ENDPOINT PROTECTOR 4

# Mobile Device Management (MDM) für iOS und Android

Mobile Device Management ist ein Modul der Endpoint Protector DLP („Data Loss Prevention") Lösung, das den Sicherheitsanforderungen bei der privaten oder geschäftlichen Verwendung von Mobilgeräten in Firmen gerecht wird. Dieser Trend wird auch als "Bring-Your-Own-Device" bezeichnet.

Endpoint Protector ist eine vollumfassende Lösung. Sie erleichtert IT-Verantwortlichen die Anwendung und Umsetzung von Datenverlust-Prävention (DLP) im Netzwerk. Dabei werden sowohl Computer (Windows, Mac OS X, Linux) als auch mobile Geräte (iOS und Android) effizient und wirtschaftlich geschützt.

In einer Welt, in der mobile (Lifestyle-)Geräte unsere Lebens- und Arbeitsweise verändern, gewährleistet Endpoint Protector 4 uneingeschränkte Produktivität und macht das Arbeiten entspannter und sicherer.

Endpoint Protector als Hardware-/Virtuelle-Appliance, oder Cloud-Variante kann innerhalb weniger Minuten in Betrieb genommen werden. Die Risiken durch interne Gefahren, die zu Sicherheitslecks und gestohlenen Daten führen können, werden minimiert.

## Die wichtigsten Funktionen

- Schutz für iOS und Android
- Mobile Application Management
- Web-basierte Oberfläche
- VMware kompatibel
- Hardware- oder Virtuelle Appliance oder Cloud kann in Minuten eingerichtet werden
- Intuitives Management der Mobilgeräte und Endpunkte
- Pro-aktiver Schutz vor Gerätemissbrauch und Datendiebstahl
- Gesteigerte Produktivität durch optimierte Netzwerkeinstellungen

## Sicherheit für mobile Endpunkte

Strenge Sicherheitsrichtlinien auf Firmen-Smartphones und –Tablets gewährleisten proaktiven Schutz von vertraulichen Daten, unabhängig von wo aus auf diese zugegriffen wird.

## Unterstützt iOS- und Android Mobilgeräte

Kontrolliert und steuert die beiden meistverbreiteten und wachstumsstärksten mobilen Plattformen, um Ihre Unternehmensdaten optimal zu schützen.

## Erzwungene Passworteingabe

Setzen Sie regelmäßige Passwortwechsel durch – entweder direkt und kontaktlos („Over-the-Air") oder mit Einbindung des Users.

## Verfolgung und Ortung

Behalten Sie die mobilen Firmengeräte genau im Auge und den Überblick darüber, wo sich Ihre sensiblen, auf den Geräten gespeicherten Daten befinden. Lokalisieren Sie verlorene Geräte.

## Remote Nuke (Remote Wipe)/Remote Lock - Diebstahlschutz

Verhindern Sie, dass Daten auf gestohlenen/verlorenen Mobilgeräten in die falschen Hände gelangen. Daten können kontaktlos („Over-the-Air") gelöscht und Geräte gesperrt werden.

## Einschränkungen für iOS verwalten

Stellen Sie sicher, dass bei Bedarf nur geschäftsrelevante Inhalte verwendet werden. iOS-Funktionen wie iCloud, FaceTime, YouTube, App Store, In-App Käufe, iTunes, Siri, AirDrop, die Kamera und viele weitere können deaktiviert werden.

## Verlorene Geräte wiederfinden – dank Tonwiedergabe

Kinderleichtes Wiederfinden verlorener Smartphones/Tablets dank Tonwiedergabe.

## E-Mail und WLAN Einstellungen auf iOS-Geräten verwalten

Legen Sie „Over-the-Air" Einstellungen für E-Mail und WLAN auf iOS-Geräten fest.

## E-Mail and WLAN Einstellungen auf iOS Geräten löschen

Entfernen Sie „Over-the-Air" Inhalte und Einstellungen des Firmen-E-Mail Kontos sowie WLAN-Einstellungen. Private Inhalte und private E-Mail Konten werden nicht beeinträchtigt.

## Mobile Application Management / Apps Verwalten

Stellen Sie sicher, dass keine Malware oder unseriöse Apps die Sicherheit Ihrer Unternehmensdaten gefährden. Zudem können im Rahmen des Mobile Application Managements firmeninterne Apps auf iOS- und Android-Geräten installiert und verwaltet werden.

## Unterstützung für das "Bring-Your-Own-Device" Modell

Unabhängig davon, ob sich vertrauliche Daten auf privaten oder auf Firmengeräten befinden: Sie haben die volle Kontrolle und können Sicherheit gewährleisten – gleichzeitig sind Ihre Mitarbeiter produktiv.

