bitdefender

TOTAL SECURITY 2008

Kullanıcı Kılavuzu

BitDefender Total Security 2008

Kullanıcı Kılavuzu

Yayımlanma 2008.06.20

Yasal Uyarı


bitdefender

İçindekiler

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 dökümantasyonda veya bunların herhangi bir kopyasında tanımlanan uygulamaların ilgili dökümantasyonunu 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 BITDEFENDER arasında, bilgisayar yazılım ve hizmetlerini içeren, yukarıda tanımlı BITDEFENDER 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 dökümantasyonları (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. BITDEFENDER, 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.

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

LİSANS BİTİMİ. Ürün, lisans süresinin dolduğu andan itibaren işlevselliğini yitirecektir

YÜKSELTMELER (UPGRADE). BitDefender yükseltme olarak etiketlenmişse, BitDefender'ı kullanmak amacıyla yükseltilebilir olan ve BITDEFENDER 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 BITDEFENDER 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 BITDEFENDER' a 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 lisansı kiralanamaz, satılamaz, paylaşılamaz veya alt lisans yoluyla başkasına verilemez. BitDefender kaynak kodunu bulmak için ters mühendislik, yeniden derleme, sökme, derivatif çalışmalar yapma, değiştirme, tercüme veya başka herhangi bir girişimde bulunamazsınız.

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

BU ANLAŞMADA AÇIKÇA BELİRTİLMEDİĞİ SÜRECE, BITDEFENDER, ÜRÜNLER, GELİŞTİRMELER, BAKIM VEYA DESTEK VEYA DİĞER MATERYALLER (MADDİ VEYA MADDİ OLMAYAN) VEYA BITDEFENDER TARAFINDAN SAĞLANAN HİZMET İLE İLGİLİ, AÇIKÇA VEYA İMA YOLUYLA BELİRTİLMİŞ TÜM DİĞER GARANTİLERİ

KABUL ETMEMEKTEDİR. BITDEFENDER BURADA, TİCARİ SATIMA UYGUNLUK GARANTİLERİ, BELİRLİ BİR AMACA UYGUNLUK, TASARRUF HAKKI, MÜDAHALE 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 BITDEFENDER uyarılmış olsa dahi, BITDEFENDER' in hiç bir yükümlülüğü bulunmamaktadır. BAZI ÜLKELER KAZARA VEYA SONUÇSAL ZARARLAR İÇİN SORUMLULUK SINIRLANDIRILMASI VEYA HARİÇ TUTULMASINA İZİN VERMEMEKTEDİR. BU NEDENLE YUKARIDAKİ SINIRLANDIRMALAR VEYA İSTİSNAİ DURUMLAR SİZİN İÇİN GEÇERLİ OLMAYABİLİR. HİÇ BİR KOŞULDA, BITDEFENDER'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 BITDEFENDER'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 BITDEFENDER 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.

BITDEFENDER 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 BITDEFENDER tarafından yayınlanan İngilizce sürümü geçerli olacaktır.

İrtibat: BITDEFENDER, 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 Total Security 2008**' i 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 Total Security 2008**' i, bunu yaratan Şirket ve ekibini tanıtacak, kurulum sürecinde size rehberlik edecek ve nasıl yapılandırılacağını öğretecektir. **BitDefender Total Security 2008**' in nasıl kullanılacağını, nasıl güncelleneceğini, test edileceğini ve kişiselleştirileceğini öğreneceksiniz. BitDefender'dan en iyi şekilde nasıl yararlanabileceğinizi öğreneceksiniz.

Size tatmin edici ve faydalı bir çalışma diliyoruz.

1. Bu Kitapta Kabul Edilen Yazım Kolaylıkları

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

Bu kitap birbirinden farklı birkaç ana başlıktan meydana gelmektedir. Ayrıca teknik terimleri anlayabilmek için açıklayıcı bir sözlük bulunmaktadır.

Kurulum Adımları. BitDefender' ın bir çalışma istasyonuna kurulması için gerekli olan talimatları adım adım verir. **BitDefender Total Security 2008**' in 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.

Temel Yönetim. BitDefender temel yönetim ve bakım açıklamaları.

Gelişmiş Güvenlik Yönetimi. Güvenlik kapasitesinin detaylı bir sunumu BitDefender tarafından sağlanıyor. Gelişmiş ayarlar konsolunun tüm seçeneklerini ayrıntılı bir şekilde açıklayan bölümler. Bilgisayarınızı tüm tehditlere karşı (kötücül yazılımlar, spamlar, hackerlar, uygunsuz içerik ve bunun gibi) nasıl verimli şekilde korumak için nasıl yapılandıracağınızı ve BitDefender' ın tüm modüllerini kullanmayı öğreneceksiniz.

Gelişmiş Yedekleme Yönetimi. Gelişmiş yedekleme yönetiminin tanımı. Bu, yedekleme, geri yükleme ve yakma operasyonlarını nasıl yapacağınız ve bunları nerden öğreneceğinizdir.

BitDefender Kurtarma CD'si. BitDefender Kurtarma CD'si anlatımı. 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 döküman 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 dökümantasyonu size sunabilmek için lütfen bize yazın.

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

Önemli

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

Kurulum Adımları

1. BitDefender Total Security 2008 Kurulumu

Bu kullanım kılavuzunun **BitDefender Total Security 2008 Kurulumu** bölümü aşağıdaki bölümlerden oluşmaktadır:

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

1.1. Sistem Gereksinimleri

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

- İşletim platformu: Windows 2000 SP4 / XP SP2 32b & 64b / Vista 32b & 64b; Internet Explorer 6.0 (veya üstü)
- Desteklenen e-mail istemcileri: Microsoft Outlook 2000 / 2003 / 2007; Microsoft Outlook Express; Microsoft Windows Mail; Thunderbird 1.5 and 2.0

Windows 2000

- 800 MHz işlemci veya üzeri
- Minimum 256 MB RAM Bellek (512 MB tavsiye edilmektedir)
- Minimum 60 MB boş sabit disk alanı

Windows XP

- 800 MHz işlemci veya üzeri
- Minimum 256 MB RAM Bellek (1 GB tavsiye edilmektedir)
- Minimum 60 MB boş sabit disk alanı

Microsoft Windows Vista

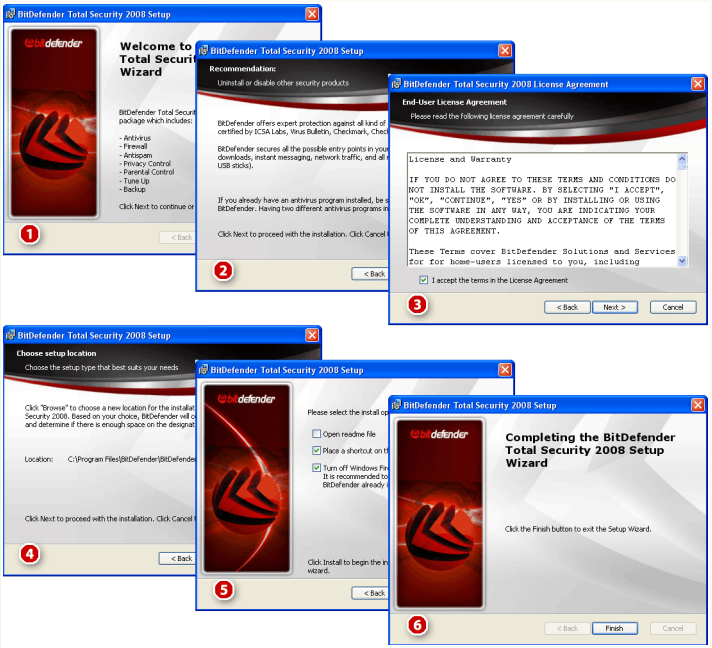
- 800 MHz işlemci veya üzeri
- Minimum 512 MB RAM Bellek (1 GB tavsiye edilmektedir)
- Minimum 60 MB boş sabit disk alanı

BitDefender Total Security 2008' i değerlendirmek amacıyla, http://www.bitdefender.com web sitesinden indirebilirsiniz.

1.2. Kurulum Adımları

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

Kurulum sihirbazını çalıştırmadan önce, BitDefender yeni sürümleri kontrol edecek. Daha yeni bir sürüm var ise onu indirmeniz için sizi yönlendirecek. Tıklayın **Evet** yeni versiyonu indirin ya da **Hayır**Yüklemeye devam edin.



Kurulum Adımları

BitDefender Total Security 2008' i yüklemek için bu adımları takip edin:

1. Devam etmek için **İleri**'yi veya kurulumdan çıkmak için **İptal**'i tıklayın.
2. **İleri**'yi tıklayın.

BitDefender Total Security 2008, bilgisayarınızda yüklü olan başka virüs koruma ürünleri olduğunda sizi uyaracaktır. Benzer ürünü kaldırmak için**Kaldır**'ı tıklayın. Bulunan ürünü kaldırmadan devam etmek için **İleri**'yi tıklayınız.

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.

3. 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.
4. Varsayılan olarak, BitDefender Total Security 2008 `C:\Program Files\BitDefender\BitDefender 2008` klasörüne yüklenecektir. Başka bir yere yüklemek istiyorsanız, **Gözat**' a tıklayın ve açılan pencerede BitDefender Total Security 2008' i yüklemek istediğiniz klasörü seçin.

   İleri'yi tıklayın.
5. Yükleme işleminin seçeneklerini belirleyin. 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 Total Security 2008 kısayolunu oluşturmak için.
   - **Kurulum bittiğinde CD'yi çıkart** - Kurulum bitince CD çıkacaktır; bu seçenek CD den kurulum yapıldığında görünür.
   - **Windows Güvenlik Duvarını Kapat** - Windows Güvenlik Duvarını kapatmak için

     Önemli
     BitDefender Total Security 2008 gelişmiş bir güvenlik duvarı içerdiği için Windows Güvenlik Duvarını kapatmanızı öneririz. İki güvenlik duvarının aynı bilgisayarda olması problem yaratabilir.

   - **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 Total Security 2008**' inizi 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.

6. **Bitir** seçeneğini tıklayın. Kurulum sihirbazının kurulum sürecinin tamamlayabilmesi için sistemi yeniden başlatmanız istenebilir. Bu opsiyonu seçili bırakmanızı tavsiye ediyoruz

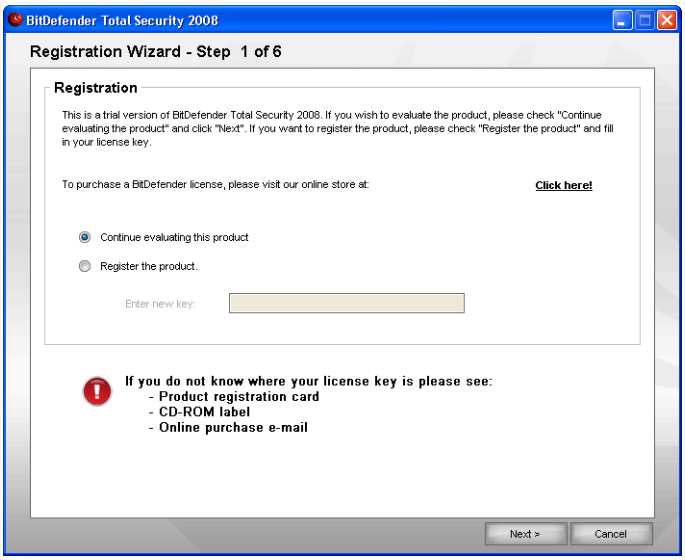
   Ürün kurulumunu tamamlamak için **Bitir**'i tıklayın. Kurulumda varsayılan ayarları kabul ettiyseniz, `Program Files`'ta `BitDefender` adında yeni bir klasör yaratılacak ve burada `BitDefender 2008` alt klasörü bulunacaktır.

1.3. Başlangıç Kurulum Sihirbazı

Kurulum sürecinde bir sihirbaz ortaya çıkacaktır. Sihirbaz **BitDefender Total Security 2008**' inizi 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 Total Security 2008 kurulmadan önce sistemin güvenli olduğundan emin olmak için yapılmasını tavsiye ediyoruz.

1.3.1. Adım 1/6 - BitDefender Total Security 2008' i Kaydedin



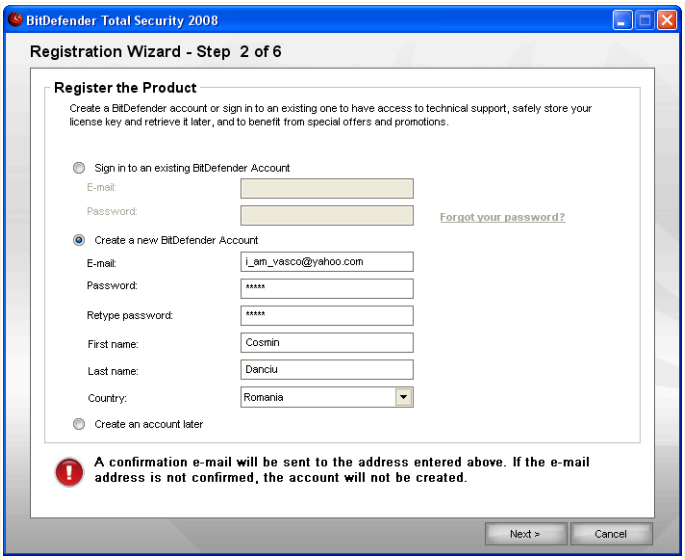
Kayıt

BitDefender Total Security 2008' i 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.

1.3.2. Adım 2/6 BitDefender Hesabının Açılması



Hesap Yaratma

BitDefender hesabım yok

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

Not
BitDefender hesabınızı daha sonra yaratmak istiyorsanız uygun seçeneği seçiniz.

BitDefender hesabı açmak için **BitDefender Hesabı Yarat** seçeneğini seçip, gerekli alanları doldurun. Internet bağlantısı gereklidir. Burada sağlayacağınız bilgiler gizli kalacaktır.

- **E-mail** – Email adresinizi girin.
- **Şifresi** – daha önce tanımlanan kullanıcı için geçerli bir şifre girin.

Not
Şifre en az dört karakter uzunluğunda olmalıdır.

- **Şifreyi Tekrar Gir** – daha önce tanımlanan kullanıcı için geçerli bir şifreyi tekrar girin.
- **Ad** – Adınızı girin.
- **Soyad** – Soyadınızı girin.
- **Ülke** – Ülke adını seçin.

Not
E-mail adresinizi ve şifrenizi kullanarak http://myaccount.bitdefender.com hesabınıza girin.

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.

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

BitDefender hesabım var

Eğer daha önceden bilgisayarınızda bir hesabınız varsa, BitDefender bunu otomatik olarak algılayacaktır. Bu pencereyi kapatmak istiyorsanız,**İleri**' ı tıklayınız.

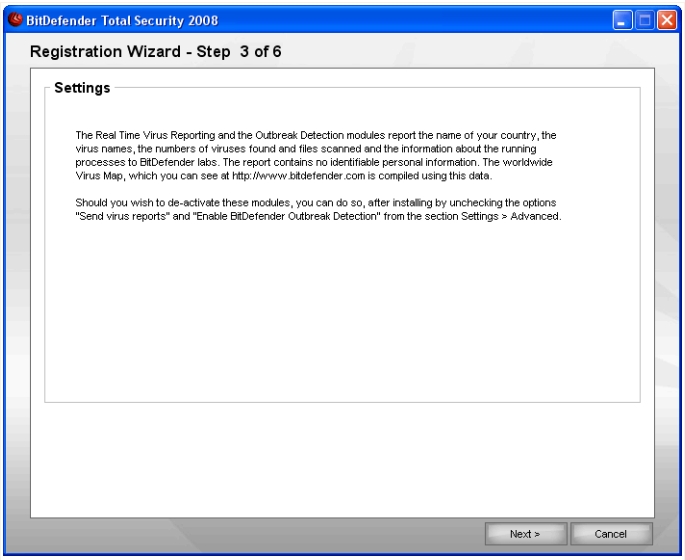
Zaten bir BitDefender hesabınız varsa, **BitDefender Hesabınıza girin** Hesabınız e-posta adresiniz ve hesap şifrenizden oluşur.

Not
Yanlış bir şifre girerseniz, **İleri** tıkladığınızda şifreyi yeniden yazmanız istenecektir. Yeniden şifre girmek için **İleri** seçeneğine tıklayın. Devam etmek için **İleri** veya sihirbazdan çıkmak için **İptal** seçeneğine tıklayın.

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

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

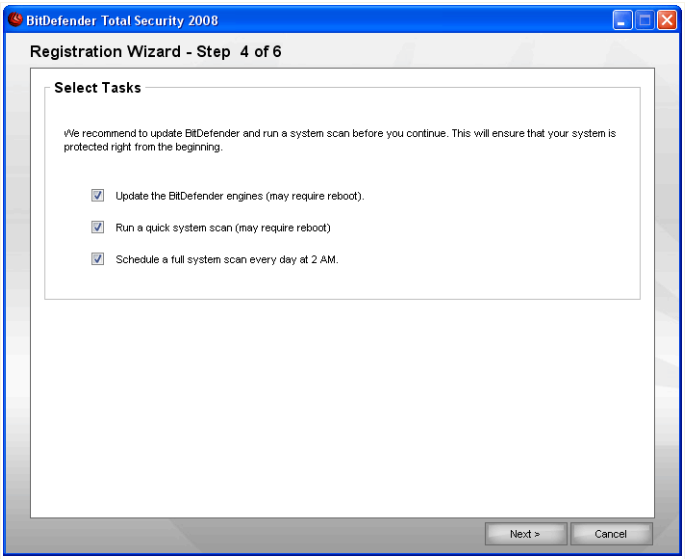
1.3.3. Adım 3/6 – RTVR Hakkında Bilgi



RTVR Bilgisi

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

1.3.4. Adım 4/6 – Çalıştırılacak Görevlerin Seçilmesi



Görev Seçimi

Sisteminizin güvenliği için gerekli olan önemli görevleri gerçekleştirmek üzere BitDefender Total Security 2008' i ayarlayın.

Aşağıdaki seçenekler mevcuttur:

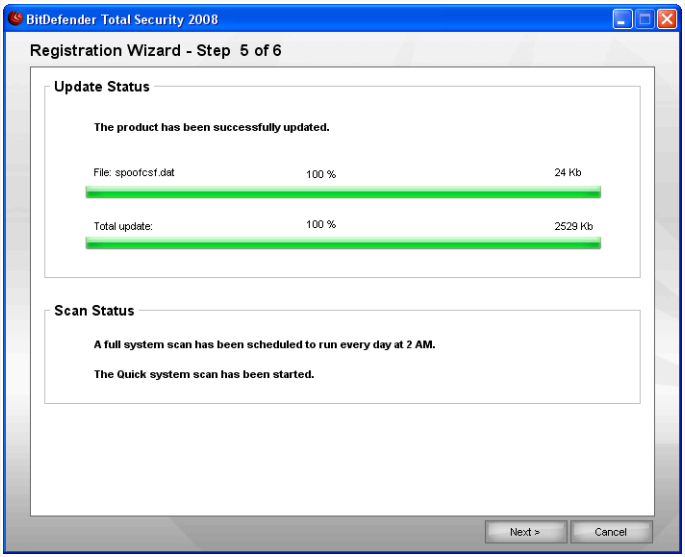
- **BitDefender motorlarını (yeniden başlatma gerekebilir) güncelle** -Bir sonraki adımda, en son tehditlere karşı bilgisayarınızı korumak için BitDefender motorlarının güncellenmesi
- **Hızlı bir sistem tarama gerçekleştirin (yeniden başlatma gerekebilir)** – bir sonraki adımda, BitDefender Antivirus 2008`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 ya da hiç birini seçmediyseniz, bir sonraki adım atlanacaktır.

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

1.3.5. Adım 5/6 – Görevlerin Tamamlanmasını Bekleyin

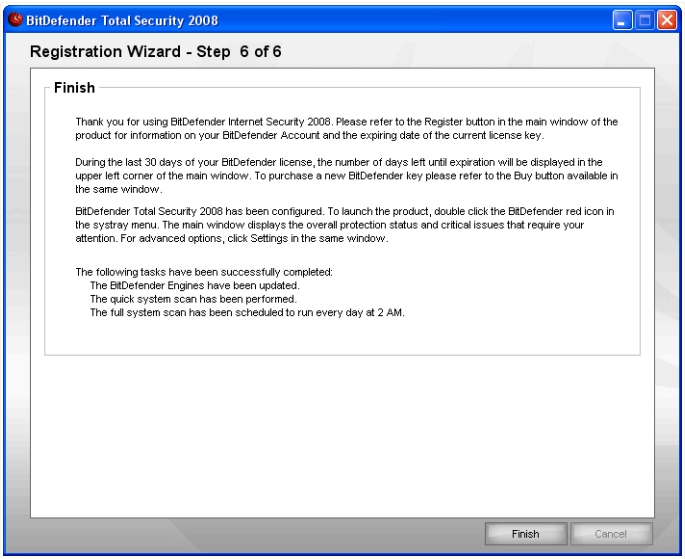


Görev Durumu

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

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

1.3.6. Adım 6/6 – Özet



Bitir

Bu, yapılandırma sihirbazının en son adımıdır.

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

1.4. 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. 3) 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. 3) bölümünde anlatıldığı şekilde yükleyin.

  Önemli
  BitDefender v8 veya daha üst bir yazılımdan yükseltme yapıyorsanız, BitDefender ayarlarınızı, arkadaşlar listenizi ve Spam'ciler listenizi kaydetmenizi tavsiye ediyoruz. Yükseltme işlemi tamamlandıktan sonra, bunları yükleyebilirsiniz.

1.5. BitDefender Özelliklerini Düzeltme veya Kaldırma

BitDefender Total Security 2008' i kaldırmak, yenilemek, düzenlemek isterseniz aşağıdaki adımları takip ediniz. **Başlat** → **Programlar** → **BitDefender 2008** → **Düzelt veya Kaldır**.

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

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

  Önemli
  Ürünü onarmadan önce Arkadaşlar listenizi ve Spam'cılar listenizi kaydetmenizi öneririz. BitDefender Ayarlarınızı ve Bayesian veritabanını da saklamanızı öneririz. Yeniden yükleme süreci sona erdiğinde bunları yeniden yükleyebilirsiniz.

  BitDefender'ı onarmayı seçtiğinizde, yeni bir pencere açılacaktır. Onarma işlemine başlamak için**Onar**'ı tıklayınız .

  Bilgisayarınız yeniden başladıktan sonra **Yükle**' ye basarak BitDefender Total Security 2008' i yeniden yükleyebilirsiniz.

  Yükleme işlemi biter bitmez yeni bir pencere açılacak. **Bitir** seçeneğini tıklayın.
- **Kaldır**- tüm yüklü bileşenleri kaldırmak için

  Not
  Temiz bir yeniden kurulum için öncelikle **Kaldır**' a basarak tüm yüklü bileşenleri kaldırmanızı öneririz.

  BitDefender'ı kaldırmayı seçtiğinizde, yeni bir pencere açılacaktır:

Önemli

BitDefender' i kaldırdığınızda virüsler ve spywareler gibi kötücül yazılım tehditlerine karşı bir korumanız kalmayacak. BitDefender' ı kaldırma işleminden sonra Windows Defender' in aktif olmasını istiyorsanız, uygun kutucuğu işaretleyiniz.

Kaldır BitDefender Total Security 2008' i bilgisayarınızdan kaldırır.

Kaldırma işlemi sırasında bize izlenimlerinizi aktarmanız istenecektir. **Tamam**' a tıklayarak 5 kısa soruya yanıt verin. Sorulara cevap vermek istemiyorsanız, sihirbazdan çıkmak için **Bitir**'i tıklayın.

Kaldırma işlemi tamamlandığında, yeni bir pencere açılacaktır: **Bitir** seçeneğini tıklayın.

Not

Kaldırma işlemi tamamlandıktan sonra,`BitDefender`klasörünü `Program Dosyaları`'ndan silmenizi tavsiye ediyoruz.

BitDefender kaldırma işlemi sırasında bir hata oluştu

BitDefender kaldırma işlemi sırasında bir hata oluşursa, işlem iptal edilecek ve yeni bir pencere açılacak. **Kaldırma Aracı**' nı çalıştırarak BitDefender' in tamamıyla kaldırıldığından emin olabilirsiniz. Kaldırma aracı, otomatik kaldırma işlemi sırasında kaldırılamayan tüm dosyaları ve kayıt defteri kayıtlarını kaldıracaktır.

Temel Yönetim

2. Başlangıç

BitDefender bilgisayarınıza yüklendikten hemen sonra korumaya başlar. BitDefender Güvenli Merkezi' ni açarak sistem güvenlik durumunu kontrol edebilir, önleyici tedbirle alabilir ya da ürünü tam olarak konfigüre edebilirsiniz.

BitDefender Güvenlik Merkezi' ne ulaşmak için Windows Başlat menüsünü kullanarak sırasıyla **Başlat → Programlar → BitDefender 2008 → BitDefender Total Security 2008**' i seçin veya sistem tepsisinden **BitDefender ikonuna** çift tıklayarak daha çabuk bir şekilde erişin.

BitDefender Güvenlik Merkezi

BitDefender Güvenlik Merkezi iki alan içerir:

- **Durum** alanı: Bilgisayarınızdaki güvenlik açıklarını giderme konusunda size yardımcı bilgiler verir. Kırmızı alanlara tıklayarak bilgisayarınızı etkileyen faktörleri kolayca görebilirsiniz. **Tüm Sorunları Düzelt** butonu bilgisayarınızın kırılganlık noktalarını düzeltecektir, ya da size nasıl kolayca çözebileceğiniz konusunda yardımcı olacaktır. Aynı zamanda, 4 ayrı güvenlik kategorisi için 4 ayrı buton bulunur. Yeşil durumdaki

butonlar herhangi bir risk olmadığını gösterirken, Sarı ve Kırmızı durumdaki butonlar, orta ve yüksek güvenlik risklerini gösterir. Bunları düzeltmek için Sarı/Kırmızı butonlara tıkladıktan sonra, **Düzelt'** e tıklayarak birer birer düzeltebilir veya **Hepsini Düzelt'** e tıklayabilirsiniz. Gri olanlar ise henüz konfigüre edilmemiş bileşenleri ifade eder.

- **Çabuk Görevler** alanı: sisteminizi güvenli tutabilmeniz ve verilerinizi koruyabilmeniz için önleyici tedbirler almanız konusunda size yardımcı olur. Üç tip güvenlik eylemine uygun olarak üç sekmeden oluşur. Burada ürününüzü güncelleyebilir, bilgisayarınızı tarayabilir, verilerinizi yedekleyip geri yükleyebilir, diskinizi birleştirebilir, geçici internet dosyalarını ve cookieleri temizleyebilir, kayıt defterini temizleyip, geri alabilir ve çift olan dosyaları bulup bunları güvenli olarak silebilirsiniz.

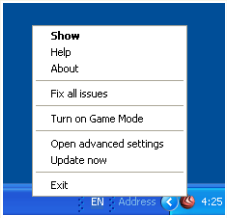
Ayrıca, BitDefender Güvenlik Merkezi bir takım kullanışlı kısayollar içerir.

Link	*Açıklama*
Satın Al	Ürünü satın alabileceğiniz bir sayfa açar
Hesabım	BitDefender hesap sayfanızı açar.
Kayıt	Kayıt Sihirbazını çalıştırır.
Yardım	Yardım dosyalarını açar.
Destek	BitDefender destek web sayfasını açar.
Ayarlar	Gelişmiş ayarlar konsolunu açar.
Geçmiş	Geçmiş ve Olay günlüğü penceresini açar.

2.1. Sistem Tepsisindeki Bitdefender İkonu

Sistem Tepsisindeki Bitdefender İkonu' nu kullanarak tüm ürünleri hızlı bir şekilde yönetebilirsiniz.

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



Bitdefender İkonu

- **Göster** - BitDefender Güvenlik Merkezi' ni açar.
- **Yardım** - yardım dosyasını açar.
- **Hakkında** - BitDefender web sayfasını açar.
- **Tüm sorunları düzelt** - Güvenlik açıklarını gidermede yardımcı olur
- **Oyun Modu aç / kapat** Oyun Modu aç / kapat.

- **Gelişmiş ayarlar** – Gelişmiş ayarlar konsoluna erişimi sağlar.
- **Şimdi güncelle** – anında güncelleme gerçekleştirir. Güncelleme durumunu görebileceğiniz bir pencere açılacak.
- **Çıkış** - Uygulamayı kapatır.

Oyun modu aktifken, BitDefender ikonu'nun üzerinde G harfini görebilirsiniz.

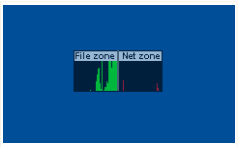
Eğer sistem güvenliğini etkileyen kritik bir durum varsa BitDefender ikonu'nun üzerinde bir ünlem işareti görünür. Sistem güvenliğinizi etkileyen sorunun adedini farenizi ikon'un üzerinde tutarak görebilirsiniz.

2.2. Tarama Etkinlik Çubuğu

Tarama etkinlik çubuğu, sisteminizdeki tarama etkinliğinin grafiksel olarak gösterimidir

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

Net Bölgesindeki Kırmızı çubuklar 0 ila 100 aralığında, saniyede transfer edilen (Internetten gönderilen ve alınan) Kbyte sayısını gösterir.



Etkinlik Çubuğu

Not
Tarama etkinlik çubuğu, **Dosya Bölgesi** üzerinde kırmızı çarpı işareti varsa size gerçek zamanlı korumanın kapalı olduğunu gösterecektir.

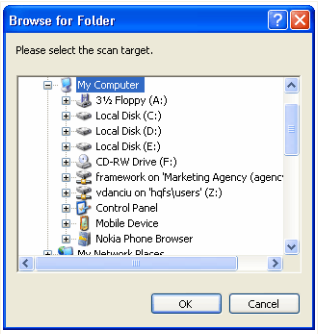
Tarama etkinlik çubuğu' nu objeleri taramak için kullanabilirsiniz. Taramak istediğiniz objeyi çubuk üzerine sürükleyip bıraktığınız taktirde taranmış olacaktır. Daha fazla bilgi için bakınız,"*Sürükle&Bırak Taraması*" (shf. 95)

Grafik gösterimini daha fazla görmek istemiyorsanız, sadece sağ tıklayarak **Gizle** seçeneğini seçin. Bu pencereyi tamamen kapatmak istiyorsanız, yönetim konsolundaki **Gelişmiş** tuşuna basarak, **Tarama etkinlik çubuğunu etkin kıl (Grafik gösterim)** kutucuğundaki işareti kaldırın.

2.3. BitDefender Manuel Tarama

Belirli bir klasörü hızlı şekilde taramak istiyorsanız, BitDefender Manuel Tarama' yı kullanabilirsiniz.

BitDefender Manuel Tarama Menüsüne erişmek için Windows Başlat menüsüne giderek takip eden adımları izleyebilirsiniz. **Başlat** → **Programlar** → **BitDefender 2008** → **BitDefender Manuel Tarama** Sıradaki pencere çıkacaktır:



BitDefender Manuel Tarama

Tüm klasörleriniz görüntülenecektir. Taramak istediğiniz klasörü seçip, **Tamam'** a basın. BitDefender Tarayıcısıaçılacak ve size tarama sürecinde rehberlik yapacaktır.

2.4. Oyun Modu

Yeni Oyun Modu geçici olarak koruma ayarlarını değiştirerek, sistem performansının en az düzeyde etkilenmesini sağlar. Oyun Modunu açtığınızda, aşağıdaki ayarlar uygulanır:

- Tüm BitDefender alarmları ve pop-upları kapatılır.
- BitDefender gerçek zamanlı koruma düzeyi **İsteğe Bağlı Düzey**'e iner
- BitDefender Güvenlik Duvarı**Oyun Modu** için ayarlamak

Oyun modu aktifken, BitDefender ikonu'nun üzerinde `G` harfini görebilirsiniz.

2.4.1. Oyun Modunu Kullanmak

Oyun Modunu açmak istiyorsanız, aşağıdaki metodlardan birini kullanınız.

- Sistem tepsisinden BitDefender ikonunu sağ-tıklayın ve **Oyun Modunu Aç**'ı seçin.
- `Alt+G` (Kısayol Tuşu) tuşlarına basınız.

Önemli
Oyun Modunu kapatmayı unutmayın. Açtığınız metodlarla kapatabilirsiniz.

2.4.2. Oyun Modu kısayol tuşunu değiştir

Kısayol tuşunu değiştirmek istiyorsanız, adımları takip edin:

1. BitDefender Güvenlik Merkezindeki ayarlar konsolundan**Ayarlar**' ı tıklayın.

   Not
   Veya Sistem tepsisinden BitDefender ikonunu sağ-tıklayın ve **Gelişmiş ayarları aç**'ı seçin.

2. **Gelişmiş**'i tıklayın.
3. **Oyun modu için kısayol tuşu**seçeneğinden istediğiniz tuşu atayabilirsiniz:
   - Kısayol tuşunu kullanımınıza göre atayabilirsiniz. Control tuşu (`Ctrl`), Shift tuşu (`Shift`) veya Alternatif tuş (`Alt`).
   - Düzenleme sahasında, istediğiniz herhangi bir harfi kısayol olarak atayabilirsiniz.

   Örnek olarak `Ctrl+Alt+D` kutucukları işaretleyin`Ctrl` ve`Alt` ve `D`yazın.

   Not
   Kutucuklardaki işaretleri kaldırırsanız **Oyun Modu için kısayol tuşu** Kısayol tuşu kapatılacaktır.

3. Güvenlik Durumu

Güvenlik durumu, bilgisayarınızdaki güvenlik açıklarını düzenli ve kolay yönetilebilir bir liste halinde sistematik olarak size gösterir. BitDefender Total Security 2008 bilgisayar güvenliği etkilendiğinde size haber verecektir.

Dört güvenlik durumu butonu bulunmaktadır:

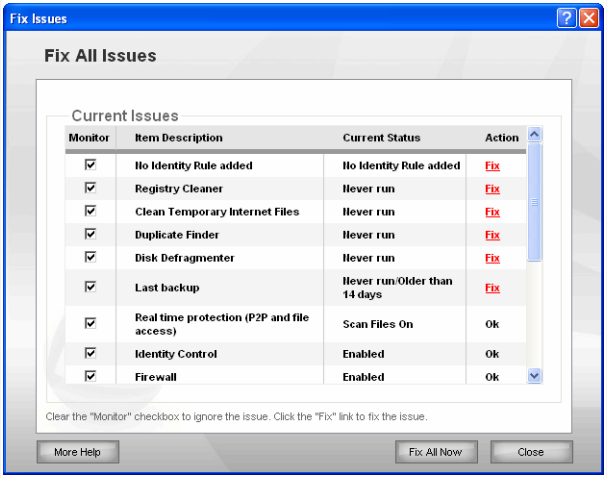
- **GÜVENLİK**
- **EBEVEYN KONTROLÜ**
- **İYİLEŞTİRME**
- **YEDEKLEME**

Aynı zamanda sol tarafta sisteminizi etkileyen sorunlar ve**Tüm Sorunları Gider**butonunu görebilirsiniz.

Durum butonları o andaki koruma düzeyine bağlı olarak, yeşil, sarı, kırmızı ve gri renkte görünebilirler.

- **Yeşil**Bilgisayarınız için düşük dereceli güvenlik riski.
- **Sarı**Bilgisayarınız için orta dereceli güvenlik riski.
- **Kırmızı**Bilgisayarınız için yüksek dereceli güvenlik riski.
- **Gri**Konfigüre edilmemiş bileşen.

Güvenlik problemlerini çözmeniz için sadece **Tüm Sorunları Gider**butonuna tek dokunuş yapmanız yeterli. Yeni bir pencere çıkacaktır.



Güvenlik Sorunu

Güvenlik sorunlarını ve kısa açıklamalarını bir liste halinde göreceksiniz.

Sadece belirli sorunları düzeltmek için uygun olan **Düzelt**butonuna basın. Eğer sorunların hepsini düzeltmek istiyorsanız, **Tümünü Düzelt** butonuna basabilirsiniz.

Ek yardıma ihtiyacınız varsa**Daha Çok Yardım** linkine tıklayın. Bağlamsal yardım sayfası, bu sorunları nasıl çözeceğiniz hakkında size ayrıntılı bilgileri görüntüler.

Önemli

Her soruna ait kutucuk varsayılan olarak işaretli gelecektir. Eğer belirli sorunların güvenlik risk düzeyi belirlenirken dikkate alınmasını istemiyorsanız, kutucuktaki işareti kaldırabilirsiniz. Lütfen bu seçeneği dikkatli kullanın, bilgisayarınız artan güvenlik risklerine maruz kalabilir.

Sorunları daha sonra düzeltmek istiyorsanız, **Kapat'** a basın.

3.1. Güvenlik Durumu Butonu

Güvenlik durum butonu yeşil ise endişe etmeye gerek yok. Eğer sarı, kırmızı veya gri ise bilgisayarınız orta veya yüksek güvenlik riskleri ile karşı karşıya olabilir.

Durum butonlarının renkleri, sadece siz güvenlik ayarlarını konfigüre ettiğinizde değişmeyebilir. Örnel olarak, son sistem tarama tarihi eski ise sarıya, çok eski ise kırmızıya dönecektir.

Aşağıdaki tablo, güvenlik risk düzeyi belirlenirken hangi elementlerin dikkate alındığı hakkında size bilgi verecektir.

Sorun	*Renk*
Son sistem tarama tarihi eski	Sarı
Son sistem tarama tarihi çok eski	Kırmızı
Gerçek-zamanlı koruma kapalı	Kırmızı
Antivirüs koruma düzeyi isteğe göre ayarlanmış	Sarı
Kişisel Gizlilik koruması kapalı	Kırmızı
Güvenlik Duvarı kapalı	Kırmızı
Gizlilik Modu kapalı	Kırmızı
Kablosuz bağlantı güvenli değil	Kırmızı
Otomatik Güncelleme Kapalı	Kırmızı
Son güncelleme tarihi eski	Kırmızı
Antispam kapalı	Gri

Sorunları düzeltmek için bu adımları takip edin:

1. Güvenlik Durumu butonuna basın.
2. Tek tek düzeltmek için**Düzelt** butonuna basın, veya hepsini düzeltmek için **Hepsini Düzelt** butonuna basın.
3. Eğer herhangi bir sorun düzelmiyor ise sihirbazı takip ederek düzeltin.

3.2. Ebeveyn Kontrolü Durum Butonu

Eğer Ebeveyn Kontrolü durum butonu yeşil ise etkin gri ise kapalı durumdadır.

Ebeveyn Kontrolünü etkinleştirmek için bu adımları takip edin:

1. Ebeveyn Kontrolü Durumu butonuna basın.
2. Aşağıdaki işlemlerden birini yapabilirsiniz:
   - Ebeveyn Kontrolünü tüm kullanıcılara etkinleştirmek için, **Hepsini Düzelt'** e basın.

- Edit Ebeveyn Kontrolünü sadece belirli kullanıcılara etkinleştirmek için,**Düzelt'** e basın.

3.3. İyileştirme Durumu Butonu

İyileştirme durum butonu yeşil ise endişe etmeye gerek yok. Eğer sarı, kırmızı veya gri ise bilgisayarınız orta veya yüksek güvenlik riskleri ile karşı karşıya olabilir.

Durum butonlarının renkleri, sadece siz güvenlik ayarlarını yapılandırdığınızda değişmeyebilir. Örnel olarak, son sistem tarama tarihi eski ise sarıya, çok eski ise kırmızıya dönecektir.

Örnek olarak, uzun zamandır bilgisayarınıza disk birleştirme yapmadıysanız, durum butonu kırmızı olacaktır.

Aşağıdaki tablo, güvenlik risk düzeyi belirlenirken hangi elementlerin dikkate alındığı hakkında size bilgi verecektir.

Sorun	*Renk*
Son internet dosyaları ve cookie temizleme zamanı eski	Sarı
Son internet dosyaları ve cookie temizleme zamanı çok eski	Kırmızı
Son kayıt defteri temizleme zamanı eski	Sarı
Son kayıt defteri temizleme zamanı çok eski	Kırmızı
Son çift dosyaları temizleme zamanı eski	Sarı
Son disk birleştirme zamanı eski	Sarı
Son disk birleştirme zamanı çok eski	Kırmızı

Sorunları düzeltmek için bu adımları takip edin:

1. İyileştirme Durumu butonuna basın.
2. Tek tek düzeltmek için**Düzelt** butonuna basın, veya hepsini düzeltmek için **Hepsini Düzelt** butonuna basın.
3. Eğer herhangi bir sorun düzelmiyor ise sihirbazı takip ederek düzeltin.

Not
Bu sihirbazlar hakkında daha fazla bilgi için "*İyileştirme*" (shf. 41) bölümüne bakınız.

3.4. Yedekleme Durumu Butonu

Yedekleme durum butonu yeşil ise endişe etmeye gerek yok. Eğer sarı, kırmızı veya gri ise bilgisayarınız orta veya yüksek güvenlik riskleri ile karşı karşıya olabilir.

Durum butonlarının renkleri, sadece siz güvenlik ayarlarını yapılandırdığınızda değişmeyebilir. Örnek olarak, son sistem tarama tarihi eski ise sarıya, çok eski ise kırmızıya dönecektir.

Örnek olarak, bilgisayarınızdaki verileri uzun zamandır yedeklemediyseniz, durum butonu kırmızı olacaktır.

Aşağıdaki tablo, güvenlik risk düzeyi belirlenirken hangi elementlerin dikkate alındığı hakkında size bilgi verecektir.

Sorun	*Renk*
Son veri yedekleme zamanı eski	Sarı
Son veri yedekleme zamanı çok eski	Kırmızı

Sorunları düzeltmek için bu adımları takip edin:

1. Yedekleme Durumu butonuna basın.
2. Tek tek düzeltmek için**Düzelt** butonuna basın, veya hepsini düzeltmek için **Hepsini Düzelt** butonuna basın.
3. Eğer herhangi bir sorun düzelmiyor ise sihirbazı takip ederek düzeltin.

Not
Bu sihirbaz hakkında daha fazla bilgi için "*Yedekleme*" (shf. 32) bölümüne bakınız.

4. Hızlı Görevler

Dört durum butonunun altında gösterilen üç sekme vardır, ve üç tip güvenlik görevine uygundur.

- **Güvenlik**
- **Yedekleme**
- **İyileştirme**

4.1. Güvenlik

BitDefender, güncel ve bilgisayarınızın virüssüz kalabilmesi amacıyla bir Güvenlik Modülü ile birlikte gelir.

Güvenlik modülüne girmek için, **Güvenlik** sekmesine tıklayın.

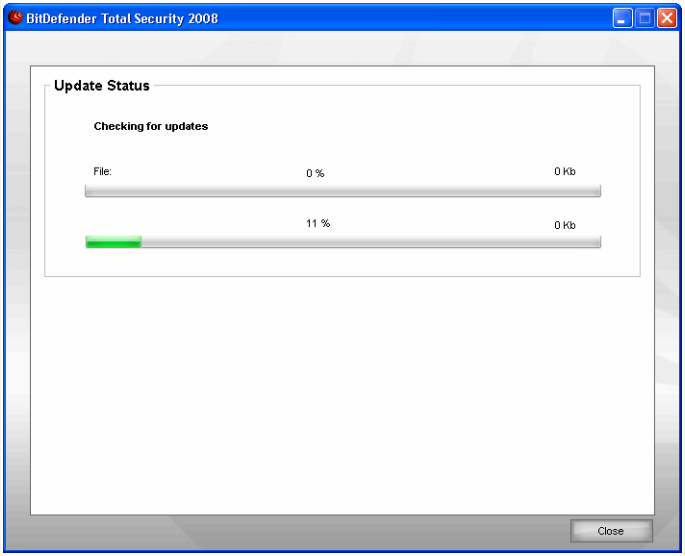
Aşağıdaki butonlar mevcuttur:

- **Şimdi güncelle** – anında güncelleme gerçekleştirir.
- **Belgelerimi Tara** – document and settings klasörünüz için hızlı tarama başlatır.
- **Yoğun sistem tarama** bilgisayarınız için tam tarama başlatır.
- **Tam sistem tarama** bilgisayarınız için tam tarama başlatır.

4.1.1. BitDefender Güncelleme

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.

BitDefender güncellemeyi kendisi yapar. Bilgisayarınızı açtığınızda ve daha sonra her **saatte bir** güncellemeleri kontrol eder. Bununla beraber, eğer BitDefender' ı anında güncellemek istiyorsanız sadece **Şimdi Güncelle**' ye tıklamanız yeterli. Güncelleme işlemi aşağıdaki pencereyi açacaktır:



BitDefender Güncelleme

Bu pencerede güncelleme işleminin durumunu görebilirsiniz.

Güncelleme işlemi hemen başlayarak, dosyaları kademeli olarak günceller. Güncelleme işlemi devam eden operasyonları etkilemeyecek, tüm kırılganlıkları dışarıda tutacaktır.

Bu pencereyi kapatmak istiyorsanız,**Kapat**' ı tıklayınız. Ancak, bu güncelleme sürecini durdurmayacaktır.

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.

Bilgisayarı yeniden başlatın. Büyük bir güncelleme olduğu taktirde, bilgisayarı yeniden başlatın ibaresi belirecektir. Güncelleme sonrası bilgisayarı yeniden başlatın ibaresini görmek istemiyorsanız, **Bilgisayarı yeniden başlatmadan devam et**seçeneğini işaretleyin. Bu yolla bir sonraki güncelleme sonrası ürün, sistem tekrar başlatılana dek eski dosyalar ile çalışmaya devam edecektir.

Yeniden başlat' a tıklarsanız, sistem yeniden başlatılacaktır.

Eğer sistemi daha sonra yeniden başlatmak istiyorsanız, **Tamam'** a tıklayın Sisteminizi hemen yeniden başlatmanız tavsiye edilir.

4.1.2. BitDefender ile taramak

Bilgisayarınızı kötücül yazılımlara karşı tararken, belirli tarama görevlerini çalıştırmak için uygun butona basınız. Aşağıdaki tabloda, mevcut tarama görevlerini, açıklamaları ile birlikte göreceksiniz.

Görev	Açıklama
Belgelerimi tara	Bu görev geçerli kullanıcının önemli klasörlerini tarar:`Belgelerim`, `Masaüstü` ve `Başlangıç`. Bu belgelerinizin güvenliğini, güvenli bir çalışma alanı ve başlangıçta temiz uygulamaların çalışmasını sağlayacak.
Derin sistem tarama	Tüm sistemi tarar. Varsayılan konfigürasyonda tüm kötücül yazılım tehditleri için tarama yapılır, virüsler, spywareler, adwareler, rootkitler ve diğerleri gibi.
Tam Sistem Tarama	Virüs ve spyware'lere karşı, arşivler hariç olarak, tüm sistemi tarar. Varsayılan konfigürasyonda tüm kötücül yazılım tehditleri için tarama yapılır, virüsler, spywareler, adwareler, rootkitler ve diğerleri gibi.

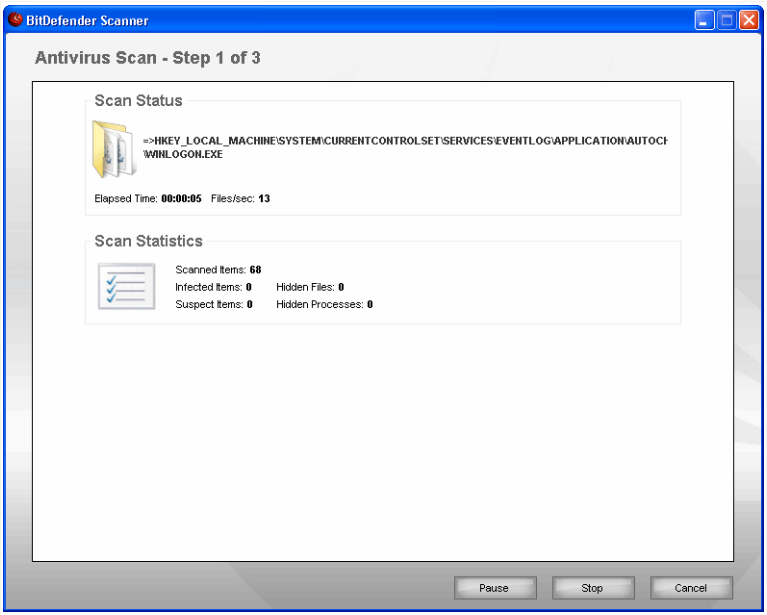
Not
Yoğun sistem tarama ve **Tam sistem tarama** görevleri tüm sistemi analiz edeceği için belirli bir süre almaktadır. Bu nedenle düşük öncelikli seçilmesi ve sistem boşta iken çalışması tavsiye edilir.

İsteğe bağlı tarama işleminde taramanın hızlı veya tam bir tarama olup olmayacağını BitDefender Tarayıcısı bize gösterecektir.

Takip eden üç adımda tarama süreci rehber eşliğinde tamamlanır.

Adım 1/3 – Tarama

BitDefender seçili objeleri taramaya başlayacak.



Tarama

Tarama durumunu ve istatistikleri görebilirsiniz (tarama hızı, geçen süre, taranan sayısı / bulaşmış / şüpheli / gizli objeler ve diğerleri)

Not
Tarama süreci, taramanın karmaşıklığına bağlı olarak, belirli bir zaman alabilir

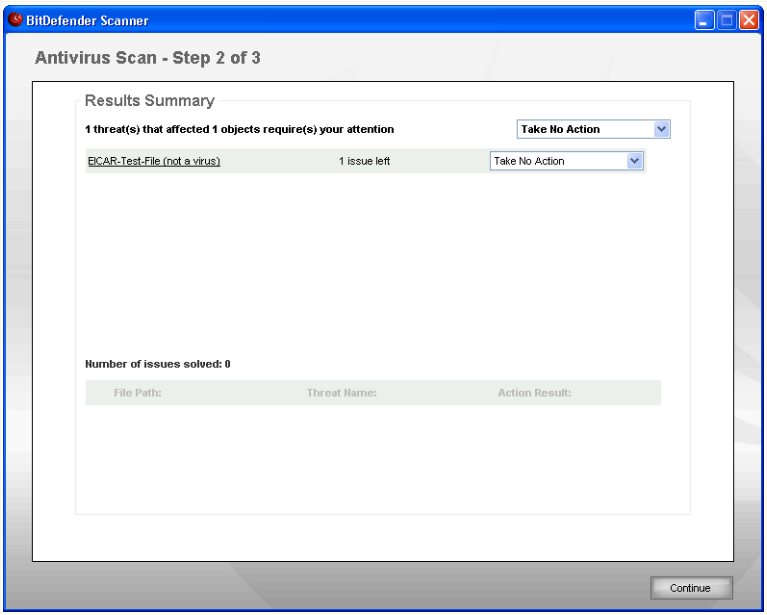
Tarama sürecini geçici olarak duraklatmak için **Duraklat**, devam etmek için **Devam** tuşuna basabilirsiniz.

Herhangi bir anda taramayı durdurmak için, **dur&Evet** tuşuna basıp son adıma geçebilirsiniz.

BitDefender' in taramayı bitirmesini bekleyin.

Adım 2/3 - İşlemi Seçin

Tarama bittiğinde, açılacak yeni pencerede tarama sonuçlarını görebilirsiniz.



İşlem

Sisteminizi etkileyen sorunun adedini görebilirsiniz.

Kötücül yazılımlar temel alınarak etkilenmiş objeler gruplarda görüntülenir. Uygun linke tıklayarak, tehditlerden etkilenmiş objeler hakkında daha fazla bilgi alabilirsiniz.

Her grup için bütün işlemleri seçebilir veya her sorun için ayrılmış işlemi seçebilirsiniz.

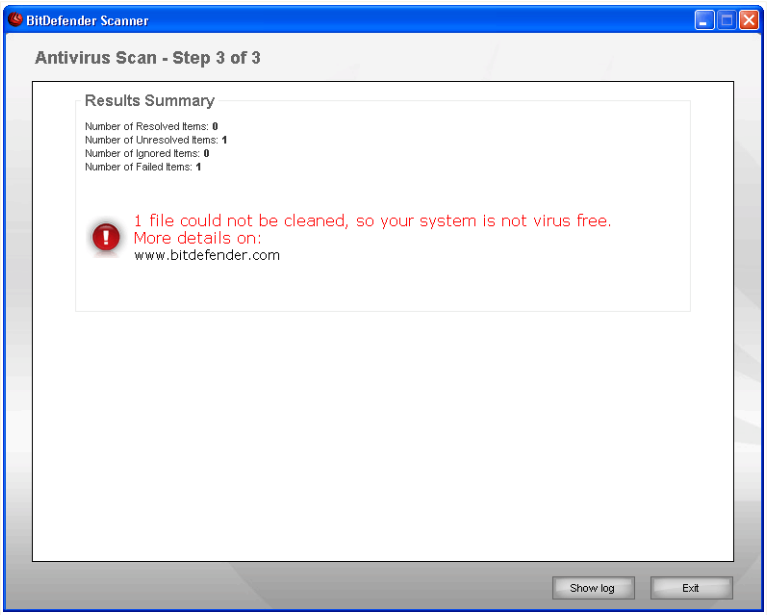
Menüde aşağıdaki seçenekler mevcuttur:

İşlem	*Açıklama*
İşlem Yapma	Virus bulaşmış dosyalar üzerinde hiç bir işlem yapılmaz.
Dosyaları temizle	Virüs bulaşan dosyayı temizler.
Dosyayı Sil	Saptanan dosyayı siler.
Açığa Çıkar	Gizli objeleri görünür yapar.

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

Adım 3/3 – Sonuçları Görüntüle

BitDefender sorunları düzeltmeyi bitirdiğinde, tarama sonuçlarının göründüğü yeni bir pencere açılır.



Özet

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

Önemli
Kurulum sihirbazının kurulum sürecinin tamamlayabilmesi için sistemi yeniden başlatmanız istenebilir.

Pencereyi kapatmak için **Tamam** seçeneğini tıklayın.

BitDefender Bazı Sorunları Çözemeyebilir.

BitDefender, birçok durumda enfekte olan dosyaları başarı ile temizler veye enfeksiyondan yalıtır Ancak, çözülemeyen sorunlar var.

Eğer çözümsüz sorunlar varsa bizim tavsiyemiz BitDefender Destek Takımı ile irtibata geçmenizdir www.bitdefender.com. Destek ekibimizbaşınıza gelen sorunları çözmede size yardımcı olacak.

BitDefender Şifre Korumalı Öğeler Algıladı

Şifre koruma kategorisi arşiv ve yükleme dosyaları olmak üzere iki tip içerir. Bunlar, eğer çalışan enfekte olan dosyalar içermiyorlarsa, sistemin güvenliği için gerçek bir tehdit oluşturmazlar.

Bu öğelerin temizliğinden emin olmak için:

- Eğer şifre korumalı öğe bir arşiv ise, dosyayı açıp onu bağımsız olarak taramak gerekir. Taranmasını istediğiniz dosya veya klasöre sağ tıklayıp **BitDefender Antivirus 2008**' i seçin.
- Eğer şifre korumalı öğe bir yükleme dosyası ise, çalıştırmadan önce, gerçek zamanlı koruma ile kontrol ettiğinize emin olun. Eğer yükleme dosyası enfekte olmuş ise, Bitdifender algılar ve enfeksiyonu izole eder.

Eğer BitDefender' ın bu öğeleri tekrar algılamasını istemiyorsanız, onları tarama harici tutulacaklara eklemelisiniz. Tarama harici tutulacaklara eklemek için, Ayarlar konsolundan **Ayarlar**' a ve sonra **Antivirus > Hariç Tut**' a tıklayın. Objeleri dışarıda bırakarak tarama

BitDefender şüpheli Dosyalar Algıladı

Sezgisel analiz tarafından saptanan şüpheli dosyalar ve henüz kötücül yazılım adıyla adlandırılmamış dosyalar.

Eğer tarama süresince şüpheli bir dosya tespit edilirse bunların BitDefender Lab.'ına gönderimi için sorulacaktır. **Tamam** tuşuna basarak bu dosyaları daha ileri araştırma için BitDefender Laboratuarlarına gönderebilirsiiniz

4.2. Yedekleme

BitDefender beraberinde sisteminizdeki değerli verilerin kopyasını tutmak için bir yedekleme ünitesi ile beraber gelir. Verilerinizi bilgisayarınıza, taşınabilir medyalara, veya bir ağda herhangi bir yere yedekleyebilir, ve onları ihtiyaç durumunda geri yükleyebilirsiniz. Verilerinizi geri yükleme işlemi son derece kolaydır.

