

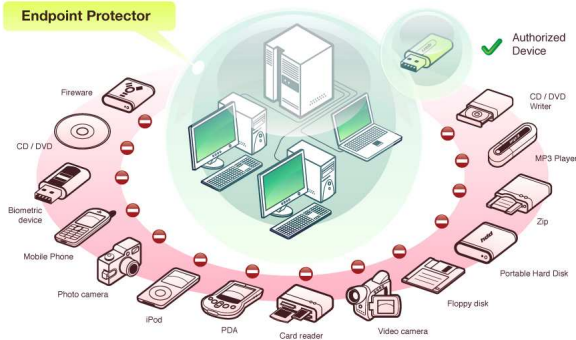


Endpoint Protector 2008™

Prevent data leakage in sensitive business environments

32bit Client Version: 2.3.4.3
 Windows 32bit Server Version: 2.2.4
 Linux 32bit Server Version: 2.2.2

Your sensitive data is only as safe as your endpoints are.



Endpoint Protector 2008 complements signature-based security solutions and provides a policy based approach to enforcing your rules of use for endpoint devices. In a world where portable and lifestyle devices are increasingly transforming the way we work and live, Endpoint Protector 2008 is designed to maintain productivity and make work and life more convenient, secure and enjoyable. The whitelist based approach allows the use of specific devices for certain users/groups so they stay productive while maintaining control of what devices are used, and what data users are transferring to and from devices. Endpoint Protector 2008 dramatically reduces the risk posed by internal threats that could lead to your confidential data being leaked, stolen, damaged or otherwise compromised.

Controlled Endpoint Device Types:

- USB Flash Drives
(Normal USB Drives, U3, etc.)
- Wireless USB
- Memory Cards
(SD, MMC, CF, etc.)
- Card Readers
(internal and external)
- ZIP Drives
- Floppy Drives
- CD/DVD-Player/Burner
(internal and external)
- Digital Cameras
- Smartphones/Handhelds/PDAs
- iPods
- external HDDs
- FireWire Devices
- MP3 Player/Media Player Devices
- Biometric Drives

Endpoint Protector 2008 acts like a Firewall between PC and the controlled devices

The Endpoint Protector 2008 set of features enables companies to better comply with internal device usage policies, government regulations, standards regarding security responsibility, data breach management and IT governance.



Enforcing encryption at endpoints by using TrustedDevices.



Endpoint Security for Workstations and Notebooks

Protects PCs from threats posed by removable portable storage and endpoint devices like USB Flash Drives, iPods, internal CD/DVD-Player/Burner, Floppy Drives and other devices that could be intentionally or accidentally used to leak, steal, lose, virus or malware infect your data. Even self-executing devices like USB Drives with CD-ROM autorun feature such as U3 Drives will not be accessible and pose no threats.

Centralized web based Device Management / Dashboard

Network administrators have the ability to centrally manage and authorize the use of devices. The Endpoint Protector 2008 Dashboard is designed to meet the needs of both management and security staff and offer access to real-time information, charts and reports about organization wide controlled devices and data transfer activity. All in an integrated single view web based Administration and Reporting Tool.

Control your data flow: File Tracing / File Shadowing

This thorough record of information streams at the network's endpoints is supporting audits of data flow and controlling the impact of data leakage. The *File Tracing* feature will track all data that was copied to and from prior authorized portable storage devices. The *File Shadowing* feature saves a copy of all, even deleted files that were used in connection with controlled devices on a network storage server.

Device Activity Logging – Audit Trail

A device activity log is saved for all clients and devices connected along with all administrative actions such as device authorizations, giving a history for devices, PCs and users for future audits and detailed analysis.

Reporting and Analysis Tools

Endpoint Protector 2008 is equipped with powerful reporting and analysis tools to make the data audit processes easy and straightforward.

Easy Enforcement of Your Security Policies (Active Directory)

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

Network "Offline" Mode to Support Your Field Employees

Protected PCs that are temporary or frequently disconnected from the network like laptops stay protected based on the last locally saved policy. All notifications are transmitted at the next network connection.

