TREND MICRO

Worry-Free™ Business Security Standard6

#1 for Small Business Security

Yükleme Kılavuzu

Belge Kısım Numarası: WAEM64048/90311

Çıkış Tarihi: Aralık 2009

Ürün Adı ve Sürüm No.: Trend Micro™ Worry-Free™ Business Security 6.0

Şu numaralı ABD Patentleri kapsamında korunmaktadır: 5.951.698 ve 7.188.369

Trend Micro™ Worry-Free™ Business Security için kullanıcı belgeleri, ürün ortamınızın yazılım ve yükleme yönergelerinin temel özelliklerini açıklama amacını taşımaktadır. Yazılımı yükleyip kullanmadan önce dikkatlice okuyun.

Yazılımdaki ek özelliklerin kullanımına ilişkin ayrıntılı bilgi, çevrimiçi yardım dosyasında ve Trend Micro sitesindeki Bilgi Bankası'nda mevcuttur.

Trend Micro, her zaman belgelerini iyileştirmek için çalışmaktadır. İstediğiniz zaman geribildirimde bulunabilirsiniz. Bu belgeyi lütfen aşağıdaki adreste değerlendirin:

http://www.trendmicro.com/download/documentation/rating.asp

İçerik

Bölüm 1: Trend Micro™ Worry-Free™ Business Security Ürününün Tanıtımı

Bölüm 2: Yüklemeye Hazırlama

Bölüm 3: Sunucuyu Yükleme

Bölüm 4: Yükseltme ve Geçirme

Bölüm 5: Başlarken

Bölüm 6: Temel Güvenlik Ayarlarını Yönetme

Ek A: Sorun Giderme ve Sık Sorulan Sorular

Ek B: Yardım Alma

Ek C: Sözlük

Dizin

Bölüm 1

Trend Micro™ Worry-Free™ Business Security Ürününün Tanıtımı

Bu bölümde, Trend Micro Worry-Free Business Security (WFBS) uygulamasının başlıca özellikleri ve yetenekleri ele alınmaktadır.

Bu bölümde ele alınan başlıklar şunlardır:

Trend Micro Worry-Free Business Security Ürününe Genel Bakış

Trend Micro Worry-Free Business Security (WFBS), küçük işletme kullanıcılarını ve varlıklarını veri ve kimlik hırsızlığına, riskli Web sitelerine karşı korur. Trend Micro™ Smart Protection Network tarafından desteklenen Worry-Free Business Security:

- **Daha güvenlidir:** Virüslerin, casus yazılımların, ve Web tehditlerinin bilgisayarlara veya sunuculara ulaşmasını önler. URL filtreleme özelliği, riskli Web sitelerine erişimi engeller ve kullanıcının verimini artırmaya yardımcı olur.
- **Daha akıllıdır:** Hızlı taramalar ve sürekli güncellemeler, kullanıcıların bilgisayarlarında en az etkiyi yaratarak yeni tehditleri önler.
- **Daha kolaydır:** Dağıtımı kolay olan ve yönetim gerektirmeyen WFBS, tehditleri daha etkili bir şekilde tespit eder, böylece güvenliğe değil işletmenize odaklanabilirsiniz.

Yenilikler

Sürüm 6.0

- **Smart Scan:**

  Smart Scan, önemli miktarda kötü amaçlı yazılım ve casus yazılım tarama işlevini bir tarama sunucusuna aktarır.

  İstemcinin görev yükünü azaltır ve istemcilerinin sürekli güncelleme indirme gereksinimini azaltarak olağanüstü bir hızla yayılan tehditlere karşı koruma sağlar.

  Tek tek istemcileri güncellemek yerine sunucu düzeyinde çözüm geliştirerek neredeyse anında en yeni korumayı sağlayabilir.

  Daha fazla bilgi için bkz. *Tarama Yöntemleri*, sayfa 8-2 ve*Tarama Yöntemini Seçme*, sayfa 8-3.

- **URL Web İçeriği Filtreleme:**

  Uygunsuz içerik barındıran Web sitelerini engellemesi için Trend Micro'ya güvenebilirsiniz. URL filtreleme, çalışanların verimini artırmaya, ağ kaynaklarının güvenliğini sağlamaya ve özel bilgileri korumaya yardımcı olabilir.

  Daha fazla bilgi için bkz. *URL Filtrelemesini Yapılandırma*, sayfa 6-17.

- **Smart Protection Network Tümleştirmesi:**

  Trend Micro Smart Protection Network, en son tehditlere karşı güncel koruma sağlamak amacıyla Internet üzerinde tehditlere ilişkin büyük miktarda bilgiyi bir araya getiren bir teknoloji bileşimidir.

  URL Filtreleme, Web Reputation ve Smart Scan, Trend Micro Smart Protection Network'ün ayrılmaz parçalarıdır.

  Daha fazla bilgi için bkz. *Participating in the Smart Protection Network* on page 13-5.

- **Daha Basit ve Daha Kolay Canlı Durum:**

  Canlı Durum panosunu okumak artık daha da kolay.

  Daha fazla bilgi için bkz. *Canlı Durum*, sayfa 5-5.

- **Worry-Free™ Remote Manager 2.1 ile Tümleşik Yükleme:**

  Tedarikçiler artık yeni yüklenmiş bir WFBS Security Server'ı uzaktan yönetmelerine olanak tanıyan Worry-Free Remote Manager Agent'ı yükleme seçeneğine sahip.

  Daha fazla bilgi için bkz. *Installing the Trend Micro™ Worry-Free™ Remote Manager Agent* on page 3-35.

- **Restore Encrypted Virus Karantina Aracı İçin Yeni Grafik Arayüzü:**

  Restore Encrypted Virus aracını kullanırken daha kolay karantina yönetimi sağlar.

  Daha fazla bilgi için bkz. *Restore Encrypted Virus* on page E-8.

- **CPU Kullanımına Dayalı Değişken Tarama:**

  CPU kullanımı yüksek olduğunda tarama için daha fazla esneklik sağlar. WFBS, artık CPU'ya duyarlıdır ve CPU kullanımı yüksek olduğunda duraklatılacak şekilde yapılandırılabilir.

  Daha fazla bilgi için bkz. *El İle ve Zamanlanmış Tarama Seçeneklerini Yapılandırma*, sayfa 8-4.

- **USB Otomatik Çalışma Tehditlerine Karşı Koruma:**

  Sürücü bir istemcinin USB bağlantı noktasına takıldığında USB sürücülerindeki otomatik çalıştırma dosyalarının yürütülmesini engeller.

  Daha fazla bilgi için bkz. *Restore Encrypted Virus* on page E-8.

Sürüm 6.0 Service Pack 1

- **Gelişmiş İstemci Güvenliği**

  Kötü amaçlı yazılımların aracı üzerindeki önemli bileşenleri değiştirmesini ya da sona erdirmesini önler.

- **Güvenlik Duvarını Tüm İstemciler için Devre Dışı Bırakabilme**

  Güvenlik Duvarını Genel Ayarlar'daki yeni seçeneği kullanarak tüm İstemciler için devre dışı bırakır.

- **Yeni İşletim Sistemleri İçin Destek**

  WFBS artık Windows 7, Windows Server 2008 R2 ve Windows Server 2008 Foundation'ı destekliyor.

Temel Özellikler

Bu sürümün ürün özellikleri arasında Trend Micro Smart Protection Network ile daha iyi tümleştirme yer almaktadır.

Trend Micro Smart Protection Network

Trend Micro Smart Protection Network, müşterileri Web tehditlerinden korumak için tasarlanmış yeni nesil, bulut-istemci içerik güvenlik alt yapısıdır. Smart Protection Network'ün temel özelliklerini aşağıda görebilirsiniz:

Smart Feedback

Trend Micro Smart Feedback, Trend Micro ürünleri ve şirketin 7/24 tehdit araştırma merkezleri ve teknolojileri arasında kesintisiz iletişim sağlar. Tek bir müşterinin rutin geçmiş denetimi sırasında tespit edilen her yeni tehdit, Trend Micro tehdit veritabanlarının tümünü otomatik olarak günceller ve müşterilerin söz konusu tehditle bir daha karşılaşmamasını sağlar. Müşteri ve ortaklardan oluşan kapsamlı genel ağı üzerinden topladığı tehdit bilgilerini sürekli olarak işleyen Trend Micro, en yeni tehditlere karşı otomatik, gerçek zamanlı koruma sağlar ve komşuların birbirinin evine göz kulak olduğu, otomatikleştirilmiş semt gözetimi programları gibi "elbirliğiyle" güvenlik sağlar. Toplanan tehdit bilgileri, söz konusu iletişimin içeriğine değil, iletişim kaynağının geçmişine bağlı olduğundan, müşterinin kişisel veya işletme bilgilerinin gizliliği her zaman korunur.

Web Reputation

Dünyanın en büyük etki alanı geçmişi veritabanlarından birine sahip olan Trend Micro Web reputation teknolojisi, Web sitesinin yaşı, geçmişteki yer değişiklikleri ve kötü amaçlı yazılım davranış analizleriyle tespit edilen şüpheli etkinlikler gibi faktörlere dayanarak bir geçmiş puanı atama yoluyla Web etki alanlarının güvenilirliğini izler. Ardından siteleri taramaya ve kullanıcıların virüslü sitelere erişmesini engellemeye devam eder. Doğruluk oranını artırmak ve hatalı pozitif sonuçları azaltmak için, Trend Micro Web reputation teknolojisi, birçok zaman yasal sitelerin yalnızca bazı kısımları saldırılardan etkilendiğinden ve geçmiş durumu zaman içinde dinamik olarak değişebildiğinden sitelerin tamamını sınıflandırmak veya engellemek yerine belirli sayfalara veya bağlantılara geçmiş puanları atar.

Dosya Geçmişi

Trend Micro dosya geçmişi teknolojisi, kullanıcı erişimine izin vermeden önce her dosyanın geçmişini kapsamlı bir bulut içi veritabanını kullanarak kontrol eder. Kötü amaçlı yazılım bilgileri bulut içinde depolandığından, tüm kullanıcılara anında sunulur. Yüksek performanslı içerik dağıtım ağları ve yerel önbelleğe alma sunucuları, denetim işlemi sırasında gecikme süresini en aza indirir. Bulut-istemci mimarisi, daha hızlı koruma sağlar ve istemcinin genel iş yükünü önemli ölçüde azaltırken desen dağıtımı yükünü ortadan kaldırır.

Smart Scan

Trend Micro Worry-Free Business Security, Smart Scan adında yeni bir teknoloji kullanmaktadır. WFBS istemcileri, geçmişte tarama işlemi gerçekleştirmek için her istemcinin taramaya ilişkin bileşenler indirmesini gerektiren Geleneksel Tarama'yı kullanıyordu. Smart Scan ile istemci Smart Scan sunucusu üzerindeki desen dosyasını kullanır.

Smart Scan'in yararlarından bazıları şunlardır:

- **Daha az donanım kaynağı:** dosyaları taramak için yalnızca Tarama Sunucusunun kaynakları kullanılır.

URL Filtrelemesi

URL filtreleme, çalışanların iş dışında uğraşlara ayırdığı zamanı kısıtlamak, Internet bant genişliği kullanımını azaltmak ve daha güvenli bir çalışma ortamı yaratmak amacıyla Web sitelerine erişimi denetlemenize yardımcı olur. Bir URL filtreleme koruması düzeyi seçebilir veya taramak istediğiniz Web sitesi türlerini özelleştirebilirsiniz.

Korumanın Yararları

Aşağıdaki tabloda farklı WFBS bileşenlerinin bilgisayarlarınızı tehditlerden nasıl koruduğu anlatılmaktadır.

TABLO 1-1. Korumanın Yararları

TEHDIT	KORUMA
Virüs/Kötü Amaçlı Yazılım. Virüs, Truva Atları, Solucanlar, Arka Kapılar ve Davetsiz Misafirler. **Casus Yazılım/Grayware.** Casus Yazılım, Çeviriciler, Korsanlık araçları, Parola kırma uygulamaları, Reklam Yazılımı, Şaka programları ve Tuş Kaydediciler	Antivirüs ve Casus Yazılımdan Koruma Tarama Motorları ile Client/Server Security Agent'taki Desen Dosyaları
E-posta iletileri ve istenmeyen posta yoluyla yayılan Virüs/Kötü Amaçlı Yazılım ve Casus Yazılım/Grayware	Client/Server Security Agent'ta POP3 Posta Taraması
Ağ Solucanları/Virüsler	Client/Server Security Agent'ta Güvenlik Duvarı
İzinsiz girişler	Client/Server Security Agent'ta Güvenlik Duvarı
Zararlı olabilecek Web siteleri/Kimlik Avı siteleri	Client/Server Security Agent'ta Web Reputation ve TrendProtect
Kötü Amaçlı Davranış	Client/Server Security Agent'ta Behavior Monitoring
Sahte erişim noktaları	Client/Server Security Agent'ta Transaction Protector
IM uygulamalarındaki müstehcen/kısıtlı içerik	Client/Server Security Agent'ta IM İçerik Filtreleme

Bileşenler

Antivirüs

- **Client/Server Security Agent için Tarama motoru (32 bit/64 bit):** Tarama motoru, kullanıcılarınızın açtığı ve/veya kaydettiği dosyalardaki virüs/kötü amaçlı yazılım ve diğer güvenlik risklerini tespit etmek için virüs deseni dosyasını kullanır.

  Tarama motoru, kalıp eşleme olarak adlandırılan bir işlemi kullanarak ilk düzey algılamayı gerçekleştirmek için virüs kalıp dosyası ile birlikte çalışır. Her virüs, kendisini diğer kodlardan ayıran benzersiz bir "imza" veya gösterge karakterleri dizilimi içerdiğinden, Trend Micro'da çalışan virüs uzmanları desen dosyasında bu kodun etkisiz parçalarını yakalar. Ardından motor, taranan her dosyanın belirli bölümlerini virüs desen dosyasındaki desenlerle karşılaştırarak bir eşleşme arar.
- **Virüs deseni:** Security Agent'ların bir virüsün varlığına işaret eden virüs imzalarını, benzersiz bit ve bayt desenlerini tanımlamasına yardımcı olan bir dosyadır.
- **Virüs temizleme şablonu:** Virüs Temizleme Motoru tarafından kullanılan bu şablon, motorun bunları ortadan kaldırabilmesi için Truva atlarını ve Truva işlemlerini, solucanları ve casus yazılım/grayware öğelerini tanımlamaya yardımcı olur.
- **Virüs temizleme motoru (32 bit/64 bit):** Temizleme Hizmetleri'nin Truva atı dosyalarını ve Truva atı işlemlerini, solucanları ve casus yazılım/grayware öğelerini taramak ve kaldırmak için kullandığı motordur.
- **IntelliTrap kural dışı durum kalıbı:** IntelliTrap ve tarama motorları tarafından, sıkıştırılmış dosyalarda zararlı kod taraması yapmak için kullanılan kural dışı durum deseni.
- **IntelliTrap deseni:** IntelliTrap ve tarama motorları tarafından, sıkıştırılmış dosyalarda zararlı kod taraması yapmak için kullanılan desen.
- **Smart Scan Agent Deseni:** İstemcinin tehditleri tanımlamak için kullandığı desen dosyası. Bu desen dosyası aracının makinesinde saklanır.
- **Geribildirim motoru 32 bit** ve **64 bit:** Trend Micro Smart Protection Network'üne geribildirim gönderme motoru.
- **Smart Scan Deseni:** İstemcinizin bilgisayarındaki dosyalara özgü veriler içeren desen dosyasıdır.

Casus yazılımdan koruma

- **Casus yazılım tarama motoru (32 bit):** i386 (32 bit) işletim sistemleri çalıştıran etkilenen bilgisayar ve sunuculardaki casus yazılım/grayware öğelerini tarayan, tespit eden ve kaldıran ayrı bir tarama motorudur.
- **Casus yazılım tarama motoru (64 bit):** 32 bit sistemlerinin casus yazılım/grayware tarama motoruna benzeyen bu tarama motoru, x64 (64 bit) işletim sistemlerindeki casus yazılımları tarar, tespit eder ve kaldırır.
- **Casus yazılım kalıbı:** Bilinen casus yazılım imzalarını içerir ve casus yazılım tarama motorları (hem 32 bit hem de 64 bit) tarafından El İle ve Zamanlanmış Taramalar için bilgisayar ve sunucularda bulunan casus yazılım/grayware öğelerini tespit etmek amacıyla kullanılır.
- **Casus yazılım etkin izleme kalıbı:** Casus yazılım desenine benzer ama tarama motoru tarafından casus yazılımdan koruma amaçlı tarama için kullanılır.

Anti-spam

- **Anti-spam motoru (32 bit/64 bit):** Spam olarak da bilinen istenmeyen ticari e-posta iletilerini (UCE) veya istenmeyen toplu e-posta iletilerini (UBE) tespit eder.
- **Anti-spam kalıbı:** E-posta iletilerindeki istenmeyen postaları tespit etmek amacıyla anti-spam motorunu etkinleştirmek üzere istenmeyen e-posta tanımları içerir.

Salgın Savunması

Salgın Savunması, Internet tehditleri ve/veya dünya genelindeki diğer salgınlar hakkında erken uyarı sağlar. Salgın Savunması, bilgisayarlarınızı ve ağınızı korumak için otomatik olarak önleyici adımlar atar ve ardından sorunu tespit etmek ve hasarı gidermek için koruyucu önlemler alır.

- **Güvenlik açığı kalıbı:** Tüm güvenlik açıklarını içeren veritabanının bulunduğu dosyadır.

  Güvenlik açığı deseni, tarama motorunun bilinen güvenlik açıklarını taraması için yönergeler sağlar.

Ağ Virüsü

- **Genel güvenlik duvarı motoru (32 bit/64 bit):** Güvenlik Duvarı, bilgisayarları korsanların saldırılarından ve ağ virüslerinden korumak üzere ağ virüs deseni dosyasıyla birlikte bu motoru kullanır.
- **Ortak güvenlik duvarı kalıbı:** Virüs kalıbı dosyası gibi, bu dosya da WFBS ürününün ağ virüs imzalarını tanımlamasına yardımcı olur.
- **Transport Driver Interface (TDI) (32 bit/64 bit):** Ağ trafiğini tarama modüllerine yeniden yönlendiren modüldür.
- **WFP sürücüsü (32 bit/64 bit):** Windows™ Vista İstemcileri için Güvenlik Duvarı, ağ virüslerine yönelik tarama yapmak için ağ virüsü kalıp dosyasıyla bu sürücüyü kullanır.

Web Reputation

- **Trend Micro Security veritabanı:** Web Reputation, istenen Web sayfasını görüntülemeden önce sayfanın potansiyel riskini değerlendirir. Veritabanından alınan dereceye ve yapılandırılan güvenlik düzeyine bağlı olarak, Client/Server Security Agent, isteği engeller veya onaylar.
- **URL Filtreleme Motoru (32 bit/64 bit):** Sayfayı değerlendirmek için Trend Micro Security veritabanını sorgulayan motor.

TrendProtect

- **Trend Micro Security database:** TrendProtect, bir Web sayfasında görüntülenen köprülerin güvenlik riski potansiyelini değerlendirir. Veritabanının döndürdüğü derecelendirmeye ve tarayıcı eklentisinde yapılandırılan güvenlik düzeyine bağlı olarak, eklenti, bağlantıyı derecelendirir.

Yazılım Koruması

- **Yazılım Koruma Listesi:** Korunan program dosyaları (EXE ve DLL) değiştirilemez veya silinemez. Bir programı kaldırmak, güncellemek veya yükseltmek için klasörün korumasını geçici olarak kaldırın.

Behavior Monitoring

- **Behavior Monitoring Sürücüsü:** Bu sürücü, istemciler üzerinde süreç davranışını tespit eder.
- **Behavior Monitoring Core Service:** CSA, Behavior Monitor Core Drivers'ı işlemek için bu hizmeti kullanır.
- **İlke Uygulama Deseni:** Security Server üzerinde Aracılar tarafından uygulanması gereken ilkelerin listesi.
- **Dijital İmza Deseni:** Yazılımı güvenle kullanılabilecek, Trend Micro tarafından kabul edilen şirketlerin listesi.
- **Behavior Monitoring Yapılandırma Deseni:** Bu desende varsayılan Behavior Monitoring İlkeleri bulunur. Bu desendeki dosyalar, tüm ilke eşlemelerinde atlanır.
- **Behavior Monitoring Algılama Deseni:** Şüpheli tehdit davranışını algılamaya ilişkin kuralları içeren bir desen.

Transaction Protector

- **Wi-Fi Advisor:** SSID'lerinin geçerliliğine, kimlik doğrulama yöntemlerine ve şifreleme gereksinimlerine dayanılarak kablosuz ağların güvenliğini denetler.

İçerik Filtreleme

- **Kısıtlanmış Sözcük/Tümcecik Listesi:** Kısıtlanmış Sözcük/Tümcecik Listesi, anında mesajlaşma uygulamalarıyla aktarılamayan sözcükleri/tümcecikleri içerir.

Canlı Durum ve Bildirimler

- Canlı Durum, Salgın Savunması, Antivirüs, Casus Yazılıma Karşı Koruma ve Ağ Virüsleri ile ilgili güvenlik durumunu bir bakışta görmenizi sağlar. . Benzer şekilde, WFBS önemli olaylarda Yöneticilere bildirim gönderebilir.

Tehditleri Anlama

Bilgisayar güvenliği sürekli değişen bir konudur. Yöneticiler ve bilgi güvenliği uzmanları, bilgisayarları ve ağları tehdit eden potansiyel riskleri veya davetsiz olayları açıklamak için çeşitli terimler ve tümcecikler geliştirir ve benimser. Aşağıda, bu belgede kullanılan terimlerle bu terimlerin anlamları ele alınmaktadır.

Virüs/Kötü Amaçlı Yazılım

Bilgisayar virüsü/kötü amaçlı yazılımı, benzersiz çoğalma yeteneğine sahip bir program, yürütülebilir bir koddur. Virüsler/kötü amaçlı yazılımlar, kendilerini hemen her tür yürütülebilir dosyaya ekleyebilir ve dosyalar kopyalanıp kullanıcıdan kullanıcıya gönderildikçe yayılır.

Çoğalmanın yanı sıra, bazı bilgisayar virüslerinin/kötü amaçlı yazılımlarının başka ortak bir özelliği daha vardır: virüs yükünü dağıtan bir zarar yordamı. Bazı yükler, yalnızca iletileri veya resimleri görüntülerken bazıları, dosyaları yok edebilir, sabit diskinizi yeniden biçimlendirebilir veya başka hasarlara neden olabilir.

- **Kötü amaçlı yazılım:** Kötü amaçlı yazılım, bilgisayar sahibinin bilgisi ve rızası olmadan bilgisayar sistemine girecek ve zarar verecek şekilde tasarlanmış bir yazılımdır.
- **Truva atları:** Truva atı, zararsız bir uygulama kimliğine bürünen kötü amaçlı bir programdır. Truva atları, virüslerden/kötü amaçlı yazılımlardan farklı olarak çoğalmazlar, ama onlar kadar yıkıcı olabilirler. Truva atına örnek olarak, bilgisayarınızı virüsten/kötü amaçlı yazılımdan kurtarmayı vadedip bilgisayarınıza virüs/kötü amaçlı yazılım bulaştıran bir uygulama verilebilir.
- **Solucanlar:** Bilgisayar solucanı, kendi yapısının bir kısmının veya tümünün işlevsel kopyalarını diğer bilgisayar sistemlerine yayabilen, kendi içinde bir program veya program grubudur. Yayılma genellikle ağ bağlantıları veya e-posta ekleri üzerinden gerçekleşir. Virüslerden/kötü amaçlı yazılımlardan farklı olarak, solucanların kendilerini ana makine programlarına eklemesi gerekmez.
- **Arka kapılar:** Arka kapı, yakalanmadan normal kimlik doğrulamasını atlatmanın, bir bilgisayara uzaktan erişim ve/veya bilgilere erişim sağlamanın bir yöntemidir.
- **Davetsiz misafirler:** Davetsiz misafir, bir işletim sisteminin kullanıcıları tarafından yasal kullanımına zarar vermek üzere tasarlanmış bir dizi programdır. Davetsiz misafir, genellikle, kurulumunu gizler ve standart sistem güvenliğini tahrip ederek kullanıcılar tarafından kaldırılmasını engellemeye çalışır.

- **Makro Virüsler:** Makro virüsler uygulamaya özgüdür. Bu virüsler, Microsoft Word (.doc) ve Microsoft Excel (.xls) gibi uygulamalara ait dosyaların içinde bulunur. Dolayısıyla, .doc, .xls ve .ppt gibi makro yetenekleri olan uygulamalarda yaygın olarak görülen uzantılara sahip dosyalarda tespit edilebilirler. Makro virüsler, uygulama içindeki veri dosyaları arasında gezinir ve engellenmemeleri durumunda zamanla yüzlerce dosyaya hasar verebilir.

İstemci bilgisayarlarında bulunan ve Client/Server Security Agent Antivirüs taraması sırasında virüsleri/kötü amaçlı yazılımları tespit edebilir. Trend Micro, virüsleri/kötü amaçlı yazılımları *temizlemenizi* önerir.

Casus Yazılım/Grayware

Grayware, beklenmedik veya yetkilendirilmemiş eylemler gerçekleştiren bir programdır. Casus yazılım, reklam yazılımı, çevirici, şaka programları, uzaktan erişim araçları ve diğer istenmeyen dosya ve programlar için kullanılan genel bir terimdir. Türüne bağlı olarak, çoğalan veya çoğalmayan kötü amaçlı kod içerebilir.

- **Casus yazılım:** Casus yazılım, kullanıcının rızası veya haberi olmadan bilgisayara yüklenen ve kişisel bilgileri toplayıp başkalarına aktaran bilgisayar yazılımıdır.
- **Çeviriciler:** Geniş bant olmayan bağlantılar için Internet'e bağlanırken çeviriciler gerekir. Kötü amaçlı çeviriciler, doğrudan ISS'nıza bağlanmak yerine yüksek dereceli numaralarla bağlantı kuracak şekilde tasarlanmıştır. Bu kötü amaçlı çevirilerin sağlayıcıları, elde edilen ekstra parayı kendilerine ayırır. Diğer çevirici kullanıcıları arasında kişisel bilgileri aktarma ve kötü amaçlı yazılım indirme bulunur.
- **Korsanlık Araçları:** Korsanlık aracı, korsanlığa yardımcı olmak üzere tasarlanmış bir program veya program dizisidir.
- **Reklam Yazılımı:** Reklam yazılımı veya reklamcılık destekli yazılım, yazılım yüklendikten sonra veya uygulama kullanımdayken bir bilgisayarda otomatik olarak reklamcılık malzemesi yürüten, görüntüleyen veya indiren herhangi bir yazılım paketine verilen addır.
- **Tuş Kaydediciler:** Tuş kaydedici, kullanıcının bastığı tüm tuşları kaydeden bir bilgisayar yazılımıdır. Daha sonra bu bilgiler korsan tarafından alınır ve kişisel amaçlarla kullanılır.

- **Bot'lar:** Bot ("robot" ifadesinin kısaltması), bir kullanıcı veya başka bir program için aracı görevi gören veya gerçek bir kullanıcının etkinliklerini taklit eden bir programdır. Bot'lar yürütüldüklerinde, kendi kopyalarını çoğaltabilir, sıkıştırabilir ve dağıtabilirler. Bot'lar, ağ bilgisayarları üzerinde otomatik saldırılar düzenlemek üzere kullanılabilir.

Client/Server Security Agent'lar grayware öğelerini algılayabilir. Trend Micro, casus yazılım/grayware öğelerini *temizlemenizi* önerir.

Ağ Virüsleri

Bir ağ üzerinden yayılan her virüs, ağ virüsü olmak zorunda değildir. Bu bölümde ele alınan tehditlerden yalnızca bazıları, örneğin solucanlar, ağ virüsü kategorisine girer. Daha net belirtmek gerekirse, ağ virüsleri çoğalmak için TCP, FTP, UDP, HTTP ve e-posta protokolleri gibi ağ protokollerini kullanır.

Güvenlik duvarı, ağ virüslerini tanımlamak ve engellemek için bir ağ virüsü desen dosyasını kullanır.

İstenmeyen Posta (Spam)

Spam, genellikle ticari amaçlı, ayrım yapılmaksızın birden çok posta listesine, kullanıcıya veya haber grubuna gönderilen istenmeyen e-posta iletilerinden (önemsiz e-posta iletileri) oluşur. İki tür istenmeyen posta vardır: İstenmeyen ticari e-posta iletileri (UCE) veya istenmeyen toplu e-posta iletileri (UBE).

İzinsiz girişler

İzinsiz girişler, bir ağa veya bilgisayara güç kullanarak ya da izinsiz girmek anlamına gelir. Bir ağın veya bilgisayarın güvenliğini atlatmak anlamına da gelebilir.

Kötü Amaçlı Davranış

Kötü Amaçlı Davranış, bir yazılım tarafından işletim sisteminde, kayıt defteri girdilerinde, diğer yazılımlarda veya dosya ve klasörlerde yapılabilecek yetkisiz değişiklikler anlamına gelir.

Sahte Erişim Noktaları

Kötü İkizi olarak da bilinen Sahte Erişim Noktaları, kullanıcının bulunduğu yerde sağlanan yasal bir erişim noktası gibi görünen, ama aslında kablosuz iletişimleri izlemek üzere bir korsan tarafından oluşturulmuş sahte bir Wi-Fi erişim noktasına verilen addır.

IM Uygulamalarındaki Müstehcen/Kısıtlı İçerik

Müstehcen veya kuruluşunuza özgü metin içeriğinin anında mesajlaşma uygulamalarıyla üçüncü taraflara aktarılması. Örneğin, gizli şirket bilgileri.

Çevrimiçi Tuşlama Dinleyicileri

Tuş kaydedicinin çevrimiçi sürümü. Daha fazla bilgi için bkz. *Casus Yazılım/Grayware*, sayfa 1-12.

Paketleyiciler

Paketleyiciler, yürütülebilir programları sıkıştırmak için kullanılan araçlardır. Yürütülebilir bir dosyanın sıkıştırılması, dosya içindeki kodun geleneksel antivirüs tarama ürünleri tarafından tespit edilmesini zorlaştırır. Paketleyici, bir Truva atı veya solucan gizleyebilir.

Trend Micro tarama motoru, paketlenmiş dosyaları tespit edebilir ve bu tür dosyalar için önerilen eylem *karantinadır*.

Ürün Bileşeni Teknolojisi

Aşağıdaki tabloda ürün belgelerinde görünen terimler tanımlanmaktadır:

TABLO 1-2. Ürün Bileşeni Teknolojisi

ÖĞE	AÇIKLAMA
Security Server	Security Server, ürün için merkezileştirilmiş, Web tabanlı yönetim konsolu olan Web konsolu barındırır.
Tarama Sunucusu	Tarama Sunucusu Smart Scan için yapılandırılmış istemcileri taramaya yardımcı olur. Varsayılan olarak, Tarama Sunucusu Security Server'a yüklenir.
Agent/CSA/MSA	Client/Server Security Agent. Aracılar yüklü oldukları istemciyi korur.
İstemci	İstemciler, masaüstü bilgisayarlar, taşınabilir bilgisayarlar ve Client/Server Security Agent yüklü olan sunuculardır.
Web konsolu	Web konsolu, tüm Aracıları yöneten merkezi bir Web tabanlı yönetim konsoludur. Web konsolu, Security Server üzerindedir.

Bölüm 2

Yüklemeye Hazırlama

Bu aşamadaki adımlar, WFBS yüklemesi ve dağıtımı için plan geliştirmenize yardımcı olur. Trend Micro, yükleme işleminden önce bir yükleme ve dağıtım planı oluşturmanızı önerir. Bu, ürünün yeteneklerini mevcut antivirüs ve ağ koruma girişiminizle birleştirmenize yardımcı olacaktır.

Bu bölümde ele alınan başlıklar şunlardır:

Başlamadan Önce

Aşağıdaki yükleme ve dağıtım aşamalarını inceleyin.

Aşama 1: Dağıtım Planlama

WFBS dağıtımının planlanması aşağıdaki görevleri içerir:

1. Sistem gereksinimlerini doğrulama. Daha fazla bilgi için, bkz. *Sunucu ve Aracı Sistem Gereksinimleri*, sayfa 2-4.
2. Security Server'ın nereye yükleneceğini belirleme. Daha fazla bilgi için, bkz. *Security Server'ın Nereye Yükleneceğini Belirleme*, sayfa 2-26.
3. İstemcilerinin sayısını belirleme. Daha fazla bilgi için, bkz. *İstemci Sayısını Tanımlama*, sayfa 2-26.
4. Ağ trafiği için planlama. Daha fazla bilgi için, bkz. *Ağ Trafiği İçin Planlama*, sayfa 2-27.
5. Masaüstü bilgisayar ve sunucu gruplarını belirleme. Daha fazla bilgi için, bkz. *Masaüstü Bilgisayar ve Sunucu Grubu Sayısını Belirleme*, sayfa 2-29.
6. Client/Server Security Agent'lar için yükleme/dağıtım seçeneklerini belirleme. Daha fazla bilgi için, bkz. *Aracılar İçin Dağıtım Seçenekleri Belirleme*, sayfa 2-29.

Aşama 2: Security Server'ı Yükleme

Bu aşama aşağıdaki görevleri içerir:

1. Yükleme için hedef sunucuyu hazırlama. Daha fazla bilgi için, bkz. *Sunucu ve Aracı Sistem Gereksinimleri*, sayfa 2-4.

   İpucu: WFBS *Yönetici Kılavuzu'nun* Sistem Denetim Listeleri bölümünü güncelleme. WFBS ürününü yüklerken bu bilgilerden yararlanın.

2. WFBS ürününü yükleme veya yükseltme. Daha fazla bilgi için bkz. *Yüklemeye Genel Bakış*, sayfa 2-20 veya *En İyi Uygulamaları Yükseltme*, sayfa 4-3.
3. Yüklemeyi doğrulama. Daha fazla bilgi için, bkz. *Yüklemeyi Doğrulama*, sayfa 3-35.

Aşama 3: Aracıları Yükleme

Security Server'ı yükledikten sonra, tüm sunuculara ve masaüstü bilgisayarlara Client/Server Security Agent'ı yükleyin. Bu aşama aşağıdaki görevleri içerir:

Not: Genel bir bakış için bkz. *Aracı Yüklemeye Genel Bakış*, sayfa 3-2.

