



**ENDPOINT
PROTECTOR**

MacSysAdmin
2019

What is DLP

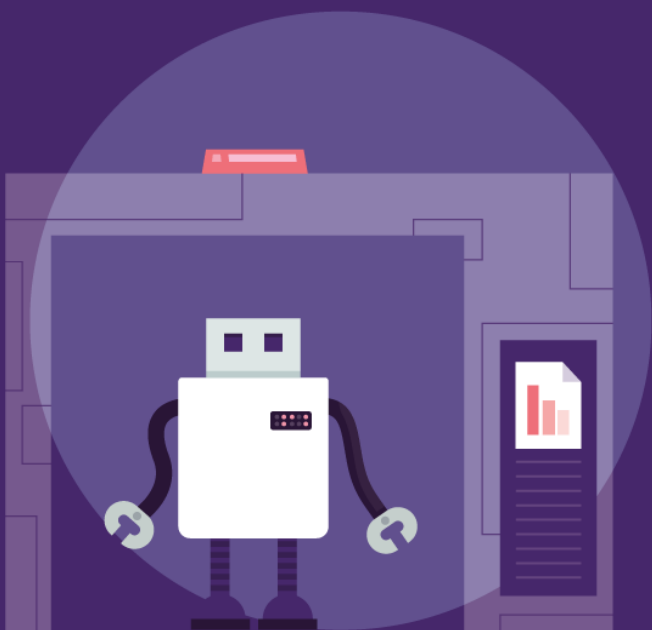
Why do we need DLP

How to choose a DLP solution for macOS

How Endpoint Protector can help

Why have a DLP solution?

endpointprotector.com



Concerns:

- | Data loss / Data leakage / Data theft
- | Uncontrolled use of devices in the workplace
- | Regulatory compliance
- | Protection of intellectual property
- | Mobile device management

Data Protection Regulations Worldwide

endpointprotector.com

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) requires health care providers and organizations to ensure the confidentiality and security of protected health information (PHI).

GDPR

The General Data Protection Regulation (GDPR) applies in all businesses and organizations established in the European Union, regardless whether the data processing takes place in the EU or not.

NIST 800-171

NIST 800-171 works as a guide for federal agencies to guarantee that Controlled Unclassified Information (CUI) is protected when processed, stored and used in non-federal information systems.

CCPA

The California Consumer Privacy Act (CCPA) will apply to businesses and organizations worldwide, if they receive personal data of California residents, directly or indirectly.

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is administrated by PCI Security Standards Council and applies to all entities that store, process or transmit cardholder data.

Choosing a DLP solution for macOS

endpointprotector.com



Zero-day support

Minimum device performance impact

Easy to update

Test for Kernel Panics

Feature parity between operating systems



**ENDPOINT
PROTECTOR**



100% Deployment Flexibility

endpointprotector.com



Hardware Appliance

- | Out-of-the-box solution
- | Implementation within minutes
- | Friendly web management interface
- | Available models for networks ranging from 20 to 4000+ endpoints



Virtual Appliance

- | Formats: .ovf, .ova, .vmx, .vhd, .pvm, .xva
- | Up & Running in less than 30 minutes
- | Compatible with VMware, VirtualBox, Parallels Desktop for Mac, Microsoft Hyper-V and Citrix XenServer
- | Eco friendly – use the hardware you already have



Cloud – Amazon Web Services, Google Cloud, Microsoft Azure

- | Flexibility and Adaptability
- | Sustainability
- | Easy access to administration and reports
- | Time-saving



Administrative Interface

endpointprotector.com

Modular and intuitive Web-based administration interface

Multilingual Interface

English
Deutsch
Spanish
French
Korean
Russian
Others

User-friendly interface

Responsive interface

Centralized Management

All modules in a single management console





Main Modules

endpointprotector.com



Content Aware Protection

Scanning data in motion

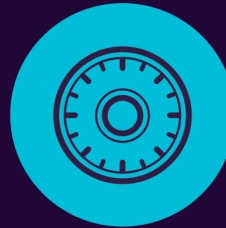
Monitor, control and block file transfers. Detailed control through both content and context inspection



Device Control

USB & peripheral port control

Lockdown, monitor and manage devices. Granular control based on Vendor ID, Product ID, Serial Number and more



Enforced Encryption

Automatic USB Encryption

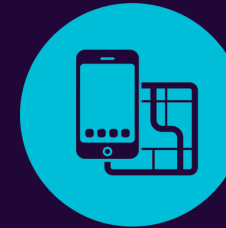
Encrypt, manage and secure USB storage devices by safeguarding data in transit. Password-based, easy to use and very efficient.



eDiscovery

Scanning data at rest

Discover, encrypt and delete sensitive data. Detailed content and context inspection through manual or automatic scans.



