ENDPOINT PROTECTOR

MacSysAdmin 2019

Agenda

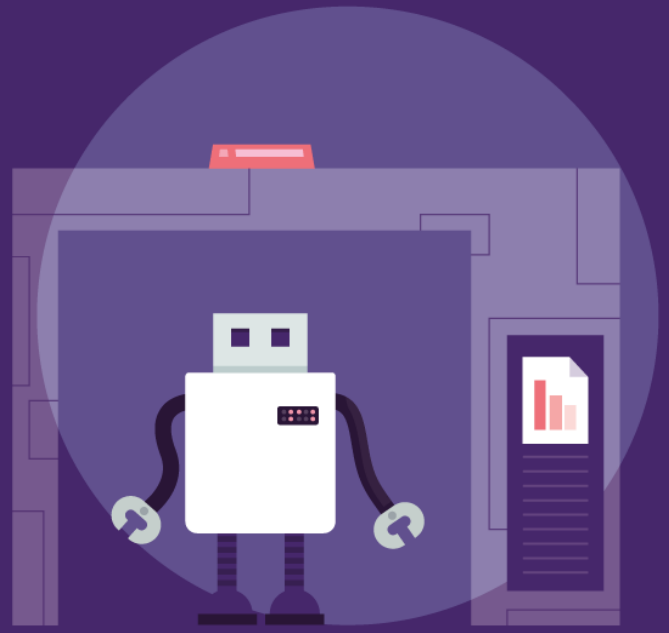
What is DLP

Why do we need DLP

How to choose a DLP solution for macOS

How Endpoint Protector can help

Why have a DLP solution?



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

- Zero-day support
- Minimum device performance impact
- Easy to update
- Test for Kernel Panics
- Feature parity between operating systems

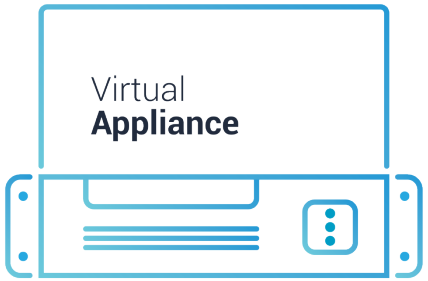
ENDPOINT PROTECTOR

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.

