bitdefender
ANTIVIRUS v10

10th anniversary

Kullanıcı Kılavuzu

Antivirus

Antispyware

bitdefender
secure your every bit

BitDefender Antivirus v10

Kullanıcı Kılavuzu

BitDefender

Yayımlanma 2007.06.09
Version 10.2

Yasal Uyarı


bitdefender
secure your every bit

İçindekiler

Lisans ve Garanti ..... **ix**

Önsöz ..... **xiii**

1. Bu Kitapta Kabul Edilen Yazım Kuralları xiii
   1.1. Tipografik Kurallar xiii
   1.2. Uyarılar xiv
2. Kitabın Yapısı xiv
3. Yorumlarınız xv

BitDefender Hakkında 1

1. BitDefender Kimdir? **3**
   1.1. Neden BitDefender? 3

Ürün Kurulumu 5

2. BitDefender Antivirus v10 Kurulumu **7**
   2.1. Sistem Gereksinimleri 7
   2.2. Kurulum Adımları 7
   2.3. Başlangıç Kurulum Sihirbazı 10
      2.3.1. Adım 1/8 – BitDefender Başlangıç Kurulum Sihirbazı 11
      2.3.2. Adım 2/8- BitDefender Antivirus v10'u Kaydedin 11
      2.3.3. Adım 3/8 – BitDefender Hesabı Yarat 12
      2.3.4. Adım 4/8 – Hesap Detaylarının Girilmesi 13
      2.3.5. Adım 5/8 – RTVR Hakkında Bilgi 14
      2.3.6. Adım 6/8 – Çalıştırılacak Görevlerin Seçilmesi 14
      2.3.7. Adım 7/8 – Görevlerin Tamamlanmasını Bekleyin 15
      2.3.8. Adım 8/8 – Özeti Görüntüle 16
   2.4. Yükseltme 16
   2.5. BitDefender Özelliklerini Kaldırma, Düzeltme veya Değiştirme 17

Tanım ve Özellikler 19

3. BitDefender Antivirus v10 ..... **21**
   3.1. Antivirus 21
   3.2. Antispyware 22
   3.3. Diğer Özellikler 22

4. BitDefender Modülleri **25**
   4.1. Genel Modülü 25
   4.2. Virüs Koruma Modülü 25
   4.3. Antispyware Modülü 25
   4.4. Güncelleme Modülü 26

Yönetim Konsolu 27

5. Tanıtma 29
5.1. Sistem Tepsisi 30
5.2. Tarama Etkinlik Çubuğu 31

6. Genel Modülü 33
6.1. Merkezi Yönetim 33
6.1.1. Hızlı Görevler 34
6.1.2. Güvenlik Seviyesi 34
6.1.3. Kayıt Durumu 35
6.2. Yönetim Konsolu Ayarları 36
6.2.1. Genel Ayarlar 36
6.2.2. Virüs Raporu Ayarları 37
6.2.3. Kabuk Ayarları 38
6.2.4. Ayarların Yönetimi 38
6.3. Olaylar 39
6.4. Ürün Kaydı 40
6.4.1. Kayıt Sihirbazı 40
6.5. Hakkında 45

7. Virüs Koruma Modülü 47
7.1. Erişim anında tarama 47
7.1.1. Koruma Seviyesi 48
7.2. Isteğe bağlı tarama 52
7.2.1. Tarama Görevleri 52
7.2.2. Kısayol Menüsü 54
7.2.3. Tarama Görevi Özellikleri 54
7.2.4. Isteğe bağlı tarama Tipleri 65
7.2.5. Rootkit Taraması 69
7.3. Karantina 71

8. Antispyware Modülü 75
8.1. Antispyware Durumu 76
8.1.1. Koruma Seviyesi 77
8.2. Gelişmiş Ayarlar – Kişisel Gizlilik Kontrolü 77
8.2.1. Yapılandırma Sihirbazı 78
8.2.2. Kuralları Yönetmek 81
8.3. İleri Ayarlar – Kayıt Kontrolü 82
8.4. İleri Ayarlar- Arama (Dial) Kontrolü 84
8.4.1. Yapılandırma Sihirbazı 86
8.5. İleri Ayarlar - Cookie Kontrolü 88
8.5.1. Yapılandırma Sihirbazı 91
8.6. İleri Ayarlar - Script Kontrolü 92
8.6.1. Yapılandırma Sihirbazı 93
8.7. Sistem Bilgileri 95

9. Güncelleme Modülü 97

9.1. Otomatik Güncelleme 97
9.2. Manuel Güncelleme 98
9.2.1. `Weekly.exe` dosyası ile manuel güncelleme 99
9.2.2. `Zip arşivleri` ile Manuel Güncelleme 99
9.3. Güncelleme Ayarları 101
9.3.1. Güncelleme Yeri Ayarları 101
9.3.2. Otomatik Güncelleme Seçenekleri 102
9.3.3. Manuel Güncelleme Ayarları 103
9.3.4. İleri Seçenekler 103

En İyi Uygulamalar 105

10. En İyi Uygulamalar 107
10.1. Kötü amaçlı yazılım tehditlerine karşı bilgisayarınız nasıl korunur? 107
10.2. Bir Tarama Görevi Nasıl Yapılandırılır 108

BitDefender Kurtarma CD'si 109

11. Tanıtma 111
11.1. KNOPPIX Nedir? 111
11.2. Sistem Gereksinimleri 111
11.3. Dahil edilen Yazılımlar 112
11.4. BitDefender Linux Güvenlik Çözümleri 112
11.4.1. BitDefender SMTP Proxy 112
11.4.2. BitDefender Uzaktan Yönetim 113
11.4.3. BitDefender Linux Edition 113

12. LinuxDefender Nasıl? 115
12.1. Başlatma ve Durdurma 115
12.1.1. LinuxDefender'ın Başlatılması 115
12.1.2. LinuxDefender'i Durdur 116
12.2. Internet Bağlantısının Yapılandırılması 117
12.3. BitDefender Güncelleme 118
12.4. Virüs Tarama 118
12.4.1. Windows verilerime nasıl erişebilirim? 118
12.4.2. Bir virüs koruma taraması nasıl yapabilirim? 119
12.5. Anlık Posta Filteleme Toaster'ın Oluşturulması 119
12.5.1. Ön Gereksinimler 120
12.5.2. E-posta Toaster 120
12.6. Ağ Güvenlik Denetiminin Yapılması 121
12.6.1. Rootkit'lerin Kontrolü 121
12.6.2. Nessus – Ağ Tarayıcısı 121
12.7. Sisteminizin RAM Durumunun Kontrolü 122

Yardım Alma 123

13. Destek 125

13.1. Destek Departmanı 125
13.2. Çevrimiçi Yardım 125
13.2.1. BitDefender Bilgi Üssü 125
13.3. İrtibat Bilgileri 126
13.3.1. Web Adresleri 126
13.3.2. Şubeler 126
Sözlük 129

Lisans ve Garanti

BU ŞART VE KOŞULLARI KABUL ETMİYORSANIZ YAZILIMI YÜKLEMEYİNİZ. “KABUL EDİYORUM”, “TAMAM”, "DEVAM ET", “EVET”’İ SEÇEREK VEYA HERHANGİ BİR ŞEKİLDE YAZILIMI YÜKLEYEREK VEYA KULLANARAK, BU ANLAŞMANIN ŞARTLARINI TAMAMEN ANLADIĞINIZI VE KABUL ETTİĞİNİZİ BELİRTMİŞ OLUYORSUNUZ.

Bu Şartlar, satın alınan lisans veya herhangi bir ilgili hizmet anlaşması altında size teslim edilen ve dokümantasyonda ve bunların herhangi bir kopyasından tanımlanan uygulamaların ilgili dokümantasyonunu ve herhangi bir güncelleme ve yükseltmesini (upgrade) içeren, sizin için lisanslanmış olan, ev kullanıcıları için BitDefender Çözüm ve Hizmetlerini kapsamaktadır.

Bu Lisans Anlaşması, siz (gerçek veya tüzel kişi) ve SOFTWIN arasında, bilgisayar yazılım ve hizmetlerini içeren, yukarıda tanımlı SOFTWIN yazılım ürünlerinin kullanımı için yapılan yasal bir anlaşmadır ve tümü, uluslararası telif hakları kanunları ve uluslararası anlaşmalar tarafından korunan ilgili medya, basılı materyaller ve “çevrimiçi” veya elektronik dokümantasyonları (bundan sonra “BitDefender” olarak anılacaktır) içerebilir. BitDefender’ı yükleyerek, kopyalayarak veya kullanarak, bu anlaşma şartları ile bağlı olduğunuzu kabul etmiş oluyorsunuz.

Bu anlaşma şartlarını kabul etmiyorsanız, BitDefender’ı yüklemeyin veya kullanmayın.

BitDefender Lisansı. BitDefender telif hakları kanunları ve uluslararası telif hakları anlaşmaları ve de diğer fikri mülkiyet hakları ve anlaşmaları ile korunmaktadır. BitDefender satılmamaktadır, sadece lisansı verilmektedir.

LİSANSIN VERİLMESİ. SOFTWIN, BitDefender’ı kullanmak için size ve sadece size aşağıdaki münhasır olmayan, sınırlı, devredilemez ve lisans ücretine tabi olan lisansı vermektedir.

UYGULAMA YAZILIMI. BitDefender’ı, toplam lisanslı kullanıcı sayısı sınırı altında kalma koşulu ile, gereken sayıdaki bilgisayara yükleyebilir ve kullanabilirsiniz. Yedekleme amacı ile bir ek kopya alabilirsiniz.

MASAÜSTÜ KULLANICI LİSANSI. Bu lisans, tek bir bilgisayara yüklenebilen ve ağ hizmetleri sağlamayan BitDefender yazılımı için geçerlidir. Her ana kullanıcı bu yazılımı tek bir bilgisayara yükleyebilir ve yedekleme amacıyla başka bir cihazda bir ek kopyasını alabilir. İzin verilen ana kullanıcı sayısı, lisans kullanıcı sayısıdır.

LİSANSIN SÜRESİ. Burada verilen lisans, BitDefender’ın satın alınma tarihinde başlayacak ve satın alınan lisansın süresinin sonunda sona erecektir.

YÜKSELTMELER (UPGRADE). BitDefender yükseltme olarak etiketlenmişse, BitDefender'ı kullanmak amacıyla yükseltme edilebilir olan ve SOFTWIN tarafından tanımlanan bir ürünü kullanmak için uygun şekilde lisans almanız gerekmektedir. Yükseltme olarak etiketlenen bir BitDefender, yükseltme yapabilmenizin temelini oluşturan ürünün yerine geçer ve/veya onu tamamlar. Yükseltilmiş ürünü ancak bu Lisans Anlaşması şartlarına göre kullanabilirsiniz. BitDefender, tek bir ürün olarak lisansını aldığınız yazılım programları paketinin bir bileşeninin yükseltmesi ise, BitDefender yalnızca bu tek ürün paketinin bir parçası olarak kullanılabilir ve transfer edilebilir ve toplam lisanslı kullanıcı sayısından daha fazlasına ayrılamaz. Bu lisansın şart ve koşulları siz ve SOFTWIN arasında asıl ürün veya yükseltme ürünlerle ilgili önceki tüm anlaşmaların yerine geçer.

TELİF HAKKI. BitDefender içindeki ve BitDefender'a ait tüm haklar, isimler ve BitDefender içindeki ve BitDefender'a ait tüm telif hakları (BitDefender içindeki herhangi bir resim, fotoğraf, logo, animasyon, video, ses, müzik, metin, ve "küçük uygulamalar" dahil olmak fakat bunlarla sınırlı olmamak üzere), birlikte gelen basılı materyaller ve BitDefender kopyaları Softwin'e aittir. BitDefender telif hakları kanunları ve uluslararası anlaşma hükümleri tarafından korunmaktadır. Bu nedenle, BitDefender'ı herhangi diğer bir tescilli materyal gibi kullanmanız gerekmektedir. BitDefender ile birlkte gelen basılı materyalleri kopyalayamazsınız. BitDefender'ın bulunduğu medya veya yollardan hangisi tarafından yaratılmış olursa olsun, tüm kopyalardaki tüm telif hakkı uyarıları, asıl şekillerinde üretilecek ve dahil edilecektir. BitDefender lisansını kiralayamaz, satamaz, paylaşamaz veya alt lisans yoluyla başkasına veremez. BitDefender kaynak kodunu bulmak için ters mühendislik, yeniden derleme, sökme, derivatif çalışmalar yapma, değiştirme, tercüme veya başka herhangi bir girişimde bulunamazsınız.

SINIRLI SORUMLULUK. SOFTWIN, BitDefender'ın üzerinde dağıtıldığı medyada, BitDefender'ın size teslim edildiği tarihten itibaren otuz günlük bir süre içinde hiç bir sorun olmayacağını garanti etmektedir. Bu garantinin ihlal edilmesi durumunda, tek çözüm şekli, SOFTWIN'in, takdiri kendisinde olmak üzere, hasarlı medyanın alınmasından sonra bu medyayı değiştirmek veya BitDefender'a ödediğiniz ücretin size geri ödenmesi olacaktır. SOFTWIN, BitDefender'ın hiç bozulmayacağını veya hatasız olduğunu veya hataların düzeltileceğini garanti etmemektedir. SOFTWIN, BitDefender'ın sizin ihtiyaç ve gerekliliklerinizi karşılayacağını garanti etmemektedir.

BU ANLAŞMADA AÇIKÇA BELİRTİLMEDİĞİ SÜRECE, SOFTWIN ÜRÜNLER, GELİŞTİRMELER, BAKIM VEYA DESTEK İLE İLGİLİ VEYA DİĞER MATERYALLER (MADDİ VEYA MADDİ OLMAYAN) VEYA SOFTWIN TARAFINDAN SAĞLANAN HİZMET İLE İLGİLİ, AÇIKÇA VEYA İMA YOLUYLA BELİRTİLMİŞ TÜM DİĞER GARANTİLERİ KABUL ETMEMEKTEDİR. SOFTWIN BURADA, TİCARİ SATIMA UYGUNLUK GARANTİLERİ, BELİRLİ BİR AMACA UYGUNLUK, TASARRUF HAKKI, MÜDEHALE ETMEME, VERİ DOĞRULUĞU, BİLGİ İÇERİĞİ DOĞRULUĞU, SİSTEM ENTEGRASYONU VE ÜÇÜNCÜ ŞAHIS YAZILIMLARINI, SPYWARE, ADWARE,

COOKIE'LER, E-POSTALAR, DOKÜMANLAR, REKLAMLAR VEYA BENZER ÜRÜNLERİNİ FİLTRELEYEREK, ETKİSİZ KILARAK VEYA SİLEREK BU ÜÇÜNCÜ ŞAHISLARIN YASA, KANUN, ANLAŞMA, GELENEK VE UYGULAMA VEYA TİCARİ KULLANIM YOLUYLA KAZANILMIŞ HAKLARININ İHLAL EDİLMEMESİ GİBİ, FAKAT BUNLARLA SINIRLI KALMAMAK ÜZERE İMA EDİLMİŞ HERHANGİ BİR GARANTİYİ AÇIKÇA REDDETMEKTEDİR.

HASARLAR İÇİN YASAL UYARI. BitDefender'ı kullanan, test eden veya değerlendiren herkes BitDefender kalitesi ve performansı ile ilgili tüm riskleri üzerine almaktadır. Hiç bir durumda, BitDefender'ın kullanımı, performansı veya teslimatı da dahil olmak fakat bunlarla sınırlı olmamak üzere, doğrudan veya dolaylı olarak meydana gelen hiç bir zarar için, bu zararların varlığı veya ihtimali konusunda SOFTWIN uyarılmış olsa dahi, SOFTWIN'in hiç bir yükümlülüğü bulunmamaktadır. BAZI ÜLKELER KAZARA VEYA SONUÇSAL ZARARLAR İÇİN SORUMLULUK SINIRLANDIRILMASI VEYA HARİÇ TUTULMASINA İZİN VERMEMEKTEDİR. BU NEDENLE YUKARIDAKİ SINIRLANDIRMALAR VEYA HARİÇ DURUMLAR SİZİN İÇİN GEÇERLİ OLMAYABİLİR. HİÇ BİR KOŞULDA, SOFTWIN'IN YÜKÜMLÜLÜĞÜ BITDEFENDER'IN SİZE SATILDIĞI FİYATI AŞAMAZ. Yukarıda belirtilen yasal uyarılar ve sınırlandırmalar, BitDefender'ı kullanmayı, değerlendirmeyi veya denemeyi kabul edip etmemeniz dikkate alınmaksızın geçerli olacaktır.

KULLANICILAR İÇİN ÖNEMLİ UYARILAR. BU YAZILIM HATA TOLERANSLI DEĞİLDİR VE HATASIZ PERFORMANS VEYA KULLANIM GEREKTİREN HERHANGİ BİR TEHLİKELİ ORTAMDAKİ KULLANIM İÇİN TASARLANMAMIŞ VE AMAÇLANMAMIŞTIR. BU YAZILIM, UÇAK NAVİGASYONU, NÜKLEER TESİSLER VEYA İLETİŞİM SİSTEMLERİ, SİLAH SİSTEMLERİ, DOĞRUDAN VEYA DOLAYLI HAYAT-DESTEK SİSTEMLERİ, HAVA TRAFİĞİ KONTROLÜ İŞLEMLERİNDE VEYA HATALARIN ÖLÜM, CİDDİ FİZİKSEL YARALANMA VEYA MÜLKE ZARAR VERME İLE SONUÇLANABİLECEĞİ UYGULAMA VE KURULUMLARDA KULLANILMAK ÜZERE TASARLANMAMIŞ VE AMAÇLANMAMIŞTIR.

GENEL. Bu Anlaşma Romanya kanunları ve uluslararası yönetmelik ve anlaşmalar tarafından yürütülecektir. Bu Lisans Şartlarından kaynaklanacak herhangi bir ihtilafın çözümünde münhasır yargı yetkisi Romanya mahkemelerine aittir.

BitDefender kullanım ücretleri ve maliyetleri, size önceden bildirimde bulunma şartı olmadan değişmeye tabidir.

Bu Anlaşmanın herhangi bir hükmünün geçersiz olması durumunda, bu geçersizlik Anlaşmanın diğer hükümlerinin geçerliliğini etkilemeyecektir.

BitDefender ve BitDefender logoları SOFTWIN'in ticari markalarıdır. Bu üründe ve ürünün ilgili materyallerinde kullanılan tüm diğer ticari markalar ilgili sahiplerinin mülkiyeti altındadır.

Bu şart ve koşulların herhangi birini ihlal etmeniz durumunda, önceden bildirimde bulunulmadan, lisansınız hemen iptal edilecektir. Lisansın iptal edilmesi durumunda SOFTWIN veya diğer BitDefender satıcılarının hiç birinden herhangi bir geri ödeme alma hakkınız olmayacaktır. Gizlilik ve kullanım kısıtlamaları ile ilgili şart ve koşullar lisansın iptal edilmesinden sonra da geçerli olmaya devam edecektir.

SOFTWIN bu şartları herhangi bir zamanda yenileyebilir ve yenilenen şartlar otomatik olarak, Yazılımın ilgili versiyonlarına uygulanacaktır. Bu Şartların herhangi bir kısmının geçersiz veya etkisiz olduğu anlaşılırsa, bu durum geri kalan Şartların geçerliliğini etkilemeyecek, bunlar geçerli ve yürülükte olmaya devam edeceklerdir.

Bu Şartların diğer dillere tercüme edilmesinde, tercümeler arasında tutarsızlık veya karşıtlık olması durumunda SOFTWIN tarafından yayınlanan İngilizce sürümü geçerli olacaktır.

İrtibat: SOFTWIN, at 5, Fabrica de Glucoza street, 72322-Sector 2, Bucharest, Romania, veya Tel No: 40-21-2330780 veya Fax:40-21-2330763, e-posta adresi:<office@bitdefender.com>.

Önsöz

Bu kılavuz, **BitDefender Antivirus v10**'u kişisel bilgisayarları için bir güvenlik çözümü olarak seçen tüm kullanıcılar için amaçlanmıştır. Bu kitapta sunulan bilgiler, yalnızca bilgisayar eğitimi almış kişiler için değil, aynı zamanda Windows altında çalışabilen herkes için uygundur.

Bu kitap size, **BitDefender Antivirus v10**'u, bunu yaratan Şirket ve ekibini tanıtacak, kurulum sürecinde size rehberlik edecek ve nasıl yapılandırılacağını öğretecektir. **BitDefender Antivirus v10**'un nasıl kullanılacağını, nasıl güncelleneceğini, test edileceğini ve kişiselleştirileceğini öğreneceksiniz. BitDefender'dan en iyi şekilde nasıl yaralanabileceğinizi öğreneceksiniz.

Size tatmin edici ve faydalı bir ders diliyoruz.

1. Bu Kitapta Kabul Edilen Yazım Kuralları

1.1. Tipografik Kurallar

Kitapta, okumayı kolaylaştırması amacıyla bazı metin stilleri kullanılmıştır. Görünüşleri ve anlamları aşağıdaki tabloda açıklanmıştır.

Görünüş	Açıklama
`sample syntax`	Söz dizimi örnekleri `tek boşluklu` karakterler ile yazılmıştır
http://www.bitdefender.com	URL linki http veya ftp sunucuları üzerindeki bazı dış lokasyonları işaret etmektedir.
`<support@bitdefender.com>`	E-posta adresleri, irtibat bilgisi olarak metin içine eklenmiştir.
"Önsöz" (shf. xiii)	Bu, doküman içindeki bazı yerleri işaret eden dahili bir linktir.
`filename`	Dosya ve dizinler `tek boşluklu` font kullanılarak yazılmıştır.
option	Tüm ürün opsiyonları **koyu** karakterler ile yazılmıştır.

Görünüş	Açıklama
`sample code listing`	Kod listeleri `tek boşluklu` karakterler ile yazılmıştır.

1.2. Uyarılar

Uyarılar grafiklerle işaretlenmiş, mevcut paragraf ile ilgili ek bilgiye dikkatinizi çeken, metin içindeki notlardır.

Not

Not sadece kısa bir gözlemdir. Her ne kadar bunlar ihmal edilebilir olsa bile, notlar belirli bazı özellikler veya bazı ilgili başlıklara linkler gibi değerli bilgiler sağlayabilirler.

Önemli

Bunlara dikkat edilmesi gerekir ve bunların atlanması tavsiye edilmemektedir. Genellikle çok kritik olmayan fakat önemli bilgiler sunmaktadırlar.

Uyarı

Çok dikkatli olarak ele almanız gereken kritik bilgilerdir. Bu uyarılara riayet ettiğinizde hiç bir kötü sonuç ortaya çıkmayacaktır. Bunları okumalı ve anlamalısınız, çünkü oldukça riskli olan şeyleri açıklamaktadırlar.

2. Kitabın Yapısı

Kitap 7 bölümden oluşmakta ve şu ana konuları içermektedir: BitDefender Hakkında, Ürün Kurulumu, Tanım ve Özellikler, Yönetim Konsolu, En İyi Uygulamalar, BitDefender Kurtarma CD'si ve Yardım Alma. Bunlara ek olarak, bazı teknik terimleri açıklayan bir sözlük de bulunmaktadır.

BitDefender Hakkında. BitDefender için kısa açıklama

Ürün Kurulumu. BitDefender'ın bir çalışma istasyonuna kurulması için gerekli olan talimatları adım adım verir. **BitDefender Antivirus v10**'nun yüklenmesini anlatan kapsamlı bir derstir. Başarılı bir kurulum için gerekli ön koşullardan başlanarak, tüm kurulum süreci boyunca yönlendirilirsiniz. Son olarak, BitDefender'ı silmeniz gerekmesi durumunda uygulamak üzere, silme prosedürü anlatılmaktadır.

Tanım ve Özellikler. BitDefender Antivirus v10, özellikleri ve ürün modülleri tanıtılır.

Yönetim Konsolu. BitDefender'ın temel yönetim ve bakımını anlatır. Bu bölümlerde **BitDefender Antivirus v10**'un tüm opsiyonları, ürünün nasıl kaydettirileceği, bilgisayarınızın nasıl taranacağı, güncellemelerin nasıl yapılacağı detaylı olarak açıklanır. Tüm BitDefender modüllerinin nasıl yapılandırılacağı ve kullanılacağı öğretilir.

En İyi Uygulamalar. BitDefender'dan en iyi şekilde yararlanmak için bu talimatları yerine getiriniz.

BitDefender Kurtarma CD'si. BitDefender Kurtarma CD'si anlatılır. Başlangıç CD'si ile sunulan özellikleri anlamanıza ve kullanmanıza yardım eder.

Yardım Alma. Beklenmeyen herhangi bir şey olduğunda nereye bakmanız gerektiği ve nasıl yardım isteyeceğinizi anlatır.

Sözlük. Sözlük, bu doküman sayfalarında rastlayabileceğiniz bazı teknik ve pek olağan olmayan terimleri açıklamaya çalışmaktadır.

3. Yorumlarınız

Bu kitabı daha da geliştirmek için sizden yorumlarınızı bekliyoruz. Tüm bilgileri yapabileceğimizin en iyisi düzeyinde test ettik ve doğruladık. Bu kitapta bulduğunuz herhangi bir sorunu ve bunun nasıl düzeltilebileceği ile ilgili fikrinizi bize iletmek ve mümkün olan en iyi dokümantasyonu size sunabilmek için lütfen bize yazın.

Yorumlarınızı lütfen <documentation@bitdefender.com> adresine e-posta yoluyla gönderin.

Önemli

Dokümantasyon ile ilgili e-postalarınızı daha etkin ve hızlı olarak değerlendirebilmemiz için lütfen İngilizce dilinde gönderin.

BitDefender Hakkında

1. BitDefender Kimdir?

BitDefender, bugünün bilgi işlem ortamlarının güvenlik gereksinimlerini karşılayan güvenlik çözümlerinin önde gelen global sağlayıcısıdır. Şirket sektörün en hızlı ve çok etkili güvenlik yazılımlarını, tehdit önlemede, zamanında saptama ve azaltmada yeni standartlar koyarak sunmaktadır. BitDefender, 180'den fazla ülkede 41 milyondan fazla ev ve kurumsal kullanıcılara ürünler ve hizmetler sunmaktadır. BitDefender'ın **Amerika Birleşik Devletleri**, **Birleşik Krallık**, **Almanya**, **İspanya** ve **Romanya**'da ofisleri bulunmaktadır.

- Ev ve kurumsal kullanıcılar için antivirüs, güvenlik duvarı, antispam ve ebeveyn kontrolü özellikleri;
- BitDefender ürünleri, kompleks IT yapıları (iş istasyonları, dosya sunucuları, posta sunucuları ve ağ geçitleri), Windows, Linux ve FreeBSD platformları üzerinde uygulanmak üzere amaçlanmıştır;
- Dünya çapında dağıtım, 18 dilde mevcut olan ürünler;
- Kullanıcıları kurulum süreci boyunca yönlendiren ve sadece bazı sorular soran bir kurulum sihirbazı ile kullanım kolaylığı;
- Uluslararası düzeyde sertifikalandırılmış ürünler: Virus Bulletin, ICSA Labs, Checkmark, IST Prize, vs;
- Her saatte müşteri hizmeti – müşteri hizmetleri ekibi haftanın 7 günü 24 saat hizmet vermektedir;
- Yeni bilgisayar saldırılarına hızlı yanıt süresi;
- En iyi tespit oranı;
- Virüs imzalarının saatlik Internet güncellemeleri – en yeni virüslere karşı koruma sağlayan otomatik veya programlı eylemler.

1.1. Neden BitDefender?

Kanıtlanmış. En reaktif antivirüs üreticisi. En son CodeRed, Nimda ve Sircam ve Badtrans.B veya diğer tehlikeli, hızlı yayılan kod saldırıları gibi bilgisayar virüsü saldırılarında, BitDefender hızlı yanıt sisteminin başarısı kanıtlanmıştır. Bu kodlara karşı panzehir bulan ve bunları tüm etkilenen kişilerin kullanımı için ücretsiz olarak Internet'te sunan ilk üretici BitDefender'dır. Şu anda Klez virüsünün sürekli olarak farklı versiyonları artarken, bir bilgisayar sistemi için anında virüs koruma programının ne kadar önemli olduğu bir kez daha ortaya çıkmaktadır.

Yenilikçi. Avrupa Komisyonu ve EuroCase tarafından yenilikçilik ödülü. BitDefender, Avrupa Komisyonu ve Avrupa'daki 18 akademinin temsilcileri tarafından Avrupa Birincilik Ödülü ile ödüllendirilmiştir. Sekizinci yılını kutlayan Avrupa Birincilik Ödülü, bilgi teknolojisinde Avrupa'daki en iyi yenilikleri temsil eden, devrim yaratan ürünlere verilen bir ödüldür.

Kapsamlı. Tam güvenlik sağlayarak, ağınızın her bir noktasını kapsamaktadır. Kurumsal ortamlar içinde BitDefender güvenlik çözümleri, küçük bir yerel alandan geniş çoklu sunuculara ve birden fazla platformlu WAN'lara kadar, bir ağı tehdit eden kompleks tehditleri yönetimini mümkün kılarak bugünün iş dünyasında gerekli olan tüm koruma şartlarını yerine getirmektedir.

Üstün Koruma. Bilgisayar sisteminize gelebilecek tüm muhtemel tehlikelere karşı nihai sınır. Kod analizine dayalı bir virüs tespiti her zaman iyi sonuçlar vermediği için, BitDefender, yeni ortaya çıkan kötü amaçlı yazılımlara karşı koruma sağlayan davranış tabanlı koruma geliştirmiştir.

Aşağıda kurumların kaçınmak istediği **maliyetler** ve güvenlik ürünlerinin neleri önlemek için tasarlandıkları belirtilmektedir.

- Worm saldırıları
- Zarar gören e-postalar nedeniyle iletişim kaybı
- E-postaların durması
- Temizleme ve kurtarma sistemleri
- Sistemin kullanılamaması nedeniyle son kullanıcılar tarafından yaşanan üretkenlik kaybı
- Zarar veren korsanlık ve yetkisiz erişimler

BitDefender güvenlik programı kullanılarak bazı eşzamanlı **gelişmeler ve faydalar** sağlanabilir:

- Kötü amaçlı kod saldırılarının (örn. Nimda, Trojan horses, DDoS) yayılmasını durdurarak ağ kullanımını artırır.
- Uzaktaki kullanıcıları saldırılara karşı korur.
- Yönetsel maliyetleri azaltır ve BitDefender Enterprise yönetim becerileri ile hızlı bir şekilde uygulanır.
- Şirket ağ geçidinde bir BitDefender e-posta koruması kullanarak kötü amaçlı e-postaların yayılmasını önler. Yetkisiz, şüpheli ve masraflı uygulama bağlantılarını geçici veya kalıcı olarak bloklar.

Bitdefender hakkında daha fazla bilgi http://www.bitdefender.com adresi ziyaret edilerek sağlanabilir.