Yedekleme modülüne girmek için, dört durum butonu altındaki**Yedekleme** sekmesine tıklayın.

Aşağıdaki butonlar mevcuttur:

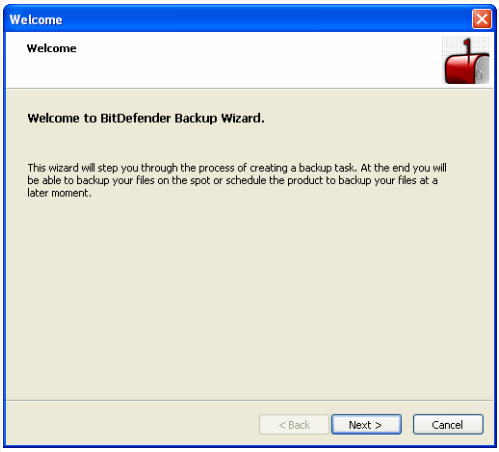
- **Yedekleme Sihirbazı** – beş kolay adımda verilerinizin yedeğini alma işlemini gerçekleştirir.
- **Gelişmiş Ayarlar** - burada yedekleme işlemlerini ayrıntılı olarak kurma ve çalıştıma işlemlerini yapabilirsiniz.
- **Geri Yükleme Sihirbazı** – dört kolay adımda verilerinizi geri yükleme işlemini gerçekleştirir.

4.2.1. Yedekleme Sihirbazı

Yedekleme Sihirbazı' na tıkladığınızda bir sihirbaz yedekleme görevi yaratma sürecinde yanınızda olacak. İşlemin sonunda verilerinizi anında yedeklemiş veya yedeklemeyi sonrası için zamanlamış olacaksınız.

Adım 1/5 - Hoşgeldiniz Ekranı

Bu sadece hoşgeldiniz ekranı.

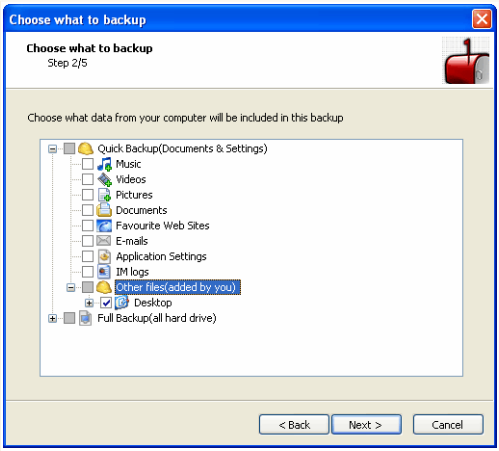


Hoşgeldiniz Ekranı

İleri'yi tıklayın.

Adım 2/5 - Neyi yedekleyeceğinizi seçin

Burada bilgisayarınızdaki hangi verinin yedeğini alacağınızı seçebilirsiniz.



Neyi yedekleyeceğinizi seçin

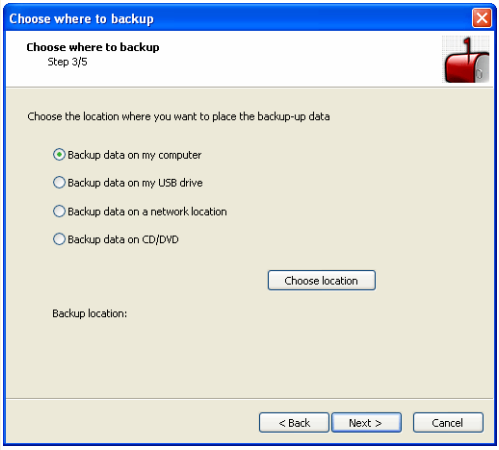
Çabuk Yedekleme (müzikler, videolar, resimler e-postalar, uygulama ayarları gibi yedeklemeler için) ya da **Tam Yedekleme** (tüm disk bölümlerini yedekleme) ikisinden birini seçebilirsiniz.

Masaüstünüzdeki diğer dosyaları **Çabuk Yedekleme**' ye eklemek için, **Diğer dosyalar**' ı tıklayın. **Tam Yedekleme** ile belirli disk bölümlerinden isteğinize göre seçebileceğiniz klasörleri kolayca yedekleyebilirsiniz.

İleri'yi tıklayın.

Adım 3/5 - Nereye yedekleyeceğinizi seçin

Burada yedeklerinizi tutacağınız lokasyonu seçebilirsiniz.



Nereye yedekleyeceğinizi seçin

Aşağıdaki seçenekler mevcuttur:

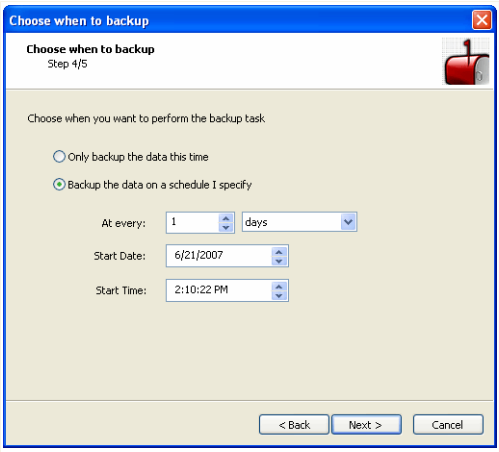
- **Yedeklemeyi bilgisayarıma yap**
- **Yedeklemeyi USB sürücüme yap**
- **Yedeklemeyi ağ üzerine yap**
- **Yedeklemeyi CD/DVD sürücüye yap**

Eğer yedeklemeyi bilgisayarınıza, USB sürücünüze veya ağda herhangi bir yere yapmaya karar verdiyseniz, **Yeri seç**' e tıklayıp verilerinizi nereye kaydedeceğinizi seçin.

İleri'yi tıklayın.

Step 4/5 - Ne zaman yedekleyeceğinizi seçin

Burada yedeklemeyi ne zaman yapacağınızı seçebilirsiniz.



Ne zaman yedekleyeceğinizi seçin

Aşağıdaki seçenekler mevcuttur:

- **Verileri sadece şu anda yedekle**
- **Verileri belirlediğim zamanda yedekle**

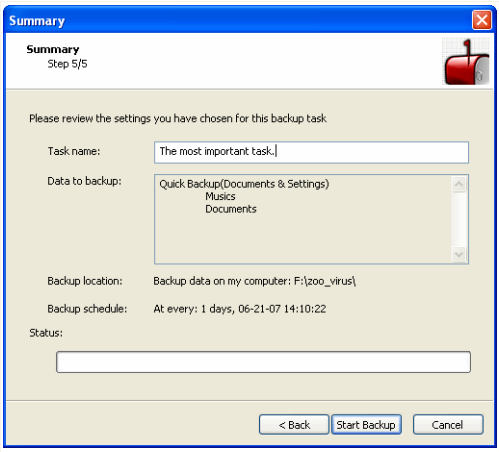
Dosyalarınızı yedeğini hemen almak için, **Verileri sadece şu anda yedekle**, dosyalarınızın yedeğini daha sonra belirli bir zamanda almak için, **Verileri belirlediğim zamanda yedekle**' yi tıklayın.

Eğer **Verileri belirlediğim zamanda yedekle**' yi seçti iseniz, zamanlanmış görevin günlük veya haftalık olarak hangi zaman aralıklarında çalışacağını, aynı zamanda başlama tarihini ve saatini de belirleyebilirsiniz.

İleri'yi tıklayın.

Adım 5/5 – Özet

Bu bölümde yedekleme ayarlarını gözden geçirebilirsiniz.



Özet

Uygun alana görev ismini yazmalısınız.

Eğer ayarlarınızdan memnunsanız **Yedeklemeye başla**'yı tıklayın.

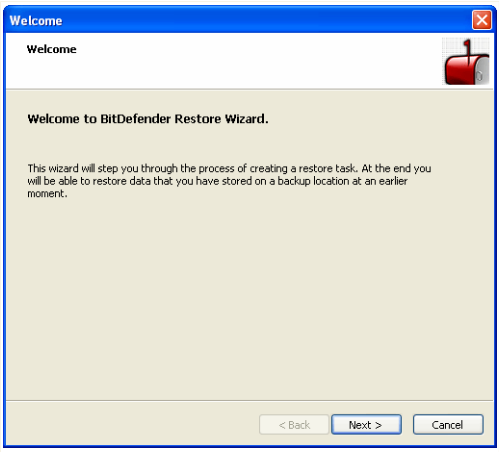
Bitir seçeneğini tıklayın.

4.2.2. Geri Yükleme Sihirbazı

Geri Yükleme Sihirbazı' nı tıkladığınızda, bir sihirbaz yedeklerinizi geri yükleme işlemi boyunca size eşlik edecek.

Adım 1/4 - Hoşgeldiniz Ekranı

Bu sadece hoşgeldiniz ekranı.

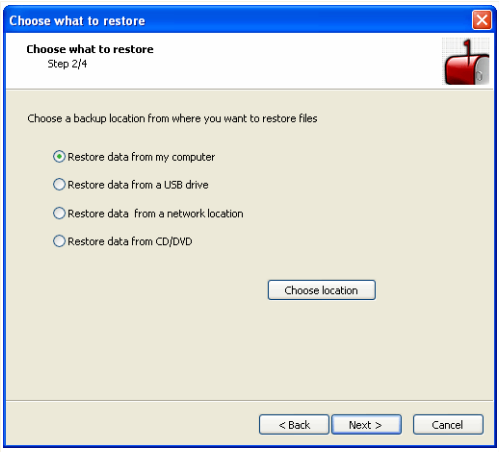


Hoşgeldiniz Ekranı

İleri'yi tıklayın.

Adım 2/4 - Geri yüklenecek yedeği seçin

Burada, geri yüklenecek dosyaların nereden geri yükleneceğini seçebilirsiniz.



Geri yüklenecek yedeği seçin

Aşağıdaki seçenekler mevcuttur:

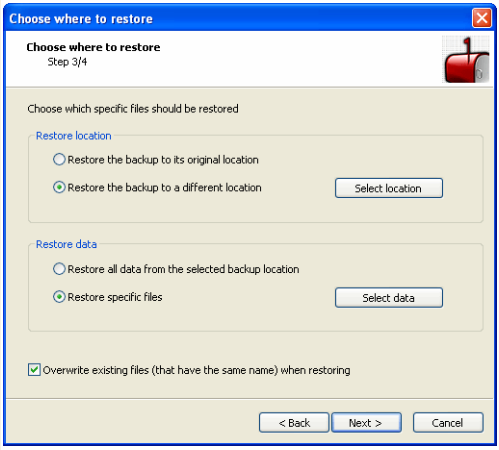
- **Verileri bilgisayarımdan geri yükle**
- **Verileri bir USB sürücüden geri yükle**
- **Verileri bir ağ lokasyonundan geri yükle**
- **Verileri CD/DVD' den geri yükle**

Yolu seç' i tıklayın ve verilerinizin kayıtlı olduğu yeri seçin.

İleri'yi tıklayın.

Adım 3/4 - Geri yüklenecek lokasyonu ve dosyaları seçin

Burada belirleyeceğiniz yere hangi dosyaları geri yükleyeceğinizi seçebilirsiniz.



Geri yüklenecek lokasyonu ve dosyaları seçin

Aşağıdaki seçenekler mevcuttur:

- **Yedeklemeyi orjinal yerine geri yükleyin**
- **Yedeklemeyi farklı bir lokasyona geri yükleyin**
- **Seçtiğiniz yedekleme lokasyonunudaki tüm verileri geri yükleyin**
- **Belirli dosyaları geri yükleyin**
- **Geri yükleme sırasında var olan dosyaların üzerine yaz**

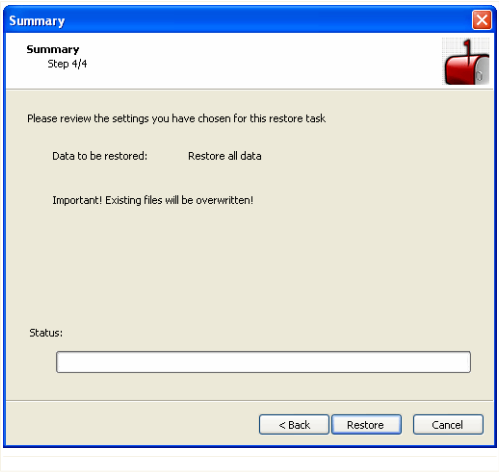
Eğer diğer bir lokasyondan sadece belirli dosyaları geri yüklemek istiyorsanız, lokasyon ve veriyi seçip uygun butona basın.

Geri yükleme sırasında var olan dosyaları korumak için, Geri yükleme sırasında var olan dosyaların üzerine yaz kutucuğundaki işareti kaldırın.

İleri'yi tıklayın.

Adım 4/4 – Özet

Bu bölümde geri yükleme ayarlarını gözden geçirebilirsiniz.



Eğer ayarlarınızdan memnunsanız **Geri Yükleme**'yi tıklayın.

Bitir seçeneğini tıklayın.

4.3. İyileştirme

BitDefender sisteminizin bütünlüğünü sürdürmekte size yardımcı olmak için bir İyileştirme modülü ile beraber gelir. Bakım araçları sisteminizdeki kritik düzeltmeler ve sabit diskinizi daha verimli kullanabilmek için size yardımcı olur.

PC' nizdeki bakım operasyonlarını yapmak için, **İyileştirme** tabına tıklayarak sağlanan araçları kullanın. Aşağıdaki butonlar mevcuttur:

- **Disk Birleştirici** - Yerel sisteminizdeki diskleri birleştirmek için bir sihirbaz başlatır.
- **Tekrarlanan Dosyaları Bul** - Tekrarlanan dosyaları bulabilmeniz için bir sihirbaz başlatır.
- **Internet Dosyalarını Temizle** - Geçici internet dosyaları ve cookieleri temizlemeniz için bir sihirbaz başlatır.
- **Dosyaları Sil** - Dosyaları sisteminizden kalıcı olarak silmek için bir sihirbaz başlatır.
- **Kayıt Defterini Temizle** - Windows kayıt defterini temizlemek için bir sihirbaz başlatır.
- **Kayıt Defterini Geri Al** - Temizlenmiş Windows kayıt defterini geri almak için bir sihirbaz başlatır.

4.3.1. Sabit Disk Birleştirme

Çok büyük dosyaları sabit diske kopyaladığınız zaman, bu dosyayı parçalayarak mümkün olur. Çünki dosyayı tek bir parça halinde kopyalayacak kadar büyük boşluk yoktur. Bu parçalanmış dosyalara ulaşılmak istendiğinde ancak diskin çeşitli bölümlerinden okunarak olur.

Dosyaların parçalanması erişim hızını ve sistem performansını düşürür. Ayrıca sabit diskin hızlı çalışmasını engeller.

Dosya parçalanmasını azaltmak için periyodik olarak disk birleştirme yapmalısınız. Disk birleştirme disk üzerindeki verileri fiziksel olarak yeniden düzenler ve her dosyanın bütün halinde depolanmasını sağlar. Disk üzerindeki boşluklar da geniş olacağı için dosya parçalanması önlenir.

Disk birleştirme şu amaçlar doğrultusunda tavsiye edilir:

- dosyalara hızlı erişim.
- genel sistem performansını arttırmak.
- sabit disk ömrünü uzatmak.

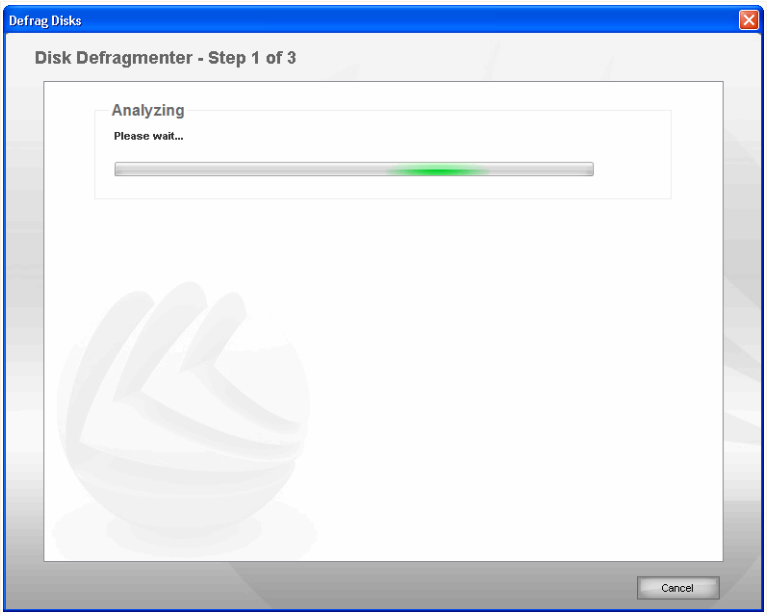
Diski birleştirmek için, Güvenlik Merkezindeki **İyileştirme** tabından **Disk Birleştirici**'yi seçin. Üç adımlık bir prosedür rehberliğinde tamamlayacaksınız.

Not

Disk birleştirme işlemi, verileri sabit disk üzerinde başka yerlere taşıyacağı için zaman alabilir. Bu nedenle disk birleştirme işlemini bilgisayarınızda çalışmadığınız zamanlarda yapmanızı tavsiye ederiz.

Adım 1/3 – Analiz...

Disk Birleştirici sabit diskinizin birleştirmeye ihtiyacı olup olmadığına karar vermek için analiz edecek.

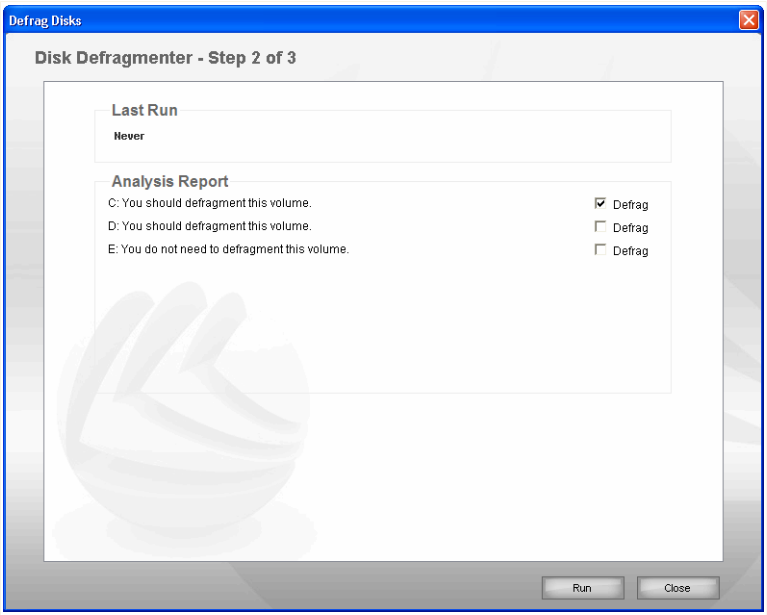


Analiz

Disk Birleştiricinin analizi bitirmesini bekleyin.

Adım 2/3 – Analiz Raporunu Görün

Analiz bittiğinde, açılacak olan yeni pencerede analiz sonuçlarını ve bisk birleştirmeye gerek olup olmadığını görebilirsiniz.



Analiz Raporu

Analiz raporunu kontrol edin.

Eğer disk birleştirmeye gerek yoksa, pencereyi kapatmak için **Tamam** seçeneğini tıklayın. Aksi halde, **Birleştir** seçneğini ihtiyacı olan sabit disk bölümüne uygulamak için, **Çalıştır**' a tıklayarak birleştirmeyi başlatın.

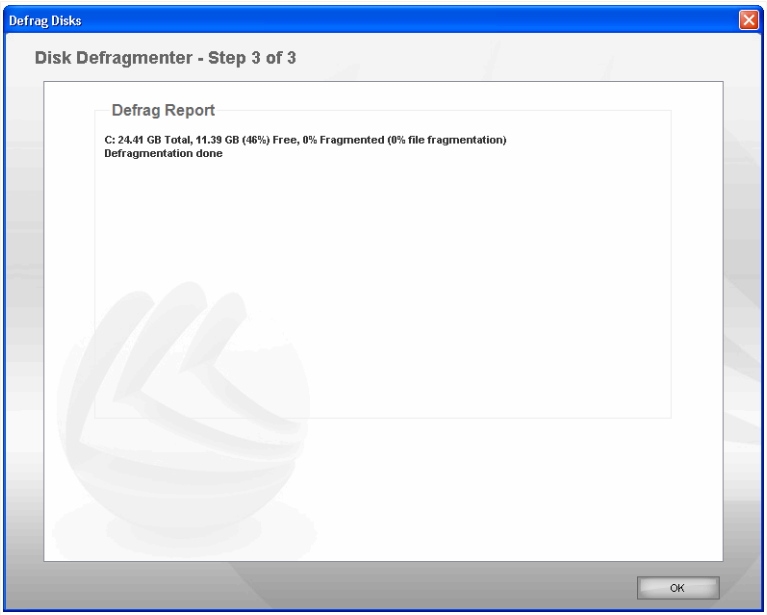
Not
Disk birleştiricinin operasyonu düzgün bir şekilde yapabilmesi için, disk alanının %15' i boş alana ihtiyacı olacaktır. Eğer yeterli boş alan yok ise birleştirme iptal olacaktır.

Herhangi bir anda disk birleştiriciyi iptal etmek için, **İptal**' e tıklayın.

Disk birleştiricinin tamamlanmasını bekleyin.

Adım 3/3 – Birleştirme Raporunu Görün

Birleştirme bittiğinde, açılacak yeni pencerede birleştirme sonuçlarını istatistiksel olarak görebilirsiniz.



Birleştirme Raporu

Pencereyi kapatmak için **Tamam** seçeneğini tıklayın.

4.3.2. Tekrarlanan Dosyaları Bulma

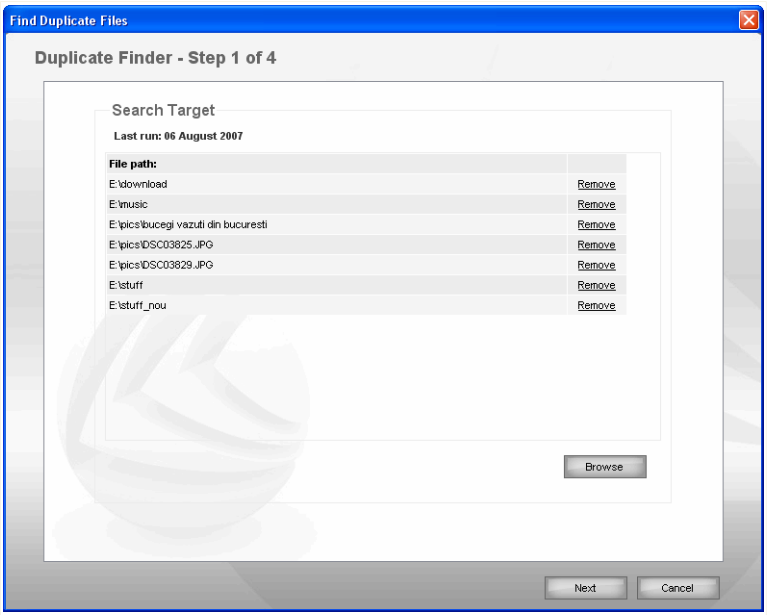
Tekrarlanan dosyalar sabit diskinizdeki boş alanı harcarlar. Sadece aynı `.mp3` dosyasının üç farklı yerde olduğunu düşünün.

Bilgisayarınızdaki tekrarlanan dosyaları bulmak ve silmek için, Kopya Bulucusu' nu kullanabilirsiniz. Bu yolla sabit diskinizdeki boş alanları daha iyi yönetebilirsiniz.

Tekrarlanan dosyaları bulmak için, Güvenlik Merkezindeki **İyileştirme** tabından **Tekrarlanan Dosyaları Bul'** a tıklayınız. Dört adımlık bir prosedür rehberliğinde tamamlayacaksınız.

Adım 1/4 - Arama Hedefini Seçin

Burada tekrarlanan dosyaları nerede arayacağınızı seçebilirsiniz.



Arama Hedefi

Gözat'a tıklayın, ve Kopya Bulucunun tekrarlanan dosyaları nerede arayacağını seçin.

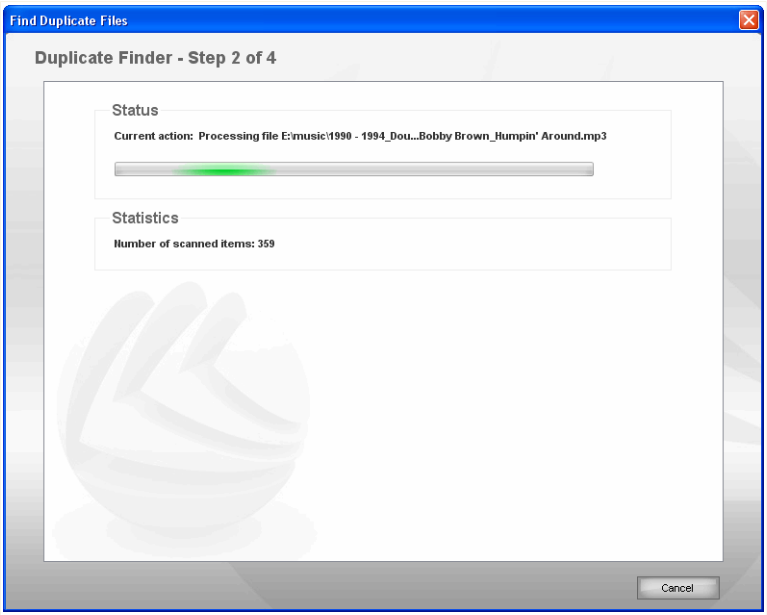
Not
Bir veya birden fazla lokasyon seçebilirsiniz:

Seçilen lokasyonun yolu **Dosya Yolu** kolonunda görünecektir. Eğer lokasyonu değiştirmeyi isterseniz sadece **Kaldır**' a tıklamanız yeterli olacaktır.

İleri'yi tıklayın.

Adım 2/4 – Arama...

Kopya Bulucu tekrarlanan dosyaları aramaya başlayacaktır.



Arama...

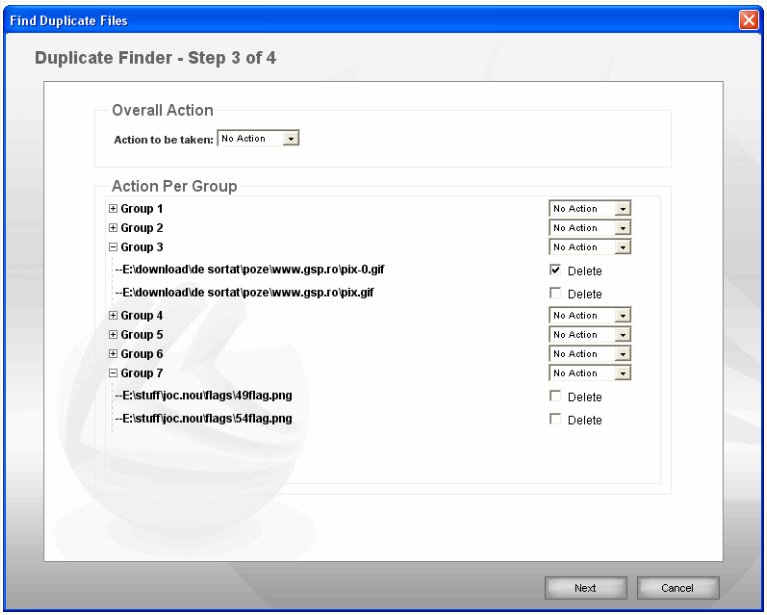
Arama durumunu ve istatistikleri görebilirsiniz.

Kopya bulucunun tekrarlanan dosyaları aramayı bitirmesini bekleyin.

Adım 3/4 - İşlemi Seçin

Arama bittiğinde, açılacak yeni pencerede bulunan tekrarlanmış dosyalara uygulayacağınız işlemi belirleyebilirsiniz.

Not
Eğer tekrarlanan dosya bulunamamışsa, bu adımı atlayın.



İşlem

Bulunan tekrarlanan dosyalar için tam işlemi seçebilir ya da tekrarlanan dosyaların grugları için işlemler seçebilirsiniz.

Aşağıdaki işlemler mevcuttur:

İşlem	Açıklama
Yeni Olanı Tut	Tekrarlanan dosyalardan en yeni olan tutulup, diğerleri silinecektir.
Eski Olanı Tut	Tekrarlanan dosyalardan en eski olan tutulup, diğerleri silinecektir.
İşlem Yapma	Tekrarlanan dosyalar üzerinde hiç bir işlem yapılmaz.

"+" işaretine tıkladığınızda bir grubun içerdiği nesneler görünür. Eğer gruptaki tüm nesnelere tam işlemi uygulamak istiyorsanız, uygun menüden arzuladığınız işlemi

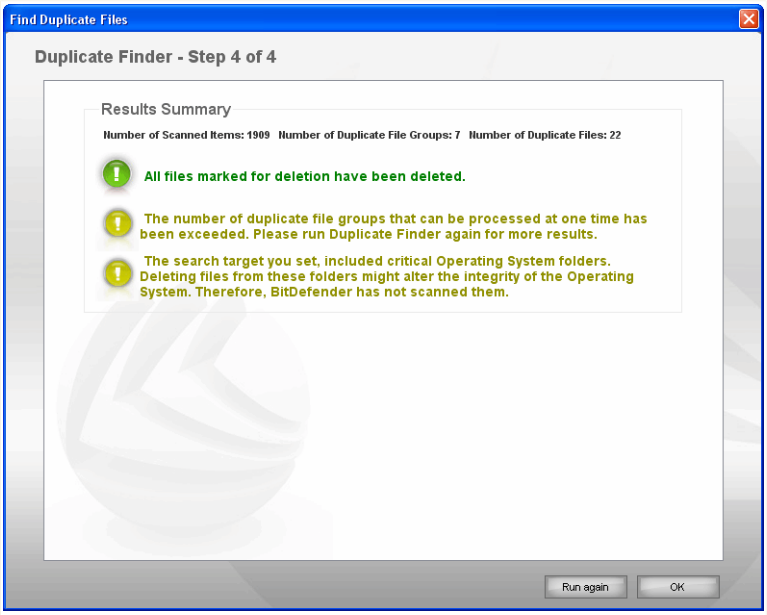
seçin. Eğer gruptaki belirli bazı dosyaları silmek istiyorsanız sırasıyla **Sil** seçeneğini işaretleyin.

Not
Tam işlem belirli dosyalar ve gruplar için seçilen işlemi üzerine yazmayacaktır. Bunun anlamı, örneğin, eğer tam işlemde **Taze Tut**' u ayarladıysanız, ve belirli bir gruba işlem uygulamak istemiyorsanız, tam işlem bu belirlenmiş grubu dışarıda tutarak uygulayacaktır.

İleri'yi tıklayın.

Adım 4/4 – Sonuçları Görüntüle

Burada Kopya Bulucunun tarama sonuçlarını görebilirsiniz.



Özet

Yeni bir arama yapmak için, **Tekrar Çalıştır**, pencereyi kapatmak için, **Tamam**' a tıklayın.

4.3.3. İnternet Dosyalarını Temizleme

Bir web sayfasını ziyaret ettiğiniz her seferinde, bir dahaki sefere daha kolay erişebilmeniz için, geçici internet dosyaları yaratılır.

Bu dosyalar geçici olarak adlandırılmasına rağmen tarayıcınızı kapattığınızda silinmezler. Bu durum, bilgisayarınıza erişebilen herkes bu dosyaları görebileceğinden gizlilik sorunları yaratabilir. Diğer taraftan bu dosyalar hatırı sayılır büyüklüklere ulaşarak sabit diskinizi işgal edebilir.

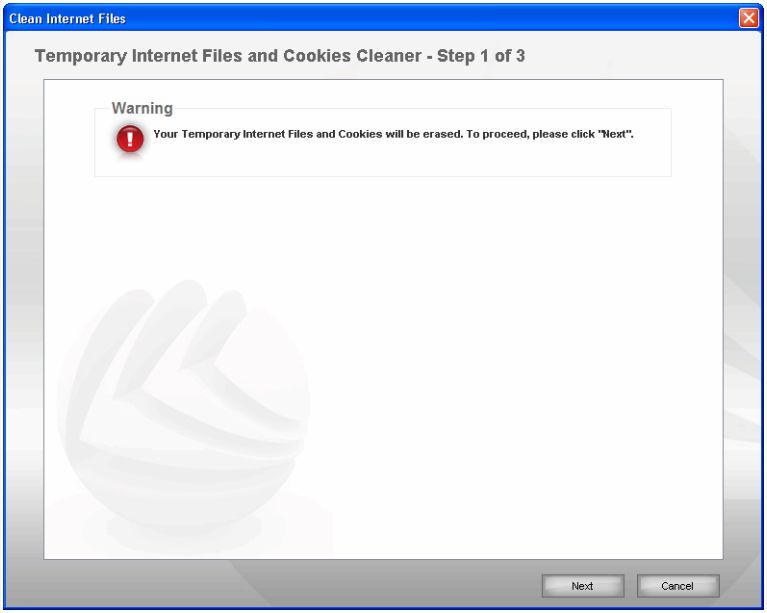
Cookieler de web sayfalarını ziyaret ettiğinizde bilgisayarınızda tutulur. Cookieler, web gezme özelliklerinizi içeren küçük dosyalardır. Bunların görülmesi de sorun yaratabilir, ayrıca online ilgi alanlarınız reklamcılar tarafından analiz edilip kullanılabilir.

Geçici internet dosyalarını ve cookieleri temizleyerek, disk alanından kazanacak ve gizliliğinizi koruyacaksınız.

Internet Explorer' ın geçici internet dosyaları ve cookieleri tuttuğu Temporary Internet Files klasörünü temizlemek için, Güvenlik Merkezindeki **İyileştirme** tabından **Internet Dosyalarını Temizle**' ye tıklayın. Üç adımdan oluşan bir rehber işlem tamamlanana kadar sizinle olacak.

Adım 1/3 - Silmeyi Başlat

Burada geçici internet dosyalarını ve cookieleri silmeyi başlatabilirsiniz.

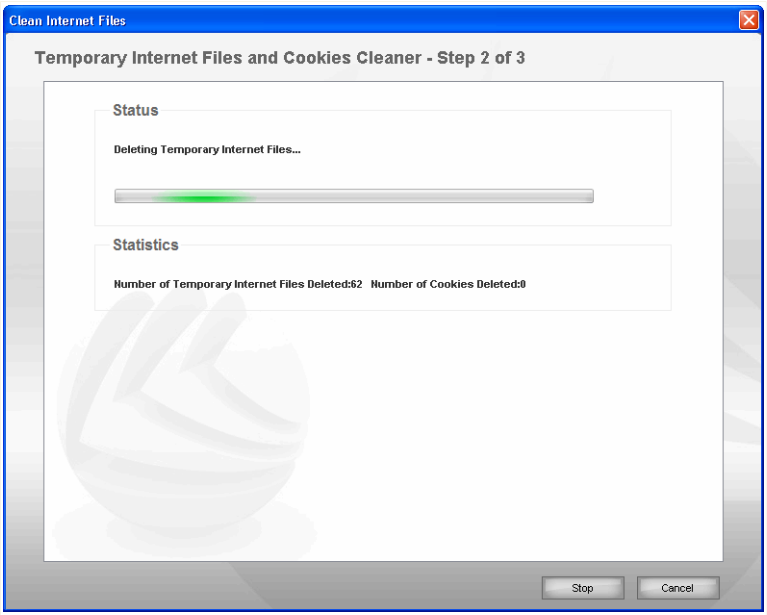


Hoşgeldiniz Ekranı

İleri'yi tıklayın.

Adım 2/3 - Dosyalar Siliniyor...

Temizleyici geçici internet dosyalarını ve cookieleri silmeyi başlatacak

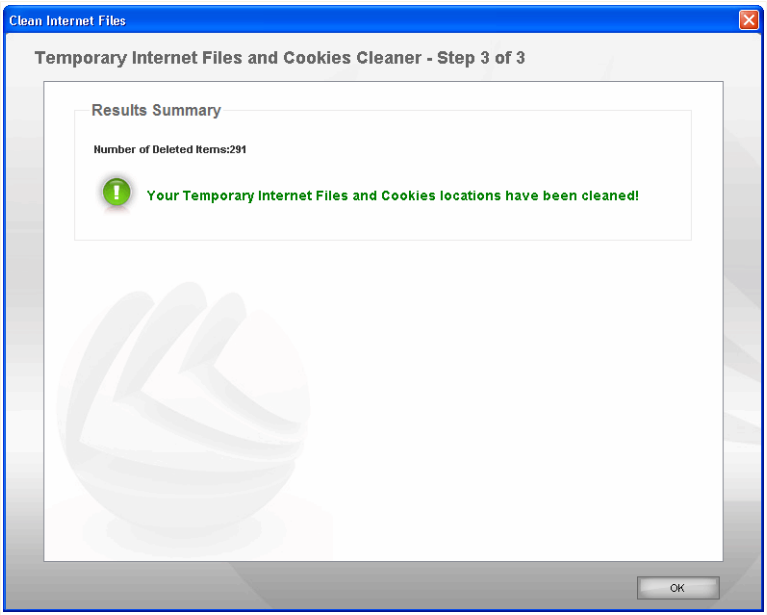


Dosyalar Siliniyor...

Temizleyicinin geçici internet dosyalarını ve cookieleri silmesini bekleyin.

Adım 3/3 – Sonuçları Görüntüle

Temizleyici tüm dosyaları sildiğinde, açılacak yeni pencerede sonuçları görebilirsiniz.



Özet

Silinen nesneler hakkındaki istatistikleri görebilirsiniz.

Pencereyi kapatmak için **Tamam** seçeneğini tıklayın.

4.3.4. Dosyaları Kalıcı Olarak Silmek

Bir dosyayı sildiğinizde, o dosyaya artık normal yollarla erişilemez, fakat üzerine yeni bir dosya yazılıncaca kadar sabit diskinizde yer tutmaya devam eder.

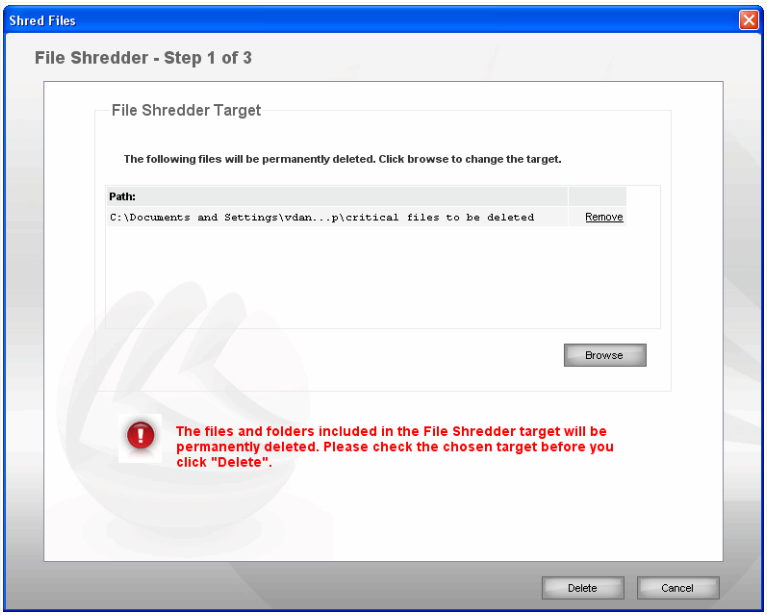
Bir dosya silinmiş olsa bile, özel programlar kullanılarak geri alınabilir. Bu sizin gizli verilerinizi almak adına kötü niyetli denemeler olabileceği gibi gizliliğinize de tehdit olabilir.

Önemli verilerinizin sildikten sonra geri alınmasını önlemek için, BitDefender kalıcı olarak silmeyi kullanabilirsiniz. Bu verileri diskinizden fiziksel olarak silecektir.

Dosyaları kalıcı olarak silmek için, Güvenlik Merkezindeki **İyileştirme** tabından, **Dosyaları Sil**' i tıklayın. Üç adımdan oluşan bir rehber işlem tamamlanana kadar sizinle olacak.

Adım 1/3 – Hedef Seçin

Burada kalıcı olarak sileceğiniz dosya veya klasörleri belirleyebilirsiniz.



Hedef

Gözat' a tıklayın, silinecek dosya veya klasörü seçin ve **Tamam** seçeneğini tıklayın.

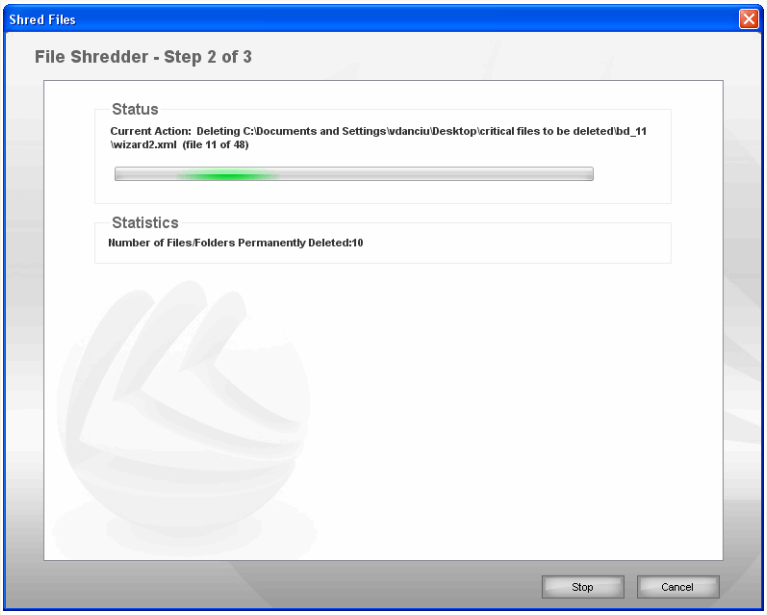
Not
Bir veya birden fazla lokasyon seçebilirsiniz:

Seçtiğiniz lokasyonun yolu tabloda görünecektir. Lokasyon hakkında fikrinizi değiştirirseniz, seçin ve **Kaldır** seçeneğini tıklayın.

Sil' i tıklayın.

Adım 2/3 - Dosyalar Siliniyor...

BitDefender belirlediğiniz lokasyondaki dosyaları kalıcı olarak silecektir.

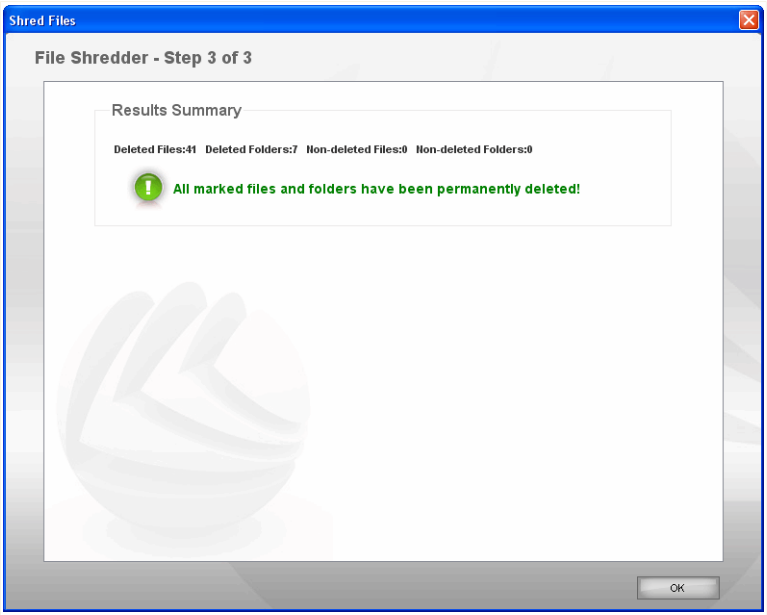


Siliniyor...

İşlemin Tamamlanmasını Bekleyin

Adım 3/3 – Sonuçları Görüntüle

Tüm dosyalar silindikten sonra, açılacak yeni pencerede sonuçları görebilirsiniz.



Özet

Pencereyi kapatmak için **Tamam** seçeneğini tıklayın.

4.3.5. Kayıt Defteri Temizleme

Windows kayıt defteri, Windows tabanlı işletim sistemlerinin önemli bir parçasıdır. Donanım ve işletim sistemi, uygulamalar, kullanıcılar, bilgisayarınızın özellikleri ve diğerleri için bilgileri ve ayarları içeren bir veri tabanıdır.

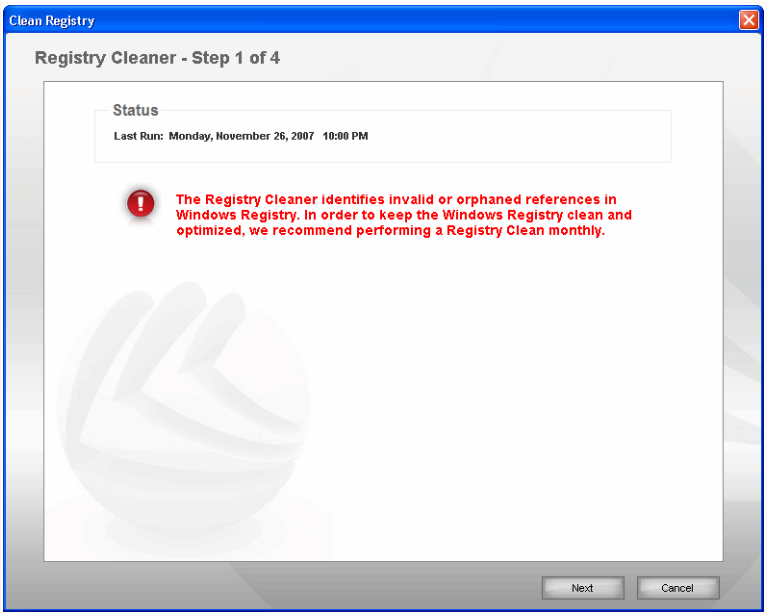
Birçok uygulama yükleme sırasında Windows kayıt defterine anahtar bilgiler yazar. Böyle uygulamalar kaldırılırken bazı kayıt anahtarları silinmeyip Windows kayıt defterinde kalırlar, bu durum sisteminizin karasızlaşmasına ve yavaşlamasına neden olur. Aynı durum sisteminize yüklü uygulamaların kısayolları ve birtakım dosyalarını kaldırırken de gerçekleşir, aynı zamanda sürücüleri de bozar.

Windows kayıt defterini temizlemek ve sistem performansını arttırmak için, Kayıt Temizleyici' yi kullanın. Kayıt Temizleyici, Windows kayıt defterini tarayarak geçersiz kayıt anahtarlarını siler.

Windows kayıt defterini temizlemek için, Güvenlik Merkezi' ndeki **İyileştirme** tabındanKayıt Defterini Temizle' yi tıklayın. Dört adımdan oluşan bir rehber işlem tamamlanana kadar sizinle olacak.

Adım 1/4 – Taramayı Başlat

Burada kayıt defteri taramayı başlatabilirsiniz.



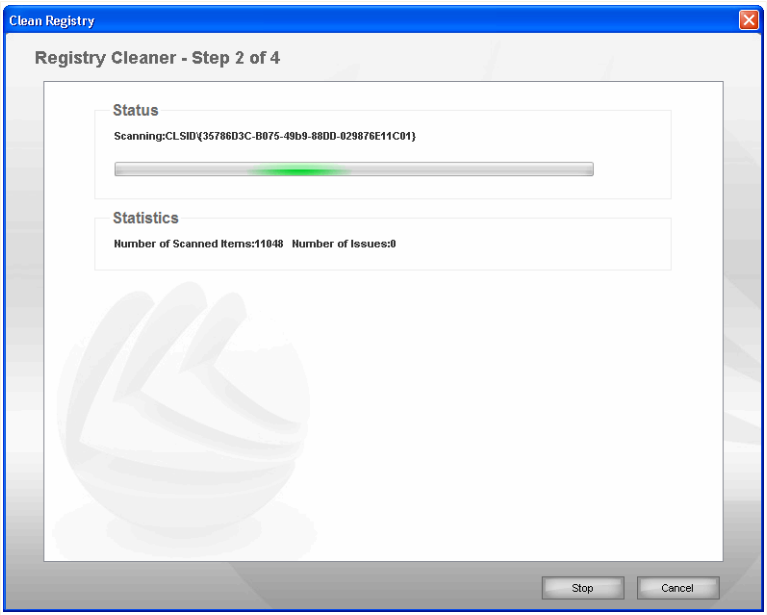
Durum

Kayıt Temizleyici çalıştıktan sonra BitDefender' ın tavsiyelerini görebilirsiniz.

İleri'yi tıklayın.

Adım 2/3 – Tarama

Kayıt Temizleyici Windows kayıt defterini taramaya başlayacak.



Taranıyor...

Son kayıt anahtarı tarandıktan sonra ilgili istatistikleri görebilirsiniz.

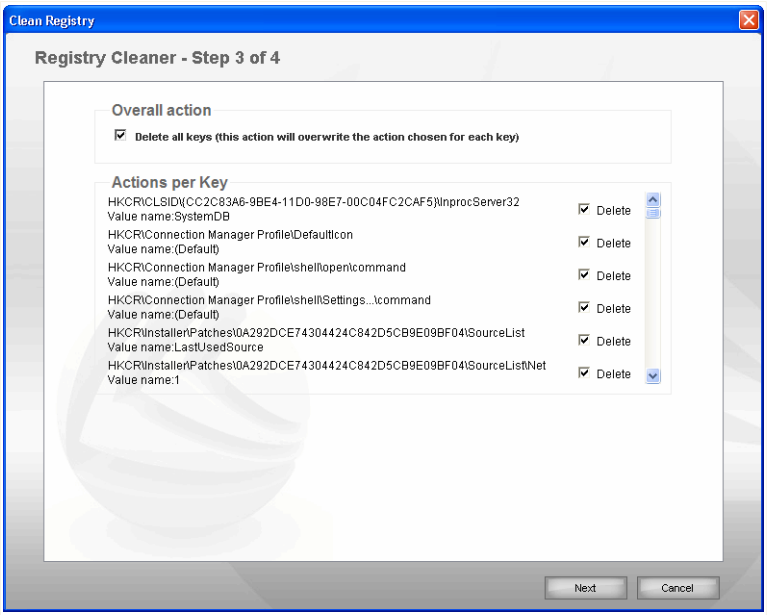
Kayıt Temizleyicinin Windows kayıt defterini taramayı tamamlamasını bekleyin

Not
Taramayı durdurmak isterseniz sadece, **Dur'** a basın. bir sonraki adıma atlayacaksınız.

Adım 3/4 - İşlemi Seçin

Tarama bittiğinde, açılacak yeni pencerede tarama sonuçlarını görebilirsiniz.

Not
Eğer herhangi bir sorun bulunmamışsa, ya da durdurmayı seçtiyseniz bir sonraki adıma atlayacaksınız.



İşlem

Algılanan tüm kayıt anahtarlarını görebilirsiniz, tümünü, veya sadece belirli anahtarları silebilirsiniz.

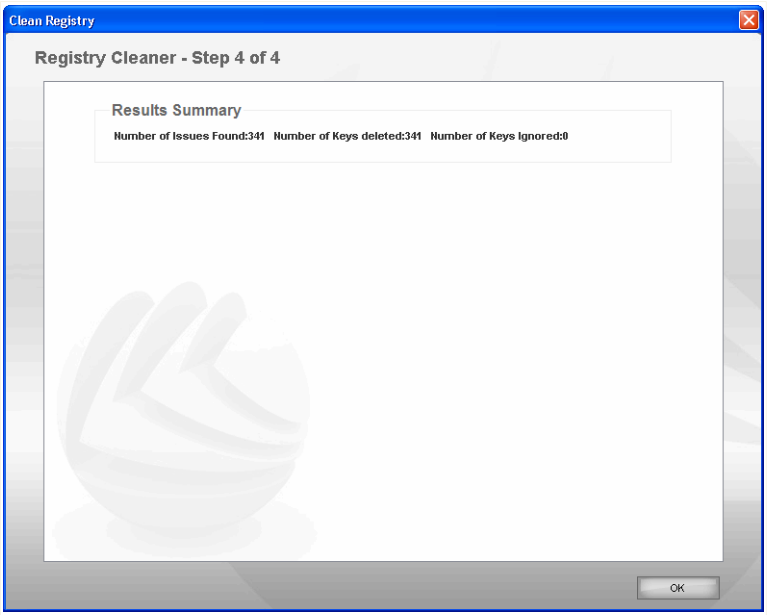
Eğer **Tümünü Sil** seçeneğini seçerseniz algılanan tüm anahtarları silinecektir. Eğer sadece belirli anahtarları silmek istiyorsanız ilgili anahtarın yanındaki **Sil** seçeneğini işaretleyin.

Not
Varsayılan olarak, tüm geçersiz anahtarlar silinecektir.

İleri'yi tıklayın.

Adım 4/4 – Sonuçları Görüntüle

Burada Kayıt Temizleyici tarafından uygulanan taramanın sonuçlarını görebilirsiniz.



Özet

Eğer tüm anahtarları silmeyi seçmediyseniz, bir uyarı mesajı görüntülenecek. Bunu gözden geçirmenizi tavsiye ederiz.

Pencereyi kapatmak için **Tamam** seçeneğini tıklayın.

4.3.6. Silinmiş Kayıtları Kurtarma

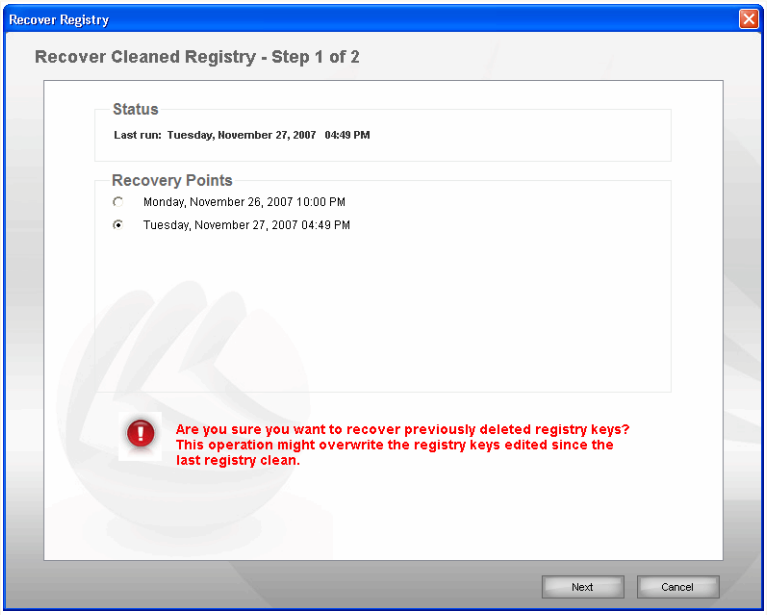
Bazen kayıt temizleme işleminden sonra, kayıp kayıt anahtarlarından dolayı sisteminizin iyi çalışmadığına dair uyarı alabilirsiniz veya bazı uygulamalar hata verebilir. Bunun nedeni belki de paylaşılan anahtarların kayıt silme esnasında silinmiş olması olabilir. Bu problemi çözmek için, silinen kayıtları kurtarılmalıdır.

Silinen kayıtları kurtarmak için, Güvenlik Merkezindeki **İyileştirme** tabından **Kayıt Kurtarma'** yı tıklayın.

Önemli
Sadece yönetim hakları olan kullanıcılar silinen kayıtları kurtarabilir.

Adım 1/2 - Kayıt Kurtarmayı Başlatmak

Burada temizlenen kayıt defterini kurtarmayı başlatabilirsiniz.