Enforce endpoint security policies and know by whom and how data is transferred.

SYSTEM REQUIREMENTS

Client(s)

- Windows Vista (32 bit)
- Windows XP (SP2) (32 bit)
- Windows 2003 (32 bit)
- .Net 2.0 Framework
- min. 32 MB of HDD Space

Server

Supported Operating Systems:

- Windows 2003 Server or
- Debian, Red Hat (and other Linux Distributions)

Supported Web servers:

- IIS 6.0 or
- Apache (Version 5 or newer)

Supported Databases:

- Microsoft SQL 2005 (Express) or
- MySQL (Version 5 or newer)

Additional Server Requirements:

- PHP (Version 5) with SOAP support
- OpenSSL Version 0.9.8

Directory Service

- Active Directory

Easy setup through established MSI deployment mechanisms.

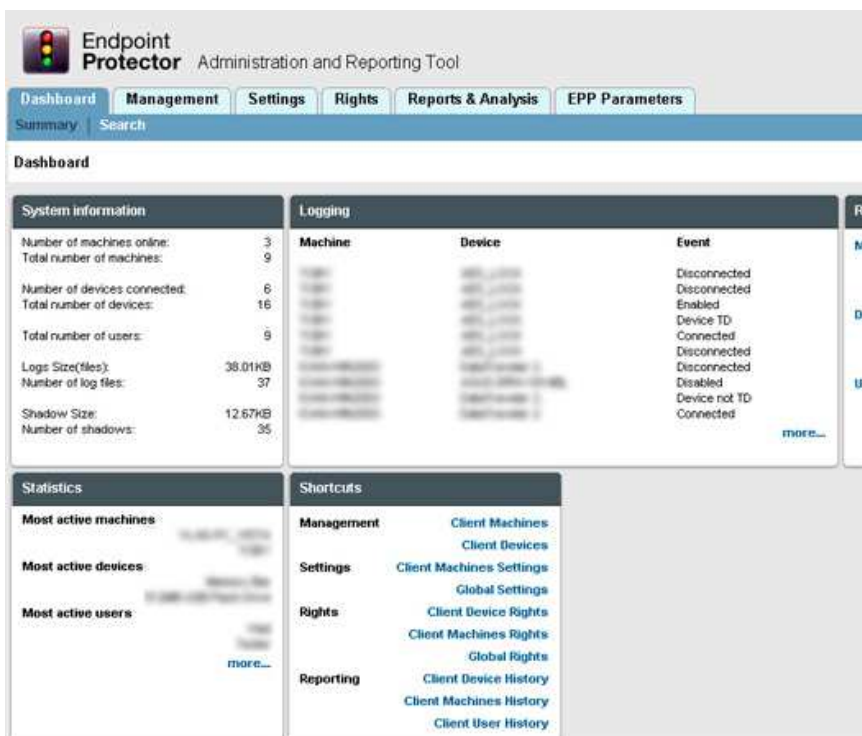
The Endpoint Protector 2008 server is compatible with different server platforms to assure a fast and cost efficient integration with your existing infrastructure.

The intuitive web based administrative interface allows efficient management.

- 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 2008 is built on a three Pillar Security Architecture. Prevention - Monitoring - Encryption



Endpoint Protector offers you a safe and secure working environment with portable storage and endpoint devices. User efficiency is not restricted since any authorized device can be used continuously on protected PCs while the networks endpoint security policy is enforced.

TrustedDevice / Enforced Encryption - protecting sensitive data in transit

The technology behind TrustedDevices is designed to certify that in the corporate environment all the endpoint devices are not only authorized and controlled via endpoint software and 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.



Computer Communications Limited

E-Mail: sales@ccl.co.uk
 Phone: +44-844-8732668
 Fax: +44-844-8732669



© Copyright 2004-2008 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 and Endpoint Protector are trademarks of CoSoSys SRL. Other brand names mentioned herein are for identification purposes only and may be trademarks of their respective holder(s).