1. Yükleme yöntemi seçme
2. Aracıları yükleme veya yükseltme
3. Yüklemeyi doğrulama
4. Yüklemeyi test etme

Aşama 4: Güvenlik Seçeneklerini Yapılandırma

Client/Server Security Agent'ı istemcilere yükledikten sonra gerekirse varsayılan ayarları özelleştirin. Bu, aşağıdaki görevleri içerir:

1. Masaüstü ve sunucu gruplarını yapılandırma
2. Tercihleri yapılandırma

Sunucu ve Aracı Sistem Gereksinimleri

WFBS Security Server'ı (tarama sunucusunu içerir) ve aracıyı yüklemek için aşağıdakiler gerekir:

Not: Client/Server Security Agent, Citrix Presentation Server™ 4.0/4.5/5.0 ile Uzak Masaüstü'nü destekler.
Bu sürüm VMware® ESX™ 3.0/3.5, VMWare Server 1.0.3/2.0.1, WMware Workstation 6.0/6.5 ve Microsoft Hyper-V™ Server 2008'i destekler.

TABLO 2-3. Sistem Gereksinimleri

Öğe	Minimum Özelikler
Security Server	
İşlemci	Geleneksel tarama modu: Intel™ Pentium™ 4 veya üzeri Smart Scan modu: Intel Core 2 Duo™ veya üzeri önerilir
Bellek	Smart Scan modu: 1GB minimum, 2GB önerilir 512MB minimum (x86 sistemleri); 1GB önerilir 1GB (x64 sistemleri); 2GB önerilir 4GB (Windows™ Essential Business Server 2008 veya Windows™ Small Business Server 2008 sistemleri)
Disk alanı	6GB (CSA disk kullanım alanı hariç)

TABLO 2-3. Sistem Gereksinimleri (Devamı)

Öğe	Minimum Özelikler	
İşletim sistemi	**Seri veya Aile**	**Desteklenen Hizmet Paketleri veya Sürümler**
	Windows 2000	SP3 veya SP4
	Windows Small Business Server (SBS) 2000	Hizmet paketi yok veya SP1a
	Windows XP (yalnızca Professional)	SP2 veya SP3
	Windows Server™ 2003 R2 (Storage Server 2003 ile birlikte)	SP1 veya SP2
	Windows Server™ 2003 (Storage Server 2003 ile birlikte)	SP1 veya SP2
	Windows SBS 2003 R2	SP1 veya SP2
	Windows SBS 2003	SP1 veya SP2
	Windows Vista™	SP1 veya SP2
	Windows Home Server	Hizmet paketi yok veya SP1
	Windows Server 2008 R2	Hizmet paketi yok
	Windows Server 2008	SP1 veya SP2
	Windows SBS 2008	SP1 veya SP2
	Windows 2008 Foundation	SP1 veya SP2
	Windows Essential Business Server (EBS) 2008	SP1 veya SP2
	Not: Tersi belirtilmemişse bu işletim sistemlerinin tüm büyük sürümleri ve 64 bit sürümleri desteklenir.	

TABLO 2-3. Sistem Gereksinimleri (Devamı)

Öğe	Minimum Özelikler
Web sunucusu	Microsoft™ Internet Information Server (IIS) 5.0 (Windows 2000 veya SBS 2000) IIS 6.0 (Windows Server 2003, SBS 2003 veya Home Server) IIS 7.0 (Windows Server 2008, SBS 2008 veya EBS 2008) IIS 7.5 (Windows 7, Windows Server 2008 R2) Apache™ HTTP Server 2.0.63 veya daha yeni sürümü **Not:** IIS; Windows XP veya Windows Vista'da desteklenmez. Apache bu işletim sistemlerinde kullanılmalıdır. Zaten yüklenmiş bir Apache sunucunuz varsa, Trend Micro bunu kaldırmanızı önerir. Security Server ile birlikte bir Apache sunucusu yüklenir.
Web Konsolu	
Web tarayıcısı	Internet Explorer 6.0 veya daha yenisi (yalnızca 32 bit)
PDF okuyucu (raporlar için)	Adobe™ Acrobat™ Reader 4.0 veya daha yenisi
Görüntü	1024x768 piksel veya daha yüksek çözünürlüklü, yüksek renkli ekran

TABLO 2-3. Sistem Gereksinimleri (Devamı)

Öğe	Minimum Özelikler
Client/Server Security Agent	
İşlemci	Intel™ Pentium™ x86 veya uyumlu işlemci AMD64 ve Intel 64 teknolojilerini destekleyen x64 işlemci Saat hızı gereksinimleri işletim sistemine göre değişir: 1GHz (Windows Server 2008, SBS 2008 veya EBS 2008) 800MHz (Windows Vista, Windows 7) 450MHz (Windows 2000, SBS 2000, XP, Server 2003, SBS 2003 veya Home Server)
Bellek	128MB (x86 sistemleri); 256MB önerilir
Disk alanı	450MB

TABLO 2-3. Sistem Gereksinimleri (Devamı)

Öğe	Minimum Özelikler	
İşletim sistemi	**Seri veya Aile**	**Desteklenen Hizmet Paketleri veya Sürümler**
	Windows 2000	SP3 veya SP4
	Windows Small Business Server (SBS) 2000	Hizmet paketi yok veya SP1a
	Windows XP Home	SP2 veya SP3
	Windows XP Tablet PC	SP2 veya SP3
	Windows XP	SP1 veya SP2
	Windows Server 2003 R2 (Storage Server 2003 ile birlikte)	SP1 veya SP2
	Windows Server 2003 (Storage Server 2003 ile birlikte)	SP1 veya SP2
	Windows SBS 2003 R2	SP1 veya SP2
	Windows SBS 2003	SP1 veya SP2
	Windows Vista	SP1 veya SP2
	Windows Home Server	Hizmet paketi yok veya SP1
	Windows Server 2008 R2	SP1 veya SP2
	Windows Server 2008	SP1 veya SP2
	Windows SBS 2008	SP1 veya SP2
	Windows 2008 Foundation	SP1 veya SP2
	Windows Essential Business Server (EBS) 2008	SP1 veya SP2
	Windows 7	Hizmet paketi yok (Not: Windows 7 Starter Edition desteklenmez.)

TABLO 2-3. Sistem Gereksinimleri (Devamı)

Öğe	Minimum Özelikler
Web tarayıcısı (Web tabanlı kurulum için)	Internet Explorer 6.0 veya daha yenisi
Görüntü	256 renkli görüntü ya da 800x600 veya daha üzeri çözünürlükte daha fazla renk

Not: CSA, Gigabit ağ arabirim kartlarını (NIC) destekler.

Diğer Gereksinimler

- Smart Scan'i kullanan istemciler çevrimiçi modda olmalıdır. Çevrimdışı istemciler Smart Scan'i kullanamaz.
- Security Server'ı barındıran bilgisayarda Yönetici veya Etki Alanı Yöneticisi erişimi
- Yüklü Microsoft Ağları için dosya ve yazıcı paylaşımı
- Yüklü Transmission Control Protocol/Internet Protocol (TCP/IP) desteği

Not: Ağ üzerinde Microsoft ISA Server veya bir proxy ürünü yüklüyse, Web konsoluna erişim izni vermek ve istemci-sunucu iletişiminin kurulabilmesini sağlamak için HTTP bağlantı noktasını (varsayılan olarak 8059) ve SSL bağlantı noktasını (varsayılan olarak 4343) açmanız gerekir.

Sürümünüzü Seçme

Tam Sürüm ve Değerlendirme Sürümü

WFBS ürününün tam sürümünü veya ücretsiz bir değerlendirme sürümü yükleyebilirsiniz.

- **Tam sürüm:** Teknik destek, virüs deseni indirmeleri, gerçek zamanlı tarama ve bir yıllık program güncellemeleriyle gelir. Bir bakım yenilemesi satın alarak tam bir sürümü yenileyebilirsiniz. Tam sürümü yüklemek için Etkinleştirme Kodu gerekir.
- **Değerlendirme sürümü:** 30 gün boyunca gerçek zamanlı tarama ve güncellemeler sağlar. İstediğiniz zaman değerlendirme sürümünden tam sürüme yükseltebilirsiniz. Değerlendirme sürümünü yüklemek için Etkinleştirme Kodu gerekmez.
  - **Email Reputation Services ile veya onsuz:** Email Reputation Services (ERS) ürününü değerlendirme sürümüne eklemeyi veya hariç tutmayı seçebilirsiniz. ERS, Trend Micro tarafından barındırılan bir anti-spam çözümüdür.

Kayıt Anahtarı ve Etkinleştirme Kodları

WFBS sürümünüz bir Kayıt Anahtarı ile gelir. Yükleme sırasında, WFBS sizden bir Etkinleştirme Kodu girmenizi ister.

Etkinleştirme Kodlarına sahip değilseniz, ürününüzle birlikte verilen Kayıt Anahtarını kullanarak Trend Micro Web sitesine kaydolun ve Etkinleştirme Kodlarını alın. WFBS yükleyici sizi otomatik olarak Trend Micro Web sitesine yeniden yönlendirebilir:

http://www.trendmicro.com/support/registration.asp

Kayıt Anahtarı veya Etkinleştirme Kodu olmadan da değerlendirme sürümü yükleyebilirsiniz. Daha fazla bilgi edinmek için Trend Micro satış temsilcinizle bağlantı kurun (bkz. *Trend Micro ile Bağlantı Kurma*, sayfa B-5).

Not: Kayıt hakkında sorunuz varsa, lütfen aşağıdaki adrese giderek Trend Micro Web sitesini ziyaret edin:
http://esupport.trendmicro.com/support/viewxml.do?ContentID=en-116326

Worry-Free Business Security ve Worry-Free Business Security Advanced

Her sürüm için desteklenen özelliklerin listesini aşağıdaki tabloda bulabilirsiniz.

TABLO 2-4. Ürün Sürümüne Göre Kullanılabilen Özellikler

Özellikler	Worry-Free Business Security	Worry-Free Business Security Advanced
Bileşen Güncellemeleri	Evet	Evet
Antivirüs/Casus yazılımdan koruma	Evet	Evet
Firewall	Evet	Evet
Web Reputation	Evet	Evet
Behavior Monitoring	Evet	Evet
TrendSecure	Evet	Evet
Anında Mesajlaşma İçerik Filtreleme	Evet	Evet
Posta Taraması (POP3)	Evet	Evet
Anti-Spam (POP3)	Evet	Evet
Posta Taraması (IMAP)	Hayır	Evet
Anti-Spam (IMAP)	Hayır	Evet
E-posta İletisi İçerik Filtreleme	Hayır	Evet
Ek Engelleme	Hayır	Evet
URL Filtrelemesi	Evet	Evet

Her lisans türü için desteklenen özelliklerin listesini aşağıdaki tabloda bulabilirsiniz.

TABLO 2-5. Lisans Durumu Sonuçları

	Tam Lisanslı	Değerlendirme (30 günlük)	Süresi Doldu
Kullanım Süresi Sonu Bildirimi	Evet	Evet	Evet
Virüs Desen Dosyası Güncellemeleri	Evet	Evet	Hayır
Program Güncellemeleri	Evet	Evet	Hayır
Teknik Destek	Evet	Hayır	Hayır
Gerçek Zamanlı Tarama*	Evet	Evet	Hayır

*Süresi dolmuş lisanslar için, gerçek zamanlı taramada süresi dolmuş bileşenler kullanılır.

Not: Sürümünüzü yükseltmek için bir Trend Micro satış temsilcisiyle bağlantı kurun.

Lisans ve Bakım Sözleşmesi

Worry-Free Business Security veya Worry-Free Business Security Advanced ürününü satın aldığınızda, size ürünün lisansı ve standart bir Bakım Sözleşmesi verilir. Standart Bakım Sözleşmesi, kuruluşunuz ile Trend Micro arasında imzalanan, ilgili ücretlerin ödenmesi karşılığında size sağlanacak teknik destek ve ürün güncellemelerine ilişkin bir sözleşmedir. Trend Micro yazılım lisansı genellikle, yalnızca satın alma tarihinden itibaren bir (1) yıl süreyle ürün güncellemeleri, model dosyası güncellemeleri ve temel teknik destek bakımı hakkını içerir. Birinci yıldan sonra, yıllık esaslı olarak Trend Micro'nun o zamanki güncel Bakım ücretleriyle Bakım yenilemesi yapmanız gerekir.

Not: Bakım Sözleşmesi'nin süresi dolar, ama Lisans Sözleşmenizin süresi dolmaz. Bakım Sözleşmesi'nin süresi dolsa da tarama yapılmaya devam edilebilir, ama virüs deseni dosyasını, tarama motorunu veya program dosyalarını (el ile bile) güncelleyemezsiniz. Trend Micro'dan teknik destek alma hakkınızı da kaybedersiniz.

Bakım Sözleşmenizin süresinin dolmasından altmış (60) gün önce, Canlı Durum ekranında lisansınızı yenilemeniz için sizi uyaran bir ileti görüntülenir. Bayinizden, Trend Micro satıştan veya aşağıdaki adreste bulunan Trend Micro Çevrimiçi Kaydı'ndan yenileme bakımı satın alarak Bakım Sözleşmenizi güncelleyebilirsiniz:

https://olr.trendmicro.com/registration/

Lisans Sürümleri

Trend Micro, Worry-Free Business Security ve Worry-Free Business Security Advanced'in farklı sürümlerini sunar. Her sürüm farklı bir Etkinleştirme Kodu kullanır.

- **Worry-Free Business Security:** Yerel ağınız üzerindeki masaüstü bilgisayarları, dizüstü bilgisayarları ve sunucu bilgisayarlarını korumak üzere tasarlanmıştır. Salgın Savunması, Güvenlik Duvarı ve Antivirüs ve Casus Yazılıma Karşı Koruma taraması içerir.
- **Worry-Free Business Security Advanced:** Yerel ağınız üzerindeki Microsoft Exchange sunucularını korumak üzere tasarlanmıştır. Worry-Free Business Security Advanced for SMB'nin tüm özelliklerini, ayrıca Anti-spam, İçerik Filtreleme ve Ek Engelleme özelliklerini içerir.
- **Worry-Free Business Security Advanced Değerlendirme Sürümü (Email Reputation Services ile veya onsuz):** 30 günlük değerlendirme süresince Worry-Free Business Security Advanced for SMB'nin tüm özelliklerini test edin. Değerlendirme süresi sona erdiğinde, Security Server güncellenen bileşenleri almaz. Varsayılan olarak, yükleme sırasında Etkinleştirme Kodu girilmediyse bu, değerlendirme sürümünün yüklendiği anlamına gelir.

Süresi Dolmuş Lisansın Sonuçları

Tam lisanslı bir sürümün Etkinleştirme Kodu'nun süresi dolduğunda, motor veya desen dosyası güncellemelerini indiremezsiniz. Ancak, değerlendirme sürümü Etkinleştirme Kodu'ndan farklı olarak, tam lisanslı bir sürümün Etkinleştirme Kodu'nun süresi olduğunda, tüm mevcut yapılandırmalar ve diğer ayarlar geçerliliğini korur. Bu hazırlık, fark etmeden lisans sürenizin dolmasına izin vermeniz durumunda bir koruma düzeyi sağlar.

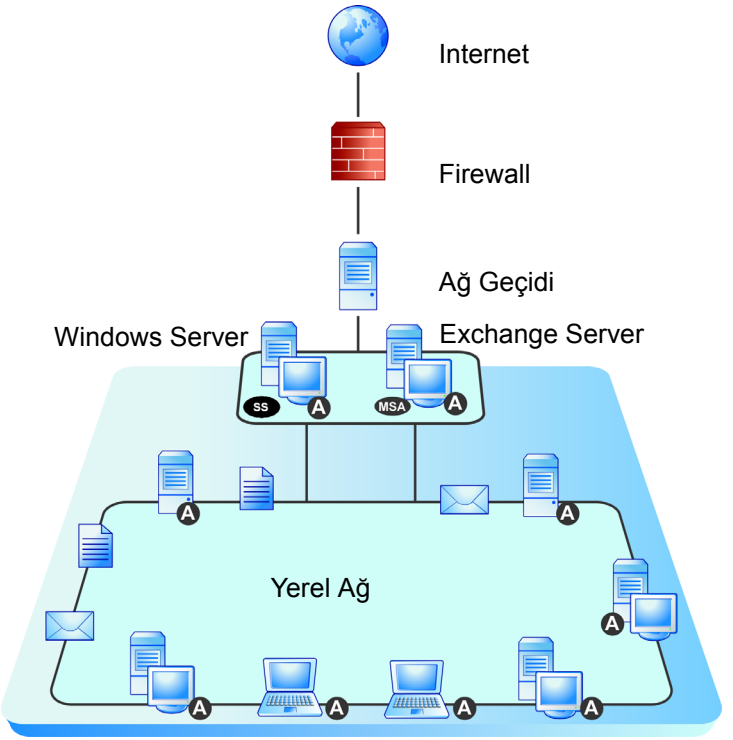
Ağınızı Koruma

WFBS koruması, aşağıdaki bileşenlerden oluşmaktadır:

- **Web konsolu:** tüm aracıları tek bir konumdan yönetir.
- **Security Server:** Web konsolunu barındırır, Trend Micro ActiveUpdate Server'dan güncellemeleri indirir, günlükleri toplar ve depolar ve virüs/kötü amaçlı yazılım salgınlarını denetlemeye yardımcı olur.
- **Client/Server Security Agent:** Windows Vista/2000/XP/Server 2003/Server 2008 bilgisayarlarını virüs/kötü amaçlı yazılım, casus yazılım/grayware, Truva atı ve benzeri tehlikelerden korur.
- **Messaging Security Agent:** Microsoft Exchange sunucularını korur, istenmeyen posta filtresi uygular ve içerik engeller.
- **Tarama Sunucusu:** Trend Micro'dan taramaya özgü bileşenleri indirir ve bu bileşenleri istemcileri taramak için kullanır. Security Server uygulaması, otomatik olarak Security Server'ın yüklü olduğu bilgisayara yüklenir.

Not: Smart Scan'in WFBS uygulamasında, aynı bilgisayar hem Security Server hem de Smart Scan sunucusu görevi üstlenir.

Aşağıdaki şekilde WFBS bileşenlerinin tipik bir ağa nasıl yüklendiği gösterilmektedir.



ŞEKIL 2-1. Ağ topolojisi örneği

TABLO 2-6. Ağ Topolojisi Örneği Açıklamaları

SEMBOL	AÇIKLAMA
A	İstemcilere yüklenen Client/Server Security Agent
MSA	Exchange sunucusuna yüklenen Messaging Security Agent (yalnızca Worry-Free Business Security Advanced ile kullanılabilir)
SS	Windows sunucusuna yüklenen Security Server veya Tarama Sunucusu (Scan Server)

Web Konsolu

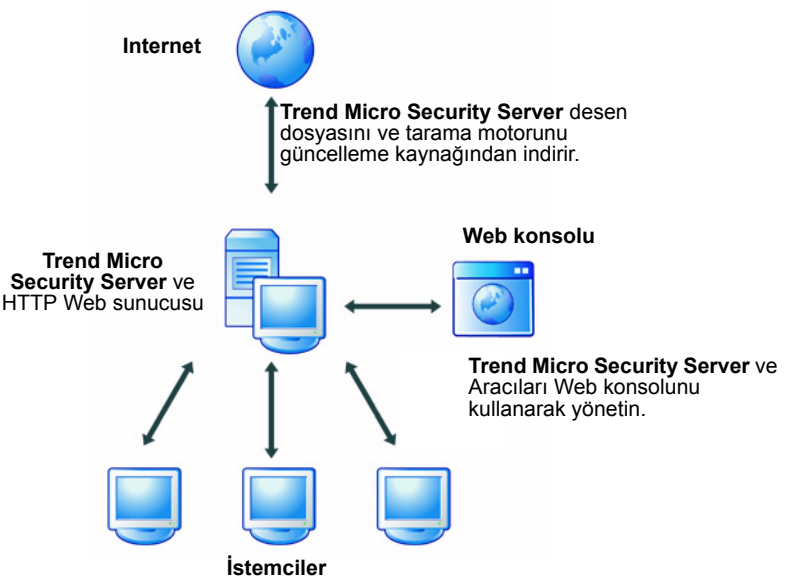
Web konsolu, merkezi bir Web tabanlı yönetim konsoludur. Aracıları yapılandırmak için Web konsolunu kullanın. Web konsolu, Trend Micro Security Server'ı yüklediğinizde yüklenir ve ActiveX, CGI, HTML ve HTTP/HTTPS gibi Internet teknolojilerini kullanır.

Web konsolunu kullanarak aşağıdakileri de yapabilirsiniz:

- Aracıları sunuculara, masaüstü bilgisayarlara ve taşınabilir bilgisayarlara dağıtma.
- Eşzamanlı yapılandırma ve yönetim için masaüstü bilgisayarları, taşınabilir bilgisayarları ve sunucuları mantıksal gruplar halinde birleştirme.
- Virüsten ve casus yazılımda koruma amaçlı tarama yapılandırmaları ayarlama ve tek bir grupta veya birden çok grupta El ile Tarama'yı başlatma.
- Virüs/kötü amaçlı yazılım etkinlikleri için bildirim alma ve günlük raporlarını görüntüleme.
- İstemciler üzerinde tehdit algılandığında e-posta iletileri, SNMP Tuzağı veya Windows Etkinlik Günlüğü ile bildirim alma ve salgın uyarıları gönderme.
- Salgın Önleme'yi yapılandırarak ve etkinleştirerek salgınları önleme.

Security Server

WFBS ürününün merkezinde Security Server bulunur (*Şekil 2-1* altında **SS** ile gösterilir). Security Server WFBS için merkezi Web tabanlı yönetim konsolu olan Web konsolunu barındırır. Security Server, ağ üzerindeki istemciler aracılar yükler ve aracılarla birlikte bir istemci-sunucu ilişkisi oluşturur. Security Server, tek bir merkezden güvenlik durumu bilgilerini görüntülemeyi, aracıları görüntülemeyi, sistem güvenliğini yapılandırmayı ve bileşenleri indirmeyi etkinleştirir. Security Server ayrıca aracılar tarafından kendisine bildirilen tespit edilmiş Internet tehditlerinin günlüklerini kaydettiği veritabanını içerir.



ŞEKIL 2-2. HTTP üzerinden İstemci/Sunucu iletişimi nasıl çalışır

Client/Server Security Agent

Client/Server Security Agent (*Şekil 2-1* altında **A** ile gösterilir), yükleme kaynağı olan Trend Micro Security Server'a rapor verir. Sunucuya en son istemci bilgilerini sağlamak için, aracı, olay durum bilgilerini gerçek zamanlı olarak gönderir. Aracılar, tehdit algılama, aracı başlangıcı, aracı kapanışı, tarama başlangıcı ve bir güncellenmenin tamamlaması gibi olayları rapor eder.

Client/Server Security Agent, üç tarama yöntemi sağlar: Gerçek Zamanlı Tarama, Zamanlanmış Tarama, El ile Tarama.

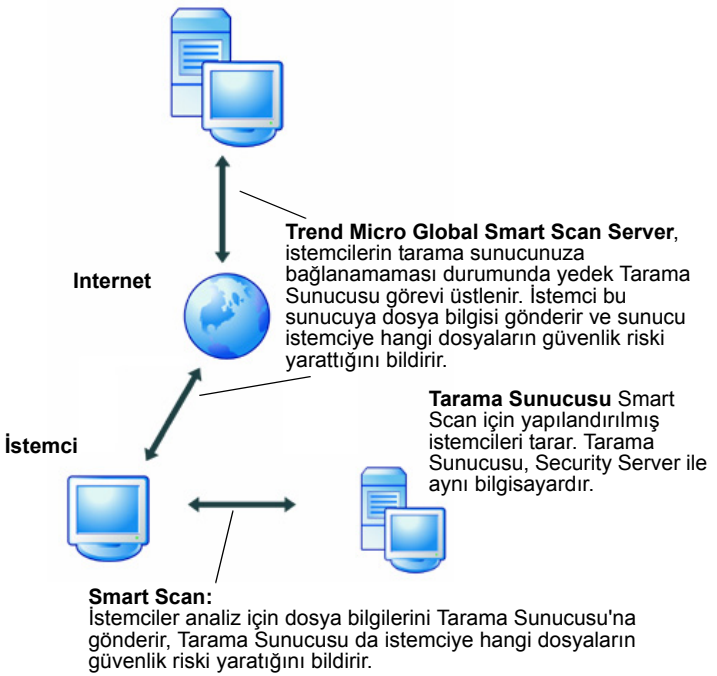
Web konsolundan aracılar üzerinde tarama ayarlarını yapılandırın. Ağ üzerinde tek tip masaüstü koruması uygulamak için, kullanıcılara tarama ayarlarını değiştirme veya aracıyı kaldırma ayrıcalığı vermemeyi seçin.

Tarama Sunucusu

Smart Protection Network'ün bir parçası olarak, WFBS, şimdi istemcilerinizi bir Tarama Sunucusu ile tarama yeteneği sağlamaktadır. Bu bileşen indirme ve istemci bilgisayarlarını tarama yükünü istemcilerinizden alarak tarama sunucusuna aktarır.

İki tür tarama sunucusu vardır:

- **Scan Server:** Security Server ile otomatik olarak bir Tarama Sunucusu yüklenir. Bu, sunucunuzun hem aracılarınız için merkezi bir denetim merkezi hem de tarayıcı görevi üstlenmesini sağlar.
- **Trend Micro Tarama Sunucusu:** Trend Micro, tüm istemciler için yedek olarak bir Tarama Sunucusu sağlar. Ağınız üzerindeki Tarama Sunucusu herhangi bir nedenle çökerse, Trend Micro sizi korur.



ŞEKIL 2-3. Smart Scan iletişimi nasıl çalışır

Not: Security Server ile otomatik olarak bir Tarama Sunucusu yüklenir. Yüklemenin ardından, hangi bilgisayarların Tarama Sunucusu'nu kullanacağını belirtebilirsiniz.

Yüklemeye Genel Bakış

Yükleyici, yükleme sırasında sizden aşağıdaki bilgileri ister:

- **Security Server ayrıntıları:** Güvenlik sunucusunun etki alanı/ana sistem adı veya IP adresi ve WFBS ürününün güvenlik sunucusu dosyalarını yüklediği hedef dizini.
- **Proxy sunucu ayrıntıları:** Ağınız üzerindeki Internet trafiği bir proxy sunucu tarafından işleniyorsa, proxy sunucu bilgilerini (ve gerekirse, kullanıcı adını ve parolayı) yapılandırmanız gerekir. Trend Micro güncelleme sunucusundan en yeni bileşenleri indirmek için bu bilgiler gerekir. Yükleme sırasında veya yüklemenin ardından proxy sunucu bilgilerini girebilirsiniz. Yüklemenin ardından bilgileri girmek için Web konsolunu kullanın.
- **SMTP sunucusu:** Bildirim göndermek için bir SMTP sunucusu kullanıyorsanız, SMTP sunucusunun adını, bağlantı noktası numarasını ve göndericinin ve alıcının e-posta adreslerini girin.

Not: SMTP sunucusu, WFBS ile aynı bilgisayardaysa ve 25 numaralı bağlantı noktasını kullanıyorsa, yükleme programı SMTP sunucusunun adını algılar ve **SMTP Sunucusu** ve **Bağlantı Noktası** alanlarını günceller.

- **Security Server Web konsolu parolası:** Web konsoluna yetkisiz erişimi engellemek için bir parola belirtin.
- **İstemciyi bellekten kaldırma/parola kaldırma:** Client/Server Security Agent ürününün yetkisiz bir şekilde kaldırılmasını veya bellekten kaldırılmasını engellemek için parola ayarlayın.
- **İstemci yazılımı yükleme yolu:** İstemci kurulumu sırasında Client/Server Security Agent dosyalarının kopyalanacağı istemci yükleme yolunu yapılandırın.
- **Hesap ve Ayrıcalıklar:** Yükleme işlemine geçmeden önce, etki alanı veya yerel yönetici ayrıcalıklarına sahip bir hesabı kullanarak oturum açın.

Bağlantı Noktaları

WFBS, iki tür bağlantı noktası kullanır:

- **Sunucu dinleme bağlantı noktası (HTTP bağlantı noktası):** Trend Micro Security Server'a erişmek için kullanılır. Varsayılan olarak, WFBS aşağıdakilerden birini kullanır:
  - **IIS sunucusu varsayılan Web sitesi:** HTTP sunucunuzun TCP bağlantı noktasıyla aynı bağlantı noktası numarası.
  - **IIS sunucusu sanal Web sitesi:** 8059
  - **Apache sunucusu:** 8059
- **İstemci dinleme bağlantı noktası:** İstemcinin Trend Micro Security Server'dan komut aldığı rastgele oluşturulmuş bağlantı noktası numarası.
- **Tarama Sunucusu bağlantı noktaları:** Aracılarınızı taramak için kullanılır: Bkz. *Tablo 2-7*:

TABLO 2-7. Tarama Sunucusu Bağlantı Noktaları

	IIS VARSAYILAN	IIS SANAL	ÖNCEDEN YÜKLENMIŞ APACHE	YENI APACHE YÜKLEMESI
YENI YÜKLEMELER VE YÜKSELTMELER				
SSL olmayan bağlantı noktası	Web sunucusunda SSL olmayan bağlantı noktası	8082 ila 65536 aralığındaki ilk açık bağlantı noktası	Web sunucusunda SSL olmayan bağlantı noktası	Web sunucusunda SSL olmayan bağlantı noktası
SSL bağlantı noktası SSL kullanılıyor	Web sunucusunda SSL bağlantı noktası	4345 ila 65536 aralığındaki ilk açık bağlantı noktası	Yok	Web sunucusunda SSL bağlantı noktası

Dinleme bağlantı noktalarını yalnızca yükleme sırasında değiştirebilirsiniz.

UYARI! Pek çok korsan ve virüs saldırısında HTTP kullanılır ve bu saldırıların çoğu 80 ve/veya 8080 bağlantı noktalarından yönlendirilir. Bunlar, pek çok kuruluşun HTTP iletişimleri için yaygın olarak kullandığı varsayılan Transmission Control Protocol (TCP) bağlantı noktalarıdır.
Kuruluşunuz şu anda HTTP bağlantı noktası olarak bu bağlantı noktalarından birini kullanıyorsa, Trend Micro, başka bir bağlantı noktası numarası kullanmanızı önerir.

Not: Aracılarınızın tarama sunucusuna bağlanmak için hangi bağlantı noktasını kullandığını öğrenmek üzere, sunucunun yüklü olduğu dizinde `SSCFG.ini` dosyasını açın.

Trend Micro Security Server Ön Tarama

Yükleyici yükleme işlemini başlatmadan önce bir ön tarama gerçekleştirir. Bu ön tarama, hedef bilgisayarın virüs, Truva atı veya tehlikeli olabilecek başka kötü amaçlı kod içermediğinden emin olmak amacıyla bir virüs taraması ve Hasar Temizleme Hizmetleri içerir.

Ön tarama, bilgisayarın en büyük güvenlik açığı olan alanlarını hedefler. Bu alanlar şunlardır:

- Önyükleme alanı ve önyükleme dizini (önyükleme virüsleri için)
- Windows klasörü
- Program Dosyaları klasörü

Ön Tarama Algılama Eylemleri

WFBS kurulum programı virüs, Truva atı veya tehlikeli olabilecek başka kötü amaçlı kod tespit ederse, aşağıdaki eylemleri gerçekleştirebilirsiniz:

- **Temizleme:** Virüs veya kötü amaçlı yazılım uygulamasını kaldırarak virüslü dosyayı temizler. Dosya temizlenemiyorsa, WFBS dosyayı şifreler ve yeniden adlandırır.

- **Yeniden adlandır:** Dosyayı şifreler ve dosya uzantısını VIR, VIR1, VIR2 vb. olarak adlandırır. Dosya aynı konumda kalır. WFBS tarafından şifrelenmiş bir dosyanın şifresini açmak için WFBS *Yönetici Kılavuzuna* bakın.
- **Sil:** Dosyayı siler.
- **Geçir:** Dosya üzerinde hiçbir işlem yapmaz.

İpucu: Trend Micro, etkilenen dosyaları temizlemenizi veya silmenizi önerir.

Diğer Yükleme Notları

Trend Micro Security Server'ı yüklediğinizde bilgisayarı yeniden başlatmanız gerekmez. Yükleme işlemini tamamladıktan sonra, Trend Micro Security Server'ı anında yapılandırın ve ardından Client/Server Security Agent programını başlatın. Bir IIS Web sunucusu kullanıyorsanız, kurulum programı otomatik olarak durur ve Web sunucusu yüklenirken IIS/Apache hizmetini yeniden başlatır.

UYARI! **Web sunucusunu, IIS'nin kilitlenmesine yol açabilecek uygulamalar çalıştıran bir bilgisayara yüklemediğinizden emin olun. Bu, kurulumun başarısız olmasına yol açabilir. Daha fazla bilgi için ISS belgelerinize bakın.**

İpucu: Trend Micro, ağınız üzerindeki etkiyi en aza indirmek için WFBS ürününü yoğunluğun en düşük olduğu saatlerde yüklemenizi önerir.

Güvenlik sunucusunda Apache Web sunucusunun desteklenmeyen bir sürümü yüklüyse, Apache yerine IIS ürününü kullanın. İki Web sunucusu uygulaması aynı anda çalışıyorsa, bağlantı noktası numaralarının çakışmadığını ve bilgisayarın yeterli bellek/CPU/disk kaynağına sahip olduğunu doğrulayın.

Windows SBS ve EBS 2008 Kullanıcıları İçin Notlar

WFBS ile Windows Small Business Server (SBS) 2008 veya Windows Essential Business Server (EBS) 2008 ile sağlanan güvenlik özellikleri arasındaki uyumsuzluklar nedeniyle, yükleme sırasında aşağıdaki durumlarla karşılaşılır:

- Client/Server Security Agent (CSA) yüklenmediğinde, hedef bilgisayarlardaki Microsoft OneCare istemcisi otomatik olarak kaldırılır.

Trend Micro, Security Server'ı Windows EBS bilgisayarlarına mutlaka Management Server rolüyle yüklemenizi önermektedir. Bu sunucularda, EBS konsolu eklentisi otomatik olarak Security Server ile birlikte eklenir.

