ENDPOINT PROTECTOR 4

Mobile Device Management (MDM) pour iOS et Android

Mobile Device Management est un module de la Suite Endpoint Protector DLP (Data Loss Prevention) Suite qui couvre les besoins spécifiques issus de l'usage toujours croissant des dispositifs mobiles d'entreprise ou personnels (BYOD) dans les entreprises et institutions.

Endpoint Protector est une solution tout-en-un qui fait possible que les Administrateurs IT implémentent et gèrent une solution de Prévention des Pertes de Données dans tout leur réseau couvrant les ordinateurs (Windows, Mac OS X, Linux) et les dispositifs mobiles (iOS and Android) d'une façon efficace et économique.

Dans un monde où les dispositifs mobiles transforment la manière dont on travaille et on vit, Endpoint Protector 4 est désigné pour maintenir la productivité et rendre le travail convenable, sûr, convivial.

Avec Endpoint Protector 4 offert comme hardware ou virtual appliance, il peut être mis en place en quelques minutes, vous permettant de réduire les risques posés par les menaces internes qui peuvent conduire à des fuites, vols, endommagements ou corruptions des dispositifs et données mobiles.

Principaux Avantages

- Protection pour iOS et Android
- Hardware ou Virtual Appliance peut être implémentée et mise en place dans des minutes
- Interface Web-basée
- Gestion intuitive des dispositifs mobiles et terminaux
- Protection pro-active contre l'abus des dispositifs et le vol de données
- Prêt pour VMware

Sécurité des Terminaux Mobiles

Des fortes Politiques de Sécurité appliquées sur les smartphones et tablettes de l'entreprise assureront une protection proactive des données critiques d'entreprise n'importe d'où elles ont été accédées.

Compatible avec les Dispositifs Mobiles iOS et Android

Contrôlez et gérez les deux plate-formes mobiles les plus populaires et croissantes pour protéger les données de votre entreprise.

Renforcement du Mot de Passe

Renforcez le changement périodique du mot de passe soit directement à distance soit avec l'intervention de l'utilisateur.

Surveillance et Localisation

Surveillez la flotte de dispositifs mobiles de l'entreprise et sachez en tout moment où se trouvent les données sensibles de l'entreprise. Pour iOS l'app EPP MDM doit être installée sur le dispositif.

Suppression/Verrouillage à Distance–Protection contre le vol

Evitez que les données confidentielles arrivent entre mauvaises mains en prenant le contrôle à distance et en renforçant la suppression à distance des données ou le verrouillage du dispositif en cas de perte ou vol du dispositif mobile.

Restrictions pour iOS

Assurez-vous que seul l'usage professionnel est possible si désiré. Désactivez les fonctionnalités telles que iCloud, FaceTime, YouTube, App Store, Achats In-App, iTunes, Siri, Caméra si elles ne sont pas conformes à la politique de l'entreprise.

Localisation d'un Dispositif Perdu par Jouer un Son (Android)

Détection facile de tout dispositif mobile égaré en activant à distance un son à être joué juste le temps suffisant pour localiser votre smartphone/tablette perdu.

Gestion des Paramètres E-Mail et Wi-Fi sur les mobiles iOS

Gérez les paramètres E-Mail et Wi-Fi à distance.

Suppression des Paramètres E-Mail et Wi-Fi sur les mobiles iOS

Effacez à distance le Contenu et Paramètres de l'E-Mail professionnel, les Paramètres Wi-Fi. Le contenu de l'E-Mail professionnel peut être supprimé tandis que les comptes et le contenu des e-mails personnels restent intacts.

Surveillance des Apps

Assurez-vous qu'aucun malware ou apps qui ne sont pas de confiance vont compromettre les données critiques de l'entreprise en ayant un rapport complet sur toutes les apps installées sur chaque smartphone ou tablette personnel ou d'entreprise.

Support pour le Modèle Bring-Your-Own-Device

Prenez le contrôle complet sur les données sensibles d'entreprise stockées sur des dispositifs mobiles personnels ou d'entreprise et concentrez-vous sur rendre le travail des employés plus efficace sans compromettre de données critiques ou restreindre l'usage personnel.

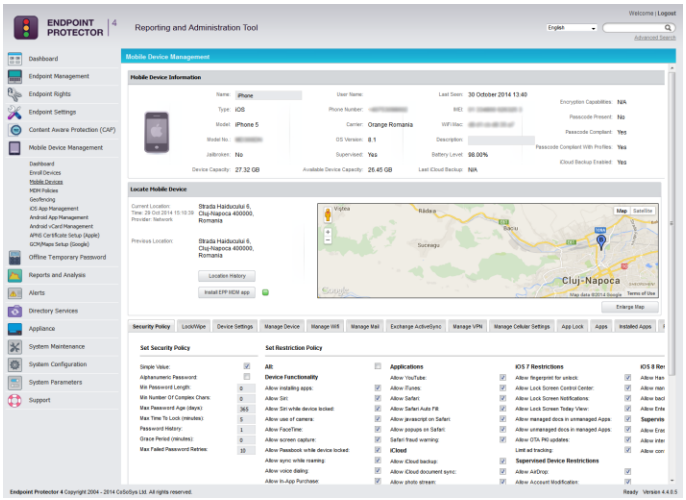
Les entreprises doivent définir clairement et renforcer les politiques des dispositifs mobiles pour se protéger!

