ENDPOINT PROTECTOR | by CoSoSys

DATASHEET 5.5.0.0

Industry-Leading Data Loss Prevention (DLP)

Enterprise-grade security solution for any industry

DLP for Windows, macOS and Linux

Protecting the entire network

ENDPOINT PROTECTOR | by CoSoSys

Our advanced Data Loss Prevention (DLP) solution puts an end to data leaks and data theft while offering control of portable storage devices and ensuring compliance with data protection regulations.

It is designed to protect confidential data against insider threats while maintaining productivity and making work more convenient, secure, and enjoyable.

Endpoint Protector is an enterprise-grade DLP software for Windows, macOS and Linux computers, Thin Clients and Desktop-as-a-Service (DaaS) solutions. The solution is an ideal choice for companies running on multi-OS networks and it has a modular format that allows them to mix and match the right tools to serve specific needs.

By deploying it, organizations can safeguard personal information and meet compliance requirements for regulations such as the GDPR, HIPAA, LGPD, CCPA, PCI DSS, etc. Endpoint Protector also offers protection to the company's intellectual property and trade secrets.

Device Control

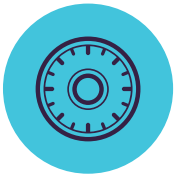
Lockdown, control, and monitor USB and peripheral ports to stop data theft and data loss. Set Rights per Device, User, Computer, Group or Globally.

Windows / macOS / Linux

Content Aware Protection

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

Windows / macOS / Linux



Enforced Encryption

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

Windows / macOS

eDiscovery

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.

Windows / macOS / Linux

Key Benefits

Easy to install and manage

Endpoint Protector can be up and running in 30 minutes. It is easy to run by both technical and non-technical personnel.

Predefined compliance profiles

With the predefined data protection policies, it is easy to find regulated data and to ensure compliance requirements of the GDPR, CCPA, HIPAA, PCI DSS and more.

Cross-platform protection

The solution offers the same security features and level of protection for Windows, macOS and Linux computers. It also supports Apple devices with Arm-based M1 processors.

Detailed reports of user activity

With Endpoint Protector it is possible to track, report and get valuable insights about what sensitive data is being transferred where and by whom.

Flexible deployment options

Endpoint Protector can be deployed in multiple ways, depending on the needs and existing infrastructure of the company.

Granular policies

Granular access rights for removable devices and peripheral ports, as well as security policies for users, computers, and groups, can be easily defined.

DLP for Enterprises

In the age of digital transformation and workstream collaboration platforms (WSC), addressing the risks of data loss and noncompliance is a must for enterprises, as the consequences of data breaches include not only hefty fines but legal problems and reputational damages also.
Endpoint Protector Enterprise comes with a more effective data security solution on the market, enabling enterprises to continuously identify, monitor, and control the data that they need to protect, wherever they are.

User remediation

Endpoint Protector Enterprise flavor adds more flexibility to security policies. Through the user remediation feature, end-users are allowed to self-remediate, meaning that after they justificate their activity, the transfer of specific sensitive information is allowed for a defined amount of time.

Management console

Data loss prevention policies can be easily set for the entire network from Endpoint Protector's centralized dashboard that offers an enhanced user experience.

Seamless integration

Our solution offers integration with Active Directory (AD) integration, and Security Information & Event Management (SIEM) technology. Integration with SIEM allows to transfer activity events to a SIEM server for analysis and reporting. With AD large deployments can be simpler.

Device Control

for Windows, macOS and Linux

USB Drives / Printers / Bluetooth Devices / CD & DVD / External HDDs / Teensy Board / Digital Cameras / Webcams / Thunderbolt / WiFi / Network Share / FireWire / iPhones / iPads / iPods ZIP Drives / Card Readers / Android Smartphones / USB Modems / 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. The rights can be applied to a type of device or can be device specific (based on VID, PID and Serial Number).

Custom Classes
Apply device rights based on Vendor ID and Product ID to make management easier for devices 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
Outside Network policies can be set to apply when outside the company's network. Enforcement is based on FQDN and DNS 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 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 of users' actions.

File Shadowing
Create shadow copies of files transferred to authorized devices for detailed audits.

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

Create E-mail Alerts
Get real time e-mail alerts for various events related to removable media usage on company computers.

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.

Transfer limit
Limit the number of files or the file size that can be transferred within a set time interval. Include or exclude transfers through devices, online applications, and network shares.

Enforced Encryption

for Windows and macOS

256bit AES military grade encryption / Anti-tampering techniques / Centralized password management / Send messages to users / Remote wipe / 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.

Password management and remote wipe
Change user passwords remotely and wipe encrypted data in case of compromised devices.

