ENDPOINT PROTECTOR | by CoSoSys

DATASHEET 5.2.0.9

Leader dans le secteur Data Loss Prevention (DLP)

Une solution de sécurité de niveau d'entreprise pour tous les secteurs

DLP pour Windows, Mac et Linux

La protection de l'ensemble du réseau

ENDPOINT PROTECTOR | by CoSoSys

Notre solution avancée pour le Data Loss Prevention (DLP), arrête les fuites et le vol de données tout en offrant un contrôle des périphériques de stockage portables et en assurant la conformité avec les réglementations de protection des données.

Il est conçu pour protéger les données confidentielles contre les menaces provenant du personnel, mais aussi pour maintenir la productivité et rendre le travail plus pratique, plus sécurisé et plus agréable.

Endpoint Protector est un logiciel DLP de niveau entreprise pour les ordinateurs Windows, macOS et Linux, les clients légers et les solutions Desktop-as-a-Service (DaaS). Cette solution est un choix idéal pour les entreprises fonctionnant sur des réseaux multi-OS et son format modulaire leur permet de combiner les bons outils pour répondre aux besoins de specific.

En déployant ce logiciel, les organisations peuvent protéger les informations personnelles et répondre aux exigences de conformité à des réglementations telles que la RGPD, la PCI DSS, l'HIPAA, l'ACCP etc. Endpoint Protector offre également une protection de la propriété intellectuelle et des secrets commerciaux de l'entreprise.

Device Control

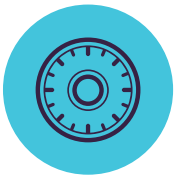
Verrouillez, contrôlez et surveillez les ports USB et périphériques pour empêcher le vol et la perte de données. Définissez les droits par dispositif, utilisateur, ordinateur, groupe ou globalement.

Windows / macOS / Linux

Content Aware Protection

Surveillez et contrôlez les données en cours de transfert, en décidant quels fichiers confidentiels peuvent ou non quitter l'entreprise. Les filtrages peuvent être définis par type de fichier, par application, par contenu prédéfini et personnalisé, par Regex, etc.

Windows / macOS / Linux



Enforced Encryption

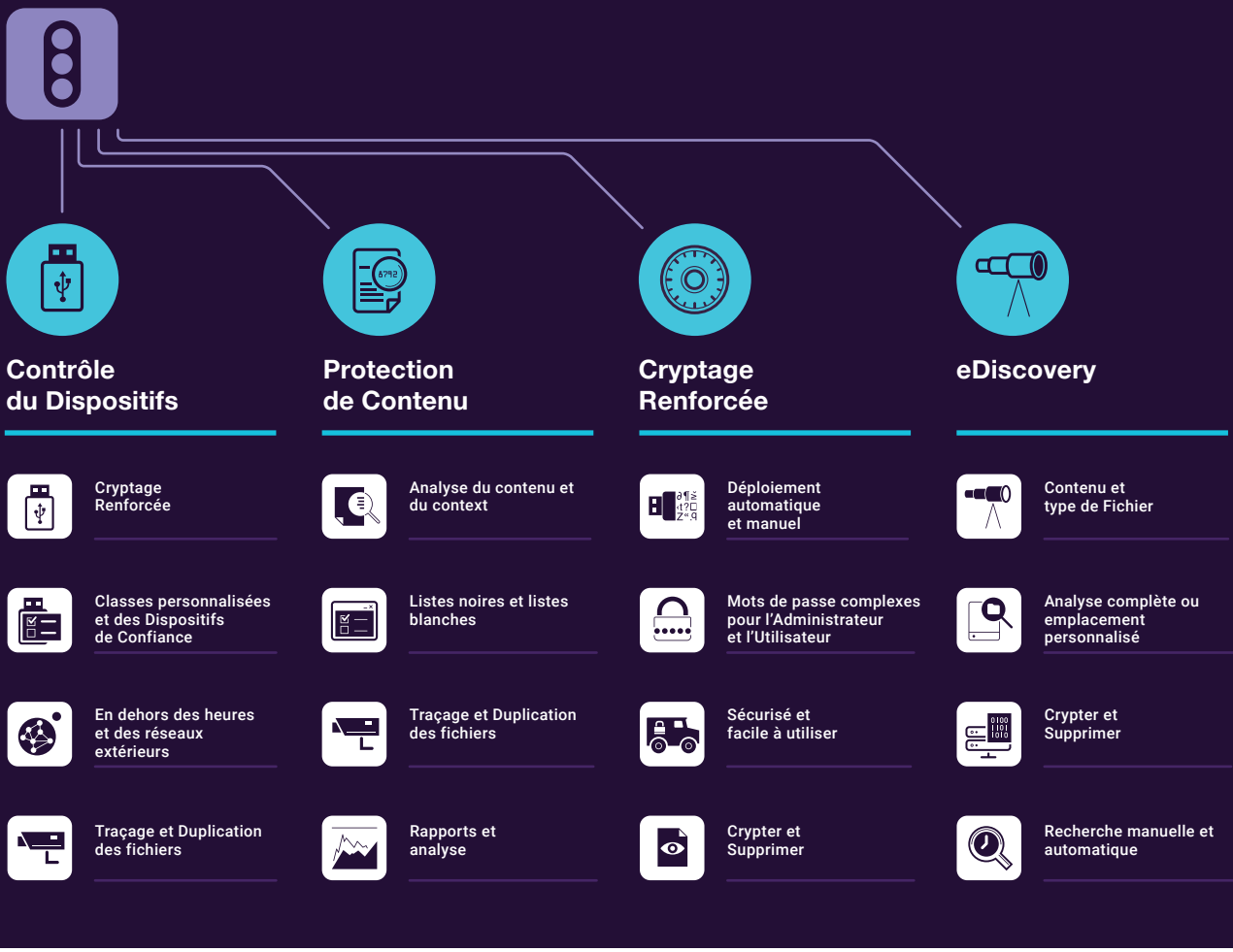
Sécurisation automatique des données copiées sur des périphériques de stockage USB avec un cryptage AES 256 bits. Fonctionnement multiplateforme, basé sur un mot de passe, facile à utiliser et très efficace.

