ENDPOINT PROTECTOR | by CoSoSys

DATASHEET 5.2.0.0

Veri Sızıntısı Önleme & Mobil Cihaz Yönetimi

Her Ağ Büyüklüğü ve Sektöre Uyumlu Çözüm

Windows, Mac ve Linux için DLP

Ağınızı Uçtan Uca Koruyun

ENDPOINT PROTECTOR

by CoSoSys

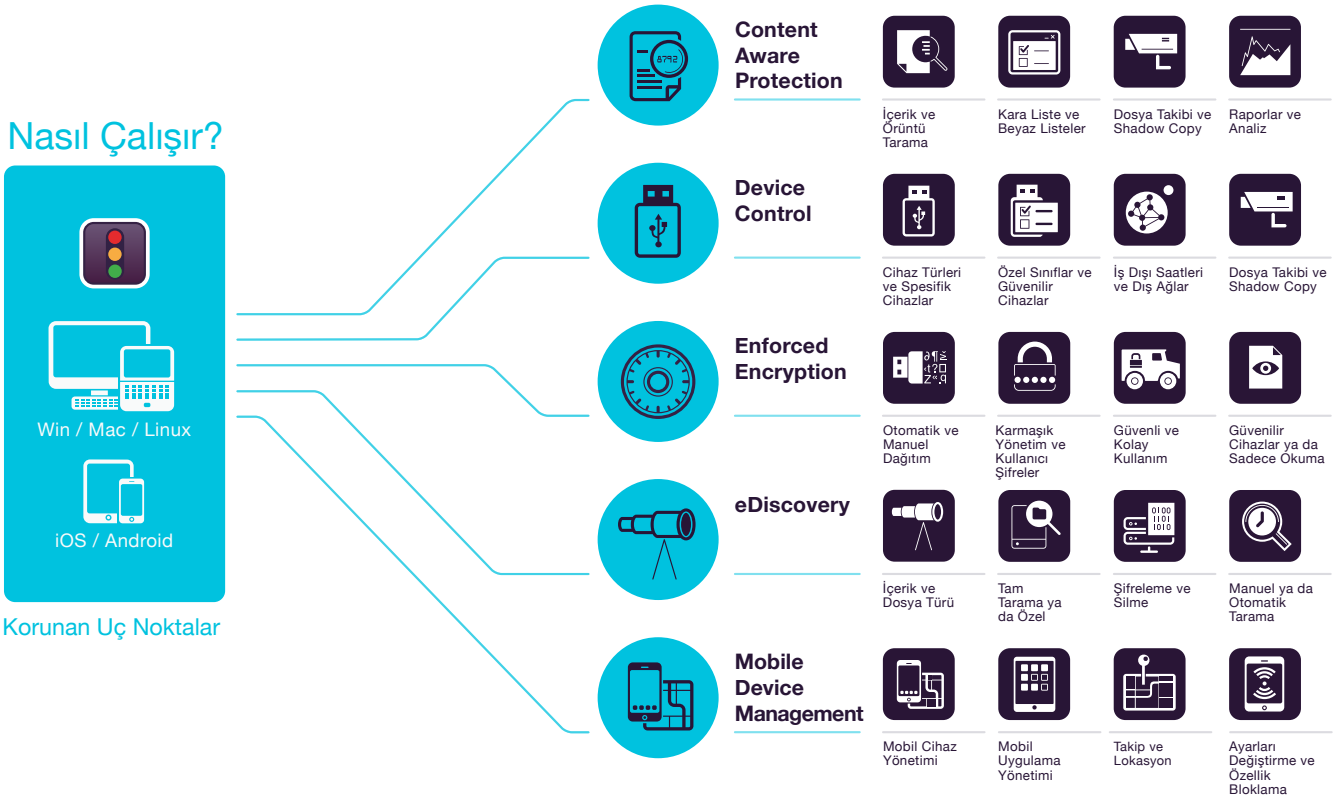
Hassas verilerinizi, taşınabilir depolama aygıtlarının, bulut hizmetlerinin ve mobil aygıtların oluşturduğu tehditlerden koruyun.

