ENDPOINT PROTECTOR | by CoSoSys

FEATURES & BENEFITS

DLP
Device Control
Content Aware Protection
Encryption
MDM

Protecting the entire network

Overview

Available as:

Hardware Appliance

Virtual Appliance

Cloud Solution

Solution for:

Data Loss Prevention
Mobile Device Management
Enforced USB Encryption

Choose the best way to deploy the solution into your network

From increased control of an on-premise appliance to leveraging the flexibility of the cloud

A single solution to protect your entire network

Manage everything from a single dashboard and support your mobile workforce without compromising productivity or letting confidential data leave the safety of your network

Modules:

Device Control
for Windows, Mac OS X and Linux

Manage use of USB and other portable storage devices and enforce strong security policies to protect vital data
USB sticks, memory cards, external HDD, MP3 player, etc.

Content Aware Protection
for Windows, Mac OS X and Linux

Ensure sensitive data does not leave the network whether copied on devices, emails or online applications
Outlook, Thunderbird, Skype, Messengers, Dropbox, etc.

Mobile Device Management
for Android, iOS and OS X

Gain control and detailed monitoring of mobile devices, ensure data is safe and increase productivity
Embrace the BYOD trend and maintain control

Benefits

File Type Filters

Based on your specific requirements choose the best way to deploy our solutions in your network.
It provides the best TCO on the market for a solution of its kind. It is a modular product, allowing organizations to set up Endpoint Protector in multiple steps, according to their needs and budget.

Client-Server architecture

The Server part comes as a simple plug-and-play appliance and has everything set up.
The Client has a small footprint and does not interfere or compromise users' productivity.

Low resources consumption

Minimal hardware requirements, providing exactly what you need from a DLP Solution.
No additional servers or solutions required in order for Endpoint Protector to run.

Simple deployment

Deploy the agents using Active Directory, Apple Remote Desktop or other 3rd party solutions.

Hassle-free

End the headaches of configuration and deployment of overcomplicated solutions.
Extremely intuitive with a very short learning curve.
Administration can easily be made even by staff with a limited IT background.

Intuitive interface

Unlike other solutions where the interface takes time to work through, Endpoint Protector has a great user-friendly interface with an extremely short learning curve.

Fast and efficient

Policies and Rights can be created and easily changed with just a few clicks.
Any user can quickly request and receive temporary access to devices or to transfer files.

Feedback and improvements

Feedback is always encouraged and appreciated.
Any feature suggestion or improvement are taken into consideration and if possible, included in the roadmap.
Most features suggested by costumers have been implemented successfully.

Fantastic support

In average, queries are answered within 24 hours but most are resolved faster.
No levels of escalation – a single support contact person will ensure query resolution.
Support is available via online chat, email, phone and remote connection.

No additional software required

Endpoint Protector does not require any additional software installation or licensing. Other products' system requirements include Windows 2003, Web Edition/SP2, Windows 2008 R2, SQL Server 2005, Express/SP3/SQL Server 2008 R2, IIS 6.0, .NET Framework 3.5, MS internet Explorer 7 and others.

Device Control

for Windows, Mac OS X and Linux

Monitor and control all peripheral ports and USB storage devices to stop data loss and data theft.

Functionality Overview

Precise and extremely granular control

Specify which devices can and cannot be used, define rights per user, computer or group, and more controls are available.

Custom Classes and whitelisting devices

Create lists with devices that are allowed to connect to the network based on Vendor ID, serial number or Product ID.

Protection outside the corporate network with Offline Temporary Password

Grant USB access remotely and have access to complete log reports when computer reconnects to the network. Time frames: starting from 30 minutes up to 30 days.

Full reporting for monitoring and audits

View full activity history, great graphics for a quick overview but also extensive CSVs that can be used for audits and additional reports for executives. Additionally, the Administrator has access to transferred files on portable storage devices and can save a copy of those files to verify their exact content.

Complete history alerts

All sent notifications and email alerts also appear in the history section, accessible whenever they are needed.

Extending security with Enforced Encryption - TrustedDevice

Encrypted devices can be used throughout the company and all data copied onto USB storage devices are automatically encrypted, the devices themselves becoming TrustedDevices. There are 4 TrustedDevice Levels, allowing the enforced encryption functionality to be used with a wide range of devices. EasyLock, USB encryption software, can be deployed automatically to connected devices on computers with Endpoint Protector client installed.

Benefits

Allow just the right users to access the right devices

The Marketing department may need access to a digital camera while the Accounts Payable department should not. Company-owned USB sticks should be accessible throughout the network, regardless of department.

Allow temporary access to USB devices

If a USB stick needs to be connected to a laptop during a presentation, the user can request temporary access remotely.

Know at all-time what is happening in the network

Based on the company policy and the configuration set in place, full reports are available. Email alerts can be set to monitor specific events, like a specific user connecting or disconnecting a device, as well as other events.

Content Aware Protection

for Windows, Mac OS X and Linux

With information leaving the corporate network through emails, cloud storage solutions, instant messengers, social media and other online applications, it's essential to ensure sensitive data does not get lost, stolen or leaked.