Mobile Device Management

Manage mobile devices

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





Content Aware Protection

Scanning data in motion

Monitor, control and block file transfers.
Detailed control through both content
and context inspection.





Content Aware Protection

endpointprotector.com

**ENDPOINT
PROTECTOR**

Dashboard

Device Control

Content Aware Protection

Dashboard

Content Aware Policies

eDiscovery

Blacklists and Whitelists

Enforced Encryption

Mobile Device Management

Offline Temporary Password

Reports and Analysis

Alerts

Directory Services

Appliance

System Maintenance

System Configuration

System Parameters

Support

Content Aware Protection - Create Policy

Policy Information

Details

OS Type: ☒ Windows ☐ macOS ☐ Linux

Policy Name:

Policy Description:

Policy Action:

Thresholds

Global Threshold:

Threat Threshold:

File size threshold:

Policy Status: ☒ ON

Client Notifications: ☒ ON

Policy Exit Points

Applications

☒ Storage Devices ☐ Network Share ☐ Thin Clients ☐ Clipboard ☐ Print Screen ☐ Printers

File transfers through selected applications from the list below will be inspected for sensitive content. Depending on the Policy Action, they will be reported or reported and blocked.

Web Browser

☐ Internet Explorer
☐ Chrome
☐ Mozilla Firefox
☐ Opera
☐ Safari
☐ AOL Desktop 9.6
☐ Aurora Firefox
☐ FrontMotion Firefox
☐ K-Meleon
☐ Maxthon

☐ Social Media / Others

☐ EasyLock
☐ Windows DVD Maker
☐ ALFTP
☐ ADB
☐ AI-Drive
☐ AnyDesk

E-mail

☐ Outlook (Attachments)
☐ Outlook (Body)
☐ Mozilla Thunderbird
☐ Mozilla Thunderbird (Body)
☐ IBM Lotus Notes (Attachments)
☐ IBM Lotus Notes (Body)
☐ Windows Live Mail
☐ GroupWise Client
☐ Outlook Express
☐ Windows Mail

Instant Messaging

☐ ICQ
☐ AIM
☐ Skype
☐ Windows Live Messenger
☐ Yahoo! Messenger
☐ Gaim
☐ HamibroTalk
☐ Pidgin
☐ Trillian
☐ NateOn Messenger

Cloud Services / File Sharing

☐ Google Drive Client
☐ iCloud Drive
☐ uTorrent
☐ BitComet
☐ Daaun Cloud
☐ KT Olleh uCloud
☐ Never N Drive
☐ Azureus
☐ OneDrive (Skydrive)
☐ OneDrive for Business

© 2004 - 2018 CoSoSys Ltd. All rights reserved.

Version 5.2.0.0



Content Aware Protection

endpointprotector.com



Content and Context Scanning

Enable an advanced inspection mechanism for a more accurate detection of sensitive content such as PII's. Context customization is available.



Blacklists and Whitelists

Create blacklists based on predefined content, custom content, file names, or generate whitelists to avoid redundancy and increase productivity.



File tracing and 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.



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.



Device Control

USB & peripheral port control

Lockdown, monitor and manage devices. Granular control based on Vendor ID, Product ID, Serial Number and more.







