ENDPOINT PROTECTOR 4

Data Loss Prevention for Mac OS X
Protecting Macs in your network and securing sensitive data against loss, leakage and theft

Most company networks are seeing more and more Macs used as regular work computers next to the well-established and secured Windows desktops and laptops.
To secure Macs against data loss has become a top priority for every IT department in charge of securing data.

Data Loss Prevention for Macs from Endpoint Protector is providing the industry's only solution for Device Control and Content Aware Protection to secure Mac endpoints from USB port to cloud services like Dropbox.

To secure any sensitive data against leakage and theft through online applications, cloud services, E-Mail, portable/removable devices and other exit points is easy to implement and enforce with Endpoint Protector DLP for Mac, giving Administrators unparalleled control over device and data use on Mac OS X.

As an out-of-the-box solution administrators are able to block or monitor all data transfers using easy to configure policies. All with a short implementation time using a Virtual/Hardware-Appliance or Amazon Web Services EC2 to manage all Mac and Windows endpoints from one place.

Any type of data can be protected, from regulated data such as Credit Card Numbers or Social Security Numbers to different File Types or Keywords defined in individual dictionaries as part of DLP policies.

"I am calmer since we've been using the Endpoint Protector DLP solution. It's good to know that it's not even theoretically possible for someone to steal original or synchronized movies with the help of USB sticks or DVDs from our studio."
Executive Director
Mafilm Audio

Key Advantages

- Mac OS X and Windows support
- Block / report movement of confidential data
- Easy policy setup and enforcement
- Offline protection
- Available as Hardware / Virtual Appliance / AWS EC2 can be implemented in minutes
- Web-based intuitive interface
- Pro-active Mac endpoint protection against device abuse, data loss and data theft
- VMware ready

Using Macs, take control of data flow to Applications:

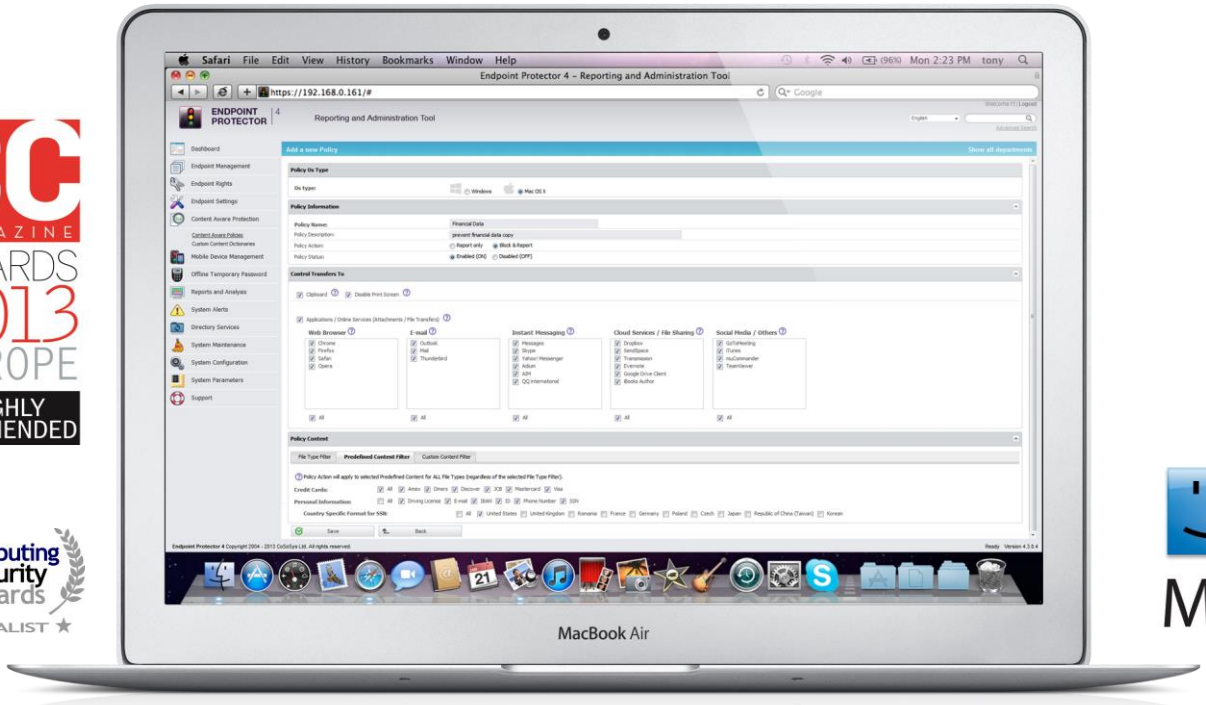
- **E-Mail Clients**
  - Mail
  - Outlook
  - Thunderbird
- **Web Browsers**
  - Safari
  - Firefox
  - Chrome
  - Opera
- **Cloud Services/ File Sharing**
  - Dropbox
  - iCloud, AirDrop
  - Google Drive, Evernote
- **Instant Messaging**
  - iMessage
  - Skype
  - Yahoo Messenger, etc.
- **Other Applications**
  - iTunes,
  - Team Viewer,
  - EasyLock, and more

