklinde programlayin.

Tarama zamanlamasi Tarama seçenekleri iletisim kutusundaki ***Zamanlanmis taramayi yönet*** dügmesiyle erisilebilen ***Zamanlanmis taramalar*** iletisim kutusunda olusturulabilir / düzenlenebilir. Yeni ***Zamanlanmis Tarama*** iletisim kutusunda geçerli olarak zamanlanmis olan tüm taramalarin genel görünümünü görebilirsiniz:



Iletisim kutusunda kendi taramalarinizi belirleyebilirsiniz. Kendi istediginiz yeni bir tarama zamanlamasi olusturmak için ***Tarama zamanlamasi ekle*** dügmesini tiklatin. Planlanan tarama parametreleri üç sekmeden düzenlenebilir (*ya da yeni bir zamanlama ayarlanabilir*):

- Zamanla
- Ayarlar
- Konum

Her sekmede "trafik isigi" dügmesini kullanarak  zamanlamasi belirlenen testi geçici olarak devre disi birakabilir ve gerek duydugunuzda tekrar açabilirsiniz.

11.4.1. Zamanla

Zamanla sekmesinin üst bölümünde geçerli olarak tanimlanmis tarama zamanlamasi için ad belirleyebileceginiz metin alanini bulabilirsiniz. Programladiginiz taramalari digerlerinden kolaylikla ayirabilmek için her zaman taramalariniza kisa, açiklayici adlar vermeye çalisin. Örnegin, Taramayi "Yeni Tarama" veya "Taramam" adiyla adlandirmaniz uygun degildir çünkü bu adlar, taramanin fiilen neyi kontrol ettigini açiklamaz. Diger bir yandan "Sistem alani taramasi" vb. oldukça açiklayici bir isim olacaktir.

Bu iletisim kutusunda taramanin asagidaki parametrelerini de tanimlayabilirsiniz:

- ***Çalismayi programla*** - Burada, yeni programlanan tarama baslatmasi için zaman araliklari belirtebilirsiniz. Zamanlama belirli bir sürenin ardindan tekrarlanan tarama baslatmasi ile *(Her ...'de bir)* ya da kesin bir tarih ve saat tanimlayarak *(Belirli bir zaman araliginda çalistir ...)*, veya tarama baslangiciyla ilgili bir olay tanimlanarak *(Bilgisayarin baslatilmasinda çalistir)* tanimlanabilir.

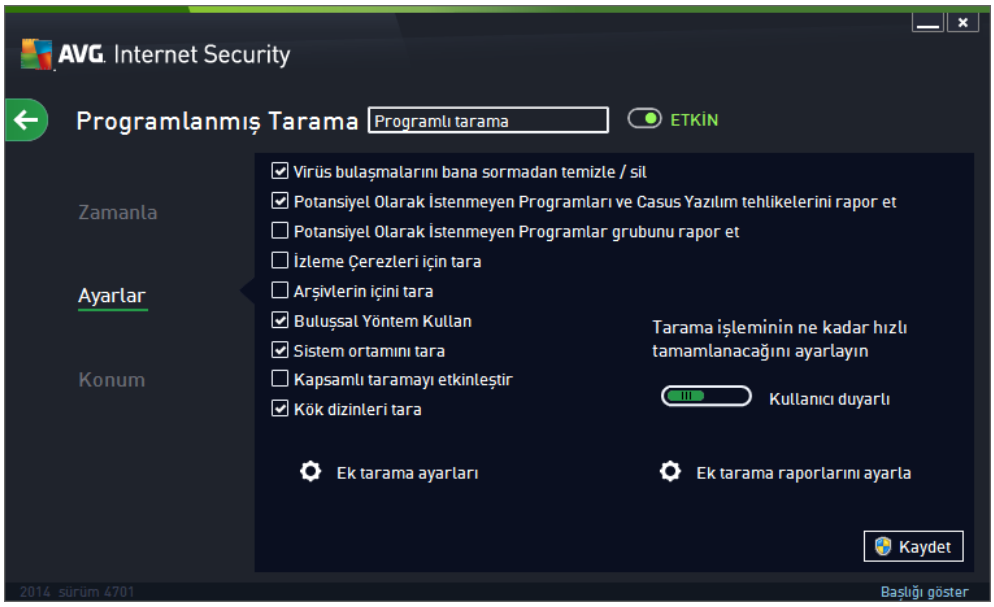
- ***Gelismis planlama seçenekleri*** - Bu bölümde, bilgisayar düsük güç modundaysa veya tamamen kapatilmissa hangi kosullar altinda taramanin baslatilmasi/baslatilmamasi gerektigini belirleyebilirsiniz. Programlanan tarama belirttiginiz saatte baslatildiginda, AVG sistem tepsisi simgesi üzerinde bir açilir pencere ile bu konuda bilgilendirileceksiniz. Bunun ardindan yeni bir AVG sistem tepsisi simgesi görüntülenir (üzerinde beyaz bir ok bulunur ve tamamen renklidir) ve programlanan taramanin basladigini bildirir. Çalisan taramayi duraklatmaya hatta durdurmaya karar verebileceginiz ve o anda çalismakta olan taramanin önceligini degistirebileceginiz baglam menüsü açmak için, çalisan taramayi sag tiklatin.

Iletisim kutusundaki kontroller

- ***Kaydet*** - Bu sekmede veya bu iletisim kutusunun baska herhangi bir sekmesinde gerçeklestirdiginiz tüm degisiklikleri kaydeder ve Zamanlanmis taramalar genel görünümüne geri döner. Bu nedenle tüm sekmelerdeki test parametrelerini yapilandirmak istiyorsaniz gereksinimlerinizin tamamini belirledikten sonra bunlari kaydetmek için dügmeye basin.

-  - Zamanlanmis taramalar genel görünümüne dönmek için sol üst kisimdaki yesil oku kullanin.

11.4.2. Ayarlar



Ayarlar sekmesinin üst bölümünde geçerli olarak tanimlanmis tarama zamanlamasi için ad belirleyebileceginiz metin alanini bulabilirsiniz. Programladiginiz taramalari digerlerinden kolaylikla ayirabilmek için her zaman taramalariniza kisa, açiklayici adlar vermeye çalisin. Örnegin, Taramayi "Yeni Tarama" veya "Taramam" adiyla adlandirmaniz uygun degildir çünkü bu adlar, taramanin fiilen neyi kontrol ettigini açiklamaz. Diger bir yandan "Sistem alani taramasi" vb. oldukça açiklayici bir isim olacaktir.

Ayarlar sekmesinde, istege bagli olarak açilip/kapatilabilen tarama parametrelerine iliskin bir liste bulabilirsiniz. ***Söz konusu ayarlari degistirmek açisindan geçerli bir nedeniniz yoksa öntanimli yapilandirmayi oldugu gibi muhafaza etmeniz önerilir***:

- ***Bulasmayi bana sormadan temizle / kaldir*** *(varsayilan olarak açik):* Tarama sirasinda virüs tanimlanirsa, bir giderme yazilimi mevcutsa otomatik olarak temizlenir. Bulasmis dosya otomatik olarak temizlenemezse, bulasmis nesne Virüs Kasasi'na tasinir.

- ***Potansiyel olarak istenmeyen programlari ve casus yazilim tehlikelerini rapor et*** *(varsayilan olarak açik):* Virüslerin yani sira casus yazilimlari da taramak için isaretleyin. Casus yazilim, süpheli kötü amaçli yazilim kategorisini ifade eder: genellikle bir güvenlik riskini olusturmasina ragmen bu programlardan bazilari bilerek yüklenebilir. Bilgisayarinizin güvenligini artirdigindan, bu özelligi etkin durumda tutmanizi öneririz.

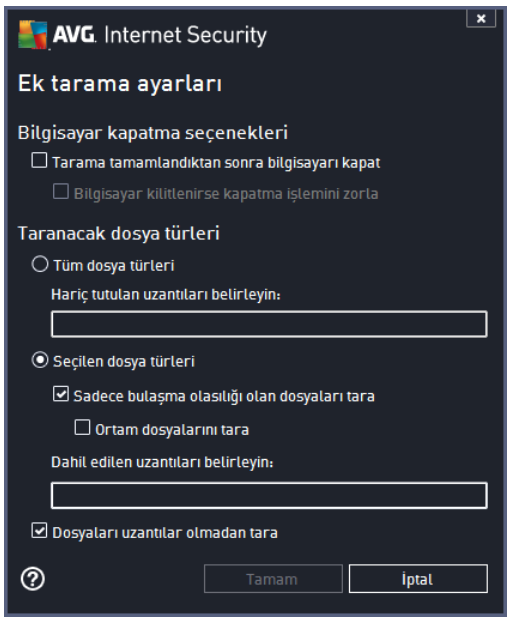
- ***Potansiyel olarak istenmeyen programlar gelismis grubunu rapor et*** (*varsayilan olarak kapali*): Casus yazilimlarin, yani dogrudan üreticiden alindiginda tamamen zararsiz olan, ancak daha sonra kötüye kullanilabilecek programlarin genisletilmis paketinin tespit edilmesi için isaretleyin. Bu, bilgisayar güvenliginizi daha da artiran ek bir önlemdir, ancak yasal programlari da engelleyebilir ve bu yüzden varsayilan olarak kapalidir.