Principaux Avantages

- Renforce les politiques d'usage des dispositifs mobiles
- Protège les données d'entreprise
- Conformité
- Solution de sécurité BYOD
- Contrôle immédiat sur l'utilisation des dispositifs mobiles
- Déploiement à distance
- Impact et effort minimal pour les utilisateurs et admins

Gestion Centralisée Web-basée / Tableau de Bord

Gère de manière centralisée l'utilisation des dispositifs mobiles via l'interface d'Administration & Rapports tout en répondant aux besoins de la direction et du service de sécurité IT et en offrant des informations en temps réel sur l'activité des dispositifs contrôlés dans toute l'organisation.



Gestion de l'Inventaire des Dispositifs Mobiles

Permet un contrôle et inventaire facile de la flotte des dispositifs mobiles personnels ou d'entreprise avec des journaux et rapports détaillés de l'activité des dispositifs pour un audit ultérieur.

Cryptage des Dispositifs

Les iPhones et iPads viennent avec un cryptage matériel 256bit AES embarqué qui est toujours active et renforcé lors de paramétrer un mot de passé sur le dispositif.
Assure la protection complète des données sensibles à l'intérieur et à l'extérieur de l'entreprise en renforçant le cryptage des dispositifs.

Auto-inscription et Inscription à Distance / Provisionnement

L'auto-inscription ou inscription à distance avec un one-time-code assurera un déploiement et une inscription facile et sûre de la plate-forme MDM dans toute infrastructure IT existante dans une entreprise.

Gestion d'Actifs pour les Dispositifs Mobiles

Une façon facile de maintenir une vue d'ensemble sur les dispositifs mobiles personnels (BYOD) ou d'entreprise.

Dispositifs Mobiles Supportés

- iPad, iPhone, iOS 4.0, iOS 5.0, iOS 6.0, iOS 7.0
- Android 2.2+
- certaines fonctionnalités disponibles uniquement pour les versions plus récentes d'OS

Réquisitions pour MDM

- Pour iOS MDM, un compte Apple Push Notification Service (APNS) gratuit (fait avec un Apple ID) est nécessaire.
- Pour Android MDM, un compte Google Cloud Messaging pour Android (GCM) gratuit (fait avec un Google Account) est nécessaire.

Vue d'ensemble des Fonctionnalités et Comparaison pour iOS et Android

Notre liste de Fonctionnalités pour iOS et Android est étendue en parallèle et continue à s'accroitre pour couvrir des réquisitions de sécurité toujours nouvelles.

Fonctionnalités MDM	iOS	Android
Enrollment	✔	✔
Inscription par e-mail, URL, le code QR ou SMS (Disponible pour l'Allemagne, Etats-Unis, Royaume-Uni, et plus de 100 autres pays)	✔	✔
Mot de passe forcées	✔	✔
Paramètre de Mot de passe (Longueur, max. Nombre de répétitions, numérique, lphabétique, etc.)	✔	✔
Temps pour verrouiller l'écran	✔	✔
Passwort erzwungen	✔	✔
Dispositifs de cryptage (appareil / OS cryptage intégré)	✔	✔
Localisation et suivi App nécessaire	✔ oui	✔ non
Remote Lock (blocage externe)	✔	✔
Nuke à distance (effacement à distance)	✔	✔
Daten auf Gerät löschen	✔	✔
Supprimer le contenu / paramètres de compte de messagerie d'entreprise	✔	
Supprimer la carte SD		✔
Gestion des applications mobile	✔	✔
Geofencing	✔	✔
Gestion d'actifs de dispositif mobile	✔	✔
Pousser les paramètres réseau	✔	✔
E-mail, VPN, WiFi	✔	
Bloquer WiFi, Bluetooth		✔
Limiter l'utilisation caméra	✔	✔
Over-the-air dispositif	✔	✔
Fixez des limites sur		
iTunes, iCloud, App Store, In-App Purchases Siri FaceTime Enforce encrypted iTunes backup Safari, YouTube etc.	✔ ✔ ✔ ✔ ✔ ✔ ✔ ✔	
Et beaucoup plus de fonctionnalités	...	...
Versions prises en charge	Apple iOS 4, 5, 6, 7, 8	Android 2.2+

Le Contrôle des Périphériques pour les Terminaux (Desktops, Laptops, etc.) est une autre fonctionnalité disponible pour la Prévention des Pertes de Données

Endpoint Protector offre des fonctionnalités additionnelles pour contrôler les Dispositifs de stockage portables et les ports sur Windows, Mac OS X et Linux pour la Prévention des Pertes de Données.