Windows / macOS

eDiscovery

Analysez les données conservées sur les postes de travail du réseau et appliquez des mesures correctives telles que le cryptage ou la suppression au cas où des données confidentielles sont identifiées sur des ordinateurs non autorisés.

Windows / macOS / Linux



Avantages Majeurs

Facile à installer et à gérer

Endpoint Protector peut être opérationnel en 30 minutes. Son installation est facile à réaliser par du personnel technique et non technique.

Profiles prédéfinies pour la conformité

Avec les Politiques Predefinits pour la Protection des données il est facile de mettre en place une réglementation et d'assurer la conformité aux exigences de la RGPD, CCPA, HIPAA, PCI DSS et autres.

Protection multiplateforme

La solution offre les mêmes caractéristiques de sécurité et le même niveau de protection pour un poste de travail avec système d'exploitation Windows, macOS ou Linux.

Rapports détaillés sur l'activité des utilisateurs

Avec Endpoint Protector, il est possible de surveillez, de rapporter et d'obtenir des informations pertinentes sur les données personnelles qui sont transférées, à quel endroit et par qui.

Des options de déploiement flexibles

Endpoint Protector peut être déployé de plusieurs manières, en fonction des besoins et de l'infrastructure existante de l'entreprise.

Politiques granulaires

Les droits d'accès granulaires pour les dispositifs amovibles et les ports de périphériques, ainsi que les politiques de sécurité pour les utilisateurs, les ordinateurs et les groupes, peuvent être facilement appliqués.

Contrôle du Dispositifs

pour Windows, macOS et Linux

Clients de messagerie: Outlook / Thunderbird / Lotus Notes / Navigateurs Web: Internet Explorer / Firefox / Chrome / Safari / Messagerie instantanée: Skype / Microsoft Communicator / Yahoo Messenger / Services Cloud et partage de fichiers: Dropbox / iCloud / SkyDrive / BitTorrent / Kazaa / Autres Applications: iTunes / Samsung Kies / Windows DVD Maker / Total Commander / Team Viewer / AUTRES

Définir les Droits de manière granulaire

Les droits des dispositifs peuvent être configurés globalement, par groupe, ordinateur, utilisateur et périphérique. Utilisez les paramètres par défaut ou ajustez au besoin.

Types de Dispositifs et Dispositifs spécifiques

Définissez les droits - refuser, autoriser, lecture seule, etc. - pour les types de périphériques ou les périphériques spécifiques (en utilisant le VID, le PID et le numéro de série).

Classes Personnalisées

Les droits peuvent être créés en fonction des classes de périphériques rendant la gestion plus facile pour les produits d' un même fournisseur.

Politiques en dehors des heures de travail

Les stratégies de contrôle de dispositifs peuvent être définies pour s'appliquer en dehors des heures normales de travail. Les heures d'ouverture et de fermeture et les jours ouvrables peuvent être définis.

Politiques concernant les réseaux externes

Politiques concernant l'utilisation du poste de travail sur des réseaux n'appartenant pas à l'entreprise peuvent être définies. L'application est basée sur les adresses IP FQDN et DNS.