Taşınabilir cihazlar ile bulut teknolojilerinin çalışma ve yaşam biçimimizi değiştirdiği bu dönemde Endpoint Protector, üretkenliği koruyarak, işinizi daha rahat, güvenli ve eğlenceli hale getirirken, içeriden gelen tehditlere karşı verileri korumak için tasarlanmıştır. Blacklist ve Whitelist tabanlı yaklaşım, politika oluşturmada esneklik sağlar.

Endpoint Protector, ağ bünyesinde bulunan hassas verilerin denetimini, performanstan ödün vermeden gerçekleştirebilir. Bunu yaparken, belirli bilgisayarlara, kullanıcılara, gruplara, URL'lere, taşınabilir medyalara ve domain'lere aktarımlarına izin verirken, belirli bulut uygulamaları, çevrimiçi hizmetler ve kişisel taşınabilir cihazlar vasıtası ile izinsiz veri aktarımını engelleyebilirsiniz.

Endpoint Protector, donanım veya sanal cihaz olarak alınabilir ve dakikalar içinde kurulur. Dahası, kolay anlaşılır yönetim arayüzü, politikaların yönetilmesine ve masaüstü bilgisayardan tablete herhangi bir cihazdan raporların kontrol edilmesine izin verir. Endpoint Protector, verilerin sızma, çalınma veya benzeri bir şekilde tehlikeye girmesine yol açabilecek dahili tehditlerin neden olduğu riskleri önemli ölçüde azaltır. Bunlara ek olarak, çeşitli sektörel kural ve düzenlemelere (KVKK, GDPR, ISO27001 vb.) uyum sağlanmasına da yardımcı olmaktadır.

Nasıl Çalışır?



Content Aware Protection (İçerik Tanıyan Koruma) Windows, macOS ve Linux için	Hareket eden verileri izleyin ve denetleyin, hassas verilerin hangi çıkış noktalarından çıkabileceğine veya çıkamayacağına karar verin. Filtreler; Dosya Türü, Uygulama, Önceden Belirlenmiş ve Özelleştirilmiş İçerik, Regex ve daha fazlası için ayarlanabilir.
Device Control (Cihaz Kontrolü) Windows, macOS ve Linux için	USB'leri ve çevre bağlantı noktalarını izleyin ve denetleyin. Cihaz, Kullanıcı, Bilgisayar, Grup veya Global olarak hakları ayarlayın.
Enforced Encryption (Şifreleme Çözümü) Windows ve macOS için	AES 256bit şifreleme ile USB depolama aygıtlarında kopyalanan verileri otomatik olarak güvenceye alın. Çoklu platformda çalışır, şifre tabanlıdır, kullanımı kolay ve verimlidir.
eDiscovery (e-Keşif) Windows, macOS ve Linux için	Durağan verileri, ağın uç noktalarında tarayın ve onaysız bilgisayarlarda kimlik bilgilerinin bulunması durumunda şifreleme veya silme gibi düzeltici eylemleri uygulayın.
Mobile Device Management (Mobil Cihaz Yönetimi) Android, iOS ve macOS için	Akıllı telefon ve tabletlerdeki güvenlik seviyesini yönetin ve kontrol edin. Güvenlik ayarları, ağ ayarları, uygulamalar, telefon rehberi, kamera vb. kontrolü sizde olsun.

Content Aware Protection

Windows, macOS ve Linux için

Email: Outlook / Thunderbird / Lotus Notes vb. • Web Tarayıcılar: Internet Explorer / Firefox / Chrome / Safari • Anlık Mesajlaşma: Skype / Microsoft Communicator / Yahoo Messenger • Bulut Servisleri & Dosya Paylaşımı: Dropbox / iCloud / SkyDrive / BitTorrent / Kazaa • Diğer Uygulamalar: iTunes / Samsung Kies / Windows DVD Maker / Total Commander / Team Viewer • Ve Daha Birçoğu...

Çıkış Noktasna Göre BlackList
Filtreler, izlenen uygulamaların listesine göre ayarlanabilir. İçerik için USB depolama cihazları, ağ paylaşımları ve diğer çıkış noktaları izlenebilir.

Dosya Türüne Göre BlackList
Dosya Türü Filtreleri, kullanıcılar tarafından manüel olarak değiştirilse bile, uzantılarına bağlı olarak belirli dokümanları engellemek için kullanılabilir.

Ön Tanımlı İçerikler İçin BlackList
Filtreler, Kredi Kartı Numaraları, Sosyal Güvenlik Numaraları ve daha fazlası gibi önceden belirlenmiş içeriklere dayanarak oluşturulabilir.

