



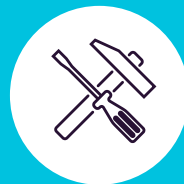
**ENDPOINT
PROTECTOR**

by CoSoSys

DATENBLATT 4.4.0.9

Data Loss Prevention & Mobile Device Management

Geeignet für alle Netzwerkgrößen und Unternehmen



DLP für Windows, Mac und Linux

Schutz für das gesamte Netzwerk





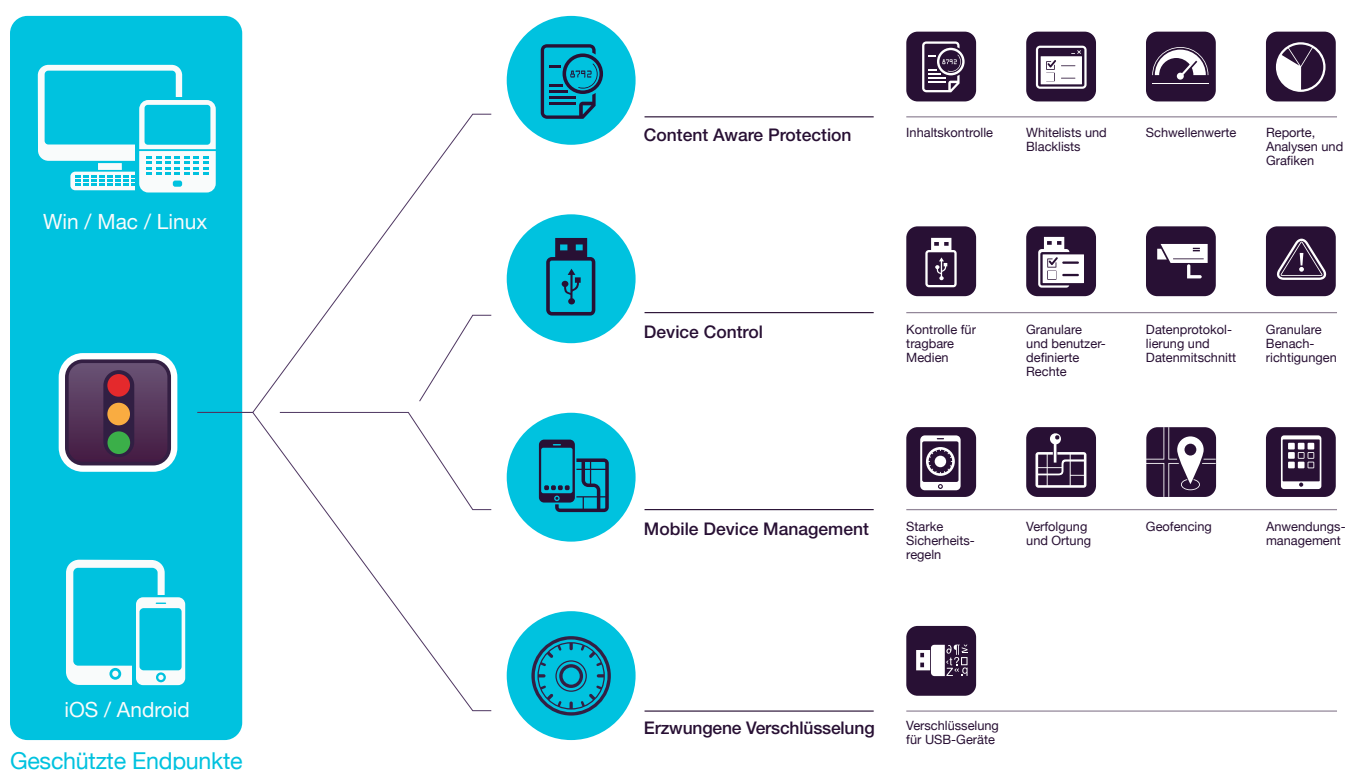
ENDPOINT PROTECTOR

by CoSoSys

Fertig einsetzbare Lösung, damit sensible Daten für die Bedrohungen durch tragbare Speichergeräte, Clouddienste und mobile Geräte gewappnet sind

