Endpoint Protector Appliance™

Device Control / Data Loss Prevention appliance for PCs and MACs

Out-of-the-Box, Endpoints secured against device threats

The Endpoint Protector Appliance provides a policy based approach to enforce the rules for portable device use on endpoints.
It is the only solution to offer protection for PCs and MACs.
Portable devices are transforming the way we work and live. The whitelist based approach allows the use of specific devices for certain users/groups so that they stay productive while maintaining control of what devices are used and what data users are allowed to transfer.
Endpoint Protector Appliance dramatically reduces the risks posed by internal threats that could lead to data being leaked, stolen, damaged or otherwise compromised.

Controlled Device Types:

- *USB Flash Drives (Normal USB Drives, U3, etc.)**
- *Memory Cards (SD, MMC, CF, etc.)**
- *CD/DVD-Player/Burner (internal and external)**
- *external HDDs**
- *Floppy Drives*
- *Card Readers (internal, external)**
- *ZIP Drives*
- *Digital Cameras**
- *Smartphones/BlackBerry/PDAs*
- *iPhones / iPads / iPods**
- *FireWire Devices**
- *MP3 Player/Media Player Devices**
- *Biometric Drives*
- *Bluetooth Devices*
- *Printers*
- *ExpressCards (SSD)*
- *Wireless USB*
- *Serial Port*

Endpoint Protector Appliance is the Firewall between Computer and Devices

Endpoint Protector enables companies to better comply with internal device usage policies, regulations and standards regarding data security, data breach management and IT governance.

Info Security Products Guide 2011 GLOBAL EXCELLENCE FINALISTS AWARDS

COSOSYS

Endpoint Security as an appliance for PCs and MACs

Protection against threats posed by removable portable devices. Stops intentional or accidental leakage, theft, loss, or malware infection of data.

Device Management / Device Control*

Defines the rights for devices / users or computers in your network.

Centralized web based Management / Dashboard

Centrally manages the use of removable portable devices. The web based Administrative & Reporting interface meets the needs of management and IT security staff and offers real-time information about organization wide controlled devices and data transfer activity.

File Tracing* / File Shadowing

File Tracing records all data that was copied to and from previously authorized devices. *File Shadowing* saves a copy of all files, even of deleted ones, that were used in connection with controlled devices.

File Whitelisting

Only authorized files can be transferred to authorized devices. All other files are blocked and attempted transfers are reported.

Device Activity Logging – Audit Trail

Device activity logs are saved for all clients and devices connected giving a history of devices, PCs and users for audits and detailed analysis.

Reporting and Analysis

Powerful reports, graphics and analysis tool to easily review activity.

Easy Enforcement of Your Security Policies (Active Directory)

Simplified device management policies with customizable templates for defined User Groups (Active Directory GPOs) allow easy enforcement and maintenance of security policies across your network.

Temporary Offline Password* / Network "Offline" Mode

Secured PCs that are disconnected from the network stay protected. To keep productive on the road, devices can be temporarily allowed via the Temporary Offline Password functionality.

Endpoint Protector Client Self Defense

Provides protection even on PCs where users have Administrative rights.

Enforce endpoint security policies and take control of how and by whom data can be transferred.

SYSTEM REQUIREMENTS

Client(s)

- *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 of HDD Space*

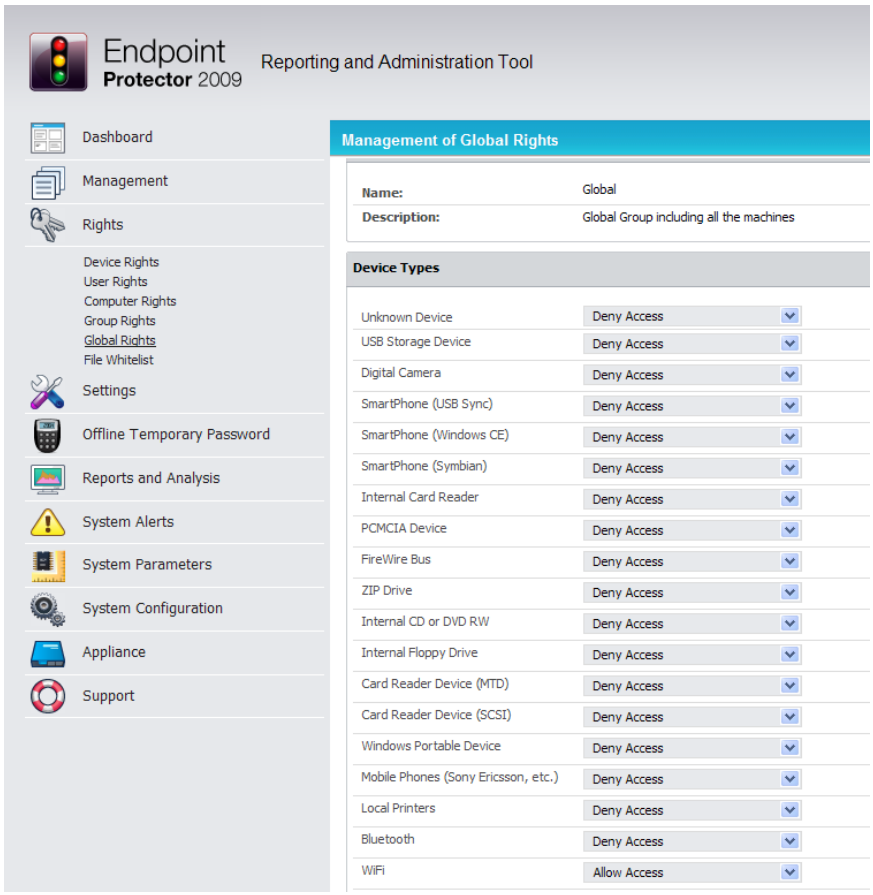
Directory Service

- *Active Directory*

Easy setup through automatically configured MSI deployment mechanisms.

Endpoint Protector Appliance includes the all required Server Hardware. Simply unpack and connect to your network, distribute clients to PCs and MACs and within minutes all ports are secured against uncontrolled device use.

The intuitive web based administrative interface allows an efficient management.



Endpoint Protector Appliance web-based interface Reporting & Administration Tool

Models	A50	A100	A250	A1000	A4000
Protection for Computer (PC / MAC)	50	100	250	1000	4000
Addition capacity	25	50	125	500	2000
Housing (Rack mount)	1U	1U	1U	1U	3U
Processor	ULV Dual Core	ULV Dual Core	Quad Core	Quad Core	2x Quad Core
Hard Drive	160 GB	320 GB	500 GB	2x 1 TB (Raid 1)	6x 1 TB (Raid 5)
Power Supply	200W, 100-240V	200W, 100-240V	260W, 100-240V	260W, 100-240V	2x 800W, 100-240V
Hardware Warranty	2-year included. Additional warranty and replacement options are available.				

Enforced Encryption - protecting sensitive data in transit with EasyLock

The TrustedDevice technology with the optional EasyLock software is designed to certify that in the protected environment all the portable devices are not only authorized and controlled via security policies, but also certified and trusted for protecting sensitive and confidential data in transit. This will assure that, in the event a device is stolen or lost, all the data stored on it is encrypted and therefore not accessible for other parties.

Visit **www.EndpointProtector.com** for a free trial and more information

CoSoSys Ltd.
E-Mail: sales@cososys.com
Phone: +40-264-593110
Fax: +40-264-593113

CoSoSys North America
sales.us@cososys.com
+1-208-850 7563

CoSoSys Germany
sales.de@cososys.com
+49-7541-978-2627-0
+49-7541-978-2627-9

Created on 14 December 2010