Durum

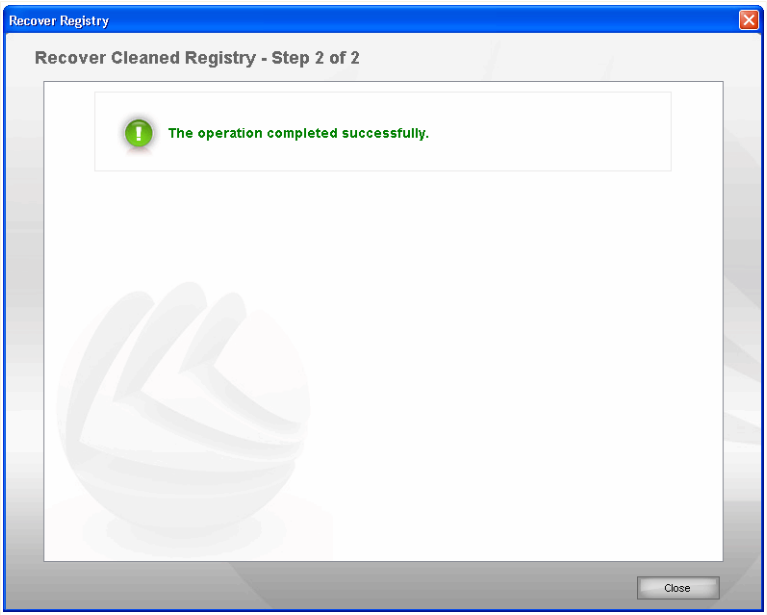
Windows kayıt defterinin son temizlendiği zamanı görebilirsiniz.

Silinen kayıt anahtarlarını kurtarmaya eminseniz **İleri**'yi tıklayınız.

Uyarı
Temizlenen kayıtların kurtarılması, son temizlemede silinen kayıtları anahtarlarını tekrar üzerine yazacaktır.

Adım 2/2 – Sonuçları Görüntüle

Burada kurtarmanın başarılı olup olmadığını görebilirsiniz.

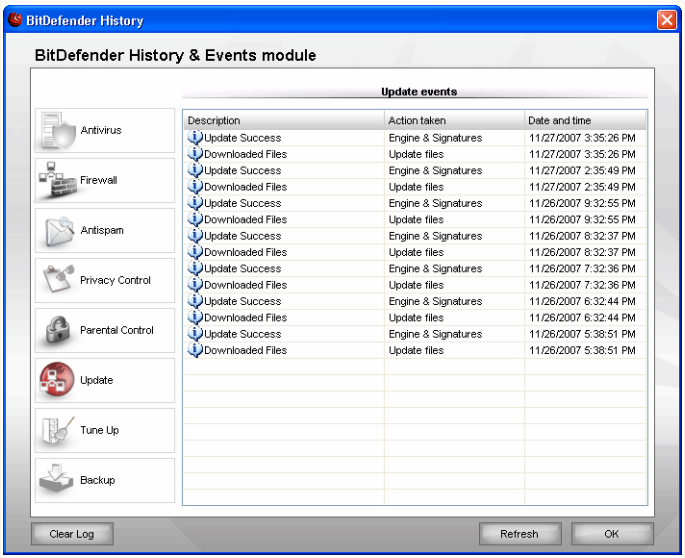


Sonuçlar

Pencereyi kapatmak için **Tamam** seçeneğini tıklayın.

5. Geçmiş

BitDefender Güvenli Merkezi penceresinin alt sağ köşesinde bulunan **Geçmiş** linkine tıkladığınızda, geçmiş & olaylar penceresi açılır. Bu pencerede güvenlikle ilgili olaylar yer alır. Örneğin güncellemelerin başarı durumu, varsa bilgisayarınızda bulunan kötücül yazılımlar, başarıyla tamamlanan yedekleme görevleri gibi.



Olaylar

Size yardımcı olmak amacıyla BitDefender geçmiş & olaylar penceresinin sol tarafında, kategoriler tek tek sıralanmıştır.

- **Antivirus**
- **Güvenlik Duvarı**
- **Antispam**
- **Gizlilik Kontrolü**
- **Ebeveyn Kontrolü**
- **İyileştirme**
- **Yedekleme**
- **Güncelle**

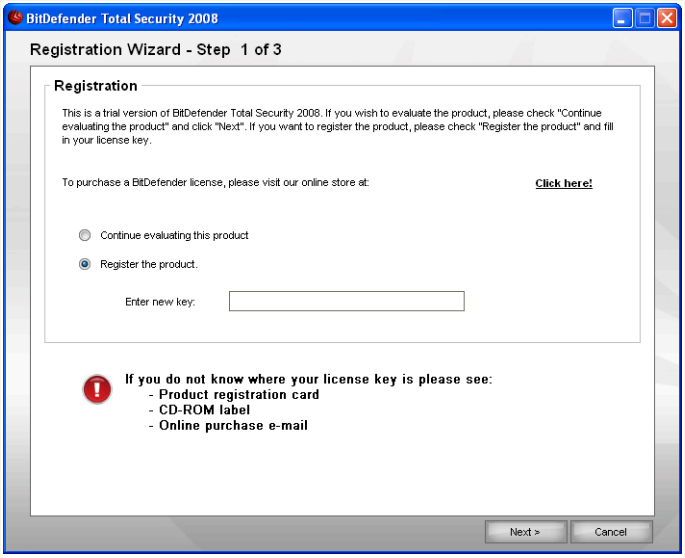
Olaylar listesi her kategori için geçerlidir. Her olay bir bilgi içerir: Kısa bir açıklama, BitDefender' in ne gibi bir işlem yaptığı, hangi tarih ve saatte meydana geldiği gibi. Eğer belirli bir olay hakkında daha fazla bilgi almak istiyorsanız, o olaya çift tıklamanız yeterlidir.

Eğer kayıtları silmek istiyorsanız, **Kayıtları Sil** veya listeyi yenilemek istiyorsanız, **Yenile** tuşuna basınız.

6. Kayıt

BitDefender Total Security 2008, 30 günlük deneme sürümü ile birlikte gelir. BitDefender Total Security 2008' i kayıt etmek istiyorsanız, lisans anahtarını değiştirmek veya bir BitDefender hesabı yaratmak için, BitDefender Güvenlik Merkezi penceresinin üst tarafındaki **Kayıt** linkine tıklayın. Kayıt sihirbazı 5 adımlı bir prosedürdür.

6.1. Adım 1/3 - BitDefender Total Security 2008' i Kaydedin



Kayıt

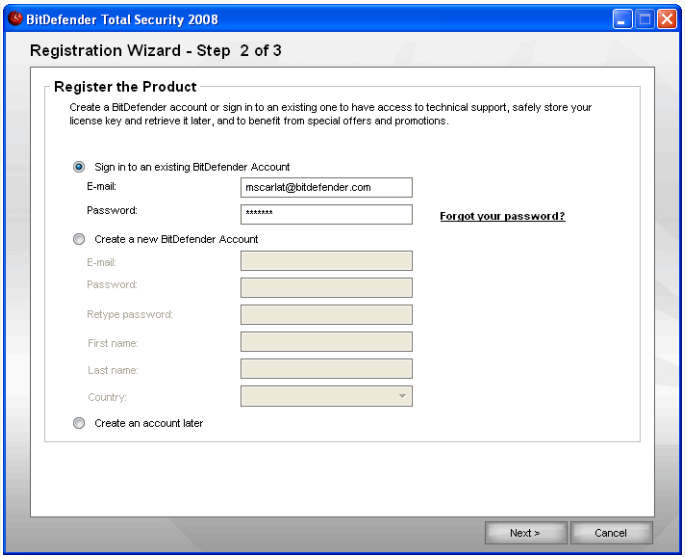
Eğer BitDefender lisansınız yok ise, linke tıklayarak BitDefender online satış mağazasından bir lisans anahtarı alın.

BitDefender Total Security 2008' i kaydetmek için **Ürünü kaydet** seçeneğini seçin. **Yeni anahtarı gir** alanına lisans anahtarını yazın.

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

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

6.2. Adım 2/3 BitDefender Hesabının Açılması



Hesap Yaratma

BitDefender hesabım yok

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

Not
BitDefender hesabınızı daha sonra yaratmak istiyorsanız uygun seçeneği seçiniz.

BitDefender hesabı açmak için **BitDefender Hesabı Yarat** seçeneğini seçip, gerekli alanları doldurun. Internet bağlantısı gereklidir. Burada sağlayacağınız bilgiler gizli kalacaktır.

- **E-mail** – Email adresinizi girin.

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

Not
Şifre en az dört karakter uzunluğunda olmalıdır.

- **Şifreyi Tekrar Gir** – daha önce tanımlanan kullanıcı için geçerli bir şifreyi tekrar girin.
- **Ad** – Adınızı girin.
- **Soyad** – Soyadınızı girin.
- **Ülke** – Ülke adını seçin.

Not
E-mail adresinizi ve şifrenizi kullanarak http://myaccount.bitdefender.com hesabınıza girin.

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.

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

BitDefender hesabım var

Eğer daha önceden bilgisayarınızda bir hesabınız varsa, BitDefender bunu otomatik olarak algılayacaktır. Bu pencereyi kapatmak istiyorsanız,**İleri**' ı tıklayınız.

Zaten bir BitDefender hesabınız varsa, **BitDefender Hesabınıza girin** Hesabınız e-posta adresiniz ve hesap şifrenizden oluşur.

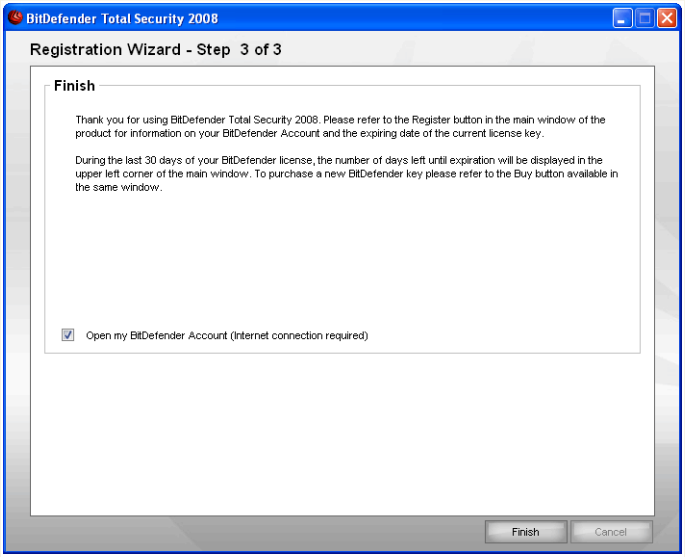
Not

Yanlış bir şifre girerseniz, **İleri** tıkladığınızda şifreyi yeniden yazmanız istenecektir. Yeniden şifre girmek için **İleri** seçeneğine tıklayın. Devam etmek için **İleri** veya sihirbazdan çıkmak için **İptal** seçeneğine tıklayın.

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

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

6.3. Adım 3/3 - BitDefender Total Security 2008' i Kaydedin



Özet

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

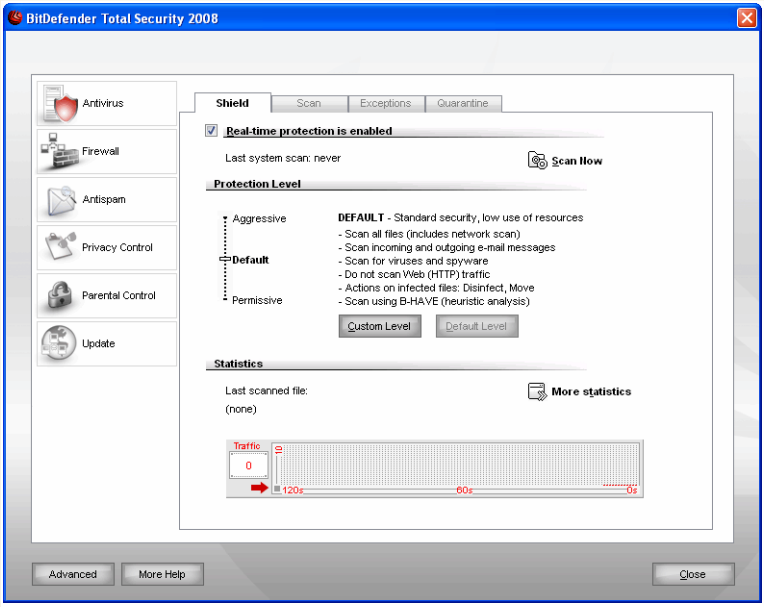
Pencereyi kapatmak için **Bitir** seçeneğini tıklayın.

Gelişmiş Güvenlik Yönetimi

7. Yönetim Konsolu

BitDefender Total Security 2008, BitDefender' ı gelişmiş olarak ayarlayıp yönetebilmek için bir merkezi yönetim konsolu ile birlikte gelir.

Bu bölüme erişmek için, Güvenlik Merkezini alt tarafındaki**Ayarlar** linkine tıklayın.



Yönetim Konsolu

Ayarlar konsolu, **Antivirus**, **Güvenlik Duvarı**, **Antispam**, **Kişisel Gizlilik Kontrolü**, **Ebeveyn Kontrolü** ve **Güncelle** modüllerinden oluşur. Bu BitDefender' ı, güvenlik sorununun tipine göre kolayca yönetmeye izin verir.

Yönetim konsolunun sol tarafında modül seçicisini göreceksiniz:

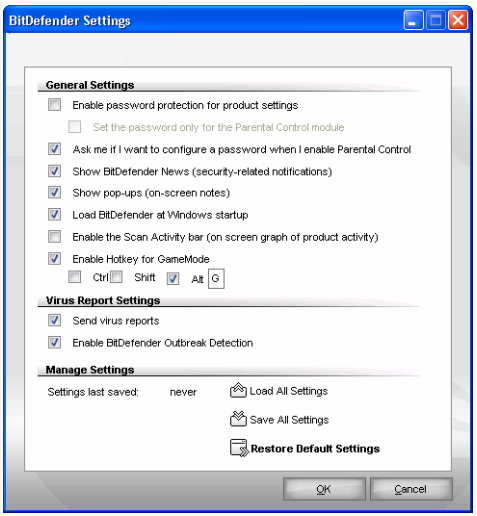
- Antivirüs – bu bölümde **Antivirüs** modülünü yapılandırabilirsiniz.
- Güvenlik Duvarı – bu bölümde **Güvenlik Duvarı** modülünü yapılandırabilirsiniz.
- Antispam – bu bölümde **Antispam** modülünü yapılandırabilirsiniz
- Gizlilik Kontrolü - bu bölümde **Gizlilik Kontrolü** modülünü yapılandırabilirsiniz.

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

Ek yardıma ihtiyacınız varsa**Daha Çok Yardım** linkine tıklayın. Bağlamsal yardım sayfası, bulunduğunuz bölüm hakkında size ayrıntılı bilgileri görüntüler.

7.1. Genel Ayarları Yapılandırma

BitDefender Total Security 2008' in genel ayarlarını yönetmek için **Gelişmiş'** e basın. Yeni bir pencere çıkacaktır.



Genel Ayarlar

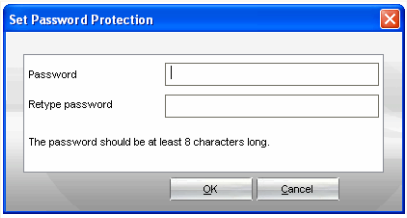
Burada, genel BitDefender davranışlarını ayarlayabilirsiniz. Fabrika ayarları olarak, BitDefender Windows başlangıcında yüklenir ve daha sonra görev çubuğunda küçültülmüş olarak çalışır.

7.1.1. 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 **Tamam**'ı tıklayın.

Bir kere şifre girdiğinizde, BitDefender ayarlarını değiştirmek istediğiniz her seferinde size şifre soracaktır. Başka sistem yöneticileri varsa, BitDefender ayarlamaları için bu şifreyi kullanmak zorundadırlar.

Sadece ebeveyn kontrolü için şifre uygulamak istiyorsanız, **Sadece Ebeveyn Kontrolü için şifre uygula** bölümünü kontrol etmelisiniz. Sadece Ebeveyn Kontrolü için şifre uygula bölümü seçili ise ve siz bu kutucuktaki işareti kaldırırsanız, artık herhangi bir BitDefender seçeneğini yapılandırmak istediğinizde şifre sorulacaktır.

Önemli
Şifreyi unuttuğunuzda, BitDefender konfigürasyonunu değiştirmek için ürünü onarmanız gerekecektir.

- **Ebeveyn Kontrolü Etkinleştirildiğinde şifre sor** seçeneği işaretli ise ve bir şifre ayarlanmamışsa, Ebeveyn Kontrolünü etkinleştirdiğinizde bir şifre ayarlanması 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. Bu opsiyonu seçili bırakmanızı tavsiye ediyoruz
- **Tarama Etkinlik Çubuğunu Etkin Kıl (ürün etkinliği ekran grafiğinde)** - Tarama Etkinlik Çubuğunu etkin yapar Tarama Etkinlik Çubuğunun görüntülenmesini istemiyorsanız, kutucuktaki işareti kaldırın.

Not
Bu seçenek sadece geçerli Windows hesabı ile yapılandırılabilir.

- **Oyun Modu için kısayol tuşunu etkin kıl** klavyeyi kullanarak oyun modunu açıp / kapatmayı mümkün kılar. Varsayılan kısayol `Alt+G` olarak belirlenmiştir.

  Kısayolu değiştirmek için aşağıdakileri yapın:

  1. Kısayol tuşunu kullanımınıza göre atamak için. Control tuşu (`Ctrl`), Shift tuşu (`Shift`) veya Alternatif tuş (`Alt`).
  2. Düzenleme sahasında, istediğiniz herhangi bir harfi kısayol olarak atayabilirsiniz.

7.1.2. 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

7.1.3. 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

8. Antivirus

BitDefender bilgisayarınızı her türlü kötücül yazılıma karşı korur (virüsler, Truva atları, spywareler, rootkitler gibi)

Dosyaların sezgisel taramasını kullanmak için. Sezgisel taramanın amacı, bir virüs tanımı 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.

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. Örnek olarak, Bitdefender bir word dökümanı açtığınızda veya bir e-mail aldığınızda onu bilinen tehditlere karşı tarayacaktır.
- **İsteğe 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. Tarama görevleri isteğe göre düzenlenebilir ve planlama dahilinde düzenli olarak çalıştırılabilir.

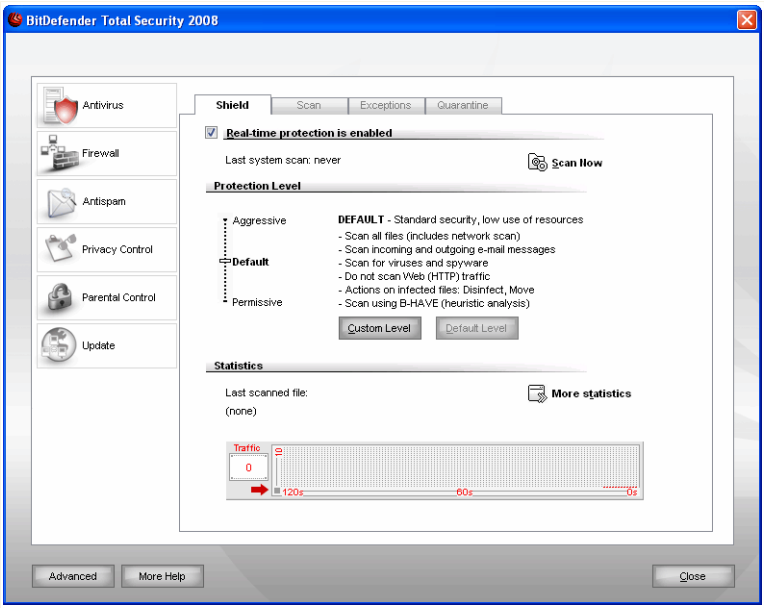
Bu kullanım kılavuzunun **Antivirüs** bölümü aşağıdaki başlıklardan oluşmaktadır.

- Erişim anında tarama
- İsteğe bağlı tarama
- Objeleri dışarıda bırakarak tarama
- Karantina

8.1. Erişim anında tarama

Erişim anında tarama erişilen dosyaları ve Anlık Mesajlaşma Yazılımlarından (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger) kurulan iletişimi tüm bilinen kötü amaçlı yazılım tehditlerine karşı tarar.

Gerçek zamanlı koruma ayarlarını konfigüre etmek için yönetim konsolundan**Antivirus>Kalkan'**ı tıklayınız Sıradaki pencere çıkacaktır:



Gerçek-zamanlı Koruma

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.

Hızlı sistem taramayı çalıştırmak için, **Şimdi Tara**' ya tıklayınız

8.1.1. Koruma Seviyesi Yapılandırma

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

3 koruma seviyesi bulunmaktadır:

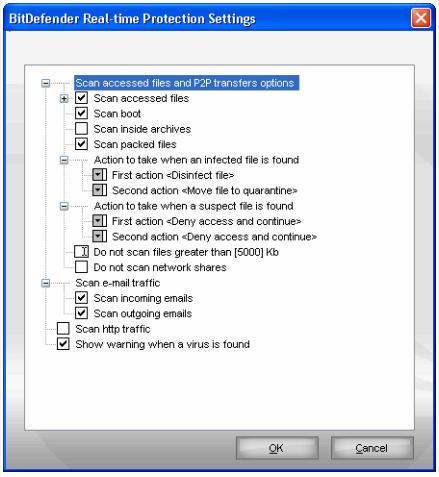
Koruma Seviyesi	Açıklama
Hoşgörülü	Temel güvenlik ihtiyaçlarını karşılar. Kaynak tüketim seviyesi çok düşüktür Yalnızca programlar ve gelen e-postalar virüse karşı taranır. Klasik imza tabanlı taramanın yanında sezgisel analiz de kullanılır. Virüs bulaşmış olan dosyalar üzerinde yapılan faaliyetler şunlardır: 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

8.1.2. Koruma Seviyesini Özelleştirme

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.

Not

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;`

Seçenek		Açıklama
		.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
	Riskware için tara	Gizli kötü amaçlı yazılımlara karşı hafızayı tarar. 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.
Boot sektörü tara		Sistem boot sektörlerini 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 dosyalara ilk uygulanacak işlemi menüden seçin
	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.

Seçenek		Açıklama
İkinci işlem		Birinci işlemin başarısız olması durumunda, virus bulaşmış dosyalara uygulamak için menüden ikinci işlemi seçin
	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.
	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
Ağ paylaşımlarını tarama		Bu seçenek etkin durumda ise, BitDefender hızlı ağ erişimi için paylaşılmış ağ klasörlerini taramayacaktır Eğer ağınızın bir bölümü antivirüs yazılımları tarafından korunuyorsa, biz bu seçeneğin etkin olmasını tavsiye ediyoruz.

- **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.

8.1.3. Gerçek-zamanlı Korumayı Kapat

Gerçek-zamanlı korumayı kapatırsanız, bir uyarı penceresi açılacaktır.

Gerçek-zamanlı Korumayı Kapat

Gerçek zamanlı korumayı ne kadar süre için kapatacağınızı menüden seçerek belirlemelisiniz. Bunu 5, 15, 30, dakika veya 1 saat için, ya da sürekli olarak veya sistem tekrar başlatılana dek kapatabilirsiniz.

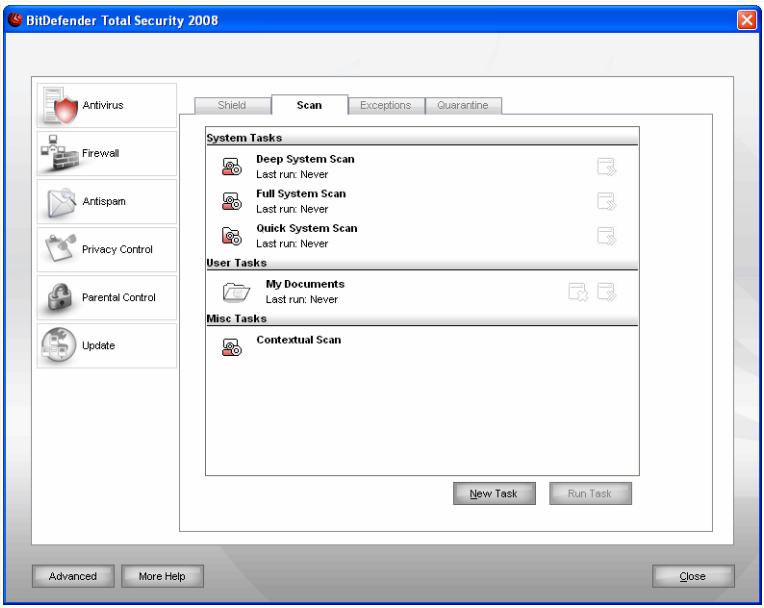
Uyarı
Bu kritik bir güvenlik sorunudur. Eğer gerçek zamanlı koruma kapatılırsa tehditlere karşı korumasız kalırsınız, bu nedenle biz bunu kısa süreler için tavsiye ediyoruz.

8.2. İsteğe bağlı tarama

BitDefender'ın temel amacı, bilgisayarınızı virüslerden uzak tutmaktır. Bunun için yapılacak ilk ve en önemli şey, bilgisayarınızı yeni virüslerden uzak tutmak ve daha sonra e-posta mesajlarınızı 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.

İsteğe bağlı taramayı yapılandırmak için, yönetim konsolundan **Antivirus>Tara**' yı tıklayın. Sıradaki pencere çıkacaktır:



Tarama Görevleri

İsteğe bağlı tarama, tarama gövleri tabanlı olup, belirli tarama seçenekleri ile belirli objeler taranabilir. İstediğinizde bilgisayarınızı varsayılan veya kendinize özgü görevlerle (kullanıcı tanımlı görevler) tarayabilirsiniz. Ayrıca zamanlanmış görevlerle, bilgisayarınız boşta iken ve işlerinizi etkilemeden, düzenli olarak tarayabilirsiniz.

8.2.1. Tarama Görevleri

BitDefender, yaygın güvenlik sorunlarına karşı, varsayılan olarak oluşturulmuş çeşitli görevlerle birlikte gelir. Ayrıca kendi düzenlediğiniz tarama görevlerini de oluşturabilirsiniz.

Her görev, onu düzenleyebileceğiniz ve tarama sonuçlarını görebileceğiniz, **Özellikler** penceresine sahiptir. Daha fazla bilgi için lütfen linke tıklayın. "*Tarama Görevlerini Yapılandırmak*" (shf. 84)

Üç tarama görevi kategorisi bulunmaktadır:

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

Varsayılan Görev	Açıklama
Derin sistem tarama	Tüm sistemi tarar. Varsayılan konfigürasyonda tüm kötücül yazılım tehditleri için tarama yapılır, virüsler, spywareler, adwareler, rootkitler ve diğerleri gibi.
Tam Sistem Tarama	Virüs ve spyware'lere karşı, arşivler hariç olarak, tüm sistemi tarar. Varsayılan konfigürasyonda tüm kötücül yazılım tehditleri için tarama yapılır, virüsler, spywareler, adwareler, rootkitler ve diğerleri gibi.
Hızlı Sistem Tarama	`Windows`, `Program Files` and `All Users` klasörleri taranır. Varsayılan konfigürasyon, her tipteki kötücül yazılımı tarar rootkitleri dışarıda tutar, fakat belleği, kayıt defterini ve çerezleri taramaz.

Not
Yoğun sistem tarama ve **Tam sistem tarama** görevleri tüm sistemi analiz edeceği için belirli bir süre almaktadır. Bu nedenle düşük öncelikli seçilmesi ve sistem boşta iken çalışması tavsiye edilir.

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

  `Belgelerim` adlı bir görev mevcuttur Bu görev, önemli kullanıcı klasörlerini taramak için kullanılır: `Belgelerim`, `Masaüstü` ve `Başlangıç` Bu, dökümanlarınızın güvenliğini sağlayacak, başlangıçta temiz çalışan uygulamalarla güvenli bir çalışma ortamında çalışmanızı sağlayacak.
- **Çeşitli görevler**– çeşitli tarama görevlerini içermektedir. Bu tarama görevleri, bu pencereden çalıştırılamayan alternatif 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.

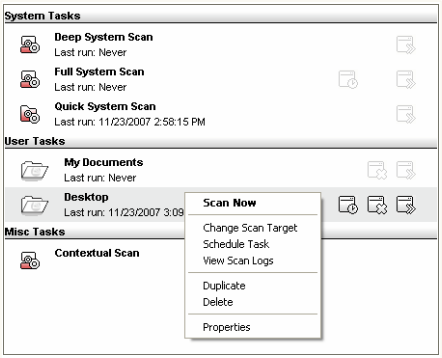
Her görevin solunda görebileceğiniz **Özellikler**butonu, görevi düzenlemeyi ve tarama kayıtlarını görebilmenizi sağlar.

8.2.2. Kısayol Menüsünü Kullanmak

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

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.



Kısayol Menüsü

Not
Sistem görevlerinde bu seçenek**Tarama Yolunu Göster** olarak değişir, sadece taranan hedefi görebilirsiniz

- **Görevi Zamanla** - seçilen görevi zamanlayabileceğiniz **Özellikler** penceresi, **Zamanlayıcı** sekmesini açar.
- **Tarama Kayıtlarını Göster** – seçilen görev çalıştırıldıktan sonra üretilen raporları görebileceğiniz **Özellikler** penceresi, **Tarama Kayıtları** sekmesini açar.
- **Çoğalt** - seçilen görevi kopyalar.

Not
Çoğaltılmış görevin ayarlarını değiştirebileceğiniz için, bu özellik yeni görev yarattığınızda yararlı olur.

- **Sil** – seçilen görevi siler.

Not
Sistem görevleri için uygun değildir. Bir sistem görevini silemezsiniz

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

Not
Farklı özellikleri nedeniyle, sadece **Özellikler** ve **Tarama Kayıtlarını Göster** seçenekleri, **Çeşitli Görevler** kategorisindeki görevler için uygundur.

8.2.3. Tarama Görevleri Yaratmak

Tarama görevi için bu metodlardan birini kullanın:

- 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.

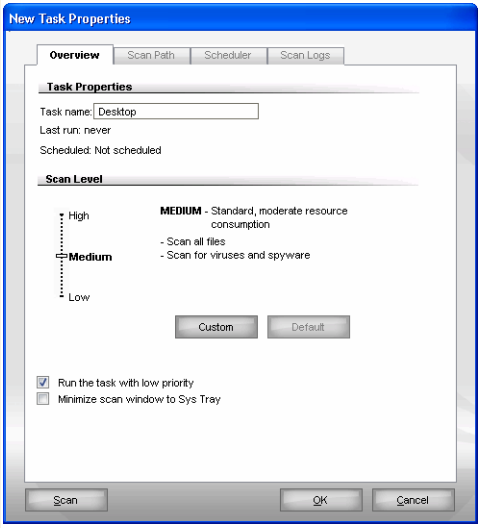
8.2.4. Tarama Görevlerini Yapılandırmak

Her tarama görevinin kendi **Özellikler** penceresi vardır. Burada tarama seçeneklerini yapılandırabilir, tarama hedefini ve görevin zamanını belirleyebilir veya raporları görebilirsiniz. Bu pencereyi açmak için, görevin sağ tarafındaki**Özellikler**butonunu tıklayın (veya görevin üzerine sağ tıklayarak **Özellikler'** i tıklayın).

Not
Daha fazla bilgi için, **Kayıtlar** sekmesine veya "*Tarama Kayıtları*" (shf. 101) bölümüne bakınız.

Tarama Ayarlarını Yapılandırma

Belirli bir tarama görevinin tarama seçeneklerini yapılandırmak için, görevin üzerine sağ tıklayarak **Özellikler'** i seçin. Sıradaki pencere çıkacaktır:



Tanıtma

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

Tarama Seviyesini Seçme

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.
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.

Koruma Seviyesi	Açıklama
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.

Tarama süreci için bir dizi genel seçenek bulunmaktadır:

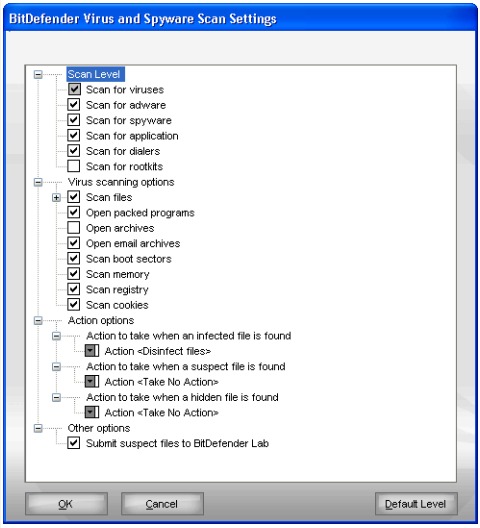
Seçenek	Açıklama
Görevi Düşük öncelikli olarak çalıştır	Tarama sürecinin önceliğini düşürür. Diğer programların daha hızlı çalışmasını ve tarama sürecinin tamamlanması için gerekli zamanı artırmayı sağlayabilirsiniz.
Tarama penceresini başlangıçta sistem tepsisine gönder	Tarama penceresini sistem tepsisi'ne gönderir. Açmak için BitDefender ikonuna çift tıklayın

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

Tarama Seviyesini Yapılandırmak

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

Tarama seçenekleri dört kategori olarak gruplanmaktadır:

- **Tarama Seviyesi**
- **Virus tarama seçenekleri**
- **İşlem seçenekleri**
- **Diğer seçenekler**

- BitDefender' in belirli tiplerdeki kötü niyetli yazılımlar için tarama yapmasını istiyorsanız, **Tarama Seviyesi** bölümünden uygun opsiyonları seçmelisiniz.

  Aşağıdaki seçenekler mevcuttur:

Seçenek	Açıklama
Virüsler için Tara	Bilinen virüsleri tarar.

Seçenek	Açıklama
	BitDefender tamamlanmamış virüs yapılarını da tespit eder, böylece olası tehditleri silerek sistem güvenliğinizi etkileyebilecek tehditlerden korur.
Adware için tara	Adware' leri tarar. Bu dosyalar virus bulaşmış dosyalar olarak ele alınır. Bu seçenek etkin kılındığında, adware bileşen içeren yazılımların çalışması durabilir.
Spyware için tara	Bilinen spyware tehditleri için taranır. Tespit edilen dosyalar virüs bulaşmış olarak ele alınacaktır.
Uygulama için tara	Uygulamalar taranır (`.exe` ve `.dll` uzantılı dosyalar).
Arayıcılar için tara	Yüksek faturalara neden olan arama uygulamaları için tarama yapılır. Bunlar tespit edildiğinde virüs bulaşmış olarak ele alınır. Bu seçenek etkinken arama bileşeni içeren yazılımların çalışması durdurulur.
Rootkitler için tarama	Gizli objeler için tarama (dosyalar ve işlemler) bunlar genel olarak rootkit olarak bilinirler.

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

  Aşağıdaki seçenekler mevcuttur:

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 aşağıdaki 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`.

Seçenek		Açıklama
	Kullanıcı tanımlı uzantıları tara	Sadece kullanıcı tarafından belirlenmiş uzantıları olan dosyalar taranacaktır. Bu uzantılar ";" ile ayrılmalıdır
Paketlenmiş programları aç		Paketlenmiş dosyaları tarar
Arşivleri aç		Dahili arşivleri tarar.
E-posta arşivlerini aç		Dahili posta arşivlerini tarar
Boot sektörlerini tara		Sistem boot sektörlerini tarar
Hafızayı tara		Virüs ve diğer kötü amaçlı yazılımlara karşı hafızayı tarar.
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 dosya üzerinde aşağıdaki işlemleri yapmayı seçebilirsiniz. Aşağıdaki seçenekler mevcuttur:

İşlem	Açıklama
Hiçbiri (nesneleri kaydet)	Virus bulaşmış dosyalar üzerinde hiç bir işlem yapılmaz. Bu dosyalar rapor dosyasında olacaktır.
Dosyaları temizle	Virüs bulaşan dosyayı temizler.
Dosyaları sil	Hiç bir uyarı vermeden virus bulaşan dosyayı siler.
Dosyaları karantinaya taşı	Virus bulaşan dosyaları karantinaya taşır.

  - Şüpheli dosyalar üzerinde aşağıdaki işlemleri yapmayı seçebilirsiniz. Aşağıdaki seçenekler mevcuttur:

İşlem	Açıklama
Hiçbiri (nesneleri kaydet)	Şüpheli dosyalar üzerinde hiç bir işlem yapılmaz. Bu dosyalar rapor dosyasında olacaktır.
Dosyaları sil	Hiç bir uyarı vermeden şüpheli dosyayı siler.
Dosyaları karantinaya taşı	Şüpheli dosyaları karantinaya taşır.

Not
Eğer sezgisel analiz tarafından şüpheli dosyalar tespit edilirse bunların BitDefender Lab.'ına gönderimi için sorulacaktır.

- Gizli (rootkit) dosyalar üzerinde aşağıdaki işlemleri yapmayı seçebilirsiniz Aşağıdaki seçenekler mevcuttur:

İşlem	*Açıklama*
Hiçbiri (nesneleri kaydet)	Gizli (rootkit) dosyalar üzerinde hiç bir işlem yapılmaz. Bu dosyalar rapor dosyasında olacaktır.
Dosyaları karantinaya taşı	Gizli (rootkit) dosyaları karantinaya taşır.
Görünür yap	Gizli (rootkit) dosyaları görebilmeniz için açığa çıkarır.

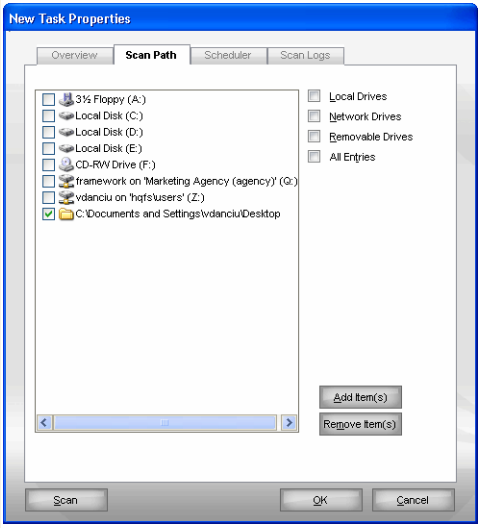
Not
Eğer tespit edilen dosyaları gözardı etmeyi seçtiyseniz ya da seçiminiz başarısızlıkla sonuçlandıysa, tarama sihirbazından bir işlem seçmek zorunda kalacaksınız.

■ Tüm şüpheli dosyaları BitDefender Lab' a bildirmek için, **Diğer seçenekler** bölümündeki **Şüpheli dosyaları BitDefender Lab' a bildir**' i seçin.

Eğer **Varsayılan Seviye**'yi tıklarsanız, varsayılan ayarları yükleyeceksiniz. Değişiklikleri kaydetmek ve pencereyi kapatmak için **Tamam**'ı tıklayın.

Tarama Hedefi Ayarı

Belirli bir kullanıcının tarama görevlerinin tarama hedefini ayarlamak için, **Tarama Hedefi Değiştir'** e sağ tıklayıp görevi seçin. Sıradaki pencere çıkacaktır:



Tarama Hedefi

Yerel ağ ve çıkarılabilir cihazların bir listesini, yanısıra önceden eklenmiş dosya ve klasörleri görebilirsiniz. Tüm işaretli nesneler görev çalıştığında taranacaktır.

Bu bölümde aşağıdaki butonlar bulunmaktadır:

- **Dosya(lar)Ekle** - taramak istediğiniz dosya (dosyaları) seçebileceğiniz bir gözatma penceresini açar

> ***Not***
> Listeye dosya/klasör eklemek için ayrıca sürükle bırak özelliğini de kullanabilirsiniz.

- **Nesne(ler)i Kaldır** önceden seçilmiş dosya/klasör ler listeden kaldırılır.

> ***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.

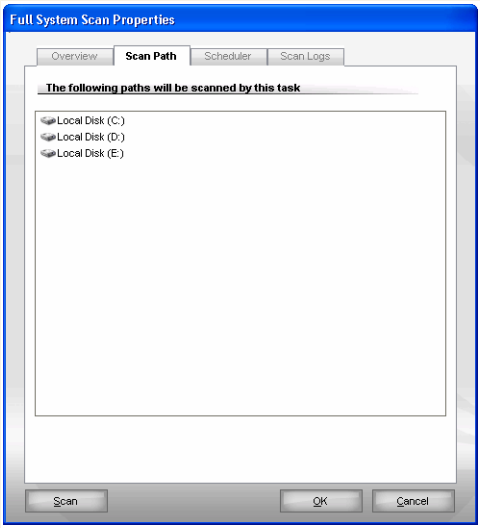
Not
Tüm bilgisayarın virüslere karşı taranmasını isterseniz, **Tüm girişler**. seçeneği yanındaki kutuyu işaretleyin.

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

Sistem Görevlerinin Tarama Hedefine Bakmak

Sistem görevlerinin tarama hedeflerini **Sistem Görevleri** bölümünden değiştiremezsiniz. Burada tarama hedefini görebilirsiniz.

Belirli bir sistem tarama görevinin hedefini görmek için, **Görev Yolunu Göster** seçeneğini sağ tıklayıp görevi seçin. **Tam Sistem Taraması** için, aşağıdaki pencere açılacaktır:



Tam Sistem Taramasının Tarama Hedefi

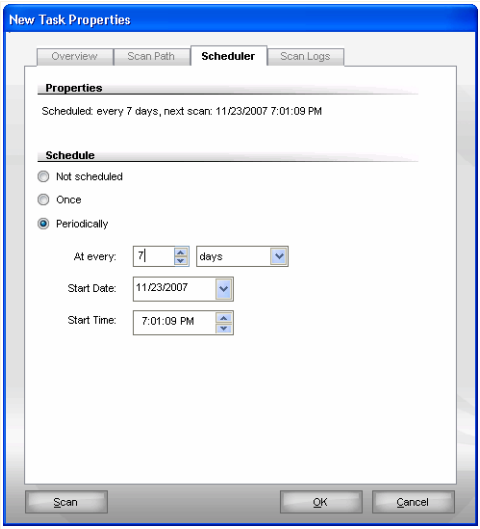
Tam sistem taraması ve **Yoğun sistem taraması** tüm yerel sürücüleri tararken, **Hızlı sistem taraması** sadece `Windows` ve `Program Dosyaları` klasörlerini tarayacaktır.

Pencereyi kapatmak için **Tamam** seçeneğini tıklayın. Görevi çalıştırmak için **Tara**'ya basınız.

Tarama Görevlerini Zamanlamak

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.

Belirli bir görevin zamanlamasını görmek veya değiştirmek için, **Görev Programlayıcı**'ya sağ tıklayıp, görevi seçin. Sıradaki pencere çıkacaktır:



Zamanlayıcı

Herhangi bir görev zamanlayıcıyı görebilirsiniz.

Bir görevi zamanlarken, aşağıdaki seçeneklerden birini seçmeniz gerekecektir:

- **Zamanlanmamış** - 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.

8.2.5. Taranan Objeler

Tarama işlemine başlamadan önce, BitDefender' ın güncellenmiş olduğundan emin olun. Güncellenmemiş bir veritabanı ile tarama yapmak BitDefender' ın yeni kötücül yazılımları bulmasına engel olacaktır. Son güncellemeleri kontrol etmek için ayarlar konsolundaki **Güncelle**' ye basın.

Not
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

Tarama Metodları

BitDefender, dört 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 2008' i seçin.
- Sürükle&Bırak taraması Tarama Etkinlik Çubuğundaki bir dosya veya klasör sürüklenip bırakılınca tarar.
- Manuel tarama – bir dosya veya klasör üzerine sağ tıklayıp BitDefender Antivirus 2008' i seçin.

Anında Tarama

Bilgisayarınızın tamamını veya bir kısmını taramak için, varsayılan tarama görevlerini kullanabilir veya kendi tarama görevlerinizi yaratabilirsiniz. Anında Tarama

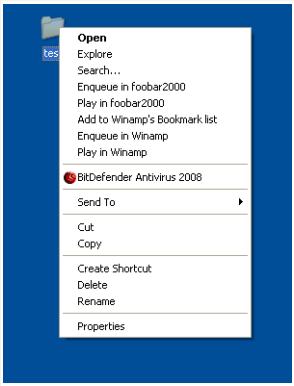
Aşağıdaki işlemlerden birini görebilirsiniz:

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

BitDefender Tarayıcı penceresi açılacak ve tarama başlatılacaktır. Daha fazla bilgi için "*BitDefender Tarayıcısı*" (shf. 97) bölümüne bakınız.

Bağlamsal Tarama

Dosya veya klasörleri yeni bir tarama görevi yaratmadan taramak için, bağlamsal tarama menüsünü kullanabilirsiniz. Bağlamsal Tarama



Bağlamsal Tarama

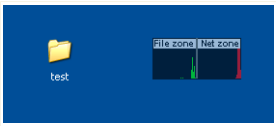
Taranmasını istediğiniz dosya veya klasöre sağ tıklayıp **BitDefender Antivirus 2008**' i seçin.

BitDefender Tarayıcı penceresi açılacak ve tarama başlatılacaktır. Daha fazla bilgi için "*BitDefender Tarayıcısı*" (shf. 97) bölümüne bakınız.

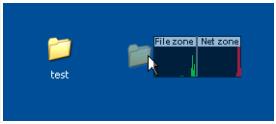
Bağlamsal Menü Tarama görevinin **Özellikler** penceresine girerek tarama seçeneklerini değiştirebilir ve rapor dosyalarını görebilirsiniz.

Sürükle&Bırak Taraması

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



Dosya Sürükle



Dosya Bırak

BitDefender Tarayıcı penceresi açılacak ve tarama başlatılacaktır. Daha fazla bilgi için "*BitDefender Tarayıcısı*" (shf. 97) bölümüne bakınız.

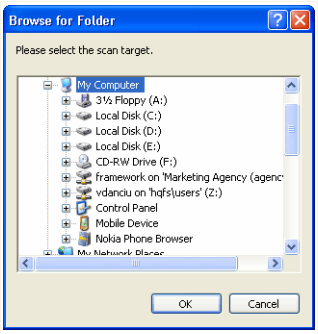
Manuel Tarama

Manuel tarama, Başlat menüsündeki BitDefender program grubundaki BitDefender Manuel Tarama seçeneğini kullanarak seçilen objeleri direk olarak taramaktan ibarettir.

Not
Manuel tarama son derece kullanışlıdır ve Windows Güvenli Mod da çalışırken dahi kullanılabilir.

BitDefender tarafından taranacak olan objeleri Windows Başlat menüsünden seçmek için şu sırayı takip edin; **Başlat → Programlar → BitDefender 2008 → BitDefender Manuel Tarama**.

Sıradaki pencere çıkacaktır:



Manuel Tarama

Taramak istediğiniz objenin üzerine tıklayıp, daha sonra**Tamam**' a tıklayın.

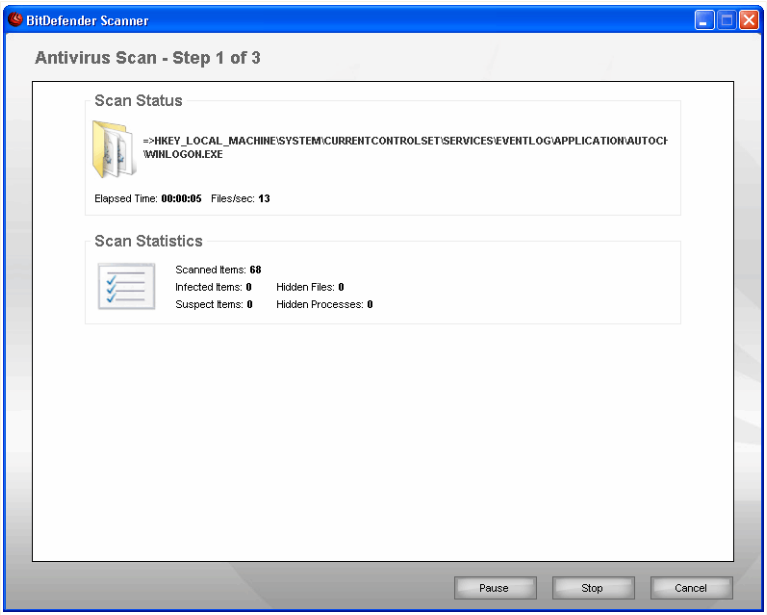
BitDefender Tarayıcı penceresi açılacak ve tarama başlatılacaktır. Daha fazla bilgi için "*BitDefender Tarayıcısı*" (shf. 97) bölümüne bakınız.

BitDefender Tarayıcısı

İsteğe bağlı taramayı başlattığınızda, BitDefender Tarayıcısı açılacaktır. Takip eden üç adımda tarama süreci rehber eşliğinde tamamlanır.

Adım 1/3 – Tarama

BitDefender seçili objeleri taramaya başlayacak.



Tarama

Tarama durumunu ve istatistikleri görebilirsiniz (tarama hızı, geçen süre, taranan sayısı / bulaşmış / şüpheli / gizli objeler ve diğerleri)

Not
Tarama süreci, taramanın karmaşıklığına bağlı olarak, belirli bir zaman alabilir

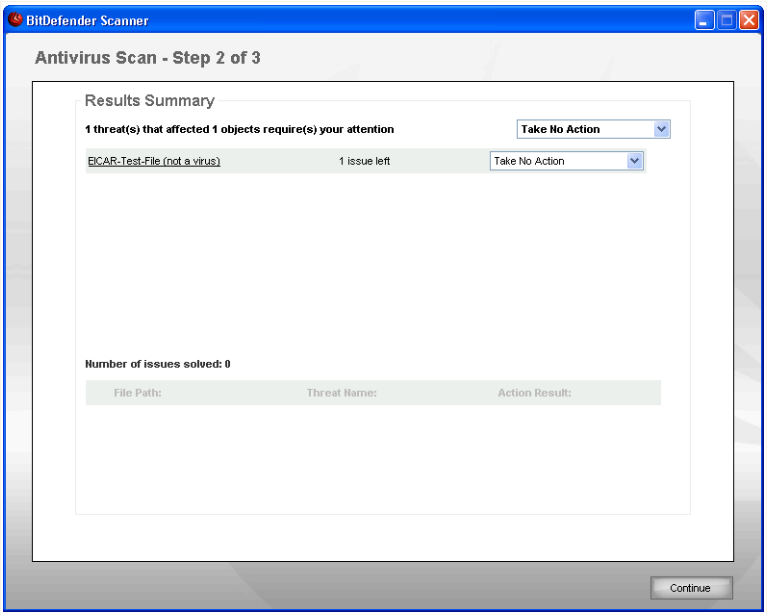
Tarama sürecini geçici olarak duraklatmak için **Duraklat**, devam etmek için **Devam** tuşuna basabilirsiniz.

Herhangi bir anda taramayı durdurmak için, **dur&Evet** tuşuna basıp son adıma geçebilirsiniz.

BitDefender' in taramayı bitirmesini bekleyin.

Adım 2/3 - İşlemi Seçin

Tarama bittiğinde, açılacak yeni pencerede tarama sonuçlarını görebilirsiniz.



İşlem

Sisteminizi etkileyen sorunun adedini görebilirsiniz.

Kötücül yazılımlar temel alınarak etkilenmiş objeler gruplarda görüntülenir. Uygun linke tıklayarak, tehditlerden etkilenmiş objeler hakkında daha fazla bilgi alabilirsiniz.

Her grup için bütün işlemleri seçebilir veya her sorun için ayrılmış işlemi seçebilirsiniz.

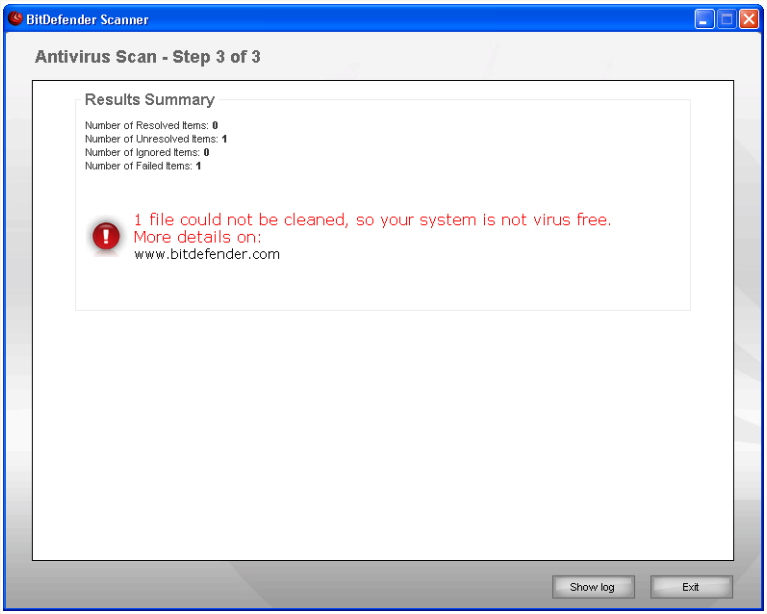
Menüde aşağıdaki seçenekler mevcuttur:

İşlem	*Açıklama*
İşlem Yapma	Virus bulaşmış dosyalar üzerinde hiç bir işlem yapılmaz.
Dosyaları temizle	Virüs bulaşan dosyayı temizler.
Dosyayı Sil	Saptanan dosyayı siler.
Açığa Çıkar	Gizli objeleri görünür yapar.

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

Adım 3/3 – Sonuçları Görüntüle

BitDefender sorunları düzeltmeyi bitirdiğinde, tarama sonuçlarının göründüğü yeni bir pencere açılır.



Özet

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

Önemli
Kurulum sihirbazının kurulum sürecinin tamamlayabilmesi için sistemi yeniden başlatmanız istenebilir.

Pencereyi kapatmak için **Tamam** seçeneğini tıklayın.

BitDefender Bazı Sorunları Çözemeyebilir.

BitDefender, birçok durumda enfekte olan dosyaları başarı ile temizler veye enfeksiyondan yalıtır Ancak, çözülemeyen sorunlar var.

Eğer çözümsüz sorunlar varsa bizim tavsiyemiz BitDefender Destek Takımı ile irtibata geçmenizdir www.bitdefender.com. Destek ekibimizbaşınıza gelen sorunları çözmede size yardımcı olacak.

BitDefender Şifre Korumalı Öğeler Algıladı

Şifre koruma kategorisi arşiv ve yükleme dosyaları olmak üzere iki tip içerir. Bunlar, eğer çalışan enfekte olan dosyalar içermiyorlarsa, sistemin güvenliği için gerçek bir tehdit oluşturmazlar.

Bu öğelerin temizliğinden emin olmak için:

- Eğer şifre korumalı öğe bir arşiv ise, dosyayı açıp onu bağımsız olarak taramak gerekir. Taranmasını istediğiniz dosya veya klasöre sağ tıklayıp **BitDefender Antivirus 2008**' i seçin.
- Eğer şifre korumalı öğe bir yükleme dosyası ise, çalıştırmadan önce, gerçek zamanlı koruma ile kontrol ettiğinize emin olun. Eğer yükleme dosyası enfekte olmuş ise, Bitdifender algılar ve enfeksiyonu izole eder.

Eğer BitDefender' ın bu öğeleri tekrar algılamasını istemiyorsanız, onları tarama harici tutulacaklara eklemelisiniz. Tarama harici tutulacaklara eklemek için, Ayarlar konsolundan **Ayarlar'** a ve sonra **Antivirus > Hariç Tut'** a tıklayın. Objeleri dışarıda bırakarak tarama

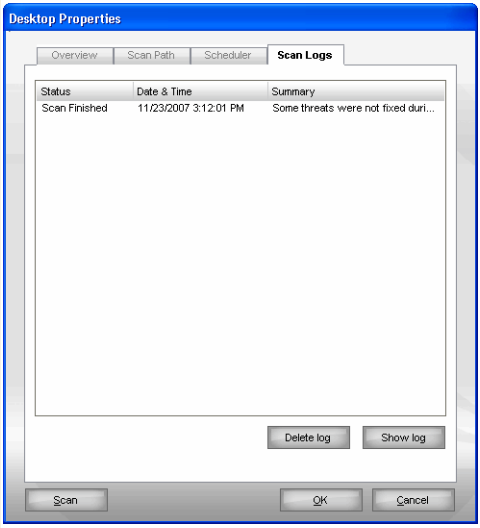
BitDefender şüpheli Dosyalar Algıladı

Sezgisel analiz tarafından saptanan şüpheli dosyalar ve henüz kötücül yazılım adıyla adlandırılmamış dosyalar.

