



Mobile Device Management (MDM) pentru iOS and Android

Mobile Device Management este un modul al Familiei de Produse Endpoint Protector. Acesta acoperă în mod specific nevoile de securitate apărute în urma utilizării sporite a dispozitivelor mobile în întreprinderi și organizații.

Endpoint Protector este o soluție completă, care facilitează ca administratorii IT să implementeze și să gestioneze o soluție de prevenire a pierderii de date în rețeaua lor, acoperind calculatoare (Windows, Mac OS X, Linux) și dispozitive mobile (iOS și Android). Totul într-un mod eficient și economic.

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.

Endpoint Protector 4 este oferit ca hardware sau mașină virtuală, putând fi configurat în câteva minute. Acesta reduce dramatic riscurile prezentate de amenințările interne care ar putea duce la scurgeri, deteriorări sau compromiterea datelor.



Avantaje Cheie

- Protecție pentru iOS și Android
- Mobile Application Management
- Interfață web-based
- Pregătit pentru VMware
- Appliance-ul Hardware sau Virtual poate fi instalat în câteva minute.
- Management intuitiv al dispozitivelor mobile
- Protecție proactivă împotriva abuzului dispozitivelor și furt de date
- Creșterea productivității prin gestionarea setărilor de rețea

Securizare Dispozitive Mobile

Politici de securitate puternice aplicate pe smartphone-uri și tablete de companie vor asigura o protecție proactivă a datelor de afaceri critice, indiferent de unde și de pe ce dispozitiv mobil sunt accesate.

Suporta Dispozitive Mobile iOS și Android

Controlul și gestionarea celor mai populare platforme mobile pentru a proteja datele companiei dumneavoastră.

Fortărețe Parolă

Impunerea schimbării periodice a parolei, fie direct, over-the-air sau cu implicarea utilizatorului.

Urmărire și Localizare

Monitorizarea flotei de dispozitive mobile a companiei, știind tot timpul unde sunt datele sensibile ale companiei. Pentru iOS aplicația EPP MDM trebuie să fie instalat pe dispozitiv.

Ștergere sau blocare de la distanță - Protecție furt

Evitați ca datele confidențiale să ajungă pe mâini greșite prin blocarea sau ștergerea datelor de la distanță, în cazul pierderii sau furtului dispozitivului mobil.

Restricții pentru iOS

Asigurați-vă ca dispozitivele sunt utilizare doar în interes de afaceri. Funcționalități precum iCloud, FaceTime, Safari, App Store, In-App Purchases, iTunes, Siri, Camera se pot dezactiva.

Localizare prin Sunet al Dispozitivelor Pierdute (Android)

Detectare ușoară a dispozitivelor mobile rătăcite prin activarea over-the-air a unei melodii, suficient pentru a localiza smartphone-ul / tableta dvs.

Gestionați Setări E-Mail și Wi-Fi de pe dispozitive iOS

Gestionați de la distanță Setări E-Mail, VPN și Wi-Fi.

Ștergere Setări E-Mail și Wi-Fi de pe dispozitive iOS

Șterge de la distanță a conținutului și setărilor de e-mail și Wi-Fi. E-mail-urile companiei pot fi șterse în timp ce conturile personale rămân neatinsse.

Mobile Application Management

Monitorizarea și gestionarea aplicațiilor, prevenind malware-ul sau a aplicațiilor neautorizate de la compromiterea datelor critice ale companiei. Creșteți productivitatea prin împingerea simultană a aplicațiilor spre mai multe dispozitive.

Support pentru modelul Bring Your Own Device (BYOD)

Control complet asupra datelor sensibile ale companiei, indiferent dacă sunt stocate pe dispozitivele aflate în proprietate privată sau a companiei. Focus pe eficiența angajaților fără a compromite date de afaceri critice sau restricționarea utilizării personale.

Servicii bazate pe locație / Geofencing

Definirea unui perimetru virtual pe o zonă geografică, folosind un serviciu bazat pe locație. Acesta oferă o mai bună gestionare a politicilor MDM care se aplică numai într-o anumită zonă.

Pentru a se proteja, companiile trebuie să definească în mod clar și să aplice politicile de management al dispozitivelor mobile!

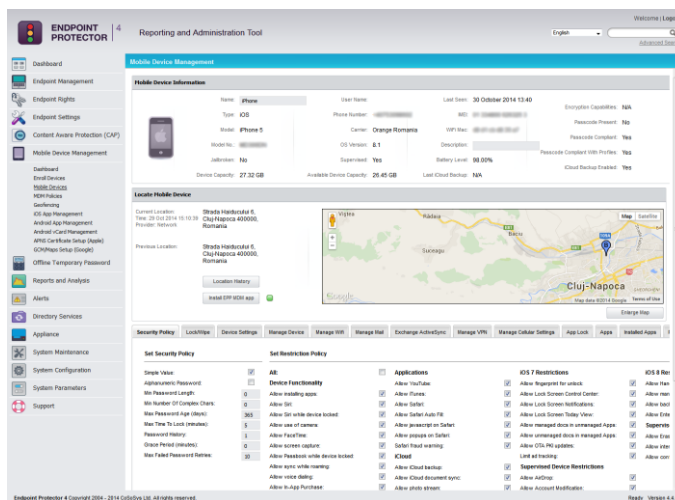


Principalele Beneficii

- Impune politici de utilizare ale dispozitivelor mobile
- Protejarea datelor companiei
- Controlul imediat asupra utilizării dispozitivelor mobile
- Implementare de la distanță
- Impact și efort minim pentru utilizatori și administratori
- Conformitate / Productivitate
- Soluții de securitate BYOD

