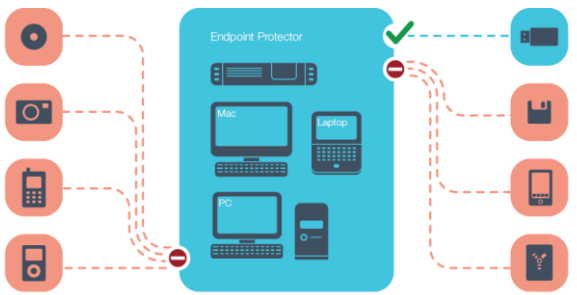




Geräteüberwachung und Datenverlust-Prävention für Firmen zum Schutz von Windows- Mac- und Linux Rechnern

Out of the Box“-Endpoint Security-Lösung zum Schutz vor Gefahren durch portable Geräte.

In einer Welt in der mobile Lifestyle Geräte unsere Lebens- und Arbeitsweise verändern, gewährleistet Endpoint Protector 4 uneingeschränkte Produktivität und macht das Arbeiten bequemer, sicherer und entspannter. Der Whitelist-basierte Ansatz erlaubt die Verwendung von spezifischen Geräten für bestimmte Computer/ Benutzer und Gruppen. Die Produktivität bleibt erhalten. Welche Geräte eingesetzt werden und welche User Daten transferieren, lässt sich leicht regeln und kontrollieren. Endpoint Protector 4 als Hardware oder Virtuelle Appliance kann innerhalb weniger Minuten in Betrieb genommen werden. Die Risiken der internen Gefahren, die zu Sicherheitslecks, gestohlenen oder anderweitig beschädigten Daten führen können, werden stark reduziert.



Endpoint Security für Arbeitsplätze, Notebooks und Netbooks

Freigegebenes Gerät
Gesperrtes Gerät

Die wichtigsten Funktionen

- Hardware- oder Virtuelle Appliance kann innerhalb weniger Minuten eingerichtet werden
- Web-basierte Oberfläche
- Intuitives Geräte Management
- Schützt Windows-, Mac- und Linux Clients
- Pro-aktiver Schutz vor Geräte-Missbrauch und Datenklau
- VMware ready

Endpoint Security für Windows und Mac OS X Arbeitsplätze, Notebooks und Netbooks

Schutz gegen Gefahren, die durch portable Datenträger entstehen. Stoppt versehentlichen oder gewollten Datenverlust, Datendiebstahl und mit Malware infizierte Daten.

Geräteüberwachung – kontrollieren Sie diese und mehr Geräte:

- USB Geräte*
- USB Flash Drives* (Normale USB Drives, U3, etc.)*
- Speicherkarten* (SD, MMC, CF, Smartcard, etc.)
- CD/DVD-Player / Brenner (interne, externe)*
- externe HDDs* (inkl. sATA HDDs)
- Drucker*
- Floppy Disks
- Card Readers* (interne, externe)
- Webcams*
- WiFi Netzwerkkarten
- Digitalkameras*
- iPhones / iPads / iPods*
- Smartphones/BlackBerry/PDAs
- FireWire Geräte*
- MP3 Player/Media Player Geräte*
- Biometrische Geräte
- Bluetooth Geräte*
- ZIP Drives
- ExpressCards (SSD)
- Wireless USB
- Serien Ports
- Teensy Board
- PCMCIA Speichergeräte

Zentrales webbasiertes Management / Dashboard

Die zentrale Verwaltung aller tragbaren Datenspeicher (das "Dashboard") liefert den Überblick zu allen wichtigen Informationen für IT-Mitarbeiter und Management. Unternehmensweit können die Speichergeräte überwacht und Datentransfers in Echtzeit überwacht werden.