Özel İçerikler İçin BlackList
Filtreler, anahtar kelimeler ve ifadeler gibi özel içeriğe dayalı olarak da oluşturulabilir. Çeşitli kara liste sözlükleri oluşturulabilir.

Dosya Adına Göre BlackList
Dosya isimlerine göre filtreler oluşturulabilir. Ad ve uzantı, sadece isim veya sadece uzantıya dayalı olarak da ayarlanabilirler.

Dosya Lokasyonuna Göre Black ve WhiteList
Yerel sabit disk üzerindeki dosyaların konumuna göre filtreler oluşrutabilir. Bu filtreler, alt klasörleri dahil etmek veya hariç tutmak için de tanımlanabilir.

RegEx'e Göre BlackList
Korumalı ağ üzerinden aktarılan verilerde belirli bir örüntüyü bulmak için gelişmiş özel filtreler oluşturulabilir.

İzinli Dosyalar İçin WhiteList
Tüm diğer transfer girişimleri engellenmiş olduğu durumlarda, gereksizlikleri önlemek ve verimliliği artırmak için beyaz liste oluşturulabilir.

Alanadı & URL'ler İçin WhiteList
Şirket politikalarını zorunlu kılın, ancak çalışanların işlerini yapmak için ihtiyaç duydukları esnekliğe izin verin. Şirket portalları veya e-posta adresleri için beyaz listeler oluşturun.

Print Screen ve Clipboard İzleme
Ekran görüntüsü alma özelliklerini iptal edin. Veri güvenliği politikasını geliştirerek, Kopyala ve Yapıştır / Kes ve Yapıştır aracılığıyla hassas içeriğin veri sızıntılarını ortadan kaldırın.

Optik Karakter Tanıma (OCR)
Taranan belgelerden ve diğer benzer içeriklerden gelen gizli bilgileri tespit ederek, fotoğraflarda ve görüntülerde içerik inceleyin.

Dosya Takibi ve Shadow Copy
Tüm dosya transferlerini veya çevrimiçi uygulama ve diğer çıkış noktalarına çıkmaya çalışma girişimlerini kaydedin. Dosyaların bir kopyasını kaydederek eylemlerin net bir görünümünü alın.

Filtreler için Eşikler
Kaç adet ihlale kadar dosyanın transferine izin verilebileceğini belirleyin. Her tür içerik veya tüm ihlallerin toplamı için geçerli ayarlamalar yapılabilir.

Transfer Limitleme
Belirli bir zaman aralığı için transfer limiti ayarlayın. Dosya sayısına veya dosya boyutuna bağlı olarak Limite ulaşıldığında e-posta uyarıları yapılabilir.

Bağlam Bazlı İçerik Tarama
Kişisel bilgiler gibi hassas içeriklerin daha doğru tespit edilmesi için gelişmiş bir inceleme mekanizmasını etkinleştirin. İçerik özelleştirme yapılması mümkündür.

Çevrimdışı Geçici Şifre (OTP)
Geçici süreli olarak ağ bağlantısı kesilmiş bilgisayarlara veri aktarım izni verebilirsiniz.

Göstergeler, Raporlar ve Analizler
Güçlü bir raporlama ve analiz aracı ile dosya transferleriyle ilgili aktiviteyi izleyin. Loglar ve raporlar SIEM çözümlerine de ihraç edilebilir.

Uyumluluk (GDPR, HIPAA, vb.)
KVKK, PCI DSS, GDPR, HIPAA vb. gibi endüstri kurallarına ve yönetmeliklere uyumlu olun. Para cezaları ve diğer sorunlardan kaçının.

Yazıcılar için DLP
Yerel ve ağ yazıcıları için gizli belgelerin yazdırılmasını engelleyen, veri kaybını ve veri hırsızlığını önleyen politikalar oluşturulabilir.

İnce İstemciler için DLP
Terminal Sunucularındaki verileri koruyun ve diğer ağ türlerinde olduğu gibi İnce İstemci ortamlarında da veri kaybını önleyin.

