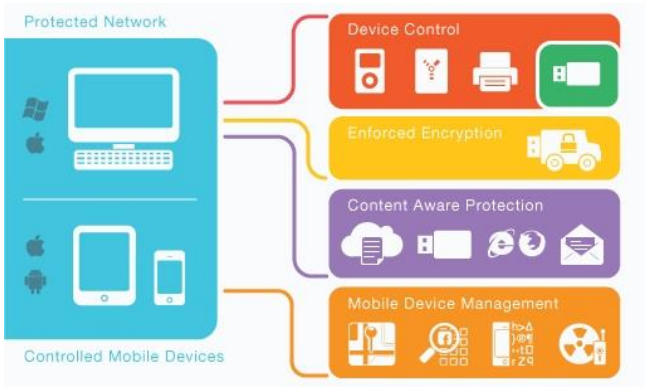
ENDPOINT PROTECTOR 4

Data Loss Prevention Solution, Device Control and iOS & Android Mobile Device Management (MDM) for businesses

Out-of-the-Box Solution to secure data against portable device threats, manage Data Loss Prevention and MDM.

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 whitelist based approach allows the use of specific devices for certain computers/users/groups so that they stay productive while maintaining control of what devices are used and what data users transfer.
With Endpoint Protector 4 being offered as hardware or virtual appliance, it can be setup in minutes, allowing you to dramatically reduce the risks posed by internal threats that could lead to data being leaked, stolen, damaged or otherwise compromised.



Key Advantages

- Hardware or Virtual Appliance is implemented in minutes
- Three in One Solution, Device Control, DLP and MDM
- Intuitive management of devices and endpoints
- Web-based interface
- Protection for Windows, Mac, Linux, iOS and Android
- Pro-active protection against device abuse and data theft
- VMware ready

Endpoint Security for Windows/Mac OS X and Linux Workstations, Notebooks and Netbooks

Protection against threats posed by removable portable devices. Stops intentional or accidental leakage, theft, loss of data or malware infection.

iOS and Android Mobile Device Management (MDM)

- Enforce Password and Security Policy
- Locate Devices / Lock Devices, Wipe Devices
- Restrictions to disable iCloud, Camera, FaceTime, etc
- BYOD Solution, for detailed info see MDM Data Sheet

Take Control of these and more Devices and Applications:

- **Devices**
- USB Devices*
- USB Drives* (normal, U3)
- Memory Cards* (SD, CF, etc.)
- CD/DVD-Burner (int., ext.)
- External HDDs* (incl. sATA)
- Printers*
- Floppy Drives
- Card Readers* (int., ext.)
- Webcams*
- WiFi Network Cards
- Digital Cameras*
- iPhones / iPads / iPods*
- Smartphones/BlackBerry/PDAs
- FireWire Devices*
- MP3 Player/Media Players*
- Biometric Devices
- Bluetooth Devices*
- ZIP Drives
- ExpressCards (SSD)
- Wireless USB
- Serial Port
- Teensy Board
- PCMCIA Storage Devices

- **E-Mail Clients**
  - Outlook
  - Lotus Notes
  - Thunderbird, etc.
- **Web Browsers**
  - Internet Explorer
  - Firefox
  - Chrome, etc.
- **Instant Messaging**
  - Skype, etc.
  - Microsoft Communicator
  - Yahoo Messenger, etc.
- **Cloud Services/File Sharing**
  - Dropbox, iCloud, SkyDrive
  - BitTorrent, Kazaa, etc.
- **Other Applications**
  - iTunes
  - Samsung Kies
  - Windows DVD Maker
  - Total Commander
  - FileZilla
  - Team Viewer
  - EasyLock, and many more

