ENDPOINT PROTECTOR | by CoSoSys

DATASHEET 4.4.0.9

Prevenirea Pierderilor de Date & Managementul Dispozitivelor Mobile

Pentru rețele de orice mărime și orice industrie

DLP pentru Windows, Mac și Linux

Protecția întregii rețele

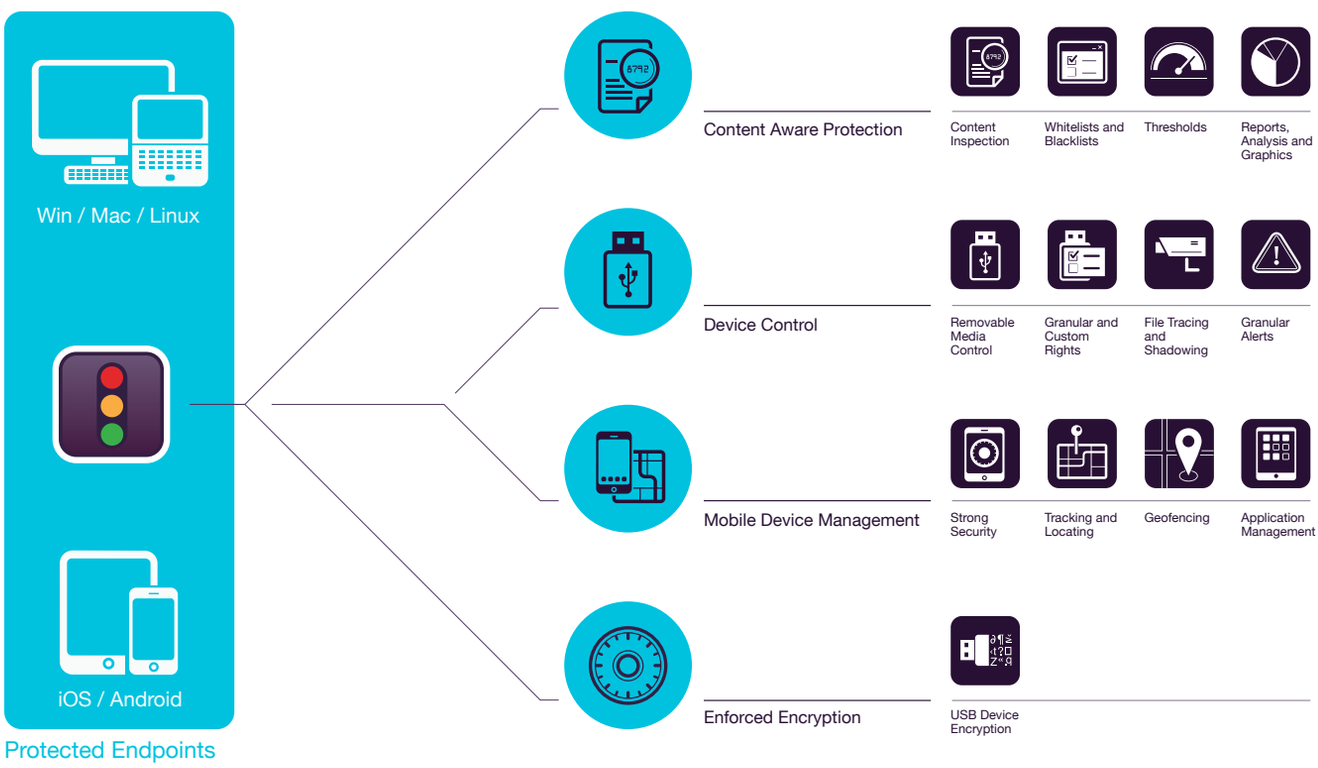
ENDPOINT PROTECTOR

by CoSoSys

Soluție la cheie pentru protejarea datelor împotriva amenințărilor reprezentate de dispozitivele portabile, mobile și serviciile cloud.

