ENDPOINT PROTECTOR 4

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

Soluţie la cheie pentru securizarea datelor împotriva scurgerilor şi furtului de date prin e-mailuri, mesagerii, social media, aplicatii on-line, servicii de cloud, dispozitive portabile şi alte puncte de ieşire.

Content Aware Protection este un modul din Endpoint Protector DLP (Prevenirea Pierderilor de Date) care acoperă nevoile de securitate generate de numeroasele punctele de ieşire al datele sensibile din companii.

Într-o lume în care dispozitivele portabile transformă modul în care lucrăm şi trăim, Endpoint Protector 4 este proiectat pentru a menţine productivitatea şi a face munca mai convenabilă, sigură si placută. Abordarea bazată pe "liste albe" de permiterea a utilizării de dispozitive, URL-uri şi nume de domenii pentru calculatoare/utilizatori/ grupuri, creşte productivitatea menţinând în acelaşi timp controlul dispozitivelor şi a datelor. Endpoint Protector 4 este oferit ca hardware sau maşină virtuală, putând fi configurat în câteva minute. Acesta reduce dramatic riscurile reprezentate de ameninţările interne care ar putea duce la scurgeri, deteriorări sau compromiterea datelor.

Avantaje Cheie

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

Content-Aware Data Loss Prevention
Protecţie împotriva ameninţărilor reprezentate de transferurile de date către dispozitive mobile şi portabile, aplicaţii şi servicii on-line. Opreşte furtul, pierderea şi scurgerea intenţionată sau accidentală de date.

Suport pentru calculatoare Windows şi Mac OS
Monitorizarea şi blocarea fluxului de date pe cele mai populare şi mai puternice platforme pentru a proteja datele companiei dvs.

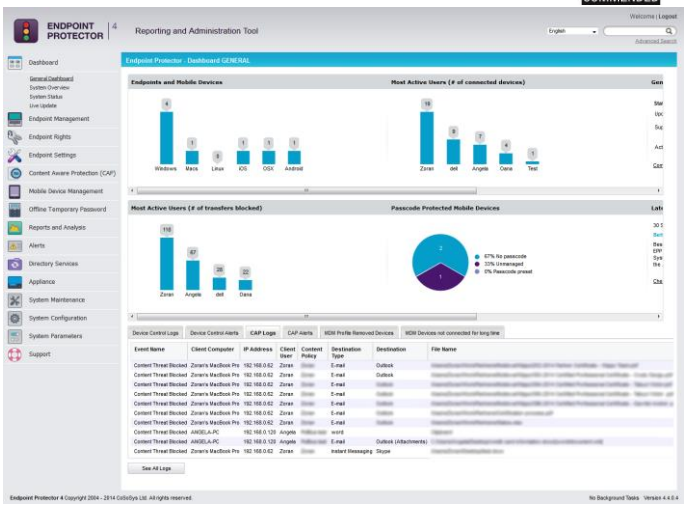
Controlaţi următoarele (dar şi alte) dispozitive şi aplicaţii

- **Dispozitive**
- Unităţi USB (normal, U3)
- Carduri de Memorie (SD, etc.)
- CD/DVD-Burner (int., ext.)
- HDD-uri Externe (incl. sATA)
- Imprimante
- Unităţi Floppy
- Cititoare de Carduri (int., ext.)
- Camere Web
- Carduri de Reţea 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
- **Clienţi 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 Aplicaţii**
  - iTunes
  - Samsung Kies
  - Windows DVD Maker
  - Total Commander
  - FileZilla
  - Team Viewer
  - EasyLock, şi multe altele

Administrare centralizată Web / Dashboard
Administrează centralizat utilizarea dispozitivelor portabile. Interfaţa Web de Administrare şi Raportare răspunde nevoilor conducerii şi personalului de securitate IT şi oferă informaţii în timp real despre dispozitivele controlate şi despre activităţile de transfer de date la nivelul întregii organizaţii.

Parolă Offline Temporară / Reţea în mod "Offline"
Calculatoarele securizate care sunt deconectate de la reţea rămân protejate. Pentru a menţine productivitatea în deplasare, dispozitivele şi transferurile de fişiere pot fi autorizate temporar prin funcţionalitatea Parolă Offline Temporară.

Principalele Beneficii
- Opreşte pierderea de date
- Endpoint Protector implică un TCO cu 50% mai mic decât media pieţei
- Se instalează într-un timp cu 70% mai scurt decât alte soluţii
- Costă cu 45% mai puţin decât alte soluţii similare



Crearea politicilor de securitate pentru entităţi specifice
Politicile Content Aware oferă un control flexibil de scanare a documentelor, permiţând monitorizare selectivă în funcţie de utilizatori, computere, grupuri sau departamente.