Device Control

endpointprotector.com



Device Types and Specific Devices

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



Custom Classes and Trusted Devices

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



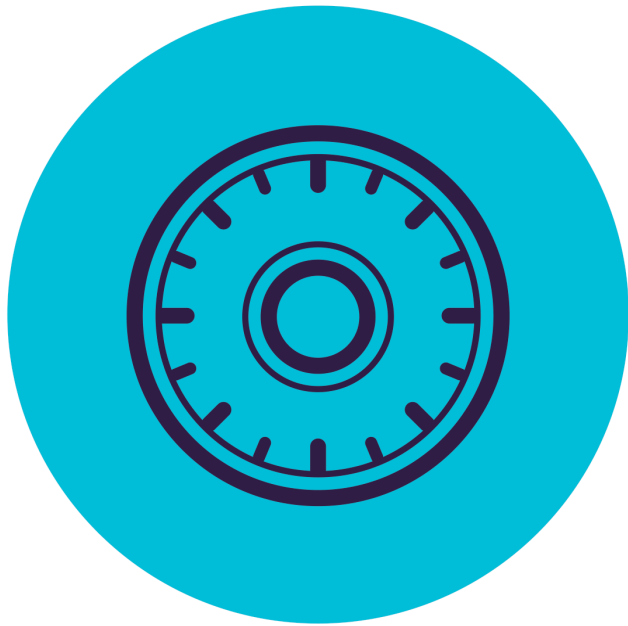
Outside Hours and Outside Networks

Device Control Policies can be set to apply when outside normal working hours. Also, the policies can be set to apply when outside the company's network.



File Tracing and Shadowing

Record all file transfers or attempts to various USB storage devices, providing a clear view on users' actions, and save a copy of files that were transferred to controlled devices.



Enforced Encryption

Automatic USB encryption

Encrypt, manage and secure USB storage devices by using 256-bit AES encryption. Password-based, easy to use and very efficient.





Enforced Encryption

endpointprotector.com

ENDPOINT
PROTECTOR

Dashboard

Device Control

Content Aware Protection

eDiscovery

Blacklists and Whitelists

Enforced Encryption

EasyLock

Mobile Device Management

Offline Temporary Password

Reports and Analysis

Alerts

Directory Services

Appliance

System Maintenance

System Configuration

System Parameters

Support

« Enforced Encryption - EasyLock

Deployment

Manual deployment ⓘ

To manually deploy EasyLock and utilize the Enforced Encryption feature, follow the steps below:

① Select a USB storage device.

② Download or Copy the EasyLock package directly to the root of the selected USB storage device.

③ Follow the simple setup procedure and set a password.

④ Copy & Paste or Drag & Drop files to encrypt and protect them through EasyLock.

Select device:

Select device

Select operating system:

Select operating system

Download

Automatic deployment ⓘ

To automatically deploy EasyLock on all supported devices or only on specific ones, ensure the "Allow Access if device is Trusted Device Level 1+" is selected for USB Storage Devices. When USB Storage Devices will be plugged in to computers where Endpoint Protector Clients are deployed, EasyLock will be automatically pushed on the devices.

Settings

Update EasyLock ⓘ

Automatically:

OFF

EasyLock Multi Server ⓘ

Multi Server:

ON

Save

Master Password Settings

Enforce Complex Password:

OFF

Define Master Password

Old Master Password:

Old Master Password

Master Password:

Master Password

Save

EasyLock Installation and Execution ⓘ

Endpoint Protector Client presence required:

ON

Additional Server IP Address:

User Password Settings

Enforce Complex Password:

OFF

Confirm Master Password:

Confirm Master Password

© 2004 - 2018 CoSoSys Ltd. All rights reserved.

Version 5.2.0.0



Enforced Encryption

endpointprotector.com



Automatic and manual Deployment

Both automatic and manual deployment is available.



Complex Master and User Passwords

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



Secure and easy to use

Password-based, easy to use and very efficient.



Trusted Devices or Read Only

Authorize only encrypted USB devices and ensure all data copied on removable storage devices is automatically secured. The option to allow Read Only rights until encryption is needed is also possible.

| Why DLP?

| Choosing a DLP solution:

- Zero-day support
- Cross-platform support
- Easy deployment
- Easy management

Feel free to contact us

endpointprotector.com

(HQ) Romania:

E-mail: sales@cososys.com

Sales: + 40 264 593 110/ ext. 103

Filip Cotfas

E-mail: filip.cotfas@endpointprotector.com

Phone: + 40 742 517 711

LinkedIn: linkedin.com/in/filipcotfas/

Social Media



linkedin.com/company/endpointprotector



facebook.com/EndpointProtector



twitter.com/cososys



youtube.com/user/CoSoSys

Weekly News

endpointprotector.com/blog

endpointprotector.com