## Standortabhängige Richtlinien / Geofencing

Definieren Sie einen virtuellen Bereich in einem geografischen Abschnitt durch Verwendung von Ortungsdiensten. Dadurch erhalten Sie ein noch besseres Management der MDM Richtlinien, die ausschließlich in einem speziellen Bereich gelten sollen.

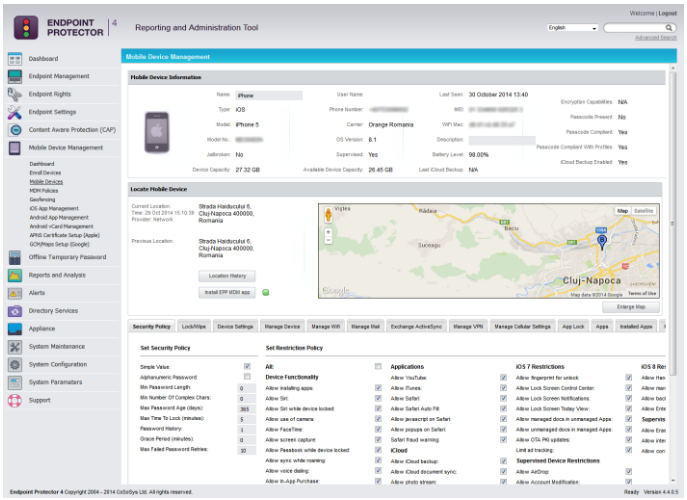
*Unternehmen sollten sich mit klaren und strikten Richtlinien im Mobile Device Management schützen!*

## Die wichtigsten Vorteile

- Setzt Richtlinien für Mobilgeräte durch
- Schützt Firmendaten
- Sofortige Kontrolle aller Mobilgeräte im Unternehmen
- Kontaktlose Registrierung
- Minimaler Aufwand für Benutzer und Admins
- Compliance *und* Produktivität
- "BYOD" sicher umsetzen

## Zentrales web-basiertes Management / Dashboard

Die zentrale Verwaltung aller mobilen Geräte liefert den Überblick zu allen wichtigen Informationen für IT-Verantwortliche und das Management. Unternehmensweit können Geräte- und Geräteaktivitäten in Echtzeit überwacht werden.




## Bestandsaufnahme mobiler Geräte

Ermöglicht eine einfache Bestandsaufnahme und Kontrolle der privaten und firmeneigenen Mobilgeräte und erstellt detaillierte Reports und Analysen der Geräteaktivitäten für spätere Audits.

## Geräte verschlüsseln

Durch das Festlegen eines Gerätepassworts werden iPhones und iPads mit permanent aktiver 256bit AES Hardware Verschlüsselung geschützt.

## Kontaktlose oder manuelle Konfiguration

Die manuelle oder „Over-the-Air" Konfiguration mittels Einmalcode erleichtert die Registrierung der mobilen Geräte mit Endpoint Protector.

## Überblick über den gesamten Mobilgeräte Bestand

Der einfachste Weg, die Übersicht über alle Mobilgeräte zu behalten. Egal ob private (Stichwort "BYOD") oder firmeneigene.

## Unterstützte mobile Geräte

- iPad, iPhone, iOS 4.0, iOS 5.0, iOS 6.0, iOS 7.0, iOS 8.0
- Android 2.2+
- einige Funktionen sind nur für neuere iOS und Android Versionen verfügbar

## Anforderungen für MDM

- Für iOS MDM ist ein kostenloses Benutzerkonto für Apple Push Notification Services (APNS) erforderlich (wird mit einer Apple ID erstellt).
- Für Android MDM ist ein kostenloses Benutzerkonto für Google Cloud Messaging (GCM) erforderlich (wird mit einem Google Account erstellt).

## Übersicht der Funktionen und Vergleich zwischen iOS und Android

Die Liste unserer Funktionen für iOS und Android ist hier parallel aufgeführt und wächst kontinuierlich, um auch den neuesten Sicherheitsanforderungen gerecht zu werden.