Protection de Contenu pour les Terminaux (Laptops, etc.)

La Protection de Contenu pour les Terminaux Windows Desktop offre un contrôle détaillé des données sensibles quittant le réseau de l'entreprise. Via l'inspection efficace du contenu, les transferts des documents importants d'entreprise seront journalisés, rapportés et bloqués. Cette fonctionnalité va prévenir les fuites de données via tous les points de sortie, des dispositifs USB jusqu'aux applications incluant Microsoft Outlook, Skype, Yahoo Messenger ou Dropbox.

Endpoint Protector Hardware Appliance

Les Appliances Hardware Endpoint Protector sont disponibles en différentes capacités pour répondre aux besoins de votre entreprise. Tous les Appliances Hardware sont bases sur le matériel le

Endpoint Protector Virtual Appliance

Endpoint Protector Virtual Appliance peut être utilisée par les entreprises de toute dimension. L'Appliance Virtuelle est disponible dans les formats VMX, OVF et VHD pour être compatible avec les plus populaires plate-formes de virtualisation.

En utilisant l'Appliance Virtuelle vous pouvez protéger contre l'utilisation non-autorisée des dispositifs et contre la perte de données dans votre réseau en quelques minutes.

VMWARE CERTIFIED VIRTUAL APPLIANCE

vmware READY

Environnements Virtuels Supportés	Version	.ovf	.vmx	.vhd	.xva	.pvm
VMware Workstation	7.1.4	-	*	-	-	-
VMware Workstation *	9.0.2	*	*	-	-	-
VMware Player *	6.0.0	*	*	-	-	-
VMware Fusion *	5.0.0	-	*	-	-	-
VMware vSphere (ESXi)	5.1.0	*	-	-	-	-
Oracle VirtualBox	4.2.18	*	-	-	-	-
Parallels Desktop for Mac	9.0.2	-	-	-	-	*
Microsoft Hyper-V Server	2008/2012	-	-	*	-	-
Citrix XenServer 64bit	6.2.0	-	-	-	*	-

Bitte kontaktieren Sie unseren Support, falls Ihre Plattform mit einem * gekennzeichnet ist.
Weitere Plattformen werden ebenfalls unterstützt.

Visitez http://www.EndpointProtector.fr pour un essai gratuit.

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 HQ
sales@cososys.com
+40-264-593110
+40-264-593113

Contactez votre partnenaire local pour plus d'informations:

Trusted Device

COSOSYS

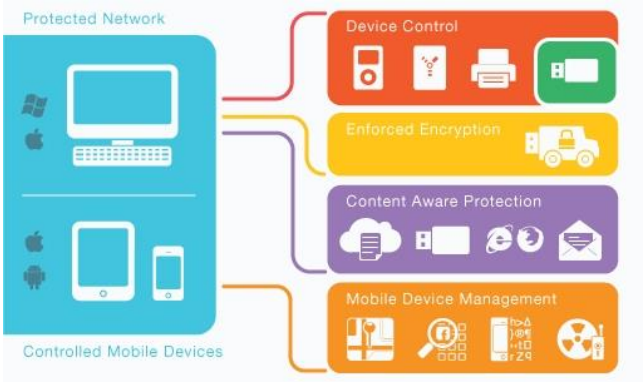
Created on 25-Feb-2015

ENDPOINT PROTECTOR 4

Solution pour la Prévention des Pertes de Données, le Contrôle des Dispositifs et le Mobile Device Management (MDM) pour iOS et Android pour les entreprises

Solution out-of-the-box pour sécuriser les données contre les menaces posées par les dispositifs portables, les services cloud et les dispositifs mobiles

Dans un monde où les dispositifs portables transforment la manière dont on travaille et on vit, Endpoint Protector 4 a été développé pour maintenir la productivité et rendre le travail plus convenable, plus sûr et plus agréable. Notre approche basée sur la liste blanche permet l'utilisation des dispositifs spécifiques, URLs et noms de domaine pour certains ordinateurs/utilisateurs/groupes, haussant la productivité en maintenant le contrôle des dispositifs et données. Proposé sous forme d'appliance matériel ou virtuel, Endpoint Protector 4 peut être installé en quelques minutes. Il réduit les risques posés par les menaces internes qui peuvent conduire à des pertes, vols, endommagements ou corruptions des données.