Tragbare und Lifestyle-Geräte beeinflussen immer stärker die Art und Weise, wie wir arbeiten und leben. Endpoint Protector hält die Produktivität aufrecht, die Arbeit gestaltet sich sowohl bequemer als auch sicherer und sie bereitet mehr Freude. Der blacklist-basierte Ansatz verhindert den Einsatz bestimmter Geräte, URLs und Domainnamen auf Computer-, Benutzer- oder Gruppenebene, wodurch die Produktivität zunimmt und die Kontrolle von Geräten und Daten erhalten bleibt. Endpoint Protector 4 kann als Hardware oder virtuelle Appliance innerhalb von Minuten eingerichtet werden. Die Risiken durch interne Bedrohungen, die zu Datenverlusten und -diebstählen oder beschädigten oder kompromittierten Daten führen kann, werden drastisch reduziert. Compianceregeln werden eingehalten.

Wie funktioniert das



Content Aware Protection
für Windows, Mac OS X und Linux

Verfolgen und kontrollieren Sie, welche vertraulichen Daten über verschiedene Endpunkte transferiert werden dürfen und welche nicht.

Device Control
für Windows, Mac OS X und Linux

Verfolgen und kontrollieren Sie USB und periphere Ports. Setzen Sie Rechte auf Geräte-, Benutzer-, Computer- oder Gruppenebene oder für das gesamte Netzwerk.

Mobile Device Management
für Android, iOS und OS X

Verwaltung, Kontrolle und Anpassung des Sicherheitsniveaus auf Smartphones und Tablets, u.a. Sicherheits- und Netzwerkeinstellungen sowie Apps können gepusht werden.

Erzwingene Verschlüsselung
für Windows und Mac OS X

Automatischer Schutz für sensible Daten auf USB-Speichergeräten mit einer AES 256bit Verschlüsselung. Cross-Plattform-fähig, passwortbasiert, mit benutzerfreundlicher Anwendung und hocheffizient.



Content Aware Protection

für Windows, Mac OS X und Linux

Email Clients: Outlook / Thunderbird / Lotus Notes • Webbrowser: Internet Explorer / Firefox / Chrome / Safari • Instant Messaging: Skype / Microsoft Communicator / Yahoo Messenger • Cloud-Services & File Sharing: Dropbox / iCloud / SkyDrive / BitTorrent / Kazaa • Andere Anwendungen: iTunes / Samsung Kies / Windows DVD Maker / Total Commander / Team Viewer • UND VIELE MEHR



Vorkonfigurierte Inhaltefilter

Filter können auf Basis vorkonfigurierter Inhalte erstellt werden, z.B. für Kreditkarten- oder Sozialversicherungsnummern und viele weitere.



Benutzerdefinierte Inhaltefilter

Filter können auch auf Grundlage eigener Inhalte, wie z.B. Schlüsselwörtern, angelegt und verschiedene Wörterbücher blacklistbasiert erstellt werden.



Regular Expressions Filters

Erweiterte benutzerdefinierte Filter können erstellt werden, um Wiederholungen bei Datentransfers berücksichtigen zu können



Dateitypbasierte Filter

Blockt bestimmte Dokumente abhängig vom Dateityp, auch wenn die Dateiendung manuell vom Benutzer verändert wurde.



Dateiwhitelisting

Während alle anderen Datentransfers blockiert werden, können whitelistbasiert Ausnahmen definiert werden zur Vermeidung von Redundanzen und zur Erhöhung der Produktivität.



Domain & URL Whitelisting

Erlaubt whitelistbasiert Firmenportale oder Emailadressen, damit Mitarbeiter bei der Arbeit flexibel bleiben und zugleich die Unternehmensrichtlinien umgesetzt werden können.



Screenshot blockieren

Verhindert die Nutzung der Screenshot-Funktion, damit sensible Daten auf dem Bildschirm nicht aus dem geschützten Netzwerk heraus entfernt werden können.



Zwischenablage überwachen

Verhindert den Verlust sensibler Inhalte über Copy & Paste / Cut & Paste und verleiht Ihnen zusätzlichen Schutz.



Reporte und Analysen

Kontrolle der Aktivitäten bei Datentransfers mit einem leistungsstarken Reporte- und Analyse-Werkzeug. Logs und Reporte können auch in SIEM-Lösungen exportiert werden.



Dashboard und Grafiken

Mit den Grafiken und Charts erhalten Sie jederzeit einen schnellen Überblick über die wichtigsten Ereignisse und Statistiken.