Eğer tarama süresince şüpheli bir dosya tespit edilirse bunların BitDefender Lab.'ına gönderimi için sorulacaktır. **Tamam** tuşuna basarak bu dosyaları daha ileri araştırma için BitDefender Laboratuarlarına gönderebilirsiiniz

8.2.6. Tarama Kayıtları

Tarama kayıtlarını görmek için, görevin üzerinde sağ tıklayıp, **Tarama Kayıtları**seçeneğini seçin. Sıradaki pencere çıkacaktır:



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:

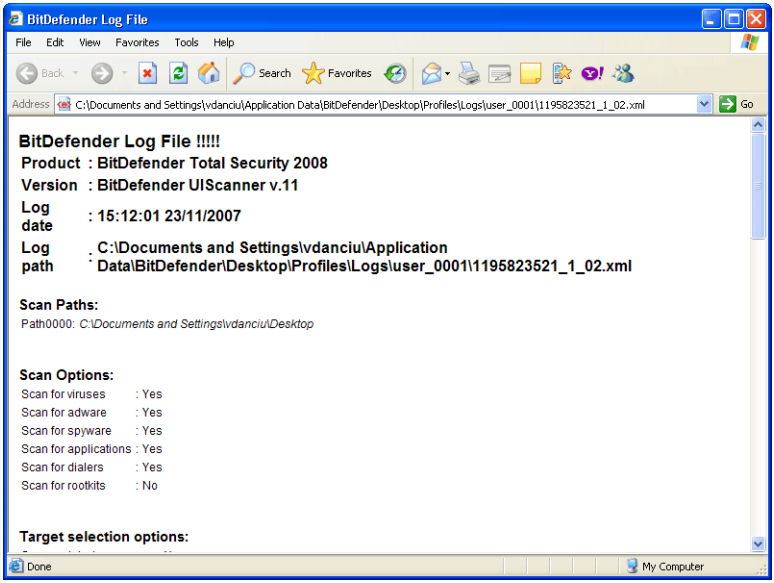
- **Kaydı sil** – seçilen rapor dosyasını silmek için
- **Kaydı göster** – seçilen rapor dosyasını görüntülemek için. Tarama kaydı geçerli web tarayıcınızda açılacaktır.

Not
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.

Tarama Kaydı Örneği

Aşağıdaki şekil tarama kaydına bir örnektir:



Tarama Kaydı Örneği

Tarama kaydı, tarama işlemine ait detaylı bilgi içerir. Tarama seçenekleri, bulunan tehditler ve bunlara uygulanan işlemler gibi.

8.3. Nesne Hariç Tarama

Çeşitli dosyaları tarama dışında tutmak isteyeyeğiniz durumlar olabilir. Örneğin EICAR dosyalarını erişim anında taramada veya `.avi` dosyalarını isteğe bağlı taramada, tarama dışında tutabilirsiniz.

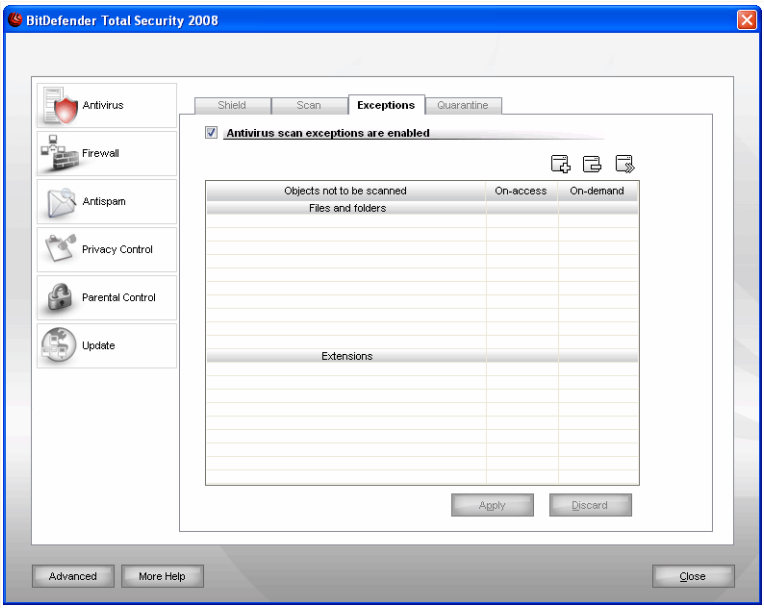
BitDefender erişim anında veya isteğe bağlı taramada yada her ikisinde birden nesneleri hariç tutmaya izin verir. Bu özellik tarama zamanını azaltmak ve işlerinizi engellememek için tasarlanmıştır.

Nesne harici tarama iki şekilde yapılabilir:

- Bir dosya veya bir klasör yolu belirleyip, tarama dışında tutabilirsiniz.
- Dosya uzantılarına göre tarama dışı olacak nesneleri seçebilirsiniz

Not
Erişim anında tarama dışında tutulan nesneler taranmayacaktır, sizin veya bir uygulamanın kullanıyor olması önemli değildir.

Nesne hariç taramayı yönetmek ve görmek için, ayarlar konsolundan **Antivirus>İstisnalar'** ı tıklayın. Sıradaki pencere çıkacaktır:



İstisnalar

Tarama dışında tutulan nesneleri (dosyalar, klasörler, uzantılar) görebilirsiniz.

Not
İstisnalar bağlamsal taramalara uygulanmayacaktır.

Bir girişi kaldırmak için, girişi seçin ve **Sil** seçeneğini tıklayın.

Bir girişi düzenlemek için, girişi seçin ve **Düzenle** seçeneğini tıklayın veya kural üzerine çift tıklayın. Yeni pencere görünecektir. Açılacak olan yeni pencerede tarama

dışı tutmak istediğiniz dosya uzantısını, dosya veya klasörleri değiştirebilirsiniz. Bunun için değişikliği yapıp **Tamam** tuşuna basın.

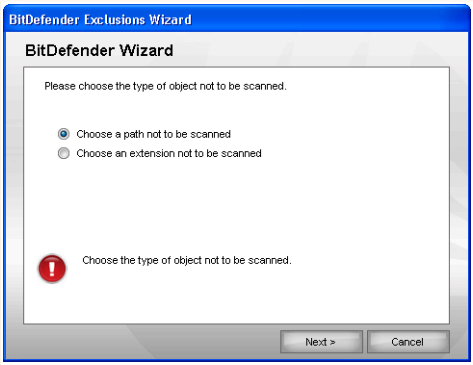
Not
Ayrıca sağ tıklayarak kısayol menüsünden, düzenleme yapabilir ya da silebilirsiniz.

Uygula' ya basarak kaydedilmediyse, **Vazgeç**' e basarak eski hale dönmeyi sağlayabilirsiniz.

8.3.1. Yolları taramadan hariç tutmak

İstediğiniz yolun hariç tutulacağı bir tarama yapmak için, **Ekle** tuşuna basınız. Size tarama boyunca rehberlik edecek yapılandırma sihirbazı görünecektir.

Adım 1/3 - Nesne Tipini Seçin

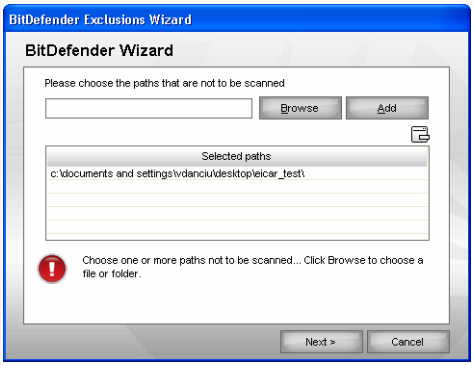


Nesne Tipi

Tarama harici tutacağınız yol tercihlerini seçin.

İleri'yi tıklayın.

Adım 2/3 – Yolu belirleyin



Hariç Tutulan Yollar

Belirlenen yolları tarama harici tutmak için iki metod vardır.

- **Gözat**'a tıklayın, taranmayacak dosya veya klasörü seçin ve **Ekle** seçeneğini tıklayın.
- Düzenleme alanına, hariç tutmak istediğiniz yolu yazmak için, **Ekle**' ye tıklayın.

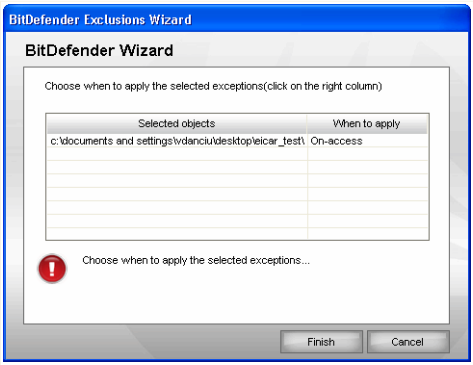
Not
Eğer yol adı yok ise bir hata mesajı alacaksınız. **Tamam**' basıp yolu kontrol edin.

Eklediğiniz yol tabloda görünecektir. İsterseniz bir çok yol daha ekleyebilirsiniz.

Bir girişi kaldırmak için, girişi seçin ve **Sil** seçeneğini tıklayın.

İleri'yi tıklayın.

Adım 3/3 – Tarama Tipini Seçin



Tarama Tipi

Tablo içeriğinde tarama harici tutulacak yolları ve tarama tipini görebilirsiniz.

Varsayılan olarak her iki tarama tipide seçili durumdadır. Değiştirmek isterseniz, sağ kolona tıklayarak arzuladığınız seçeneği seçebilirsiniz.

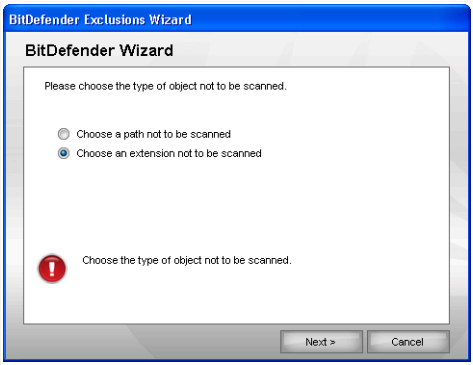
Bitir seçeneğini tıklayın.

Değişiklikleri kaydetmek için **Uygula** tuşuna basınız.

8.3.2. Uzantıları Hariç Tutarak Tarama

Uzantıları hariç tutarak tarama yapmak için, **Ekle**'ye tıklayın. Size tarama boyunca rehberlik edecek yapılandırma sihirbazı görünecektir.

Adım 1/3 - Nesne Tipini Seçin

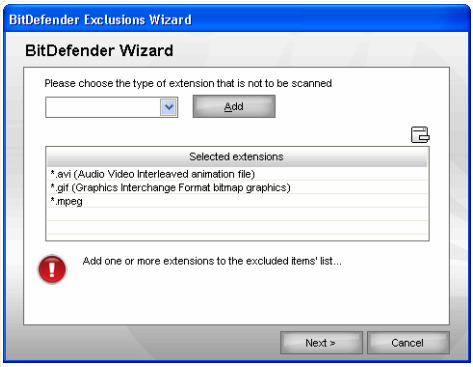


Nesne Tipi

Tarama harici tutmak istediğiniz uzantı tercihlerini seçin.

İleri'yi tıklayın.

Adım 2/3 - Tarama Harici Uzantıları Belirleyin



Tarama Harici Uzantılar

Tarama harici tutulacak uzantıları belirlemek için, aşağıdaki metodlardan herhangi birini kullanınız.

- Tarama harici tutulacak uzantıları seçmek için, **Ekle**' ye tıklayın.

> ***Not***
> Menüde sisteminize kayıtlı olan tüm uzantılar listelenecektir. Uzantıyı seçtiğinizde, eğer varsa ona ait açıklamayı görebilirsiniz.

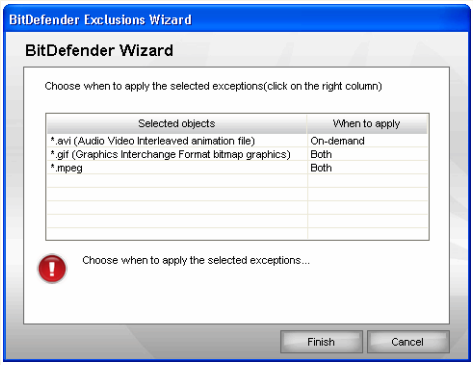
- Düzenleme alanında tarama harici tutmak istediğiniz uzantı tipini **Ekle**' ye tıklayarak seçin.

Eklediğiniz uzantı tabloda görünecektir. İsterseniz bir çok uzantı daha ekleyebilirsiniz.

Bir girişi kaldırmak için, girişi seçin ve **Sil** seçeneğini tıklayın.

İleri'yi tıklayın.

Adım 3/3 – Tarama Tipini Seçin



Tarama Tipi

Tablo içeriğinde tarama harici tutulacak uzantıları ve tarama tipini görebilirsiniz.

Varsayılan olarak her iki tarama tipide seçili durumdadır. Değiştirmek isterseniz, sağ kolona tıklayarak arzuladığınız seçeneği seçebilirsiniz.

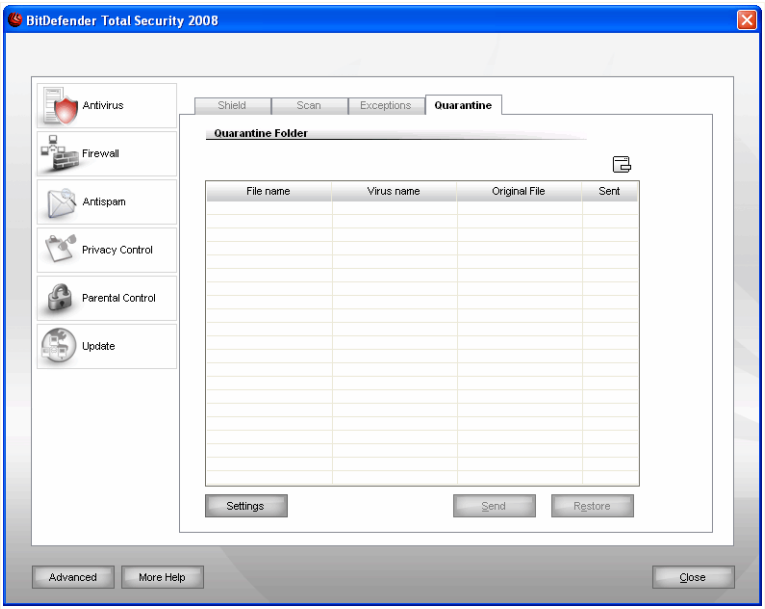
Bitir seçeneğini tıklayın.

Değişiklikleri kaydetmek için **Uygula** tuşuna basınız.

8.4. Karantina Alanı

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.

Karantinaya alınmış dosyaları görmek ve yönetmek ve karantina ayarlarını yapılandırmak için, ayarlar konsolundan**Antivirus>Karantina**' yı tıklayın.



Karantina

8.4.1. Karantinaya Alınmış Dosyaları Yönetmek

Görebileceğiniz gibi, **Karantina** bölümünde, şu ana kadar izole edilmiş dosyaların bir listesi vardır. Her dosyada dosyanın adı, boyutu, izole edilme tarihi ve BitDefender'a gönderildiği tarih bilgileri bulunmaktadır.

Not
Virüs karantinadayken, zarar veremez, çünkü çalıştırılamaz veya okunmayacaktır

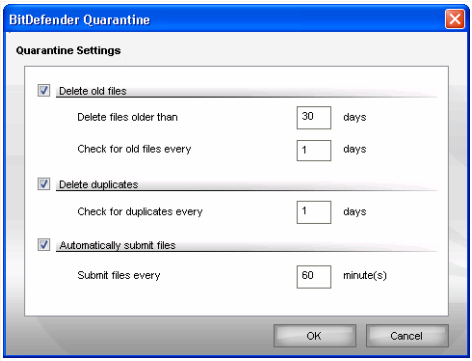
Karantinadan seçilen bir dosyayı silmek için **Kaldır** butonuna tıklayın. Seçilen bir dosyayı orijinal yerine geri yüklemek istiyorsanız, **Geri yükle**'yi tıklayın.

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

Bağlamsal Menü. Bağlamsal menü, karantinaya alınan dosyaları kolayca yönetmenize imkan verir. Ayrıca **Yenile** tuşuna basarak karantina bölümünü yenileyebilirsiniz.

8.4.2. Karantina Ayarlarını Yapılandırma

Karantina ayarlarını yapılandırmak için, **Ayarlar'** ı tıklayınız. Yeni bir pencere çıkacaktır.



Karantina Ayarları

Karantina ayarlarını kullanarak, BitDefender' ın aşağıdaki işlemleri otomatik olarak yapmasını sağlayabilirsiniz:

Eski dosyaları siler. Eski karantina dosyalarını otomatik olarak silmek için, uygun seçeneği kontrol edin. Karantinadaki dosyaların silinmesi ve BitDefender' ın eski dosyaları belirli frekanslarla kontrol etmesi için gün sayısı belirlemelisiniz.

Not
Varsayılan olarak, BitDefender hergün eski dosyaları kontrol edip 10 günden eski olanları silecektir.

Silme Tekrarı. Karantinadaki dosyaları silme tekrarı otomatik olarak gerçekleşir. Uygun seçeneği kontrol edin. Birbirini takip edecek silme tekrarlarının arası için gün sayısı belirlemelisiniz.

Not
Varsayılan olarak, Bitdefender karantinadaki dosyaları silme tekrarı için hergün kontrol eder.

Otomatik olarak gönderilen dosyalar. Dosyaları karantinaya otomatik olarak göndermek için uygun seçeneği kontrol edin. Gönderilecek dosyalar için bir frekans belirlemelisiniz.

Not
Varsayılan olarak, BitDefender her 60 dakikada bir yapacaktır.

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

9. Güvenlik Duvarı

Güvenlik duvarı bilgisayarınızı, gelen ve giden yetkisiz bağlantı girişimlerine karşı korur. Bu, kapıdaki bir korumaya benzer – Internet bağlantınızı dikkatli bir şekilde denetler ve kime Internet'e erişim izni verileceğini ve kimin engelleneceğinin takibini yapar.

Not
Güvenlik duvarı, eğer bir geniş band veya DSL bağlantınız varsa çok gereklidir.

Gizlilik (stealth) modunda, bilgisayarınız kötü amaçlı yazılım ve bilgisayar korsanlarından "gizlenmektedir". Güvenlik duvarı, port taramalarını ("erişim noktaları"nı bulmak için bir makineye gönderilen paketler akışı, genellikle bir saldırı için hazırlık yaparken) otomatik olarak tespit etme ve bunlara karşı koruma özelliğine sahiptir.

Bu kullanım kılavuzunun **Güvenlik Duvarı** bölümü aşağıdaki başlıklardan oluşmaktadır:

- Güvenlik Duvarı Kavrama
- Güvenlik Duvarı Durumu
- Trafik Koruma
- İleri Ayarlar
- Güvenlik Duvarı Aktivitesi
- Ağ Bölgesi

9.1. Güvenlik Duvarı Kavrama

BitDefender Güvenlik Duvarı, sizin onu yapılandırmanıza gerek kalmadan ağınız ve internet bağlantınız için en iyi korumayı sağlamak üzere tasarlanmıştır. İnternete direk olarak bağlı olmanız, basit bir ağ yapısına veya geniş ve çeşitli bir ağ yapısına (Ethernet, kablosuz, VPN veya diğer ağ tipleri gibi) sahip olmanız önemli değildir. Güvenlik duvarı kendini bulunduğu ortama adapte edecektir.

Varsayılan olarak BitDefender, bilgisayarınızdaki ağ yapılandırmasını otomatik olarak saptayacak ve uygun temel bir güvenlik duvarı profili yaratacaktır. Aynı zamanda yapılandırmaya bağlı olarak, saptadığı ağları güvenilir veya güvenilmez olarak yarattığı profile ekleyecektir.

9.1.1. Güvenlik Duvarı Profili Nedir?

Bir güvenlik duvarı profili ağ ve internet erişimi kontrol uygulamalarının kurallarını ayarlamak anlamına gelir.

Bilgisayarınızdaki ağ yapılandırmasına bağlı olarak, BitDefender belli bir tipte profil yaratır. Yaratılan temel profil, sistem uygulamaları ve BitDefender bileşenleri tarafından istenen, ağ erişim kurallarını veya internet erişim kurallarını içerir.

Not
Temel bir profil, kaç adet ağa bağlı olduğunuzu göz önüne almadan yaratılır.

Üç adet temel profil bulunmaktadır:

Profil	*Açıklama*
Doğrudan bağlantı	İnternete direk olarak bağlanan bir ağ yapılandırması için tavsiye edilen temel internet erişim kurallarını içerir. Kurallar, her bir ağ kullanıcısının sizin bilgisayarınına erişimine ya da sizin ağa göz atmanıza izin vermez.
Güvenilmeyen	Güvenilmeyen bir ağ yapısı ile ilgili olarak, tavsiye edilen temel internet erişim kurallarını içerir. Kurallar, sizin ağa göz atmanıza izin verirken, diğer ağ üyelerinin sizin bilgisayarınıza erişimini engeller.
Güvenilir	Güvenilir bir ağ yapısı ile ilgili olarak, tavsiye edilen temel internet erişim kurallarını içerir. Erişilen ağda herhangi bir sınırlama yapılmaz. Bu tüm ağ paylaşımlarına erişimi içerir, ağ yazıcıları ve diğer ağ kaynakları gibi. Aynı zamanda diğer ağ üyeleri sizin bilgisayarınıza bağlanıp paylaşımlarınıza erişebilirler.

Uygulamalar internete bağlanmayı denediğinde, ona tahsis edilen kurallar profile eklenir. Uygulamaların internete erişimi için henüz yapılandırılmamış kurallarda siz, "izin ver" veya "reddet" olarak seçim yapabilirsiniz, ya da "sadece beyaz listede olanlara izin ver" ve "diğer uygulamaların izinleri için sor" diyebilirsiniz.

Not

Uygulamaların internete ilk kez bağlandığındaki erişim politikalarını belirlemek için, Durum bölümüne gidip koruma düzeyini ayarlayın. Var olan profili düzenlemek için, Trafik bölümünden **Profil Düzenle**' yi tıklayın.

9.1.2. Ağ bölgesi nedir?

Bir ağ bölgesi, ağın içindeki bir bilgisayarı ya da sizin bilgisayarınızdan ayrılmış tüm ağı veya tam aksine bilgisayarınızın bağlandığı bir ağı temsil eder. Pratik olarak bir ağ bölgesi sizin bilgisayarınıza izin veren ya da reddeden IP adresi veya IP adres aralığından oluşur.

Varsayılan olarak, BitDefender özel ağ yapılandırmaları için bölgeleri otomatik olarak ekler. Bir bölge, yaratılan uygun ağ erişimi kuralları tarafından eklenir, tüm ağdaki geçerli profiller için uygulanabilir.

Bölgelerin iki tipi vardır:

Bölge Tipi	Açıklama
Güvenilir Bölge	Güvenilir bölgeden olan bilgisayarlar sizin bilgisayarınıza bağlanabilir ve siz de onlara bağlanabilirsiniz. Böyle bir bölgeden gelen tüm bağlanma denemeleri, aynı zamanda sizin bilgisayarınızdan böyle bir bölge için gelen bağlantı denemeleri kabul edilir. Eğer bir ağ güvenilir bölge olarak eklenmiş ise, ağ yazıcıları ve diğer ağ kaynakları gibi ağ paylaşımlarına sınırsız erişebilirsiniz. Ayrıca ağ üyeleri de sizin bilgisayarınız ve paylaşımlarınıza ulaşabilirler.
Güvenilmeyen Bölge	Güvenilmeyen bölgeden olan bilgisayarlar size bağlanamazlar ve sizde onlara bağlanamazsınız. Böyle bir bölgeden gelen tüm bağlanma denemeleri, aynı zamanda sizin bilgisayarınızdan böyle bir bölge için gelen bağlantı denemeleri bloklanır. ICMP trafiği reddedilmiş ve Gizlilik Modu etkin ise, bilgisayarınız pratik olarak o bölgedeki bilgisayarlar için görünmezdir.

Not

Bir bölgeyi düzenlemek için, Bölgeler bölümüne gidin. Bir bölge ile ilgili kuralı düzenlemek için, Trafik bölümüne gidin ve **Profil Düzenle**' ye tıklayın.

9.1.3. Güvenlik Duvarı Operasyonu

Sisteminiz ilk yüklemeden sonra tekrar başladığında, BitDefender ağ yapılandırmanızı otomatik olarak tanır, uygun olan temel profili yaratır ve saptanan ağa bağlı olarak bir bölge ekler.

Not

Eğer internete direk olarak bağlı iseniz, uyan ağ yapılandırması için ağ bölgesi yaratılmaz. Eğer birden fazla ağa bağlı iseniz, bağlanılan ağlara göre sırası ile bölgeler eklenir.

Başka bir ağa bağlandığınızda ya da ağ bağlantınızı kapattığınızda her zaman ağ yapılandırmaları değişir, yeni bir güvenlik duvarı profili yaratılır. Aynı zamanda ağ bölgesi buna göre değiştirilir.

Yeni bir güvenlik duvarı profili yaratıldığında, eski profil kaydedilir, siz önceki ağ yapılandırmasına dönmek istediğinizde geri yüklenebilir.

Ağ yapılandırmasına bağlı olarak, BitDefender yapılandırmayı kendi kendine yapacaktır. Bu BitDefender Güvenlik Duvarının varsayılan olarak nasıl yapılandırıldığıdır:

- Eğer internete direk olarak bağlanıyorsanız, bağlı olduğunuz diğer ağların önemi yoktur, bir Direk Bağlantı profili yaratılır. Aksi taktirde BitDefender bir Güvenilmeyen güvenlik duvarı profili yaratacaktır.

  Not

  Bir güvenlik durumu olduğu için güvenilen profiller varsayılan olarak yaratılmaz. Güvenilir bir profil yaratmak için, var olan profili sıfırlamanız (reset) gerekmektedir. Daha fazla bilgi için bakınız, “*Profillerin Sıfırlanması*” (shf. 128).

- Ağ yapılandırmasına bağlı olarak eklenen bölgeler.

Bölge Tipi	*Ağ Yapılandırması*
Güvenilir Bölge	**Ağ geçidi atanmamış özel IP** - Bilgisayar yerel ağın (LAN) bir parçasıdır ve internete bağlanamaz. Örnek olarak bu gibi durumlar aile üyelerinin dosya, yazıcı ya da diğer kaynak paylaşımlarına izin vermek için yaratılan ev ağlarında söz konusudur.
	Etki alanı için özel IP Bilgisayar yerel ağın (LAN) bir parçasıdır ve bir etki alanına bağlıdır. Bu gibi durumlara örnek; ofis kullanıcılarının dosya, yazıcı ya da diğer kaynak

Bölge Tipi	Ağ Yapılandırması
	paylaşımlarına bir etki alanı içinde izin vermektir. Bir etki alanı, mevcut bir takım politikalar ile bu politikalar ile çalışan üye bilgisayarlardan oluşur.
Güvenilmeyen Bölge	**Açık (güvenilmeyen) kablosuz ağ** - Bilgisayar kablosuz ağın (WLAN) bir parçasıdır. Bu gibi durumlara örnek; Halka açık yerlerde ücretsiz internet erişimleri kullanıldığında söz konusu olur.

Not

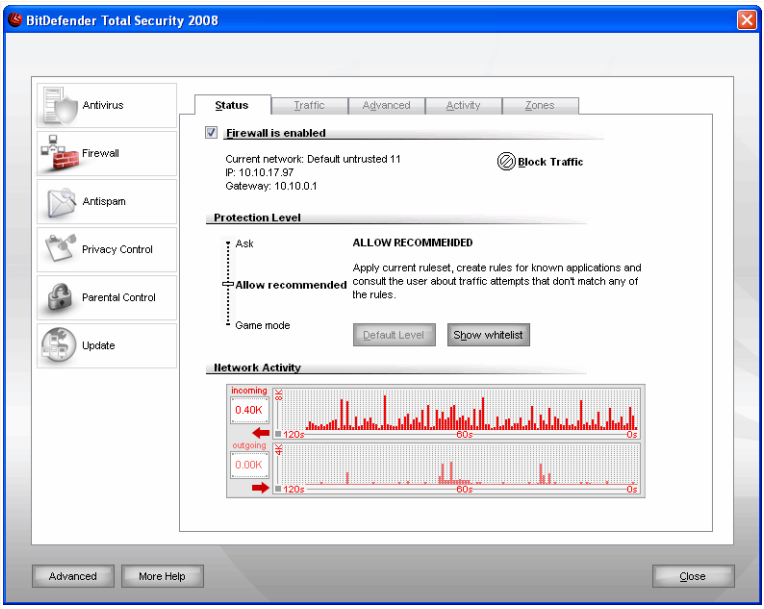
Bazı ağ yapılandırılmaları için bölgeler yaratılmaz, örneğin:

- **Halka açık (yönlendirilebilir) IP** - Bilgisayar direk olarak internete bağlıdır.
- **Etki alanı olmadan, ağ geçidi ile özel IP** - Bilgisayar herhangi bir etki alanına üye olmadan ağın bir parcasıdır, ve internete ağ geçidi üzerinden bağlanır. Örnek olarak bu gibi durumlar, okul kampüs ağlarında dosya, yazıcı ya da diğer kaynak paylaşımlarına izin vermek içindir.

- Gizlilik (Stealth) Modu Etkin.
- İzin verilen VPN ve Uzaktan bağlantı.
- İnternet Bağlantı Paylaşımı' na güvenilmeyen bölgeler için izin verilmez.
- Beyaz listedeki uygulamaların erişimine otomatik olarak izin verilir, oysa diğer uygulamalar ilk bağlanma denemelerinde izin almak için size sorulacaktır.

9.2. Güvenlik Duvarı Durumu

Güvenlik Duvarı koruma ayarlarını yapılandırmak için, ayarlar konsolundan **Güvenlik Duvarı >Durumu**' nu tıklayınız Sıradaki pencere çıkacaktır:



Güvenlik Duvarı Durumu

Bu bölümde, **Güvenlik Duvarını** etkin/etkisiz kılabilir, tüm ağ/Internet trafiğini engelleyebilir ve yeni olaylar için varsayılan davranışları belirleyebilrsiniz.

Önemli
Internet saldırılarına karşı korunmak için, **Güvenlik Duvarını** etkin bırakın

Tüm Internet trafiğini engellemek için sadece **Trafiği Engelle** seçeneğine tıklayın. Bununla, bilgisayarınızı ağdaki diğer bilgisayarlardan izole edilmesini sağlayacaksınız.

Tüm ağ/Internet trafiğini engellememek için **Trafiği Engelleme** seçeneğine tıklayın.

Bölümün alt kısmında, gelen ve giden trafikle ilgili BitDefender istatistiklerini görebilirsiniz. Grafikte, son iki dakikadaki internet trafiği hacmi gösterilmektedir.

Not
Grafik, **Güvenlik Duvarı** etkin olmasa bile görünecektir.

9.2.1. Koruma Seviyesi Yapılandırma

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

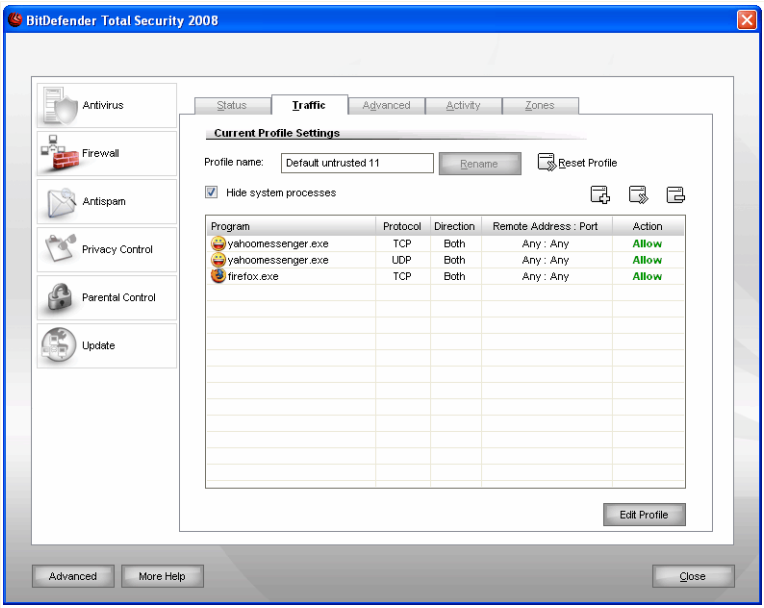
3 koruma seviyesi bulunmaktadır:

Koruma Seviyesi	*Açıklama*
Oyun Modu	Mevcut kurallara uymayan trafik girişimlerine izin verilip verilmeyeceğini sorar. Mevcut kurallara uymayan trafik girişimlerine bilgi istenmeden izin verir. Bu politika kesinlikle tavsiye edilmemektedir, fakat ağ yöneticileri için yararlı olabilir.
İzin ver	BitDefender tarafından yasal olduğu bilinen programlardan dışarı giden tüm bağlantı girişimlerine izin verir. Trafik bölümünde, yaratılan trafik kurallarını görebilirsiniz. Beyaz listelenmiş programlar, dünyada en yaygın kullanılan uygulamalardır. Bunlar arasında çok iyi bilinen web tarayıcıları, ses&video oynatıcıları, sohbet ve dosya paylaşım programları ve sunucu istemci ve işletim sistemi uygulamaları bulunmaktadır. Hangi programların beyaz listede olduğunu görmek için **Beyaz Liste**' yi tıklayın.
Sor	Mevcut kurallara uymayan trafik girişimlerine izin verilip verilmeyeceğini sorar.

Varsayılan Düzey' e tıklayarak varsayılan politikaya getirebilirsiniz (**İzin Ver**).

9.3. Trafik Kontrolü

Geçerli profilin güvenlik duvarı kurallarını yönetmek için, ayarlar konsolundan **Güvenlik Duvarı>Trafik'** i tıklayın. Sıradaki pencere çıkacaktır:



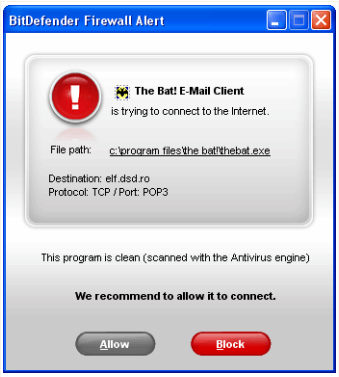
Trafik Kontrolü

Bu bölüm gelen veya giden bağlantılardan hangisine izin verileceğini, hangisinin reddedileceğini kesin olarak tanımlamaktadır. Belirli protokoller, portlar, uygulamalar ve/veya uzak adresler ile ilgili kuralları tanımlamaktadır.

Kurallar otomatik olarak (uyarı penceresiyle) veya manuel olarak (**Ekle** butonuna tıklayın ve kural parametrelerini seçin) girilebilir.

9.3.1. Otomatik Kural Ekleme

Güvenlik Duvarı etkin iken, her Internet'e bağlantı yapıldığında, BitDefender sizin izninizi ister.



Güvenlik Duvarı Uyarısı

Aşağıdakileri görebilirsiniz: Internet' e erişmek isteyen uygulama, protokol, IP adresi ve uygulamanın üzerinden bağlanmaya çalıştığı port .

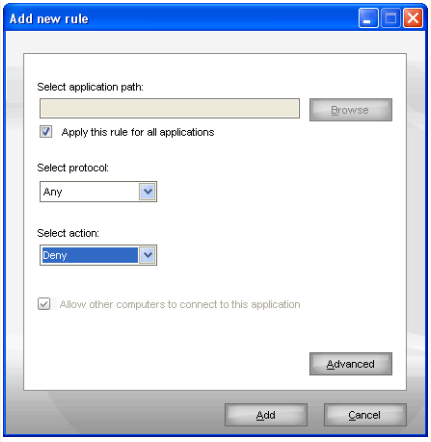
İzin Ver' e tıklarsanız IP protokolü ve tüm portlar üzerinden bu uygulamanın oluşturduğu tüm gelen ve giden trafiğe izin vermiş olursunuz. Eğer **Engelle**' ye tıklarsanız uygulamanın IP üzerinden internete erişimi reddedilecektir.

Cevabınıza dayalı olarak bir kural yaratılacak, tabloda listelenecek ve uygulanacaktır. Bir sonraki sefer uygulama bağlanmayı denediğinde, bu kural varsayılan olarak uygulanacaktır.

Önemli
Sadece açıkça güvendiğiniz IP'ler veya Alan adlarından gelen bağlantı girişimlerine izin verir.

9.3.2. Manuel Kural Ekleme

Kural Ekle tuşuna basınız ve kural için parametreler seçiniz. Sıradaki pencere çıkacaktır:



Kural Eklemek

Yeni bir güvenlik duvarı kuralı eklemek için bu adımları takip edin:

1. Yeni güvenlik duvarı kuralı eklenecek uygulamayı seçin.

   Uygulamayı seçmek için, **Gözat'** a basıp yerini belirledikten sonra, **Tamam'** a basın

   Tüm uygulamalar için bir kural yaratmak istiyorsanız sadece, **Bu kuralı tüm uygulamalar için uygula'** yı seçmeniz yeterli.
2. Kural uygulanacak protokolü seçin.

   Belirli bir protokolü seçmenize yardım etmek amacıyla, en yaygın kullanılan protokollerin listesi sağlanmıştır. İlgili menüden istenen protokolü seçin (kuralın uygulandığı) veya tüm protokolleri seçmek için **Herhangi biri**'ni seçin.

   Aşağıdaki tabloda, seçebileceğiniz protokolleri kısa açıklamaları ile birlikte göreceksiniz.

Protokol	*Açıklama*
ICMP	Internet Kontrolü Mesaj Protokolü – Internet Protokol'ünün (IP) bir uzantısıdır. ICMP hata, kontrol ve bilgi mesajları taşıyan paketleri destekler. Örneğin PING komutu, Internet bağlantısını test etmek için ICMP kullanır.

Protokol	Açıklama
TCP	İletim Kontrol Protokolü – TCP, bağlantı kurmak ve veri akışlarını değiştirmek için iki ana sistemi etkin kılar. TCP, verilerin ulaştırılmasını ve ayrıca, paketlerin gönderildikleri aynı sıra ile teslim edilmelerini garanti eder.
UDP	Kullanıcı Datagram Protokolü – UDP, yüksek performans için tasarlanmış IP tabanlı bir iletimdir. Oyunlar ve diğer video tabanlı uygulamalar genellikle UDP kullanır.

3. Kural eylemini uygun menüden seçin.

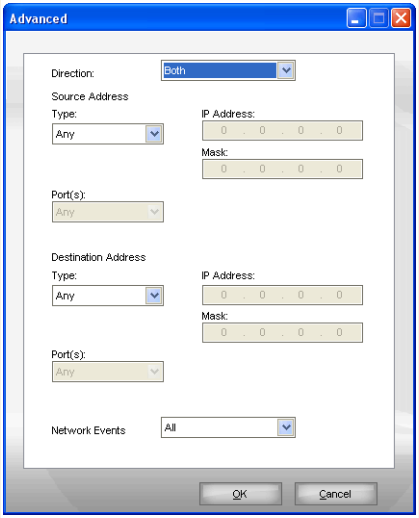
İşlem	Açıklama
İzin ver	Belirli uygulamaların ağ / internet erişimine belirli bazı şartlar altında izin verilecektir.
Reddet	Belirli uygulamaların ağ / internet erişimi belirli bazı şartlar altında engellenecektir.

4. Eğer önceden seçilen protokoller TCP veya UDP ise, uygulama için uygulanacak kuralın bir sunucu gibi davranıp davranmayacağını belirleyebilirsiniz.

   Tüm ağ olaylarına bu eylemi uygulamak için, **Diğer bilgisayarların bu uygulamaya bağlanmasına izin ver'** i seçerseniz, bu uygulamalara dolaylı olarak açık portlar üzerinden izin verme veya reddetme hakkı vermiş olacaksınız.

   Eğer eylemi sadece UDP trafiği ve TCP bağlantıları için uygulamak istiyorsanız, uygun kutucuktaki işareti kaldırın.

Eğer kural için daha fazla gelişmiş ayarlar yapılandırmak istiyorsanız, **Gelişmiş'** e tıklayın. Yeni bir pencere açılacaktır.



Gelişmiş Kural Ayarları

Yapılandırmayı aşağıdaki şekilde yapabilirsiniz:

- **Yön** – trafik yönünü seçin

Tip	*Açıklama*
Giden	Kural sadece dışarı giden trafiğe uygulanır
Gelen	Kural sadece dışardan gelen trafiğe uygulanır.
Her ikisi	Kural her iki yöndede geçerli olacaktır

- **Kaynak adresi** – Kuralın uygulanacağı kaynak adını girin.

  Kaynak adresini belirlemek için, adres tipi menüsünden gerekli veriyi seçin. Aşağıdaki seçenekler mevcuttur:

Tip	*Açıklama*
Herhangi	Kural herangi bir kaynak adresi için uygulanacaktır.

Tip	Açıklama
Ana Bilgisayar	Kural sadece kaynak ana bilgisayara aitse uygulanır. Ana bilgisayarın IP adresini girmelisiniz.
Ağ	Kural sadece kaynak belirli bir ağa aitse uygulanır. Ağın ve ağ maskesinin IP adresini girmelisiniz.
Yerel Sistem	Kural sadece kaynak yerel sisteme aitse uygulanır. Eğer birden fazla ağ arayüzü kullanıyorsanız, kuralın uygulanacağı ağ arayüzünü menüden seçin. Tüm yerel sistemlere kuralı uygulamak istiyorsanız, **Herhangi Bir'** i seçin.
Yerel Ağ	Kural sadece, kaynak yerel ağa aitse uygulanır. Eğer birden fazla ağa bağlıysanız, kuralın uygulanacağı ağı menüden seçin. Tüm yerel ağlara kuralı uygulamak istiyorsanız, **Herhangi Bir'** i seçin.

Eğer TCP yada UDP protokolleri seçtiyseniz, belirlediğiniz porta 0 ile 65535 arasında bir numara verebilirsiniz. Tüm portlara kuralı uygulamak istiyorsanız, **Herhangi Bir'** i seçin.

- **Hedef Adres** - Hedef adresi belirleyin.

Hedef adresini belirlemek için, adres tipi menüsünden gerekli veriyi seçin. Aşağıdaki seçenekler mevcuttur:

Tip	Açıklama
Herhangi	Kural herhangi bir hedef adrese uygulanır.
Ana Bilgisayar	Kural sadece, hedef belli bir ana bilgisayarsa uygulanır. Ana bilgisayarın IP adresini girmelisiniz.
Ağ	Kural sadece, hedef belli bir ağsa uygulanır. Ağın ve ağ maskesinin IP adresini girmelisiniz.
Yerel Sistem	Kural sadece, hedef belli bir yerel sistemse uygulanır. Eğer birden fazla ağ arayüzü kullanıyorsanız, kuralın uygulanacağı ağ arayüzünü menüden seçin. Tüm yerel sistemlere kuralı uygulamak istiyorsanız, **Herhangi Bir'** i seçin.
Yerel Ağ	Kural sadece, hedef belli bir yerel ağsa uygulanır. Eğer birden fazla ağa bağlıysanız, kuralın uygulanacağı ağı menüden seçin. Tüm yerel ağlara kuralı uygulamak istiyorsanız, **Herhangi Bir'** i seçin.

Eğer TCP yada UDP protokolleri seçtiyseniz, belirlediğiniz porta 0 ile 65535 arasında bir numara verebilirsiniz. Tüm portlara kuralı uygulamak istiyorsanız, **Herhangi Bir'** i seçin.

- **Ağ Olayları** - Eğer TCP veya UDP gibi bir protokol seçtiyseniz, kuralın uygulanacağı ağ olaylarını seçin.

Pencereyi kapatmak için **Tamam** seçeneğini tıklayın.

Güvenlik Duvarı kuralı eklemek için, **Ekle'** ye tıklayın.

9.3.3. Kuralların Yönetimi

Kuralın tabloda listelendiğini göreceksiniz.

Sistemle veya BitDefender süreçleriyle ilgili kuralları gizlemek için **Sistem süreçlerini gizle** kutusunu işaretleyin.

Kurallar, öncelik sırasına göre yukarıdan aşağıya doğru listelenirler. İlk kural en yüksek önceliğe sahiptir. **Profili düzenle**'ye tıkladığınızda,kuralların önceliğini, aşağı yukarı hareket ettirerek değiştirebileceğiniz **Detaylı görüntü** ekranına girersiniz.

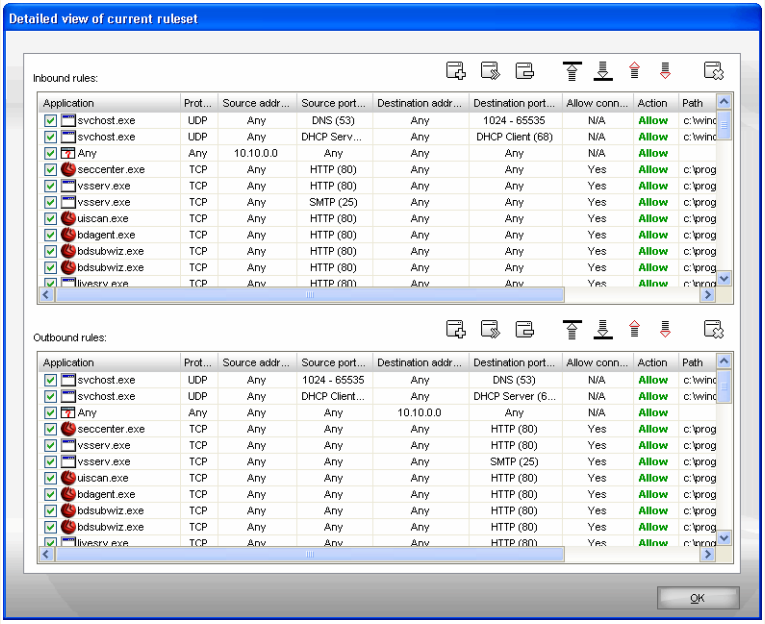
Bir kuralı silmek için, kuralı seçin ve **Kuralı Sil** tuşuna basın.

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

Not
Ayrıca bağlamsal bir menü bulunmakta ve aşağıdaki seçenekleri içermektedir: **Kural ekle**, **Kuralı sil** ve **Kuralı düzenle**.

9.3.4. Profillerin Düzenlenmesi

Profili düzenle'ye tıklayarak profili düzenleyebilirsiniz. Aşağıdaki pencere görülecektir:



Detaylı Görünüm

Kurallar 2 bölüme ayrılmaktadır: Geliş kuralları ve gidiş kuralları. Her kuralın uygulama ve kural parametrelerini (kaynak adresi, varış adresi, kaynak portları, varış portu, işlem, vs.) görebilirsiniz.

Bir kuralı silmek için, sadece bu kuralı seçmeniz ve **Kuralı sil** butonuna basmanız yeterlidir. Tüm kuralları silmek için **Listeyi temizle** butonunu tıklayın. Kuralı değiştirmek için, ya kuralı seçip **Kuralı düzenle** butonuna tıklayın ya da kuralın üzerine çift tıklayın. Kuralı silmeden geçici olarak inaktif hale getirmek için, ilgili kutudaki işareti kaldırın.

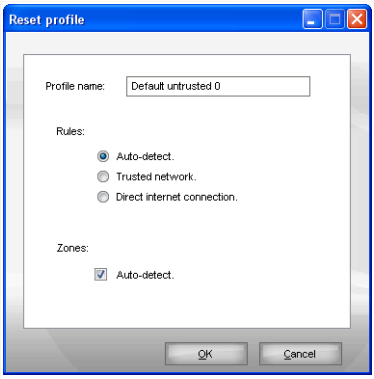
Kuralın önceliğini artırabilir veya azaltabilirsiniz. Seçilen kuralın önceliğini bir seviye artırmak için **Listede yukarı çıkar** butonuna tıklayın veya seçilen kuralın önceliğini bir seviye azaltmak için **Listede aşağı indir** butonuna tıklayın. Bir kurala en yüksek önceliği atamak için, **En Başa Taşı** tuşuna, bir kurala en düşük önceliği atamak için, **En Sona Taşı** tuşuna basın.

Not
Ayrıca bağlamsal bir menü bulunmakta ve aşağıdaki seçenekleri içermektedir: **Kural ekle**, **Kuralı düzenle**, **Kuralı sil**, **Yukarı çık**, **Aşağı in**, **En başa git**, **En sona git** ve **Listeyi temizle**.

Pencereyi kapatmak için **Tamam** seçeneğini tıklayın.

9.3.5. Profillerin Sıfırlanması

İleri düzeydeki kullanıcılar güvenlik duvarı profilini özelleştirmek veya korumayı optimize etmek için, kendi ihtiyaçlarına göre yeniden yapılandırabilirler. Profili sıfırlamak için, **Profili Sıfırla**' ya tıklayın. Sıradaki pencere çıkacaktır:



Profili Sıfırla

Yapılandırmayı aşağıdaki şekilde yapabilirsiniz:

- **Profil Adı** – Düzenleme sahasına yeni bir ad girin.
- **Kurallar** – Sistem uygulamaları için kuralların ne tipte yaratılacağını belirleyin.

  Aşağıdaki seçenekler mevcuttur:

Seçenek	Açıklama
Otomatik Algılama	BitDefender ağ yapılandırmasını algılar ve buna uygun olarak bir temel kurallar seti yaratır.
Güvenilir Ağ	Yaratılan temel kurallar seti güvenilir bir ağ içindir.

Seçenek	Açıklama
Direk internet bağlantısı	Yaratılan temel kurallar seti direk bir internet bağlantısı içindir.

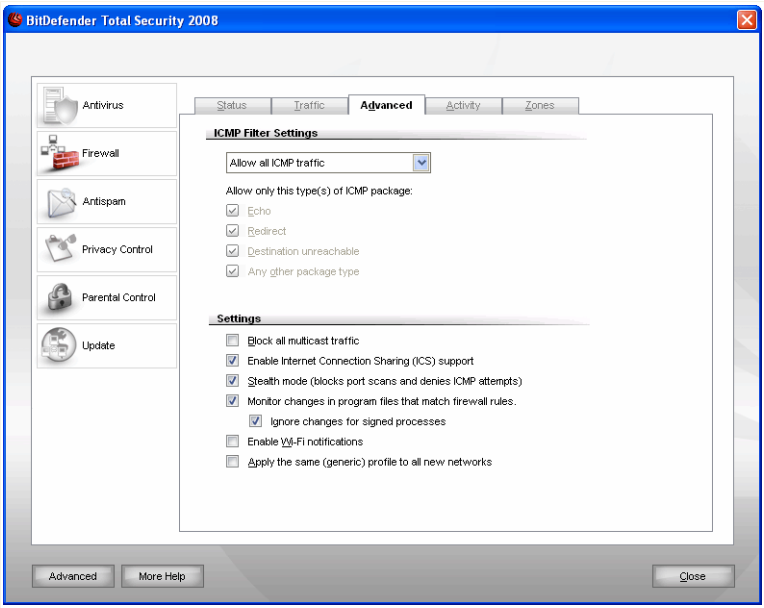
- **Bölgeler** bölümünden **Otomatik algıla'** yı seçtiğinizde, BitDefender algıladığı ağlar için uygun bölgeyi yaratır.

Pencereyi kapatmak ve profili sıfırlamak için, **Tamam'** a tıklayın.

Önemli
Güvenlik Duvarı profilini yeniden yapılandır' ı seçerseniz, bu bölüme eklediğiniz tüm kurallar kaybolacaktır.

9.4. Gelişmiş Ayarlar

BitDefender Güvenlik Duvarının gelişmiş ayarlarını yapılandırmak için, ayarlar konsolundan, **Güvenlik Duvarı>Gelişmiş'** i tıklayın. Sıradaki pencere çıkacaktır:



Gelişmiş Ayarlar

Bu bölümde, BitDefender Güvenlik Duvarının gelişmiş ayarlarını yapılandırabilirsiniz. Bu bölümde, BitDefender güvenlik duvarı ayarlarını yapılandırabilirsiniz. Gelişmiş ayarlar, ICMP trafiği (ICMP Ayarları) için filtreleme kurallarını belirlemenize ve çoklu-yayım trafiğini engelleyerek, internet bağlantınızı paylaşmanıza veya kötü amaçlı yazılım veya korsanlar için bilgisayarınızı görünmez yapmanıza olanak sağlamaktadır. (Ayarlar).

9.4.1. ICMP Filtre Ayarlarını Yapılandırma

ICMP trafiğni filtrelemek için menüden aşağıda belirtilen politikalardan birini seçebilirsiniz:

- **Tüm ICMP trafiğine izin ver** – Tüm ICMP trafiğine izin verir
- **Tüm ICMP trafiğini engelle** – Tüm ICMP trafiğini engeller.
- **Özel ICMP filtreleme** – ICMP trafiğinin filtrelenme şeklini değiştirir. Ne tip ICMP paketlerine izin vereceğinizi seçebileceksiniz.

Aşağıdaki seçenekler mevcuttur:

Seçenek	Açıklama
Echo	Bu seçenek, “Echo Reply” ve “Echo Request” mesajlarını etkinleştirir. “Echo Request”, bir ICMP mesajı olup, ana sisteme bir veri paketi gönderir ve bu verinin bir Echo Reply olarak kendine geri gönderilmesini bekler. Ana sistem tüm Echo Request’lere istek mesajıyla alınan verilerin aynısını içeren bir Echo Reply göndererek cevap vermelidir. Echo Reply bir ICMP mesajı olup, bir ICMP Echo Request mesajına bir yanıt olarak üretilir ve tüm Ana sistem ve Yönlendiriciler için zorunludur.
Yeniden yönlendirme	Bu bir ICMP mesajı olup, ana bilgisayara kendi yönlendirme bilgilerini yeniden adreslemesini bildirir (paketleri alternatif bir yoldan gönderme). Eğer ana bilgisayar, diğer bir ana bilgisayara erişmesi için veriyi bir yönlendirici (R1) üzerinden ve daha sonra başka bir yönlendirici (R2) üzerinden göndermeye çalışırsa ve R2 ile anabilgisayar arasında direkt bir bağlantı varsa, Yeniden yönlendirme, ana bilgisayara böyle bir yol olduğunu bildirecektir. Yönlendirici, orijinal datagramı hedeflenen adrese hala gönderecektir. Ancak, datagram yönlendirme bilgisini içeriyorsa, bu mesaj daha iyi bir yol var olsa bile gönderilmeyecektir.
Hedef erişilemez	Bu bir ICMP mesajı olup, datagram bir çoklu yayım adresi içermiyorsa, istemciye hedeflenen ana bilgisayarın (sunucunun) erişilemez olduğunu bildirmek için yönlendirici tarafından üretilir. Bu mesajın üretilme nedenleri: ana bilgisayarla fiziksel bir bağlantının olmaması (mesafe sonsuzdur), belirtilen protokolün veya portun etkin olmaması veya “parçalanmaz (don’t fragment)” bayrağı etkin olmasına rağmen veri bölünmüş olabilir.
Diğer Paket Tipleri	Bu seçenek etkinleştirildiğinde, **Echo**, **Hedef Erişilemez** veya **Yeniden yönlendirme** haricindeki diğer paketler geçecektir.

9.4.2. Gelişmiş Güvenlik Duvarı Ayarları

Aşağıda belirtilen gelişmiş güvenlik duvarı ayarları mevcuttur:

- **Tüm çoklu yayım trafiğini engelle** - Alınan herhangi bir çoklu yayım paketi düşürülür.

  Çoklu yayım trafiği, bir ağ içinde belirli bir gruba hitap eden trafik adreslemesidir. Paketler, çoklu yayım istemcisinin kabul etmesi durumunda, alabileceği özel bir adrese gönderilirler.

  Örneğin, TV-kartına sahip bir ağ üyesi, video dizinini yayınlayabilir (ağ üyelerinin her birine gönderebilir) veya çoklu yayım yapabilir (özel bir adrese gönderebilir). Çoklu yayım adresini dinleyen bilgisayarlar paketi kabul edebilir veya reddedebilir. Eğer kabul edilirse, video dizini çoklu yayım istemcileri tarafından seyredilebilir.

  Çok fazla miktardaki çoklu yayım trafiği, bant genişliği ve kaynak kullanır. Bu seçenek etkinleştirildiğinde, alınan herhangi bir çoklu yayım paketi atılacaktır. Ancak, bu seçeneğin seçilmesi önerilmez.
- **Internet Bağlantı Paylaşımı Desteğini(ICS) Etkinleştir** - İnternet Bağlantı Paylaşımı Desteği(ICS) etkinleştirilir.

  > ***Not***
  > Internet bağlantısı paylaşımı (ICS) için destek oluşturur. Bu seçenek, bilgisayarınızda ICS'yi otomatik olarak etkinleştirmez, sadece işletim sisteminizden etkinleştirmeniz durumunda böyle bir bağlantı şekline olanak tanır.