Uyumluluk Sorunları

Bu bölümde, belirli üçüncü taraf uygulamalarıyla ortaya çıkabilecek uyumluluk sorunları açıklanmaktadır. Her zaman Security Server'ı ve diğer bileşenleri yüklediğiniz bilgisayarda yüklü olan tüm üçüncü taraf uygulamalarının belgelerine bakın.

Diğer Antivirüs Uygulamaları

Trend Micro, Trend Micro Security Server'ı yüklediğiniz bilgisayardan diğer antivirüs uygulamalarını kaldırmanızı önerir. Aynı bilgisayarda başka antivirüs uygulamalarının bulunması, Trend Micro Security Server'ın gerektiği gibi yüklenmesini ve performans göstermesini engelleyebilir.

Not: WFBS, herhangi bir üçüncü taraf antivirüs ürününün sunucu bileşenini kaldıramaz, ama istemci bileşenini kaldırabilir (talimatlar ve WFBS ürününün kaldırabileceği üçüncü taraf uygulamalarının listesi için bkz. *Diğer Antivirüs Uygulamalarından Geçirme*, sayfa 4-6)

EBS ve SBS 2008'deki Güvenlik Uygulamaları

WFBS, hem Windows™ Small Business Server (SBS) 2008 hem de Windows Essential Business Server (EBS) 2008 ile uyumludur. Ancak bu işletim sistemleriyle yüklenen veya yönetilen bazı güvenlik uygulamaları WFBS ile çakışabilir. Bu nedenle, bu güvenlik uygulamalarını kaldırmanız gerekebilir.

CSA ve OneCare

Security Server Microsoft Windows Live™ OneCare for Server ile yüklenebildiği halde, Client/Server Security Agent (CSA) OneCare istemcisiyle yüklenemez. CSA yükleyici, OneCare'ı istemci bilgisayarlarından otomatik olarak kaldırır.

Veritabanları

Veritabanlarını tarayabilirsiniz ama bu, veritabanlarına erişen uygulamaların performansını düşürebilir. Trend Micro, veritabanlarını ve yedek klasörlerini Gerçek Zamanlı Tarama'nın dışında tutmanızı önerir. Bir veritabanını taramanız gerekiyorsa, etkiyi en aza indirmek için el ile bir tarama yapın veya taramayı yoğunluğun düşük olduğu saatlerde gerçekleştirin.

Diğer Güvenlik Duvarı Uygulamaları

WFBS güvenlik duvarını yüklemek istiyorsanız, Trend Micro, diğer güvenlik duvarı uygulamalarını (Windows Vista, Windows XP SP2 ve Windows Server 2003 tarafından sağlanan Internet Connection Firewall (ICF) dahil) kaldırmanızı veya devre dışı bırakmanızı önerir. Ancak ICF'yi veya başka bir üçüncü taraf güvenlik duvarını çalıştırmak istiyorsanız, Trend Micro Security Server dinleme bağlantı noktalarını güvenlik duvarının istisna listesine ekleyin (güvenlik duvarları hakkında bilgi için *Bağlantı Noktaları*, sayfa 2-21 bölümüne, istisna listelerinin nasıl yapılandırılacağı konusunda ayrıntılar için de güvenlik duvarınızın belgelerine bakın).

Dağıtım Denetim Listesi

WFBS ürününü dağıtmadan önce aşağıdakileri gözden geçirin.

Security Server'ın Nereye Yükleneceğini Belirleme

WFBS, çeşitli ağ ortamlarına uyum sağlayacak esnekliğe sahiptir. Örneğin, Trend Micro Security Server ile Client/Server Security Agent çalıştıran istemciler arasına bir güvenlik duvarı yerleştirebilir veya hem Trend Micro Security Server'ı hem de tüm istemcileri tek bir ağ güvenlik duvarının arkasına yerleştirebilirsiniz.

Birden fazla siteyi yönetiyorsanız, hem ana sitede hem de yönetilen sitelerin her birinde bir güvenlik sunucusu bulunması, ana site ile yönetilen siteler arasında bant genişliği kullanımını azaltır ve desen dağıtımı hızlarını artırır.

İstemcilerin Windows Güvenlik Duvarı etkinse, WFBS, bu Güvenlik Duvarı'nı otomatik olarak İstisna listesine ekler.

Not: Trend Micro Security Server ile istemcileri arasında bir güvenlik duvarı bulunuyorsa, istemcinin dinleme bağlantı noktası ile Trend Micro Security Server'ın dinleme bağlantı noktası arasında trafik akışına izin vermek için güvenlik duvarını yapılandırmanız gerekir.

İstemci Sayısını Tanımlama

İstemci, Client/Server Security Agent yüklemeyi planladığınız bir bilgisayardır. Bu, evden çalışan kişilere ait olanlar dahil olmak üzere masaüstü bilgisayarları, sunucuları ve taşınabilir bilgisayarları içerir.

Ağınızda Windows 2000, XP, Server 2003 veya Vista gibi farklı Windows işletim sistemleri bulunuyorsa, belirli bir Windows sürümünün kullandığı istemci sayısını belirleyin. Ortamınızda hangi istemci dağıtımı yönteminin en iyi sonucu vereceğini belirlemek için bu bilgileri kullanın. Bkz. *Aracılar İçin Dağıtım Seçenekleri Belirleme*, sayfa 2-29.

Not: Yüklenen tek bir Security Server, 2500 istemciyi yönetebilir. İstemci sayınız daha fazlaysa, Trend Micro, birden fazla Security Server yüklemenizi önerir.

Ağ Trafiği İçin Planlama

Dağıtım planlaması yaparken, WFBS tarafından oluşturulacak ağ trafiğini göz önünde bulundurun. Security Server ve istemciler birbirleriyle iletişim kurduğunda, WFBS ağ trafiği üretir.

Security Server/Tarama Sunucusu aşağıdaki durumlarda trafik üretir:

- İstemcileri yapılandırma değişikliklerinden haberdar etme
- İstemcileri güncellenen bileşenlerini indirmeleri için uyarma
- Güncellenen bileşenleri kontrol etmek ve indirmek için Trend Micro ActiveUpdate Server'a bağlanma
- Smart Scan için yapılandırılmış istemciler üzerinde tarama gerçekleştirme
- Trend Micro Smart Protection Network'e geribildirim gönderme

İstemciler aşağıdaki durumlarda trafik üretir:

- Başlangıç
- Kapanış
- Günlük oluşturma
- Dolaşım modu ile normal arasında geçiş yapma
- Zamanlanmış güncellemeler gerçekleştirme
- El ile güncellemeler gerçekleştirme ("Şimdi Güncelle")
- Smart Scan için Tarama Sunucusuna bağlanma

Not: Güncellemeler dışında tüm diğer eylemler az miktarda trafik üretir.

Desen Dosyası Güncellemeleri Sırasında Ağ Trafiği

Trend Micro herhangi bir ürün bileşeninin güncellenmiş sürümünü yayınladığında önemli miktarda ağ trafiği üretilir.

Desen dosyası güncellemeleri sırasında üretilen ağ trafiğini azaltmak için, WFBS, artırımlı güncelleme adı verilen bir yöntem kullanır. Trend Micro Security Server, her defasında tam güncellenmiş desen dosyasını indirmek yerine, yalnızca son sürümün ardından eklenen yeni desenleri indirir. Trend Micro Security Server, yeni desenleri eski desen dosyasıyla birleştirir.

Düzenli olarak güncellenen istemcilerin yalnızca yaklaşık boyutu 5 KB ile 200 KB arasında olan artırımlı deseni indirmesi gerekir. Tam desen, sıkıştırıldığında yaklaşık 20 MB'dir ve indirilmesi çok daha uzun sürer.

Trend Micro her gün yeni desen dosyalarını kullanıma sunar. Ancak, çok zararlı vir virüsün aktif olarak dolaşımda olduğu durumlarda, Trend Micro, tehdidin deseni belirlenir belirlenmez yeni bir desen dosyasını kullanıma sunar.

Ağ Bant Genişliğini Azaltmak İçin Güncelleme Aracılarını Kullanma

İstemciler ve Security Server arasında ağınızın "düşük bant genişliği" veya "ağır trafik" olarak tanımladığınız bölümleri varsa, diğer istemciler için güncelleme kaynağı (Güncelleme Aracıları) görevini üstlenecek istemciler belirleyebilirsiniz. Bu, bileşenleri tüm istemcilere dağıtma yükünü paylaştırmaya yardımcı olur.

Örneğin, ağınız konuma göre kesimliyse ve kesimler arasındaki ağ bağlantısı ağır trafik yüküyle karşılaşıyorsa, Trend Micro, her kesimde Güncelleme Aracısı görevini üstlenmesi için en az bir istemciye izin vermenizi önerir.

Ayrılmış Bir Sunucu Belirleme

WFBS ürününü barındıracak bir sunucu seçerken aşağıdakileri göz önünde bulundurun:

- Sunucunun taşıdığı CPU yükü nedir?
- Sunucunun diğer işlevleri nelerdir?

Başka amaçlarla da kullanılan bir sunucuya (örneğin uygulama sunucusuna) WFBS ürününü yüklemeyi düşünüyorsanız, Trend Micro, görev kritik veya kaynak kullanımı yoğun uygulamaları tercih etmemenizi önerir.

Program Dosyalarının Konumu

Trend Micro Security Server yüklenirken, program dosyalarının istemciler üzerinde hangi konuma yükleneceğini belirtin. Varsayılan istemci yükleme yolunu kabul edin veya değiştirin. Trend Micro, bu ayarları değiştirmek için önemli bir neden (disk alanının yeterli olmaması gibi) olmadıkça varsayılan ayarları kullanmanızı önerir.

Varsayılan istemci yükleme yolu:

```
C:\Program Files\Trend Micro\Security Server Agent
```

Masaüstü Bilgisayar ve Sunucu Grubu Sayısını Belirleme

Her Client/Server Security Agent, bir güvenlik grubuna ait olmalıdır. Bir güvenlik grubunun tüm üyeleri, aynı yapılandırmaya sahiptir ve aynı görevleri gerçekleştirir. İstemcileri gruplar halinde düzenleyerek, diğer grupların yapılandırmasını etkilemeden tek bir grubu eşzamanlı olarak yapılandırabilir, yönetebilir ve özelleştirilmiş bir yapılandırma uygulayabilirsiniz.

WFBS güvenlik grubu, bir Windows etki alanından farklıdır. Tek bir Windows etki alanı içinde birden çok güvenlik grubu oluşturabilirsiniz. Ayrıca farklı Windows etki alanlarından bilgisayarları aynı güvenlik grubuna atayabilirsiniz. Tek koşul, bir gruptaki tüm istemcilerin aynı Security Server'a kayıtlı olmasıdır.

İstemcileri ait oldukları gruplara veya gerçekleştirdiklere işlevlere göre gruplandırabilirsiniz. Ya da tehditlerden etkilenme riski daha yüksek olan istemcileri bir araya toplayabilir ve bu istemcilere, diğer istemcilere uyguladığınızdan daha güvenli bir yapılandırma uygulayabilirsiniz. Oluşturmak istediğiniz her benzersiz istemci yapılandırması için en az bir gruba ihtiyacınız olacaktır.

Aracılar İçin Dağıtım Seçenekleri Belirleme

WFBS, Client/Server Security Agent'larını dağıtmak için çeşitli seçenekler sunar. Geçerli yönetim uygulamalarınıza ve son kullanıcılara atanan hesap ayrıcalıklarına bağlı olarak ortamınız için en uygun seçeneklerin hangileri olduğunu belirleyin.

Tek site dağıtımı için, BT yöneticileri Uzaktan Yükleme'yi veya Oturum Açma Komut Dosyası Kurulumu'nu kullanarak dağıtımı tercih edebilirler. Oturum Açma Komut Dosyası Kurulumu yöntemi için, oturum açma komut dosyasına `autopcc.exe` adlı bir program eklenir. Korunmayan bir istemci Windows etki alanında oturum açtığında, Security Server istemciyi algılar ve otomatik olarak istemci kurulumu programını dağıtır. Client/Server Security Agent, arka planda dağıtılır ve son kullanıcı yükleme işlemini fark etmez.

BT ilkelerinin sıkı biçimde uygulandığı organizasyonlarda, Uzaktan Yükleme ve Oturum Açma Komut Dosyası Kurulumu önerilir. Uzaktan yükleme ve oturum açma komut dosyası kurulumları için son kullanıcıya yönetici ayrıcalığı atanması gerekmez. Yönetici, bir yönetici hesabının parolasını kullanarak yükleme programının kendisini yapılandırır. Son kullanıcının izinlerini değiştirmeniz gerekmez.

Not: Uzaktan yükleme yalnızca Windows Vista/2000/XP (yalnızca Professional Edition) ve Server 2003 ile çalışır.

BT politikalarının daha esnek bir şekilde uygulandığı kuruluşlarda, Client/Server Security Agent'ın dahili Web sayfası kullanılarak yüklenmesi önerilir. Yönetici, kullanıcılara Client/Server Security Agent'ı yükleyebilecekler dahili bir Web sayfasını ziyaret etmelerini söyleyen bir e-posta iletisi gönderir. Ancak bu yöntemi kullanmak, Agent'ı yükleyecek son kullanıcıların yönetici ayrıcalığına sahip olmasını gerektirir.

WFBS, WFBS tarafından korunmayan bilgisayarları tespit etmenize yardımcı olabilecek Güvenlik Açığı Tarayıcısı adında bir araç içerir. Güvenlik Açığı Tarayıcısı, korunmayan bir bilgisayarı tespit ettiğinde, o bilgisayara Client/Server Security Agent'ı dağıtır. Bir dizi IP adresi girdiğinizde, Güvenlik Açığı Tarayıcısı, belirtilen aralıktaki tüm bilgisayarları denetler ve her bir bilgisayarda yüklü olan antivirüs yazılımı sürümünü (üçüncü taraf yazılımı dahil) rapor eder.

Not: Güvenlik Açığı Tarayıcısı'nı kullanarak Client/Server Security Agent'ı yüklemek için yönetici haklarına sahip olmanız gerekir. Bu sorunun üstesinden gelmek için, Güvenlik Açığı Tarayıcısı'nın Client/Server Security Agent'ı yüklemek için kullanacağı yönetici düzeyinde oturum açma kimlik bilgileri sağlayabilirsiniz.

Bir WFBS aracı olan Client Packager, e-posta iletisi, CD-ROM veya dahili bir FTP aracılığıyla kolayca gönderilebilmesi için kurulum ve güncelleme dosyalarını kendiliğinden ayıklanan bir dosya içine sıkıştırabilir. Kullanıcılar paketi aldıklarında, dosyayı çift tıklatarak kurulum programını başlatabilirler.

İpucu: Uzaktan Yükleme, Active Directory kullanan ağlar için etkilidir. Ağınız Active Directory kullanmıyorsa Web yüklemesini tercih edin.

Yükleme yöntemleri hakkında daha fazla bilgi için WFBS *Yönetici Kılavuzu*'na bakın.

Bağlantı Noktaları Denetim Listesi

WFBS, aşağıdaki varsayılan bağlantı noktalarını kullanmaktadır.

TABLO 2-8. Bağlantı Noktası Denetim Listesi

PORT	ÖRNEK	DEĞERINIZ
SMTP	25	
Proxy	Yönetici Tanımlı	
Security Server: SSL Olmayan Bağlantı Noktası	8059	
Security Server: SSL Bağlantı Noktası	4343	
Client/Server Security Agent	21112	
Messaging Security Agent	16372	
Tarama Sunucusu SSL Bağlantı Noktası	4345	
Tarama Sunucusu SSL Olmayan Bağlantı Noktası	8082	

Security Server Adres Kontrol Listesi

WFBS, yükleme ve yapılandırma sırasında aşağıdaki bilgileri gerektirir. Kolay başvuru için aşağıdaki ayrıntıları kaydedin.

TABLO 2-9. Sunucu Adresi Kontrol Listesi

GEREKLI BILGI	ÖRNEK	DEĞERINIZ
TREND MICRO SECURITY SERVER BILGISI		
IP adresi	192.168.1.1	
Tam Etki Alanı Adı (FQDN)	server.company.com	
NetBIOS (ana bilgisayar) adı	sunucunuz	
WEB SUNUCUSU BILGISI		
IP adresi	192.168.1.1	
Tam Etki Alanı Adı (FQDN)	server.company.com	
NetBIOS (ana bilgisayar) adı	sunucunuz	
BILEŞEN INDIRMEK IÇIN PROXY SUNUCUSU		
IP adresi	192.168.1.1	
Tam Etki Alanı Adı (FQDN)	proxy.company.com	
NetBIOS (ana bilgisayar) adı	proxysunucusu	
SMTP SUNUCU BILGISI (İSTEĞE BAĞLI; E-POSTA BILDIRIMLERI IÇIN)		
IP adresi	192.168.1.1	
Tam Etki Alanı Adı (FQDN)	mail.company.com	
NetBIOS (ana bilgisayar) adı	postasunucusu	

TABLO 2-9. Sunucu Adresi Kontrol Listesi (Devamı)

GEREKLI BILGI	ÖRNEK	DEĞERINIZ
SNMP YAKALAMA BILGISI (İSTEĞE BAĞLI; SNMP YAKALAMA BILDIRIMLERI IÇIN)		
Topluluk adı	şirket	
IP adresi	192.168.1.1	

Bölüm 3

Sunucuyu Yükleme

Bu bölümde, WFBS'nın nasıl yükleneceğini anlamak için ihtiyacınız olan bilgiler verilmektedir.

Bu bölümde ele alınan başlıklar şunlardır:

Yüklemeye Genel Bakış

WFBS'yı yüklemenin üç yöntemi vardır:

- **Tipik:** Trend Micro varsayılan değerlerini kullanarak basit ve kolay bir WFBS yükleme çözümü sağlar. Bu yöntem, tek bir Trend Micro Security Server ve en fazla on istemci kullanan küçük ölçekli bir işletme için uygundur.
- **Özel:** Ağ güvenlik stratejinizi uygulamada esneklik sağlar. Bu yöntem, çok fazla bilgisayarınız ve sunucunuz .
- **Sessiz:** Sessiz yükleme gerçekleştirmeniz, diğer bilgisayar ve ağlarda aynı yüklemeleri gerçekleştirmek üzere kullanabileceğiniz bir kayıt dosyası oluşturur.

İpucu: WFBS'nın bu sürümüne yükselttiğinizde veya WFBS'nın bu sürümünü yeniden yüklemeniz gerekiyorsa istemci ayarlarınızı koruyabilirsiniz. Talimatlar için bkz. *Client/Server Security Agent'ı Yükseltme, sayfa 4-11*, sayfa 4-1.

Not: İstemcide önceki MSA yüklemesinden bilgi varsa, MSA'yı başarıyla yükleyemezsiniz. Önceki yüklemenin kalıntılarını temizlemek için Windows Installer Temizleme Yardımcı Programı'nı kullanın. Windows Installer Temizleme Yardımcı Programı'nı indirmek için şu adresi ziyaret edin:
http://support.microsoft.com/kb/290301/en-us

Tarama Sunucusunu Yükleme

WFBS sunucusunu yüklediğinizde, Tarama Sunucusu otomatik olarak yüklenir. Tarama Sunucusunu yüklemeyi seçmenize veya herhangi bir ayarı yapılandırmanıza gerek yoktur.

Normal Yüklemeyi Gözden Geçirme

Normal Yükleme yöntemi, Özel yükleme yöntemiyle aynı akışı izler (bkz. *Özel Yüklemeyi Gözden Geçirme*, sayfa 3-4). Normal yükleme sırasında, aşağıdaki seçenekler Trend Micro varsayılan ayarlarını kullandıkları için kullanılabilir değildir:

- **WFBS program klasörü.** `C:\Program Files\Trend Micro\Security Server\PCCSRV`
- **Web sunucusu:** Microsoft Internet Information Services (IIS)

  Not: Security Server (Smart Scan hizmeti de dahil olmak üzere) Windows XP üzerine yüklenirse, Microsoft IIS Smart Scan hizmetiyle yalnızca maksimum 10 istemci bağlantısını destekleyebilir. İstemciler Smart Scan'i kullanacaksa ve Security Server Windows XP üzerine yüklüyse, IIS yerine Apache Web sunucusunu seçin.

- **Web sunucusu ayarları**
  - **Web Sitesi:** OfficeScan
  - **Varsayılan URL:** `https://<IP_ADRESİ>:4343/SMB`
- **Client/Server Security Agent ayarları:** Bilgi için WFBS *Yönetici Kılavuzu*'na başvurun.

Normal yöntemi kullanarak yükleme gerçekleştirmek için, Özel Yükleme ile ilgili adımları göz ardı ederek *Özel Yüklemeyi Gözden Geçirme*, sayfa 3-4 dahilindeki adımları izleyin.

Özel Yüklemeyi Gözden Geçirme

Özel Yükleme yöntemi, ağ güvenlik stratejinizi uygulamada en büyük esnekliği sunar. Özel ve Normal yükleme işlemleri benzer bir akış izler:

1. Önceden yapılandırma görevlerini gerçekleştirin. Bkz. *Bölüm 1: Önceden Yapılandırma Görevleri*, sayfa 3-4.
2. Trend Micro Security Server ve Web konsolu için ayarları girin. Bkz. *Bölüm 2: Sunucu ve Web Konsolu Ayarları*, sayfa 3-10.
3. Client/Server Security Agent seçeneklerini yapılandırın. Bkz. *Bölüm 3: Aracı Yükleme Seçenekleri*, sayfa 3-23.
4. Yükleme işlemini başlatın. Bkz. *Bölüm 4: Yükleme İşlemi*, sayfa 3-28.
5. **İsteğe bağlı.** Uzak Exchange sunucuları için Remote Messaging Security Agent yükleme seçeneğini yapılandırın. Bkz. *Bölüm 5: Remote Messaging Security Agent Yüklemesi*, sayfa 3-29.

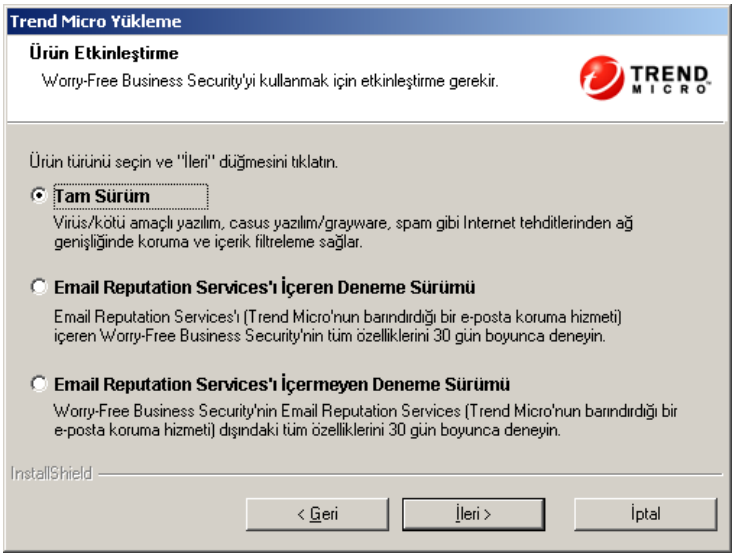
Bölüm 1: Önceden Yapılandırma Görevleri

Önceden yapılandırma görevleri; yükleme sihirbazını başlatma, lisans ve etkinleştirme ayrıntılarını sağlama, sunucuda önceden virüs taraması yapma ve yükleme türü seçmeden oluşur.

İpucu: WFBS'yı yüklemeden önce çalışan tüm uygulamaları kapatın. Diğer uygulamalar çalışırken yükleme yaparsanız, yükleme işleminin tamamlanması daha uzun sürebilir.

Önceden yapılandırma görevlerini başlatmak için:

1. Kurulum dosyalarını içeren klasörü açın ve `SETUP.EXE` dosyasını çift tıklatın. **Trend Micro Yükleme**ekranı görünür.
2. **İleri**'yi tıklatın. **Lisans Sözleşmesi** ekranı görünür.
3. Lisans sözleşmesini okuyun. Koşulları kabul ediyorsanız, **Lisans sözleşmesinin koşullarını kabul ediyorum**.
4. **İleri**'yi tıklatın. **Ürün Etkinleştirme** ekranı görünür.



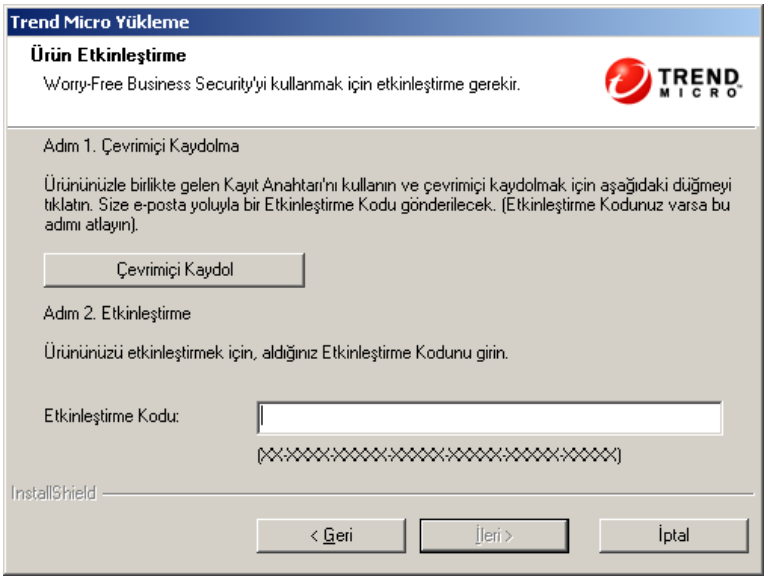
ŞEKIL 3-1. Ürün Etkinleştirme ekranı

5. **Ürün Etkinleştirme** ekranından, aşağıdaki seçeneklerden birini seçin ve **İleri**'yi tıklatın:
   - **Tam Sürüm**
   - **Email Reputation Services'ı İçeren Deneme Sürümü:** Email Reputation Services hakkında daha fazla bilgi edinmek için,

     http://us.trendmicro.com/us/products/enterprise/network-reputation-services/

     adresine başvurun.
   - **Email Reputation Services'ı İçermeyen Deneme Sürümü**

Not: Tam sürümü ve Email Reputation Services'ı içeren deneme sürümünü yüklemek için bir Etkinleştirme Koduna veya Kayıt Anahtarına ihtiyacınız vardır.



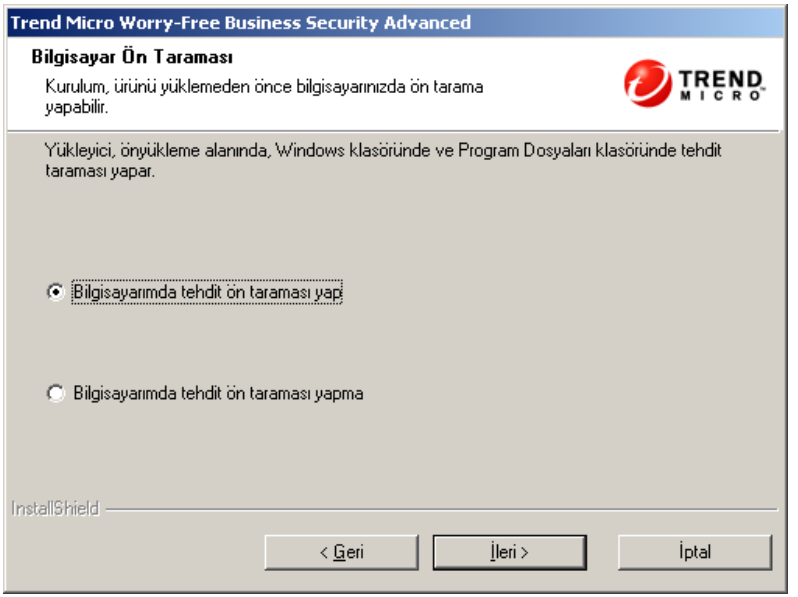
ŞEKIL 3-2. Ürün Etkinleştirme ekranı

6. WFBS henüz kayıtlı değilse **Çevrimiçi Kaydolma**'yı tıklatın. Bir tarayıcı penceresi açılır. **Kayıt** ekranındaki yönergeleri izleyin.
7. Etkinleştirme Kodunu **Etkinleştirme Kodu** alanına girin.

Not: **Etkinleştirme Kodunuz** yoksa, deneme sürümünü yüklemek için **İleri**'yi tıklatın. 30 günlük deneme süreniz dolmadan önce tam sürüme yükseltin, böylece tüm ayarlar korunacaktır.

---

8. **İleri**'yi tıklatın. **Bilgisayar Ön Taraması** ekranı görünür.

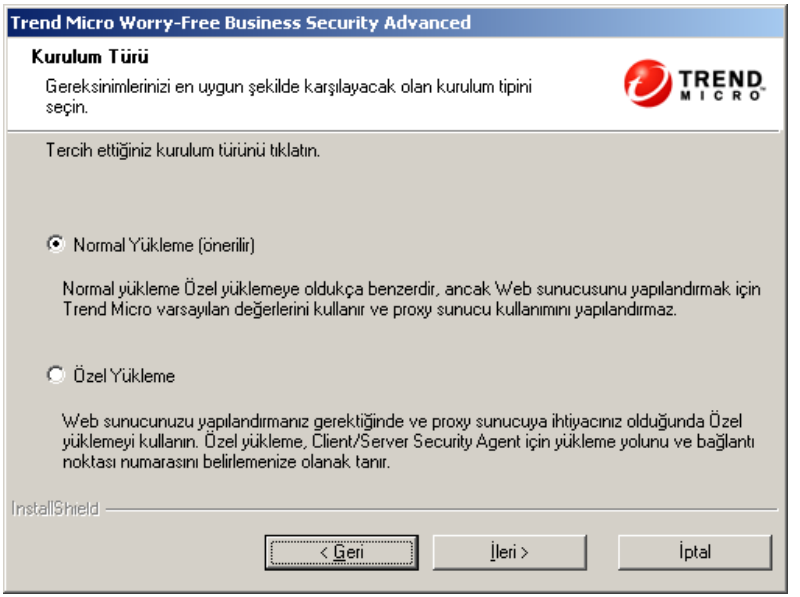


ŞEKIL 3-3. Bilgisayar Ön Taraması ekranı

9. Aşağıdaki seçeneklerden birini belirleyerek bilgisayarınızda tehditler için ön tarama yapılıp yapılmayacağını seçin:
   - **Bilgisayarımda tehditler için ön tarama yap**
   - **Bilgisayarımda tehditler için ön tarama yapma**
   - Trend Micro, güvenlik tehditleri nedeniyle bilgisayarınızda ön tarama yapmanızı önemle önerir. Bilgisayarda ön tarama yapmamak başarılı yüklemeyi engelleyebilir.

Not: Bilgisayarınızda tehditler için ön tarama yapmayı seçerseniz, tarama gerçekleştirilirken bir tehdit ilerlemesi ekranı görünecektir.

10. **İleri**'yi tıklatın. **Kurulum Türü** ekranı görünür.



ŞEKIL 3-4. Kurulum Türü ekranı

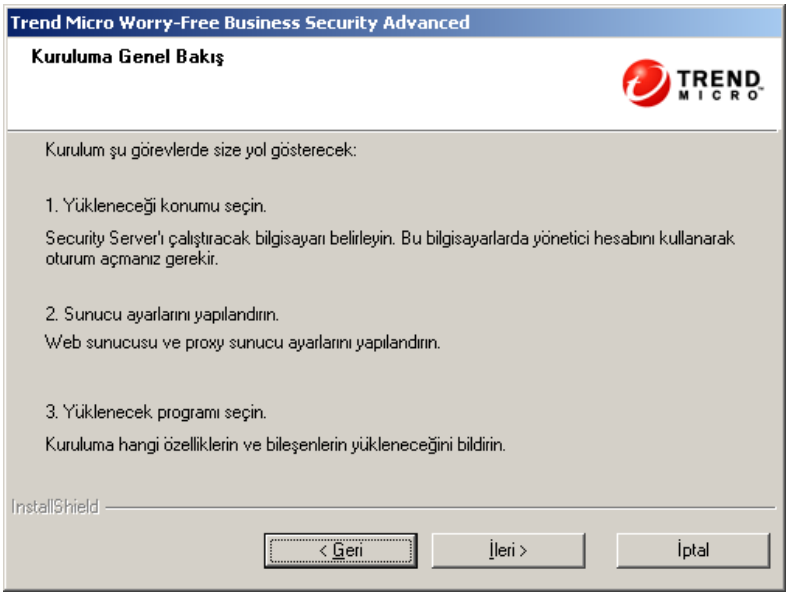
11. **Kurulum Türü** ekranından, şu seçeneklerden birini belirleyin:
    - **Normal yükleme (önerilir)**
    - **Özel yükleme**

    Farklılıklar için, bkz. *Yüklemeye Genel Bakış*, sayfa 3-2.

    Not: Normal ve Özel yükleme için varsayılan değerler aynıdır.

12. **İleri**'yi tıklatın. **Kuruluma Genel Bakış** ekranı görünür.

    Bu, tüm yükleme öncesi görevlerini tamamlar.



ŞEKIL 3-5. Yükleme Kurulumuna Genel Bakış ekranı

13. **Kuruluma Genel Bakış** ekranı; Trend Micro Security Server'ı, Web konsolunu, Messaging Security Agent ve Client/Server Security Agent'ı yüklemek için tamamlamanız gereken görevleri kısaca listeler.

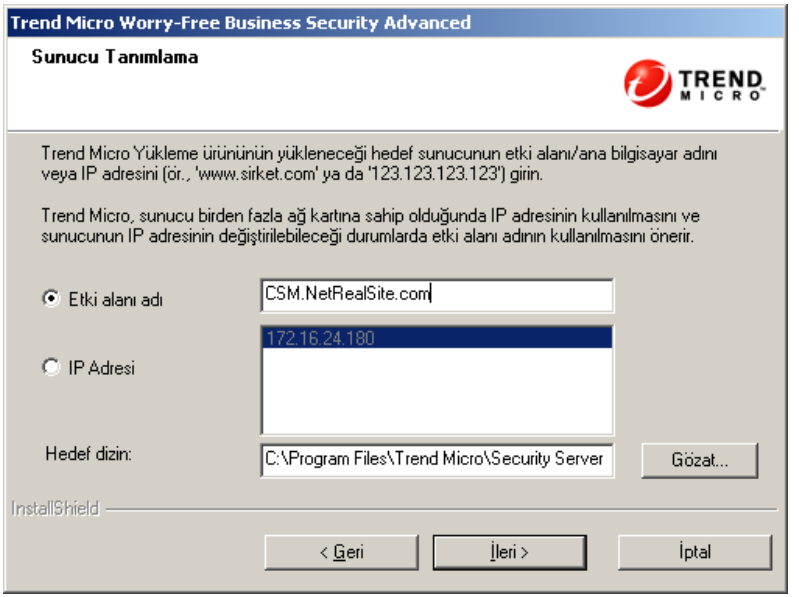
Bölüm 2: Sunucu ve Web Konsolu Ayarları

Security Server'ı ve Web konsolunu yapılandırmak için:

1. **Kuruluma Genel Bakış** ekranından, **İleri**'yi tıklatın. Security Server simgesi vurgulanmış şekilde **Yükleme Aşaması** ekranı görünür.

