ENDPOINT PROTECTOR 4

Data Loss Prevention Solution, Device Control e iOS & Android Mobile Device Management (MDM) per le imprese

Soluzione per proteggere i dati sensibili da furti esterni e/o interni nel perimetro aziendale tramite dispositivi di archiviazione portatile, servizi cloud e dispositivi mobili.

In un mondo in cui i dispositivi portatili e gli stili di vita stanno trasformando il modo in cui lavoriamo e viviamo, Endpoint Protector 4 è stato progettato per mantenere la produttività e rendere il lavoro più efficiente e sicuro. Endpoint Protector 4 viene offerto come appliance hardware o virtuale, il tutto configurabile in pochi minuti. Riduce drasticamente il rischio di furti o di danneggiamento delle informazioni derivanti da minacce interne ed esterne.

Vantaggi principali

- Hardware o Virtual Appliance installata in pochi minuti
- 3 livelli di sicurezza in uno: Device control, Data Loss Prevention e MDM
- Gestione intuitiva dei dispositivi e degli endpoint.
- Interfaccia Web-based
- Protezione per Windows, Mac, Linux, iOS, Android
- Protezione pro-attiva contro l'uso non autorizzato di dispositivi o di copie dei dati
- VMware ready

Endpoint Protection per Windows, Mac OS X e Linux Workstations, Notebooks e Netbooks

Protezione contro attacchi tramite dispositivi portatili. Inibisce furti o perdite, accidentali o intenzionali, di dati e infezioni maligne.

Controllo di questi ed altri dispositivi ed applicazioni:

- **Devices**
- USB Drives (normal, U3)
- Memory Cards (SD, CF, etc.)
- CD/DVD-Burner (int., ext.)
- External HDDs (incl. sATA)
- Printers
- Floppy Drives
- Card Readers (int., ext.)
- Webcams
- WiFi Network Cards
- Digital Cameras
- iPhones / iPads / iPods
- Smartphones/BlackBerry/PDAs
- FireWire Devices
- MP3 Player/Media Players
- Biometric Devices
- Bluetooth Devices
- ZIP Drives
- ExpressCards (SSD)
- Wireless USB
- Serial Port
- Teensy Board
- PCMCIA Storage Devices
- Thunderbolt
- Network Share

- **E-Mail Clients**
  - Outlook
  - Lotus Notes
  - Thunderbird, etc.
- **Web Browsers**
  - Internet Explorer
  - Firefox
  - Chrome
  - Safari, etc.
- **Instant Messaging**
  - Skype, ICQ, AIM
  - Microsoft Communicator
  - Yahoo Messenger, etc.
- **Cloud Services/File Sharing**
  - Dropbox, iCloud, SkyDrive
  - BitTorrent, Kazaa, etc.
- **Altre Applicazioni**
  - iTunes
  - Samsung Kies
  - Windows DVD Maker
  - Total Commander
  - FileZilla
  - Team Viewer
  - EasyLock, e molte altre

Gestione di dispositivi mobili OS X, iOS e Android (MDM)

- Definisce password e Security Policy
- Localizza, blocca, disinfetta i dispositivi
- Forza i settaggi di rete: E-Mail, VPN, WiFi
- Gestione delle applicazioni
- Policy basate sulle localizzazioni geografiche
- Soluzioni BYOD

Gestione web based / Cruscotto

Gestione centralizzata, intuitiva, web-based tramite la quale gestire le informazioni sensibili e tutti i dispositivi. L'interfaccia gestionale offre funzioni di reportisticae informazioni in real time sul traffico dei dati sensibili.