- ***Izleme çerezleri için tara*** (*varsayilan olarak kapali*): Bu parametre tarama sirasinda çerezlerin tespit edilmesi gerektigini belirtir (*HTTP çerezleri kimlik dogrulamasi, izleme ve kullanicilar hakkindaki site tercihleri veya elektronik alisveris sepetlerinin içerigi gibi belirli bilgilerin korunmasi için kullanilir*).

- ***Arsivleri tara*** (*varsayilan olarak kapali*): Bu parametre, tarama isleminde ZIP, RAR vb. bir arsiv ile saklanmis olsa bile tüm dosyalarin taranmasi gerektigini belirtir.
- ***Bulussal yöntem kullan*** (*varsayilan olarak açik*): Bulussal analiz (*taranan nesnenin yönergelerinin sanal bir bilgisayar ortaminda dinamik olarak canlandirilmasi*) tarama sirasinda kullanilacak virüs tespit yöntemlerinden biridir.
- ***Sistem ortamini tara*** (*varsayilan olarak açik*): Tarama islemi, bilgisayarinizin sistem alanlarini da kontrol edecektir.
- ***Kapsamli taramayi etkinlestir*** (*varsayilan olarak kapali*) belirli durumlarda (*bilgisayariniza bulasma olmasindan süpheleniliyorsa*) yalnizca emin olmak üzere bilgisayarinizin bulasma olmasi çok zor olan alanlarini bile tarayan en kapsamli tarama algoritmalarini etkinlestirmek için bu seçenegi isaretleyebilirsiniz. Ancak, bu yöntemin çok fazla zaman aldigini unutmayin.
- ***Kök dizinleri tara*** *(varsayilan olarak açik):* Anti-Rootkit taramasi bilgisayarinizi olasi rootkitlere, örnegin bilgisayarinizda kötü amaçli etkinlik içerebilecek programlar ve teknolojilere karsi tarar. Bir kök dizin algilanirsa, bu, bilgisayarinizda mutlaka virüs oldugu anlamina gelmez. Bazi durumlarda, belirli sürücüler veya normal uygulamalarin bölümleri kök dizin olarak yanlis algilanabilir.

Ek tarama ayarlari

Baglanti, su parametreleri belirtebileceginiz yeni bir ***Ek Tarama Ayarlari*** iletisim kutusu açar:



- ***Bilgisayar kapatma seçenekleri*** - Çalisan tarama islemi bittiginde bilgisayarin otomatik olarak kapatilmasi gerekip gerekmedigine karar verir. Bu seçenegi onaylarsaniz (*Tarama bittikten sonra bilgisayari kapat*) bilgisayar mevcut durumda kilitli olsa bile bilgisayarin kapatilmasini saglayan bir seçenegin bulundugu bir pencere açilacaktir (*Bilgisayar kilitliyse bilgisayari kapanmaya zorla*).

- ***Taranacak dosya türleri*** - taranacak dosya türleriyle ilgili asagidaki tercihlerden birini yapmaniz gerekir:

    - o ***Tüm dosya türleri*** taranmamasi gereken virgülle ayrilmis dosya uzantilarinin listesini saglayarak taramada istisnalari tanimlama seçenegiyle.

    - o ***Seçili dosya türleri*** - yalnizca virüs bulasabilme olasiligi olan dosyalari taramayi istediginizi belirtebilirsiniz (*virüs bulasamayan dosyalar taranmayacaktir, örnegin, bazi düz metin dosyalari veya bazi diger çalistirilamayan dosyalar*); ortam dosyalari (*video, ses dosyalari - bu onay kutusunun isaretini kaldirirsaniz, bu dosyalar genellikle çok büyük oldugundan ve virüs bulasma olasiliklari çok az oldugundan tarama süresini daha da azaltir)*. Tekrar, her zaman taranmasi gereken dosyalari uzantilarina göre belirtebilirsiniz.

    - o Istege bagli olarak, ***Uzantilari olmayan dosyalari taramaya*** da karar verebilirsiniz ve bu seçenek varsayilan olarak açiktir ve gerçekten bir nedeniniz yoksa degistirmemeniz önerilir. Uzantisi olmayan dosyalar süpheli olabilir ve her zaman taranmalidir.

Taramanin ne kadar hizli tamamlanacagini ayarla

Bu bölümde ayrica istenen tarama hizini, sistemin kaynak kullanimina bagli olarak belirleyebilirsiniz. Varsayilan olarak, bu seçenek otomatik kaynak kullaniminin *kullaniciya duyarli* seviyesine ayarlidir. Tarama isleminin daha hizli ilerlemesini istiyorsaniz tarama islemi daha kisa sürecektir fakat tarama islemi sirasinda sistem kaynaklari oldukça yüklü bir sekilde kullanilacak ve bilgisayar üzerindeki diger islemleri yavaslatacaktir (*bu seçenek bilgisayariniz açikken kullanilmadigi sirada seçilebilir*). Öte yandan, tarama süresini uzatarak sistem kaynaklarinin kullanimini azaltabilirsiniz.

Ek tarama raporlarini ayarla

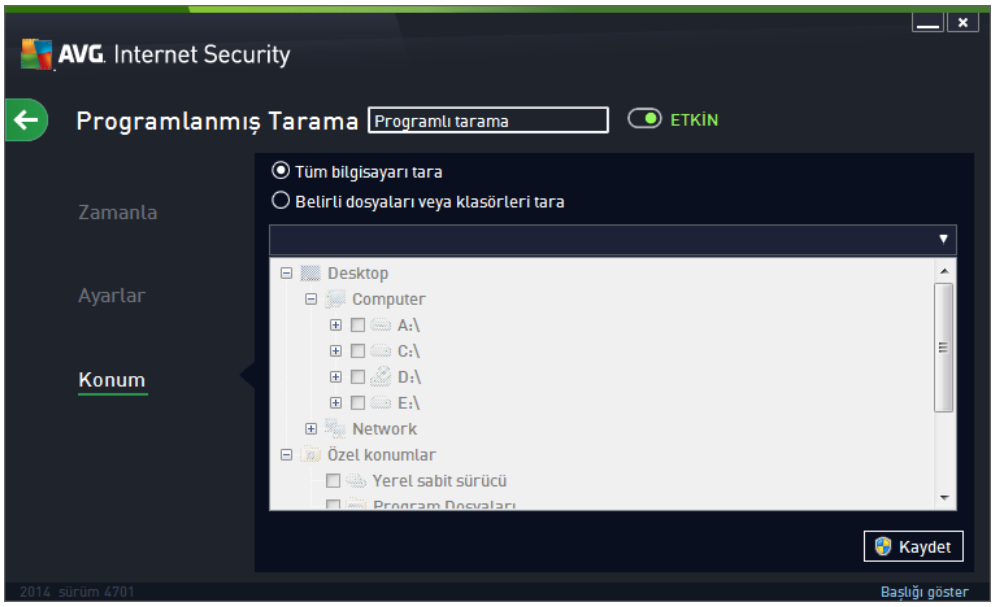
Tarama bulgularinin rapor edilmesi gerekip gerekmedigini tanimlamak üzere birden fazla ögeyi ayarlayabileceginiz ***Tarama raporlari*** olarak adlandirilan bagimsiz bir iletisim penceresi açmak için ***Ek tarama raporlarini ayarla...*** baglantisini tiklatin:

Iletisim kutusundaki kontroller

- ***Kaydet*** - Bu sekmede veya bu iletisim kutusunun baska herhangi bir sekmesinde gerçeklestirdiginiz tüm degisiklikleri kaydeder ve Zamanlanmis taramalar genel görünümüne geri döner. Bu nedenle tüm sekmelerdeki test parametrelerini yapilandirmak istiyorsaniz gereksinimlerinizin tamamini belirledikten sonra bunlari kaydetmek için dügmeye basin.

-  - Zamanlanmis taramalar genel görünümüne dönmek için sol üst kisimdaki yesil oku kullanin.

11.4.3. Konum



Konum sekmesinde, tüm bilgisayari tarama veya belirli dosya veya klasörleri taramayi programlamak isteyip istemediginizi tanimlayabilirsiniz. Belirli dosya ve klasörlerin taranmasini seçmeniz durumunda, bu iletisim kutusunun alt tarafinda görüntülenen agaç yapisi etkinlesir ve taranacak klasörleri belirleyebilirsiniz (*taramak istediginiz klasörü buluncaya kadar arti isaretini tiklatarak ögeleri genisletin*). Ilgili kutulari isaretleyerek birden fazla klasör seçebilirsiniz. Seçilen klasörler, iletisim kutusunun üstünde bulunan metin alaninda görüntülenir. Açilir menü seçilen tarama geçmisini daha sonra kullanilmak üzere saklar. Alternatif olarak, istediginiz klasörün tam yolunu elle girebilirsiniz (*birden fazla yol girerseniz, bunlari ekstra bosluk birakmadan noktali virgülle ayirmaniz gerekir*).