Syncronisation Active Directory

Profitez de l'AD pour simplifier les déploiements de grande envergure. Tenez les entités à jour, en reflétant agroupes de réseaux, les ordinateurs et les utilisateurs.

Informations sur les utilisateurs et les ordinateurs

Obtenez une meilleure visibilité avec des informations telles que les ID d'employé, les équipes, l'emplacement, les coordonnées précises et plus (adresses IP, adresses MAC, etc.).

Traçage des Fichiers

Enregistrer tous les transferts ou les tentatives de divers périphériques de stockage USB, en offrant une vue claire sur les actions des utilisateurs.

Duplication des Fichiers

Enregistrer une copie des fichiers qui ont été transférés vers des dispositifs contrôlés qui peuvent ensuite être utilisés à des fins d'audit.

Hors connexion : Accès Temporaire par Mot de Passe

Autoriser temporairement l'accès des périphériques aux ordinateurs déconnectés du réseau. Assurer la sécurité et la productivité.

Créer des Alertes par E-mail

Des alertes de courrier électronique prédéfinies et personnalisées peuvent être configurées pour fournir des informations sur les événements les plus importants liés à l'utilisation des dispositifs.

Tableau de Bord et Graphiques

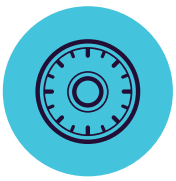
Pour un aperçu visuel rapide sur les événements les plus importants et les statistiques, des Tableaux et des graphiques sont disponibles.

Rapports et Analyse

Surveiller l'activité liée aux transferts avec un puissant outil de rapport et d'analyse. Les journaux et les rapports peuvent également être exportés vers les solutions SIEM.

Limitation des transferts

Limiter le nombre ou la taille des fichiers qui peuvent être transférés dans un intervalle de temps défini. Inclure ou exclure les transferts par des périphériques, des applications en ligne et des partages de reseau.



Cryptage Renforcé

pour Windows et macOS

Chiffrement AES 256 bits approuvé par le gouvernement / Techniques anti-effraction / Intégrité de l'application / Envoyer des messages aux utilisateurs / Restaurer les paramètres par défaut / Paramètres de mot de passe / AUTRES

Cryptage Renforcé des USB

Autoriser uniquement les dispositifs USB cryptés et assurer que toutes les données copiées sur les périphériques de stockage amovibles sont automatiquement sécurisées.

Déploiement automatique et en lecture seule

Le déploiement automatique et manuel est disponible. L'option d'autoriser les droits de lecture seule jusqu'à ce que le chiffrement soit nécessaire est également possible.

Mot de Passe Principal Mots de passe utilisateur complexes

La complexité du mot de passe peut être définie au besoin. Le mot de passe principal assure la continuité dans des circonstances telles que la réinitialisation du mot de passe des utilisateurs.

Gestion des mots de passe et suppression à distance

Modification des mots de passe des utilisateurs faite à distance et effacement des données cryptées en cas de piratage des dispositifs.

Protection de Contenu

pour Windows, macOS et Linux

Clients de messagerie: Outlook / Thunderbird / Lotus Notes / Navigateurs Web: Internet Explorer / Firefox / Chrome / Safari / Messagerie instantanée: Skype / Microsoft Communicator / Yahoo Messenger / Services Cloud et partage de fichiers: Dropbox / iCloud / SkyDrive / BitTorrent / Kazaa / Autres Applications: iTunes / Samsung Kies / Windows DVD Maker / Total Commander / Team Viewer / AUTRES

Listes noires de points de sortie

Les filtres peuvent être définis en fonction d'une grande liste d'applications surveillées. Les périphériques de stockage USB, les partages réseau et autres points de sortie peuvent être surveillés pour le contenu.

Listes noires de Type de Fichiers

Les filtres par Type de fichier peuvent être utilisés pour bloquer des documents spécifiques en fonction de leur extension, même si ceux-ci sont modifiés manuellement par les utilisateurs.

Listes noires Contenu Personnalisés

Les filtres peuvent également être créés en fonction de contenus personnalisés tels que des mots clés et des expressions. Différents dictionnaires de liste noire peuvent être créés.

Listes noires a Contenu Prédéfinis

Les filtres peuvent être créés en fonction de contenus prédéfinis tels que les numéros de carte de crédit, les numéros de sécurité sociale et beaucoup d'autres.

Listes noires des Nom de fichier

Des filtres basés sur les noms de fichiers peuvent être créés. Ils peuvent être définis en fonction du nom et de l'extension du fichier, juste du nom ou simplement de l'extension

Listes Noires et Listes Blanches par Location des fichiers

Filtres basés sur l'emplacement des fichiers sur le disque dur local. Ceux-ci peuvent être définis pour inclure ou exclure des sous-dossiers.