Ürün Kurulumu

2. BitDefender Antivirus v10 Kurulumu

Bu kullanım kılavuzunun **BitDefender Antivirus v10 Kurulumu** bölümü aşağıdaki bölümlerden oluşmaktadır:

- Sistem Gereksinimleri
- Kurulum Adımları
- Başlangıç Kurulum Sihirbazı
- Yükseltme
- BitDefender'ı Kaldırma, Düzeltme veya Değiştirme

2.1. Sistem Gereksinimleri

Ürünün doğru şekilde çalıştığından emin olmak için, kurulumdan önce, aşağıdaki sistem gerekliliklerinin sağlandığını doğrulayın:

Microsoft Windows 98 SE / NT-SP6 / Me / 2000 / XP 32-bit

- Pentium II 350 MHz veya daha yüksek bir işlemci
- Minimum 128 MB RAM Bellek (256 MB tavsiye edilmektedir)
- Minimum 60 MB sabit disk alanı
- Internet Explorer 5.5 veya üzeri

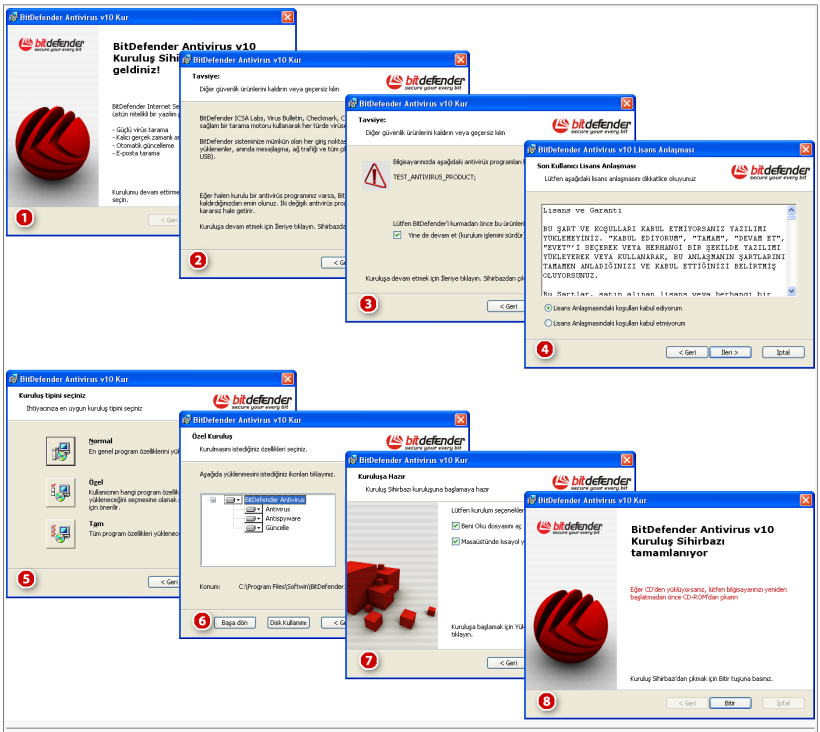
Microsoft Windows Vista 32-bit

- 800 MHz işlemci veya üzeri
- Minimum 512 MB RAM Bellek (1 GB tavsiye edilmektedir)
- Minimum 60 MB sabit disk alanı

BitDefender Antivirus v10'u değerlendirmek amacıyla, veri güvenliği ile ilgili olarak hazırlanan softwin kurumsal web sitesini http://www.bitdefender.com dan ziyaret edebilirsiniz.

2.2. Kurulum Adımları

Kurulum dosyası üzerine çift tıklayın. Bu, sizi kurulum süreci boyunca yönlendirecek olan bir sihirbazı başlatacaktır.



Kurulum Adımları

1. Devam etmek için **İleri**'yi veya kurulumdan çıkmak için **İptal**'i tıklayın.
2. Devam etmek için **İleri**'yi veya ilk adıma dönmek için **Geri**'yi tıklayın.
3. BitDefender Antivirus v10, bilgisayarınızda yüklü olan başka virüs koruma ürünleri olduğunda sizi uyaracaktır.

Uyarı

BitDefender'ı yüklemeden önce, tespit edilen diğer virüs koruma programlarının kaldırılması önemle tavsiye edilmektedir. Bilgisayar üzerinde aynı zamanda iki veya daha fazla virüs koruma ürününün çalıştırılması genellikle sistemi kullanılamaz hale getirmektedir.

Bir önceki adıma dönmek için **Geri**'yi veya kurulumdan çıkmak için **İptal**'i tıklayın. Devam etmek için **İleri**'yi tıklayın.

Not

BitDefender Antivirus v10 sisteminizde başka bir virüs koruma programı tespit etmezse bu adımı atlayacaksınız.

4. Lütfen Lisans Anlaşmasını okuyun, **Lisans Anlaşmasındaki şartları kabul ediyorum**'u seçin ve **İleri**'yi tıklayın. Bu şartları kabul etmiyorsanız **İptal**'i tıklayın. Bu durumda kurulum süreci iptal edilecek ve kurulumdan çıkacaksınız.
5. Ne tür bir yükleme yapmak istediğinizi seçebilirsiniz: tipik, özel veya tam.

   Tipik
   Program en yaygın seçeneklerle yüklenecektir. Bu, çoğu kullanıcı için tavsiye edilen seçenektir.

   Özel
   Yüklemek istediğiniz bileşenleri seçebilirsiniz. Yalnızca ileri kullanıcılar için tavsiye edilmektedir.

   Tam
   Ürünün tam kurulumu için. Tüm BitDefender modülleri yüklenecektir.

   Tipik veya **Tam** seçeneğini seçerseniz 6. adım atlanacaktır.
6. **Özel** seçeneğini seçtiğinizde, yüklemek istediğiniz bileşenleri seçebileceğiniz tüm BitDefender bileşenleri listesini içeren yeni bir pencere açılacaktır.

   Herhangi bir bileşen adına tıkladığınızda sağ tarafta kısa bir açıklama (sabit diskte olması gereken minimum alan dahil) çıkacaktır. Herhangi bir bileşen ikonunu tıkladığınızda, seçilen modülü yüklemeyi veya yüklememeyi seçebileceğiniz yeni bir pencere çıkacaktır.

   Ürünü yüklemek istediğiniz klasörü seçebilirsiniz. Varsayılan klasör:`C:\Program Files\Softwin\BitDefender 10`.

   Başka bir klasör seçmek istiyorsanız, **Gözat**'a tıklayın ve açılan pencerede BitDefender Antivirus v10'u yüklemek istediğiniz klasörü seçin. **İleri**'yi tıklayın.
7. Varsayılan olarak seçili iki seçenek bulunmaktadır:
   - **Beni oku dosyasını aç** – kurulum sonunda beni oku dosyasını açmak için.
   - **Masaüstünde kısayol oluştur** – kurulum sonunda masa üstünüzde BitDefender Antivirus v10 kısayolunu oluşturmak için.
   - **Windows Defenderi kapat** - Windows Defenderi kapatmak için; bu seçenek sadece Windows Vista'da ortaya çıkar.

   Ürünün kurulumunu başlatmak için **Yükle**'yi tıklayın.

Önemli

Kurulum sürecinde bir sihirbaz ortaya çıkacaktır. Sihirbaz **BitDefender Antivirus v10**'unuzu kaydettirmenizde,BitDefender hesabı açmanızda ve önemli güvenlik işlemlerini gerçekleştirmek için BitDefender'ı ayarlamanızda size yardım edecektir. Bir sonraki adıma geçmek için sihirbaz destekli süreci tamamlayın.

8. Ürün kurulumunu tamamlamak için **Bitir**'i tıklayın. Kurulumda varsayılan ayarları kabul ettiyseniz, `Program Files`'ta `Softwin` adında yeni bir klasör yaratılacak ve burada `BitDefender 10` alt klasörü bulunacaktır.

Not

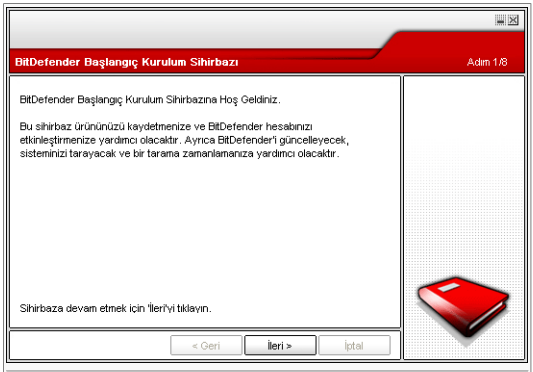
Kurulum sihirbazının kurulum sürecinin tamamlayabilmesi için sistemi yeniden başlatmanız istenebilir.

2.3. Başlangıç Kurulum Sihirbazı

Kurulum sürecinde bir sihirbaz ortaya çıkacaktır. Sihirbaz **BitDefender Antivirus v10**'unuzu kaydettirmenizde, bir BitDefender hesabı açmanızda ve önemli güvenlik işlemlerini gerçekleştirmek için BitDefender'ı ayarlamanızda size yardım edecektir.

Bu sihirbaz işlemini tamamlamak zorunlu değildir; ancak, zaman kazanmak ve BitDefender Internet Security v10 kurulmadan önce sistemin güvenli olduğundan emin olmak için yapılmasını tavsiye ediyoruz.

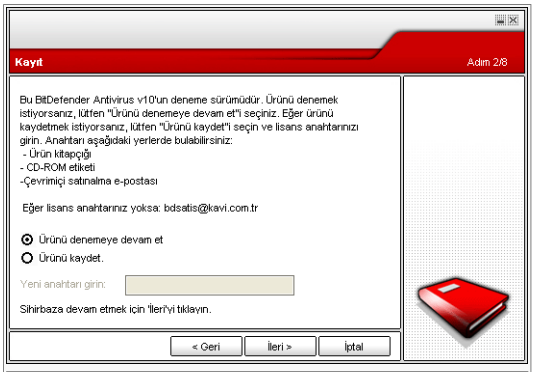
2.3.1. Adım 1/8 – BitDefender Başlangıç Kurulum Sihirbazı



Hoşgeldiniz Ekranı

İleri'yi tıklayın.

2.3.2. Adım 2/8- BitDefender Antivirus v10'u Kaydedin



Kayıt

BitDefender Antivirus v10'u kaydetmek için **Ürünü kaydet** seçeneğini seçin. **Yeni anahtarı gir** alanına lisans anahtarını yazın.

Ürünü denemeye devam etmek için **Ürünü denemeye devam et**'i seçin.

İleri'yi tıklayın.

2.3.3. Adım 3/8 – BitDefender Hesabı Yarat

Hesap Yaratma

BitDefender hesabım yok

BitDefender'ın teknik destek ve diğer ücretsiz hizmetlerinden yararlanabilmek için bir hesap açtırmanız gerekmektedir.

E-posta alanına geçerli bir e-posta adresi yazın. Bir şifre belirleyip **Şifre** alanına yazın. **Şifreyi yeniden gir** alanına şifrenizi yeniden girin. http://myaccount.bitdefender.com'da hesabınıza giriş yapmak için e-posta adresinizi ve şifrenizi kullanın.

Not

Şifre en az dört karakter uzunluğunda olmalıdır.

Hesabınızın açılmasını gerçekleştirmek için önce e-posta adresinizi aktif hale getirmeniz gerekmektedir. e-posta adresinizi kontrol edin ve BitDefender kayıt hizmetleri tarafından size gönderilen e-postadaki talimatları uygulayın.

Önemli

Bir sonraki adıma geçmeden önce hesabınızı aktif hale getirin.

Bir BitDefender hesabı açtırmak istemiyorsanız, sadece **Bu adımı geç** seçeneğini tıklayın. Sihirbazın bir sonraki adımını da atlayacaksınız.

Devam etmek için **İleri** veya sihirbazdan çıkmak için **İptal** seçeneğine tıklayın.

BitDefender hesabım var

Zaten bir BitDefender hesabınız varsa, e-posta adresinizi ve hesap şifrenizi girin. Yanlış bir şifre girerseniz, **İleri** tıkladığınızda şifreyi yeniden yazmanız istenecektir. Yeniden şifre girmek için **Tamam** veya sihirbazdan çıkmak için **İptal** seçeneğine tıklayın.

Şifrenizi unuttuysanız, **Şifremi unuttum**'u tıklayın ve talimatları uygulayın.

Devam etmek için **İleri** veya sihirbazdan çıkmak için **İptal** seçeneğine tıklayın.

2.3.4. Adım 4/8 – Hesap Detaylarının Girilmesi

Hesap Detayları

Not

Üçüncü adım daki **Bu adımı geç** seçeneğini işaretlediyseniz bu adım atlanacaktır.

Adınızı ve soyadınızı yazın ve yaşadığınız ülkeyi seçin.

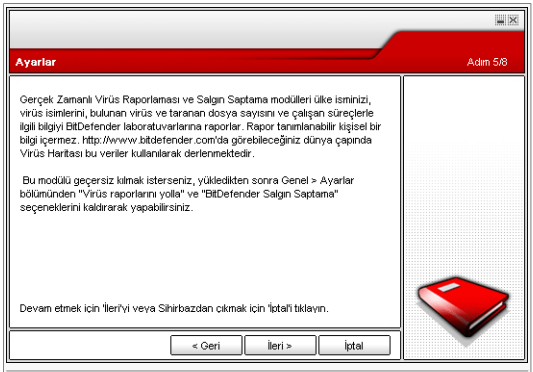
Zaten bir hesabınız varsa, sihirbaz daha önce belirttiğiniz bilgileri gösterecektir (varsa). İsterseniz bu bilgileri değiştirebilirsiniz.

Önemli

Burada belirttiğiniz bilgiler gizli kalacaktır.

Devam etmek için **İleri** veya sihirbazdan çıkmak için **İptal** seçeneğine tıklayın.

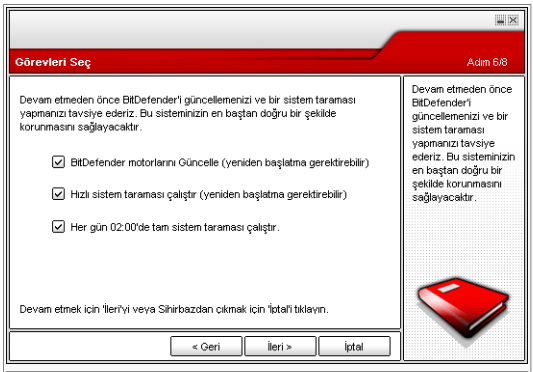
2.3.5. Adım 5/8 – RTVR Hakkında Bilgi



RTVR Bilgisi

Devam etmek için **İleri** veya sihirbazdan çıkmak için **İptal** seçeneğine tıklayın.

2.3.6. Adım 6/8 – Çalıştırılacak Görevlerin Seçilmesi



Görev Seçimi

Sisteminizin güvenliği için gerekli olan önemli görevleri gerçekleştirmek üzere BitDefender Antivirus v10'u ayarlayın.

Aşağıdaki seçenekler mevcuttur:

- **BitDefender Antivirus v10 motorlarını (yeniden başlatma gerekebilir) güncelle** -Bir sonraki adımda, en son tehditlere karşı bilgisayarınızı korumak için BitDefender Antivirus v10 motorlarının güncellenmesi
- **Hızlı bir sistem tarama gerçekleştirin (yeniden başlatma gerekebilir)** – bir sonraki adımda, BitDefender Antivirus v10'nun `Windows` ve `Program Files` klasörlerinin etkilenmemesini sağlaması için hızlı bir sistem taraması yapılacaktır.
- **Hergün saat 02:00'de tam sistem taraması gerçekleştir** - hergün saat 02:00'de tam bir sistem taraması gerçekleştirir.

Önemli

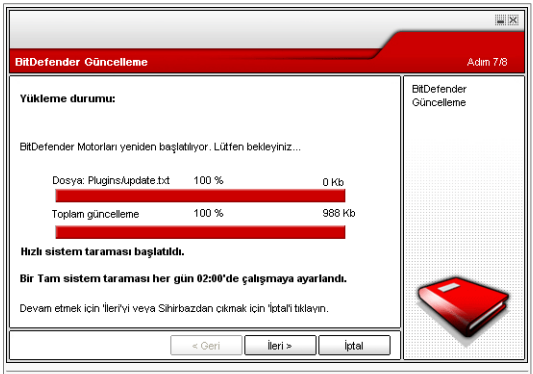
Sistemin güvenliğini sağlamanız için bir sonraki adıma geçmeden önce bu seçenekleri etkin kılmanızı tavsiye ediyoruz.

Sadece son seçeneği seçtiyseniz yada hiç birini seçmediyseniz, bir sonraki adım atlanacaktır.

Bir sonraki adıma dönerek istediğiniz herhangi bir değişikliği yapabilirsiniz (**Geri**'yi tıklayın). Daha sonraki süreç geri dönme imkanı yoktur: Devamı seçerseniz önceki adımlara geri dönemeyeceksiniz.

Devam etmek için **İleri** veya sihirbazdan çıkmak için **İptal** seçeneğine tıklayın.

2.3.7. Adım 7/8 – Görevlerin Tamamlanmasını Bekleyin

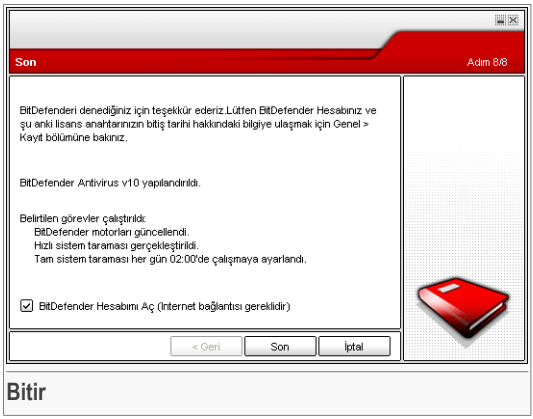


Görev Durumu

Görev(ler)in tamamlanmasını bekleyin. Önceki adımda seçilen görev(ler)in durumunu görebilirsiniz.

Devam etmek için **İleri** veya sihirbazdan çıkmak için **İptal** seçeneğine tıklayın.

2.3.8. Adım 8/8 – Özeti Görüntüle



Bitir

Bu, yapılandırma sihirbazının en son adımıdır.

BitDefender hesabınıza giriş yapmak için **BitDefender Hesabımı Aç** seçeneğini seçin. Internet bağlantısı gereklidir.

Sihirbazı tamamlamak için **Bitir**'i tıklayarak kurulum sürecine devam edin.

2.4. Yükseltme

Yükseltme işlemi aşağıdaki şekillerde yapılabilir:

- **Önceki sürümü kaldırmadan yüklemek - v8 veya üzeri için, Internet Security hariç**

  Kurulus dosyasına çift tıklayın ve sihirbazı "*Kurulum Adımları*" (shf. 7) bölümündeki gibi takip edin.

  Önemli

  Kurulum işlemi sırasında `Filespy servisi` tarafından oluşan bir hata görünecektir. **Tamam**'a tıklayarak kuruluma devam edin.

- **Önceki sürümü kaldırın ve yeni sürümü yükleyin – tüm BitDefender sürümleri için**

Önce eski sürümü kaldırmanız gerekmektedir, daha sonra, bilgisayarı yeniden başlatın ve yeni sürümü "*Kurulum Adımları*" (shf. 7) bölümünde anlatıldığı şekilde yükleyin.

Önemli

BitDefender v8 veya daha üst bir yazılımdan yükseltme yapıyorsanız, BitDefender ayarları'nı kaydetmenizi tavsiye ediyoruz. Yükseltme işlemi tamamlandıktan sonra, bunları yükleyebilirsiniz.

2.5. BitDefender Özelliklerini Kaldırma, Düzeltme veya Değiştirme

BitDefender Antivirus v10'u kaldırmak, yenilemek, düzenlemek isterseniz aşağıdaki adımları takip ediniz. **Başlat → Programlar → BitDefender 10 → Değiştir, Düzelt veya Kaldır**.

İleri seçeneğine tıklayarak seçiminizi onaylamanız istenecektir. Seçim yapabileceğiniz yeni bir pencere açılacaktır

- **Modify** - eklemek için yeni program bileşenlerini seçmek ve kaldırmak için yüklü olan bileşenleri seçmek için.

  Not

  Kuruluş dosyasına çift tıklayın ve sihirbazı "*Kurulum Adımları*" (shf. 7) bölümündeki gibi takip edin.

- **Onar** - yüklenmiş olan tüm program bileşenlerini yeniden yüklemek için

  Önemli

  Ürünü yeniden yüklemeden önce BitDefender Ayarlarını kaydetmenizi öneririz.Yeniden yükleme süreci sona erdiğinde bunları yeniden yükleyebilirsiniz.

- **Kaldır**- tüm yüklü bileşenleri kaldırmak için

  Eğer BitDefender'i kaldırmayı seçerseniz, artık virüslere,spywarelere ve hackerlara karşı korunmayacaksınız.Eğer BitDefender'i kaldırdıktan sonra Windows Güvenlik Duvarı ve Windows Defenderi etkinleştirmek isterseniz bir sonraki adımdaki uygun check box'ları seçiniz.

  BitDefender'i kaldırma sebeplerinizi bize bildirmeniz bizi çok memnun edecektir. **Geribildirim Gönder** seçeneğini işaretleyiniz ve önerilerinizi içeren online formu bize gönderiniz.

Kuruluma devam etmek için aşağıda verilen üç seçenekten birini seçin. Düzgün bir yeniden yükleme için **Kaldır** seçeneğini seçmenizi tavsiye ediyoruz. Eski sürümün kaldırılması işlemi tamamlandıktan sonra,`Softwin`klasörünü `Program Dosyaları`'ndan silmenizi tavsiye ediyoruz.

Tanım ve Özellikler

3. BitDefender Antivirus v10

Kişisel bilgisayarınız için antivirüs ve antispyware yazılım çözümü!

BitDefender Antivirus v10 güvenlik gereksinimlerinizi en iyi şekilde karşılayacak özellikleriyle etkili bir antivirüs ve antispyware aracıdır.

3.1. Antivirus

Virüs koruma modülünün amacı, tüm virüslerin tespit edilmesini ve yokedilmesini sağlamaktır. BitDefender Virüs Koruma programı, ICSA laboratuarları, Virüs Bulletin, Checkmark, CheckVir ve TUV tarafından onaylanan güçlü tarama motorlarını kullanmaktadır.

Proaktif Tespit. B-HAVE (Sanal Ortamlarda Davranışsal, Sezgisel Analiz), potansiyel kötü amaçlı hareketlerin kontrol edilebilmesi için yazılım parçalarının çalıştırıldığı sanal bir bilgisayar-içinde-bilgisayar gibi hareket etmektedir. BitDefender'ın tescilli teknolojisi, kod kimlikleri henüz yayınlanmamış olan kötü amaçlı kodları tespit ederek işletme sistemini bilinmeyen virüslere karşı korumaktadır.

Sürekli Virüs Koruma Programı. Yeni ve geliştirilmiş BitDefender tarama motorları erişimdeki virüs bulaşmış dosyaları tarayıp etkisiz hale getirerek veri kaybını minimuma indirecektir. Virüs bulaşmış dosyalar silinmek yerine artık kurtarılabilmektedir.

Rootkit Tespit ve Temizleme. Yeni bir BitDefender modülü rootkit'leri (arka planda gizlenerek bilgisayarları kontrol etmek için tasarlanmış kötü amaçlı programlar) bularak temizlemektedir.

Web tarama. Web trafiği, henüz tarayıcınıza ulaşmadan gerçek zamanlı olarak filtrelenerek güvenli ve keyifli bir web deneyimi yaşamanız sağlanmaktadır.

Eşler Arası ve IM Uygulamaları Koruması. Anlık mesaj gönderme ve dosya paylaşan yazılım uygulamaları ile yayılan virüslere karşı filtreler.

Tam E-posta Koruması. BitDefender, POPS/SMTP protokol seviyelerinde çalışarak, kullanılan e-posta istemcisi ne olursa olsun (Outlook™, Outlook Express™, The Bat!™, Netscape®, vs.), ek bir yapılandırmaya gerek duymadan, gelen ve giden e-postaları filtrelemektedir.

3.2. Antispyware

BitDefender, gerçek zamanlı olarak potansiyel spyware'ler sisteminize zarar vermeden önce bunları denetler ve önler. Kapsamlı bir spyware imzaları veritabanını kullanarak, bilgisayarınızı spyware'lere karşı korur.

Gerçek Zamanlı Antispyware. BitDefender, sisteminizde spyware'lerin saldırabileceği pek çok potansiyel "sıcak noktaları" denetler ve sisteminize ve yazılımınıza yapılan herhangi bir değişikliği kontrol eder. Bilinen spyware saldırıları da eş zamanlı olarak engellenir.

Spyware Tarama ve Temizleme. BitDefender bilinen spyware tehditleri için tüm sisteminizi veya bir kısmını tarar. Taramada sürekli güncellenen spyware imza veritabanı kullanılır.

Kişisel Gizlilik Koruması. Kişisel gizlilik koruyucusu, bilgisayardan HTTP (web) ve SMTP (posta) trafiğine akan kredi kartı numaraları, sosyal güvenlik numaraları ve diğer kullanıcı tanımlı bilgileri (örn. Şifre bitleri) gibi kişisel olabilecek bilgilerin denetimini yapar.

Çevirmeli Ağ Kontrolü. Yapılandırılabilir bir çevirmeli ağ kontrolü, kötü amaçlı uygulamaların sizin adınıza yüksek telefon ücretleri meydana getirmesini engeller.

Çerez Kontrolü. Antispyware siz internetde dolaşırken gelen ve giden çerez tipi dosyaları kimliğinizi ve gizliliğinizi korumak için filitreler.

Etkin İçerik Kontrolü. ActiveX, Java Appletler veya Java Script tipli kodlar gibi potansiyel kötü niyetli uygulamaları bloklar

3.3. Diğer Özellikler

Açma ve Kullanma. Kurulumdan hemen sonra bir ayar sihirbazı çıkarak, kullanıcıların en uygun ve güncel ayarları seçmesine yardım etmekte, bir tarama modülü uygulamakta ve ürünün kaydı ve aktivasyonu için hızlı bir yol sunulmaktadır.

Kullanıcı Deneyimi. BitDefender, kullanım kolaylığına önem vererek ve karmaşık yapılardan kaçınarak kullanıcı deneyimini yeniden tasarlamıştır. Sonuç olarak, çoğu BitDefender v10 modülü, otomasyon ve makine öğrenimini rahat bir şekilde kullanılmasını sağlayarak, çok daha az kullanıcı etkileşimi gerektirmektedir.

Saatlik Güncellemeler. BitDefender'ınız, doğrudan veya bir Vekil (Proxy) Sunucu aracılığıyla Internet üzerinde 24 saat boyunca güncellenecektir. Ürün, gerekirse, BitDefender sunucularından hasar görmüş veya kayıp dosyaları yükleyerek kendi kendini onarma yeteneğine sahiptir

7 Gün 24 Saat Destek. Nitelikli destek temsilcileri tarafından çevrimiçi olarak veya Sık Sorulan Sorulara cevapları içeren çevrimiçi bir veritabanına erişim yoluyla sunulmaktadır.

Kurtarma Diski. BitDefender Antivirus v10 bir başlangıç CD'si ile birlikte teslim edilmektedir. Bu CD, başlatılamayan tehlikedeki bir sistemi analiz etmek/onarmak/temizlemek için kullanılabilir.

4. BitDefender Modülleri

BitDefender Antivirus v10 bu modülleri içerir: **Genel**, **Antivirus**, **Antispyware** and **Güncelleme**.

4.1. Genel Modülü

BitDefender maksimum güvenlik için tamamen yapılandırılmış şekilde sunulmaktadır

Genel modülünde, güvenlik seviyesini yapılandırabilir ve önemli güvenlik işlemlerini gerçekleştirebilirsiniz. Ayrıca ürününüzü kaydettirebilir ve BitDefender'ın genel davranışı ayarlayabilirsiniz.

4.2. Virüs Koruma Modülü

BitDefender; dosyalarınızı, e-postalarınızı, yüklenen programları ve diğer içerikleri tarayarak, sisteminize giren virüslere, spyware ve diğer kötü amaçlı yazılımlara karşı sizi korur

BitDefender'ın sunduğu koruma iki kategoriye ayrılmaktadır:

- Erişim anında tarama yeni virüs, spyware ve diğer kötü amaçlı yazılımların sisteminize girmesini engeller. Aynı zamanda gerçek zamanlı koruma olarak da adlandırılır – kullanıcı, dosyalara eriştikçe dosyalar taranır. BitDefender, örneğin, bir word dosyasını açtığınızda bilinen tehditlere karşı bu dosyayı tarar veya bir e-posta aldığınızda e-posta mesajını tarar.BitDefender eriştiğiniz "dosyaları siz kullandıkça" tarar.
- Isteğe bağlı tarama sisteminizde mevcut olan virüs, spyware ve diğer kötü amaçlı yazılımları tesbit eder. Bu, kullanıcı tarafından başlatılan klasik bir taramadır – BitDefender'ın hangi sürücü, klasör veya dosyayı taraması gerektiğini seçersiniz ve BitDefender bunları talebiniz üzerine tarar.

4.3. Antispyware Modülü

BitDefender, sisteminizde spyware'lerin saldırabileceği pek çok potansiyel "sıcak noktaları" denetler ve sisteminize ve yazılımınıza yapılan herhangi bir değişikliği kontrol eder. Gizli bilgilerinizi ele geçirmeye çalışan ve kredi kartı bilgileri gibi kişisel bilgileri bilgisayarınızdan korsana göndermeye çalışan korsanlar tarafından yüklenen Trojan Horses (Truva Atı) ve diğer araçların engellenmesinde etkin bir modüldür

4.4. Güncelleme Modülü

Hergün yeni bir kötü amaçlı yazılım bulunmakta ve tanımlanmaktadır. Bu nedenle, BitDefender'ın en yeni kötü amaçlı yazılım imzaları ile güncel kılınması çok önemlidir. Fabrika ayarlarında, BitDefender her saatte güncellemeleri kontrol etmek üzere ayarlanmıştır.

Güncellemeler aşağıdaki şekillerde olmaktadır:

- **Virüs koruma motorları için güncellemeler** – yeni bir tehdit ortaya çıktıkça, bunlara karşı sürekli olarak güncel bir koruma sağlamak amacıyla, virüs imzaları taşıyan dosyaların güncelleştirilmesi gerekmektedir. Bu güncelleme tipi aynı zamanda **Virüs Tanımları Güncellemesi** olarak da bilinmektedir
- **Antispyware motorları güncellemesi** - yeni spyware imzalaları veritabanına eklenecektir. Bu güncelleme tipi aynı zamanda **Antispyware Güncellemesi** olarak da bilinmektedir.
- **Ürün yükseltmeleri** - yeni bir ürün sürümü çıkarıldığında, ürün performansını geliştiren yeni özellikler ve tarama teknikleri tanıtılmaktadır.Bu güncelleme tipi aynı zamanda **Ürün Güncellemesi** olarak da bilinmektedir

Kullanıcının dahil olması açısından aşağıdaki güncellemeleri dikkate alabiliriz.