Management Web Centralizat / Dashboard

Gestionează la nivel centralizat utilizarea dispozitivelor mobile prin intermediul interfeței administrative și de raportare web. Vine în întâmpinarea nevoilor de management și a personalului de securitate IT și oferă informații în timp real despre activitate dispozitivelor controlate la nivel de organizație.



Inventarierea și Managementul Dispozitivelor Mobile

Permite inventarierea și controlul ușor al flotei de dispozitive mobile aparținând companiei sau angajaților, oferind rapoarte detaliate pentru audit ulterior.

Criptarea Dispozitivelor

iPhone-urile și iPad-urile vin cu criptare hardware 256bit AES încorporate. Aceasta este mereu activă, aplicându-se la setarea parolei pentru dispozitiv.

Înregistrare Personală și La Distanță (Over-the-Air)

Folosind un cod unic de înregistrare va asigura o implementare ușoară și securizată a platformei MDM în orice fel de infrastructură IT existentă în companie.

Asset Management pentru Dispozitive Mobile

Modalitate ușoară de a păstra o imagine de ansamblu asupra dispozitivelor mobile deținute de companie sau personale (BYOD).

Dispozitive Mobile Suportate

- iPad, iPhone, iOS 4.0, iOS 5.0, iOS 6.0, iOS 7.0, iOS 8
- Android 2.2+
- unele funcționalități sunt disponibile numai pentru versiunile mai noi ale sistemelor de operare

Cerințe pentru MDM

- Pentru iOS MDM, un cont gratuit Apple Push Notification Service (APNS) este necesar (creat cu un Apple ID).
- Pentru iOS Android, un cont gratuit Google Cloud Messaging pentru Android (GCM) este necesar (creat cu un Cont Google).

Dezvoltare și Comparație Funcționalități iOS și Android

Lista noastră de Funcționalități pentru iOS și Android se extinde în paralel și continuă să crească, acoperind mereu noile cerințe și tehnologiile emergente de securitate.

Funcționalități MDM	iOS	Android
Inregistrare	✓	✓
Inolare prin E-mail, URL, QR-Code sau SMS (US, UK, Germania, 100+ alte țări suportate)	✓	✓
Politici de Securitate Puternice	✓	✓
Parametri Parolă (lungime, încercări, numeric, etc.)	✓	✓
Timp blocare ecran	✓	✓
Forțare Parolă	✓	✓
Forțare Criptare Dispozitiv (Criptare încorporată în Dispozitiv/ Sistem Operare)	✓	✓
Urmărire și Localizare necesită app	da	nu
Localizare Dispozitive Pierdute (redă sunet)		✓
Blocare de la distanță	✓	✓
Ștergere de la distanță (Remote Nuke)	✓	✓
Ștergere Dispozitiv	✓	✓
Ștergere conținut E-mail/Setări compania	✓	
Ștergere Card SD		✓
Mobile Application Management	✓	✓
Geofencing	✓	✓
Mobile Device Asset Management	✓	✓
Trimitere Setări de Rețea	✓	✓
E-mail, VPN, WiFi	✓	
Blocare WiFi, Bluetooth		✓
Limitarea utilizării Camerei	✓	✓
Control la distanță Over-the-Air	✓	✓
Limitarea utilizării de la		
iTunes, iCloud, App Store, In-App Purchases, Siri, FaceTime, Enforce encrypted iTunes backup, Safari etc.	✓ ✓ ✓ ✓ ✓ ✓ ✓	
Multe alte funcții disponibile	...	...
Versiuni Suportate	Apple iOS 4, 5, 6, 7, 8	Android 2.2+

Anumite caracteristici de securitate dispozitiv și gestionare nu sunt accesibile pe sisteme de operare / dispozitive mai vechi.

Controlul Dispozitivelor Portabile (pentru calculatoare) Device Control

Endpoint Protector oferă caracteristici suplimentare pentru prevenirea pierderii datelor, controlând dispozitivele de stocare portabile și porturile pentru calculatoare Windows, Mac OS X și Linux.

