



E-Data Teknoloji



Endpoint Protector 2009™

İşletmeler için Cihaz Kontrolü ve Veri Kaybı Önleyici

Windows XP/Vista/7 Müşteri Sürümü: 3.0.8.4 Windows 2003/2008 Server Sürümü: 3.0.4.5
Mac OS X Sürümü: 1.0.1.8 Linux Server Sürümü: 3.0.4.5

Verileriniz ancak uç noktalarınız kadar güvencedir.



Kontrol edilen cihaz tipleri

- USB flaş diskler (Normal USB diskler, U3 vs.)*
- Bellek kartları (SD/MMC/CF vs.)*
- CD/DVD oynatıcı/yazıcı (dahili ve harici)*
- harici Hard Diskler*
- Disket sürücüler
- Kart okuyucuları (dahili ve harici)*
- ZIP diskler
- Dijital kameralar*
- Smartphone/Blackberry/PDA
- iPhone/iPad/iPod*
- FireWire cihazları*
- MP3 Çalar/Medya oynatıcı cihazlar
- Biyometrik sürücüler
- Bluetooth cihazlar
- Yazıcılar
- Express kartlar (SSD)
- Kablosuz USB

Endpoint Protector 2009

PC ve Cihazlar arasındaki Güvenlik Duvarı

Endpoint Protector şirketlerin veri güvenliği, veri ihlali yönetimi ve Bilişim (IT) yönetimiyle ilgili dahili cihaz kullanım politikaları, yönetmelikleri ve standartlarına daha iyi uyabilmelerine olanak sağlar.

Hareket halindeyken Güvenilir Cihazlar kullanarak verilerinizin şifrelenmesini sağlar.

Trusted Device

Endpoint Protector 2009 uç noktalarda kullanılacak taşınabilir cihazlarla ilgili kuralların uygulanmasında politika tabanlı bir yaklaşım sunar.

PC'ler ve MAC'lar için koruma sağlayan tek çözümdür.

Taşınabilir ve yaşam tarzı cihazlarını çalışma ve yaşama biçimimizi dönüştürdüğü bir dünyada Endpoint 2009 verimliliği korumak ve çalışmayı daha kolay, güvenli ve keyifli hale getirmek için tasarlanmıştır.

Whitelist (Beyaz Liste) yaklaşımı spesifik cihazların belli kullanıcı/gruplar için kullanılarak bir yandan verimli kalırken bir yandan da hangi cihazların kullanıldığı ve hangi veri kullanıcılarının aktarmaya izinli oldukları konusunda kontrolü ellerinde tutmalarına olanak sağlar.

Endpoint Protector 2009 verilerin sızdırılması, çalınması, bozulması veya diğer şekillerde güvenliğini kaybetmesine yol açabilecek dahili tehditlerin getirdiği riskleri önemli ölçüde azaltır.

İş İstasyonları, Notebook ve Netbook'lar için Endpoint Security (Güvenlik)

Çıkarılabilir bellek cihazlarının getirdiği tehditlere karşı koruma. Bilerek veya kazayla veri sızması, çalınması, kaybı ve kötü niyetli bulaştırma olaylarını durdurur.

Cihaz Yönetimi / Cihaz Kontrolü*

Ağınızdaki cihazlar / kullanıcılar veya bilgisayarlar için hakları tanımlar.

Merkezi web tabanlı Yönetim / Ön Panel

Çıkarılabilir bellek cihazlarının kullanımını merkezi olarak yönetir. Web-tabanlı Yönetimsel ve Raporlama arayüzü yönetim ve IT (Bilişim) Güvenliği personelinin gereksinimlerini karşılayarak organizasyon genelinde kontrol edilen cihazlar ve veri transferi faaliyetleri hakkında gerçek zamanda bilgi verir.

Dosya İzleme / Dosya Yedekleme

Dosya izleme, izin verilen cihazlara ve cihazlardan kopyalanan tüm verilerin kayıtlarını tutar. Dosya yedekleme ise kontrol edilen cihazlarla ilgili olarak kullanılan tüm dosyaların, silinmiş de olsa, birer kopyasını kaydeder.

Whitelisting Dosyası

Sadece izin verilen dosyalar yetki verilen cihazlara aktarılabilir. Tüm diğer dosyalar bloke edilir ve transfer teşebbüsleri rapor edilir.

Cihaz Faaliyeti Kayıtları – Denetim Yolu

Bağlanan tüm müşteri ve cihazlar için kaydedilen cihaz faaliyet kayıtlarını saklar, PC'ler ve kullanıcılar hakkında denetim ve ayrıntılı analiz için geçmiş bilgilerini sağlar.

Raporlama ve Analiz

Faaliyetleri kolayca gözden geçirmek için güçlü raporlama, grafik ve analiz aygıtları

Güvenlik Politikalarınızın Kolayca Uygulanması (Aktif Dizin)

Tanımlanan Kullanıcı Grupları için basitleştirilmiş cihaz yönetimi politikaları ve özelleştirilebilir şablonlar (Aktif Dizin GPO'ları) güvenlik politikalarının ağ genelinde kolayca uygulanmasını ve bakımını sağlar.

Geçici Çevrimdışı Şifre / Ağ "Çevrimdışı" Modu

Ağdan ayrılmış korunmuş PC'ler, korunmuş olarak kalır. Yolda verimliliği devam ettirmek için cihazlara Geçici Şifre görevi ile geçici olarak izin verilebilir.