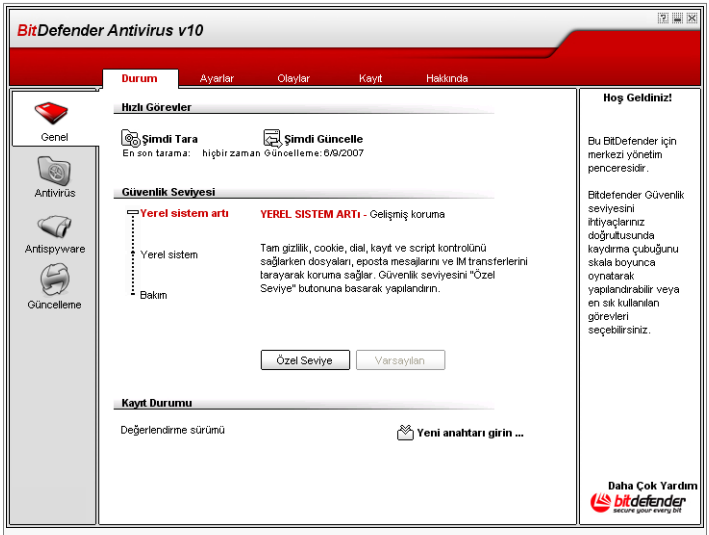
- Otomaik güncelleme - BitDefender herhangi bir güncellemenin yapılıp yapılmadığını kontrol etmek için otomatik olarak güncelleme sunucusu ile iletişim kurar. Eğer yapılmışsa, BitDefender otomatik olarak güncellenir.Güncelleme modulünden **Şimdi güncelle** seçeneğine tıklanarak, istediğiniz herhangi bir zamanda da gerçekleştirilebilir.
- Manual güncelleme - manuel olarak en son tehdit imzalarını indirmeniz ve yüklemeniz gerekmektedir.

Yönetim Konsolu

5. Tanıtma

BitDefender Antivirus v10, tüm BitDefender modüllerinin koruma seçeneklerinin yapılandırılmasını sağlayan merkezi bir yönetim konsolu ile tasarlanmıştır. Başka bir deyişle, tüm modüllere erişmek için tek yapmanız gereken yönetim konsolunu açmaktır.**Antivirus**, **Antispyware** and **Güncelleme**.

Yönetim konsoluna ulaşmak için Windows Başlat menüsünü kullanarak sırasıyla **Başlat → Programlar → BitDefender 10 → BitDefender Antivirus v10**'u seçin veya sistem tepsisinden **BitDefender ikonuna** çift tıklayarak daha çabuk bir şekilde erişin.



Yönetim Konsolu

Yönetim konsolunun sol tarafında modül seçicisini göreceksiniz:

- Genel • Genel - bu bölümde güvenlik seviyesini yapılandırabilir ve önemli güvenlik işlemlerini gerçekleştirebilirsiniz. Burada ayrıca ürünü kaydettirebilir ve tüm BitDefender ana ayarlarının özetini, ürün detaylarını ve iletişim bilgilerini görebilirsiniz.
- Virüs koruma – bu bölümde **Virüs Koruma**modülünü yapılandırabilirsiniz.
- Antispyware -bu bölümde **Antispyware** modülünü yapılandırabilirsiniz

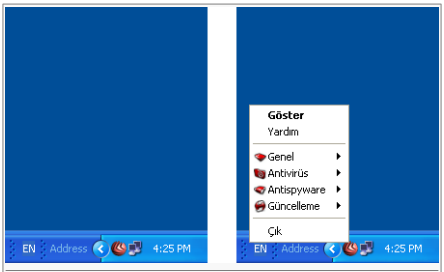
- Güncelleme – bu bölümde **Güncelleme**modülünü yapılandırabilirsiniz.

Yönetim konsolunun sağ tarafında, içinde bulunduğunuz bölümle ilgili bilgileri göreceksiniz. Sağ alt kısımdaki **Daha Çok Yardım** seçeneği **Yardım** dosyasını açar.

5.1. Sistem Tepsisi

Konsol küçültüldüğünde sistem tepsisinde bir ikon görülecektir:

Bu ikona çift tıkladığınızda, yönetim konsolu açılacaktır. Ayrıca sağ tıkladığınızda bağlamsal bir menü görülecektir. Bu, BitDefender'ın hızlı yönetimini sağlamaktadır.



Sistem Tepsisindeki Bitdefender İkonu

- **Göster / Kapat**– yönetim konsolunu açar veya küçülterek sistem tepsisine taşır.
- **Yardım** - yardım dosyasını açar.
- **Genel** - Genel modülünün yönetimi.
  - **Yeni anahtar gir** – ürünün kaydettirilmesi sürecinde sizi yönlendirecek olan sihirbazı başlatır.
  - **Hesabı Düzenle** – bir BitDefender hesabı açmanıza yardım edecek olan bir sihirbazı başlatır.
- **Virüs Koruma** - Virüs Koruma modülünün yönetimi.
  - **Gerçek zamanlı koruma etkin/etkin değil** gerçek zamanlı korumanın durumunu (etkin/etkin değil) gösterir. Gerçek zamanlı korumayı etkin kılıp kılmamak için bu seçeneğe tıklayın.
  - **Tarama** – tarama bölümünde bulunan Tarama görevlerinden birini çalıştırmak için seçebileceğiniz bir alt menüyü açar
- **Antispyware** - Antispyware modülünün yönetimi.
  - **Davranışsal Antispyware etkin/etkin değil**- shows the status of the davranışsal antispyware korumasının durumunu (etkin/etkin değil) gösterir. Davranışsal Antispyware korumasını etkin kılıp kılmamak için bu seçeneğe tıklayın.
  - **Gelişmiş ayarkar** – antispyware kontrollerini yapılandırmanızı sağlar
- **Güncelleme** - Güncelleme modülünün yönetimi.
  - **Şimdi güncelle** – anında güncelleme gerçekleştirir.
  - **Otomatik güncelleme etkin/etkin değil**otmatik güncellemenindurumunu (etkin/etkin değil) gösterir. Otomatik güncellemeyi etkin veya etkisiz kılmak için bu seçeneğe tıklayın.

- **Çıkış** - uygulamayı kapatır. Bu seçenek seçildiğinde, sistem tepsisindeki ikon kaybolur ve yönetim konsoluna ulaşmak için konsolu tekrar Windows Başlat menüsünden başlatmanız gerekecektir.

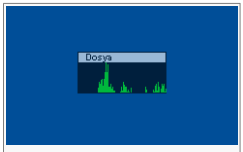
Not

Bir veya daha fazla BitDefender modülünü etkisiz kıldığınızda ikon siyah olacaktır. Buşekilde yönetim konsolunu açmadan bazı modüllerin çalışmadığını bilebileceksiniz. Bir güncelleme mümkün olduğunda ikon yanıp sönecektir.

5.2. Tarama Etkinlik Çubuğu

The **Tarama etkinlik çubuğu**, sisteminizdeki tarama etkinliğinin grafiksel olarak gösterimidir

Yeşil çubuklar (**Dosya Bölgesi**) 0 ila 50 aralığında, saniyede taranan dosya sayısını gösterir



Etkinlik Çubuğu

Not

Virüs Kalkanını etkisiz kıldığınızda **Tarama Etkinlik Çubuğu** ilgili alan (**Dosya Alanı**) üzerine kırmızı bir çarpı koyarak sizi bilgilendirir. Bu şekilde, yönetim konsolunu açmadan bazı modüllerin çalışmadığını bilebileceksiniz.

Grafik gösterimini daha fazla görmek istemiyorsanız, sadece sağ tıklayarak **Gizle** seçeneğini seçin.

Not

Bu pencereyi tamamen gizlemek için, **Tarama Etkinlik çubuğunu (ürün etkinliği ekran grafiği üzerinde) etkin kıl**seçeneğini tıklayın**Genel** modülünde, Ayarlar bölümü).

6. Genel Modülü

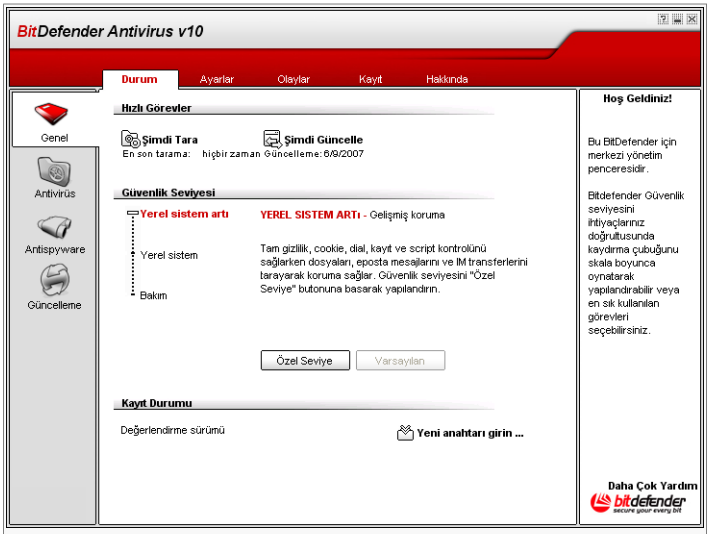
Bu kullanım kılavuzunun **Genel Modül Bölümü** aşağıdaki başlıklardan oluşmaktadır:

- Merkezi Yönetim
- Yönetim Konsolu Ayarları
- Olaylar
- Ürün Kaydı
- Hakkında

Not

Genel modülü ile ilgili daha fazla bilgi için "*Genel Modülü*" (shf. 25) bölümüne bakınız.

6.1. Merkezi Yönetim



Merkezi Yönetim

Bu bölümde genel güvenlik seviyesini yapılandırabilir ve önemli BitDefender işlemlerini gerçekleştirebilirsiniz. Ayrıca ürünü kaydettirebilir ve sona erme tarihini görebilirsiniz.

6.1.1. Hızlı Görevler

BitDefender önemli güvenlik görevlerine hızlı bir şekilde erişmenizi sağlamaktadır. Bu görevleri kullanarak, BitDefender'ı güncel tutabilir, sistemi tarayabilir veya trafiği engelleyebilirsiniz.

Tüm sistemi taramak için sadece To scan the entire system just click **Şimdi Tara**'yı tıklayın.Tarama penceresi görünecek ve tam sistem taraması başlatılacaktır

Önemli

En az haftada bir kez tam sistem taraması yapmanızı tavsiye ediyoruz. Tarama görevleri ve tarama süreci ile ilgili daha fazla bilgi için kullanım kılavuzunun Talep üzerine tarama bölümüne başvurunuz.

Sisteminizi taramadan önce, en son tehditlerin tespit edilebilmesi için BitDefender'ı güncellemenizi tavsiye ediyoruz. BitDefender'ı güncellemek için **Şimdi Güncelle**'ye tıklayın. Güncelleme işleminin tamamlanması için birkaç saniye bekleyin veya en iyisi, güncelleme durumunu görmek için Güncelleme bölümünü kontrol edin.

Not

Güncelleme süreci ile ilgili daha fazla bilgi için kullanım kılavuzunun Otomaik Güncellemebölümüne başvurunuz.

6.1.2. Güvenlik Seviyesi

Koruma ihtiyaçlarınıza en uygun güvenlik seviyesini seçebilirsiniz. Uygun güvenlik seviyesini belirlemek için kaydırma çubuğunu ölçek üzerinde kaydırın.

3 güvenlik seviyesi bulunmaktadır:

Güvenlik Seviyesi	Açıklama
Koruma	Hiçbir koruma önermez. Sadece **Otomatik Güncelleme** etkindir. Sadece BitDefender'i günceller. Hiçbir koruma sağlamamasına rağmen bu güvenlik seviyesi sistem yöneticileri için kullanışlı olabilir.
Yerel Sistem	Standart bir koruma sunmaktadır.Özellikle ağı olmayan veya Internet erişimi olmayan bilgisayarlar için tercih edilir. Kaynak tüketim seviyesi düşüktür. Erişilen dosyalar virüsler ve spyware'lere karşı taranır.

Güvenlik Seviyesi	Açıklama
Yerel Sistem Artı	Antivirus&antispyware korumaları sunar.Internet veya ağ erişimi olmayan bilgisayarlar için özellikle önerilir.Kaynak tüketim seviyesi düşüktür Erişilen dosyalar virüsler ve spywareler için taranır.

BitDefender Antivirus v10 Internet veya ağ erişimi olmayan bilgisayarlar için önerir.

Güvenlik seviyesini **Özel Serviye**'ye tıklayarak özelleştirebilirsiniz.Görünecek olan pencerede etkin hale getirmek istediğiniz koruma seçeneğini seçiniz ve **Tamam** tuşuna basınız.

Varsayılan seviyede olan çubuğu ayarlamak için **Varsayılan Seviye**'yi tıklayın.

6.1.3. Kayıt Durumu

BitDefender lisansınızın durumu hakkındaki bilgileri görebilirsiniz. Burada ürünü kaydettirebilir ve ürünün sona erme tarihini görebilirsiniz.

Yeni bir anahtar girmek için **Yeni Anahtar Gir**'i tıklayın.BitDefender'ı başarılı bir şekilde kaydettirmek için kayıt sihirbazını tamamlayın.

Not

Kayıt süreci ile ilgili daha fazla bilgi için kullanım kılavuzunun Ürün Kaydı bölümüne başvurunuz

6.2. Yönetim Konsolu Ayarları

Yönetim Konsolu Ayarları

Burada, genel BitDefender davranışlarını ayarlayabilirsiniz. Fabrika ayarları olarak, BitDefender Windows başlangıcında yüklenir ve daha sonra görev çubuğunda küçültülmüş olarak çalışır.

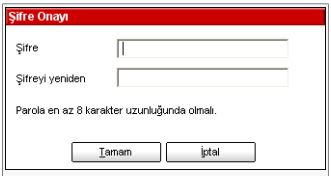
6.2.1. Genel Ayarlar

- **Ürün ayarları için parola korumasını etkin kıl** - BitDefender Yönetim Konsolu konfigürasyonunu korumak için bir parola belirlenmesine imkan verir

Not

Bu bilgisayarı kullanan, yönetim hakları olan tek kişi değilseniz, BitDefender ayarlarınızı bir şifre ile korumanızı tavsiye ediyoruz.

Bu opsiyonu seçtiğinizde, bir sonraki pencere açılacaktır:



Şifre Giriniz

Şifre alanına şifrenizi yazın ve **Şifreyi yeniden yazın** alanında şifrenizi tekrar yazarak **OK**'ı tıklayın.

Bundan sonra, BitDefender konfigürasyon seçeneklerini değiştirmek istediğinizde şifre girmeniz istenecektir.

Önemli

Şifreyi unuttuğunuzda, BitDefender konfigürasyonunu değiştirmek için ürünü onarmanız gerekecektir.

- **BitDefender Haberlerini Göster (güvenlikle ilgili bildirimler)** - zaman zaman virüs saldırıları ile ilgili BitDefender sunucusu tarafından gönderilen güvenlik bildirimlerini gösterir.
- **Açılır Pencereleri Göster (ekran üzerindeki notlar)** - shows pop-up windows regarding the product status.
- **BitDefender'ı Windows başlangıcında yükle**– BitDefender'ı otomatik olarak sistem başlangıcında başlatır.

Not

Bu opsiyonu seçili bırakmanızı tavsiye ediyoruz

- **Tarama Etkinlik Çubuğunu Etkin Kıl (ürün etkinliği ekran grafiğinde)** - Tarama Etkinlik Çubuğunu etkin/etkisiz kılar
- **Konsolu başlangıçta küçültür** –BitDefender yönetim konsolunu, sistem başlangıcında yüklendikten sonra küçültür. Yalnızca BitDefender Ikonu sistem tepsisinde gözükür.

6.2.2. Virüs Raporu Ayarları

- **Virüs raporları gönder**BitDefender Laboratuarlarına, bilgisayarınızda belirlenen virüsler ile ilgili raporlar gönderir. Bu bizim, virüs saldırılarının kaydını tutmamıza yardım eder.

Raporlarda, adınız, IP adresiniz veya diğer gizli bilgiler bulunmayacak ve ticari amaçlar için kullanılmayacaklardır. Verilen bilgilerde sadece virüs adı olacak ve sadece istatistiki raporlar oluşturmak için kullanılacaklardır

- **BitDefender Saldırı Tespitini Etkin Kıl** BitDefender Laboratuarlarına, potansiyel virüs saldırıları ile ilgili raporlar gönderir.

  Raporlarda, adınız, IP adresiniz veya diğer gizli bilgiler bulunmayacak ve ticari amaçlar için kullanılmayacaklardır. Verilen bilgilerde sadece potansiyel virüs adı olacak ve sadece yeni virüsleri tespit etmek için kullanılacaklardır

6.2.3. Kabuk Ayarları

Yönetim konsolunun rengini seçmenizi sağlar. Kabuk, arayüzdeki arka plan görüntüsünü temsil eder. Farklı bir kabuk seçmek için ilgili renge tıklayın.

6.2.4. Ayarların Yönetimi

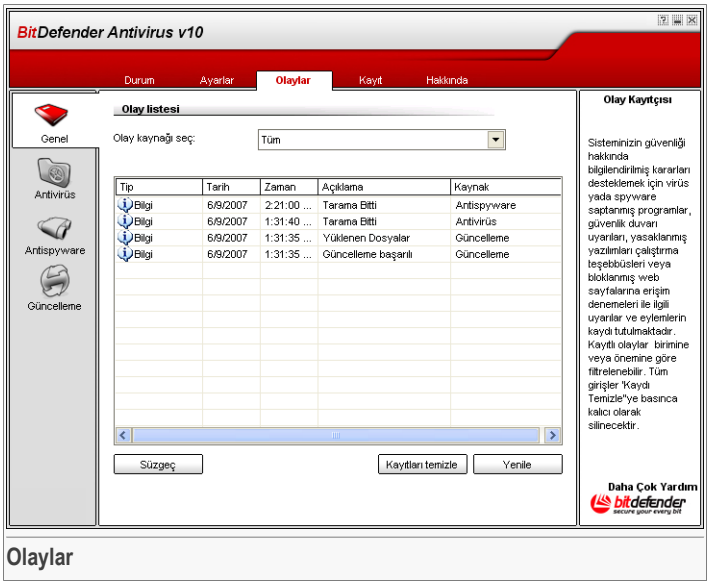
BitDefender için yapmış olduğunuz ayarları, istediğiniz bir yere kaydetmek/yüklemek için **Tüm ayarları kaydet** / **Tüm ayarları yükle** butonlarını kullanın. Bu şekilde, BitDefender ürününü yeniden kurduktan veya onardıktan sonra aynı ayarları kullanabilirsiniz.

Önemli

Sadece yönetim hakları olan kullanıcılar ayarları kaydedebilir ve yükleyebilir

Varsayılan ayarları yüklemek için **Varsayılan Ayarları Geri Yükle** tuşuna basınız

6.3. Olaylar



Olaylar

Bu bölümde, BitDefender tarafından üretilen tüm olaylar gösterilmektedir.

3 olay tipi bulunmaktadır: **Bilgi**, **Uyarı** ve **Kritik**.

Olay örnekleri:

- **Bilgi** - bir e-posta tarandığında
- **Uyarı**– şüpheli bir dosya tespit edildiğinde;
- **Kritik**– virüs bulaşmış bir dosya tespit edildiğinde

Her bir olay için aşağıdaki bilgiler sunulur: Olayın meydana geldiği tarih ve zaman, kısa bir açıklama ve kaynağı (**Virüs Koruma**, **Güvenlik Duvarı**, **Antispyware** veya **Güncelleme**) Özelliklerini görmek için olaya çift tıklayın.

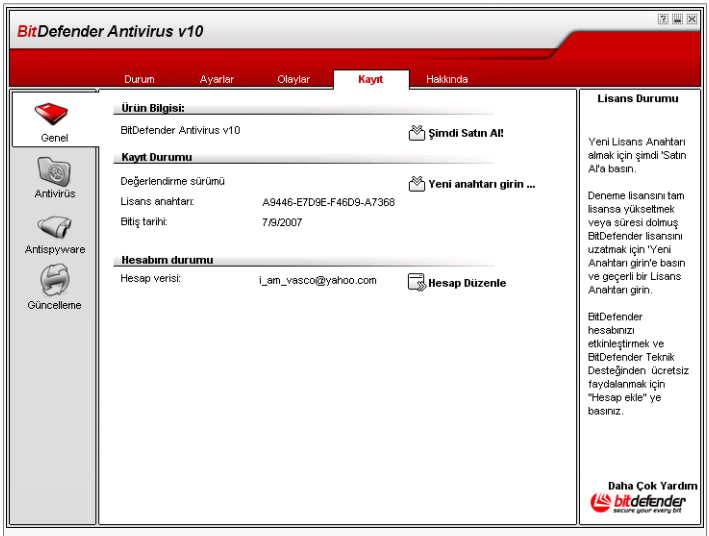
Bu olayları 2 yolla (tipi veya kaynağı) filtreleyebilirsiniz

- Hangi tip olayların gösterileceğini seçmek için **Filitre**'yi tıklayın.
- Aşağıya doğru açılan menüde olay kaynağını seçin

Eğer yönetim konsoluOlaylar bölümünde açık ise ve aynı zamanda bir olay meydana gelirse, olayı görmek için **Yenile** seçeneğini tıklamanız gerekmektedir.

Listedeki tüm olayları silmek için **Kaydı Temizle**'yi tıklayın ve tercihinizi onaylamak için **Evet** tuşuna basınız.

6.4. Ürün Kaydı



Ürün Kaydı

Bu bölümde, BitDefender ürünü (kayıt durumu, ürün kimlik numarası, sona erme tarihi) ve BitDefender hesabı ile ilgili bilgiler bulunmaktadır. Burada ürünü kaydettirebilir ve BitDefender hesabınızı yapılandırabilirsiniz.

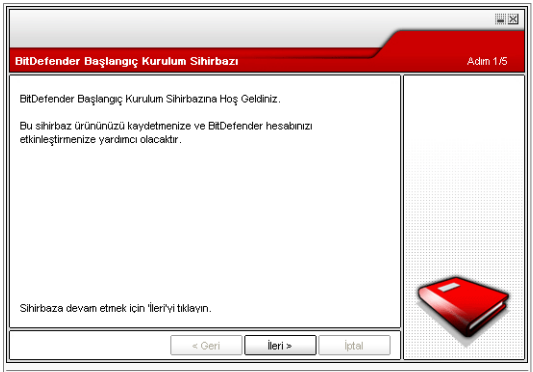
BitDefender çevrim içi mağazasından yeni bir lisans anahtarı almak için **Şimdi Satın Al** butonuna tıklayın.

Yeni Anahtar Gir'i tıklayarak ürünü kaydettirebilir, kayıt anahtarını veya hesap bilgilerini düzenleyebilirsiniz. BitDefender hesabınızı yapılandırmak için **Hesanı Düzenle** seçeneğine tıklayın. Her iki durumda da kayıt sihirbazı başlatılacaktır

6.4.1. Kayıt Sihirbazı

Kayıt sihirbazı 5 adımlı bir prosedürdür.

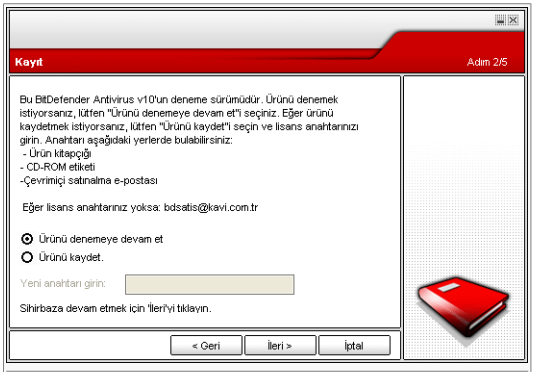
BitDefender Kayıt Sihirbazına Hoş Geldiniz



Hoşgeldiniz Ekranı

İleri'yi tıklayın.

BitDefender'ın Kaydettirilmesi



Kayıt

BitDefender Antivirus v10'u kaydetmek için **Ürünü kaydet** seçeneğini seçin. **Yeni anahtarı gir** alanına lisans anahtarını yazın.

Ürünü denemeye devam etmek için **Ürünü denemeye devam et'i** seçin.

İleri'yi tıklayın.

BitDefender Hesabının Açılması

Hesap Yaratma

BitDefender hesabım yok

BitDefender'ın teknik destek ve diğer ücretsiz hizmetlerinden yararlanabilmek için bir hesap açtırmanız gerekmektedir.

E-posta alanına geçerli bir e-posta adresi yazın. Bir şifre belirleyip **Şifre** alanına yazın. **Şifreyi yeniden gir** alanına şifrenizi yeniden girin. http://myaccount.bitdefender.com'da hesabınıza giriş yapmak için e-posta adresinizi ve şifrenizi kullanın.

Not

Şifre en az dört karakter uzunluğunda olmalıdır.

Hesabınızın açılmasını gerçekleştirmek için önce e-posta adresinizi aktif hale getirmeniz gerekmektedir. e-posta adresinizi kontrol edin ve BitDefender kayıt hizmetleri tarafından size gönderilen e-postadaki talimatları uygulayın.

Önemli

Bir sonraki adıma geçmeden önce hesabınızı aktif hale getirin.

Bir BitDefender hesabı açtırmak istemiyorsanız, sadece **Bu adımı geç** seçeneğini tıklayın. Sihirbazın bir sonraki adımını da atlayacaksınız.

Devam etmek için **İleri**'yi tıklayın.

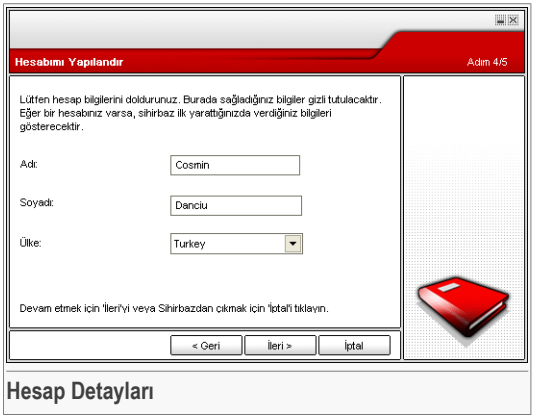
BitDefender hesabım var

Zaten bir BitDefender hesabınız varsa, e-posta adresinizi ve hesap şifrenizi girin. Yanlış bir şifre girerseniz, **İleri** tıkladığınızda şifreyi yeniden yazmanız istenecektir. Yeniden şifre girmek için **Tamam** veya sihirbazdan çıkmak için **İptal** seçeneğine tıklayın.

Şifrenizi unuttuysanız, **Şifremi unuttum**'u tıklayın ve talimatları uygulayın.

Devam etmek için **İleri**'yi tıklayın.

Hesap Detaylarının Girilmesi



Hesap Detayları

Not

Üçüncü adımdaki **Bu adımı geç** seçeneğini işaretlediyseniz bu adım atlanacaktır.

Adınızı ve soyadınızı yazın ve yaşadığınız ülkeyi seçin

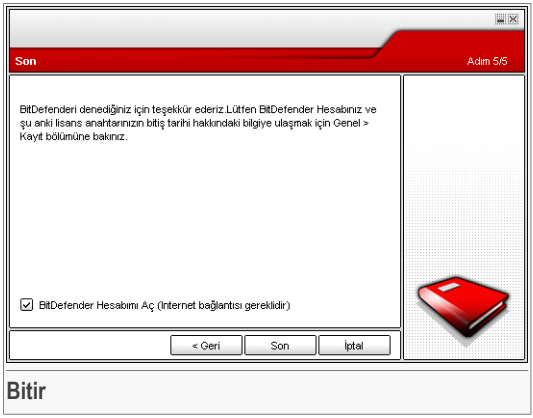
Zaten bir hesabınız varsa, sihirbaz daha önce belirttiğiniz bilgileri gösterecektir (varsa). Burada, İsterseniz bu bilgileri de değiştirebilirsiniz

Önemli

Burada belirttiğiniz bilgiler gizli kalacaktır.

İleri'yi tıklayın.

Adım 5/5 – Özet



Bu, yapılandırma sihirbazının en son adımıdır. Bir sonraki adıma dönerek istediğiniz herhangi bir değişikliği yapabilirsiniz (**Geri**)'yi tıklayın).

Herhangi bir değişiklik yapmak istemiyorsanız, sihirbazdan çıkmak için **Bitir**'i tıklayın.

BitDefender hesabınıza giriş yapmak için **BitDefender Hesabımı Aç** seçeneğini seçin. Internet bağlantısı gereklidir.

6.5. Hakkında

Genel Bilgi

Bu bölümde, iletişim bilgilerini ve ürün detaylarını bulabilirsiniz

BitDefender™, 180'den fazla ülkede 41 milyondan fazla ev ve kurumsal kullanıcılara etkin tehdit yönetimi sunarak, bugünün bilgisayar ortamında koruma şartlarını yerine getiren güvenlik çözümleri sunmaktadır.

BitDefender tüm büyük bağımsız inceleme kuruluşları tarafından onaylanmıştır **ICSA Labs**, **CheckMark** ve **Virus Bulletin**, ve **IST Ödülünü** alan tek güvenlik ürünüdür.

Bitdefender hakkında daha fazla bilgi http://www.bitdefender.com adresi ziyaret edilerek sağlanabilir.

7. Virüs Koruma Modülü

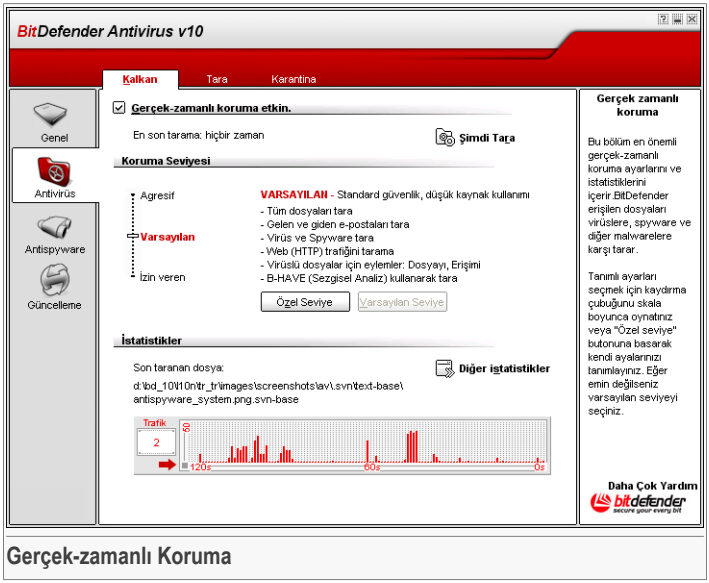
Bu kullanım kılavuzunun **Virüs Koruma** bölümü aşağıdaki başlıklardan oluşmaktadır.

- Erişim anında tarama
- İsteğe bağlı tarama
- Karantina

Not

Antivirus modülü ile ilgili daha fazla bilgi için "*Virüs Koruma Modülü*" (shf. 25) bölümüne bakınız.