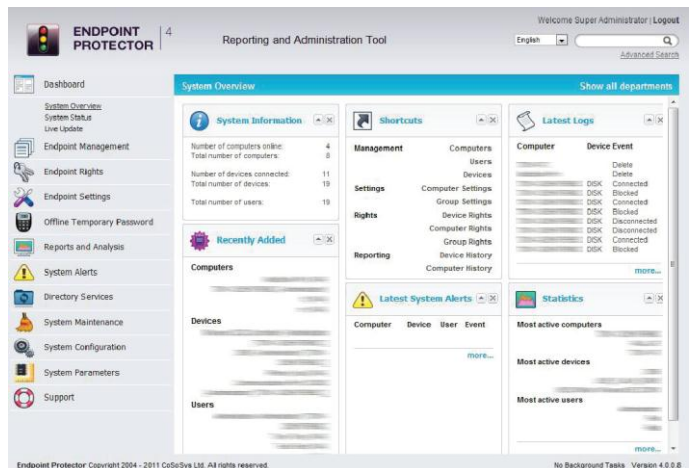
Die wichtigsten Vorteile

- Endpoint Protector Gesamtbetriebskosten, sind um 50% kleiner als der Durchschnitt am Markt.
- Ist um 70% schneller eingerichtet als andere Lösungen.
- Kostet 45% weniger als vergleichbare Systeme.



"Ich wähle die Endpoint Protector Appliance aufgrund ihrer Kosten, Bedienerfreundlichkeit und detaillierten Kontrollfunktion. Die Lösung ist leicht zu installieren, effizient, leistungsfähig und intuitiv anwendbar. Ich schätze das Aufzeichnen der Geräteaktivitäten, das File Shadowing und die Temporäre Password Funktion (wirklich sehr nützlich)."

Marc Rossi
Infrastructure Director
NASS et WIND SAS Frankreich



Gerätemanagement / Geräteüberwachung / Regelassistent* Verwaltung von Geräten, Benutzern oder Computern im Netzwerk.

Dateiprotokollierung / Datenmitschnitt*

Die Dateiprotokollierung ("File Tracing") zeichnet jeden Datentransfer von und zu mobile Datenträgern auf. Der Datenmitschnitt ("File Shadowing")zeichnet eine gespiegelte Kopie der transferierten Daten auf. Auch gelöschte Daten werden gespiegelt, wenn sie in Verbindung mit überwachten Speichergeräten standen.

Datei Whitelist-Verfahren

Ausgewählte Dateien dürfen auf berechtigte Datenspeicher kopiert werden. Die Übertragung anderer Dateien ist unterbunden.

Abteilungsmanagement/Mandantenfähigkeit*

Es können Abteilungen erstellt und separate Rechte zugewiesen werden. Die Verwendung von Speichergeräten wird je nach Bedarf einer bestimmten Abteilung erlaubt, was die Anwendung in großen Organisationen vereinfacht.

Erfassen der Geräteaktivität – Audit-Trail*

Die Aktivitäten aller Clients und Geräte wird gespeichert. So entsteht ein lückenloser Bericht über verwendete Geräte, PCs und User für Audits und detaillierte Analysen.

Reports und Analysen*

Aussagekräftige Reports, Grafiken und Analysewerkzeuge.

Einfache Umsetzung von Sicherheitsrichtlinien (Active Directory)*

Vereinfachte Umsetzung von netzwerkweiten Sicherheitsrichtlinien durch anpassbare Vorlagen für bestimmte Usergruppen (Active Directory GPOs) erlauben eine einfache Durchsetzung der Vorgaben im gesamten Netzwerk.

Temporäres Offline Passwort / Netzwerk-Offline-Modus für mobile User*

Rechner ohne Kontakt zum Netzwerk/Server sind weiterhin geschützt. Damit Mitarbeiter auf Reisen produktiv bleiben können Speichergeräte können vorübergehend über die "Temporary Offline Passwort"-Funktion erlaubt werden.

Endpoint Protector Client Selbstschutz

Gewährleistet den Schutz auch an PCs deren User Administratorenrechte haben.

Erzwungene Verschlüsselung – Daten unterwegs schützen mit EasyLock

In Kombination mit unserer EasyLock Software für portable Speichergeräte wird das Verschlüsseln von Daten beim Kopieren auf diese Geräte erzwungen. Mit der TrustedDevice Technologie kann zusätzliche Sicherheit bereitgestellt werden, indem nur zertifizierte, verschlüsselte Datenträger beim Datentransfer zum Einsatz kommen. Bei Diebstahl oder Verlust eines Datenträgers sind die Daten verschlüsselt, sicher und unzugänglich für Unberechtigte.