Filtres d'Expressions Régulières

Des filtres personnalisés avancés peuvent être créés pour rechercher certaines récurrences dans les données transférées au sein du réseau protégé.

Liste Blanche des fichiers autorisé

Bien que tous transferts de fichiers soient bloqués, des listes blanches peuvent être créées pour éviter les redondances et augmenter la productivité.

Liste Blanches de Noms de Domaine et d'URL

Appliquer la politique de l'entreprise mais permettre aux employés la flexibilité dont ils ont besoin pour faire leur travail. Autoriser par des listes blanches l'accès à des sites externes ou à des adresses électroniques.

Impression de l'écran et du Presse-Papiers

Révoquer les capacités de capture d'écran. Supprimez les fuites de données sur les contenus sensibles grâce à la fonctionnalité Copier & Coller / Couper & Coller, en améliorant la politique de sécurité des données.

Reconnaissance optique de caractères

Inspectez le contenu des photos et des images, en détectant les informations confidentielles des documents numérisés et d'autres fichiers similaires.

Traçage et Duplication des Fichiers

Enregistrez tous les transferts ou tentatives vers diverses applications en ligne et autres points de sortie. Avoir une vue claire des actions en sauvegardant une copie des fichiers.

Seuil pour les filtres

Définissez jusqu'à quel nombre de violations un transfert de fichier est autorisé. Cela s'applique à chaque type de contenu ou à la somme de toutes les violations.

Limite de transfert

Définissez une limite de transfert dans un intervalle de temps spécifique. Elle peut être basé sur le nombre de fichiers ou la taille du fichier. Les alertes par e-mail lorsque la limite est atteinte sont possible.

Analyse de contenu contextuel

Activer un mécanisme d'inspection avancé pour une détection plus précise des contenus sensibles tels que l' information personnelle. La personnalisation du contexte est disponible

Hors connexion: Accès Temporaire par Mot de Passe

Autoriser temporairement les transferts de fichiers sensibles vers des ordinateurs non connectés au réseau. Assurer la sécurité et la productivité.

Tableau de Bord et Graphiques

Surveillez l'activité liée aux transferts de fichiers avec un puissant outil de rapports et d'analyse. Les journaux et les rapports peuvent également être exportés vers les solutions SIEM.

Conformité (GDPR, HIPAA, etc.)

Devenir conforme aux règles et réglementations de l'industrie telles que GDPR, PCI DSS, HIPAA, etc. Éviter les amendes et autres préjugés.

DLP pour les Imprimantes

Politiques pour les imprimantes locales et réseau pour bloquer l'impression de documents confidentiels et prévenir la perte de données et le vol de données.

DLP pour les Clients Légers

Légers Protéger les données sur les Terminal Serveur et prévenir la perte de données dans des environnements Client Légers comme dans tous autres types de réseaux.

eDiscovery

pour Windows, macOS et Linux

Type de fichier : Fichiers graphiques / Fichiers Office / Fichiers d'archives / fichiers de Programmation / fichiers multimédias, etc. / Contenu Prédéfinis: Cartes de crédit / Informations personnelles identifiables / Adresse / SSN / ID / Passeport / Numéro Téléphone / Numéro fiscal / Numéro d'assurance maladie / Contenu personnalisée / Nom du fichier / Expression Régulier/ HIPAA/ AUTRES

Chiffrer et déchiffrer des données

Les données en repos contenant des informations confidentielles peuvent être cryptées pour empêcher l'accès des employés non autorisés. Les actions de décryptage sont également disponibles.

Supprimer les Données

Si des violations évidentes de la politique interne se produisent, supprimez les informations sensibles dès qu'elles sont détectées sur des postes de travail non autorisés.

Trouver les fichiers avec des listes noires des Localisation

Des filtres peuvent être créés en fonction de la localisation ou se trouvent les documents. Évitez la numérisation redondante des données au repos avec des inspections de contenu ciblées.

Des Analyses automatiques

En plus des analyses propres et incrémentielles, les analyses automatiques peuvent être planifiées, soit une fois, soit de manière récurrente (hebdomadaire ou mensuelle).

Traçage des fichiers

Enregistrez tous les transferts de fichiers ou les tentatives d'accès à diverses applications en ligne et services cloud, en fournissant une vue claire des actions des utilisateurs.

Rapports et analyse

Surveillez les journaux relatifs à l'analyse des données au repos et prenez les mesures correctives nécessaires. Les journaux et les rapports peuvent également être exportés vers les solutions SIEM.