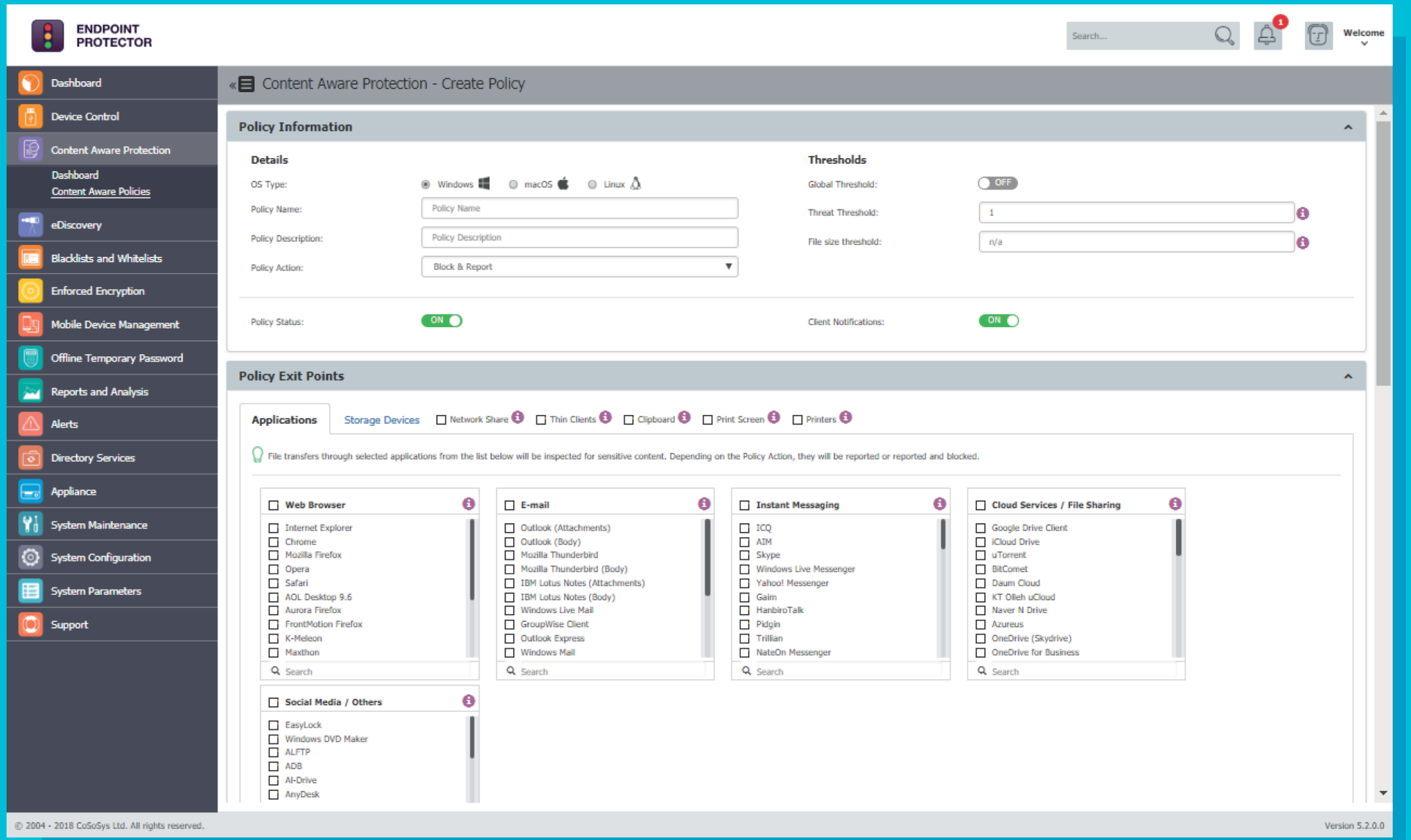
Content Aware Protection

Scanning data in motion

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

Content Aware Protection

endpointprotector.com



Content Aware Protection

endpointprotector.com

Content and Context Scanning

Enable an advanced inspection mechanism for a more accurate detection of sensitive content such as PIIs.
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.

