

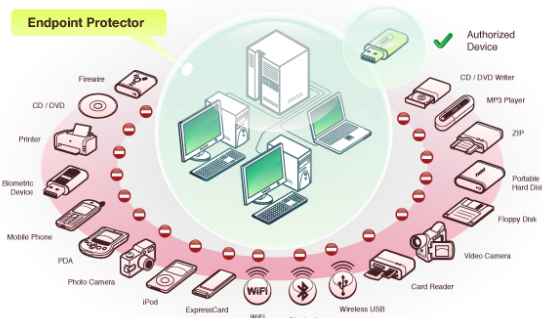


Endpoint Protector 2009™

Contrôle des dispositifs et prévention des fuites de données pour les entreprises

Windows XP/Vista/7 Client Version: 3.0.8.4 Windows 2003/2008 Server Version: 3.0.4.5
Mac OS X Version: 1.0.1.8 Linux Server Version: 3.0.4.5

Vos données confidentielles sont aussi sûres que vos ports.



Endpoint Protector 2009 fournit une approche basée sur les politiques de sécurité ayant pour objectif d'appliquer des règles d'utilisation au niveau des dispositifs portables. C'est la seule solution à offrir une protection pour les PC et les Macs. Dans un monde où les dispositifs portables transforment la manière dont on travaille et on vit, Endpoint Protector 2009 a été développé dans le but de maintenir la productivité, rendre le travail plus convenable, plus sûr et plus agréable. L'approche basée sur la liste blanche a pour objectif d'autoriser l'utilisation des dispositifs spécifiques pour certains utilisateurs/groupes. Cela permet ainsi de rester productif, tout en conservant le contrôle des dispositifs utilisés et en maîtrisant les données transférées par les utilisateurs vers/depuis leurs dispositifs. Endpoint Protector 2009 réduit d'une manière significative le risque de menaces internes, pouvant engendrer une situation dans laquelle, vos données confidentielles soient divulguées, volées, endommagées ou autrement compromises.

Types de dispositifs contrôlés:

- Disques Flash USB (disque USB régulier, U3, etc.)
- Cartes mémoire (SD, MMC, CF, etc.)
- Lecteurs/Graveurs de CD/DVD (interne et externe)
- Disques durs externes
- Lecteurs de disquettes
- Lecteurs de cartes (int. et ext.)
- Disques ZIP
- Caméras digitales
- Smartphones/BlackBerry/PDAs
- iPods / iPhones / iPads
- Dispositifs FireWire
- Lecteurs MP3 Player/Media
- Dispositifs biométriques
- Dispositifs Bluetooth
- Imprimantes
- Cartes express (SSD)
- USB Wireless

Endpoint Protector 2009 Pare-feu entre l'ordinateur et les dispositifs contrôlés

Endpoint Protector 2009 permet aux compagnies de se conformer aux politiques internes pour l'usage des dispositifs, aux réglementations gouvernementales, et aux normes de sécurité de gestion des fuites de données et de gouvernance IT.



Cryptage des données en transit en utilisant TrustedDevices.



Sécurisation des ports pour les stations de travail, les Notebooks / Netbooks

Protection contre les menaces posées par les dispositifs portables. Stoppe la fuite de données accidentelle ou intentionnelle, le vol, la perte ou l'infection des données.

Gestion des dispositifs / Contrôle des dispositifs

Établit les droits pour les dispositifs, utilisateurs ou ordinateurs dans votre réseau.

Gestion centralisée des dispositifs / Tableau de bord

Gestion centralisée de l'utilisation des dispositifs portables. L'interface de gestion et de rapports web facilite la tâche du personnel de sécurité informatique et de la direction, en offrant des informations en temps réel sur les dispositifs contrôlés, l'organisation et sur les activités de transfert de données.

Traçage fichiers / Réplication fichiers

Le *traçage des fichiers* enregistre toutes les données copiées par les dispositifs autorisés. La *réplication des fichiers* sauvegarde une copie de tout fichier utilisé par les dispositifs contrôlés.