Content Aware Protection

for Windows, macOS and Linux

Email Clients: Outlook / Thunderbird / Apple Mail / Web Browsers: Internet Explorer / Firefox / Chrome / Safari / Instant Messaging: Skype / Slack / WhatsApp / Cloud Services & File Sharing: Dropbox / iCloud / OneDrive / BitTorrent / AirDrop / Other Applications: iTunes / FileZilla / SFTP / Total Commander / TeamViewer / OTHERS

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

File Type Denylists
File Type Filters can be used to block documents based on the true type of the file, even if users change the extension.

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

Predefined and Custom Content Denylists
Filters can be created based on predefined content such as Credit Card Numbers or Social Security Numbers and custom content such as keywords or expressions.

File Name Denylists
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 Denylists and Allowlists
Filters based on files' location on the local HDD. These can be defined to include or exclude subfolders.

Regular Expressions Denylists
A powerful tool to identify a sequence of characters that define a search pattern.

Outside Hours and Outside Network
Define and set fallback policies that will apply when outside working hours or outside the network.

Domain & URL Allowlists
Enforce company policies but allow employees the flexibility they need to do their work. Enable the DPI feature and create allowlists company portals or email addresses.

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

User Remediation
Empowers users to safely override a DLP policy and offers options to justify data transfers. Helps to Increase end-user accountability and awareness of sensitive data transfers in the organization.

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

Threshold for Filters
Advanced Content Detection Rules Define complex conditions for content scanning by combining multiple criteria (PIIs, dictionary words, regular expressions, etc.) using logical operators (AND/OR).

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 more accurate detection of sensitive content such as PIIs. Context customization is available.

Offline Temporary Password
Temporarily allow file transfers on 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. Get graphic reports for C level executives.

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 are available. Find out more by requesting a demo on 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 / OTHERS

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 Denylists

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).

Scan Results

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

Scanning Status

Easily check the current status of your scan. The scan status is displayed in the format 0-100%.

Threshold for Filters

Define the number of policy violations a file can contain for the security policy to be applied and the file reported to the server.

Compliance (GDPR, HIPAA, etc.)

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

File Type Denylists

File Type Filters can be used to discover documents based on the true type of the file, even if users change the extension.

Predefined Content Denylists

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

Custom Content Denylists

Filters can also be created based on custom content such as keywords and expressions. Various Denylist Dictionaries can be created.

File Name Denylists

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.

Regular Expressions Denylists

A powerful tool to identify sequence of characters that define a search pattern.

File Allowlists

While all other attempted file transfers are blocked, allowlists can be created to avoid redundancy and increase productivity.

MIME Type Allowlists

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

SIEM Integration

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

Additional features are available. Find out more by requesting a demo on EndpointProtector.com

100% Deployment Flexibility

Our products are enterprise-grade and continually evolving to best serve any type of network and industry. With a client-server architecture, they are easy to deploy and are centrally managed from the web-based interface. Besides the Virtual Appliance, the server can be hosted by us and in major cloud infrastructures like Amazon Web Services, Microsoft Azure or Google Cloud.

Multiple login options, including local accounts, on-premise Active Directory (AD) authentication, Azure AD and OKTA Single Sign-on (SSO) are available, are available, allowing simpler and easier control for admins. Multi-factor authentication (MFA) is also possible.

Device Control, Content Aware Protection, Enforced Encryption, and eDiscovery are available for computers running on different Windows, macOS and Linux versions and distributions.

Virtual Appliance

Cloud Services

Amazon Web Services
Microsoft Azure
Google Cloud

Cloud-Hosted

Gartner peerinsights™

Highly-rated in **Gartner Peer Insights** for enterprise data loss prevention solutions.

Protected Endpoints

Windows	Windows 7 / 8 / 10	(32/64 bit)	●	●	●	●
	Windows Server 2003 - 2019	(32/64 bit)	●	●	●	●
	Windows XP / Windows Vista	(32/64 bit)	●	●	●	●
macOS (kext and kextless agent)	Apple Silicon M1		●	●	●	●
	macOS 12.00	Monterey	●	●	●	●
	macOS 11.00	Big Sur	●	●	●	●
	macOS 10.15	Catalina	●	●	●	●
	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	●	●	●	●
Linux	Ubuntu		●	●	●	n/a
	OpenSUSE / SUSE		●	●	●	n/a
	CentOS / RedHat		●	●	●	n/a
	Fedora		●	●	●	n/a

*For more information on supported versions and distributions please check EndpointProtector.com/linux

Official Partner

COSOSYS

Romania

sales@cososys.com
+40 264 593 110 / ext. 103
+40 264 593 113 / ext. 202

Germany

vertrieb@endpointprotector.de
+49 7541 97826730
+49 7541 97826734 / ext. 202

North America

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