System Center

Endpoint Protection - Mac

Yükleme El Kitabı ve Kullanıcı Kılavuzu

Microsoft

İçindekiler

System Center Endpoint Protection

Unix tabanlı işletim sistemlerinin popülerliği arttıkça, kötü amaçlı yazılım yazarları, Mac kullanıcılarını hedefleyen daha fazla tehdit geliştirmektedir. System Center Endpoint Protection, bu ortaya çıkan tehditlere karşı güçlü ve verimli koruma sunar. System Center Endpoint Protection ayrıca Windows tehditlerini saptırma yeteneğini içerir ve Windows kullanıcılarıyla etkileşime geçtikçe Mac kullanıcılarını; Mac kullanıcılarıyla etkileşime geçtikçe Windows kullanıcılarını korur. Windows kötü amaçlı yazılımı Mac için doğrudan bir tehdit oluşturmasa da, Mac makinesini etkileyen kötü amaçlı yazılımın devre dışı bırakılması, onun yerel ağ veya Internet aracılığıyla Windows tabanlı bilgisayarlara yayılmasını önler.

Sistem gereksinimleri

System Center Endpoint Protection programının en iyi performansını elde etmek için sistemin aşağıdaki donanım ve yazılım gereksinimlerini karşılaması gerekir:

System Center Endpoint Protection:

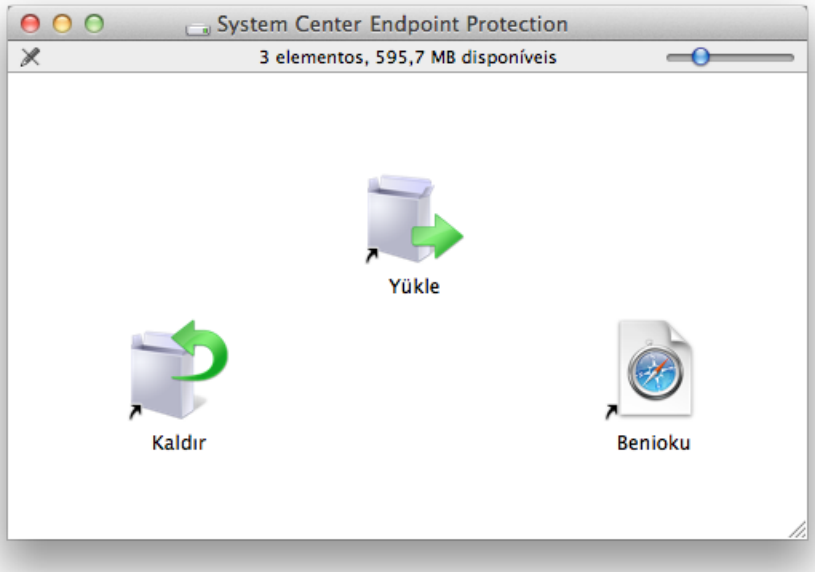
	Sistem gereksinimleri
İşlemci mimarisi	32bit, 64bit Intel®
İşletim sistemi	Mac OS X 10.6 ve üstü
Bellek	512 MB
Boş disk alanı	100 MB

Yükleme

Yükleme işlemine başlamadan önce lütfen bilgisayarınızdaki tüm açık programları kapatın. System Center Endpoint Protection, önceden bilgisayarınıza yüklenmiş olabilecek diğer antivirus programlarıyla çalışabilen bileşenler içerir. Olası sorunları önlemek için kesinlikle diğer antivirus programlarının kaldırılması önerilir. Bir yükleme CD'sinden/DVD'sinden veya web sitemizden yüklediğiniz bir dosyadan System Center Endpoint Protection uygulamasını yükleyebilirsiniz.

Yükleme sihirbazını başlatmak için aşağıdakilerden birini yapın:

- Bir yükleme CD'sinden/DVD'sinden yükleme yapıyorsanız CD'yi veya DVD'yi bilgisayarınıza takıp masaüstünden veya Finder penceresinden açın ve **Yükle** simgesini çift tıklatın.
- Karşıdan yüklenen bir dosyadan yükleme yapıyorsanız, karşıdan yüklediğiniz dosyayı açın ve **Yükle** simgesini çift tıklatın.



Yükleyiciyi başlatın; yükleme sihirbazı temel ayarlar sürecinde size yol gösterecektir. Yazılım Lisans Sözleşmesi'ni kabul ettikten ve Gizlilik Bildirimi'ni okuduktan sonra şu yükleme türleri arasından seçim yapabilirsiniz:

- Normal 4
- Özel 4

Normal yükleme

Normal yükleme modu, çoğu kullanıcı için uygun yapılandırma seçeneklerini içerir. Bu ayarlar, mükemmel sistem performansıyla birlikte maksimum güvenlik sağlar. Normal yükleme, varsayılan seçenektir ve bazı ayarlara yönelik belirli gereksinimlere sahip değilseniz önerilir.

Normal yükleme modunu seçtikten sonra, **İstenmeyen türden olabilecek uygulamaları algılama** seçeneğini yapılandırın. İstenmeyen türden olabilecek uygulamalar kötü amaçlı olmak zorunda değildir, ancak genellikle işletim sisteminizin çalışma biçimini olumsuz yönde etkileyebilir. Bu uygulamalar genellikle diğer programlarla birlikte gelir ve yükleme işlemi sırasında fark edilmeleri zor olabilir. Bu uygulamalar yükleme sırasında genellikle bir bildirim görüntülese de izniniz olmadan da kolayca yüklenebilir.

System Center Endpoint Protection ürününü yükledikten sonra kötü amaçlı kod için bir bilgisayar taraması gerçekleştirmelisiniz. Ana program penceresinden, **Bilgisayar taraması**'nı ve ardından **Smart tarama**'yı tıklatın. İsteğe bağlı bilgisayar taraması hakkında daha fazla bilgi için, İsteğe bağlı bilgisayar taraması 10 bölümüne bakın.

Özel yükleme

Özel yükleme modu, yükleme işlemi sırasında gelişmiş ayarları değiştirmek isteyen deneyimli kullanıcılar için tasarlanmıştır.

Özel yükleme modunu seçtikten sonra sizden **Proxy sunucu** ayarlarını yapılandırmanız istenir. Proxy sunucu kullanıyorsanız, **Proxy sunucu kullanıyorum** seçeneğini belirleyerek proxy sunucunun parametrelerini tanımlayabilirsiniz. Proxy sunucunuzun IP adresini veya URL'sini **Adres** alanına girin. Bağlantı noktası alanında, proxy sunucunun bağlantıları kabul ettiği bağlantı noktasını belirtin (varsayılan olarak 3128'dir). Proxy sunucunun kimlik doğrulama istemesi durumunda, proxy sunucusuna erişim vermek için geçerli bir **Kullanıcı Adı** ve **Parola** girin. Bir proxy sunucusu kullanılmadığından eminseniz, **Proxy sunucu kullanmıyorum** seçeneğini belirleyin. Emin değilseniz, **Sistem ayarlarını kullan (Önerilir)** seçeneğini belirleyerek geçerli sistem ayarlarınızı kullanabilirsiniz.

Sonraki adımda, program yapılandırmasını düzenleyebilecek **Ayrıcalıklı kullanıcıları tanımla** eylemini gerçekleştirebilirsiniz. Sol taraftaki kullanıcı listesinden kullanıcıları seçin ve bunları **Ayrıcalıklı Kullanıcılar** listesine **Ekle** eylemini gerçekleştirin. Tüm sistem kullanıcılarını görüntülemek için **Tüm kullanıcıları göster** seçeneğini belirleyin.

Yükleme işlemindeki sonraki adım **İstenmeyen türden olabilecek uygulamaları algılama** seçeneğini yapılandırmaktır. İstenmeyen türden olabilecek uygulamalar kötü amaçlı olmak zorunda değildir, ancak genellikle işletim sisteminizin çalışma biçimini olumsuz yönde etkileyebilir. Bu uygulamalar genellikle diğer programlarla birlikte gelir ve yükleme işlemi sırasında fark edilmeleri zor olabilir. Bu uygulamalar yükleme sırasında genellikle bir bildirim görüntülese de izniniz olmadan da kolayca yüklenebilir.

System Center Endpoint Protection ürününü yükledikten sonra kötü amaçlı kod için bir bilgisayar taraması gerçekleştirmelisiniz. Ana program penceresinden, **Bilgisayar taraması**'nı ve ardından **Smart tarama**'yı tıklatın. İsteğe bağlı bilgisayar taramaları hakkında daha fazla bilgi için, İsteğe bağlı bilgisayar taraması 10 bölümüne bakın.

Kaldırma

System Center Endpoint Protection ürününü bilgisayarınızdan kaldırmak isterseniz aşağıdakilerden birini yapın:

- System Center Endpoint Protection yükleme CD'sini/DVD'sini bilgisayarınıza takıp masaüstünden veya Finder penceresinden açın ve **Kaldır** simgesini tıklatın.
- System Center Endpoint Protection yükleme dosyasını (*.dmg*) açın ve **Kaldır** simgesini çift tıklatın veya
- **Finder** aracını başlatın, sabit sürücünüzdeki **Uygulamalar** klasörünü açın, ctrl tuşuna basın ve System Center Endpoint Protection simgesini tıklatıp **Paket İçeriklerini Göster** seçeneğini belirleyin. **Contents > Helpers** klasörünü açın ve **Uninstaller** simgesini çift tıklatın.

Başlangıç kılavuzu

Bu bölüm, System Center Endpoint Protection ve temel ayarları hakkında genel bir ilk bakış sağlar.

Kullanıcı arabirimi

System Center Endpoint Protection ürününün ana program penceresi iki ana bölüme ayrılır. Sağdaki birincil pencere, soldaki ana menüden seçilen seçeneğe karşılık gelen bilgileri görüntüler.

Aşağıda ana menüdeki seçeneklerin açıklaması verilmektedir:

- **Koruma durumu** - System Center Endpoint Protection ürününün koruma durumu hakkında bilgi sağlar. **Gelişmiş mod** etkinleştirilirse, **İstatistikler** alt menüsü görüntülenir.
- **Bilgisayar taraması** - Bu seçenek, İsteğe bağlı bilgisayar taramasını yapılandırmanıza ve başlatmanıza olanak sağlar.
- **Güncelle** - Virüs imza veritabanına yönelik güncellemeler hakkındaki bilgileri görüntüler.
- **Ayarlar** - Bilgisayarınızın güvenlik düzeyini ayarlamak için bu seçeneği belirleyin. **Gelişmiş mod** etkinleştirilirse, **Antivirus ve antispyware** alt menüsü görüntülenir.
- **Araçlar** - **Günlük dosyaları**, **Karantinaya al** ve **Zamanlayıcı** seçeneklerine erişilmesini sağlar. Bu seçenek yalnızca **Gelişmiş mod**'da görüntülenir.
- **Yardım** - Program bilgileri ve yardım dosyalarına erişilmesini sağlar.

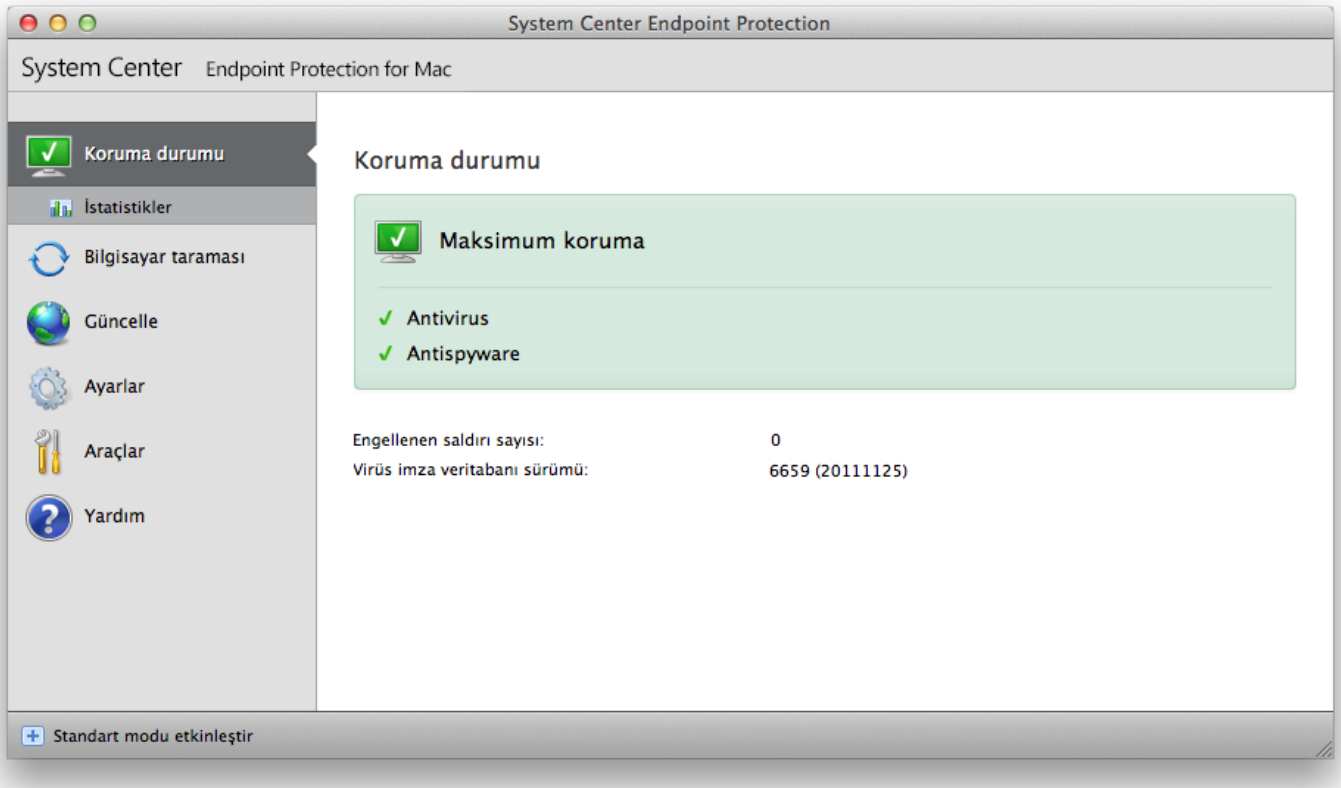
System Center Endpoint Protection kullanıcı arabirimi, kullanıcıların Standart ve Gelişmiş mod arasında geçiş yapmasına olanak sağlar. Standart mod, genel işlemler için gereken özelliklere erişilmesini sağlar. Bu, gelişmiş seçenekleri görüntülemez. Modlar arasında geçiş yapmak için ana program penceresinin sol alt köşesinde **Gelişmiş modu etkinleştir/Standart modu etkinleştir** seçeneğinin yanındaki artı simgesini (**+**) tıklatın veya cmd+M tuşlarına basın.