Liste blanche des fichiers

Seuls les fichiers autorisés peuvent être transférés sur les dispositifs portables. Tout autre fichier est bloqué et les essais de transfert seront rapportés.

Journaux des activités des dispositifs – Trace d'audit

Un journal de l'activité des dispositifs est sauvegardé pour tous les clients et les dispositifs connectés (historique des dispositifs, des ordinateurs et des utilisateurs pour les audits et pour des analyses détaillées).

Outils de rapports et d'analyse

Rapports puissants : graphiques et outils d'analyses pour une révision facile des activités.

Mise en application facile de vos politiques de sécurité (Active Directory)

Les politiques simplifiées de gestion des dispositifs, avec des modèles qui peuvent être personnalisés pour les Groupes d'Utilisateurs définis (GPOs Active Directory) permettent la mise en application et la maintenance des politiques de sécurité dans votre réseau.

Mot de passe pour le mode "Offline" temporaire / Réseau "Offline"

Les ordinateurs protégés qui sont débranchés du réseau restent protégés. Pour rester productif sur la route, les dispositifs peuvent être temporairement autorisés en utilisant la fonctionnalité « mot de passe temporaire » en mode "Offline".

Autodéfense pour le client Endpoint Protector

Fournit même une protection sur les PC où les utilisateurs ont des droits d'administration.

Mettez en application les politiques de sécurité et contrôlez à tout moment les transferts de données.

CONFIGURATION REQUISE Client(s)

- Windows 7 (32/64bit)
- Windows Vista (32/64bit)
- Windows XP (SP2) (32/64bit)
- Windows 2003/2008 (32/64bit)
- Mac OS X 10.4+
- .Net 2.0 Framework
- 32 MB d'espace sur disque dur

Serveur

Systèmes d'exploitation supportés::

- Windows 2003 Server
- Windows 2008 Server
- Debian (*Ubuntu), Red Hat (Fedora, CentOS), Suse

Serveurs Web supportés:

- IIS 6.0 / 7.0 ou
- Apache (Version 5 ou ultérieure)

Bases de données:

- Microsoft SQL 2005/2008 (Exp.)
- MySQL (Version 5 ou ultérieure)

Configurations supplémentaires:

- PHP (Version 5) avec support SOAP
- OpenSSL Version 0.9.8

Service de gestion

- Active Directory

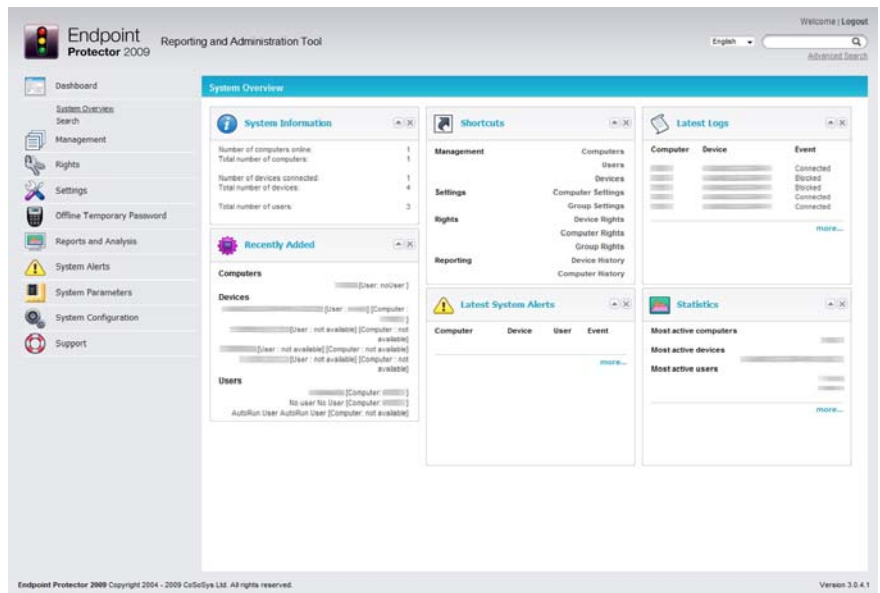
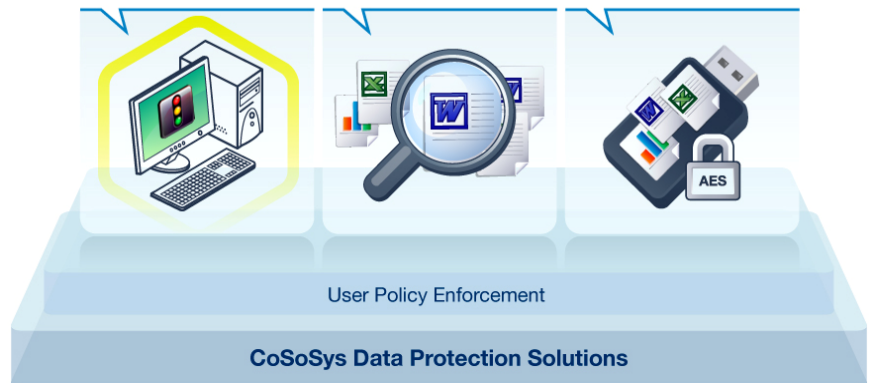