Functionality Overview

Precise control over documents

Enforce corporate policy and comply with industry rules and regulations by ensuring documents containing confidential data are not shared outside the company. Everything without compromising productivity.

Monitor or block documents based on their type

File extensions can be used to decide if documents that contain sensitive data should be shared outside the network or with unauthorized recipients.

Decide what data is confident in your organization

Take advantage of predefined filters but also have the option to create custom dictionaries to determine what content defines a confidential document and keep sensitive data inside your company.

Take advantage of regular expressions

Create custom rules to detect and block exactly the information you consider sensitive.

Support collaboration and communication

Encourage communication and collaboration using Skype, Facebook, Slack, Google Drive and other online applications while minimizing the risks posed by sharing files containing sensitive information.

File Tracing and File Shadowing

On top of extended logs and reports providing the exact information of who did what, you have the option to store an exact copy of the transferred files.

Whitelisting Domains and URLs

For most organizations, completely locking down a network is not an option. Whitelisting simplifies things by allowing the administrator to a) define a list of web addresses where uploading of confidential information will be allowed; b) define a list of email addresses; c) add a file location to the white list. More white lists are available.

Benefits

Ensure just the right content leaves the network

The Marketing department may need to share images while the Accounts Payable department should not.
On the other hand, none of the departments should be able to share editable documents containing clients' lists or PII.
Using file extensions, keywords, predefined content (credit card numbers, driving licenses, etc.) or regular expressions to create custom rules for your gift cards & discount coupons, you ensure compliance and financial losses.

Content Aware Protection

for Windows, Mac OS X and Linux

With information leaving the corporate network through emails, cloud storage solutions, instant messengers, social media and other online applications, it's essential to ensure sensitive data does not get lost, stolen or leaked.

Help communication but reduce risks

Both PR and Credit & Collection departments might need to communicate via Skype but maybe should not be able to transfer files through this tool.

White lists by domain, email addresses, and other criteria

As all departments need to constantly share information between them, by whitelisting your e-mail domain, sensitive data can be shared internally and bypass the unnecessary restrictions.

URL whitelisting

Similar to whitelisting a domain name, URLs can also be whitelisted. This will allow a Credit & Collection department to email or upload invoices to a specific location while the Design department will not be able to upload or email the layouts they are working on.

File Tracing and File Shadowing

These functionalities will provide all the information the IT admin may require for audits, for optimizing the policies or identifying possible data security violations: user, computer, file name, file type, file size, hash, as well as additional information. Moreover, having an exact copy of the transferred document stored on the server will ensure you know at all times what data was transferred.

Protection for all endpoints

Endpoint Protector is the most advanced solution of its kind with Windows, Mac OS X and Linux compatibility. Why resort to more vendors when you can have all DLP features for all Operating Systems from a single vendor?

Mobile Device Management

for Android, iOS and Mac OS X

Extend data protection to mobile devices, while supporting BYOD.

Functionality Overview

Track & Locate mobile devices

Keep a close eye on all company mobile device fleet and know where your critical business data is carried at all times.

Remotely Block / Wipe mobile devices if lost or stolen

Smartphones and tablets are frequently lost or stolen in cafeterias, in shopping malls, at the metro, etc. On most devices, company sensitive data is stored, so in the misfortune misplaced devices of in case of a robbery, data cannot be accessed if they are blocked or wiped.

Mobile Application Management

Instantly push free, enterprise and paid apps to enrolled mobile devices from the Endpoint Protector server. Have a record of all installed apps and delete the non-approved ones.

Geofencing

Define a virtual perimeter on a geographic area and apply location-based Mobile Device Management policies. E.g. disable smartphone camera only in the perimeter of your company.

Password Enforcement

Proactively protect company critical data stored on mobile devices by enforcing strong password policies.

Benefits

Centralized data protection

In the same management dashboard with the Device Control and Content Aware Protection, the MDM features complete de data protection policy, simplifying the IT security implementation.

Easy enrollment

With the bulk enrollment option, Admins can easily enroll hundreds of devices simultaneously and get devices' details in the Endpoint Protector server.

Security and management

With strong security features enforced, restrictions for apps and features' use, but also control of camera or activation of device' encryption, data protection is achieved and risk for data loss minimized. Additionally, assets management and remotely deployment of settings for VPN, e-mail and WiFi are possible, so managing the company and personal mobile devices fleet makes IT Admins lives easier.

Protecting data on all company's endpoints is crucial to avoid loopholes. Critical business data resides on multiple workstations starting with laptops, servers, desktops and continuing with mobile devices, making IT department's job complicated and challenging. A unified Data Loss Prevention and Mobile Device Management solution closes the bridge between data protection on traditional endpoints and mobile workstations.

Endpoint Protector cross-platform data security solutions are available in multiple implementation formats and offer strong DLP and MDM modules in a user-friendly dashboard. The solution fits in any company size, starting from SMBs to conglomerates and is suitable for any industry.