Gelişmiş moda geçiş yapıldığında, ana menüye **Araçlar** seçeneği eklenir. **Araçlar** seçeneği, **Günlük dosyaları**, **Karantina** ve **Zamanlayıcı** için alt menülere erişmenize olanak sağlar.

NOT: Bu kılavuzun devamındaki tüm talimatlar, **Gelişmiş mod**'da gerçekleşir.

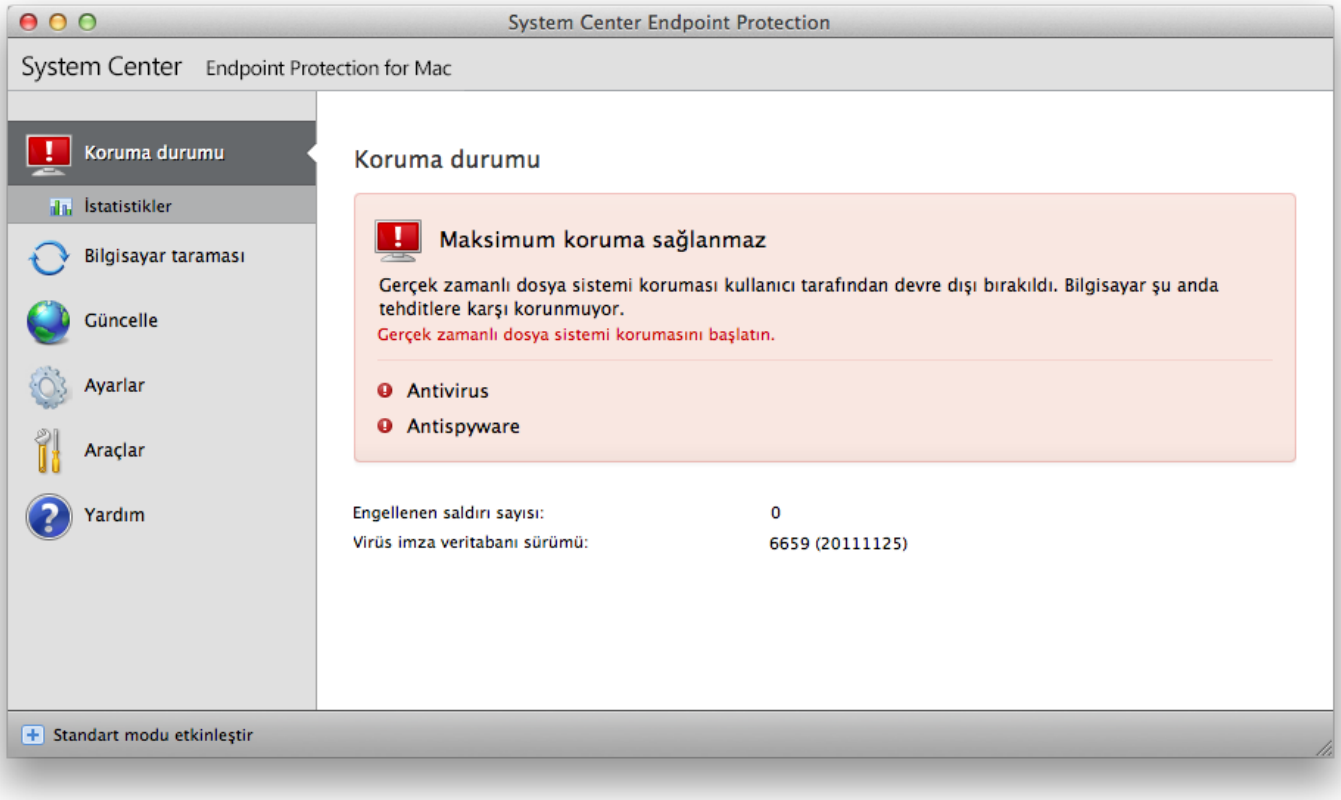
Sistemin çalışmasını denetleme

Koruma durumu'nu görüntülemek için, ana menünün en üstündeki seçeneği tıklatın. Birincil pencerede System Center Endpoint Protection ürününün çalışmasıyla ilgili bir durum özeti ve **İstatistikler**'i içeren bir alt menü görüntülenir. Sisteminizde gerçekleştirilen bilgisayar taramaları hakkında daha ayrıntılı bilgi ve istatistikleri görüntülemek için bunu seçin. İstatistikler penceresi yalnızca gelişmiş modda kullanılabilir.



Program düzgün çalışmadığında yapılacaklar

Etkinleştirilen modüller düzgün şekilde çalışıyorsa, yeşil bir onay işaretiyle belirtilir. Çalışmıyorsa kırmızı ünlem işareti veya turuncu bildirim simgesi görüntülenir ve modülle ilgili ek bilgiler pencerenin üst kısmında gösterilir. Ayrıca modülün düzeltilmesi için bir çözüm önerisi de görüntülenir. Modüllerin durumunu tek tek düzeltmek için, ana menüden **Ayarlar**'ı ve istenen modülü tıklatın.



System Center Endpoint Protection ile çalışma

Antivirus ve antispyware koruması

Antivirus koruması, olası tehdit oluşturan dosyaları değiştirerek kötü amaçlı sistem saldırılarına karşı koruma sağlar. Kötü amaçlı kod içeren bir tehdit algılanırsa, Antivirus modülü bu tehdidi engelleyerek, sonra da temizleyerek, silerek veya karantinaya taşıyarak yok edebilir.

Gerçek zamanlı dosya sistemi koruması

Gerçek zamanlı dosya sistemi koruması sistemdeki antivirüsle ilgili tüm olayları denetler. Tüm dosyalar bilgisayarınızda açıldığında, oluşturulduğunda ve çalıştırıldığında kötü amaçlı kod açısından taranır. Gerçek zamanlı dosya sistemi koruması sistem başlatma işlemi sırasında başlatılır.

Gerçek Zamanlı Koruma ayarları

Gerçek zamanlı dosya sistemi koruması tüm medya türlerini denetler ve çeşitli olayları temel alarak bir taramayı tetikler. Gerçek zamanlı dosya sistemi koruması, yeni oluşturulan dosyalar ve varolan dosyalar için değişiklik gösterebilir. Yeni oluşturulan dosyalarda daha derine inen bir denetim uygulanabilir.

Varsayılan olarak, Gerçek zamanlı koruma sistem başlatılırken başlatılır ve kesintisiz tarama sağlar. Özel durumlarda (örn. başka bir Gerçek zamanlı tarayıcıyla çakışma varsa), menü çubuğunuzdaki (ekranın en üstünde) System Center Endpoint Protection simgesi tıklatılarak ve sonra **Gerçek Zamanlı Dosya Sistemi Korumasını Devre Dışı Bırak** seçeneği belirlenerek Gerçek zamanlı koruma sonlandırılabilir. Gerçek zamanlı koruma ayrıca ana program penceresinden de sonlandırılabilir (**Ayarlar** > **Antivirus ve Antispyware** > **Devre Dışı Bırak**).

Gerçek zamanlı korumanın gelişmiş ayarlarını değiştirmek için **Ayarlar** > **Uygulama tercihlerini gir...** > **Koruma** > **Gerçek Zamanlı Koruma** seçeneğine gidin ve **Gelişmiş Seçenekler**'in yanındaki (Gelişmiş tarama seçenekleri 8 başlıklı bölümde açıklanmıştır) **Ayarlar...** düğmesini tıklatın.

Tarama (Olay tarafından tetiklenen tarama)

Varsayılan olarak tüm dosyalar **Dosya açıldığında**, **Dosya oluşturulduğunda** veya **Dosya yürütüldüğünde** taranır. Bilgisayarınız için en üst düzeyde Gerçek zamanlı koruma sağladığından, varsayılan ayarları korumanızı öneririz.

Gelişmiş tarama seçenekleri

Bu pencerede, tarama altyapısı tarafından taranacak nesne türlerini tanımlayabilir, **Gelişmiş sezgisel tarama**'yı etkinleştirebilir/devre dışı bırakabilir ve arşiv ve dosya önbelleği ayarlarını değiştirebilirsiniz.

Daha yüksek arşiv derinliği değerleri sistem performansını düşürebileceğinden, belirli bir sorunu çözmek için gerekmediği sürece, **Varsayılan arşiv ayarları** bölümündeki varsayılan değerlerin değiştirilmesini önermeyiz.

İlgili altyapı parametreleri bölümlerinin her birinde **Gelişmiş sezgisel tarama** onay kutusunu tıklatarak yürütülen, oluşturulan ve değiştirilen dosyalar için Gelişmiş sezgisel taramayı ayrı ayrı kapatıp açabilirsiniz.

Gerçek zamanlı koruma kullanırken sistem kaynaklarının minimum kullanımını sağlamak için optimizasyon önbelleğinin boyutunu tanımlayabilirsiniz. **Temiz dosya önbelleğini etkinleştir** seçeneğini kullandığınızda bu davranış etkindir. Bu devre dışıysa, tüm dosyalar her erişimde taranır. Tanımlanan önbellek boyutuna kadar dosyalar önbelleğe alındıktan sonra (değiştirilmedikleri sürece) art arda taranmaz. Her virüs imza veritabanı güncellemesinden sonra dosyalar hemen tekrar taranır.

Bu işlevi etkinleştirmek/devre dışı bırakmak için **Temiz dosya önbelleğini etkinleştir**'i tıklatın. Önbelleğe alınacak dosya miktarını ayarlamak için tek yapmanız gereken, **Önbellek boyutu**'nun yanındaki giriş alanına istediğiniz değeri girmektir.

Altyapı Ayarları penceresinde ek tarama parametreleri ayarlanabilir. Hangi tür **Nesneler**'in hangi **Seçenekler** ve **Temizleme** düzeyi kullanılarak taranacağını ve Gerçek zamanlı dosya sistemi koruması için **Uzantılar**'ı ve dosya boyutu **Sınırlar**'ını tanımlayabilirsiniz. Gelişmiş Ayarlar penceresinde **Altyapı**'nın yanındaki **Ayarlar...** düğmesini tıklatarak altyapı ayarları penceresine girebilirsiniz. Altyapı parametreleri hakkında daha ayrıntılı bilgi için bkz. Altyapı parametreleri ayarları 13.

Tarama dışı öğeler

Bu bölüm, belirli dosyaları ve klasörleri tarama dışında bırakmanızı sağlar.

- **Yol** - dışarıda bırakılan dosya ve klasörlerin yolu
- **Tehdit** - dışarıda bırakılan dosyanın yanında bir tehdit adı varsa, bu, dosyanın yalnızca söz konusu tehdit için dışarıda bırakıldığı, ancak tamamen dışarıda bırakılmadığı anlamına gelir. Bu nedenle, dosya daha sonra başka bir kötü amaçlı yazılımdan etkilenirse, antivirus modülü tarafından algılanır.

- **Ekle…** - nesneleri algılama dışında bırakır. Bir nesnenin yolunu girin (*ve ?joker karakterlerini de kullanabilirsiniz) veya ağaç yapısından klasörü ya da dosyayı seçin.
- **Düzenle…** - seçilen girişleri düzenleyebilmenizi sağlar
- **Sil** - seçilen girişleri kaldırır
- **Varsayılan** - tüm tarama dışı öğeleri iptal eder.

Gerçek zamanlı koruma yapılandırması ne zaman değiştirilir?

Gerçek zamanlı koruma, güvenli bir sistemi korumanın en temel bileşenidir. Gerçek zamanlı koruma parametrelerini değiştirirken dikkatli olun. Bu parametreleri yalnızca özel durumlarda değiştirmenizi öneririz. Örneğin, belirli bir uygulamayla veya başka bir antivirus programının Gerçek zamanlı tarayıcısıyla bir çakışma olması durumunda.