Active Directory

Verwendung von AD und anderer Anwendungen, um die Ausrollung auch in größeren Netzwerken einfacher zu gestalten. Import und Synchronisation von Gruppen und Entitäten.



Summen- und Einzelschwellenwerte für Filter

Legt die maximale Anzahl von Regelverstößen fest, bis zu denen Datentransfers noch erlaubt sind. Dies kann für jeden einzelnen Inhalt oder als Summe aller Inhalte definiert werden.



Datenprotokollierung

Protokolliert alle Datentransfers oder -versuche auf ausgewählte Onlineanwendungen und Cloud-Services und gibt einen Überblick über Nutzeraktivitäten.



Datenmitschnitt

Speichert eine gespiegelte Kopie einer Datei, die auf ein kontrolliertes Gerät oder per Email, Cloud-Speicher oder anderen Anwendungen transferiert wurde.



Offline Temporäres Passwort

Datentransfers auf vom Netzwerk getrennte Computer können vorübergehend erlaubt werden, damit Sicherheit und Produktivität gleichsam gewahrt bleiben.



E-Mail Benachrichtigungen erstellen

Vor- und benutzerkonfigurierte Benachrichtigungen können per e-mail zugestellt werden, um über die wichtigsten Ereignisse bei Datentransfers informiert zu sein.



DLP für Drucker

Richtlinienerstellung für lokale und Netzwerkdrucker, damit vertrauliche Dokumente nicht ausgedruckt werden können.



HIPAA Content Aware Richtlinien

Tiefgehender Scan von Dokumenten, bevor diese transferiert werden, für folgende Daten: PHI Info, FDA, zugelassene Medikamente, ICD-9-Codierung usw.



DLP für Thin Clients

Schützt Daten auf Terminal Servern und verhindert Datenverluste in Thin Client-Umgebungen genauso wie in jedem anderem Netzwerktyp.

Weitere Funktionen

Viele andere Funktionen sind verfügbar.

Fragen Sie uns: info@endpointprotector.com



Device Control

für Windows, Mac OS X und Linux

USB-Laufwerke / Drucker / Bluetooth-Geräte / MP3 Player / Externe HDD / Teensy Board / Digitalkameras / Webcams / Thunderbolt / PDAs / Network Share / Fire Wire / iPhones / iPads / iPods / ZIP-Laufwerke / Serielle Ports / PCMCIA Speichergeräte / Biometrische Geräte / UND VIELE MEHR



Globale Rechte vergeben

Als Grundeinstellung werden die Geräterechte im Netzwerk global umgesetzt. Das Modul lässt aber äußerst granulare Berechtigungseinstellungen zu.



Gruppenrechte vergeben

Geräterechte können granular auf Gruppenebene vergeben werden, um verschiedenen Abteilungen unterschiedliche Zugriffsmöglichkeiten einräumen zu können.



Computerrechte vergeben

Falls einzelnen Rechnern eine besondere Stellung im Unternehmen eingeräumt werden muss, können Geräterechte für einzelne Computer konfiguriert werden.



Benutzerrechte vergeben

Jedem Benutzer können auf Basis seiner Rollen und Ziele unterschiedliche Geräterechte vergeben werden.



Geräterechte vergeben

Auf Basis von Hersteller-ID, Produkt-ID und Seriennummer können Zugriffsrechte auf Geräteebene vergeben werden.



Benutzerdefinierte Geräteklassen

Für Produkte eines bestimmten Herstellers lassen sich die Zugriffsrechte mit einer eigenen Geräteklasse anlegen.



Trusted Device

Bei verschlüsselten Geräten können auf Basis der Verschlüsselung (Software, Hardware) unterschiedliche Zugriffsrechte vergeben werden.



Datenprotokollierung

Protokolliert alle Datentransfers oder -versuche auf ausgewählte Onlineanwendungen und Cloud-Services und gibt einen Überblick über Nutzeraktivitäten.



Datenmitschnitt

Speichert eine gespiegelte Kopie einer Datei ab, die auf ein kontrolliertes Gerät transferiert wurde. Kann für Auditzwecke verwendet werden.



Offline Temporäres Passwort

Datentransfers auf vom Netzwerk getrennte Computer können vorübergehend erlaubt werden, damit Sicherheit und Produktivität gleichsam gewahrt bleiben.