| MDM Funktionen | iOS | Android |
|---|---|---|
| **Registrierung** | ✔ | ✔ |
| Registrierung durch E-Mail, URL, QR-Code oder SMS (verfügbar für Deutschland, USA, GB, und mehr als 100 weitere Länder) | ✔ | ✔ |
| **Strenge Sicherheitsrichtlinien** | ✔ | ✔ |
| Passwortparameter (Länge, max. Anzahl der Wiederholungen, numerisch, alphabetisch, etc.) | ✔ | ✔ |
| Zeit bis Bildschirmsperre | ✔ | ✔ |
| **Passwort erzwungen** | ✔ | ✔ |
| **Geräteverschlüsselung erzwingen** (Geräte/OS built-in Verschlüsselung) | ✔ | ✔ |
| **Ortung und Verfolgung** App erforderlich | ✔ ja | ✔ nein |
| **Remote Lock (Externe Sperrung)** | ✔ | ✔ |
| **Remote Nuke (Remote Wipe)** | ✔ | ✔ |
| Daten auf Gerät löschen | ✔ | ✔ |
| Inhalte/Einstellungen für Firmen-Mail-Account löschen | ✔ | |
| SD Karde löschen | | ✔ |
| **Mobile Application Management** | ✔ | ✔ |
| **Geofencing** | ✔ | ✔ |
| **Mobile Device Asset Management** | ✔ | ✔ |
| **Netzwerkeinstellungen forcieren** | ✔ | ✔ |
| E-mail, VPN, WiFi | ✔ | |
| Block WiFi, Bluetooth | | ✔ |
| **Kameraverwendung unterbinden** | ✔ | ✔ |
| **Over-the-Air Einrichtung** | ✔ | ✔ |
| **Einschränkungen festlegen für** | | |
| iTunes,<br>iCloud,<br>App Store, In-App Purchases<br>Siri<br>FaceTime<br>verschlüsseltes iTunes Backup<br>Safari, YouTube<br>etc. | ✔<br>✔<br>✔<br>✔<br>✔<br>✔<br>✔<br>✔ | |
| **Und viele weitere Funktionen** | ... | ... |
| **Unterstützte Versionen** | Apple iOS 4, 5, 6, 7, 8 | Android 2.2+ |

Bestimmte Gerätesicherheits- und –Managementfunktionen werden auf älteren OS Versionen und/oder Geräten nicht angeboten.

## Schnittstellensicherheit (Device Control) für Endpunkte (Desktops, Laptops, etc.) ist ein weiteres Sicherheitsmodul von Endpoint Protector

Endpoint Protector verfügt über weitere Funktionen um die Verwendung mobiler Speichergeräte an Schnittstellen wie z.B. USB von Windows, Mac OS X und Linux Computern präventiv vor Datenverlust/-Diebstahl zu sichern.

## Content Aware Protection für Endpunkte (Laptops, etc.)

Content Aware Protection für Windows und Mac OS X Desktop Endpunkte bietet eine detaillierte Kontrolle über Daten, die das Unternehmensnetzwerk via Cloud-/Online-Diensten verlassen. Die Dateiinhalte werden gefiltert und Datentransfers blockiert, wenn die Richtlinien dadurch verletzt werden. Zu den überwachten Anwendungen zählen u.a. Microsoft Outlook, Skype, Yahoo Messenger und Dropbox.

## Endpoint Protector Hardware Appliance

Die Endpoint Protector Hardware Appliance ist in verschiedenen Kapazitäten und für jede Unternehmensgröße erhältlich. Alle Hardware Appliances basieren auf der neuesten und energie-effizientesten Hardware am Markt.


2013 MobileVillage Mobile Star Awards RISING STAR

2014 Computing Security Awards WINNER DLP Solution of the Year

## Endpoint Protector Virtual Appliance

Die Endpoint Protector Virtual Appliance kann von Unternehmen jeder Größe verwendet werden. Die virtuelle Appliance ist in den Formaten VMX, OVF und VHD erhältlich und zu den verbreitetsten Virtualisierungsplattformen kompatibel.

VMWARE CERTIFIED VIRTUAL APPLIANCE

vmware READY

| Supported Virtual Environments | Version | .ovf | .vmx | .vhd | .xva | .pvm |
|---|---|---|---|---|---|---|
| VMware Workstation | 7.1.4 | - | * | - | - | - |
| VMware Workstation * | 9.0.2 | * | * | - | - | - |
| VMware Player * | 7.0.0 | * | * | - | - | - |
| VMware Fusion * | 5.0.0 | - | * | - | - | - |
| VMware vSphere (ESXi) | 5.5.0 | * | - | - | - | - |
| Oracle VirtualBox | 4.2.18 | * | - | - | - | - |
| Parallels Desktop for Mac | 9.0.2 | - | - | - | - | * |
| Microsoft Hyper-V Server | 2008/2012 | - | - | * | - | - |
| Citrix XenServer 64bit | 6.2.0 | - | - | - | * | - |

Bitte kontaktieren Sie unseren Support, falls Ihre Plattform mit einem * gekennzeichnet ist.
Weitere Plattformen werden ebenfalls unterstützt.

Besuchen sie www.EndpointProtector.de für kostenloss Testversionen.


Endpoint Protector GmbH
E-Mail:
vertrieb@endpointprotector.de
Tel: +49-7541-978-2673-0
Fax:+49-7541-978-2627-9

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

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


Ihr lokaler Partner für nähere Informationen:

Trusted Device™

COSOSYS



Erstellt am 08-Mai-2015

# ENDPOINT PROTECTOR 4

## Datenverlust-Prävention, Gerätekontrolle und iOS- & Android Mobile Device Management für Firmen

„Out-of-the-Box"-Lösung mit MDM zum Schutz vor Datenverlust und missbräuchlicher Geräteverwendung.