Vantaggi

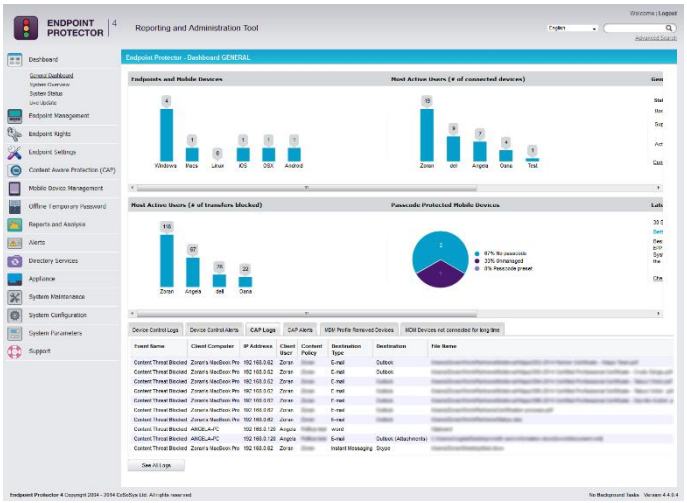
- Soluzione distribuita con una velocità del 70% superiore rispetto ai prodotti concorrenti
- Anche il costo è mediamente inferiore del 50%

2014 Computing Security Awards WINNER DLP Solution of the Year

SC Magazine Awards 2013 Europe Highly Commended

"Ho scelto Endpoint Protector per il suo costo, la facilità di gestione, e i dettagliati controlli. La soluzione è facile da installare, efficiente, potente e facilmente gestibile. Mi piacciono molto i report, lo shadowing e la funzione di password temporanee offline (veramente pratica)."

Marc Rossi
Direttore Infrastrutture
NASS e WIND SAS France



Device Control / Device Management

Definizione di diritti di accesso per i dispositivi, utenti, computer, gruppi di rete: Blocca, Consenti, Sola lettura, Consenti solo su dispositivi Trusted.

Content Aware Protection / Content Filtering

Ispezione di documenti alla ricerca di informazioni ritenute sensibili. Logging, reporting; blocco dei tentativi di copia su/da dispositivi o canali Internet non autorizzati.

Filtro per tipo di file / contenuto

Blocco basato sulla tipologia dei file. I filtri possono essere creati anche sulla base di contenuti predefiniti o personalizzati ed espressioni ricorrenti.

Tracciatura / Copia dei file sensibili

Tracciatura dei file per la registrazione di tutti i dati che sono stati copiati da/sui dispositivi autorizzati o attraverso applicazioni online. La funzione File Shadowing salva una copia di tutti i file sensibili, anche di quelli cancellati, che sono stati utilizzati su dispositivi controllati o canali esterni.

White-list di File / Dispositivi / URL / Domini

Solo i file autorizzati possono essere trasferiti ai dispositivi autorizzati e alle applicazioni online. Tutti gli altri trasferimenti sono segnalati e/o bloccati.

Reporting e analisi / Cruscotto & Grafici / Strumenti di Audit

I log delle attività vengono salvati centralmente per tutti i PC della rete, i dispositivi e le applicazioni utilizzate, fornendo una storia completa per gli audit ed una analisi dettagliata, completata con grafici e strumenti di analisi.

Facile applicazione delle policy di sicurezza (Active Directory)

Gruppi, computer e utenti integrabili in Active Directory per una costante sincronizzazione.

Modalità sicura offline / Password temporanee

Anche i computer controllati ma temporaneamente offline restano protetti. Password temporanee possono autorizzare l'uso di dispositivi per brevi periodi.

Gestione reparti

Ogni reparto aziendale può essere organizzato con le sue proprie policy.

Difesa di ogni endpoint

Sono difesi anche i computer dove l'utente ha i diritti di amministratore.

Protezione dei dati transitori / EasyLock - Cifratura

Grazie al software EasyLock, registrato su dispositivi mobili, i dati copiati nel dispositivo sono automaticamente cifrati. Con la tecnologia TrustedDevice, può essere aggiunta una ulteriore sicurezza utilizzando dispositivi cifrati. Ciò assicura che, in caso di perdita o furto del dispositivo, tutti i dati lì registrati restano inaccessibili all'utente non autorizzato.