Protecție în funcție de Conținut (pentru calculatoare) Content Aware Protection

Protecție în funcție de Conținut pentru calculatoare Windows și Mac OS X oferă un control detaliat asupra datelor sensibile care părăsesc rețeaua companiei. Prin inspecția eficientă a conținutului, transferurile documentelor importante ale companiei sunt înregistrate, raportate și blocate. Această funcție va preveni scurgerea de date prin toate punctele de ieșire posibile, de la dispozitive USB la aplicații, inclusiv Microsoft Outlook, Skype, Nvigateare Web sau Dropbox.

Endpoint Protector Hardware Appliance

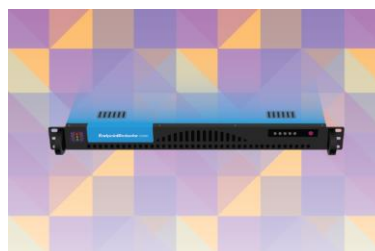
Endpoint Protector Hardware Appliance este disponibil în diverse capacități pentru a răspunde nevoilor afacerii dvs. Toate Appliance-urile Hardware se bazează pe hardware de ultimă generație, eficiente energetic.



Endpoint Protector Virtual Appliance

Endpoint Protector Virtual Appliance poate fi folosit de companii de toate dimensiunile. Appliance-ul Virtual este disponibil în diverse formate, compatibil cu cele mai populare platforme de virtualizare.

Folosind Virtual Appliance puteți proteja rețeaua în doar câteva minute împotriva utilizării neautorizate a dispozitivelor și împotriva pierderii de date.



Medii Virtuale Suportate	Versiuni	.ovf	.vmx	.vhd	.xva	.pvm
VMware Workstation	7.1.4	-	*	-	-	-
VMware Workstation *	9.0.2	*	*	-	-	-
VMware Player *	6.0.0	*	*	-	-	-
VMware Fusion *	5.0.0	-	*	-	-	-
VMware vSphere (ESXi)	5.1.0	*	-	-	-	-
Oracle VirtualBox	4.2.18	*	-	-	-	-
Parallels Desktop for Mac	9.0.2	-	-	-	-	*
Microsoft Hyper-V Server	2008/2012	-	-	*	-	-
Citrix XenServer 64bit	6.2.0	-	-	-	*	-

Pentru mediile virtuale marcate cu *, vă rugăm să contactați departamentul de Suport.

Vizitați www.EndpointProtector.com pentru a testa gratuit.

CoSoSys Germany

sales.de@cososys.com

Phone: +49-7541-978-2627-0

Fax: +49-7541-978-2627-9

CoSoSys North America

sales.us@cososys.com

+1-888-576-6177

CoSoSys HQ

sales@cososys.com

+40-264-593110

+40-264-593113

Contactați partenerul dvs. local pentru mai multe informații:



© Copyright 2004-2014 CoSoSys Ltd. All rights reserved. Lock it Easy, Surf it Easy, Carry it Easy, Carry it Easy +Plus, Carry it Easy +Plus Bio, Secure it Easy, TrustedDevices, TrustedLogin, Endpoint Protector Basic, My Endpoint Protector and Endpoint Protector are trademarks of CoSoSys Ltd. Other brand names mentioned herein are for identification purposes only and may be trademarks of their respective holder(s).

Created on 29-Oct-2014



Soluția pentru Prevenirea Pierderilor de Date (DLP), Controlul Dispozitivelor și Managementul Dispozitivelor Mobile (MDM) iOS și Android pentru companii

Soluție la cheie pentru securizarea datelor împotriva amenințărilor reprezentate de dispozitivele portabile, mobile și servicii 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" de permisiune a utilizării de dispozitive, URL-uri și nume de domenii pentru calculatoare/utilizatori/ grupuri, crește productivitatea, menținând în același timp controlul dispozitivelor și a datelor. Endpoint Protector 4 este oferit ca hardware sau mașină virtuală, putând fi configurat în câteva minute. Acesta reduce dramatic riscurile reprezentate de amenințările interne care ar putea duce la scurgeri, deteriorări sau compromiterea datelor.



Avantaje Cheie

- Appliance-ul Hardware sau Virtual poate fi instalat în câteva minute
- Soluție 3 în 1, Controlul Dispozitivelor, DLP și MDM
- Management intuitiv de politici pentru endpoint-uri
- Interfață Web
- Protecție pentru Windows, Mac, Linux, iOS și Android
- Protecție pro-activă împotriva abuzului de dispozitive și furtului de date
- Pregătit pentru VMware

Securitatea Porturilor pentru Windows și Mac OS X Desktop-uri, Notebook-uri și Netbook-uri

Oferă protecție împotriva amenințărilor generate de dispozitivele portabile mobile. Oprește scurgerile, furtul sau pierderea de date cât și infectarea cu viruși.