Într-o lume în care dispozitivele portabile transformă modul în care lucrăm și trăim, Endpoint Protector 4 este proiectat pentru a menține productivitatea și a face munca mai convenabilă, sigură și plăcută. Abordarea bazată pe “liste albe” permite utilizarea anumitor dizpozitive, upload-ul de fișiere către URL-uri și nume de domenii pentru calculatoare/utilizatori/grupuri specifice, ajutând la creșterea productivității și asigurând în același timp controlul dispozitivelor și a datelor. Endpoint Protector 4 este oferit ca Hardware sau Virtual Appliance, putând fi configurat în câteva minute. Acesta reduce dramatic riscurile reprezentate de amenințările interne care ar putea duce la scurgeri, furturi, sau pierderi de date.

Cum funcționează



Protecția Conținutului
pentru Windows, Mac OS X și Linux

Monitorizează și controlează fișierele care pot sau nu părăsi rețeaua prin diverse puncte de ieșire. Filtrele pot fi setate in funcție de Tipul Fișierului, Aplicație, Conținut Predefinit și Personalizat, Regex, etc.

Controlul Dispozitivelor
pentru Windows, Mac OS X și Linux

Monitorizează și controlează USB-urile și porturile periferice. Configurează Drepturi per Dispozitiv, Utilizator, Calculator, Grup sau la nivel Global.

Managementul Dispozitivelor Mobile
pentru Android, iOS și Mac OS X

Administrează, Controlează și Ajustează nivelul de securitate pentru smartphone-uri și tablete. Poți face push la setările de securitate, setările de rețea și aplicații.

Criptare Forțată
pentru Windows și Mac OS X

Securizează în mod automat datele copiate pe dispozitivele de stocare USB prin criptare AES 256 biți. Soluția este cross-platform, pe bază de parolă, ușor de folosit și foarte eficientă.

Protecția Conținutului

pentru Windows, Mac OS X și Linux

Clienți de e-mail: Outlook / Thunderbird / Lotus Notes • Browsere Web: Internet Explorer / Firefox / Chrome / Safari • Mesagerie Instantanee: Skype / Microsoft Communicator / Yahoo Messenger • Cloud Services & File Sharing: Dropbox / iCloud / SkyDrive / BitTorrent / Kazaa • Alte aplicații: iTunes / Samsung Kies / Windows DVD Maker / Total Commander / Team Viewer • ALTELE

Filtre în funcție de Conținut Predefinit
Filtrele pot fi create pe baza unui conținut predefinit care poate include: Numere de Card de Credit, Numere de Securitate Socială și altele.

Filtre în funcție de Conținut Personalizat
Filtrele pot fi, de asemenea, create pe baza unui conținut personalizat, precum cuvinte cheie și expresii. Totodată pot fi create diferite Liste Negre pe bază de Dicționare.

Filtre în funcție de Expresii Regulate
Sunt disponibile filtre personalizate avansate pentru a găsi o anumită recurență în datele transferate în întreaga rețea protejată.

Filtre în funcție de Tipul Fișierului
Filtrele în funcție de Tipul Fișierului pot fi folosite pentru a bloca documente specifice în funcție de tipul extensiei, chiar dacă acestea sunt modificate manual de către utilizatori.

Liste Albe de Fișiere
În timp ce toate celelalte încercări de transferuri de fișiere sunt blocate, pot fi create liste albe pentru a evita redundanța și pentru a crește productivitatea.

Liste Albe bazate pe Domeniu & URL
Poți impune politica companiei în timp ce asiguri flexibilitatea de care au nevoie angajații pentru a-și îndeplini sarcinile. Adaugă într-o listă albă (de excepții) portalurile companiei sau adrese de e-mail.

Dezactivare Print Screen
Dezactivează opțiunea print screen și asigură-te că datele valoroase afișate pe ecran nu vor părăsi rețeaua protejată.

Monitorizare Clipboard
Elimină scurgerile de date confidențiale prin Copy & Paste / Cut & Paste pentru consolidarea politicii de securitate a datelor.

Rapoarte și Analize
Monitorizează activitățile legate de transferurile de fișiere printr-un instrument puternic de raportare și analiză. Log-urile și rapoartele pot fi exportate către soluții SIEM.