Endpoint protetti

- Windows 10 (32/64bit)
- Windows 8 (32/64bit)
- Windows 7 (32/64bit)
- Windows Vista (32/64bit)
- Windows XP (SP2) (32/64bit)
- Windows 2003/2008/2012 (32/64bit)
- Mac OS X 10.5+
- Ubuntu 14.04
- Ubuntu 10.04
- openSUSE 11.4

Mobile Device Management (MDM):

- iPad, iPhone, iOS 4, iOS 5, iOS 6, iOS 7, iOS 8
- Android 2.2+,
- Android 4+ richiesto per alcune funzioni

Directory Service (non obbligatorio)

- Active Directory

Certificato:

Endpoint Protector Hardware Appliance

Le Hardware Appliance di Endpoint Protector sono disponibili in diverse dimensioni di potenza per rispondere alle reali necessità dei clienti. Tutte sono basate sui più moderni ed efficienti hardware disponibili sul mercato.

Modello	Numero di Endpoint supportati	Capacità addizionale	Housing (Rack mount)	Processore	Hard Drive	Power supply
A20	20	4	Stand-alone	ULV Single Core	320GB	60W
A50	50	10	1U	ULV Dual Core	320GB	200W
A100	100	20	1U	ULV Dual Core	320GB	200W
A250	250	50	1U	Pentium 2 Core	500GB	260W
A500	500	100	1U	Pentium 2 Core	1TB	260W
A1000	1000	200	1U	Intel Xenon 4 Core	2x TB (Raid 1)	260W
A2000	2000	400	2U	2x Intel Xenon 4 Core	4x 1TB (Raid 5)	2x720 W
A4000	4000	800	3U	2x Quad Core	6x 1TB (Raid 5)	2x800 W
Garanzia	1-anno – Disponibili altre opzioni					

Endpoint Protector Virtual Appliance

Endpoint Protector Virtual Appliance può essere usato da organizzazioni di ogni dimensione. La Virtual Appliance è disponibile in formato VMX, OVF e VHD, compatibile quindi con le più usate piattaforme virtuali.

Con la Virtual Appliance proteggete la vostra rete da furti ed uso improprio dei dati in pochi minuti.

Piattaforme virtuali supportate	Version	.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	-	-	-	*	-

* contattare il supporto, grazie.
Altre piattaforme virtuali potrebbero essere supportate.

Visita www.EndpointProtector.com per una installazione di prova

CoSoSys
Germany
E-Mail:
sales.de@cososys.com
Phone: +49-7541-978-2673-0
Fax: +49-7541-978-2627-9

CoSoSys
North America
sales.us@cososys.com
+1 888 271 9349

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

Contattate il vostro rivenditore:

ENDPOINT PROTECTOR 4

Content Aware Protection per Windows e Mac
Una parte importante per la vostra strategia di protezione degli endpoint.

Soluzione Out-of-the Box per proteggere le informazioni sensibili dale perdite di dati e furti tramite e-mail, messaggistica, social media, applicazioni online, dispositivi portatili e altri punti di uscita.

Content Protection Aware è un modulo di Endpoint Protector 4 che risponde alle esigenze di sicurezza dei dati sensibili delle aziende contro i rischi costituiti dai numerosi "punti di uscita".

Oggi, in un mondo in cui i dispositivi portatili e servizi cloud stanno trasformando il modo in cui lavoriamo e viviamo, Endpoint Protector è progettato per mantenere la produttività e rendere il lavoro più efficiente, sicuro e divertente.

Endpoint Protector 4 viene offerto come appliance hardware o virtuale e il tutto configurato in pochi minuti. Riduce drasticamente il rischio di furti o di danneggiamento delle informazioni derivanti da minacce interne ed esterne.

Vantaggi principali

- Hardware o Virtual Appliance installata in pochi minuti
- 3 livelli di sicurezza in uno: Device control, Data Loss Prevention e MDM
- Gestione intuitiva dei dispositivi e degli endpoint.
- Interfaccia Web-based
- Protezione per Windows, Mac, Linux, iOS, Android
- Protezione pro-attiva contro l'uso non autorizzato di dispositivi o di copie dei dati
- VMware ready

Content-Aware Data Loss Prevention

Protezione contro attacchi tramite dispositivi portatili e applicazioni online. Inibisce furti o perdite, accidentali o intenzionali, di dati e infezioni maligne.