Principaux Avantages

- L'Appliance Matériel ou Virtuel s'installe en quelques minutes
- Solution Trois en Un Contrôle des Dispositifs, DLP et MDM
- Gestion intuitive des dispositifs et terminaux
- Interface Web
- Protection pour Windows, Mac, Linux, iOS et Android
- Protection pro-active contre l'abus des dispositifs et le vol de données
- Prêt pour VMware

Sécurité des Terminaux pour les ordinateurs Windows/Mac OS X et Linux, Notebooks et Netbooks

Protection contre les menaces posées par les dispositifs portables amovibles. Arrête les fuites intentionnelles ou accidentelles de données, les vols et les pertes ou les infections virus.

Prenez le Contrôle de ces Dispositifs, Applications et plus :

- **Dispozitifs / Ports**
- Disques USB* (normal, U3)
- Cartes de mémoire (SD, etc.)
- CD/DVD-Player / Burner *
- Disques durs externes*
- Imprimantes
- Lecteurs de disquettes
- Lecteurs de cartes(int., ext.)
- Webcams
- Cartes réseau WiFi
- Appareils photo numériques
- iPhones / iPads / iPods
- Smartphones/BlackBerry/PDAs
- Dispositifs FireWire
- Lecteurs MP3/Media Player
- Dispositifs Biométriques
- Dispositifs Bluetooth
- Disques ZIP
- Cartes express (SSD)
- Wireless USB
- Port Série
- Carte Teensy
- Dispositifs de stockage PCMCIA
- Thunderbolt
- Partage Réseau

- **Clients E-Mail**
  - Outlook
  - Lotus Notes
  - Thunderbird, etc.
- **Navigateurs Internet**
  - Internet Explorer
  - Firefox
  - Chrome
  - Safari, etc.
- **Messagerie Instantanée**
  - Skype, etc.
  - Microsoft Communicator
  - Yahoo Messenger, etc.
- **Services Cloud /Partage de Fichiers**
  - Dropbox, iCloud, SkyDrive
  - BitTorrent, Kazaa, etc.
- **Autres Applications**
  - iTunes
  - Samsung Kies
  - Windows DVD Maker
  - Total Commander
  - FileZilla
  - Team Viewer
  - EasyLock, et bien plus

OS X, iOS et Android Device Management mobile (MDM)

- Renforcer un mot de passe et la politique de sécurité
- Suivre, localiser, verrouiller ou réinitialiser les mobiles
- Pousser paramètres réseau: E-Mail, VPN, WiFi
- Mobile Application Management
- Geofencing et politiques basées sur la localisation
- Solution BYOD, pour des informations détaillées voir Data Sheet MDM

Gestion Web centralisée / Tableau de bord

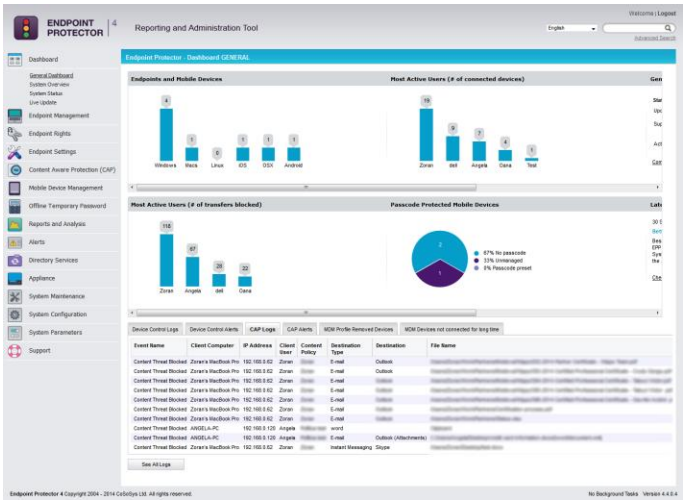
Gestion centralisée de l'utilisation des dispositifs portables. L'interface Web d'Administration et de Rapports accomplit les besoins de la direction et du personnel de sécurité informatique et offre des informations en temps réel sur les dispositifs contrôlés dans toute l'organisation et sur les activités de transfert de données.

Principaux Bénéfices

- Endpoint Protector implique un TCO 50% plus bas que la moyenne du marché
- S'installe en 70% moins de temps que d'autres solutions
- Coûte 45% moins cher en moyenne que d'autres solutions similaires

"Ich wähle die Endpoint Protector Appliance aufgrund ihrer Kosten, Benutzerfreundlichkeit und detaillierten Kontrollfunktionen. Die Lösung ist leicht zu installieren, effizient, leistungsfähig und intuitiv anwendbar. Ich schätze das Aufzeichnen der Geräteaktivitäten, das File Shadowing und die Temporäre Passwort Funktion (wirklich sehr nützlich)."