Panou Principal și Grafice
Pentru o imagine de ansamblu a celor mai importante evenimente și statistici, sunt disponibile grafice și diagrame.

Active Directory
Profită de AD sau de instrumente similare pentru a face implementarea la scară largă mai simplă. Importă și sincronizează toate grupurile și entitățile.

Prag Global și Normal pentru Filtre
Definește limita de încălcări până la care este permis transferul de fișiere. Acesta se aplică la fiecare tip de conținut sau la suma totală de încălcări.

Monitorizare Trafic Fișiere
Înregistrează toate transferurile de fișiere sau incercările de transfer către diverse aplicații online și servicii cloud pentru o imagine clară asupra acțiunilor utilizatorului.

Duplicare Fișiere
Salvează o copie a fișierelor ce au fost transferate pe dispozitive controlate sau via e-mail, cloud sau alte aplicații.

Parolă Temporară Offline
Autorizează temporar transferurile de fișiere pe calculatoarele deconectate de la rețea. Asigură securitate și productivitate.

Crearea de Alerte prin E-mail
Se pot configura alerte de e-mail predefinite și personalizate pentru ca Administratorul să primească informații despre cele mai importante evenimente legate de transferuri de fișiere confidențiale.

DLP pentru Imprimante
Creează politici pentru imprimante locale și de rețea pentru a bloca printarea documentelor confidențiale și pentru a preveni pierderea și furtul de date.

Politici HIPAA de Protecție Conținut
Acestea permit scanarea în profunzime a documentelor înainte de transfer pentru informații PHI (Protected Health Information), medicamente aprobate de FDA, coduri ICD-9, etc.

DLP pentru Thin Clients
Protejează datele pe Terminal Servers și previne pierderea de date în rețelele cu Thin Clients, la fel ca și în orice altă rețea.

Caracteristici Adiționale
Alte caracteristici sunt de asemenea disponibile.
info@endpointprotector.com

Controlul Dispozitivelor

pentru Windows, Mac OS X și Linux

Unități USB / Imprimante / Dispozitive Bluetooth / Playere MP3 / HDD-uri Externe / Placă Teensy / Camere Digitale / Camere Web / Thunderbolt / PDAs / Network Share / FireWire / iPhones / iPads / iPods /Unități ZIP / Port Serial / Dispozitive de Stocare PCMCIA / Dispozitive Biometrice / ALTELE

Setarea Drepturilor La Nivel Global

În mod implicit, drepturile de dispozitiv se aplică la nivel global în toată rețeaua. Cu toate acestea, modulul este extrem de granular.

Setarea Drepturilor per Grup

Drepturile pentru dispozitive pot fi configurate în mod granular în funcție de grupuri, permițând diferite drepturi de acces pentru diferite departamente.

Setarea Drepturilor per Computer

Drepturile dispozitivelor pot fi configurate per computer. Este util atunci când computerele au un rol unic în organizație.

Setarea Drepturilor per Utilizator

Fiecare utilizator poate primi diferite drepturi de acces pentru dispozitiv în conformitate cu politicile companiei, pe baza rolurilor și sarcinilor acestora.

Setarea Drepturilor per Dispozitiv

Granularitatea drepturilor poate fi stabilită până la nivelul dispozitivului, pe baza ID-ului furnizorului, ID-ului produsului și numărului de serie.

Clase Personalizate

Drepturile pot fi create pe baza claselor de dispozitive, determinând un management mai ușor pentru produsele de la același vendor.

Trusted Device

Pentru dispozitivele criptate, pot fi configurate diferite drepturi de acces în funcție de nivelul de criptare (software, hardware, etc).

Monitorizare Trafic Fișiere

Înregistrează toate transferurile sau incercările de transfer de fișiere pe diverse dispozitive USB pentru o imagine clară asupra acțiunilor utilizatorului.

Duplicare Fișiere

Salvează o copie a fișierelor ce au fost transferate pe dispozitive controlate, ce pot fi folosite mai târziu pentru audit.