System Center Endpoint Protection yüklendikten sonra, kullanıcılara en üst düzeyde sistem güvenliği sağlamak için tüm ayarlar en iyi duruma getirilir. Varsayılan ayarları geri yüklemek için şu konumda bulunan **Varsayılan** düğmesini tıklatın: **Gerçek Zamanlı Koruma** penceresinin (**Ayarlar** > **Uygulama tercihlerini gir …** > **Koruma** > **Gerçek Zamanlı Koruma**) sol altı.

Gerçek zamanlı korumayı denetleme

Gerçek zamanlı korumanın çalıştığını ve virüsleri algıladığını doğrulamak için eicar.com sınama dosyasını kullanın. Bu sınama dosyası tüm antivirus programları tarafından algılanabilen özel bir zararsız dosyadır. Dosya, EICAR şirketi (Avrupa Bilgisayarları Antivirus Araştırmaları Enstitüsü) tarafından antivirus programlarının işlevselliğini sınamak için oluşturulmuştur.

Gerçek zamanlı korumanın durumunu uzaktan denetlemek için **Terminal**'i kullanarak istemci bilgisayarına bağlanın ve aşağıdaki komutu gönderin:
`/Applications/.scep/Contents/MacOS/scep_daemon --status`

Gerçek zamanlı tarayıcının durumu `RTPStatus=Enabled` veya `RTPStatus=Disabled` olarak görüntülenir.

Terminal çıktısı aşağıdaki durumları da içerir:

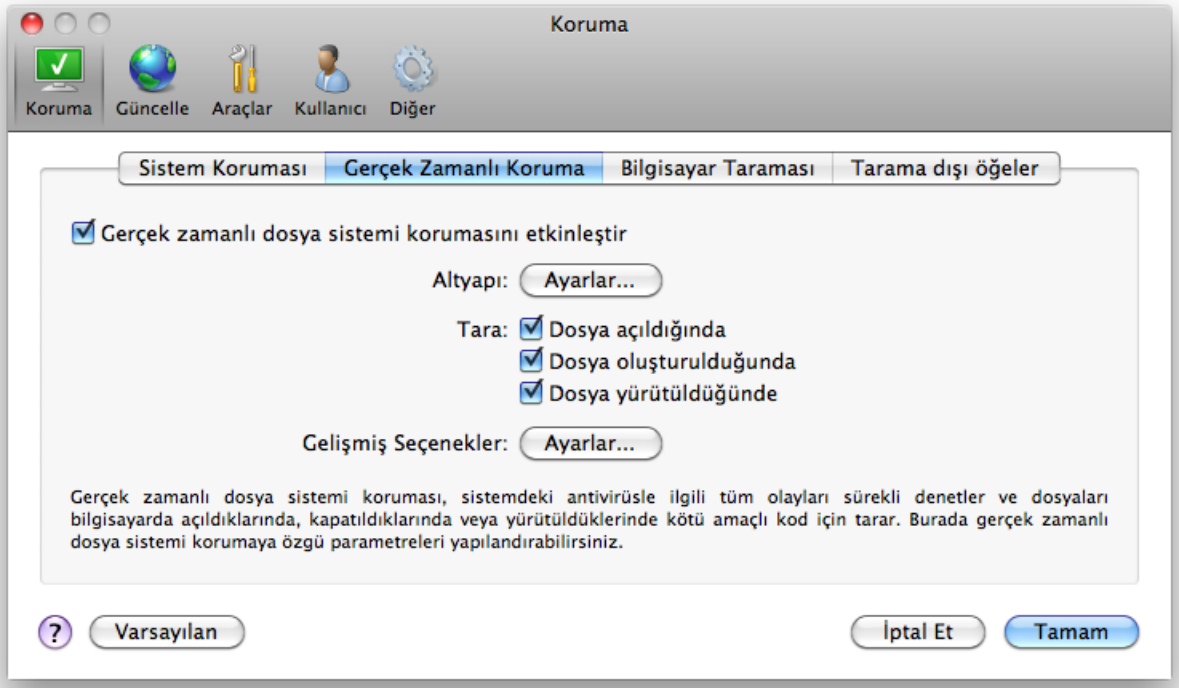
- istemci bilgisayarında yüklü System Center Endpoint Protection sürümü
- virüs imza veritabanının tarihi ve sürümü
- güncelleme sunucusu yolu

NOT: Terminal'i yalnızca ileri düzey kullanıcıların kullanması önerilir.

Gerçek zamanlı koruma çalışmıyorsa neler yapılabilir?

Bu bölümde, Gerçek zamanlı koruma kullanılırken oluşabilecek sorun durumlarını ve bu sorunları nasıl gidereceğinizi açıklıyoruz.

Gerçek zamanlı koruma devre dışı bırakılmış
Gerçek zamanlı koruma kullanıcı tarafından yanlışlıkla devre dışı bırakıldıysa, yeniden etkinleştirilmesi gerekir. Gerçek zamanlı korumayı yeniden etkinleştirmek için, **Ayarlar** > **Antivirus ve antispyware** seçeneğine gidin ve ana program penceresindeki (sağda) **Gerçek zamanlı dosya sistemi korumasını etkinleştir** bağlantısını tıklatın. Alternatif olarak, Gelişmiş ayarlar penceresinde **Koruma** > **Gerçek Zamanlı Koruma** altında **Gerçek zamanlı dosya sistemi korumasını etkinleştir** seçeneğini belirleyerek Gerçek zamanlı dosya sistemi korumasını etkinleştirebilirsiniz.



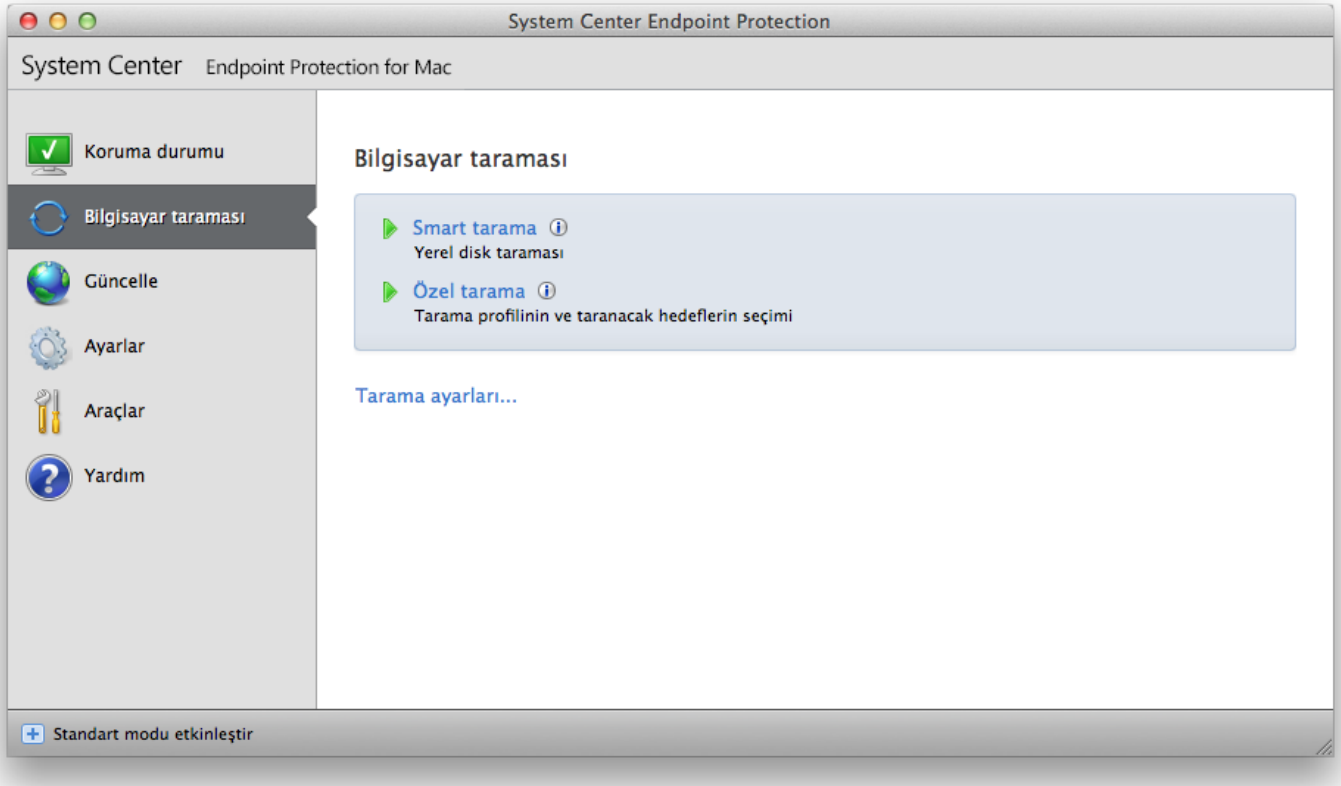
Gerçek zamanlı koruma sızıntıları algılamıyor ve temizlemiyor
Bilgisayarınızda başka antivirus programları yüklü olmadığından emin olun. İki gerçek zamanlı koruma kalkanı aynı anda etkinleştirilirse, birbirleriyle çakışabilirler. Sisteminizde bulunabilecek diğer antivirus programlarını kaldırmanızı öneririz.

Gerçek zamanlı koruma başlamıyor
Gerçek zamanlı koruma, sistem başlatılırken başlamıyorsa, bunun nedeni diğer programlarla çakışmalar olabilir. Bu durumda lütfen Müşteri Desteği uzmanlarına danışın.

İsteğe bağlı bilgisayar taraması

Bilgisayarınızın etkilendiğinden şüpheleniyorsanız (normal olmayan bir şekilde davranıyorsa), bilgisayarınızı sızıntılar açısından incelemek için **Bilgisayar taraması** > **Smart tarama** çalıştırın. Maksimum koruma için bilgisayar taramaları, yalnızca bir virüs bulaştığından şüphelenildiğinde değil, rutin güvenlik önlemlerinin parçası olarak düzenli aralıklarla çalıştırılmalıdır. Düzenli tarama, diske kaydedildiğinde Gerçek zamanlı tarayıcı tarafından algılanmayan sızıntıları algılayabilir. Sızıntı sırasında Gerçek zamanlı tarayıcı devre dışıysa veya virüs imza veritabanı güncel değilse, bu durum oluşabilir.

Ayda en az bir defa İsteğe bağlı bilgisayar taraması çalıştırmanızı öneririz. Tarama, **Araçlar** > **Zamanlayıcı**'dan zamanlanan görev olarak yapılandırılabilir.



Ayrıca masaüstünüzden veya Finder penceresinden System Center Endpoint Protection ana ekranına, dock simgesine, menü çubuğu simgesine (ekranın en üstünde) ya da uygulama simgesine (*/Applications* klasöründe bulunur) sürükleyip bırakabilirsiniz.

Tarama türü

İki tür isteğe bağlı bilgisayar taraması kullanılabilir. **Smart tarama**, tarama parametrelerinde ek bir yapılandırma işlemi gerektirmeden sistemi hızlı bir şekilde tarar. **Özel tarama**, önceden tanımlı tarama profillerinden herhangi birini seçmenize ve ayrıca belirli tarama hedefleri seçmenize olanak tanır.

Smart tarama

Smart tarama, hızlı bir şekilde bilgisayar taraması başlatmanıza ve etkilenen dosyaları kullanıcı müdahalesine gerek kalmadan temizlemenize olanak verir. Temel avantajı, ayrıntılı tarama yapılandırması gerektirmeden kolay işlem yapılmasını sağlamasıdır. Smart tarama, tüm klasörlerdeki tüm dosyaları denetler ve algılanan sızıntıları otomatik olarak temizler veya siler. Temizleme düzeyi otomatik olarak varsayılan değere ayarlanır. Temizleme türleri hakkında ayrıntılı bilgi için Temizleme 14 bölümüne bakın.

Özel tarama

Tarama hedefleri ve tarama yöntemleri gibi tarama parametreleri belirtmek istiyorsanız, **özel tarama** idealdir. Özel tarama çalıştırmanın avantajı, parametreleri ayrıntılı biçimde yapılandırabilme özelliğidir. Farklı yapılandırmalar, kullanıcı tanımlı tarama profilleri olarak kaydedilebilir; bu da taramanın aynı parametrelerle yinelenerek gerçekleştirildiği durumlarda kullanışlı olabilir.

Tarama hedefleri seçmek için **Bilgisayar taraması** > **Özel tarama** seçeneğini belirleyin ve ağaç yapısından belirli **Tarama Hedefleri** seçin. Bir tarama hedefi, dahil etmek istediğiniz klasör veya dosyaların yolu girilerek daha net bir şekilde de belirtilebilir. Ek temizleme eylemi olmadan yalnızca sistemi taramak istiyorsanız, **Temizlemeden tara** seçeneğini belirleyin. Ayrıca, **Ayarlar...** öğesini tıklatarak üç temizleme düzeyinden birini seçebilirsiniz. > **Temizleme**.

Önceden antivirus programları kullanmış olan ileri düzey kullanıcılar için özel tarama ile bilgisayar taramaları gerçekleştirilmesi önerilir.