ŞEKIL 3-6. Security Server Yükleme Aşaması ekranı

2. **İleri**'yi tıklatın. **Sunucu Tanımlama** ekranı görünür.

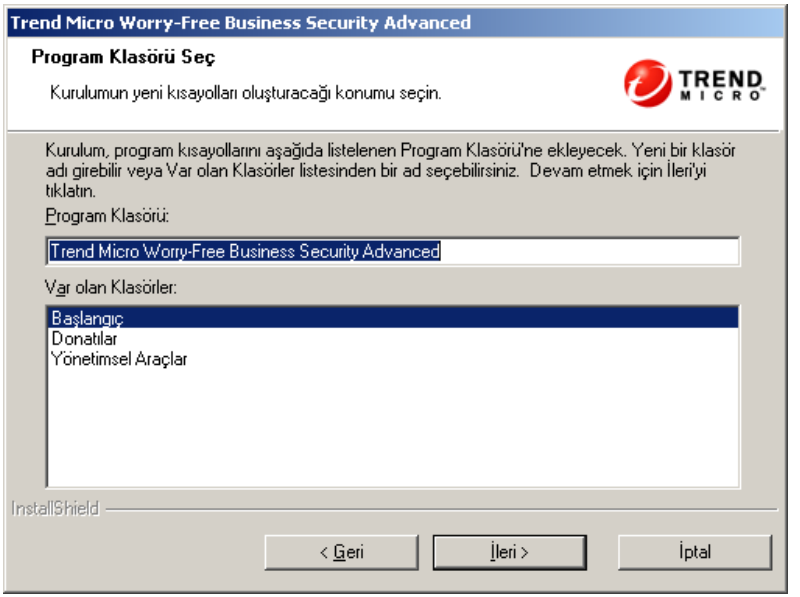


ŞEKIL 3-7. Sunucu Tanımlama ekranı

3. İstemci-sunucu iletişimi için aşağıdaki sunucu tanımlama seçeneklerinden birini belirleyin:
   - **Sunucu bilgileri:** Etki Alanı adını veya IP adresini seçin:
     - **Etki alanı adı:** Hedef sunucunun etki alanı adını doğrulayın. Başarılı bir istemci-sunucu iletişimi sağlamak için gerekirse sunucunun tam etki alanını (FQDN) da kullanabilirsiniz.
     - **IP adresi:** Hedef sunucunun IP adresinin doğru olduğunu doğrulayın.

     İpucu: Bir IP adresi kullanırken, Security Server'ı yüklediğiniz bilgisayarın statik bir IP adresi olduğundan emin olun. Sunucu, birden fazla ağ arayüzü kartına (NIC'ler) sahipse, Trend Micro, IP adresi yerine etki alanı adının veya FQDN'nin kullanılmasını önerir.

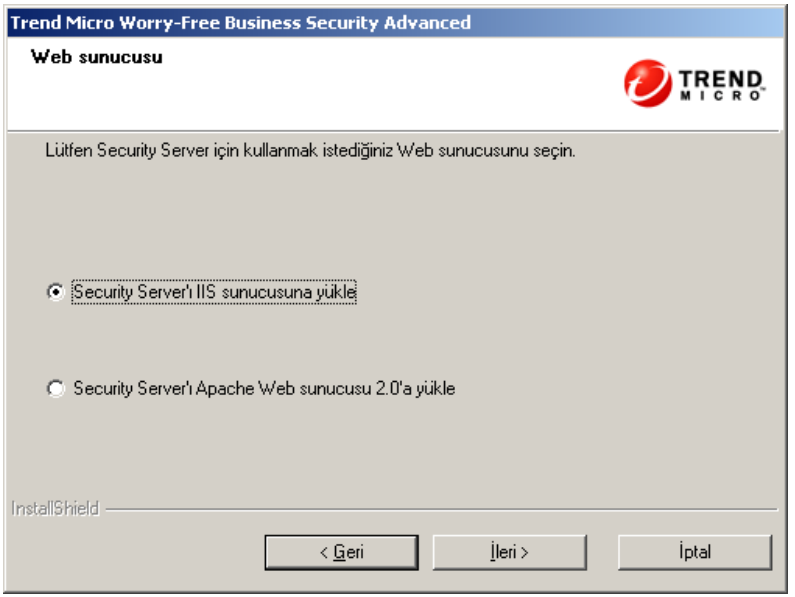
   - **Hedef dizin.** Trend Micro Security Server'ın yükleneceği hedef dizini belirtin.
4. **İleri**'yi tıklatın. **Program Klasörü Seç** ekranı görünür.



ŞEKIL 3-8. Program Klasörü Seç ekranı

Not: Normal yükleme yöntemini seçerseniz bu ekran görünmeyecektir.

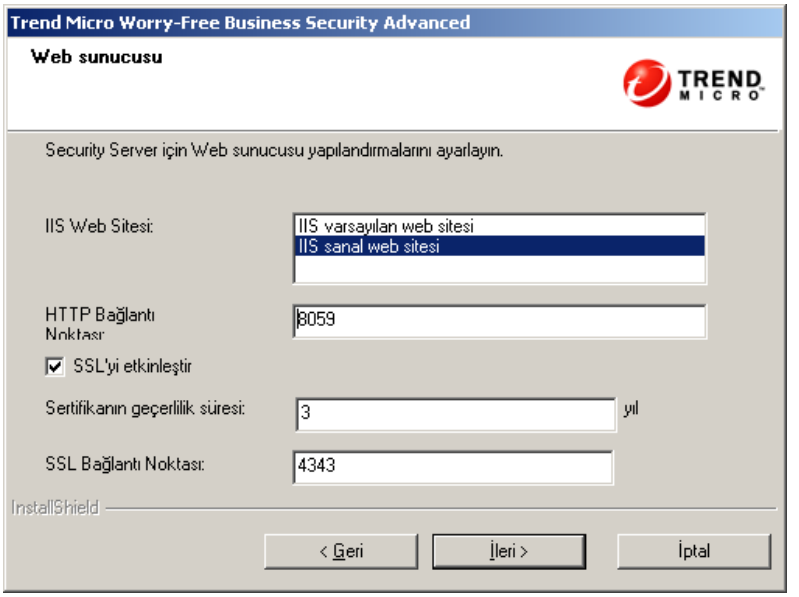
5. Program kısayollarının saklanacağı **Program klasörü** alanına bir konum girin veya varsayılan konumu kullanın.
6. **İleri**'yi tıklatın. Bir Web sunucusu seçmenize olanak tanıyan **Web Sunucusu** ekranı görünür.



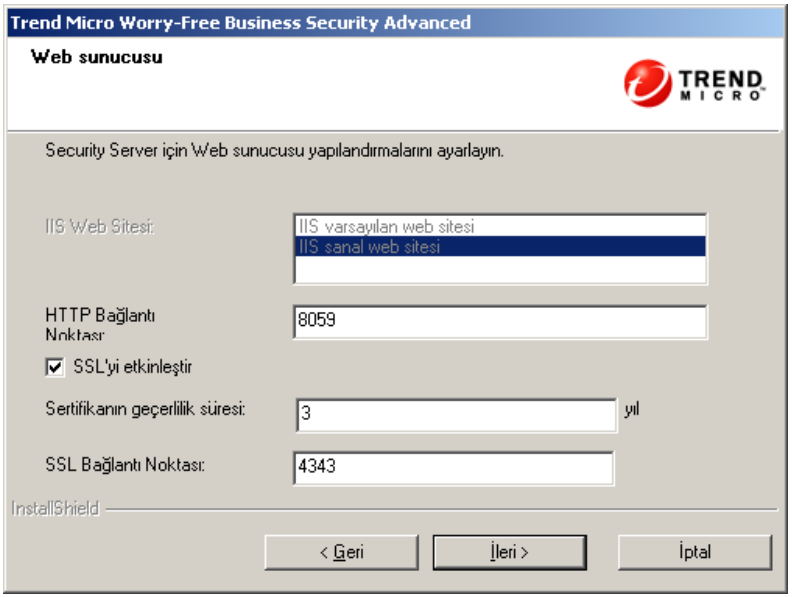
ŞEKIL 3-9. Web Sunucusu ekranı

Not: Normal yükleme yöntemini seçerseniz bu ekran görünmeyecektir.

7. **Web Sunucusu** ekranından, Web konsolunun barındırılacağı bir Web sunucusu seçin. Aşağıdakilerden birini seçin:
   - IIS sunucusu
   - Apache Web sunucusu
8. **İleri**'yi tıklatın. Seçilen sunucuya bağlı olarak, karşılık gelen ekran görünür.



ŞEKIL 3-10. IIS Web Sunucusu Yapılandırma ekranı



ŞEKIL 3-11. Apache Web Sunucusu Yapılandırma ekranı

Not: Normal yükleme yöntemini seçerseniz bu ekran görünmeyecektir.

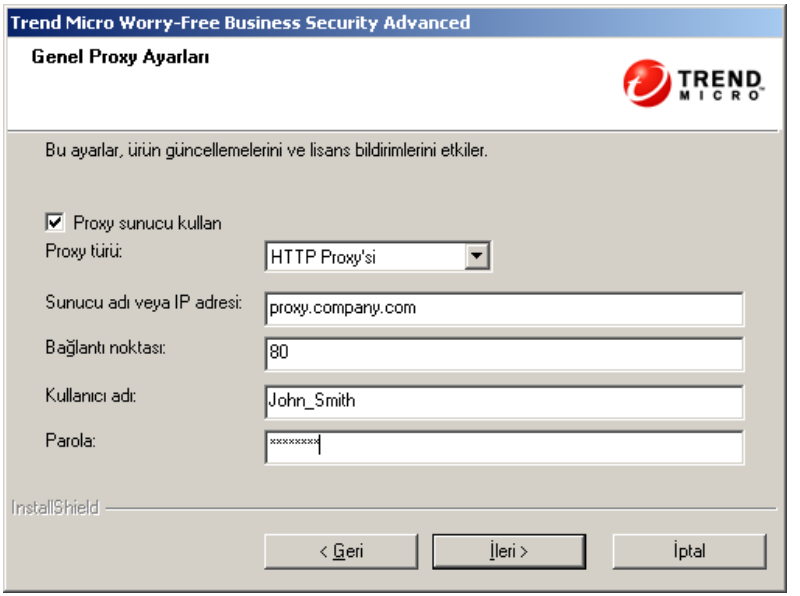
---

9. Aşağıdaki Web sunucusu ayarlarını yapılandırın:
   - **HTTP bağlantı noktası**
   - **SSL'yi etkinleştir**
   - **Sertifikanın geçerlilik süresi**
   - **SSL bağlantı noktası**

Not: IIS sunucusu kullanılıyorsa, **sanal** veya **varsayılan** bir IIS Web sitesi belirtmeniz gerekir. WFBS, ISS varsayılan Web sitesinin kullanımı için HTTP ve SSL bağlantı noktası ayarlarına varsayılan değerler atayacaktır.

---

10. **İleri**'yi tıklatın. **Proxy Sunucu** ekranı görünür.



ŞEKIL 3-12. Proxy Sunucu ekranı

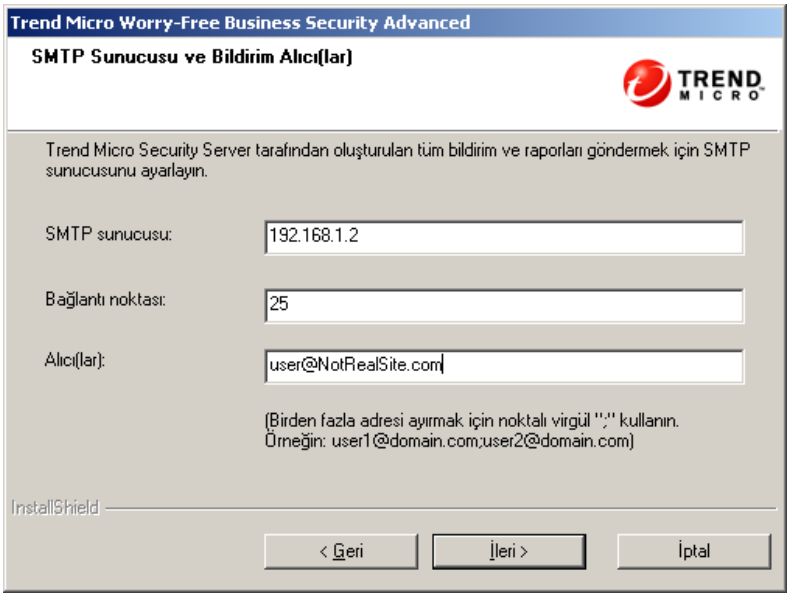
Not: Normal yükleme yöntemini seçerseniz bu ekran görünmeyecektir.

11. Proxy sunucunun Internet'e erişim sağlaması gerekliyse, **Proxy sunucu kullan** onay kutusunu işaretleyin ve aşağıdaki bilgileri verin:
    - **Proxy türü**
    - **Sunucu adı veya IP adresi**
    - **Port**
    - **Kullanıcı adı:** Yalnızca, sunucu kimlik doğrulaması gerektiriyorsa sağlayın.
    - **Parola:** Yalnızca, sunucu kimlik doğrulaması gerektiriyorsa sağlayın.

12. **İleri**'yi tıklatın. Web Reputation ve Behavior Monitoring için proxy sunucu ayarları ekranı görünür.

    Bu istemci hizmetleri, Internet Explorer'da belirtilen proxy sunucuyu ve bağlantı noktasını kullanır. Söz konusu proxy sunucu kimlik doğrulaması gerektiriyorsa, oturum açma kimlik bilgilerini belirtmek için bu ekranı kullanın.

13. **İleri**'yi tıklatın. **SMTP Sunucusu ve Bildirim Alıcı(lar)** ekranı görünür.



ŞEKIL 3-13. SMTP Sunucusu ve Bildirim Alıcı(lar) ekranı

14. **SMTP Sunucusu ve Bildirim Alıcı(lar)** ekranı şu bilgileri gerektirir:
    - **SMTP sunucusu**: posta sunucusu
    - **Port**
    - **Alıcı(lar)**

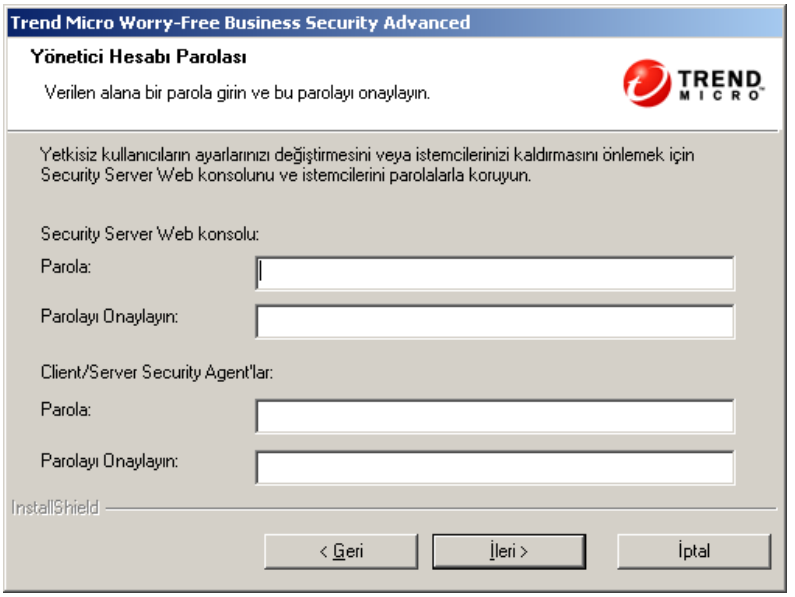
Not: SMTP sunucusu (posta sunucusu), WFBS ile aynı bilgisayardaysa ve bağlantı noktası 25'i kullanıyorsa, yükleme programı SMTP sunucusunun adını algılar ve **SMTP Sunucusu** ve **Bağlantı Noktası** alanlarını günceller.

ISP posta sunucusu ayarlarınıza başvurun. Bu ayarları bilmiyorsanız, sonraki adıma geçin. Bu ayarlar başka zaman yapılandırılabilir.

İpucu: SMTP ayarlarını yüklemeden sonra güncelleyebilirsiniz. Yönergeler için Yönetici Kılavuzu'na başvurun.

---

15. **İleri**'yi tıklatın. **Yönetici Hesabı Parolası** ekranı görünür.

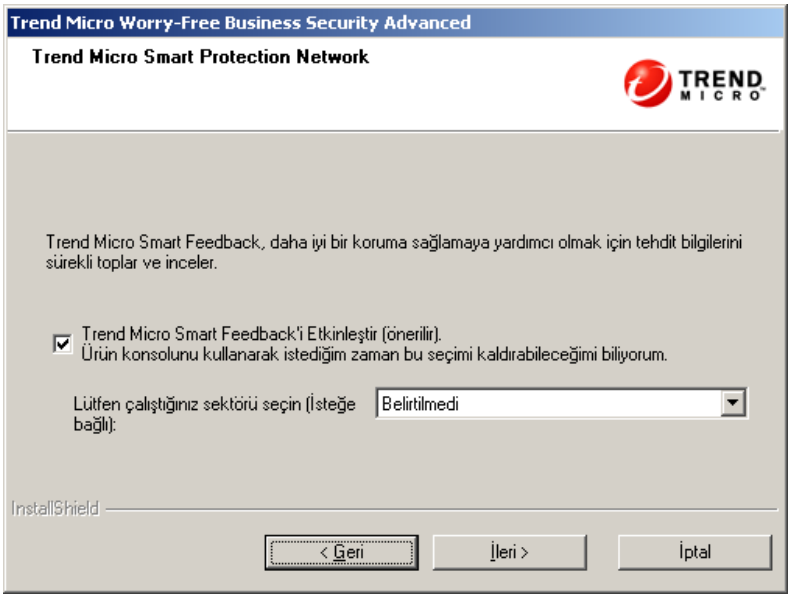


ŞEKIL 3-14. Yönetici Hesabı Parolası ekranı

16. **Yönetici Hesabı Parolası** ekranı aşağıdaki bilgileri gerektirir:
    - **Security Server Web konsolu:** Web konsolunda oturum açma gereklidir.
        - **Parola**
        - **Parolayı onaylayın**
    - **Client/Server Security Agent'lar:** Client/Server Security Agent'ların kaldırılması gereklidir.
        - **Parola**
        - **Parolayı onaylayın**

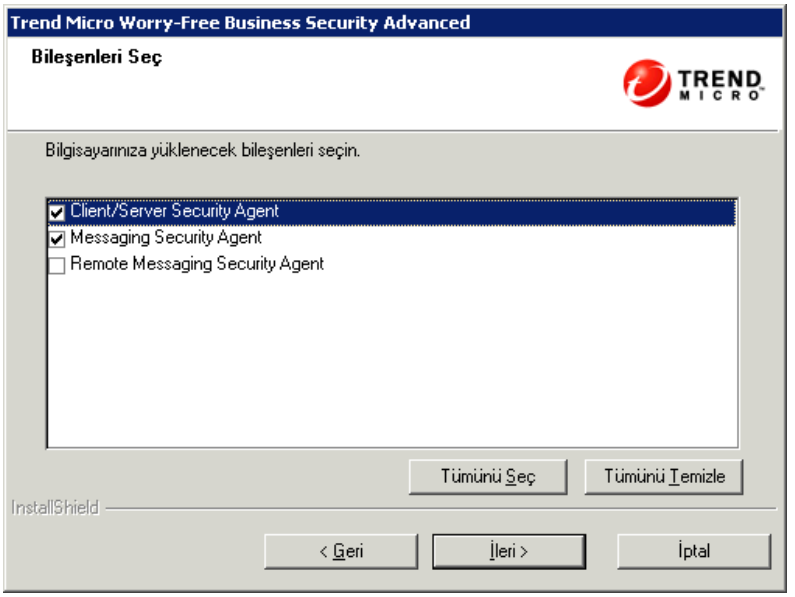
    Not: Parola alanı, 1–24 karakter içerir ve büyük/küçük harf duyarlıdır.

17. **İleri**'yi tıklatın. **Trend Micro Smart Protection Network** ekranı görünür.



ŞEKIL 3-15. Trend Micro Smart Protection Network ekranı

18. Trend Micro Smart Protection Network geribildirim programına katılıp katılmayacağınızı seçin. Daha sonra Web konsolu aracılığıyla katılımı iptal etmeyi seçebilirsiniz.
19. **İleri**'yi tıklatın. **Bileşen Seçimi** ekranı görünür.



ŞEKIL 3-16. Bileşen Seçimi ekranı

20. Aşağıdakilerden birini seçin:
    - **Client/Server Security Agent:** masaüstü bilgisayarları/sunucuları koruyan aracı
    - **Messaging Security Agent:** Microsoft Exchange sunucularını (yerel olarak bu bilgisayarda yüklü) koruyan aracıdır
    - **Remote Messaging Security Agent:** diğer Microsoft Exchange sunucularını (bu uzaktan yükleme gerçekleştirecektir) koruyan aracıdır

---

Not: İlk MSA yükleme seçeneği (yerel yükleme), yalnızca Exchange sunucunun desteklenen sürümlerine sahip bilgisayarlarda kullanılabilir olacaktır. Bu seçenek kullanılabilir değilse, Microsoft Exchange Bilgi Deposu hizmetinin başlatıldığından ve bilgisayarda Microsoft Forefront Security for Exchange Server'ın (Forefront) yüklü olmadığından emin olun.

---

21. **İleri**'yi tıklatın. Messaging Security Agent simgesi vurgulanmış şekilde Messaging Security Agent **Yükleme Aşaması** ekranı görünür.

ŞEKIL 3-17. Messaging Security Agent Yükleme Aşaması ekranı

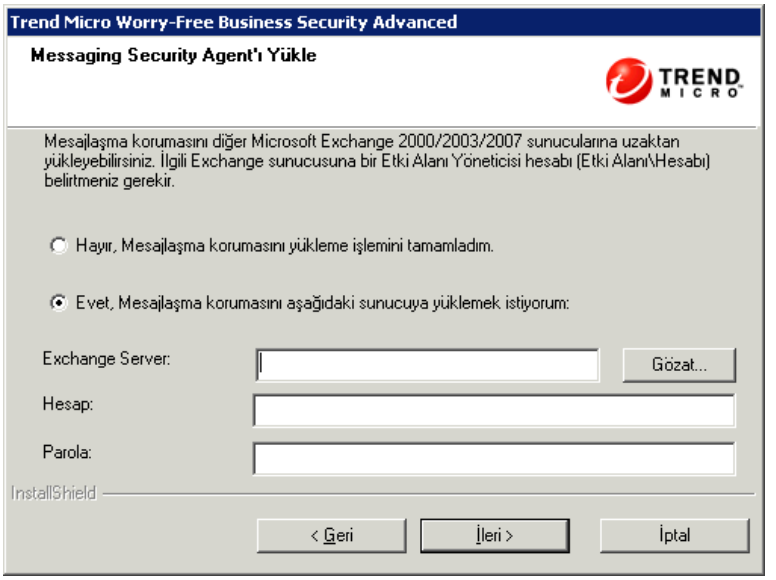
Not: Sunucu üzerinde Exchange sunucusu yoksa, Messaging Security Agent seçeneği kullanılamaz.

Bölüm 3: Aracı Yükleme Seçenekleri

Aşağıdaki seçenekler, Bileşen Seçimi ekranından seçilen bileşenlere bağımlıdır. Örneğin, yedek sunucuda Client/Server Security Agent önceden yüklüyse, Client/Server Security Agent'ı yükleme ve yapılandırma seçeneği görünmeyecektir. Yerel sunucu üzerinde Exchange sunucusu yüklü değilse, Messaging Security Agent'ı yükleme ve yapılandırma seçeneği de kullanılabilir olmayacaktır.

Messaging Security Agent'ları ve Client/Server Security Agent'ları yapılandırmak için:

1. **İleri**'yi tıklatın. Messaging Security Agent**'ı Yükleme** ekranı görünür.

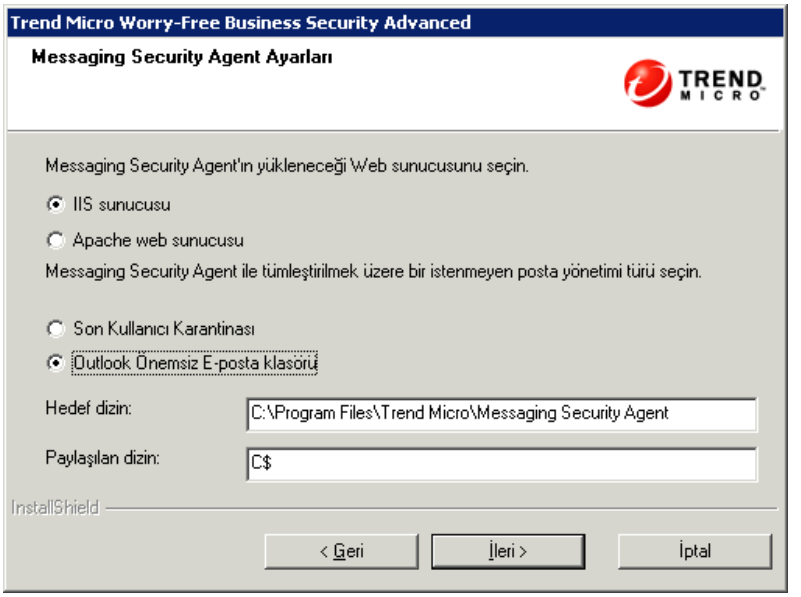


ŞEKIL 3-18. Messaging Security Agent'ı Yükleme ekranı

2. Mesajlaşma korumasını yüklemeyi seçin ve Etki Alanı Yöneticisi hesabı için aşağıdakileri girin:
   - **Exchange Server**
   - **Hesap**
   - **Parola**

Not: Yükleme programı Exchange sunucusunun adını otomatik olarak algılayacak ve Exchange sunucusu Security Server ile aynı bilgisayardaysa **Exchange Server** alanını dolduracaktır.

3. **İleri**'yi tıklatın. **Messaging Security Agent Ayarları** ekranı görünür.



ŞEKIL 3-19. Messaging Security Agent Ayarları ekranı

Not: Normal yükleme yöntemini seçerseniz bu ekran görünmeyecektir.

4. **Messaging Security Agent Ayarları** ekranından, şunları yapılandırın:
   - Web sunucusu
     - **IIS sunucusu**
     - **Apache Web sunucusu**
   - İstenmeyen posta yönetimi
     - **Son Kullanıcı Karantinası:** Seçiliyse, WFBS Microsoft Outlook'ta **Önemsiz E-posta** klasörünün yanı sıra ayrı bir istenmeyen posta klasörü oluşturur.
     - **Outlook Önemsiz E-posta klasörü:** seçiliyse, WFBS istenmeyen postayı bu klasöre kaydeder; Microsoft Outlook **Son Kullanıcı Karantinası** (EUQ) klasöründeki istenmeyen postayı tipik olarak **Önemsiz E-posta** klasörüne taşıdığı için bu seçeneğin belirlenmesi önerilir.

     Not: EUQ ve Önemsiz E-posta klasörü arasında seçim yapma seçeneği, yalnızca, bilgisayar Exchange Server 2003 çalıştırıyorsa kullanılabilir. Önemsiz E-posta özelliği Exchange Server 2000 tarafından desteklenmez. EUQ, Exchange Server 2007'de Önemsiz E-posta özelliğiyle tamamen tümleşir.

   - **Hedef dizin:** Uzak Messaging Security Agent dosyalarının yüklendiği dizin.
   - **Paylaşılan dizin:** Remote Messaging Security Agent yüklemesi için sistem kök dizini.

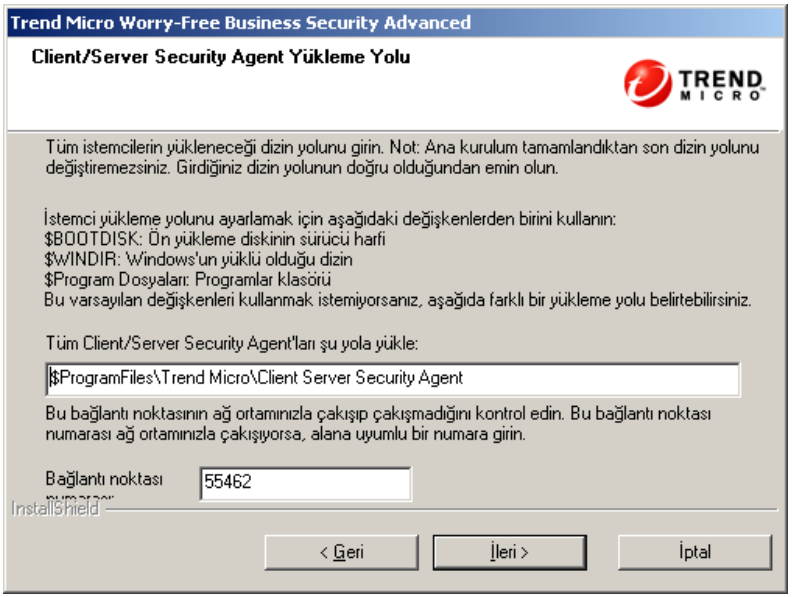
   Not: Security Server ve Messaging Security Agent arasındaki iletişim için Anonim Erişim gereklidir. Yükleme programı Messaging Security Agent için Anonim Erişim Kimlik Doğrulama Yöntemlerini otomatik olarak etkinleştirecektir. Anonim Erişim Kimlik Doğrulama Yöntemlerini görüntülemek için, ISS'de Messaging Security Agent Web sitesi ayarlarına erişin.

5. **İleri**'yi tıklatın. **Client/Server Security Agent Yükleme Aşaması** ekranı, Client/Server Security Agent ve Remote Client/Server Security Agent simgeleri vurgulanmış bir şekilde görünür.

ŞEKIL 3-20. Client/Server Security Agent Yükleme Aşaması ekranı

Not: Normal yükleme yöntemini seçerseniz bu ekran görünmeyecektir.

6. **İleri**'yi tıklatın. **Client/Server Security Agent Yükleme Yolu** ekranı görünür.



ŞEKIL 3-21. Client/Server Security Agent Yükleme Yolu ekranı

Not: Normal yükleme yöntemini seçerseniz bu ekran görünmeyecektir.

---

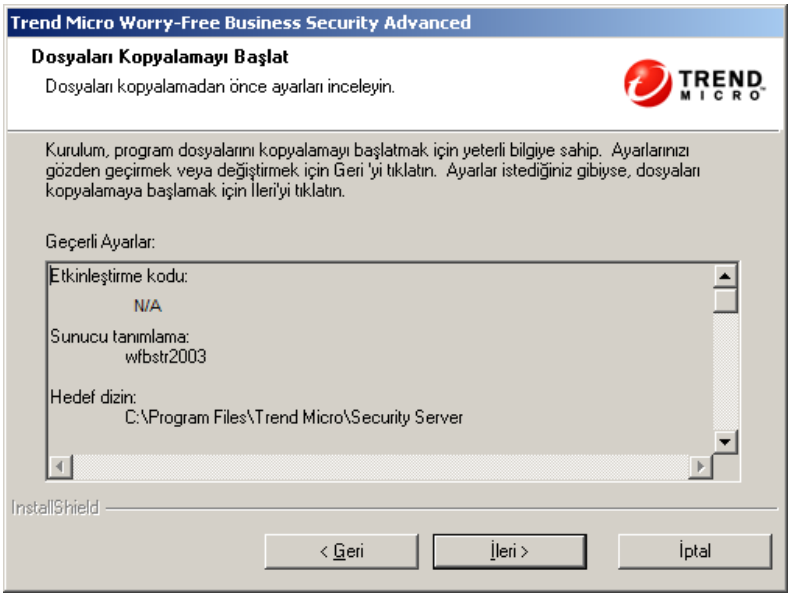
7. Şu öğeleri ayarlayın:
   - **Yol:** Client/Server Security Agent dosyalarının yüklendiği dizin.
   - **Bağlantı noktası numarası:** Client/Server Security Agent ve Security Server iletişimleri için kullanılan bağlantı noktası.

Not: Client/Server Security Agent, Yol ve Bağlantı Noktası ayarlarını hem yerel hem de uzak istemcilere uygular.

---

8. **İleri**'yi tıklatın. **Dosyaları Kopyalamayı Başlat** ekranı görünür.

Bölüm 4: Yükleme İşlemi



ŞEKIL 3-22. Dosyaları Kopyalamayı Başlat ekranı

1. **İleri**'yi tıklatın. Yükleme işlemi Security Server, Messaging Security Agent ve Client/Server Security Agent'ı yükleme ile başlar. Tamamlandıktan sonra, **Remote Messaging Security Agent Yükleme Aşaması** ekranı görünür.

Not: Sonraki adım, Bileşen Seçimi ekranından Remote Messaging Security Agent'ı seçtiğinizi kabul eder. Remote Messaging Security Agent'ı yükleme seçeneğini belirlememeyi seçtiyseniz, bir InstallShield Sihirbazı Tamamlandı ekranı görünür.