7.1. Erişim anında tarama



Gerçek-zamanlı Koruma

Bu bölümde **Gerçek-zamanlı** korumayı yapılandırabilir ve aktivitesi hakkındaki bilgileri görebilirsiniz.**Gerçek-zamanlı koruma**e-posta mesajlarını, yüklenen programları ve tüm erişilen dosyaları tarayarak bilgisayarınızın güvenliğini sağlar.

Önemli

Virüslerin bilgisayarınıza bulaşmasını önlemek için **Gerçek-zamanlı** korumayı etkin kılın.

Bölümün sonunda, taranmış dosya ve e-posta mesajları ile ilgili **Gerçek-zamanlı** koruma istatistiklerini görebilirsiniz. Bu istatistiklerle ilgili daha detaylı bir pencereyi görmek isterseniz **Daha fazla istatistik** seçeneğine tıklayın.

7.1.1. Koruma Seviyesi

Koruma ihtiyaçlarınıza en uygun olan koruma seviyesini seçebilirsiniz. Uygun Koruma seviyesini belirlemek için kaydırma çubuğunu ölçek üzerinde kaydırın

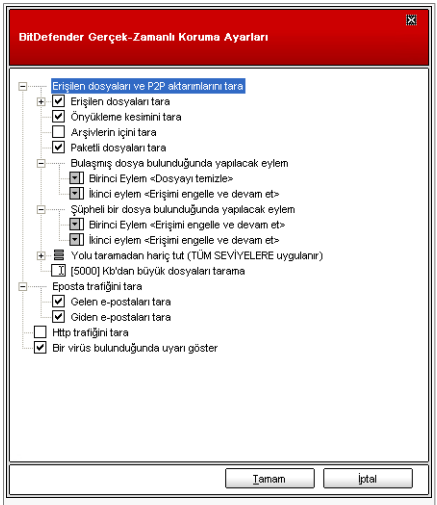
3 koruma seviyesi bulunmaktadır:

Koruma Seviyesi	Açıklama
Hoşgörülü	Temel güvenlik ihtiyaçlarını karşılar. Kaynak tüketim seviyesi çok düşüktür Yalnızca programlar ve gelen e-postalar virüse karşı taranır. Klasik imza tabanlı taramanın yanında sezgisel analiz de kullanılır. Virüs bulaşmış olan dosyalar üzerinde yapılan faaliyetler şunlardır: dosya temizleme/erişimi reddetme.
Varsayılan	Standart bir güvenlik sunar. Kaynak tüketim seviyesi düşüktür. Tüm dosyalar, gelen ve giden posta mesajları virüsler ve spyware'lere karşı taranır. Klasik imza tabanlı taramanın yanında sezgisel analiz de kullanılır. Virüs bulaşmış olan dosyalar üzerinde yapılan faaliyetler şunlardır: dosya temizleme/erişimi reddetme.
Agresif	Yüksek düzeyde bir güvenlik sunar. Kaynak tüketim seviyesi ortadır. Tüm dosyalar, gelen ve giden posta mesajları ve web trafiği, virüsler ve spyware'lere karşı taranır. Klasik imza tabanlı taramanın yanında sezgisel analiz de kullanılır. Virüs bulaşmış olan dosyalar üzerinde yapılan faaliyetler şunlardır: dosya temizleme/erişimi reddetme.

Varsayılan gerçek zamanlı koruma ayarlarını uygulamak için **Varsayılan Seviye**'yi tıklayınız

İleri düzeydeki kullanıcılar, BitDefender'ın sunduğu tarama ayarlarından yararlanmak isteyebilirler. Tarayıcı, zararsız olduğunu bildiğiniz dosya uzantılarını, dizinleri veya arşivleri atlayacak şekilde ayarlanabilir. Bu şekilde, tarama sürelerini oldukça azaltabilir ve bilgisayarınızın tarama sırasında daha iyi yanıt vermesini sağlayabilirsiniz.

Özel seviye seçeneğini tıklayarak **Gerçek-zamanlı korumayı** ayarlayabilirsiniz. Aşağıdaki pencere görülecektir:



Kalkan Ayarları

Tarama seçenekleri, Windows'taki arama menüleri gibi, genişletilebilir bir menü şeklinde düzenlenmektedir

Bir seçeneği açmak için "+" olan kutuyu, seçeneği kapatmak için "-" olan kutuyu tıklayın.

Her ne kadar "+" işareti olsa da bazı tarama seçeneklerinin açılmadığını görebilirsiniz. Bunun nedeni, bu seçeneklerin henüz seçili olmadıklarıdır. Eğer bunları seçerseniz, açılabileceklerini göreceksiniz.

- **Erişilen dosyaları ve P2P aktarım seçenekleri'ni tara** - erişilen dosyaları ve Anlık Mesajlaşma Yazılımlarından (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger) kurulan iletişimi tarar.Taranmasını istediğiniz dosyaların tipini seçiniz.

Seçenek		Açıklama
Erişilen dosyaları tara	**Tüm dosyaları tara**	Hangi tipte olursa olsun, tüm erişilen dosyalar taranacaktır
	Sadece program dosyalarını tara	Yalnızca program dosyaları taranacaktır. Bunlar aşağıdaki uzantıları olan dosyalardır: `.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`; `.hlp`; `.doc`; `.dot`; `.xls`; `.ppt`; `.wbk`; `.wiz`; `.pot`; `.ppa`; `.xla`; `.xlt`; `.vbs`; `.vbe`; `.mdb`; `.rtf`; `.htm`; `.hta`; `.html`; `.xml`; `.xtp`; `.php`; `.asp`; `.js`; `.shs`; `.chm`; `.lnk`; `.pif`; `.prc`; `.url`; `.smm`; `.pdf`; `.msi`; `.ini`; `.csc`; `.cmd`; `.bas`; `.eml` and `.nws`.

Seçenek		Açıklama
	Kullanıcı tanımlı uzantıları tara	Sadece kullanıcı tarafından belirlenmiş uzantıları olan dosyalar taranacaktır. Bu uzantılar ";" ile ayrılmalıdır
	Uzantıları taramadan hariç tut: [ ]	Kullanıcı tarafından belirlenmiş uzantıları olan dosyalar taranmayacaktır. Bu uzantılar ";" ile ayrılmalıdır
	Riskware için tara	Riskware'leri tarar. Bu dosyalar virus bulaşmış dosyalar olarak ele alınır. Bu seçenek etkin kılındığında, adware bileşen içeren yazılımların çalışması durabilir. Bu tür dosyaların taramadan çıkartılmasını istiyorsanız **Tarama'dan arayıcı ve uygulamaları atla**'yı seçin.
Erişimdeki disket sürücüyü tara		Erişildiğinde disket sürücüyü tarar
Dahili arşivleri tara		Erişilen arşivler taranır. Bu seçenek seçildiğinde, bilgisayar yavaşlayacaktır
Paketlenmiş dosyaları tara		Tüm paketlenmiş dosyalar taranır.
İlk işlem		Virus bulaşmış ve şüpheli dosyaları almak için menüdeki ilk işlemi seçer
	Erişimi reddet ve devam et	Virus bulaşmış bir dosya tespit edildiğinde, bu dosyaya erişim reddedilir.
	Dosyayı temizle	Virüs bulaşan dosyayı temizler.
	Dosyayı Sil	Hiç bir uyarı vermeden virus bulaşan dosyayı siler.
	Dosyayı karantinaya taşı	Virus bulaşan dosyaları karantinaya taşır.
İkinci işlem		Birinci işlemin başarısız olması durumunda, virus bulaşmış dosyaları almak için menüdeki ikinci işlemi seçer
	Erişimi reddet ve devam et	Virus bulaşmış bir dosya tespit edildiğinde, bu dosyaya erişim reddedilir.
	Dosyayı Sil	Hiç bir uyarı vermeden virus bulaşan dosyayı siler.

Seçenek	Açıklama
Dosyayı karantinaya taşı	Virus bulaşan dosyaları karantinaya taşır.
[x] Kb'dan büyük dosyaları tarama	Taranacak maksimum dosya boyutunu girin. Eğer boyut 0 Kb ise, boyutu ne olursa olsun tüm dosyalar taranacaktır
Klasörü taramadan hariç tut (TÜM SEVİYELERE uygulanır)	Taramadan hariç tutulacak bir klasörü belirlemek için bu seçeneğe karşılık gelen "+"'ya tıkla. Bunun sonucunda, seçenek genişleyecek ve yeni bir seçenek "Yeni öğe" çıkacaktır. Yeni öğeye karşılık gelen kutuyu tıklayın ve açılan pencerede, taramadan hariç tutmak istediğiniz klasörü seçin. Seçilen koruma seviyesi ne olursa olsun, burada seçilen öğeler taramadan hariç tutulacaktır (sadece **Özel Seviye** için geçerli değildir).

- **E-posta trafiğini tara** - e-posta trafiğini tarar

  Aşağıdaki seçenekler mevcuttur:

Seçenek	Açıklama
Gelen postaları tara	Tüm gelen e-posta mesajlarını tarar
Giden postaları tara	Tüm giden e-posta mesajlarını tarar.

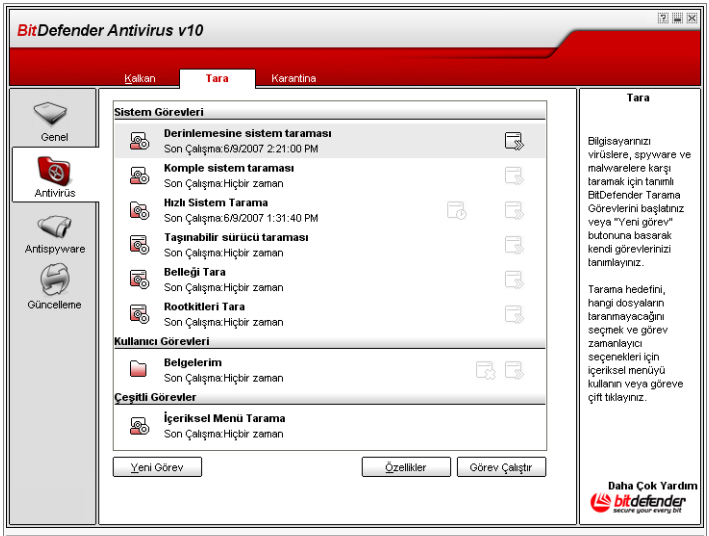
- **Http trafiğini tara** - http traffiğini tarar.
- **Bir virüs bulunduğunda uyarı göster** - dosyada veya e-posta mesajında virüs bulunduğunda bir uyarı penceresi açılır.

  Virüs bulaşmış bir dosya için, uyarı penceresinde virüsün adı, bulunduğu yer, BitDefender tarafından alınan önlem ve bununla ilgili daha fazla bilgi bulabileceğiniz BitDefender sitesine bir link bulunacaktır. Virüs bulaşmış bir dosya için, uyarı penceresinde ayrıca, gönderen ve alan hakkında bilgi olacaktır.

  Şüpheli bir dosya tespit edildiğinde, uyarı penceresinden, bu dosyayı analiz etmek üzere BitDefender Laboratuarına göndermenize yardım edecek bir sihirbazı başlatabilirsiniz. Bu raporla ilgili bilgi almak için e-posta adresinizi yazabilirsiniz.

Değişiklikleri kaydetmek ve pencereyi kapatmak için **Tamam**'ı tıklayın.

7.2. Isteğe bağlı tarama



Tarama Görevleri

Bu bölümde, bilgisayarınızı taramak için BitDefender'ı yapılandırabilirsiniz.

BitDefender'ın temel amacı, bilgisayarınızı virüslerden uzak tutumaktır. Bunun için yapılacak ilk ve en önemli şey, bilgisayarınızı yeni virüslerden uzak tutmak ve daha sonra e-posta mesjlarınızı ve sisteminize yüklenen veya kopyalanan yeni dosyaları taramaktır.

BitDefender'ı yüklemeden önce, sisteminizde hali hazırda var olan bir virüs olması riski vardır. Bu nedenle BitDefender'ı yükledikten sonra, bilgisayarınızı mevcut virüslere karşı taramanız iyi bir fikir olacaktır. Ve aynı şekilde virüslere karşı bilgisayarınızı sık sık taramanız da çok faydalı olacaktır.

7.2.1. Tarama Görevleri

Isteğe bağlı tarama, tarama görevlerine dayalıdır. Kullanıcı varsayılan görevleri veya kendi tarama görevlerini (kullanıcı tanımlı görevler) kullanarak bilgisayarı tarayabilir.

Üç tarama görevi kategorisi bulunmaktadır:

- **Sistem görevleri** – varsayılan sistem görevleri listesini içerir. Aşağıdaki görevler mevcuttur:

Varsayılan Görev	Açıklama
Yoğun sistem tarama	Virüs ve spyware'lere karşı, arşivler de dahil tüm sistemi tarar.
Tam Sistem Tarama	Virüs ve spyware'lere karşı, arşivler hariç olarak, tüm sistemi tarar.
Hızlı Sistem Tarama	Virüs ve spyware'lere karşı tüm programları tarar.
Çıkarılabilir sürücü tarama	Virüs ve spyware'lere karşı çıkarılabilir sürücüleri tarar.
Tarama Hafızası	Bilinen spyware tehditlerine karşı hafızayı tarar.
Rootkit'leri Tarama	Gizli kötü amaçlı yazılımlara karşı hafızayı tarar.

- **Kullanıcı görevleri** - kullanıcı tanımlı görevleri içerir

  `Belgelerim` adlı bir görev belirtilir. `Belgelerim` klasöründeki belgelerinizi taramak içinbu görevi kullanın.
- **Çeşitli görevler**– çeşitli tarama görevlerini içermektedir. Bu tarama görevleri, bu pencereden çalıştırılamayan alterntif tarama tipleri ile ilgilidir. Sadece ayarlarını değiştirebilir veya tarama raporlarını görebilirsiniz

Her görevin sağında üç buton vardır:

- **Zamanlanmış Görev**seçilen görevin daha sonra yapılmak üzere seçildiğini gösterir. Bu ayarı değiştirebileceğiniz, **Özellikler** penceresindeki Zamanlayıcı bölümüne gitmek için bu butonu tıklayın.
- **Sil** - seçilen görevi kaldırır.

  Not

  Sistem görevleri için uygun değildir. Bir sistem görevini silemezsiniz

- **Şimdi Tara** - hemen bir tarama. başlatarak seçilen görevi çalıştırır.

7.2.2. Kısayol Menüsü

Her bir görev için bir kısayol menüsü bulunmaktadır. Seçilen görevi açmak için üzerine sağ tıklayın.

Kısayol Menüsü

Kısayol menüsünde aşağıdaki komutlar bulunmaktadır:

- **Şimdi Tara** - hemen bir tarama başlatarak seçilen görevi çalıştırır
- **Tarama Hedefini Değiştir** – seçilen görevin tarama hedefini değiştirebileceğiniz **Özellikler** penceresi, **Tarama Yolu** sekmesini açar.
- **Görevi Programla** - seçilen görevi zamanlayabileceğiniz **Özellikler** penceresi, **Zamanlayıcı** sekmesini açar.
- **Tarama Kayıtlarını Göster** – seçilen görev çalıştırıldıktan sonra üretilen raporları görebileceğiniz **Özellikler** penceresi, **Tarama Kayıtları** sekmesini açar.
- **Kopyala** - seçilen görevi kopyalar.

Not

Kopyalanmış görevin ayarlarını değiştirebileceğiniz için, bu özellik yeni görev yarattığınızda yararlı olur.

- **Masaüstü Kısayolu Yarat** – seçilen görev için bir masaüstü kısayolu yaratır.
- **Sil** – seçilen görevi siler.

Not

Sistem görevleri için uygun değildir. Bir sistem görevini silemezsiniz

- **Özellikler** – seçilen görevlerin ayarlarını değiştirebileceğiniz **Özellikler** penceresi, **Genel** sekmesini açar

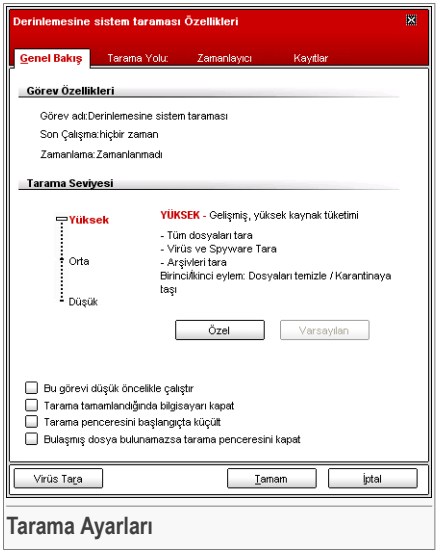
Önemli

Farklı özellikleri nedeniyle, sadece **Özellikler** ve **Tarama Kayıtlarını Göster** seçenekleri, **Çeşitli Görevler** kategorisindeki görevler için uygundur.

7.2.3. Tarama Görevi Özellikleri

Her tarama görevinin kendi **Özellikler** penceresi vardır. Burada tarama seçeneklerini yapılandırabilir, tarama hedefini ve görevin zamanını belirleyebilir veya raporları görebilirsiniz. Bu pencereye girmek için görevi seçiniz ve **Özellikler**'i tıklayınız.(veya göreve sağ tıklayın ve **Özellikler**'i seçiniz.)

Tarama Ayarları



Tarama Ayarları

Burada görev hakkındaki bilgileri görebilir (adı, son çalıştırma ve zaman durumu) ve tarama ayarlarını belirleyebilirsiniz.

Tarama Seviyesi

Öncelikle tarama seviyesini seçmeniz gerekmektedir. Uygun tarama seviyesini belirlemek için kaydırma çubuğunu ölçek üzerinde kaydırın.

3 tarama seviyesi bulunmaktadır

Koruma Seviyesi	Açıklama
Düşük	Makul tespit etkinliği sunar. Kaynak tüketim seviyesi düşüktür Programlar yalnızca virüslere karşı taranır. Klasik imza tabanlı taramanın yanında sezgisel analiz de kullanılır. Virüs bulaşmış olan dosyalar üzerinde yapılan faaliyetler şunlardır: dosyayı temizle/karantinaya taşı.
Orta	İyi tespit etkinliği sunar. Kaynak tüketim seviyesi ortadır. Tüm dosyalar virüsler ve spyware'lere karşı taranır. Klasik imza tabanlı taramanın yanında sezgisel analiz de kullanılır. Virüs

Koruma Seviyesi	Açıklama
	bulaşmış olan dosyalar üzerinde yapılan faaliyetler şunlardır: dosyayı temizle/karantinaya taşı.
Yüksek	Yüksek tespit etkinliği sunar. Kaynak tüketim seviyesi yüksektir Tüm dosya ve arşivler virüsler ve spyware'lere karşı taranır. Klasik imza tabanlı taramanın yanında sezgisel analiz de kullanılır. Virüs bulaşmış olan dosyalar üzerinde yapılan faaliyetler şunlardır: dosyayı temizle/karantinaya taşı.

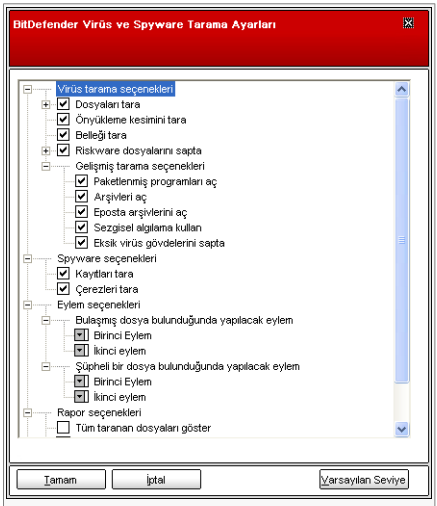
Önemli

Rootkit'lerin Taranmasıgörevinde aynı tarama seviyeleri vardır. Ancak, seçenekler farklıdır

- **Düşük** - Sadece süreçler taranır. Tespit edilen öğeler üzerinde hiç bir işlem yapılmaz
- **Orta** – Gizli öğeleri bulmak için dosya ve süreçler taranır. Tespit edilen öğeler üzerinde hiç bir işlem yapılmaz
- **Yüksek** – Gizli öğeleri bulmak için dosya ve süreçler taranır. Tespit edilen öğeler yeniden isimlendirilir.

İleri düzeydeki kullanıcılar, BitDefender'ın sunduğu tarama ayarlarından yararlanmak isteyebilirler. Tarayıcı, zararsız olduğunu bildiğiniz dosya uzantılarını, dizinleri veya arşivleri atlayacak şekilde ayarlanabilir. Bu şekilde, tarama sürelerini oldukça azaltabilir ve bilgisayarınızın tarama sırasında daha iyi yanıt vermesini sağlayabilirsiniz.

Kendi tarama seçeneklerinizi belirlemek için **Özel**seçeneğini tıklayın. Yeni bir pencere görünecektir.



Tarama Ayarları

Tarama seçenekleri, Windows'taki arama menüleri gibi, genişletilebilir bir menü şeklinde düzenlenmektedir

Tarama seçenekleri beş kategori olarak gruplanmaktadır:

- **Virus tarama seçenekleri**
- **Spyware seçenekleri**
- **İşlem seçenekleri**
- **Rapor seçenekleri**
- **Diğer seçenekler**

Bir seçeneği açmak için "+" olan kutuyu, seçeneği kapatmak için "-" olan kutuyu tıklayın.

Önemli

Rootkit'lerin Taranması sadece üç kategori bulunmaktadır: **Rootkit tarama seçenekleri** ,**Rapor seçenekleri**, ve **Diğer seçenekler**.İlk kategoride nelerin taranacağını seçebilir (dosyalar veya hafıza, veya her ikisi) ve tespit edilen öğelerde alınacak önlemleri belirleyebilirsiniz (**Hiçbiri (Kayıt nesneleri)/Dosyalara yeni isim ver**). Diğer iki kategori aşağıda anlatıldığı şekilde benzerdir.

- Taranacak nesnelerin tipini (arşivler, e-posta mesajları ve benzeri) ve diğer seçenekleri belirleyin. Bu, **Virüs tarama seçenekleri** kategorisindeki belirli seçeneklerin seçilmesiyle yapılır.

Seçenek		Açıklama
Dosyaları tara	**Tüm dosyaları tara**	Hangi tipte olursa olsun, tüm erişilen dosyalar taranacaktır
	Sadece program dosyalarını tara	Sadece program dosyaları taranacaktır. Bunun anlamı sadece şağıdaki uzantıları olan dosyaların taranacağıdır:`exe`; `bat`; `com`; `dll`; `ocx`; `scr`; `bin`; `dat`; `386`; `vxd`; `sys`; `wdm`; `cla`; `class`; `ovl`; `ole`; `exe`; `hlp`; `doc`; `dot`; `xls`; `ppt`; `wbk`; `wiz`; `pot`; `ppa`; `xla`; `xlt`; `vbs`; `vbe`; `mdb`; `rtf`; `htm`; `hta`; `html`; `xml`; `xtp`; `php`; `asp`; `js`; `shs`; `chm`; `lnk`; `pif`; `prc`; `url`; `smm`; `pdf`; `msi`; `ini`; `csc`; `cmd`; `bas`; `eml` and `nws`.
	Kullanıcı tanımlı uzantıları tara	Sadece kullanıcı tarafından belirlenmiş uzantıları olan dosyalar taranacaktır. Bu uzantılar ";" ile ayrılmalıdır
	Kullanıcı tanımlı uzantıları hariç tut	Kullanıcı tarafından belirlenmiş uzantıları olan dosyalar taranmayacaktır. Bu uzantılar ";" ile ayrılmalıdır
Boot sektörlerini tara		Sistem boot sektörlerini tarar
Hafızayı tara		Virüs ve diğer kötü amaçlı yazılımlara karşı hafızayı tarar.
Riskli yazılımları tespit et		Arayıcı ve adware gibi virüs dışındaki tehditlere karşı tarama yapar. Bu dosyalar virus bulaşmış dosyalar olarak ele alınır. Bu seçenek etkin kılındığında, adware bileşen içeren yazılımların çalışması durabilir. Bu tür dosyaların taramadan çıkartılmasını istiyorsanız **Uygulama ve Arayıcılar Hariç**'i seçin.
Gelişmiş tarama seçenekleri	**Paketlenmiş programları aç**	Paketlenmiş dosyaları tarar
	Arşivleri aç	Dahili arşivleri tarar.
	E-posta arşivlerini aç	Dahili posta arşivlerini tarar
	Sezgisel tespiti kullan	Dosyaların sezgisel taramasını kullanmak için. Sezgisel taramanın amacı, bir virüs tanımı

Seçenek	Açıklama
	bulunmadan önce, belirli kalıp ve algoritmalara göre yeni virüslerin tanımlanmasıdır. Yanlış alarm mesajları görünebilir.Böyle bir dosya tespit edildiğinde şüpheli olarak sınıflandırılır. Bu durumlarda, dosyayı analiz edilmesi için BitDefender laboratuarına göndermenizi tavsiye ediyoruz.
Eksik virüs gövdelerini tespit et	Eksik virüs gövdelerini tespit eder

- Spyware tarama hedefini (kayıt, cookie) belirleyin.Bu, **Spyware** tarama seçenekleri kategorisindeki belirli seçeneklerin seçilmesiyle yapılır.

Seçenek	Açıklama
Kaydı tara	Kayıt girişlerini tarar
Çerezleri tara	Çerezleri tarar.

- Virüs bulaşmış veya şüpheli dosyaları belirleyin. Bu dosyalardaki tüm muhtemel işlemleri görmek için **İşlem seçenekleri'ni** açın.

  Virüs bulaşmış veya şüpheli bir dosya tespit edildiğinde yapılacak işlemleri seçin. Virüs bulaşmış veya şüpheli dosyalar için farklı işlemleri seçebilirsiniz. Ayrıca ilk işlem başarısız olduğunda ikinci bir işlem de seçebilirsiniz.

İşlem	Açıklama
Hiçbiri (kayıt nesneleri)	Virus bulaşmış dosyalar üzerinde hiç bir işlem yapılmaz. Bu dosyalar rapor dosyasında olacaktır.
İşlem için kullanıcıdan bilgi iste	Virüslü bir dosya tespit edildiğinde, bu dosyadaki işlemi seçmek için kullanıcıdan bilgi isteyen bir pencere açılacaktır. Dosyanın önemine göre, dosyayı temizlemeyi, karantina bölgesine almayı veya silmeyi seçebilirsiniz.
Dosyaları temizle	Virüs bulaşan dosyayı temizler.
Dosyaları sil	Hiç bir uyarı vermeden virus bulaşan dosyayı siler.
Dosyaları karantinaya taşı	Virus bulaşan dosyaları karantinaya taşır.

İşlem	Açıklama
Dosyalara yeni isim ver	Dosyaların uzantılarını değiştir. Dosyaların yeni uzantısı `.vir` olacaktır. Dosyalara yeni isim vererek, enfeksiyonun bulaşması ve yayılması ihtimali ortadan kaldırılır.Aynı zamanda, ileride incelenmek ve analiz edilmek üzere kaydedilebilirler

Önemli

Dosyalara yeni isim verme gizli dosyalar (rootkit) üzerinde benzer etki yaratır. Tespit edilen dosyalara yeni isim vererek, enfeksiyonun bulaşması ve yayılması ihtimali ortadan kaldırılır. Aynı zamanda, ileride incelenmek ve analiz edilmek üzere kaydedilebilirler

- Rapor dosyaları için seçenekleri belirleyin. Tüm muhtemel işlemleri görmek için **Rapor seçenekleri**'ni açın.

Seçenek	Açıklama
Tüm taranan dosyaları göster	Rapor dosyasında tüm taranmış dosyaları ve durumlarını (bulaşmış veya değil) listeler. Bu seçenek seçildiğinde, bilgisayar yavaşlayacaktır.
[x] günden eski kayıtları sil	Bir raporun Tarama Kayıtları bölümünde ne kadar bir süre kalması gerektiğini belirlemenizi sağlayan düzenleme alanıdır.Bu seçeneği seçin ve yeni bir zaman aralığı girin. Varsayılan zaman aralığı 180 gündür.

Not

Rapor dosyaları, **Özellikler** penceresindeki Tarama Kayıtları bölümündedir.

- Diğer seçenekleri belirleyin. Aşağıdaki seçenekleri seçebileceğiniz **Diğer seçenekler**kategorisini açın.

Seçenek	Açıklama
Şüpheli dosyaları BitDefender Lab.'na gönder	Tarama süreci bittikten sonra tüm şüpheli dosyaları BitDefender laboratuarına göndermek için sizden bilgi istenecektir

Eğer **Varsayılan Seviye**'yi tıklarsanız, varsayılan ayarları yükleyeceksiniz.

Değişiklikleri kaydetmek ve pencereyi kapatmak için **Tamam**'ı tıklayın.

Diğer Ayarlar

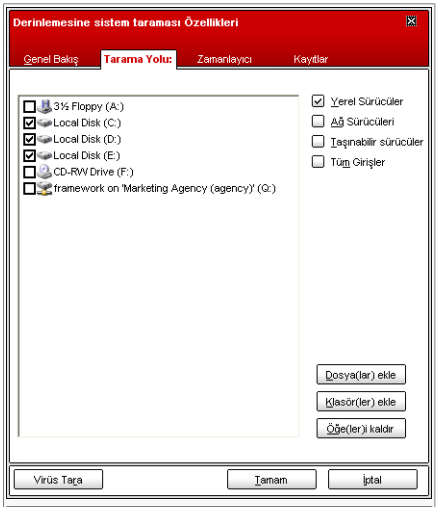
Tarama süreci için bir dizi genel seçenek bulunmaktadır:

Seçenek	Açıklama
Görevi Düşük öncelikli olarak çalıştır	Tarama sürecinin önceliğini düşürür. Diğer programların daha hızlı çalışmasını ve tarama sürecinin tamamlanması için gerekli zamanı artırmayı sağlayabilirsiniz.
Tarama tamalandığında bilgisayarı kapat	Tarama süreci tamamlandıktan sonra bilgisayarı kapatır.
Şüpheli dosyaları BitDefender Lab.'na gönder	Tarama süreci bittikten sonra tüm şüpheli dosyaları BitDefender laboratuarına göndermek için sizden bilgi istenecektir
Tarama penceresini başlangıçta sistem tepsisine gönder	Tarama penceresini sistem tepsisi'ne gönderir. Açmak için BitDefender ikonuna çift tıklayın

Değişiklikleri kaydetmek ve pencereyi kapatmak için **Tamam**'ı tıklayın. Görevi başlatmak için sadece **Tara**'ya tıklayın.

Tarama Hedefi

Bu bölüme girmek için görevi seçip **Özellikler**'e tıkladıktan sonra **Tarama Yolu** tabına basınız.



Tarama Hedefi

Burada tarama hedefini belirleyebilirsiniz.

Bu bölümde aşağıdaki butonlar bulunmaktadır:

- **Dosya(lar)Ekle** - taramak istediğiniz dosya (dosyaları) seçebileceğiniz bir gözatma penceresini açar
- **Klasör(ler)Ekle** - yukarıdaki gibidir, fakat BitDefender'dan taramasını istediğiniz dosya yerine klasörleri seçersiniz.