  Internet Bağlantı Paylaşımı (ICS), yerel alan ağı üyelerinin, bilgisayarınız yoluyla Internete bağlanmasına izin verir. Bu, özellikle belirli/özel bir Internet bağlantısından (örn. kablosuz bağlantı) yararlandığınızda ve bunu ağınızın diğer üyeleri ile paylaşmak istediğinizde faydalı olur.

  Internet bağlantınızı, yerel ağınızın diğer üyeleri ile paylaşmanız daha yüksek kaynak kullanmanıza neden olur ve bazı riskleri de beraberinde getirir. Ayrıca, çıkışlarınızdan bazılarını da meşgul eder. (Internet bağlantınızı kullanan üyeler tarafından açılanlar)
- **Gizlilik Modu** - Bilgisayarınızı kötü amaçlı yazılım ve korsanlara karşı görünmez kılar.

  Bilgisayarınızın savunmasız olup olmadığını anlamanın bir basit yolu, portlara bağlanarak herhangi bir yanıt alıp almadığınızı görmektir.

  Kötü amaçlı kişiler veya yazılım programlarının, bilgisayarınızın var olduğundan, hatta ağa hizmet verdiğinden haberleri olması gerekmez. **Gizlilik modu** seçeneği,

hangi portlarınızın açık olduğu veya bunların tam olarak nerede olduğunu bulma çabalarına makinenizin yanıt vermesini önler.

- **Program dosyalarında güvenlik duvarı kurallarına uyan değişiklikleri görüntüle** internete bağlanmayı deneyen her uygulamayı kontrol ederek, eğer değişim varsa görüntülenmesini sağlar. Eğer uygulamada değişiklik var ise size engellemeniz veya izin vermeniz için uyarıda bulunur.

  Çoğunlukla uygulamalardaki değişiklikler güncellenir. Fakat bu değişimlerin sizin bilgisayarınıza ve ağdaki diğer bilgisayarlara bulaşabilmek amacıyla kötü amaçlı yazılımlar tarafından yapılmış olma riski yüksektir.

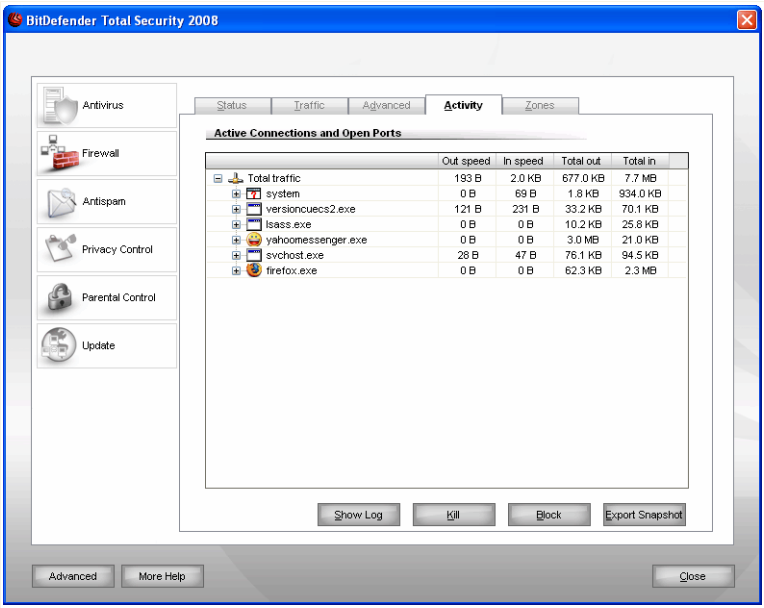
  

  Not
  Biz, bu opsiyonun seçili bırakılmasını ve sadece kural yaratıldıktan sonraki değişikliklerin erişimine izin verilmesini tavsiye ediyoruz.

  İşaretli uygulamalar güvenilir ve yüksek derecede güvenli olarak kabul edilir. **İşaretli işlemler için değişiklikleri yoksay** seçeneğini işaretleyebilirsiniz, böylece işaretlenmiş uygulamaların değişikliklerinde herhangi bir uyarı almazsınız.
- **Kablosuz bağlantıyı bildirimini etkinleştir** - Kablosuz bağlantıyı bildirimi etkinleştirilir.
- **Aynı profili (genel olarak) tüm yeni ağlara uygula** varsayılan olarak (jenerik) bir güvenlik duvarı profili yaratılır, `Jenerik Ağ` olarak adlandırılır ve yeni bir ağ yapılandırması algılandığında uygulanır. Güvenlik duvarı profili olan eski bir ağ yapılandırmasına geri dönerseniz, güvenlik duvarının kendi profili yerine jenerik profil yüklenir.

9.5. Bağlantı Kontrolü

Uygulama tarafından sınıflandırılan mevcut ağ/internet etkinliklerini (TCP ve UDP üzerinden) görebilmek, ayrıca BitDefender Güvenlik Duvarı kayıtlarına da erişebilmek için, ayarlar konsolundan **Güvenlik Duvarı>Etkinlik**' i tıklayın Sıradaki pencere çıkacaktır:



Bağlantı Kontrolü

Uygulamalara göre sıralanmış toplam trafiği görebilirsiniz. Her uygulama için, bağlantıları ve açık portları, ayrıca giden & gelen trafik hızı istatistiğini ve gönderilen / alınan veri toplamını görebilirsiniz.

Bu pencere geçerli ağda ve internetteki aktiviteyi gerçek zamanlı gösterir. Kapatılan portlar ve bağlantıları, ilişkin istatistikleri soluk olarak görebilirsiniz, daha sonra kaybolurlar. Yine, trafik yaratan bir uygulamanın tüm istetistikleri veya kapattığınız açık portlar da aynı şekilde meydana gelir.

Seçilen uygulamalar, port veya bağlantı yoluyla trafiği sınırlayan kuralları oluşturmak için **Engelle** seçeneğini tıklayın. Sizden seçiminizi onaylamanız istenecektir. Daha sonra ileri ayarları yapmak için Trafik bölümünden kurallara erişilebilir.

Not

Bir uygulamayı, port veya bağlantıyı engellemek için, üzerinde sağ tıklayıp, **Engelle**' yi seçebilirsiniz.

Öldür' ü tıklarsanız seçilen işlemin tüm aşamaları sona erdirilir. Tercihinizi doğrulamanız istenecektir.

Not
Bir işlemi öldürmek için ayrıca üzerine sağ tıklayarak **Öldür'** ü de seçebilirsiniz.

Listeyi bir `.txt` dosyasına aktarmak için **Export Snapshot** seçeneğini tıklayın.

Güvenlik Duvarı modülü kullanımı (güvenlik duvarını başlatma/durdurma, trafik engelleme, Gizlilik modunu etkinleştirme, ayarları değiştirme, profili uygulama) ile ilgili veya bunun tarafından algılanan etkinlikler (port tarama, kurallara göre bağlantı denemelerini ve trafiği engelleme) tarafından oluşturulan olayların kapsamlı bir listesi için, **Kayıtları Göster** seçeneğini tıklatılarak incelenebilecek BitDefender Güvenlik Duvarı kayıt dosyasını kontrol edin. Dosya, o andaki Windows kullanıcısının Ortak Dosyalar klasöründe; `...BitDefender\BitDefender Firewall\bdfirewall.txt` yolunda yer almaktadır

9.6. Ağ Bölgeleri

Bir bölge, profilinin içinde özel kural yaratılmış olan IP adresi veya IP adres araloğından oluşur. Kural, tanımlı tüm ağ üyelerinin bilgisayarınıza sınırsız erişimine izin verir (güvenilir bölge), ya da aksine bilgisayarınızı ağ bilgisayarlarından yalıtır, ayrı tutar (güvenilmeyen bölge)

Varsayılan olarak, BitDefender bağlandığınız ağı otomatik olarak algılar ve ağ yapılandırmasına bağlı olarak bir bölge ekler.

Not
Eğer birkaç farklı ağa bağlı iseniz, bağlanılan ağların yapılandırmalarına bağlı olarak birden fazla bölge eklenebilir.

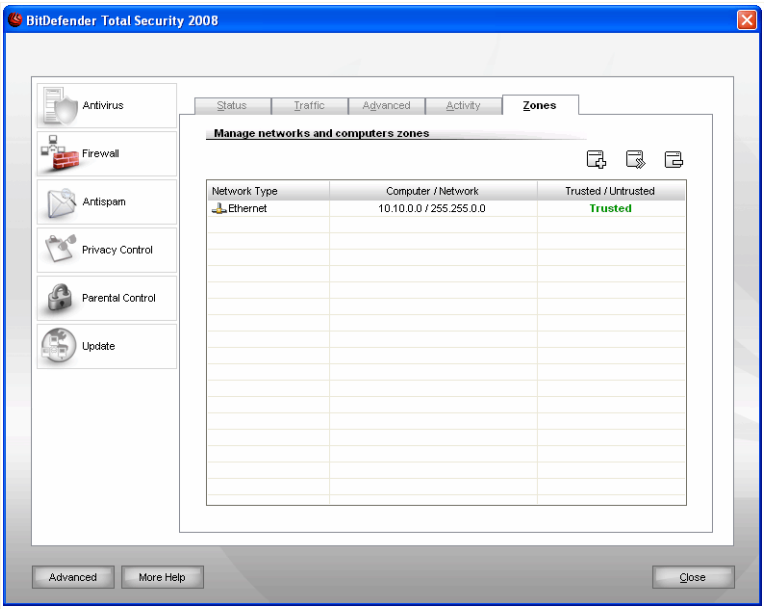
Güvenilir bölgeler, aşağıdaki ağ yapılandırmaları için varsayılan olarak eklenir:

- **Ağ geçidi atanmamış özel IP** - Bilgisayar yerel ağın (LAN) bir parçasıdır ve internete bağlanamaz.
- **Etki alanı için özel IP** Bilgisayar yerel ağın (LAN) bir parçasıdır ve bir etki alanına bağlıdır.

Güvenilmeyen bölgeler, aşağıdaki ağ yapılandırmaları için varsayılan olarak eklenir:

- **Açık (güvenilmeyen) kablosuz ağ** - Bilgisayar kablosuz ağın (WLAN) bir parçasıdır.

Ağ bölgelerini yönetmek için, ayarlar konsolundan **Güvenlik Duvarı>Bölgeler'** i tıklayın. Sıradaki pencere çıkacaktır:



Ağ Bölgeleri

Geçerli profil için ağ bölgelerini tabloda liste halinde görebilirsiniz. Her bölge için ağ tipini (Ethernet, kablosuz, PPP ve v.b.), bilgisayarın veya ağın güvenilir ya da güvenilmeyen bölgede olduğunu görebilirsiniz.

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

Not

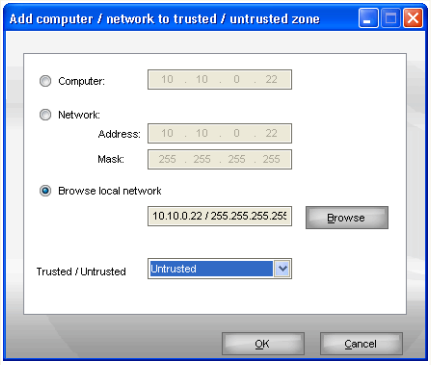
Varsayılan olarak, BitDefender açık kablosuz ağları güvenilmeyen bölgelere ekler. Eğer güvenilir bilgisayarlarla beraber özel amaçlı bir açık kablosuz ağa bağlı iseniz (evde ya da birkaç arkadaşla beraber gibi), bölgeyi düzenlemeyi isteyebilirsiniz. Bu durumda ağı güvenli bir bölge olarak ayarlayarak, kaynaklarınızı diğer ağ üyeleri ile paylaşabilirsiniz.

Bir bölgeyi silmek için, bölgeyi seçin ve **Bölge Sil** butonuna basın.

9.6.1. Bölgeler Eklemek

Bölgeleri manuel olarak ekleyebilirsiniz. Bu size, örneğin sadece arkadaşlarınızın olduğu kablosuz bir ağda dosyaları paylaştırmaya (bilgisayarları güvenilir bölgeye eklemeye) ya da güvenilir bölgedeki bilgisayarı engellemeye (bilgisayarı güvenilmeyen bölgeye eklemeye) izin verir.

Yeni bir bölge eklemek için, **Bölge Ekle** butonuna basınız. Sıradaki pencere çıkacaktır:



Bölge Ekle

Bölge eklemek için bu adımları takip edin:

1. Bölge eklemek istediğiniz bilgisayarı yerel ağdan veya tüm ağdan belirleyin. Aşağıdaki metodlardan birini kullanabilirsiniz:
   - Belirli bir bilgisayarı eklemek için, **Bilgisayar** alanına IP adresini girin.
   - Belirli bir ağı için, **Ağ** alanına IP adresini ve ağ maskesini girin.
   - Eklenecek bilgisayar veya ağı bulmak için yerel ağa gözat.

     Yerel ağa gözatmak için, **Yerel ağa gözat'** ı seçin ve **Gözat'** a tıklayın. Bağlı olduğunuz bütün ağı ve yanısıra ağdaki tüm üyeleri görebileceğiniz yeni bir pencere açılacak.

     Bölge eklemek istediğiniz bilgisayarı veya ağı listeden seçip, **Tamam'** a tıklayın.
2. Menüden ne tür bir bölge yaratmak istediğinizi seçin (güvenilir veya güvenilmeyen).
3. Bölge eklemek için **Tamam'** ı tıklayın.

10. Antispam

BitDefender Antispam, dikkate değer teknolojik yenilikler ve endüstri standardı antispam filtreleri kullanarak, spamları kullanıcıların gelen kutusuna ulaşmadan önce ayıklar.

Bu kullanım kılavuzunun **Antispam** bölümü aşağıda belirtilen konuları içermektedir:

- Antispam Kavramı
- Antispam Durumu
- Antispam Ayarları
- Microsoft Outlook / Outlook Express / Windows Mail ile integrasyon

10.1. Antispam Kavramı

Spam (istenmeyen e-postalar), hem bireyler hem de kurumlar için gittikçe büyüen bir problemdir. Hoş değildir, çocuklarınızın görmesini istemezsiniz, sizi işinizden attırabilir (çok fazla zaman harcadığını veya ofis postanızda porno bulunduğu için) ve insanların bunları göndermesini engelleyemezsiniz. Yapılması gereken en iyi şey tabi ki bunların alınmasını engellemektir. Ne yazık ki, bu e-postalar bir çok şekil ve boyutta gelebilmekte ve çok fazla sayıda bulunmaktadır

10.1.1. Antispam Filtreleri

BitDefender Antispam Motoru, gelen kutunuzda SPAM bulunmamasını sağlamak için yedi farklı filtreden oluşmuştur: Beyaz liste, Kara liste, Karakter seti filtresi, görüntü filtresi, URL filtresi, NeuNet (Sezgisel) filtresi ve Bayesian filtresi.

Not
Antispam modülünde, Ayarlar bölümünde bu filtrelerden her birini etkin veya etkisiz kılabilirsiniz.

Beyaz Liste / Kara Liste

Pek çok insan belirli bir grup insanla düzenli olarak iletişim kurmakta veya aynı alan adı içindeki şirket veya kurumlardan mesajlardan almaktadırlar. **Arkadaşlar veya spamcılar listesi**, kullanarak, mesaj içeriği ne olursa olsun kimlerden e-posta almak istediğinizi (arkadaşlar) veya kimlerden hiç bir zaman bir mesaj almak istemediğinizi (spamcı) kolayca belirleyebilirsiniz.

Not
Beyaz liste /Kara liste aynı zamanda **Arkadaşlar Listesi / Spamcılar Listesi** olarak da bilinir.

Arkadaş / Spamcı Listesi, Ayarlar Konsolundan veya Antispam araç çubuğundan yönetilebilir.

Not
Arkadaşlar listesine arkadaşlarınızın adlarını ve e-posta adreslerini eklemenizi tavsiye ediyoruz. BitDefender bu listedeki kişilerden gelen mesajları engellemeyecektir; bu nedenle arkadaşları listeye eklemek uygun mesajların gelmesini sağlayacaktır

Karakter Seti Filtresi

Çoğu Spam mesajları Kril ve/veya Asya dil karakterleri ile yazılmaktadır. Bu karakter setleri ile yazılmış tüm mesajları reddetmek isterseniz bu filtreyi yapılandırmalısınız.

Görüntü Filtresi

Sezgisel filtre tespitinden kaçınmak önemli bir sorun haline geldiği için, Gelen kutuları, istenmeyen içerikli bir görüntü içeren mesajlarla dolup taşmaktadır. Büyüyen bu problemin üstesinden gelmek için BitDefender, e-postadaki görüntü imzalarını BitDefender veritabanındaki imzalarla karşılaştıran **Görüntü Filtresini** geliştirmiştir. Bir eşleşme olması durumunda, e-posta SPAM olarak işaretlenecektir.

URL Filtresi

Çoğu Spam mesajlarında çeşitli web sitelerine bağlantılar (genellikle, daha fazla reklam içeren ve bir şeyler satınalma imkanı olan) bulunmaktadır. BitDefender'ın bu tür sitelere bağlantıları içeren bir veritabanı bulunmaktadır.

BitDefender linklerin olduğu bir veri tabanı sağlar. URL filtresi link içeren her mesajı bu veritabanı ile karşılaştırır. Eğer uyan varsa bunlar SPAM olarak etiketlenir.

NeuNet (Sezgisel) Filtresi

NeuNet (Sezgisel) Filtresi , tüm mesaj bileşenlerinde (yalnzıca başlık değil, HTML veya metin formatındaki tüm mesajda) bir dizi test gerçekleştirerek, SPAM özelliği gösteren kelime, cümle, bağlantı veya diğer içerikleri aramaktadır. Analizlerin sonuçlarına göre mesajlara SPAM puanı eklenir.

Filtre ayrıca, konu satırında `SEXUALLY-EXPLICIT:` ibaresi bulunan mesajlarıda SPAM olarak işaretler.

Not
19 Mayıs 2004 tarihinden itibaren geçerli olmak üzere, müstehcen içerikli materyaller içeren Spam mesajlarının konu alanında SEXUALLY EXPLICIT uyarısı bulunmak zorundadır. Aksi takdirde kanunların ihlali nedeniyle cezalar söz konusu olacaktır.

Bayesian Filtresi

Bayesian filtre modülü, mesajda SPAM olarak sınıflandırılan kelimelerin SPAM olmayan kelime olarak sınıflandırılan (sizin tarafınızdan veya sezgisel filtre tarafından) kelimelere oranı ile ilgili istatiksel bilgilere göre mesajları sınıflandırmaktadır.

Bunun anlamı, örneğin bir SPAM' da dört harfli bir kelimeye oldukça sık rastlanıyorsa, bu kelimeyi içeren bir sonraki gelen mesajında SPAM olma ihtimali oldukça yüksektir. Mesaj içindeki tüm ilişkili kelimeler dikkate alınmaktadır. İstatiksel bilgiler sentezlenerek, tüm mesajın SPAM olma olasılığı hesaplanmaktadır

Bu modül başka bir ilgilinç özellik de göstermektedir: Eğitilebilir bir modüldür. Belirli bir kullanıcıdan alınan mesaj tiplerine çabucak intibak ederek tümü hakkındaki bilgileri saklamaktadır. Etkin bir şekilde çalışması için filtre eğitilmelidir. Bunun anlamı, aynı bir av köpeğinin belirli bir kokuyu takip etmesi için eğitilmesi gibi, SPAM ve doğru mesaj örneklerinin gösterilmesidir. Bazen filtrenin düzeltilmesi de gerekmektedir – yanlış bir karar verdiğinde gerekli ayarlamaları yapması istenir.

Önemli
Bayesian modülünü Antispam araç çubuğundaki **'Spam'** ve **'Spam değil'** butonlarını kullanarak düzeltebilirsiniz.

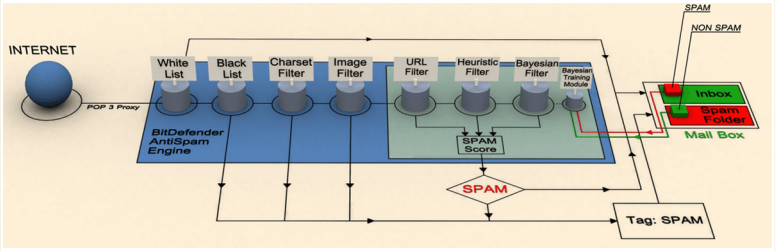
Not
Her güncelleme yaptığınızda:

- Yeni görüntü imzaları **Görüntü filtresine** eklenir.
- Yeni linkler **URL filtresine eklenir**.
- Yeni kurallar **NeuNet (Sezgisel)** filtresine eklenir.

Bu, Antispam motorunuzun etkinliğini arttırmaya yardımcı olacaktır.
Spam gönderenlere karşı sizi korumak için, BitDefender otomatik güncellemeler gerçekleştirebilir. **Otomatik Güncelleme** opsiyonunu etkin olarak bırakın.

10.1.2. Antispam Operasyonu

Aşağıdaki şemada BitDefender'ın nasıl çalıştığı gösterilmektedir.



Antispam Operasyonu

Alttaki şemadaki antispam filtreleri (Beyaz liste, Siyah liste, Karakter filtresi, Resim filtresi, URL filtresi, NeuNet (Sezgisel) filtresi ve Bayesian filtresi) Bitdefender tarafından mailin gelen kutunuza ulaşıp ulaşmaması gerektiğine karar vermek için kullanılır.

Internet'ten gelen her e-posta önce Beyaz liste/Kara liste filtreleri ile kontrol edilir. Eğer gönderenin adresi Beyaz liste'de bulunuyorsa, e-posta doğrudan **Gelen Kutunuza** taşınır.

Aksi takdirde Kara liste filtresi e-postayı alarak gönderen adresinin kendi listesinde olup olmadığını doğrular. Eğer listede ise, e-posta **SPAM** olarak etiketlenir ve Spam klasörüne gönderilir (Microsoft Outlook içinde).

Listede bulunamazsa, Karakter Seti filtresi devreye girerek, e-postanın Kril veya Asya dilleri karakterleri ile yazılıp yazılmadığını kontrol eder. Eğer bu karakterlerde yazılmışsa, **SPAM** olarak etiketlenir ve Spam klasörüne gönderilir.

Eğer e-posta Kril veya Asya dilleri karakterleri ile yazılmamışsa, Görüntü filtresine gönderilir. **Görüntü filtresi** , spam içerik taşıyan ekli resimler bulunan tüm e-postaları tespit eder.

URL filtresi linkleri kontrol edecek ve bulunan linkleri, BitDefender veritabanındaki linkler ile karşılaştıracaktır. Herhangi bir eşleşme söz konusu olduğunda, e-postaya bir SPAM puanı ekleyecektir.

NeuNet (Sezgisel) filtresi, e-postayı alarak tüm mesaj bileşenlerinde bir dizi test gerçekleştirecek ve SPAM özelliği gösteren kelime, cümle, bağlantı veya diğer içerikleri arayacaktır. Sonuçta, bu filtrede e-postaya bir SPAM puanı ekleyecektir.

Not

Eğer e-postanın konu alanı SEXUALLY EXPLICIT (müstehcen) olarak belirtilmişse, BitDefender bunu SPAM olarak algılayacaktır.

Bayesian filtre modülü, mesajda SPAM olarak sınıflandırılan kelimelerin SPAM olmayan kelime olarak sınıflandırılan (sizin tarafınızdan veya sezgisel filtre tarafından) kelimelere oranı ile ilgili istatiksel bilgilere göre mesajda daha ileri seviyede analizler gerçekleştirecektir. E-postaya bir Spam puanı eklenecektir.

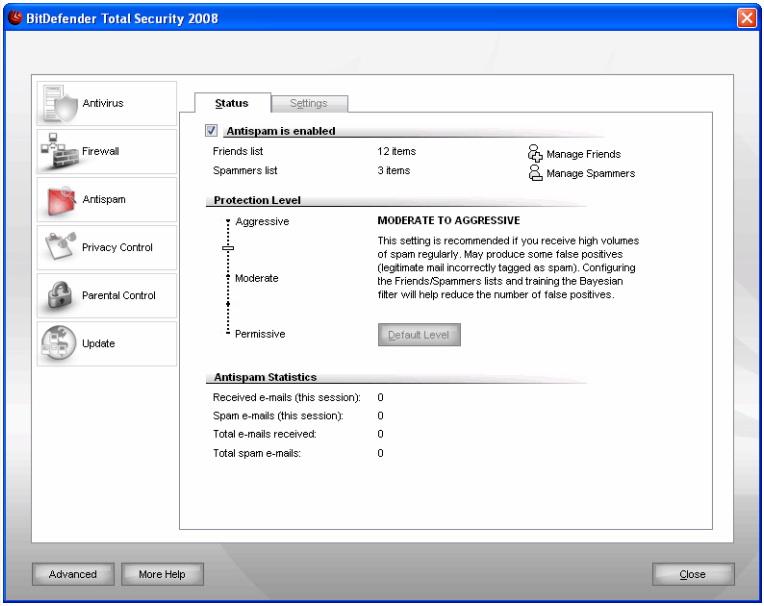
Eğer toplam puan (URL puanı + sezgisel puan + Bayesian puanı), mesaj SPAM puanını (kullanıcı tarafından Durum bölümünde tolerans seviyesi olarak ayarlanan) aşarsa, mesaj SPAM olarak ele alınacaktır.

Önemli

Microsoft Outlook veya Microsoft Outlook Express dışında bir e-posta istemcisi kullanıyorsanız, BitDefender tarafından SPAM olarak etiketlenen e-posta mesajlarını belirli bir karantina klasörüne taşımak için bir kural oluşturmalısınız. BitDefender,SPAM olarak düşünülen mesajlarının konusunda ön ek olarak `[SPAM]` ekler.

10.2. Antispam Durumu

Antispam koruma ayarlarını yapılandırmak için ayarlar konsolundan**Antispam>Durum**'u tıklayınız Sıradaki pencere çıkacaktır:



Antispam Durumu

Bu bölümde, **Antispam** modülünü yapılandırabilir ve etkinlikleri ile ilgili bilgileri inceleyebilirsiniz.

Önemli
Gelen kutunuza spam'lerin girmesini önlemek için **Antispam filtresini** etkin olarak bırakın.

İstatistikler bölümünde, her oturumda (bilgisayarınızı açtığınızdan itibaren) sunulan antispam etkinliklerinin sonuçlarına veya bir özetine (BitDefender kurulduğundan itibaren) bakabilirsiniz.

Antispam modülünü yapılandırmak için aşağıda belirtilen şekilde hareket edilmesi gerekmektedir:

10.2.1. Adım 1/2 - Tolerans Seviyesinin Ayarlanması

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

5 tolerans seviyesi bulunmaktadır:

Tolerans seviyesi	Açıklama
Toleranslı	Çok sayıda doğru ticari posta alan hesaplara koruma sağlar. Filtre, e-postaların çoğunun geçmesine izin verecektir fakat yanlış negatifler yaratabilecektir (spam, doğru posta olarak sınıflandırılabilir).
Toleranslı - Orta	Bazı doğru ticari posta alan hesaplara koruma sağlar. Filtre, e-postaların çoğunun geçmesine izin verecektir fakat yanlış negatifler yaratabilecektir (spam, doğru posta olarak sınıflandırılabilir).
Orta	Düzenli hesaplar için koruma sağlar. Filtre, yanlış pozitiflerden kaçınırken (doğru postaların yanlışlıkla spam olarak işaretlenmesi), spamların çoğunu engelleyecektir.
Orta - Agresif	Sürekli olarak çok sayıda spam alan hesaplara koruma sağlayacaktır. Filtre çok az sayıda spamın geçmesine izin verecektir. Fakat yanlış poztifiler yaratabilir (doğru posta yanlışlıkla spam olarak işaretlenebilir). Yanlış poztifleri en aza indirmek için, **Arkadaşlar/Spamcılar** listesini yapılandırın ve **Öğrenme Motorunu (Bayesian**) eğitin.
Agresif	Sürekli olarak çok yüksek hacimde spam alan hesaplara koruma sağlar. Filtre çok az sayıda spamın geçmesine izin verecektir. Fakat yanlış poztifiler yaratabilir (doğru posta yanlışlıkla spam olarak işaretlenebilir).

Tolerans seviyesi	Açıklama
	Yanlış pozitifleri en aza indirgemek için, kontaklarınızı **Arkadaşlar listesine** ekleyin.

Varsayılan güvenlik seviyesini ayarlamak için (**Orta - Agresif**) **Varsayılan Seviye**'ye tıklayınız.

10.2.2. Adım 2/2 - Adres Listelerini oluşturun

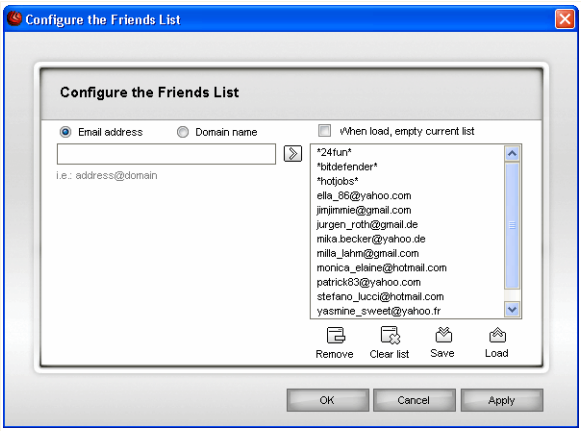
Size doğru e-posta mesajları veya spam gönderen e-posta adresleri hakkında bilgi içeren adres listeleri.

Arkadaşlar Listesi

Arkadaşlar Listesi, içeriğine bağımlı kalmaksızın, her zaman mesaj almak istediğiniz bütün e-posta adreslerini içeren listedir. İçeriği spam'i andırsa bile, Arkadaşınızdan gelen mesajlar spam olarak etiketlenmemektedir.

Not
Arkadaş listesinde yer alan bir adresten gelen herhangi bir mesaj , herhangi başka bir işleme tabi tutulmadan otomatik olarak gelen kutunuza gönderilecektir.

Arkadaşlar listesini yönetmek için, (+)'a tıklayın (**Arkadaş Listesi** anlamına gelmektedir) veya Antispam araç çubuğundan **Arkadaşlar** seçeneğini tıklayın.



Arkadaşlar Listesi

Burada, **Arkadaşlar listesinden** ekleme yapabilir veya çıkarabilirsiniz.

Bir **e-posta adresi** eklemek istiyorsanız, E-posta adresi seçeneğini işaretleyip, adresi girin ve ⊠ (+) seçeneğini tıklayın (adres **Arkadaşlar** listesinde belirecektir).

Önemli
Söz dizimi: isim@domain.com.

Bir **Alan adı** eklemek istiyorsanız, Alan adı seçeneğini işaretleyip, Alanı girin ve ⊠(+) seçeneğini tıklayın. Alan **Arkadaşlar listesinde** belirecektir.

Önemli
Söz dizimi:

- @domain.com, *domain.com ve domain.com - domain. com'dan alınan tüm e-posta mesajları, içeriğinden bağımsız olarak **gelen kutunuza** gönderilecektir;
- *domain* - domain'den (Alan soneki ne olursa olsun) gelen tüm e-posta mesajları içeriğinden bağımsız olarak **gelen kutunuz**a gönderilecektir;
- *com - Alan soneki com olan tüm gelen e-posta mesajlar ı içeriğinden bağımsız olarak **gelen kutunuza** gönderilecektir;

Listeden herhangi bir kaydı silmek için, kaydı seçin ve **Sil** seçeneğini tıklayın. Eğer, **Listeyi Temizle** seçeneğini tıklarsanız, listedeki tüm kayıtları sileceksiniz. Fakat bunları yeniden geri almanın imkansız olduğunu unutmayın.

Arkadaş listesini istenilen bir yere kaydetmek/yüklemek için, **Kaydet**/**Yükle** butonlarını kullanın. Dosya `.bwl` uzantısı alacaktır.

Daha önce kaydedilen bir listeyi yüklediğinizde, güncel listenin içeriğini yeniden kurmak için, **Yüklendiğinde, güncel listeyi boşalt** seçeneğini seçin.

Not
Arkadaşlar listesine arkadaşlarınızın adlarını ve e-posta adreslerini eklemenizi tavsiye ediyoruz. BitDefender bu listedeki kişilerden gelen mesajları engellemeyecektir; bu nedenle arkadaşları listeye eklemek uygun mesajların gelmesini sağlayacaktır

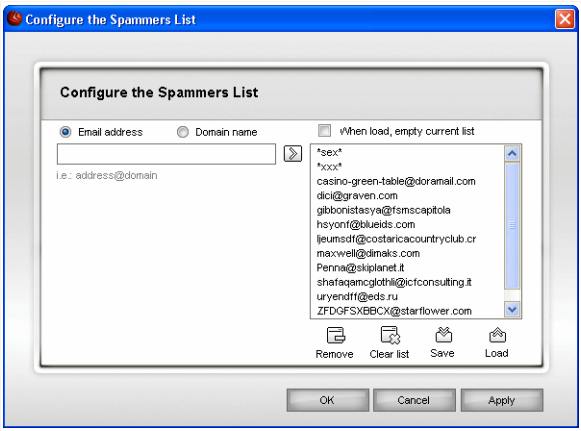
Arkadaş listesini kaydetmek ve kapatmak için **Uygula** ve **Tamam** butonlarını tıklayın.

Spamcılar Listesi

Spamcılar Listesi, içeriklerine bağlı olmaksızın kendilerinden mesaj almak istemediğiniz tüm e-posta adreslerinin bir listesidir.

Not
Spamcılar listesinde yer alan bir adresten gelen herhangi bir e-posta mesajı, herhangi başka bir işleme tabi tutulmadan, otomatik olarak SPAM şeklinde işaretlenecektir.

Spamcılar listesini yönetmek için, (corresponding to the **Spamcı listesi** seçeneğini tıklayın veya antispam araç çubuğundan **Spamcılar** seçeneğini tıklayın.



Spamcılar Listesi

Burada, **Spamcılar Listesine**, adres ekleyebilir ve çıkartabilirsiniz.

Bir e-posta adresi eklemek istiyorsanız, **E-posta adresi** seçeneğini işaretleyip, adresi girin ve (X)'i tıklayın. Adres **Spamcılar Listesinde** belirecektir.

Önemli
Söz dizimi: isim@domain.com.

Bir Alan eklemek istiyorsanız, **Alan adı** seçeneğini işaretleyip, alanı girin ve (X) seçeneğini tıklayın. Alan **Spamcılar Listesinde** belirecektir.

Önemli
Söz dizimi:

- @domain.com, *domain.com ve domain.com domain.com'dan gelen tüm e-posta mesajları SPAM olarak etiketlenecektir;
- *domain* domain'dan gelen (Alan soneki ne olursa olsun) tüm e-posta mesajları SPAM olarak etiketlenecektir;
- *comAlan soneki com olan adreslerden gelen tüm e-posta mesajları SPAM olarak etiketlenecektir.

Listeden herhangi bir kaydı silmek için, kaydı seçin ve **Sil** seçeneğini tıklayın. Eğer, **Listeyi Temizle** seçeneğini tıklarsanız, listedeki tüm kayıtları sileceksiniz. Fakat bunları yeniden geri almanın imkansız olduğunu unutmayın.

Spamcılar Listesini arzu edilen başka bir yere kaydetmek/yüklemek için **Kaydet**/ **Yükle** butonlarını kullanın. Dosya `.bwl` uzantısını alacaktır.

Daha önce kaydedilen bir listeyi yüklediğinizde, güncel listenin içeriğini yeniden kurmak için, **Yüklendiğinde, güncel listeyi boşalt** seçeneğini seçin.

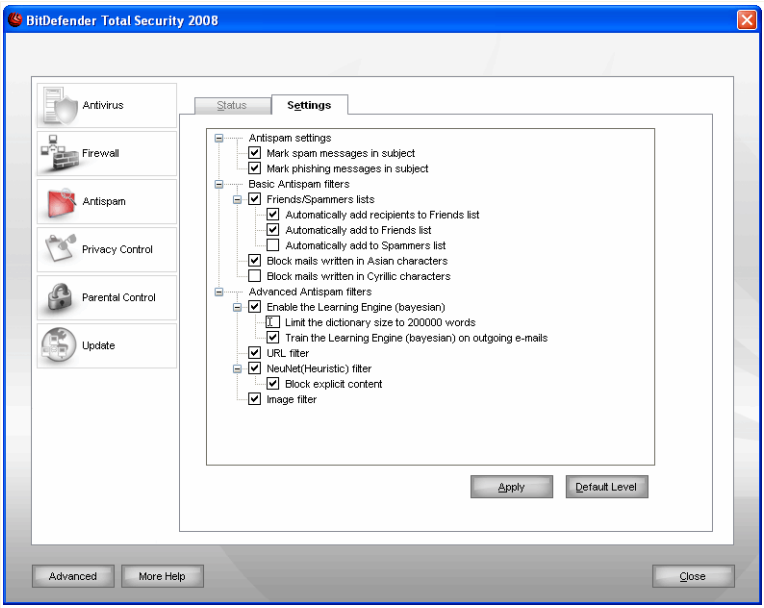
Spamcılar Listesini kaydetmek ve kapatmak için **Uygula** ve **Tamam** butonlarını tıklayın.

Önemli

BitDefender' ı yeniden yüklemek isterseniz, bunu yapmadan önce **Arkadaşlar** / **Spamcılar** listelerini kaydetmeniz iyi bir fikir olacaktır. Yeniden yükleme işlemi tamamlandıktan sonra bunları yükleyebilirsiniz.

10.3. Antispam Ayarları

Antispam ayarlarını yapılandırmak için, ayarlar konsolundan **Antispam>Ayarlar'** ı tıklayın. Sıradaki pencere çıkacaktır:



Antispam Ayarları

Burada, Antispam filtrelerinin herbirini etkinleştirip/kapatabilir ve antispam modülü ile ilgili diğer bazı ayarları belirleyebilirsiniz.

Mevcut olan üç seçenek kategorisi (**Antispam ayarları**, **Temel Antispam filtreleri** ve **İleri Antispam filtreleri**), Windows'dakilere benzer şekilde genişleyen menüler şeklinde organize edilmiştir.

Not
Bir kategoriyi açmak için "+" işaretli kutuyu veya kapatmak için "-" işaretli kutuyu tıklayın.

10.3.1. Antispam Ayarları

- **Spam mesajlarını konu satırında işaretle** – spam olduğu düşünülen tüm e-posta mesajları konu satırında SPAM ile işaretlenecektir
- **Phishing mesajlarını konu satırında işaretle** - phishing mesajı olduğu düşünülen tüm e-posta mesajları konu satırında SPAM ile işaretlenecektir.

10.3.2. Temel Antispam Filtreleri

- **Arkadaş/Spamcılar Listesi** - Arkadaş/Spamcılar listelerini etkinleştirir/kapatır.
  - **Alıcıları otomatik olarak Arkadaş listesine ekle** – gönderilen postanın alıcılarını otomatik olarak Arkadaş listesine ekler.
  - **Otomatik olarak Arkadaş listesine ekle**- Antispam araç çubuğundan **Spam değil** seçeneğini bir dahaki tıklamanızda, gönderici otomatik olarak **Arkadaş listesine** eklenecektir.
  - **Otomatik olarak Spamcılar Listesine ekle** - Antispam araç çubuğundan **Spam** seçeneğini bir dahaki tıklamanızda, gönderici otomatik olarak **Spamcılar** listesine eklenecektir.

Not

Spam değil) ve (**Spam** butonları, Bayesian filtresini eğitmek için kullanılmaktadır.

- **Asya karakterlerini engelle** – Asya karakterlerinde yazılan mesajları engelleyecektir.
- **Kril karakterlerini engelle** – Krilik karakterlerinde yazılan mesajları engelleyecektir.

10.3.3. Gelişmiş Antispam Filtreleri

- **Öğrenme Motorunu Etkinleştir (bayesian)** – Öğrenme Motorunu (bayesian) etkinleştirir/kapatır.
  - **Sözlük kapasitesini 200000 kelime ile sınırla** – Bayesian sözlüğünün kapasitesini sınırlar- daha küçük kapasite daha hızlıdır, daha büyük kapasite daha doğrudur

Not

Tavsiye edilen boyut: 200.000 kelimedir.

  - **Gönderilen e-postalar ile Öğrenme Motorunu Eğit** – gönderilen postalarda Öğrenme Motorunu (bayesian) eğitir.
- **URL filtresi** – URL filtresinietkinleştirir/kapatır.
- **NeuNet(Sezgisel) filtresi** – Sezgisel (NeuNet Heuristic) filtresini etkinleştirir /kapatır
  - **Cinsel mahiyetteki içerikleri engelle** - Konu satırında SEXUALLY EXPLICIT (Cinsel içerikli) ibaresi olan mesajları tespit etmeyi etkinleştirir/kapatır.
- **Görüntü filtresi** – Resim filtresini etkinleştirir/kapatır.

Not
Bir seçeneği etkinleştirmek/kapatmak için, buna karşılık gelen ilgili işaretleme kutusunu işaretleyin/işareti kaldırın.

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

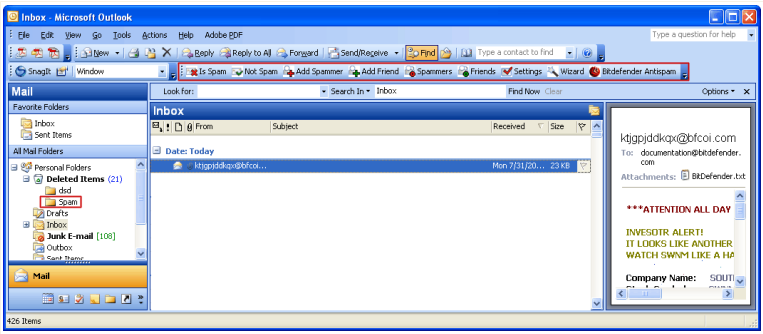
10.4. Microsoft Outlook / Outlook Express ve Windows Mail ile entegrasyon

BitDefender, sezgisel ve kullanımı kolay bir araç çubuğu sayesinde Microsoft Outlook / Outlook Express ile doğrudan entegre edilebilir.

- Microsoft Outlook
- Outlook Express
- Windows Mail
- Mozilla Thunderbird

10.4.1. Antispam Araç Çubuğu

Microsoft Outlook / Outlook Express' in üst kısmında Antispam araç çubuğunu görebilirsiniz.



Antispam Araç Çubuğu

Önemli
Microsoft Outlook için BitDefender Antispam ve Outlook Express için BitDefender Antispam arasındaki fark, Microsoft Outlook'da SPAM mesajlar **Spam** dosyasına aktarılmakta, Outlook Express içinse SPAM mesajlar **Silinen Öğeler** dosyasına aktarılmaktadır. Her iki durumda da mesajlar konu satırında SPAM olarak etiketlenirler.

Microsoft Outlook' ta **Spam** dosyası BitDefender tarafından otomatik olarak yaratılmakta ve **Klasörler listesindeki** öğeler (Takvim, Adresler, vs. gibi) ile aynı seviyede listelenirler.

BitDefender araç çubuğunda bulunan herbir buton aşağıda açıklanacaktır:

- **Spam**Bayesian modülüne seçilen postanın bir spam olduğunu belirten bir mesaj gönderir. e-posta bir SPAM olarak etiketlenecek ve **Spam** dosyasına gönderilecektir.

  Aynı şablona uyan daha sonraki e-posta mesajları SPAM olarak etiketlenecektir

  Not
  Tek bir e-posta veya istediğiniz kadar e-posta mesajı seçebilirsiniz

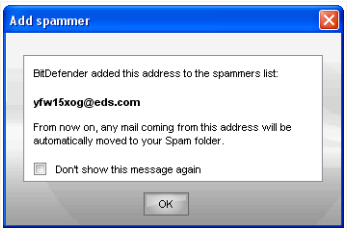
- **Spam Değil** - Bayesian modülüne, seçilen postanın bir spam olmadığını ve BitDefender tarafından işaretlenmesine gerek olmadığını belirten bir mesaj gönderir. E-posta **Spam dosyasından Gelen Kutusu** dizinine aktarılır

  Aynı şablona uyan daha sonraki e-posta mesajları artık SPAM olarak işaretlenmeyecektir.

  Not
  Tek bir e-posta veya istediğiniz kadar e-posta mesajı seçebilirsiniz

  Önemli
  BitDefender tarafından SPAM olarak işaretlenmiş bir mesajı seçtiğinizde (genelde bu mesajlar **Spam dosyasında** yer alır), **Spam Değil** seçeneği etkin hale gelir.

- **Spamcı Ekle** - seçilen e-postanın göndericisini **Spamcılar Listesine** ekler.



Spamcı Ekle

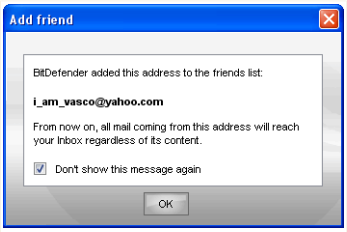
Bir spam gönderenin adresini listeye eklerken, teyit için onaylama mesajının gelmesini istemiyorsanız, **Bu mesajı tekrar gösterme** seçeneğini tıklayın.

Pencereyi kapatmak için **Tamam** seçeneğini tıklayın.

Bu adresten gelen daha sonraki e-posta mesajları SPAM olarak işaretlenecektir.

Not
Bir veya istediğiniz kadar çok gönderici seçebilirsiniz.

- **Arkadaş Ekle** seçilen e-posta mesajının gönderenini **Arkadaşlar Listesine**. ekler.



Arkadaş Ekle

Bir arkadaşın adresini listeye eklerken, teyit için onaylama mesajının gelmesini istemiyorsanız, **Bu mesajı tekrar gösterme** seçeneğini tıklayın

Pencereyi kapatmak için **Tamam** seçeneğini tıklayın.

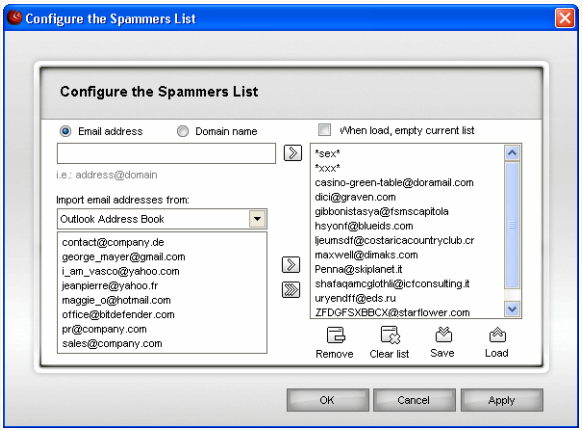
İçeriği ne olursa olsun, bu adresten gelen e-posta mesajlarını her zaman alacaksınız.

Not
Bir veya istediğiniz kadar çok gönderici seçebilirsiniz.

- **Spamcılar** - içeriklerine bağlı olmaksızın, mesaj almak istemediğiniz tüm e-posta adreslerini içeren **Spamcılar Listesini** açar.

Not

Spamcılar listesinde yer alan bir adresten gelen herhangi bir e-posta mesajı, herhangi başka bir işleme tabi tutulmadan, otomatik olarak SPAM şeklinde işaretlenecektir.



Spamcılar Listesi

Burada, **Spamcılar Listesine**, adres ekleyebilir ve çıkartabilirsiniz.

Eğer bir e-posta adresi eklemek istiyorsanız, **E-posta adresi** seçeneğini seçin, adresi girin ve ⊠ seçeneğine basın. Adres **Spamcılar listesinde** belirecektir.

Önemli

Söz dizimi: isim@domain.com.

Eğer bir Alan adı eklemek isterseniz, **Alan adı** seçeneğini seçin, alanı yazın ve ⊠ seçeneğine basın. Alan adı **Spamcılar listesinde** belirecektir.

Önemli

Söz dizimi:

- @domain.com, *domain.com ve domain.com domain.com'dan gelen tüm e-posta mesajları SPAM olarak etiketlenecektir;
- *domain* domain'dan gelen (Alan soneki ne olursa olsun) tüm e-posta mesajları SPAM olarak etiketlenecektir;
- *comAlan soneki com olan adreslerden gelen tüm e-posta mesajları SPAM olarak etiketlenecektir.

Microsoft Outlook/Outlook Express'den e-posta adreslerini yüklemek için, **Önemli e-posta adreslerini yükle** menüsünden **Windows Adres Defteri/Outlook Express Klasörleri** seçeneğini seçin.

Microsoft Outlook Express/ Windows Mail için, **Spamcılar Listesine** eklemek istediğiniz e-posta adreslerini içeren klasörü seçebileceğiniz yeni bir pencere belirecektir. Bunları seçin ve **Seç** seçeneğini tıklayın.

Her iki durumda da, e-posta adresleri import (al) listesinde belirecektir. Bunları to add them to the **Spamcılar listesine** eklemek için, eklemek istediklerinizi seçin. Eğer seçeneğini tıklarsanız tüm e-posta adresleri listeye eklenecektir.

Listeden herhangi bir kaydı silmek için, kaydı seçin ve **Sil** seçeneğini tıklayın. Eğer, **Listeyi Temizle** seçeneğini tıklarsanız, listedeki tüm kayıtları sileceksiniz. Fakat bunları yeniden geri almanın imkansız olduğunu unutmayın.

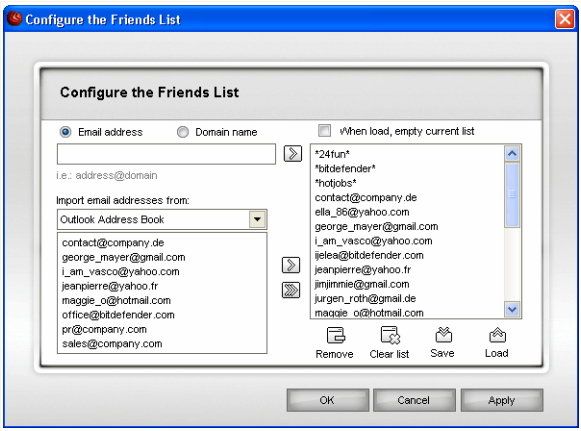
Spamcılar Listesini arzu edilen başka bir yere kaydetmek/yüklemek için **Kaydet**/ **Yükle** butonlarını kullanın. Dosya `.bwl` uzantısını alacaktır.

Daha önce kaydedilen bir listeyi yüklediğinizde, güncel listenin içeriğini yeniden kurmak için, **Yüklendiğinde, güncel listeyi boşalt** seçeneğini seçin.

Spamcılar Listesini kaydetmek ve kapatmak için **Uygula** ve **Tamam** butonlarını tıklayın.

- **Arkadaşlar** - içeriklerine bağlı kalmaksızın, e-posta mesajı almak istediğiniz tüm e-posta adreslerini içeren **Arkadaşlar listesini** açar.

> *Not*
> **Arkadaş listesinde** yer alan bir adresten gelen herhangi bir mesaj , herhangi başka bir işleme tabi tutulmadan otomatik olarak gelen kutunuza gönderilecektir.



Arkadaşlar Listesi

Burada, **Arkadaşlar listesinden** ekleme yapabilir veya çıkarabilirsiniz.

Bir e-posta adresi eklemek isterseniz, **E-posta adresi** seçeneğini seçin, adresi girin ve ⊠ seçeneğini tıklayın. Adres **Arkadaşlar Listesinde** belirecektir.

Önemli
Söz dizimi: isim@domain.com.

Bir **Alan adı** eklemek isterseniz, Alan Adı seçeneğini seçin, Alan ismini girin ve ⊠ seçeneğini tıklayın. Alan **Arkadaşlar Listesinde** belirecektir.

Önemli
Söz dizimi:

- @domain.com, *domain.com ve domain.com - domain. com'dan alınan tüm e-posta mesajları, içeriğinden bağımsız olarak **gelen kutunuza** gönderilecektir;
- *domain* - domain'den (Alan soneki ne olursa olsun) gelen tüm e-posta mesajları içeriğinden bağımsız olarak **gelen kutunuz**a gönderilecektir;
- *com - Alan soneki com olan tüm gelen e-posta mesajlar ı içeriğinden bağımsız olarak **gelen kutunuza** gönderilecektir;

Microsoft Outlook/Outlook Express'den e-posta adreslerini yüklemek için, **Önemli e-posta adreslerini yükle** menüsünden **Windows Adres Defteri/Outlook Express Klasörleri** seçeneğini seçin.

Microsoft Outlook Express/Windows Mail için, **Arkadaşlar Listesine** eklemek istediğiniz e-posta adreslerini içeren klasörü seçebileceğiniz yeni bir pencere belirecektir. Bunları seçin ve **Seç**'i tıklayın.

Her iki durumda da, e-posta adresleri import listesinde belirecektir. İstediklerinizi seçin ve seçeneğine tıklayarak, Arkadaş listesine ekleyin. Eğer seçeneğini tıklarsanız tüm e-posta adresleri listeye eklenecektir.

Listeden herhangi bir kaydı silmek için, kaydı seçin ve **Sil** seçeneğini tıklayın. Eğer, **Listeyi Temizle** seçeneğini tıklarsanız, listedeki tüm kayıtları sileceksiniz. Fakat bunları yeniden geri almanın imkansız olduğunu unutmayın.

Arkadaş listesini istenilen bir yere kaydetmek/yüklemek için, **Kaydet**/**Yükle** butonlarını kullanın. Dosya `.bwl` uzantısı alacaktır.

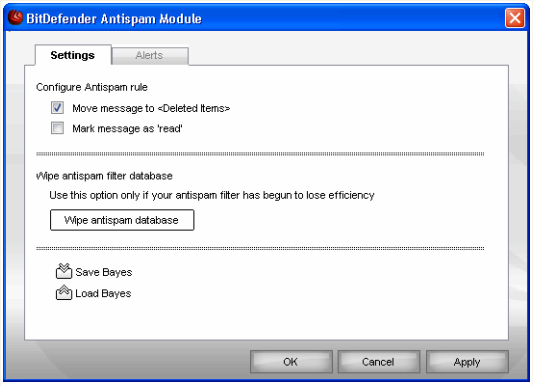
Daha önce kaydedilen bir listeyi yüklediğinizde, güncel listenin içeriğini yeniden kurmak için, **Yüklendiğinde, güncel listeyi boşalt** seçeneğini seçin.

Not

Arkadaşlar listesine arkadaşlarınızın adlarını ve e-posta adreslerini eklemenizi tavsiye ediyoruz. BitDefender bu listedeki kişilerden gelen mesajları engellemeyecektir; bu nedenle arkadaşları listeye eklemek uygun mesajların gelmesini sağlayacaktır

Arkadaş listesini kaydetmek ve kapatmak için **Uygula** ve **Tamam** butonlarını tıklayın.

- **Ayarlar** - **Antispam** modülünün bazı seçeneklerini belirleyebileceğiniz Ayarlar penceresini açar.



Ayarlar

Aşağıdaki seçenekler mevcuttur:

- **Mesajı Silinen Öğeler dosyasına taşı** - spam mesajlarını **Silinen Öğeler** dosyasına atar (sadece Microsoft Outlook Express/Windows mail için geçerli);
- **Mesajları "Okundu" olarak işaretle** - yeni spam mesajları geldiğinde rahatsızlık vermemesi için, tüm spam mesajlarını okunmuş olarak işaretler.

Eğer antispam filtreniz çok hatalı ise, Filtre veri tabanını silmeniz ve Bayesian filtresini yeniden eğitmeniz gerekebilir. Bayesian veri tabanını sıfırlamak için **Antispam Veri Tabanını Sil** seçeneğini tıklayın.

Bayes' i Kaydet/**Bayes' i Yükle** butonlarını kullanın. Dosya `.dat` uzantısına sahip olacaktır.

Spamcı Ekle ve **Arkadaş Ekle** butonları için, onaylama penceresinin imgesini etkisiz kılabileceğiniz bölüme erişmek isterseniz, **Uyarılar** seçeneğini tıklayın.

Not

Uyarılar penceresindeyken, aynı zamanda **Lütfen bir e-posta mesajı seçin** uyarısının imgesinide etkinleştirebilir veya etkisiz hale getirebilirsiniz. Bu uyarı, bir e-posta mesajı yerine bir grup seçtiğiniz zaman görüntülenir.