Centralized Web based Management / Dashboard

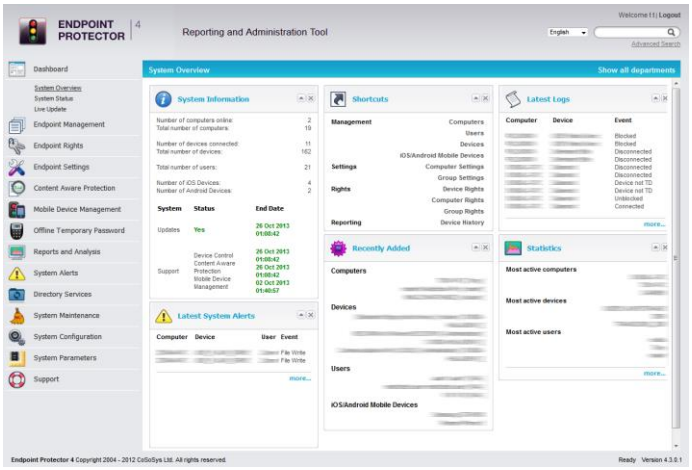
Centrally manages the use of removable portable devices. The Web based Administrative & Reporting interface meets the needs of management and IT security staff and offers real-time information about organization wide controlled devices and data transfer activity.

Key Benefits

- Endpoint Protector implies a TCO that's 50% smaller than the market average
- It is deployed in 70% less time than other solutions
- Costs 45% less than other similar solutions

"I chose Endpoint Protector Appliance for its cost, ease of administration and detailed control. The solution is easy to install, efficient, powerful and easy to manage. I really love the logging, shadowing and offline temporary password (very practical indeed) features."

Marc Rossi
Infrastructure Director
NASS et WIND SAS France



Device Management / Device Control*

Defines the rights for devices / users or computers in your network.

Content Aware Protection / Content Filtering

Document inspection for sensitive content detection, logging and reporting of content aware incidents. Blocking of data leaving exit points from portable devices to applications and online services.

File Type Filtering / File Tracing / File Shadowing*

File Type Filters blocks specified file types. File Tracing records all data that was copied to and from previously authorized devices. File Shadowing saves a copy of all files, even of deleted ones, that were used in connection with controlled devices.

File Whitelisting

Only authorized files can be transferred to authorized devices. All other files are blocked and attempted transfers are reported.

Department Management*

Departments can be organized and separate dedicated policies can be applied to manage the diverse device use needs in large organizations.

Device Activity Logging – Audit Trail* / Reporting Analysis*

Device activity logs are saved for all clients and devices connected giving a history of devices, PCs and users for audits and detailed analysis. Powerful reports, graphics and analysis tool to easily review activity.

Easy Enforcement of Security Policies (Active Directory)*

Simplified device management policies with customizable templates for defined User Groups (Active Directory GPOs) allow easy enforcement and maintenance of security policies across your network.

Temporary Offline Password / Network "Offline" Mode*

Secured PCs that are disconnected from the network stay protected. To keep productivity on the road, devices can be temporarily allowed via the Temporary Offline Password functionality.

Endpoint Protector Client Self Defense

Provides protection even on PCs where users have Administrative rights.

Enforced Encryption - protecting data in transit with EasyLock

In combination with our EasyLock software that is stored on portable storage devices the encryption of data copied to the device is enforced. With our TrustedDevice technology additional security can be applied by using certified encrypted portable storage devices to store data. This assures that, in the event a device is stolen or lost, all the data stored on it is encrypted and safe, not accessible for others.

Protected Endpoint Client(s)

- Windows 8 (32/64bit)
- Windows 7 (32/64bit)
- Windows Vista (32/64bit)
- Windows XP (SP2) (32/64bit)
- Windows 2003/2008 (32/64bit)
- Mac OS X 10.5+
- Ubuntu 10.04/openSUSE 11.4

Mobile Device Management (MDM) Supported Devices

- iPad, iPhone, iOS 4, iOS 5, iOS 6, iOS 7
- Android 2.2+,
  Android 4+ required for some features

Directory Service (not required)

- Active Directory

Endpoint Protector 4 is the only device control / DLP solution in its category available as hardware or virtual appliance. Securing your network with Endpoint Protector saves you lots of time compared to other solutions so you can take a longer lunch or go home early knowing your computer ports are protected.

Endpoint Protector Hardware Appliance

The Endpoint Protector Hardware Appliances are available in different capacities to fit your business needs. All Hardware Appliances are based on the latest and most energy efficient hardware available.