Not

Listeye dosya/klasör eklemek için ayrıca sürükle bırak özelliğini de kullanabilirsiniz.

- **Nesneleri Kaldır**

Not

Sadece daha sonra eklenen dosya/klasörler silinebilir, BitDefender tarafından otomatik olarak görülenler silinmez.

Yukarıda açıklanan butonlar dışında, tarama alanlarının hızlı seçilmesini sağlayan başka seçenekler de bulunmaktadır.

- **Yerel Sürücüler**- yerel sürücüleri taramak için.
- **Ağ Sürücüleri**- ağ sürücülerini taramak için.
- **Çıkarılabilir Sürücüler** - çıkarılabilir sürücüleri (CD-ROM, disket birimi) taramak için.
- **Tüm Girişler** - yerel, ağ veya çıkarılabilen tüm sürücüleri taramak için.

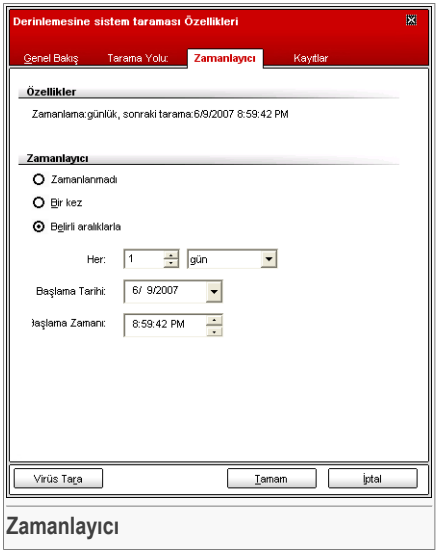
Not

Tüm bilgisayarın virüslere karşı taranmasını isterseniz, **Tüm girişler**. seçeneği yanındaki kutuyu işaretleyin.

Değişiklikleri kaydetmek ve pencereyi kapatmak için **Tamam**'ı tıklayın. Görevi başlatmak için sadece **Tara**'ya tıklayın.

Zamanlayıcı

Bu bölüme girmek için görevi seçip **Özellikler**'e bastıktan sonra **Zamanlayıcı**'ya basınız.



Zamanlayıcı

Burada, görevin belirli bir zaman için programlanıp programlanmadığını görebilir ve bu özelliği değiştirebilirsiniz

Önemli

Karmaşık görevlerde tarama süreci belirli bir zaman alacaktır; tüm diğer programlar kapatıldığında, en etkin şekilde çalışacaktır. Bu nedenle, bilgisayarınızı kullanmadığınızda ve bekleme modunda olduğunda bu görevleri programlamanız en doğru yöntem olacaktır.

Bir görevi programlarken, aşağıdaki seçeneklerden birini seçmeniz gerekecektir:

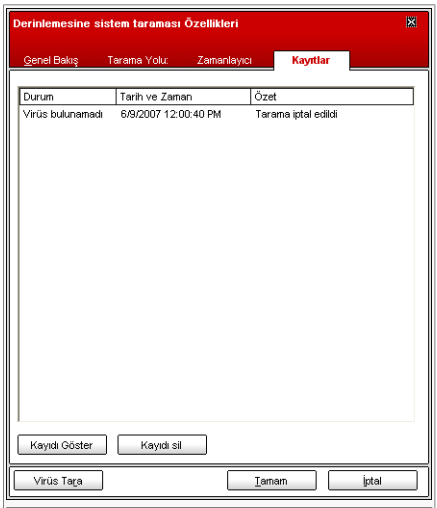
- **Programlanmamış** - yalnızca kullanıcı talep ettiğinde görevi başlatır.
- **Bir Kez** - taramayı sadece bir kez, belirli bir anda başlatır.**Başlatma Tarihi/Zamanı** alanlarına başlatma tarihini ve zamanını girin.
- **Periyodik** - belirli bir tarih ve zamandan başlayarak, taramayı periyodik olarak belirli zaman aralıklarında (saat, gün, hafta, ay, yıl) başlatır.

  Taramanın belirli aralıklarda tekrarlanmasını istiyorsanız, **Periyodik** seçeneğini seçin ve **Her** alanına sürecin sıklığını belirterek dakika/saat/gün/hafta/ay/yıl sayısını girin. Ayrıca **Başlatma Tarihi/Zamanı** alanlarına başlatma tarihini ve zamanını girmelisiniz.

Değişiklikleri kaydetmek ve pencereyi kapatmak için **Tamam**'ı tıklayın. Görevi başlatmak için sadece **Tara**'ya tıklayın.

Tarama Kayıtları

Görevi seçip **Özellikler**'e bastıktan sonra **Tarama Kayıtları** sekmesine tıklayın.



Tarama Kayıtları

Burada, her görevin gerçekleştirildiğinde üretilen raporu görebilirsiniz. Her dosyada, durumu (temiz/virüslü), taramanın hangi tarih ve zamanda gerçekleştiği hakkında ek bilgiler ve bir özet (tarama tamamlandı) olacaktır.

İki buton vardır:

- **Kaydı göster** – seçilen rapor dosyasını görüntülemek için.
- **Kaydı sil** – seçilen rapor dosyasını silmek için

Bir dosyayı görüntülemek veya silmek için ayrıca, dosyayı sağ tıklayıp kısayol menüsünden ilgili seçeneği seçin.

Değişiklikleri kaydetmek ve pencereyi kapatmak için **Tamam**'ı tıklayın. Görevi başlatmak için sadece **Tara**'ya tıklayın.

7.2.4. Isteğe bağlı tarama Tipleri

BitDefender, üç tip isteğe bağlı tarama tipi sunmaktadır:

- Anında tarama – sistem/kullanıcı görevleri arasından bir tarama görevini çalıştırır.
- Bağlamsal tarama – bir dosya veya klasör üzerine sağ tıklayıp BitDefender Antivirus v10'u seçin.

- Sürükle&Bırak taraması Tarama Etkinlik Çubuğundaki bir dosya veya klasörü sürükleyip bırakır.

Anında Tarama

Bilgisayarınızın tamamını veya bir kısmını taramak için, varsayılan tarama görevlerini kullanabilir veya kendi tarama görevlerinizi yaratabilirsiniz. tarama görevi oluşturmada iki yöntem vardır:

- Mevcut bir görevi Kopyalayıp, yeni isim verin ve Özellikler penceresinde gerekli değişiklikleri yapın;
- Yeni bir görev yaratmak ve onu **yapılandırmak** için Yeni Görev'e tıklayın.

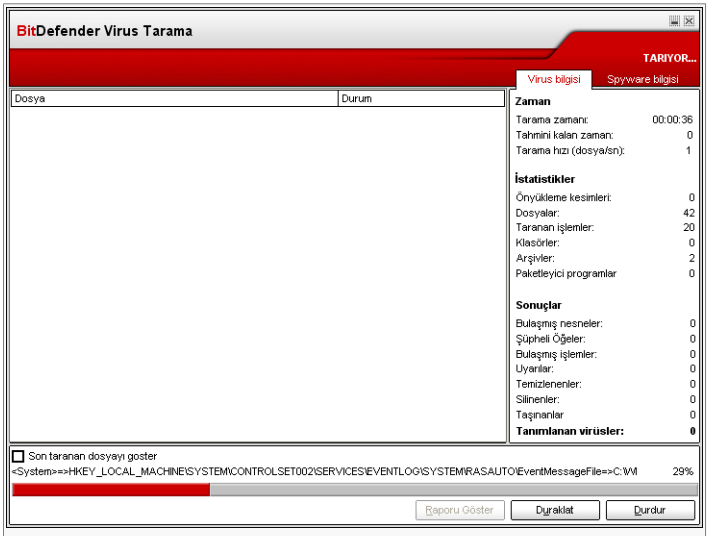
BitDefender'ın tam bir tarama yapabilmesi için tüm diğer açık programları kapatmanız gerekmektedir. Özellikle e-posta istemcinizin (örn.Outlook, Outlook Express veya Eudora) kapatılması önemlidir

BitDefender'ın bilgisayarınızı taramasından önce, hergün yeni bir virüs ortaya çıktığı ve tanımlandığı için, BitDefender'ın virüs imzalarının güncellenmiş olduğundan emin olun. Güncelle modülünün üst kısmında, en son güncellemenin ne zaman yapıldığını doğrulayabilirsiniz.

Taramayı başlatmak için bu metodlardan birini kullanın:

- Listeden istenen tarama görevine çift tıklayınız.
- İlişkili görevle ilgili **Şimdi Tara**'ya basınız.
- Görevi seçtikten sonra **Görevi Çalıştır**'a basınız.

Tarama penceresi çıkacaktır:



Tarama Penceresi

Tarama süreci çalıştığında sistem tepsisinde bir ikon görülecektir.

Tarama yapılırken, BitDefender size ilerleme durumunu gösterecek ve herhangi bir tehdit bulunduğunda sizi uyaracaktır. Sağ tarafta, tarama süreci ile ilgili istatistik bilgilerini görebilirsiniz. Tarama hedefine dayalı olarak, spyware ve/veya virüs bilgisi verilebilir. Eğer her ikisi de mümkünse, ilgili sekmeye tıklayarak, spyware veya virüs tarama süreci hakkında daha fazla bilgi alabilirsiniz.

Son taranan dosya'ya karşılık gelen kutuyu seçtiğinizde sadece en son taranan dosya ile ilgili bilgiler gösterilecektir.

Not

Tarama süreci, taramanın karmaşıklığına bağlı olarak, belirli bir zaman alabilir

Üç buton vardır:

- **Dur** – tarama sürecini sonlandırabileceğiniz yeni bir pencere açar. Tarama pencersinden çıkmak için **Evet&Kapat**'ı tıklayın.

Not

Eğer tarama süresince şüpheli bir dosya tespit edilirse bunların BitDefender Lab.'ına gönderimi için sorulacaktır.

- **Duraklat** – tarama sürecini geçici olarak durdurur – **Devam et**.'e tıklayarak süreci devam ettirebilirsiniz.
- **Raporu göster** – tarama raporunu açar.

Not

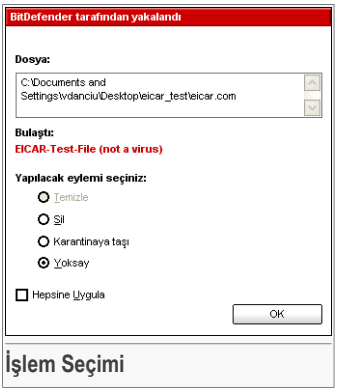
Çalışan bir göreve sağ tıkladığınızda, tarama penceresini yönetebileceğiniz bir kısayol (bağlamsal) menü açılacaktır. (**Duraklat/Devam Et**, **Dur** ve **Dur&Kapat**) seçenekleri, tarama pencersindeki butonlara benzer.

Eğer Özellikler penceresinde İşlem için **kullanıcıdan bilgi iste** seçeneği seçilmişse, virüs bulaşmış bir dosya tespit edildiğinde, bu dosya üzerinde yapılacak işlemi seçmenizi isteyen bir uyarı penceresi açılacaktır.

Dosyanın adını ve virüsün adını görebilirsiniz.

Virüs bulaşmış dosya üzerinde aşağıdaki işlemleri yapmayı seçebilirsiniz:

- **Temizle** – virüs bulaşan dosyayı temizler.
- **Sil** – virüs bulaşan dosyayı siler.
- **Karantinaya taşı** - virüs bulaşan dosyayı karantinaya taşır.
- **Gözardı et** - Bulaşmayı gözardı eder. Virus bulaşmış dosyalar üzerinde hiç bir işlem yapılmaz.



İşlem Seçimi

Bir dosyayı taradığınızda, yaptığınız işlemin tüm virüslü dosyalar için aynı olmasını istiyorsanız, **Hepsine uygula** seçeneğini işaretleyin.

Not

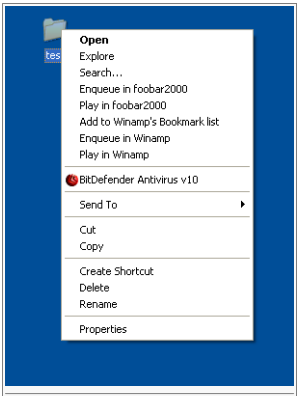
Temizle seçeneği etkin değilse, bunun anlamı dosyanın temizlenemeyeceğidir. En iyi seçenek, bunu izole ederek karantina bölgesine taşımak ve analiz edip silmek için bize göndermenizdir.

Tamam'ı tıklayın.

Not

Rapor dosyası, ilgili görevin **Özellikler** penceresindeki Tarama Kayıtları bölümünde otomatik olarak kaydedilir.

Bağlamsal Tarama



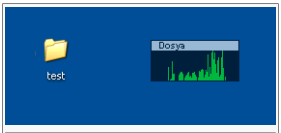
Bağlamsal Tarama

Taranmasını istediğiniz dosya veya klasöre sağ tıklayıp **BitDefender Antivirus v10**'u seçin.

Bağlamsal Menü Tarama görevinin Özellikler penceresine girerek tarama seçeneklerini değiştirebilir ve rapor dosyalarını görebilirsiniz.

Sürükle&Bırak Taraması

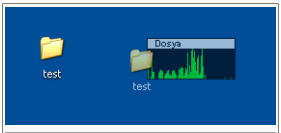
Taranmasını istediğiniz dosya veya klasörü şekilde gösterildiği gibi sürükleyerek **Tarama Etkinlik Çubuğuna** bırakın.



Dosya Sürükle

Eğer virüs bulaşmış bir dosya tespit edilirse, bu dosya üzerinde yapılmasını istediğiniz işlemi soran bir uyarı penceresi çıkacaktır.

Her iki alternatif taramada da (bağlamsal ve sürükle&bırak taraması), tarama penceresi açılacaktır.



Dosya Bırak

7.2.5. Rootkit Taraması

En son güvenlik tehditlerini çözmek için, BitDefender, etkin virüs koruma & antispyware motorları olan bir rootkit dedektörü sunmuştur. Artık, BitDefender'la gizli dosyaları,

klasörleri veya süreçleri araştırarak rootkit'leri tespit edebilirsiniz. Bununla birlikte, rootkit'leri kullanan kötü amaçlı yazılımları yeniden isimlendirerek sisteminizi koruyabilirsiniz.

Bilgisayarınızı rootkit'lere karşı taramak için **Rootkit**'leri Tara görevini çalıştırın. Bir tarama penceresi çıkacaktır

Önemli

Rootkit'leri kontrol ederken, BitDefender'ı gizli dosyalar üzerinde işlem yapmayacak şekilde ayarlamanızı önemle tavsiye ediyoruz.

Tarama sonunda, sonuçları görebilirsiniz. Eğer gizli dosyalar tespit edilmişse, bunları dikkatle kontrol edin: gizli dosyaların varlığı muhtemel bir izinsiz girişi gösteriyor olabilir.

Eğer tespit edilen dosyaların kötü amaçlı yazılımlar olduğundan eminseniz, **Dosyalara yeni isim ver** işlemini seçmenizi ve **Rootkit'leri Tara** görevini tekrar çalıştırmanızı tavsiye ediyoruz. Bu şekilde gözli dosyalar engellenecektir

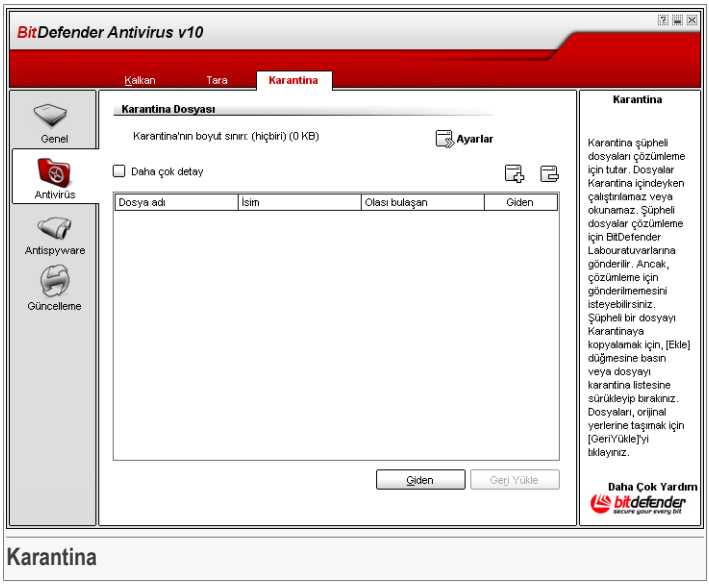
Uyarı

TÜM GİZLİ DOSYALAR KÖTÜ AMAÇLI YAZILIMLAR DEĞİLDİR! Gizli dosyalara yeniden isim vermeden önce, geçerli bir uygulama veya sisteme ait olup olmadıklarından emin olun. Bu dosyaların yeniden isimlendirilmesi sisteminizin kullanılamamasına sebep olabilir.

Önemli

Eğer sisteminiz hack'lenmişse, bundan tamamen kurtulmanın en güvenli yolu: sisteminizi yeniden yüklemektir.

7.3. Karantina



Karantina

BitDefender, virüs bulaşmış olan veya şüpheli dosyaların, karantina adı verilen güvenli bir alanda izole edilmelerini sağlar. Bu dosyaları karantinada izole ederek, virüs bulaşma riskini kaldırmış olursunuz ve aynı zamanda daha ileri analizlerin yapılabilmesi için bu dosyaları BitDefender laboratuarına gönderme imkanınız olur.

İzole edilmiş dosyaların yönetimini sağlayan bileşen **Karantina**'dır. Bu modül, virüs bulaşmış dosyaları BitDefender laboratuarlarına otomatik olarak göndermek amacı ile tasarlanmıştır.

Görebileceğiniz gibi, **Karantina** bölümünde, şuana kadar izole edilmiş dosyaların bir listesi vardır. Her dosyada dosyanın adı, boyutu, izole edilme tarihi ve BitDefender'a gönderildiği tarih bilgileri bulunmaktadır. Karantinaya alınmış dosyalar hakkında daha fazla bilgi almak için **Daha fazla detay**'a tıklayın.

Not

Virüs karantinadayken, zarar veremez, çünkü çalıştırılamaz veya okunmayacaktır

Virüs bulaşmış olduğundan şüphelendiğiniz bir dosyayı karantinaya eklemek için **Ekle** butonuna tıklayın. Açılan pencerede, diskdeki yarinden dosyayı seçebilirsiniz.

Bu şekilde, dosya karantinaya kopyalanır. Dosyayı karantinaya taşımak istiyorsanız, **Orijinal yerinden sil** seçeneğine karşılık gelen kutuyu işaretlemelisiniz. Şüpheli dosyaları karantinaya eklemenin daha çabuk bir yolu, bunları sürükle&bırak ile karantina listesine taşımaktır.

Karantinadan seçilen bir dosyayı silmek için **Kaldır** butonuna tıklayın. Seçilen bir dosyayı orijinal yerine geri yüklemek istiyorsanız, **Geri yükle**'yi tıklayın.

Seçilen bir dosyayı karantinadan BitDefender laboratuarına göndermek için **Gönder**'i tıklayın.

Önemli

Bu dosyaları göndermeden önce bazı bilgileri belirtmelisiniz. Bunun için **Ayarlar**'ı tıklayın ve **Gönderme ayarları** bölümündeki alanları aşağıdaki şekildeki gibi doldurun.

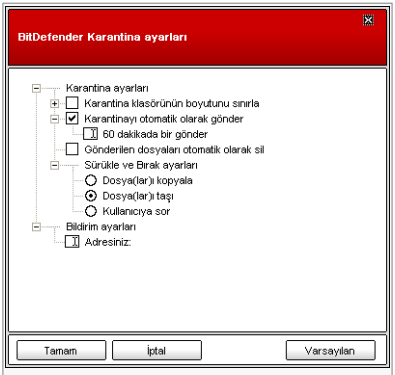
Karantina bölgesi için ileri seçenekleri açmak için Click **Ayarlar**'ı tıklayın. Yeni bir pencere görünecektir.

Karantina seçenekleri iki kategori olarak gruplanmaktadır:

- **Karantina ayarları**
- **Gönderme ayarları**

Not

Bir seçeneği açmak için "+" olan kutuyu, seçeneği kapatmak için "-" olan kutuyu tıklayın.



Karantina Seçenekleri

Karantina ayarları

- **Karantina klasörünün boyutunu sınırla** – karantinanın boyutunun kontrol altında tutulmasını sağlar. Bu seçenek varsayılan ayar olarak gelir ve boyutu 12000 kB'dir. Eğer bu değeri değiştirmek istiyorsanız, yeni değeri ilgili alana girin.

  Eski dosyaları otomatik olarak sil, seçeneğine karşılık gelen kutuyu işaretlerseniz, karantina dolduğunda ve yeni bir dosya eklendiğinde, yeni dosyalara yer açmak için karantinadaki eski dosyalar otomatik olarak silinecektir.

Not

Varsayılan olarak, karantina dosyasının boyut sınırlaması yoktur.

- **Karantinayı otomatik olarak gönder** – karantinaya alınmış dosyaları analiz edilmesi için otomatik olarak BitDefender laboratuarlarına gönderir. **Her x dakikada gönder** alanında, arka arkaya gönderme işlemleri arasındaki zamanı dakika olarak belirleyebilirsiniz.
- **Gönderilen dosyaları otomatik olarak sil** – karantinaya alınan dosyalar analiz için BitDefender laboratuarına gönderildikten sonra otomatik olarak siler.
- **Sürükle&Bırak ayarları** – karantinaya dosya eklemek için Sürükle&Bırak yöntemini kullanıyorsanız, burada işlemi belirleyebilirsiniz: Kopyala, taşı veya kullanıcıdan bilgi iste.

Gönderme ayarları

- **Adresiniz** – uzmanlardan, analiz için gönderdiğiniz şüpheli dosyalar ile ilgili e-posta mesajı almak istiyorsanız e-posta adresinizi girin.

Değişiklikleri kaydetmek için **Tamam** seçeneğine tıklayın. Eğer **Varsayılan**'ı tıklarsanız, varsayılan ayarları yükleyeceksiniz.

8. Antispyware Modülü

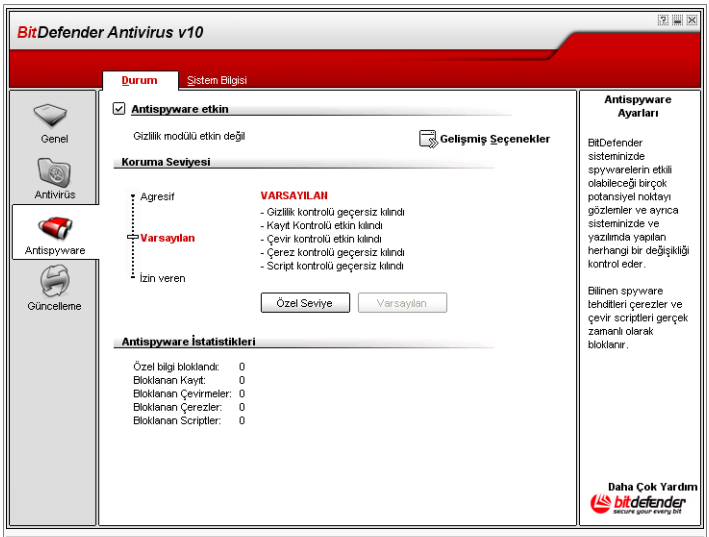
Bu kullanım kılavuzunun The **Antispyware** bölümü, aşağıdaki başlıklardan oluşmaktadır:

- Antispyware Durumu
- Gelişmiş Ayarlar - Kişisel Gizlilik Kontrolü
- İleri Ayarlar - Kayıt Kontrolü
- İleri Ayarlar - Arama Kontrolü
- İleri Ayarlar - Cookie Kontrolü
- İleri Ayarlar - Script Kontrolü
- Sistem Bilgileri

Not

Antispyware modülü ile ilgili daha detaylı bilgi için, "Antispyware Modülü" bölümüne bakın “*Antispyware Modülü*” (shf. 25).

8.1. Antispyware Durumu



Antispyware Durumu

Bu bölümde, **Davranışsal Antispyware**'i yapılandırabilir ve etkinliği ile ilgili bilgileri inceleyebilirsiniz.

Önemli

Spyware'in bilgisayarınıza virüs bulaştırmasını önlemek için, **Davranışsal Antispyware**'i etkinleştirin.

Bölümün sonunda **Antispyware İstatistikleri**'ni görebilirsiniz

Antispyware Modülü bilgisayarınızı 5 önemli koruma kontrolü ile spyware'lere karşı korur:

- Kişisel Gizlilik Kontrolü – dışarı giden tüm HTTP ve SMTP trafiğini Kişisel Gizlilik bölümünde oluşturduğunuz kurallara göre filtre ederek, kişiye özel gizli verilerinizi korur.
- Kayıt Kontrolü – bir program, Windows başlatıldığında çalıştırılmak için kayıt bilgisini değiştirmeye çalıştığında, izninizi ister.

- Arama Kontrolü – Arayıcı bir bilgisayar modemine erişmeye çalıştığında, izninizi ister.
- Cookie Kontrolü – Yeni bir web sitesi bir cookie kurmaya çalıştığında, izninizi ister.
- Script Kontrolü – Bir web sitesi bir scripti veya başka bir aktif içeriği etkinleştirmek istediğinde, izninizi ister.

Bu kontrollerin ayarlarını yapılandırmak için - Gelişmiş Ayarlar seçeneğini tıklayın.

8.1.1. Koruma Seviyesi

Koruma ihtiyaçlarınıza en uygun olan koruma seviyesini seçebilirsiniz. Uygun Koruma seviyesini belirlemek için kaydırma çubuğunu ölçek üzerinde kaydırın

3 koruma seviyesi bulunmaktadır:

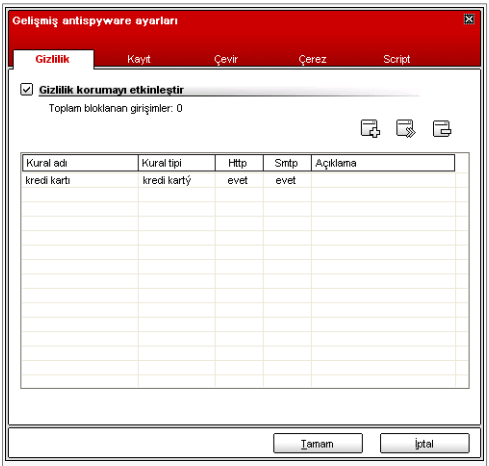
Koruma Seviyesi	Açıklama
Hoşgörülü	Sadece **Kayıt Kontrolünü** etkinleşir.
Varsayılan	**Kayıt Kontrolü** ve **Arama Kontrolünü** etkinleşir
Agresif	**Kayıt Kontrolü**, **Arama Kontrolü** ve **Kişisel Gizlilik Kontrolü** etkinleşir.

Özel Seviye seçeneğini tıklayarak, koruma seviyesini isteğinize göre özelleştirebilirsiniz. Ekranda belirecek pencereden etkinleştirmek istediğiniz Antispyware kontrollerini seçiniz ve **TAMAM**'a basınız.

Çubuğu varsayılan seviyesinekonumlamak için **Varsayılan Seviye seçeneğini tıklayın**.

8.2. Gelişmiş Ayarlar – Kişisel Gizlilik Kontrolü

Bu bölüme erişmek için, **Antispyware** modülünün Durum bölümünden **İleri Ayarlar** seçeneğini tıklayın.



Kişisel Gizlilik Kontrolü

Gizli verileri güvenli tutmak hepimizi endişenlendiren önemli bir konudur. Veri hırsızları, Internet iletişiminin gelişimine ayak uydurarak, insanları aldatıp, özel bilgileri elde edebilmek için yeni yöntemler kullanmaktadır.

İster e-postanız, ister kredi kart numaranız olsun, bu bilgiler yanlış ellere geçtiğinde size bir zarar gelmesine neden olabilir: Kendinizi spam mesajlar içinde boğuluyor vaziyette bulabilir veya boşaltılmış banka hesabınızla karşılaştığınızda şaşırabilirsiniz.

Kişisel Gizlilik Kontrolü kişiye özel gizli verilerinizi güvende tutmanıza yardımcı olur. HTTP veya SMTP trafiğini, veya her ikisini de, tanımlamış olduğunuz belirli dizgiler için tarar. Bir eşleşme bulduğunda, ilgili web sayfası veya e-posta engellenir.

Kurallar manuel olarak girilmelidir (**Ekle** seçeneğini tıklayın ve kural için parametreleri seçin). Yapılandırma sihirbazı ekrana gelecektir

8.2.1. Yapılandırma Sihirbazı

Yapılandırma sihirbazı 3 adımlı bir prosedürden oluşmaktadır.

Adım 1/3 – Kural Tipini ve Veriyi Belirle

Kural Tipini ve Veriyi Belirle

Düzenleme alanına kural ismini girin.

Aşağıda belirtilen parametreleri ayarlamanız gerekmektedir:

- **Kural Tipi** – kural tipini seçin (adres, isim, kredi kartı, PIN, SSN, vs.).
- **Kural Verisi** – Kural verisini girin

Girdiğiniz bütün veriler şifrelenecektir. Ekstra güvenlik için, korumak istediğiniz verilerin hepsini girmeyin.

İleri'yi tıklayın.

Adım 2/3 – Trafiği Seçin

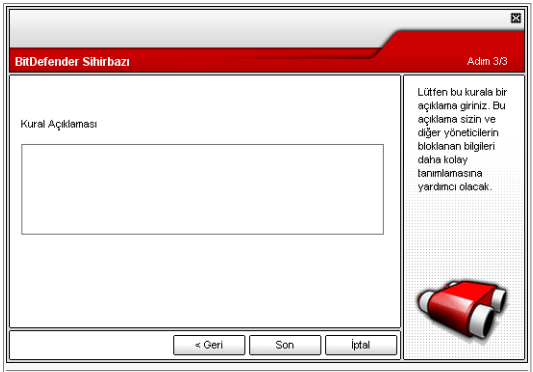
Trafiği Seç

BitDefender'ın taramasını istediğiniz trafiği seçin. Aşağıda belirtilen seçenekler mevcuttur:

- **HTTP'yi Tara**- HTTP (web) trafiğini tarar ve kural verisi ile eşleşen dışarı giden veriyi engeller.
- **SMTP'yi Tara** - SMTP (mail) trafiğini tarar ve kural verisini içeren dışarı giden e-posta mesajlarını engeller.

İleri'yi tıklayın.

Adım 3/3 – Kuralı Tanımlayın



Kural Tanımla

Düzenleme alanına, kuralın kısa bir tanımını girin.

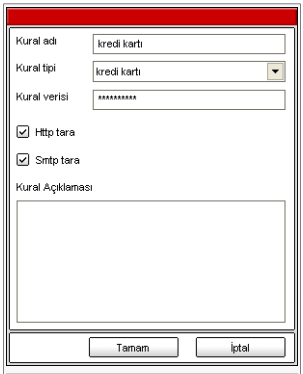
Bitir seçeneğini tıklayın.