- **Sihirbaz** – Sizi adım adım Bayesian filtresi eğitim işleminden geçirecek olan sihirbazı açar. Böylece, BitDefender antispam verimliliği daha da artacaktır. Ayrıca, **Adres Defterinizden**, **Arkadaşlar Listenize** /**Spamcılar Listenize** adresler de ekleyebilirsiniz.
- **BitDefender Antispam** - Yönetim Konsolunu açar.

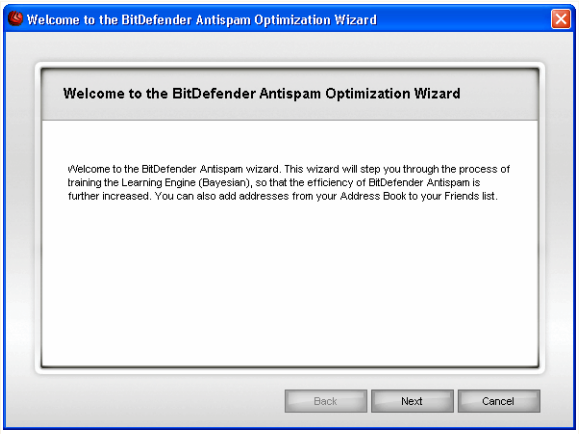
10.4.2. Antispam Yapılandırma Sihirbazı

BitDefender yüklüyken Microsoft Outlook / Outlook Express'i ilk çalıştırdığınızda, size Arkadaşlar Listesi ve Spamcılar Listesini yapılandırmanızda yardımcı olacak bir sihirbaz ekrana gelir ve antispam filtrelerinin verimliliğini artırmak için Bayesian Filtresini eğitir.

Not

Antispam araç çubuğundan **Sihirbaz** seçeneğini tıklayarak, sihirbazı istediğiniz zaman başlatabilirsiniz.

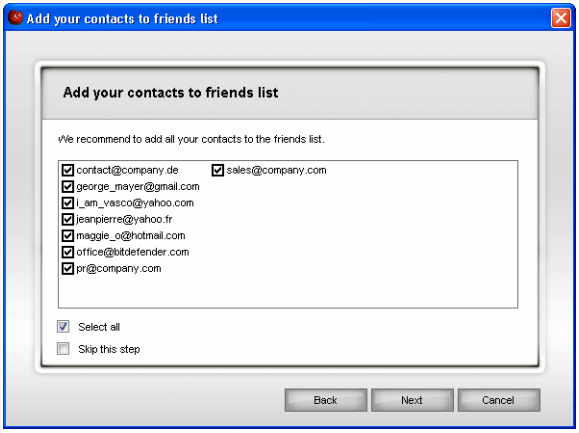
Adım 1/6 - Hoşgeldiniz Ekranı



Hoşgeldiniz Ekranı

İleri'yi tıklayın.

Adım 2/6 - Arkadaş Listesini Doldur



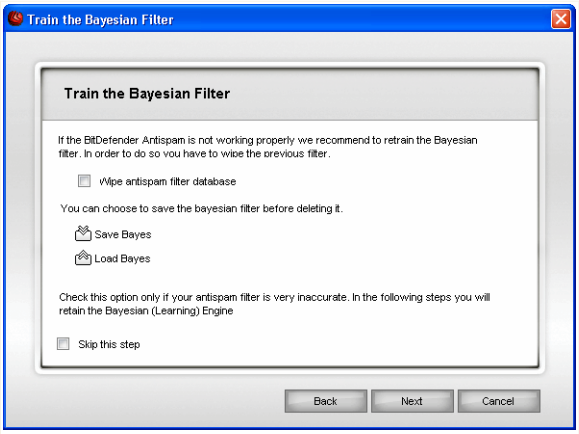
Arkadaşlar Listesini Doldurun

Burada, **Adres Defterinizdeki** tüm adresleri görebilirsiniz. Lütfen **Arkadaşlar Listenize** eklemek istediğiniz adresleri seçin (hepsini seçmenizi öneriyoruz). İçeriklerine bağlı kalmaksızın bu adreslerden gelen tüm mesajları alacaksınız.

Arkadaşlar Listesindeki tüm adresleri eklemek için, **Hepsini Seç'** i işaretleyin.

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

Adım 3/6 - Bayesian Veri Tabanını Sil



Bayesian Veri Tabanını Sil

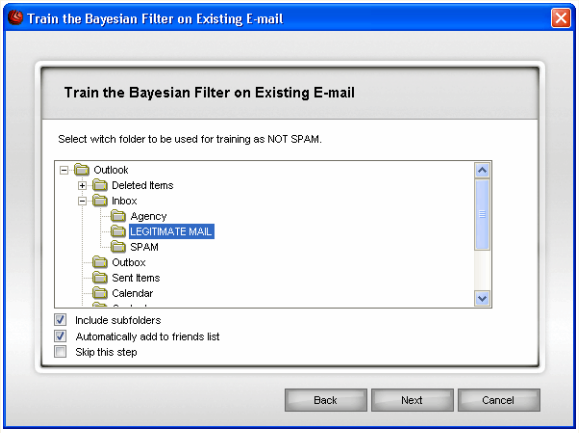
Antispam filtrenizde verim düşüklülüğü yaşamaya başlayabilirsiniz. Bu yanlış eğitmeden kaynaklanmış olabilir (yani, bir takım doğru mesajları yanlışlıkla spam olarak etiketlemiş veya bunun aksini yapmış olabilirsiniz). Eğer filtreniz çok hatalı ise, filtre veri tabanını silmeniz ve filtreyi yeniden eğitmeniz gerekebilir.

Bayesian veri tabanını sıfırlamak için **Antispam veri tabanını sil** seçeneğini tıklayın.

Bayesian veri tabanı listesini istediğiniz bir yere kaydetmek/yüklemek için **Bayes'i Kaydet** / **Bayes'i Yükle** butonlarını kullanın. Dosya `.dat` uzantısına sahip olacaktır.

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

Adım 4/6 - Bayesian Filtresini Doğru E-posta ile Eğit



Bayesian Filtresini Doğru E-posta ile Eğit

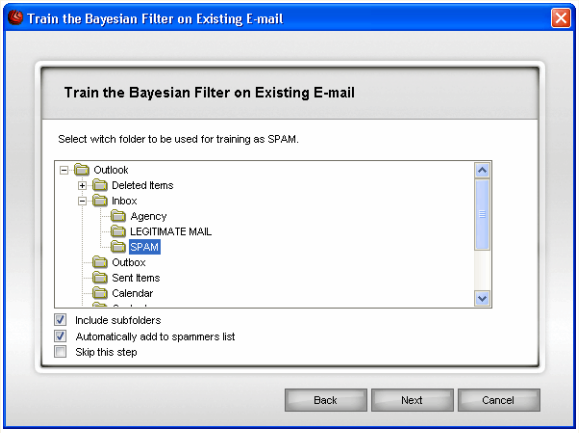
Lütfen doğru e-posta mesajları içeren bir klasör seçin. Bu mesajlar antispam filtresini eğitmek için kullanılacaktır.

Dizin listesinin iki gelişmiş seçenek vardır:

- **Alt klasörleri dahil et** - alt klasörleri seçiminize dahil etmek için;
- **Otomatik olarak Arkadaş Listesine Ekle** - göndericileri **Arkadaşlar listesine** eklemek için..

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

Adım 5/6 - Bayesian Filtresini Spam ile Eğit



Bayesian Filtresini Spam ile Eğit

Lütfen spam e-posta mesajları içeren bir klasör seçin. Bu mesajlar antispam filtresini eğitmek için kullanılacaktır.

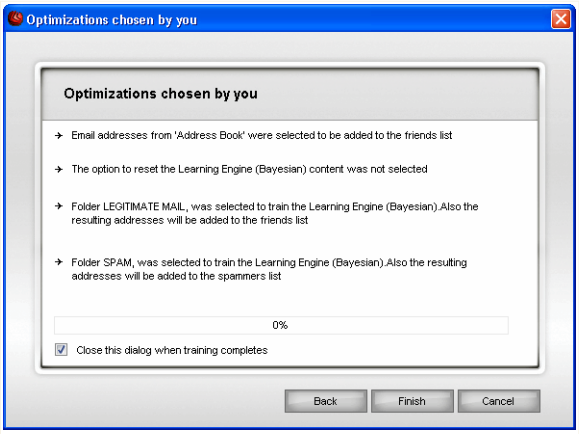
Önemli
Lütfen seçtiğiniz klasörün doğru hiçbir e-posta mesajı içermediğinden emin olun, aksi takdirde antispam performansı belirgin bir sekilde düşecektir.

Dizin listesinin iki gelişmiş seçenek vardır:

- **Alt klasörleri dahil et** - alt klasörleri seçiminize dahil etmek için;
- **Otomatik olarak Spamcılar Listesine Ekle** - göndericileri **Spamcılar listesine** eklemek için.

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

Adım 6/6 - Özet



Özet

Burada, yapılandırma sihirbazı ile ilgili tüm ayarları görebilirsiniz. Bir önceki adıma geri dönerek (**Geri** seçeneğini tıklayarak) herhangi bir değişiklik yapabilirsiniz.

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

11. Gizlilik Kontrolü

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

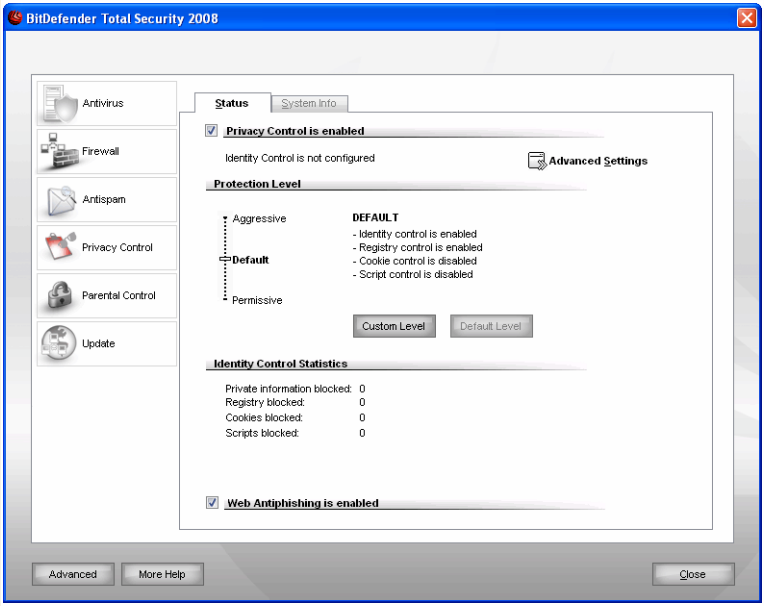
BitDefender ayrıca, gezdiğiniz web sitelerini tarayarak herhangi bir phishing tehdidi algılarsa sizi uyaracaktır.

Bu kullanım kılavuzunun **Gizlilik Kontrolü** bölümü aşağıdaki başlıklardan oluşmaktadır:

- Gizlilik Kontrolü Durumu
- Gelişmiş Ayarlar - Kişisel Gizlilik Kontrolü
- Gelişmiş Ayarlar - Kayıt Kontrolü
- Gelişmiş Ayarlar - Cookie Kontrolü
- Gelişmiş Ayarlar - Script Kontrolü
- Sistem Bilgileri
- Antiphishing Araç Çubuğu

11.1. Kişisel Gizlilik Durumu

Kişisel gizlilik kontrolünü yapılandırmak ve durumu hakkında bilgi almak için ayarlar konsolundan, **Kişisel Gizlilik Kontrolü>Durum** tuşunu tıklayın. Sıradaki pencere çıkacaktır:



Kişisel Gizlilik Durumu

11.1.1. Gizlilik Kontrolü

Önemli
Veri hırsızlığını önlemek ve kişisel bilgilerinizi korumak için, **Kişisel Gizlilik Kontrolü**'nü aktifleştirin.

Kişisel Gizlilik Kontrolü bilgisayarınızı 5 önemli koruma kontrolü Kullanarak korur:

- Kişisel Gizlilik Kontrolü – dışarı giden tüm HTTP ve SMTP trafiğini Kişisel Gizlilik bölümünde oluşturduğunuz kurallara göre filtre ederek, kişiye özel gizli verilerinizi korur.

Not
Bölümün sonunda **Kişisel Gizlilik Kontrolü İstatistikleri**'ni görebilirsiniz

- Kayıt Kontrolü – bir program, Windows başlatıldığında çalıştırılmak için kayıt bilgisini değiştirmeye 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.

Koruma Seviyesi Yapılandırma

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 **Kimlik Kontrolü'** nü etkinleşir
Agresif	**Kayıt Kontrolü**, **Kimlik Kontrolü** ve **Script Kontrolü**etkinleşir.

Koruma seviyesini yapılandırmak için, **Kullanıcı Ayarı Seviyesi**' ni tıklayınız. Görüntülenecek olan pencerede etkinleştirmek istediğiniz koruma kontrolünü seçip, **Tamam'** a basın.

Çubuğu varsayılan seviyesine konumlamak için **Varsayılan Seviye** seçeneğini tıklayın.

11.1.2. Antiphising Koruması

Phishing, sosyal mühendislik tekniklerini kullanarak insanları aldatıp, kişisel bilgilerini ele geçirmeye yönelik suç teşkil eden bir aktivitedir.

Çoğu zaman, phishing denemeleri gerçeği gibi görünüp aslında sahte olan yığın e-mailler gönderimi şeklinde gelişir. Bu aldatmaca mesajlar en azından birkaç alıcının bunlara ikna olmasını ümit edip, kişisel bilgileri açığa çıkarmayı amaçlarlar.

Bir phishing mesajı genellikle online hesabınızı ele geçirmeye çalışır. Sahte bir web sitesi tarafından sağlanan özel bilgilerinize ihtiyaç duyan bir linke tıklamanız için sizi ikna etmeye çalışır. Örneğin, hesap bilgilerinizi doğrulayın, banka hesabınızın kullanıcı adını ve şifresini girin gibi. Bazen çok inandırıcı olabilirler, mesajlar sizin halihazırda olan hesaplarınızdan geliyor numarası yapabilir veya linki kullanmazsanız hesabınızın askıya alınacağı gibi korkutma yöntemleri seçebilirler.

Phishingler ayrıca keylogger truva atları gibi spywareleri kullanarak hesap bilgilerinizi direk olarak bilgisayarınızdan çalabilirler.

Phishing mesajlarının ana hedefi eBay, PayPal, bankaların internet şubeleri gibi müşterilerin online ödeme servisleridir Son dönemde sosyalleşme websiteleri kişisel bilgileri kullanarak kimliklerin çalınmasına olanak sağladığı için phishinglerin hedefi haline gelmiştir.

İnternette dolaşırken phishing tehlikelerine karşı korunmak için **Antiphishing**' i etkin halde tutun. Bu yolla, BitDefender siz erişmeden önce her web sitesini taracayak, ve olabilecek phishing tehditlerine karşı sizi uyaracaktır. BitDefender tarafından düzenlenecek Beyaz Liste' deki web siteleri taranmayacaktır.

Antiphishing korumasını ve Beyaz Listeyi kolayca yönetebilmek için Internet Explorer' a entegre edilmiş Antiphishing araç çubuğunu kullanın. Daha fazla bilgi için "*Antiphishing Araç Çubuğu*" (shf. 185) bölümüne bakınız.

11.2. İleri Ayarlar – Kişisel Gizlilik Kontrolü

Gizli verileri güvenli tutmak hepimizi endişelendiren önemli bir konudur. Veri hırsızları, İnternet 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.

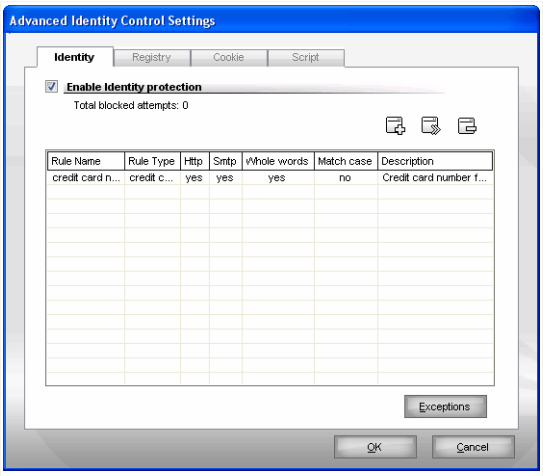
Kişisel Gizlilik Kontrolü kişiye özel gizli verilerinizi güvende tutmanıza yardımcı olur. HTTP veya SMTP trafiğini, veya her ikisini de, tanımlamış olduğunuz belirli dizgiler için tarar. Bir eşleşme bulduğunda, ilgili web sayfası veya e-posta engellenir.

Çoklu kullanıcı desteğinin sağlandığı sistemlerde, başka herhangi bir kullanıcı sizin düzenlediğiniz kuralları göremez.

Gizlilik kurallarını **Kişisel Gizlilik** bölümünden düzenleyebilirsiniz. Bu bölüme erişmek için **Gelişmiş Gizlilik Kontrol Ayarları** bölümünden **Kişisel Gizlilik** tabına tıklayınız.

Not

Bu bölüme girmek için, **Gelişmiş Gizlilik Kontrol Ayarları** bölümünden**Gizlilik Kontrolü>Durumu**' nu tıklayın. Sonra ayarlar konsolundan, **Gelişmiş Ayarlar**' ı tıklayın.



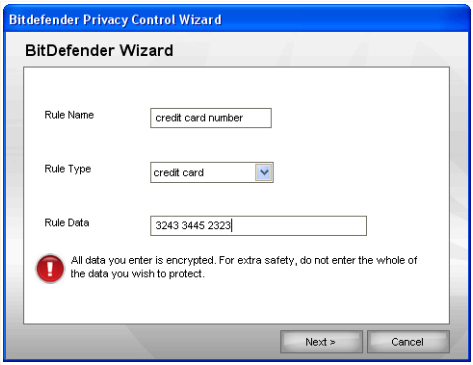
Kimlik Kontrolü

11.2.1. Kimlik Kurallarını Yaratmak

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

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

> ***Not***
> Bizim önerimiz kural isminin en az üç karakterden oluşmasıdır. Eğer kural ismi üç karakterden az olursa mesajları ve web sayfalarını engellemede problemler yaşanabilir.

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

İleri'yi tıklayın.

Adım 2/3 – Trafiği Seçin

Trafiği Seç

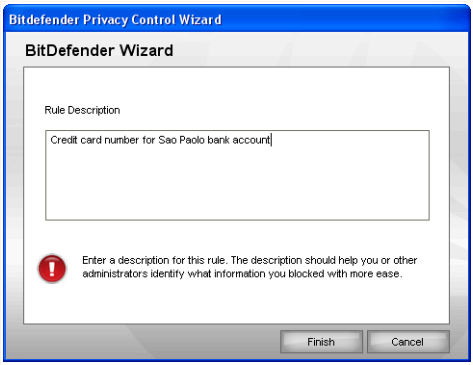
BitDefender'ın taramasını istediğiniz trafiği seçin. Aşağıdaki seçenekler mevcuttur:

- **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.

Kuralı uygulamak için kural verilerinin sadece tüm kelimelerle uymasını yada saptanan dizgi ile uymasını seçebilirsiniz.

İleri'yi tıklayın.

Adım 3/3 – Kuralı Tanımlayın



Kural Tanımla

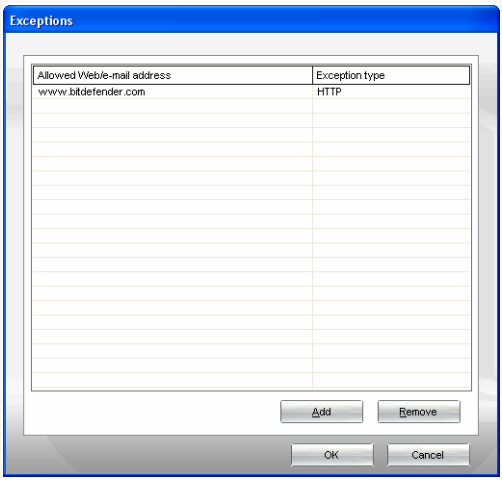
Düzenleme alanına, kuralın kısa bir tanımını girin.

Bitir seçeneğini tıklayın.

11.2.2. İstisnaları Belirleme

Bu bölüme özel kişisel gizlilik kuralları için istisnaları belirlerken ihtiyacınız olacak. Bu bölümü, HTTP (web) üzerinden kredi kartı numarası gönderilmesini engellemek için kural yaratacağımızda göz önüne alalım. Kredi kartı numaranız kullanıcı hesabınızla bir web sitesine gönderildiğinde sayfa bloklanır. Örnek olarak internet üzerinden (güvenli olduğunu bildiğiniz) bir giyim eşyası satın almak istediğinizde, bunu istisna olarak belirlemeniz gerekir.

İstisnaları yönetebileceğiniz pencereyi açmak için, **İstisnalar'** a tıklayın.



İstisnalar

İstisna eklemek için bu adımları takip edin:

1. Tabloya yeni bir giriş yapmak için **Ekle**' ye tıklayın.
2. **İzin verilen adresleri belirle**' ye çift tıklayıp istisna olarak eklemek istediğiniz web veya mail adreslerini yazın.
3. **Tipi Seçin**' ne çift tıklayıp uygun adres tipini seçin.
   - Bir web adresi belirlemek istiyorsanız **HTTP**' yi seçin.
   - Bir web adresi belirlemek istiyorsanız **SMTP**' yi seçin.

Listeden bir istisnayı kaldırmak istiyorsanız, istisnayı seçip **Kaldır**' ı tıklayın.

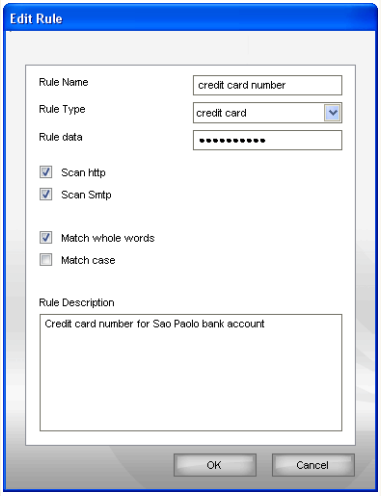
Değişiklikleri kaydetmek için **Tamam** tuşuna basın.

11.2.3. Kuralların Yönetimi

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.

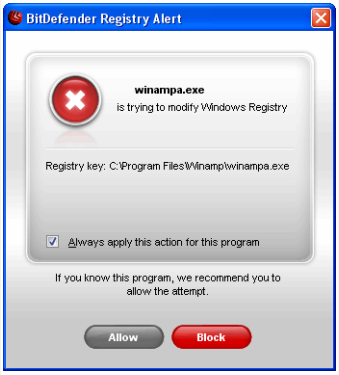
Değişiklikleri kaydetmek ve pencereyi kapatmak için **Tamam**'ı tıklayın.

11.3. Gelişmiş Ayarlar – 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 Bu yolla, bir kural yaratılacağında ve aynı eylem uygulanacağında bu program Windows başlangıcında uygulamak üzere kayıt girdisini değiştirmeye çalışacaktır.

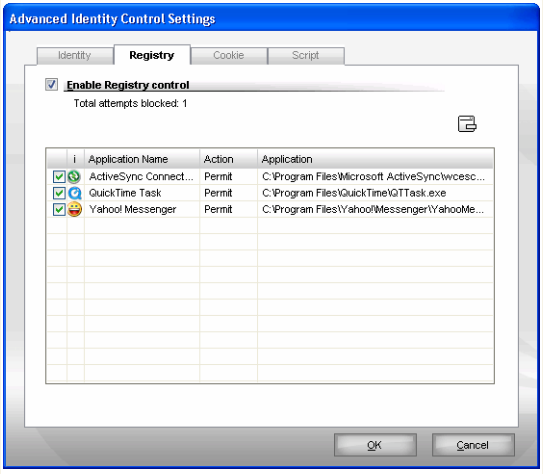
Not

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

Hatırlanan her bir kurala daha ileri ayarlar yapmak için **Kayıt** bölümünden erişebilirsiniz. Bu bölüme erişmek için **Gelişmiş Kişisel Gizlilik Ayarları** bölümünden**Kayıt** tabına tıklayınız.

Not

Bu bölüme girmek için, **Gelişmiş Gizlilik Kontrol Ayarları** bölümünden**Gizlilik Kontrolü>Durumu'** nu tıklayın. Sonra ayarlar konsolundan, **Gelişmiş Ayarlar'** ı tıklayın.



Kayıt Kontrolü

Kuralın tabloda listelendiğini göreceksiniz.

Bir kuralı silmek için, kuralı seçin ve **Sil** seçeneğini tıklayın. Bir kuralı silmeden geçici olarak devredışı bırakmak için uygun kutucuktaki işareti kaldırın.

Bir kuralın eylemini değiştirmek için, eylem sahasını çift tıklayıp menüden uygun seçeneği seçin.

Pencereyi kapatmak için **Tamam** seçeneğini tıklayın.

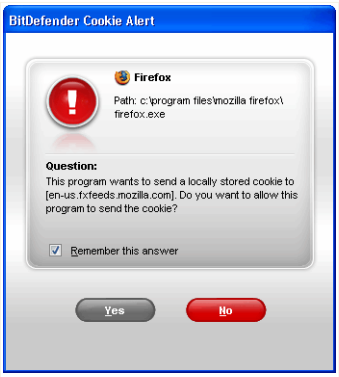
11.4. Gelişmiş Ayarlar - Cookie Kontrolü

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.

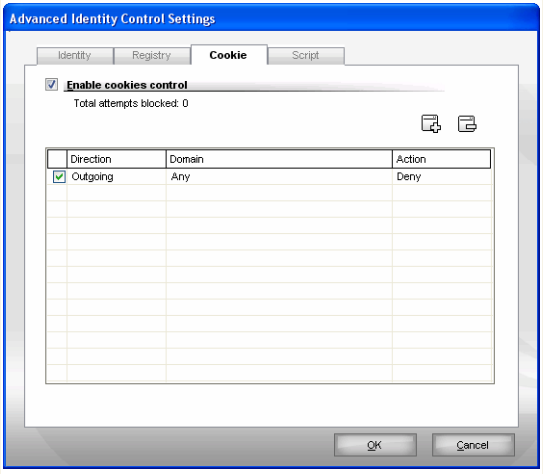
Not

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. Bu bölüme erişmek için **Gelişmiş Kişisel Gizlilik Kontrolü Ayarları** bölümünden**Cookie** tabına tıklayınız.

Not

Bu bölüme girmek için, **Gelişmiş Gizlilik Kontrol Ayarları** bölümünden**Gizlilik Kontrolü>Durumu'** nu tıklayın. Sonra ayarlar konsolundan, **Gelişmiş Ayarlar'** ı tıklayın.



Cookie Kontrolü

Kuralın tabloda listelendiğini göreceksiniz.

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.

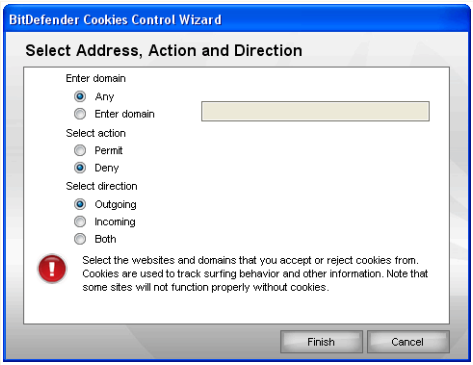
Bir kuralı silmek için, sadece kuralı seçin ve **Sil** seçeneğini tıklayın. Bir kuralın parametresini değiştirmek için, alanına çift tıklayın ve istediğiniz değişikliği yapın. Bir kuralı silmeden sadece geçici olarak etkisiz kılmak için, buna karşılık gelen onay kutusunu temizleyin.

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

11.4.1. 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 adresi** – 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.

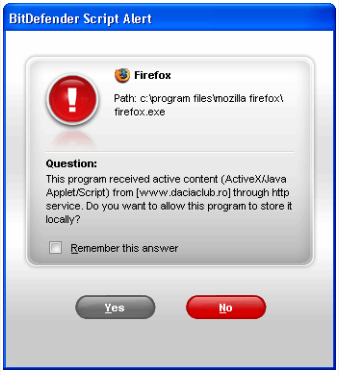
Değişiklikleri kaydetmek ve pencereyi kapatmak için **Tamam**'ı tıklayın.

11.5. Gelişmiş Ayarlar - 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 yapabilmeniz için 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

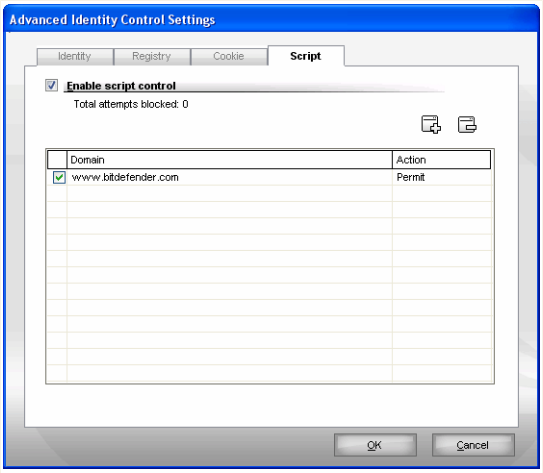
Kaynakların isimlerini görebilirsiniz.

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. Bu bölüme erişmek için **Gelişmiş Kişisel Gizlilik Kontrolü Ayarları** modülünden **Script** tabına tıklayınız.

Not

Bu bölüme girmek için, **Gelişmiş Gizlilik Kontrol Ayarları** bölümünden**Gizlilik Kontrolü>Durumu'** nu tıklayın. Sonra ayarlar konsolundan, **Gelişmiş Ayarlar'** ı tıklayın.



Script Kontrolü

Kuralın tabloda listelendiğini göreceksiniz.

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.

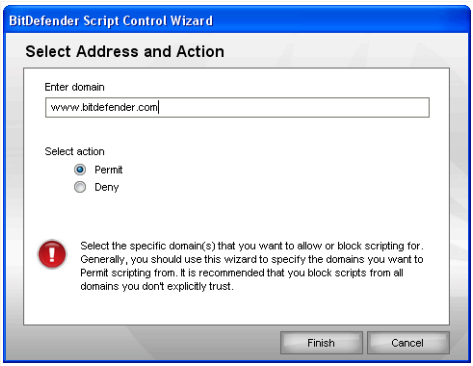
Bir kuralı silmek için, sadece kuralı seçin ve **Sil** seçeneğini tıklayın. Bir kuralın parametresini değiştirmek için, alanına çift tıklayın ve istediğiniz değişikliği yapın. Bir kuralı silmeden sadece geçici olarak etkisiz kılmak için, buna karşılık gelen onay kutusunu temizleyin.

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

11.5.1. Yapılandırma Sihirbazı

Yapılandırma sihirbazı 1 adımlı bir prosedürden oluşmaktadır.

Adım 1/1 – Adres ve İşlemi Seçin



Adres ve İşlemi Seçin

Parametreleri ayarlayabilirsiniz

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

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

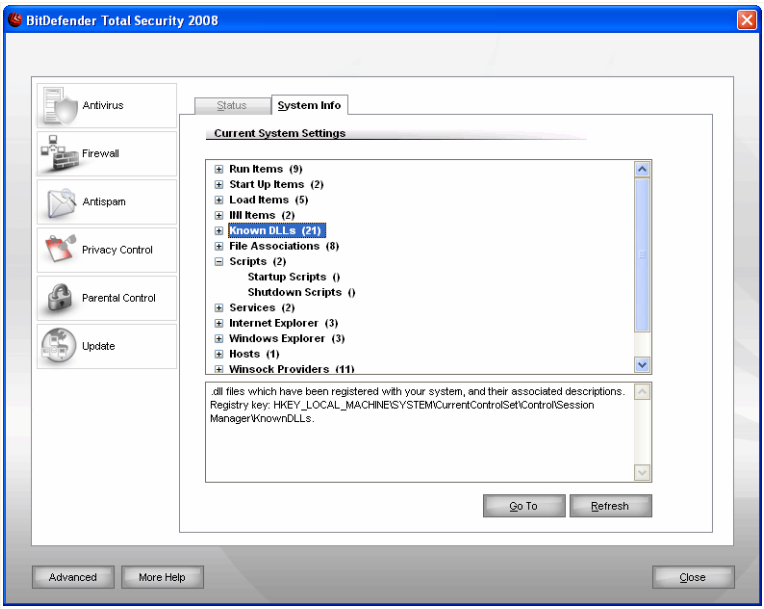
Bitir seçeneğini tıklayın.

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

11.6. Sistem Bilgileri

BitDefender, tüm sistem ayarlarını ve başlangıçta çalışan kayıtlı uygulamaları tek bir yerden görmenize izin verir. Bu yolla, sistemdeki aktiviteyi ve yüklenmiş uygulamaları görebileceksiniz, yanısıra sisteme bulaşan enfeksiyonları tanımlayabileceksiniz.

Sistem bilgisine ulaşmak için, ayarlar konsolundan **Kişisel Gizlilik Kontrolü>Sistem Bilgisi'** ni tıklayın. Sıradaki pencere çıkacaktır:



Sistem Bilgileri

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

Üç buton vardır:

- **Sil** – Seçilen bileşenleri siler. Seçiminizi doğrulamak için, **Evet'** e basmalısınız.

Not
Güncelleme sonrası seçiminizi doğrulayın ibaresini görmek istemiyorsanız, **Bu soruyu tekrar sorma**seçeneğini işaretleyin.

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

Not
Seçilen öğeye bağlı olarak **Sil** yada **Git** butonlarından biri ya da hepsi görünmeyecektir.

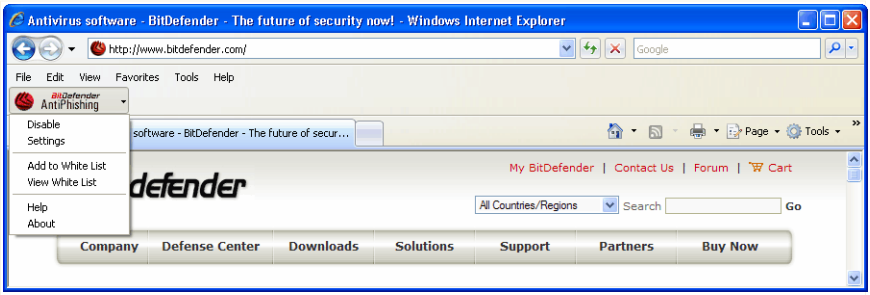
11.7. Antiphishing Araç Çubuğu

BitDefender, sizi, İnternette gezerken phishing denemelerine karşı korur. Erişilen web sitelerini tarayarak herhangi bir phishing tehdidine karşı sizi uyarır. BitDefender tarafından düzenlenecek Beyaz Liste' deki web siteleri taranmayacaktır.

Kolay ve verimli bir şekilde antiphishing korumasını yönetebilirsiniz. Beyaz Liste kullanan BitDefender Antiphishing araç çubuğu Internet Explorer' a entegre edilmiştir.

Antiphishing araç çubuğu, Internet Explorer' ın üst tarafında **BitDefender ikon**' u ile gösterilir. Araç çubuğu menüsünü açmak için üzerine tıklayın.

Not
Eğer araç çubuğunu göremiyorsanız, **Görünüm** menüsünde, **Araç Çubukları** üzerine gelerek **BitDefender Araç Çubuğu**' nu seçin.



Antiphishing Araç Çubuğu

Araç Çubuğu menüsünde aşağıdaki komutlar bulunmaktadır:

- **etkin/etkin değil** - BitDefender Antiphishing araç çubuğu etkin/etkin değil.

Not
Eğer antiphishing araç çubuğunu etkisizleştirirseniz phishing denemelerine karşı etkili bir koruma içinde olmayacaksınız.

- **Ayarlar** - antiphishing araç çubuğu ayarlarını belirleyebileceğiniz bir gözatma penceresini açar.

  Aşağıdaki seçenekler mevcuttur:
  - **Taramayı Etkinleştir** - antiphishing taraması etkinleştirilir.
  - **Beyaz Listeye eklemeden önce sor** - bir web sitesini Beyaz Listeye eklemeden önce sorar.
- **Beyaz Listeye Ekle** - geçerli web sayfasını Beyaz Liste' ye ekler

Not
Beyaz Liste' ye site eklemenin anlamı, BitDefender' ın bu siteyi bir daha taramayacağı demektir. Biz Beyaz Liste' ye sadece tam olarak güvendiğiniz siteleri eklemenizi öneririz.

- **Beyaz Liste** - Beyaz Liste' yi açar.

  BitDefender antiphishing motoru tarafından kontrol edilmeyen tüm web sitelerini görebilirsiniz.

  Bir siteyi, üzerinde var olan phishing tehditlerinden haberdar olabilmek için Beyaz Liste' den kaldırmak istiyorsanız, **Kaldır** tuşuna basın.

  Sadece tamamen güvendiğiniz siteleri Beyaz Liste' ye ekleyiniz, çünkü bu siteler antiphishing motoru tarafından bir daha taranmayacaktır. Beyaz Liste' ye site eklemek için, site adresini uygun alana yazdıktan sonra **Ekle**' ye basın
- **Yardım** - yardım dosyasını açar.
- **Hakkında** - bölümüne tıkladığınızda BitDefender hakkında bilgi alabileceğiniz bir pencere açılır ve acil bir durumda yardım alabileceğiniz yerleri görürsünüz.

12. Ebeveyn Kontrolü

Ebeveyn Kontrolü şunlara erişimi engelleyebilir:

- Uygunsuz web sayfaları.
- belirli periyotlar için, internet erişimi (örneğin ders saatlerinde).
- anahtar kelimeyi içeren web sayfaları ve e-posta mesajları.
- oyun, chat, dosya paylaşım programları ve diğerleri gibi uygulamalar.

Önemli

Bu modül, sadece yönetimsel hakları olan (sistem yöneticisi) kullanıcı tarafından erişilebilir ve yapılandırılabilir. Ayarlar şifre ile korunmuş ise, sadece şifre sağlandığında değiştirilebilir. Bir Sistem Yöneticisi, başka bir sistem yöneticisi tarafından kendisine kurallar tanımlanmış olan bir kullanıcı için yeni bir kural dizini oluşturamaz

Bu kullanım kılavuzunun **Ebeveyn Kontrolü** bölümü aşağıdaki başlıklardan oluşmaktadır:

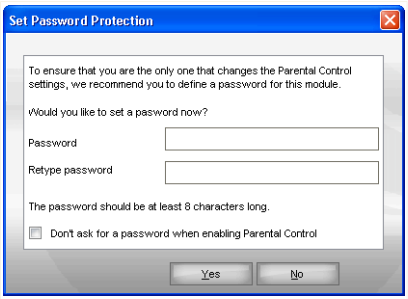
12.1. Ebeveyn Kontrolü Koruma Ayarları

Bu bilgisayarı kullanan, yönetim hakları olan tek kişi değilseniz, BitDefender ayarlarınızı bir şifre ile korumanızı tavsiye ediyoruz. Şifreleme sayesinde, belirli kullanıcılar için belirlemiş olduğunuz Ebeveyn Kontrolü ayarlarını, diğer yönetim hakları olan kullanıcılardan korumuş olacaksınız.

BitDefender, Ebeveyn Kontrolünü etkinleştirdiğinizde varsayılan olarak şifre koruması verip vermeyeceğinizi sorar.

Şifre koruması ayarlamak için aşağıdakileri yapın:

1. **Şifre** alanına belirlediğiniz şifreyi yazın.
2. **Şifreyi Tekrarla** alanına belirlediğiniz şifreyi tekrar yazın.
3. Şifreyi kaydetmek ve pencereyi kapatmak için **Tamam**' ı tıklayın.



Şifre Koruması Ayarlama

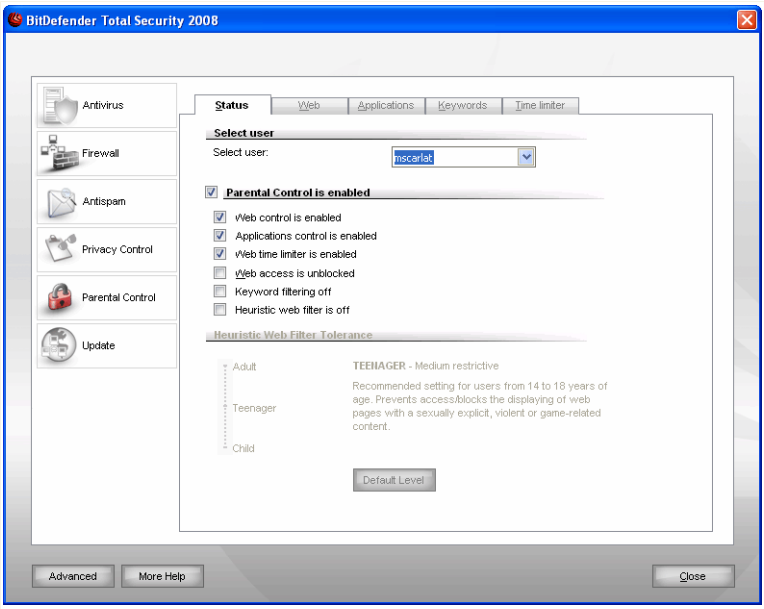
Bir kez şifre belirledikten sonra, Ebeveyn Kontrolü seçeneklerini değiştirmek istediğinizde şifre girmeniz istenecektir. Başka sistem yöneticileri varsa, BitDefender ayarlamaları için bu şifreyi kullanmak zorundadırlar.

Not
Diğer BitDefender ayarları şifre gerektirmeyecektir.

Bir şifre ayarlamayacaksanız ve bu pencerenin bir daha görünmesini istemiyorsanız, **Ebeveyn Kontrolü etkinleştirildiğinde şifre için sorma** seçeneğini işaretleyin.

12.2. Ebeveyn Kontrolü Durumu

Seçilen bir kullanıcı için Ebeveyn Kontrolünü yapılandırmak için, ayarlar konsolunda **Ebeveyn Kontrolü>Durum**' u tıklayınız. Sıradaki pencere çıkacaktır:



Ebeveyn Kontrolü Durumu

Önemli
Özelleştirilmiş bilgisayar erişim kurallarınızı kullanarak çocuklarınızı uygun olmayan içeriklere karşı korumak için, **Ebeveyn Kontrol** fonksiyonunu etkin halde tutun.

12.2.1. Koruma Kontrollerini Seçme

Koruma seviyesini yapılandırmak için, önce bu ayarların uygulanacağı kullanıcıyı seçmeniz gerekmektedir. Daha sonra, aşağıda belirtilen kontrolleri kullanarak koruma seviyesini yapılandırın:

- **Web Kontrolü** – Web bölümünde tarafınızdan tanımlanan kurallara göre web navigasyonunu filtrelemek için **Web Kontrolünü** etkin hale getirin
- **Uygulama Kontrolü** – Uygulamalar bölümünde tarafınızdan tanımlanan kurallara göre, uygulamaların bilgisayarınıza erişimini engellemek için **Uygulama Kontrolünü** etkinleştirin.

- **Web Zaman Sınırlayıcı** – Zaman Sınırlayıcı bölümünde tarafınızdan ayarlanan zaman tablosuna göre web erişimine izin vermek için **Web Zaman Sınırlayıcıyı** etkinleştirin.
- **Web Erişimi** – tüm web sitelerine (sadece Web bölümünde olanları değil) erişimi engellemek için bu seçeneği etkinleştirin
- **Anahtar Kelime Filtreleme** – Anahtar kelime bölümünde tarafınızdan tanımlanan kurallara göre web ve mail erişimini filtrelemek için **Anahtar Kelime Filtrelemeyi** etkinleştirin
- **Sezgisel web filtreleme** – web erişimini yaş kategorisi esasına dayalı önceden belirlenmiş doğru olarak filtrelemek için bu seçeneği etkinleştirin.

Not

Ebeveyn Kontrolünün tüm özelliklerinden tam olarak yararlanabilmeniz için, seçilen kontrolleri yapılandırmalısınız. Yapılandırmanın nasıl yapılacağını öğrenmek için bu bölümdeki takip eden konulara bakın.

12.2.2. Sezgisel Web Filtrelemeyi Yapılandırma

Sezgisel Web Filtreleme web sayfalarını analiz ederek, potansiyel uygunsuz içerik şablonuna uyanları engeller.

Web erişimini önceden belirlenmiş kurallara göre filtrelemek için, bir tolerans seviyesi belirlemelisiniz. Seçilen kullanıcı için uygun gördüğünüz tolerans seviyesini ayarlamak için kaydırma çubuğunu ölçek üzerinde sürükleyin.

3 tolerans seviyesi bulunmaktadır:

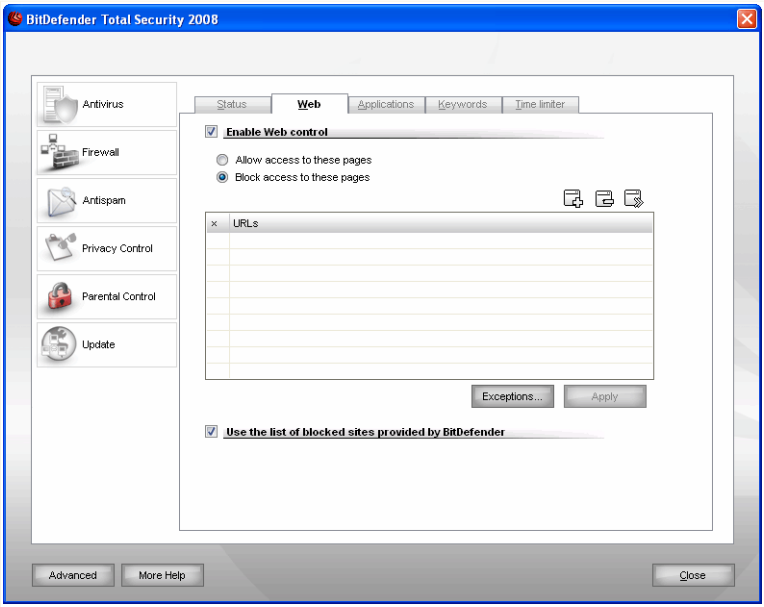
Tolerans seviyesi	Açıklama
Çocuk	14 yaşın altındaki kullanıcılar için tavsiye edilen ayarlara göre sınırlı web erişimi sağlar. Çocuklar için potansiyel olarak zararlı içerik içeren Web sayfaları (Porno, cinsellik, uyuşturucu, hack' leme, vs.) engellenir.
Genç	14-18 yaş arası kullanıcılar için tavsiye edilen ayarlara göre sınırlı web erişimi sağlar Cinsel, pornografik veya yetişkinlere yönelik içerik içeren Web sayfaları engellenir.
Yetişkin	İçeriklerine bağlı kalmaksızın tüm web sayfalarına sınırsız erişim sağlar.

Çubuğu varsayılan seviyeye ayarlamak için **Varsayılan Seviye** seçeneğini tıklayın.

12.3. Web Kontrolü

Web Kontrolü , uygun olmayan içerikli web sitelerine erişimi engellemenize yardımcı olur. Sitelere ve bunların belirli kısımlarına erişimi kısıtlamak için bir seçenekler listesi sağlanmış olup, bu liste düzenli güncellemenin bir parçası olarak BitDefender tarafından sürekli güncellenmektedir.

Web Kontrolünü yapılandırmak için ayarlar konsolundan**Ebeveyn Kontrolü>Web**' i tıklayınız. Sıradaki pencere çıkacaktır:



Web Kontrolü

Bu korumayı etkinleştirmek için, **Web Kontrolünü Etkinleştir** seçeneğine karşılık gelen onay kutusunu seçin.

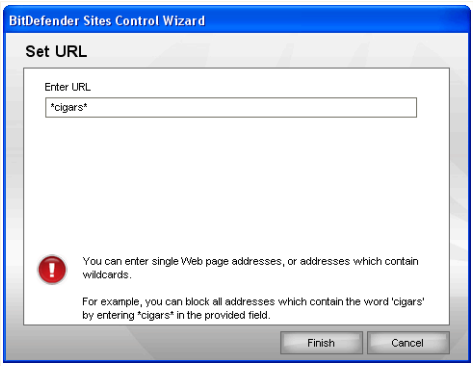
İzin verilen/engellenen siteleri görmek için, **Bu sayfalara erişime izin ver**/**Bu sayfalara erişimi engelle** seçeneğini seçin. Tamamlayıcı listeyi görebileceğiniz bir pencereye erişebilmek için, **İstisnalar...** seçeneğini tıklayın.

Kurallar elle girilmelidir. İlk olarak, sihirbazda belirleyeceğiniz web sitelerine erişime izin vermek/engellemek için, **Bu sayfalara erişime izin ver**/**Bu sayfalara erişimi engelle** seçeneğini seçin. Daha sonra, yapılandırma sihirbazını başlatmak için **Ekle...** seçeneğini tıklayın.

12.3.1. Yapılandırma Sihirbazı

Yapılandırma sihirbazı 1 adımlı bir prosedürden oluşmaktadır.

Adım 1/1 – Web Sitelerini Belirle



Web Sitelerini Belirle

Kuralın uygulanacağı web sitelerini girin ve **Bitir** seçeneğini tıklayın.

Önemli
Söz dizimi:

- `*.xxx.com` – kural işlemi, soneki `.xxx.com` olan tüm web sitelerine uygulanacaktır;
- `*porn*`- kural işlemi, web site adresinde `porn` içeren tüm web sitelerine uygulanacaktır;
- `www.*.com`- kural işlemi, Alan soneki `com` olan tüm web sitelerine uygulanacaktır;
- `www.xxx.*` - kural işlemi, Alan soneki ne olursa olsun `www.xxx.` ile başlayan tüm web sitelerine uygulanacaktır.

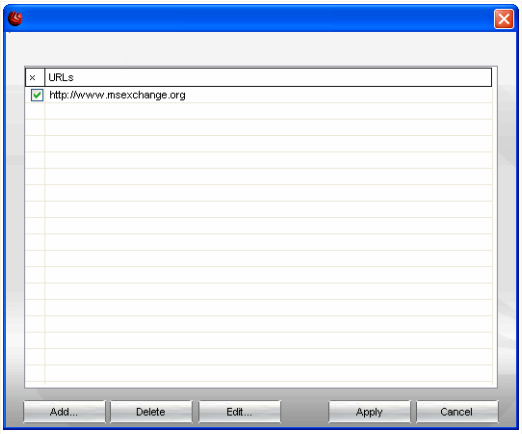
Değişiklikleri kaydetmek için **Uygula** tuşuna basınız.

Bir kuralı silmek için, sadece kuralı seçin ve **Sil** seçeneğini tıklayın. Bir kuralı değiştirmek için, kuralı seçin ve **Düzenle** seçeneğini tıklayın veya üzerine çift-tıklayın. Bir kuralı silmeden sadece geçici olarak etkisiz kılmak için, ilgili onay kutusunu boşaltın.

12.3.2. İstisnaları Belirle

Bazen, belirli bir kural için istisnaları belirlemeniz gerekebilir. Örneğin, adresinde "Katil-Killer" kelimesini içeren (Söz dizimi: `*katil*`) siteleri engellemek için bir kural seti edebilirsiniz. Aynı zamanda, ziyaretçilerin çevrimiçi müzik dinleyebildikleri `killer-music` olarak bilinen bir sitenin bulunduğununda farkındasınız. Daha önce tanımlanan kurala bir istisna oluşturmak için, **İstisnalar** penceresine erişin ve kuralın istisnalarını belirleyin.

İstisnalar.... seçeneğini tıklayın, aşağıdaki pencere belirecektir.



İstisnaları Belirleme

İstisnaları belirlemek için **Ekle...** seçeneğini tıklayın.Yapılandırma sihirbazı belirecektir. İstisnaları ayarlamak için sihirbazı tamamlayın.

Değişiklikleri kaydetmek için **Uygula** tuşuna basınız.

Bir kuralı silmek için, sadece kuralı seçin ve **Sil** seçeneğini tıklayın. Bir kuralı değiştirmek için, kuralı seçin ve **Düzenle...** seçeneğini tıklayın veya kurala çift-tıklayın. Bir kuralı silmeden sadece geçici olarak etkisiz kılmak için, ilgili onay kutusunu boşaltın.

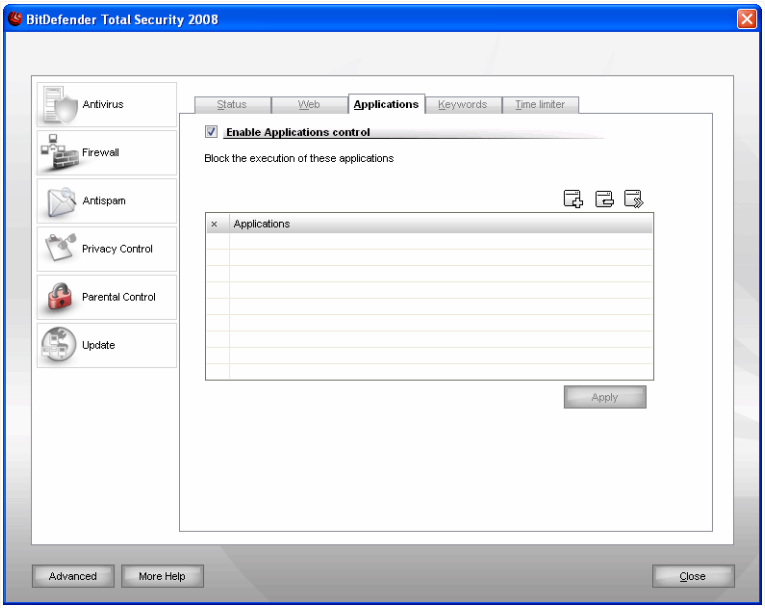
12.3.3. BitDefender Web Karalistesi

Çocuklarınızı korumanıza yardımcı olmak için, BitDefender uygun olmayan veya potansiyel olarak tehlikeli içerik içeren web sitelerinin bulunduğu bir kara liste sunar. Bu Listede yer alan siteleri engellemek için, **BitDefender tarafından sağlanan Engellenen Siteler** listesini kullan seçeneğini seçin.

12.4. Uygulama Kontrolü

Uygulama Kontrolü, herhangi bir uygulamanın çalıştırılmasını engellemenize yardımcı olmaktadır. Bu yolla; oyunlar, medya ve mesajlaşma yazılımının yanı sıra diğer yazılım ve kötü amaçlı yazılım kategorileri engellenebilir. Bu şekilde engellenen uygulama yazılımları, aynı zamanda değişikliklere karşı korunur ve kopyalanamaz veya silinemez.

Uygulama Kontrolünü yapılandırmak için, ayarlar konsolundan **Ebeveyn Kontrolü>Uygulamalar**' ı tıklayın. Sıradaki pencere çıkacaktır:



Uygulama Kontrolü

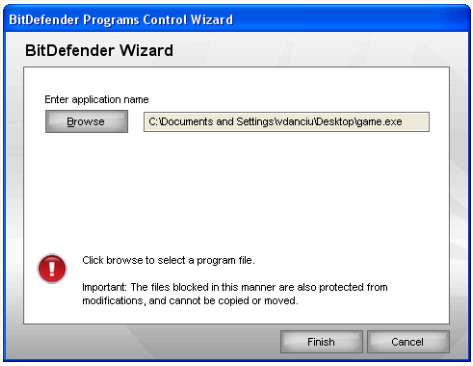
Bu korumayı etkinleştirmek için, **Uygulama Kontrolünü Etkinleştir** seçeneğine karşılık gelen onay kutusunu seçin.

Kurallar elle girilmelidir. Yapılandırma sihirbazını başlatmak için **Ekle...** seçeneğini tıklayın.

12.4.1. Yapılandırma Sihirbazı

Yapılandırma sihirbazı 1 adımlı bir prosedürden oluşmaktadır.

Adım 1/1 – Engellenecek Uygulamayı Seç



Engellenecek Uygulamayı Seç

Gözat'a tıklayın, engellenecek uygulamayı seçin ve **Bitir** seçeneğini tıklayın. Değişiklikleri kaydetmek için Uygula seçeneğini tıklayın.