Controlați următoarele (dar și alte) dispozitive și aplicații

- **Dispozitive**
 - Unități USB (normal, U3)
 - Carduri de Memorie (SD, etc.)
 - CD/DVD-Burner (int., ext.)
 - HDD-uri Externe (incl. SATA)
 - Imprimante
 - Unități Floppy
 - Citoitoare de Carduri (int., ext.)
 - Camere Web
 - Carduri de Rețea WiFi
 - Camere Digitale
 - iPhones / iPads / iPods
 - Smartphones/BlackBerry/PDAs
 - Dispozitive FireWire
 - MP3 Player/Media Players
 - Dispozitive Biometrice
 - Dispozitive Bluetooth
 - Dispozitive ZIP
 - ExpressCards (SSD)
 - USB Wireless
 - Port Serial
 - Plăci Teensy
 - PCMCIA Storage Devices
 - Thunderbolt
 - Network Share
- **Clienți E-Mail**
 - Outlook
 - Lotus Notes
 - Thunderbird, etc.
- **Navigatoare Web**
 - Internet Explorer
 - Firefox
 - Chrome
 - Safari, etc.
- **Mesagerie Instantanee**
 - Skype, ICQ, AIM
 - Microsoft Communicator
 - Yahoo Messenger, etc.
- **Servicii Cloud /File Sharing**
 - Dropbox, iCloud, SkyDrive
 - BitTorrent, Kazaa, etc.
- **Alte Aplicații**
 - iTunes
 - Samsung Kies
 - Windows DVD Maker
 - Total Commander
 - FileZilla
 - Team Viewer
 - EasyLock, și multe altele

Mobile Device Management (MDM) OS X, iOS și Android

- Forțare Parolă și Politici de Securitate
- Urmărire, Localizare, Blocare sau Ștergere Dispozitive
- Trimite Setările de Rețea: E-Mail, VPN, WiFi
- Mobile Application Management
- Geofencing și Politicilor Bazăte pe Localizare
- Soluții BYOD, informații detaliate în Data Sheet-ul de MDM

Administrare centralizată Web / Dashboard

Administrează centralizat utilizarea dispozitivelor portabile. Interfața Web de Administrare și Raportare răspunde nevoilor conducerii și personalului de securitate IT și oferă informații în timp real despre dispozitivele controlate și despre activitățile de transfer de date la nivelul întregii organizații.

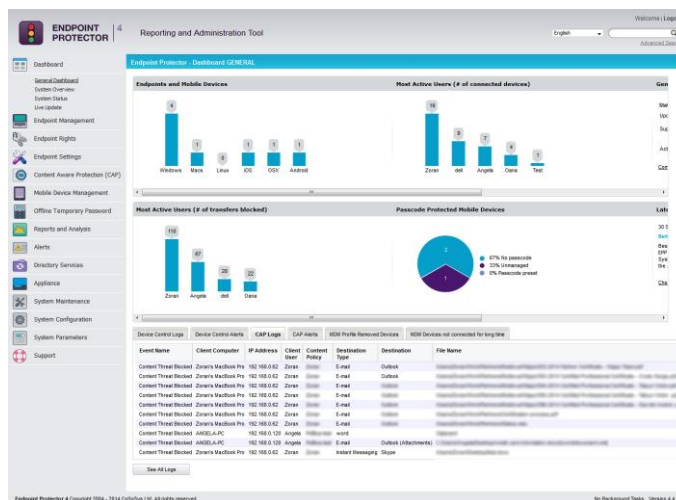
Principalele Beneficii

- Endpoint Protector implică un TCO cu 50% mai mic decât media pieței
- Se instalează într-un timp cu 70% mai scurt decât alte soluții
- Costă cu 45% mai puțin decât alte soluții similare



"Am ales Endpoint Protector Appliance pentru costul său, simplitatea de administrare și controlul detaliat. Soluția este ușor de instalat, eficientă, puternică și ușor de administrat. Îmi plac foarte mult funcționalitățile de raportare, shadowing și parola offline temporară (realmente foarte practică)."

Marc Rossi
Infrastructure Director
NASS and WIND SAS France



Administrarea Dispozitivelor / Controlul Dispozitivelor

Definirea drepturilor pe dispozitive, utilizatori, calculatoare, grupuri sau la nivel global în rețea

Content Aware Protection / Filtrarea Conținutului

Scanarea documentelor pentru detectarea conținutului confidențial, înregistrarea și raportarea incidentelor de conținut. Blocarea datelor care părăsesc punctele de ieșire, de la dispozitive portabile la aplicații și servicii online.

Filtrare după Tip Fișierului / Conținut / Expresii Regulate

File Tracing înregistrează toate datele care au fost copiate pe/de pe dispozitivele autorizate anterior sau aplicații on-line. File Shadowing salvează o copie a tuturor fișierelor, chiar și cele șterse, care au fost folosite în legătură cu dispozitivele controlate.

File Tracing / File Shadowing

File Tracing înregistrează toate datele care au fost copiate pe/de pe dispozitivele autorizate anterior sau aplicații on-line. File Shadowing salvează o copie a tuturor fișierelor, chiar și cele șterse, care au fost folosite în legătură cu dispozitive sau aplicațiile controlate.

Whitelisting Fișiere / Dispozitive / URL-uri / Domenii

Numai fișierele autorizate pot fi transferate către dispozitivele și aplicații on-line autorizate. Toate celelalte transferuri sunt blocate și raportate.