Parolă Temporară Offline

Autorizează temporar accesul dispozitivelor la calculatoarele deconectate de la rețea. Asigură securitate și productivitate.

Crearea de Alerte prin E-mail

Se pot configura alerte de e-mail predefinite și personalizate pentru ca Administratorul să primească informații despre cele mai importante evenimente legate de dispozitivele aflate în funcțiune.

Panou Principal și Grafice

Pentru o imagine de ansamblu a celor mai importante evenimente și statististici, sunt disponibile grafice și diagrame.

Rapoarte si Analize

Monitorizează activitățile legate de utilizarea dispozitivelor printr-un instrument puternic de raportare și analiză. Log-urile și rapoartele pot fi, de asemenea, exportate.

Caracteristici Adiționale

Alte caracteristici sunt de asemenea disponibile.
info@endpointprotector.com

Criptare Forțată

pentru Windows și Mac OS X

Criptare Forțată pentru USB

Autorizează doar dispozitive USB criptate și asigură-te că toate datele copiate pe dispozitivele de stocare sunt securizate automat.

Mecanisme Puternice de Securitate

Criptare AES 256 biți aprobată de guvern, protecție cu parolă și tehnici împotriva manipulării pentru a asigura integritatea aplicației.

Parolă Master

Crearea unei parole master va oferi continuitate în diverse circumstanțe, precum resetarea parolei utilizatorului.

Caracteristici Adiționale

Criptarea este de asemenea disponibilă pentru Stocarea în Cloud, Directoare Locale, CD-uri & DVD-uri
info@endpointprotector.com

Managementul Dispozitivelor Mobile

pentru Android, iOS și Mac OS X

Înregistrare over-the-air pentru iOS & Android

Dispozitivele pot fi înregistrate la distanță via SMS, E-mail, URL-uri sau Coduri QR. Alege modul cel mai convenabil pentru rețeaua ta.

Înregistrare Bulk

Pentru un proces eficient de implementare, pot fi înregistrate în același timp până la 500 de smartphone-uri și tablete.

Blocare de la Distanță

Activează blocarea instantanee de la distanță a dispozitivului mobil în cazul unor incidente de securitate. Evită scurgerile de date cauzate de dispozitive pierdute sau furate.

Urmărire și Localizare

Monitorizează îndeaproape dispozitivele mobile ale companiei pentru a ști în orice moment unde sunt datele confidențiale ale companiei.

Dezactivarea funcționalităților încorporate

Controlează permisiunea pentru caracteristici încorporate, cum ar fi camera foto, evitând breșele de date și a pierderii de date confidențiale.

Redare Sunet pentru Localizarea Dispozitivelor Pierdute

Localizează dispozitivele mobile pierdute prin activarea de la distanță a unui ringtone puternic până când sunt găsite (doar pentru Android).

Mobile Application Management

Gestionează aplicațiile în concordanță cu politicile de securitate ale organizației. Poți face push instantaneu al aplicațiilor gratuite și plătite către dispozitivele mobile înregistrate.

Push la Setările de Rețea

Configurează și fă push la setările de rețea precum E-mail, Wi-Fi și VPN sau dezactivează Bluetooth-ul, setează tipul de sonerie, etc.

Alerte

Sunt disponibile Alerte de Sistem Predefinite, precum și opțiunea de a configura Alerte de Sistem Personalizate.

Rapoarte și Analize

Monitorizează activitățile angajaților legate de utilizarea dispozitivelor printr-un instrument puternic de raportare și analiză. Log-urile și rapoartele pot fi, de asemenea, exportate.

Modul Kiosk cu Samsung Knox

Blochează dispozitivul mobil, permițând doar folosirea unei aplicații specifice. Impune de la distanță politici de securitate și transformă dispozitivele mobile în dispozitive specializate.

Managementul Mac OS X

Pentru a extinde caracteristicile DLP, Mac-urile pot fi, de asemenea, înscrise în modulul MDM, profitând de opțiuni de gestionare suplimentare.

Securitate pe bază de Parolă

Protecție proactivă a datelor critice ale companiei stocate pe dispozitive mobile prin forțarea unor politici puternice de parolă.