Supporto di Windows e Mac OS X

Monitoraggio e blocco del trasferimento di dati nelle più utilizzate piattaforme per proteggere tutti i dati della vostra organizzazione.

Controllo di questi ed altri dispositivi ed applicazioni:

- **Devices**
- USB Drives (normal, U3)
- Memory Cards (SD, CF, etc.)
- CD/DVD-Burner (int., ext.)
- External HDDs (incl. sATA)
- Printers
- Floppy Drives
- Card Readers (int., ext.)
- Webcams
- WiFi Network Cards
- Digital Cameras
- iPhones / iPads / iPods
- Smartphones/BlackBerry/PDAs
- FireWire Devices
- MP3 Player/Media Players
- Biometric Devices
- Bluetooth Devices
- ZIP Drives
- ExpressCards (SSD)
- Wireless USB
- Serial Port
- Teensy Board
- PCMCIA Storage Devices
- Thunderbolt
- Network Share

- **E-Mail Clients**
  - Outlook
  - Lotus Notes
  - Thunderbird, etc.
- **Web Browsers**
  - Internet Explorer
  - Firefox
  - Chrome
  - Safari, etc.
- **Instant Messaging**
  - Skype, ICQ, AIM
  - Pidgin, Adium
  - Yahoo Messenger, etc.
- **Cloud Services/File Sharing**
  - Dropbox, iCloud, Evernote
  - BitTorrent, OneDrive, etc.
- **Altre Applicazioni**
  - iTunes
  - Samsung Kies
  - Windows DVD Maker
  - Total Commander
  - FileZilla
  - Team Viewer
  - EasyLock, e molte altre

Gestione web based / Cruscotto

Gestione centralizzata, intuitiva, web-based tramite la quale gestire le informazioni sensibili e tutti i dispositivi. L'interfaccia gestionale offre funzioni di reportistica e informazioni in real time sul traffico dei dati sensibili.

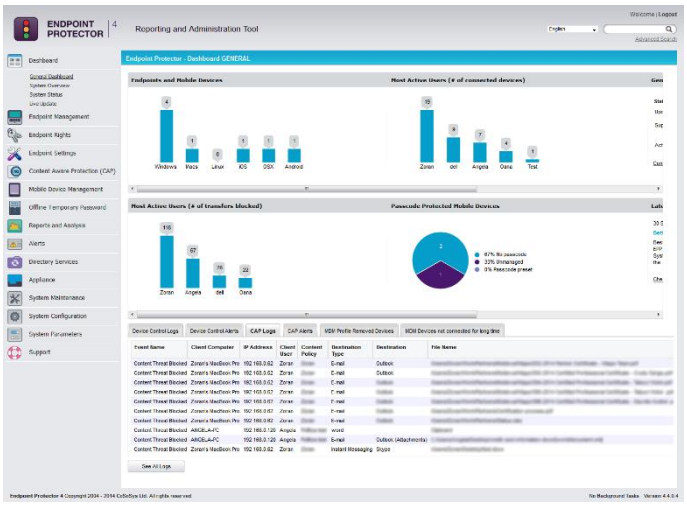
Modalità sicura offline / Password temporanee

Anche i computer controllati ma temporaneamente offline restano protetti. Password temporanee possono autorizzare l'uso di dispositivi per brevi periodi.

Vantaggi

- Stop ai furti o perdite di dati
- Soluzione distribuita con una velocità del 70% superiore rispetto ai prodotti concorrenti
- Anche il costo è mediamente inferiore del 50%

Info Security Products Guide 2012 GLOBAL EXCELLENCE FINALIST AWARDS



Crea policy di sicurezza per entità specifiche

Le policy di Content Aware Protection controllano le informazioni selezionandole per utenti, gruppi di utenti, dipartimenti, etc.

Filtra per contenuti predefiniti o parole chiave

Content Aware Protection blocca il trasferimento di dati sensibili filtrando predefiniti formati quali:

- Carte di credito
- Numeri di previdenza sociale
- Codici bancari
- Sequenze di codici creati dall'utente

Controlla Copia-Incolla e Print Screen

Monitoraggio degli "Appunti" per bloccare gli utenti dal "copia-incolla" di informazioni sensibili e dal print screen di dati inviati poi tramite posta o servizi web.