E-mail-Benachrichtigungen erstellen

Vor- und benutzerkonfigurierte Benachrichtigungen können per e-mail zugestellt werden, um über die wichtigsten Ereignisse bei Datentransfers informiert zu sein.



Dashboard und Grafiken

Mit den Grafiken und Charts erhalten Sie jederzeit einen schnellen Überblick über die wichtigsten Ereignisse und Statistiken.

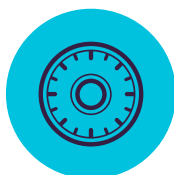


Reporte und Analysen

Kontrolle der Aktivitäten bei Datentransfers mit einem leistungsstarken Reporte- und Analyse-Werkzeug. Logs und Reporte können exportiert werden.

Weitere Funktionen

Viele andere Funktionen sind verfügbar. Fragen Sie uns: info@endpointprotector.com



Erzwungene Verschlüsselung

für Windows und Mac OS X



USB erzwungene Verschlüsselung

Erlaubt ausschließlich verschlüsselte USB-Geräte und stellt sicher, dass kopierte Daten darauf automatisch geschützt werden.



Starke Sicherheitsmechanismen

256bit AES Verschlüsselung, Passwortschutz und Anti-Manipulations-Technik stellt die Integrität der Anwendung sicher.



Master-Passwort

Die Erstellung eines Master-Passworts verleiht Ihnen Kontinuität in bestimmten Situationen, z.B. beim Reset des Benutzerkennworts.

Weitere Funktionen

Verschlüsselung ist auch für Cloudspeicher, lokale Ordner, CDs & DVDs erhältlich. Fragen Sie uns: info@endpointprotector.com



Mobile Device Management

für Android, iOS und Mac OS X



Over-the-air Ausrollung für iOS & Android

Die App kann remote per SMS, Email, URL-Link oder QR Code auf das Gerät gebracht werden. Wählen Sie die bequemste Art für Ihr Netzwerk.



Ausrollung

Bis zu 500 Smartphones und Tablets können bequem zeitgleich ausgerollt werden.



Fern-Sperrung

Bei Verlust des mobilen Gerätes kann dieses per Fernzugriff gesperrt werden, um Datenverluste zu vermeiden.



Verfolgung & Ortung

Die mobilen Geräte können verfolgt und lokalisiert werden, damit Sie immer wissen, wo sich ihre sensiblen Daten befinden.



Funktionalitäten deaktivieren

Bietet Kontrolle von integrierten Funktionen wie z.B. Kamera, Siri, Installieren von Apps.



Gerät finden durch Abspielen eines Tons

Sie können ein verlegtes Gerät wiederfinden, indem Sie von der Konsole aus einen Ton auf dem Gerät abspielen (nur für Android verfügbar).



Mobile Application Management

Verwalten Sie die unternehmensrelevanten Apps und rollen Sie diese entsprechend auf die mobilen Geräte aus.



Ausrollen von Netzwerk Einstellungen

Rollen Sie sämtliche Netzwerkeinstellungen wie E-mail, Wi-Fi und VPN Einstellungen aus oder verbieten Sie diese vollständig (Bluetooth, Klingelton etc.).



Benachrichtigungen

Sie können erweiterte Systembenachrichtigungen erstellen sowie personalisierte Benachrichtigungen.



Reporte und Analysen

Kontrolle der Aktivitäten auf den Mobilgeräten mit einem leistungsstarken Reporte- und Analyse-Werkzeug. Logs und Reporte können exportiert werden.



Kiosk Mode mit Samsung Knox

Erlaubt die Nutzung der Geräte mit genau definierten Apps. Verboten oder Erzwingen von App-Installationen per Fernzugriff aus der Konsole.



Mac OS X Management

Zur Erweiterung der DLP-Funktionen können auch Macs im MDM Modul integriert werden. Dadurch erhalten Sie zusätzliche Möglichkeiten, diese Geräte zu verwalten.



Durchsetzung von Passwörtern

Die Umsetzung von Passwort-Richtlinien gewährleistet proaktiven Schutz für die unternehmenskritischen Daten.



Fern-Löschung

In kritischen Situationen ist es wichtig, die Daten auf dem Gerät löschen zu können. Dies ist sehr einfach per Fernzugriff möglich.