Ștergere de la Distanță

Pentru situații critice în care singura modalitate de a evita scurgerile de date este ștergerea dispozitivului. Acest lucru poate fi ușor de făcut de la distanță.

Geofencing

Definește un perimetru virtual pe o zonă geografică pentru a obține o mai bună gestionare a politicilor MDM care se aplică numai într-o anumită zonă.

Restricții iOS

Asigură-te că numai utilizarea legată de afaceri este posibilă. În cazul în care nu se respectă politica companiei, dezactivează iCloud, Safari, App Store, etc.

Push vCards pe Android

Adăugă și fă push de contacte pentru dispozitivele mobile Android, asigurându-te că angajații mobili ajung rapid în contact cu oamenii potriviți.

Monitorizarea de Aplicații

Află ce aplicații descarcă angajații de pe dispozitivele mobile, păstrând o linie discretă între muncă și timpul liber.

Asset Management

Obține o perspectivă asupra flotei de dispozitive mobile cu privire la Nume Dispozitiv, Tipuri, Modele, Capacitate, Versiune OS, Operatori, IMEIs, MACS, etc.

Creare de Alerte de E-mail

Configurează alerte de e-mail pentru a primi informații despre cele mai importante evenimente legate de utilizarea dispozitivelor mobile.

Panou Principal și Grafice

Pentru o imagine de ansamblu a celor mai importante evenimente și statistici, sunt disponibile grafice și diagrame.

Caracteristici Adiționale

Alte caracteristici sunt de asemenea disponibile.
info@endpointprotector.com

100% Flexibilitate de Implementare

Potrivite pentru orice tip de rețea, produsele noastre pot fi utilizate de către clienții enterprise, întreprinderi mici și mijlocii și chiar de către utilizatorii individuali. Cu o arhitectură client-server, acestea sunt ușor de implementat și de administrat în mod centralizat din interfața web. In afară de Hardware și Virtual Appliance, sunt, de asemenea, disponibile Instanțe de Amazon Web Services, versiunea Cloud și o versiune stand-alone pentru cei care caută caracteristici de bază.

Endpoint Protector

Protecția Conținutului, Controlul Dispozitivelor și Criptarea sunt disponibile pentru computerele care rulează pe diferite versiuni și distribuții de Windows, Mac și Linux. Mobile Device Management și Mobile Application Management sunt, de asemenea, disponibile pentru dispozitive mobile iOS și Android.

My Endpoint Protector

Protecția Conținutului, Controlul Dispozitivelor și Criptarea sunt disponibile pentru computerele care rulează pe Windows și Mac. Mobile Device Management și Mobile Application Management sunt, de asemenea, disponibile pentru dispozitive mobile iOS și Android.

Hardware Appliance

Virtual Appliance

Amazon Instance

Cloud Solution

Modules

		Endpoint-uri Protejate					
Windows	Windows XP / Windows Vista	(32/64 bit)	●	●	●		
	Windows 7 / 8 / 10	(32/64 bit)	●	●	●		
	Windows Server 2000 - 2016	(32/64 bit)	●	●	●		
Mac OS X	Mac OS X 10.6	Snow Leopard	●	●	●		
	Mac OS X 10.7	Lion	●	●	●		
	Mac OS X 10.8	Mountain Lion	●	●	●		
	Mac OS X 10.9	Mavericks	●	●	●		
	Mac OS X 10.10	Yosemite	●	●	●		
	Mac OS X 10.11	El Capitan	●	●	●		
Linux	Ubuntu		●	●	n/a		
	OpenSUSE		●	●	n/a		
	CentOS / RedHat		●	●	n/a		
iOS	iOS 4, iOS 5, iOS 6, iOS 7, iOS 8, iOS 9						●
Android	Jelly Bean (4.1+), KitKat (4.4+), Lollipop (5.0+)						●

*Vă rugăm să verificați detalii privind versiunile și distribuțiile acceptate pe endpointprotector.com/linux

COSOSYS

România

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

Germania

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

Coreea

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

America de Nord

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

Official Partner