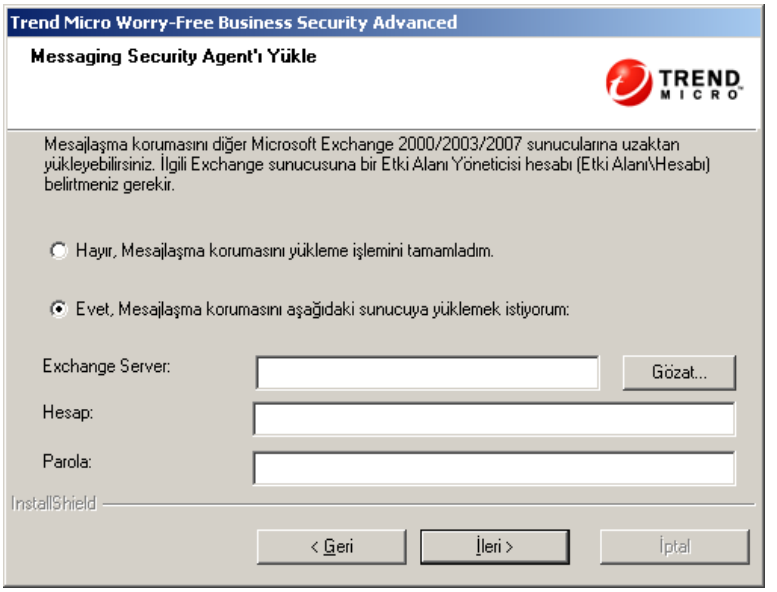
Bölüm 5: Remote Messaging Security Agent Yüklemesi

Remote Messaging Security Agent'ı yüklemek için:

1. **Remote Messaging Security Agent Yükleme Aşaması** ekranı görünür.

ŞEKIL 3-23. Remote Messaging Security Agent Yükleme Aşaması

2. **İleri**'yi tıklatın. **Remote Messaging Security Agent'ı Yükle** ekranı görünür.



ŞEKIL 3-24. Messaging Security Agent'ı Yükleme ekranı

3. Uzak bir Exchange sunucusuna mesajlaşma koruması yüklemek için, **Evet**'i tıklatın ve ardından yerleşik etki alanı yönetici hesabı için kimlik bilgilerini girin.

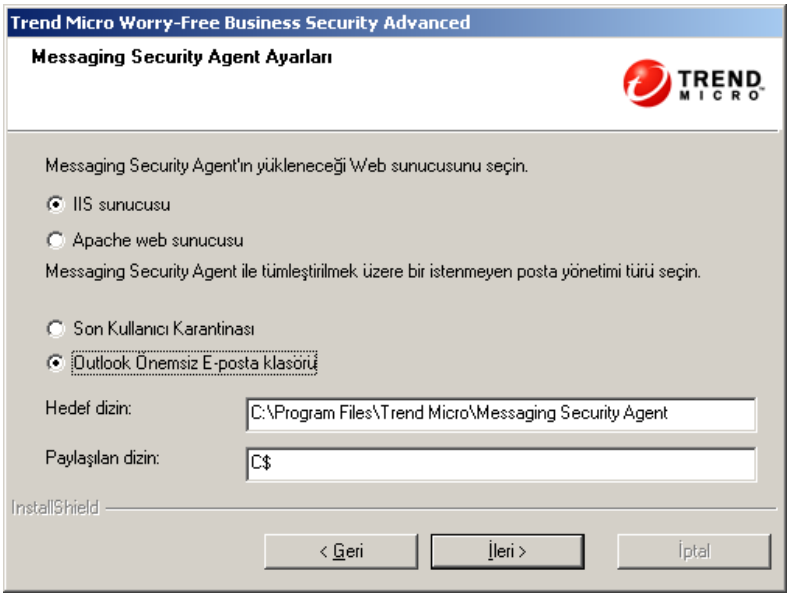
Not: Hayır'ı seçerseniz, InstallShield Sihirbazı Tamamlandı ekranı görünecek ve yükleme işlemi tamamlanmış olacaktır. Evet'i seçerseniz, Remote Messaging Security Agent yüklemesi tamamlandıktan sonra, başka bir Remote Messaging Security Agent'ı yüklemeniz istenecektir.

Aşağıdaki bilgileri girin:

- **Exchange Server:** IP adresi veya makine adı
- **Hesap**
- **Parola**

Not: Yükleyici; özel, alfasayısal olmayan karakterlere sahip parolaların Exchange Server bilgisayarına geçişini sağlayamayabilir. Bu Messaging Security Agent yüklemesini önleyecektir. Bu sorunu gidermek için, yerleşik etki alanı yönetici hesabı parolasını geçici olarak değiştirin veya Messaging Security Agent'ı doğrudan Exchange sunucusuna yükleyin.

4. **İleri**'yi tıklatın. **Remote Messaging Security Agent Ayarları** ekranı görünür.



ŞEKIL 3-25. Messaging Security Agent Ayarları ekranı

Not: Normal yükleme yöntemini seçerseniz bu ekran görünmeyecektir.

5. Remote Messaging Security Agent Ayarları ekranından, şunları gerektiği gibi güncelleyin:
   - Web sunucusu
     - **IIS sunucusu**
     - **Apache Web sunucusu**
   - İstenmeyen posta yönetimi
     - **Son Kullanıcı Karantinası:** Seçiliyse, WFBS Microsoft Outlook'ta **Önemsiz E-posta** klasörünün yanı sıra ayrı bir istenmeyen posta klasörü oluşturur.

- **Outlook Önemsiz E-posta klasörü:** seçiliyse, WFBS istenmeyen postayı bu klasöre kaydeder; Microsoft Outlook **Son Kullanıcı Karantinası** (EUQ) klasöründeki istenmeyen postayı tipik olarak **Önemsiz E-posta** klasörüne taşıdığı için bu seçeneğin belirlenmesi önerilir.

Not: EUQ ve Önemsiz E-posta klasörü arasında seçim yapma seçeneği, yalnızca, bilgisayar Exchange Server 2003 çalıştırıyorsa kullanılabilir. Önemsiz E-posta özelliği Exchange Server 2000 tarafından desteklenmez. EUQ, Exchange Server 2007'de Önemsiz E-posta özelliğiyle tamamen tümleşir.

- **Hedef dizin:** Uzak Messaging Security Agent dosyalarının yüklendiği dizin.
- **Paylaşılan dizin:** Remote Messaging Security Agent yüklemesi için sistem kök dizini.

6. **İleri**'yi tıklatın. Program, Remote Messaging Security Agent'ı uzak Exchange sunucusuna yüklemeye başlar.
7. Tamamlandıktan sonra, **Remote Messaging Security Agent Durumu** ekranı yeniden görünür. Remote Messaging Security Agent'ları diğer Exchange sunucularına yüklemek için yukarıdaki işlemi tekrarlayın.

Sessiz Yüklemeyi Gözden Geçirme

Ayrı ağlarda birden fazla aynı yüklemeyi çalıştırmanıza yardımcı olması için Sessiz yüklemeyi kullanın. Sessiz yüklemeyi çalıştırma prosedürü, aşağıdaki önceden yapılandırma ve gerçek yükleme adımları dışında Özel yüklemeyle aynıdır.

Önceden yapılandırma adımları:

1. Komut isteminde, WFBS kurulum dosyalarının bulunduğu dizine gidin.
2. İstemde, **setup -r** yazın.
3. Kurulum işlemine devam etmek ve yükleme sırasında WFBS'yı yapılandırma hakkında daha fazla bilgi almak için, bkz. *Özel Yüklemeyi Gözden Geçirme*, sayfa 3-4.

   Yüklemenin sonunda bir onay iletisi görüntülenir.

Sessiz yüklemeyi başlatma:

1. Raporları görüntülemek için,
   - **Windows 2000:** C:\WINNT
   - **Windows XP/2003:** C:\Windows
   - **Vista:** C:\Windows
2. **setup.iss** dosyasını bulun ve WFBS kurulum klasörüne kopyalayın.
3. Bir komut penceresi açın ve istemde, WFBS kurulum klasörüne gidin ve **setup -s** yazın.

Yüklemenin başarılı olduğunu doğrulamak için, WFBS klasörüne gidin ve `setup.log` dosyasını görüntüleyin. `ResultCode=0` ise, yükleme başarılı olmuştur.

Yüklemeyi Doğrulama

Yükleme veya yükseltmeyi tamamladıktan sonra, Trend Micro Security Server'ın düzgün şekilde yüklendiğini doğrulayın.

Yüklemeyi doğrulamak için:

- Trend Micro Security Server'ın Windows **Başlat** menüsünde WFBS program kısayollarını arayın.
- WFBS'nın **Program Ekle/Kaldır** listesinde olup olmadığını kontrol edin.
- Sunucunun URL'si ile Web konsolunda oturum açın:

  `https://{sunucu_adı}:{bağlantı numarası}/SMB`

  SSL KULLANMIYORSANIZ, `http` yerine `https` yazın.

Bölüm 4

Yükseltme ve Geçirme

Bu bölümde, WFBS'nın nasıl yükleneceğini anlamak için ihtiyacınız olan bilgiler verilmektedir.

Bu bölümde ele alınan başlıklar şunlardır:

Önceki Sürümden Yükseltme

Yükseltme prosedürü, Security Server'ı tanımlamanız (etki alanı adı veya IP adresi) istendiğinde var olan Security Server'ınızı girmeniz dışında normal yükleme işlemiyle aynıdır. Client/Server Security Agent'lar otomatik olarak yükseltilir. Bkz. *Aracı Yüklemeye Genel Bakış*, sayfa 3-2.

Trend Micro, bilgisayarlarınızı ve ağınızı korumak için iki benzer ürün sunmaktadır: Worry-Free Business Security ve Worry-Free Business Security Advanced.

TABLO 4-1. Ürün Sürümleri

Ürün Sürümü	Worry-Free Business Security	Worry-Free Business Security Advanced
İstemci tarafı çözümü	Evet	Evet
Sunucu tarafı çözümü	Evet	Evet

Desteklenen Yükseltmeler

WFBS 6.0 şu sürümlerin tamamından yükseltmeleri destekler:

- Client Server Security veya Client Server Messaging Security 3.6
- Worry-Free Business Security veya Worry-Free Business Security Advanced 5.0 ve 5.1'den yükseltme

Desteklenmeyen Yükseltmeler

WFBS 6.0, şu koşullar altında yükseltmeleri desteklemez:

- Client/Server Messaging Security 3.5'ten yükseltme
- Client/Server Suite 2.0'dan yükseltme
- OfficeScan 'den yükseltme
- Client/Server Security 3.0'dan yükseltme
- Bir dilden diğerine yükseltme

En İyi Uygulamaları Yükseltme

WFBS'nın en yeni sürümüne yükselttiğinizde istemci ayarlarınızı koruyabilirsiniz. Trend Micro, yükseltme başarısız olursa var olan ayarlarınızı kolaylıkla geri yükleyebilmenizi sağlamak için Security Server veritabanınızı yedeklemenizi önerir.

Security Server veritabanını yedeklemek için:

1. Trend Micro Security Server Master Service'i durdurun.
2. Windows Explorer'da Security Server klasörüne gidin ve `\PCCSRV\HTTPDB` içeriklerini başka bir konuma (örneğin, aynı sunucuda başka bir dizine, başka bir bilgisayara veya çıkarılabilir bir sürücüye) kopyalayın.

Trend Micro, yükseltmeden önce tüm günlük dosyalarını Security Server'dan silmenizi önerir.

Günlük dosyalarını silmek için:

1. **Raporlar > Bakım > El ile Günlük Silme** seçeneklerine gidin.
2. **Şu Tarihten Eski Günlükleri Sil**'i günlük türü için `0`'a ayarlayın.
3. **Sil** öğesini tıklatın.
4. Tüm günlük türleri için 2 ve 3 adımlarını tekrarlayın.

Gözden Geçirmeyi Yükseltme

Deneme sürümünüzün süresi dolmak üzereyken, **Canlı Durum** ekranında bir bildirim iletisi görüntülenir. Web konsolunu kullanarak deneme sürümünden tam lisanslı sürüme yükseltebilirsiniz. Yapılandırma ayarlarınız kaydedilecektir. Tam lisanslı sürümü satın aldığınızda, size bir Kayıt Anahtarı veya Etkinleştirme Kodu verilir.

Deneme sürümünden yükseltmek için:

1. Web konsolunu açın.
2. Ana menüde, **Tercihler** > **Ürün Lisansı** seçeneklerini tıklatın. **Ürün Lisansı** ekranı görünür.
3. **Lisans yükseltme yönergelerini görüntüle**'yi tıklatın.

4. Etkinleştirme Kodunuz varsa, bunu **Yeni bir kod gir**'i seçerek **Yeni Etkinleştirme Kodu** alanına girin ve **Etkinleştir**'i tıklatın.

Not: Etkinleştirme kodunuz yoksa, **Çevrimiçi Kaydolma**'yı tıklatın ve Etkinleştirme Kodunu edinmek için Kayıt Anahtarını kullanın.

Diğer Antivirüs Uygulamalarından Geçirme

WFBS, diğer antivirüs uygulamalarından geçirmeyi destekler. WFBS, istemci yazılımını otomatik olarak geçirebilir; ancak sunucu uygulamasını kaldıramaz.

Trend Micro Anti-Spyware'den Geçirme

Ağınızda Trend Micro Anti-Spyware varsa, şunu göz önünde bulundurun:

- Security Server'ı TMASY sunucusuyla aynı sunucuya yüklerseniz, kurulum programı TMASY sunucusunu *kesinlikle* kaldırmaz veya yükseltmez. Security Server'ı aynı makineye yüklemeden önce TMASY sunucusunu el ile kaldırmanız gerekir.
- Client/Server Security Agent'ı yüklemeden önce TMASY istemcisini kaldırmak gerekmez. Client/Server Security Agent kurulum programı, TMASY istemcisini aynı istemci bilgisayarında algılandığında otomatik olarak kaldıracak ve ardından Client/Server Security Agent'ı yükleyecektir.
- Client/Server Security Agent ve TMASY için casus yazılımdan koruma ayarları farklıdır. Client/Server Security Agent'ları yükledikten sonra, casus yazılımdan koruma ayarlarını önceki TMASY istemci ayarlarınızla aynı olmaları için yapılandırmanız gerekebilir. Client/Server Security Agent ve TMASY casus yazılımdan koruma ayarlarının bir karşılaştırması için, bkz. *Tablo 4-2*.

TABLO 4-2. Client/Server Security Agent ve TMASY Casus Yazılımdan Koruma Ayarlarının Karşılaştırması

	CLIENT/SERVER SECURITY AGENT	TREND MICRO ANTI-SPYWARE CLIENT
Gerçek Zamanlı Tarama	Etkinleştirildi	Devre Dışı (Etkin Uygulama İzlemesi)

	CLIENT/SERVER SECURITY AGENT	TREND MICRO ANTI-SPYWARE CLIENT
Varsayılan eylem	Temizle	Reddetme yürütülebilir
El ile Tarama		
Tarama türü	Tam tarama	Hızlı tarama
Varsayılan eylem	Temizle	Tara ve başka işlem yapma (otomatik temizleme varsayılan olarak devre dışı)
Başlangıçta tara	Yok	Etkinleştirildi
Ağı kontrol et	Yok	Etkinleştirildi
Zamanlanmış Tarama	Devre dışı bırakıldı	Etkinleştirildi
Tarama zamanlaması	Her Pazartesi	Günlük
Tarama zamanı	12:30	23:00
Tarama türü	Tam tarama	Hızlı tarama
Varsayılan eylem	Temizle	Tara ve başka işlem yapma (otomatik temizleme varsayılan olarak devre dışı)

Diğer Antivirüs Uygulamalarından Geçirme

Başka bir antivirüs yazılımından WFBS'ya geçirme, iki adımlı bir işlemdir: Trend Micro Security Server yüklemesini takiben istemcileri otomatik geçirme.

Otomatik istemci geçirme işlemi, var olan istemci antivirüs yazılımını Client/Server Security Agent programıyla değiştirmek anlamına gelir. İstemci kurulum programı, istemci bilgisayarlarınızdaki diğer antivirüs yazılımını otomatik olarak kaldırır ve Client/Server Security Agent ile değiştirir.

WFBS'nın otomatik olarak kaldırabileceği uygulamaların bir listesi için, bkz. *Tablo 4-3*.

Not: WFBS, sunucu yüklemelerini değil yalnızca aşağıdaki istemci yüklemelerini kaldırır.

TABLO 4-3. Kaldırılabilir Antivirüs Uygulamaları

Trend Micro™		
Trend Micro™ OfficeScan 95 istemci 3.5 Trend Micro OfficeScan NT istemci sürümü 3.1x Trend Micro OfficeScan NT istemci sürümü 3.5 Trend Micro PC-cillin™ Corp 95 istemcisi PC-cillin Corp NT istemcisi Trend Micro ServerProtect™ for Windows NT Trend Micro™ PC-cillin 2004 (AV) Trend Micro PC-cillin 2004 (TIS) Trend Micro PC-cillin 2000 7.61(WinNT) Trend Micro PC-cillin 2000(Win9X)	Trend Micro PC-cillin 2000 for Windows NT Trend Micro PC-cillin 2002 Trend Micro PC-cillin 2003 Trend Micro PC-cillin 6 Trend Micro PC-cillin 95 1.0 Trend Micro PC-cillin 95 1.0 Lite Trend Micro PC-cillin 97 2,0 Trend Micro PC-cillin 97 3,0 Trend Micro PC-cillin 98 Trend Micro PC-cillin 98 Plus Windows 95 Trend Micro PC-cillin 98 Plus Windows NT Trend Micro PC-cillin NT Trend Micro PC-cillin NT 6 Trend Micro™ Virus Buster 2000	Trend Micro Virus Buster 2000 for NT sür.1.00 Trend Micro Virus Buster 2000 for NT sür.1.20 Trend Micro Virus Buster 2001 Trend Micro Virus Buster 98 Trend Micro Virus Buster 98 for NT Trend Micro Virus Buster NT Trend Micro Virus Buster 95 1.0 Trend Micro Virus Buster 97 Trend Micro Virus Buster 97 LiteOfficeScan 95 client 3.1x Trend Micro Virus Buster Lite 1.0 Trend Micro Virus Buster Lite 2,0

TABLO 4-3. Kaldırılabilir Antivirüs Uygulamaları (Devamı)

Symantec™		
Norton AntiVirus™ 2.0 NT	Norton AntiVirus 6,524	Norton Antivirus CE 8,0 9x
Norton AntiVirus 2000 9X	Norton AntiVirus 7,0 9X	Norton Antivirus CE 8,0 NT
Norton AntiVirus 2000 NT	Norton AntiVirus 7,0 NT	Norton Antivirus CE 8.1 sunucusu
Norton AntiVirus 2001 9X	Norton AntiVirus 7,5 9X	Norton Antivirus CE 9,0
Norton AntiVirus 2001 NT	Norton AntiVirus 7,5 NT	
Norton AntiVirus 2002 NT	Norton AntiVirus 8.0 9x	
Norton AntiVirus 2003	Norton AntiVirus 8,0 NT	
Norton AntiVirus 5,0 9X	Norton Antivirus CE 10.0	
Norton AntiVirus 5,0 NT	Norton Antivirus CE 10,1	
Norton AntiVirus 5,31 9X	Norton Antivirus CE 6,524	
Norton AntiVirus 5,31 NT	Norton Antivirus CE 7.0 for Windows NT	
Norton AntiVirus 5,32 9X	Norton Antivirus CE 7.0 NT	
Norton AntiVirus 5,32 NT	Norton Antivirus CE 7.5 9x	
	Norton Antivirus CE 7,5 NT	

TABLO 4-3. Kaldırılabilir Antivirüs Uygulamaları (Devamı)

McAfee™		
Dr Solomon 7.77,7.95 NT Dr Solomon 4.0.3 Dr Solomon 4.0.3 NT ePOAgent1000 ePOAgent2000 McAfee NetShield 4.5 McAfee NetShield NT 4.03a	McAfee VirusScan 4.5 McAfee VirusScan 4.51 McAfee VirusScan 6.01 McAfee VirusScan 95(1) McAfee VirusScan 95(2) McAfee VirusScan ASaP	McAfee VirusScan Enterprise 7 McAfee VirusScan NT McAfee VirusScan TC McAfee VirusScan(MSPlus98) V3Pro 98
LANDesk™		
LANDesk VirusProtect5.0		
Computer Associates™		
CA InocuLAN_NT 4.53 CA InocuLAN_9.x 4.53	CA eTrust InoculateIT 6.0	CA InocuLAN 5
Ahnlab™		
V3Pro 2000 Deluxe	V3Pro 98 Deluxe	
Panda Software™		
Panda Antivirus Local Networks	Panda Antivirus 6.0	Panda Antivirus Windows NT WS
F-Secure™		
F-Secure 4.04 F-Secure 4.08, 4.3 5.3	F-Secure BackWeb	F-Secure Management Agent
Kaspersky™		
Antivirus Personal 4.0, Workstation 3.5. 5.4		
Sophos™		
Sophos Anti-Virus NT	Sophos Anti-Virus 9X	

TABLO 4-3. Kaldırılabilir Antivirüs Uygulamaları (Devamı)

Authentium™		
Command AV 4.64 9x		
Amrein™		
Cheyenne AntiVirus 9X	Cheyenne AntiVirus NT	
Grisoft™		
Grisoft AVG 6.0		
Diğerleri		
ViRobot 2k Professional	Tegam ViGUARD 9.25e for Windows NT	

Client/Server Security Agent'ı Yükseltme

Önceki bir sürümden veya deneme sürümünden tam sürüme yükseltebilirsiniz. Trend Micro Security Server'ı yükselttiğinizde, istemciler otomatik olarak yükseltilir.

Seçili İstemciler İçin Yükseltmeyi Önleme

Çok sayıda istemciyi eş zamanlı olarak yükseltmek, ağ trafiğini önemli ölçüde arttırabilir. WFBS, seçili istemcilerin mevcut sürüme yükseltilmesini önlemek için bir seçenek sunmaktadır. Yükseltilecek çok sayıda istemci varsa, Trend Micro, yükseltmeden önce belirli gruplar için program güncellemesini devre dışı bırakmanızı ve onları daha sonra yükseltmenizi önerir.

Program güncellemesini devre dışı bırakmak için:

1. WFBS Web konsolunda, **Güvenlik Ayarları > Bir grup seç > Yapılandır > İstemci Ayrıcalıkları** seçeneklerini belirleyin.
2. Güncelleme Ayarları'nın altında, **Program güncellemesini ve düzeltme dağıtımını devre dışı bırak**'ı seçin ve ayarlarınızı kaydedin.

   Not: Bu istemciler sonraki sürüme yükseltilmeyecek, ancak korumalarını güncel tutmak için bileşen güncellemelerini (virüs deseni dosyası gibi) almaya devam edecektir.

3. Bu istemcileri yükseltmeye hazır olduğunuzda, aynı onay kutusunu temizleyin, ayarlarınızı kaydedin ve istediğiniz yükleme yöntemini kullanarak bu istemciler için aracı yüklemesini gerçekleştirin.

Bölüm 5

Başlarken

Bu bölümde WFBS'yı nasıl başlatacağınız ve çalıştıracağınız anlatılmaktadır.

Bu bölümde ele alınan başlıklar şunlardır:

Web Konsoluna Erişim

Bu başlıkta, Web konsolu ve ona nasıl erişim sağlanacağı özetlenmektedir.

TABLO 5-1. Web Konsolunun Ana Özellikleri

Özellik	Açıklama
Ana menü	Web konsolunun üst kısmı boyunca ana menü bulunmaktadır. Bu menü her zaman kullanıma hazırdır.
Yapılandırma alanı	Ana menü öğelerinin alt kısmı, yapılandırma alanıdır. Bu alanı, seçtiğiniz menü öğesine uygun seçenekleri belirlemek için kullanın.
Menü kenar çubuğu	**Güvenlik Ayarları** ekranından bir istemci veya grup seçtiğinizde ve **Yapılandır**'ı tıklattığınızda bir menü kenar çubuğu görüntülenir. Kenar çubuğunu, masaüstü bilgisayarlarınız ve sunucularınız için güvenlik ayarlarını ve taramaları yapılandırmak üzere kullanın.
Güvenlik Ayarları araç çubuğu	**Güvenlik Ayarları** ekranını açtığınızda, çeşitli simgeler içeren bir araç çubuğu görebilirsiniz. **Güvenlik Ayarları** ekranından bir istemci veya grubu tıklatıp ardından da araç çubuğundaki bir simgeyi tıklattığınızda, Security Server ilgili görevi gerçekleştirir.

Trend Micro Security Server'ı yüklediğinizde, aynı zamanda merkezileştirilmiş Web tabanlı yönetim konsolunu da yüklersiniz. Bu konsol; ActiveX, CGI, HTML ve HTTP/HTTPS gibi Internet teknolojilerini kullanır.

Web konsolunu açmak için:

1. Web konsolunu açmak için aşağıdaki seçeneklerden birini seçin:
   - Masaüstündeki **Worry-Free Business Security** kısayolunu tıklatın.
   - Windows™ Başlat menüsünden, **Trend Micro Worry-Free Business Security > Worry-Free Business Security** seçeneklerini tıklatın.
   - Web konsolunu ağdaki herhangi bir bilgisayardan da açabilirsiniz. Bir Web tarayıcısı açın ve adres çubuğuna şunu yazın:
     `https://{Security_Server_Name}:{port number}/SMB`

Örneğin:

`https://my-test-server:4343/SMB`

`https://192.168.0.10:4343/SMB`

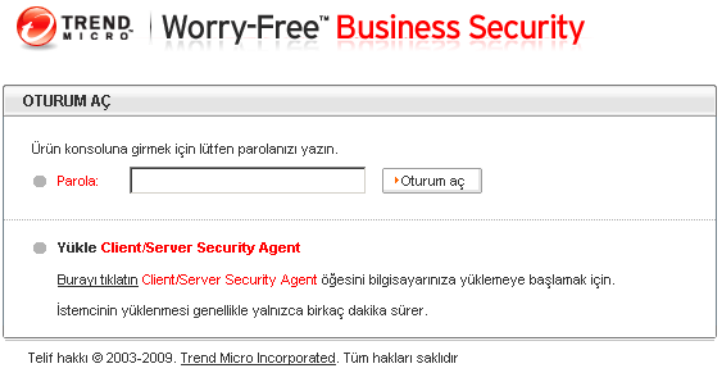
`http://my-test-server:8059/SMB`

`http://192.168.0.10:8059/SMB`

SSL KULLANMIYORSANIZ, `http` yerine `https` yazın. HTTP bağlantıları için varsayılan bağlantı noktası 8059 ve HTTPS bağlantıları için de 4343'tür.

İpucu: Ortam, sunucu adlarını DNS ile çözemezse, {Security_Server_Name} öğesini {Server_IP_Address} ile değiştirin.

2. Tarayıcı, **Trend Micro Worry-Free Business Security oturum açma** ekranını görüntüler.



ŞEKIL 5-1. WFBS oturum açma ekranı

3. Parolanızı **Parola** metin kutusuna girin, ardından da **Oturum aç**'ı tıklatın. Tarayıcı, Web konsolunun **Canlı Durum** ekranını görüntüler.

Web Konsolu Simgeleri

Aşağıdaki tablo, Web konsolunda görüntülenen simgeleri tanımlar ve onların hangi amaçla kullanıldığını açıklar.

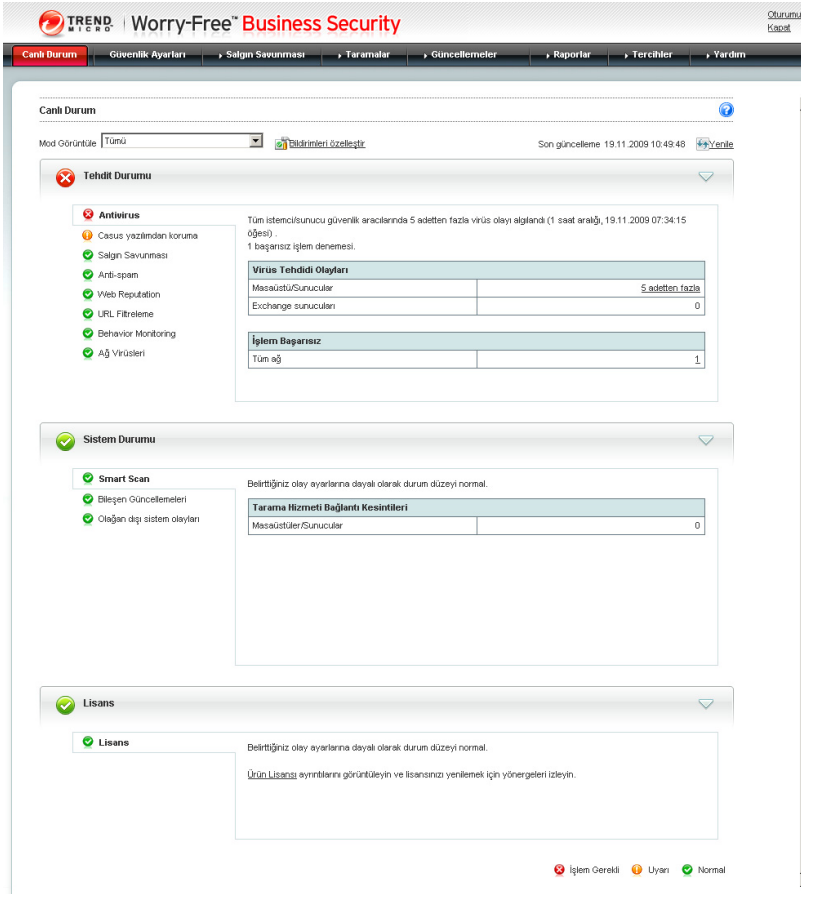
TABLO 5-2. Web Konsolu Simgeleri

Simge	Açıklama
	**Yardım** simgesi. Çevrimiçi yardımı açar.
	**Yenile** simgesi. Geçerli ekranın görünümünü yeniler.
	**Bölümü Genişlet/Daralt** simgesi. Bölümleri genişletir/gizler. Bir kerede yalnızca bir bölümü genişletebilirsiniz.
	**Bilgi** simgesi. Belirli bir öğe ile ilgili bilgileri görüntüler.

Canlı Durum

WFBS'yı yönetmek için Canlı Durum ekranını kullanın.

Canlı Durum ekranında görüntülenen bilgileri yenileme hızı her bölüme göre farklılık gösterir. Yenileme hızı genellikle 1 ila 10 dakika arasındadır. Ekran bilgilerini manuel olarak yenilemek için, **Yenile**'yi tıklatın.



ŞEKIL 5-2. Canlı Durum ekranı

Simgeleri Anlama

Simgeler, ağınızdaki bilgisayarları korumak için herhangi bir eylem gerektiğinde sizi uyarır. Daha fazla bilgi görüntülemek için bölümleri genişletin. Ayrıca, belirli ayrıntıları görüntülemek için tablodaki öğeleri tıklatabilirsiniz. Belirli istemcilerle ilgili daha fazla bilgi için, tablolarda görünen numara bağlantılarını tıklatın.

TABLO 5-3. Canlı Durum Simgeleri

Simge	Açıklama
	Normal Yalnızca birkaç istemci yama uygulamayı gerektirir. Virüs, casus yazılım, bilgisayarlarınız ve ağınızdaki diğer kötü amaçlı yazılım etkinlikleri önemli ölçüde risk taşır.
	Uyarı Ağınızın daha fazla risk altında kalmasını önlemek için harekete geçin. Bir uyarı simgesi, tipik olarak, çok fazla virüs ve diğer kötü amaçlı yazılım olayları bildiren, güvenlik açığı olan çeşitli bilgisayarlarınız olduğu anlamına gelir. Trend Micro tarafından Sarı Uyarı gönderildiğinde, uyarı Salgın Savunması için görüntülenir.
	Gerekli eylem Bir uyarı simgesi, güvenlik sorununu çözmek için yöneticinin eylemde bulunması gerektiği anlamına gelir.

Canlı Durum ekranında görüntülenen bilgiler, Security Server tarafından oluşturulur ve istemcilerden toplanan verilere dayanır.

Tehdit Durumu

Tehdit Durumu ekranında, şunlara ilişkin bilgiler görüntülenir:

- **Antivirüs:** virüs algılamaları. 5. olaydan itibaren durum simgesi Uyarıyı görüntülemek üzere değiştir. Eylemde bulunmanız gerekiyorsa:
  - Client/Server Security Agent, gerçekleştirmek üzere ayarlandığı eylemi başarıyla gerçekleştiremedi. Client/Server Security Agent'ın eylemi gerçekleştiremediği bilgisayarlar hakkında ayrıntılı bilgileri görüntülemek için numaralı bağlantıyı tıklatın.
  - Client/Server Security Agent'larda Gerçek Zamanlı tarama devre dışı. Gerçek Zamanlı taramayı tekrar başlatmak için **Şimdi Etkinleştir**'i tıklatın.
- **Casus yazılımdan koruma:** Casus yazılımdan koruma bölümünde, en son casus yazılım tarama sonuçları ve casus yazılım günlük girişleri görüntülenir. Casus Yazılım Tehdit Olayları tablosunun Olay Sayısı sütununda en son casus yazılım taramasının sonuçları görüntülenir.
  - Belirli istemciler hakkında daha fazla bilgi için, Casus Yazılım Tehdit Olayları tablosunun **Algılanan Olaylar** sütununun altında bulunan numara bağlantısını tıklatın. Buradan, istemcilerinizi etkileyen belirli casus yazılım tehditleriyle ilgili bilgi bulabilirsiniz.
- **URL Filtreleme:** yönetici tarafından belirlenerek kısıtlanmış Web siteleri. 300. olaydan itibaren, durum simgesi uyarıyı görüntülemek üzere değişir.
- **Behavior Monitoring:** davranış izleme ilkelerinin ihlalleri.
- **Ağ Virüsleri:** güvenlik duvarı ayarları tarafından belirlenen ağ virüsü algılamaları.
- **Salgın Savunması:** ağınızdaki olası bir virüs salgını.
- **Anti-spam:** spam algılamaları. Seçili Microsoft Exchange Server'ının, Anti-spam ekranından eşik düzeyini ayarlayabileceğiniz yapılandırma ekranına yeniden yönlendirilmek için **Yüksek**, **Orta** veya **Düşük** bağlantısını tıklatın. İlgili ekrana yeniden yönlendirilmek için **Devre Dışı**'yı tıklatın. Bu bilgi, saatlik bir şekilde güncellenir.
- **Web Reputation:** Trend Micro tarafından belirlenen, potansiyel olarak tehlikeli Web siteleri. 200. olaydan itibaren, durum simgesi uyarıyı görüntülemek üzere değişir.

Sistem Durumu

Aracıların yüklü olduğu bilgisayarlarda güncellenmiş bileşenler ve boş alanla ilgili bilgileri görüntüleyin.