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


### Die wichtigsten Funktionen

- Hardware-/ Virtuelle Appliance oder Cloud Lösung kann in wenigen Minuten eingerichtet werden
- Drei in Eins Lösung: Gerätekontrolle, DLP und MDM
- Intuitives Geräte- und Endpunkte-Management
- Web-basierte Oberfläche
- Schutz für Windows, Mac, Linux, iOS und Android
- Pro-aktiver Schutz vor Geräte-Missbrauch und Datendiebstahl
- VMware kompatibel

## Device Control (Schnittstellensicherheit) für Windows/Mac OS X und Linux Arbeitsplätze, Notebooks und Netbooks

Schutz vor Gefahren, die durch tragbare Datenträger entstehen. Stoppt versehentlichen oder mutwilligen Datenverlust, Datendiebstahl und mit Malware infizierte Daten(-Träger).

### Geräteklassen – kontrollieren Sie diese und mehr Geräte:

- **Geräte**
- USB Geräte (normale, U3)
- Speicherkarten (SD, CF, etc.)
- CD/DVD- Brenner (int., ext.)
- Externe Festplatten (inkl. sATA)
- Drucker
- Disketten
- Kartenleser (int., ext.)
- Webcams
- WiFi Netzwerkkarten
- Digitalkameras
- iPhones / iPads / iPods
- Smartphones/BlackBerry/PDAs
- FireWire Geräte
- MP3 Player/Media Player
- Biometrische Geräte
- Bluetooth Geräte
- ZIP Laufwerke
- ExpressCards (SSD)
- Kabelloses USB
- Serielle Ports
- Teensy Board
- PCMCIA Speichergeräte
- Thunderbolt
- Network Share

- **E-Mail Clients**
  - Outlook
  - Lotus Notes
  - Thunderbird, etc.
- **Web Browser**
  - Internet Explorer
  - Firefox
  - Chrome
  - Safari, etc.
- **Instant Messaging**
  - Skype, ICQ, AIM
  - Microsoft Communicator
  - Yahoo Messenger, etc.
- **Cloud Dienste/File Sharing**
  - Dropbox, Box, ownCloud
  - BitTorrent, Kazaa, etc.
- **Weitere Anwendungen**
  - iTunes
  - Samsung Kies
  - Windows DVD Maker
  - Total Commander
  - FileZilla
  - Team Viewer
  - EasyLock, u.v.w.

## Mobile Device Management (MDM) für iOS und Android

- Geräte Orten, kontaktlos sperren und Daten löschen
- Netzwerkeinstellungen verwalten: E-Mail, VPN, WLAN
- Mobile Application Management: Apps auf die Geräte verteilen
- „BYOD" Lösung, nähere Informationen hierzu finden Sie auf dem MDM Datenblatt

## Zentrale webbasierte Steuerung / Dashboard

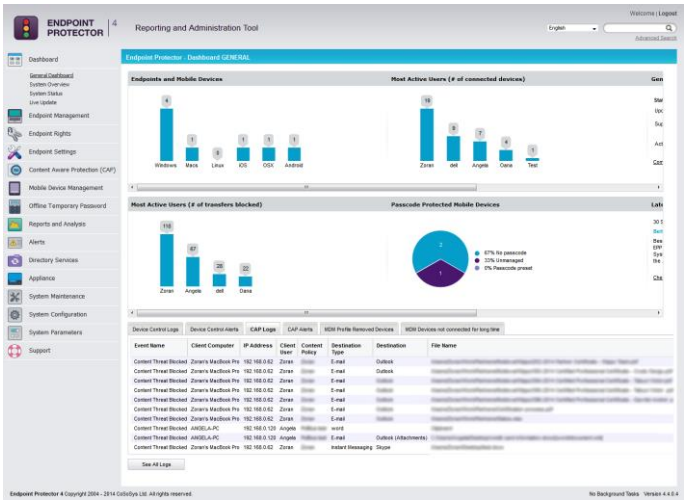
Die zentrale Verwaltung aller Endpunkte und mobilen Geräte liefert den Überblick zu allen wichtigen Informationen für IT-Mitarbeiter und das Management. Unternehmensweit können die Speichergeräte kontrolliert und Datentransfers in Echtzeit überwacht werden.

### Wesentliche Vorteile im Vergleich zu ähnlichen Lösungen am Markt

- Endpoint Protector verursacht rund 50 % niedrigere Gesamtbetriebskosten
- Die Einrichtung erfolgt um bis zu 70% schneller
- Die Kosten sind um rund 45% geringer

*"Ich wähle die Endpoint Protector Appliance aufgrund ihrer Kosten, Benutzerfreundlichkeit und detaillierten Kontrollfunktionen. Die Lösung ist leicht zu installieren, effizient, leistungsfähig und intuitiv anwendbar. Ich schätze das Aufzeichnen der Geräteaktivitäten, den Datenmitschnitt und die Offline Passwort Funktion."*

Marc Rossi
Infrastructure Director
NASS und WIND SAS France




### Gerätemanagement / Geräteüberwachung / Regelassistent
Regeln für Geräte, Benutzer oder Computer im Netzwerk festlegen.