Geschützte Endpoint Clients

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



Directory Service (nicht erforderlich)

- Active Directory

Endpoint Protector 4 ist in seiner Klasse die einzige Lösung für Geräteüberwachung und DLP in einem Netzwerk, die als Hardware und als Virtuelle Appliance erhältlich ist. Verglichen mit anderen Lösungen sparen Sie dabei viel Zeit, die Sie für andere Dinge nutzen können. Im Wissen, dass Ihre Computer-Schnittstellen gesichert sind.

Endpoint Protector Hardware Appliance

Die Endpoint Protector Hardware Appliances ist in verschiedenen Kapazitäten und für jede Unternehmensgröße erhältlich. Alle Hardware Appliances basieren auf der neuesten und energieeffizientesten Hardware, die es zurzeit am Markt gibt.

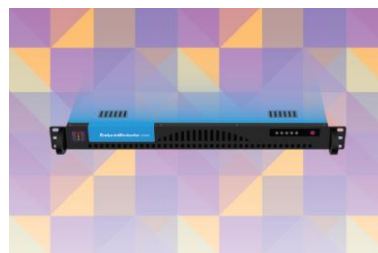


Ausgewählte Modelle	A20	A50	A100	A250	A4000
Schutz für Endpoints (Windows / Mac)	20	50	100	250	4000
Zusätzliche Kapazität	10	25	50	125	2000
Gehäuse (Rack mount)	Alleinstehend	1U	1U	1U	3U
Prozessor	ULV Single Core	ULV Dual Core	ULV Dual Core	Quad Core	2X Quad Core
Festplatte	320 GB	320 GB	320 GB	500 GB	6X 1TB (Raid 1)
Stromversorgung	60W 100-240V	200W 100-240V	200W 100-240V	260W 100-240V	2X 800W 100-240V

Hardware Gewährleistung 1 Jahr inkl. Zusätzliche Gewährleistung und Hardware-Erneuerung sind erhältlich.

Endpoint Protector Virtual Appliance

Endpoint Protector Virtual Appliance kann von Unternehmen jeder Größe verwendet werden. Die virtuelle Appliance ist in den Formaten VMX, OVF und VHD erhältlich und mit den populärsten Virtualisierungs-Plattformen kompatibel.



Die Virtual Appliance schützt Sie in Minutenschnelle vor unerlaubter Geräteverwendung und Datenverlust in Ihrem Netzwerk.



Unterstützte Virtualisierungsplattformen	Version	.ovf	.vmx	.vhd
VMware Workstation	7.1.4	-	*	-
VMware Player	3.1.4	-	*	-
VMware ESXi , vSphere Client	5.0.0	*	-	-
Virtual Box	4.0.1	*	-	-
Parallels Desktop für Mac	7.0.1	-	*	-
Microsoft Hyper V (2008 R2)	6.1	-	-	*

Weitere Virtualisierungsplattformen werden ebenfalls unterstützt.

Endpoint Protector bietet Ihnen ein sicheres und geschütztes Arbeitsumfeld bei der Verwendung portabler Speicher- und Endpoint-Geräten. Durch die Autorisierung der Geräteverwendung auf geschützten PCs bleibt die Effizienz der User uneingeschränkt und gleichzeitig werden die Sicherheitsrichtlinien eingehalten.

Besuchen sie www.EndpointProtector.de um unsere Produkte kostenlos zu testen.

CoSoSys Deutschland E-Mail: sales.de@cososys.com Phone: +49-7541-978-2627-0 Fax: +49-7541-978-2627-9	CoSoSys Nordamerika E-Mail: sales.us@cososys.com +1-208-850 7563	CoSoSys Ltd. E-Mail: sales@cososys.com +40-264-593110 +40-264-593113
---	--	---

Ihr lokaler Partner für nähere Informationen:



© Copyright 2004-2012 CoSoSys Ltd. Alle Rechte vorbehalten. Lock it Easy, Surf it Easy, Carry it Easy, Carry it Easy +Plus, Carry it Easy +Plus Bio, Secure it Easy, TrustedDevices, TrustedLogin, My Endpoint Protector and Endpoint Protector sind Markenzeichen von CoSoSys Ltd. Andere hier erwähnte Marken dienen Identifizierungszwecken und sind u.U. Markenzeichen ihrer jeweiligen Besitzer.
* Mit "*" markierte Features sind für Mac OS X verfügbar. Wir tun unser Bestes um möglichst bald alle Features für Mac OS X bereitstellen zu können.