Device Control

Windows, macOS ve Linux için

USB Sürücüleri / Yazıcılar / Bluetooth Cihazları / MP3 Çalarlar / Taşınabilir HDD'ler / Teensy Board / Dijital Kameralar / Webcam'ler / Thunderbolt / PDA'lar / Ağ Paylaşımı / FireWire / iPhone / iPad / iPod / ZIP Sürücüleri / Serial Port / PCMCIA Veri Depolama Cihazları / Biometrik Cihazlar / ve Daha Birçoğu...

Granüler Hak Tanımlama
Cihaz Hakları, grup, bilgisayar, kullanıcı ve cihaz başına global olarak yapılandırılabilir. Varsayılan ayarları kullanın veya gerektiği gibi ayarlayın.

Cihaz Tipleri ve Spesifik Cihaz
Hakları belirleyin - reddet, izin ver, salt okunur, vs.- Cihaz Tipleri veya Spesifik Cihazlar için (VID, PID ve Seri numarası kullanarak).

Özelleştirilmiş Sınıflar
Haklar, aynı üreticinin ürünleri için yönetimi kolaylaştırmak amacıyla cihaz sınıflarına dayalı olarak oluşturulabilir.

İş Dışı Saatleri Politikaları
Cihaz Kontrol Politikaları normal çalışma saatleri dışında uygulanacak şekilde ayarlanabilir. İş saatleri başlangıç ve bitiş zamanı ve çalışma günleri ayarlanabilir.

Dış Ağ Politikaları
Cihaz Kontrol Politikaları, şirketin ağı dışındayken uygulanacak şekilde ayarlanabilir. Uygulaması, DNS Alan Adlarına ve IP Adreslerine dayanmaktadır.

Active Directory Aktarım & Senkronizasyon
Büyük dağıtımları daha basit yapmak için AD'den yararlanın. Ağ gruplarını, bilgisayarları ve kullanıcıları işletmenizi güncel tutun.

Kullanıcı ve Bilgisayar Bilgileri
Çalışan Kimlikleri, Ekipler, Lokasyon, doğru iletişim bilgileri ve daha fazlası (IP'ler, MAC Adresleri, vb.) gibi bilgilerle daha iyi bir görünürlük elde edin.

Dosya Takibi
Tüm dosya aktarımlarını veya çeşitli USB depolama cihazlarına taşıma girişimlerini kayıt altında bulundurarak kullanıcıların hareketlerini net bir şekilde görüntüleyebilirsiniz.

Shadow Copy
Daha sonra denetim amacıyla kullanılabillesi adına, kontrol edilen cihazlara aktarılan dosyaların bir kopyasını kaydedin.

Çevrimdışı Geçici Şifre
Geçici süreli olarak ağ bağlantısı kesilmiş bilgisayarlara veri aktarım izni verebilirsiniz.

E-Posta Alarmları Oluşturma
Cihaz kullanımıyla ilgili en önemli olaylar hakkında bilgi vermek için önceden tanımlanmış ve özelleştirilmiş e-posta uyarıları oluşturulabilir.

Gösterge ve Grafikler
En önemli olaylara ve istatistiklere hızlı bir görsel bakış için grafikler ve tablolar mevcuttur.

Raporlar ve Analiz
Güçlü bir raporlama ve analiz aracıyla cihaz kullanımıyla ilgili tüm etkinlikleri izleyin. Loglar ve raporlar da ihraç edilebilir.

Diğer Özellikler İçin Bizimle İletişime Geçin.
cososys@e-data.com.tr

Enforced Encryption

Windows ve macOS için

256bit AES Devlet Onaylı Şifreleme / Değiştirme önleyici teknikler / Uyuglama bütünlüğü / Kullanıcılara mesaj gönderme / Fabrika ayarlarına dönme / Şifre politika ayarları / Ve Daha Birçoğu...

USB Zorunlu Şifreleme
Yalnızca şifrelenmiş USB aygıtlarını yetkilendirin ve çıkarılabilir depolama aygıtlarında kopyalanan tüm verilerin otomatik olarak güvene alındığından emin olun.

Otomatik Kurulum ve Salt Okunur
Hem otomatik hem de manuel dağıtım mevcuttur. Şifreleme gerekene kadar Salt Okunur haklarına izin verme seçeneği de mümkündür.

Karmaşık Ana Şifre ve Kullanıcı Şifreleri
Gerektiğinde şifre karmaşıklığı ayarlanabilir. Ana Şifre, kullanıcıların parola sıfırlamaları gibi durumlarda süreklilik sağlar.