### Content Aware Protection / Inhaltsfilter
Überprüft Dokumente auf vertrauliche Inhalte. Datentransfers werden protokolliert und ggf. wird über Zwischenfälle benachrichtigt. Sperrt Datentransfers zu mobilen Geräten, Anwendungen und Online Diensten.

### Dateityp- und inhaltsbasierte Filter / Regular Expression
Dateityp-Filter sperren Transfers bestimmter Dateitypen. Filter können auch für vorgegebene oder selbst erstellte Inhaltsrichtlinien oder unter Berücksichtigung von Regular Expression erstellt werden.

### Datei Protokollierung / Daten Mitschnitt
Datei Protokollierung ("File Tracing") zeichnet jeden Datentransfer von und zu mobilen 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 / Geräte / URLs / Domains
Ausgewählte Dateien dürfen auf berechtigte Datenspeicher kopiert werden. Die Übertragung anderer Dateien wird unterbunden.

### Reports und Analysen / Dashboards & Grafiken / Audit-Trail
Aktivitäten aller Clients und Geräte werden gespeichert. So entsteht ein lückenloser Bericht über verwendete Geräte, PCs und User für Audits und detaillierte Analysen. Aussagekräftige Reports, Grafiken und Analysewerkzeuge stehen zur Verfügung.

### Temporäres Offline Passwort / Netzwerk-Offline-Modus
Rechner ohne Kontakt zum Netzwerk/Server bleiben unverändert geschützt. Damit Mitarbeiter auf Reisen produktiv bleiben, können Speichergeräte vorübergehend mittels Temporärem Offline Passwort erlaubt werden (zwischen 30 Minuten und 30 Tagen).

## Endpoint Protector Client Selbstschutz

Gewährleistet den Schutz auch an PCs, deren Anwender lokale Administrator-Rechte haben.

## Erzwungene Verschlüsselung – Datentransporte mit EasyLock sichern

In Kombination mit unserer EasyLock Software für tragbare Speichergeräte wird das Kopieren der Daten in den verschlüsselten Container der Geräte erzwungen. Mit der TrustedDevice Technologie kann zusätzliche Sicherheit bereitgestellt werden, indem nur zertifizierte, verschlüsselte Datenträger für Datentransfers eingesetzt werden. Bei Diebstahl oder Verlust eines Datenträgers sind die Daten verschlüsselt, sicher und unzugänglich für Unberechtigte.

### Geschützte Client Betriebssysteme

- Windows 10 (32/64bit)
- 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

### Mit Mobile Device Management unterstützte Mobilgeräte

- iPad, iPhone, iOS 4, iOS 5, iOS 6, iOS 7, iOS 8
- Android 2.2+,
  Android 4+ erforderlich für Geräteverschlüsselung

### Directory Dienste (nicht erforderlich)

- Active Directory

## Zertifizierungen:

## Endpoint Protector Hardware Appliance

Die Endpoint Protector Hardware Appliances sind in verschiedenen Größen erhältlich. Alle Hardware Appliances basieren auf den neusten und energie-effizientesten Standards am Markt.


| Ausgewählte Modelle | Anzahl Endpunkte (Windows/ Mac) | Zusatz-Kapazität | Gehäuse (Rack Mount) | Prozessor | Festplatte | Stromversorgung |
|---|---|---|---|---|---|---|
| A20 | 20 | 4 | Standalone | 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 |

| | |
|---|---|
| Hardware Gewährleistung | 1 Jahr inkl. zusätzliche Gewährleistung und Hardware-Erneuerung sind erhältlich. |

## Endpoint Protector Virtual Appliance

Die 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 Ihr Netzwerk innerhalb weniger Minuten vor unberechtigtem Gerätezugriff und Datenverlust.

| Unterstützte Virtualisierungsplattformen | Version | .ovf | .vmx | .vhd | .xva | .pvm |
|---|---|---|---|---|---|---|
| VMware Workstation | 7.1.4 | - | * | - | - | - |
| VMware Workstation * | 9.0.2 | * | * | - | - | - |
| VMware Player * | 7.0.0 | * | * | - | - | - |
| VMware Fusion * | 5.0.0 | - | * | - | - | - |
| VMware vSphere (ESXi) | 5.5.0 | * | - | - | - | - |
| Oracle VirtualBox | 4.2.18 | * | - | - | - | - |
| Parallels Desktop for Mac | 9.0.2 | - | - | - | - | * |
| Microsoft Hyper-V Server | 2008/2012 | - | - | * | - | - |
| Citrix XenServer 64bit | 6.2.0 | - | - | - | * | - |

Bitte kontaktieren Sie unseren Support, falls Ihre Plattform mit einem * gekennzeichnet ist.
Weitere Plattformen werden ebenfalls unterstützt.