Tableau de bord Endpoint Protector 2009
Outil de gestion et rapports

- Endpoint Security
- Data Loss Prevention
- Portable Device Management
- Data Theft Prevention
- Data Monitoring
- Analysis & Reporting
- Data Transfer Monitoring
- File Tracing
- Data Encryption and Sync
- Protecting sensitive data in transit



Endpoint Protector 2009 est développé sur une architecture composée de trois éléments. Prévention - Surveillance - Cryptage

Installation facile par des mécanismes de déploiement MSI.

Le serveur Endpoint Protector 2009 est compatible avec différentes plateformes afin d'assurer une intégration rapide, efficace et compétitive, avec votre infrastructure existante, tant en terme de coût que de qualité.

L'interface administrative intuitive assure une gestion très efficace.

Endpoint Protector vous offre un environnement de travail sécurisé dans le cadre de l'utilisation des dispositifs de stockage portables. L'efficacité des utilisateurs n'est pas restreinte, tout dispositif autorisé peut être utilisé continuellement sur les ordinateurs protégés, quand bien même la politique de sécurité des ports réseaux est applicable.

Cryptage automatique - pour protéger les données confidentielles en transit avec TrustedDevices

La technologie TrustedDevices est conçue pour certifier que, dans l'environnement protégé, tous les dispositifs sont autorisés et contrôlés par le logiciel et la politique de sécurité, mais également que les données sensibles et confidentielles en transit sont protégées. Cette technologie assure le cryptage des données sur les dispositifs (dans certaines situations comme le vol ou la perte du dispositif, les informations ne seront pas accessibles aux autres personnes).

Visitez www.EndpointProtector.fr pour un essai gratuit et plus d'informations.



CoSoSys Ltd.

E-Mail: sales@cososys.com

Tél.: +40-264-593110 x 117

Fax: +40-264-593113

CoSoSys North America

sales.us@cososys.com

+1-208-850 7563

CoSoSys Germany

sales.de@cososys.com

+49-177-555 6435

+49-721-151 497421



© Copyright 2004-2010 CoSoSys Ltd. All rights reserved. EasyLock, Lock it Easy, Surf it Easy, Carry it Easy, Carry it Easy +Plus, Carry it Easy +Plus Bio, Secure it Easy, TrustedDevices, TrustedLogin My Endpoint Protector and Endpoint Protector are trademarks of CoSoSys Ltd. Other brand names mentioned herein are for identification purposes only and may be trademarks of their respective holder(s).