E-Data Teknoloji



Endpoint Protector Müşteri Kendini Koruması

Kullanıcıların yönetici hakları bulunduğu PC'lerde bile koruma sağlar.

Endpoint güvenlik politikalarını uygulayarak verilerin kimler tarafından ve nasıl transfer edileceğini kontrol altına alın.

SİSTEM GEREKSİNİMLERİ (Müşteri/ler)

- Windows 7 (32/64 bit)
- Windows Vista (32/64 bit)
- Windows XP (SP2) (32/64 bit)
- Windows 2003/2008 (32/64 bit)
- Mac OS X 10.4 +
- Net 2.0 Framework
- Min. 32 MB Hard Disk alanı

Server

Desteklenen İşletim Sistemleri

- Windows 2003 server
- Windows 2008 server
- Debian (*Ubuntu) Red Hat (Fedora, CentOS), Suse

Desteklenen Web Serverleri

- IIS 6.0 / 7.0 veya
- Apache (Sürüm 5 veya daha yeni)

Desteklenen Veritabanları

- Microsoft SQL 2005/2008 (Exp), veya
- My SQL (Sürüm 5 veya daha yeni)
- PHP (Sürüm 5), SOAP desteğiyle
- OpenSSL Sürüm 0.9.8

İlave Server Gereksinimleri

- PHP (Sürüm 5), SOAP desteğiyle
- OpenSSL Sürüm 0.9.8

Dizin Hizmeti

- Aktif Dizin

Kurulu bulunan MSI dağıtım mekanizmalarıyla kolay kurulum

Endpoint Protector server mevcut altyapıya hızlı ve uygun fiyatlı bir entegrasyon sağlamak için farklı server platformlarıyla uyumludur.

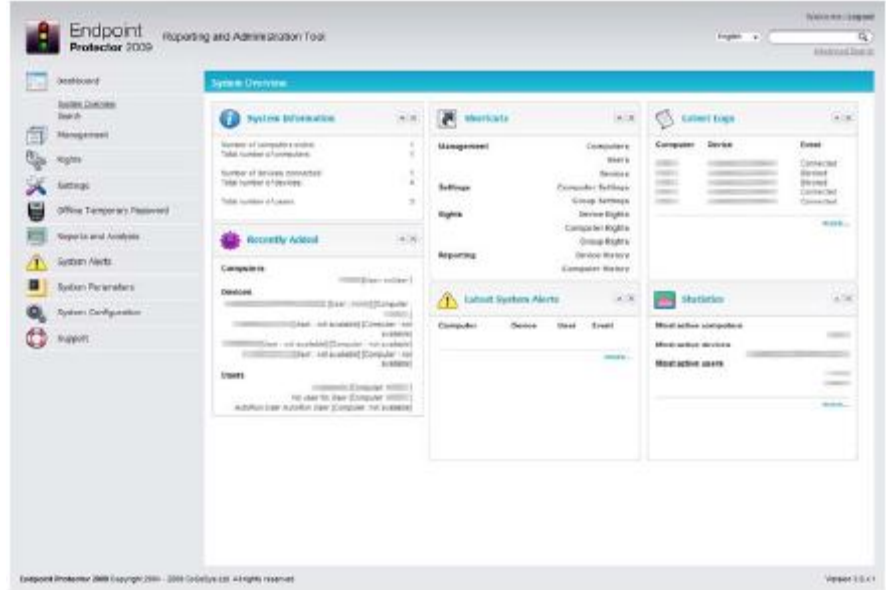
Sezgisel web-tabanlı arayüz etkin bir yönetime olanak sağlar.

Endpoint Protector, taşınabilir bellek ve uç noktası cihazlarıyla güvenli ve emin bir çalışma ortamı sunar. Yetki verilen cihaz devamlı olarak korunmuş PC'lerle kullanılırken ağ uç noktası güvenlik politikası uygulandığından kullanıcı verimliliği sınırlanmaz.

Şifrelemeye zorlama – EasyLock Güvenilir Cihaz Teknolojisi ile hareket halindeyken hassas verilerin korunması

TrustedDevice (Güvenilir Cihaz) teknolojisi korunan ortamdaki tüm taşınabilir cihazların sadece endpoint yazılımı ve güvenlik politikalarıyla yetkilendirilmesi ve kontrol edilmesini için onaylı değil, aynı zamanda hareket halindeyken hassas ve gizli bilgilerin korunması için de onaylı ve güvenilirdir. Bununla cihaz çalındığında veya kaybolduğunda üzerinde yüklü tüm verilerin şifrelenmiş olması ve bu nedenle başkalarının erişememesi sağlanır.

Ücretsiz bir deneme ve daha fazla için www.EndpointProtector.com sitesini ziyaret ediniz



Endpoint Protector 2009 Ön Paneli
Raporlama ve Yönetim Aracı

- Endpoint güvenlik
- Veri kaybı önleme
- Taşınabilir aygıt yönetimi
- Veri hırsızlığı önleme
- Veri izleme
- Analiz ve Raporlama
- Veri Aktarımı izleme
- Dosya takibi
- Veri Şifreleme ve senkron.
- Yoldayken hassas verilerin korunması



Kullanıcı Politikası Uygulaması
CoSoSys Veri Koruma Çözümleri

Endpoint Protector 2009 üç aşamalı bir Güvenlik Mimarisi üzerine inşa edilmiştir:
Önleme – İzleme – Şifreleme ve Uygulama