Selected Models (more available)	A20	A50	A100	A250	A1000
Protection for Endpoints (Windows / Mac)	20	50	100	250	1000
Additional capacity	4	10	20	50	200
Housing (Rack mount)	Stand-alone	1U	1U	1U	1U
Processor	ULV Single Core	ULV Dual Core	ULV Dual Core	1X Dual Core	1X Quad Core
Hard Drive	320 GB	320 GB	320 GB	500 GB	2X 1TB (Raid 1)
Power Supply	60W 100-240V (external)	200W 100-240V	200W 100-240V	260W 100-240V	260W 100-240V
Hardware Warranty	1-year included. Additional warranty and replacement options are available.				

Endpoint Protector Virtual Appliance

Endpoint Protector Virtual Appliance can be used by all business sizes. The Virtual Appliance is available both in VMX, OVF and VHD formats to be compatible with the most popular virtualization platforms.

Using the Virtual Appliance you can protect against unauthorized device use and data loss in your network within minutes.

Supported Virtual Environments	Version	.ovf	.vmx	.vhd
VMware Workstation	7.1.4	-	*	-
VMware Player	3.1.4	-	*	-
VMware vSphere (ESXi)	5.0.0	*	-	-
Oracle VirtualBox	4.1.16	*	-	-
Parallels Desktop for Mac	7.0.1	-	*	-
Microsoft Hyper V (2008 R2)	6.1	-	-	*

Other virtualization environments are supported as well.

Endpoint Protector offers you a safe and secure working environment with portable storage and endpoint devices. User efficiency is not restricted since any authorized device can be used continuously on protected PCs while the network's endpoint security policy is enforced.

Contact your local partner for more information:

Created on 11-Mar-2013

ENDPOINT PROTECTOR 4

Content Aware Protection for Windows
An important part of your endpoint DLP strategy

Out-of-the-Box Solution to secure data against leakage and theft through online applications, cloud services, portable devices and other exit points.

Content Aware Protection is a module of the Endpoint Protector DLP (Data Loss Prevention) suite which covers the security needs coming from risks posed by the numerous exit points for companies' sensitive data.
Today, in a world where portable devices and cloud services are transforming the way we work and live, Endpoint Protector 4 is designed to maintain productivity and make work more convenient, secure and enjoyable. Endpoint Protector 4, the easy to implement and deploy DLP solution, prevents confidential data on laptops and desktops from being leaked outside of the company.
With Endpoint Protector 4 being offered as a hardware or virtual appliance, it can be setup in minutes, allowing you to dramatically reduce the risks posed by internal threats that could lead to data being leaked, stolen, damaged or otherwise compromised.

Key Advantages

- Hardware or Virtual Appliance can be implemented in minutes
- Web-based interface
- Intuitive management of policies and endpoints
- Protection for Windows endpoints
- Pro-active protection against device abuse and data theft
- VMware ready

Content-Aware Data Loss Prevention
Protection against threats posed by data transfers to removable portable devices and to online applications and services. Stops intentional or accidental data leakage, theft and loss.

Supports Windows endpoints
Monitoring and blocking data flow on the most popular and strongest platforms to protect your company data.

Take Control of the data flow to these and more Applications and Devices:

- **E-Mail Clients**
  - Outlook
  - IBM Lotus Notes
  - Thunderbird, etc.
- **Web Browsers**
  - Internet Explorer
  - Firefox
  - Chrome, etc.
- **Instant Messaging**
  - Skype, etc.
  - Microsoft Communicator
  - Yahoo Messenger, etc.
- **Cloud Services/File Sharing**
  - Dropbox, iCloud, SkyDrive
  - BitTorrent, Kazaa, etc.
- **Other Applications**
  - iTunes
  - Samsung Kies
  - Windows DVD Maker
  - Total Commander
  - FileZilla
  - Team Viewer
  - HTC Sync for Android
  - LogMeIn Pro
  - EasyLock, and many more