Agaç yapisi içinde ***Özel konumlar*** adinda bir dal da görürsünüz. Asagida, ilgili onay kutusu isaretlendiginde taranacak konumlarin listesi bulunmaktadir:

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

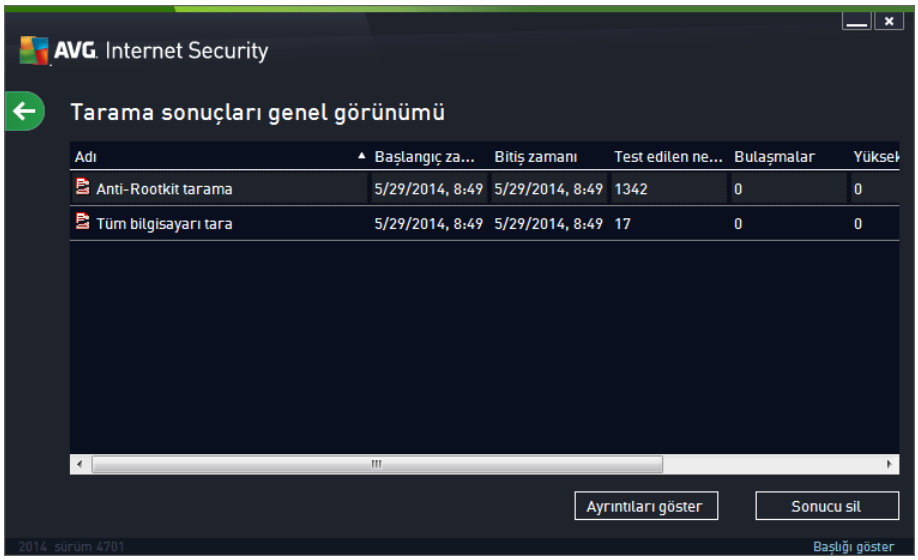
- *Win XP için:* C:\Documents and Settings\Default User\Belgelerim\
- *Windows Vista/7 için*: C:\Users\user\Documents\

- ***Paylasilan Belgeler***
  - *Win XP için*: C:\Documents and Settings\All Users\Documents\
  - *Windows Vista/7 için*: C:\Users\Public\Documents\
- ***Windows klasörü*** - C:\Windows\
- ***Diger***
  - *Sistem sürücüsü* - isletim sisteminin yüklü oldugu 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 Internet Dosyalari* - C:\Documents and Settings\User\Local Settings\Geçici Internet Dosyalari\ (*Windows XP*) veya C:\Users\user\AppData\Local\Microsoft\Windows\Geçici Internet Dosyalari (*Windows Vista/7*)

Iletisim kutusundaki kontroller

- ***Kaydet*** - Bu sekmede veya bu iletisim kutusunun baska herhangi bir sekmesinde gerçeklestirdiginiz tüm degisiklikleri kaydeder ve Zamanlanmis taramalar genel görünümüne geri döner. Bu nedenle tüm sekmelerdeki test parametrelerini yapilandirmak istiyorsaniz gereksinimlerinizin tamamini belirledikten sonra bunlari kaydetmek için dügmeye basin.
-  - Zamanlanmis taramalar genel görünümüne dönmek için sol üst kisimdaki yesil oku kullanin.

11.5. Tarama Sonuçları



Tarama sonuçlari genel görünümü iletisim kutusu o ana kadar gerçeklestirilmis tüm taramalarin sonuçlarini listeler. Tabloda her tarama sonucuna iliskin olarak su bilgiler bulunur:

- ***Simge*** - Ilk sütunda taramanin durumunu açiklayan bir bilgi simgesi gösterilir:
  - Bulasma bulunmadi, tarama tamamlandi
  - Bulasma bulunmadi, tarama tamamlanmadan yarida kesildi
  - Bulasma bulundu ve iyilestirilmedi, tarama tamamlandi
  - Bulasma bulundu ve temizlenmedi, tarama tamamlanmadan yarida kesildi
  - Bulasmalar bulundu ve tümü iyilestirildi veya kaldirildi, tarama tamamlandi
  - Bulasmalar bulundu ve tümü temizlendi veya kaldirildi, tarama tamamlanmadan yarida kesildi
- ***Ad*** - Bu sütun ilgili taramanin adini gösterir. Bu ya iki öntanimli taramadan biridir ya da sizin kendi zamanlanmis taramanizdir.
- ***Baslangiç zamani*** - Taramanin baslatildigi tarih ve saati verir.
- ***Bitis zamani*** - Taramanin tamamlandigi, duraklatildigi veya kesildigi tarih ve saati verir.
- ***Test edilen nesneler*** - Taranan toplam nesne sayisini gösterir.
- ***Bulasmalar*** - Kaldirilan/bulunan toplam bulasma sayisini verir.
- ***Yüksek / Orta / Düsük*** - Sonraki üç sütun sirasiyla bulunan yüksek, orta ve düsük öncelikli bulasma sayisini verir.

- ***Rootkitler*** - Tarama sirasinda bulunan toplam rootkit sayisini gösterir.

Iletisim kutusu kontrolleri

Ayrintilari göster - Seçilen bir tarama hakkindaki ayrintili bilgileri görmek için bu dügmeyi tiklatin *(yukaridaki tabloda vurgulanir)*.

Sonuçlari sil - Seçilen bir tarama sonucunu tablodan kaldirmak için bu dügmeyi tiklatin.

 - Bilesen genel bilgilerinin bulundugu ana kullanici arayüzüne dönmek için iletisim kutusunun sol üst kisminda bulunan yesil oku kullanin.

11.6. Tarama sonuçlari ayrintilari

Seçilen bir tarama sonucunun ayrintili bilgilerini açmak için Tarama sonuçlari genel görünümü iletisim kutusundan erisilebilen ***Ayrintilari göster*** dügmesini tiklatin. Ayni iletisim kutusu arayüzünde ilgili tarama sonucu hakkinda ayrintili bilgilerin açiklandigi bölüme yönlendirilirsiniz. Bilgiler üç sekmede gösterilir:

- ***Özet*** - Bu sekme tarama hakkindaki temel bilgileri sunar: Taramanin basariyla tamamlanip tamamlanmadigi, tehdit tespit edilip edilmedigi ve tespit edilenlere ne oldugu.
- ***Ayrintilar*** - Bu sekme tespit edilen tüm tespitlerin ayrintilari da dahil olmak üzere tarama hakkindaki tüm bilgileri gösterir. Genel görünümü dosyaya aktar ayrintilari .csv dosyasi olarak kaydetmenize olanak tanir.
- ***Tespitler*** - Bu sekme ancak tarama sirasinda tehdit tespit edilmisse görüntülenir ve tehditler hakkinda ayrintili bilgiler sunar:

   ***Bilgi önem derecesi***: bilgiler veya uyarilar, gerçek tehditler degildir. Genellikle makro içeren belgeler, parola ile korunan belgeler veya arsivler , kilitli dosyalar vb.

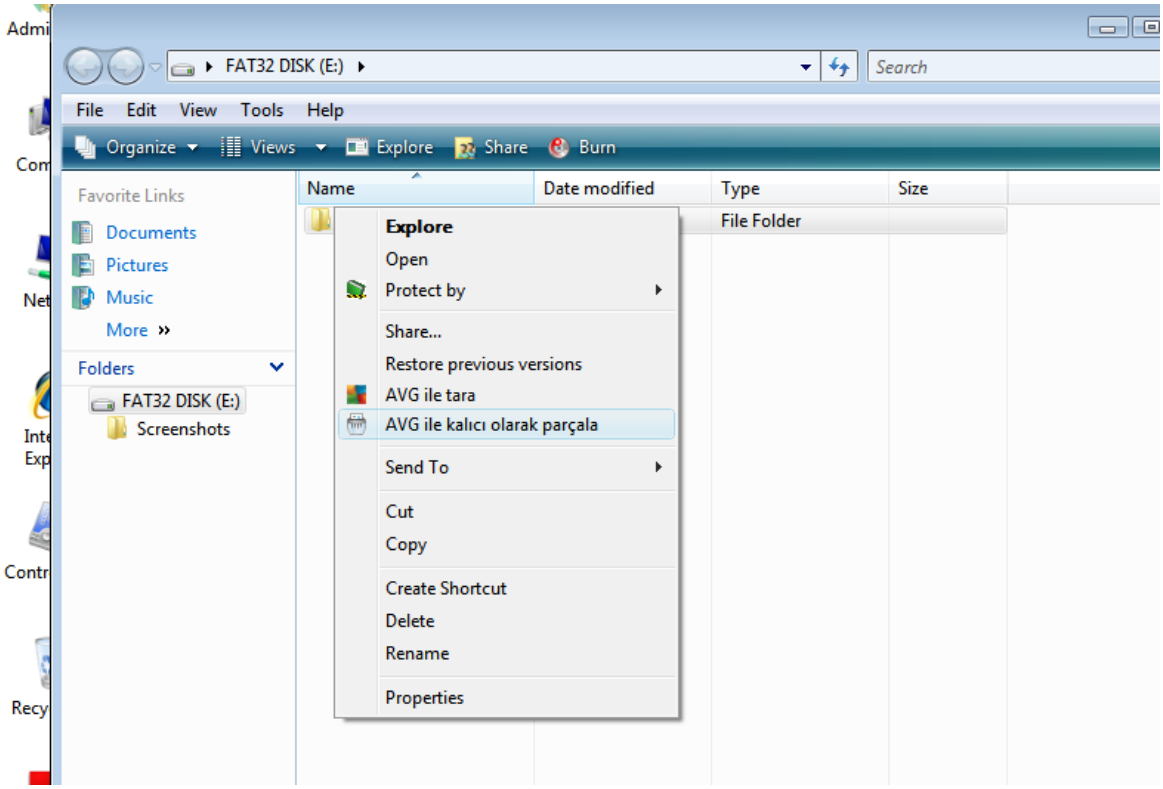
   ***Orta önem derecesi***: genellikle PUP *(potansiyel olarak istenmeyen programlar, reklam yazilimi gibi)* veya izleme çerezleri