8.2.2. Kuralları Yönetmek

Kuralın tabloda listelendiğini göreceksiniz.

Bir kuralı silmek için, sadece kuralı seçin ve **Sil** seçeneğini tıklayın. Bir kuralı silmeden, geçici olarak etkisiz kılmak için karşılık gelen onay kutusunu temizleyin.

Bir kuralı düzenlemek için, kuralı seçin ve **Düzenle** seçeneğini tıklayın veya kural üzerine çift tıklayın. Yeni pencere görünecektir.



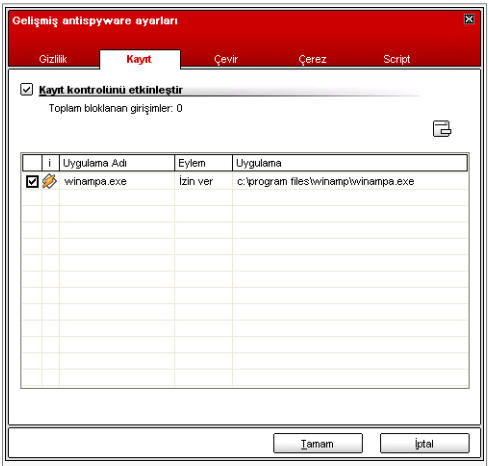
Kural Düzenle

Bu bölümde, kuralın ismini tanımını ve parametrelerini (tip, veri ve trafik) değiştirebilirsiniz. Değişiklikleri kaydetmek için **Tamam** seçeneğini tıklayın.

Değişiklikleri kaydetmek ve pencereyi kapatmak için **Tamam**'ı tıklayın.

8.3. İleri Ayarlar – Kayıt Kontrolü

Bu bölüme erişmek için, **İleri Antispyware Ayarları** penceresine girin (**Antispyware** Modülünün Durumu bölümüne gidin ve **İleri Ayarlar** seçeneğini tıklayın) ve **Kayıt** sekmesine tıklayın.

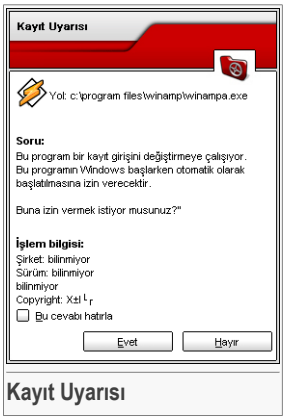


Kayıt Kontrolü

Windows işletim sisteminin en önemli kısımlarından biri **Kayıt** olarak adlandırılmaktadır. Windows; kendisi ile ilgili ayarları, yüklenmiş programları, kullanıcı bilgilerini ve bunun gibi diğer bilgileri burada tutar.

Kayıt, ayrıca Windows başlatıldığında hangi programların otomatik olarak çalıştırılacağını belirlemek için de kullanılır. Kullanıcı bilgisayarını yeniden çalıştırdığı zaman virüsler otomatik olarak başlatılmak için bunu kullanırlar.

Kayıt Kontrolü Windows'un Kaydını kontrol eder – Bu aynı zamanda Truva atları (Tojan Horses) algılamak içinde faydalıdır. Bir program, Windows başlatıldığında çalıştırılmak için kayıt bilgilerini değiştimeye çalıştığında sizi uyaracaktır.



Kayıt Uyarısı

Bu değişikliği reddetmek için **Hayır**seçeneğini tıklayabilir veya değişiklik yapılmasına izin vermek için **Evet** seçeneğini tıklayabilirsiniz.

BitDefender'ın sizin yanıtınızı hatırlaması için, **Bu yanıtı hatırla** seçeneğine karşılık gelen onay kutusunu işaretlemeniz gerekir

Not

Yanıtınız kural listesinin temelini oluşturacaktır.

Bir kayıt girişini silmek için, sadece girişi seçin ve **Sil** seçeneğini tıklayın. Bir kayıt bilgisini silmeden, geçici olarak etkisiz kılmak için karşılık gelen onay kutusunu temizleyin.

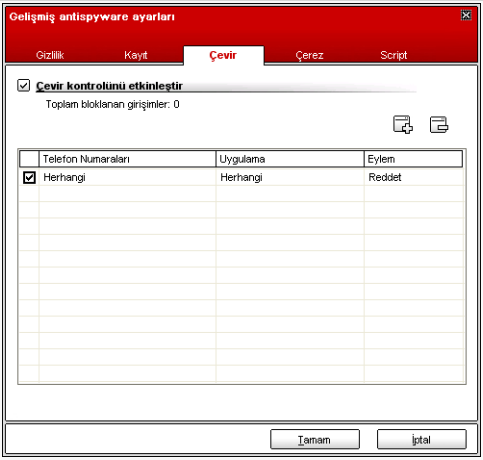
Not

Bilgisayarınızın bir sonraki başlatılmasında çalıştırılması gereken yeni programlar yüklediğinizde, BitDefender genelde sizi uyaracaktır. Çoğu durumda, bu programlar yasal ve güvenilirdir

Pencereyi kapatmak için **Tamam** seçeneğini tıklayın.

8.4. İleri Ayarlar- Arama (Dial) Kontrolü

Bu bölüme girmek için, **Antispyware İleri Ayarlara girin** (**Antispyware** Modülünün Durum bölümüne gidin ve **İleri Ayarlar**) seçeneğini tıklayın) ve **Çevir (Dial) seçeneğini tıklayın**.



Arama Kontrolü

Arayıcılar, değişik telefon numaralarını aramak için bilgisayarın modemini kullanan uygulama programlarıdır. Genel olarak arayıcılar, yüksek-maliyetli telefon numaralarını arayarak çeşitli yerlere erişmek için kullanılır.

Arama Kontrolü ile, farklı telefon numara bağlantılarından hangisine izin verileceği veya engelleneceği hakkında kontroller sizin elinizde olacaktır. Bu fonksiyon, bir bilgisayar modemine erişmeye çalışan tüm Arayıcıları izlemekte olup, kullanıcıyı derhal uyararak böyle bir işlemin yapılmasına izin vermesi veya engellemesi arasında seçim yapmasını ister:

Arama Uyarısı

Uygulama programının ismini ve telefon numarasını görebilirsiniz.

Bu yanıtı hatırla seçeneğini seçip, **Evet** veya **Hayır** seçeneğini tıklayın; kurallar tablosunda bir kural oluşturulacak, uygulanacak ve listelenecektir. Uygulama, aynı telefon numarasını daha sonra tekrar aramaya çalıştığında, artık bilgilendirilmeyeceksiniz.

Hatırlanan her kurala, daha sonra ileri ayarlar yapmak için **Arama** bölümünden erişilebilir.

Önemli

Kurallar üstten başlayarak aşağıya doğru önceliklerine göre listelenir, yani listedeki ilk kural en büyük önceliğe sahiptir. Önceliğini değiştirmek için, kuralı listedeki yerinden sürükleyerek istediğiniz yere bırakın.

Bir kuralı silmek için, sadece kuralı seçin ve **Sil** seçeneğini tıklayın. Bir kuralın parametresini değiştirmek için, alanına çift tıklayın ve istediğiniz değişikliği yapın. Bir kuralı silmeden sadece geçici olarak etkisiz kılmak için, buna karşılık gelen onay kutusunu temizleyin.

Kurallar otomatik olarak (uyarı penceresi aracılığıyla) veya elle manuel olarak girilebilirler (**Ekle** seçeneğini tıklayın ve kural için parametreleri seçin). Yapılandırma sihirbazı belirecektir.

8.4.1. Yapılandırma Sihirbazı

Yapılandırma sihirbazı iki adımlı bir prosedürden oluşmaktadır.

Adım 1/2 – Uygulamayı ve İşlemi Seçin

Uygulama ve Eylem Seçimi

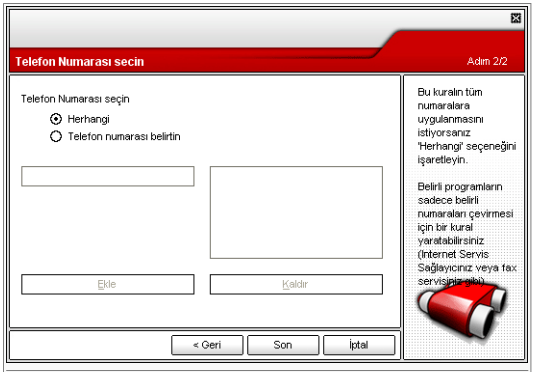
Parametreleri ayarlayabilirsiniz

- **Uygulama** – Kural için uygulamayı seçin. Sadece bir uygulamayı(Önce **Uygulamayı Seç** seçeneğini tıklayın ve daha sonra **Gözat**'la uygulamayı seçin) veya tüm uygulamaları seçebilirsiniz (sadece **Herhangi biri** seçeneğini tıklayın).
- **İşlem** – Kuralın işlemini seçin.

İşlem	Açıklama
İzin Ver	İşleme izin verilecektir.
Reddet	İşlem reddedilecektir.

İleri'yi tıklayın.

Adım 2/2 – Telefon Numaralarını Seçin



Telefon Numaralarını Seçin

Telefon Numaralarını Belirle seçeneğini tıklayın, kuralın uygulanacağı telefon numarasını girin ve **Ekle** seçeneğini tıklayın.

Not

Yasaklanan telefon numaraları için wild card kullanabilirsiniz. Örneğin, 1900* 'ın anlamı 1900 ile başlayan tüm telefon numaraları engellenecek demektir.

Bu kuralın tüm telefon numaralarına uygulanmasını istiyorsanız, **Herhangi biri** seçeneğine karşılık gelen onay kutusunu işaretleyin. Bir telefon numarasını silmek için, numarayı seçin ve **Sil** seçeneğini tıklayın.

Not

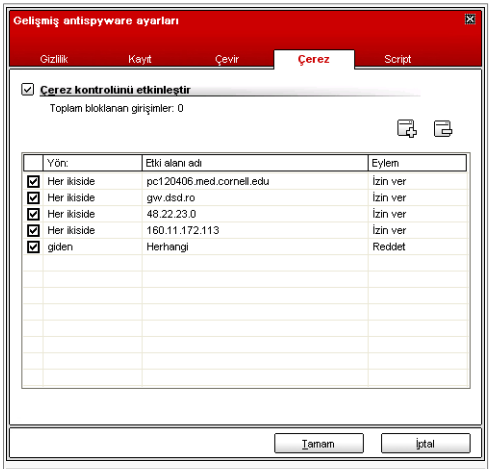
Aynı zamanda, belirli bir programın sadece belirli numaraları aramasına izin veren bir kural da oluşturabilirsiniz (Internet Hizmet Sağlayıcınızın veya faks haber servisinin numarası gibi)

Bitir seçeneğini tıklayın.

Değişiklikleri kaydetmek ve pencereyi kapatmak için **Tamam**'ı tıklayın.

8.5. İleri Ayarlar - Cookie Kontrolü

Bu bölüme girmek için, **Antispyware İleri Ayarlar**'a girin (**Antispyware** Modülünün Durum bölümüne gidin ve **İleri Ayarlar** seçeneğini tıklayın) ve **Cookie** seçeneğini tıklayın.



Cookie Kontrolü

Cookie'ler Internette çok yaygın olarak rastlanmaktadır. Bunlar, bilgisayarınıza kaydedilen küçük dosyalardır. Web siteleri, sizin hakkınızda belirli bilgileri izlemek için bu cookie'leri yaratırlar.

Cookie'ler genel olarak hayatınızı kolaylaştırmak için yaratılmışlardır. Örneğin, web sitesinin sizin isminizi ve tercihlerinizi hatırlamasına yardımcı olur ve bu sayede web sitesini her ziyaret ettiğinizde bu bilgileri tekrar girmenize gerek kalmaz.

Fakat cookie'ler aynı zamanda tarama şablonunuzu izleyerek sizin gizliliğinizden ödün vermenize neden olacak şekilde de kullanılabilir.

Cookie Kontrolü işte bu noktada size yardımcı olur. Etkinleştirildiğinde, yeni bir web sitesi bir cookie kurmak istediği zaman, **Cookie Kontrolü** sizin izninizi ister

Cookie Uyarısı

Cookie dosyası göndermeye çalışan uygulamanın ismini görebilirsiniz.

Bu yanıtı hatırla seçeneğini seçin, **Evet** veya **Hayır** seçeneğini tıklayın; kurallar tablosunda bir kural oluşturulacak, uygulanacak ve listelenecektir. Böylece, daha sonra aynı siteye bağlandığınızda artık bilgilendirilmeyeceksiniz.

Bu, hangi web sitelerine güvendiğinizi ve hangilerine güvenmediğinizi seçmeniz konusunda size yardımcı olacaktır.

Not

Günümüzde, internette çok sayıda cookie kullanıldığı için, **Cookie Kontrolü** ilk başlangıçta oldukça sıkıcı olabilir. İlk olarak, bilgisayarınıza cookie yerleştimeye çalışan siteler hakkında çok sayıda soru yöneltecektir. Kurallar listesine düzenli olarak taradığınız siteleri ekledikten sonra, internette tarama artık eskisi kadar rahat bir hale gelecektir.

Hatırlanan her kurala, daha sonra ileri ayarlar yapmak için **Cookie** bölümünden erişilebilir.

Önemli

Kurallar üstten başlayarak aşağıya doğru önceliklerine göre listelenir, yani listedeki ilk kural en büyük önceliğe sahiptir. Önceliğini değiştirmek için, kuralı listedeki yerinden sürükleyerek istediğiniz yere bırakın.

Bir kuralı silmek için, sadece kuralı seçin ve **Sil** seçeneğini tıklayın. Bir kuralın parametresini değiştirmek için, alanına çift tıklayın ve istediğiniz değişikliği yapın. Bir kuralı silmeden sadece geçici olarak etkisiz kılmak için, buna karşılık gelen onay kutusunu temizleyin.

Kurallar otomatik olarak (uyarı penceresi aracılığıyla) veya elle manuel olarak girilebilirler (**Ekle** seçeneğini tıklayın ve kural için parametreleri seçin). Yapılandırma sihirbazı belirecektir.

8.5.1. Yapılandırma Sihirbazı

Yapılandırma sihirbazı 1 adımlı bir prosedürden oluşmaktadır.

Adım 1/1 – Adres, İşlem ve Yönü Seçin

Adres, İşlem ve Yönü Seçin

Parametreleri ayarlayabilirsiniz

- **Alan addresi** – Kuralın uygulanacağı Alan adını girin.
- **İşlem** – Kuralın işlemini seçin.

İşlem	Açıklama
İzin Ver	Alandaki cookie çalışacak
Reddet	Alandaki cookie'ler çalışmayacak.

- **Yön** – trafik yönünü seçin

Tip	Açıklama
Giden	Kurallar sadece bağlanılan sitelere geri gönderilen cookie'ler için geçerli olacaktır.
Gelen	Kurallar sadece bağlanılan sitelerden alınan cookie'ler için geçerli olacaktır.
Her ikisi	Kural her iki yöndede geçerli olacaktır

Bitir seçeneğini tıklayın.

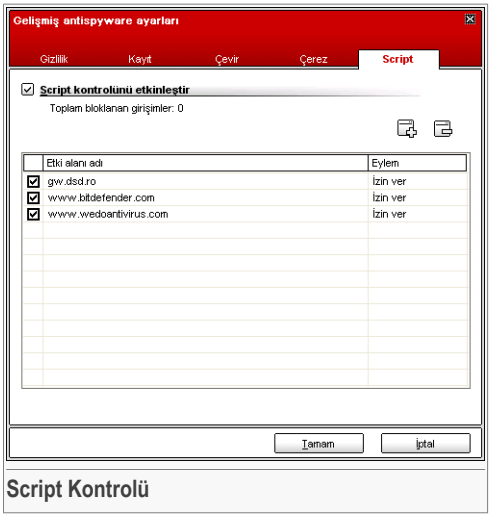
Not

Cookie'leri kabul edebilirsiniz, fakat işlemi **Reddet** ve yönü **Giden** olarak ayarlayarak asla geri gönderemezsiniz.

Değişiklikleri kaydetmek ve pencereyi kapatmak için **Tamam**'ı tıklayın.

8.6. İleri Ayarlar - Script Kontrolü

Bu bölüme girmek için, **Antispyware İleri Ayarlar**'a girin (**Antispyware** Modülünün Durum bölümüne gidin ve **İleri Ayarlar** seçeneğini tıklayın) ve **Script** seçeneğini tıklayın.



Script Kontrolü

Etkileşimli web sayfaları yaratmak için kullanılan Script ve ActiveX kontrolleri ve Java uygulamaları gibi diğer kodlar zararlı etkiler gösterecek şekilde programlanmış olabilir. Örneğin, ActiveX bileşenleri, çevrimiçi olduğunuzda verilerinize tam erişim sağlayabilir ve bilgisayarınızdaki verileri okuyabilir, bilgileri silebilir, şifreleri elde edebilir ve mesajlarınızı yakalayabilir. Bu yüzden, sadece iyi bildiğiniz ve güvendiğiniz sitelerden gelen aktif içerikleri kabul etmelisiniz.

BitDefender size bu bileşenlerin çalıştırılması veya engellenmesi konusunda seçim yapabilmenize olanak sağlamaktadır.

Script Kontrolü ile, hangi sitelere güveneceğiniz hangilerine güvenemeyeceğiniz hakkında karar verme kontrolü sizin elinizde olacaktır. BitDefender, bir web sitesi, script veya diğer aktif içerikleri etkin hale getirmeye çalıştığınızda, sizin izninizi isteyecektir:

Script Uyarısı

Kaynakların isimlerini görebilirsiniz.

Bu yanıtı hatırla seçeneğini seçip, **Evet** veya **Hayır** seçeneğini tıklayın; kurallar tablosunda bir kural oluşturulacak, uygulanacak ve listelenecektir. Bu site daha sonra size tekrar aktif bir içerik göndermeye çalıştığında artık bilgilendirilmeyeceksiniz

Hatırlanan her bir kurala daha ileri ayarlar yapmak için **Script** bölümünden erişebilirsiniz.

Önemli

Kurallar üstten başlayarak aşağıya doğru önceliklerine göre listelenir, yani listedeki ilk kural en büyük önceliğe sahiptir. Önceliğini değiştirmek için, kuralı listedeki yerinden sürükleyerek istediğiniz yere bırakın.

Bir kuralı silmek için, sadece kuralı seçin ve **Sil** seçeneğini tıklayın. Bir kuralın parametresini değiştirmek için, alanına çift tıklayın ve istediğiniz değişikliği yapın. Bir kuralı silmeden sadece geçici olarak etkisiz kılmak için, buna karşılık gelen onay kutusunu temizleyin.

Kurallar otomatik olarak (uyarı penceresi aracılığıyla) veya elle manuel olarak girilebilirler (**Ekle** seçeneğini tıklayın ve kural için parametreleri seçin). Yapılandırma sihirbazı belirecektir.

8.6.1. Yapılandırma Sihirbazı

Yapılandırma sihirbazı 1 adımlı bir prosedürden oluşmaktadır.

Adım 1/1 – Adres ve Işlemi Seçin

Adres ve Işlemi Seçin

Parametreleri ayarlayabilirsiniz

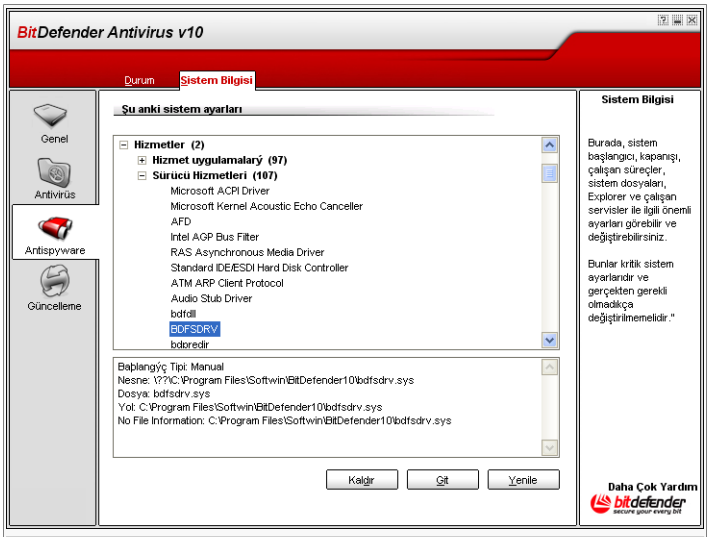
- **Alan addresi** – Kuralın uygulanacağı Alan adını girin.
- **İşlem** – Kuralın işlemini seçin.

İşlem	Açıklama
İzin Ver	Alandaki Scripts çalışacaktır.
Reddet	Alandaki Scripts çalışmayacaktır.

Bitir seçeneğini tıklayın.

Değişiklikleri kaydetmek ve pencereyi kapatmak için **Tamam**'ı tıklayın.

8.7. Sistem Bilgileri



Sistem Bilgileri

Bu bölümde anahtar bilgi ayarlarını görebilir ve değiştirebilirsiniz.

Liste, sistem çalıştırıldığında yüklenmiş olan bütün bileşenlerin yanı sıra farklı uygulamalar tarafından yüklenen bileşenleri içermektedir.

Üç buton vardır:

- **Sil** – Seçilen bileşenleri siler.
- **Git** – seçilen bileşenlerin bulunduğu bir pencere açar (Örneğin, **Kayıt**).
- **Yenile** – **Sistem Bilgi** bölümünü yeniden açar.

9. Güncelleme Modülü

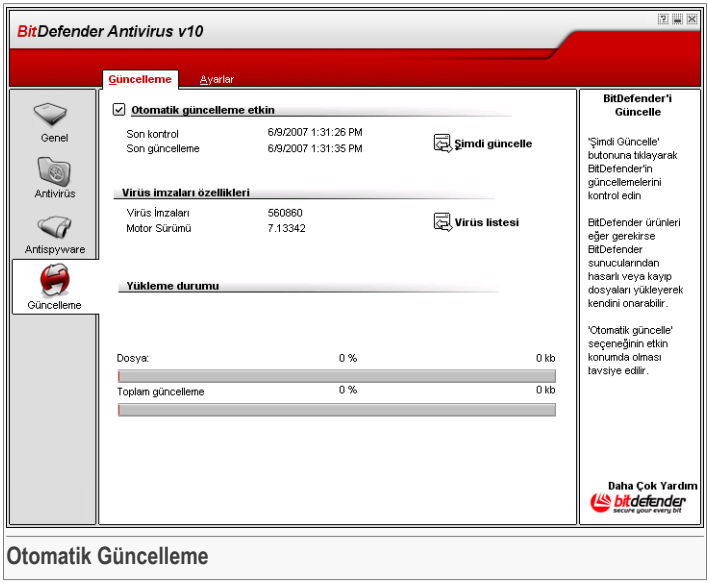
Bu kullanım kılavuzunun **Güncelleme** modülü aşağıdaki konuları içermektedir:

- Otomatik Güncelleme
- Manual Güncelleme
- Güncelleme Ayarları

Not

Güncelleme modülü ile ilgili daha detaylı bilgi için "**Güncelleme** Modülü" tanımlarına bakın. ("*Güncelleme Modülü*" (shf. 26))

9.1. Otomatik Güncelleme



Otomatik Güncelleme

Bu bölümde, güncelleme ile ilgili bilgileri görebilir ve güncelleme yapabilirsiniz

Önemli

En son tehlikelere karşı korunmak için **Otomatik Güncelleme**'yi etkin halde tutun.

Internete geniş bant veya DSL ile bağlı iseniz, BitDefender güncellemeyi kendisi yapar. Bilgisayarınızı açtığınızda ve daha sonra her **saatte bir** güncellemeleri kontrol eder.

Bir güncelleme tespit edildiğinde, Otomatik Güncelleme Seçenekleri bölümündeki seçeneklerin ayarına bağlı olarak, güncellemeyi teyit etmenizi isteyecek veya güncellemeler otomatik olarak yapılacaktır.

Şimdi Güncelle seçeneği tıklayarak otomatik güncellemeyi istediğiniz herhangi bir zamanda yapabilirsiniz. Bu güncelleme **Kullanıcı isteği** üzerine güncelleme olarak da bilinir.

Güncelleme Modülü, BitDefender Güncelleme Sunucusuna bağlanacak ve herhangi bir güncelleme varsa bunu teyit edecektir. Bir güncelleme tespit edildiğinde, Manuel Güncelleme Seçenekleri bölümündeki seçeneklerin ayarlarına bağlı olarak, güncellemeyi teyit etmeniz istenecek veya güncelleme otomatik olarak yapılacaktır.

Önemli

Güncellemeyi tamamladıktan sonra bilgisayarınızı yeniden başlatmanız gerekebilir. Bunu mümkün olan en kısa zamanda yapmanızı öneririz.

Not

Eğer internete bir çevirmeli bağlantı ile bağlıysanız, bu takdirde BitDefender'ı kullanıcı isteği ile güncellemeyi düzenli bir alışkanlık haline getirmeniz iyi bir fikir olacaktır.

BitDefender'ınızın kötü amaçlı yazılım imzalarını **Virüs Listesini Göster** seçeneğini tıklayarak görebilirsiniz. Mevcut tüm imzaları içeren bir HTML dosyası oluşturulacaktır. Listeyi görmek için **Virüs Listesini Göster** seçeneğini tekrar tıklayın. Özel bir kötü amaçlı yazılım imzasını veri tabanından arayabilir veya BitDefender imza veri tabanına gitmek için **BitDefender Virüs Listesi** seçeneğini tıklayabilirsiniz.

9.2. Manuel Güncelleme

Bu yöntem en son virüs tanımlarını yüklemenize olanak tanır. Bir ürün yükseltmesinin en son versiyonunu yüklemek için Otomatik Güncellemeyi kullanın.

Önemli

Otomatik güncellemenin yapılamadığı veya bilgisayarın internete bağlı olmadığı durumlarda manuel güncelleme yöntemini kullanın.

Manuel güncellemeyi yapabilmek için iki yol vardır:

- `weekly.exe` dosyası ile;
- `zip arşivleri` ile.

9.2.1. Weekly.exe dosyası ile manuel güncelleme

Weekly.exe güncelleme paketi her Cuma günü yayınlanır ve yayınlanma tarihine kadar mevcut olan tüm virüs tanımlarını ve tarama motorlarını içerir.

Weekly.exe dosyasını kullanarak BitDefender'ı güncellemek için aşağıda belirtilen adımları takip edin:

1. weekly.exe dosyasını indirerek, lokal olarak sabit diskinize kaydedin.
2. İndirilen dosyayı bulun ve güncelleme sihirbazını başlatmak için dosyaya çift yıklayın.
3. **İleri**'yi tıklayın.
4. **Lisans Anlaşmasındaki şartları kabul ediyorum**'u işaretleyin ve **İleri** seçeneğini tıklayın.
5. **Yükle** seçeneğini tıklayın
6. **Bitir** seçeneğini tıklayın.

9.2.2. Zip arşivleri ile Manuel Güncelleme

Güncelleme sunucusunda, tarama motorlarının ve virüs imzalarının güncellemelerini içeren iki zip arşivi bulunmaktadır: cumulative.zip ve daily.zip.

- cumulative.zip her hafta Pazartesi günleri yayınlanmakta ve yayın tarihine kadar olan tüm virüs tanımlarını ve tarama motorlarının güncellemelerini içermektedir.
- daily.zip her gün yayınlanmakta ve son cumulative yayınında o güne kadar olan tüm virüs tanımlarını ve tarama motorlarının güncellemelerini içermektedir.

BitDefender hizmete-dayalı bir mimariye sahiptir. Bu nedenle, virüs tanımlarını değiştirme işlemleri işletim sistemine bağlı olarak farklıdır.

- Windows NT-SP6, Windows 2000, Windows XP,Windows Vista.
- Windows 98, Windows Millennium.

Windows NT-SP6, Windows 2000, Windows XP, Windows Vista

Takip edilecek adımlar:

1. **Uygun güncellemeyi indir.** Eğer günlerden Pazartesi ise, lütfen cumulative.zip dosyasını indirin ve bilgi mesajı geldiğinde diskinizde herhangi bir yere kaydedin. Aksi taktirde, daily.zip dosyasını indirin ve diskinize kaydedin. Eğer ilk defa manuel güncelleme yapıyorsanız, lütfen her iki arşivi de indirin.

2. **BitDefender antivirüs korumasını durdurun.**
   - **BitDefender Yönetim Konsolundan çıkın.** Sistem tepsisinden BitDefender ikonunu sağ-tıklayın ve **Çıkış**'ı seçin.
   - **Servisleri Aç.** **Başlat**'ı tıklayın, daha sonra sırasıyla **Kontrol Panel**'ini tıklayın, sonra **Yönetim Araçlar**'ını çift tıklayın ve daha sonra da **Servisler**'i tıklayın.
   - **BitDefender Virüs Kalkanı Servisini Durdur.** Listeden **BitDefender Virüs Kalkanı** servisini seçin ve **Durdur** seçeneğini tıklayın.
   - **BitDefender Tarama Sunucusu Servisini Durdur.** Listeden **BitDefender Tarama Sunucusu** servisini seçin ve **Durdur** seçeneğini tıklayın.
3. **Arşiv içeriğini kopyala.** Her iki güncelleme arşivi de mevcutsa, önce `cumulative.zip` ile başlayın. `C:\Program Fiies\commonFiles\Softwin\BitDefender Scan Server\Plugins\` klasörü içindeki içeriği kopyalayın ve var olan dosyaların üzerine yazmayı kabul edin.
4. **BitDefender antivirüs korumasını tekrar başlatın.**
   - **BitDefender Tarama Sunucusu Servisi'ni Başlat.** Listeden **BitDefender Tarama Sunucusu** servisini seçin ve **Başlat** seçeneğini tıklayın.
   - **BitDefender Virüs Kalkanı servisini başlat.** **Listeden BitDefender Virüs Kalkanı** servisini seçin ve **Başlat** seçeneğini tıklayın.
   - **BitDefender Yönetim Konsolunu Açın.**

Not

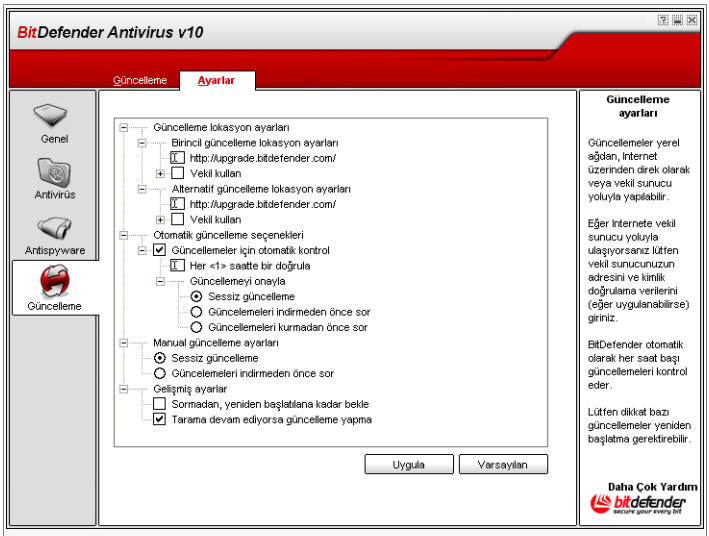
Eğer Windows Vista kurumuşsanız, bu işlemlerin çoğunu onaylamanız için sorulacaktır.