Geofencing

Richtet einen virtuellen Bereich auf einer Karte ein, in dem ortsgebundene MDM-Richtlinien ausschließlich umgesetzt werden.



iOS Einschränkungen

Stellen Sie sicher, dass nur unternehmens-relevante Nutzung möglich ist. Deaktivieren Sie iCloud, Safari, den App Store etc.



Push vCards auf Android

Kontakte durch push hinzufügen, damit diese auf allen Geräten immer zur Verfügung stehen.



App Verwaltung

Sehen Sie welche Apps Ihre Mitarbeiter heruntergeladen und auf Ihren Mobilgeräten nutzen.



Asset Management

Enthält Informationen zu den Mobilgeräten, wie Gerätenamen, Typ, Modell, Speicherplatz, Betriebssystem, Carriers, IMEIs, MACs, etc.



Email Benachrichtigungen erstellen

Benachrichtigungen können per e-mail übermittelt werden, um über die wichtigsten Ereignisse bei Datentransfers informiert zu sein.



Dashboard und Grafiken

Mit den Grafiken und Charts erhalten Sie jederzeit einen schnellen Überblick über die wichtigsten Ereignisse und Statistiken.

Weitere Funktionen

Viele andere Funktionen sind verfügbar. Fragen Sie uns: info@endpointprotector.com

100% Flexibler Einsatz und Bereitstellung

Unsere Produkte können sowohl von Geschäftskunden, kleinen und mittleren Unternehmen als auch privaten Anwendern verwendet werden und sind für jede Art von Netzwerk geeignet. Durch eine Client-Server- Architektur sind sie einfach zu implementieren und zentral über die webbasierte Konsole zu verwalten. Neben der Hardware und virtuellen Appliance, Amazon Web Services Instanz und Cloud- Version ist ebenfalls eine Stand-alone-Lösung mit allen Grundfunktionen verfügbar.

Endpoint Protector

Content Aware Protection, Device Control und Verschlüsselung sind für unterschiedliche Betriebssysteme verfügbar (Windows, Mac und Linux Distributionen). Mobile Device Management und Mobile Application Management sind für iOS and Android verfügbar.

My Endpoint Protector

Content Aware Protection, Device Control und Verschlüsselung sind für Computer mit den Betriebssystemen Windows und Mac verfügbar. Mobile Device Management und Mobile Application Management sind für iOS und Android verfügbar.



Hardware Appliance



Virtuelle Appliance



Amazon Instanz



Cloud Lösung

Module

Geschützte Endpunkte



| | | | | | |
|--|----------|---|---|---|-----|
| | Windows | Windows XP / Windows Vista (32/64 bit) | ● | ● | ● |
| | | Windows 7 / 8 / 10 (32/64 bit) | ● | ● | ● |
| | | Windows Server 2000 - 2016 (32/64 bit) | ● | ● | ● |
| | Mac OS X | Mac OS X 10.6 Snow Leopard | ● | ● | ● |
| | | Mac OS X 10.7 Lion | ● | ● | ● |
| | | Mac OS X 10.8 Mountain Lion | ● | ● | ● |
| | | Mac OS X 10.9 Mavericks | ● | ● | ● |
| | | Mac OS X 10.10 Yosemite | ● | ● | ● |
| | | Mac OS X 10.11 El Capitan | ● | ● | ● |
| | Linux | Ubuntu | ● | ● | n/a |
| | | OpenSUSE | ● | ● | n/a |
| | | CentOS / RedHat | ● | ● | n/a |
| *Detaillierte Informationen zu den Versionen und Distributionen unter endpointprotector.com/linux | | | | | |
| | iOS | iOS 4, iOS 5, iOS 6, iOS 7, iOS 8, iOS 9 | | | ● |
| | Android | Jelly Bean (4.1+), KitKat (4.4+), Lollipop (5.0+) | | | ● |



HQ (Romania)

E-mail: sales@cososys.com
 Sales: +40 264 593 110 / ext. 103
 Support: +40 264 593 113 / ext. 202

Korea

E-mail: contact@cososys.co.kr
 Sales: +82 70 4633 0353
 Support: +82 20 4633 0354

Germany

vertrieb@endpointprotector.de
 +49 7541 978 26730
 +49 7541 978 26733

North America

sales.us@endpointprotector.com
 +1 888 271 9349
 +1 877 377 6475

Official Partner

www.endpointprotector.de