Tarama hedefleri

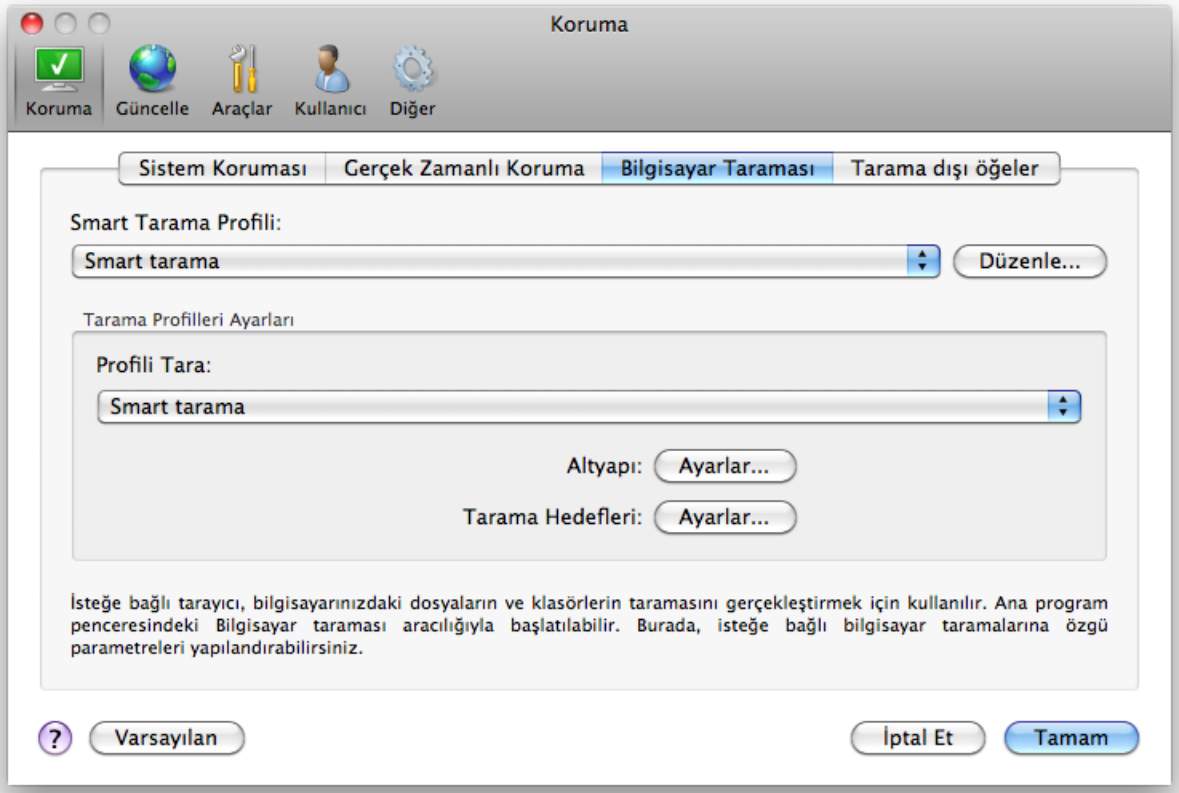
Tarama hedefleri ağaç yapısı, virüs taraması yapılacak dosyaları ve klasörleri seçmenize olanak sağlar. Bir profilin ayarlarına göre de klasörler seçilebilir.

Bir tarama hedefi, taramaya dahil etmek istediğiniz klasör veya dosyaların yolu girilerek daha net bir şekilde de tanımlanabilir. Bilgisayardaki tüm kullanılabilir klasörleri listeleyen ağaç yapısından hedefleri seçin.

Tarama profilleri

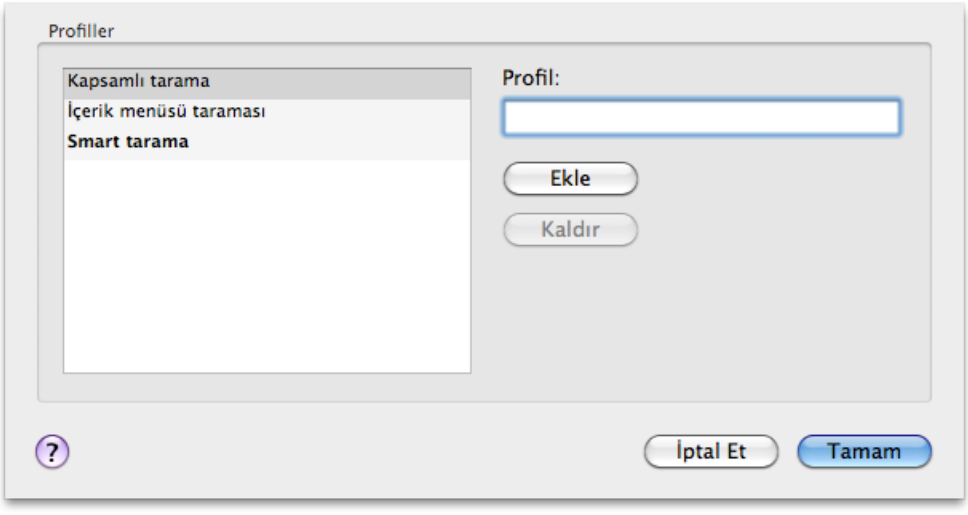
Tercih edilen tarama ayarlarınız daha sonraki taramalar için kaydedilebilir. Düzenli olarak kullanılan her tarama için farklı bir profil (çeşitli tarama hedefleriyle, tarama yöntemleriyle ve diğer parametrelerle) oluşturmanızı öneririz.

Yeni bir profil oluşturmak için **Ayarlar** > **Uygulama tercihlerini gir...** > **Koruma** > **Bilgisayar Taraması** seçeneğine gidin ve geçerli profiller listesinin yanındaki **Düzenle...** düğmesini tıklatın.



İhtiyaçlarınıza uygun bir tarama profili oluşturmanıza yardımcı olması için, tarama ayarlarının her bir parametresine yönelik bir açıklama içeren Altyapı parametreleri ayarları 13 bölümüne bakın.

Örnek: Kendi tarama profilinizi oluşturmak istediğinizi ve Smart tarama yapılandırmasının kısmi olarak uygun olduğunu, ancak tarama çalışma zamanı paketleyicileri veya tehlikeli olabilecek uygulamaları istemezken, Katı kurallı temizleme uygulamak istediğinizi varsayalım. **İsteğe Bağlı Tarayıcı Profilleri Listesi** penceresine profil adını yazın, **Ekle** düğmesini tıklatın ve **Tamam**'ı tıklatarak onaylayın. Ardından **Altyapı** ve **Tarama Hedefleri** seçeneklerini ayarlayarak parametreleri gereksinimlerinize uyacak şekilde ayarlayın.



Altyapı parametreleri ayarları

System Center Endpoint Protection uygulamasında kullanılan tarama teknolojisi proaktiftir; başka bir deyişle, yeni bir tehdidin ilk yayılmaya başladığı saatlerde de koruma sağlar. Sistem güvenliğini önemli ölçüde yükseltmek üzere birlikte çalışan birkaç yöntemin (kod analizi, kod öykünmesi, genel imzalar, virüs imzaları) bir bileşimini kullanır. Tarama altyapısı birkaç veri akışını aynı anda denetleme, böylece verimliliği ve algılama hızını azamiye çıkarma yeteneğindedir. Bu teknoloji aynı zamanda kök kullanıcı takımlarını (rootkit'ler) da başarıyla önler.

Altyapı teknolojisi ayarları seçenekleri, birkaç tarama parametresi belirtmenize olanak sağlar:
- Taranacak dosya türleri ve uzantılar
- Çeşitli algılama yöntemlerinin bileşimi
- Temizleme düzeyleri, vb.

Ayarlar penceresine girmek için **Ayarlar** > **Antivirus ve antispyware** > **Gelişmiş Antivirus ve antispyware koruması ayarları** seçeneğini tıklatın ve sonra **Sistem Koruması**, **Gerçek Zamanlı Koruma** ve **Bilgisayar Taraması** joker karakterlerinde bulunan **Ayarlar...** düğmesini tıklatın. Farklı güvenlik senaryoları farklı yapılandırmalar gerektirebilir. Bu göz önüne alınarak, altyapı parametreleri aşağıdaki koruma modülleri için ayrı ayrı yapılandırılabilir nitelikte hazırlanmıştır:
- **Sistem Koruması** > Başlangıçta otomatik dosya denetimi
- **Gerçek Zamanlı Koruma** > Gerçek zamanlı dosya sistemi koruması
- **Bilgisayar Taraması** > İsteğe bağlı bilgisayar taraması

Altyapı parametreleri her modül için özel olarak en iyi duruma getirilmiştir ve bu parametrelerin değiştirilmesi sistemin çalışmasını önemli ölçüde etkileyebilir. Örneğin, ayarların her zaman çalışma zamanı paketleyicileri taranacak şekilde değiştirilmesi veya Gerçek zamanlı dosya sistemi koruma modülünde gelişmiş sezgisel taramanın etkinleştirilmesi, sistemin yavaşlamasına neden olabilir. Bu nedenle, Bilgisayar taraması dışındaki tüm modüller için varsayılan altyapı parametrelerini değiştirmeden bırakmanızı öneririz.

Nesneler

Nesneler bölümü, hangi bilgisayar dosyalarının sızıntı açısından taranacağını tanımlamanıza olanak sağlar.

- **Dosyalar** - tüm genel dosya türlerinin (programlar, resimler, ses, video dosyaları, veritabanı dosyaları, vb.) taranmasını sağlar.
- **Sembolik bağlantılar** - (Yalnızca isteğe bağlı tarayıcı), işletim sistemi tarafından başka bir dosya veya dizin yolu olarak yorumlanan ve izlenilen bir metin dizesinin yer aldığı özel dosya türlerini tarar.
- **E-posta dosyaları** - (Gerçek zamanlı korumada kullanılamaz), e-posta iletilerinin bulunduğu özel dosyaları tarar.
- **Posta kutuları** - (Gerçek zamanlı korumada kullanılamaz), sistemdeki kullanıcı posta kutularını tarar. Bu seçeneğin yanlış şekilde kullanılması, e-posta istemcinizle çakışmaya neden olabilir.
- **Arşivler** - (Gerçek zamanlı korumada kullanılamaz), arşivlerdeki sıkıştırılmış dosyaların (.rar, .zip, .arj, .tar, vb.) taranmasını sağlar.
- **Kendiliğinden açılan arşivler** - (Gerçek zamanlı korumada kullanılamaz), kendiliğinden açılan arşiv dosyalarında bulunan dosyaları tarar.
- **Çalışma zamanı paketleyicileri** - standart arşiv türlerinden farklı olarak çalışma zamanı paketleyicileri, standart statik paketleyicilere (UPX, yoda, ASPack, FGS, vb.) ek olarak bellekte açılır.

Seçenekler

Seçenekler bölümünde, sistem sızıntılara karşı taranırken kullanılacak yöntemleri seçebilirsiniz. Kullanılabilir seçenekler şunlardır:

- **Sezgisel tarama** - Sezgisel tarama, programların etkinliğini (kötü amaçlı) analiz eden bir algoritma kullanır. Sezgisel taramanın temel avantajı, önceden var olmayan veya bilinen virüsler listesinde (virüs imza veritabanı) bulunmayan yeni kötü amaçlı yazılımları algılama özelliğidir.
- **Gelişmiş sezgisel tarama** - Gelişmiş sezgisel tarama, yüksek düzey programlama dillerinde yazılmış bilgisayar solucanlarının ve truva atlarının algılanması için en iyi duruma getirilmiş benzersiz bir sezgisel tarama algoritmasından oluşur. Gelişmiş sezgisel tarama sonucunda programın algılama yeteneği çok daha yüksektir.
- **İstenmeyen türden olabilecek uygulamalar** - Bu uygulamalar kötü amaçlı olmak zorunda değildir, ancak bilgisayarınızın performansını olumsuz yönde etkileyebilir. Bu tür uygulamalar genellikle yüklenmeden önce onay ister. Bilgisayarınızda bu tür uygulamalar varsa, sisteminiz farklı davranır (bu uygulamalar yüklenmeden önceki davranışıyla karşılaştırıldığında). En önemli değişiklikler arasında; istenmeyen açılır pencereler, gizli işlemlerin etkinleştirilmesi ve çalıştırılması, daha yüksek sistem kaynakları kullanımı, arama sonuçlarında değişiklikler ve uzak sunucularla iletişim kuran uygulamalar yer alır.
- **Tehlikeli olabilecek uygulamalar** - bu uygulamalar; kullanıcının bilgisi olmadan yüklendiyse saldırganlar tarafından kötü amaçla kullanılabilecek ticari ve yasal yazılımlara başvurur. Bu sınıf, uzaktan erişim araçları gibi programları kapsar; bu seçeneğin varsayılan olarak devre dışı bırakılmasının nedeni budur.