Reportare și Analiză / Panouri de Comandă & Grafice / Audit

Sunt salvate rapoarte privind activitatea clienților a dispozitivelor conectate și transferuri de fișiere, oferind un istoric complet pentru audit și analiză detaliată. Rapoarte puternice, grafice și instrumente de analiză pentru a revizui cu ușurință activitatea.

Implementare a Politicilor de Securitate (Active Directory)

Prin integrarea cu Active Directory, se pot importa grupuri, calculatoare și utilizatorii. Funcția AD Sync va sincroniza noile entități.

Parolă Offline Temporară / Rețea în mod "Offline"

Calculatoarele securizate care sunt deconectate de la rețea rămân protejate. Pentru a menține productivitatea în deplasare, dispozitivele și transferurile de fișiere pot fi autorizate temporar prin funcționalitatea Parolă Offline Temporară.

Managementul Departamentelor

Departamentele pot fi gestionate și separate prin politici dedicate.

Modul de Auto-apărare a Clientului Endpoint Protector

Oferă protecție chiar și pentru calculatoarele unde utilizatorii au drepturi de administrator.

Protecția datelor în tranzit / EasyLock - Criptare Impusă

În combinație cu software-ul nostru EasyLock se forțează criptarea datelor copiate pe dispozitiv. Cu tehnologia noastră TrustedDevice se aplică o securitate adițională prin folosirea dispozitivelor portabile criptate certificate pentru stocarea datelor. Astfel, în cazul pierderii sau furtului dispozitivului, datele stocate pe el sunt criptate și în siguranță, fără a fi accesibile pentru alții.

Securitate pentru:

Clienți Protejați

- Windows 8 (32/64bit)
- Windows 7 (32/64bit)
- Windows Vista (32/64bit)
- Windows XP (SP2) (32/64bit)
- Windows 2003/2008 (32/64bit)
- Mac OS X 10.5+
- Ubuntu 14.04
- Ubuntu 10.04
- openSUSE 11.4



Managementul Dispozitivelor Mobile (MDM) Dispozitive Suportate

- iPad, iPhone, iOS 4, iOS 5, iOS 6, iOS 7, iOS 8
- Android 2.2+,
- Android 4+ necesar pentru unele funcționalități

Directory Service (opțional)

- Active Directory

Certificări:



Endpoint Protector Hardware Appliance

Endpoint Protector Hardware Appliance este disponibil în diverse capacități pentru a răspunde nevoilor afacerii dvs. Toate Appliance-urile Hardware se bazează pe hardware-ul cel mai nou și mai eficient energetic.



Modele (+ altele)	Protecție Terminale	Capacitate Adițională	Montare (Rack mount)	Procesor	Hard Drive	Alimentare
A20	20	4	Stand- alone	ULV Single Core	320GB	60W
A50	50	10	10	ULV Dual Core	320GB	200W
A100	100	20	1U	ULV Dual Core	320GB	200W
A250	250	50	10	Pentium 2 Core	500GB	260W
A500	500	100	10	Pentium 2 Core	1TB	260W
A1000	1000	200	10	Intel Xeon 4 Core	2x TB (Raid 1)	260W
A2000	2000	400	20	2x Intel Xeon 4 Core	4x 1TB (Raid 5)	2x720W
A4000	4000	800	30	2x Quad Core	6x 1TB (Raid 5)	2x800W

Garanție Hardware 1 an inclus. Garanție suplimentară și opțiuni de înlocuire disponibile.

Endpoint Protector Virtual Appliance

Endpoint Protector Virtual Appliance poate fi folosit de companii de toate dimensiunile. Appliance-ul Virtual este disponibil în diverse formate, compatibil cu cele mai populare platforme de virtualizare.



Folosind Virtual Appliance puteți proteja rețeaua în doar câteva minute împotriva utilizării neautorizate a dispozitivelor și împotriva pierderii de date.



Medii Virtuale Suportate	Versiuni	.ovf	.vmx	.vhd	.vxa	.pvm
VMware Workstation	7.1.4	-	*	-	-	-
VMware Workstation *	9.0.2	*	*	-	-	-
VMware Player *	6.0.0	*	*	-	-	-
VMware Fusion *	5.0.0	-	*	-	-	-
VMware vSphere (ESXi)	5.1.0	*	-	-	-	-
Oracle VirtualBox	4.2.18	*	-	-	-	-
Parallels Desktop for Mac	9.0.2	-	-	-	-	*
Microsoft Hyper-V Server	2008/2012	-	-	*	-	-
Citrix XenServer 64bit	6.2.0	-	-	-	*	-

Pentru mediile virtuale marcate cu *, vă rugăm să contactați departamentul de Suport.

Endpoint Protector vă oferă un mediu sigur și securizat de lucru cu dispozitive portabile de stocare, calculatoare și dispozitive mobile. Eficiența utilizatorilor nu este limitată întrucât orice dispozitiv autorizat poate fi folosit continuu pe calculatoarele protejate, în timp ce doar transferul de fișiere ce încalcă politicile de securitate a rețelei sunt blocate.