Previene l'uscita di dati sensibili come allegati di E-Mail

Blocco o semplicemente controllo degli utenti che cercano di inviare file confidenziali come allegati di e-mail. Anche se l'azienda utilizza PGP per la cifratura di e-mail, il corpo del messaggio viene controllato prima che il contenuto venga crittografato e inviato.

Filtro dei dati trasferiti via Web browser

Firefox, Google Chrome e molti altri browser usati nei computer rappresentano un grosso pericolo per il furto dei dati dal momento che gli utenti possono liberamente trasferire ogni file a cui accedono. Lo scarico di file a siti quali sendspace.com o a Dropbox rappresentano una notevole possibilità di furti. E' quindi essenziale monitorare ogni accesso a file da web browser prima che il file venga trasferito. Ciò può essere fatto solo a livello endpoint, come fa Endpoint Protector. Prevenire il furto al gateway non funziona, in questo contesto.

Filtro dei dati usati dale applicazioni prima di lasciare l'endpoint protetto.

Endpoint Protector protegge l'uso di dati riservati in molte applicazioni, quali Skype, Yahoo Messenger, Dropbox, Outlook, ecc.

Difesa di ogni endpoint

Sono difesi anche i computer dove l'utente ha i diritti di amministratore.Endpoint protetti:

- Windows 10 (32/64bit)
- Windows 8 (32/64bit)
- Windows 7 (32/64bit)
- Windows Vista (32/64bit)
- Windows XP (SP2) (32/64bit)
- Windows 2003/2008/2012 (32/64bit)
- Mac OS X 10.5+

Directory Service (non obbligatorio)

- Active Directory

Endpoint Protector Hardware Appliance

Le Hardware Appliance di Endpoint Protector sono disponibili in diverse dimensioni di potenza per rispondere alle reali necessità dei clienti. Tutte sono basate sui più moderni ed efficienti hardware disponibili sul mercato.

Modello	Numero di Endpoint supportati	Capacità addizionale	Housing (Rack mount)	Processore	Hard Drive	Power supply
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)	2x720 W
A4000	4000	800	30	2x Quad Core	6x 1TB (Raid 5)	2x800 W
Garanzia	1-anno – alter opzioni disponibili					

Device Control per Endpoints (Desktops, Laptops, ecc.) è un'altra funzione disponibile per la prevenzione dei furti (Data Loss Prevention)

Endpoint Protector offer ulteriori funzioni per controllare dispositivi portatili e le porte di comunicazione di Windows, Mac OS X e Linux. Grazie al Device Control, l'amministratore del Sistema ottiene dettagliati report e log su ogni trasferimento di file; non solo ma può anche ottenere una copia di questi file grazie alle funzioni di File Tracing & File Shadowing.

Mobile Device Management (MDM) per smartphone e tablet iOS e Android

Si possono applicare policy di sicurezza sui dispositivi mobili iOS e Android. Sono disponibili funzioni quali Tracking & Locating, Remote Nuke and Lock, oltre alla Gestione delle Mobile Application

Endpoint Protector Virtual Appliance

Endpoint Protector Virtual Appliance può essere usato da organizzazioni di ogni dimensione. La Virtual Appliance è disponibile in formato VMX, OVF e VHD, compatibile quindi con le più usate piattaforme virtuali.

Con la Virtual Appliance proteggete la vostra rete da furti ed uso improprio dei dati in pochi minuti.

Piattaforme virtuali supportate	Version	.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	-	-	-	*	-

* contattare il supporto, grazie.
Altre piattaforme virtuali potrebbero essere supportate.

Visita www.EndpointProtector.com per una installazione di prova

CoSoSys
Germany
E-Mail:
sales.de@cososys.com
Phone: +49-7541-978-2673-0
Fax: +49-7541-978-2627-9

CoSoSys
North America
sales.us@cososys.com
+1 888 271 9349

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

Contattate il vostro rivenditore:

www.partnerdata.it
info@partnerdata.it
partner data
Via E. Olivari, 9
20131 Milano
+39.02.26147380