ENDPOINT PROTECTOR | by CoSoSys

DATASHEET 5.2.0.5

Data Loss Prevention & Mobile Device Management

Suitable for any network size and any industry

DLP for Windows, Mac and Linux

Protecting the entire network

ENDPOINT PROTECTOR

by CoSoSys

Out-of-the-Box Solution to secure sensitive data from threats posed by portable storage devices, cloud services and mobile devices

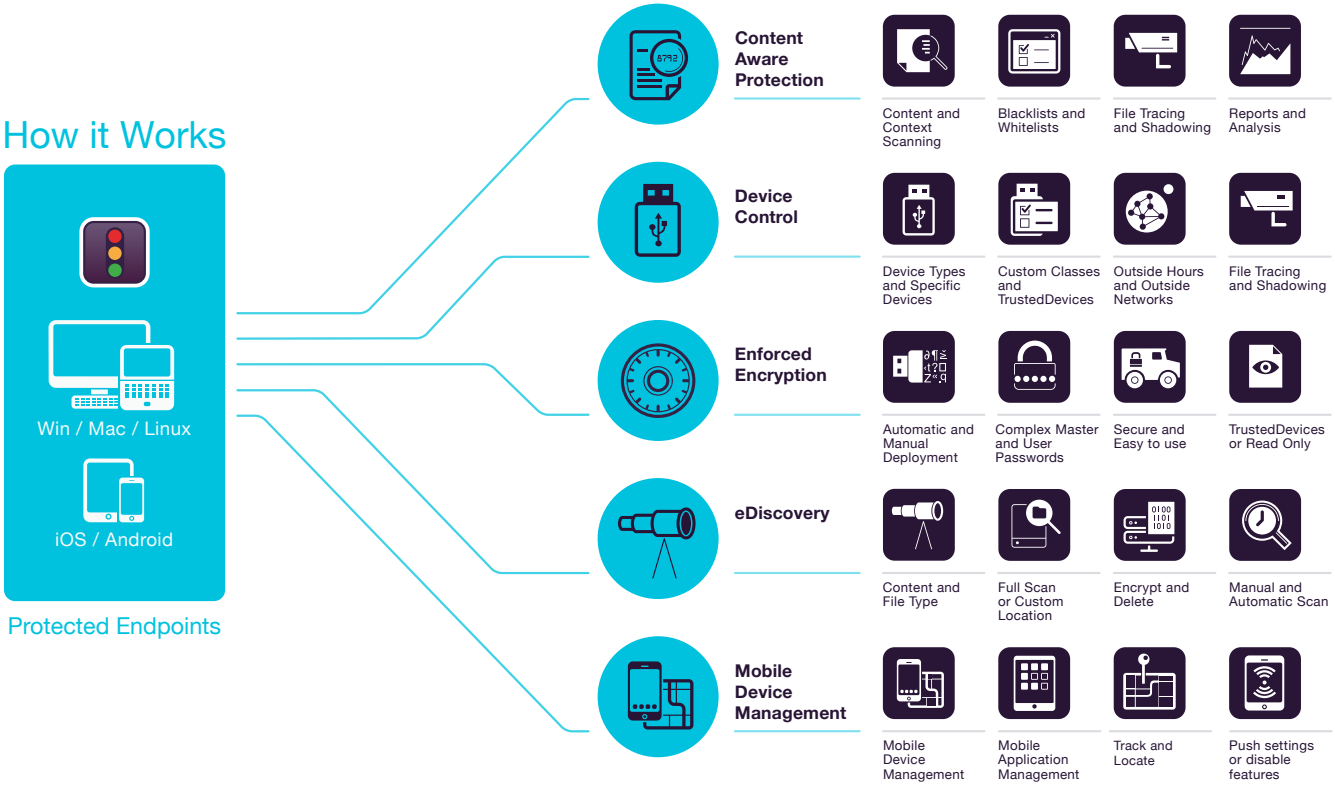
In a world where portable, lifestyle devices, and the cloud are transforming the way we work and live, Endpoint Protector is designed to protect confidential data against insider threats, while maintaining productivity and making work more convenient, secure and enjoyable.

The blacklist and whitelist-based approach grants flexibility in policy building. Organizations have the option to prohibit the use of specific removable devices and data transfers to file cloud sharing applications and other online services, to scan for certain PIIs, but to allow transfers to specific URLs and domain names for certain computers/users/groups, avoiding task interruption.

With Endpoint Protector being offered as hardware or virtual appliance, it can be setup in minutes. Moreover, the responsive management interface allows managing policies and checking reports from any device, from desktop to tablet.

Endpoint Protector dramatically reduces the risks posed by internal threats that could lead to data being leaked, stolen, or otherwise compromised. In addition to these, compliance with various rules and regulations is also met.