Devices/Ports:

- USB Devices
- USB Flash Drives
- Thunderbolt
- FireWire
- iPhones / iPads / iPods
- Memory Cards (SD, CF...)
- Card Readers (int., ext.)
- CD/DVD-Burner (int., ext.)
- External HDDs
- Printers (local)
- Webcams
- WiFi Network Cards
- Digital Cameras
- Smartphones
- MP3 Player/Media Players
- Bluetooth Devices

SC MAGAZINE AWARDS 2013 EUROPE
HIGHLY COMMENDED

2012 Computing Security Awards
★ FINALIST ★



Mac

Filter by Regulated Data/Predefined Content or keywords

Filter the data leaving the protected endpoints based on a predefined content format which includes:

- Credit Card Details (CCN) *all major Credit Cards supported
- Social Security Numbers (SSN) *many different country formats supported
- Bank Account Information
- etc.

Filter by File Type

Endpoint Protector blocks the documents leaving the company based on their true file type. Supports the most important file types in use: office files, graphic files, archives, executables, media and others.

Filter by Dictionary

The Content Aware Protection module looks for keyword matching data and stops containing files 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.

Filter data leaving through Web browsers

Safari, Firefox, Google Chrome and other browsers are used and 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 the 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.

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: Mail, Outlook and Thunderbird.

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.

Enforce policy | Define sensitive data | Inspect data in motion | Stop data loss

Supports Mac OS X and Windows endpoints

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

Protected Endpoint Client(s)

- Mac OS X 10.5+
- Windows XP, Vista, 7, 8 (32/64bit)

Directory Service (not required)

- Active Directory

Endpoint Protector Device Control module (is required)

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

Strong security policies can be applied on both iOS and Android mobile devices. 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.

Hardware Appliance

Endpoint Protector is available as Hardware Appliances with different capacities ranging from capacities of just 20 endpoints to 5.000 and more.

Virtual Appliance

As Virtual Appliance Endpoint Protector is available for most virtualization platforms in VMX, OVF, VHD, etc formats.

Amazon Web Service EC2

On Amazon Web Services Endpoint Protector is available as ready to use EC2 instance.

Find more info at: www.EndpointProtector.com
contact@endpointprotector.com
+1-888-271-9349

CoSoSys
Germany
E-Mail:
sales.de@cososys.com
Phone: +49-7541-978-2627-0
Fax: +49-7541-978-2627-9

CoSoSys
North America
sales.us@cososys.com
+1-888-271-9349

CoSoSys Ltd.
sales@cososys.com
+40-264-593110
+40-264-593113

Contact your local partner for more information:

Created on 13-May-2013