Windows 98, Windows Millennium

Takip edilecek adımlar:

1. **Uygun güncellemeyi indir.** Eğer günlerden Pazartesi ise, lütfen cumulative.zip dosyasını indirin ve bilgi mesajı geldiğinde diskinizde herhangi bir yere kaydedin. Aksi taktirde, daily.zip dosyasını indirin ve diskinize kaydedin. Eğer ilk defa manuel güncelleme yapıyorsanız, lütfen her iki arşivi de indirin.
2. **Arşiv içeriğini kopyala.** Her iki güncelleme arşivi de mevcutsa, önce `cumulative.zip` ile başlayın. `C:\Program Fiies\commonFiles\Softwin\BitDefender Scan Server\Plugins\` klasörü içindeki içeriği kopyalayın ve var olan dosyaların üzerine yazmayı kabul edin.
3. **Bilgisayarı yeniden başlatın.**

9.3. Güncelleme Ayarları



Güncelleme Ayarları

Güncellemeler, yerel ağda, internet üzerinden direkt olarak veya vekil Sunucu üzerinden yapılabilir.

Güncelleme ayarlarının bulunduğu pencere 4 seçenek kategorisi (**Güncelleme Yer Ayarları** , **Otomatik Güncelleme Seçenekleri**, **Manuel Güncelleme Ayarları** ve **İleri Seçenekler**) içermekte olup, Windows'dakilere benzer şekilde genişleyen menüler halinde düzenlenmiştir.

Not

Bir kategoriyi açmak için "+" işaretli kutuyu veya kapatmak için "-" işaretli kutuyu tıklayın.

9.3.1. Güncelleme Yeri Ayarları

Daha güvenilir ve hızlı bir güncelleme için, iki güncelleme yeri yapılandırabilirsiniz: biri **Ana Güncelleme Yeri** ve diğeri **Alternatif Güncelleme Yeri**'dir. Her ikisi için de aşağıdaki seçenekleri yapılandırmalısınız:

- **Güncelleme Yeri** – BitDefender virüs imzalarının lokal olarak bulunduğu bir yerel ağa bağlı iseniz, burada güncelleme yerini değiştirebilirsiniz. Bu, varsayılan olarak: http://upgrade.bitdefender.com'dur
- **Vekil Kullan** – Şirketin bir vekil sunucu kullanıyor olması durumunda, bu seçeneği işaretleyin. Aşağıda belirtilen ayarların tanımlanması gerekmektedir:
  - **Vekil Ayarları** – IP veya vekil sunucunun ismini ve BitDefender'ın vekil sunucuya bağlanmak için kullandığı portu girin.

    Önemli

    Söz Dizimi: `isim:port` veya `ip:port`.

  - **Vekil Kullanıcısı** – Vekil tarafından kabul edilen bir kullanıcının ismini girin.

    Önemli

    Söz dizimi: `domair\user`.

  - **Vekil şifresi** – daha önce tanımlanan kullanıcı için geçerli bir şifre girin.

9.3.2. Otomatik Güncelleme Seçenekleri

- **Güncellemeler için Otomatik Kontrol Et** - BitDefender mevcut güncellemeler için otomatik olarak sunucunuzu kontrol eder.
- **Her x saatte bir teyit et** – BitDefender'ın hangi sıklıkla güncelleme kontrolü yapacağını belirler. Varsayılan zaman aralığı 1 saattir.
- **Sessiz Güncelleme** - BitDefender güncellemeyi otomatik olarak indirir ve uygular.
- **İndirmeden önce sor** – güncellemenin her bulunuşunda, indirmeden önce sizi uyaracaktır.
- **Yüklemeden önce sor** – güncellemenin her indirilişinde, yüklemeden önce sizi uyaracaktır.

Önemli

Eğer **İndirmeden önce sor** veya **Yüklemeden önce sor** seçeneğini seçer, Yönetim Konsolunu kapatıp çıkarsanız, otomatik güncelleme yapılmayacaktır.

9.3.3. Manuel Güncelleme Ayarları

- **Sessiz Güncelleme** – manuel güncelleme arka planda otomatik olarak yapılacaktır.
- **İndirmeden önce sor** – her manuel güncelleme yaptığınızda, güncellemeler indirilmeden ve yüklenmeden önce uyarılacaksınız.

Önemli

Eğer **İndirmeden önce sor** seçeneğini seçer, Yönetim Konsolunu kapatıp çıkarsanız, otomatik güncelleme yapılmayacaktır.

9.3.4. İleri Seçenekler

- **Uyarı yerine, yeniden başlatma için bekle** - Eğer bir güncelleme bilgisayarın yeniden başlatılmasını gerektiriyorsa, sistem tekrar başlatılana kadar ürün eski dosyalar ile çalışmaya devam edecektir. Kullanıcıya sistemin yeniden başlatılması bilgisi verilmeyecek ve bu nedenle BitDefender güncelleme süreci, kullanıcının çalışmasını engellemeyecektir.
- **Eğer tarama çalıştırılıyorsa, güncelleme yapma** - Eğer bir tarama işlemi çalışıyorsa, BitDefender güncelleme yapmayacaktır. Bu şekilde, BitDefender güncelleme süreci tarama işlemlerini engellemeyecektir

Not

Tarama çalışırken BitDefender güncellenirse, tarama işlemi yarıda kesilecektir.

Değişiklikleri kaydetmek için **Uygula** seçeneğini tıklayın veya varsayılan ayarları yüklemek için **Varsayılan** seçeneğini tıklayın.

En İyi Uygulamalar

10. En İyi Uygulamalar

Bu kullanım kılavuzunun **En İyi Uygulamalar**, bölümü aşağıdaki başlıklardan oluşmaktadır:

- Kötü amaçlı yazılım tehditlerine karşı bilgisayarınız nasıl korunur?
- Bir tarama görevi nasıl yapılandırılır?

10.1. Kötü amaçlı yazılım tehditlerine karşı bilgisayarınız nasıl korunur?

Bilgisayarınızı virüslere,spywarelere ve diğer kötü amaçlı yazılım tehditlerine karşı korumak için bu adımları takip edin:

1. **Başlangıç ayarı sihirbazını tamamlayın.** Yükleme işlemi esnasında bir sihirbaz belirecek ve ücretsiz sağlanan teknik destekten faydalanabilmeniz için BitDefender'ı kaydettirmenize ve bir BitDefender hesabı açmanıza yardımcı olacaktır. Aynı zamanda, önemli güvenlik görevlerinin yerine getirilmesi için BitDefender'ı ayarlamanıza da yardımcı olacaktır.

   Önemli

   Eğer bir BitDefender Kurtarma CD'niz varsa, sisteminizde halihazırda kötü amaçlı yazılım bulunmadığından emin olmak için, BitDefender'ı yüklemeden önce sisteminizi tarayın.

2. **BitDefender'ı Güncelleyin.** Yükleme işlemi esnasında başlangıçtaki yapılandırma sihirbazını tamamlamadıysanız, bir kullanıcı talebine göre güncelleme işlemi yapın (**Güncelleme modülünün** Güncelleme bölümüne girin ve **Şimdi Güncelle** seçeneğini tıklayın).
3. **Tam sistem taraması yapın. Antivirüs** modülünün Kalkan bölümüne girin ve **Şimdi Tara** seçeneğini tıklayın.

   Not

   Tam sistem taramasını Tarama bölümünden de yapabilirsiniz. **Tam sistem taraması** görevini seçin ve **Görevi Başlat** seçeneğini tıklayın.

4. **Bulaşmayı Önle.** Virüs, spyware ve diğer kötü amaçlı yazılımlara karşı korunma sağlanması için, **Kalkan** bölümündeki gerçek-zamanlı korumayı etkin durumda

tutun.Koruma seviyesini ihtiyaçlarınızı en iyi karşılayacak şekilde ayarlayın. Özel Seviye seçeneğini tıklayarak istediğiniz zaman özelleştirebilirsiniz

Önemli

Tarama bölümünden **Tam Sistem Tarama** işlemini programlayarak BitDefender'ı sisteminizi haftada en az bir kere tarayacak şekilde programlayın.

5. **BitDefender'ınızı güncel tutun.** En son tehlikelere karşı koruma sağlamak için, **Güncelleme** modülünün Güncelleme bölümünde, **Otomatik Güncellemeyi** etkin durumda tutun.
6. **Bir Tam Sistem Taraması görevi programlayın. Tarama** bölümüne gidin ve **Tam Sistem Taraması** görevi programlayarak BitDefender'ın sisteminizi haftada en az bir kere taraması için programlayın

10.2. Bir Tarama Görevi Nasıl Yapılandırılır

Bir tarama görevi oluşturmak ve yapılandırmak için aşağıda belirtilen adımları takip edin:

1. **Yeni bir görev oluşturun.** Tarama bölümüne gidin ve **Yeni Görev** seçeneğini tıklayın. Özellikler penceresi belirecektir

Not

Ayrıca, halihazırda mevcut olan bir görevi kopyalayarak da yeni bir görev oluşturabilirsiniz. Bunu yapmak için, bir görevi sağ-tıklayın ve kısayol menüsünden **Kopyala** seçeneğini seçin. **Özellikler** penceresinin açılması için, çoğaltılan kopyayı çift tıklayın.

2. **Tarama seviyesini belirleyin.** Tarama seviyesini belirlemek için **Genel** bölümüne gidin. Eğer isterseniz, tarama ayarlarını Özelleştir seçeneğini tıklayarak özelleştirebilirsiniz.
3. **Tarama hedefini belirleyin. Tarama Yolu** bölümüne gidin ve taranmasını istediğiniz nesneleri seçin.
4. **Görevi Programlayın.** Eğer tarama görevi karmaşıksa, bilgisayarınız bekleme modundayken çalışması için daha sonraya programlamanız gerekebilir. Bu BitDefender'ın sisteminizi hassas bir şekilde taramasına yardımcı olacaktır. Görevi zamanlamak için **Zamanlayıcı** bölümüne gidin

BitDefender Kurtarma CD'si

BitDefender Antivirus v10, işletim sisteminiz başlamadan önce tüm mevcut sabit diskleri tarayacak ve temizleyecek nitelikte bir başlangıç CD'si ile birlikte gelmektedir (BitDefender Kurtarma CD'si LinuxDefender tabanlıdır).

BitDefender Kurtarma CD'sini, virüs bulaşması nedeniyle işletim sisteminizin düzgün olarak çalışmadığı durumlarda kullanmalısınız. Bu durum, çoğu zaman bir virüs koruma programı kullanılmadığı takdirde ortaya çıkar.

Virüs imzalarının güncellenmesi, BitDefender kurtarma CD'sini her başlattığınızda kullanıcı müdahelesine gerek kalmadan otomatik olarak yapılır.

LinuxDefender, BitDefender ile yeniden yapılandırılmış bir Knoppix dağıtımı olup, Linux güvenlik çözümü için yaratılan en son BitDefender versiyonunu GNU/Linux Knoppix Live CD ile entegre ederek, kullanımı kolay SMTP virüs koruma/antispam koruma sağlayan ve mevcut sabit diskleri (Windows NTFS ana bellek kesimleri dahil), Samba/Windows paylaşımlarını veya NFS yükleme noktalarını tarayan ve temizleyen bir masaüstü virüs koruma yazılım paketi sunmaktadır. BitDefender çözümlerine ulaşmak için Web tabanlı bir yapılandırma arayüzü de pakete dahil edilmiştir.

11. Tanıtma

Yeni Özellikler

- Anında e-posta koruması (Virüs koruma ve Antispam)
- Sabit disklerinizin Virüs koruma çözümleri
- NTFS yazma desteği (Captive project kullanan)
- Windows Xplerdeki virüs bulaşmış dosyaların temizlenmesi

11.1. KNOPPIX Nedir?

http://knopper.net/knoppix sitesinden alıntı:

" KNOPPIX is a bootable CD with a collection of GNU/Linux (http://www.linux.com/) software, automatic hardware detection, and support for many graphic cards, sound cards, SCSI and USB devices and other peripherals. KNOPPIX can be used as a Linux demo, educational CD, rescue system, or adapted and used as a platform for commercial software product demos. It is not necessary to install anything on a hard disk. "

11.2. Sistem Gereksinimleri

LinuxDefender'ı başlatmadan önce, ilk olarak sisteminizin aşağıda belirtilen gereksinimleri karşılayıp karşılamadığını teyit etmeniz gerekmektedir

İşlemci tipi

x86 uyumlu, minimum 166 MHz, fakat bu durumda mükemmel bir performans beklenmemelidir. 800MHz, i686 nesil bir işlemci daha iyi bir seçim olacaktır.

Bellek

Kabul edilebilir minimum değer 64MB olup, daha iyi bir performans için 128 MB önerilir.

CD-ROM

LinuxDefender bir CD-ROM'dan çalıştırılır. Bu nedenle, bir CD-ROM ve başlatılabileceği bir BIOS gerekmektedir.

Internet bağlantısı

LinuxDefender internet bağlantısı olmadan da çalışabilmesine rağmen, güncelleme işlemleri için, bir vekil sunucu üzerinden olsa bile faal bir HTTP bağlantısı

gerekmektedir. Bu yüzden, güncel bir koruma için internet bağlantısı, bir GEREKLİLİKTİR.

Grafik çözünürlüğü

Web-tabanlı yönetim için en az 800x600 grafik çözünürlük olması tavsiye edilir.

11.3. Dahil edilen Yazılımlar

BitDefender Kurtarma CD'si aşağıda belirtilen yazılım paketlerini içermektedir.

- BitDefender SMTP Proxy (Antispam & Virüs koruma)
- BitDefender Uzaktan Yönetim (web-tabanlı yapılandırma)
- BitDefender Linux Edition (virüs koruma tarayıcı) + GTK Arayüzü
- BitDefender Dokümantasyonu (PDF & HTML formatında)
- BitDefender Ekstralar (Artwork, Broşürler)
- Linux-Kernel 2.6
- Captive NTFS write project
- LUFS - Linux Userland Dosya Sistemi
- Veri kurtarma ve sistem onarım araçları (hatta diğer işletim sistemleri için bile)
- Ağ yöneticileri için, ağ ve güvenlik analiz araçları
- Amanda yedekleme çözümü
- thttpd
- Ethereal ağ trafik analizörü, IPTraf IP LAN Monitörü
- Nessus ağ güvenliği denetliyicisi
- Parted, QTParted ve partimage, bölümleme yeniden boyutlama, kaydetme & kurtarma çözümü
- Adobe Acrobat Reader
- Mozilla Firefox Web browser

11.4. BitDefender Linux Güvenlik Çözümleri

LinuxDefender CD'si; Linux için BitDefender SMTP Vekil Virüs koruma/Antispam yazılımı, BitDefender Uzaktan Yönetim yazılımı (BitDefender SMTP Proxy'i yapılandırmak için web-tabanlı bir arayüz) ve BitDefender Linux Edition isteğe bağlı virüs koruma tarayıcı içermektedir.

11.4.1. BitDefender SMTP Proxy

Linux Posta Sunucuları için BitDefender - SMTP Proxy güvenli içeriğe sahip, bilinen ve bilinmeyen kötü amaçlı yazılımlar için tüm e-posta trafiğini tarayarak ağ geçidi seviyesinde virüs koruma ve antispam koruma sağlayan bir denetleme çözümüdür.

Eşsiz tescilli teknolojisi sayesinde, Posta Sunucusu için BitDefender mevcut e-posta platformlarının çoğu ile uyumlu olup, "RedHat Ready" sertifikasına sahiptir.

Bu Virüs koruma ve Antispam çözümü; platform ve işletim sistemine bağlı olmaksızın, mevcut tüm posta sunucuları için e-posta trafiğini taramakta, temizlemekte ve filtrelemektedir. BitDefender SMTP Proxy başlangıçta çalıştırılır ve gelen e-posta trafiğinin tümünü tarar. BitDefender SMTP Proxy'i yapılandırmak için aşağıda belirtilen talimatları takip ederek BitDefender Uzaktan Yönetim modülünü kullanın.

11.4.2. BitDefender Uzaktan Yönetim

BitDefender hizmetlerini, aşağıda belirtilen adımları takip ederek uzaktan yapılandırabilir ve yönetebilirsiniz (ağınızı yapılandırdıktan sonra):

1. 1. Firefox tarayıcıyı başlatın ve BitDefender Uzaktan Yönetimi yükleyin. URL:https://localhost:8139(veya masaüstü bilgisayarınızdan BitDefender Uzaktan Yönetim ikonunu çift tıklayın)
2. "bd" kullanıcı ve "bd" şifresi ile giriş yapın
3. Sol-taraftaki menüden "SMTP Proxy" seçeneğini seçin
4. Real SMTP sunucuyu ve dinleme portunu ayarlayın
5. Posta aktarımı için e-posta alanlarını (domain) ekleyin
6. Aktarım için ağ alanlarını ekleyin.
7. Antispam olanaklarını yapılandırmak için, sol taraftaki menüden "AntiSpam" seçeneğini seçin
8. BitDefender Virüs koruma işlemleri için (virüs bulunduğunda ne yapılması gerektiğini, karantina dizinini) "AntiVirus" seçeneğini seçin
9. Ayrıca, "Posta Bildirimleri" ve kayıt olanaklarını da ("Logger") yapılandırabilirsiniz

11.4.3. BitDefender Linux Edition

LinuxDefender ile birlikte sunulan virüs koruma tarayıcısı direkt olarak masaüstüne entegre edilir. Bu versiyonun GTK+ grafik arayüz özellikleri bulunmaktadır.

Sabit diskinizi (veya yüklenmiş uzak paylaşımları) tarayarak, herhangi bir dosya veya klasörü sağ-tıklayın ve "BitDefender ile Tara" seçeneğini seçin. BitDefender Linux Edition seçilen kayıtları tarayacak ve bir durum raporu görüntüleyecektir. Hassas ayarlı seçenekler için BitDefender Linux Edition dokümantasyonuna (BitDefender Dokümantasyon klasörü veya Kılavuz sayfası) ve **/opt/BitDefender/lib/bdc** programına bakın.

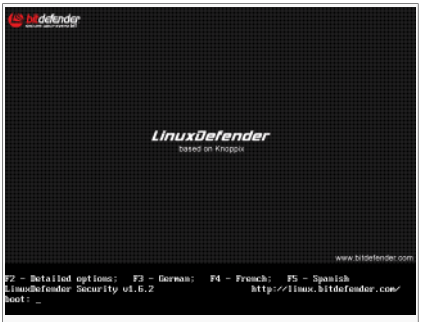
12. LinuxDefender Nasıl?

12.1. Başlatma ve Durdurma

12.1.1. LinuxDefender'ın Başlatılması

CD'yi başlatmak için, bilgisayarınızın BIOS'unu CD'yi yükleyecek şekilde ayarlayın, CD'yi sürücüye yerleştirin ve bilgisayarı yeniden başlatın. Bilgisayarınızın CD'den ön yükleme yapabileceğinden emin olun.

Bir sonraki ekran belirene kadar bekleyin ve LinuxDefender'ı çalıştırmak için ekrandaki talimatları takip edin.



Boot Splash Ekranı

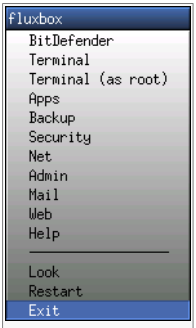
Seçeneklerin detayı için F2'ye basın. Almanca dilinde seçenek detayları için F3'e basın. Fransızca dilinde seçenek detayları için F4'e basın. İspanyolca seçenek detayları için F5'e basın. Varsayılan seçeneklerle hızlı başlatma için sadece ENTER tuşuna basın.

Ön yükleme işlemi tamamlandıktan sonra bir sonraki masaüstünü göreceksiniz. Artık LinuxDefender'ı kullanmaya başlayabilirsiniz.

Masaüstü

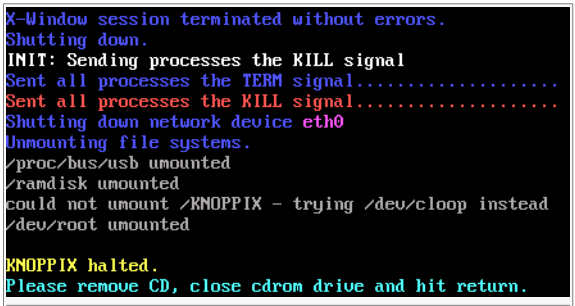
12.1.2. LinuxDefender'i Durdur

LinuxDefender'dan düzgün şekilde çıkmak için, **unmount** komutunun kullanılarak tüm yüklü kısımların kapatılması veya masaüstündeki ikonunların sağ-tıklanıp **unmount** komutunun seçilerek kapatılması önerilir. Daha sonra, LinuxDefender menüsünden **Çık** seçeneğini seçerek veya bir terminalde **halt** komutu vererek bilgisayarınızı güvenli bir şekilde kapatabilirsiniz..



"ÇIKIŞ"'ı seçiniz

LinuxDefender tüm programları başarılı bir şekilde kapattığında, aşağıdaki gibi bir ekran görünecektir. Bilgisayarınızı sabit diskinizden başlatmak için CD'yi sürücüden çıkartabilirsiniz. Şimdi bilgisayarınızı kapatabilir veya yeniden başlatabilirsiniz



Kapanırken bu mesaj için bekleyin

12.2. Internet Bağlantısının Yapılandırılması

Bir DHCP ağı içindeyseniz ve bir ethernet kartınız varsa, internet bağlantısının zaten algılanmış ve yapılandırılmış olması gerekir. Manuel bir yapılandırma için aşağıda belirtilen adımları takip edin.

1. LinuxDefender menüsünü açın (sağ-tıkla) ve bir konsol açmak için **Terminal**'i seçin
2. Ağ yapılandırma araçlarını başlatmak için, açık terminalde **netcardconfig** yazın.
3. Ağınız DHCP kullanıyorsa, **Evet**'i seçin (emin değilseniz, ağ yöneticinize sorun). Aksi takdirde aşağıda belirtilenlere bakın
4. Ağ bağlantısının şimdi otomatik olarak yapılandırılmış olması gerekir. **ifconfig** komutu ile IP ve ağ kart ayarlarınızı görebilirsiniz
5. Eğer statik bir IP adresiniz varsa (DHCP kullanmıyorsunuz demektir), DHCP sorusunda **Hayır**'ı seçin
6. Ekrandaki talimatları takip edin. Eğer ne yazmanız gerektiğinden emin değilseniz, detaylı bilgi için sistem veya ağ yöneticiniz ile temasa geçin.

Eğer herşey yolunda giderse, `bitdefender.com`'u pingleyerek internet bağlantınızı test edebilirsiniz:

```
$ ping -c 3 bitdefender.com
```

Eğer çevirmeli bir bağlantı kullanıyorsanız, LinuxDefender/Admin menüsünden **pppconfig** seçeneğini seçin. Daha sonra, bir PPP internet bağlantısı kurmak için ekrandaki talimatları takip edin.

12.3. BitDefender Güncelleme

LinuxDefender için BitDefender paketleri, güncellenebilen dosyalar için sistemin ram diskini kullanır. Bu şekilde, LinuxDefender CD'si gibi salt okunur bir medyadan sistemi çalıştırıyor olsanız bile, tüm virüs imzalarını, tarama motorlarını veya antispam veri tabanlarını güncelleyebilirsiniz

Çalışan bir internet bağlantınız olduğundan emin olun. Önce, BitDefender Uzaktan Yönetimi açın ve Sol taraftaki menüden **Canlı! Güncelle** seçeneğini seçin. Yeni güncellemelerin olup olmadığını kontrol etmek için, **Şimdi Güncelle** seçeneğine tıklayın.

Alternatif olarak, bir sonraki komutu terminalde verebilirsiniz

```
# /opt/BitDefender/bin/bd  update
```

Tüm güncelleme işlemleri, varsayılan BitDefender kaydına kaydedilmektedir. Bunu bir sonraki komut ile izleyebilirsiniz.

```
# tail  -f /ramdisk/BitDefender/var/log/bd.log
```

Giden bağlantılar için bir vekil sunucu kullanıyorsanız, **Canlı! Güncelleme** menüsü içinde **Yapılandırma** Sekmesini seçerek vekil ayarlarını yapılandırın.

12.4. Virüs Tarama

12.4.1. Windows verilerime nasıl erişebilirim?

NTFS Yazma desteği

Captive NTFS write project'i kullanan NTFS yazma desteği bulunmaktadır. Windows kurulumunuzdan iki sürücü dosyasına ihtiyacınız vardır: `ntoskmi.exe` ve `ntfs.sys`. Şu anda, sadece Windows XP sürücüleri desteklenmektedir. Bunları aynı zamanda Windows 2000/NT/2003 bellek kesimlerine erişebilmek için de kullanabileceğinizi unutmayın.

NTFS Sürücülerinin Yüklenmesi

NTFS Windows bölümlemelerinize erişmek ve bunlar üzerine veri yazabilmek için, önce NTFS sürücülerini yüklemeniz gerekmektedir. Windows bölümlemeleriniz için

NTFS yerine FAT kullanıyorsanız veya verilerinize salt okunur erişim istiyorsanız, sürücüleri direkt olarak yükleyebilir ve Windows sürücülerine herhangi bir Linux sürücü gibi erişebilirsiniz.

NFTS bölümlemeleri için destek eklemek için, önce sabit disklerinizden, uzak paylaşımlardan, USB çubukları veya Windows'dan NTFS sürücülerini yüklemeniz gerekmektedir. Bilinen-güvenli bir yerden alınan sürücüleri kullanmanız önerilir. Çünkü, Windows ana bilgisayarından alınan lokal sürücüler virüslü veya bozuk olabilir.

BitDefender Captive NTFS Installer'ı çalıştırmak için, **NTFS Yazma Sürücülerini Yükle** masaüstü ikonunu çift-tıklayın. Sürücüleri yerel sabit diskten yüklemek istiyorsanız ilk seçeneği seçin.

Eğer sürücüler ortak kullanılan bir yerdeyseler, sürücüleri bulmak için **Hızlı Arama**'yı kullanın.

Sırasıyla, sürücülerinizin nerede bulunabileceğini belirleyebilir veya sürücüleri Windows Güncelleme SP1'den indirebilirsiniz

Sürücüler sabit diske yüklenmezler, fakat geçici olarak LinuxDefender tarafından Windows NTFS bölümlemelerine erişmek için kullanılırlar. Eğer program NTFS sürücülerini yüklerse, masaüstü NTFS bölümleme ikonunu çift-tıklayabilir ve içeriği tarayabilirsiniz. Güçlü bir dosya yöneticisi için, LinuxDefender menüsünden Midnight Commander'ı kullanın (veya bir konsolda **mc** yazın).

12.4.2. Bir virüs koruma taraması nasıl yapabilirim?

Klasörlerinize gözatın, bir dosya veya klasörü sağ-tıklayın ve **Gönder** seçeneğini seçin. Sonra, **BitDefender Tarayıcıyı** seçin.

Veya bir sonraki komutu bir kaynak olarak (root) terminalde verebilirsiniz. **BitDefender Virüs koruma Tarayıcı**, varsayılan tarama yeri olarak seçilen dosya veya klasör ile başlayacaktır.

```
# /opt/BitDefender/bin/bdgtk2 /path/to/scan/
```

Daha sonra **Taramayı Başlat**'a tıklayın.

Virüs koruma seçeneklerini yapılandırmak isterseniz, programın sol panelinden **Virüs korumasını Yapılandır** sekmesini seçin.

12.5. Anlık Posta Filteleme Toaster'ın Oluşturulması

LinuxDefender'ı herhangi bir yazılım yüklemeden veya posta sunucusunu değiştirmeden amaca uygun bir posta filtreleme çözümü oluşturmak için kullanabilirsiniz. Bunun

amacı, bir LinuxDefender sistemini posta sunucunuzun önüne koyarak, BitDefender'ın tüm SMTP trafiğini spam ve virüs için taramasını ve trafiği gerçek posta sunucusuna aktarmasını sağlamaktır.

12.5.1. Ön Gereksinimler

Pentium 3 uyumlu veya daha üst kapasitede işlemcisi olan bir PC, en az 256 MB RAM ve yükleme yapabileceğiniz bir CD/DVD sürücüsüne ihtiyacınız olacaktır. Gerçek posta sunucusu yerine, SMTP trafiğini LinuxDefender sisteminin alması gerekecektir. Bu ayarları yapmak için çeşitli yöntemler mevcuttur.

1. Gerçek posta sunucunuzun IP adresini değiştirin ve bu eski IP adresini LinuxDefender sisteminize atayın
2. Alanlarınızın MX kaydı LinuxDefender sistemini işaret edecek şekilde, DNS kayıtlarınızı değiştirin.
3. E-posta istemcilerinizi, Yeni LinuxDefender sistemini SMTP sunucusu olarak kullanacak şekilde ayarlayın.
4. Güvenlik duvarı ayarlarınızı, tüm SMTP bağlantılarını gerçek posta sunucusu yerine LinuxDefender'a gönderecek/yeniden yönlendirecek şekilde değiştirin

LinuxDefender Nasıl, yukarıdaki konuların hiç birini açıklamayacaktır. Daha fazla bilgi için Linux Ağ Oluşturma Kılavuzlarına ve Netfiltre dokümantasyonuna başvurabilirsiniz.

12.5.2. E-posta Toaster

LinuxDefender CD'nizi yükleyin ve XWindow sistemi tamamen yüklenene ve işlevsel hale gelene kadar bekleyin.

BitDefender SMTP Vekil Sunucuyu yapılandırmak için, masaüstünden **BitDefender Uzaktan Yönetim** ikonunu çift-tıklayın. Ekranda aşağıdaki pencere görüntülenecektir. `bd kullanıcı ismi` ve `bd` şifresini kullanarak BitDefender Uzaktan Yönetime giriş yapın.

Başarılı bir girişten sonra, BitDefender SMTP Vekil Sunucuyu artık yapılandırabilirsiniz.

Spam ve virüslere karşı korumak istediğiniz gerçek posta sunucusunu yapılandırmak için, **SMTP Vekil Sunucu** seçeneğini seçin.

E-posta almak istediğiniz tüm e-posta alanlarını eklemek için **E-posta Alanları** sekmesini seçin.

E-posta Alanı Ekle veya **Toplu Alanları Ekle** tuşuna basın ve e-posta aktarma alanlarını tanımlamak için ekrandaki talimatları takip edin.

E-posta aktarmak istediğiniz tüm ağları girmek için **Ağ Alanları** sekmesini seçin.

Ağ Alanı Ekle veya **Toplu Ağ Alanlarını Ekle** tuşuna basın ve ağ aktarma alanlarını tanımlamak için ekrandaki talimatları takip edin.

