ENDPOINT PROTECTOR 4

Data Loss Prävention (DLP) für Mac OS X schützt Macs in Ihrem Netzwerk und sichert vertrauliche Daten gegen Verlust und Diebstahl sowie gegen Datenlecks

In einem Großteil der Unternehmensnetzwerke werden neben den etablierten und geschützten Windows Desktops/Laptops mehr und mehr Macs als Arbeitsgeräte verwendet.
Um Datensicherheit zu gewährleisten nimmt der Schutz von Macs in den IT Abteilungen eine Schlüsselrolle ein.

Endpoint Protector Data Loss Prävention für Macs bietet die branchenweit einzige Lösung für Device Control und Content Aware Protection zum Schutz der Mac-Endpunkte vor missbräuchlicher Verwendung von USB Geräten, Cloud-Diensten wie Dropbox und vielen weiteren Schnittstellen.

Sensible Daten vor Lecks und Diebstahl über Online- und Cloud-Dienste, E-Mail, tragbare Speichermedien und über weitere Wege zu schützen ist mit der DLP Lösung für Macs leicht umsetzbar. Die Implementierung erfolgt intuitiv und ermöglicht den IT Administratoren sofort einmalige Möglichkeiten zur Kontrolle der Geräte- und Datenverwendung mit Macs OS X.

Als "out-of-the-Box" Lösung gibt sie den Administratoren zahlreiche Funktionen an die Hand um Datentransfers zu sperren, aufzuzeichnen und individuell konfigurierbare Richtlinien zu erstellen. Mit der Virtual/Hardware Appliance oder Amazon Web Services EC2 können alle Mac- und Windows Endpunkte von einem Ort aus verwaltet werden.

Viele Daten können durch DLP Richtlinien geschützt werden; seien es Kreditkarten- und Sozialversicherungsdaten oder aber bestimmte Dateitypen und Schlüsselwörter, die in einem individuellen Wörterbuch bestimmt werden können.

"Ich bin ruhiger seit wir die Endpoint Protector DLP Lösung verwenden. Es tut gut zu wissen, dass es für Unberechtigte nicht einmal theoretisch möglich ist originale oder synchronisierte Filme per USB Stick oder DVD-Laufwerk aus unserem Studio zu stehlen."

Executive Director
Mafilm Audio

Wichtigste Vorteile

- Mac OS X und Windows werden unterstützt
- Kopieren von vertraulichen Daten wird blockiert und/oder aufzeichnen
- Leichtes erstellen und Durchsetzen von Richtlinien
- Offline Schutz
- Erhältlich als Hardware / Virtual Appliance / AWS EC2 kann in Minuten implementiert werden
- Web-basierte intuitive Steuerungsoberfläche
- Pro-aktiver Schutz für Mac Endpunkte vor Datenmissbrauch, -Verlust und -Diebstahl
- VMware kompatibel

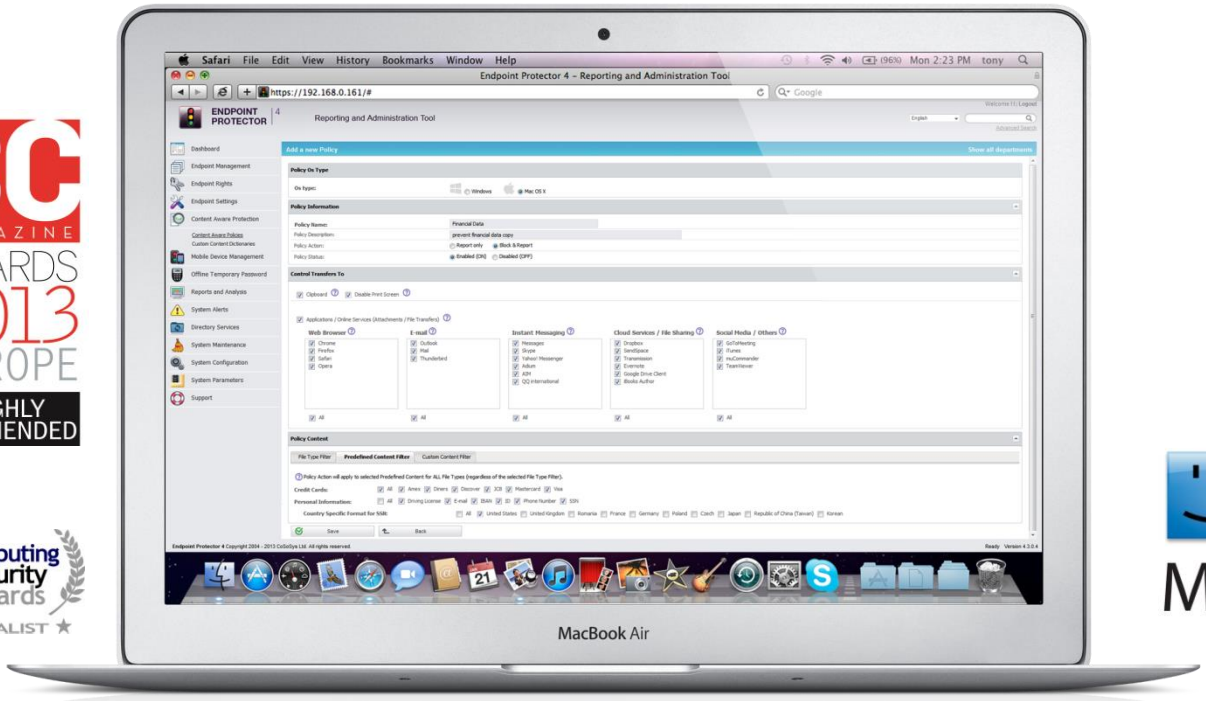
Datentransfers von und zu folgenden Schnittstellen kontrollieren:

Applikationen:

- **E-Mail Clients**
  - Mail
  - Outlook
  - Thunderbird
- **Web Browser**
  - Safari
  - Firefox
  - Chrome
  - Opera
- **Cloud Dienste/ File Sharing**
  - Dropbox
  - iCloud, AirDrop
  - Google Drive, Evernote
- **Instant Messaging**
  - iMessage
  - Skype
  - Yahoo Messenger, etc.
- **Andere Anwendungen**
  - iTunes,
  - Team Viewer,
  - EasyLock, u.v.m.