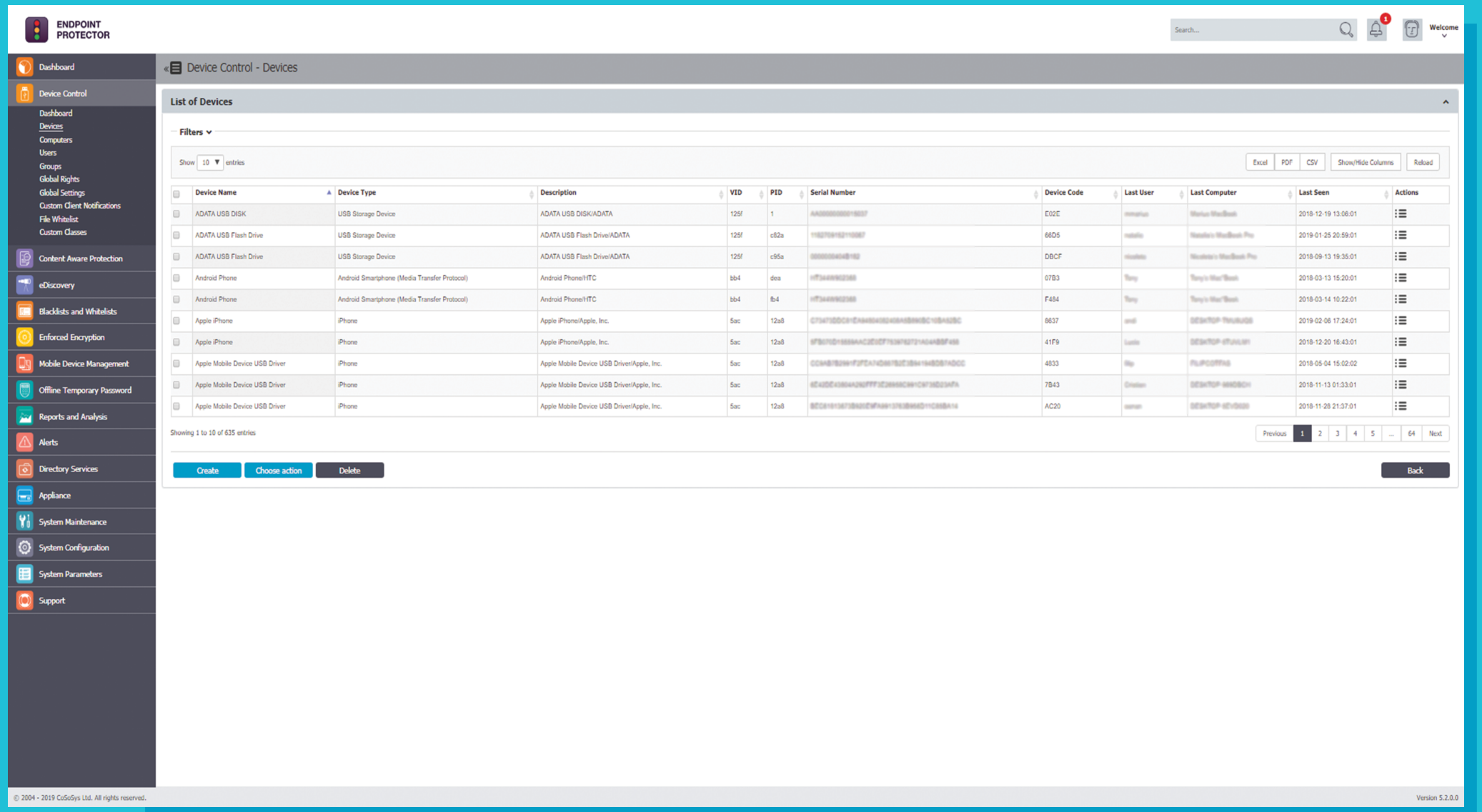
Device Control

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 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

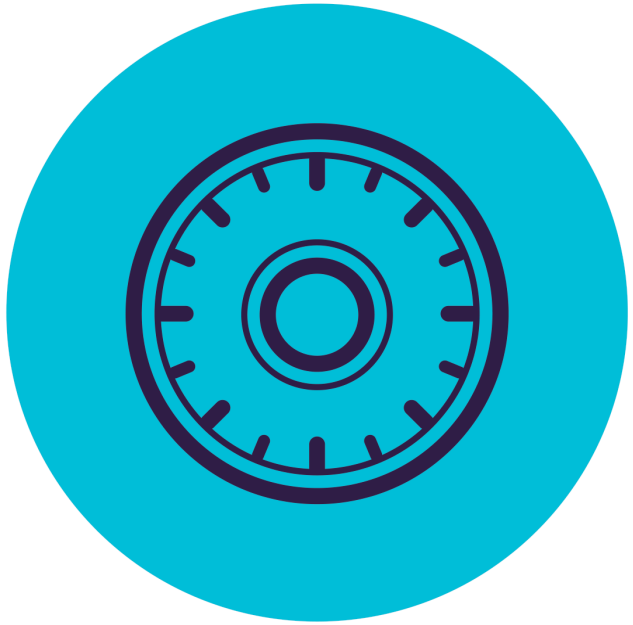
Rights can be created based on classes of devices making management easier for products
from the same vendor.

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.