- **Bileşen Güncellemeleri:** Security Server için bileşen güncellemelerinin durumu veya güncellenmiş bileşenlerin aracılara dağıtımı.
- **Olağan dışı sistem olayları:** sunucu olarak görev yapan (sunucu işletim sistemlerini çalıştıran) istemcilere ilişkin disk alanı bilgisi.
- **Smart Scan:** atandıkları tarama sunucusuna bağlanamayan istemciler.

İpucu: Web konsolunu Uyarı veya Eylem Gerekli simgesini görüntüleyecek şekilde tetikleyen parametreleri, **Tercihler > Bildirimler** seçeneklerinden özelleştirebilirsiniz.

Lisans Durumu

Lisans durumuna ilişkin bilgileri görüntüleyin.

- **Lisans:** ürün lisansınızın durumuna ilişkin bilgiler, özellikle geçerlilik sonu bilgileri.

Canlı Durum Güncelleme Aralıkları

Canlı Durum bilgilerinin hangi sıklıkta güncelleneceğini anlamak amacıyla aşağıdaki tabloya bakın.

TABLO 5-4. Canlı Durum Güncelleme Aralıkları

Öğe	Güncelleme Aralığı (dakika)	Aracı Günlükleri Sunucuya Şunun Ardından Gönderir... (dakika)
Salgın Savunması	3	Yok
Antivirüs	1	CSA: Hemen MSA: 5
Casus yazılımdan koruma	3	1

TABLO 5-4. Canlı Durum Güncelleme Aralıkları (Devamı)

Öğe	Güncelleme Aralığı (dakika)	Aracı Günlükleri Sunucuya Şunun Ardından Gönderir... (dakika)
Anti-spam	3	60
Web Reputation	3	60
URL Filtrelemesi	3	60
Behavior Monitoring	3	60
Ağ Virüsü	3	60
Smart Scan	10	Yok
Lisans	10	Yok
Bileşen Güncellemeleri	3	Yok
Olağan Dışı Sistem Olayları	10	Dinleme hizmeti TmListen başlatıldığında

Güvenlik Ayarlarını Görüntüleme

Güvenlik Ayarları ekranı, aracıları yüklediğiniz tüm bilgisayarları yönetmenize izin verir. Güvenlik Grubu Ağacı'ndan bir grup seçtiğinizde, ilgili gruptaki bilgisayarlar sağ tarafta bir tabloyla görüntülenir.

Güvenlik Ayarları ekranı iki (2) ana bölüme ayrılır:

Genel Gezinme Menüsü

Bu menü öğeleri, Güvenlik Ayarları ekranında belirlenen seçeneklerden bağımsız olarak kullanılabilir olmaya devam eder ve diğer tüm ekranlar için sabittir.

Yapılandırma Alanı

Yapılandırma alanı; Security Server bilgi çubuğunu, yapılandırma araç çubuğunu ve araç çubuğunun alt kısmında Güvenlik Grubu Ağacı ve Güvenlik Aracısı bilgi tablosunu içerir.

Security Server bilgi çubuğu: Security Server hakkında Etki Alanı adı, bağlantı noktası numarası ve yönetilen masaüstü bilgisayar ve sunucu sayısı gibi bilgileri görüntüler.

Araç çubuğu:

- **Yapılandır:** Yapılandır aracı, yalnızca Güvenlik Grubu Ağacı'ndaki öğelerden biri seçildiğinde kullanılabilir. Yapılandır aracı, ilgili grup dahilindeki tüm aracılar için ayarları yapılandırmanıza olanak tanır. Bir gruptaki tüm bilgisayarlar aynı yapılandırmayı paylaşmalıdır. Şunları yapılandırabilirsiniz:

  Tarama yöntemi, Antivirüs/Casus Yazılıma Karşı Koruma, Güvenlik Duvarı, Web Reputation, URL Filtreleme, Behavior Monitoring, TrendSecure Araç Çubukları ve İstemci Ayrıcalıkları.
- **Ayarları Kopyala:** Ayarları Kopyala aracı, yalnızca Güvenlik Grubu Ağacı'ndaki öğelerden biri seçildiğinde ve Güvenlik Grubu Ağacı'nda aynı türden en az bir tane daha öğe varsa kullanılabilir.
- **İçe Aktarma/Dışa Aktarma Ayarları:** Yapılandırma ayarlarınızı kaydedin veya önceden kaydettiğiniz ayarları içe aktarın.
- **Grup Ekle:** Grup Ekle aracı, yeni masaüstü bilgisayar veya sunucu grupları eklemenize olanak tanır.
- **Ekle:** Ekle aracı, Client/Server Security Agent'ları belirttiğiniz bilgisayarlara dağıtarak belirli gruplara bilgisayar eklemenize olanak tanır.
- **Kaldır:** Kaldır aracı, aracıyı belirttiğiniz bilgisayarlardan kaldıracaktır.
- **Taşı:** Taşı aracı, seçili bilgisayar veya sunucuları bir güvenlik sunucusundan diğerine taşımanıza olanak tanır.
- **Sayaçları Sıfırla:** Sayaçları Sıfırla aracı, bir grup dahilindeki tüm bilgisayarlarda çalışır. Tıklatıldığında, Güvenlik Aracısı bilgi tablosunun Algılanan Virüsler ve Algılanan Casus Yazılım sütunlarındaki değer sıfırlanacaktır.
- **Güvenlik Grubu Ağacı:** Güvenlik Grubu Ağacı'ndan, ilgili gruptaki bilgisayarların bir listesini sağ tarafta görüntülemek için bir grup seçin.
- **Güvenlik Aracısı bilgi tablosu:** Bir istemci seçtiğinizde ve araç çubuğundan bir aracı tıklattığınızda, Web konsolu yeni yapılandırmaların alanını görüntüler.

Bölüm 6

Temel Güvenlik Ayarlarını Yönetme

Bu bölümde ağınızı korumak için ayarların nasıl yapılandırıldığı açıklanır.

Bu bölümde ele alınan başlıklar şunlardır:

Masaüstü ve Sunucu Grupları İçin Seçenekler

WFBS içinde Gruplar, aynı yapılandırmayı paylaşan ve aynı görevleri çalıştıran istemcilerin toplanmasıdır. İstemcileri gruplandırarak, birden fazla istemciyi aynı anda yapılandırın ve yönetin. Daha fazla bilgi için, bkz. *Gruplara Genel Bakış*, sayfa 4-2.

Güvenlik Ayarları ekranından bir grup seçilerek ve **Yapılandır** tıklatılarak aşağıdaki öğeler değerlendirilebilir:

TABLO 6-1. Masaüstü ve Sunucu Grupları için Yapılandırma Seçenekleri

Seçenek	Açıklama	Varsayılan
Tarama Yöntemi	Smart Scan ve Geleneksel Tarama Arasında Geçiş	Geleneksel Tarama (yükseltme için) Smart Scan (yeni yükleme için)
Antivirüs/Casus yazılımdan koruma	Gerçek Zamanlı Taramayı, antivirüsü ve casus yazılımdan korunma seçeneklerini yapılandırma	Etkin (Gerçek Zamanlı Tarama)
Firewall	Güvenlik Duvarı seçeneklerini yapılandırma	Devre dışı bırakıldı
Web Reputation	Ofis İçinde ve Ofis Dışında Web Reputation seçeneklerini yapılandırma	Ofis İçinde: Etkin, Düşük Ofis Dışında: Etkin, Orta
Behavior Monitoring	Behavior Monitoring seçeneklerini yapılandırma	Etkinleştirildi
URL Filtrelemesi	URL filtrelemesi, yapılandırılan ilkeleri ihlal eden Web sitelerini engeller.	Etkinleştirildi
TrendSecure	Transaction Protector ve TrendProtect için Ofis İçi ve Ofis Dışı seçeneklerin yapılandırma	Ofis İçinde: Devre dışı bırakıldı Ofis Dışında: Etkinleştirildi
POP3 Posta Taraması	POP3 e-posta iletileri taramasını yapılandırma	Devre dışı bırakıldı

TABLO 6-1. Masaüstü ve Sunucu Grupları için Yapılandırma Seçenekleri (Devamı)

Seçenek	Açıklama	Varsayılan
İstemci Ayrıcalıkları	İstemci konsolundan ayarlara erişimi yapılandırma	Yok
Karantinaya Al	Karantina dizinini belirleme	Yok

Not: IM İçerik Filtreleme gibi diğer istemci ayarları tüm istemcilere uygulanır ve bu ayarlara **Tercihler > Genel Ayarlar** ekranındaki **Masaüstü/Sunucu** sekmesi aracılığıyla erişilebilir.

Tarama Türleri

Virüs taraması, Worry-Free Business Security stratejisinin önemli bir parçasıdır. Tarama sırasında, Trend Micro tarama motoru, desen eşleme olarak adlandırılan bir işlemi kullanarak ilk düzey algılamayı gerçekleştirmek için virüs desen dosyası ile birlikte çalışır. Her virüs, kendisini diğer kodlardan ayıran benzersiz bir imza veya gösterge karakterleri dizilimi içerdiğinden, TrendLabs'de çalışan virüs uzmanları desen dosyasında bu kodun etkisiz parçalarını yakalar. Ardından motor, taranan her dosyanın belirli bölümlerini virüs desen dosyasındaki desenle karşılaştırarak bir eşleşme arar.

Tarama motoru virüs veya kötü amaçlı yazılım içeren dosya algıladığında, temizleme, karantinaya alma, silme veya metin/dosya ile değiştirme gibi bir eylem gerçekleştirir. Tarama görevlerinizi ayarlarken bu eylemleri özelleştirebilirsiniz.

WFBS, istemcileri internet tehditlerine karşı korumak için üç tür tarama sağlar:

- **Gerçek Zamanlı Tarama:** Gerçek Zamanlı Tarama, kalıcı ve sürekli bir taramadır. Her defasında bir dosya alınır, açılır, indirilir, kopyalanır veya değiştirilir, Gerçek Zamanlı Tarama, dosyaları tehditlere karşı tarar.

- **El ile Tarama:** El ile Tarama, isteğe bağlı bir taramadır. El ile Tarama dosyalardaki tehditleri ortadan kaldırır. Bu tarama, aynı zamanda, yeniden etkilenmeyi en aza indirmek için, varsa, eski etkilenmeleri de temizler. El ile Tarama sırasında, aracılar Yönetici (veya Kullanıcı) tarafından belirlenen eylemlere göre tehditlere karşı işlem yapar. Taramayı durdurmak için, tarama devam ediyorken **Taramayı Durdur**'u tıklatın.

  Not: Tarama için geçen zaman istemcinin donanım kaynaklarına ve taranacak dosya sayısına bağlıdır.

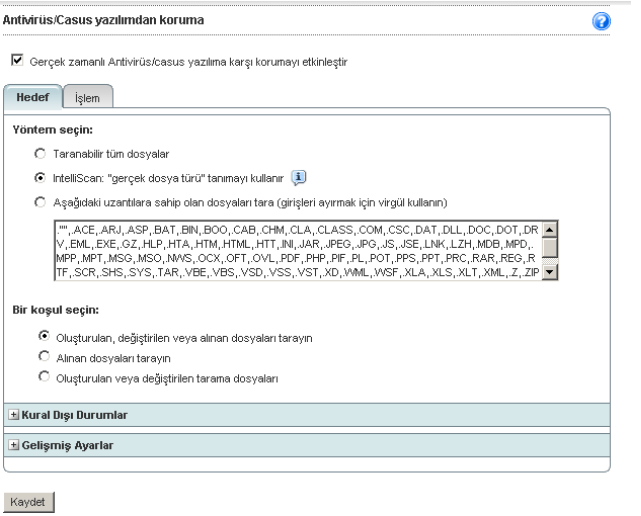
- **Zamanlanmış Tarama:** Zamanlanmış Tarama El ile Taramaya benzerdir, ancak tüm dosyaları ve e-posta iletilerini yapılandırılan zamanda ve sıklıkta tarar. İstemcilerinizde rutin taramaları otomatikleştirmek için Zamanlanmış Taramalar seçeneğini kullanın ve tehdit yönetiminin etkinliğini artırın.

  Zamanlanmış bir tarama yapılandırmak için, **Taramalar > Zamanlanmış Tarama** düğmesini tıklatın. Daha fazla bilgi için, bkz. *Zamanlanmış Taramalar*.

Not: Yukarıdaki tarama türlerini tarama yöntemleriyle karıştırmayın. Tarama yöntemi ile Smart Scan ve Geleneksel Tarama kastedilmektedir (*Tarama Yöntemleri*, sayfa 7-2).

Gerçek Zamanlı Tarama Yapılandırma

Gezinme Yolu: Güvenlik Ayarları > Grup Seç > Yapılandır > Antivirüs/Casus Yazılıma Karşı Koruma



ŞEKIL 6-1. Güvenlik Ayarları > Antivirüs/Casus Yazılıma Karşı Koruma ekranı

Gerçek Zamanlı Taramayı yapılandırmak için:

1. **Antivirüs/Casus Yazılıma Karşı Koruma** ekranında **Hedef** sekmesinden, aşağıdakini gereken şekilde güncelleyin:
   - **Gerçek zamanlı Antivirüs/Casus yazılıma karşı korumayı etkinleştirin**
   - **Taranacak dosyalar**
     - **Tüm taranabilir dosyalar:** Yalnızca şifreli ve parola korumalı dosyalar dışlanır.
     - **IntelliScan:** Dosyaları gerçek dosya türüne dayalı olarak tarar. Daha fazla bilgi için, bkz. *Trend Micro IntelliScan*, sayfa C-4.
     - **Aşağıdaki uzantılara sahip dosyaları tara:** WFBS, seçili uzantılara sahip dosyaları tarayacaktır. Birden fazla girişleri virgüllerle (,) ayırın.

- **Dosyaları tarama zamanını seçin**
  - **Oluşturulan, değiştirilen veya alınan tarama dosyaları**
  - **Alınan tarama dosyaları**
  - **Oluşturulan veya değiştirilen tarama dosyaları**
- **Dışlamalar:** Özel dosyaları, klasörleri veya belirli uzantıları olan dosyaları taramadan dışlayın.
  - **Dışlamaları etkinleştir**
  - **Trend Micro ürünlerinin yüklendiği dizinleri tarama**
  - **Aşağıdaki dizinleri tarama:** Taramadan dışlanacak klasör adını yazın. **Ekle**'yi tıklatın. Klasörü kaldırmak için klasörü seçin ve **Sil** öğesini tıklatın.
  - **Aşağıdaki dosyaları tarama:** Taramadan dışlanacak dosya adını yazın. **Ekle**'yi tıklatın. Dosyayı kaldırmak için dosyayı seçin ve **Sil** öğesini tıklatın.
  - **Aşağıdaki uzantılara sahip olan dosyaları tarama:** Taramadan dışlanacak uzantı adını yazın. **Ekle**'yi tıklatın. Uzantıyı kaldırmak için uzantıyı seçin ve **Sil** öğesini tıklatın.
- **Gelişmiş Ayarlar**
  - **IntelliTrap özelliğini etkinleştir** (antivirüs için)**:** IntelliTrap, sıkıştırılmış dosyalarda botlar gibi zararlı kod algılar. Daha fazla bilgi için, bkz. *Trend Micro IntelliTrap*, sayfa C-7.
  - **Ağdaki eşlenmiş sürücüleri ve paylaşılan klasörleri tara** (antivirüs için)
  - **Sistem kapatılırken disketi tara** (antivirüs için)
  - **Sıkıştırılmış dosyaları tara** (antivirüs için)**:** Taranacak katman sayısını seç.
  - **Casus Yazılım/Grayware Onaylanan Listesi** (casus yazılımdan koruma için)**:** Bu liste, onaylanan casus yazılım/grayware uygulamalarına ilişkin ayrıntıları içerir. Listeyi güncellemek için bağlantıyı tıklatın. Daha fazla bilgi için, bkz. *Casus Yazılım/Grayware Onaylanan Listesini Düzenleme*, sayfa 7-7.

2. **Antivirüs/Casus Yazılıma Karşı Koruma** ekranındaki **Eylem** sekmesinde, algılanan tehditlerin WFBS tarafından nasıl işleneceğini belirtin:
   - **Virüs Algılamalarına Yönelik Eylem**
     - **ActiveAction:** Tehditler için, Trend Micro önceden yapılandırılmış eylemlerini kullanın. Daha fazla bilgi için, bkz. *Trend Micro ActiveAction*, sayfa C-5.
     - **Algılanan tüm Internet tehditleri için aynı eylemi gerçekleştir:** Geç, Sil, Yeniden Adlandır, Karantinaya Al veya Temizle işlemlerinden birini seçin. Temizle seçeneğini belirlerseniz temizlenemeyen tehdit için gerçekleştirilecek eylemi belirleyin.
     - **Algılanan aşağıdaki tehditler için özelleşmiş eylem:** Her tehdit türü için Geç, Sil, Yeniden Adlandır, Karantinaya Al veya Temizle işlemlerinden birini seçin. Temizle seçeneğini belirlerseniz temizlenemeyen tehdit için gerçekleştirilecek eylemi belirleyin.
     - **Temizlemeden önce algılanan dosyayı yedekle:** İstemci üzerindeki aşağıda dizinde virüslü dosyanın şifrelenmiş bir kopyasını kaydeder:

       ```
       C:\Program Files\Trend Micro\Client Server Security Agent\Backup
       ```
   - **Casus Yazılım/Grayware Algılamaları için Eylem**
     - **Temizleme:** Casus yazılım/grayware temizlenirken, WFBS tarafından ilgili kayıt defteri girişleri, dosyalar, tanımlama bilgileri ve kısayollar silinebilir. Casus yazılım/grayware ile ilişkili işlemler de sonlandırılabilir.
     - **Erişimi Reddet**

     UYARI! **İstemciye casus yazılım/grayware erişimin reddedilmesi etkilenen istemcilerden casus yazılım/grayware tehdidini kaldırmaz.**

   - **Gelişmiş Ayarlar**
     - **Bir virüs/casus yazılım algılandığında masaüstünde veya sunucuda bir uyarı iletisi görüntüle**
3. **Kaydet**'i tıklatın.

   Ayrıca, bir etkinlik gerçekleştiğinde bildirim alacak kişileri yapılandırın. Bkz. *Bildirimler için Olayları Yapılandırma*, sayfa 8-3.

Güvenlik Duvarını Yönetme

İstemci ile ağ arasında bir bariyer oluşturarak istemcileri bilgisayar korsanlarının saldırılarından ve ağ virüslerinden korumaya yardımcı olur. Güvenlik duvarı belirli ağ trafiği türlerini engelleyebilir veya bunlara izin verebilir. Ek olarak, Güvenlik Duvarı istemcilere bir saldırıyı gösterebilen ağ paketlerindeki desenleri da belirleyecektir.

WFBS, Güvenlik Duvarı yapılandırılırken seçilmek üzere basit mod veya gelişmiş mod olarak iki seçeneğe sahiptir. Basit mod, Trend Micro tarafından önerilen varsayılan ayarlar ile güvenlik duvarını etkinleştirir. Güvenlik Duvarı ayarlarını özelleştirmek için gelişmiş modu kullanın.

İpucu: Trend Micro, Güvenlik Duvarını dağıtıp etkinleştirmeden önce diğer yazılım tabanlı güvenlik duvarlarını kaldırmanızı önerir.

Varsayılan Güvenlik Duvarı Basit Mod Ayarları

Güvenlik duvarı, istemci güvenlik duvarı koruma stratejinizi uygulamanız için size bir temel sağlayan varsayılan ayarları sağlar. Varsayılanlar, internet erişimi ihtiyacı ve FTP kullanarak dosyaları indirme veya yükleme gibi istemciler üzerinde mevcut olabilecek ortak koşulları içermeyi amacını taşır.

Not: Varsayılan olarak, WFBStüm yeni Gruplar ve istemciler üzerinde Güvenlik Duvarını devre dışı bırakır.

TABLO 6-2. Varsayılan Güvenlik Duvarı Ayarları

Güvenlik Düzeyi	Açıklama
Düşük	Gelen ve giden trafiğe izin verildi, yalnız ağ virüsleri engellendi.

Ayarlar	Durum
Davetsiz Misafir Algılama Sistemi	Devre dışı bırakıldı
Uyarı İletisi (gönderme)	Devre dışı bırakıldı

Kural Dışı Durum Adı	Eylem	Yön	Protokol	Port
DNS	İzin ver	Gelen ve giden	TCP/UDP	53
NetBIOS	İzin ver	Gelen ve giden	TCP/UDP	137, 138, 139, 445
HTTPS	İzin ver	Gelen ve giden	TCP	443
HTTP	İzin ver	Gelen ve giden	TCP	80
Telnet	İzin ver	Gelen ve giden	TCP	23
SMTP	İzin ver	Gelen ve giden	TCP	25
FTP	İzin ver	Gelen ve giden	TCP	21
POP3	İzin ver	Gelen ve giden	TCP	110
MSA	İzin ver	Gelen ve giden	TCP	16372, 16373

Konum	Güvenlik Duvarı Ayarları
Ofis İçi	Kapalı
Ofis Dışı	Kapalı

Trafik Filtreleme

Güvenlik duvarı, aşağıdaki ölçütlere dayanarak belirli trafik türlerini engellenebilmesini sağlayarak tüm gelen ve giden trafiği izler:

- Yön (gelen veya giden)
- Protokol (TCP/UDP/ICMP)
- Hedef bağlantı noktaları
- Hedef bilgisayar

Ağ Virüsleri Taraması Yapılıyor

Güvenlik Duvarı, bir ağ virüsünden etkilenip etkilenmediğini belirlemek için her veri paketini inceler.

Durum Denetlemesi

Güvenlik Duvarı, bir durum denetlemesi güvenlik duvarıdır; işlemlerin geçerli olmasını sağlamak için istemciye yapılan tüm bağlantıları izler. Bir işlemdeki özel koşulları belirleyebilir, hangi işlemin izlenmesi gerektiğini öngörebilir ve normal koşulların ne zaman ihlal edildiğini algılayabilir. Filtreleme kararları bu nedenle yalnız profillere ve ilkelere değil aynı zamanda bağlantıları analiz ederek ve önceden güvenlik duvarından geçen paketleri filtreleyerek kurulan bağlama da dayanır.

Davetsiz Misafir Algılama Sistemi

Güvenlik Duvarı Davetsiz Misafir Algılama Sistemi'ni (IDS) de içerir. IDS, istemcilere bir saldırıyı gösterebilen ağ paketlerindeki desenleri belirlemeye yardımcı olabilir. Güvenlik Duvarı, iyi bilinen aşağıdaki davetsiz misafirleri önlemeye yardımcı olabilir:

- **Büyük Parça:** Bu açıklardan yararlanan yazılım, IP datagramında aşırı büyük parçaları içerir. Bazı işletim sistemleri büyük parçaları düzgün biçimde işlemez ve kural dışı durumlar oluşturabilir veya diğer istenmeyen şekillerde davranabilir.
- **Ölüm Pingi:** Bir ölüm pingi (kısaltılmış hali **"**POD**"**), bir bilgisayara bozuk veya diğer şekillerde zararlı ping göndermeyi içeren bir bilgisayar saldırısı türüdür. Bir ping boyutu normal olarak 64 bayttır (veya IP başlığı dikkate alındığında 84 bayt); birçok bilgisayar sistemi maksimum IP paket büyüklüğü olan 65.535 bayttan daha büyük bir pingi işleyemez. Bu boyutta bir ping göndermek hedef bilgisayarı bozabilir.

- **Çakışan ARP:** Kaynak ve hedef IP adresleri aynı olduğunda bu durum ortaya çıkar.
- **SYN taşması:** SYN taşması, bir saldırganın bir hedefin sistemine ard arda `SYN` isteği gönderdiği servis reddi saldırısının bir biçimidir.
- **Çakışan Parça:** Bu açıklardan yararlanan yazılım, aynı IP datagramı içinde iki parça içerir ve datagram içindeki konumu paylaştığını gösteren uzaklıklara sahiptir. Bu, B parçasının tamamen A parçasının üzerine veya B parçasının kısmi olarak A parçasının üzerine yazıldığı anlamına gelebilir. Bazı işletim sistemleri, çakışan parçaları düzgün biçimde işleyemez. Bu işletim sistemleri, kural dışı durumlar oluşturabilir veya diğer istenmeyen şekillerde davranabilir. Bu, Teardrop Servis Reddi Saldırıları olarak adlandırılan durumun temelidir.
- **Teardrop Saldırısı:** Teardrop saldırısı, hedef makineye çakışan, aşırı büyük boyutlu, yük içeren IP parçaları göndermeyi içerir. Farklı işletim sistemlerinin TCP/IP parçalanması yeniden derleme kodundaki bir hata, parçaların uygun olmayan biçimde işlenmesine neden olur ve bunun sonucunda işletim sistemlerini kilitler.
- **Küçük Parça Saldırısı:** Son parça dışındaki parçaların 400 bayttan az olduğu, böylelikle parçanın muhtemelen bilerek yapıldığını gösteren durum. Küçük parçalar, servis reddi saldırılarında veya güvenlik önlemlerinin veya algılamasını atlatma girişiminde kullanılabilir.
- **Parçalanmış IGMP:** Bir istemci, parçalanmış bir Internet Grup Yönetimi Protokolü (IGMP) paketi aldığında istemcinin performansı düşebilir veya bilgisayar yanıt vermeyi durdurarak (askıda kalma) işlevi geri yüklemek için yeniden başlatmayı gerektirebilir.
- **LAND Saldırısı:** LAND saldırısı, bir bilgisayarın istenmeyen biçimde davranmasına neden olacak şekilde o bilgisayara özel bir tehlikeli, sahte paket gönderilmesinden oluşan bir DoS (Servis Reddi) saldırısıdır. Saldırı, hedef ana sistemin IP adresini ve hem kaynak hem hedef olarak açık bir bağlantı noktası içeren sahte bir `TCP SYN` paketi (bağlantı başlatma) göndermeyle ilişkilidir.

Durum Denetlemesi

Güvenlik Duvarı, bir durum denetlemesi güvenlik duvarıdır; işlemlerin geçerli olmasını sağlamak için istemciye yapılan tüm bağlantıları izler. Bir işlemdeki özel koşulları belirleyebilir, hangi işlemin izlenmesi gerektiğini öngörebilir ve normal koşulların ne zaman ihlal edildiğini algılayabilir. Filtreleme kararları bu nedenle yalnız profillere ve ilkelere değil aynı zamanda bağlantıları analiz ederek ve önceden güvenlik duvarından geçen paketleri filtreleyerek kurulan bağlama da dayanır.

Güvenlik Duvarını Yapılandırma

Not: Ofis İçi ve Ofis Dışı için Güvenlik Duvarını yapılandırın. Konum Tanıma devre dışı bırakılmışsa, Ofis İçi ayarları Ofis Dışı bağlantılar için kullanılacaktır. Bkz. *Konum Tanıma*, sayfa 9-6.

Gezinme Yolu: Güvenlik Ayarları > Grup Seç > Yapılandır > Güvenlik Duvarı > Ofis İçi/Ofis Dışı

ŞEKIL 6-2. Güvenlik Duvarı - Ofis İçi ekranı

Güvenlik Duvarını yapılandırmak için:

1. **Güvenlik Duvarı** ekranından, aşağıdaki seçenekleri gerektiği gibi güncelleyin:
   - **Güvenlik Duvarını Etkinleştir:** Grup ve konum için güvenlik duvarını etkinleştirmeyi seçin.
     - **Basit Mod:** Güvenlik duvarını varsayılan ayarlarla etkinleştirir. Bkz. *Varsayılan Güvenlik Duvarı Ayarları*, sayfa 6-9.
     - **Gelişmiş Mod:** Güvenlik duvarını özel ayarlarla etkinleştirir. Yapılandırma seçenekleri için bkz. *Gelişmiş Güvenlik Duvarı Seçenekleri*, sayfa 6-13.
2. **Kaydet**'i tıklatın. Değişiklikler hemen etkili olacaktır.

Gelişmiş Güvenlik Duvarı Seçenekleri

Belirli bir istemci grubuna ilişkin özel güvenlik ayarlarını yapılandırmak için Gelişmiş Güvenlik Duvarı seçeneklerini kullanın.

Gelişmiş güvenlik duvarı seçeneklerini yapılandırmak için:

1. **Güvenlik Duvarı** ekranından, **Gelişmiş Mod**'u seçin.
2. Aşağıdaki seçenekleri gerektiği gibi güncelleyin:
   - **Güvenlik Düzeyi:** Güvenlik düzeyi, kural dışı durum listesinde olmayan bağlantı noktaları için uygulanacak trafik kurallarını kontrol eder.
     - **Yüksek:** Gelen ve giden trafiği engeller.
     - **Orta:** Gelen trafiği engeller ve giden trafiğe izin verir.
     - **Düşük:** Gelen ve giden trafiğe izin verir.
   - Ayarlar
     - **Davetsiz Misafir Algılama Sistemi:** Davetsiz Misafir Algılama Sistemi, bir saldırıyı belirtebilecek ağ paketlerindeki desenleri tanımlar. Daha fazla bilgi için, bkz. *Davetsiz Misafir Algılama Sistemi*, sayfa 6-10.
     - **Uyarı İletilerini Etkinleştir:** WFBS bir ihlal belirlediğinde istemciye bildirilir.
   - **Kural dışı durumlar:** Kural dışı durum listesindeki bağlantı noktaları engellenmeyecektir. Daha fazla bilgi için, bkz. *Güvenlik Duvarı Kural Dışı Durumlarıyla Çalışma*, sayfa 6-14.
3. **Kaydet**'i tıklatın.

Güvenlik Duvarını Devre Dışı Bırakma

Gezinme Yolu: Güvenlik Ayarları > Grup Seç > Yapılandır > Güvenlik Duvarı > Ofis İçi/Ofis Dışı

Güvenlik Duvarını devre dışı bırakmak için:

1. Grup ve bağlantı türüne ilişkin güvenlik duvarını devre dışı bırakmak için, **Güvenlik Duvarını Etkinleştir** onay kutusunu temizleyin.
2. **Kaydet**'i tıklatın.

Not: Güvenlik Duvarını tamamen devre dışı bırakmak için, her iki bağlantı türü (Ofis İçi ve Ofis Dışı) için yukarıdaki işlemi tekrarlayın.

Güvenlik Duvarı Kural Dışı Durumlarıyla Çalışma

Kural Dışı Durumlar Yön, Protokol, Bağlantı Noktası ve Makineler temelinde farklı trafik türlerine izin veren veya bunları engelleyen özel ayarlardan oluşur.

Örneğin, bir salgın sırasında HTTP bağlantı noktası (bağlantı noktası **80**) dahil tüm istemci trafiğini engellemek isteyebilirsiniz. Ancak engellenen istemcilere internet erişimi vermek istiyorsanız kural dışı durum listesine Web proxy sunucusunu ekleyebilirsiniz.

Kural Dışı Durumlar Ekleme

Kural dışı bir durum ekleme:

1. **Kural Dışı Durumlar** bölümünde **Güvenlik Duvarı - Gelişmiş Mod** ekranından, **Ekle**'yi tıklatın.
2. Seçenekleri gerektiği gibi güncelleyin:
   - **Ad:** Kural dışı durum için benzersiz bir ad belirleyin.
   - **Eylem:** Seçilen protokol, bağlantı noktaları ve istemciler için trafiği **Engelle** veya **İzin Ver**.
   - **Yön: Gelen** internetten ağınıza akan trafik anlamındadır. **Giden** ağınızdan internete akan trafik anlamındadır.
   - **Protokol:** Bu dışlama için ağ trafiği protokolü.

- **Bağlantı noktaları**
  - **Tüm bağlantı noktaları** (varsayılan)
  - **Aralık**
  - **Belirtilen bağlantı noktaları:** Kişisel girişleri virgülle ayırın.
- **Makine**
  - **Tüm IP adresleri** (varsayılan)
  - **IP aralığı**
  - **Tek IP:** Belirli bir istemcinin IP adresi.

3. **Kaydet**'i tıklatın. **Güvenlik Duvarı Yapılandırması** ekranında kural dışı durum listesindeki yeni kural dışı durum görünür.

Kural Dışı Durumları Düzenleme

Kural dışı bir durumu düzenlemek için:

1. **Kural Dışı Durumlar** bölümünde **Güvenlik Duvarı - Gelişmiş Mod** ekranından, düzenlemek istediğiniz dışlamayı seçin.
2. **Düzenle**'yi tıklatın.
3. Seçenekleri gerektiği gibi güncelleyin. Daha fazla bilgi için, bkz. *Kural Dışı Durumlar Ekleme*, sayfa 6-14.
4. **Kaydet**'i tıklatın.

Kural Dışı Durumları Kaldırma

Kural dışı bir durumu kaldırmak için:

1. **Kural Dışı Durumlar** bölümünde **Güvenlik Duvarı - Gelişmiş Mod** ekranından, silmek istediğiniz dışlamayı seçin.
2. **Kaldır**'ı tıklatın.

Web Reputation Kullanma

Web Reputation, istenen herhangi bir URL'yi Trend Micro Web Güvenliği veritabanına dayanarak kontrol eder ve böylece olası güvenlik riskleri doğrudan URL'lere erişimi engeller. İstemcinin bulunduğu yere bağlı olarak (Ofis İçi/Ofis Dışı) farklı bir güvenlik düzeyi yapılandırın.

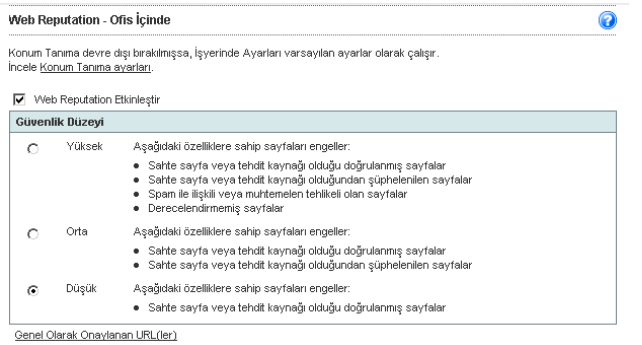
Web Reputation sizin güvenli olduğuna inandığınız bir URL'yi engelliyorsa, o URL'yi Onaylanan URL listesine ekleyin. Onaylanan URL listesine bir URL eklemeye ilişkin bilgi için, ayrıntılar için bkz. *Onaylanan URL'ler*, sayfa 9-8.

Web Reputation Yapılandırma

Gezinme Yolu: Güvenlik Ayarları > Grup Seç > Yapılandır > Web Reputation > Ofis İçi/Ofis Dışı

Web Reputation, her HTTP isteğinde Trend Micro Security veritabanını sorgulayarak istenen tüm URL'lerin olası güvenlik riskini değerlendirir.