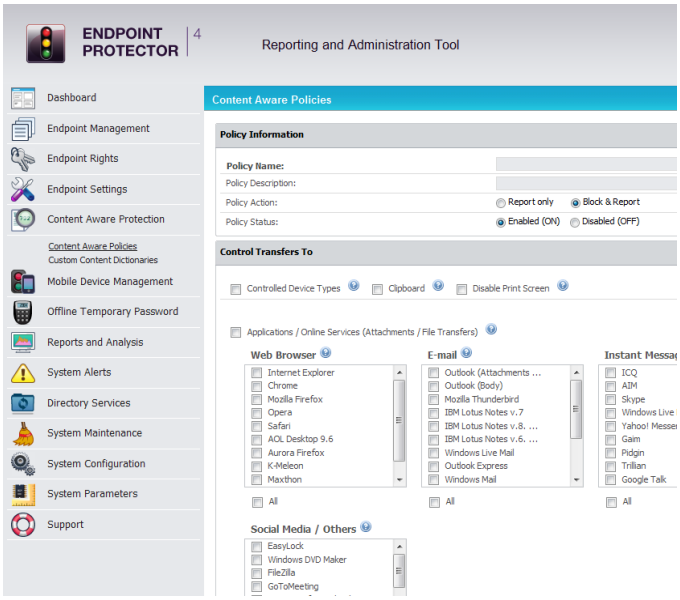
- **Devices / Ports**
- USB Devices*
- USB Drives* (normal, U3)
- Memory Cards* (SD, CF...)
- CD/DVD-Burner (int., ext.)
- External HDDs* (incl. sATA)
- Printers*
- Floppy Drives
- Card Readers* (int., ext.)
- Webcams*
- WiFi Network Cards
- Digital Cameras*
- iPhones / iPads / iPods*
- Smartphones/BlackBerry
- FireWire Devices*
- MP3 Player/Media Players*
- Biometric Devices
- Bluetooth Devices*
- ZIP Drives
- ExpressCards (SSD)
- Wireless USB
- Serial Port
- Teensy Board
- PCMCIA Storage Devices

Centralized Web based Management / Dashboard
Centrally manages and monitors data transferred outside of companies' networks. The Web based Administrative & Reporting interface meets the needs of management and IT security staff and offers real-time information about organization wide controlled devices and applications and data transfer activity.

Key Benefits
- Stops Data from being lost or stolen
- Endpoint Protector implies a TCO that's 50% smaller than the market average
- It saves valuable time, since it is deployed in 70% less time than other solutions
- Reduces costs with data security, since it is 45% more affordable than other similar solutions

2012 Computing Security Awards ★ FINALIST ★

SC MAGAZINE AWARDS 2013 EUROPE HIGHLY COMMENDED



Create security policies for specific entities
Content Aware Protection policies offer a flexible control of document scanning, by allowing selection of users, computers, groups or departments to be monitored.

Filter by Predefined Content or relevant keywords
Filter the data leaving the protected endpoints based on a predefined content format which includes:
- Credit Card Details (all major Credit Cards supported)
- Social Security Numbers (many different country formats supported)
- Bank Account Information
- etc.

Filter by File Types
Endpoint Protector blocks the documents leaving the company based on their true file type. Supports the most important file types in current use, applications such as MS Office and graphic files, archives, executables, media and other files.

Filter by Dictionary
The Content Aware Protection module looks for keyword matching data, and stops the data / files which contain them from being leaked or stolen through protected exit points. Multiple dictionaries can be created for policies.

Monitor Clipboard to prevent Copy & Paste of sensitive data
Monitoring the Clipboard will stop users from copying & pasting sensitive company information from documents to outlook clients, web mail apps or other channels on which the information could get leaked.

Disable Print Screen
Disabling the print screen option in your policy will prevent users from making print screens of data shown on their screen and taken them out of the company as images. Disabling print screen further strengthens your DLP policy.

Prevent sensitive data leaving by E-Mail Attachment
Block or just monitor users trying to send confidential files through e-mail attachment. Content Aware Protection supports most common e-mail clients: Outlook, Thunderbird, Lotus Notes, etc.

Prevent sensitive data leaving via Outlook and Thunderbird
As attachment or even if confidential data is contained in the body text of an e-mail, it is prevented from being sent out and the incident is reported. Even if your company uses PGP for e-mail encryption the e-mail body is inspected before the content is encrypted and sent.

Filter data leaving through Web browsers

Firefox, Google Chrome and many other browsers are used on PCs and they represent a big concern for data loss since users can virtually upload any file they have access to. Uploads to websites like sendspace.com or to their Dropbox web interface account for many data thefts. Therefore it is vital to monitor all file accesses by web browsers before the file reaches the internet. This can be done only at the endpoint level like Endpoint Protector does. Preventing data loss on the gateway is not working in these cases.