CoSoSys

Germany

E-Mail:

sales.de@cososys.com

Phone: +49-7541-978-2627-0

Fax: +49-7541-978-2627-9

CoSoSys

North America

sales.us@cososys.com

+1-888-576-6177

CoSoSys Ltd.

HQ

sales@cososys.com

+40-264-593110

+40-264-593113

Vizitați www.EndpointProtector.com pentru a testa gratuit.

Contactați partenerul dvs. local pentru mai multe informații:



© Copyright 2004-2014 CoSoSys Ltd. All rights reserved. Lock it Easy, Surf it Easy, Carry it Easy, Carry it Easy +Plus, Carry it Easy +Plus Bio, Secure it Easy, TrustedDevices, TrustedLogin, Endpoint Protector Basic, My Endpoint Protector and Endpoint Protector are trademarks of CoSoSys Ltd. Other brand names mentioned herein are for identification purposes only and may be trademarks of their respective holder(s).

Created on 29-Oct-2014



Content Aware Protection pentru Windows și Mac OS X O parte importantă a strategiei tale DLP la nivel de endpoint

Soluție la cheie pentru securizarea datelor împotriva scurgerilor și furtului de date prin e-mailuri, mesagerii, social media, aplicații on-line, servicii de cloud, dispozitive portabile și alte puncte de ieșire.

Content Aware Protection este un modul din Endpoint Protector DLP (Prevenirea Pierderii de Date) care acoperă nevoile de securitate generate de numeroasele puncte de ieșire ale datelor sensibile din companii.

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" de permitere a utilizării de dispozitive, URL-uri și nume de domenii pentru calculatoare/utilizatori/grupuri, crește productivitatea menținând în același timp controlul dispozitivelor și a datelor. Endpoint Protector 4 este oferit ca hardware sau mașină virtuală, putând fi configurat în câteva minute. Acesta reduce dramatic riscurile reprezentate de amenințările interne care ar putea duce la scurgeri, deteriorări sau compromiterea datelor.



Avantaje Cheie

- Appliance-ul Hardware sau Virtual poate fi instalat în câteva minute
- Interfață Web
- Management intuitiv de politici pentru endpoint-uri
- Protecție pentru Windows, Mac, Linux, iOS și Android
- Protecție pro-activă împotriva abuzului de dispozitive și furtului de date
- Pregătit pentru VMware

Content-Aware Data Loss Prevention

Protecție împotriva amenințărilor reprezentate de transferurile de date către dispozitive mobile și portabile, aplicații și servicii on-line. Oprește furtul, pierderea și scurgerea intenționată sau accidentală de date.

Support pentru calculatoare Windows și Mac OS

Monitorizarea și blocarea fluxului de date pe cele mai populare și mai puternice platforme pentru a proteja datele companiei dvs.

Controlați următoarele (dar și alte) dispozitive și aplicații

- **Dispozitive**
 - Unități USB (normal, U3)
 - Carduri de Memorie (SD, etc.)
 - CD/DVD-Burner (int., ext.)
 - HDD-uri Externe (incl. SATA)
 - Imprimante
 - Unități Floppy
 - Cititoare de Carduri (int., ext.)
 - Camere Web
 - Carduri de Rețea WiFi
 - Camere Digitale
 - iPhones / iPads / iPods
 - Smartphones/BlackBerry/PDAs
 - Dispozitive FireWire
 - MP3 Player/Media Players
 - Dispozitive Biometrice
 - Dispozitive Bluetooth
 - Dispozitive ZIP
 - ExpressCards (SSD)
 - USB Wireless
 - Port Serial
 - Plăci Teensy
 - PCMCIA Storage Devices
 - Thunderbolt
 - Network Share
- **Clienți E-Mail**
 - Outlook
 - Lotus Notes
 - Thunderbird, etc.
- **Navigatoare Web**
 - Internet Explorer
 - Firefox
 - Chrome
 - Safari, etc.
- **Mesagerie Instantanee**
 - Skype, ICQ, AIM
 - Microsoft Communicator
 - Yahoo Messenger, etc.
- **Servicii Cloud /File Sharing**
 - Dropbox, iCloud, SkyDrive
 - BitTorrent, Kazaa, etc.
- **Alte Aplicații**
 - iTunes
 - Samsung Kies
 - Windows DVD Maker
 - Total Commander
 - FileZilla
 - Team Viewer
 - EasyLock, și multe altele