   ***Yüksek önem derecesi***: virüsler, Truva atlari, açiktan yararlanma girisimleri vb. ciddi tehditler. Ayrica Bulussal Yöntem tespit yöntemi tarafindan tespit edilen nesneler, virüs veritabaninda henüz tanimlanmamis tehditler gibi.

12. AVG File Shredder

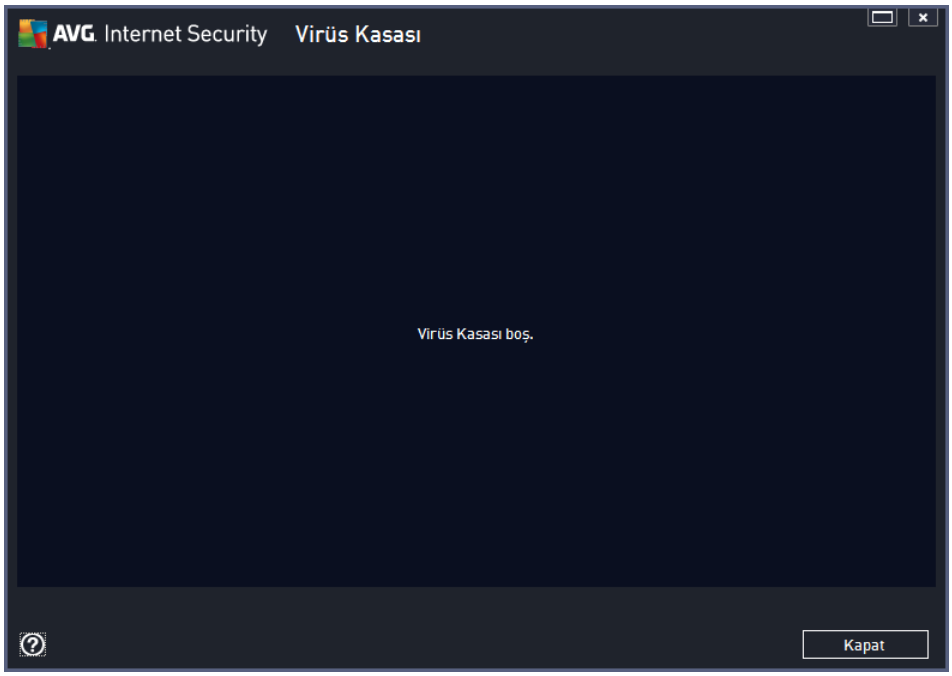
AVG File Shredder dosyalari tamamen güvenli biçimde silmek (yani kurtarma amaçli tasarlanmis gelismis yazilim araçlariyla bile kurtarma ihtimali olmayacak biçimde silmek) üzere tasarlanmistir.

Bir dosya veya klasörü parçalamak için dosyayi/klasörü bir dosya yöneticisinde *(Windows Explorer, Total Commander, ...)* sag tiklatin ve baglam menüsünden ***AVG ile kalici olarak parçala***'yi seçin. Geri Dönüsüm Kutusu içindeki dosyalar da parçalanabilir. Belirli bir konumdaki *(örnegin CD-ROM)* belirli bir dosya güvenilir biçimde parçalanamiyorsa bu konuda bilgilendirilirsiniz veya baglam menüsündeki seçenek tamamen kullanilmaz olur.



Lütfen her zaman aklinizda tutun: Parçaladiginiz bir dosya artik sonsuza dek yok olur.

13. Virüs Kasası



Virüs Kasasi AVG taramalari sirasinda tespit edilen süpheli/bulasmis nesnelerin yönetilmesi için güvenli bir ortamdir. Tarama sirasinda bulasmis bir nesne tespit edildikten sonra AVG, söz konusu bulasmayi otomatik olarak temizleyemiyorsa süpheli nesne hakkinda ne yapmak istediginiz sorulur. Önerilen çözüm, nesneyi daha sonra ilgilenmek üzere ***Virüs Kasasina*** tasimaktir. ***Virüs Kasasi***'ni satin almanin ana amaci silinen bir dosyayi belirli bir süre için saklamasidir, böylece dosyayi orijinal konumunda artik istemediginizden emin olabilirsiniz. Dosyanin yoklugu sorun olusturuyorsa, bu dosyayi analize gönderebilir veya orijinal konumuna geri yükleyebilirsiniz.

Virüs Kasasi arayüzü, yeni bir pencerede açilir ve karantina altindaki bulasmis nesneler hakkinda genel bilgi içerir:

- ***Ekleme Tarihi*** - Süpheli dosyanin tespit edildigi ve Virüs Kasasi'na kaldirildigi tarih ve saati gösterir.
- ***Önem seviyesi*** - Kimlik bilesenini **AVG Internet Security 2014** yaziliminiza yüklemeye karar verdiginizde, ilgili bulgunun önem seviyesi, sakincasiz *(üç yesil nokta)* ile çok tehlikeli *(üç kirmizi nokta)* arasinda degisen dört seviyeli bir ölçekte grafik olarak bu bölümde gösterilir; bulasma türü hakkindaki bilgiler (*bulasma seviyesine bagli olarak - listelenen tüm nesnelere virüs bulasmistir veya bulasma olasiligi vardir*) de gösterilir.
- ***Tehdit Adi*** - Tespit edilen bulasmanin adini çevrimiçi virüs ansiklopedisine göre belirtir.
- ***Kaynak*** - Ilgili tehdidi hangi **AVG Internet Security 2014** bileseninin tespit ettigini belirtir.
- ***Mesaj*** - Çok nadiren, bu sütunda ilgili tehdit hakkinda ayrintili açiklamalar sunan notlar gösterilebilir.

Kontrol dügmeleri

Virüs Kasasi arayüzünden ulasabileceginiz kontrol dügmeleri sunlardir:

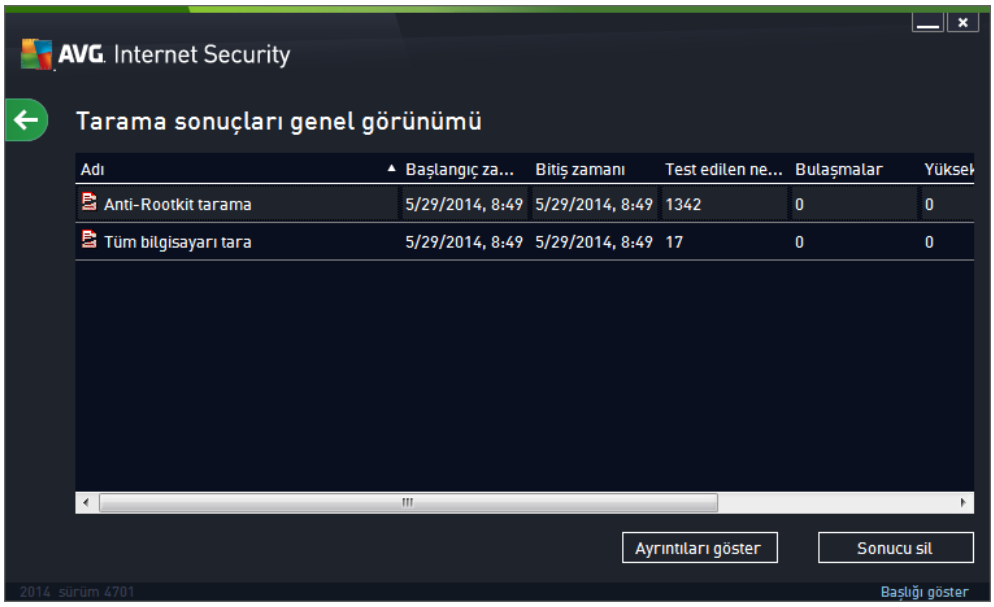
- ***Geri Yükle*** - bulasmis dosyayi sabit diskinizdeki orijinal konumuna geri yükler.
- ***Farkli Geri Yükle*** - bulasmis dosyayi seçili klasöre tasir.
- ***Ayrintilar*** - ***Virüs Kasasi***'nda karantinaya alinan tehdit hakkinda ayrintili bilgi için listede seçili ögeyi vurgulayin ve ***Ayrintilar*** dügmesini tiklatarak tespit edilen tehdidin açiklamasini içeren yeni bir iletisim kutusu açin.
- ***Sil*** - bulasmis dosyayi ***Virüs Kasasi***'ndan tamamen ve geri döndürülemeyecek sekilde siler.
- ***Kasayi Bosalt*** - ***Virüs Kasasi*** içerigini tamamen temizler. Dosyalari ***Virüs Kasasi***'ndan kaldirdiginizda, bu dosyalar diskten geri alinmayacak biçimde kaldirilir (*Geri Dönüsüm Kutusu'na tasinmaz*).