Not: Ofis İçi ve Ofis Dışı için Web Reputation'ı yapılandırın. Konum Tanıma devre dışı bırakılmışsa, Ofis İçi ayarları Ofis Dışı bağlantılar için kullanılacaktır. Bkz. *Konum Tanıma*, sayfa 9-6.



ŞEKIL 6-3. Güvenlik Ayarları > Web Reputation ekranı

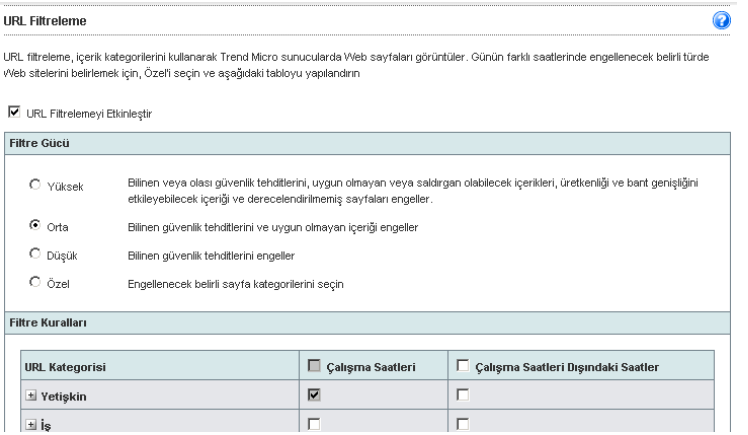
Web Reputation ayarlarını düzenlemek için:

1. **Web Reputation** ekranından, aşağıdaki seçenekleri gerektiği gibi güncelleyin:
   - **Web Reputation'ı etkinleştir**
   - **Güvenlik Düzeyi**
     - **Yüksek:** Doğrulanmış sahte sayfalar veya tehdit kaynakları, şüpheli sahte sayfaları veya tehdit kaynakları, istenmeyen posta ile ilişkili veya muhtemelen tehlikeli olan, derecelendirilmemiş sayfaları engeller
     - **Orta:** Doğrulanmış sahte sayfalar veya tehdit kaynakları, şüpheli sahte sayfaları veya tehdit kaynakları olan sayfaları engeller
     - **Düşük:** Sahte sayfa veya tehdit kaynağı olduğu doğrulanmış sayfaları engeller
2. Onaylanan Web siteleri listesini değiştirmek için, **Genel Olarak Onaylanan URL(ler)** seçeneğini tıklatın ve Genel Ayarlar ekranından ayarlarınızı değiştirin.
3. **Kaydet**'i tıklatın.

URL Filtrelemesini Yapılandırma

Gezinme Yolu: Güvenlik Ayarları > Grup Seç > Yapılandır > URL Filtrelemesi

İnternet kaynaklı istenmeyen içeriği engellemek için URL filtrelemesini kullanın. Özel seçeneğini işaretleyerek günün farklı zamanlarında engellenecek özel Web sitesi türlerini seçebilirsiniz. Ayrıca günün farklı saatlerinde Web sitelerini engelleyen Çalışma Saatlerini ve Çalışma Saatleri Dışındaki Saatleri tanımlayın.



ŞEKIL 6-4. Güvenlik Ayarları > URL Filtreleme ekranı

URL Filtrelemesini yapılandırmak için:

1. URL Filtrelemesi ekranından aşağıdakileri gerektiği gibi güncelleyin:
   - **URL Filtrelemeyi Etkinleştir**
   - **Filtre Gücü**
     - **Yüksek:** Bilinen veya olası güvenlik tehditlerini, uygun olmayan veya saldırgan olabilecek içerikleri, üretkenliği ve bant genişliğini etkileyebilecek içeriği ve derecelendirilmemiş sayfaları engeller.
     - **Orta:** Bilinen güvenlik tehditlerini ve uygun olmayan içeriği engeller
     - **Düşük:** Bilinen güvenlik tehditlerini engeller
     - Özel: Kendi kategorilerinizi ve çalışma saatlerinde veya çalışma saatleri dışındaki saatlerde kategorilerin engellenmesini isteyip istemediğinizi seçin.
2. **Çalışma Saatlerinizi** tanımlayın.
3. Onaylanan Web Siteleri listesini değiştirmek için, **Genel Olarak Onaylanan URL(ler)** seçeneğini tıklatın ve Genel Ayarlar ekranından ayarlarınızı değiştirin.
4. **Kaydet**'i tıklatın.

Behavior Monitoring Kullanma

Aracılar, istemcilerin işletim sistemi veya yüklenen yazılım üzerindeki normal olmayan değişikliklerini sürekli olarak izler. Yöneticiler (veya kullanıcılar), belirli programların izlenen değişikliği ihlal ederken başlatılmasına veya belirli programların tamamen engellenmesine izin veren kural dışı durum listeleri oluşturabilir. Ek olarak, geçerli bir dijital imza içeren programların başlatılmasına her zaman izin verilir.

İzlenen değişiklere ilişkin tanımı ve varsayılan değeri görüntülemek için aşağıdaki tabloya bakın.

TABLO 6-3. İzlenen Olası Değişiklikler

İzlenen Değişiklik	Açıklama	Varsayılan Değer
Çoğaltılan Sistem Dosyası	Birçok kötü amaçlı program, Windows sistem dosyaları tarafından kullanılan dosya adlarını kullanarak kendilerinin veya diğer kötü amaçlı programların kopyalarını oluşturur. Bu genelde sistem dosyalarının üzerine yazılma veya değiştirilmesi şeklinde yapılır. Böylece algılanmalarını ve kullanıcıların kötü amaçlı dosyaları silmelerini engeller.	Gerektiğinde sor
Hosts Dosyası Değişikliği	Hosts dosyası etki alanı adlarıyla IP adreslerini eşler. Çoğu zararlı program, Hosts dosyasında değişiklik yaparak Web tarayıcısının virüslü, var olmayan veya sahte Web sitelerine yönlendirilmesini sağlar.	Her zaman engelle
Şüpheli Davranış	Şüpheli davranış, normal programlar tarafından nadiren gerçekleştirilen belirli bir eylem veya eylem grubu olabilir. Şüpheli davranış gösteren programlar dikkatle kullanılmalıdır.	Gerektiğinde sor
Sistem Dosyasında Değişiklik	Bazı Windows sistem dosyaları başlangıç programları ve ekran koruyucusu ayarları gibi belirli sistem davranışlarını belirler. Birçok kötü amaçlı program sistem dosyalarını, kendilerini başlangıçta otomatik olarak başlatacak ve sistem davranışını denetleyecek şekilde yapılandırır.	Her zaman engelle

TABLO 6-3. İzlenen Olası Değişiklikler (Devamı)

İzlenen Değişiklik	Açıklama	Varsayılan Değer
Yeni Internet Explorer Eklentisi	Casus yazılım/greyware programları genellikle, araç çubukları ve Tarayıcı Yardımcı Nesneleri gibi istenmeyen Internet Explorer eklentileri yükler.	Gerektiğinde sor
Internet Explorer Ayar Değişikliği	Birçok virüs/casus yazılım programı; ana sayfa, güvenilen Web siteleri, proxy sunucu ayarları ve menü uzantıları gibi Internet Explorer ayarlarını değiştirir.	Her zaman engelle
Güvenlik İlkesi Değişikliği	Windows Güvenlik İlkesi'nde yapılan değişiklikler, istenmeyen uygulamaların çalışmasına ve sistem ayarlarını değiştirmesine izin verebilir.	Her zaman engelle
Güvenlik Duvarı İlkesi Değişikliği	Windows Güvenlik Duvarı İlkesi, ağa erişimi olan uygulamaları, iletişime açık bağlantı noktalarını ve bilgisayarla iletişim kurabilecek IP adreslerini tanımlar. Birçok kötü amaçlı program kendilerinin ağa ve Internet'e erişmelerine izin verecek şekilde ilkeyi değiştirir.	Gerektiğinde sor
Program Kitaplığı Sızdırma	Bir çok kötü amaçlı program Windows'u otomatik olarak bir program kitaplığı (DLL) yüklemek üzere yapılandırır. Bu sayede bir uygulamanın her başlatılışında DLL içinde kötü amaçlı rutinlerin çalışması sağlanır.	Gerektiğinde sor
Kabuk Değişikliği	Bir çok kötü amaçlı program kendilerini belirli dosya türleriyle eşleştirmek için Windows kabuk ayarlarını değiştirir. Bu prosedür, kullanıcı Windows Gezgini'nde ilişkili dosyaları açtığında kötü amaçlı programların otomatik olarak başlatılmasını sağlar. Windows kabuk ayarlarına yapılan değişiklikler, kötü amaçlı programların izlenmesini ve yasal uygulamalarla birlikte başlatılmasını da sağlayabilir.	Gerektiğinde sor

TABLO 6-3. İzlenen Olası Değişiklikler (Devamı)

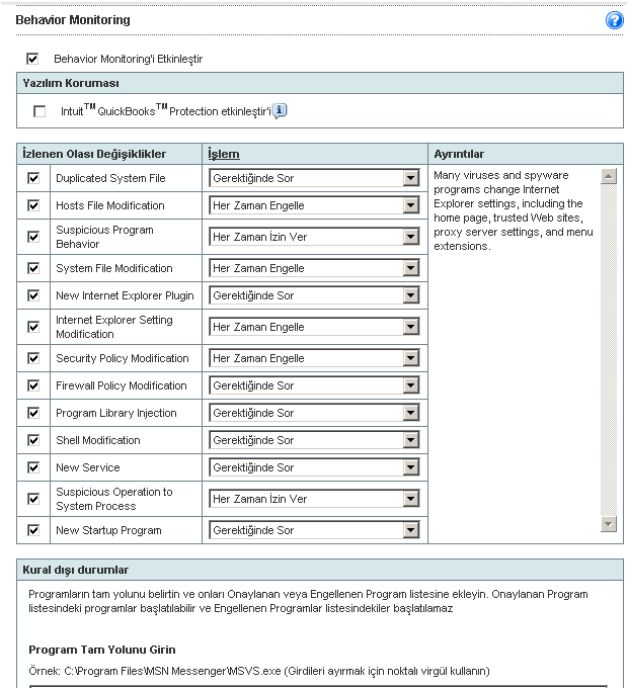
İzlenen Değişiklik	Açıklama	Varsayılan Değer
Yeni Hizmet	Windows hizmetleri, özel işlevleri olan ve genellikle tam yönetici erişimine sahip olarak arka planda sürekli olarak çalışan işlemlerdir. Zararlı programlar bazen gizli kalmak için kendilerini hizmet gibi yükler.	Gerektiğinde sor
Sistem İşleminde Değişiklik	Birçok kötü amaçlı program yerleşik Windows işlemlerinde değişik eylemler gerçekleştirebilir. Bu eylemler, çalışan işlemleri sonlandırma veya değiştirme olabilir.	Gerektiğinde sor
Yeni Başlangıç Programı	Bir çok kötü amaçlı program Windows'u otomatik olarak bir program kitaplığı (DLL) yüklemek üzere yapılandırır. Bu sayede bir uygulamanın her başlatılışında DLL içinde kötü amaçlı rutinlerin çalışması sağlanır.	Gerektiğinde sor

Behavior Monitoring'in diğer bir özelliği EXE ve DLL dosyalarını silinmeye veya değiştirilmeye karşı korur. Bu ayrıcalığa sahip kullanıcılar özel klasörlerini koruyabilir. Ek olarak, kullanıcılar tüm Intuit QuickBooks programlarının toplu olarak korunmasını seçebilir.

Behavior Monitoring Yapılandırma

Gezinme Yolu: Güvenlik Ayarları > Grup Seç > Yapılandır > Behavior Monitoring

Behavior Monitoring, istemcileri, işletim sisteminde, kayıt defteri girdilerinde, diğer yazılımlarda veya dosya ve klasörlerde yapılabilecek yetkisiz değişikliklerden korur.



ŞEKIL 6-5. Behavior Monitoring ekranı

Behavior Monitoring ayarlarını değiştirmek için:

1. **Behavior Monitoring** ekranından, aşağıdaki seçenekleri gerektiği gibi güncelleyin:
   - **Behavior Monitoring'i Etkinleştir**

     Not: **Güvenlik Ayarları > Grup Seç > Yapılandır > İstemci Ayrıcalıkları** sekmelerine gidin ve **Behavior Monitoring bölümünde Kural dışı durum listesini düzenle**'yi seçin.

   - **Intuit™ QuickBooks™ Korumasını Etkinleştir:** Tüm Intuit QuickBooks dosyalarını ve klasörlerini diğer programlar tarafından yapılacak yetkisiz değişiklere karşı korur. Bu özelliği etkinleştirilmesi Intuit QuickBooks programları içinde yapılan değişiklikleri etkilemez, yalnız diğer yetkisiz uygulamalar tarafından dosyalara yapılan değişiklikleri önler.

     Aşağıdaki ürünler desteklenir:

     QuickBooks Basit Başlatma

     QuickBooks Pro

     QuickBooks Premier

     QuickBooks Çevrimiçi
   - **USB eklenti cihazlarındaki uygulamaların otomatik olarak açılmasını önler:** USB cihazlarındaki programların istemciler üzerinde otomatik olarak çalıştırılmasını durdurmak için bu seçeneği işaretleyin.
   - **İzlenen Olası Değişiklikler:** İzlenen her değişiklik için **Her Zaman İzin Ver**, **Gerektiğinde Sor** veya **Her Zaman Engelle** seçeneklerini seçin. Farklı değişikliklere ilişkin bilgi için bkz. Tablo 6-3, sayfa 6-19.
   - **Kural Dışı Durumlar:** Kural dışı programlar **Onaylanan Program Listesi** ve **Engellenen Program Listesi** içerir: **Engellenen Program Listesi** içindeki programlar asla başlatılamazken, **Engellenen Program Listesi** içindeki programlar izlenen değişikliği ihlal etseler bile başlatılabilir.
     - **Programın Tam Yolu:** Programın tam yolunu yazın. Birden fazla girişleri noktalı virgülle (;) ayırın. **Onaylanan Programlar Listesine Ekle** veya **Engellenen Programlar Listesine Ekle** seçeneklerini tıklatın. Gerekirse yolları belirtmek için ortam değişkenlerini kullanın. Desteklenen değişkenlerin listesi için bkz. *Tablo 6-4*, sayfa 6-24.

- **Onaylanan Programlar Listesi:** Bu listedeki programlar (maksimum 100) başlatılabilir. Bir girişi silmek için ilişkili simgesini tıklatın.
- **Engellenen Programlar Listesi:** Bu listedeki programlar (maksimum 100) kesinlikle başlatılamaz. Bir girişi silmek için ilişkili simgesini tıklatın.

2. **Kaydet**'i tıklatın.

Ortam Değişkenleri

WFBS istemci üzerindeki özel klasörleri belirtmek için ortam değişkenlerini destekler. Özel klasörler için kural dışı durumlar oluşturan bu değişkenleri kullanın. Aşağıdaki tabloda kullanılabilir değişkenler açıklanır:

TABLO 6-4. Desteklenen Değişkenler

Ortam Değişkeni	İşaret ettiği yer...
$windir$	Windows klasörü
$rootdir$	kök klasör
$tempdir$	Windows geçici klasörü
$programdir$	Program Dosyaları klasörü

TrendSecure

TrendSecure, kullanıcıların güvenli bir şekilde Web'de gezinmelerini sağlayan bir dizi tarayıcı tabanlı araç içerir (TrendProtect ve Transaction Protector). TrendProtect, kullanıcıları kötü amaçlı web siteleri ve kimlik avı web siteleri hakkında uyarır. Transaction Protector, erişim noktasının özgünlüğünü kontrol ederek kablosuz bağlantınızın güvenliğini belirler.

TrendSecure, kablosuz bağlantınızın güvenliğine bağlı olarak rengi değiştiren bir tarayıcı araç çubuğu ekler. Aşağıdaki özelliklere erişmek için araç çubuğu düğmesini de tıklatabilirsiniz:

- **Wi-Fi Advisor:** SSID'lerinin geçerliliğine, kimlik doğrulama yöntemlerine ve şifreleme gereksinimlerine dayanılarak kablosuz ağların güvenliğini denetler.

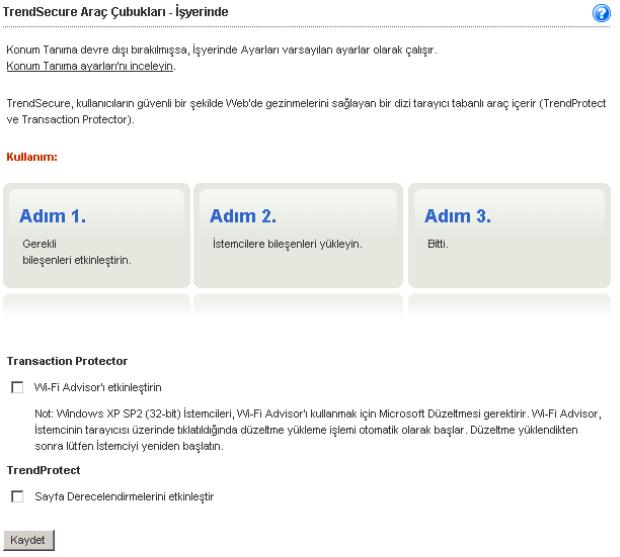
- **Sayfa Derecelendirmeleri:** Geçerli sayfanın güvenliğini belirler.

Not: Ofis İçi ve Ofis Dışı için TrendSecure ayarlarını yapılandırın. Konum Tanıma devre dışı bırakılmışsa, Ofis İçi ayarları Ofis Dışı bağlantılar için kullanılacaktır. Bkz. *Konum Tanıma*, sayfa 9-6.

TrendSecure Yapılandırma

Gezinme Yolu: Güvenlik Ayarları > Grup Seç > Yapılandır > TrendSecure Araç Çubukları > Ofis İçi/Ofis Dışı

TrendSecure araçları kullanılabilirliğini, konumlarına bağlı olarak kullanıcılar için yapılandırın.



ŞEKIL 6-6. TrendSecure Araç Çubukları - Ofis İçi ekranı

TrendSecure araçlarının kullanılabilirliğini düzenlemek için:

1. **TrendSecure Ofis İçi/Ofis Dışı** ekranından, aşağıdaki seçenekleri gerektiği gibi güncelleyin:
   - **Wi-Fi Advisor'ı etkinleştirin:** SSID'lerinin geçerliliğine, kimlik doğrulama yöntemlerine ve şifreleme gereksinimlerine dayanılarak kablosuz ağların güvenliğini denetler.
   - **Sayfa Derecelendirmelerini etkinleştir:** Geçerli sayfanın güvenliğini belirler.
2. **Kaydet**'i tıklatın.

Not: TrendSecure Araç Çubukları yalnız Web konsolundaki aracılar tarafından kullanılabilir. Kullanıcılar, aracının konsolundan araçları yüklemeli veya kaldırmalıdır.

POP3 Posta Taramasını Yönetme

POP3 Posta Taraması ve Trend Micro Anti-Spam araç çubuğu eklentisi, istemcileri gerçek zamanlı olarak POP3 e-posta iletileri aracılığıyla aktarılan güvenlik risklerine ve istenmeyen postaya karşı korur.

Not: Varsayılan olarak, POP3 Posta Taraması yalnız Gelen Kutusu ve Önemsiz Posta klasörlerine bağlantı noktası 110 aracılığıyla gönderilen yeni iletileri tarar. Exchange Server 2007 tarafından varsayılan olarak kullanılan güvenli POP3'ü (SSL POP3) desteklemez.

POP3 Posta Tarama Gereksinimleri

POP3 Posta Taraması aşağıdaki posta istemcilerini destekler:

- Microsoft Outlook™ 2000, 2002 (XP), 2003 ve 2007
- Outlook Express™ 6.0, Service Pack 2 ile (yalnız Windows XP üzerinde)

- Windows Mail™ (yalnız Windows Vista için)
- Mozilla Thunderbird 1.5 ve 2.0

Not: POP3 Posta Taraması IMAP iletilerindeki güvenlik risklerini ve istenmeyen postayı algılayamaz.

Anti-Spam Araç Çubuğu Gereksinimleri

Trend Micro Anti-Spam araç çubuğu aşağıdaki posta istemcilerini destekler:

- Microsoft Outlook 2000, 2002 (XP), 2003 ve 2007
- Outlook Express 6.0, Service Pack 2 ile (yalnız Windows XP için)
- Windows Mail (yalnız Windows Vista için)

Anti-Spam araç çubuğu aşağıdaki işletim sistemlerini destekler:

- Windows XP SP2 32-bit
- Windows Vista 32 ve 64 bit

Posta Taraması Yapılandırması

Gezinme Yolu: Güvenlik Ayarları > Grup Seç > Yapılandır > Posta Taraması

Posta Taraması kullanılabilirliğini düzenlemek için:

1. **Posta Taraması** ekranından aşağıdakileri gerektiği gibi güncelleyin:
   - **POP3 postası için gerçek zamanlı taramayı etkinleştirin**
   - **Trend Micro Anti-Spam araç çubuğunu etkinleştir**
2. **Kaydet**'i tıklatın.

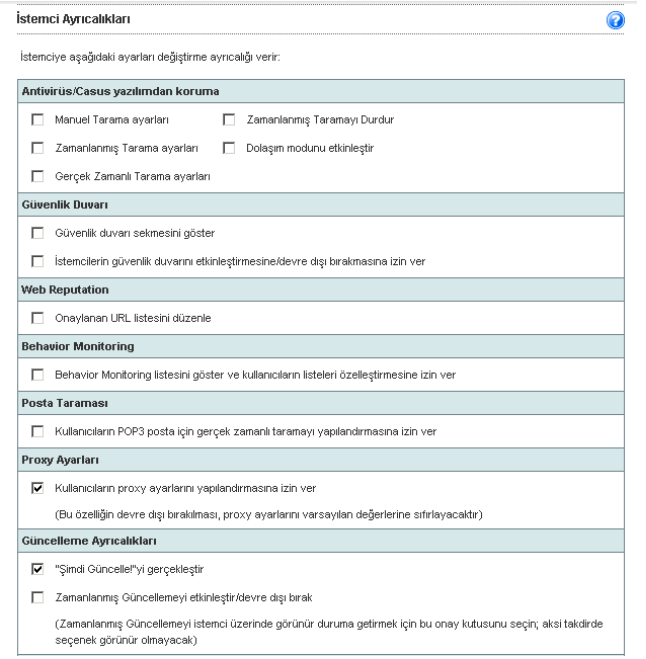
İstemci Ayrıcalıkları

Gezinme Yolu: Güvenlik Ayarları > Grup Seç > Yapılandır > İstemci Ayrıcalıkları

Kullanıcıların, bilgisayarlarında yüklü aracının ayarlarını değiştirmesine izin vermek için İstemci Ayrıcalıkları verin.

İpucu: Organizasyonunuz içinde düzenlenmiş bir güvenlik ilkesini gerçekleştirmek için Trend Micro kullanıcılara sınırlı ayrıcalık vermenizi önerir. Bu, kullanıcıların tarama ayarlarını değiştirmemesini veya Client/Server Security Agent'i bellekten kaldırmamasını sağlar.

İstemci Ayrıcalıklarını Yapılandırma



ŞEKIL 6-7. İstemci Ayrıcalıkları ekranı

İstemcilere ayrıcalıklar vermek için:

1. **İstemci Ayrıcalıkları** ekranından, aşağıdakileri gerektiği gibi güncelleyin:
   - **Antivirüs/Casus yazılımdan koruma**
     - **El ile Tarama ayarları**
     - **Zamanlanmış Tarama ayarları**
     - **Gerçek Zamanlı Tarama ayarları**
     - **Zamanlanmış Taramayı durdurur**
     - **Dolaşım modunu etkinleştirir**
   - **Firewall**
     - **Güvenlik duvarı sekmesini gösterir**
     - **İstemcilerin güvenlik duvarını etkinleştirmesine/devre dışı bırakmasına izin verir**

     Not: Kullanıcıların güvenlik duvarını etkinleştirmesine veya devre dışı bırakmasına izin verirseniz, bu ayarları Web konsolundan değiştiremezsiniz. Kullanıcılara bu ayrıcalığı vermezseniz, bu ayarları Web konsolundan değiştirebilirsiniz. Aracıya ilişkin **Yerel Güvenlik Duvarı ayarları** altındaki bilgi Web konsolu değil her zaman aracı tarafından yapılandırılan ayarları yansıtır.

   - **Web Reputation**
     - **Onaylanan URL listesini düzenler**
   - **Behavior Monitoring**
     - **Behavior Monitoring sekmesini gösterir ve kullanıcıların listeleri özelleştirmesine izin verir:** Kullanıcıların Behavior Monitoring'i etkinleştirmesine/devre dışı bırakmasına ve Kural Dışı Durum Listesi ve Yazılım Koruma Listesini yapılandırmasına izin verir.
   - **Posta Taraması**
     - **Kullanıcıların POP3 posta için gerçek zamanlı taramayı yapılandırmasına izin verir**
   - **Proxy Ayar**ları
     - **Kullanıcıların proxy ayarlarını yapılandırmasına izin verir**

- **Güncelleme Ayrıcalıkları**
  - **"Şimdi Güncelle"yi gerçekleştirir**
  - **Zamanlanmış Güncellemeyi etkinleştirir/devre dışı bırakır**
- **Ayarları Güncelleme**
  - **Trend Micro ActiveUpdate Sunucusundan indirme:** Kullanıcılar güncellemeyi başlattıklarında aracı **Güncelleme Kaynağı** ekranında belirtilen güncelleme kaynağından güncellemeleri alır. Güncelleme başarısız olursa, aracılar Security Server kaynağından güncelleme yapmayı dener. **Trend Micro ActiveUpdate Server kaynağından indir** seçeneğin işaretlenmesi, Security Server kaynağından güncelleme başarısız olursa Trend Micro ActiveUpdate Server kaynağından güncellemeyi denemesi için aracıları etkinleştirir.

İpucu: Ofis dışında olduklarında taşınabilir istemciler üzerindeki aracıların güncellenmesini sağlamak için **Trend Micro ActiveUpdate Server kaynağından indir** seçeneğini etkinleştirin.

  - **Zamanlanmış Güncellemeyi Etkinleştirme**
  - **Program güncellemesini ve düzeltme dağıtımını devre dışı bırakma**
- **İstemci Güvenliği**
  - **Yüksek**
    - İstemci kayıt defteri anahtarları ve istemci yükleme klasörüne yazma erişimi vermeyi reddeder.
    - İstemci işlemlerinin ve hizmetlerinin durdurulmasını engeller.

- **Normal:** Aracı klasörlerine, dosyalarına ve kayıt defteri girişlerine okuma/yazma erişimine izin verir.

Not: **Yüksek** seçeneğini seçerseniz, aracı klasörlerinin, dosyalarının ve kayıt defteri girişlerinin erişim izni ayarları Program Files klasöründen aktarılır (Windows Vista/2000/XP/Server 2003 çalıştıran istemciler için).
Bu nedenle, Windows dosyasının veya Program Files klasörünün izin ayarları (Windows içinde güvenlik ayarları) tam okuma/yazma erişimine izin verecek şekilde belirlenir, **Yüksek** seçilmesi hala istemcilerin Client/Server Security Agent klasörlerine, dosyalarına ve kayıt defteri girişlerine tam okuma/yazma erişimi izni verir.

---

2. **Kaydet**'i tıklatın.

Karantinayı Yönetme

Karantina dizini etkilenen dosyaları depolar. Karantina dizini kendini istemci veya başka bir sunucu üzerine yerleştirebilir. Geçersiz bir karantina dizini belirlendiğinde aracılar istemci üzerinde varsayılan karantina dizinini kullanır:

```
C:\Program Files\Trend Micro\Client Server Security Agent\SUSPECT
```

Sunucundaki varsayılan klasör:

```
C:\Program Files\Trend Micro\Security Server\PCCSRV\Virus
```

Not: CSA, ağ bağlantı problemi gibi herhangi bir nedenle Security Server'a dosya gönderemiyorsa dosya istemci şüpheli klasöründe kalır. Aracı, Security Server'a yeniden bağlanıldığında dosyayı yeniden göndermeye çalışır.

Karantina Dizinini Yapılandırma

Gezinme Yolu: Güvenlik Ayarları > Grup Seç > Yapılandır > Karantina

ŞEKIL 6-8. Karantina Dizini ekranı

Karantina dizinini belirlemek için:

1. Karantina Dizini ekranından aşağıdakileri gerektiği gibi güncelleyin:
   - **Karantina dizini:** Etkilenen dosyaları depolamak için Tekdüzen Kaynak Konum Belirleyicisi (URL) veya Evrensel Adlandırma Kuralı (UNC) yolu yazın. Örneğin, `http://www.example.com/quarantine` veya `\\TempServer\Quarantine`.
2. **Kaydet**'i tıklatın.

Ek A

Sorun Giderme ve Sık Sorulan Sorular

Bu ekte, genel sorunlara ve sorulara ilişkin çözüm ve yanıtlar verilmektedir.

Bu ekte ele alınan başlıklar şunlardır:

Sorun Giderme

Bu bölüm, WFBS'yı yüklerken veya kullanırken karşılaşabileceğiniz sorunları gidermenize yardımcı olmaktadır.

Kısıtlı Bağlantılara Sahip Ortamlar

Ortamınızda Internet'e bağlanmaya yönelik kısıtlamalar varsa, Internet bağlantısının olmaması veya kapalı LAN durumunda, şu prosedürleri kullanın:

Aracılar Security Server'a erişebiliyorsa:

1. Client Packager'ı (*Client Packager ile Yükleme*, sayfa 3-8) kullanarak yeni bir paket oluşturun.
2. Paketi bilgisayara el ile yükleyin.

Böylece, aracı, güvenlik ayarlarını sunucuda yapılandırıldığı şekilde uygular.

Aracılar Security Server'a erişemiyorsa:

1. Client Packager'ı kullanarak yeni bir paket oluşturun.
2. Paketi bilgisayara el ile yükleyin.

Client Packager Yükleme Sonrası Sorunlar

Aracıyı Client Packager kullanarak yüklediyseniz ve sorunlarla karşılaşıyorsanız, şunları göz önünde bulundurun:

- **Yükle:** Aracı Security Server'a bağlanamazsa, istemci varsayılan ayarları koruyacaktır. Grup ayarlarını, yalnızca, istemci Security Server'a bağlanabildiği zaman alabilir.
- **Yükseltme:** Aracıyı Client Packager ile yükseltmede sorun yaşıyorsanız, Trend Micro öncelikle aracının önceki sürümünü kaldırmanızı, ardından da yeni sürümü yüklemenizi önerir.

Program Ayarlarını Kaydetme ve Geri Yükleme

WFBS programınızı geri almak için, WFBS veritabanının ve önemli yapılandırma dosyalarının bir kopyasını kaydedebilirsiniz. Birtakım sorunlarla karşılaşıyorsanız ve WFBS'yı yeniden yüklemek istiyorsanız ya da eski yapılandırmaya geri dönmek istiyorsanız, bunu gerçekleştirebilirsiniz.

Geri alma veya yeniden yükleme işleminden sonra program ayarlarını geri yüklemek için:

1. Trend Micro Security Server Master Service'ı durdurun.
2. Aşağıdaki dosya ve klasörleri klasörden farklı bir konuma el ile kopyalayın:

   UYARI! **Bu görev için yedekleme araçlarını veya uygulamalarını kullanmayın.**

   ```
   C:\Program Files\Trend Micro\Security Server\PCCSRV
   ```

   - **`ofcscan.ini`:** Genel ayarları içerir.
   - **`ous.ini`:** Antivirüs bileşen dağıtımı için güncelleme kaynağı tablosunu içerir.
   - **`Private` klasörü:** Güvenlik duvarı ve güncelleme kaynağı ayarlarını içerir.
   - **`Web\TmOPP` klasörü:** Salgın Savunması ayarlarını içerir.
   - **`Pccnt\Common\OfcPfw.dat`:** Güvenlik duvarı ayarlarını içerir.
   - **`Download\OfcPfw.dat`:** Güvenlik duvarı dağıtım ayarlarını içerir.
   - **`Log` klasörü:** Sistem olaylarını ve bağlantı doğrulama günlüğünü içerir.
   - **`Virus` klasörü:** WFBS'nın etkilenen dosyaları karantinaya aldığı klasör.
   - **`HTTDB` klasörü:** WFBS veritabanını içerir.
3. WFBS'yı kaldırın.
4. Yüklemeyi yeniden gerçekleştirin. WFBS *Yükleme Kılavuzu*'na başvurun.
5. Ana yükleyici tamamlandıktan sonra, hedef bilgisayarda Trend Micro Security Server Master Service'ı durdurun.
6. Yedekleme dosyasından virüs deseni sürümünü güncelleyin:
   a. Yeni sunucudan geçerli virüs deseni sürümünü edinin.

   ```
   \Trend Micro\Security Server\PCCSRV\Private\component.ini.
   [6101]

   ComponentName=Virüs deseni

   Sürüm=xxxxxx 0 0
   ```

b. Yedeklenen dosyada virüs deseninin sürümünü güncelleyin:

`\Private\component.ini`

Not: Security Server yükleme yolunu değiştirirseniz, yedekleme dosyaları `ofcscan.ini` ve `\private\ofcserver.ini`'de yol bilgilerini güncellemeniz gerekir.

---

7. Oluşturduğunuz yedeklemeleri, hedef makinede `PCCSRV` klasöründeki WFBS veritabanının ve ilgili dosya ve klasörlerin üzerine yazın.
8. Trend Micro Security Server Master Service'ı yeniden başlatın.

Bazı Bileşenler Yüklü Değil

Trend Micro ürünlerinin çeşitli bileşenlerinin lisansları bölgeye göre farklılık gösterebilir. Yüklemeden sonra, Kayıt Anahtarınızın/Etkinleştirme Kodunuzun kullanmanıza izin verdiği bileşenlerin bir özetini göreceksiniz. Lisanslarına sahip olduğunuz bileşenleri doğrulamak için satıcınıza veya tedarikçinize başvurun.

Web Konsoluna Erişilemiyor

Bu bölümde, Web konsoluna erişememenin olası nedenleri ele alınmaktadır.