Administrare centralizată Web / Dashboard

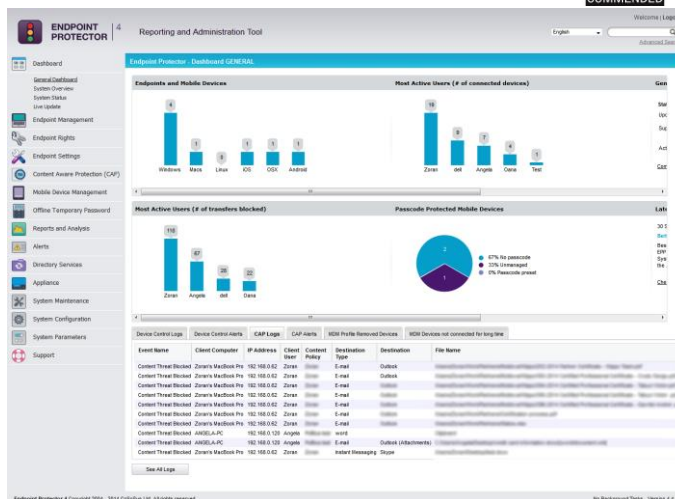
Administrează centralizat utilizarea dispozitivelor portabile. Interfața Web de Administrare și Raportare răspunde nevoilor conducerii și personalului de securitate IT și oferă informații în timp real despre dispozitivele controlate și despre activitățile de transfer de date la nivelul întregii organizații.

Parolă Offline Temporală / Rețea în mod "Offline"

Calculatoarele securizate care sunt deconectate de la rețea rămân protejate. Pentru a menține productivitatea în deplasare, dispozitivele și transferurile de fișiere pot fi autorizate temporar prin funcționalitatea Parolă Offline Temporală.

Principalele Beneficii

- Oprește pierderea de date
- Endpoint Protector implică un TCO cu 50% mai mic decât media pieței
- Se instalează într-un timp cu 70% mai scurt decât alte soluții
- Costă cu 45% mai puțin decât alte soluții similare



Crearea politicilor de securitate pentru entități specifice

Politicile Content Aware oferă un control flexibil de scanare a documentelor, permițând monitorizare selectivă în funcție de utilizatori, computere, grupuri sau departamente.

Filtru în funcție de Conținut Predefinit sau Cuvinte Cheie

Filtrează datele care părăsesc calculatoarele protejate pe baza conținutului predefinit, care include:

- Detaliile Cardului de Credit (principalele carduri sunt suportate)
- Numere de Securitate Socială (diferite formate sunt suportate)
- Informații despre Conturi Bancare; etc.

Filtru în funcție de Dicționare / Conținut Personalizat și Expresii Regulate

Filtre personalizate pot fi create, astfel modulul de Content Aware Protection caută cuvintele cheie și oprește fișierele care le conțin de a ajunge la punctele de ieșire. Dicționare multiple pot fi create, cât și politici avansate bazate pe RegEx.

Filtru în funcție de Tipul Fișierului

Endpoint Protector blochează documentele care părăsesc compania în funcție de adevăratul lor tip de fișier. Suportă cele mai importante tipuri de fișiere, aplicații precum MS Office și fișiere grafice, arhive, executabile, media și multe alte fișiere.

Prag pentru Filtre

Pragul definește limita de încălcări până de la care este permis transferul de fișiere. Acesta se aplică la fiecare tip de conținut confidențial și nu se referă la suma totală de încălcări.

Monitorizare Clipboard pentru prevenirea Copy & Paste a datelor sensibile

Monitorizarea Clipboard va opri utilizatorii de la copierea și lipirea informațiilor sensibile ale companiei din documente către clienți Outlook, aplicații e-mail sau alte canale prin care se scurg informații.

Dezactivare Print Screen

Dezactivarea opțiunii print screen în politica va împiedica utilizatorii de la a scoate din companie informațiile afișate pe ecran, ca imagini. Acest lucru întărește și mai mult politica dumneavoastră DLP.

Prevenirea trimiterii datelor sensibile ca atașament de e-mail

Blocarea sau doar monitorizarea utilizatorilor care încearcă trimiterea de fișiere confidențiale prin atașamente e-mail. Content Aware Protection suportă cei mai utilizați clienți de e-mail: Outlook, Thunderbird, Lotus Notes dar și Webmail.

Prevenirea trimiterii datelor sensibile prin Outlook și Thunderbird

Ca atașament sau chiar dacă datele confidențiale sunt conținute în corpul de text a unui e-mail, acesta este împiedicat să fie trimis și incidentul este raportat. Chiar dacă firma dvs. utilizează PGP pentru criptarea e-mail-urilor, conținutul este inspectat înainte de criptare și trimiteri.

Filtrarea datelor la ieșirea prin browsere Web

Firefox, Google Chrome și multe alte browsere sunt folosite pe calculatoare și este o cale simplă pentru pierderea de date, deoarece utilizatorii pot încărca orice fișier la care au acces. Încărcările pe site-uri precum sendspace.com sau folosirea interfeței web a Dropbox-ului, sunt principalele surse de furt de date. Prin urmare, monitorizarea tuturor fișier accesate de browsere web înainte să ajungă pe internet este vitală. Prevenirea pierderilor de date la nivel de gateway este inefficientă în aceste cazuri.