Marc Rossi Infrastructure Director NASS et WIND SAS France



Gestion des dispositifs / Contrôle des dispositifs

Définit les droits pour les dispositifs /utilisateurs, ordinateurs, groupes ou globalement dans le réseau : Bloquer, Permettre, Lecture Seule, Permettre si TD (Trusted Device)

Protection de Contenu / Filtrage de Contenu

Inspection des documents pour la détection du contenu sensible, journalisation des incidents de contenu. Blocage des données sortant via les périphériques portables, applications, services en ligne et d'autres points de sortie.

Filtrage par Type de Fichier / Contenu / Expressions Régulières

Le Filtre par Type de Fichier bloque les types de fichiers spécifiés. Des filtres peuvent être créés aussi selon de Contenu Prédéfini ou Personnalisé et Expressions Régulières.

Traçage des Fichiers / Duplication des Fichiers

Traçage des Fichiers enregistre toutes les données qui ont été copiées sur et depuis des dispositifs précédemment autorisés ou vers des applications Internet. Duplication des Fichiers fait une copie de tout fichier, même supprimé, qui a été utilisé en relation avec un dispositif ou application contrôlée.

Ajouter Fichiers/ Dispositifs/ URLs/ Domaine à la Liste Blanche

Seuls les fichiers autorisés peuvent être transférés vers les dispositifs et applications en ligne. Toute autre tentative de transfert de fichier est bloquée et rapportée.

Journaux d'Activité des Dispositifs – Audit / Rapports

Des Journaux d'Activité sont sauvegardés pour tous les clients, dispositifs connectés et fichiers transférés, fournissant un historique pour des audits et d'analyses détaillées. Un outil puissant de rapports, graphiques et analyse pour examiner facilement l'activité.

Mot de Passe Offline Temporaire / Réseau Mode "Offline"

Les PCs sécurisés qui sont déconnectés du réseau restent protégés. Pour rester productif sur la route, les dispositifs et les transferts de fichiers peuvent être autorisés temporairement via la fonctionnalité Mot de Passe Offline Temporaire (entre 30 minutes et 30 jours).

Gestion par Départements

Des Départements peuvent être organisés et séparés par des politiques dédiées.

Protection des données en transit / EasyLock - Cryptage Renforcé

En combinaison avec notre logiciel EasyLock, stocké sur les périphériques de stockage portables, les données copiées sur le périphérique sont automatiquement cryptés. Avec notre technologie TrustedDevices, nous appliquons une sécurité supplémentaire en utilisant des dispositifs cryptés certifiés pour stocker des données. Cela assurera que, si un périphérique est volé ou perdu, toutes les données qui y sont stockées seront chiffrées et donc ne seront pas accessibles aux tiers.

Plate-formes Client Supportées/ Terminaux Protégés

- Windows 8 (32/64bit)
- Windows 7 (32/64bit)
- Windows Vista (32/64bit)
- Windows XP (SP2) (32/64bit)
- Windows 2003/2008 (32/64bit)
- Mac OSX 10.5+
- Ubuntu 14.04
- Ubuntu 10.04
- openSUSE 11.4

Dispositifs Mobiles Supportés par Mobile Device Management (MDM)

- iPad, iPhone, iOS 4, iOS 5, iOS 6, iOS 7, iOS 8
- Android 2.2+, Android 4+ requis pour quelques fonctionnalités

Service d'Annuaire (pas réquis)

- Active Directory

Certifié:

Endpoint Protector Hardware Appliance

Les Endpoint Protector Hardware Appliances sont disponibles en différentes capacités pour répondre aux besoins de votre entreprise. Tous les Appliances Matériels sont basés sur les matériels les plus récents et les plus économes en énergie.

Modèles Selectés (+more)	Protection pour Terminaux	Capacité Supplémentaire	Montage (Rack)	Procésseur	Disque Dur	Alimentation
A20	20	4	Stand-alone	ULV Single Core	320GB	60W
A50	50	10	10	ULV Dual Core	320GB	200W
A100	100	20	1U	ULV Dual Core	320GB	200W
A250	250	50	10	Pentium 2 Core	500GB	260W
A500	500	100	10	Pentium 2 Core	1TB	260W
A1000	1000	200	10	Intel Xenon 4 Core	2x TB (Raid 1)	260W
A2000	2000	400	20	2x Intel Xenon 4 Core	4x 1TB (Raid 5)	2x720 W
A4000	4000	800	30	2x Quad Core	6x 1TB (Raid 5)	2x800 W

Garantie Matérielle	1 annee incluse. Garantie supplementaire et Options de remplacement sont disponibles.

Endpoint Protector Virtual Appliance

Endpoint Protector Virtual Appliance peut être utilisé par les entreprises de toute dimension. L'Appliance Virtuel est disponible dans les formats VMX, OVF et VHD pour être compatible avec les plateformes de virtualisation les plus populaires.

