ENDPOINT PROTECTOR | by CoSoSys

DATASHEET 4.4.0.9

Data Loss Prevention & Mobile Device Management

Suitable for any network size and any industry

DLP for Windows, Mac and Linux

Protecting the entire network

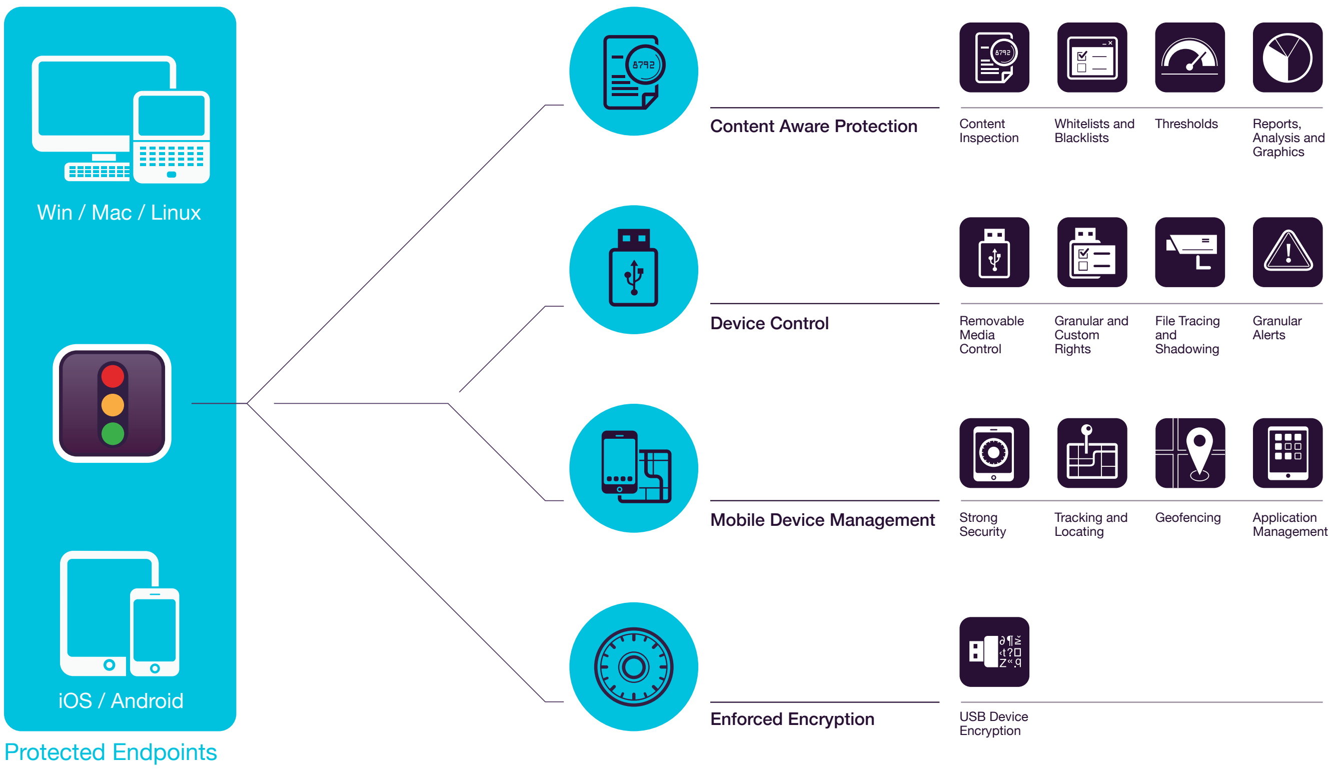
ENDPOINT PROTECTOR

by CoSoSys

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

In a world where portable and lifestyle devices are transforming the way we work and live, Endpoint Protector 4 is designed to maintain productivity and make work more convenient, secure and enjoyable. The blacklist based approach prohibits the use of specific devices, URLs and domain names for certain computers/users/groups, increasing productivity while maintaining control of devices and data. With Endpoint Protector 4 being offered as hardware or virtual appliance, it can be setup in minutes. It dramatically reduces the risks posed by internal threats that could lead to data being leaked, stolen, damaged or otherwise compromised. In addition to these, compliance with various rules and regulations is also met.

How it Works



Protected Endpoints

Content Aware Protection
for Windows, Mac OS X and Linux

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

Device Control
for Windows, Mac OS X and Linux

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

Mobile Device Management
for Android, iOS and OS X

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

Enforced Encryption
for Windows and Mac OS X

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

Mobile Device Management

for Android, iOS and Mac OS X

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 device 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 permission for built-in features such as the 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.

Mac OS X 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

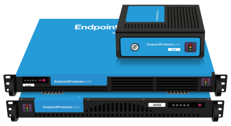
Suitable for any type of network, our products can be used by enterprise customers, small and medium business and even home users. With a client-server architecture, they are easy to deploy and centrally manage from the web-based interface. Besides the Hardware and Virtual Appliance, Amazon Web Services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

Endpoint Protector

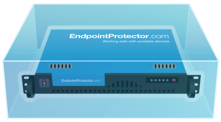
Content Aware Protection, Device Control and Encryption are available for computers running on different Windows, Mac and Linux versions and distributions. Mobile Device Management and Mobile Application Management are also available for iOS and Android mobile devices.

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 XP / Windows Vista	(32/64 bit)	●	●	●	
	Windows 7 / 8 / 10	(32/64 bit)	●	●	●	
	Windows Server 2000 - 2016	(32/64 bit)	●	●	●	
Mac OS X	Mac OS X 10.6	Snow Leopard	●	●	●	
	Mac OS X 10.7	Lion	●	●	●	
	Mac OS X 10.8	Mountain Lion	●	●	●	
	Mac OS X 10.9	Mavericks	●	●	●	
	Mac OS X 10.10	Yosemite	●	●	●	
	Mac OS X 10.11	El Capitan	●	●	●	
Linux	Ubuntu		●	●	n/a	
	OpenSUSE		●	●	n/a	
	CentOS / RedHat		●	●	n/a	
	*Please check for details regarding supported versions and distributions on endpointprotector.com/linux					
iOS	iOS 4, iOS 5, iOS 6, iOS 7, iOS 8, iOS 9					●
Android	Jelly Bean (4.1+), KitKat (4.4+), Lollipop (5.0+)					●

COSOSYS

	HQ (Romania)	Germany
E-mail	sales@cososys.com	vertrieb@endpointprotector.de
Sales	+40 264 593 110 / ext. 103	+49 7541 978 26730
Support	+40 264 593 113 / ext. 202	+49 7541 978 26733

	Korea	North America
E-mail	contact@cososys.co.kr	sales.us@endpointprotector.com
Sales	+82 70 4633 0353	+1 888 271 9349
Support	+82 20 4633 0354	+1 877 377 6475

Official Partner

www.endpointprotector.com