Filtrarea datelor transferate prin diferite Aplicații, înainte să părăsească calculatorul protejat

Endpoint Protector protejează utilizarea datelor confidențiale în raport cu multe aplicații, cum ar fi: Skype, Yahoo Messenger, Dropbox, Outlook, etc.

Modul de Auto-apărare a Clientului Endpoint Protector

Ofereă protecție chiar și pentru calculatoarele unde utilizatorii au drepturi administrative.

Clienți Protejați

- Windows 8 (32/64bit)
- Windows 7 (32/64bit)
- Windows Vista (32/64bit)
- Windows XP (SP2) (32/64bit)
- Windows 2003/2008 (32/64bit)
- Mac OS X 10.5+



Directory Service (opțional)

- Active Directory

Endpoint Protector Device Control module (necesar)

Endpoint Protector Hardware Appliance

Endpoint Protector Hardware Appliance este disponibil în diverse capacități pentru a răspunde nevoilor afacerii dvs. Toate Appliance-urile Hardware se bazează pe hardware-ul cel mai nou și mai eficient energetic.



Modele (+ altele)	Protecție Terminale	Capacitate Adțională	Montare (Rack mount)	Procesor	Hard Drive	Alimentare
A20	20	4	Stand- alone	ULV Single Core	320GB	60W
A50	50	10	10	ULV Dual Core	320GB	200W
A100	100	20	1U	ULV Dual Core	320GB	200W
A250	250	50	10	Pentium 2 Core	500GB	260W
A500	500	100	10	Pentium 2 Core	1TB	260W
A1000	1000	200	10	Intel Xeon 4 Core	2x TB Raid 1	260W
A2000	2000	400	20	2x Intel Xeon 4 Core	4x 1TB Raid 5	2x720W
A4000	4000	800	30	2x Quad Core	6x 1TB Raid 5	2x800W

Garanție Hardware 1 an inclus. Garanție suplimentară și opțiuni de înlocuire disponibile.

Controlul Dispozitivelor pentru calculatoare (desktop-uri, laptop-uri, etc.), este o altă funcționalitate disponibilă pentru Data Loss Prevention – Prevenirea Pierderii de Date

Endpoint Protector oferă funcționalități pentru controlul dispozitivelor portabile și a porturilor pe calculatoare Windows, Mac OS X și Linux. Cu Device Control, administratorii IT primesc rapoarte și log-uri, indicând calea fișierului, putând să salveze o copie a acestora prin File Tracing și File Shadowing.

Mobile Device Management (MDM) pentru iOS și Android smartphone-uri și tablete



Politicele de securitate pot fi aplicate pe dispozitive mobile iOS și Android. Funcționalități precum Tracking & Locating, Remote Nuke and Lock, Mobile Application Management cât și Trimiterea Setărilor de Rețea, sunt disponibile și cresc productivitatea.

Endpoint Protector Virtual Appliance

Endpoint Protector Virtual Appliance poate fi folosit de companii de toate dimensiunile. Appliance-ul Virtual este disponibil în diverse formate, compatibil cu cele mai populare platforme de virtualizare.



Folosind Virtual Appliance puteți proteja rețeaua în doar câteva minute împotriva utilizării neautorizate a dispozitivelor și împotriva pierderii de date.



Medii Virtuale Suportate	Versiuni	.ovf	.vmx	.vhd	.xva	.pvm
VMware Workstation	7.1.4	-	*	-	-	-
VMware Workstation *	9.0.2	*	*	-	-	-
VMware Player *	6.0.0	*	*	-	-	-
VMware Fusion *	5.0.0	-	*	-	-	-
VMware vSphere (ESXi)	5.1.0	*	-	-	-	-
Oracle VirtualBox	4.2.18	*	-	-	-	-
Parallels Desktop for Mac	9.0.2	-	-	-	-	*
Microsoft Hyper-V Server	2008/2012	-	-	*	-	-
Citrix XenServer 64bit	6.2.0	-	-	-	*	-

Pentru mediile virtuale marcate cu *, vă rugăm să contactați departamentul de Suport.

Vizitați www.EndpointProtector.com pentru a testa gratuit.

CoSoSys
Germany
E-Mail:
sales.de@cososys.com
Phone: +49-7541-978-2627-0
Fax: +49-7541-978-2627-9

CoSoSys
North America
sales.us@cososys.com
+1-888-576-6177

CoSoSys Ltd.
HQ
sales@cososys.com
+40-264-593110
+40-264-593113

Contactați partenerul dvs. local pentru mai multe informații:



© Copyright 2004-2014 CoSoSys Ltd. All rights reserved. Lock it Easy, Surf it Easy, Carry it Easy, Carry it Easy +Plus, Carry it Easy +Plus Bio, Secure it Easy, TrustedDevices, TrustedLogin, Endpoint Protector Basic, My Endpoint Protector and Endpoint Protector are trademarks of CoSoSys Ltd. Other brand names mentioned herein are for identification purposes only and may be trademarks of their respective holder(s).

Created on 29-Oct-2014