Filtru în funcţie de Conţinut Predefinit sau Cuvinte Cheie
Filtrează datele care părăsesc calculatoarele protejate pe baza conţinutului predefinit, care include:
- Detaliile Cardului de Credit (principalele carduri sunt suportate)
- Numere de Securitate Socială (diferite formate sunt suportate)
- Informaţii despre Conturi Bancare; etc.

Filtru în funcţie de Dicţionare / Conţinut Personalizat şi Expresii Regulate
Filtre personalizate pot fi create, astfel modulul de Content Aware Protection caută cuvintele cheie şi opreşte fişierele care le conţin de a ajunge la punctele de ieşire. Dicţionare multiple pot fi create, cât si politici avansate bazate pe RegEx.

Filtru în funcţie de Tipul Fişierului
Endpoint Protector blocheaza documentele care părăsesc compania în funcţie de adevăratul lor tip de fişier. Suportă cele mai importante tipuri de fişiere, aplicaţii precum MS Office şi fişiere grafice, arhive, executabile, media şi multe alte fişiere.

Prag pentru Filtre
Pragul defineşte limita de încălcări până de la care este permis transferul de fişiere. Acesta se aplică la fiecare tip de conţinut confidenţial şi 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 si lipirea informatiilor sensibile ale companie din documente către clienţi Outlook, aplicaţii e-mail sau alte canale prin care se scurg informaţii.

Dezactivare Print Screen
Dezactivarea opţiunii print screen în politica va împiedica utilizatorii de la a scoate din companie informaţiile afişate pe ecran, ca imagini. Acest lucru întăreşte şi mai mult politica dumneavoastră DLP.

Prevenirea trimiterii datelor sensibile ca ataşament de e-mail
Blocarea sau doar monitorizarea utilizatorilor care încearcă trimiterea de fişiere confidenţiale prin ataşamente e-mail. Content Aware Protection suportă cei mai utilizaţi clienţi de e-mail: Outlook, Thunderbird, Lotus Notes dar si Webmail.

Prevenirea trimiterii datelor sensibile prin Outlook şi Thunderbird
Ca ataşament sau chiar dacă datele confidenţiale sunt conţinute în corpul de text a unui e-mail, acesta este împiedicat să fie trimis şi incidentul este raportat. Chiar dacă firma dvs. utilizează PGP pentru criptarea e-mail-urilor, conţinutul este inspectat înainte de criptare şi trimitere.

Filtrarea datelor la ieşirea prin browsere Web

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

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

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

Modul de Auto-apărare a Clientului Endpoint Protector

Oferă protecţie chiar şi pentru calculatoarele unde utilizatorii au drepturi administrative.

Clienţi Protejaţi

- 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 (opţional)

- Active Directory

Endpoint Protector Device Control module (necesar)

Endpoint Protector Hardware Appliance

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

Common Criteria

Modele (+ altele)	Protecţie Terminale	Capacitate Adţională	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 Xenon 4 Core	2x TB Raid 1	260W
A2000	2000	400	20	2x Intel Xenon 4 Core	4x 1TB Raid 5	2x720W
A4000	4000	800	30	2x Quad Core	6x 1TB Raid 5	2x800W

Garanţie Hardware 1 an inclus. Garanţie suplimentară şi opţiuni de înlocuire disponibile.

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

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

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

Politicile de securitate pot fi aplicate pe dispozitive mobile iOS şi Android. Funcţionalităţi precum Tracking & Locating, Remote Nuke and Lock, Mobile Application Management cât şi Trimiterea Setărilor de Reţea, sunt disponibile si 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 puteţi proteja reţeaua în doar câteva minute împotriva utilizării neautorizate a dispozitivelor şi împotriva pierderii de date.

VMWARE CERTIFIED VIRTUAL APPLIANCE

vmware READY

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 sa contactaţi departamentul de Suport.

Vizitaţi 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

Contactaţi partenerul dvs. local pentru mai multe informaţii:

Trusted Device

COSOSYS

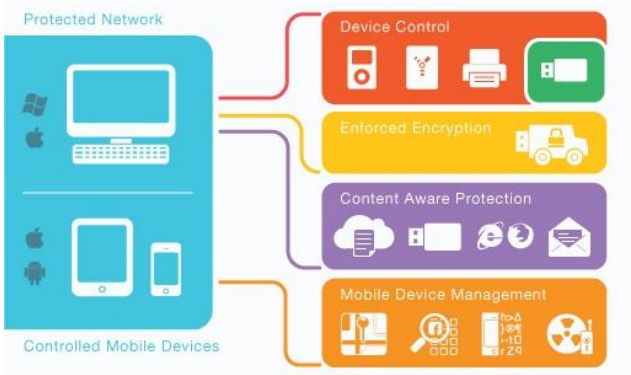
Created on 06-Mar-2013

ENDPOINT PROTECTOR 4

Soluţia pentru Prevenirea Pierderilor de Date (DLP), Controlul Dispozitivelor şi Managementul Dispozitivelor Mobile (MDM) iOS & Android pentru companii

Soluţie la cheie pentru securizarea datelor împotriva ameninţărilor reprezentate de dispozitivele portabile, mobile şi servicii cloud.

