ENDPOINT PROTECTOR 4

Prévention des Pertes de Données pour Mac OS Protège les Macs de votre réseau et sécurise les données sensibles contre la perte, la fuite et le vol

La plupart des entreprises utilisent de plus en plus de Macs en tant qu'ordinateurs de travail à côté des ordinateurs de bureau et portables bien connus et sécurisés sous Windows. Sécuriser les Macs contre la perte de données est devenue une priorité pour chaque département IT chargé de sécuriser les données.

La Prévention des Pertes de Données pour les Macs par Endpoint Protector fournit la seule solution de l'industrie pour le Contrôle des Périphériques et la Protection de Contenu pour sécuriser les terminaux Mac de ports USB jusqu'aux services cloud tels que Dropbox.

Pour sécuriser toute donnée sensible contre la fuite et le vol via des applications en ligne, services cloud, E-mail, dispositifs portables/amovibles et d'autres points de sortie est facile à implémenter et renforcer avec Endpoint Protector DLP pour Mac, donnant aux administrateurs un contrôle sans précédent sur l'utilisation des dispositifs et des données sur Mac OS.

En tant que solution out-of-the-box les administrateurs sont capables de bloquer ou surveiller tous les transferts de données en utilisant des politiques faciles à configurer. Tout cela dans un court temps d'implémentation utilisant une Appliance Virtuelle/Matérielle ou Amazon Web Services EC2 pour gérer tous les terminaux Mac et Windows à partir d'un seul endroit.

Tout type de données peut être protégé, à partir des données réglementées telles que les Numéros de Cartes de Crédit ou Numéros de Sécurité Sociale jusqu'à des Différents Types de Fichiers ou Mots-Clé définis dans des dictionnaires individuels comme part des politiques DLP.

"Je suis plus calme maintenant que j'utilise la solution DLP Endpoint Protector. C'est bon de savoir qu'il est impossible même théoriquement pour quelqu'un de voler des films originaux ou synchronisés par le biais des clés USB ou des DVDs de notre studio."

Directeur Exécutif
Mafilm Audio

Avantages-clé

- Support pour Mac OS X et Windows
- Blocage / surveillance des mouvements de données confidentielles
- Mise en place et renforcement facile des politiques
- Protection Offline
- Disponible en tant qu'Appliance Matérielle / Virtuelle / AWS EC2 peut être implémentée en quelques minutes
- Interface Web intuitive
- Protection pro-active des terminaux Mac contre l'abus des dispositifs, la perte et le vol de données
- Prêt pour VMware

Utilisant des Macs, contrôlez les flux de données vers

Applications:

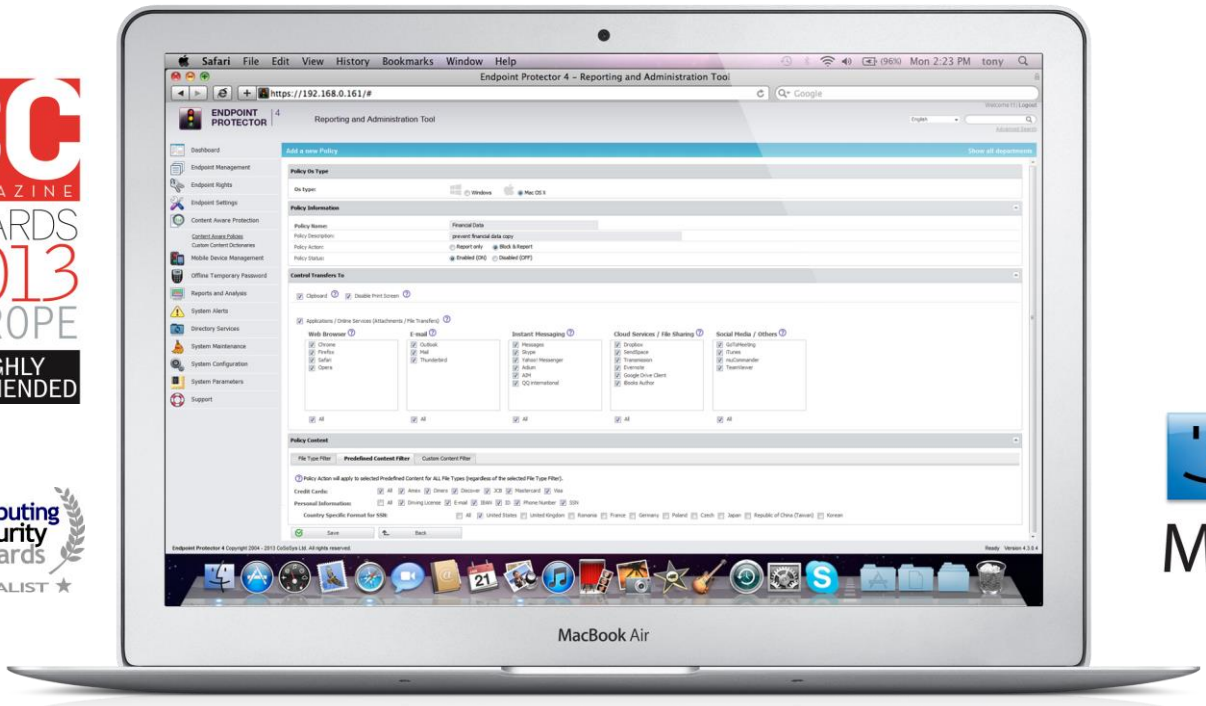
- **Clients E-Mail**
  - Mail
  - Outlook
  - Thunderbird
- **Navigateurs Internet**
  - Safari
  - Firefox
  - Chrome
  - Opera
- **Services Cloud/ Partage des Fichiers**
  - Dropbox
  - iCloud, AirDrop
  - Google Drive, Evernote
- **Messagerie Instantanée**
  - iMessage
  - Skype
  - Yahoo Messenger, etc.
- **Autres Applications**
  - iTunes,
  - Team Viewer,
  - EasyLock, etc.

