



## Endpoint Protector Cihazı™

PC ve MAC bilgisayarlar için Cihaz Kontrolü / Veri Kaybı Önleme cihazı



### 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
- Seri Port

### Endpoint Protector Cihazı Bilgisayar ve Cihazlar arasındaki Güvenlik Duvarıdır

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.

### Kutudan çıktığı gibi kullanılabilen, Uç Noktalar cihaz tehditlerine karşı güvenli

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

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

Taşınabilir cihazlar çalışma ve yaşama biçimimizi dönüştürmektedir. 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 Cihazı verilerin sızdırılması, çalınması, bozulması veya diğer şekillerde güvenliğini kaybetmesine yol açabilecek dahili tehditlerin getirdiği riskleri önemli ölçüde azaltır.

### PC ve MAC'lar için bir cihaz olarak 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 Politikalarının 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.

### 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

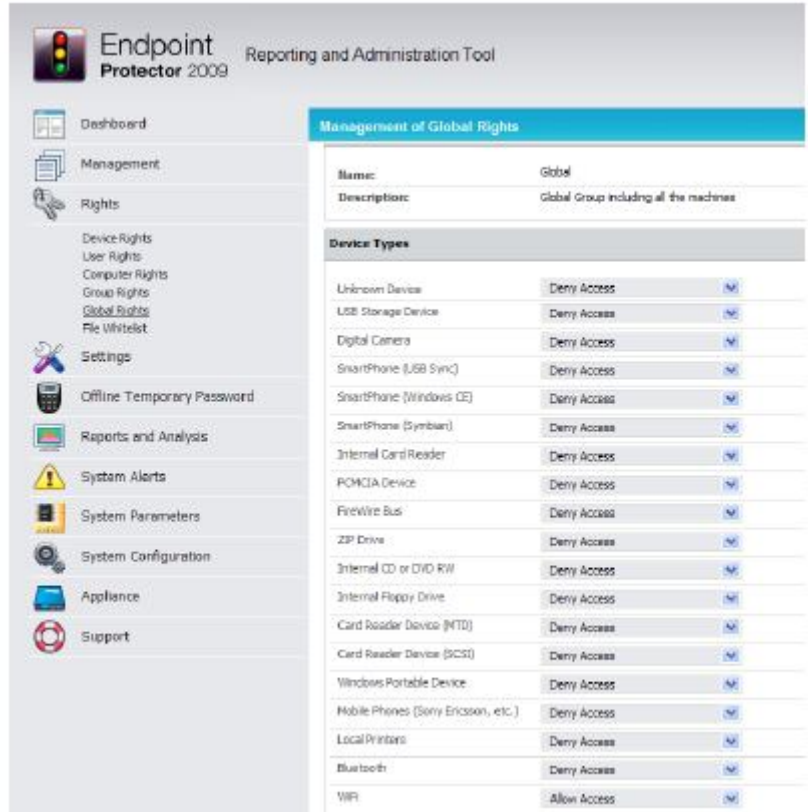
### Dizin Hizmeti

- Aktif Dizin

Otomatik yapılandırılan MSI dağıtım mekanizmalarıyla kolay kurulum

Endpoint Protector Cihazına gerekli tüm Server Donanımları dahildir. Sadece ambalajdan çıkarıp bilgisayar ağınıza bağlayarak müşterilerinizi PC'lere ve MAC'lara dağıtın, birkaç dakika içinde tüm portlar kontrol edilmeyen cihazların kullanımına karşı korunmuş olacaktır.

Sezgisel web-tabanlı yönetim arayüzü etkin bir yönetime olanak sağlar.



Endpoint Protector Cihazı web tabanlı Raporlama ve Yönetim Aracı Arayüzü

Modeller	A50	A100	A250	A1000	A4000
Bilgisayar için Koruma (PC/MAC)	50	100	250	1000	4000
İlave kapasite	25	50	125	500	2000
Gövde (Rafa monte)	1U	1U	1U	1U	3U
İşlemci	ULV Çift Çekirdek	ULV Çift Çekirdek	Dört Çekirdek	Dört Çekirdek	2xDört Çekirdek
Hard Disk	160 GB	320 GB	500 GB	2 x 1 TB (Raid 1)	6 x 1 TB (Raid 5)
Güç Kaynağı	200W, 100-240V	200W, 100-240V	260W, 100-240V	260W, 100-240V	2x800W, 100-240V
Donanım Garantisi	2-yıl dahil. İlave garanti ve değişime seçenekleri mevcuttur.				

### Şifrelemeye zorlama – EasyLock ile hareket halindeyken hassas verilerin korunması

İsteğe bağlı EasyLock yazılımıyla birlikte TrustedDevice (Güvenilir Cihaz) teknolojisi korunan ortamdaki tüm taşınabilir cihazların sadece 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](http://www.EndpointProtector.com) sitesini ziyaret ediniz