Temizleme

Temizleme ayarları, tarayıcının etkilenen dosyaları temizleme şeklini belirler. Üç temizleme düzeyi vardır:

- **Temizleme yok** - Etkilenen dosyalar otomatik olarak temizlenmez. Program bir uyarı penceresi görüntüler ve bir eylem seçmenize olanak sağlar.
- **Standart temizleme** - Program virüsten etkilenen dosyayı otomatik olarak temizlemeye veya silmeye çalışır. Doğru eylem otomatik olarak seçilemiyorsa, program izleme eylemlerinden oluşan bir seçim listesi sunar. Önceden tanımlanmış bir eylem tamamlanamadığında da izleme eylemleri seçimi görüntülenir.
- **Katı kurallı temizleme** - Program etkilenen tüm dosyaları (arşivler dahil) temizler veya siler. Yalnızca sistem dosyaları bu işlemin dışında tutulur. Bunlar temizlenemiyorsa, uyarı penceresi aracılığıyla bir eylem gerçekleştirmeniz istenir.

Uyarı: Varsayılan Standart temizleme modunda, yalnızca arşivdeki tüm dosyalar etkilenmişse arşiv dosyası tümüyle silinir. Arşiv yasal dosyalar da içeriyorsa silinmez. Katı kurallı temizleme modunda etkilenen bir arşiv dosyası algılanırsa, içinde temiz dosyalar olsa bile arşiv tümüyle silinir.

Uzantılar

Uzantı, dosya adının nokta ile ayrılmış olan parçasıdır. Uzantı, dosyanın türünü ve içeriğini tanımlar. Altyapı parametresi ayarlarının bu bölümü, tarama dışında bırakılacak dosya türlerini tanımlamanızı sağlar.

Varsayılan olarak, uzantılarına bakılmaksızın tüm dosyalar taranır. Tarama dışında bırakılan dosyaların listesine herhangi bir uzantı eklenebilir. **Ekle** ve **Kaldır** düğmelerini kullanarak, istenen uzantıların taranmasını etkinleştirebilir veya engelleyebilirsiniz.

Bazen belirli dosya türlerinin taranması, programın düzgün şekilde çalışmasını önlüyorsa dosyaların tarama dışında bırakılması gerekir. Örneğin, *.log*, *.cfg* ve *.tmp* uzantılarının tarama dışında bırakılması önerilebilir.

Sınırlar

Sınırlar bölümü, taranacak nesnelerin maksimum boyutunu ve taranacak arşivlerin derinlik seviyelerini belirtmenize olanak sağlar:

- **Maksimum Boyut:** Taranacak nesnelerin maksimum boyutunu tanımlar. Daha sonra antivirus modülü yalnızca belirtilen boyuttan küçük olan nesneleri tarayacaktır. Genellikle gerek olmadığından, varsayılan değeri değiştirmenizi önermeyiz. Bu seçenek yalnızca büyük nesneleri tarama dışında tutmaya yönelik belirli gerekçeleri olan ileri düzey kullanıcılar tarafından değiştirilmelidir.
- **Maksimum Tarama Süresi:** Bir nesneyi taramaya ayrılan maksimum zaman değerini tanımlar. Buraya kullanıcı tanımlı bir değer girilirse, söz konusu süre geçtikten sonra antivirus modülü, taramanın bitmiş olup olmadığına bakmaksızın nesneyi taramayı durdurur.
- **Maksimum İç İçe Geçme Düzeyi:** Arşiv taramanın maksimum derinliğini belirtir. 10 varsayılan değerinin değiştirilmesini önermeyiz; normal koşullarda bunun değiştirilmesini gerektirecek bir durum olmaz. İç içe geçmiş arşiv sayısı nedeniyle tarama zamanından önce sonlandırılırsa, arşiv denetlenmeden kalır.
- **Maksimum Dosya Boyutu:** Bu seçenek, taranacak arşivlerde bulunan dosyalar için (ayıklandıklarında) maksimum dosya boyutunu belirtmenize olanak sağlar. Tarama bu sınır nedeniyle zamanından önce sonlandırılırsa, arşiv denetlenmeden kalır.

Diğerleri

Smart Optimizasyon etkin durumdayken, en yüksek tarama hızları korunurken en etkili tarama düzeyinin sağlanması için en uygun ayarlar kullanılır. Çeşitli koruma modülleri, farklı tarama yöntemlerinden faydalanarak ve bunları belirli dosya türlerine uygulayarak smart tarama yapabilir. Smart Optimizasyon, ürün içinde değişmez bir şekilde tanımlanmamıştır. Geliştirme ekibimiz, sürekli olarak düzenli güncellemeler yoluyla daha sonra System Center Endpoint Protection uygulamanızla tümleştirilen yeni değişiklikler uygulamaktadır. Smart Optimizasyon devre dışı bırakılırsa, bir tarama gerçekleştirilirken yalnızca belirli modüllerin altyapı temelindeki kullanıcı tanımlı ayarlar uygulanır.

Alternatif veri akışlarını tara (Yalnızca isteğe bağlı tarayıcı)
Dosya sistemi tarafından kullanılan alternatif veri akışları (kaynak/veri ayırmaları), normal tarama teknikleriyle görülemeyen dosya ve klasör ilişkilendirmeleridir. Pek çok sızıntı, kendisini alternatif veri akışı olarak göstererek algılanmamaya çalışır.

Sızıntı algılandı

Sızıntılar, çeşitli giriş noktalarından sisteme ulaşabilir: web sayfaları, paylaşılan klasörler, e-posta veya çıkarılabilir bilgisayar aygıtları (USB, harici diskler, CD'ler, DVD'ler, disketler, vb.).

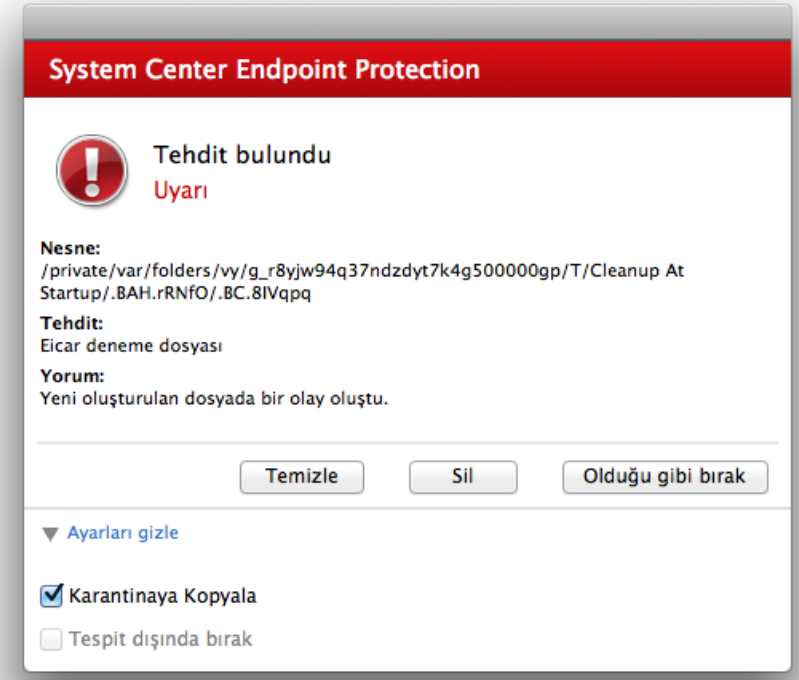
Bilgisayarınız yavaşlama, sık sık donup kalma gibi kötü amaçlı yazılımdan etkilenme işaretleri gösteriyorsa, şu adımları uygulamanızı öneririz:

1. System Center Endpoint Protection uygulamasını açın ve **Bilgisayar taraması**'nı tıklatın.
2. **Smart tarama** düğmesini tıklatın (daha fazla bilgi için Smart tarama 11 bölümüne bakın).
3. Tarama bittikten sonra taranan, etkilenen ve temizlenen dosyaların sayısını görmek için günlüğü inceleyin.

Diskinizin yalnızca belli bir bölümünü taramak istiyorsanız **Özel tarama**'yı tıklatın ve virüs taraması yapılacak hedefleri belirleyin.

System Center Endpoint Protection içinde sızıntıların nasıl işlendiğine ilişkin genel bir örnek olarak şu verilebilir: Varsayılan temizleme düzeyini kullanan Gerçek zamanlı dosya sistemi izleyicisi tarafından bir sızıntı algılandığını varsayın. Uygulama, dosyayı temizlemeye veya silmeye çalışır. Gerçek zamanlı koruma modülü için kullanılabilir olan önceden tanımlı bir eylem yoksa, uyarı penceresinde bir seçenek belirlemeniz istenir. Genellikle, **Temizle**, **Sil** ve **Eylem yok** seçenekleri kullanılabilir. Etkilenen dosya (dosyalar) olduğu gibi bırakılacağından, **Eylem yok**'un seçilmesi önerilmez. Yalnızca dosyanın zararsız olduğundan ve yanlışlıkla algılandığından emin olduğunuzda istisnai olarak bu seçeneği belirleyebilirsiniz.

Temizleme ve silme - Bir dosya, kendisine kötü amaçlı kod ekleyen bir virüsün saldırısına uğradıysa temizleme işlemi uygulayın. Bu durumda, öncelikle etkilenen dosyayı özgün durumuna geri yüklemek için temizlemeyi deneyin. Dosya tümüyle kötü amaçlı kod içeriyorsa silinir.



Arşivlerdeki dosyaları silme - Varsayılan temizleme modunda, arşiv yalnızca etkilenen dosyalar içeriyor ve temiz dosya içermiyorsa tümüyle silinir. Başka bir deyişle, arşivler zararsız temiz dosyalar da içeriyorsa silinmez. Bununla birlikte, **Katı kurallı temizleme** taraması gerçekleştirirken dikkatli olun; katı kurallı temizlemede arşivde tek bir etkilenen dosya bulunsa bile, arşivdeki diğer dosyaların durumuna bakılmaksızın arşiv tümüyle silinir.

Programı güncelleme

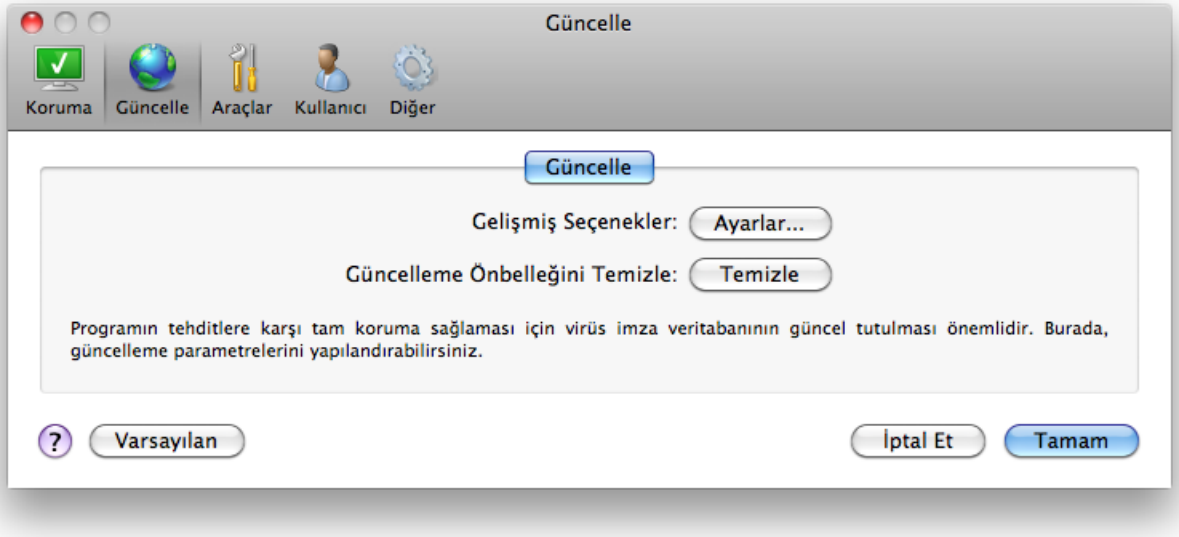
Maksimum güvenlik düzeyini korumak için System Center Endpoint Protection ürününün düzenli olarak güncellenmesi gerekir. Güncelleme modülü, en son virüs imza veritabanını yükleyerek programın her zaman güncel olmasını sağlar.

Ana menüden **Güncelle**'yi tıklatarak, son başarılı güncellemenin tarih ve saati ile güncelleme gerekip gerekmediği de dahil olmak üzere geçerli güncelleme durumunu görebilirsiniz. Güncelleme işlemini el ile başlatmak için **Virüs imza veritabanını güncelle**'yi tıklatın.

Normal şartlar altında, güncellemeler düzgün bir şekilde karşıdan yüklendiğinde Güncelleme penceresinde *Güncelleme gerekmiyor. Yüklenen virüs imza veritabanı geçerli* iletisi görüntülenir.

Güncelleme penceresi aynı zamanda virüs imza veritabanı sürümü hakkında bilgileri de içerir. Bu sayısal gösterge, web sitesine giden ve söz konusu güncelleme sırasında eklenen tüm imzaları listeleyen etkin bir bağlantıdır.

Güncelleme ayarları



Sınama modunun kullanılmasını etkinleştirmek için, **Gelişmiş Seçenekler**'in yanındaki **Ayarlar...** düğmesini tıklatın ve **Sınama modunu etkinleştir** onay kutusunu seçin. Her bir başarılı güncellemenin ardından görüntülenen sistem tepsisi bildirimlerini devre dışı bırakmak için **Başarılı güncelleme hakkında bildirim görüntüleme** onay kutusunu seçin.