Bir virüs bulunduğu zaman ne yapılacağını seçmek ve diğer virüs koruma seçeneklerini yapılandırmak için, sol taraftaki menüden t **Virüs koruma** seçeneğini seçin.

Artık tüm SMTP trafiği BitDefender tarafından taranıp filtrelenmektedir. Standart olarak, tüm virüslü mesajlar temizlenmekte veya atılmakta ve BitDefender tarafından algılanan tüm spam mesajlar konu satırlarına `[SPAM]` kelimesi girilerek işaretlenmektedir. İstemci-tarafı filtrelemeyi kolaylaştırmak için, tüm e-postalara bir e-posta başlığı (`X-BitDefender-Spam:Evet/Hayır`) eklenmektedir.

12.6. Ağ Güvenlik Denetiminin Yapılması

Kötü amaçlı yazılımlara karşı koruma, veri kurtarma ve posta filtreleme olanaklarının yanı sıra, LinuxDefender detaylı ana bilgisayar ve ağ güvenlik denetimi yapılabilmesi için bir dizi araçlarla birlikte sunulmaktadır. Ayrıca, LinuxDefender'a dahil edilen güvenlik araçlarının kullanılmasıyla, müdahale edilmiş sistemlerin adli analizlerinin de yapılabilmesi mümkündür. Ana bilgisayarlarınıza ve ağlarınıza hızlı bir güvenlik denetimini nasıl yapabileceğinizi öğrenmek için bu kısa bölümü okuyun

12.6.1. Rootkit'lerin Kontrolü

Ağa bağlı bilgisayarlardaki güvenlik hususlarına bakmaya başlamadan önce, ilk olarak LinuxDefender ana bilgisayarına herhangi bir müdahale yapılıp yapılmadığından emin olun. **Virüs Tarama** bölümünde gösterildiği gibi yüklü sabit diskler üzerinde bir virüs veya Unix rootkit taraması yapabilirsiniz.

İlk olarak, masaüstü ikonlarını çift-tıklayarak veya konsoldan **mount** komutunu vererek tüm sabit-disk bölümlemelerini bağlayın. Daha sonra, CD içeriğini kontrol etmek için **ChkRootKit** ikonunu çift-tıklayın `-r NEWROOT` veya ana bilgisayarın yeni/(root) dizinini belirtmek için -r NEWROOT parametresini kullanarak, konsoldan **chkrootkit** komutunu verin.

```
# chkrootkit  -r  /dev/hda3
```

Bir rootkit bulunursa, chkrootkit bunu **KALIN** büyük harfler kullanarak gösterecektir

12.6.2. Nessus – Ağ Tarayıcısı

Nessus dünyanın en popüler açık-kaynak hassasiyet tarayıcıs olup, dünya çapında 75,000'i aşkın organizasyon tarafından kullanılmaktadır. Dünyanın en büyük organizasyonlarının bir çoğu, ticari hassasiyete sahip kurumsal

cihazları ve uygulamaları denetlemek için Nessus kullanarak önemli maliyet tasarrufları elde etmektedir.

—*www.nessus.org*

Nessus, ağ bilgisayarlarınızı çeşitli savunmasız noktalara karşı uzaktan taramak için de kullanılabilir. Güvenlik risklerini azaltmak ve güvenlik ihlal olaylarını engellemek için alınması gereken bazı önlemleri de önermektedir.

Nessus Güvenlik Tarayıcısı masaüstü ikonunu çift-yıklayın veya bir terminalden **startnessus** komutunu verin. Takip eden pencere açılana kadar bekleyin. Donanım kaynaklarınıza bağlı olarak, Nessus'un hassaslık veri tabanlarını içeren 5000'i aşkın bağlantılarla birlikte yüklenmesi 10 dakika kadar sürebilir. Sisteme girmek için, `knoppix` kullanıcı adını ve `knoppix` şifresini kullanın.

Hedef Seçimi sekmesini tıklayın ve hassaslık taraması yapmak istediğiniz bilgisayarın IP adresini veya ana bilgisayarın ismini girin. Tonlarca bant genişliği ve kaynak tasarrufu sağlamak ve daha kesin tarama sonuçları elde edebilmek için, taramayı başlatmadan önce, tüm tarama seçeneklerini ağ veya sistem konfigürasyonunuza göre özelleştirin. Daha sonra, **Taramayı Başlat** seçeneğini tıklayın.

Tarama işlemi tamamlandığında, Nessus bulguları ve önerileri ekranda görüntüleyecektir. Diyagram ve grafikler ihtiva eden HTML de dahil olmak üzere, raporu çeşitli formatlarda kaydedebilirsiniz. Kaydedilen raporları, sevdiğiniz bir tarayıcıyı kullanarak gözden geçirebilirsiniz.

12.7. Sisteminizin RAM Durumunun Kontrolü

Genellikle, sisteminiz beklenmeyen davranışlarda bulunduğunda (donma veya ara sıra kendi kendini yeniden başlatması), bu bir bellek problemi olabilir. RAM modüllerinizi **memtest** programı ile aşağıda açıklanan şekilde test edebilirsiniz

Bilgisayarınızı açın ve LinuxDefender CD'si ile başlatın. Ön yükleme değerine **memtest** yazın ve ENTER tuşuna basın.

Memtest programı derhal başlayacak ve RAM durumunu kontrol etmek için birkaç test yapacaktır. `C`'ye basarak, hangi testlerin yapılacağını ve diğer memtest seçeneklerini yapılandırabilirsiniz.

Tam bir memtest, sisteminizin RAM kapasitesine ve hızına bağlı olarak 8 saat sürebilir. RAM hatalarını tamamıyla kontrol etmesi için memtest'in tüm testleri yapmasına müsaade etmeniz önerilir. `ESC` tuşuna basarak programdan istediğiniz zaman çıkabilirsiniz.

Yeni donanım satın alma niyetiniz varsa (komple sistem veya bazı parçalar) hatalarının kontrol edilmesi veya uyumluluk konuları için LinuxDefender'ı ve memtest'i kullanmanız önerilir.

Yardım Alma

13. Destek

13.1. Destek Departmanı

Saygın bir tedarikçi olarak, BitDefender müşterilerine eşsiz derecede hızlı ve doğru destek verebilmek için elinden gelen tüm gayreti göstermektedir. Destek Merkezi (aşağıda belirtilen adresten temas kurabilirsiniz) en son tehditler sürekli olarak takip etmektedir. Burası tüm sorularınızın zamanında cevaplandırıldığı bir yerdir.

İleri teknoloji ürünlerini en makul fiyatlarla sunarak müşterilerine zaman ve para tasarrufu sağlama, BitDefender için her zaman bir öncelik olmuştur. Ayrıca, başarılı bir iş yerinin, iyi iletişime ve müşteriye verilen desteğin mükemmelliğine olan bağlılığa dayalı olduğuna inanıyoruz.

Her zaman <bddestek@kavi.com.tr>'den destek talep edebilirsiniz. Derhal yanıt alabilmek için, lütfen e-postanızda BitDefender'ınız ve sisteminiz hakkında mümkün olduğu kadar fazla bilgi verin ve karşılaştığınız problemi mümkün olduğu kadar doğru tarif edin.

13.2. Çevrimiçi Yardım

13.2.1. BitDefender Bilgi Üssü

BitDefender Bilgi Üssü, BitDefender ürünleri hakkında bilgi alınabilen çevrimiçi bir bilgi bankasıdır. Burada; kolaylıkla erişilebilen bir formatta, BitDefender destek ve geliştirme ekiplerinin süre gelen teknik destek ve arıza giderme faaliyetlerinin sonuçları hakkında raporların yanı sıra, detaylı açıklamalar içeren virüs önleme ve BitDefender çözümlerinin yönetimi hakkında genel makaleler ile çok sayıda diğer makaleler bulunmaktadır.

BitDefender Bilgi Üssü halka açık olup, serbestçe incelenebilmektedir. İçerdiği kapsamlı bilgiler, BitDefender müşterilerine ihtiyaç duydukları teknik bilgi ve anlayışı elde edebilecekleri diğer bir alternatifi oluşturmaktadır. BitDefender müşterilerinden gelen tüm geçerli bilgi talepleri veya arıza raporları, sonunda ürün yardım dosyalarını destekleyici arıza giderme raporları, yararlı broşür kopyaları veya bilgilendirici makaleler olarak BitDefender Bilgi üssünde toplanmaktadır.

BitDefender Bilgi Üssüne http://kb.bitdefender.com adresinden istenildiği zaman erişilebilir.

13.3. İrtibat Bilgileri

Verimli iletişim, başarılı bir işin anahtarıdır. Son 10 yıl içinde, SOFTWIN, müşterilerimizin ve ortaklarımızın beklentilerini aşabilmek için sürekli daha iyi iletişim sağlama çabası göstererek tartışmasız saygın bir üne kavuşmuştur. Herhangi bir sorunuz olursa, lütfen bizimle irtibata geçmekten çekinmeyin.

13.3.1. Web Adresleri

Satış Bölümü: <bdsatis@kavi.com.tr>
Teknik Destek: <bddestek@kavi.com.tr>
Dokümantasyon: <documentation@bitdefender. com>
Ortaklık Programı: <partners@bitdef ender.com>
Pazarlama: <marketing@bitdefender. com>
Medya İlişkileri: <pr@bitdefender.com>
İş Olanakları: <jobs@bitdefender.com>
Virüs Bildirimleri:< virus_submission@bitdefender.com>
Spam Bildirimleri:< spam_submission@bitdefender.com>
Suistimal Bildirimleri: <abuse@bitdef ender. com>
Ürün web sitesi: http://www.bitdefender.com
Ürün ftp arşivler: ftp://ftp.bitdefender.com/pub
Yerel distribütörler: http://www.bitdefender.com/partner_list
BitDefender Bilgi Üssü: http://kb.bitdefender.com

13.3.2. Şubeler

BitDefender şubeleri faaliyet bölgeleri ile ilgili olarak, gerek ticari gerekse genel konularda her türlü sorularınıza yanıt vermeye hazırdır. İlgili adresleri ve irtibat bilgileri aşağıda listelenmiştir.

Almanya

Softwin GmbH
Batı Avrupa Merkezi
Karlsdorferstrasse 56
88069 Tettnang
Almanya
Tel: +49 7542 9444 44
Fax: +49 7542 9444 99
Email: <info@bitdefender.com>
Satış: <bdsatis@kavi.com.tr>

Web: http://www.bitdefender.com
Teknik Destek: <support@bitdefender.com>

İngiltere ve İrlanda

One Victoria Square
Birmingham
B1 1BD
Tel: +44 207 153 9959
Fax: +44 845 130 5069
Email: <info@bitdefender.com>
Satış: <bdsatis@kavi.com.tr>
Web: http://www.bitdefender.co.uk
Teknik Destek: <bddestek@kavi.com.tr>

İspanya

Constelación Negocial, S.L
C/ Balmes 195, 2a planta, 08006
Barcelona
Teknik Destek: <soporte@bitdefender-es.com>
Satış: <comercial@bitdefender-es.com>
Tel: +34 932189615
Fax: +34 932179128
Web: http://www.bitdefender-es.com

A.B.D

BitDefender, LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33309
Teknik Destek: <bddestek@kavi.com.tr>
Müşteri Hizmetleri: 954-776-6262
Web: http://www.bitdefender.com

Romanya

SOFTWIN
5th Fabrica de Glucoza St.
PO BOX 52-93
Bucharest
Teknik Destek: <suport@bitdefender.ro>
Satış: <sales@bitdefender.ro>

Tel: +40 21 2330780
Fax: +40 21 2330763
Web: http://www.bitdefender.ro

Sözlük

ActiveX

ActiveX, diğer programların ve işletim sistemlerinin çağırabileceği şekilde bir program yazmak için kullanılan bir modeldir. ActiveX teknolojisi, statik sayfalar yerine bir bilgisayar programı gibi görünen ve davranan etkileşimli web sayfaları hazırlamak için Microsoft Internet Explorer ile birlikte kullanılmaktadır. ActiveX ile, kullanıcılar Web sayfasında sorular sorabilir veya cevap verebilir, basmalı butonları kullanabilir ve diğer şekillerde etkileşim sağlayabilir. ActiveX kontrolleri genelde Visual Basic kullanılarak yazılmıştır.

Active X, güvenlik kontrollerinin bulunmaması dikkate alınmalıdır. Bilgisayar güvenlik eksperleri internet üzerinden kullanılmasını tavsiye etmemektedir.

Adware

Adware, genelde kullanıcının adware'i kabul ettiği taktirde ücretsiz olarak sağlanan bir ana bilgisayar programı ile birlikte gelmektedir. Adware uygulamaları, genelde kullanıcının uygulamanın amacını belirten bir lisans anlaşmasını kabul etmesinden sonra yüklenmesi nedeniyle, yasalara aykırı bir davranış teşkil etmemektedir.

Ancak, açılır pencere reklamları rahatsız edecek bir düzeye gelebilir ve bazen sistem performansını olumsuz yönde etkileyebilir. Ayrıca, bu uygulamalardan bazılarının topladığı bilgiler, lisans anlaşması içinde bulunan şartları tam olarak anlamayan kullanıcılar için gizlilik sorunu yaratabilir.

Arşiv

Yedeklenen dosyaları içeren bir disk, bant veya klasördür.

Şıkıştırılmış formatta bir veya birden fazla dosya içeren bir dosyadır.

Arka Kapı

Tasarımcılar veya bakımcılar tarafından bir sistemin güvenliğinde bilinerek bırakılan bir boşluktur. Bu tür boşlukların bırakılmasındaki neden her zaman kötü amaçlı değildir. Örneğin bazı işletim sistemlerinde, saha servis elemanlarının veya üreticinin bakım zamanlayıcılarının kullanması amacıyla öncelikli kullanıcı hesapları bulunmaktadır.

Ön yükleme sektörü

Her diskin başında bulunan ve diskin mimarisini (kesim boyutu, küme boyutu ve bunun gibi) tanımlayan sektördür. Başlangıç disklerinde, ön yükleme sektörü aynı zaman da işletim sistemini yükleyen bir program içermektedir.

Ön yükleme virüsü

Sabit disk veya disketin ön yükleme sektörüne bulaşan bir virüstür. Ön yükleme sektörü bulaşmış bir disketle sistemin başlatılmaya çalışılması, virüsün bellekte aktif hale gelmesine neden olacaktır. Bu noktadan sonra, sisteminizi her başlattığınızda virüs bellekte aktif halde bulunacaktır

Tarayıcı

Web tarayıcısı teriminin kısaltılmış halidir. Web sayfalarını bulmak ve görüntülemek için kullanılan bir uygulama yazılımıdır. En yaygın iki tarayıcı: Netscape Navigator ve Microsoft Internet Explorer'dır. Bunların her ikisi de grafiksel tarayıcıdır. Bir başka deyişle, her ikisi de, metnin yanı sıra grafikleri de görüntüleyebilmektedir. Ayrıca, en modern tarayıcılar, bazı formatlar için ara programlar gerektirmesine rağmen, ses ve video da dahil olmak üzere çoklu-ortam bilgilerini sunabilirler.

Komut Satırı

Bir komut satırı arayüzünde, kullanıcı ekranda sağlanan boşluğa komut dilini kullanarak komutu direkt olarak girer.

Cookie

Internet endüstrisinde, cookie'ler sizin çevrimiçi ilgi alanlarınızı ve zevklerinizi izlemek için reklamcılar tarafından analiz edilebilen ve kullanılabilen bireysel bilgisayar bilgilerini içeren küçük dosyalar olarak tanımlanmaktadır. Bu alanda, cookie teknolojisi hala geliştirilmekte olup, amaç, reklamları doğrudan söylemiş olduğunuz ilgi alanlarına hedeflemektir. Çoğu insan için, bu iki tarafı da keskin bir bıçaktır. Çünkü, bir taraftan sadece ilgilendiğiniz alanla ilgili reklamları gördüğünüz için verimli ve uygun olmakta, diğer taraftan nereye gittiğiniz ve neyi tıkladığınız gerçekten "izlenmekte" ve takip edilmektedir'. Anlaşılacağı üzere, gizlilik ile ilgili tartışmaların ortaya çıkmasına neden olmakta ve bir çok kişi "SKU numarası" gibi (paketlerin arkasında bulunan ve süpermarket kasalarında taranan bildiğimiz barkod'lar gibi) fark edilme fikrinden rahatsızlık duymaktadır. Bu bakış açısı, biraz abartılı olmasına rağmen, bazı konularda gerçeği yansıtmaktadır.

Disk sürücü

Bir diskten veri okuyan ve disket üzerine veri yazan bir cihazdır.

Bir sabit disk sürücü, sabit diskleri okur ve sabit disk üzerine yazar.

Bir disket sürücü, disket sürücülere erişir.

Disk sürücüler dahili (bilgisayar içinde yer alırlar) veya harici (bilgisayara bağlanan ayrı bir kutu içinde yer alırlar) olabilirler.

İndirme

Bir ana kaynaktan bir çevresel aygıta veri kopyalamadır (genel olarak, bir dosyanın tümü). Terim genelde bir dosyayı bir çevrimiçi servisten kişinin kendi bilgisayarına kopyalama işlemini tanımlamak için kullanılır. İndirme, aynı zamanda bir dosyanın

bir ağ dosya sunucusundan ağdaki bir bilgisayara kopyalanmasını da kapsamaktadır.

E-posta
Elektronik posta. Yerel veya global ağlar üzerinden bilgisayarlara mesajlar gönderilmesini sağlayan bir hizmettir.

Olaylar
Bir program tarafından algılanan bir işlem veya eylemdir. Olaylar, bir fare butonunun tıklanması veya bir tuşa basılması gibi kullanıcı eylemleri veya belleğin yetmemeye başlaması gibi sistem olayları olabilir.

Yanlış Olumlu
Bir tarayıcı, bir dosyayı gerçekten virüs bulaşmamışken, virüs bulaşmış olarak tanımlandığında meydana gelir.

Dosya adı uzantısı
Dosya adından sonraki noktayı takip eden kısmı olup, dosyaya kaydedilen veri türünü belirtir.

Çoğu işletim sistemi dosya adı uzantılarını kullanır. Örneğin, Unix, VMS ve MS-DOS. Genelde bir ile üç harften oluşur (bazı eski işletim sistemleri üçten fazla desteklememektedir). Örnekler arasında; C kaynak kodları için “c”, Dipnotlar için “ps”, gelişigüzel metin için “txt” verilebilir.

Sezgisel
Yeni virüsleri belirlemek için kullanılan kural-tabanlı bir yöntemdir. Bu tarama yöntemi, belirli virüs imzalarına dayanmamaktadır. Sezgisel taramanın avantajı varolan bir virüsün yeni bir versiyonu tarafından aldatılamamasıdır. Ancak, bazen normal programlarda şüpheli kod bildirerek “yanlış olumlu” üretebilir.

IP
Internet Protokolü – TCP/IP protokol takımı içindeki IP adreslemesinden, yönlendirme ve IP paketlerinin bölünmesinden ve yeniden birleştirilmesinden sorumlu olan gönderilebilir bir protokoldür.

Java applet
Sadece bir web sayfasında çalışacak şekilde tasarlanmış bir Java programıdır. Bir web sayfasında bir applet’i kullanmak için, applet’in kullanacağı applet ismini ve boyutunu (uzunluk ve genişlik piksel olarak) belirtmelisiniz. Web sayfasına erişildiğinde, tarayıcı applet’i bir sunucudan indirerek kullanıcının bilgisayarında (istemci) çalıştırır. Applet’ler çok sıkı bir güvenlik protokolü tarafından yönetildikleri için uygulamalardan farklıdır.

Örneğin, applet’ler istemci üzerinde çalışmasına rağmen, istemci makinenin üzerinde veri okuma veya yazma yapamazlar. Ayrıca, applet’ler daha da

sınırlandırılmış olup, sunulmuş oldukları aynı alan içinde veri okuyabilir veya yazabilirler.

Makro virüs

Bir doküman içine bir makro olarak saklanmış olan bir bilgisayar virüs tipidir. Microsoft Word ve Excel gibi bir çok uygulama güçlü makro dillerini desteklemektedir.

Bu uygulmalar, bir doküman içine bir makro yerleştirmenize olanak sağlar ve doküman her açıldığında bu makroyu çalıştırır.

Posta İstemcisi

Bir e-posta istemcisi, e-posta almanızı ve göndermenizi sağlayan bir uygulamadır.

Bellek

Bilgisayar içindeki dahili depolama alanlarıdır. Bellek terimi, çip şeklinde gelen veri depolamayı tanımlar. Depolama kelimesi, teyp veya disklerdeki belleği tanımlamak için kullanılır. Tüm bilgisayarlar, genelde ana bellek veya RAM olarak bilinen belirli bir fiziksel belleğe sahiptir.

Sezgisel-olmayan

Bu tarama yöntemi belirli virüs imzalarını esas almaktadır. Sezgisel-olmayan bu taramanın avantajı, virüs gibi görünenler tarafından aldatılamaması ve böylece yanlış alarmlar vermemesidir.

Sıkıştırılmış programlar

Sıkıştırılmış formatta olan bir dosyadır. Bir çok işletim sistemi ve uygulamalar bir dosyayı daha az bellek alacak şekilde sıkıştırmanızı sağlayacak komutlar içermektedir. Örneğin, içinde peş peşe on boşluk karakteri bulunan bir metin dosyanız olduğunu varsayın. Normal olarak, bu 10 bayt depolama yeri kullanacaktır.

Ancak, dosyaları sıkıştıran bir program, bu boşluk karakterlerini özel bir boşluk-serisi karakter ve sonuna boşluk adetini belirten bir rakam ekleyerek değiştirebilir. Bu durumda, 10 boşluk sadece iki bayt gerektirecektir. Bu sadece bir sıkıştırma tekniğidir. Çok sayıda başka tekniklerde vardır.

Yol

Bir bilgisayardaki bir dosyaya giden kesin yolu gösterir. Bu yollar, genelde üsten aşağıya doğru olan bir hiyerarşi dosyalama sistemi ile tanımlanırlar.

Herhangi iki nokta arasındaki yön iki bilgisayar arasındaki iletişim kanalı gibidir.

Phishing

Kimlik hırsızlığında kullanmak üzere özel bilgilerini vermesi için, kullanıcıya, kurulu yasal bir kuruluş olduğunu iddia ederek bir e-posta mesajı gönderme eylemidir. E-posta, kullanıcıyı bir web sitesini ziyaret etmeye yönlendirirerek, şifre ve kredi

kartı, sosyal sigorta numarası ve banka hesap numarası gibi, yasal organizasyonun halihazırda elinde mevcut olan kişisel bilgileri güncellemesi ister. Web sitesi aslında sahte olup, sadece kullanıcının bilgilerini çalmak için kurulmuştur.

Polimorfik virüs

Bulaştığı her dosyayla şeklini değiştiren virüstür. Düzenli bir ikili formatı olmadığı için, bu tür virüsleri belirlemek oldukça zordur.

Port

Bir cihazı bilgisayara bağlayabileceğiniz bir arayüzdür. Kişisel bilgisayarların çeşitli tipte portları bulunmaktadır. Disk sürücülerini, görüntü ekranlarını ve klavyeyi bağlamak için dahili olarak bir çok port bulunmaktadır. Harici olarak, kişisel bilgisayarların modem, yazıcı, fare ve diğer çevre cihazlarını bağlamak için portları bulunmaktadır.

TCP/IP ve UDP ağlarında, mantıksal bağlantı için uç noktalar bulunmaktadır. Port numarası, ne tür bir port olduğunu tanımlar. Örneğin, port 80 HTTP trafiği için kullanılır.

Rapor Dosyası

Meydana gelen işlemlerin listelendiği bir dosyadır. BitDefender, taranan yolları, klasörleri, taranan arşiv ve dosya sayısını, kaç tanesine virüs bulaştığını ve kaç tane şüpheli dosya bulunduğunu listeleyen bir rapor dosyası tutar.

Rootkit

Bir rootkit, bir sisteme yönetici-seviyesinde erişim sağlayan bir dizi yazılım aracıdır. Terim ilk olarak Linux işletim sistemi için kullanılmış olup, davetsiz misafirlere yönetimsel haklar sağlayan ve onların sistem yöneticileri tarafından görünmeyecek şekilde varlıklarını saklayan yeniden-derlenmiş araçlar olarak bilinmektedir.

Rootkit'lerin ana görevi işlemleri, dosyaları, girişleri ve kayıtları saklamaktır. Ayrıca, uygun yazılımları dahil ettiklerinde terminallerden, ağ bağlantılarından veya çevre birimlerinden gelen verileri de yakalayabilirler.

Rootkit'ler karakter olarak kötü amaçlı değildir. Örneğin, sistemler hatta bazı uygulamalar rootkit kullanarak kritik dosyaları saklar. Ancak, genelde kötü amaçlı yazılımları saklamak veya sisteme izinsiz olarak giren kişilerin varlığını saklamak için kullanılmaktadır. Kötü amaçlı yazılımlarla birleştirildiğinde, rootkit'ler sistemin bütünlüğü ve güvenliği için büyük tehlike oluştururlar. Trafiği denetleyebilir, sistem içine arka kapılar yaratabilir, dosyaları ve kayıtları değiştirebilir ve tespit edilmekten kurtulabilirler.

Script

Makro veya toplu dosya için kullanılan diğer bir terimdir. Script, kullanıcı müdahalesi olmadan çalıştırılabilen bir komutlar listesidir.

Spam

Elektronik işe yaramaz posta veya lüzumsuz haber grubu postalarıdır. Yaygın olarak, talep edilmeyen herhangi bir e-posta olarak bilinmektedir.

Spyware

Kullanıcının internet bağlantısını haberi olmadan kullanarak, kullanıcı bilgilerini gizlice ve genelde reklam amaçlı olarak toplayan herhangi bir yazılımdır. Spyware uygulamaları, internetten indirilebilen ücretsiz veya shareware programlarına bunların gizlenmiş bir parçası olarak dahil edilirler. Ancak, shareware ve ücretsiz uygulama yazılımlarının çoğunun spyware ihtiva etmediği unutulmamalıdır. Bir kere yüklendikten sonra, spyware, kullanıcının internet üzerindeki etkinliklerini izler ve bu bilgileri arka planda bir başkasına gönderir.Spyware aynı zamanda e-posta adresleri ve hatta şifreler ve kredi kartı numaralarını da toplayabilir.

Spyware'in bir Truva atına olan benzerliği, kullanıcıların farkında olmadan başka bir şey yüklerken bu ürünleri de yüklemesi gerçeğinde yatmaktadır. Bir spyware kurbanı olmanın en yaygın yolllarından biri, bugün mevcut olan belirli eşler-arası (P2P) dosya alıp verme ürünlerinin internetten indirilmesidir.

Etik ve gizlilik konularını gündeme getirmesinin haricinde, spyware, bilgisayarın bellek kaynaklarını kullanarak ve aynı zamanda kullanıcının internet bağlantısı üzerinden spyware'in ana üssüne bilgi gönderirken bant genişliğini kullanarak kullanıcıdan çalmaktadır. Spyware bellek ve sistem kaynaklarını kullandığı için, arka planda çalışan uygulamalar sistemin çökmesine veya genel sistem dengesizliğine neden olabilirler.

Başlangıç öğeleri

Bu klasöre yerleştirilen herhangi bir dosya bilgisayar başlatıldığında açılacaktır. Örneğin, bir başlangıç ekranı, bilgisayar ilk açıldığında çalınacak olan bir ses dosyası, bir hatırlatma takvimi veya uygulama programları başlangıç öğeleri olabilir. Normal olarak, bu klasöre dosyanın kendisi yerine takma isimli başka bir dosya yerleştirilir.

Sistem Tepsisi

Windows 95 ile ilk kez ortaya çıkan sistem tepsisi, Windows görev çubuğunda (genelde altta, saatin yanında) yer almakta ve faks, modem, ses ayarı ve bir sürü diğer olanaklar gibi sistem fonksiyonlarına kolay erişim sağlayan minyatür ikonlar içermektedir. Detayları ve kontrollerini görmek için ikonu çift veya sağ-tıklayın.

TCP/IP

Transmission Control Protocol/Internet Protocol (İletim Kontrol Protokolü/ Internet Protokolü) – Farklı donanım mimarileri ve çeşitli işletim sistemlerine sahip birbirine bağlı bilgisayarların oluşturduğu ağlar üzerinden iletişim sağlayan, internet üzerinde yaygın olarak kullanılan bir dizi ağ protokolleridir. TCP/IP, bilgisayarların nasıl

iletişim kuracağı ile ilgili standartlar ve bağlantılı ağlar ve yönlendirilen trafik ile ilgili standartları içermektedir.

Trojan (Truva)

İyi huylu bir uygulama gibi rol yapan yıkıcı bir programdır. Virüslerden farklı olarak, Truva atları kendilerini kopyalamazlar, ancak onlar kadar yıkıcı olabilirler. Truva atlarının en sinsi tiplerinden biri, bilgisayarlarınızdan virüsü temizlediğini iddia eden, fakat aslında bilgisayarınıza virüs bulaştırandır.

Terim, Homer'in İlyada'sındaki bir hikayeden gelmektedir. Bu hikayede, Yunanlılar düşmanlarına devasa bir tahta at hediye ederler. Truvalılar için bu görünüşte bir barış adağıdır. Fakat Truvalılar atı şehir duvarlarının içine çektiklerinde, atın boş karnından gizlice çıkan Yunanlılar şehir kapılarını açar ve diğer askerleri içeri sokarak Truva'nın ele geçirilmesini sağlarlar.

Güncelleme

Aynı ürünün daha eski versiyonunun yerini alması için tasarlanan bir yazılım veya donanım ürününün yeni versiyonudur. Ayrıca, Güncelleme için kurulum rutinleri genellikle daha eski bir versiyonun bilgisayarınızda olup olmadığını kontrol eder. Eğer yoksa, güncellemeyi yükleyemezsiniz.

BitDefender'ın, size güncellemeleri manuel olarak kontrol etmenizi sağlayan veya otomatik olarak ürünü güncelleyen, kendi güncelleme modülü bulunmaktadır.

Virüs

Bilginiz olmadan bilgisayarınıza yüklenen ve iradeniz dışında çalışan bir program veya kod parçasıdır. Virüslerin bir çoğu aynı zaman da kendilerini kopyalayabilirler. Tüm bilgisayar virüsleri insan yapımıdır. Kendini tekrar ve tekrar kopyalayan basit bir virüs yapmak oldukça basittir. Böyle basit bir virüs bile, mevcut tüm belleği kullanacağı ve sistemi kilitlenme noktasına getireceği için tehlikelidir. Daha tehlikeli bir virüs türü, kendini ağ üzerinden yayan ve güvenlik sistemlerini baypas eden virüstür.

Virus tanımı

Virüsü algılamak ve yok etmek için virüs koruma programı tarafından kullanılan, virüsün ikili şablonudur.

Worm

Kendini ağ üzerinden yayan ve yol aldıkça kendini yeniden üreten bir programdır. Kendini diğer programlarla birleştiremez.