



MacSysAdmin 2019

Agenda





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

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).

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.

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.

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

endpointprotector.com



ENDPOINT PROTECTOR

100% Deployment Flexibility

endpointprotector.com



Hardware Appliance



Virtual Appliance



Cloud – Amazon Web Services, Google Cloud, Microsoft Azure

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

- Formats: .ovf, .ova, .vmx, .vhd, .pvm, .xva
- I 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

- I Flexibility and Adaptability
- Sustainability
- I Easy access to administration and reports

I Time-saving



Administrative Interface

endpointprotector.com

Modular and intuitive Webbased 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











Content Aware Protection

Scanning data in motion

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





Content Aware Protection

PROTECTOR				Search	Q 4 we	elcome
🕥 Dashboard	« Content Aware Protection	- Create Policy				
Device Control	Policy Information				^	
Content Aware Protection	Details		Thresholds			ч
Dashboard Content Aware Policies	OS Type: 🛞	Windows 💐 🔘 macOS 🇯 🔘 Linux 🔬	Global Threshold:	OFF		
	Policy Name:	Policy Name	Threat Threshold:	1	•	
eDiscovery	Policy Description:	Policy Description	File size threshold:	n/a	8	
Blacklists and Whitelists	Policy Action:	Block & Report	T			
Enforced Encryption	l ———					
Mobile Device Management	Policy Status:		Client Notifications:	ON O		
Offline Temporary Password						- 1
Reports and Analysis	Policy Exit Points				^	
Alerts	Applications Storage Devices	Network Share 3 Thin Clients 3 Clipboard 3	🗆 Print Screen 🚯 🔲 Printers 🚯			
🦰 e	O File transfers through colorted application	s from the list below will be imported for consider content. Personal	ndian on the Delicy Action. they will be expected as repeated and block	select		
Directory Services	G File transfers through selected application	is from the list below will be inspected for sensitive content. Deper	nding on the Policy Action, they will be reported or reported and blo	ocked.		
Directory Services Appliance	File transfers through selected applications Web Browser	is from the list below will be inspected for sensitive content. Deper	Inding on the Policy Action, they will be reported or reported and bit Instant Messaging	ocked.		
	Web Browser Internet Explorer	E-mail Outlook (Attachments)	Instant Messaging ICQ	Cloud Services / File Sharing		
Appliance	Web Browser Internet Explorer Chrome Mozilla Firefox	E-mail Outlook (Attachments) Outlook (Body) Mozilla Thunderbird	Instant Messaging Image: Constant Messaging Image: Con	Cloud Services / File Sharing () Google Drive Client Cloud Drive UTorrent		
Appliance	Web Browser Internet Explorer Chrome Mozilla Firefox Opera Safari	E-mail Outlook (Attachments) Outlook (Body) Mozilla Thunderbird Mozilla Thunderbird (Body) IBM Lotus Notes (Attachments)	Instant Messaging ICQ ICQ AIM Skype Windows Live Messenger Yahool Messenger	Cloud Services / File Sharing Google Drive Client Cloud Drive UTorrent BitComet Daum Cloud		
Appliance System Maintenance System Configuration System Parameters	Web Browser Internet Explorer Chrome Mozilla Firefox Opera Safari AOL Desktop 9.6 Aurora Firefox	E-mail Outlook (Attachments) Outlook (Body) Mozilla Thunderbird Mozilla Thunderbird (Body) IBM Lotus Notes (Attachments) IBM Lotus Notes (Body) Windows Live Mai	Instant Messaging ICQ IQ I	Cloud Services / File Sharing Google Drive Client Cloud Drive UTorrent BRComet Daum Cloud KT Olleh uCloud Naver N Drive		