Ek Özellikler
Bulut Depolama, Lokal Klasörler, CD'ler & DVD'ler için şifreleme mevcuttur.
cososys@e-data.com.tr

eDiscovery

Windows, macOS ve Linux için

Dosya Tipleri: Grafik Dosyaları / Office Dosyaları / Arşiv Dosyaları / Programlama Dosyaları / Medya Dosyaları vb. • Ön Tanımlı İçerikler: Kredi Kartı / Kişisel Bilgiler / Adresler / Sosyal Sigorta No / TCKN / Pasaport / Telefon Numarası / Vergi Kimlik No / Sağlık Sigorta Numarası vb. • Özel İçerik / Dosya Adı / RegEx / HIPAA / vb.

Veri Şifreleme ve Şifre Çözme
Gizli bilgileri içeren durağan veriler, yetkisiz çalışanların erişimlerini önlemek için şifrelenebilir. Şifre çözme eylemleri de mevcuttur.

Veri Silme
İç politikanın açık ihlalleri ortaya çıkarsa, yetkisiz son noktalarda tespit edildiği anda hassas bilgileri silin.

BlackList ile Lokasyon Tarama
Önceden belirlenmiş lokasyonlara göre filtreler oluşturulabilir. Hedeflenen içerik denetimleri ile durağan veriler için gereksiz taramalardan kaçının.

Otomatik Taramalar
Tüm ve kademeli taramalara ek olarak, Otomatik Taramalar da planlanabilir - bir kere veya tekrarlı (haftalık veya aylık).

Dosya Takibi
Tüm çevrimiçi aktarımları kaydederek, çeşitli çevrimiçi uygulamalara ve bulut hizmetlerine iletim denemesinde, kullanıcıların eylemlerini net bir şekilde görmenizi sağlar.

Raporlar ve Analiz
Durağan verileri taramakla ilgili kayıtları izleyin ve gerektiğinde iyileştirme işlemlerini yapın. Loglar ve raporlar SIEM çözümlerine de ihraç edilebilir.

Filtreler için Eşik Değerleri
Kaç adet ihlale kadar dosyanın transferine izin verilebileceğini belirleyin. Her tür içerik veya tüm ihlallerin toplamı için geçerli ayarlamalar yapılabilir.

Uyumluluk (KVKK,GDPR, HIPAA, vb.)
KVKK, PCI DSS, GDPR, HIPAA vb. Gibi endüstri kurallarına ve yönetmeliklere uyumlu olun. Para cezaları ve diğer sorunlardan kaçının.

SIEM Entegrasyonu
Logları harici kaynaklarla paylaşarak SIEM ürünlerinden yararlanın. Güvenlik ürünleri genelinde sorunsuz bir deneyim sağlayabilirsiniz.

Dosya Türüne Göre BlackList
Dosya Türü Filtreleri, kullanıcılar tarafından manüel olarak değiştirilse bile, uzantılarına bağlı olarak belirli dokümanları engellemek için kullanılabilir.

Ön Tanımlı İçeriğe Göre BlackList
Filtreler, Kredi Kartı Numaraları, Sosyal Güvenlik Numaraları ve daha fazlası gibi önceden belirlenmiş içeriklere dayanarak oluşturulabilir.

Özel İçerikler İçin BlackList
Filtreler, anahtar kelimeler ve ifadeler gibi özel içeriğe dayalı olarak da oluşturulabilir. Çeşitli kara liste sözlükleri oluşturulabilir.

Dosya Adına Göre BlackList
Dosya isimlerine göre filtreler oluşturulabilir. Ad ve uzantı, sadece isim veya sadece uzantıya dayalı olarak da ayarlanabilirler.

Dosya Lokasyonuna Göre Black ve WhiteList
Yerel sabit disk üzerindeki dosyaların konumuna göre filtreler oluşrutabilir. Bu filtreler, alt klasörleri dahil etmek veya hariç tutmak için de tanımlanabilir.

RegEx'e Göre BlackList
Korumalı ağ üzerinden aktarılan verilerde belirli bir örüntüyü bulmak için gelişmiş özel filtreler oluşturulabilir.