14. Geçmiş

Geçmis bölümü tüm geçmis olaylarla ilgili bilgileri içerir*(güncellemeler, taramalar, tespitler vb.)* ve bu olaylar hakkinda rapor verir. Bu bölüme ana kullanici arayüzündeki ***Seçenekler / Geçmis*** ögeleri yoluyla erisilebilir. Kaydedilen olaylarin tüm geçmisi su bölümlere ayrilmistir:

- Tarama sonuçlari
- Yerlesik Kalkan tespiti
- E-posta Korumasi tespiti
- Online Shield tespitleri
- Olay geçmisi günlügü
- Firewall günlügü

14.1. Tarama sonuçları



Tarama sonuçlari genel görünümü iletisim kutusuna **AVG Internet Security 2014** ana penceresinin üst satirindaki gezinme bölümünden ***Seçenekler / Geçmis / Tarama sonuçlari*** menü ögesi yoluyla erisilebilir. Iletisim kutusunda, daha önce baslatilan tüm taramalar ve sonuçlari hakkinda bilgi bulunmaktadir.

- ***Adi*** - taramanin amaci; öntanimli taramalardan birinin adi ya da programladiginiz taramaya verdiginiz adlardan biri olabilir. Her ismin yaninda tarama sonucunu belirten bir simge bulunmaktadir:

  - yesil simge tarama sirasinda herhangi bir bulasmanin tespit edilemedigini gösterir

- mavi simge tarama sirasinda bir bulasmanin tespit edildigini ancak bulasmis nesnenin otomatik olarak silindigini gösterir

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

Simgeler bütün halinde ya da yarisi kesilmis olabilir - bütün halindeki simge, tarama isleminin dogru sekilde tamamlandigini ve bitirildigini gösterirken yarisi kesilmis simge, taramanin iptal edildigini ya da kesildigini gösterir.

Not: *Taramalarin her biri hakkinda ayrintili bilgi almak için lütfen Ayrintilari göster dügmesine (bu pencerenin alt kismindadir) basarak ulasabileceginiz Tarama Sonuçlari penceresini inceleyin.*

- ***Baslangiç zamani*** - taramanin baslatildigi tarih ve saati gösterir.
- ***Bitis zamani*** - taramanin bittigi tarih ve saati gösterir.
- ***Taranan nesneler*** - tarama sirasinda kontrol edilen nesne sayisidir
- ***Bulasmalar*** - tespit edilen / silinenvirüs bulasmasi sayisi
- ***Yüksek / Orta*** - bu sütunlar kaldirilan/bulunan toplam bulasma sayisini sirasiyla yüksek ve orta önem seviyesine göre gösterir
- ***Bilgi*** - tarama islemine ve sonucuna iliskin bilgiler *(genellikle islemin tamamlanmasinin ya da kesilmesinin hemen ardindan görüntülenir)*
- ***Kök dizinler*** - algilanan kök dizinlerin

Kontrol dügmeleri

Tarama sonuçlarina genel bakis penceresindeki kontrol dügmeleri sunlardir:

- ***Ayrintilari göster*** - seçili taramada ayrintili verileri görüntülemek için Tarama sonuçlari iletisim kutusuna geçmek için basin
- ***Sonucu sil*** - seçili ögeyi tarama sonuçlarina genel bakistan silmek için basin
- - varsayilan AVG ana iletisim kutusuna *(bilesen genel görünümü) geri dönmek için* bu iletisim kutusunun sol üst kismindaki oku kullanin

14.2. Yerleşik Kalkan Sonuçları

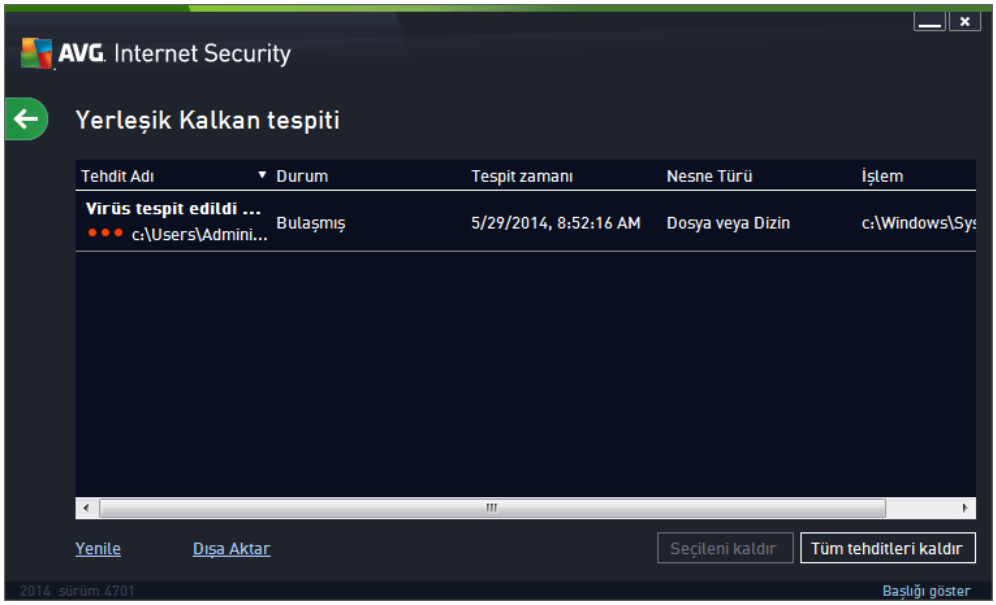
Yerlesik Kalkan hizmeti ***Bilgisayar*** bilesenin bir parçasidir ve kopyalanan, açilan veya kaydedilen dosyalari tarar. Herhangi bir virüs ya da bir tehlike tespit edildigi zaman asagidaki iletisim kutusu ile aninda uyarilirsiniz:

Bu uyari iletisim kutusunda tespit edilen ve virüs bulasmis olarak atanan nesne hakkinda daha fazla bilgi (*Tehdit*) ve ilgili bulasma hakkinda bazi açiklamalar (*Açiklama*) bulabilirsiniz. Ayrintilari göster baglantisi, sizi tespit edilen bulasma hakkinda ayrintili bilgi bulabileceginiz (biliniyorsa) çevrimiçi virüs ansiklopedisine yönlendirir. Iletisim kutusunda, tespit edilen tehdide yönelik olarak kullanabileceginiz çözümler hakkinda genel bilgiler de bulabilirsiniz. Alternatiflerden birin önerilen olarak etiketlenir: ***Beni Koru (önerilir). Yapabiliyorsaniz, her zaman bu seçenegi kullanin!***

Not: *Tespit edilen nesnenin büyüklügü, Virüs Kasasi'ndaki bos alan sinirini asabilir. Bu durumda, bulasmis nesneyi Virüs Kasasi'na tasimaya çalistiginizda size bu sorun hakkinda bilgi veren bir uyari iletisi görüntülenir. Ancak Virüs Kasasi boyutu degistirilebilir. Sabit diskinizin gerçek boyutunun uyarlanabilir yüzdesi olarak tanimlanir. Virüs Kasanizin boyutunu arttirmak için, 'Virüs Kasasi boyutunu sinirlandir' seçenegi araciligiyla AVG Gelismis Ayarlardaki Virüs Kasasi iletisim kutusuna gidin.*

Iletisim kutusunun alt kisminda ***Ayrintilari göster*** baglantisini bulabilirsiniz. Baglantiyi tiklatarak bulasma tespit edildiginde çalisan islem ve islemin tanimlanmasi hakkinda ayrintili bilgilerin bulundugu yeni bir pencere açabilirsiniz.

Yerlesik Kalkan tespitlerinin tamaminin listesine ***Yerlesik Kalkan tespiti*** iletisim kutusundan erisilebilir. Bu iletisim kutusuna **AVG Internet Security 2014** ana penceresinin üst bölümünde yer alan ***Seçenekler / Geçmis / Yerlesik Kalkan tespiti*** menü ögesi yoluyla erisilebilir. Iletisim kutusu yerlesik kalkan tarafindan tespit edilip tehlikeli oldugu görülen ve temizlenen ya da Virüs Kasasi'na tasinan nesneler hakkinda genel bilgi vermektedir.