En utilisant l'Appliance Virtuel vous pouvez protéger votre réseau contre l'utilisation non-autorisée des périphériques et contre la perte de données en quelques minutes.

Environnements Virtuels Supportés	Version	.ovf	.vmx	.vhd	.xva	.pvm
VMware Workstation	7.1.4	-	*	-	-	-
VMware Workstation *	9.0.2	*	*	-	-	-
VMware Player *	6.0.0	*	*	-	-	-
VMware Fusion *	5.0.0	-	*	-	-	-
VMware vSphere (ESXi)	5.1.0	*	-	-	-	-
Oracle VirtualBox	4.2.18	*	-	-	-	-
Parallels Desktop for Mac	9.0.2	-	-	-	-	*
Microsoft Hyper-V Server	2008/2012	-	-	*	-	-
Citrix XenServer 64bit	6.2.0	-	-	-	*	-

Pour les Environnements marqués avec*, veuillez contacter le Support. D'autres environnements de virtualisation peuvent être supportés.

Endpoint Protector offre un environnement de travail avec des dispositifs de stockage, terminaux et mobiles sûr et sécurisé. L'efficacité des utilisateurs n'est pas limitée car tout dispositif autorisé peut être utilisé continuellement sur les PCs protégés et seuls les transferts de fichiers violant la politique de sécurité du réseau sont bloqués.

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

Visitez www.EndpointProtector.fr pour un essai gratuit.

Contactez votre partenaire local pour plus d'informations:

Created on 25-Feb-2015

ENDPOINT PROTECTOR 4

Protection de contenu pour Windows et Mac OS X
Une partie importante de votre stratégie DLP des terminaux

Solution Out-of-the-Box pour sécuriser les données contre les fuites et les vols via des applications en ligne, des services de cloud computing, des dispositifs portables et d'autres points de sortie.

La Protection de Contenu est un module de la suite DLP Endpoint Protector (Data Loss Prevention) qui couvre les besoins de sécurité provenant des risques posés par les nombreux points de sortie pour les données sensibles des entreprises.
Aujourd'hui, dans un monde où les dispositifs portables et les services cloud transforment la façon dont on travaille et on vit, Endpoint Protector 4 est conçu pour maintenir la productivité et rendre le travail plus convivial, plus sûr et plus agréable. Endpoint Protector 4, la solution DLP facile à mettre en place et à déployer, empêche les données confidentielles sur les ordinateurs portables et les PCs d'être emportées à l'extérieur de l'entreprise.
Offert en tant qu'appliance matériel ou virtuel, Endpoint Protector 4 peut être configuré en quelques minutes, vous permettant de réduire considérablement les risques posés par les menaces internes qui pourraient conduire à des fuites, vols, endommagements ou d'autres corruptions des données.

Principaux Avantages

- L'Appliance Matériel ou Virtuel s'installe en quelques minutes
- Interface Web
- Gestion intuitive des politiques et terminaux
- Protection pour les terminaux Windows
- Protection pro-active la contre l'abus des dispositifs et le vol de données
- Prêt pour VMware

Prévention des Pertes de Données avec Protection de Contenu

Protection contre les menaces posées par les transferts de données vers les dispositifs amovibles et les applications et services en ligne. Arrête les fuites intentionnelles ou accidentelles de données, les pertes et le vol.

Compatible avec les terminaux Windows et Mac OS X

Surveille et bloque les flux de données sur les plateformes les plus populaires et puissantes pour protéger vos données d'entreprise.

Prenez le contrôle des flux de données vers ces Applications et Dispositifs:

- **Dispozitifs / Ports**
- Disques USB* (normal, U3)
- Cartes de mémoire (SD, etc.)
- CD/DVD-Player / Burner *
- Disques durs externes*
- Imprimantes
- Lecteurs de disquettes
- Lecteurs de cartes (int., ext.)
- Webcams
- Cartes réseau WiFi
- Appareils photo numériques
- iPhones / iPads / iPods
- Smartphones/BlackBerry/PDAs
- Dispositifs FireWire
- Lecteurs MP3/Media Player
- Dispositifs Biométriques
- Dispositifs Bluetooth
- Disques ZIP
- Cartes express (SSD)
- Port Série
- Carte Teensy
- Dispositifs de stockage PCMCIA
- Thunderbolt
- Partage Réseau

- **Clients E-Mail**
  - Outlook
  - IBM Lotus Notes
  - Thunderbird, etc.
- **Navigateurs Internet**
  - Internet Explorer
  - Firefox
  - Chrome, etc.
- **Messagerie Instantanée**
  - Skype, etc.
  - Microsoft Communicator
  - Yahoo Messenger, etc.
- **Services Cloud /Partage de Fichiers**
  - Dropbox, iCloud, SkyDrive
  - BitTorrent, Kazaa, etc.
- **Autres Applications**
  - iTunes
  - Samsung Kies
  - Windows DVD Maker
  - Total Commander
  - FileZilla
  - Team Viewer
  - EasyLock, et bien plus