Tüm geçici olarak depolanan güncelleme verilerini silmek için, **Güncelleme Önbelleğini Temizle**'nin yanındaki **Temizle** düğmesini tıklatın. Güncelleme sırasında zorluk yaşıyorsanız bu seçeneği kullanın.

Güncelleme görevleri nasıl oluşturulur?

Güncellemeler, ana menüden **Güncelle** tıklatıldıktan sonra görüntülenen birincil pencerede **Virüs imza veritabanını güncelle** seçeneği tıklatılarak el ile tetiklenebilir.

Güncellemeler ayrıca zamanlanan görev olarak da çalıştırılabilir. Zamanlanan bir görevi yapılandırmak için **Araçlar** > **Zamanlayıcı**'yı tıklatın. Varsayılan olarak, System Center Endpoint Protection içinde aşağıdaki görevler etkinleştirilir:

- **Düzenli otomatik güncelleme**
- **Kullanıcı oturum açtıktan sonra otomatik güncelleme**

Her güncelleme görevi, ihtiyaçlarınızı karşılayacak şekilde değiştirilebilir. Varsayılan güncelleme görevlerinin dışında, kendi tanımlı yapılandırmayla yeni güncelleme görevleri oluşturabilirsiniz. Güncelleme görevleri oluşturma ve yapılandırma hakkında daha fazla bilgi için Zamanlayıcı 17 bölümüne bakın.

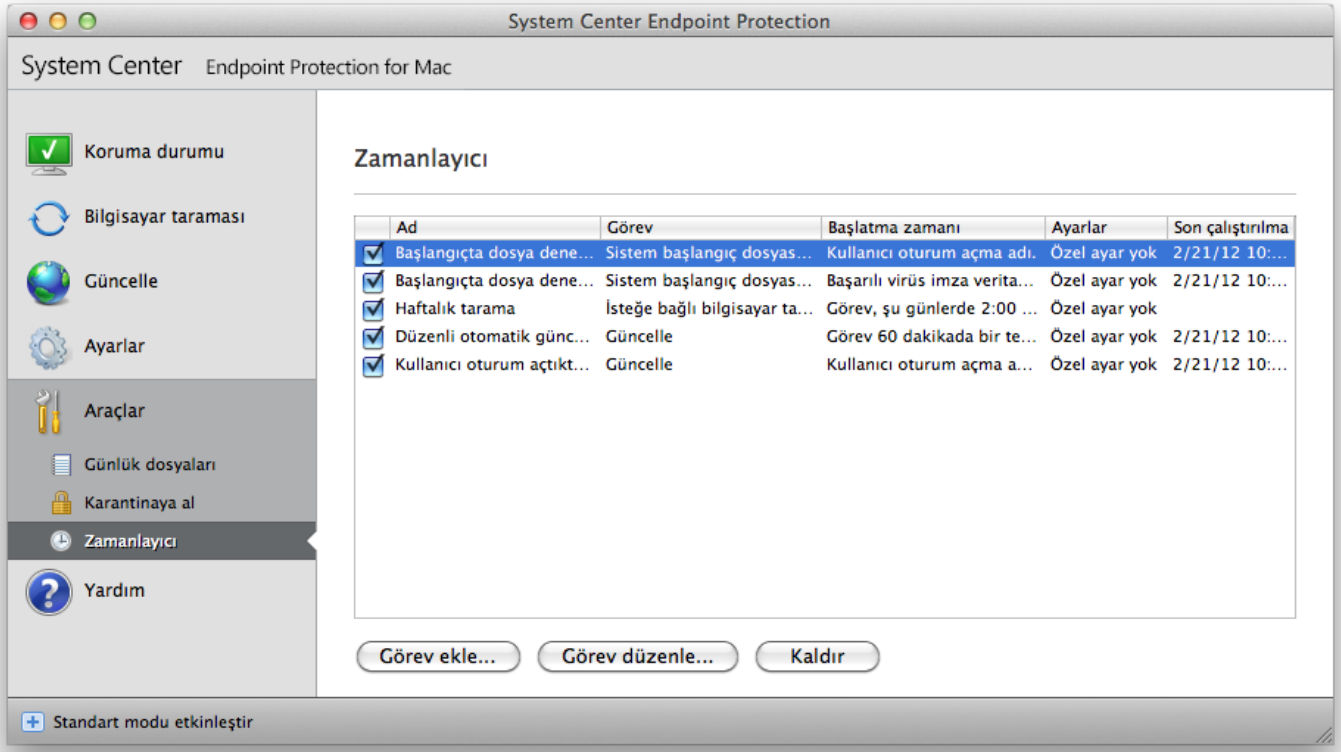
Yeni bir sürüme yükseltme

Maksimum koruma için, en son System Center Endpoint Protection sürümünün kullanılması önemlidir. Yeni bir sürümü denetlemek için, soldaki ana menüden **Güncelle**'yi tıklatın. Yeni bir sürüm kullanılabilir durumdaysa, pencerenin en altında *Ürünün yeni bir sürümü mevcut!* iletisi görüntülenir. Yeni sürümün sürüm numarasını ve değişiklik günlüğünü içeren yeni bir pencere görüntülemek için **Daha fazla bilgi...** seçeneğini tıklatın.

En son sürümü karşıdan yüklemek için **Karşıdan Yükle** seçeneğini tıklatın. Pencereyi kapatıp yükseltmeyi daha sonra karşıdan yüklemek için **Kapat**'ı tıklatın.

Zamanlayıcı

System Center Endpoint Protection uygulamasında Gelişmiş mod etkinse **Zamanlayıcı** kullanılabilir. Zamanlayıcı, System Center Endpoint Protection ana menüsünde **Araçlar**'ın altında bulunabilir. **Zamanlayıcı**, tüm zamanlanan görevlerin ve önceden tanımlı tarih, saat ve kullanılan tarama profili gibi yapılandırma özelliklerinin listesini içerir.



Varsayılan olarak, Zamanlayıcı'da aşağıdaki zamanlanan görevler görüntülenir:

- Düzenli otomatik güncelleme
- Kullanıcı oturum açtıktan sonra otomatik güncelleme
- Kullanıcı oturum açtıktan sonra başlangıçta dosya denetimi
- Virüs imza veritabanının başarılı güncellemesinden sonra başlangıçta dosya denetimi
- Günlük bakımı (zamanlayıcı ayarlarında **Sistem görevlerini göster** seçeneği etkinleştirildikten sonra)
- Haftalık tarama

Varolan bir zamanlanan görevin (hem varsayılan hem de kullanıcı tanımlı) yapılandırmasını düzenlemek için, ctrl tuşuna basın, değiştirmek istediğiniz görevi tıklatın ve **Düzenle...** öğesini seçin veya görevi seçin ve **Görevi düzenle...** düğmesini tıklatın.

Zamanlama görevlerinin amacı

Zamanlayıcı, zamanlanan görevleri önceden tanımlanmış yapılandırma ve özelliklerle başlatır ve yönetir. Yapılandırma ve özellikler tarih ve saat gibi bilgilerin yanı sıra görev yerine getirilirken kullanılacak belirtilmiş olan profilleri de içerir.

Yeni görev oluşturma

Zamanlayıcıda yeni bir görev oluşturmak için, **Görev ekle...** düğmesini tıklatın veya ctrl tuşuna basın, boş alanı tıklatıp içerik menüsünden **Ekle...** öğesini seçin. Beş tür zamanlanmış görev kullanılabilir:

- **Uygulamayı çalıştırma**
- **Güncelleme**
- **Günlük bakımı**
- **İsteğe bağlı bilgisayar taraması**
- **Sistem başlangıcında dosya denetimi**

Güncelleme en sık kullanılan zamanlanmış görevlerden biri olduğu için, yeni güncelleme görevinin nasıl ekleneceğini açıklayacağız.

Zamanlanan görev açılır menüsünden **Güncelle** öğesini seçin. **Görev adı** alanına görevin adını girin. **Görev çalıştır** açılan menüsünden görevin sıklığını seçin. Kullanılabilir seçenekler şunlardır: **Kullanıcı tanımlı**, **Bir kere**, **Yinelenen**, **Günlük**, **Haftalık** ve **Olay**

tetiklendiğinde. Seçilen sıklığa bağlı olarak sizden farklı güncelleme parametreleri istenir.

Kullanıcı tanımlı seçeneğini belirlerseniz, tarihi/saati cron biçiminde belirtmeniz istenir (daha fazla ayrıntı için Kullanıcı tanımlı görev oluşturma 18 bölümüne bakın).

Sonraki adımda, görev zamanlanan saatte yapılamadığında veya tamamlanamadığında hangi eylemin gerçekleştirileceğini tanımlayın. Aşağıdaki üç seçenek kullanılabilir:

- **Bir sonraki zamanlanan saate kadar bekle**
- **Görevi en kısa sürede çalıştır**
- **Görevin son yürütülmesi üzerinden belirtilen aralıktan daha uzun süre geçtiyse görevi hemen çalıştır** (**Minimum görev aralığı** seçeneği kullanılarak aralık tanımlanabilir).

Sonraki adımda, geçerli zamanlanmış görevle ilgili bilgileri içeren bir özet penceresi görüntülenir. **Son** düğmesini tıklatın.

Zamanlanan yeni görev o an için zamanlanmış olan görevler listesine eklenir.

Sistem, doğru ürün işlevselliğini güvence altına almak için varsayılan olarak temel zamanlanan görevleri içerir. Bunlar değiştirilmemeli ve varsayılan olarak gizlenmemelidir. Bu seçeneği değiştirmek ve bu görevleri görünür hale getirmek için, **Ayarlar** > **Uygulama tercihlerini gir...** > **Araçlar** > **Zamanlayıcı** öğesine gidin ve **Sistem görevlerini göster** seçeneğini belirleyin.

Kullanıcı tanımlı görev oluşturma

Kullanıcı tanımlı görevinin tarihi ve saati, yıl uzantılı cron biçiminde girilmelidir (boşlukla ayrılmış 6 alandan oluşan bir dize):
`dakika(0-59) saat(0-23) ayın günü(1-31) ay(1-12) yıl(1970-2099) haftanın günü(0-7)(Pazar = 0 veya 7)`

Örnek:
`30 6 22 3 2012 4`

Cron ifadelerinde desteklenen özel karakterler:
- yıldız işareti (`*`) - İfade, alanın tüm değerleriyle eşleşir. Örneğin, 3. alandaki (ayın günü) yıldız işareti her gün anlamına gelir.
- kısa çizgi (`-`) - Aralıkları tanımlar. Örneğin, `3-9`
- virgül (`,`) - Liste öğelerini ayırır. Örneğin, `1,3,7,8`
- eğik çizgi (`/`) - Aralıkların artışını tanımlar. Örneğin, `3-28/5` 3. alanda (ayın günü) ayın 3. günü ve ondan sonraki her 5 günde bir anlamına gelir.

Gün adları (Pazartesi-Pazar) ve ay adları (Ocak-Aralık) desteklenmez.

NOT: Hem ayın gününü hem de haftanın gününü tanımlarsanız komut, yalnızca her iki alan eşleştiğinde uygulanır.

Karantinaya alma

Karantinanın ana görevi etkilenen dosyaları güvenli bir şekilde saklamaktır. Dosyalar temizlenemiyorsa, silinmeleri güvenli değilse ya da önerilmiyorsa veya System Center Endpoint Protection tarafından hatalı bir şekilde algılanıyorsa, bunların karantinaya alınmaları gerekir.

Herhangi bir dosyayı karantinaya almayı seçebilirsiniz. Bir dosya şüpheli davranıyorsa ancak antivirus tarayıcısı tarafından algılanmıyorsa, bu önerilebilir.

Karantina klasörüne depolanmış dosyalar karantinanın tarih ve saatini, etkilenen dosyanın özgün konumunun yolunu, bayt olarak boyutunu, nedenini (örneğin, kullanıcı tarafından eklenmesi) ve tehdit sayısını (örneğin, birden çok sızıntıyı içeren bir arşiv olup olmadığını) görüntüleyen bir tabloda görülebilir. Karantinaya alınmış dosyaları içeren karantina klasörü (*/Library/Application Support/Microsoft/scep/cache/quarantine*), System Center Endpoint Protection uygulaması kaldırıldıktan sonra da sistemde kalır. Karantinaya alınan dosyalar, güvenli olarak şifrelenmiş şekilde depolanır ve System Center Endpoint Protection yüklendikten sonra geri yüklenebilir.

Dosyaları karantinaya alma

System Center Endpoint Protection, silinen dosyaları otomatik olarak karantinaya alır (bu seçeneği uyarı penceresinde iptal etmediyseniz). İstiyorsanız, herhangi bir şüpheli dosyayı **Karantina...** düğmesini tıklatarak el ile karantinaya alabilirsiniz. Bu amaçla içerik menüsü de kullanılabilir - ctrl tuşuna basın, boş alanı tıklatın, **Karantinaya al...** seçeneğini belirleyin, karantinaya almak istediğiniz dosyayı seçin ve **Aç** düğmesini tıklatın.