Filter data use through different Applications before leaving the protected endpoint

Endpoint Protector secures the use of confidential data in many applications such as Skype, Yahoo Messenger, Dropbox, Outlook, etc.

Endpoint Protector Client Self Defense

Provides protection even on PCs where users have Administrative rights.

Protected Endpoint Client(s)

- Windows 8 (32/64bit)
- Windows 7 (32/64bit)
- Windows Vista (32/64bit)
- Windows XP (SP2) (32/64bit)
- Windows 2003/2008 (32/64bit)

Directory Service (not required)

- Active Directory

Endpoint Protector Device Control module (is required)

Endpoint Protector 4 is the only DLP solution available as hardware or virtual appliance. Securing your network with Endpoint Protector saves you lots of time during implementation and administration compared to other solutions so you can take focus on other tasks or go home early knowing your computers are protected.

Endpoint Protector Hardware Appliance

The Endpoint Protector Hardware Appliances are available in different capacities to fit your business needs. All Hardware Appliances are based on the latest and most energy efficient hardware available.

Selected Models (more available)	A20	A50	A100	A250	A1000
Protection for Endpoints (Windows / Mac)	20	50	100	250	1000
Additional capacity	4	10	20	50	200
Housing (Rack mount)	Stand-alone	1U	1U	1U	1U
Processor	ULV Single Core	ULV Dual Core	ULV Dual Core	1X Dual Core	1X Quad Core
Hard Drive	320 GB	320 GB	320 GB	500 GB	2X 1TB (Raid 1)
Power Supply	60W 100-240V (external)	200W 100-240V	200W 100-240V	260W 100-240V	260W 100-240V
Hardware Warranty	1-year included. Additional warranty and replacement options are available.				

Device Control for Endpoints (Desktops, Laptops, etc.) is another feature available for Data Loss Prevention

Endpoint Protector offers additional features for controlling portable storage devices and ports on Windows, Mac OS X and Linux computers for Data Loss Prevention. With Device Control, IT Administrators receive detailed reports and logs indicating the path of a transferred file and they are also able to save a copy of those files, through File Tracing & File Shadowing.

Mobile Device Management (MDM) for iOS and Android smartphones and tablets

Strong security policies can be applied on iOS and Android mobile devices, too. Features like Remote Nuke (Wipe), Remote Lock are required in case a device is lost or stolen and has confidential data on it. Tracking & Locating mobile devices are possible with MDM by Endpoint Protector, among other security features.

Endpoint Protector Virtual Appliance

Endpoint Protector Virtual Appliance can be used by all business sizes. The Virtual Appliance is available in VMX, OVF and VHD formats to be compatible with the most popular virtualization platforms.

Using the Virtual Appliance you can protect against unauthorized device use and data loss in your network within minutes.

Supported Virtual Environments	Version	.ovf	.vmx	.vhd
VMware Workstation	7.1.4	-	*	-
VMware Player	3.1.4	-	*	-
VMware vSphere (ESXi)	5.0.0	*	-	-
Oracle VirtualBox	4.1.16	*	-	-
Parallels Desktop for Mac	7.0.1	-	*	-
Microsoft Hyper V (2008 R2)	6.1	-	-	*

Other virtualization environments are supported as well.

Endpoint Protector offers you a safe and secure working environment with mobile and portable devices. User efficiency is not restricted since any authorized device can be used continuously on protected PCs while the network's endpoint security policy is enforced.

Contact your local partner for more information:

Created on 06-Mar-2013

ENDPOINT PROTECTOR 4

Mobile Device Management (MDM) for iOS and Android

Mobile Device Management is a module of the Endpoint Protector DLP (Data Loss Prevention) Suite especially covering the security needs arising by the increased use of company owned or personal (BYOD) mobile devices in enterprises and institutions.

Endpoint Protector is an all in one solution that makes it possible for IT Administrators to implement and manage a Data Loss Prevention Solution throughout their network covering computers (Windows, Mac OS X, Linux) and mobile devices (iOS and Android) in an efficient and economical way.

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.

With Endpoint Protector 4 being offered as hardware or virtual appliance, it can be setup in minutes, allowing you to dramatically reduce the risks posed by internal threats that could lead to mobile devices and data being leaked, stolen, damaged or otherwise compromised.