Gestion Web centralisée / Tableau de bord

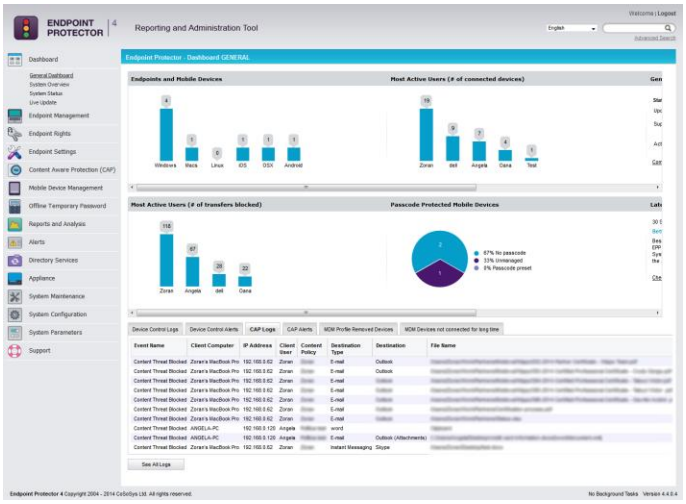
Gestion et surveillance centralisée des transferts de données hors des réseaux des entreprises. L'interface Web d'Administration et de Rapports accomplit les besoins de la direction et du personnel de sécurité informatique et offre des informations en temps réel sur les dispositifs contrôlés dans toute l'organisation et sur les activités de transfert de données.

Mot de Passe Offline Temporaire / Réseau Mode "Offline"

Les PCs sécurisés qui sont déconnectés du réseau restent protégés. Pour rester productif sur la route, les dispositifs et les transferts de fichiers peuvent être autorisés temporairement via la fonctionnalité Mot de Passe Offline Temporaire (entre 30 minutes et 30 jours).

Principaux Bénéfices

- Arrête les pertes et le vol de données
- Endpoint Protector implique un TCO 50% plus bas que la moyenne du marché
- Epargne de temps précieux car il s'installe en 70% moins de temps que d'autres solutions
- Réduit les frais de la sécurité des données car il coûte 45% moins cher en moyenne que d'autres solutions similaires



Créer des politiques de sécurité pour des entités spécifiques

Les politiques de Protection de Contenu offrent un contrôle flexible des scans des documents, en permettant de sélectionner les utilisateurs, ordinateurs, groupes ou départements à surveiller.

Filtrage par Contenu Prédéfini ou mots-clé sensibles

Filtrage des données quittant les terminaux protégés selon un format de contenu prédéfini qui inclut:

- Détails des Cartes de Crédit (toutes les cartes de crédit majeures supportées)
- Numéros de Sécurité Sociale (beaucoup de différents formats de pays supportés)
- Informations sur les Comptes Bancaires, etc.

Filtrage par Types de Fichiers

Endpoint Protector bloque les documents quittant l'entreprise selon leur type de fichier réel. Supporte les plus importants types de fichiers d'usage courant, applications telles que MS Office et fichiers graphiques, archives, exécutables, média et d'autres fichiers.

Filtrage par Dictionnaire

Le module Protection de Contenu recherche pour des données égalant les mots-clé et arrête les données/fichiers qui les contiennent d'être fuités ou volés via les points de sortie protégés. Plusieurs dictionnaires peuvent être créés pour les politiques.

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

Surveiller le Clipboard va arrêter les utilisateurs de copier & coller les informations sensibles d'entreprise vers les clients Outlook, les applications web mail ou d'autres moyens via lesquels l'information peut être fuitée.

Désactiver Capture d'Ecran

Désactiver l'option Capture d'Ecran dans vos politiques va empêcher les utilisateurs de faire des captures d'écran des données montrées sur leur écran et les emporter hors de l'entreprise en tant qu'images. Désactiver les captures d'écran renforce encore plus votre politique DLP.

Prévenir les fuites de données sensibles par Pièce-Jointe d'Email

Bloquez ou surveillez simplement les utilisateurs qui essayent d'envoyer des fichiers confidentiels via les pièces-jointes d'email. La Protection de Contenu supporte les clients e-mail les plus populaires : Outlook, Thunderbird, Lotus Notes, etc.

Prévenir les fuites de données sensibles via Outlook et Thunderbird

En tant que pièce-jointe ou même si les données confidentielles sont contenues dans le corps texte d'un e-mail, l'envoi est arrêté et l'incident est rapporté. Même si votre entreprise utilise PGP pour crypter les e-mails, le corps de l'e-mail est inspecté avant que le contenu soit crypté et envoyé.