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

Endpoint Protector GmbH
Deutschland
E-Mail:
vertrieb@endpointprotector.de
Tel: +49-7541-978-2673-0
Fax:+49-7541-978-2627-9

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

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

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

## Ihr lokaler Partner für nähere Informationen:



Erstellt am 08-Mai-2015

# ENDPOINT PROTECTOR 4

## Content Aware Protection für Windows und Mac OS X Essentieller Bestandteil Ihrer DLP Strategie

"Out-of-the-Box" Lösung zum Schutz vor Datenlecks und -Diebstahl durch Online-/Cloud-Dienste, tragbare Datenspeicher und andere Schnittstellen.

Content Aware Protection ist ein Modul der Endpoint Protector DLP ("Data Loss Prevention") Suite und richtet sich an die Risiken, vor denen Unternehmensdaten angesichts zahlreicher Schnittstellen geschützt werden müssen.
In einer Welt, in der mobile Lifestyle Geräte unsere Lebens- und Arbeitsweise verändern, gewährleistet Endpoint Protector 4 uneingeschränkte Produktivität und macht das Arbeiten entspannter und sicherer. Die Implementierung erfolgt schnell und unkompliziert. Vertrauliche Daten auf Laptops und Desktop PCs werden vor Angriffen innerhalb des Netzwerks geschützt. Mit Endpoint Protector 4, als Virtual und Hardware Appliance oder Cloud Service erhältlich, sinkt nach einem nur wenige Minuten dauernden Setup das Risiko von Datenlecks, Datendiebstahl und ähnlichen Zwischenfällen drastisch.


### Die wichtigsten Funktionen

- Hardware-/Virtuelle-Appliance oder Cloud Lösung kann in wenigen Minuten eingerichtet werden
- Web-basierte Oberfläche
- Intuitives Geräte- und Endpunkte-Management
- Schutz für Windows und Mac OS X Endpunkte
- Pro-aktiver Schutz vor Geräte-Missbrauch und Datendiebstahl
- VMware kompatibel

### Content-Aware Datenverlust-Prävention

Schutz vor Gefahren durch Datentransfers von und zu Speichergeräten, Anwendungen und Online-/Cloud-Diensten. Stoppt absichtlichen und versehentlichen Datendiebstahl und Datenverlust.

### Unterstützung von Windows und Mac OS X Endpunkten

Datentransfers werden mit vorher definierten Sicherheitsrichtlinien abgeglichen und ggf. unterbunden. Deckt zum bestmöglichen Schutz Ihrer Unternehmensdaten die gängigsten Betriebssysteme ab.

### Überwachen Sie Datentransfers von und zu diesen und weiteren Anwendungen und Geräten:

- **Geräte / Schnittstellen**
- USB Geräte (normal, U3)
- Speicherkarten (SD, CF, etc.)
- CD/DVD-Brenner (int., ext.)
- Externe Festplatten (incl. sATA)
- Drucker
- Disketten
- Kartenleser (int., ext.)
- Webcams
- WiFi Netzwerkkarten
- Digitalkameras
- iPhones / iPads / iPods
- Smartphones/BlackBerry/PDAs
- FireWire Geräte
- MP3 Player/Media Players
- Biometrische Geräte
- Bluetooth Geräte
- ZIP Laufwerke
- ExpressCards (SSD)
- Wireless USB
- Serielle Ports
- Teensy Board
- PCMCIA Speichergeräte
- Thunderbolt
- Network Share

- **E-Mail Clients**
  - Outlook
  - Lotus Notes
  - Thunderbird, etc.
- **Web Browser**
  - 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.
- **Weitere Anwendungen**
  - iTunes
  - Samsung Kies
  - Windows DVD Maker
  - Total Commander
  - FileZilla
  - Team Viewer
  - EasyLock, u.v.w.