Tespit edilen tüm nesneler için asagidaki bilgiler verilir:

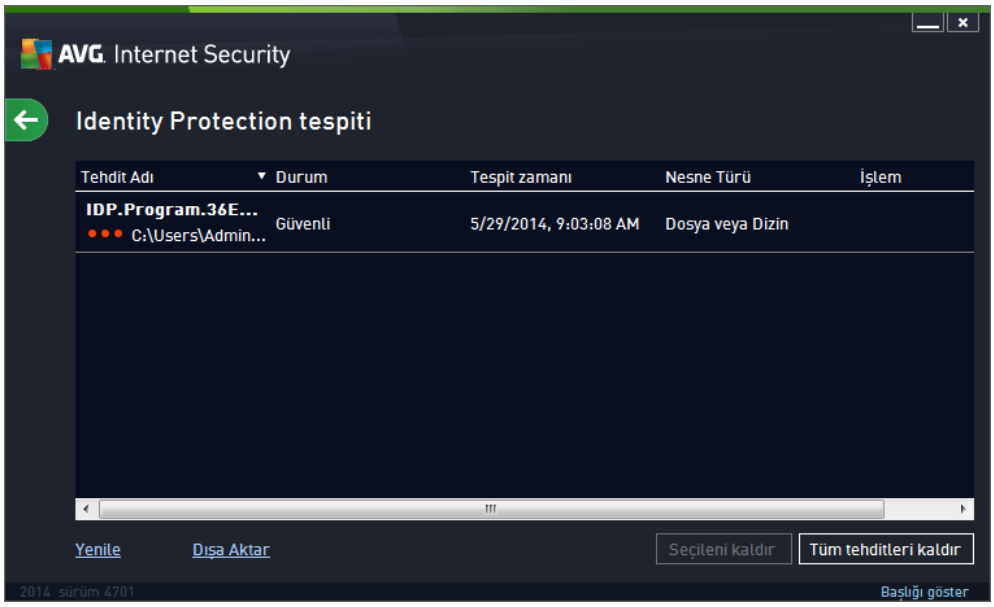
- ***Tespit Adi*** - tespit edilen nesnenin açiklamasi (*muhtemelen adi da*) ve konumu
- ***Sonuç*** - tespit edilen nesne ile gerçeklestirilen eylem
- ***Tespit Zamani*** - tehdidin tespit edildigi ve engellendigi tarih ve saat
- ***Nesne Türü*** - tespit edilen nesnenin türü
- ***Islem*** - tespit edilmesi amaciyla potansiyel tehlike tasiyan nesneyi uyaran islem nedir

Kontrol dügmeleri

- ***Yenile*** - ***Online Shield***
- ***Disa aktar*** - tespit edilen tüm nesneleri bir dosyada disa aktarin
- ***Seçileni kaldir*** - listeden seçilen kayitlari vurgulayabilir ve bu dügmeyi kullanarak yalnizca bu seçilen ögeleri silebilirsiniz
- ***Tüm tehditleri kaldir*** - iletisim kutusunda listelenen tüm kayitlari silmek için bu dügmeyi kullanin
- - varsayilan AVG ana iletisim kutusuna *(bilesen genel görünümü) geri dönmek için* bu iletisim kutusunun sol üst kismindaki oku kullanin

14.3. Identity Protection Sonuçları

Identity Protection Sonuçları iletisim kutusuna **AVG Internet Security 2014 ana penceresinin üst satirindaki gezinme bölümünden *Seçenekler / Geçmis / Identity Protection Sonuçlari*** menü ögesi yoluyla erisilebilir.



Iletisim kutusunda Identity Protection bilesenin tespit ettigi tüm bulgularin listesi bulunur. Tespit edilen tüm nesneler için asagidaki bilgiler verilir:

- ***Tehdit Adi*** - tespit edilen nesnenin açiklamasi (*muhtemelen adi da*) ve kaynagi
- ***Sonuç*** - tespit edilen nesne için yapilan islem
- ***Tespit Zamani*** - süpheli nesnenin tespit edildigi tarih ve saat
- ***Nesne Türü*** - tespit edilen nesnenin türü
- ***Islem*** - tespit edilmesi amaciyla potansiyel tehlike tasiyan nesneyi uyaran islem nedir

Iletisim penceresinin alt kisminda, listenin altinda yukarida listelenen tespit edilen nesnelerin toplam sayisi hakkinda bilgi bulabilirsiniz. Ayrica, tespit edilen nesneler listesini ayri bir dosyada disa aktarabilir (***Listeyi dosyaya aktar***) ve tespit edilen nesneler hakkindaki tüm girisleri silebilirsiniz (***Listeyi temizle***).

Kontrol dügmeleri

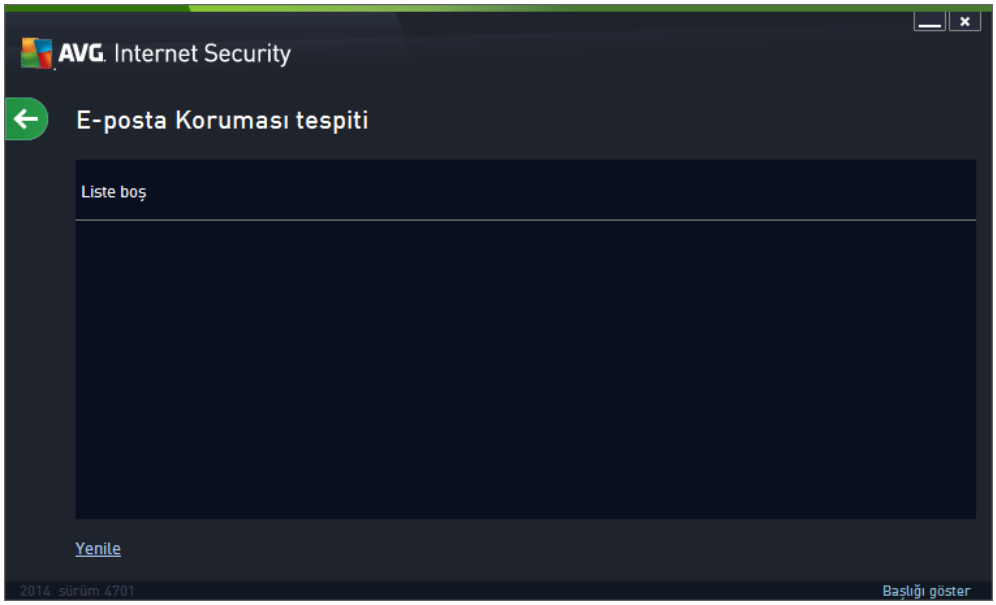
Identity Protection Sonuçlari arayüzünde bulunan kontrol dügmeleri sunlardir:

- ***Listeyi yenile*** - Tespit edilen tehlikelerin listesini günceller
- - Varsayilan AVG ana iletisim kutusuna *(bilesen genel görünümü) geri dönmek için* bu

iletisim kutusunun sol üst kismindaki oku kullanin

14.4. E-posta Koruması Sonuçları

E-posta Korumasi Sonuçlari iletisim kutusuna **AVG Internet Security 2014 ana penceresinin üst satirindaki gezinme bölümünden *Seçenekler / Geçmis / E-posta Korumasi Sonuçlari*** menü ögesi yoluyla erisilebilir.



Iletisim kutusunda E-posta Tarayicisi bilesenin tespit ettigi tüm bulgularin listesi bulunur. Tespit edilen tüm nesneler için asagidaki bilgiler verilir:

- ***Tespit adi*** - tespit edilen nesnenin açiklamasi (*muhtemelen adi da*) ve kaynagi
- ***Sonuç*** - tespit edilen nesne ile gerçeklestirilen eylem
- ***Algilama zamani*** - Süpheli nesnenin algilandigi tarih ve saat
- ***Nesne Türü*** - tespit edilen nesnenin türü
- ***Islem*** - tespit edilmesi amaciyla potansiyel tehlike tasiyan nesneyi uyaran islem nedir

Iletisim penceresinin alt kisminda, listenin altinda yukarida listelenen tespit edilen nesnelerin toplam sayisi hakkinda bilgi bulabilirsiniz. Ayrica, tespit edilen nesneler listesini ayri bir dosyada disa aktarabilir (***Listeyi dosyaya aktar***) ve tespit edilen nesneler hakkindaki tüm girisleri silebilirsiniz (***Listeyi temizle***).