Karantinadan geri yükleme

Karantinaya alınan dosyalar ayrıca özgün konumlarına geri yüklenebilir. Bu amaçla **Geri Yükle** düğmesini kullanın. Ctrl tuşuna basılıp **Karantinaya Al** penceresinde ilgili dosya tıklatılıp ardından **Geri Yükle** seçeneği tıklatılarak içerik menüsünden de geri yükleme yapılabilir. İçerik menüsü aynı zamanda dosyayı silinmiş olduğu konumdan farklı bir konuma geri yüklemenize olanak tanıyan **Geri yükleme konumu...** seçeneğini de sunar.

Günlük dosyaları

Günlük dosyaları, gerçekleşen tüm önemli program olayları hakkında bilgi içerir ve algılanan tehditlere genel bir bakış sağlar. Günlüğe kaydetme işlemi, sistem çözümlemesi, tehdit algılama ve sorun giderme açısından önemli bir araçtır. Günlüğe kaydetme işlemi herhangi bir kullanıcı müdahalesi olmadan arka planda etkin biçimde gerçekleşir. Bilgiler, geçerli günlük ayrıntı ayarlarına göre kaydedilir. Doğrudan System Center Endpoint Protection içinden metin iletileri ile günlükleri görüntülemek ve günlükleri arşivlemek mümkündür.

Günlük dosyalarına, System Center Endpoint Protection ana menüsünden **Araçlar** > **Günlük dosyaları** tıklatılarak erişilebilir. Pencerenin üst kısmındaki **Günlük** açılır menüsünü kullanarak istenen günlük türünü seçin. Şu günlükler görüntülenebilir:

1. **Algılanan tehditler** - Sızıntı algılama ile ilgili olaylar hakkında bilgileri görüntülemek için bu seçeneği kullanın.
2. **Olaylar** - Bu seçenek, sistem yöneticileri ve kullanıcıların sorunları gidermesi için tasarlanmıştır. System Center Endpoint Protection tarafından gerçekleştirilen tüm önemli eylemler, Olay günlüklerine kaydedilir.
3. **Bilgisayar taraması** - Tüm tamamlanan taramaların sonuçları bu pencerede görüntülenir. İlgili isteğe bağlı bilgisayar taramasının ayrıntılarını görüntülemek için girişi çift tıklatın.

Her bölümde, giriş seçilerek ve **Kopyala** düğmesi tıklatılarak, görüntülenen bilgiler doğrudan panoya kopyalanabilir.

Günlük bakımı

System Center Endpoint Protection için günlük yapılandırmasına, ana program penceresinden erişilebilir. **Ayarlar** > **Uygulama tercihlerini gir...** seçeneklerini tıklatın > **Araçlar** > **Günlük Dosyaları**. Günlük dosyaları için aşağıdaki seçenekleri belirleyebilirsiniz:

- **Eski günlük kayıtlarını otomatik olarak sil** - belirtilen gün sayısından eski olan günlük girdileri otomatik olarak silinir.
- **Günlük dosyalarını otomatik olarak en iyi duruma getir** - kullanılmayan kayıtlar için belirtilen yüzde aşılırsa, günlük dosyalarının otomatik olarak birleştirilmesini etkinleştirir.

Grafik kullanıcı arabiriminde görüntülenen tüm ilgili bilgiler, tehdit ve olay iletileri düz metin veya CSV (Virgülle ayrılmış değerler) gibi okunabilir metin formatlarında saklanabilir. Bu dosyaları üçüncü taraf araçlar kullanarak işlemek için kullanılabilir duruma getirmek istiyorsanız **Metin dosyalarına günlüğe kaydetmeyi etkinleştir** öğesinin yanındaki onay kutusunu işaretleyin.

Günlük dosyalarının kaydedileceği hedef klasörü belirtmek için **Gelişmiş ayarlar**'ın yanındaki **Ayarlar...** öğesini tıklatın.

Metin Günlük Dosyaları: Düzenle altındaki belirlenmiş seçeneklere bağlı olarak günlükleri aşağıdaki bilgiler yazılmış şekilde kaydedebilirsiniz:

- Başlangıç tarayıcısı, Gerçek Zamanlı Koruma veya Bilgisayar Taraması tarafından algılanan tehditler threatslog.txt adlı dosyada saklanır.
- *Geçersiz kullanıcı adı ve parola*, *Virüs imza veritabanı güncellenemiyor* vb. olaylar eventslog.txt dosyasına yazılır.
- Tüm tamamlanan taramaların sonuçları scanlog.NUMARA.txt formatında kaydedilir.

Varsayılan Bilgisayar Taraması Günlük Kayıtları için filtreleri yapılandırmak üzere, bu seçeneğin hemen yanındaki **Düzenle...** düğmesini tıklatın ve gerektiği şekilde günlük türlerini seçin veya seçimlerini kaldırın. Bu günlük türleriyle ilgili daha fazla açıklama bu bölümde 19 bulunabilir.

Günlük filtreleme

Günlükler önemli sistem olaylarıyla ilgili bilgileri depolar. Günlük filtreleme özelliği, belirli bir olay türü hakkındaki kayıtları görüntülemenize olanak sağlar.

En sık kullanılan günlük türleri aşağıda listelenmektedir:

- **Kritik uyarılar** - kritik sistem hataları (örn. Antivirus koruması başlatılamadı)
- **Hatalar** - "*Dosya karşıdan yükleme hatası*"gibi hata iletileri ve kritik hatalar
- **Uyarılar** - uyarı iletileri
- **Bilgilendirici kayıtlar**- başarılı güncellemeler, uyarılar, vb. gibi bilgilendirici iletiler
- **Tanılama kayıtları** - programı hassas bir şekilde ayarlamak için gereken bilgiler ve yukarıda açıklanan tüm kayıtlar.

Kullanıcı arabirimi

System Center Endpoint Protection kullanıcı arabirimi yapılandırma seçenekleri, çalışma ortamını ihtiyaçlarınıza göre ayarlayabilmenizi sağlar. Bu yapılandırma seçeneklerine, **Ayarlar** > **Uygulama tercihlerini gir...** > **Kullanıcı** > **Arabirim** seçeneğinden erişilebilir.

Bu bölümde, Gelişmiş mod seçeneği kullanıcılara Gelişmiş moda geçişe izin verme yeteneğini sunar. Gelişmiş mod, System Center Endpoint Protection için daha ayrıntılı ayarları ve ek denetimleri görüntüler.

Başlangıçta açılış ekranı işlevselliğini etkinleştirmek için **Açılış ekranını başlangıçta göster** seçeneğini belirleyin.

İlgili görüntüleme modlarında ana program penceresinde standart menü kullanılmasını etkinleştirmek için **Standart menü kullan** bölümünde **Standart modda/Gelişmiş modda** seçeneklerini belirleyebilirsiniz.

Araç ipuçlarını etkinleştirmek için, **Araç ipuçlarını göster** seçeneğini belirleyin. **Gizli dosyaları göster** seçeneği, bir **Bilgisayar taraması** 'nın **Tarama Hedefleri** ayarlarında gizli dosyaları görüntülemenize ve seçmenize olanak sağlar.

Uyarılar ve bildirimler

Uyarılar ve Bildirimler bölümü, System Center Endpoint Protection uygulamasında tehdit uyarılarının ve sistem bildirimlerinin işlenme şeklini yapılandırmanıza olanak sağlar.

Uyarıları görüntüle seçeneğinin devre dışı bırakılması tüm uyarı pencerelerini iptal eder ve bu yalnızca belirli durumlarda uygundur. Birçok kullanıcı için bu seçeneğin varsayılan ayarında (etkin) kalmasını öneriyoruz.

Bildirimleri masaüstünde görüntüle seçeneği belirlendiğinde, masaüstünde (varsayılan olarak ekranın sağ üst köşesinde) görüntülenmesi için kullanıcı etkileşimi gerektirmeyen uyarı pencereleri etkinleştirilir. **Şu süre sonunda bildirimleri otomatik olarak kapat:** X **saniye** değerini ayarlayarak bir bildirimin görüntüleneceği dönemi tanımlayabilirsiniz.

Uyarı ve bildirimler gelişmiş ayarları

Yalnızca kullanıcı müdahalesi gerektiren bildirimleri görüntüle
Bu seçenekle, kullanıcı etkileşimi gerektiren iletileri görüntülemeyi etkinleştirebilir veya devre dışı bırakabilirsiniz.

Uygulamalar tam ekran modunda çalışırken yalnızca kullanıcı müdahalesi gerektiren bildirimleri görüntüle
Bu seçenek, sunum yapılırken veya ekranın tamamını gerektiren başka etkinlikler yapılırken kullanışlıdır.

Ayrıcalıklar

System Center Endpoint Protection ayarları, kuruluşunuzun güvenlik politikaları bakımından çok önemli olabilir. Yetkisiz olarak yapılabilecek değişiklikler sisteminizin kararlılığını ve korunmasını tehlikeye atabilir. Sonuç olarak, hangi kullanıcıların program yapılandırmasını düzenleme iznine sahip olacağını seçebilirsiniz.

Ayrıcalıklı kullanıcıları belirtmek için, **Ayarlar** > **Uygulama tercihlerini gir...** > **Kullanıcı** > **Ayrıcalıklar** seçeneğine gidin.

Sisteminize en yüksek düzeyde güvenlik sağlamak için programın doğru yapılandırılması gerekir. Yetkisiz olarak yapılabilecek değişiklikler, önemli verilerin kaybıyla sonuçlanabilir. Ayrıcalıklı kullanıcıların bir listesini ayarlamak için, soldaki **Kullanıcılar** listesinden kullanıcıları seçin ve **Ekle** düğmesini tıklatın. Bir kullanıcıyı kaldırmak için, sağ taraftaki **Ayrıcalıklı Kullanıcılar** listesinden kullanıcının adını seçin ve **Kaldır**'ı tıklatın.

NOT: Ayrıcalıklı kullanıcılar listesi boşsa, tüm sistem kullanıcıları program ayarlarını düzenleme iznine sahip olacaktır.

İçerik menüsü

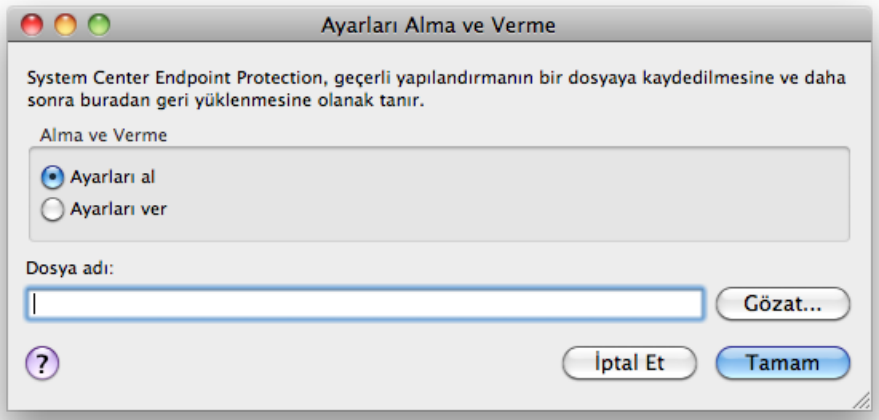
İçerik menüsü tümleştirmesi, **Ayarlar** > **Uygulama tercihlerini gir...** > **Kullanıcı** > **İçerik Menüsü** bölümünde **İçerik menüsüne tümleştir** onay kutusu seçilerek etkinleştirilebilir.

İleri düzey kullanıcı

Ayarları alma ve verme

System Center Endpoint Protection uygulamasının alma ve verme yapılandırmaları, **Ayarlar**'ın altında Gelişmiş modda mevcuttur.

Alma ve Verme, yapılandırmayı depolamak için arşiv dosyalarını kullanır. Geçerli System Center Endpoint Protection yapılandırmasını daha sonra kullanabilmek için yedeklemeniz gerekiyorsa alma ve verme işlemleri kullanışlıdır. Ayarları ver seçeneği aynı zamanda tercih ettikleri System Center Endpoint Protection yapılandırmasını birden çok sistem üzerinde kullanmak isteyen kullanıcılar için de uygundur. Bu kullanıcılar, istedikleri ayarları aktarmak için yapılandırma dosyasını kolayca alabilir.



Ayarları alma

Yapılandırma almak son derece kolaydır. Ana menüden **Ayarlar** > **Ayarları al ve ver...** öğesini tıklatın ve ardından **Ayarları al** seçeneğini belirleyin. Yapılandırma dosyasının adını girin veya almak istediğiniz yapılandırma dosyasına göz atmak için **Gözat...** düğmesini tıklatın.

Ayarları verme

Yapılandırma verme adımları da bu işleme son derece benzer. Ana menüden, **Ayarlar** > **Ayarları al ve ver...** öğesini tıklatın. **Ayarları ver** seçeneğini belirleyin ve yapılandırma dosyasının adını girin. Bilgisayarınızda yapılandırma dosyasının kaydedileceği konumu seçmek için tarayıcıyı kullanın.

Proxy sunucu ayarları

Proxy sunucu ayarları, **Diğer** > **Proxy Sunucu** altında yapılandırılabilir. Proxy sunucunun bu düzeyde belirtilmesi, tüm System Center Endpoint Protection işlevleri için global proxy sunucusu ayarlarını tanımlar. Buradaki parametreler Internet bağlantısının gerekli olduğu tüm modüller tarafından kullanılır.

