

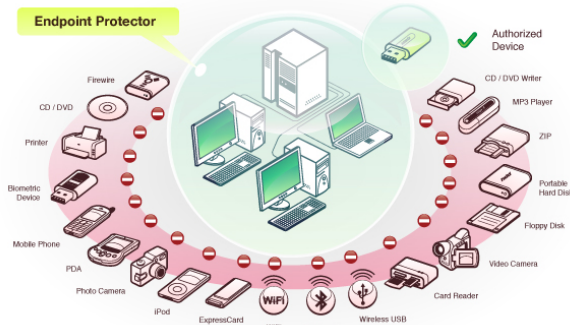


# Endpoint Protector 2009™

## Aktiver End-Geräte-Manager schützt PC und Mac vor Datenverlust

Windows XP/Vista/7 Client Version: 3.0.7.3 Windows 2003/2008 Server Version: 3.0.4.1  
Mac OS X Version: 1.0.4.4 Linux Server Version: 3.0.4.1

### Ihre Daten sind nur so sicher wie Ihre Endpunkte.



Mit Endpoint Protector 2009 regeln Sie die Verwendung von tragbaren Datenträgern (wie z.B. USB Sticks). Mit dem intuitiven Regelasistenten gestalten Sie die Sicherheitsrichtlinien Ihrer Organisation. Heutzutage ist die Art und Weise, wie wir leben und arbeiten, durch den Gebrauch von tragbaren Datenspeichern und Lifestylegeräten geprägt. Endpoint Protector 2009 kontrolliert den Umgang mit diesen Geräten ohne die Produktivität einzuschränken. Einzelne Geräte und Dateien können für Benutzer oder Gruppen freigegeben werden, während andere Dateien, Geräte oder Gerätetypen komplett von einer Verwendung ausgeschlossen sind. Endpoint Protector 2009 verringert das Risiko der internen Bedrohung durch mobile Speichermedien wie beispielsweise Datendiebstahl, Datenverlust oder Vireninfectionen.

#### Überwachte Gerätetypen:

- USB Sticks  
(Normale USB Sticks, U3, etc.)
- Speicherkarten  
(SD, MMC, CF, etc.)
- CD/DVD-Spieler/Brenner  
(intern und extern)
- Externe Festplatten
- Floppy Laufwerke
- Kartenleser (intern und extern)
- ZIP Laufwerke
- Digitalkameras
- Smartphones/BlackBerry/PDAs
- iPods / iPhone
- FireWire Geräte
- MP3 Player/Media Player Geräte
- Biometrische Geräte
- Bluetooth Geräte
- Drucker
- ExpressCard (SSD)
- Wireless USB

#### Endpoint Protector 2009 Firewall zwischen PC und Geräten

Endpoint Protector ermöglicht den Unternehmen, eigene Richtlinien, gesetzliche Vorgaben oder Standards in Bezug auf die Verwendung von tragbaren Datenspeichern durchzusetzen.



Erzwungene Verschlüsselung mit Trusted Device Technologie.



#### Endpunktsicherheit für PCs, Notebooks und Netbooks

Sicherheitslücken, die von tragbaren Datenträgern ausgehen, wie vorsätzlicher Diebstahl, unbeabsichtigter Datenverlust oder Vireninfection von Daten, werden geschlossen.

#### Gerätemanagement / Geräteüberwachung / Regelasistent

Verwaltung von Geräten, Benutzern und Zugriffsberechtigungen.

#### Zentrales web-basiertes Management / Dashboard

Die zentrale Verwaltung aller tragbarer Datenspeicher (das „Dashboard“) liefert den Überblick zu allen wichtigen Informationen für IT-Mitarbeiter und Management. Verdächtige Aktivitäten werden automatisch erkannt und können auch automatisch als E-Mail „Alert“ gemeldet werden.

#### Dateiprotokollierung / Datenmitschnitt

Die *Dateiprotokollierung* („File Tracing“) zeichnet jeden Datentransfer von und zu mobilen Datenträgern auf. Der *Datenmitschnitt* (File Shadowing) zeichnet eine gespiegelte Kopie der transferierten Daten auf. So entsteht ein lückenloser Bericht mit Dateinamen, Zeitstempel, Benutzerdaten und ggf. mit der Datei selbst.

#### Datei Whitelist-Verfahren

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

#### Geräteprotokoll

Für Audits und Revisionen wird ein lückenloses Protokoll geführt. Erfasst werden alle mobilen Datenträger, die mit dem PC verbunden waren.

#### Reports und Analysen

Aussagekräftige Reporte, Grafiken und Analysewerkzeuge.

#### Einfache Umsetzung von Sicherheitsrichtlinien (Active Directory)

Vereinfachte Umsetzung von netzwerkweiten Sicherheitsrichtlinien durch Abstimmung mit Active Directory GPOs.

#### Netzwerk-Offline-Modus für mobile Benutzer

Rechner ohne Kontakt zum Netzwerk/Server sind weiterhin geschützt. Die vom Server festgelegten „Policies“ bleiben auch offline erhalten.

#### Endpoint Protector Client Administratoren Passwort

PC-Benutzer mit Admin-Rechten können den Schutz nicht umgehen.

Pro-aktives Management aller Geräte, die im Unternehmen eingesetzt werden.