Kontrol dügmeleri

E-posta Tarayicisi algilama arayüzünde bulunan kontrol dügmeleri sunlardir:

- ***Listeyi yenile*** - Algilanan tehlikelerin listesini günceller

-  - Varsayilan AVG ana iletisim kutusuna *(bilesen genel görünümü) geri dönmek için* bu iletisim kutusunun sol üst kismindaki oku kullanin

14.5. Online Shield Sonuçları

Online Shield ziyaret ettiginiz web sitelerinin içeriklerini ve sitelerin içindeki muhtemel dosyalari, ilgili web sitesi henüz tarayicinizda görünmeden ya da bilgisayariniza indirmeden tarar. Bir tehdit tespit edilirse asagidaki iletisim kutusu vasitasiyla hemen uyarilirsiniz:

Bu uyari iletisim kutusunda tespit edilen ve virüs bulasmis olarak atanan nesne hakkinda daha fazla bilgi (*Tehdit*) ve ilgili bulasma hakkinda bazi açiklamalar (*Nesne adi*) bulabilirsiniz. Daha fazla bilgi baglantisi, sizi tespit edilen bulasma hakkinda ayrintili bilgi (biliniyorsa) bulabileceginiz çevrimiçi virüs ansiklopedisine yönlendirir. Iletisim kutusundan asagidaki kontrol ögeleri bulunur:

- ***Ayrintilari göster*** - bulasma tespit edildiginde çalisan islem ve islemin tanimi ile ilgili bilgileri bulabileceginiz yeni bir açilir pencere açmak için bu baglantiyi tiklatin.
- ***Kapat*** - uyari iletisim kutusunu kapatmak için bu dügmeyi tiklatin.

Süpheli web sayfasi açilmaz ve tehlike tespiti ***Online Shield tespitleri*** listesinde kaydedilir. Bu tespit edilen tehditler genel görünümüne **AVG Internet Security 2014** ana penceresinin üst bölümünde yer alan ***Seçenekler / Geçmis / Online Shield tespiti menü ögesi yoluyla erisilebilir.***

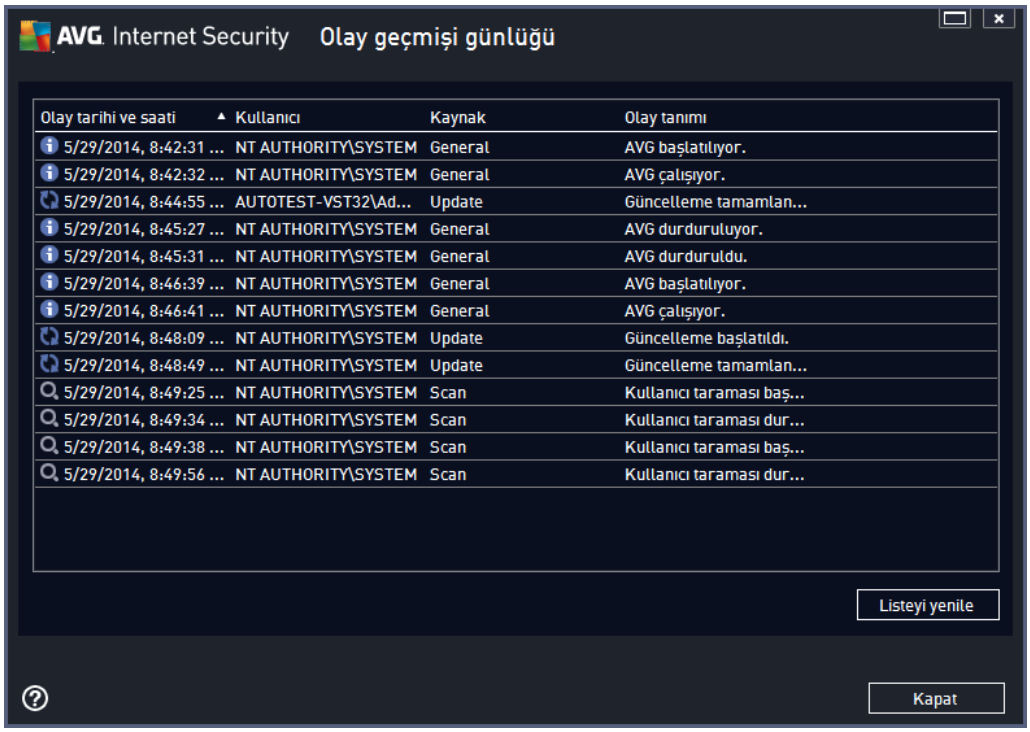
Tespit edilen tüm nesneler için asagidaki bilgiler verilir:

- ***Tehdit Adi*** - tespit edilen nesnenin açiklamasi (*muhtemelen adi da*) ve kaynagi (*web sayfasi*)
- ***Sonuç*** - tespit edilen nesne ile gerçeklestirilen eylem
- ***Tespit Zamani*** - tehdidin tespit edildigi ve engellendigi tarih ve saat
- ***Nesne Türü*** - tespit edilen nesnenin türü
- ***Islem*** - tespit edilmesi amaciyla potansiyel tehlike tasiyan nesneyi uyaran islem nedir

Kontrol dügmeleri

- ***Yenile*** - ***Online Shield***
- ***Disa aktar*** - tespit edilen tüm nesneleri bir dosyada disa aktarin
- - varsayilan AVG ana iletisim kutusuna *(bilesen genel görünümü) geri dönmek için* bu iletisim kutusunun sol üst kismindaki oku kullanin

14.6. Olay Geçmişi



Olay geçmisi iletisim kutusuna **AVG Internet Security 2014 ana penceresinin üst satirindaki gezinme bölümünden *Seçenekler / Geçmis / Olay Geçmisi*** menü ögesi yoluyla erisilebilir. Bu iletisim kutusunda, **AVG Internet Security 2014** uygulamasinin çalismasi sirasinda olusan önemli olaylarin bir özetini bulabilirsiniz. Bu iletisim kutusunun kayitlarini sagladigi olay türleri: AVG uygulamasi güncellemeleri hakkinda bilgiler; tarama baslangici, sonu veya durdurulmasi hakkinda bilgiler(*otomatik olarak gerçeklestirilen testler de dahil*); virüs tespitiyle baglantili olaylar hakkinda gerçeklestigi konumu da içeren bilgiler (*yerlesik kalkan veya tarama* kaynakli) ve diger önemli olaylar.

Her olay için su bilgiler listelenir:

- ***Olay Tarihi ve Saati*** olayin gerçeklestigi kesin tarihi ve saati belirtir.
- ***Kullanici*** olayin gerçeklestigi sirada oturum açmis olan kullanicinin adini gösterir.
- ***Kaynak***, kaynak bileseni veya AVG sisteminin olayi tetikleyen bölümü hakkinda bilgi verir.
- ***Olay Açiklamasi*** tam olarak ne oldugu hakkinda kisa bir açiklama sunar.

Kontrol dügmeleri

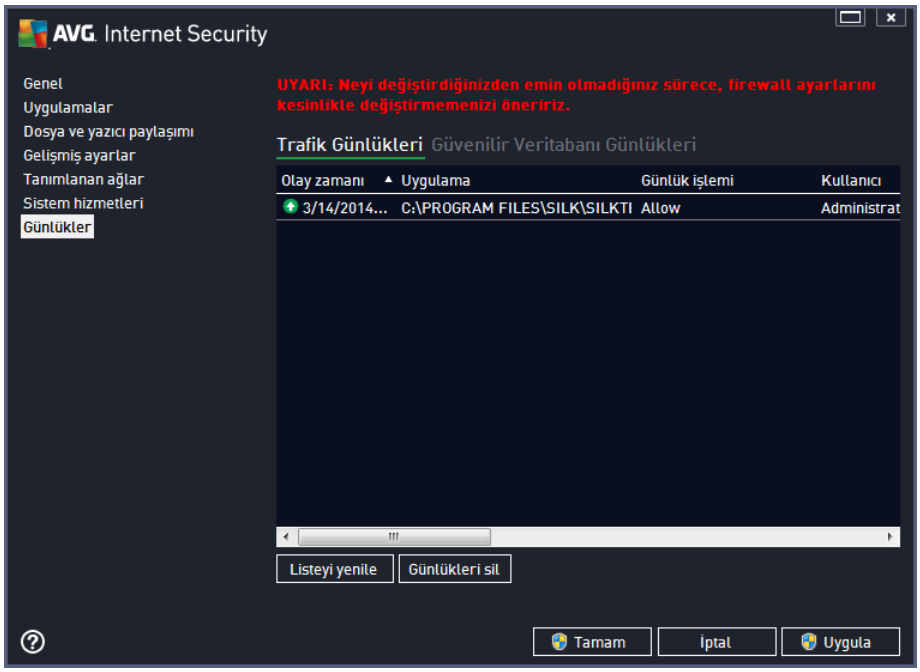
- ***Listeyi yenile*** - olaylar listesindeki tüm girisleri güncellemek için bu dügmeye basin
- ***Kapat*** - **AVG Internet Security 2014** ana penceresine dönmek için bu dügmeyi tiklatin

14.7. Firewall günlüğü

Bu iletisim kutusu uzman düzeyinde yapilandirma için tasarlanmistir ve yapacaginiz degisiklikten kesinlikle emin degilseniz hiçbir ayari degistirmemenizi tavsiye ederiz!