How it Works



Content Aware Protection
for Windows, macOS and Linux

Monitor and Control data in motion, deciding what confidential files can or cannot leave the company via various exit points. Filters can be set per File Type, Application, Predefined and Custom Content, Regex and more.

Device Control
for Windows, macOS and Linux

Monitor and Control USBs and peripheral ports. Set Rights per Device, User, Computer, Group or Globally.

Enforced Encryption
for Windows and macOS

Automatically secure data copied on USB storage devices with an AES 256bit encryption. Cross-platform, password-based, easy to use and very efficient.

eDiscovery
for Windows, macOS and Linux

Scan data at rest on network's endpoints and apply remediation actions such as encrypt or delete in case confidential data is identified on unauthorized computers.

Mobile Device Management
for Android, iOS and macOS

Manage, Control and Adjust the security level on smartphones and tablets. Push security settings, network settings, applications, etc.

Content Aware Protection

for Windows, macOS and Linux

Email Clients: Outlook / Thunderbird / Lotus Notes • Web Browsers: Internet Explorer / Firefox / Chrome / Safari • Instant Messaging: Skype / Microsoft Communicator / Yahoo Messenger • Cloud Services & File Sharing: Dropbox / iCloud / SkyDrive / BitTorrent / Kazaa • Other Applications: iTunes / Samsung Kies / Windows DVD Maker / Total Commander / Team Viewer • OTHERS

Exit Points Blacklists
Filters can be set based on a large list of monitored applications. USB storage devices, network shares and other exit points can be monitored for content.

File Type Blacklists
File Type Filters can be used to block specific documents based on their extension, even if these are manually modified by users.

Predefined Content Blacklists
Filters can be created based on predefined content such as Credit Card Numbers, Social Security Numbers and many more.

Custom Content Blacklists
Filters can also be created based on custom content such as keywords and expressions. Various Blacklist Dictionaries can be created.

File Name Blacklists
Filters based on file names can be created. They can be set based on the file name and extension, just the name or just the extension.

File Location Blacklists and Whitelists
Filters based on files' location on the local HDD. These can be defined to include or exclude containing subfolders.

Regular Expressions Blacklists
Advanced custom filters can be created to find a certain recurrence in data transferred across the protected network.

Allowed File Whitelists
While all other attempted file transfers are blocked, whitelists can be created to avoid redundancy and increase productivity.

Domain & URL Whitelisting
Enforce company policies but allow employees the flexibility they need to do their work. Whitelist company portals or email addresses.

Print Screen and Clipboad Monitoring
Revoke screen capture capabilities. Eliminate data leaks of sensitive content through Copy & Paste / Cut & Paste, enhancing the data security policy.

Optical Character Recognition
Inspect content from photos and images, detecting confidential information from scanned documents and other similar files.

File Tracing and File Shadowing
Record all file transfers or attempts to various online applications and other exit points. Have a clear view of actions by saving a copy of the files.

Threshold for Filters
Define up to which number of violations a file transfer is allowed. It applies to each type of content or to the sum of all violations.

Transfer Limit
Set a transfer limit within a specific time interval. It can be either based on the number of files or file size. E-mail alerts when the limit is reached are available.

Contextual Content Scanning
Enable an advanced inspection mechanism for a more accurate detection of sensitive content such as PIIs. Context customization is available.

Offline Temporary Password
Temporarily allow file transfers to computers disconnected from the network. Ensure security and productivity.

Dashboards, Reports and Analysis
Monitor activity related to file transfers with a powerful reporting and analysis tool. Logs and reports can also be exported to SIEM solutions.

Compliance (GDPR, HIPAA, etc.)
Become compliant with industry rules and regulations like PCI DSS, GDPR, HIPAA etc. Avoid fines and other prejudices.

DLP for Printers
Policies for local and network printers to block printing of confidential documents and prevent data loss and data theft.

DLP for Thin Clients
Protect data on Terminal Servers and prevent data loss in Thin Client environments just like in any other type of network.

Additional Features / Many other features are also available. / info@endpointprotector.com

Device Control

for Windows, macOS and Linux

USB Drives / Printers / Bluetooth Devices / MP3 Players / External HDDs / Teensy Board / Digital Cameras / Webcams / Thunderbolt / PDAs / Network Share / FireWire / iPhones / iPads / iPods ZIP Drives / Serial Port / PCMCIA Storage Devices / Biometric Devices / OTHERS

Set Rights Granularly

Device Rights can be configured globally, per group, computer, user and device. Use default settings or adjust as needed.

Device Types and Specific Device

Set rights - deny, allow, read only, etc. - for Device Types or Specific Devices (using VID, PID and Serial Number).

Custom Classes

Rights can be created based on classes of devices making management easier for products from the same vendor.