Într-o lume în care dispozitivele portabile transformă modul în care lucrăm şi trăim, Endpoint Protector 4 este proiectat pentru a menţine productivitatea şi a face munca mai convenabilă, sigură şi plăcută. Abordarea bazată pe "liste albe" de permitere a utilizării de dispozitive, URL-uri şi nume de domenii pentru calculatoare/utilizatori/ grupuri, creşte productivitatea, menţinând în acelaşi timp controlul dispozitivelor şi a datelor. Endpoint Protector 4 este oferit ca hardware sau maşină virtuală, putând fi configurat în câteva minute. Acesta reduce dramatic riscurile reprezentate de ameninţările interne care ar putea duce la scurgeri, deteriorări sau compromiterea datelor.



Avantaje Cheie

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

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

Oferă protecţie împotriva ameninţărilor generate de dispozitivele portabile mobile. Opreşte scurgerile, furtul sau pierderea de date cât şi infectarea cu viruşi.

Controlaţi următoarele (dar şi alte) dispozitive şi aplicaţii

- **Dispozitive**
- Unităţi USB (normal, U3)
- Carduri de Memorie (SD, etc.)
- CD/DVD-Burner (int., ext.)
- HDD-uri Externe (incl. sATA)
- Imprimante
- Unităţi Floppy
- Cititoare de Carduri (int., ext.)
- Camere Web
- Carduri de Reţea 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

- **Clienţi 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 Aplicaţii**
  - iTunes
  - Samsung Kies
  - Windows DVD Maker
  - Total Commander
  - FileZilla
  - Team Viewer
  - EasyLock, şi multe altele

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

- Forţare Parolă şi Politici de Securitate
- Urmărire, Localizare, Blocare sau Ştergere Dispozitive
- Trimite Setările de Reţea: E-Mail, VPN, WiFi
- Mobile Application Management
- Geofencing şi Politicilor Bazate pe Localizare
- Soluţii BYOD, informaţii detaliate în Data Sheet-ul de MDM

Administrare centralizată Web / Dashboard

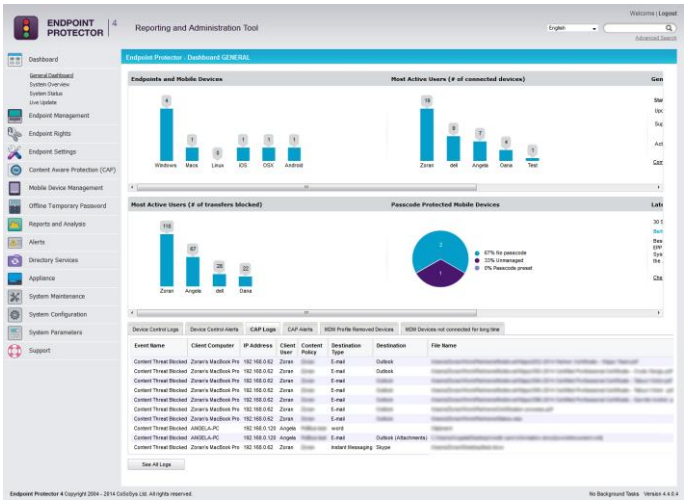
Administrează centralizat utilizarea dispozitivelor portabile. Interfaţa Web de Administrare şi Raportare răspunde nevoilor conducerii şi personalului de securitate IT şi oferă informaţii în timp real despre dispozitivele controlate şi despre activităţile de transfer de date la nivelul întregii organizaţii.

Principalele Beneficii

- Endpoint Protector implică un TCO cu 50% mai mic decât media pieţei
- Se instalează într-un timp cu 70% mai scurt decât alte soluţii
- Costă cu 45% mai puţin decât alte soluţii similare

"Am ales Endpoint Protector Appliance pentru costul său, simplitatea de administrare şi controlul detaliat. Soluţia este uşor de instalat, eficientă, puternică şi uşor de administrat. Îmi plac foarte mult funcţionalităţile de raportare, shadowing şi 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 reţea

Content Aware Protection / Filtrarea Conţinutului

Scanarea documentelor pentru detectarea conţinutului confidenţial, înregistrarea şi raportarea incidentelor de conţinut. Blocarea datelor care părăsesc punctele de ieşire, de la dispozitive portabile la aplicaţii şi servicii online.