İzinli Dosyalar İçin WhiteList
Tüm diğer transfer girişimleri engellenmiş olduğu durumlarda, gereksizlikleri önlemek ve verimliliği artırmak için beyaz liste oluşturulabilir.

Alanadı & URL'ler İçin WhiteList
Şirket politikalarını zorunlu kılın, ancak çalışanların işlerini yapmak için ihtiyaç duydukları esnekliğe izin verin. Şirket portalları veya e-posta adresleri için beyaz listeler oluşturun

MIME Tipine Göre WhiteList
Belirli MIME Tipleri için içerik denetimini hariç tutarak, global düzeyde gereksiz taramadan kaçının.

Diğer Özellikler İçin Bizimle İletişime Geçin / cososys@e-data.com.tr

Mobile Device Management

Android, iOS and macOS için

iOS & Android için OTA Kayıt
Cihazlar SMS, E-posta, URL bağlantısı veya QR Kodu ile uzaktan kaydedilebilir. Ağınız için en uygun yolu seçin.

Toplu Kayıt
Etkin bir dağıtım süreci için, aynı anda 500'e kadar akıllı telefon ve tablet kaydedilebilir.

Uzaktan Kilitleme
İlgili herhangi bir olay durumunda mobil cihazların anında kilitlenmesini uzaktan sağlayın. Kaybolan veya unutulan cihazlar nedeniyle veri sızıntılarından kaçının.

Takip ve Yer Gösterme
Şirketin mobil cihazlarını yakından takip edin ve şirketinizin hassas verilerinin yerini her zaman bilin.

Yerleşik Özellikleri Devre Dışı Bırakın
Kamera gibi yerleşik özellikler için izinleri kontrol edin, veri ihlallerinden kaçının ve hassas verilerin kaybolmasını önleyin.

Kayıp Cihazları Bulmak İçin Sesli Uyarı
Bulunana kadar yüksek bir zil sesini uzaktan etkinleştirerek, kaybolan mobil cihazı bulabilme (yalnızca Android için desteklenmektedir).

Mobil Uyuglama Yönetimi
Uygulamaları kuruluşun güvenlik politikalarına göre yönetin. Kayıtlı mobil cihazlara ücretsiz ve ücretli uygulamaları anında aktarın.

Ağ Ayarlarını Yükleme
E-posta, Wi-Fi ve VPN ayarları gibi ağ ayarlarını yapın veya Bluetooth, zil sesi modu vb. dahil olmak üzere, devre dışı bırakın.

Alarmlar
Genişletilmiş Sistem Uyarıları yanı sıra Özel Sistem Uyarıları oluşturma seçeneği de mevcuttur.

Raporlar ve Analiz
Güçlü bir raporlama ve analiz aracıyla cihaz kullanımıyla ilgili tüm kullanıcıların etkinliklerini izleyin. Loglar ve raporlar ihraç edilebilir.

Samsung Knox ile Kiosk Modu
Mobil cihazı belirli uygulamalara kilitleyin veya dahil edin. Mobil aygıtta güvenliği uzaktan zorlama ile cihazları işe özel aygıtlara dönüştürür.

macOS Yönetimi
DLP özelliklerini genişletmek için, Mac'ler ek yönetim seçeneklerinden yararlanarak MDM modülüne de kaydedilebilir.

Şifre Uygulaması
Güçlü parola ilkelerini uygulayarak mobil cihazlarda depolanan şirket kritik verilerin proaktif korumasını sağlar.

Uzaktan Silme
Veri sızıntılarını önlemenin tek yolunun aygıtı silmek olan kritik durumlarda, bu işlem uzaktan kolayca yapılabilir.

Coğrafik Koruma
Coğrafi bir alanda bir sanal çevre tanımlayın ve sadece belirli bir alanda geçerli olan MDM politikalarının daha iyi kontrolünü elde edin.

iOS Kısıtlamaları
Yalnızca işle ilgili kullanımın mümkün olduğundan emin olun. Şirket politikasına uymuyorsa, iCloud, Safari, App Store vb.'yi devre dışı bırakın.

Android'de vCard İletimi
Android mobil cihazlar için kişileri ekleyin ve iletin, mobil çalışanlarınızın hızlı bir şekilde doğru kişilerle iletişim kurmasını sağlayın.