Outside Hours Policies

Device Control Policies can be set to apply when outside normal working hours. Business hours start & end time and working days can be set.

Outside Network Policies

Device Control Polices can be set to apply when outside the company's network. Enforcement is based on DNS Domain Names and IP Addresses.

Active Directory Sync

Take advantage of AD to make large deployments simpler. Keep entities up to date, reflecting the network groups, computers and users.

Users and Computers Information

Gain a better visibility with information such as Employee IDs, Teams, Location, accurate contact details and more (IPs, MAC Addresses, etc.)

File Tracing

Record all file transfers or attempts to various USB storage devices, providing a clear view on users' actions.

File Shadowing

Save a copy of files that were transferred to controlled devices that can later be used for auditing purposes.

Offline Temporary Password

Temporarily allow device access to computers disconnected from the network. Ensure security and productivity.

Create E-mail Alerts

Predefined and Custom e-mail alerts can be set up to provide information on the most important events related to device use.

Dashboard and Graphics

For a quick visual overview of the most important events and statistics, graphics and charts are available.

Reports and Analysis

Monitor all activity related to device use with a powerful reporting and analysis tool. Logs and reports can also be exported.

Additional Features

Many other features are also available.
info@endpointprotector.com

Enforced Encryption

for Windows and macOS

256bit AES Goverment approved encryption / Anti-tampering techniques / Application integrity / Send messages to users / Restore to factory default / Password policy settings / others

USB Enforced Encryption

Authorize only encrypted USB devices and ensure all data copied on removable storage devices is automatically secured.

Automatic deployment and Read Only

Both automatic and manual deployment is available. The option to allow Read Only rights until encryption is needed is also possible.

Complex Master and User Passwords

The password complexity can be set as needed. The Master Password provides continuity in circumstances like users' password resets.

Additional Features

Encryption is also available for Cloud Storage, Local Folders, CDs & DVDs
info@endpointprotector.com

eDiscovery

for Windows, macOS and Linux

File type: Graphic Files / Office Files / Archive Files / Programming Files / Media Files / etc. • Predefined Content: Credit Cards / Personally Identifiable Information / Addresses / SSNs / IDs / Passports / Phone Numbers / Tax IDs / Health Insurance Numbers / etc. • Custom Content / File Name / Regular Expression / HIPAA / etc.

Encrypt and Decrypt Data
Data at rest containing confidential information can be encrypted to prevent unauthorized employees' access. Decryption actions are also available.

Delete Data
If clear violations of the internal policy occur, delete sensitive information as soon as it is detected on unauthorized endpoints.

Scan Location Blacklists
Filters can be created based on predefined locations. Avoid redundant scanning for data at rest with targeted content inspections.

Automatic Scans
In addition to the Clean and Incremental Scans, Automatic Scans can be scheduled – either one time or recurring (weekly or monthly).

File Tracing
Record all file transfers or attempts to various online applications and cloud services, providing a clear view of users' actions.

Reports and Analysis
Monitor logs relating to scanning data at rest and take remediation actions as needed. Logs and reports can also be exported to SIEM solutions.

Threshold for Filters
Define up to which number of violations a file transfer is allowed. It applies to each type of content or to the sum of all violations.

Compliance (GDPR, HIPAA, etc.)
Become compliant with industry rules and regulations like PCI DSS, GDPR, HIPAA etc. Avoid fines and other prejudices.

SIEM Integration
Leverage Security Information and Event Management products by externalizing logs. Ensure a seamless experience across security products.

File Type Blacklists
File Type Filters can be used to block specific documents based on their extension, even if these are manually modified by users.

Predefined Content Blacklists
Filters can be created based on predefined content such as Credit Card Numbers, Social Security Numbers and many more.

Custom Content Blacklists
Filters can also be created based on custom content such as keywords and expressions. Various Blacklist Dictionaries can be created.

File Name Blacklists
Filters based on file names can be created. They can be set based on the file name and extension, just the name or just the extension.

File Location Blacklists and Whitelists
Filters based on files' location on the local HDD. These can be defined to include or exclude containing subfolders.

Regular Expressions Blacklists
Advanced custom filters can be created to find a certain recurrence in data transferred across the protected network.

Allowed File Whitelists
While all other attempted file transfers are blocked, whitelists can be created to avoid redundancy and increase productivity.

Domain & URL Whitelisting
Enforce company policy but allow employees the flexibility they need to do their work. Whitelist company portals or email addresses.

MIME Type Whitelist
Avoid redundant scanning at a global level by excluding content inspection for certain MIME Types.

Mobile Device Management

for Android, iOS and macOS

Over-the-air Enrollment for iOS & Android

Devices can be remotely enrolled via SMS, E-mail, URL link or QR Code. Pick the most convenient way for your network.