Filtrare după Tip Fişierului / Conţinut / Expresii Regulate

File Tracing înregistrează toate datele care au fost copiate pe/de pe dispozitivele autorizate anterior sau aplicaţii on-line. File Shadowing salvează o copie a tuturor fişierelor, chiar şi cele şterse, 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 aplicaţii on-line. File Shadowing salvează o copie a tuturor fişierelor, chiar şi cele şterse, care au fost folosite în legătură cu dispozitive sau aplicaţiile controlate.

Whitelisting Fişiere / Dispozitive / URL-uri / Domenii

Numai fişierele autorizate pot fi transferate către dispozitivele şi aplicaţii on-line autorizate. Toate celelalte transferuri sunt blocate şi raportate.

Reportare şi Analiză / Panouri de Comandă & Grafice / Audit

Sunt salvate rapoarte privind activitatea clienţilor a dispozitivelor conectate şi transferuri de fişiere, oferind un istoric complet pentru audit şi analiză detaliată. Rapoarte puternice, grafice şi instrumente de analiză pentru a revizui cu uşurinţă activitatea.

Implementare a Politicilor de Securitate (Active Directory)

Prin integrarea cu Active Directory, se pot importa grupuri, calculatoare şi utilizatorii. Funcţia AD Sync va sincroniza noile entităţi.

Parolă Offline Temporară / Reţea în mod "Offline"

Calculatoarele securizate care sunt deconectate de la reţea rămân protejate. Pentru a menţine productivitatea în deplasare, dispozitivele şi transferurile de fişiere pot fi autorizate temporar prin funcţionalitatea 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 Xenon 4 Core	2x TB (Raid 1)	260W
A2000	2000	400	20	2x Intel Xenon 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	.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.

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 doart transferul de fișere 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:

Created on 29-Oct-2014

ENDPOINT PROTECTOR 4

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 sporită 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 reteaua 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 placută.

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.

Advantaje Cheie

- Protectie 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 tabletele companiei 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.

Forțare 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 dispozitivle 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 neatinse.

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.

Suport 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.

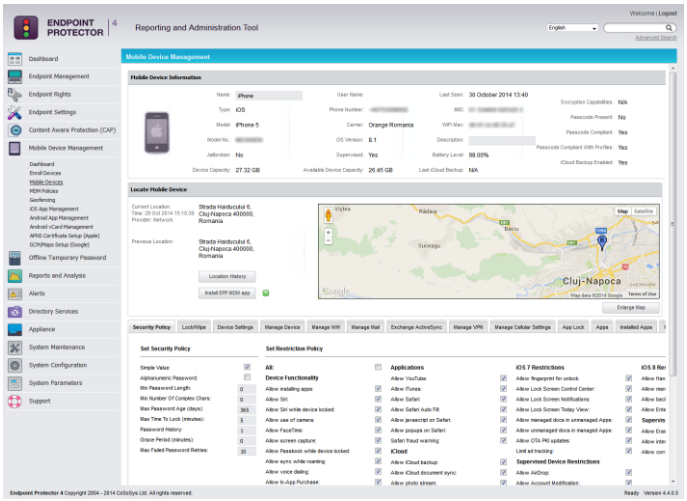
Pentru a se proteja, companiile trebuie să definească în mod clar și să aplice politicile de management al dispozitivelor mobile!

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 incorporate. Aceasta este mereu activă, aplicându-se la setarea parolei pentru dispozitiv.

Inregistrare 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 infrastructura 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.

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

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

Controlul Dispozitivelor Portabile (pentru calculatoare)
Device Control

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

Protecţie în funcţie de Conţinut (pentru calculatoare)
Content Aware Protection

Protecţie în funcţie de Conţinut pentru calculatoare Windows si Mac OS X oferă un control detaliat asupra datelor sensibile care părăsesc reţeaua companiei. Prin inspecţia eficientă a conţinutului, transferurile documentelor importante ale companiei sunt inregistrate, raportate şi blocate. Această funcţie va preveni scurgerea de date prin toate punctele de ieşire posibile, de la dispozitive USB la aplicaţii, inclusiv Microsoft Outlook, Skype, Nvigatoare Web sau Dropbox.

Endpoint Protector Hardware Appliance

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

2013 MobileVillage Mobile Star Awards RISING STAR

2014 Computing Security Awards WINNER DLP Solution of the Year

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 puteţi proteja reţeaua în doar câteva minute împotriva utilizării neautorizate a dispozitivelor şi împotriva pierderii de date.

VMWARE CERTIFIED VIRTUAL APPLIANCE

vmware READY

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 contactaţi departamentul de Suport.

Vizitaţi 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

Contactaţi partenerul dvs. local pentru mai multe informaţii:

Trusted Device

COSOSYS

Created on 29-Oct-2014