Bu düzey için proxy sunucu ayarını belirtmek üzere **Proxy sunucu kullan** onay kutusunu ve ardından **Proxy Sunucu** alanında proxy sunucunuzun IP adresini veya URL'sini seçin. Bağlantı noktası alanında, proxy sunucunun bağlantıları kabul ettiği bağlantı noktasını belirtin (varsayılan olarak 3128'dir). Proxy sunucu ile iletişim kimlik doğrulaması gerektiriyorsa, **Proxy sunucu kimlik doğrulaması gerektirir** onay kutusunu seçin ve ilgili alanlara geçerli **Kullanıcı adı**'nı ve **Parola**'yı girin.

Çıkarılabilir medya engelleme

Çıkarılabilir medya (örneğin, CD'ler veya USB anahtarları), kötü amaçlı kod içererek bilgisayarınızı risk altına sokabilir. Çıkarılabilir medyayı engellemek için **Çıkarılabilir medya engellemeyi etkinleştir**'in yanındaki onay kutusunu işaretleyin. Belirli medya türlerine erişime izin vermek için, izin vermek istediğiniz medya türlerinin yanındaki onay kutularının işaretlerini kaldırın.

Bu ayarları CD, DVD, FireWire veya USB dışındaki medya türlerine uygulamak istiyorsanız **Diğer**'in yanındaki onay kutusunu işaretleyin. Bu ayar özellikle bilgisayarınıza Thunderbolt arabirimi aracılığıyla bağlı olan çevre birimleri için uygulanır.

Sözlük

Sızıntı türleri

Sızıntı, kullanıcının bilgisayarına girmeye ve/veya zarar vermeye çalışan kötü amaçlı yazılım parçasıdır.

Virüsler

Bilgisayar virüsü bilgisayarınızdaki dosyaları bozan bir sızıntıdır. Virüsler, bir bilgisayardan diğerine yayılmak için biyolojik virüslere benzer teknikler kullandıklarından bu adı almıştır.

Bilgisayar virüsleri genellikle yürütülebilir dosyalara, komut dosyalarına ve belgelere saldırır. Virüs çoğalmak için hedef dosyanın sonuna kendi "gövdesini" ekler. Bilgisayar virüsünün çalışması kısaca şu şekilde açıklanabilir: etkilenen dosyanın yürütülmesinden sonra, virüs kendisini etkinleştirir (özgün uygulamadan önce) ve önceden tanımlanmış görevini gerçekleştirir. Özgün uygulamanın çalışmasına ancak bundan sonra izin verilir. Kullanıcı yanlışlıkla veya bilerek kötü amaçlı programı çalıştırmadıkça veya açmadıkça, virüs bilgisayarı etkileyemez.

Bilgisayar virüsleri amaçları ve şiddetleri açısından farklılık gösterebilir. Bazıları kasıtlı olarak sabit disk sürücüsündeki dosyaları silebildiğinden aşırı tehlikelidir. Diğer yandan bazı virüsler zarara neden olmaz; yalnızca kullanıcıyı rahatsız eder ve yazarlarının teknik becerilerini gösterir.

Kötü amaçlı yazılım yazarları için ticari açıdan cazip olmadıklarından, virüslerin (truva atları veya casus yazılım ile kıyaslandığında) gitgide daha az görüldüğünü unutmamak önemlidir. Ayrıca "virüs" terimi, genelde tüm sızıntı türlerini kapsayacak şekilde yanlış kullanılmaktadır. Bu kullanım yavaş yavaş değiştirilerek yeni ve daha doğru "kötü amaçlı yazılım" (zararlı yazılım) terimine yerini bırakmaktadır.

Bilgisayarınız virüsten etkilendiyse, etkilenen dosyaları özgün durumlarına geri yüklemeniz (antivirus programı kullanarak temizlemeniz) gerekir.

Virüslere örnek olarak şunlar verilebilir: *OneHalf*, *Tenga* ve *Yankee Doodle*.

Solucanlar

Bilgisayar solucanı, ana bilgisayarlara saldıran ve ağ aracılığıyla yayılan kötü amaçlı kod içeren bir programdır. Virüs ile solucan arasındaki en temel fark, solucanların kendi kendilerine çoğalabilmesi ve dolaşabilmesidir. Bunlar, ana bilgisayar dosyalarına (veya önyükleme kesimlerine) bağlı değildir. Solucanlar iletişim listenizdeki e-posta adresleri üzerinden yayılır ve ağ uygulamalarındaki güvenlik açıklarından yararlanır.

Bu nedenle solucanlar bilgisayar virüslerinden daha çok yaşayabilir. Internet'in yaygın kullanımı sayesinde, ortaya çıktıktan sonra birkaç saat içinde, hatta bazı durumlarda bir kaç dakikada tüm dünyaya yayılabilir. Bağımsız olarak ve hızlı bir şekilde çoğalabilme özelliği nedeniyle, solucanlar diğer kötü amaçlı yazılımlar türlerinden daha tehlikelidir.

Sistemde etkinleştirilen solucan çeşitli sıkıntılara neden olabilir: Dosyaları silebilir, sistem performansını düşürebilir, hatta programları devre dışı bırakabilir. Bilgisayar solucanı doğası gereği diğer sızıntı türleri için "taşıma yöntemi" görevi yapar.

Bilgisayarınız bir solucandan etkilendiyse, etkilenen dosyalar kötü amaçlı kod içerebileceğinden bu dosyaları silmenizi öneririz.

Tanınmış solucanlara örnek olarak şunlar verilebilir: *Lovsan/Blaster*, *Stration/Warezov*, *Bagle* ve *Netsky*.

Truva atları

Tarihlerine baktığımızda bilgisayarlardaki truva atlarının kendilerini yararlı programlar olarak göstererek kullanıcıları kandırmayı ve çalışmalarına izin vermeye ikna etmeyi hedefleyen sızma programları sınıfına dahil olduklarını görürüz. Truva atlarının artık kendilerini başka bir program gibi göstermeleri gerekmiyor. Tek amaçları sisteme mümkün olduğunca hızla sızmak ve amaçlarını gerçekleştirmek. "Truva atı" herhangi bir sızma sınıfına girmeyen tüm sızma programlarını tanımlayan çok genel bir terim haline geldi.

Bu sınıf çok geniş bir kategori oluşturduğundan genellikle pek çok alt kategoriye bölünür:

- Yükleyici - Internet'ten diğer sızma programlarını yükleme becerisi olan kötü amaçlı program.
- Dağıtıcı - Güvenliği aşılan bilgisayarlara diğer kötü amaçlı yazılım türlerini dağıtmak üzere tasarlanmış bir truva atı türü.
- Arka kapı programı - Uzak saldırganlarla iletişim kurarak bir sisteme erişmelerine ve denetimini ele geçirmelerine olanak veren uygulama.
- Tuş kaydedici - (tuş vuruşu kaydedici) - Kullanıcının bastığı her tuşu kaydederek uzak saldırganlara gönderen program.

- Numara çevirici - Numara çeviriciler, özel ücretli numaralara bağlanmak için tasarlanan programlardır. Kullanıcının yeni bir bağlantı oluşturulduğunu anlaması neredeyse imkansızdır. Numara çeviriciler yalnızca artık pek sık kullanılmayan çevirmeli bağlantı kullanan kullanıcıları etkiler.
- Truva atları genellikle yürütülebilir dosya biçimini alır. Bilgisayarınızda truva atı olarak belirlenen bir dosya varsa, büyük olasılıkla kötü amaçlı kod içeriyor olduğundan bunu silmeniz önerilir.

Bilinen truva atlarına örnek olarak şunlar verilebilir: *NetBus*, *Trojandownloader.Small.ZL*, *Slapper*.

Reklam yazılımı

Reklam yazılımı, reklamları destekleyen yazılımın kısaltılmış biçimidir. Reklam malzemelerini görüntüleyen programlar bu kategoriye girer. Reklam yazılımı uygulamaları genellikle otomatik olarak Internet tarayıcısında reklam içeren bir pencere açar veya tarayıcının giriş sayfasını değiştirir. Reklam yazılımı genelde ücretsiz sağlanan programlarla birlikte verilerek, ücretsiz yazılım programlarını oluşturanların, uygulamalarını (bu uygulamalar genellikle yararlıdır) geliştirme maliyetlerini karşılamalarına olanak sağlar.

Reklam yazılımı tek başına tehlikeli değildir; kullanıcılar yalnızca reklamlardan rahatsız olabilir. Gerçek tehlike, reklam yazılımlarının izleme işlevleri de gerçekleştirebilmesidir (casus yazılımların yaptığı gibi).

Ücretsiz sağlanan bir ürün kullanmaya karar verirseniz, lütfen yükleme programına özellikle dikkat edin. Yükleyici büyük bir olasılıkla ek bir reklam yazılımı programının yüklendiğini size bildirir. Çoğunlukla bu yüklemeyi iptal etmenize ve programı reklam yazılımı olmadan yüklemenize izin verilir.

Bazı programlar reklam yazılımı olmadan yüklenmez veya işlevleri sınırlı olur. Bu da, kullanıcılar kabul ettiğinden, söz konusu reklam yazılımının sisteme çoğu kez "yasal" yoldan erişebileceği anlamına gelir. Bu durumda, üzülmektense güvenli tarafta kalmak daha iyidir. Bilgisayarınızda reklam yazılımı olarak algılanan bir dosya varsa, kötü amaçlı kod içerme olasılığı yüksek olduğundan bu dosyayı silmeniz önerilir.

Casus yazılım

Bu kategori kullanıcının onayı/bilgisi olmadan özel bilgileri gönderen tüm uygulamaları kapsar. Casus yazılım ziyaret edilen web siteleri listesi, kullanıcının ilgili kişiler listesindeki e-posta adresleri veya kaydedilen kullanılmış tuş listesi gibi çeşitli istatistik verilerini göndermek için izleme işlevlerini kullanır.

Casus yazılım yazarları bu tekniklerin kullanıcıların ihtiyaçları ve ilgi alanları konusunda daha çok bilgi toplayarak hedefleri daha iyi belirlenmiş reklamlar yayımlamayı amaçladığını iddia eder. Buradaki sorun şudur: Yararlı uygulamalarla kötü amaçlı uygulamalar arasında net bir ayrım yoktur ve toplanan bilgilerin kötü niyetle kullanılmayacağından kimse emin olamaz. Casus yazılımlar tarafından toplanan veriler güvenlik kodları, PIN'ler, banka hesap numaraları ve benzer bilgileri içerebilir. Casus yazılımlar sıklıkla yazarı tarafından gelir elde etme veya yazılımı satın alanlara özel bir teklif sunma amacıyla bir programın ücretsiz sürümüyle birlikte gelir. Kullanıcılar sıklıkla programı yüklerken kendilerine ücretli sürüme yükseltme konusunda bir teklif sunulursa casus yazılımın varlığı konusunda bilgi sahibi olur.

Casus yazılımlarla birlikte geldikleri bilinen tanınmış ücretsiz yazılım ürünlerine örnek olarak P2P (eş düzey) ağların istemci uygulamaları verilebilir. Spyfalcon veya Spy Sheriff (ve daha pek çoğu) belirli bir casus yazılım alt kategorisine dahildir; casus yazılım önleme programları gibi görünürler, ancak gerçekte birer casus yazılım programıdırlar.

Bilgisayarınızda bir dosya casus yazılım olarak algılanırsa, kötü amaçlı kod içerme olasılığı yüksek olduğundan bu dosyayı silmeniz önerilir.

Tehlikeli olabilecek uygulamalar

Ağdaki bilgisayarların yönetimini basitleştirme işlevine sahip pek çok geçerli program vardır. Ancak, kötü niyetli kişilerin elinde bu programlar kötü amaçlarla kullanılabilir. System Center Endpoint Protection, bu tür tehditleri algılama seçeneğini sunar.

"Tehlikeli olabilecek uygulamalar" ticari ve geçerli uygulamalar için kullanılan bir sınıftır. Bu sınıf uzaktan erişim araçları, parola kırma uygulamaları ve tuş kaydediciler (kullanıcının bastığı her tuşu kaydeden program) gibi programları içerir.

Bilgisayarınızda tehlikeli olabilecek bir uygulamanın bulunduğunu ve çalıştığını belirlerseniz (ve bunu siz yüklemediyseniz) lütfen ağ yöneticinize başvurun veya uygulamayı kaldırın.

İstenmeyen türden olabilecek uygulamalar

İstenmeyen türden olabilecek uygulamaların mutlaka zararlı olması gerekmez, ancak bilgisayarınızın performansını olumsuz yönde etkileyebilirler. Bu tür uygulamalar genellikle yüklenmeden önce onay ister. Bilgisayarınızda bu tür uygulamalar varsa sisteminiz yüklemeden önceki davranış şekliyle karşılaştırıldığında farklı davranır. En belirgin değişiklikler şunlardır:

- önceden görmediğiniz yeni pencereler açılır
- gizli işlemler etkinleştirilir ve çalıştırılır
- sistem kaynaklarının kullanımı artar
- arama sonuçları değiştirilir
- uygulama uzak sunucularla iletişim kurar.