Bulk Enrollment

For an efficient deployment process, up to 500 smartphones and tablets can be enrolled at the same time.

Remote Lock

Remotely enable instant locking of mobile devices in case of any related incidents. Avoid data leaks due to lost or misplaced devices.

Track & Locate

Closely monitor company's mobile devices and know at all times where your company sensitive data is.

Disable built-in functionalities

Control the permissions for built-in features such as camera, avoiding data breaches and loss of sensitive data.

Play Sound to locate lost devices

Locate a misplaced mobile device by remotely activating a loud ringtone until it is found (only supported for Android).

Mobile Application Management

Manage apps accordingly to the organization's security policies. Instantly push free and paid apps to enrolled mobile devices.

Push Network Settings

Push network settings like E-mail, Wi-Fi and VPN settings or disable them, including Bluetooth, set ringer mode, etc.

Alerts

Extended Predefined System Alerts are available, as well as the option to set up Custom System Alerts.

Reports and Analysis

Monitor all users' activity related to device use with a powerful reporting and analysis tool. Logs and reports can also be exported.

Kiosk Mode with Samsung Knox

Lock or contain the mobile device into specific apps. Remotely enforce security on the mobile fleet and turn them into dedicated devices.

macOS Management

To extend the DLP features, Macs can also be enrolled into the MDM module, taking advantage of additional management options.

Password Enforcement

Proactive protection of company critical data stored on mobile devices by enforcing strong password policies.

Remote Wipe

For critical situations where the only way to avoid data leaks is wiping the device, this can easily be done remotely.

Geofencing

Define a virtual perimeter on a geographic area, gaining a better control of the MDM policies that apply only in a specific area.

iOS Restrictions

Make sure only business related use is possible. If not compliant to company policy, disable iCloud, Safari, App Store, etc.

Push vCards on Android

Add and push contacts for Android mobile devices, making sure your mobile workforce can quickly get in touch with the right people.

App Monitoring

Know what apps your employees are downloading on their mobile devices, keeping a discreet line between work and leisure.

Asset Management

Gain insight into the mobile device fleet about Device Names, Types, Models, Capacity, OS Versions, Carriers, IMEIs, MACs, etc.

Create E-mail Alerts

Email alerts can be set up to provide information on the most important events related to mobile devices' use.

Dashboard and Graphics

For a quick visual overview on the most important events and statistics, graphics and charts are available.

Additional Features

Many other features are also available.
info@endpointprotector.com

100% Deployment Flexibility

Suitable for any type of network, our products can be used by enterprise customers, small and medium businesses and even home users. With a client-server architecture, they are easy to deploy and centrally manage from the web-based interface. Besides the Hardware and Virtual Appliance, Amazon Web Services Instance and Cloud version, a Stand-alone version is also available for those looking for basic features.

Endpoint Protector

Content Aware Protection, eDiscovery, Device Control, and Encryption are available for computers running on different Windows, macOS and Linux versions and distributions. Mobile Device Management and Mobile Application Management are also available for iOS and Android mobile devices.

My Endpoint Protector

Content Aware Protection, Device Control and Encryption are available for computers running on Windows and Mac. Mobile Device Management and Mobile Application Management are available for iOS and Android mobile devices.

Hardware Appliance

Virtual Appliance

Amazon Instance

Cloud Solution

Modules

		Protected Endpoints					
Windows	Windows 7 / 8 / 10	(32/64 bit)	●	●	●	●	
	Windows Server 2003 - 2016	(32/64 bit)	●	●	●	●	
	Windows XP / Windows Vista	(32/64 bit)	●	●	●	●	
macOS	macOS 10.14	Mojave	●	●	●	●	
	macOS 10.13	High Sierra	●	●	●	●	
	macOS 10.12	Sierra	●	●	●	●	
	macOS 10.11	El Capitan	●	●	●	●	
	macOS 10.10	Yosemite	●	●	●	●	
	macOS 10.9	Mavericks	●	●	●	●	
	macOS 10.8	Mountain Lion	●	●	●	●	
	macOS 10.7	Lion	●	●	●	●	
Linux	Ubuntu		●	●	●	n/a	
	OpenSUSE / SUSE		●	●	●	n/a	
	CentOS / RedHat		●	●	●	n/a	
	Fedora		●	●	●	n/a	
iOS	iOS 4, iOS 5, iOS 6, iOS 7, iOS 8, iOS 9, iOS 10, iOS 11, iOS 12						●
Android	Jelly Bean (4.1+), KitKat (4.4+), Lollipop (5.0+), Marshmallow (6.0+), Nougat (7.0+), Oreo (8.0+), Pie (9.0+)						●

*Please check for details regarding supported versions and distributions on endpointprotector.com/linux

COSOSYS

HQ (Romania)

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

Germany

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

Korea

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

North America

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

Official Partner