### Zentrale web-basierte Steuerung / Dashboard

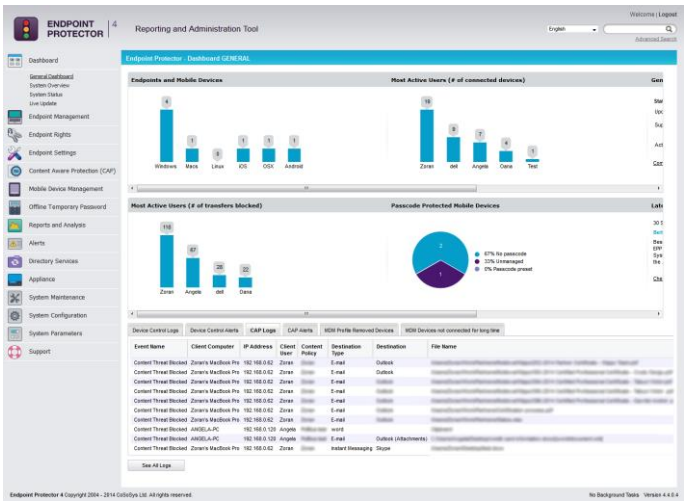
Die zentrale web-basierte Verwaltung liefert den Überblick zu allen wichtigen Informationen für IT-Mitarbeiter und das Management. Unternehmensweit können Endpunkte und Datentransfers in Echtzeit überwacht werden.

### Temporäres Offline Passwort / Netzwerk-Offline-Modus

Rechner ohne Kontakt zum Netzwerk/Server bleiben geschützt. Damit Mitarbeiter auf Reisen produktiv bleiben, können Speichergeräte vorübergehend mittels Temporärem Offline Passwort erlaubt werden (zwischen 30 Minuten und 30 Tagen).

### Wesentliche Vorteile im Vergleich zu ähnlichen Lösungen am Markt

- Verhindert Datenverluste und -Diebstahl
- Gesamtbetriebskosten sind um rund 50% geringer
- Spart wertvolle Zeit. Die Implementierung erfolgt 70% schneller als bei anderen Lösungen
- Die Lizenzpreise sind um rund 45% günstiger




### Sicherheitsrichtlinien für bestimmte Abteilungen erstellen

Content Aware Protection Richtlinien bieten flexible Kontroll-möglichkeiten durch die Inhaltsprüfung von Dokumenten, dem Zuweisen von Berechtigungen auf Benutzer-, Computer-, Gruppen- oder Abteilungsebene sowie umfassenden Analysetools.

### Filter auf Basis vordefinierter Inhalte oder Schlüsselwörter

Filtert die Daten, bevor diese das Netzwerk verlassen. Anhand vordefinierter Inhalte und Schlüsselwörter erkennt das CAP Modul u.a.:

- Kreditkartendaten (alle gängigen Kreditkarten werden unterstützt)
- Sozialversicherungsnummern (viele verschiedene Länderformate werden unterstützt)
- Kontodaten, etc.

### Filter auf Basis individueller Wörterbücher / benutzerdefinierter Inhalte und Regular Expression

Es ist möglich, benutzerdefinierte Filter anzulegen. Das Modul Content Aware Protection durchsucht Dateien vor dem Transfer nach Schlüsselwörtern und stoppt den Vorgang, falls er gegen eine Richtlinie verstößt. Mehrere Wörterbücher und Richtlinien auf Basis von Regular Expression können zu diesem Zweck erstellt werden.

### Filter auf Dateityp-Ebene

Endpoint Protector ermöglicht, Richtlinien für den Transfer bestimmter Dateitypen zu erstellen. Dabei wird stets der wahre Dateityp erkannt. Unterstützt werden alle gängigen Dateiformate: Office-, Grafik-, Archiv- und Medien- sowie ausführbare Dateien.

### Threshold (Schwellenwert) für CAP-Filter

Der Threshold legt fest, bis zu welcher Anzahl Richtlinienverstöße der Datentransfer zugelassen wird. Er gilt entweder für jede Art von vertraulichen Inhalten oder er bezieht sich auf die Gesamtsumme der Verstöße.

### Zwischenablage und Copy & Paste deaktivieren

Diese Funktion verhindert, dass Benutzer sensible Daten per Copy & Paste in Anwendungen wie Outlook, Webmailer oder sonstige richtlinienwidrige Anwendungen übertragen.

### Print Screen deaktivieren

Diese Funktion deaktiviert das Erstellen von Printscreens. Somit können als Bilder getarnte Daten nicht mehr unbehelligt aus dem Firmennetzwerk geschleust werden und die DLP Richtlinien werden noch wirkungsvoller.

### Datentransfers im E-Mail Anhang verhindern

Blockieren oder überwachen Sie, welche Dateien Anwender als E-Mail Anhang verschicken. Die gängigsten E-Mail Clients werden unterstützt: Outlook, Thunderbird, Lotus Notes, etc.

### Datenlecks via Outlook und Thunderbird verhindern

Als Anhang oder im Nachrichtentext: vertrauliche Daten sollten nicht unbehelligt verschickt werden. Die Funktion scannt die Inhalte der Mails und benachrichtigt über Vorgänge, die gegen Richtlinien verstoßen. Funktioniert auch bei PGP-verschlüsselten E-Mails.