Filtrage des données sortant par les navigateurs Web

Firefox, Google Chrome et de nombreux autres navigateurs sont utilisés sur les PC et ils représentent une grande préoccupation pour la perte de données car les utilisateurs peuvent télécharger pratiquement tout fichier auquel ils ont accès. Des téléchargements vers des sites comme sendspace.com ou vers leur compte Dropbox est la source de nombreux vols de données. Par conséquent, il est indispensable de surveiller tous les accès aux fichiers par les navigateurs Web avant que le fichier arrive sur l'internet. Cela peut se faire uniquement au niveau du terminal comme Endpoint Protector le fait. La prévention des pertes de données au niveau de la passerelle ne fonctionne pas dans ces cas.

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

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

Auto-défense du Client Endpoint Protector

Protège même les PCs où les utilisateurs ont des droits d'administration.

Terminaux Client(s) Protégés

- 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+

Service d'Annuaire (pas requis)

- Active Directory

Module Contrôle des Dispositifs Endpoint Protector (requis)

Endpoint Protector Hardware Appliance

Les Endpoint Protector Hardware Appliances sont disponibles en différentes capacités pour répondre aux besoins de votre entreprise. Tous les Appliances Matériels sont basés sur les matériels les plus récents et les plus économes en énergie.

Common Criteria

Modèles Selectés (+more)	Protection pour Terminaux	Capacité Supplémentaire	Montage (Rack)	Procésseur	Disque Dur	Alimentation
A20	20	4	Stand-alone	ULV Single Core	320GB	60W
A50	50	10	10	ULV Dual Core	320GB	200W
A100	100	20	1U	ULV Dual Core	320GB	200W
A250	250	50	10	Pentium 2 Core	500GB	260W
A500	500	100	10	Pentium 2 Core	1TB	260W
A1000	1000	200	10	Intel Xenon 4 Core	2x TB (Raid 1)	260W
A2000	2000	400	20	2x Intel Xenon 4 Core	4x 1TB (Raid 5)	2x720 W
A4000	4000	800	30	2x Quad Core	6x 1TB (Raid 5)	2x800 W

Garantie Matérielle	1 année incluse. Garantie supplémentaire et Options de remplacement sont disponibles.

Contrôle des Dispositifs pour les terminaux (Desktops, Laptops, etc) est une autre fonctionnalité disponible pour la Prévention des Pertes de

Endpoint Protector offre des fonctionnalités supplémentaires pour contrôler les dispositifs de stockage amovibles et les ports sur Windows, Mac OS X et Linux pour la Prévention des Pertes de Données. Avec le Contrôle des Dispositifs, les administrateurs IT reçoivent des rapports et des journaux détaillés indiquant le chemin d'un fichier transféré et ils sont également capables d'enregistrer une copie de ces fichiers, via le Traçage et Duplication des Fichiers.

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

Des fortes politiques de sécurité peuvent être appliquées aussi sur les dispositifs mobiles iOS et Android. Des fonctionnalités telles que le Verrouillage(Suppression) à distance sont nécessaires dans le cas où un dispositif mobile contenant des données confidentielles est perdu ou volé. Il est possible de Tracer & Localiser les dispositifs mobiles avec MDM par Endpoint Protector, entre autres fonctions de sécurité.

Endpoint Protector Virtual Appliance

Endpoint Protector Virtual Appliance peut être utilisé par les entreprises de toute dimension. L'Appliance Virtuel est disponible dans les formats VMX, OVF et VHD pour être compatible avec les plateformes de virtualisation les plus populaires. En utilisant l'Appliance Virtuel vous pouvez protéger votre réseau contre l'utilisation non-autorisée des périphériques et contre la perte de données en quelques minutes.

VMWARE CERTIFIED VIRTUAL APPLIANCE

vmware READY

Environnements Virtuels Supportés	Version	.ovf	.vmx	.vhd	.xva	.pvm
VMware Workstation	7.1.4	-	*	-	-	-
VMware Workstation *	9.0.2	*	*	-	-	-
VMware Player *	6.0.0	*	*	-	-	-
VMware Fusion *	5.0.0	-	*	-	-	-
VMware vSphere (ESXi)	5.1.0	*	-	-	-	-
Oracle VirtualBox	4.2.18	*	-	-	-	-
Parallels Desktop for Mac	9.0.2	-	-	-	-	*
Microsoft Hyper-V Server	2008/2012	-	-	*	-	-
Citrix XenServer 64bit	6.2.0	-	-	-	*	-

Contactez votre partenaire local pour plus d'informations:

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. HQ
sales@cososys.com
+40-264-593110
+40-264-593113

Trusted Device

COSOSYS

Created on 25-Feb-2015