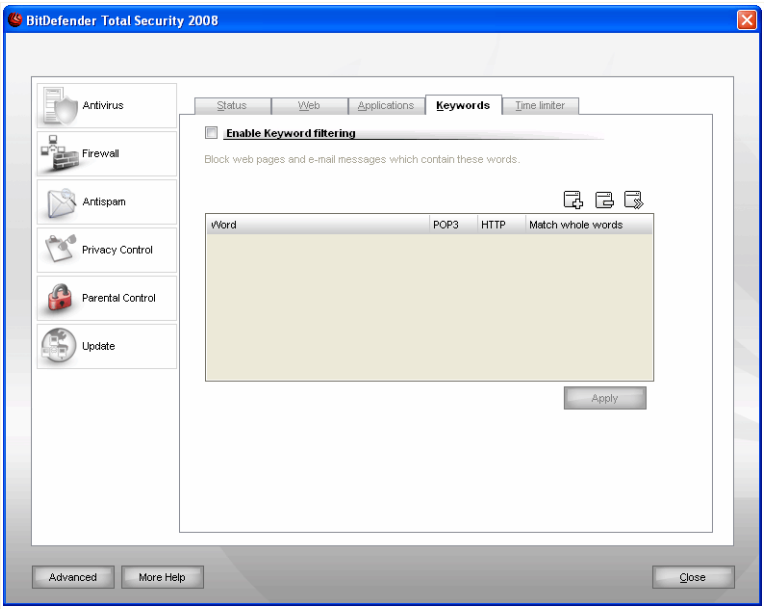
Değişiklikleri kaydetmek için **Uygula** tuşuna basınız.

Bir kuralı silmek için, sadece kuralı seçin ve **Sil** seçeneğini tıklayın. Bir kuralı değiştirmek için, kuralı seçin ve **Düzenle** seçeneğini tıklayın veya üzerine çift-tıklayın. Bir kuralı silmeden sadece geçici olarak etkisiz kılmak için, ilgili onay kutusunu boşaltın.

12.5. Anahtar Kelime Filtreleme

Anahtar kelime filtresi, belirli bir kelime içeren e-posta mesajlarına veya web sayfalarına erişimi engellemenize yardımcı olur. Bu şekilde kullanıcıların uygun olmayan kelimeler veya deyimleri görmesini engelleyebilirsiniz.

Anahtar kelime filtrelemeyi yapılandırmak için, ayarlar konsolundan **Ebeveyn Kontrolü>Anahtar Kelime**' yi tıklayın. Sıradaki pencere çıkacaktır:



Anahtar Kelime Filtreleme

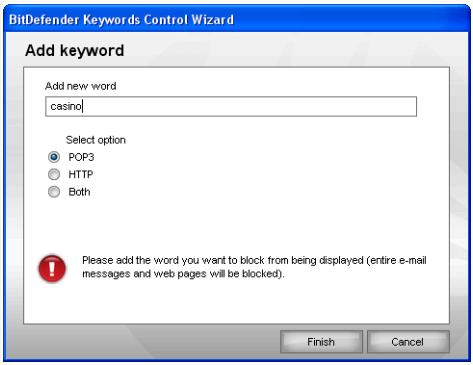
Bu korumayı etkinleştirmek için **Anahtar Kelime Filtreleme** seçeneğine karşılık gelen onay kutusunu seçin.

Kurallar elle girilmelidir. Yapılandırma sihirbazını başlatmak için **Ekle...** seçeneğini tıklayın.

12.5.1. Yapılandırma Sihirbazı

Yapılandırma sihirbazı 1 adımlı bir prosedürden oluşmaktadır.

Adım 1/1 – Anahtar Kelimeyi Girin



Anahtar Kelimeyi Girin

Aşağıda belirtilen parametreleri ayarlamanız gerekmektedir:

- **Anahtar kelime** – Düzenleme alanında engellemek istediğiniz kelime veya deyimi girin.
- **Protokol** – Bu kelime için BitDefender'ın taraması gereken protokolü seçin. Aşağıda belirtilen seçenekler bulunmaktadır:

  Aşağıdaki seçenekler mevcuttur:

Seçenek	Açıklama
POP3	Anahtar kelimeyi içeren e-posta mesajları engellenir.
HTTP	Anahtar kelimeyi içeren web sayfaları engellenir.
Her ikisi	Anahtar kelimeyi içeren e-posta mesajları ve web sayfaları engellenir.

Değişiklikleri kaydetmek için **Uygula** tuşuna basınız.

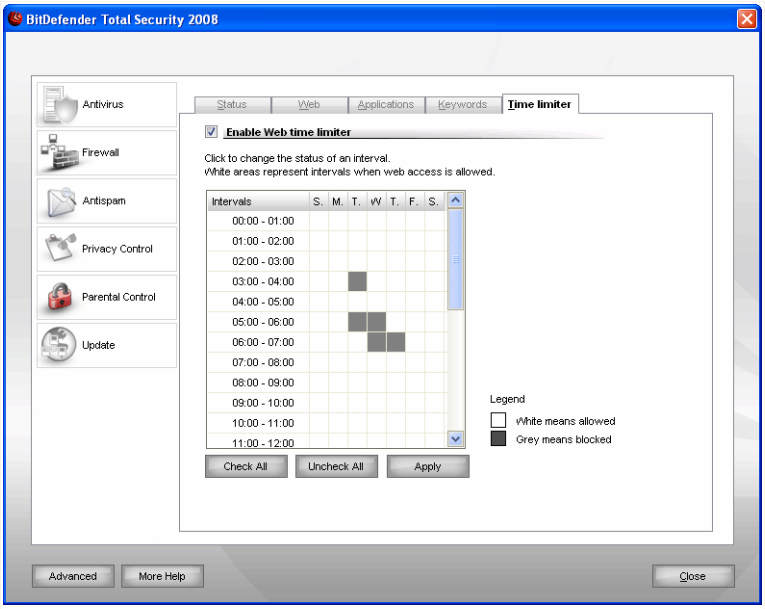
Bir kuralı silmek için, sadece kuralı seçin ve **Sil** seçeneğini tıklayın. Bir kuralı değiştirmek için, kuralı seçin ve **Düzenle** seçeneğini tıklayın veya üzerine çift-tıklayın. Bir kuralı silmeden sadece geçici olarak etkisiz kılmak için, ilgili onay kutusunu boşaltın.

12.6. Web Zaman Sınırlayıcı

Web Zaman Sınırlayıcı, belirli zaman aralıklarında kullanıcıların veya uygulamaların web erişimine izin vermenize veya engellemenize yardımcı olur.

Not
Web Zaman Sınırlayıcı' nın ayarları ne olursa olsun, BitDefender her saatte bir güncelleme yapacaktır.

Web zaman sınırlayıcıyı yapılandırmak için, ayarlar konsolundan **Ebeveyn Kontrolü>Zaman Sınırlayıcı**' yı tıklayın. Sıradaki pencere çıkacaktır:



Web Zaman Sınırlayıcı

Bu korumayı etkin kılmak için, **Web Zaman Sınırlayıcıyı Etkinleştir** seçeneğine karşılık gelen onay kutusunu seçin.

Tüm internet bağlantılarının engelleneceği zaman aralıklarını seçin. Bireysel hücreleri tıklayabilir veya tıklayıp sürükleyerek daha uzun süreleri kapsayabilirsiniz. Ayrıca, tüm

hücreleri seçmek ve tüm web erişimini tamamen engellemek için **Hepsini İşaretle** seçeneğini seçebilirsiniz. Eğer, **Hepsini Kaldır** seçeneğini tıklarsanız, internet bağlantılarına her zaman izin verilecektir.

Önemli
Gri renkli kutular tüm internet bağlantılarının engellendiği zaman aralıklarını temsil etmektedir.

Değişiklikleri kaydetmek için **Uygula** tuşuna basınız.

13. Güncelleme

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.

Internete geniş bant veya DSL ile bağlıysanız, 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.

Güncelleme işlemi hemen başlayarak, dosyaları kademeli olarak günceller. Güncelleme işlemi devam eden operasyonları etkilemeyecek, tüm kırılganlıkları dışarıda tutacaktır.

Güncellemeler aşağıdaki şekillerde olmaktadır:

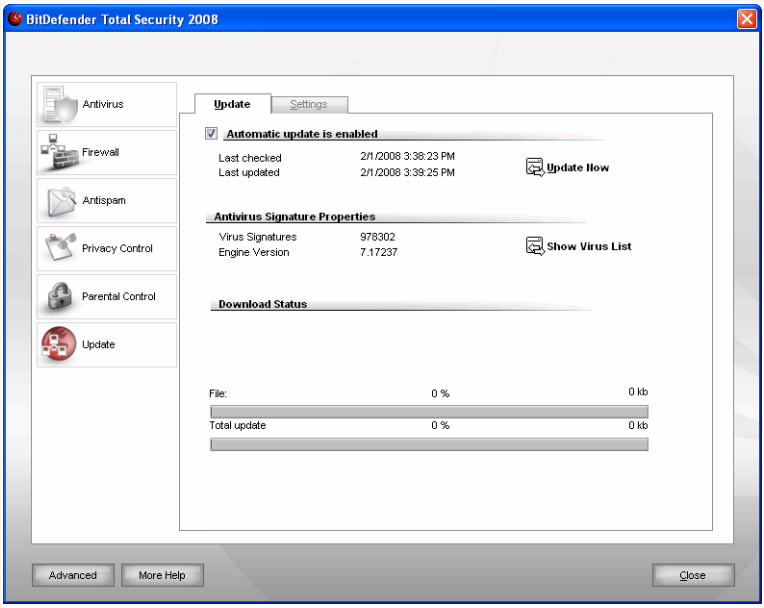
- **Virüs koruma motorları için güncellemeler** – yeni bir tehdit ortaya çıktıkça, bunlara karşı sürekli olarak güncel bir koruma sağlamak amacıyla, virüs imzaları taşıyan dosyaların güncelleştirilmesi gerekmektedir. Bu güncelleme tipi aynı zamanda **Virüs Tanımları Güncellemesi** olarak da bilinmektedir
- **Antispam motorları güncellemeleri** – yeni kurallar sezgisel filtreye ve URL filtresine eklenecek ve yeni görüntüler Görüntü filtresine eklenecektir. Bu, Antispam motorunuzun etkinliğini artıracaktır. Bu güncelleme tipi aynı zamanda **Antispam Güncellemesi** olarak da bilinmektedir.
- **Antispyware motorları güncellemesi** - yeni spyware imzaları 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

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

- Otomatik Güncelleme
- Güncelleme Ayarları

13.1. Otomatik Güncelleme

Güncelleme bilgilerini görmek ve güncellemeleri otomatik yapmak için, ayarlar konsolundan **Güncelle>Güncelle**' yi tıklayın Sıradaki pencere çıkacaktır:



Otomatik Güncelleme

Burada, son güncelleme kontrollerini ve son gerçekleşen güncellemeyi görebilir, ayrıca son güncelleme hakkında bilgi alabilirsiniz (güncelleme başarılı mı, ya da oluşan hatalar). Hem geçerli versiyon numarası hem de imza sayısı görüntülenir.

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.

Eğer bu pencereyi bir güncelleme esnasında açarsanız, yükleme durumunu görebilirsiniz.

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

13.1.1. Güncelleme İsteği

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

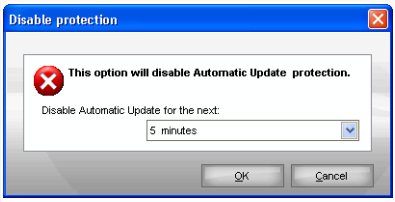
Güncelleme Modülü, BitDefender Güncelleme Sunucusuna bağlanacak ve herhangi bir güncelleme varsa bunu teyit edecektir. Bir güncelleme tespit edildiğinde, Manuel Güncelleme Seçenekleri bölümündeki seçeneklerin ayarlarına bağlı olarak, güncellemeyi teyit etmeniz istenecek veya güncelleme otomatik olarak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

13.1.2. Otomatik Güncellemeyi Kapatma

Otomatik güncellemeyi kapatırsanız, bir uyarı penceresi açılacaktır.



Otomatik Güncellemeyi Kapat

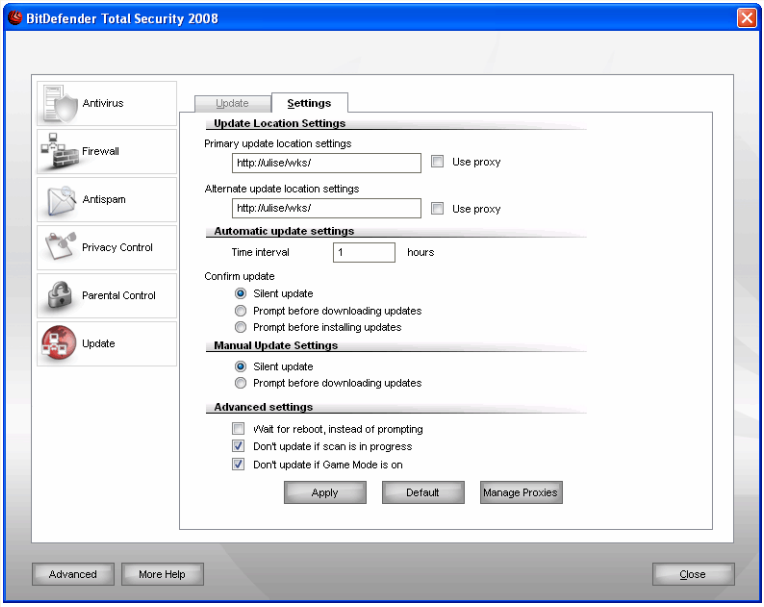
Gerçek zamanlı korumayı ne kadar süre için kapatacağınızı menüden seçerek belirlemelisiniz. Bunu 5, 15, 30, dakika veya 1 saat için, ya da sürekli olarak veya sistem tekrar başlatılana dek kapatabilirsiniz.

Uyarı
Bu kritik bir güvenlik sorunudur. Eğer gerçek zamanlı koruma kapatılırsa tehditlere karşı korumasız kalırsınız, bu nedenle biz bunu kısa süreler için tavsiye ediyoruz.

13.2. Güncelleme Ayarları

Güncellemeler, yerel ağda, internet üzerinden direkt olarak veya Vekil Sunucu üzerinden yapılabilir. Varsayılan olarak, BitDefender, saatbaşı güncelleme yapar, internet üzerinden mevcut güncellemeleri size herhangi bir uyarı yapmadan yükler.

Güncelleme ayarlarını ve vekil sunucuları yapılandırmak için, **Güncelleme>Ayarları'** nı tıklayın. Sıradaki pencere çıkacaktır:



Güncelleme Ayarları

Güncelleme ayarlarının bulunduğu pencere 4 seçenek kategorisi (**Güncelleme Yer Ayarları** , **Otomatik Güncelleme Seçenekleri**, **Manuel Güncelleme Ayarları** ve **Gelişmiş Ayarlar**) içerir. Her kategori ayrı olarak tanımlanacaktır.

13.2.1. Güncelleme Yeri Ayarları

Güncelleme yerini ayarlamak için, **Güncelleme Yeri Ayarları** kategorisindeki seçenekleri kullanın.

Not
Buradaki seçenekleri sadece, bir yerel ağa bağlı iseniz ve bu ağda BitDefender güncellemeleri tutuluyorsa veya internete bir vekil sunucu üzerinden çıkıyorsanız yapılandırabilirsiniz.

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 yerini değiştirmek için, **URL** alanına yerel ağınızdaki yolu yazabilirsiniz.

Not
Biz, öncelikli güncelleme yerine yerel ağınızdaki yolu gösterdiğinizde, herhangi bir şekilde oraya ulaşılamaması durumuna karşı, alternatif güncelleme yerini değiştirmemenizi öneririz.

İnternete bağlanmak için bir vekil sunucu kullanıldığı durumlarda, **Vekil Sunucu Kullan** kutucuğunu işaretleyip, **Vekil Sunucular** tuşuna basarak ayarları yapınız.

Not
Daha fazla bilgi için bakınız,"*Vekil Sunucuları Yönetmek*" (shf. 206)

13.2.2. Otomatik Güncelleme Yapılandırma

BitDefender' ın güncellemeleri otomatik olarak yapmasını istiyorsanız **Otomatik Güncelleme Ayarları**' nı kullanın.

Güncelleme zamanını **Zaman aralığı** alanından belirleyebilirsiniz. Varsayılan olarak 1 saate ayarlanmıştır.

Otomatik güncellemenin nasıl yapılacağını aşağıdaki seçeneklerden belirleyebilirsiniz.

- **Sessiz Güncelleme** - BitDefender güncellemeyi otomatik olarak indirir ve uygular.
- **İndirmeden önce sor** – güncellemenin her bulunuşunda, indirmeden önce sizi uyaracaktır.

Not
Güvenlik Merkezinin dışında olsanız dahi güncelleme indirmeleri yapılacaktır.

- **Yüklemeden önce sor** – güncellemenin her indirilişinde, yüklemeden önce sizi uyaracaktır.

Not
Güvenlik Merkezinin dışında olsanız dahi güncelleme yapılacaktır.

13.2.3. Manuel Güncelleme Yapılandırma

Manuel güncellemenin (kullanıcı isteği ile güncelleme) nasıl yapılacağını belirlemek için, **Manuel Güncelleme Ayarları** kategorisinden bir seçenek seçmelisiniz.

- **Sessiz Güncelleme**manuel güncelleme arka planda otomatik olarak yapılacaktır.
- **İndirmeden önce sor** – güncellemenin her bulunuşunda, indirmeden önce sizi uyaracaktır.

Not
Güvenlik Merkezinin dışında olsanız dahi güncelleme indirmeleri yapılacaktır.

13.2.4. Gelişmiş Ayarları Yapılandırma

BitDefender güncelleme işleminin sizi engellemesine engel olmak için, **Gelişmiş Ayarlar** kategorisindeki seçenekleri yapılandırın.

- **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.

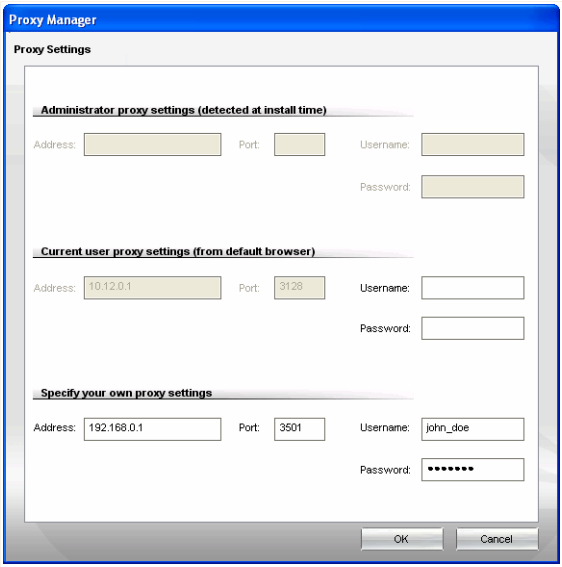
- **Oyun modu açık iken güncelleme yapma** - BitDefender oyun modu açık ise güncelleme yapmayacaktır. Bu yolla, oyun esnasında sistem performansına etkisi en az derecede olur.

13.2.5. Vekil Sunucuları Yönetmek

Eğer internet bağlantısı için vekil sunucu kullanıyorsanız, BitDefender' ın güncellemeleri kendi başına yapabilmesi için vekil sunucu ayarlarını belirlemelisiniz. Aksi taktirde geçerli kullanıcı için yüklü olan tarayıcının, yada yöneticinin ayarlarını kullanacaktır.

Not
Vekil sunucu ayarları sadece yönetici yetkisine sahip kullanıcılar tarafından yapılandırılabilir.

Vekil sunucu ayarlarını yönetmek için, **Vekil Sunucuları Yönet'** i tıklayın. **Vekil Sunucu Yönetimi** diye bir pencere açılacaktır.



Vekil Sunucu Yöneticisi

Vekil sunucu ayarlarında üç adet ayar bulunmaktadır:

- **Yönetici vekil sunucu ayarları (Yükleme esnasında saptanan)** Vekil sunucu ayarları, yükleme sırasında bir yönetici hesabı saptar ve sadece bu hesapla girildiğinde yapılandırılabilir. Eğer vekil sunucunuz için kullanıcı adı ve şifre gerekiyorsa uygun alanlara yazmalısınız.
- **Geçerli kullanıcı vekil sunucu ayarları(from default browser)** - Geçerli kullanıcının vekil sunucu ayarları, varsayılan tarayıcıdan alınır. Eğer vekil sunucunuz için kullanıcı adı ve şifre gerekiyorsa uygun alanlara yazmalısınız.

Not

Dekteklenen web tarayıcılar, Internet Explorer, Mozilla Firefox ve Opera' dır. Eğer varsayılan tarayıcınız başka biri ise, BitDefender geçerli kullanıcının vekil sunucu ayarlarını sağlayamayacaktır.

- **Kendi vekil sunucu ayarlarınız** – yönetici olarak giriş yaptıysanız vekil sunucu ayarlarınızı yapılandırabilirsiniz.

  Aşağıdaki seçenekler mevcuttur:
  - **Adres** – Vekil sunucunun IP adresini yazın.
  - **Port** –BitDefender' ın vekil sunucuya bağlanmak için kullanacağı port numarasını yazın.
  - **Vekil Kullanıcısı** – Vekil tarafından kabul edilen bir kullanıcının ismini girin.
  - **Vekil şifresi** – daha önce tanımlanan kullanıcı için geçerli bir şifre girin.

Internete bağlanmaya çalışıldığında, BitDefender bağlantıyı yönetene kadar her vekil sunucu ayarı çalışacaktır.

İlk önce kendi vekil sunucu ayarlarınız kullanılarak internete bağlanılacaktır. Bağlantı başarısız olursa vekil sunucu ayarları yükleme anında saptadığı ayarlar ile bağlanmayı deneyecektir. Son olarak, bunların hiçbiri çalışmazsa varsayılan tarayıcıdan alınan ayarlar ile internete bağlanılacaktır.

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

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

Gelişmiş Yedekleme Yönetimi

14. Gelişmiş Yedekleme Yönetimi

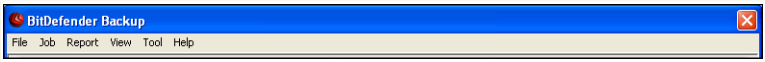
Bu bölümde BitDefender Yedekleme grafik arayüzü hakkında ayrıntılı bir tanıtım bulacaksınız.

Yedekleme ayarlarını yapılandırmaya başlamak için, **Hızlı Görevler** alanından **Yedekleme** tabına tıklayıp, daha sonra **Gelişmiş Ayarlar'** ı tıklayın.

Yedekleme işlemini gerçekleştirebilmek için iki yol seçeneğiniz var. İster üst taraftaki **Menü Çubuğu'** na ister **Yön Bulma Çubuğu'** na tıklayın.

14.1. Menü Çubuğu

Altı adet menü ile, BitDefender' ın sunmuş olduğu yedekleme çözümünün tüm fonksiyonlarını kullanabilirsiniz.



Menü Çubuğu

Dosya

- **Yeni Görev Yarat:** Yeni bir görev yaratmak amacıyla bir iletişim kutusu görüntülenir.
- **Yedek Setini Aç:** Yedek veya katalog setini açmak amacıyla bir iletişim kutusu görüntülenir.
- **Çıkış:** BitDefender yedekleme bölümünden çıkmanızı sağlar.

Görev

- **Yedekleme:** Seçilen görevin yedeklemesini başlatır. Eğer birden fazla görev seçilmişse, tüm seçilen görevler için gerçekleştirir.
- **Dosyaları Geri Yükle:** Seçilen görevi geri yükler. Eğer birden fazla görev seçilmişse, tüm seçilen görevler için gerçekleştirir.
- **Verileri Zaman Noktasına Geri Yükle:** Seçilen görevi belirli bir zaman noktasına geri yükler. Eğer birden fazla görev seçilmişse, tüm seçilen görevler için gerçekleştirir.
- **Zamanlama:** Görev yaratmak ve olanları değiştirmek için zamanlama yapar.
- **Zamanlamayı Sil** Seçilen görevdeki zamanlamayı siler.
- **Sil:** Seçilen görevi siler.Eğer birden fazla görev seçilmişse, tüm seçilen görevler için gerçekleştirir.
- **Hepsini Sil** Görev yöneticideki tüm görevleri siler.

- **Hedefe Gözat:** Seçilen görevin yedekleme hedefini görüntüler.
- **Seçenekleri Değiştir:** Seçilen görevin seçeneklerini değiştirmeyi sağlar.
- **Özellikler:** Seçilen görevin veri kaynağı içeriği, ismi, hedefi ve bunun gibi özelliklerini değiştirmeyi sağlar.

Rapor

- **Raporu Görüntüle:** Eğer seçilen görev güvenlik ayarları ise, bu seçenek görev raporunun içeriğini görüntüler.
- **Farklı Kaydet:** Seçilen içeriğini belirli bir dosyaya kaydeder.
- **Yazdır:** Seçilen raporun içeriğini yazdırır.
- **Tümünü Temizle:** Seçilen raporun içeriğini temizler.
- **Yenile:** Seçilen raporun içeriğini yeniler.

Görünüm

- **Başlat:** Eğer başlangıç penceresi açılmadı ise, bu seçenek onu açar.
- **Görev Yöneticisi:** Eğer görev yöneticisi açılmadı ise, bu seçenek onu açar.
- **Kayıt Görüntüleyici:** Eğer kayıt görüntüleyici açılmadı ise, bu seçenek onu açar.
- **Araç Kutusu:** Eğer araç kutusu açılmadı ise, bu seçenek onu açar.
- **Menü Çubuğunu Görüntüle:** Gizli menü çubuğunu görüntülemek için, **ALT'** a basın.
- **Kılavuz Çizgisi Görüntüle:** Kılavuz çizgileri gizlenir veya görüntülenir. Kayıt görüntüleyici ve görev yöneticisi pencerelerine uygulanır.

Araç

- **Yedekleme Sihirbazı:** Yedekleme sihirbazını başlatır.
- **Geri Yükleme Sihirbazı:** Geri yükleme sihirbazını başlatır.
- **Yak:** CD/DVD/ISO yakma aracını veya yakma yönetim aracını başlatır.
  - **CD/DVD Yak**
  - **ISO Dosyası Yak**
  - **Yakıcı Bilgisi Görüntüle**
- **Tüm Görevleri Dışarı Ver:** Tüm yaratılmış görevler belirli bir dosyaya verilir.
- **Dışarıdan Görev Al:**, `.JOB`, `.TXT` veya `.XML` uzantılı dosyalardan görevler alınabilir.
- **Dışa Verme Kaydı:** Kayıtlar, `.TXT` veya `.XML` uzantılı dosyalar olarak tutulabilir.
  - `TXT` dosyası için
  - `XML` dosyası için
- **Kaydı Dışarıdan Alma:** Kayıtlar, `.TXT` veya `.XML` uzantılı dosyalar olarak tutulabilir.
  - `TXT` dosyası için
  - `XML` dosyası için
- **Seçenekler:** Genel yedekleme seçeneklerini değiştirebilirsiniz.

- **Genel**
- **Raporlar & Kayıt**
- **Görev Zamanlama**

Yardım

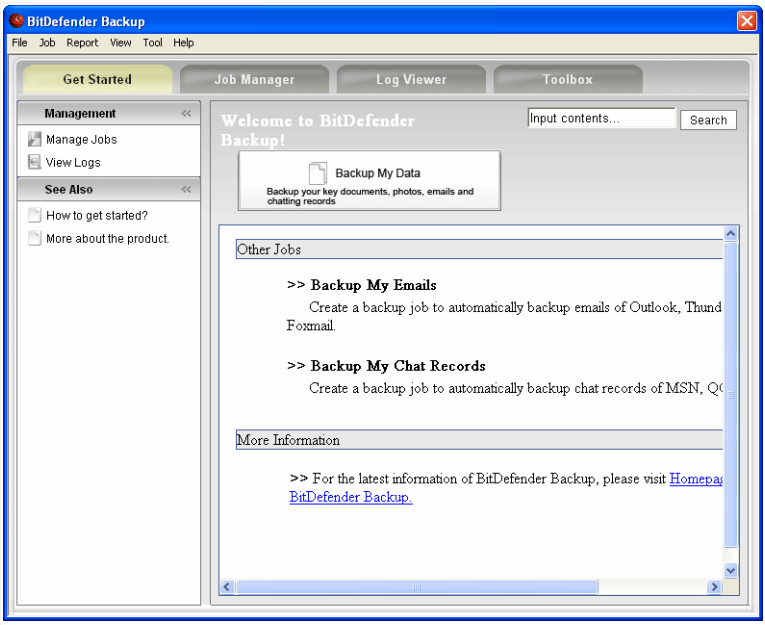
- **Yardım Konuları** Yardım Konularını görüntüler.
- **Arama:** Girmiş olduğunuz kelimeler yardım konuları içinde aranır.
- **BitDefender Websitesi:** BitDefender internet sitesine erişim sağlayarak BitDefender haberlerine ve online desteğe ulaşmanızı sağlar.
- **BitDefender Yedekleme Hakkında:** Bitdefender Yedeklemenin telif hakkı, sürümü, sürüm ile ilgili bilgileri görüntülenir.

14.2. Yön Bulma Çubuğu

Yön Bulma Çubuğu, ana pencerenin üstünde, **Menü Çubuğu'** nun altında görüntülenir, dört bölümden oluşur.

- **Başlangıç**
- **Görev Yöneticisi**
- **Kayıt Görüntüleyici**
- **Araç Kutusu**

14.2.1. Başlangıç



Başlangıç

Başlangıç aşağıdaki şekilde değiştirilebilir:

- **Yön Bulma Çubuğu**' ndaki **Başlangıç**' a tıklayın
- **Menü Çubuğu**' ndaki **Görünüm**' e tıklayın ve **Başlangıç**' ı seçin.
- **CTRL+Alt+S** kısayolunu kullanabilirsiniz.

Önemli dökümanlarınızın, fotoğraflarınızın, e-maillerinizin ve mesaj kayıtlarınızın yedeğini aynı görevde almak için, **Belgelerimi Yedekle** tuşuna basın ve üç adımlık işlemi takip edin.

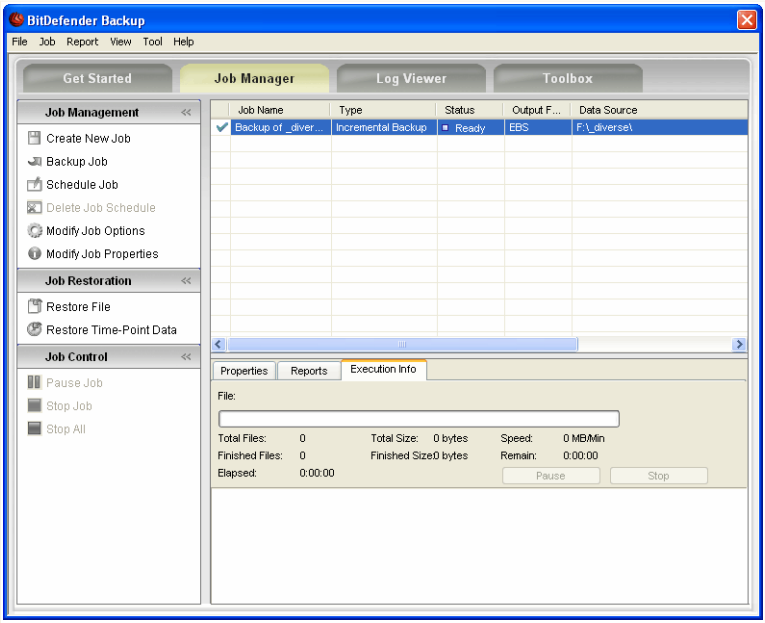
Sadece e-mallerin yedeğini almak için, **E-mailleri Yedekle** tuşuna basın ve üç adımlık işlemi takip edin.

Sadece mesaj kayıtlarının yedeğini almak için, **Mesaj Kayıtlarını Yedekle** tuşuna basın ve üç adımlık işlemi takip edin.

Not
Buradaki üç adımlık işlem, Yeni Görev Yarat bölümünde tanımlanmıştır.

14.2.2. Görev Yöneticisi

Görev Yöneticisi yedekleme görevlerini görüntülemek ve yönetmek için kullanılır, görev özellikleri ve raporları ayrıca görev hızı görüntülenebilir. **Görev Yöneticisi** görev özelliklerini ve geçerli durumu kontrol etmeyi sağlar, yanısıra yedekleme veya geri yükleme görevlerini yerine getirir.



Görev Yöneticisi

Görev Yöneticisi aşağıdaki şekilde değiştirilebilir:

- **Yön Bulma Çubuğu**' ndaki **Görev Yöneticisi**' ne tıklayın
- **Menü Çubuğu**' ndaki **Görünüm**' e tıklayın ve **Görev Yöneticisi**' ni seçin.
- **CTRL+Alt+M** kısayolunu kullanabilirsiniz.

Aşağıda olduğu gibi, sol tarafta hızlı işlem linklerini göreceksiniz

Görev Yönetimi

- **Yeni Görev Yarat**
- **Yedekleme Görevi**
- **Zamanlanmış Görev**
- **Zamanlanmış Görevleri Sil**
- **Görev Seçeneklerini Değiştir**
- **Görev Özelliklerini Değiştir**

Geri Yükleme Görevi

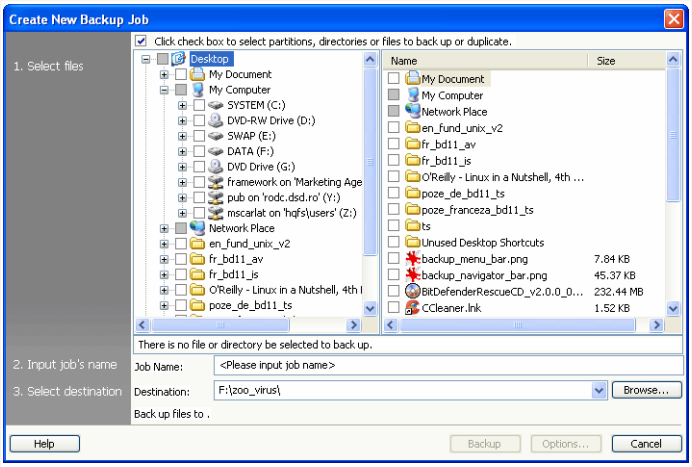
- **Dosya Geri Yükleme**
- **Verileri Zaman Noktasına Geri Yükle**

Görev Kontrolü

- **Görevi Duraklat**
- **Görevi Durdur**
- **Hepsini Durdur**

Yeni bir görev yaratın

Önemli dökümanlarınızın, fotoğraflarınızın, e-maillerinizin ve mesaj kayıtlarınızın yedeğini aynı görevde almak için, **Yeni Görev Yarat** tuşuna basın ve üç adımlık işlemi takip edin.



Yeni bir görev yaratın

1. Yedeklenecek disk bölümünü, dizinleri veya dosyaları seçmek için kutucuğu işaretleyin.

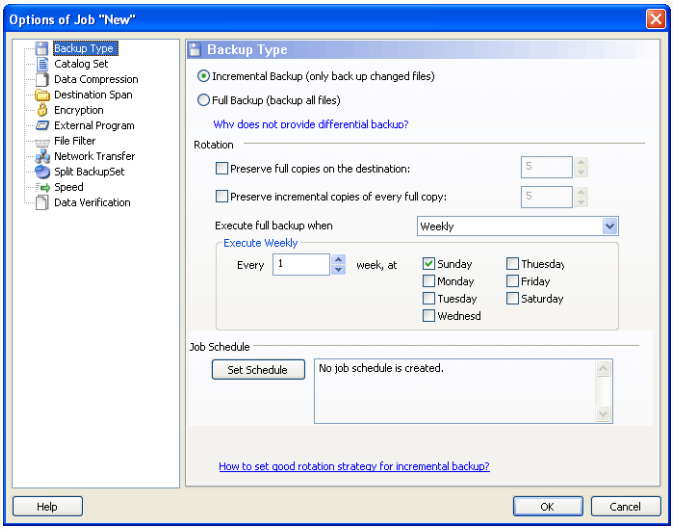
   Daha iyi bir seçim yapmanıza yardımcı olmak için, pencerenin sol tarafındaki öğeleri seçtiğinizde, pencerenin sağ tarafında seçilen öğenin içeriği görüntülenecektir.
2. Yedekleme görevinin adını yazın ya da varsayılan adı kabul edin.

   Varsayılan görev adı, dizin ya da dosyalar seçildiğinde otomatik olarak yaratılır, fakat değiştirilebilir.
3. Yedekleme görevini nereye kaydedeceğini belirlemek için, **Gözat**' a tıklayın.

Not
Başlamak için **Yedekle** veya durdurmak için **İptal**' e tıklamayı unutmayın.
Daha iyi bir seçim yapmak için, **Seçenekler**' e tıklayın.

Yedekleme Seçenekleri İletişim Kutusu

Seçenekler iletişim kutusunda birkaç alt seçenek bulunmaktadır.



Yedekleme Seçenekleri İletişim Kutusu

Yedek Tipi

BitDefender Yedekleme iki tip yedeklemeyi destekler.

- **Tam Yedek:** Belirlenen hedefteki veri kaynaklarının tam bir yedeğini alabilirsiniz. Tam yedek çalıştığında, BitDefender Yedekleme sadece değişen verileri değil, verilerin tümünün yedeğini alır.
- **Artımlı Yedekleme:** Artımlı yedekleme ile ilk seferinde aynı tam yedekde olduğu gibi, belirlenen hedefteki veri kaynaklarının tam bir yedeğini alırsınız. Daha sonra sadece değişen ve yeni yaratılan dosyalar yedeklenir. Artımlı yedekleme çalıştığında bir yedekleme seti yaratılır.

Artımlı ve tam yedek birlikte **Rotasyon Yedek'** i oluşturur. Örneğin, haftada bir gün diyelim ki Pazar günü tam yedek alırken, bir artımlı yedekleme ayarlayabilirsiniz. Nasıl olur: Açılan menüden **Haftalık'** ı seçin, **Her Hafta** bölümünden `1`' i işaretleyin ve Pazar gününü seçin. Bu Pazar tam yedek, eski yedeği değiştirecek ve bunu temel alarak yeni artımlı yedekleme başlayacaktır.

Katalog Seti

Her yedeğin dosya indeks bilgisini kullanır, ve Artımlı Yedekleme ve Geri Yükleme işlemini temel alır. Katalog seti (`*.ecs`) yedek setindeki bütün dosya ve dizinlerin indekslerinin belirtildiği bir seri katalog içerir. İndeks verileri yedekleme zamanı, yedekleme dizini, dosya adı ve özellikleri gibi bilgilerden oluşur. Veri katalog setinden geri yüklenebilir.

Bir katalog seti ismi, görev hedefi yoluyla otomatik olarak yaratılır. Bir görevin katalog setini değiştirmek için aşağıdakileri yapın:

1. **Katalog Seti'** ni tıklayın.
2. Dosya ismini yazın.
3. Katalog Seti dosyalarını kaydedecek dizini seçmek için **Gözat'** a tıklayın.
4. **Tamam**' ı tıklayın.

Veri Sıkıştırma

BitDefender, boş alanı korumak için, yedekleme setinin sıkıştırılarak kaydedilmesini sağlar. Hızlı Sıkıştırma, Standart Sıkıştırma, Yüksek yoğunlukta Sıkıştırma seçeneklerdir. Örneğin Standart Sıkıştırma ile orta dereceli sıkıştırma oranı ve hız için, şu adımları izleyin:

1. **Veri Sıkıştırma'** yı tıklayın.
2. **Standart Sıkıştırma'** yı tıklayın.
3. **Tamam**' ı tıklayın.

Hedef Yayılımı

BitDefender Yedek, yedekleme setlerini farklı hedef sürücülere dağıtmaya izin verir. Bu durumda hedefte yeterli boşluk olmasa bile, yedekleme işlemi devam edecektir.

Yedeklemenin devamı için, bir hedef daha ekleyebilirsiniz, değiştirmek veya silmek için aşağıdaki yolların birini uygulayın:

1. **Hedef Yayılımı'** nı tıklayın.
2. Yedeklenececek verilere yeni bir hedef seçmek için, **Ekle'** yi tıklayın
3. Seçilen yedekleme hedefini değiştirmek için, **Düzenle'** yi tıklayın.
4. Seçilen yedekleme hedefini silmek için, **Sil'** i tıklayın.
5. Tüm yedekleme hedeflerini silmek için, **Hepsini Sil'** i tıklayın.
6. **Tamam**' ı tıklayın.

Şifreleme

BitDefender Yedekleme, yedek setini güvende tutabilmek için kaydetmeden önce onu şifreler. Görevin güvenlik ayarlarında şifreli koruma vardır.

Yedeklemeden önce verileri şifrelemek için, şu adımları izleyin:

1. **Şifreleme'** ye tıklayın.
2. Açılır menüden şifreleme tipini seçin.
3. Uygun alana şifrenizi yazın.
4. Şifrenizi tekrar yazın.
5. **Tamam**' ı tıklayın.

Harici Program

Görev yedeklemeden önce veya sonra diğer komutları da çalıştırabilir. Bu komutlar, `.exe`, `.com` veya `.bat` uzantılı dosyalar olabilir, ya da "yedeklemeden sonra bilgisayarı kapat" gibi belirli olaylar olabilir.

Yedekleme başlangıcında komutları çalıştırmak için bu adımları takip edin:

1. **Harici Program'** ı tıklayın
2. **Görevden Önce** opsiyonunu seçin.
3. Çalıştıracağınız komutu seçmek için **Gözat'** ı tıklayın.
4. **Tamam**' ı tıklayın.

Yedekleme sonunda komutları çalıştırmak için bu adımları takip edin:

1. **Harici Program'** ı tıklayın
2. **Görevden Sonra** opsiyonunu seçin.
3. Çalıştıracağınız komutu seçmek için **Gözat'** ı tıklayın.
4. Veya yedekleme bittiğinde**Bilgisayarı Kapat** opsiyonunu tıklayın.
5. Veya yedekleme bittiğinde**Bilgisayarı Yeniden Başlat** opsiyonunu tıklayın.
6. Veya yedekleme bittiğinde**Geçerli Kullanıcıyı Kapat** opsiyonunu tıklayın.
7. **Tamam**' ı tıklayın.

Not

Eğer işi yedeklemede hata olsa bile yapılandırmak istiyorsanız, **Harici Uygulamayı görevde hata olsa bile çalıştır** kutucuğunu işaretleyin.

Dosya Filtreleme

BitDefender Yedekleme belirli dosya tipleri veya dizinleri hariç tutmak veya dahil etmek, depolanacak alanı korumak ya da yedek hızını arttırmak için güçlü bir filtreleme fonksiyonu sağlar.

Şu adımları izleyerek, belirli dosya tiplerine göre filtreleme yapabilirsiniz:

1. **Dosya Filtreleme**' yi tıklayın.
2. **Filtre Tipi**' ni tıklayın.
3. Hariç tutulacak veya dahil edilecek dosya tiplerini, açılır penceredeki **Sadece seçili dosya tiplerini dahil et** veya **Seçili dosya tiplerini hariç tut** seçeneklerini kullanarak belirleyebilirsiniz.
4. Eğer gerekirse, diğer dosya tiplerini de **Özel Tip** alanına `.abc` formatına uygun olarak yazdığınızdan emin olarak kullanabilirsiniz. Aralarında `,` (virgül) kullanarak daha fazla özel tip belirleyebilirsiniz. Uygun alana kısa açıklamalar ekleyebilirsiniz.
5. **Tamam**' ı tıklayın.

Şu adımları izleyerek, belirli dosyaları filtreleyebilirsiniz:

1. **Dosya Filtreleme**' yi tıklayın.
2. **Dosya Filtreleme**' yi tıklayın.
3. Hariç tutulacak veya dahil edilecek dosyaları, açılır penceredeki **Sadece belirli dosyaları dahil et** veya **Belirli dosyaları hariç tut** seçeneklerini kullanarak belirleyebilirsiniz.
4. **Gözat**' a tıklayın ve dosyayı seçin. Dosya lokasyonunun yolu **Uygulanacak dizinler** sahasına otomatik olarak eklenecektir. Dosyaları lokasyona bakmaksızın hariç tutmak veya dahil etmek için, **Tüm dizinler için uygula**' yı tıklayın.
5. **Tamam**' ı tıklayın.

Şu adımları izleyerek, belirli dizin tiplerine göre filtreleme yapabilirsiniz:

1. **Dosya Filtreleme**' yi tıklayın.
2. **Dizin Filtreleme**' yi tıklayın.
3. Hariç tutulacak veya dahil edilecek dosyaları, açılır penceredeki **Sadece belirli dizinleri dahil et** veya **Belirli dizinleri hariç tut** seçeneklerini kullanarak belirleyebilirsiniz.
4. **Gözat**' a tıklayın ve dizini seçin. Dizin lokasyonunun yolu **Uygulanacak dizinler** sahasına otomatik olarak eklenecektir. Dosyaları lokasyona bakmaksızın hariç tutmak veya dahil etmek için, **Tüm dizinler için uygula**' yı tıklayın.
5. **Tamam**' ı tıklayın.

Şu adımları izleyerek, filtreleri değiştirebilirsiniz:

1. **Dosya Filtreleme**' yi tıklayın.

2. Değiştirmek istediğiniz filtreyi seçin ve, **Düzenle'** ye tıklayın.
3. İletişim kutusunda seçeneklerinizi değiştirin.
4. **Tamam**' ı tıklayın.

Şu adımları izleyerek, filtreleri silebilirsiniz:
1. **Dosya Filtreleme'** yi tıklayın.
2. Silmek istediğiniz filtreyi seçin ve, **Sil'** e tıklayın.
3. Ya da **Hepsini Sil'** e tıklayarak direk olarak tüm dosyaları silin.
4. **Tamam**' ı tıklayın.

Ağ Transferi

BitDefender Yedekleme, paylaşılan veriyi çalışma grubu ağına yedeklemeye ve geri yüklemeye izin verir, ve eğer ağa erişilemiyor ise zaman zaman bunu dener. Yedeklemeyi hangi sıklıkta ve kaç sefer deneyeceğini belirlemek için aşağıdaki adımları izleyin.
1. **Ağ Transferi**' ne tıklayın.
2. **Ağ bağlantısı kesildiğinde, ağ dosyaları okunamadığında, yeniden bağlanmayı dene'** yi tıklayın.
3. Yedeklemeyi hangi sıklıkta denemesini istediğinizi yazın (saniye olarak).
4. Yedeklemeyi kaç sefer denemesini istediğinizi yazın.
5. **Tamam**' ı tıklayın.

Not
Ağ hatası bilgilerinden şaşkına dönmekten kaçınmak için, **Ağ bağlantı hatası raporu üretilmesin'** e tıklayın.

Yedek setini bölmek

Yedekleme hedefi veya dosya sistemi kısıtlı olabileceği için, yedekleme seti yaratılırken bölünmüş olarak yaratılabilir, BitDefender Yedekleme, iki bölme metodu sağlar: oto-bölme ve boyutlu-bölme.

Görevin yedek bölme ayarlarını aşağıdaki şekilde değiştirebilirsiniz.
1. **Yedek setini bölme**' yi tıklayın.
2. **Hedef Boyutuna göre Otomatik Bölme'** yi seçin.
3. Ya da **Parça boyutunu belirleyin'** i seçerek, açılır menüden arzuladığınız boyutu seçin.
4. **Tamam**' ı tıklayın.

Hız

BitDefender Yedekleme üç çeşit hız destekler.

Aşağıdaki adımları izleyerek, yedekleme hızını belirleyebilirsiniz.
1. **Hız**' ı tıklayın.
2. **Hızlı**, **Orta** veya **Düşük** hızı seçin

3. **Tamam**' ı tıklayın.

Veri Doğrulama

Yedek verilerinizin daima sağlam olduğundan emin olmak için, aşağıdaki adımları izleyin.

1. **Veri Doğrulama'** ya tıklayın.
2. **Yedekleme işleminde veriyi doğrula'** ya tıklayın.
3. **Tamam**' ı tıklayın.

Yedekleme Görevi

Görev birkez yaratılınca, yedekleme otomatik olarak gerçekleşir. Bununla birlikte, **Görev Yönetici'** ye girerek, menüdeki **Yedekleme Görevi'** ni tıklayarak seçilen yedeklemeyi çalıştırabilirsiniz.

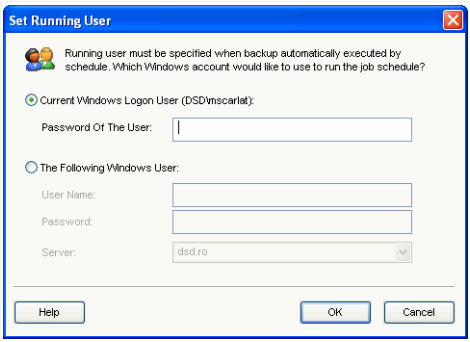
Dosyaları geri yüklerken yedek detaylarını almak için, açılır pencereye kısa açıklamalar yazmalısınız. Açılır pencereyi reddetmek için, **İptal'** e veya devam etmek için, **Tamam'** a tıklayın. Ayrıca, yedekleme görevini **Yedek İptali** butonuna tıklayarak iptal edebilirsiniz.

Not

Ayrıntılı bilgileri, **Özellikler**, **Raporlar** ve **Uygulama Bilgisi** olarak durum çubuğundan görebilirsiniz.

Görev Zamanlayıcı

Görev Zamanlayıcı ile yedekleme görevini elverişli anlarda zamanlayabilirsiniz. Görevleri günlük, haftalık, aylık veya belirlenen anlar (örneğin sistem başlangıcında) olarak zamanlayabilirsiniz. **Görev Zamanlayıcı** otomatik yedeklemeyi temel alır.



Görev Zamanlayıcı

Eğer bilgisayarınız bir etki alanının üyesi ise, görev zamanlama eklemek için bir sıra ekstra adım gerekir.

1. Görevi seçtikten sonra **Görevi Zamanlama'** yı tıklayın.
2. **Çalışan Kullanıcı** iletişim kutusu görünecektir. Eğer bir etki alanı kullanıcısı iseniz lütfen etki alanı şifrenizi girin.
3. Aksi halde **Aşağıdaki Windows kullanıcısı ile çalış'** ı seçin.
4. Kullanıcı adınızı, şifrenizi ve etki alanı sunucu adını yazın.
5. **Tamam**' ı tıklayın.

Çalışan kullanıcı ayarlandığında, **Zamanlayıcı** iletişim kutusu görünecektir, görevin çalışması için elverişli zamanı ayarlayabilirsiniz.

Zamanlanmış görevlerin hangi sıklıkta çalışacağını günlük, haftalık, aylık, bir kereye mahsus, sistem başlangıcında, bilgisayar boşta iken gibi seçeneklerle belirleyebilirsiniz. Eğer görev günlük, haftalık, aylık veya bir kereye mahsus olarak zamanlandı ise, başlangıç zamanını da belirleyebilirsiniz. Ayrıca zamanlanmış görevin ayın veya haftanın hangi günleri çalışacağını da seçebilirsiniz. Diğer bir ayar da zamanlanmış görev başladıktan sonra boşta kalma süresinin (dakika olarak) belirtilebilmesidir.

Ayrıca bir görev için çoklu zamanlama yapmanız da mümkündür, bunun için, **Çoklu zamanlamaları göster'** e tıklayıp, sonra **Gelişmiş'** e tıklayın, ilave zamanlama seçeneklerini ayarlayabilirsiniz. Örneğin, görev başlangıç ve bitiş tarihini tanımlayabilirsiniz.

İyileştirilmiş bir görev zamanlaması için, **Ayarlar** sekmesine tıklayın. Üç alt seçenek vardır.

- **Zamanlanmış Görev Tamamlandı**
  - Eğer zamanlama tekrar çalışmayacaksa, görevi silin.

    Bu görev zamanlayıcının bir kereye mahsus çalışması için kullanışlıdır.
  - Görevi durdur

    Görev başladıktan ne kadar zaman sonra durdurulması gerektiğini belirtir.
- **Boşta Kalma Zamanı**
  - Görev sadece, eğer bilgisayar boşta ise başlasın:

    Görev başlamadan önce (dakika olarak) fare ve klavyesiz ne kadar zaman geçireceğini belirtir.
  - Eğer bilgisayar uzun süredir boşta kalmamış ise, tekrar dene.

    Bilgisayar boşta iken, (dakika olarak) görevin kadar zaman kullanacağını belirtir.
  - Bilgisayarın boşta olma durumu sona erdiyse görevi durdur.

    Görev çalışıyorken, bilgisayarı kullanmaya başlarsanız, görevin durdurulması gerektiğini belirtir.
- **Güç Yönetimi**
  - Bilgisayar bataryadan çalışıyorsa görevi başlatma.

    Bilgisayarınız bataryadan çalışıyorsa, görev engellenecektir. Bu kutucuğu işaretleyerek, bataryanızın ömrünü uzatabilirsiniz.
  - Batarya modu devreye girerse görevi durdur.

    Bilgisayarınız bataryadan çalışmaya başladığında görevin durdurulmuş olması gerektiğini belirtir.
  - Görevin çalışması için bilgisayarı çalıştır.

    Bilgisayar uyku modundayken dahi, zamanlanmış görevin çalışıyor olduğunu belirtir.

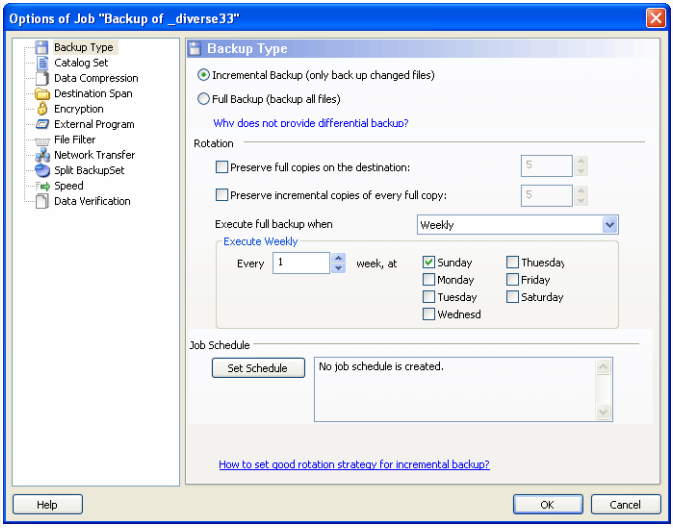
Zamanlanmış Görevi Sil

Görevi silmek için seçin ve, **Görev Yönetimi** bölümünden **Zamanlanmış Görevi Sil'** i tıklayın.

Eğer görev zamanlanmadıysa, **Zamanlanmış Görevi Sil** gri olarak görünecektir, bunun anlamı kullanılamaz olduğudur.

Görev Seçeneklerini Değiştir

Görev seçeneklerini değiştirmek için, görevi seçin ve **Görev Yönetimi** bölümünden **Görev Seçeneklerini Değiştir'** i tıklayın.

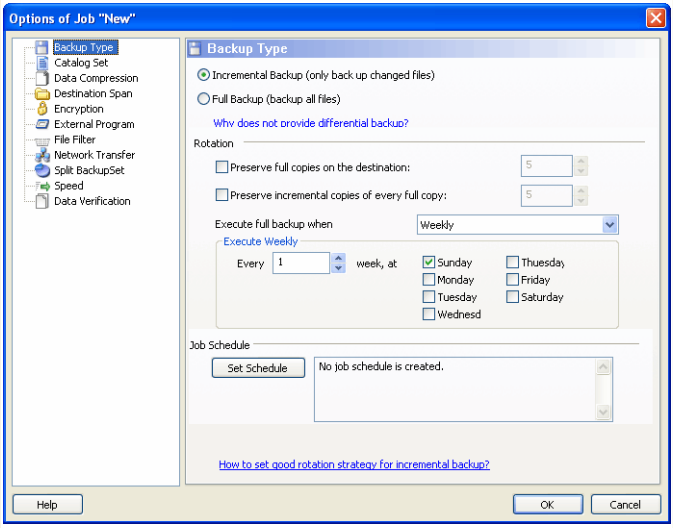


Görev Seçeneklerini Değiştir

Seçilen görev bir yedekleme veya yakma görevi olabilir.

Yedekleme Seçenekleri İletişim Kutusu

Seçenekler iletişim kutusunda birkaç alt seçenek bulunmaktadır.



Yedekleme Seçenekleri İletişim Kutusu

Yedek Tipi

BitDefender Yedekleme iki tip yedeklemeyi destekler.