### Filtert Datentransfers via Webbrowser

Internet Explorer, Firefox, Google Chrome und weitere Browser sind allgegenwärtig auf den PCs (genauso wie Safari auf Macs) und bereiten IT-Verantwortlichen Sorgen. Anwender können Daten auf Seiten wie sendspace.com oder die Dropbox Web-Oberfläche hochladen. Deshalb

ist es wichtig, alle Daten, die über einen Browser verschoben werden, anzuzeigen. Und zwar bevor sie online gestellt werden. Das kann lediglich auf Endpunkte-Level erfolgen und Endpoint Protector bietet exakt diese Möglichkeit. Das Verhindern von Datenverlusten im Gateway ist keine adäquate Alternative.

### Filtert Dateien vor Verlassen eines geschützten Endpunkts und scannt die Verwendung durch verschiedene Anwendungen

Endpoint Protector sichert die Verwendung vertraulicher Daten in vielen Anwendungen, darunter Skype, Yahoo Messenger, Dropbox, Outlook, etc.

### Endpoint Protector Client Selbstverteidigung

Bietet Schutz, auch wenn der Benutzer über lokale Administratorrechte verfügt

#### Geschützte Endpoint Clients

- Windows 10 (32/64bit)
- 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 Dienste (nicht erforderlich)

- Active Directory

#### Endpoint Protector Modul Schnittstellensicherheit / Gerätekontrolle (erforderlich)

### Endpoint Protector Hardware Appliance

Die Endpoint Protector Hardware Appliance ist in verschiedenen Kapazitäten und für jede Unternehmensgröße erhältlich. Alle Hardware Appliances basieren auf der neuesten und energieeffizientesten Hardware am Markt.


Common Criteria

| Ausgewählte Modelle (+mehr ) | Anzahl Endpunkte | Zusatz-Kapazität | Gehäuse (Rack Mount) | Prozessor | Festplatte | Stromversorgung |
|---|---|---|---|---|---|---|
| A20 | 20 | 4 | alleinstehend | 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 |

| | |
|---|---|
| Hardware Gewährleistung | 1 Jahr inkl. zusätzliche Gewährleistung und Hardware-Erneuerung erhältlich. |

### Schnittstellensicherheit/Gerätekontrolle für Endpunkte (Desktops, Laptops, etc.) ist ein weiteres Modul der DLP

Endpoint Protector bietet weitere DLP-Module zur Kontrolle tragbarer Speichergeräte und Schnittstellen von Windows, Mac OS X und Linux Rechnern an. Mit Schnittstellensicherheit/Gerätekontrolle verfügen IT Administratoren über umfassende Reporte, Analysen und Log-Dateien um Datentransfers zu überwachen und bei Bedarf eine Kopie zu speichern (Datei Protokollierung / Daten Mitschnitt).

### Mobile Device Management (MDM) für iOS und Android Smartphones und Tablets

Starke Sicherheitsrichtlinien ermöglichen die Verwendung von iOS- und Android-Geräten im Unternehmensumfeld. Funktionen wie kontaktloses Datenlöschen oder Gerätesperren verhindern, dass Daten bei Verlust oder Diebstahl missbräuchlich verwendet werden. Zudem können Geräte geortet und mit starken Passwörtern geschützt werden.

### 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 zu den verbreitetsten

Virtualisierungs-Plattformen kompatibel. Mit der Virtual Appliance schützen Sie Ihr Netzwerk innerhalb weniger Minuten vor unberechtigtem Gerätezugriff und Datenverlust

VMWARE CERTIFIED VIRTUAL APPLIANCE

vmware READY

| Unterstützte Virtualisierungsumgebungen | Version | .ovf | .vmx | .vhd | .xva | .pvm |
|---|---|---|---|---|---|---|
| VMware Workstation | 7.1.4 | - | * | - | - | - |
| VMware Workstation * | 9.0.2 | * | * | - | - | - |
| VMware Player * | 7.0.0 | * | * | - | - | - |
| VMware Fusion * | 5.0.0 | - | * | - | - | - |
| VMware vSphere (ESXi) | 5.5.0 | * | - | - | - | - |
| Oracle VirtualBox | 4.2.18 | * | - | - | - | - |
| Parallels Desktop for Mac | 9.0.2 | - | - | - | - | * |
| Microsoft Hyper-V Server | 2008/2012 | - | - | * | - | - |
| Citrix XenServer 64bit | 6.2.0 | - | - | - | * | - |

Bitte kontaktieren Sie unseren Support, falls Ihre Plattform mit einem * gekennzeichnet ist.
Weitere Plattformen werden ebenfalls unterstützt.

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

Endpoint Protector GmbH
Germany
E-Mail:
vertrieb@endpointprotector.de
Tel: +49-7541-978-2673-0
Fax: +49-7541-978-2627-9

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

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

### Ihr lokaler Partner für nähere Informationen

Trusted Device



Erstellt am 08-Mai-2015