Günlükler iletisim kutusu, kaydedilen tüm Firewall eylemlerini ve etkinliklerini ilgili parametrelerin ayrintili tanimlari ile birlikte iki sekmede görüntüleyebilmenizi saglar.

- ***Trafik Günlükleri*** - Bu sekme aga baglanmaya çalisan tüm uygulamalarin etkinlikleri hakkindaki bilgileri sunar. Her öge için olay zamani, uygulama adi, ilgili günlük islemi, kullanici adi, PID, trafik yönü, protokol türü, uzak ve yerel baglanti noktalarinin numaralariyla yerel ve uzak IP adresleri hakkindaki bilgileri bulabilirsiniz.



- ***Güvenilir Veritabani Günlükleri*** - *Güvenilir veritabani*, her zaman çevrimiçi iletisime izin verebilen sertifikali ve güvenilir uygulamalar hakkinda bilgi toplayan AVG dahili veritabanidir. Yeni bir uygulama aga ilk baglanmaya çalistiginda (*diger bir deyisle, bu uygulama için henüz güvenlik duvari kurali belirtilmediginde*), ilgili uygulama için ag iletisimine izin verilip verilmeyecegini ögrenmek önemlidir. Ilk önce, AVG *Güvenilir veritabanini* arar ve uygulama listelenmisse otomatik olarak aga erisim izni verir. Ancak bundan sonra, veritabaninda uygulama hakkinda mevcut bilgi yoksa, uygulamanin aga erismesine izin vermek isteyip istemediginiz tek bir iletisim kutusuyla size sorulur.

Kontrol dügmeleri

- ***Listeyi yenile*** - kaydedilen tüm parametreler seçilen davranis özelliklerine göre düzenlenebilir: kronolojik olarak (*tarihler*) ya da alfabetik olarak (*diger sütunlarda*) sadece ilgili sütun basligini tiklatin. O anda görüntülenen bilgileri yenilemek için ***Listeyi yenile*** dügmesini kullanin.

- ***Günlükleri sil*** - tablodaki tüm girisleri silmek için basin.

15. AVG Güncellemeleri

Güvenlik yazilimlarinin hiçbiri, rutin olarak güncellenmedigi takdirde sizi çesitli tehlikelere karsi korumayi garanti edemez! Virüs yazarlari, yazilim ve isletim sistemlerinde yararlanabilecekleri güvenlik açiklari aramaktadir. Her gün yeni virüsler, yeni kötü amaçli yazilimlar ve yeni bilgisayar saldirilari gerçeklestirilmektedir. Bu nedenle yazilim gelistiricileri,tespit edilen güvenlik açiklarini kapatmak üzere devamli olarak güncellemeler ve güvenlik paketleri yayinlamaktadir.

Yeni ortaya çikan tehditler ve bunlarin yayilma hizi dikkate alindiginda **AVG Internet Security 2014** ürününüzü düzenli olarak güncellemek hayati bir öneme sahiptir. En iyi çözüm, otomatik güncellemenin yapilandirildigi program varsayilan ayarlarina güvenmektir. **AVG Internet Security 2014** ürününüzün virüs veritabani güncel degilse, programin en yeni tehditleri tespit edemeyecegini lütfen unutmayin!

AVG'nizi rutin olarak güncellemeniz çok önemlidir! Gerekli virüs tanimi güncellemelerinin mümkün ise her gün yapilmasi gerekmektedir. Daha az önem tasiyan program güncellemeleri haftada bir yapilabilir.

15.1. Güncelleme başlatma

Mümkün olan en yüksek güvenligi saglamak için, **AVG Internet Security 2014** varsayilan olarak her dört saatte bir yeni virüs veritabani güncellemeleri kontrol etmeye ayarlanmistir. AVG güncellemeleri belirli bir takvime göre degil yeni tehditlerin miktari ve ciddiyetine göre yayinlandigindan, bu kontrol AVG virüs veritabaninizin sürekli güncel tutulmasi açisindan çok önemlidir.

Yeni güncelleme dosyalarini hemen kontrol etmek istiyorsaniz, ana kullanici arayüzündeki Simdi güncelle hizli baglantisini kullanin. Bu baglantiya her zaman herhangi bir kullanici arayüzü iletisim kutusundan ulasabilirsiniz. Güncellemeyi baslatmanizin ardindan AVG, yeni güncelleme dosyalari olup olmadigini dogrular. Varsa, **AVG Internet Security 2014** güncellemeleri indirmeye baslar ve güncelleme islemini kendisi baslatir. Güncelleme sonuçlari hakkinda AVG sistem tepsisi simgesi üzerinde beliren iletisim kutusuyla bilgilendirilirsiniz.

Güncelleme baslatmalarinin sayisini azaltmak istiyorsaniz, kendi güncelleme baslatma parametrelerinizi ayarlayabilirsiniz. Ancak, ***günde en az bir kez güncellemeyi baslatmaniz kesinlikle önerilir!*** Yapilandirma Gelismis ayarlar/Programlar bölümünde, asagidaki iletisim kutularindan düzenlenebilir:

- Tanim güncelleme programi
- Program güncelleme programi
- Anti-Spam güncelleme programi

15.2. Güncelleme seviyeleri

AVG Internet Security 2014 seçilebilecek iki güncelleme düzeyi sunar:

- ***Tanim güncellemeleri*** güvenilir virüsten korunma, istenmeyen postalardan korunma ve kötü amaçli yazilimlara karsi korunma yazilimlari için gerekli degisiklikleri içerir. Genellikle kodu degistirmez ve yalnizca tanimlama veritabanini günceller. Bu güncelleme sunulur sunulmaz yüklenmelidir.

- ***Program güncellemesi*** çesitli program degisikliklerini, onarimlari ve iyilestirmeleri içerir.

Bir güncelleme programlarken, her iki güncelleme düzeyi için de belirli parametreler tanimlamak mümkündür:

- Tanim güncelleme programi
- Program güncelleme programi

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

16. SSS ve Teknik Destek

AVG Internet Security 2014 uygulamanizin satisiyla ilgili veya teknik sorunlariniz olmasi durumunda yardim için birçok yol mevcuttur. Lütfen asagidaki seçeneklerden birini seçin:

- ***Destek Alin***: Dogrudan AVG uygulamasi içinden AVG web sitesindeki (*http://www.avg.com/*) özel bir müsteri destek sayfasina erisebilirsiniz. AVG web sitesindeki destek seçeneklerine erismek için ***Yardim / Destek Alin*** ana menü ögesini seçin. Devam etmek için lütfen web sayfasindaki talimatlari izleyin.

- ***Destek*** *(ana menü baglantisi)*: AVG uygulama menüsünde (*ana kullanici arayüzünün en üstünde*) yardim bulmaya çalisirken ihtiyaciniz olabilecek tüm bilgileri içeren yeni bir iletisim kutusu açan ***Destek*** baglantisi bulunur. Iletisim kutusunda kurulu AVG programiniz ile ilgili temel bilgiler (*program / veritabani sürümü*), lisans ayrintilari ve hizli destek baglantilari listesi bulunur.

- ***Yardim dosyasinda sorun giderme***: Dogrudan **AVG Internet Security 2014 içindeki yardim dosyasindan erisilebilen yeni bir *Sorun giderme*** bölümü mevcuttur *(yardim dosyasini açmak için uygulamadaki herhangi bir pencerede F1 tusuna basin)*. Bu bölüm, kullanici teknik bir sorun hakkinda profesyonel yardim aradiginda en sik karsilasilan durumlar hakkinda bir liste sunar. Lütfen sizin sorununuzu en iyi açiklayan durumu seçin ve sorunun çözümüne dair ayrintili talimatlar almak için tiklatin.

- ***AVG web sitesi Destek Merkezi***: Sorunuzun çözümünü AVG web sitesinde de (*http://www.avg.com/*) arayabilirsiniz. ***Destek Merkezi*** bölümünde hem satis sorunlari hem de teknik sorunlarla ilgili tematik olarak gruplandirilmis konular bulabilirsiniz.

- ***Sik sorulan sorular***: AVG web sitesinde (*http://www.avg.com/*) ayri ve çok ayrintili bir sik sorulan sorular bölümü de bulabilirsiniz. Bu bölüme ***Destek Merkezi / SSS'ler ve Egitimler*** menü seçeneginden erisilebilir. Burada da tüm sorular satis, teknik ve virüs kategorileri olarak organize bir sekilde siniflandirilmistir.

- ***AVG ThreatLabs***: AVG ile iliskili özel bir web sitesi (*http://www.avgthreatlabs.com/website-safety-reports/*) olarak virüs sorunlari baglaminda çevrimiçi tehditler hakkinda genel bilgiler vermek üzere hazirlanmistir. Virüs, casus yazilim silme talimatlari ve nasil güvenli kalacaginiza dair öneriler de bulabilirsiniz.

- ***Tartisma forumu***: Ayrica http://forums.avg.com adresindeki AVG kullanicilari tartisma forumunu kullanabilirsiniz.