- **Tam Yedek:** Belirlenen hedefteki veri kaynaklarının tam bir yedeğini alabilirsiniz. Tam yedek çalıştığında, BitDefender Yedekleme sadece değişen verileri değil, verilerin tümünün yedeğini alır.
- **Artımlı Yedekleme:** Artımlı yedekleme ile ilk seferinde aynı tam yedekde olduğu gibi, belirlenen hedefteki veri kaynaklarının tam bir yedeğini alırsınız. Daha sonra sadece değişen ve yeni yaratılan dosyalar yedeklenir. Artımlı yedekleme çalıştığında bir yedekleme seti yaratılır.

Artımlı ve tam yedek birlikte **Rotasyon Yedek**' i oluşturur. Örneğin, haftada bir gün diyelim ki Pazar günü tam yedek alırken, bir artımlı yedekleme ayarlayabilirsiniz. Nasıl olur: Açılan menüden **Haftalık**' ı seçin, **Her Hafta** bölümünden `1`' i işaretleyin ve Pazar gününü seçin. Bu Pazar tam yedek, eski yedeği değiştirecek ve bunu temel alarak yeni artımlı yedekleme başlayacaktır.

Katalog Seti

Her yedeğin dosya indeks bilgisini kullanır, ve Artımlı Yedekleme ve Geri Yükleme işlemini temel alır. Katalog seti (`*.ecs`) yedek setindeki bütün dosya ve dizinlerin indekslerinin belirtildiği bir seri katalog içerir. İndeks verileri yedekleme zamanı,

yedekleme dizini, dosya adı ve özellikleri gibi bilgilerden oluşur. Veri katalog setinden geri yüklenebilir.

Bir katalog seti ismi, görev hedefi yoluyla otomatik olarak yaratılır. Bir görevin katalog setini değiştirmek için aşağıdakileri yapın:

1. **Katalog Seti'** ni tıklayın.
2. Dosya ismini yazın.
3. Katalog Seti dosyalarını kaydedecek dizini seçmek için **Gözat'** a tıklayın.
4. **Tamam**' ı tıklayın.

Veri Sıkıştırma

BitDefender, boş alanı korumak için, yedekleme setinin sıkıştırılarak kaydedilmesini sağlar. Hızlı Sıkıştırma, Standart Sıkıştırma, Yüksek yoğunlukta Sıkıştırma seçeneklerdir. Örneğin Standart Sıkıştırma ile orta dereceli sıkıştırma oranı ve hız için, şu adımları izleyin:

1. **Veri Sıkıştırma'** yı tıklayın.
2. **Standart Sıkıştırma'** yı tıklayın.
3. **Tamam**' ı tıklayın.

Hedef Yayılımı

BitDefender Yedek, yedekleme setlerini farklı hedef sürücülere dağıtmaya izin verir. Bu durumda hedefte yeterli boşluk olmasa bile, yedekleme işlemi devam edecektir.

Yedeklemenin devamı için, bir hedef daha ekleyebilirsiniz, değiştirmek veya silmek için aşağıdaki yolların birini uygulayın:

1. **Hedef Yayılımı'** nı tıklayın.
2. Yedeklenecek verilere yeni bir hedef seçmek için, **Ekle'** yi tıklayın
3. Seçilen yedekleme hedefini değiştirmek için, **Düzenle'** yi tıklayın.
4. Seçilen yedekleme hedefini silmek için, **Sil'** i tıklayın.
5. Tüm yedekleme hedeflerini silmek için, **Hepsini Sil'** i tıklayın.
6. **Tamam**' ı tıklayın.

Şifreleme

BitDefender Yedekleme, yedek setini güvende tutabilmek için kaydetmeden önce onu şifreler. Görevin güvenlik ayarlarında şifreli koruma vardır.

Yedeklemeden önce verileri şifrelemek için, şu adımları izleyin:

1. **Şifreleme'** ye tıklayın.
2. Açılır menüden şifreleme tipini seçin.
3. Uygun alana şifrenizi yazın.
4. Şifrenizi tekrar yazın.
5. **Tamam**' ı tıklayın.

Harici Program

Görev yedeklemeden önce veya sonra diğer komutları da çalıştırabilir. Bu komutlar, `.exe`, `.com` veya `.bat` uzantılı dosyalar olabilir, ya da "yedeklemeden sonra bilgisayarı kapat" gibi belirli olaylar olabilir.

Yedekleme başlangıcında komutları çalıştırmak için bu adımları takip edin:
1. **Harici Program'** ı tıklayın
2. **Görevden Önce** opsiyonunu seçin.
3. Çalıştıracağınız komutu seçmek için **Gözat'** ı tıklayın.
4. **Tamam**' ı tıklayın.

Yedekleme sonunda komutları çalıştırmak için bu adımları takip edin:
1. **Harici Program'** ı tıklayın
2. **Görevden Sonra** opsiyonunu seçin.
3. Çalıştıracağınız komutu seçmek için **Gözat'** ı tıklayın.
4. Veya yedekleme bittiğinde**Bilgisayarı Kapat** opsiyonunu tıklayın.
5. Veya yedekleme bittiğinde**Bilgisayarı Yeniden Başlat** opsiyonunu tıklayın.
6. Veya yedekleme bittiğinde**Geçerli Kullanıcıyı Kapat** opsiyonunu tıklayın.
7. **Tamam**' ı tıklayın.

Not

Eğer işi yedeklemede hata olsa bile yapılandırmak istiyorsanız, **Harici Uygulamayı görevde hata olsa bile çalıştır** kutucuğunu işaretleyin.

Dosya Filtreleme

BitDefender Yedekleme belirli dosya tipleri veya dizinleri hariç tutmak veya dahil etmek, depolanacak alanı korumak ya da yedek hızını arttırmak için güçlü bir filtreleme fonksiyonu sağlar.

Şu adımları izleyerek, belirli dosya tiplerine göre filtreleme yapabilirsiniz:
1. **Dosya Filtreleme'** yi tıklayın.
2. **Filtre Tipi'** ni tıklayın.
3. Hariç tutulacak veya dahil edilecek dosya tiplerini, açılır penceredeki **Sadece seçili dosya tiplerini dahil et** veya **Seçili dosya tiplerini hariç tut** seçeneklerini kullanarak belirleyebilirsiniz.
4. Eğer gerekirse, diğer dosya tiplerini de **Özel Tip** alanına `.abc` formatına uygun olarak yazdığınızdan emin olarak kullanabilirsiniz. Aralarında `,` (virgül) kullanarak daha fazla özel tip belirleyebilirsiniz. Uygun alana kısa açıklamalar ekleyebilirsiniz.
5. **Tamam**' ı tıklayın.

Şu adımları izleyerek, belirli dosyaları filtreleyebilirsiniz:
1. **Dosya Filtreleme'** yi tıklayın.

2. **Dosya Filtreleme'** yi tıklayın.
3. Hariç tutulacak veya dahil edilecek dosyaları, açılır penceredeki **Sadece belirli dosyaları dahil et** veya **Belirli dosyaları hariç tut** seçeneklerini kullanarak belirleyebilirsiniz.
4. **Gözat'** a tıklayın ve dosyayı seçin. Dosya lokasyonunun yolu **Uygulanacak dizinler** sahasına otomatik olarak eklenecektir. Dosyaları lokasyona bakmaksızın hariç tutmak veya dahil etmek için, **Tüm dizinler için uygula'** yı tıklayın.
5. **Tamam**' ı tıklayın.

Şu adımları izleyerek, belirli dizin tiplerine göre filtreleme yapabilirsiniz:

1. **Dosya Filtreleme'** yi tıklayın.
2. **Dizin Filtreleme'** yi tıklayın.
3. Hariç tutulacak veya dahil edilecek dosyaları, açılır penceredeki **Sadece belirli dizinleri dahil et** veya **Belirli dizinleri hariç tut** seçeneklerini kullanarak belirleyebilirsiniz.
4. **Gözat'** a tıklayın ve dizini seçin. Dizin lokasyonunun yolu **Uygulanacak dizinler** sahasına otomatik olarak eklenecektir. Dosyaları lokasyona bakmaksızın hariç tutmak veya dahil etmek için, **Tüm dizinler için uygula'** yı tıklayın.
5. **Tamam**' ı tıklayın.

Şu adımları izleyerek, filtreleri değiştirebilirsiniz:

1. **Dosya Filtreleme'** yi tıklayın.
2. Değiştirmek istediğiniz filtreyi seçin ve, **Düzenle'** ye tıklayın.
3. İletişim kutusunda seçeneklerinizi değiştirin.
4. **Tamam**' ı tıklayın.

Şu adımları izleyerek, filtreleri silebilirsiniz:

1. **Dosya Filtreleme'** yi tıklayın.
2. Silmek istediğiniz filtreyi seçin ve, **Sil'** e tıklayın.
3. Ya da **Hepsini Sil'** e tıklayarak direk olarak tüm dosyaları silin.
4. **Tamam**' ı tıklayın.

Ağ Transferi

BitDefender Yedekleme, paylaşılan veriyi çalışma grubu ağına yedeklemeye ve geri yüklemeye izin verir, ve eğer ağa erişilemiyor ise zaman zaman bunu dener. Yedeklemeyi hangi sıklıkta ve kaç sefer deneyeceğini belirlemek için aşağıdaki adımları izleyin.

1. **Ağ Transferi**' ne tıklayın.
2. **Ağ bağlantısı kesildiğinde, ağ dosyaları okunamadığında, yeniden bağlanmayı dene'** yi tıklayın.
3. Yedeklemeyi hangi sıklıkta denemesini istediğinizi yazın (saniye olarak).
4. Yedeklemeyi kaç sefer denemesini istediğinizi yazın.

5. **Tamam**' ı tıklayın.

Not

Ağ hatası bilgilerinden şaşkına dönmekten kaçınmak için, **Ağ bağlantı hatası raporu üretilmesin**' e tıklayın.

Yedek setini bölmek

Yedekleme hedefi veya dosya sistemi kısıtlı olabileceği için, yedekleme seti yaratılırken bölünmüş olarak yaratılabilir, BitDefender Yedekleme, iki bölme metodu sağlar: oto-bölme ve boyutlu-bölme.

Görevin yedek bölme ayarlarını aşağıdaki şekilde değiştirebilirsiniz.

1. **Yedek setini bölme**' yi tıklayın.
2. **Hedef Boyutuna göre Otomatik Bölme**' yi seçin.
3. Ya da **Parça boyutunu belirleyin**' i seçerek, açılır menüden arzuladığınız boyutu seçin.
4. **Tamam**' ı tıklayın.

Hız

BitDefender Yedekleme üç çeşit hız destekler.

Aşağıdaki adımları izleyerek, yedekleme hızını belirleyebilirsiniz.

1. **Hız**' ı tıklayın.
2. **Hızlı**, **Orta** veya **Düşük** hızı seçin
3. **Tamam**' ı tıklayın.

Veri Doğrulama

Yedek verilerinizin daima sağlam olduğundan emin olmak için, aşağıdaki adımları izleyin.

1. **Veri Doğrulama**' ya tıklayın.
2. **Yedekleme işleminde veriyi doğrula**' ya tıklayın.
3. **Tamam**' ı tıklayın.

Yakma Görevi Seçeneklerini Değiştir

Yakma görevi diyalog kutusunda çeşitli alt seçenekler bulunur.

Yak

Disk yakma işleminden sonra diski kapatmayı seçebilir veya Joliet dosya sistemini kullanarak yazdırabilirsiniz.

Eğer görevi zamanlamak istiyorsanız,**Zamanlama Ayarla**' yı tıklayınız.

Görev Zamanlayıcı ile yedekleme görevini elverişli anlarda zamanlayabilirsiniz. Görevleri günlük, haftalık, aylık veya belirlenen anlar (örneğin sistem

başlangıcında) olarak zamanlayabilirsiniz. **Görev Zamanlayıcı** otomatik yedeklemeyi temel alır.

Eğer bilgisayarınız bir etki alanının üyesi ise, görev zamanlama eklemek için bir sıra ekstra adım gerekir.

1. Görevi seçtikten sonra **Görevi Zamanlama'** yı tıklayın.
2. **Çalışan Kullanıcı** iletişim kutusu görünecektir. Eğer bir etki alanı kullanıcısı iseniz lütfen etki alanı şifrenizi girin.
3. Aksi halde **Aşağıdaki Windows kullanıcısı ile çalış'** ı seçin.
4. Kullanıcı adınızı, şifrenizi ve etki alanı sunucu adını yazın.
5. **Tamam**' ı tıklayın.

Çalışan kullanıcı ayarlandığında, **Zamanlayıcı** iletişim kutusu görünecektir, görevin çalışması için elverişli zamanı ayarlayabilirsiniz.

Zamanlanmış görevlerin hangi sıklıkta çalışacağını günlük, haftalık, aylık, bir kereye mahsus, sistem başlangıcında, bilgisayar boşta iken gibi seçeneklerle belirleyebilirsiniz. Eğer görev günlük, haftalık, aylık veya bir kereye mahsus olarak zamanlandı ise, başlangıç zamanını da belirleyebilirsiniz. Ayrıca zamanlanmış görevin ayın veya haftanın hangi günleri çalışacağını da seçebilirsiniz. Diğer bir ayar da zamanlanmış görev başladıktan sonra boşta kalma süresinin (dakika olarak) belirtilebilmesidir.

Ayrıca bir görev için çoklu zamanlama yapmanız da mümkündür, bunun için, **Çoklu zamanlamaları göster'** e tıklayıp, sonra **Gelişmiş'** e tıklayın, ilave zamanlama seçeneklerini ayarlayabilirsiniz. Örneğin, görev başlangıç ve bitiş tarihini tanımlayabilirsiniz.

İyileştirilmiş bir görev zamanlaması için, **Ayarlar** sekmesine tıklayın. Üç alt seçenek vardır.

- **Zamanlanmış Görev Tamamlandı**
  - Eğer zamanlama tekrar çalışmayacaksa, görevi silin.

    Bu görev zamanlayıcının bir kereye mahsus çalışması için kullanışlıdır.
  - Görevi durdur

    Görev başladıktan ne kadar zaman sonra durdurulması gerektiğini belirtir.
- **Boşta Kalma Zamanı**
  - Görev sadece, eğer bilgisayar boşta ise başlasın:

    Görev başlamadan önce (dakika olarak) fare ve klavyesiz ne kadar zaman geçireceğini belirtir.
  - Eğer bilgisayar uzun süredir boşta kalmamış ise, tekrar dene.

Bilgisayar boşta iken, (dakika olarak) görevin kadar zaman kullanacağını belirtir.

- Bilgisayarın boşta olma durumu sona erdiyse görevi durdur.

  Görev çalışıyorken, bilgisayarı kullanmaya başlarsanız, görevin durdurulması gerektiğini belirtir.

■ **Güç Yönetimi**

- Bilgisayar bataryadan çalışıyorsa görevi başlatma.

  Bilgisayarınız bataryadan çalışıyorsa, görev engellenecektir. Bu kutucuğu işaretleyerek, bataryanızın ömrünü uzatabilirsiniz.

- Batarya modu devreye girerse görevi durdur.

  Bilgisayarınız bataryadan çalışmaya başladığında görevin durdurulmuş olması gerektiğini belirtir.

- Görevin çalışması için bilgisayarı çalıştır.

  Bilgisayar uyku modundayken dahi, zamanlanmış görevin çalışıyor olduğunu belirtir.

Harici Program

Görev yedeklemeden önce veya sonra diğer komutları da çalıştırabilir. Bu komutlar, `.exe`, `.com` veya `.bat` uzantılı dosyalar olabilir, ya da "yedeklemeden sonra bilgisayarı kapat" gibi belirli olaylar olabilir.

Yedekleme başlangıcında komutları çalıştırmak için bu adımları takip edin:

1. **Harici Program'** ı tıklayın
2. **Görevden Önce** opsiyonunu seçin.
3. Çalıştıracağınız komutu seçmek için **Gözat'** ı tıklayın.
4. **Tamam**' ı tıklayın.

Yedekleme sonunda komutları çalıştırmak için bu adımları takip edin:

1. **Harici Program'** ı tıklayın
2. **Görevden Sonra** opsiyonunu seçin.
3. Çalıştıracağınız komutu seçmek için **Gözat'** ı tıklayın.
4. Veya yedekleme bittiğinde**Bilgisayarı Kapat** opsiyonunu tıklayın.
5. Veya yedekleme bittiğinde**Bilgisayarı Yeniden Başlat** opsiyonunu tıklayın.
6. Veya yedekleme bittiğinde**Geçerli Kullanıcıyı Kapat** opsiyonunu tıklayın.
7. **Tamam**' ı tıklayın.

Not

Eğer işi yedeklemede hata olsa bile yapılandırmak istiyorsanız, **Harici Uygulamayı görevde hata olsa bile çalıştır** kutucuğunu işaretleyin.

Dosya Filtreleme

BitDefender Yedekleme belirli dosya tipleri veya dizinleri hariç tutmak veya dahil etmek, depolanacak alanı korumak ya da yedek hızını arttırmak için güçlü bir filtreleme fonksiyonu sağlar.

Şu adımları izleyerek, belirli dosya tiplerine göre filtreleme yapabilirsiniz:

1. **Dosya Filtreleme'** yi tıklayın.
2. **Filtre Tipi'** ni tıklayın.
3. Hariç tutulacak veya dahil edilecek dosya tiplerini, açılır penceredeki **Sadece seçili dosya tiplerini dahil et** veya **Seçili dosya tiplerini hariç tut** seçeneklerini kullanarak belirleyebilirsiniz.
4. Eğer gerekirse, diğer dosya tiplerini de **Özel Tip** alanına `.abc` formatına uygun olarak yazdığınızdan emin olarak kullanabilirsiniz. Aralarında `,` (virgül) kullanarak daha fazla özel tip belirleyebilirsiniz. Uygun alana kısa açıklamalar ekleyebilirsiniz.
5. **Tamam**' ı tıklayın.

Şu adımları izleyerek, belirli dosyaları filtreleyebilirsiniz:

1. **Dosya Filtreleme'** yi tıklayın.
2. **Dosya Filtreleme'** yi tıklayın.
3. Hariç tutulacak veya dahil edilecek dosyaları, açılır penceredeki **Sadece belirli dosyaları dahil et** veya **Belirli dosyaları hariç tut** seçeneklerini kullanarak belirleyebilirsiniz.
4. **Gözat'** a tıklayın ve dosyayı seçin. Dosya lokasyonunun yolu **Uygulanacak dizinler** sahasına otomatik olarak eklenecektir. Dosyaları lokasyona bakmaksızın hariç tutmak veya dahil etmek için, **Tüm dizinler için uygula'** yı tıklayın.
5. **Tamam**' ı tıklayın.

Şu adımları izleyerek, belirli dizin tiplerine göre filtreleme yapabilirsiniz:

1. **Dosya Filtreleme'** yi tıklayın.
2. **Dizin Filtreleme'** yi tıklayın.
3. Hariç tutulacak veya dahil edilecek dosyaları, açılır penceredeki **Sadece belirli dizinleri dahil et** veya **Belirli dizinleri hariç tut** seçeneklerini kullanarak belirleyebilirsiniz.
4. **Gözat'** a tıklayın ve dizini seçin. Dizin lokasyonunun yolu **Uygulanacak dizinler** sahasına otomatik olarak eklenecektir. Dosyaları lokasyona bakmaksızın hariç tutmak veya dahil etmek için, **Tüm dizinler için uygula'** yı tıklayın.
5. **Tamam**' ı tıklayın.

Şu adımları izleyerek, filtreleri değiştirebilirsiniz:

1. **Dosya Filtreleme'** yi tıklayın.

2. Değiştirmek istediğiniz filtreyi seçin ve, **Düzenle**' ye tıklayın.
3. İletişim kutusunda seçeneklerinizi değiştirin.
4. **Tamam**' ı tıklayın.

Şu adımları izleyerek, filtreleri silebilirsiniz:

1. **Dosya Filtreleme**' yi tıklayın.
2. Silmek istediğiniz filtreyi seçin ve, **Sil**' e tıklayın.
3. Ya da **Hepsini Sil**' e tıklayarak direk olarak tüm dosyaları silin.
4. **Tamam**' ı tıklayın.

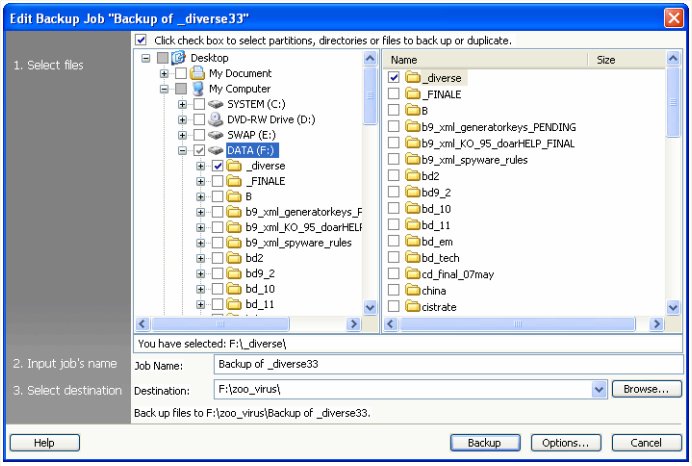
Veri Doğrulama

Yedek verilerinizin daima sağlam olduğundan emin olmak için, aşağıdaki adımları izleyin.

1. **Veri Doğrulama**' ya tıklayın.
2. **Yedekleme işleminde veriyi doğrula**' ya tıklayın.
3. **Tamam**' ı tıklayın.

Görev Özelliklerini Düzenle

Görev özelliklerini düzenlemek için, ilgili görevi seçin ve **Görev Yönetimi** bölümünden **Görev Özelliklerini Düzenle**' yi tıklayın



Görev Özelliklerini Düzenle

1. Yedeklenecek disk bölümünü, dizinleri veya dosyaları seçmek için kutucuğu işaretleyin.

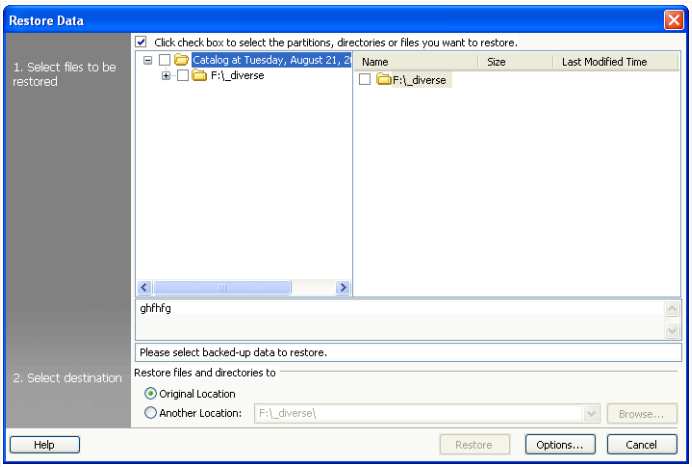
   Daha iyi bir seçim yapmanıza yardımcı olmak için, pencerenin sol tarafındaki öğeleri seçtiğinizde, pencerenin sağ tarafında seçilen öğenin içeriği görüntülenecektir.
2. Yedekleme görevinin adını yazın ya da varsayılan adı kabul edin.

   Varsayılan görev adı, dizin ya da dosyalar seçildiğinde otomatik olarak yaratılır, fakat değiştirilebilir.
3. Yedekleme görevini nereye kaydedeceğini belirlemek için, **Gözat**' a tıklayın.

Not
Başlamak için **Yedekle** veya durdurmak için **İptal**' e tıklamayı unutmayın.
Daha iyi bir seçim yapmak için, **Seçenekler**' e tıklayın.

Dosya Geri Yükleme

Yedeklenmiş veriyi geri yüklemek için, geri yüklemek istediğiniz veriyi seçin ve **Görev Yönetimi** bölümünden **Dosya Geri Yükleme**' yi tıklayın



Dosya Geri Yükleme

1. Kutucuğu işaretleyerek seçtiğiniz disk bölümleri, dizinler veya dosyalar geri yüklenecektir.

Daha iyi bir seçime yardımcı olmak için, pencerenin sol tarafındaki öğelerden birini seçtiğinizde, pencerenin sağ tarafında içeriği görüntülenir.

2. **Geri Yükleme Lokasyonu Seç** penceresinde, herhangi bir değişiklik yapmadan orjinal lokasyonu seçebilir, veya geri yükleme için farklı bir lokasyon belirleyebilirsiniz.

   Yedekleme görevini nereye kaydedeceğini belirlemek için, **Gözat'** a tıklayın.

Not

Geri yüklemeye başlamak için, **Geri Yükle** veya durdurmak için, **İptal'** e tıklamayı unutmayın.
Daha iyi bir seçim yapmak için, **Seçenekler'** e tıklayın.

Geri Yükleme Seçenekleri İletişim Kutusu

Geri yükleme seçenekleri, dosyaların geri yükleme zamanında ve hedefinde halihazırda geri yüklenmiş olup olmadığının belirlenmesine, ve eğer geri yüklenmişse her dosyanın güncellenmesine ve değiştirilmesine olanak tanır.

Geri yükleme esnasında halihazırda var olan dosyalar

- **Dosya atla** BitDefender var olan dosyaları atlar.
- **Kullanıcıya Sor** BitDefender var olan dosyaları yenisi ile değiştirmek için size sorar.
- **Yenisi ile Değiştir** BitDefender var olan dosyaları sormadan yenisi ile değiştirir.
- **Eskileri Değiştir** BitDefender sadece eski olan dosyaları yenisi ile değiştirir. Eski dosyalar değiştirilme tarihi baz alınarak saptanır.

Dosya Değiştirilme Tarihi

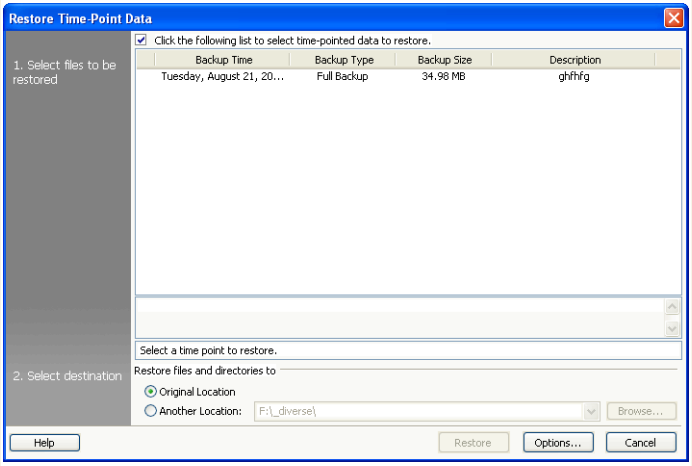
Eğer opsiyon seçilmiş ise, BitDefender dosyaları ve dizinleri geri yüklerken günün tarihini kullanır. Opsiyon seçilmemiş ise, BitDefender yedek alınma tarihini kullanır.

Dizin Yapısı

Sadece geri yükleme için farklı bir lokasyon seçildiğinde etkinleşir. Ayrıca verilerinizin dizin yapısını korumuş olursunuz.

Zaman Noktasına Geri Yükle

Yedeklediğiniz verileri belirli bir zaman noktasına geri yüklemek için, geri yüklenecek verilerden istediğiniz görevi seçin, **Geri Yükleme Görevi** menüsündeki **Zaman Noktasına Geri Yükle'** yi tıklayın takip eden adımları izleyin.



Zaman Noktasına Geri Yükle

1. Yedek setini belirtilen zaman noktası listesinden seçin. İşaretlenenler altta görünecektir.
2. **Geri Yükleme Lokasyonu Seç** penceresinde, bir değişiklik yapmadan orjinal lokasyonu kullanabilir veya başka bir lokasyon belirleyebilirsiniz.

   Yedekleme görevini nereye kaydedeceğini belirlemek için, **Gözat'** a tıklayın.

> ***Not***
> Geri yüklemeye başlamak için, **Geri Yükle** veya durdurmak için, **İptal'** e tıklamayı unutmayın.
> Daha iyi bir seçim yapmak için, **Seçenekler'** e tıklayın.

Geri Yükleme Seçenekleri İletişim Kutusu

Geri yükleme seçenekleri, dosyaların geri yükleme zamanında ve hedefinde halihazırda geri yüklenmiş olup olmadığının belirlenmesine, ve eğer geri yüklenmişse her dosyanın güncellenmesine ve değiştirilmesine olanak tanır.

Geri yükleme esnasında halihazırda var olan dosyalar

- **Eskileri Değiştir** BitDefender sadece eski olan dosyaları yenisi ile değiştirir. Eski dosyalar değiştirilme tarihi baz alınarak saptanır.

Dosya Değiştirilme Tarihi
Eğer opsiyon seçilmiş ise, BitDefender dosyaları ve dizinleri geri yüklerken günün tarihini kullanır. Opsiyon seçilmemiş ise, BitDefender yedek alınma tarihini kullanır.

Dizin Yapısı
Sadece geri yükleme için farklı bir lokasyon seçildiğinde etkinleşir. Ayrıca verilerinizin dizin yapısını korumuş olursunuz.

Görev Kontrolü

Bir göreve ait üç yol gözlemlenir: görevi duraklat, görevi durdur ve hepsini durdur.

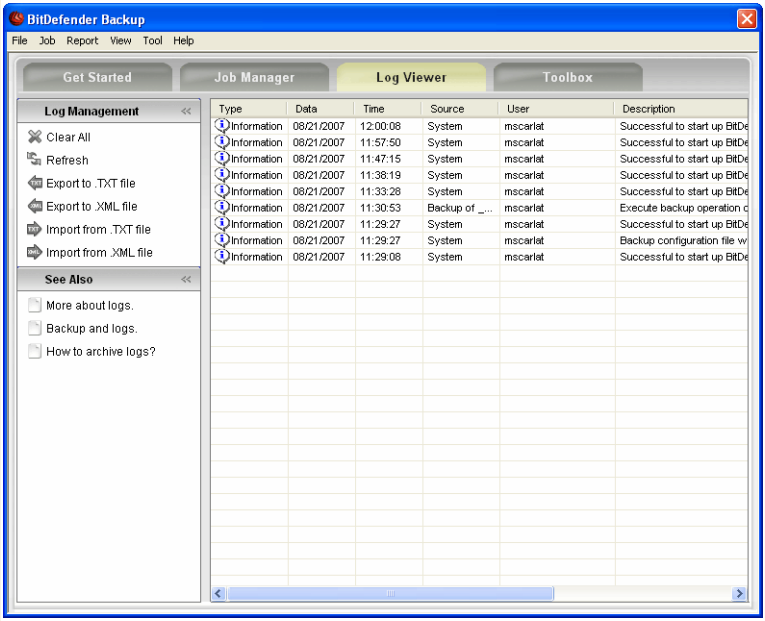
Duraklat
Devam eden yedekleme veya geri yükleme görevini duraklatmak için, **Görev Kontrolü** menüsünden **Duraklat'** a tıklayın.

Durdur
Devam eden yedekleme veya geri yükleme görevini durdurmak için, **Görev Kontrolü** menüsünden **Durdur'** a tıklayın.

Hepsini Durdur
Eğer birden fazla çalışan görev varsa, bunları teker teker kapatmanıza gerek yok. **Görev Kontrolü** menüsünden **Hepsini Durdur'** a tıklayın, tüm görevler durdurulur.

14.2.3. Kayıt Görüntüleyici

Bu bölüm, dışarıya verilen, dışarıdan alınan ve temiz kayıtların nasıl görüntüleneceğini gösterir. Kayıt seçenekleri yedeklerin veya geri yüklemelerin neler olduğunu ve ne zaman yapıldığını, ayrıca işlemdeki uyarı ve hataları görmede yardımcı olur. Örneğin, herhangi bir hata meydana geldiğinde, BitDefender uyarı mesajı kaydını tutar.



Kayıt Görüntüleyici

Kayıt Görüntüleyici' yi aşağıdaki işlemi yaparak değiştirebilirsiniz.

- **Yön Bulma Çubuğu'** ndaki **Kayıt Görüntüleyici'** yi tıklayın.
- **Menü Çubuğu'** ndaki **Görünüm** menüsünü tıklayarak, **Kayıt Görüntüleyici'** yi seçin.
- **CTRL+Alt+L** kısayolunu kullanabilirsiniz.

Kayıtları Göster

Kayıt göster seçenekleri işlemlerinizi geriye dönük izlemenizi ve işlemlerdeki hataların nedenlerini bulmanızı sağlar.

BitDefender Yedeklemenin kayıt maddelerinin içerikleri aşağıdaki unsurlardır:

Tip

Kayıt öğeleri önemine göre sınıflandırılmıştır. BitDefender Yedekleme de önem şiddetine göre dört derece vardır.

- **Ölümcül:** Önemli bir problemdir, BitDefender Yedeklemenin normal çalışmasını engeller. Örneğin, BitDefender Yedeklemenin yapılandırma dosyaları zarar görmüştür.
- **Hata:** Bir problem işlemin başarısızlığına yol açar. Örneğin, sunucuyu yedeklemek için bir görev belirlenmiştir, fakat sunucuya ulaşılamıyordur.
- **Uyarı:** Oluşan problem işlemi etkilemez ancak, sonradan sınıflandırılabilir. Örneğin, yedeklemede bir dosya okunamaz.
- **Bilgi** Başarılı bir işlemi tanımlar. Örneğin, görev başarı ile silindi.

Tarih
Kayıt öğesinin meydana geldiği tarihtir.

Zaman
Kayıtlanan öğenin meydana geldiği yerel saattir.

Kaynak
Kaynaklar, BitDefender Yedekleme uygulaması veya bir göreve ait olabilir ve sırası ile kayıtlanmıştır. Örneğin, BitDefender Yedekleme uygulaması tarafından kayıtlanan bir öğenin sistem tarafından işaretlendiğini gösterir. Diğer işaretli isimler ise BitDefender Yedekleme görevleri tarafından kayıt altına alınan öğelerdir.

Kullanıcı
Kayıtlanan öğenin, hangi kullanıcının yaptığı işlem sonucu kayıtlandığını gösterir.

Tanımlama
Kayıtlanmış öğenin, içeriğinin açıklamasıdır.

Kayıtları Temizle

BitDefender Yedekleme otomatik ve manuel olmak üzere iki çeşit kayıt temizlemeyi destekler.

Önemli
Kayıt silindiğinde geri tekrar alınamaz. Bu nedenle, kayıtları gelecekteki incelemeler için, bir dosyaya vermek en iyi yöntemdir.

Otomatik Temizleme
BitDefender Yedekleme başladığında, varolan kayıt boyutu ile varsayılanı karşılaştırır. BitDefender Yedekleme, varsayılan boyutu aşmış olan tüm kayıtları temizler.

Not
Varsayılan kayıt boyutunu görmek veya değiştirmek için şu adımları izleyin:
1. **Menü Çubuğu'** ndaki **Araçlar'** a tıklayın.

2. **Seçenekler**' e bastıktan sonra **Raporlar & Kayıtlar**' a tıklayın.
3. Uygun alana arzu ettiğiniz boyut limitini (MB olarak) girin. Kayıt boyutu bu limite ulaştığında BitDefender Yedekleme tüm kayıtları temizleyecektir.

Manuel Temizleme

Kayıtları manuel olarak temizlemek için şu adımları takip edin:

1. **Kayıt Yönetimi** menüsünden **Hepsini Sil**' e tıklayın.
2. Kayıtları silmeden önce dışarı vermek için, **Tamam**' ı veya herhengi bir kaydı korumak istemiyorsanız **Hayır**' ı tıklayın.

Kayıtları, Dışarı Verme ve Dışarıdan Alma

BitDefender Yedekleme, iki formatta kayıtları dışarı verme ve dışarıdan almayı destekler: `.TXT` ve `.XML`

Not

Bizim tavsiyemiz kayıtları silmeden önce onları bir dosyaya çıkarıp kaydetmenizdir.

Kayıtları çıkarıp kaydetmek için şu adımları takip edin:

1. **Kayıt Yönetimi** menüsünden **.TXT dosyasına ver** veya **.XML dosyasına ver**' i tıklayın.
2. Kaydedeceğiniz dosyanın adını yazın ve lokasyonunu belirleyin.
3. **Kaydet**' i tıklayın.

Dışarıdan (belirli bir dosyadan) kayıt almak için şu adımları takip edin:

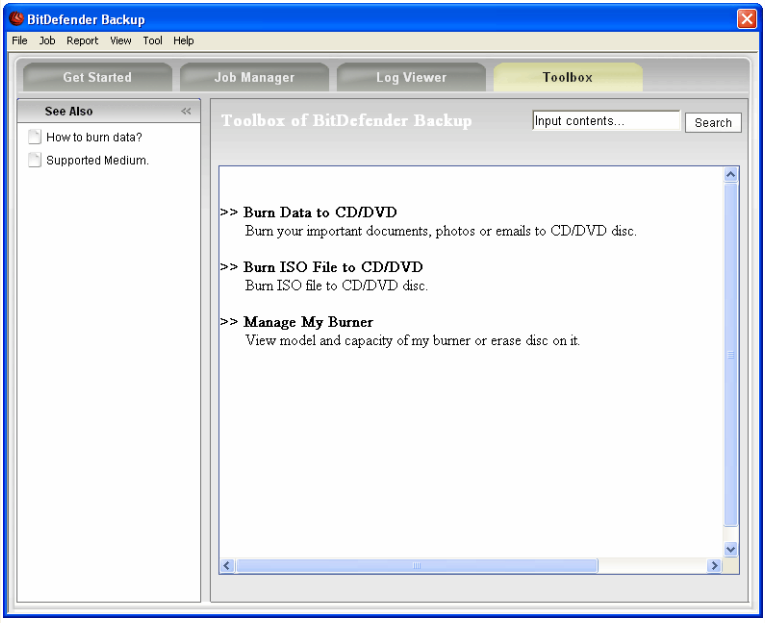
1. **Kayıt Yönetimi** menüsünden **.TXT dosyasından al** veya **.XML dosyasından al**' ı tıklayın.
2. Dosyanızı bulun.
3. **Aç**' a tıklayın.

Not

Son kayıtları gördüğünüzden emin olmak için, **Kayıt Yönetimi** menüsünden, **Yenile**' ye tıklayın.

14.2.4. Araç Kutusu

Bu bölümde, BitDefender Yedeklemenin CD/DVD veya ISO dosyaların nasıl kullandığı gösterilir. Bu konu CD-R/RW, DVD-R/RW/RAM, DVD+R/RW/DL gibi medyaların ve yedeği alınmış verilerin korunmasını kapsar.



Araç Kutusu

Araç Kutusu' nu açarak aşağıdakileri yapabilirsiniz.

- **Yön Bulma Çubuğu**' ndaki **Araç Kutusu**' nu tıklayın.
- **Menü Çubuğu**' ndaki **Görünüm**' ü tıklayarak **Araç Kutusu**' nu seçin.
- **CTRL+Alt+T** kısayolunu kullanabilirsiniz.

CD/DVD Yak

CD/DVD' yi manuel olarak yakmak için, şu adımları takip edin:

1. **CD/DVD Yak**' ı tıklayın
2. Eğer tekrar yazılabilir bir CD' yi yeniden kullanmak istiyorsanız **Sil**' i tıklayın. Hızlı silmek için, **Hızlı**' yı tıklayın. Eğer track kayıtlarını tam olarak silecekseniz, **Tam**' ı tılayın. Fakat bu biraz zaman alacaktır.
3. **Diyalog ile Yak**

Disk yakma işleminden sonra diski kapatmayı seçebilir veya Joliet dosya sistemini kullanarak yazdırabilirsiniz.

4. Açılır pencereden yakmak istediğiniz veriyi seçmek için, **Dosya** veya **Dizin'** i tıklayın.
5. Veri eklendikten sonra yakıcıyı seçip, disk adını yazın ve **Yak'** a tıklayın.

CD/DVD ye ISO imaj Dosyası Yakmak

CD/DVD ye ISO imaj dosyası yakmak için, şu adımları takip edin:

1. **CD/DVD ye ISO imaj Dosyası Yak'** ı tıklayın.
2. Eğer tekrar yazılabilir bir CD' yi yeniden kullanmak istiyorsanız **Sil'** i tıklayın. Hızlı silmek için, **Hızlı'** yı tıklayın. Eğer track kayıtlarını tam olarak silecekseniz, **Tam'** ı tılayın. Fakat bu biraz zaman alacaktır.
3. **Diyalog ile Yak**

   Disk yakma işleminden sonra diski kapatmayı seçebilir veya Joliet dosya sistemini kullanarak yazdırabilirsiniz.
4. **Ekle**' yi tıklayın.
5. Bir ISO imajı seçip **Aç'** ı tıklayın.
6. **Yak**' ı tıklayın.

Yakıcımı Yönet

Kayıt cihazını ve sistemdeki medyayı izlemenize ve yönetmenize yardımcı olur. Aşağıdaki linkleri içerir.

- **Çıkar** Seçilen kayıt cihazı çıkarılır.
- **Kapat**Seçilen kayıt cihazı kapatılır.
- **Medya Bilgileri** kayıt cihazının medya bilgileri görüntülenir.
- **Cihaz Bilgileri** kayıt cihazının bilgileri görüntülenir.
- **Kapasite** kayıt cihazının medya kayıt kapasitesi görüntülenir.
- **Medyayı Sil** disk içeriği silinir.

BitDefender Kurtarma CD'si

15. Tanıtma

BitDefender Total Security 2008, işletim sisteminiz başlamadan önce tüm mevcut sabit diskleri tarayacak ve temizleyecek nitelikte bir başlangıç CD'si ile birlikte gelmektedir.

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.

BitDefender Kurtarma CD'si, 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.

Not
BitDefender Kurtarma CD' sini indirmek için: http://download.bitdefender.com/rescue_cd/

15.1. Sistem Gereksinimleri

Bilgisayarınızı BitDefender Kurtarma CD'si ile 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
Minimum 512 MB RAM Bellek (1 GB tavsiye edilmektedir)

CD-ROM
BitDefender Kurtarma CD'si bir CD-ROM'dan çalıştırılır. Bu nedenle, bir CD-ROM ve başlatılabileceği bir BIOS gerekmektedir.

Internet bağlantısı
BitDefender Kurtarma CD'si 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
Standard SVGA-uyumlu grafik kartı.

15.2. Dahil edilen Yazılımlar

BitDefender Kurtarma CD'si aşağıda belirtilen yazılım paketlerini içermektedir.

Xedit
Bu bir text dosyası editörüdür.

Vim
Bu sözdizimi vurgularını, GUI ve daha fazlasını içeren güçlü bir text dosyası editörüdür. Daha fazla bilgi için lütfen, Vim Anasayfası sitesine başvurun.

Xcalc
Bu bir hesaplayıcıdır.

RoxFiler
RoxFiler, hızlı ve güçlü bir grafik dosya yöneticisidir.

Daha fazla bilgi için lütfen, Daha fazla bilgi için lütfen, RoxFiler homepage sitesine başvurun.

MidnightCommander
GNU Midnight Commander (mc) bir text-mode dosya yöneticisidir.

Daha fazla bilgi için lütfen, Daha fazla bilgi için lütfen, MC homepage sitesine başvurun.

Pstree
Pstree çalışan işlemleri görüntüler.

Top
En üstte Linux görevleri görüntülenir.

Xkill
Xkill, müşteri tarafından onun X kaynaklarını öldürür.

Partition Image

Partition Image, EXT2, Reiserfs, NTFS, HPFS, FAT16, and FAT32 dosya sistemi formatlarını bir imaj dosyasına yedeklemenize yardımcı olur. Bu program yedekleme amacı ile kullanılabilir.

Daha fazla bilgi için lütfen, Partimage homepage sitesini ziyaret edin.

GtkRecover

GtkRecover, GTK versiyonlarının konsol program kurtarıcısıdır. Dosya kurtarmanıza yardımcı olur.

Daha fazla bilgi için lütfen, GtkRecover homepage sitesini ziyaret edin.

ChkRootKit

ChkRootKit, bilgisayarınızı rootkitlere karşı taramanıza yardımcı olur.

Daha fazla bilgi için lütfen, ChkRootKit homepage sitesini ziyaret edin.

Nessus Network Scanner

Nessus, Linux, Solaris, FreeBSD, ve Mac OS X için bir uzak güvenlik tarayıcısıdır.

Daha fazla bilgi için lütfen, Nessus homepage sitesini ziyaret edin.

Iptraf

Iptraf bir IP ağ görüntüleme yazılımıdır.

Daha fazla bilgi için lütfen, Iptraf homepage sitesini ziyaret edin.

Iftop

Iftop arayüzün kullandığı bant genişliğini görüntüler.

Daha fazla bilgi için lütfen, Iftop homepage sitesini ziyaret edin.

MTR

MTR bir ağ tanımlama aracıdır.

Daha fazla bilgi için lütfen, MTR homepage sitesini ziyaret edin.

PPPStatus

PPPStatus, gelen ve giden TCP/IP trafiğinin istatistiklerini görüntüler.

Daha fazla bilgi için lütfen, PPPStatus homepage sitesini ziyaret edin.

Wavemon

Wavemon, kablosuz ağ cihazları için bir görüntüleme uygulamasıdır.

Daha fazla bilgi için lütfen, Wavemon homepage sitesini ziyaret edin.

USBView

USBView, USB noktalarında bağlı olan cihazları gösterir.

Daha fazla bilgi için lütfen, USBView homepage sitesini ziyaret edin.

Pppconfig

Pppconfig, otomatik olarak çevirmeli ppp bağlantısını ayarlar.

DSL/PPPoe

DSL/PPPoe, PPPoE (ADSL) bağlantısına göre yapılandırılmıştır.

I810rotate

I810rotate, i810 üzerinde i810switch(1) donanımı kullanan bir video çıkışıdır.

Daha fazla bilgi için lütfen, I810rotate homepage sitesini ziyaret edin.

Mutt

Mutt güçlü text tabanlı bir MIME mail istemcisidir.

Daha fazla bilgi için lütfen, Mutt homepage sitesini ziyaret edin.

Mozilla Firefox

Mozilla Firefox tanınan bir web tarayıcısıdır.

Daha fazla bilgi için lütfen, Mozilla Firefox homepage sitesini ziyaret edin.

Elinks

Elink text mode bir web tarayıcısıdır.

Daha fazla bilgi için lütfen, Elinks homepage sitesini ziyaret edin.

16. BitDefender Kurtarma CD'si nasıl kullanılır.

Bu bölümde bilgisayarınızı kötücül yazılımlara karşı, BitDefender ile taramanın ve Windows PC' nizin yedeklerinin nasıl alınacağını bulacaksınız. Bununla birlikte bu CD ile beraber gelen yazılım uygulamaları ile bu kullanıcı rehberindeki açıklamalar dışında daha bir çok görev yapabilirsiniz.

16.1. BitDefender' ı Başlatmak

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 BitDefender' ı çalıştırmak için ekrandaki talimatları takip edin.

Boot Splash Ekranı

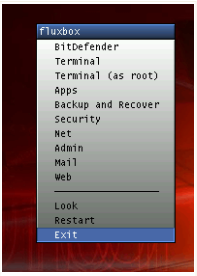
Virüs imzalarının güncellenmesi, yükleme başlangıcında otomatik olarak yapılır. Bu biraz zaman alabilir.

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

Masaüstü

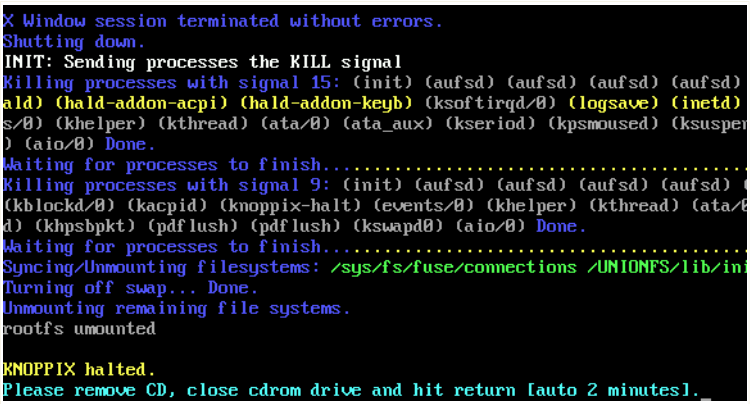
16.2. BitDefender Kurtarma CD'sini Durdur

BitDefender Kurtarma CD'sinden düzgün şekilde çıkmak için, BitDefender menüsünden **Çık** seçeneğini seçerek veya bir terminalde **halt** komutu vererek bilgisayarınızı güvenli bir şekilde kapatabilirsiniz..



"ÇIKIŞ"'ı seçiniz

BitDefender Kurtarma CD'si 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

16.3. Bir virüs koruma taraması nasıl yapabilirim?

CD' den başlama işlemi bittiğinde, bilgisayarınızı tam olarak tarayabileceğiniz bir sihirbaz görünecektir. **Başla** tuşuna basın.

Not
Eğer ekran çözünürlüğünüz yeterince yüksek değilse, taramaya text modda başlamanız istenecektir.

Takip eden üç adımda tarama süreci rehber eşliğinde tamamlanır.

1. Tarama durumunu ve istatistikleri görebilirsiniz (tarama hızı, geçen süre, taranan sayısı / bulaşmış / şüpheli / gizli objeler ve diğerleri)

   Not
   Tarama süreci, taramanın karmaşıklığına bağlı olarak, belirli bir zaman alabilir

2. Sisteminizi etkileyen sorunun adedini görebilirsiniz.

   Gruplarda görünen sorunlar. Bir seçeneği açmak için “+” olan kutuyu, seçeneği kapatmak için “-” olan kutuyu tıklayın.

   Her grup için bütün işlemleri seçebilir veya her sorun için ayrılmış işlemi seçebilirsiniz.

3. Sonuçların özetini görebilirsiniz.

Sadece belirli bir dizini taramak istiyorsanız, aşağıdaki adımları takip edin:

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.

```
# bdscan /path/to/scan/
```

16.4. BitDefender' ı bir vekil sunucu üzerinden nasıl güncelleştirebilirim?

Eğer internete bağlanmak için bir vekil sunucu kullanıyorsanız, güncelleştirme için bazı yapılandırmalar virüs imzalarına göre olacaktır.

BitDefender' ı vekil sunucu üzerinden güncellemek için aşağıdaki adımları takip edin.

1. Masaüstüne sağ tıklayın. BitDefender Kurtarma CDsi bağlamsal menüsü görünecektir.
2. Kök menüde iken **Terminal'** i seçin.
3. **cd /ramdisk/BitDefender-scanner/etc** komutunu yazın.
4. **mcedit bdscan.conf** komutunu yazın, dosyayı düzenlemek için GNU Midnight Commander (mc) programı kullanılacak.
5. Aşağıdaki satır hakkında yorum yapmadan `#HttpProxy =` sadece `#` işaretini silin) ve etki alanını belirleyin, kullanıcı adı, şifre ve vekil sunucunun portu, takip eden satır buna benzemelidir:

   ```
   HttpProxy = myuser:mypassword@proxy.company.com:8080
   ```
6. Değişiklikleri kaydetmek için **F2'** ye basıp kayıt işlemini onaylayın, kapatmak için **F10'** a basın.
7. **bdscan update** komutunu yazın.

16.5. Verilerimi nasıl kaydedebilirim?

Varsayalım ki Windows yüklü bilgisayarınız bilinmeyen bir sorun dolayısı ile açılmıyor. Aynı zamanda bilgisayarınızdaki çok önemli verilere umutsuzca ihtiyacınız var. Bu durumda BitDefender Kurtarma CD' si işinize yarayacak.

Bilgisayarınızdaki verileri çıkarılabilir bir cihaza, örneğin USB hafıza kartı gibi kaydetmek için, aşağıdaki adımları takip edin.

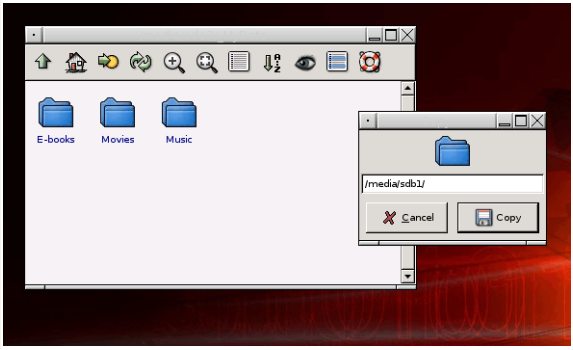
1. BitDefender Kurtarma CD' sini CD sürücüsüne koyun, hafıza kartını USB sürücüye takıp, bilgisayarı yeniden başlatın.
2. Aşağıdaki pencere açılacaktır.

Masaüstü Ekranı

3. Yedeklerini almak istediğiniz verilerin olduğu disk bölümüne çift tıklayın (örneğin `[sda3]` gibi).

> ***Not***
> BitDefender Kurtarma CD' si ile çalışırken, Linux tipindeki disk bölüm isimleri ile çalışacaksınız. Örneğin `[sda1]` Windowstaki `(C:)` yerine, `[sda3]` yine `(F:)` yerine ve `[sdb1]` memory kartı yerine kullanılacaktır.

4. Klasörlerinize göz atarak arzuladığınız dizini açın. Örnek olarak `Belgelerim` içindeki `Videolarım`, `Müziğim` gibi.
5. İstediğiniz dizini sağ tıklayarak **Kopyala** tuşuna basın. Aşağıdaki pencere açılacak.



Verileri Kaydetme

6. Text kutusunda uygun yere `/media/sdb1/` yazarak, **Kopyala** tuşuna basın.

Yardım Alma

17. Destek

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 tehditleri 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.

17.1. 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.

17.2. Yardım Almak

17.2.1. Web Selfservisine Gidin

Herhangi bir sorununuz olduğunda, destek uzmanlarımız 7/24 telefon, email, veya chat yolu ile hiç bir ek ücret ödemeden yardımcı olacaktır.

Lütfen aşağıdaki linki takip ediniz.

İngilizce

http://www.bitdefender.com/site/KnowledgeBase/browseProducts/2193/

Almanca

http://www.bitdefender.com/de/KnowledgeBase/browseProducts/2193/

Fransızca

http://www.bitdefender.com/fr/KnowledgeBase/browseProducts/2193/

Romence

http://www.bitdefender.com/ro/KnowledgeBase/browseProducts/2193/

İspanyolca

http://www.bitdefender.com/es/KnowledgeBase/browseProducts/2193/

17.2.2. Bir destek kaydı açın

Bir destek kaydı açıp email ile destek almak istiyorsanız, aşağıdaki linkleri takip edin:

İngilizce: http://www.bitdefender.com
Almanca: http://www.bitdefender.com
Fransızca: http://www.bitdefender.com
Romence: http://www.bitdefender.com
İspanyolca: http://www.bitdefender.com

17.3. İletişim Bilgileri

Verimli iletişim, başarılı bir işin anahtarıdır. Son 10 yıl içinde, BITDEFENDER, 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.

17.3.1. 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.kavi.com.tr http://www.bitdefender.com.tr
Ürün ftp arşivler: ftp://ftp.bitdefender.com/pub
Yerel distribütörler: http://www.bitdefender.com/partner_list
BitDefender Bilgi Üssü: http://kb.bitdefender.com

17.3.2. 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.

A.B.D

BitDefender, LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33309
Web: http://www.bitdefender.com
Teknik Destek:

- E-mail: support@bitdefender.com
- Telefon:

- 1-888-868-1873 (Sadece kayıtlı kullanıcılar için A.B.D içi erişim numarası)
- 1-954-776-6262 (Sadece kayıtlı kullanıcılar için)

Müşteri Hizmetleri:

- E-mail: customerservice@bitdefender.com
- Telefon:
  - 1-888-868-1873 (Sadece kayıtlı kullanıcılar için A.B.D içi erişim numarası)
  - 1-954-776-6262 (Sadece kayıtlı kullanıcılar için)

Almanya

BitDefender GmbH
Batı Avrupa Merkezi
Karlsdorferstrasse 56
88069 Tettnang
Almanya
Tel: +49 7542 9444 60
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

Romanya

BITDEFENDER
5th Fabrica de Glucoza St.
Bucharest
Teknik Destek: bddestek@kavi.com.tr
Satış: bdsatis@kavi.com.tr
Tel: +40 21 4085600
Fax: +40 21 2330763
Ürün web sitesi: http://www.kavi.com.tr http://www.bitdefender.com.tr

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 konusu dikkate alınmalıdır. Bilgisayar güvenlik uzmanları 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-mail

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

Bu uygulamalar, bir döküman içine bir makro yerleştirmenize olanak sağlar ve döküman 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.

Paket 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 üstten 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 yönlendirerek, 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 UNIX 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, Homeros' un 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.