Seuil pour les filtres

Définissez jusqu'à quel nombre de violations un transfert de fichier est autorisé. Cela s'applique à chaque type de contenu ou à la somme de toutes les violations.

Conformité (GDPR, HIPAA, etc.)

Se mettre en conformité avec les règles et règlements de l'industrie comme la norme PCI DSS, GDPR, HIPAA, etc. Évitez les pénalités et autres préjugés.

Liste Noire par Type de Fichier

La liste noire par Type de fichier peut être utilisée pour détecter des documents spécifiques en fonction de leur extension, même si ceux-ci sont manuellement modifiés par les utilisateurs.

Liste Noire par Contenu Prédéfini

Ces Listes Noire peuvent être créés en fonction du contenu prédéfini, comme les numéros de carte de crédit, les numéros de sécurité sociale et bien d'autres.

Liste Noire par Contenu Personnalisé

Les filtres peuvent également être créés en fonction d'un contenu personnalisé, tel que des mots-clés et des expressions. Divers dictionnaires de liste noire peuvent être créés.

Liste noire par Nom de Fichier

Des filtres basés sur les noms de fichiers peuvent être créés. Ils peuvent être définis en fonction du nom et de l'extension du fichier, juste du nom ou simplement de l'extension.

Liste noire par expressions régulières

Les listes noires personnalisées avancées peuvent être créées pour trouver une certaine récurrence dans les données stockées sur le réseau protégé.

Liste blanche des fichiers autorisés

Alors que toutes les autres tentatives de transferts de fichiers sont bloquées, des listes blanches peuvent être créées pour éviter la redondance et augmenter la productivité.

Liste blanche de type MIME

Exclure les types MIME de la numérisation, en les ajoutant dans les listes blanches pour éviter la redondance et augmenter la productivité.

Intégration SIEM

Tirer parti des produits de sécurité et de gestion des événements en externalisant les journaux. Assurer une expérience transparente entre les produits de sécurité.

Caractéristiques supplémentaires. Beaucoup d'autres fonctionnalités sont également disponibles: EndpointProtector.com

100% Flexibilité de Déploiement

Nos solutions sont adaptées aux entreprises et évoluent en permanence pour mieux servir tout type de réseau et d'industrie. Avec une architecture client-serveur, ils sont faciles à déployer et sont gérés de manière centralisée à partir d'une interface web. En dehors l'Appliance Virtuelle, le serveur peut être hébergé par nous et dans les principales infrastructures cloud comme Amazon Web Services, Microsoft Azure or Google Cloud.

Le Device Control, Content Aware Protection, Enforced Encryption, et le eDiscovery sont disponibles pour les ordinateurs fonctionnant sous différentes versions et distributions Windows, macOS et Linux.

Virtual Appliance

Cloud Services

Amazon Web Services
Microsoft Azure
Google Cloud

Cloud-Hosted

Gartner peerinsights™

Très bien classé par le **Gartner Peer Insights** pour les solutions de prévention des pertes de données d'entreprise.

Protected Endpoints

Windows	Windows 7 / 8 / 10	(32/64 bit)	●	●	●	●
	Windows Server 2003 - 2019	(32/64 bit)	●	●	●	●
	Windows XP / Windows Vista	(32/64 bit)	●	●	●	●
macOS (kext and kextless agent)	macOS 11.00	Big Sur	●	●	●	●
	macOS 10.15	Catalina	●	●	●	●
	macOS 10.14	Mojave	●	●	●	●
	macOS 10.13	High Sierra	●	●	●	●
	macOS 10.12	Sierra	●	●	●	●
	macOS 10.11	El Capitan	●	●	●	●
	macOS 10.10	Yosemite	●	●	●	●
	macOS 10.9	Mavericks	●	●	●	●
	macOS 10.8	Mountain Lion	●	●	●	●
Linux	Ubuntu		●	●	●	n/a
	OpenSUSE / SUSE		●	●	●	n/a
	CentOS / RedHat		●	●	●	n/a
	Fedora		●	●	●	n/a

*For more information on supported versions and distributions please check EndpointProtector.com/linux

Official Partner

COSOSYS

Siège (Roumanie)

sales@cososys.com
+40 264 593 110 / ext. 121
+40 264 593 113 / ext. 202

Allemagne

vertrieb@endpointprotector.de
+49 7541 978 26730
+49 7541 978 26733

Amérique du Nord

sales.us@endpointprotector.com
+1 888 271 9349
+1 877 377 6475

Corée

contact@cososys.co.kr
+82 70 4633 0353
+82 20 4633 0354