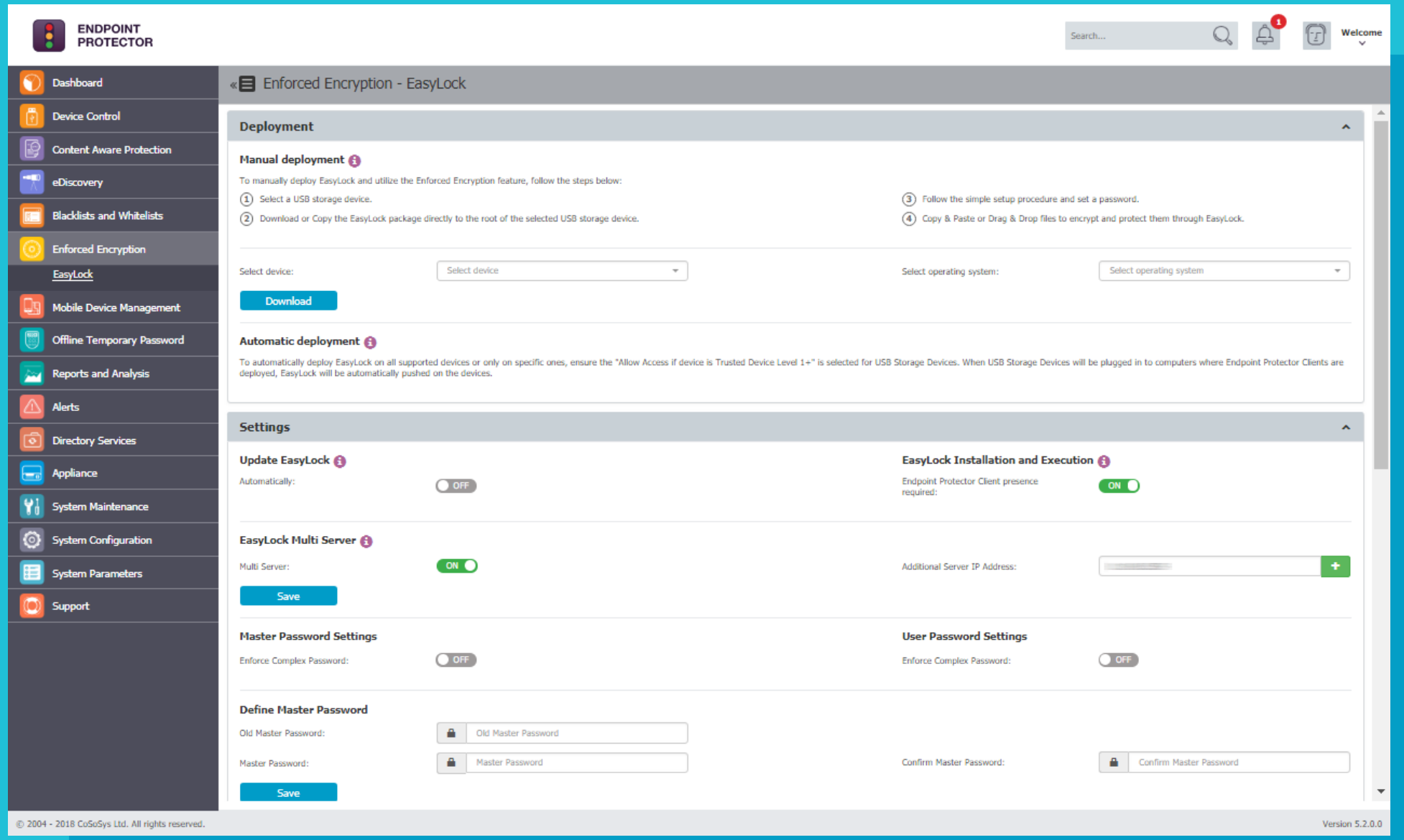
Enforced Encryption

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



Enforced Encryption

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.

In a nutshell

- Why DLP?

- Choosing a DLP solution:
  - Zero-day support
  - Cross-platform support
  - Easy deployment
  - Easy management

Feel free to contact us

(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