Dispositifs/Ports:

- Dispositifs USB
- Disques Flash USB
- Thunderbolt
- FireWire
- iPhones / iPads / iPods
- Cartes de Memoire
- Lesteurs de Cartes
- Graveur CD/DVD
- Disques Durs Externes
- Imprimantes (locale)
- Webcams
- Cartes Réseau WiFi
- Appareils Photo Numériques
- Smartphones
- Baladeurs MP3/ Media Players
- Dispositifs Bluetooth
- etc.

SC MAGAZINE AWARDS 2013 EUROPE HIGHLY COMMENDED

2012 Computing Security Awards ★ FINALIST ★



Mac

Filtrage par Données Réglementées/Contenu Prédéfini ou Mots-Clé

Filtrage des données quittant les terminaux protégés en se basant sur un format de contenu prédéfini qui inclut:

- Détails des Cartes de Crédit (CCN) *toutes les Cartes de Crédit majeures supportées
- Numéros de Sécurité Sociale (SSN) *différents formats spécifiques aux pays supportés
- Informations de Compte Bancaire
- etc.

Filtrage par Type de Fichier

Endpoint Protector bloque les documents quittant l'entreprise en se basant sur leur type de fichier reel. Supporte les plus importants types de fichiers utilisés: fichiers office, fichiers graphiques, archives, exécutables, média et autres.

Filtrage par Dictionnaire

Le module Protection de Contenu cherche les données corréspondantes aux mots-clé et arrête les fichiers qui les contiennent d'être siphonnés ou volés via les points de sortie protégés. Multiples dictionnaires peuvent être créés pour les politiques.

Surveillance du Clipboard pour prévenir de Copier & Coller les données sensibles

Surveiller le Clipboard empêchera les utilisateurs de copier & coller les données sensibles de l'entreprise dans les clients outlook, les apps web mail, ou d'autres canaux par lesquels l'information pourrait être siphonnée.

Filtrage des données sortant via les navigateurs Internet

Safari, Firefox, Google Chrome et d'autres navigateurs sont utilisés et représentent un souci majeur pour les pertes de données car les utilisateurs peuvent télécharger pratiquement tout fichier auquel ils ont accès. Des téléchargements vers des sites tels que sendspace.com ou vers l'interface web de Dropbox sont la cause de beaucoup de vols de données. C'est pourquoi il est vital de surveiller tous les accès aux fichiers par les navigateurs avant que le fichier atteint l'internet. Cela peut être fait uniquement au niveau du terminal comme Endpoint Protector le fait. La prévention des pertes de données au niveau du gateway ne fonctionne pas dans ces cas.

Filtrage de l'utilisation des données par des différentes applications avant de quitter le terminal protégé

Endpoint Protector sécurise l'utilisation des données confidentielles par beaucoup d'applications telles que Skype, Yahoo Messenger, Dropbox, Outlook, etc.

Empêcher les données sensibles de sortir en PJ d'E-mail

Bloquez ou surveillez les utilisateurs qui essayent d'envoyer des fichiers confidentiels en tant que pièce-jointe d'e-mail. La Protection de Contenu supporte les plus connus clients d'e-mail: Mail, Outlook et Thunderbird.

Créer des politiques de sécurité pour des entités spécifiques

Les politiques de Protection de Contenu offrent un contrôle flexible de l'inspection des documents, en permettant de sélectionner les utilisateurs, ordinateurs, groupes et départements à être surveillés.

Renforcer les politiques Définir les données sensibles Inspecter les données en mouvement Arrêter les pertes de données

Support pour les terminaux Mac OS X et Windows

Surveillance et blocage des flux de données sur les plate-formes les plus populaires et les plus puissantes pour protéger vos données d'entreprise.

Terminaux Clients Protégés

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

Service d'Annuaire (pas requis)

- Active Directory

Module Contrôle des Périphériques Endpoint Protector (requis)

Mobile Device Management (MDM) pour smartphones et tablettes iOS et Android

Des fortes politiques de sécurité peuvent être appliquées sur les dispositifs mobiles iOS et Android. Des fonctionnalités telles que Suppréssion à Distance, Vérrouillage à Distance sont requises pour les cas où un dispositif est perdu ou volé ayant des données confidentielles déssus. Il est possible de Tracer et Localiser les dispositifs mobiles avec MDM par Endpoint Protector, entre autres fonctionnalités de sécurité.

Appliance Hardware

Endpoint Protector est disponible en tant que Appliances Hardware ayant des différentes capacités allant de 20 terminaux jusqu'à 5.000 et plus.

Appliance Virtuelle

En tant qu'Appliance Virtuelle Endpoint Protector est disponible pour la majorité des plate-formes de virtualisation dans les formats VMX, OVF, VHD, etc.

Amazon Web Service EC2

Sur Amazon Web Services Endpoint Protector est disponible en tant qu'instance EC2 prête à utiliser.

Pour plus d'infos: 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

Contactez votre partenaire local pour plus d'informations:

Created on 12-Jun-2013