Appliance System Maintenance System Configuration	Web Browser Internet Explorer Chrome Mozilla Firefox Opera Safari AOL Desktop 9.6 Aurora Firefox Firefox FrontMotion Firefox K-Meleon	E-mail Outlook (Attachments) Outlook (Body) Mozilla Thunderbird Mozilla Thunderbird Mozilla Thunderbird (Body) IBM Lotus Notes (Attachments) IBM Lotus Notes (Attachments) IBM Lotus Notes (Body) Windows Live Mai GroupWise Client Outlook Express	Instant Messaging Image: Constant Messaging ICQ Image: Constant Messanger Skype Windows Live Messenger Yahoo! Messenger Gaim HanbitoTalk Pidgin Trillian Trillian	Cloud Services / File Sharing Google Drive Client Good Drive UTorrent BitCond Dature Dature Cloud KT Olleh uCloud Naver N Drive Azureus OneDrive (Skydrive)		
Appliance System Maintenance System Configuration System Parameters	Web Browser Internet Explorer Chrome Mozilla Firefox Opera Safari ADL Desktop 9.6 Aurora Firefox FrontMotion Firefox	E-mail Outlook (Attachments) Outlook (Oddy) Mozilla Thunderbird Mozilla Thunderbi	Instant Messaging ICQ ICQ AIM Skype Windows Live Messenger Yahoo! Messenger Gaim HanbinoTalk Pidgin	Cloud Services / File Sharing Google Drive Client Cloud Drive U Torrent BitComet Daum Cloud KT Olleh uCloud Naver N Drive Azureus		
Appliance System Maintenance System Configuration System Parameters	Web Browser Internet Explorer Chrome Mozilla Firefox Opera Safari AOL Desktop 9.6 Aurora Firefox Firefox K-Meleon Maxthon	E-mail Outlook (Attachments) Outlook (Attachments) Outlook (Body) Mozilla Thunderbird Mozilla Thunderbird (Body) IBM Lotus Notes (Attachments) IBM Lotus Notes (Gody) Windows Live Mail GroupWise Client Outlook Express Windows Mail	Instant Messaging Image: Constant Messaging ICQ Image: Constant Messenger Skype Windows Live Messenger Yahoo! Messenger Gaim HanbitoTalk Pidgin Pidgin Trillan NateOn Messenger NateOn Messenger	Cloud Services / File Sharing () Google Drive Client Cloud Drive UTorrent BitComet Dearn Cloud KT Oleh uCloud Naver N Drive Azureus OneDrive (Skydrive) OneDrive for Business		
Appliance System Maintenance System Configuration System Parameters	Web Browser Internet Explorer Chrome Mozilla Firefox Opera Safari AOL Desktop 9.6 Aurora Firefox FrontMotion Firefox K-Meleon Maxthon Search Social Media / Others EasyLock	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 Q. Search	Instant Messaging Image: Constant Messaging ICQ Image: Constant Messenger Skype Windows Live Messenger Yahoo! Messenger Gaim HanbitoTalk Pidgin Pidgin Trillan NateOn Messenger NateOn Messenger	Cloud Services / File Sharing () Google Drive Client Cloud Drive UTorrent BitComet Dearn Cloud KT Oleh uCloud Naver N Drive Azureus OneDrive (Skydrive) OneDrive for Business		
Appliance System Maintenance System Configuration System Parameters	Web Browser Internet Explorer Chrome Mozilla Firefox Opera Safari AOL Desktop 9.6 Aurora Firefox FrontMotion Firefox K-Meteon Maxthon Search Social Media / Others EasyLock Windows DVD Maker ALFTP	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 Q. Search	Instant Messaging Image: Constant Messaging ICQ Image: Constant Messenger Skype Windows Live Messenger Yahoo! Messenger Gaim HanbitoTalk Pidgin Pidgin Trillan NateOn Messenger NateOn Messenger	Cloud Services / File Sharing () Google Drive Client Cloud Drive UTorrent BitComet Dearn Cloud KT Oleh uCloud Naver N Drive Azureus OneDrive (Skydrive) OneDrive for Business		
Appliance System Maintenance System Configuration System Parameters	Web Browser Internet Explorer Chrome Mozilla Firefox Opera Safari AOL Desktop 9.6 Aurora Firefox FrontMotion Firefox K-Meleon Maxthon Search Social Media / Others EasyLock Windows DVD Maker	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 Q. Search	Instant Messaging Image: Constant Messaging ICQ Image: Constant Messenger Skype Windows Live Messenger Yahoo! Messenger Gaim HanbitoTalk Pidgin Pidgin Trillan NateOn Messenger NateOn Messenger	Cloud Services / File Sharing () Google Drive Client Cloud Drive UTorrent BitComet Dearn Cloud KT Oleh uCloud Naver N Drive Azureus OneDrive (Skydrive) OneDrive for Business		