Tarayıcı Önbelleği

WFBS'nın önceki bir sürümünden yükselttiyseniz, Web tarayıcı ve proxy sunucu önbellek dosyaları Web konsolunun yüklenmesini engelleyebilir. Tarayıcınızda ve Trend Micro Security Server ile Web konsoluna erişmek için kullandığınız bilgisayar arasında bulunan tüm proxy sunucularında önbelleği temizleyin.

SSL Sertifikası

Ayrıca, Web sunucunuzun düzgün çalıştığını da doğrulayın. SSL kullanıyorsanız, SSL sertifikanızın geçerliliğini koruduğunu doğrulayın. Ayrıntılar için Web sunucusu belgelerine bakın.

Sanal Dizin Ayarları

Web konsolunu IIS sunucusunda çalıştırıyorsanız ve aşağıdaki ileti görünüyorsa, sanal dizin ayarlarıyla ilgili bir sorun olabilir:

Sayfa görüntülenemiyor
HTTP Hatası 403.1 - İzin Yok: Yürütme erişimi reddedildi.
Internet Information Services (IIS)

Konsola erişmek için aşağıdaki adreslerden herhangi biri kullanıldığında bu ileti görünebilir:

`http://<sunucu adı>/SMB/`

`http://<sunucu adı>/SMB/default.htm`

Ancak, şu adresi kullanırken konsol sorunsuz bir şekilde açılabilir:

`http://<sunucu adı>/SMB/console/html/cgi/cgichkmasterpwd.exe`

Bu sorunu çözmek için, SMB sanal dizininin yürütme izinlerini kontrol edin.

Komut dosyalarını etkinleştirmek için:

1. Internet Information Services (IIS) yöneticisini açın.
2. SMB sanal dizininde, **Özellikler**'i seçin.
3. **Sanal Dizin** sekmesini seçin ve yürütme izinlerini hiçbiri seçeneğinden **Komut Dosyaları**'na getirin. Ayrıca, istemci yükleme sanal dizininin yürütme izinlerini de değiştirin.

Web Konsolunda Yanlış Sayıda İstemci

Web konsolunda yansıtılan istemci sayısının yanlış olduğunu görebilirsiniz.

Bu, aracıyı kaldırdıktan sonra istemci kayıtlarını veritabanında tutmaya devam ettiğinizde gerçekleşir. Örneğin, aracıyı kaldırırken istemci-sunucu iletişimi kaybolursa, sunucu aracının kaldırılmasıyla ilgili bildirim almaz. Sunucu istemci bilgilerini veritabanında tutmaya ve istemci simgesini konsolda göstermeye devam eder. Aracıyı yeniden yüklediğinizde, sunucu veritabanında yeni bir kayıt oluşturur ve konsolda yeni bir simge görüntüler.

Yinelenen istemci kayıtlarını kontrol etmek için Web konsolundan Bağlantı Doğrulama özelliğini kullanın.

Yüklemeden Sonra İstemci Simgesi Görünmüyor

Aracıyı yükledikten sonra istemci simgesinin Web konsolunda görünmediğini fark edebilirsiniz. Bu, istemci sunucuya durumunu iletemediğinde gerçekleştir.

İstemciler ve Web konsolu arasındaki iletişimi kontrol etmek için:

- İstemcide yeni bir Web tarayıcısı açın, adres metin kutusuna `https://{Trend Micro Security Server_Name}:{port number}/SMB/cgi/cgionstart.exe` yazın ve ardından ENTER'a basın. Sonraki ekranda "-2" görünmesi, istemcinin sunucuyla iletişim kurabildiği anlamına gelir. Bu, aynı zamanda, istemcinin kaydı olmayabilir ve sorunun sunucu veritabanında olduğunu belirtebilir.
- Ping ve telnet kullanarak istemci-sunucu iletişiminin var olduğunu doğrulayın.
- Kısıtlı bant genişliğine sahipseniz, bunun sunucu ve istemci arasında bağlantı zaman aşımına neden olup olmadığını kontrol edin.
- Sunucudaki \PCCSRV klasörünün paylaşma ayrıcalıklarına sahip olup olmadığını ve tüm kullanıcılara tam kontrol ayrıcalıklarının verilip verilmediğini kontrol edin.
- Trend Micro Security Server proxy ayarlarının doğru olduğunu onaylayın.

Diğer Antivirüs Yazılımından Geçirme Sırasında Karşılaşılan Sorunlar

Bu bölümde, üçüncü taraf antivirüs yazılımından geçirme işlemi gerçekleştirirken karşılaşabileceğiniz bazı sorunlar ele alınmaktadır.

Client/Server Security Agent kurulum programı, üçüncü taraf yazılımı kullanıcıların sisteminden otomatik olarak kaldırmak ve Client/Server Security Agent ile değiştirmek için üçüncü taraf yazılımın kaldırma programını kullanır. Otomatik kaldırma başarısız olursa, kullanıcılar şu iletiyi alır:

```
Kaldırma başarısız.
```

Bu hatanın çeşitli olası nedenleri vardır:

- Üçüncü taraf yazılımın sürüm numarası veya ürün anahtarı tutarsız.
- Üçüncü taraf yazılımın kaldırma programı çalışmıyor.
- Üçüncü taraf yazılımın bazı dosyaları eksik veya bozuk.
- Üçüncü taraf yazılımın kayıt defteri anahtarı temizlenemiyor.
- Üçüncü taraf yazılımın kaldırma programı yok.

Bu hataya ilişkin çeşitli olası çözümler de vardır:

- Üçüncü taraf yazılımı el ile kaldırın.
- Üçüncü taraf yazılım hizmetini durdurun.
- Üçüncü taraf yazılım hizmetini veya işlemini kaldırın.

Başarısız Web Sayfası veya Uzaktan Yükleme

Kullanıcılar dahili Web sayfasından yükleyemediklerini bildirirse veya Uzaktan yükleme yoluyla yükleme başarısız olursa, şu yöntemleri deneyin.

- Ping ve telnet kullanarak istemci-sunucu iletişiminin var olduğunu doğrulayın.
- İstemcide TCP/IP'nin etkinleştirildiğini ve düzgün şekilde yapılandırıldığını doğrulayın.
- İstemci-sunucu iletişimi için proxy sunucu kullanıyorsanız, proxy ayarlarının doğru yapılandırılıp yapılandırılmadığını kontrol edin.
- Web tarayıcısında, Trend Micro eklentilerini ve gözatma geçmişini silin.

Sık Sorulan Sorular (SSS)

Aşağıda, sık sorulan soruların ve onların yanıtlarının bir listesi verilmiştir.

Etkinleştirme Kodumu ve Kayıt Anahtarımı Nerede Bulabilirim?

WFBS'yı yükleme işlemi sırasında veya daha sonra Web konsolunu kullanarak etkinleştirebilirsiniz. WFBS'yı etkinleştirmek için, bir Etkinleştirme Koduna ihtiyacınız vardır.

Etkinleştirme Kodu Edinme

Worry-Free Business Security'yi Trend Micro Web sitesinden indirirseniz, otomatik olarak bir deneme sürümü Etkinleştirme Kodu edinirsiniz.

Çevrimiçi Etkinleştirme Kodu edinmek için Kayıt Anahtarını kullanabilirsiniz.

Etkinleştirme Kodları 37 karakterden oluşur ve şu şekilde görünür:

```
xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx
```

Kayıt Anahtarı Edinme

Kayıt Anahtarı şu konumlarda bulunabilir:

- Ürün CD'si
- Lisans Sertifikası (ürünü satın aldıktan sonra edindiğiniz)

WFBS'nızın kopyasını kaydetmeniz ve etkinleştirmeniz size şu avantajları kazandırır:

- WFBS desen dosyaları ve tarama motoru güncellemeleri
- Teknik destek
- Lisans geçerlilik sonu güncellemesini, kayıt ve lisans bilgilerini ve yenileme anımsatıcılarını görüntülemek için kolay erişim
- Lisansınızı yenilemek ve müşterilerin profilini güncellemek için kolay erişim

Kayıt Anahtarları 22 karakterden oluşur ve şu şekilde görünür:

```
xx-xxxx-xxxx-xxxx-xxxx
```

Tam sürümün süresi dolduğunda, güvenlik güncellemeleri devre dışı bırakılır; deneme döneminin süresi dolduğunda ise, hem güvenlik güncellemeleri hem de tarama özellikleri devre dışı bırakılır. Ürün Lisansı ekranında, çevrimiçi Etkinleştirme Kodu edinebilir, yenileme yönergelerini görüntüleyebilir ve ürününüzün durumunu kontrol edebilirsiniz.

Kayıt

WFBS'yı kaydetmeyle ilgili çeşitli sorularım var. Yanıtlarını nerede bulabilirim?

Kayıtla ilgili sık sorulan sorular için şu Web sitesine başvurun:

http://esupport.trendmicro.com/support/viewxml.do?ContentID=en-116326

Yükleme, Yükseltme ve Uyumluluk

Worry-Free Business Security veya Worry-Free Business Security Advanced'in hangi sürümleri bu sürüme yükseltilebilir?

Bilgi için WFBS *Yükleme Kılavuzu*'na başvurun.

Ağ ortamım için en uygun Aracı yükleme yöntemi hangisidir?

Mevcut çeşitli aracı yükleme yöntemlerinin özeti veya kısa bir karşılaştırması için bkz. *Aracı Yüklemeye Genel Bakış*, sayfa 3-2.

Trend Micro Security Server, Citrix veya Windows Terminal Hizmetleri kullanılarak uzaktan yüklenebilir mi?

Evet. Trend Micro Security Server, Citrix veya Windows Terminal Hizmetleri ile uzaktan yüklenebilir.

WFBS, 64-bit platformları destekler mi?

Evet. x64 platformu için Client/Server Security Agent'ın azaltılmış bir sürümü mevcuttur. Ancak, IA-64 platformu henüz desteklenmemektedir.

Trend Micro™ ServerProtect'ten WFBS'ya yükseltebilir miyim?

Hayır. WFBS'nın yüklenebilmesi için öncelikle ServerProtect'in kaldırılması gerekir.

Security Server'ı yüklediğim bilgisayarda Apache Web sunucusunun önceden var olan yüklemesini kullanabilir miyim?

Trend Micro, Apache'nin önceden var olan yüklemesini kullanmamanızı önerir. Doğru sürüm, Security Server'ı yüklediğinizde aynı anda yüklenecektir..

Kayıp veya Unutulmuş Bir Parolayı Nasıl Kurtarabilirim?

Worry-Free Business Security konsoluna erişim, ilk olarak yükleme sırasında tanımlanan, daha sonra istendiği zaman değiştirilebilen bir parola gerektirir. Parolanızı kaybettiyseniz veya unuttuysanız Desteğe başvurun.

Intuit Yazılım Koruması

Intuit güncelleme denemesi engellendiğinde ne olur?

Tüm yürütülebilir Intuit dosyaları, dijital bir imzaya sahiptir ve bu dosyaların güncellemeleri engellenmez. Intuit ikili dosyasını değiştirmeye çalışan başka programlar varsa, aracı ikili dosyaları güncellemeye çalışan programın adını içeren bir ileti görüntüler.

Başka programların Intuit dosyalarını güncellemesine izin verilebilir mi? Trend Micro korumasını, durumdan duruma değişecek şekilde atlayabilir miyim?

Evet. Buna izin vermek için, aracıda Behavior Monitoring Kural Dışı Durum Listesine gerekli programı ekleyin.

UYARI! **Güncellemenin ardından programı kural dışı durum listesinden kaldırmayı unutmayın.**

Ayarları Yapılandırma

WFBS ayarlarını yapılandırmaya ilişkin bazı sorularım var. Yanıtlarını nerede bulabilirim?

Tüm WFBS belgelerini şu siteden indirebilirsiniz:

http://www.trendmicro.com/download/emea/?lng=en

SBS 2003'e sahip Antivirüs yazılımı için hangi klasörleri dışlamam gerekir?

SBS 2003 dışlamaları için aşağıdaki tablolara başvurun:

TABLO A-1. DIIS Dışlamaları

IIS Sistem Dosyaları	C:\WINDOWS\system32\inetsrv
IIS Sıkıştırma Klasörü	C:\WINDOWS\IIS Temporary Compressed Files

TABLO A-2. Etki Alanı Denetleyicisi Dışlamaları

Active Directory veritabanı dosyaları	C:\WINDOWS\NTDS
SYSVOL	C:\WINDOWS\SYSVOL
NTFRS Veritabanı Dosyaları	C:\WINDOWS\ntfrs

TABLO A-3. Windows SharePoint Services Dışlamaları

Geçici SharePoint klasörü	C:\windows\temp\FrontPageTempDir

TABLO A-4. İstemci Masaüstü Klasör Dışlamaları

Windows Update Deposu	C:\WINDOWS\SoftwareDistribution\ DataStore

TABLO A-5. Ek Dışlamalar

Çıkarılabilir Depolama Veritabanı (SBS Yedekleme tarafından kullanılır)	C:\Windows\system32\NtmsData
SBS POP3 bağlayıcısı Hatalı Posta	C:\Program Files\Microsoft Windows Small Business Server\Networking\POP3\Failed Mail
SBS POP3 bağlayıcısı Gelen Posta	C:\Program Files\Microsoft Windows Small Business Server\Networking\POP3\Incoming Mail
Windows Update Deposu	C:\WINDOWS\SoftwareDistribution\ DataStore
DHCP Veritabanı Deposu	C:\WINDOWS\system32\dhcp
WINS Veritabanı Deposu	C:\WINDOWS\system32\wins

En Son Desen Dosyasına veya Hizmet Paketine Sahip miyim?

Güncellenebilir dosyalar, hangi ürünü yüklediğinize bağlı olarak farklılık gösterir.

En son desen dosyasına veya hizmet paketine sahip olup olmadığınızı öğrenmek için:

1. Web konsolundan, **Tercihler > Ürün Lisansı** seçeneklerini tıklatın. Ürün Lisansı ekranı görünür.
2. Mevcut ürün sürümü de dahil olmak üzere ürün lisansı ayrıntıları görünür.

Mevcut en son desenleri bulmak için, aşağıdakilerden herhangi birini gerçekleştirmek için bir Web tarayıcısı açın:

- Trend Micro Güncelleme Merkezi:

  http://www.trendmicro.com/download/emea/?lng=en

- Trend Micro Desen Dosyası:

  http://www.trendmicro.com/download/emea/pattern.asp?lng=emea

Smart Scan

Smart Scan nedir?

Smart Scan, istemcileri tarama yükünün bir kısmını almak için ağda merkezi bir tarama sunucusu kullanan, Trend Micro'nun sunduğu yeni bir teknolojidir.

Smart Scan güvenilir midir?

Evet. Smart Scan, başka bir bilgisayarın, Smart Scan Server'ın, istemcilerinizi taramaya yardımcı olmasına izin verir. İstemcileriniz Smart Scan için yapılandırıldıkları halde Smart Scan Server'a bağlanamıyorsa, Trend Micro Global Smart Scan Server'a bağlanmaya çalışacaktır.

Smart Scan Server'ın düzgün çalışıp çalışmadığını nasıl anlarım?

Security Server'da aşağıdaki hizmetin çalıştığını doğrulayın:

```
TMiCRCScanService
```

Scan Server'ı kaldırabilir veya yüklememeyi seçebilir miyim?

Hayır. Smart Scan'i kullanmak istemiyorsanız tüm istemcileri Geleneksel Tarama'ya geçiren ve Security Server'da Smart Scan'i durduran Smart Scan hizmetini devre dışı bırakın.Bu işlem Security Server'ın performansının iyileştirilmesine de yardımcı olur.

Yönergeler için Yönetici Kılavuzu'nun 10-7. sayfasında bulunan Genel Tarama Ayarları kısmına bakın.

Bilinen Sorunlar

Bilinen sorunlar, WFBS yazılımında geçici bir çözüm gerektirebilecek özelliklerdir. Bilinen sorunlar, tipik olarak, ürününüzün beraberinde gelen Benioku belgesinde belirtilmektedir. Trend Micro ürünlerinin benioku dosyaları, aynı zamanda Trend Micro Güncelleme Merkezi'nde de bulunabilir:

http://www.trendmicro.com/download/emea/?lng=en

Bilinen sorunlar teknik destek Bilgi Bankası'nda bulunabilir:

http://esupport.trendmicro.com/support/

Trend Micro, yüklemeyi veya performansı etkileyebilecek bilinen sorunlara ilişkin bilgi ve belirli bir sürümdeki yeniliklere, sistem gereksinimlerine ve diğer ipuçlarına ilişkin açıklama için Benioku metnini her zaman incelemenizi önerir.

Ek B

Yardım Alma

Bu ekte nasıl yardım alabileceğiniz, ek bilgilere nasıl ulaşabileceğiniz ve Trend Micro ile nasıl bağlantı kurabileceğiniz açıklanmaktadır.

Bu ekte ele alınan başlıklar şunlardır:

Ürün Belgeleri

WFBS belgeleri aşağıdakilerden oluşur:

- Çevrimiçi Yardım

  Web konsolundan erişilebilen web tabanlı belgeler.

  WFBS *Çevrimiçi Yardım*, ürün özelliklerini anlatır ve ürünlerin kullanımına ilişkin talimatlar verir. Ayarlarınızı özelleştirme ve güvenlik görevlerini gerçekleştirme hakkında ayrıntılı bilgi içerir. Bağlama duyarlı yardımı açmak için simgeyi tıklatın.

  Çevrimiçi yardımı kimler kullanmalıdır?

  Belirli bir ekranla ilgili yardıma ihtiyacı olan WFBS Yöneticileri.

- Yükleme Kılavuzu

  Kurulum Kılavuzu, ürünü yüklemek/yükseltmek ve kullanmaya başlamak için gerekli talimatları içerir. WFBS ürününün temel özelliklerinin ve varsayılan ayarlarının açıklamasını sağlar.

  Kurulum Kılavuzu, Trend Micro SMB CD'sinde yer alır veya Trend Micro Güncelleme Merkezi'nden indirilebilir:

  http://www.trendmicro.com/download/emea/?lng=en

  Bu kılavuzu kimler okumalıdır?

  WFBS'yı yüklemek ve onunla başlamak isteyen WFBS Yöneticileri.

- Yönetici Kılavuzu

  Yönetici Kılavuzu, ürünün yapılandırılması ve bakımı için kapsamlı talimatlar sağlar.

  Yönetici Kılavuzu, Trend Micro SMB CD'sinde yer alır veya Trend Micro Güncelleme Merkezi'nden indirilebilir.

  http://www.trendmicro.com/download/emea/?lng=en

  Bu kılavuzu kimler okumalıdır?

  WFBS'yı özelleştirmesi, sürdürmesi ya da kullanması gereken WFBS Yöneticileri.

- Benioku dosyası

  Benioku dosyası, çevrimiçi veya basılı belgelerde bulunmayan en güncel ürün bilgilerini içerir. Yeni özelliklerin açıklamalarını, yükleme ipuçlarını, bilinen sorunları, lisans bilgilerini vb. bu kılavuzda bulabilirsiniz.

- Bilgi Bankası

  Bilgi Bankası, sorun giderme bilgilerini içeren çevrimiçi bir veritabanıdır. Bilinen ürün sorunları hakkında en son bilgileri sağlar. Bilgi Bankası'na erişmek için aşağıdaki Web sitesine gidin:

  http://esupport.trendmicro.com

Trend Micro, her zaman belgelerini iyileştirmek için çalışmaktadır. Bu veya herhangi bir Trend Micro belgesi hakkında soru, yorum veya önerileriniz için docs@trendmicro.com adresinden bize ulaşabilirsiniz. Geribildiriminiz bizim için her zaman önemlidir. Ayrıca bu belgeleri aşağıdaki sitede değerlendirebilirsiniz:

http://www.trendmicro.com/download/documentation/rating.asp

Bilgi Bankası

Trend Micro Bilgi Bankası, Trend Micro ürünleri için binlerce kendin yap teknik destek prosedürü içeren çevrimiçi bir kaynaktır. Örneğin bir hata iletisi alıyor ve bu konuda ne yapmanız gerektiğini öğrenmek istiyorsanız her gün yeni çözümlerin eklendiği Bilgi Bankası'nı kullanın.

Bilgi Bankası'nda ayrıca ürün SSS'leri, ipuçları, virüs/kötü amaçlı yazılım sorunlarını önlemeye ilişkin öneriler ve destek ve satışlar için bölgesel iletişim bilgileri bulunur.

Bilgi Bankası'na tüm Trend Micro müşterileri ve bir ürünün değerlendirme sürümünü kullanan herkes erişebilir. Şu adresi ziyaret edin:

http://esupport.trendmicro.com/support/smb/search.do

Teknik Destek

Trend Micro Teknik Destek ile bağlantı kurduğunuzda, sorununuzun daha hızlı çözülebilmesi için Durum Tanı Aracı'nı çalıştırın (bkz. *Durum Tanı Aracı'nı kullanma*, sayfa B-4) veya aşağıdaki bilgilere sahip olduğunuzdan emin olun:

- İşletim sistemi
- Ağ türü
- Bilgisayarın markası ve modeli ve bağlı donanım
- Bellek miktarı ve makinenizdeki boş sabit disk alanı
- Yükleme ortamının ayrıntılı açıklaması
- Hata iletilerinin tam metni
- Sorunun tekrar ortaya çıkmasını sağlayacak adımlar

Trend Micro Teknik Desteği ile bağlantı kurmak için:

1. Durum Tanı Aracı'nı çalıştırın. Daha fazla bilgi için bkz. *Durum Tanı Aracı'nı kullanma*, sayfa B-4.
   - Aşağıdaki URL'yi ziyaret edin:

     http://esupport.trendmicro.com/support/srf/questionentry.do

     Gerekli bölgenin bağlantısını tıklatın. Bulunduğunuz bölgede destek ile bağlantı kurmak için gerekli talimatları uygulayın.
   - E-posta iletisiyle iletişim kurmayı tercih ediyorsanız, aşağıdaki adrese bir sorgu gönderin:

     virusresponse@trendmicro.com
   - ABD'de, aşağıdaki ücretsiz telefon numarasını da arayabilirsiniz:

     `(877) TRENDAV veya 877-873-6328`

Durum Tanı Aracı'nı kullanma

Bilgisayardan Trend Micro yazılım ayarlarını ve ortam kurulum belirtimlerini almak için Durum Tanı Aracı'nı kullanın. Bu bilgiler, yazılımla ilgili sorunları gidermek için kullanılır.

Durum Tanı Aracı'nı aşağıdaki adresten indirin:

http://www.trendmicro.com/download/product.asp?productid=25

Trend Micro ile Bağlantı Kurma

Trend Micro, dünya genelinde pek çok şehirde satış bürolarına ve kurumsal ofislere sahiptir. Genel iletişim bilgileri için Trend Micro Worldwide sitesini ziyaret edin:

http://us.trendmicro.com/us/about/contact_us

Not: Bu Web sitesindeki bilgiler, haber verilmeden değiştirilebilir.

Şüpheli Dosyaları Trend Micro'ya Gönderme

Virüs/kötü amaçlı yazılım, virüslü dosyalar, Truva atları, olası solucanlar ve diğer şüpheli dosyaları değerlendirilmek üzere Trend Micro'ya gönderebilirsiniz. Bunun için, destek sağlayıcınızla bağlantı kurun veya Trend Micro Gönderme Sihirbazı URL'sini ziyaret edin:

http://subwiz.trendmicro.com/SubWiz

İstediğiniz gönderme türünün altındaki bağlantıyı tıklatın.

Not: Gönderme sihirbazı/virüs doktoru tarafından gönderilen bildirimler hızla ele alınır ve Trend Micro Virüs Yanıt Hizmeti Düzeyi Sözleşmesi kapsamında belirlenen ilkelerden ve kısıtlamalardan muaf tutulur.

Durumunuzu gönderdiğinizde, bir onay ekranı görüntülenir. Bu ekranda bir de durum numarası görüntülenir. İzleme amacıyla durum numarasını kaydedin.

Virüs Bilgileri Merkezi

Internet üzerinden ücretsiz olarak Trend Micro Security Bilgileri web sitesinde kapsamlı güvenlik bilgilerine erişebilirsiniz:

http://www.trendmicro.com/vinfo/emea/virusencyclo/default.asp

Güvenlik Bilgileri sitesini ziyaret ederek:

- O hafta tetikleneceği tahmin edilen tehlikelerin listesini içeren ve o hafta için dünya genelinde en yaygın 10 tehdidi açıklayan Haftalık Virüs Raporu'nu okuyun.
- Dünya genelindeki en büyük 10 tehdidin Virüs Haritasını görüntüleyin.
- Risk derecelendirmesi, enfeksiyonun göstergeleri, zayıf platformlar, zarar yordamı ve tehdidin nasıl ortadan kaldırılacağına ilişkin talimatlarla bilgisayar hileleri hakkında bilgiler içeren Virüs Ansiklopedisi'ne bakın.
- Güvenlik ürününüzün doğru bir şekilde yapılandırılıp yapılandırılmadığını test etmenize yardımcı olması için Avrupa Bilgisayarları Virüsten Koruma Araştırmaları Enstitüsü'nden (EICAR) test dosyalarını indirin.
- Genel virüs/kötü amaçlı yazılım bilgilerini okuyun. Örneğin:
  - Virüs/kötü amaçlı yazılım, Truva atları, solucanlar ve diğer tehditler arasındaki farkları anlamanıza yardımcı olabilecek Virüslere Giriş.
  - Trend Micro *Güvenli Bilgi İşlem Kılavuzu*
  - Derecelendirmesi Çok Düşük veya Düşük ya da Orta veya Yüksek risk olan bir tehdidin zarar potansiyelini anlamanıza yardımcı olacak risk derecelendirmeleri açıklaması
  - Virüs/kötü amaçlı yazılım ve diğer güvenlik tehdidi terminolojisini içeren bir sözlük
- Kapsamlı sektör teknik belgelerini indirin
- En son salgınlar ve Haftalık Virüs Raporu hakkında bilgi edinmek için Trend Micro Virüs Uyarı hizmetine abone olun
- Web yöneticilerine sunulan ücretsiz virüs/kötü amaçlı yazılım güncelleme araçları hakkında bilgi edinin.
- Trend Micro genel virüsten koruma araştırma ve destek merkezi TrendLabs^{SM} hakkındaki belgeleri okuyun

TrendLabs

TrendLabs, Trend Micro müşterilerine güncel güvenlik bilgileri sağlayan Trend Micro virüsten koruma araştırması ve ürün destek merkezleri küresel altyapısıdır.

TrendLabs'taki "virüs doktorları", Trend Micro ürünlerini yeni tehditlerden korumak için dünya genelindeki olası güvenlik risklerini izler. Sık virüs deseni dosya güncellemeleri ve tarama motoru hassaslaştırmaları yoluyla bu çabaların günlük sonuçları müşterilerle paylaşılır.

TrendLabs, çeşitli ürün ve teknik destek hizmetleri sağlayan birkaç yüz mühendisten ve sertifikalı destek personelinden oluşan bir ekibe sahiptir. Tokyo, Manila, Taype, Münih, Paris ve Kaliforniya'nın Lake Forest kentinde bulunan özel hizmet merkezleri ve hızlı yanıt ekipleri, virüs salgınlarına karşı koruma ve 7/24 acil destek sağlar.

TrendLabs'in büyük bir Metro Manila BT parkında yer alan modern merkezi, kaliteli yönetim uygulamaları için 2000 yılında ISO 9002 sertifikası almaya hak kazanarak bu ödüle layık görülen ilk antivirus araştırma ve destek tesislerinden biri oldu. Trend Micro, antivirüs sektöründe öncü hizmet ve destek ekibinin TrendLabs olduğuna inanmaktadır.

Ek C

Sözlük

Sözlük, bu belgede kullanılan önemli terimlerin ve kavramların açıklamalarını içerir. Güvenlik tehditleri hakkında bilgi için bkz:
http://threatinfo.trendmicro.com/vinfo/

Trend Micro Smart Protection Network'ün sizi nasıl koruduğu hakkında bilgi için bkz:
http://itw.trendmicro.com/smart-protection-network

Terim	Açıklama
ActiveUpdate	Trend Micro güncelleme Web sitesine bağlı olan ActiveUpdate, virüs desen dosyaları, tarama motorları ve program dosyaları gibi bileşenlerin güncel indirme fırsatlarını sunar. ActiveUpdate, pek çok Trend Micro ürününde bulunan bir işlevdir.
Aracı	İstemci üzerinde çalışan WFBS programı.
ayrıcalıklar (istemci ayrıcalıkları)	Yöneticiler, Web konsolundan Client/Server Security Agent için ayrıcalık ayarlayabilir. Ardından son kullanıcılar, Client/Server Security Agent uygulamalarını istemcilerini sizin izin verdiğiniz ayrıcalıklara göre tarayacak şekilde ayarlayabilir. Kuruluşunuzun içinde tek tip bir antivirüs ilkesi uygulamak için istemci ayrıcalıklarını kullanın.
Canlı Durum	Web Konsolu'nun ana ekranı veya panosu. Canlı Durum, Salgın Savunması, Antivirüs, Casus Yazılıma Karşı Koruma ve Ağ Virüsleri ile ilgili güvenlik durumunu bir bakışta görmenizi sağlar.
desen eşlemesi	Her virüs kendisini diğer kodlardan ayıran benzersiz bir "imza" veya anormal karakter dizisi içerdiğinden, Trend Micro'daki virüs uzmanları desen dosyasında bu kodun hareketsiz kod parçacıklarını yakalar. Ardından motor, taranan her dosyanın belirli bölümlerini virüs desen dosyasındaki desenle karşılaştırarak bir eşleşme arar. Motor bir eşleşme bulduğunda, bu, bir virüs saptandığı anlamına gelir ve Yönetici'ye bir e-posta bildirimi gönderilir.
Etkinleştirme Kodu	Tarama ve ürün güncellemelerini etkinleştirmek için sayısal bir kod gerekir. Yükleme sırasında veya daha sonra herhangi bir zaman ürününüzü etkinleştirebilirsiniz. Etkinleştirme Kodlarına sahip değilseniz, ürününüzle birlikte verilen Kayıt Anahtarını kullanarak Trend Micro Web sitesine kaydolun ve Etkinleştirme Kodlarını alın.
Geleneksel Tarama	İstemci üzerindeki yerel bir tarama motoru istemci bilgisayarını tarar.
Güncelleme Aracısı	Diğer aracılar için güncelleme kaynağı işlevi gören aracılar.

Terim	Açıklama
İçerik Filtreleme	Kuruluşunuzun İnsan Kaynakları veya BT ileti politikaları tarafından yasaklanan, nefret uyandırıcı posta, küfür ve pornografik gibi içerik (sözcük veya sözcük grubu) içerip içermediğini anlamak için e-posta iletilerini tarama.
İstemciler	İstemciler, Microsoft Exchange sunucuları, masaüstü bilgisayarlar, taşınabilir bilgisayarlar ve bir Messaging Security Agent ya da Client/Server Security Agent yüklü olan sunuculardır.
Kayıt Defteri Anahtarı	Trend Micro'ya kaydolmak ve bir Etkinleştirme Kodu almak için gereken sayısal koddur.
Security Server	WFBS uygulamasını ilk kez yüklediğinizde, Security Server haline gelen bir Windows sunucusuna yüklersiniz. Security Server, Client/Server Security Agent uygulamalarıyla ve istemcide yüklü Messaging Security Agent uygulamalarıyla iletişim kurar. Security Server ayrıca tüm WFBS çözümü için merkezi Web tabanlı yönetim konsolu olan Web konsolunu barındırır.
Smart Scan	Tarama Sunucusu istemciyi taramaya yardımcı olur.
Son Kullanıcı Lisans Sözleşmesi (EULA)	Son Kullanıcı Lisans Sözleşmesi veya EULA, bir yazılım yayıncısı ve yazılım kullanıcısı arasındaki yasal bir sözleşmedir. Genellikle yükleme sırasında "Kabul ediyorum" seçeneğini tıklatmayarak sözleşmeyi reddedebilecek kullanıcıya ilişkin kısıtlamaları içerir. "Kabul etmiyorum" seçeneğinin tıklatılması doğal olarak yazılım ürününün yüklenmesinin sonlandırılmasına neden olacaktır. Pek çok kullanıcı, bazı ücretsiz yazılımların kurulumu sırasında görüntülenen EULA istemlerinde "Kabul ediyorum" seçeneğini tıklatarak casus yazılım/grayware ve başka grayware türlerinin bilgisayarlarına yüklenmesini istemeden kabul eder.
Tarama Sunucusu	İstemcilerin tarama işleminin tamamını gerçekleştirmek zorunda kalmaması için istemcileri taramaya yardımcı olan bir sunucu.
temiz	Bir dosya veya iletiden virüs kodunu kaldırmak için.

Terim	Açıklama
Temizleme	Temizleme, Truva atlarını ya da Truva atları tarafından yüklenen uygulamaları veya süreçleri algılar ve kaldırır. Truva atları tarafından değiştirilen dosyaları onarır.
TrendLabs	TrendLabs, dünyanın dört bir yanındaki Trend Micro müşterilerine 7/24 hizmet sağlayan Trend Micro antivirüs araştırması ve ürün destek merkezleri küresel ağıdır.
TrendSecure	TrendSecure, kullanıcıların güvenli bir şekilde Web'de gezinmelerini sağlayan bir dizi tarayıcı tabanlı eklenti aracı içerir (TrendProtect ve Transaction Protector). TrendProtect, kullanıcıları kötü amaçlı web siteleri ve kimlik avı web siteleri hakkında uyarır. Transaction Protector, erişim noktasının özgünlüğünü kontrol ederek kablosuz bağlantınızın güvenliğini belirler.
Web konsolu	Web konsolu, merkezi bir Web tabanlı yönetim konsoludur. Web konsolunu, tüm uzak masaüstü bilgisayarlarınızı, sunucularınızı ve Microsoft Exchange sunucularını koruyan Client/Server Security Agent ve Messaging Security Agent uygulamalarının ayarlarını yapılandırmak için kullanabilirsiniz. Web konsolu, Trend Micro Security Server'ı yüklediğinizde yüklenir ve ActiveX, CGI, HTML ve HTTP gibi Internet teknolojilerini kullanır.
yapılandırma	Trend Micro ürününüzün işlevlerine ilişkin seçenekleri belirleme, örneğin, virüs bulaşmış bir e-posta iletisinin karantinaya alınmasına veya silinmesine karar verme.
Yönetici	ActiveX denetimleri yürüten Web sayfalarında bulunan bir virüs türüdür.

Dizin

D

E

F

G

H

I

T