Geräte/Ports:

- USB Geräte
- USB Flash Drives
- Thunderbolt
- FireWire
- iPhones / iPads / iPods
- Speicherkarten
- Kartenleser (int., ext.)
- CD/DVD-Brenner
- Externe Festplatten
- lokale Drucker
- Webcams
- WiFi Netzwerkkarten
- Digitalkameras
- Smartphones
- MP3 Player/Media Player
- Bluetooth Geräte



SC MAGAZINE AWARDS 2013 EUROPE HIGHLY COMMENDED

2012 Computing Security Awards ★ FINALIST ★

Mac

Inhalte nach regulierten Daten und vordefinierten Inhalten und Schlüsselbegriffen filtern

Filtert die Daten beim Verlassen des geschützten Endpunktes basierend auf den vordefinierten Richtlinien bezüglich Inhalten wie:

- Kreditkartendaten (CCN) *alle gängigen Kreditkarten werden unterstützt
- Sozialversicherungsnummern (SSN) *viele verschiedene Länderformate werden unterstützt
- Kontendaten
- etc.

Dateityp-Filter

Endpoint Protector sperrt Dokumente, die das Netzwerk verlassen auf Basis ihres wahren Dateityps. Alle gängigen Dateitypen werden unterstützt: Office Dateien, Grafikdateien, Archivdateien, ausführbare Dateien, Mediadateien und weitere.

Schlüsselwort-/Wörterbuch-Filter

Das Content Aware Protection Modul durchsucht Daten nach Schlüsselbegriffen, stoppt den Transfer wenn vordefinierte Wörter enthalten sind und verhindert damit Datenlecks und –Diebstahl über die geschützten Endpunkte. Mehrere Wörterbücher können erstellt und als Richtlinie angewendet werden.

Copy & Paste von vertraulichen Daten verhindern

Die Überwachung der Zwischenablage verhindert, dass User per Copy & Paste sensible Daten via Outlook Client, Webmail-Anwendungen oder über andere Kanäle entwenden.

Filter von Datentransfers über Webbrowser

Safari, Firefox, Google Chrome und weitere Browser bieten zahlreiche Möglichkeiten zum Upload von Daten. So z.B. mittels Webseiten wie sendspace.com oder der Dropbox Weboberfläche. Folglich ist es wichtig festzulegen, welche Daten über einen Browser den Mac verlassen dürfen und welche nicht. Endpoint Protector bietet die Möglichkeit, die über eine Gateway Lösung nicht möglich ist.

Filterung der Datennutzung durch verschiedene Anwendungen vor Verlassen des Macs

Endpoint Protector sichert die Verwendung vertraulicher Daten durch zahlreiche Applikationen wie Skype, Yahoo Messenger, Dropbox, Outlook, etc.

Verhindert den Transfer von Dateien als E-Mail Anhang

Zeichnet Datentransfers als E-Mail Anhang auf und/oder verhindert sie. Content Aware Protection unterstützt die populärsten E-Mail Clients: Mail, Outlook und Thunderbird.

Sicherheitsrichtlinien für bestimmt Einheiten erstellen

Content Aware Protection Richtlinien bieten eine flexible Kontrolle durch das Scannen von Dokumenten und dem Zuteilen von Berechtigungen auf User-, Computer- oder Abteilungsebene.

Richtlinien durchsetzen | Sensible Inhalte definieren | Datentransfers überwachen | Datenverlust stoppen

Support von Mac OS X und Windows Endpunkten

Datenflüsse auf den populärsten Plattformen aufzeichnen und/oder verhindern zum bestmöglichen Schutz Ihrer Unternehmensdaten.

Geschützte Client Endpunkte

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

Directory Dienste (nicht erforderlich)

- Active Directory

Das Modul Device Control von Endpoint Protector ist erforderlich.

Mobile Device Management (MDM) für iOS und Android Smartphones und Tablets

Starke Sicherheitsrichtlinien für mobile iOS- und Android Geräte. Funktionen wie externes Datenlöschen, Gerät sperren helfen bei Diebstahl oder Verlust eines Geräts, dass die Daten nicht in die Hände Unberechtigter gelangen. Verfolgung & Ortung mobiler Geräte und viele weitere Sicherheitsfunktionen sind mit MDM von Endpoint Protector leicht anwendbar.

Hardware Appliance

Endpoint Protector ist als Hardware Appliances in verschiedenen Größen für Kapazitäten von nur 20 bis zu 5000+ Endpunkten erhältlich.

Virtual Appliance

Als Virtual Appliance ist Endpoint Protector für die meisten Virtualisierungsplattformen erhältlich: VMX, OVF, VHD, etc.

Amazon Web Service EC2

In Amazon Web Services ist Endpoint Protector als betriebsbereite EC2 Instance erhältlich.

Mehr Informationen unter: www.EndpointProtector.de
contact@endpointprotector.com
+49-7541-978-2627-0 DW.1

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

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

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

Kontaktieren Sie unseren lokalen Partner für nähere Informationen:

Created on 24-May-2013