Key Advantages

- Protection for iOS and Android
- Hardware or Virtual Appliance can be implemented and setup within minutes
- Web-based interface
- Intuitive management of mobile devices and endpoints
- Pro-active protection against device abuse and data theft
- VMware ready

Mobile Endpoint Security

Strong Security Policies enforced on companies' smartphones and tablets will ensure a proactive protection of business critical data wherever and on whatever mobile device they are accessed from.

Supports iOS and Android Mobile Devices

Controlling and managing the two most popular and strongest growing mobile platforms to protect your company data.

Password Enforcement

Enforce periodical change of password either directly over-the-air or with the user involvement.

Tracking and Locating

Closely monitor company's mobile devices fleet and know at all times where your company sensitive data is. For iOS the EPP MDM app needs to be installed on the device.

Remote Wipe (Nuke) / Remote Lock - Theft Protection

Avoid confidential data reaching into the wrong hands by having over-the-air control and enforce Remote Nuke of device (remote data wiping) or device locking in case of mobile device loss and theft.

Restrictions for iOS

Make sure only business related use is possible if desired. Disable features such as iCloud, FaceTime, YouTube, App Store, In-App Purchases, iTunes, Siri, Camera if not compliant to company policy.

Locate Lost Device by Play-Sound (for Android only)

Easy detection of any misplaced mobile device by enabling over-the-air a loud favorite song to be played just enough time to locate your lost smartphone / tablet.

Manage E-Mail and Wi-Fi Settings on iOS devices

Manage over-the-air E-Mail and Wi-Fi Settings.

Wipe E-Mail and Wi-Fi Settings on iOS devices

Wipe remotely company E-Mail Content and Settings, Wi-Fi Settings. Company E-Mail content can be deleted while personal E-Mail accounts and content remain untouched.

App Monitoring

Make sure no malware or untrusted apps will compromise company critical data by having a complete reporting of all installed apps on each personally or company owned smartphone and tablet.

Support for Bring-Your-Own-Device Model

Have complete control over sensitive company data no matter if stored on privately or company owned devices and focus on making employees work more efficient without compromising any business critical data or restricting personal usage.

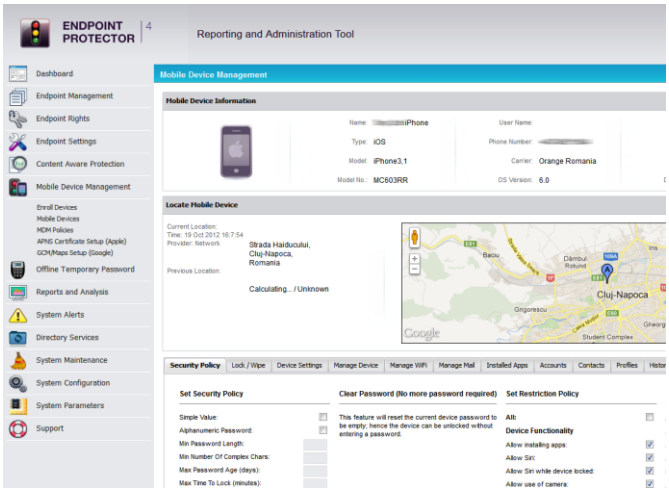
Companies have to clearly define and enforce mobile device management policies to protect themselves!

Key Benefits

- Enforces mobile device use policy
- Protecting company data
- Immediate control over mobile device use
- Over-the-air deployment
- Minimal impact and effort for users and admins
- Compliance
- BYOD security solution

Centralized Web based Management / Dashboard

Centrally manages the use of mobile devices through the web based Administrative & Reporting interface, meets the needs of management and IT security staff and offers real-time information about organization wide controlled device activity.



Mobile Device Inventory Management

Allows for an easy control and inventory over company or employee owned mobile device fleet with detailed logging and reporting of devices activity for later auditing.

Device Encryption

iPhones and iPads come with build in 256bit AES hardware encryption that is always active and enforced when setting a password to the device.

Self and Over-the-Air Enrollment / Provisioning

The self or over-the-air one-time-code enrollment process will ensure an easy and secured deployment and enrollment of the MDM platform in any company existing IT infrastructure.