Uygulama İzleme
Çalışanlarınızın mobil cihazlarında hangi uygulamaları indirdiklerini izleyerek, iş ve eğlence arasındaki ince çizgiyi koruyun.

Varlık Yönetimi
Cihazın Adlarını, Türlerini, Modellerini, Kapasitesini, İşletim Sistemlerini, Hat Sağlayıcılarını, IMEI'leri, MAC'leri vb. hakkında mobil cihaz hakkında bilgi edinin.

E-Posta Alarmları Oluşturma
Mobil cihazların kullanımıyla ilgili en önemli olaylar hakkında bilgi sağlamak için e-posta uyarıları ayarlanabilir.

Gösterge ve Grafikler
En önemli olaylar ve istatistikler hakkında hızlı bir görsel bakış için grafikler ve çizelgeler mevcuttur.

Diğer Özellikler İçin Bizimle İletişime Geçin.

cososys@e-data.com.tr

%100 Kurulum Esnekliği

Her tür ağ için uygun olan ürünlerimiz kurumsal müşteriler, küçük ve orta ölçekli işletmeler ve hatta ev kullanıcıları tarafından kullanılabilir. Bir istemci-sunucu mimarisi ile, web tabanlı arayüzden dağıtımı ve merkezi olarak yönetilmesi kolaydır. Donanım ve Sanal Cihazlar, Amazon Web Servisleri Sunucusu ve Bulut versiyonunun yanı sıra, temel özellikleri arayanlar için tek başına çalışan bir versiyonu da mevcuttur.

Endpoint Protector

Content Aware Protection, eDiscovery, Device Control ve Enforced Encryption, Windows, macOS ve Linux versiyonları ve sürümleri üzerinde çalışabilir. Mobil Cihaz Yönetimi ve Mobil Uygulama Yönetimi de iOS ve Android mobil cihazlarda çalışır.

My Endpoint Protector

Content Aware Protection, eDiscovery, Device Control ve Enforced Encryprion, Windows ve Mac versiyonları ve sürümleri üzerinde çalışabilir. Mobil Cihaz Yönetimi ve Mobil Uygulama Yönetimi de iOS ve Android mobil cihazlarda çalışır.

Donanım Çözümü

Sanal Çözüm

Amazon Sunucusu

Bulut Çözümü

Modüller

			Korunan Uç Noktalar				
Windows	Windows 7 / 8 / 10	(32/64 bit)	●	●	●	●	
	Windows Server 2003 - 2016	(32/64 bit)	●	●	●	●	
	Windows XP / Windows Vista	(32/64 bit)	●	●	●	●	
macOS	macOS 10.13	High Sierra	●	●	●	●	
	macOS 10.12	Sierra	●	●	●	●	
	macOS 10.11	El Capitan	●	●	●	●	
	macOS 10.10	Yosemite	●	●	●	●	
	macOS 10.9	Mavericks	●	●	●	●	
	macOS 10.8	Mountain Lion	●	●	●	●	
	macOS 10.7	Lion	●	●	●	●	
Linux	Ubuntu		●	●	●	n/a	
	OpenSUSE / SUSE		●	●	●	n/a	
	CentOS / RedHat		●	●	●	n/a	
	Fedora		●	●	●	n/a	
iOS	iOS 4, iOS 5, iOS 6, iOS 7, iOS 8, iOS 9, iOS 10, iOS 11						●
Android	Jelly Bean (4.1+), KitKat (4.4+), Lollipop (5.0+), Marshmallow (6.0+), Nougat (7.0+), Oreo (8.0+)						●

*Desteklenen sürümler ve dağıtımlarla ilgili ayrıntıları kontrol edin endpointprotector.com/linux

COSOSYS

Genel Müdürlük (Romanya)

E-mail sales@cososys.com
Sales +40 264 593 110 / ext. 103
Support +40 264 593 113 / ext. 202

Almanya

vertrieb@endpointprotector.de
+49 7541 978 26730
+49 7541 978 26733

Kore

E-mail contact@cososys.co.kr
Sales +82 70 4633 0353
Support +82 20 4633 0354

Kuzey Amerika

sales.us@endpointprotector.com
+1 888 271 9349
+1 877 377 6475

e-data TEKNOLOJİ

Ankara

cososys@e-data.com.tr
+90 312 472 36 56

İstanbul

cososys@e-data.com.tr
+90 216 576 48 48