## SYSTEMANFORDERUNGEN

### Client

- Windows 7 (32/64bit)
- Windows Vista (32/64bit)
- Windows XP (SP2) (32/64bit)
- Windows 2003/2008 (32/64bit)
- Mac OS X 10.4+
- .Net 2.0 Framework
- min. 32 MB HDD Speicher

### Server

Unterstützte Betriebssysteme:

- Windows 2003 Server
- Windows 2008 Server
- Debian (\*Ubuntu), Red Hat (Fedora, CentOS), Suse

Unterstützte Webserver:

- IIS 6.0 / IIS 7.0 oder
- Apache (Version 5+)

Unterstützte Datenbanken:

- Microsoft SQL 2005/2008 (Exp.)
- Oder MySQL (Version 5+)

Zusätzliche Server Anforderungen:

- PHP (Version 5) mit SOAP
- OpenSSL Version 0.9.8

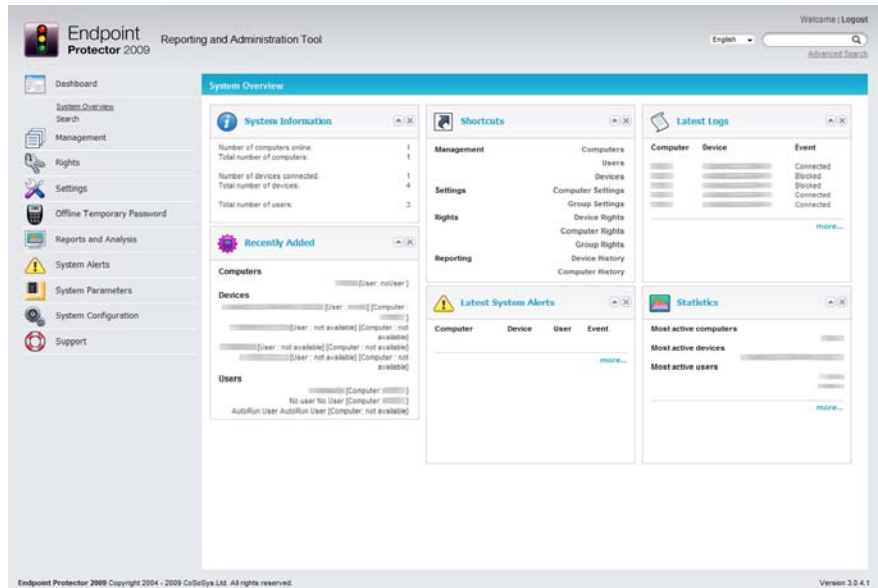
### Directory Service

- Active Directory

Einfaches Setup durch MSI Verteiler Mechanismen.

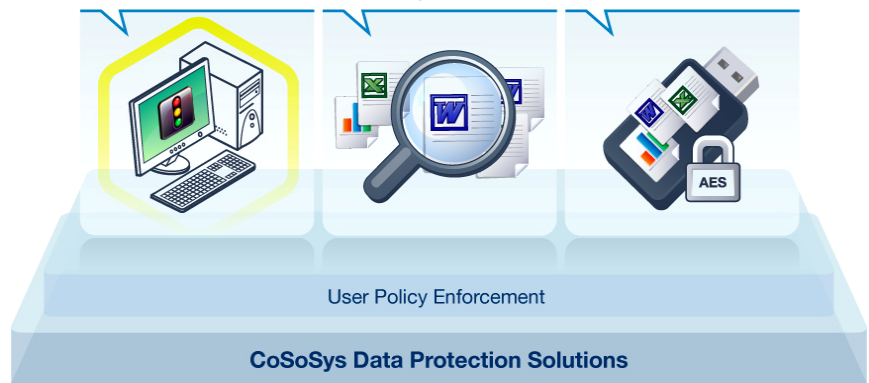
Endpoint Protector Server kann auf verschiedenen Betriebssystemen installiert werden. Dadurch ist eine kostengünstige Installation in die existierende Infrastruktur gegeben.

Die intuitive web-basierte Bedienoberfläche ermöglicht einen effektiven Betrieb und Management.



Endpoint Protector 2009 Dashboard  
Report- & Administrations-Ansicht

- Endpoint Security
- Data Loss Prevention
- Portable Device Management
- Data Theft Prevention
- Data Monitoring
- Analysis & Reporting
- Data Transfer Monitoring
- File Tracing
- Data Encryption and Sync
- Protecting sensitive data in transit



Endpoint Protector 2009 ist auf einer Drei-Säulen-Architektur aufgebaut.  
Prävention – Überwachung – Verschlüsselung

Erzwungene Verschlüsselung – schützt Daten auf tragbaren Datenträgern – TrustedDevice Technologie  
Endpoint Protector sorgt mit dem Zusatzmodul *EasyLock* dafür, dass Daten auf tragbaren Speichermedien zwingend verschlüsselt werden. Geht der USB Datenträger verloren oder wird gestohlen, sind die Informationen geschützt (256bit AES Verschlüsselung).

Besuchen sie [www.EndpointProtector.de](http://www.EndpointProtector.de) für eine kostenlose Testversion und weitere Informationen



#### CoSoSys Deutschland

E-Mail: [sales.de@cososys.com](mailto:sales.de@cososys.com)  
Phone: +49-7541-978-2627-0  
Fax: +49-7541-978-2627-9

#### CoSoSys North America

[sales.us@cososys.com](mailto:sales.us@cososys.com)  
+1-208-850 7563

#### CoSoSys Ltd.

[sales@cososys.com](mailto:sales@cososys.com)  
+40-264-593110  
+40-264-593113



© Copyright 2004-2010 CoSoSys Ltd. All rights reserved. Lock it Easy, Surf it Easy, Carry it Easy, Carry it Easy +Plus, Carry it Easy +Plus Bio, Secure it Easy, TrustedDevices, TrustedLogin, EasyLock, My Endpoint Protector and Endpoint Protector are trademarks of CoSoSys Ltd. Other brand names mentioned herein are for identification purposes only and may be trademarks of their respective holder(s).