Asset Management for Mobile Devices

Easy way to keep an overview over company owned and personal owned (BYOD) mobile devices.

Mobile Devices Supported

- iPad, iPhone, iOS 4.0, iOS 5.0, iOS 6.0, iOS 7.0
- Android 2.2+
- some features are available only for newer OS versions

Requirements for MDM

- For iOS MDM, a free Apple Push Notification Service (APNS) account (made with an Apple ID) is required.
- For Android MDM, a free Google Cloud Messaging for Android (GCM) account (made with Google Account) is required.

Feature Overview and Comparison for iOS and Android

Our Feature list for iOS and Android is being extended in parallel and continues to grow to cover always new and emerging security requirements.

MDM Features	iOS	Android
Strong Security Policies	✔	✔
Password length	✔	✔
Password retries	✔	✔
Password quality (Numeric, Alphabetical, etc.)	✔	✔
Screen lock time	✔	✔
Password Enforcement	✔	✔
Enforce Device Encryption (Device/OS build-in encryption)	✔	(coming soon)
Tracking and Locating	✔ (app required)	✔
Locate Lost Device (play sound)		✔
Remote Lock	✔	✔
Remote Nuke (Remote Wipe)	✔	✔
Wipe Device	✔	✔
Wipe company E-Mail content/settings	✔	
Wipe SD Card		✔
App Monitoring	✔	✔
Enrollment / Provisioning Over-the-Air	✔	✔
E-mail enrollment or URL	✔	✔
SMS enrollment (US, UK, Germany + 100 more countries supported)	✔	✔
QR-Code	✔	✔
Over-the-Air Provisioning/Control	✔	✔
E-Mail Settings (Provision and Wipe company E-Mails and settings) Wi-Fi Settings	✔	
Restrict use of		
iTunes, iCloud, App Store, In-App Purchases Siri Camera, FaceTime Enforce encrypted iTunes backup Safari, YouTube etc.	✔ ✔ ✔ ✔ ✔ ✔ ✔ ✔	
Mobile Device Asset Management	✔	✔
Many More Features Available	...	...
Versions Supported	Apple iOS 4, 5, 6, 7	Android 2.2+

Certain device security and management features capabilities are not supported on older OS versions and / or devices.

Device Control for Endpoints (Desktops, Laptops, etc.) is another feature available for Data Loss Prevention

Endpoint Protector offers additional features for controlling portable storage Devices and ports on Windows, Mac OS X and Linux computers for Data Loss Prevention.

Content Aware Protection for Endpoints (Laptops, etc.)

Content Aware Protection for Windows Desktop Endpoints offers detailed control over sensitive data leaving the company's network. Through efficient content inspection, transfers of important company documents will be logged, reported and blocked. This feature will prevent data leakage through all possible exit points, from USB devices to applications including Microsoft Outlook, Skype, Yahoo Messenger or Dropbox.

Endpoint Protector Hardware Appliance

The Endpoint Protector Hardware Appliances are available in different capacities to fit your business needs. All Hardware Appliances are based on the latest and most energy efficient hardware available.

Endpoint Protector Virtual Appliance

Endpoint Protector Virtual Appliance can be used by all business sizes. The Virtual Appliance is available both in VMX, OVF and VHD formats to be compatible with the most popular virtualization platforms.

Using the Virtual Appliance you can protect against unauthorized device use and data loss in your network within minutes.

VMWARE CERTIFIED VIRTUAL APPLIANCE

vmware READY

Supported Virtual Environments	Version	.ovf	.vmx	.vhd
VMware Workstation	7.1.4	-	*	-
VMware Player	3.1.4	-	*	-
VMware vSphere (ESXi)	5.0.0	*	-	-
Oracle VirtualBox	4.1.16	*	-	-
Parallels Desktop for Mac	7.0.1	-	*	-
Microsoft Hyper V (2008 R2)	6.1	-	-	*

Other virtualization environments are supported as well.

Endpoint Protector offers you a safe and secure working environment with mobile devices / portable storage and endpoint devices. User efficiency is not restricted since any authorized device can be used continuously while the network's endpoint security policy is enforced.

Contact your local partner for more information:

Trusted Device

COSOSYS

Created on 03-Jan-2013