Content and Context Scanning



Blacklists and Whitelists



File tracing and Shadowing



Reports and Analysis

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

available.

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





										Search	Q, E	•
Dashboard		Device Control - Devices										
Device Control Dashboard	List o	of Devices										
Devices Computers Users Groups Global Rights	Filters Show 10 Filters						Excel	PDF CSV Show/Hide C	lumns Reload			
Global Settings		Device Name	Device Type	Description	♦ VID	PID	Serial Number	Device Code	👌 Last User	Last Computer	👌 Last Seen	Actions
Custom Client Notifications File Whitelist		ADATA USB DISK	USB Storage Device	ADATA USB DISK/ADATA	125/	1	AA00000000+\$037	E02E	matus	Marius MacBook	2018-12-19 13:06:01	:=
ustom Classes		ADATA USB Flash Drive	USB Storage Device	ADATA USB Flash Drive/ADATA	125/	c82a	1182706152110067	66D5	natalio	Natala's MacBook Pro	2019-01-25 20:59:01	:=
ntent Aware Protection		ADATA USB Flash Drive	USB Storage Device	ADATA USB Flash Drive/ADATA	125/	c95a	0000004048102	DBCF	nicolato	Micatelia's MacBeak Pro	2018-09-13 19:35:01	:=
Discovery		Android Phone	Android Smartphone (Media Transfer Protocol)	Android Phone/HTC	bb4	dea	HT3448902368	07B3	Bary	Tary's Mac'Bash	2018-03-13 15:20:01	:=
		Android Phone	Android Smartphone (Media Transfer Protocol)	Android Phone/HTC	bb4	fb4	1173448962368	F484	Tary	Tary's Mar'Book	2018-03-14 10:22:01	:=
acklists and Whitelists		Apple iPhone	iPhone	Apple iPhone/Apple, Inc.	5ac	12:8	C754730008+DA64804082408A5884080108A5280	8637	andi	OCSKTOP THURUDS	2019-02-06 17:24:01	:=
nforced Encryption		Apple iPhone	iPhone	Apple iPhone/Apple, Inc.	5ac	12a8	6FB070D16568AAC2E0EF7638782721A04ABBF468	41F9	Latin	DESKTOP-ITUNUM	2018-12-20 16:43:01	:=
obile Device Management		Apple Mobile Device USB Driver	iPhone	Apple Mobile Device USB Driver/Apple, Inc.	5ac	12a8	CC6A8782991727CA14088782C38941948087A0CC	4833	89p	PL/PCOTTA6	2018-05-04 15:02:02	:=
ffline Temporary Password		Apple Mobile Device USB Driver	iPhone	Apple Mobile Device USB Driver/Apple, Inc.	5ac	12a8	604200438044280FFF30288680089108738023AFA	7843	Cristian	DESKTOP-MHOBCH	2018-11-13 01:33:01	:=
eports and Analysis		Apple Mobile Device USB Driver	iPhone	Apple Mobile Device USB Driver/Apple, Inc.	5ac	12:8	8C0819136735921C9FA89137638956D11C858A14	AC20	coman	0554707-6510620	2018-11-28 21:37:01	:=
Alerts Directory Services Appliance	Showin	g 1 to 10 of 635 entries Create Choose action	Delete							Prev	ious 1 2 3 4 5	64 Back
System Maintenance												
System Configuration												
System Parameters												
Support												
- 2019 CoSoSys Ltd. All rights reserved.												Version





Device Types and Specific Devices

<u></u>	
I	

Custom Classes and Trusted Devices

Set rights - deny, allow, read only, etc. - for Device Types or Specific Devices (using VID, PID and Serial Number). Rights can be created based on classes of devices making management easier for products from the same vendor.



Outside Hours and Outside Networks



File Tracing and Shadowing

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. 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

ENDPOINT PROTECTOR				Sear	ch Q	_ 1	(7) Wel	come V	
🕥 Dashboard	« Enforced Encryption - Eas	syLock							
Device Control	Deployment						^	L A	
Content Aware Protection	Manual deployment 🚯						1		
eDiscovery	To manually deploy EasyLock and utilize the En (1) Select a USB storage device.	forced Encryption feature, follow the steps below:		(3) Follow the simple setup procedure and set a password.					
Blacklists and Whitelists	<u> </u>	lirectly 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. 					
Enforced Encryption		Contract of the second	۰. ۲		Estado analiza antes				
	Select device:	Select device 👻	J	Select operating system:	Select operating system		*		
Mobile Device Management									
Offline Temporary Password	Automatic deployment (3) To automatically deploy EasyLock on all suppor	ted devices or only on specific ones, ensure the "Allow Access if d	evice is Trusted Device Level 1+" is selected for USB	Storage Devices. When USB Storage Devices will	be plugged in to computers where Er	ndpoint Protecto	r Clients are		
Reports and Analysis	deployed, EasyLock will be automatically pushe	I on the devices.							
Alerts	Settings						^		
Directory Services	Update EasyLock 🚯			EasyLock Installation and Execution	n 🚯				
System Maintenance	Automatically:	OFF		Endpoint Protector Client presence required:	ON D				
System Configuration	EasyLock Multi Server 🚯								
System Parameters	Multi Server:			Additional Server IP Address:			+		
Support	Save								
	Master Password Settings			User Password Settings					
	Enforce Complex Password:	OFF		Enforce Complex Password:	OFF				
	Define Master Password								
	Old Master Password:	Old Master Password]						
	Master Password:	Master Password)	Confirm Master Password:	Confirm Master Passwor	d			
	Save							-	
© 2004 - 2018 CoSoSys Ltd. All rights reserved.							Version 5	.2.0.0	





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

(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



You Tube facebook.com/EndpointProtector



twitter.com/cososys

youtube.com/user/CoSoSys

Weekly News endpointprotector.com/blog