ENDPOINT PROTECTOR | by CoSoSys

DATASHEET 5.5.0.0

Le Leader du Secteur La prévention des pertes de données (DLP)

Une sécurité de haut niveau pour tous les secteurs d'activité

DLP pour Windows, macOS et Linux

Protéger l'ensemble de votre réseau

ENDPOINT PROTECTOR | by CoSoSys

Notre solution de prévention avancée de la perte de données (DLP) met fin aux fuites et aux vols de données tout en offrant un contrôle des dispositifs de stockage mobiles et en assurant la conformité aux réglementations en matière de protection des données.

Il est conçu pour protéger les données confidentielles contre les menaces internes tout en préservant la productivité et en rendant le travail plus pratique, plus sûr et plus agréable.

Endpoint Protector est un logiciel DLP de qualité professionnelle destiné aux ordinateurs Windows, macOS, Linux, ainsi que pour les Thin Clients et les solutions Desktop-as-a-Service (DaaS). La solution est un choix idéal pour les entreprises fonctionnant sur des réseaux multi-OS grâce à son format modulable qui permet de mélanger et d'assortir les bons outils pour répondre à des besoins spécifiques.

En le déployant, les organisations peuvent protéger les données personnelles et respecter réglementations telles que le GDPR, HIPAA, LGPD, CCPA, PCI DSS, etc. Endpoint Protector offre également une protection de la propriété intellectuelle et des secrets commerciaux de l'entreprise.

Contrôle des dispositifs

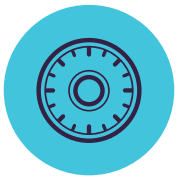
Verrouillez, contrôlez et surveillez les ports USB et périphériques pour mettre fin au vol et à la perte de données. Définissez des droits par dispositif, utilisateur, ordinateur, groupe ou au global.

Windows / macOS / Linux

Protection du contenu

Surveillez et contrôlez les données en circulation, en décidant quels dossiers confidentiels peuvent ou non quitter l'entreprise. Les filtres sont configurables par type de fichier, application, contenu prédéfini et personnalisé, regex et plus encore.

Windows / macOS / Linux



Cryptage renforcé

Sécurisez automatiquement les données copiées sur les périphériques de stockage USB avec un cryptage AES 256 bits. C'est un système multiplateforme, basé sur un mot de passe, facile à utiliser et très efficace.

Windows / macOS

eDiscovery

Analysez les données en attente sur les points d'extrémité du réseau et appliquez des actions de remédiation telles que le cryptage ou la suppression en cas d'identification de données confidentielles sur des ordinateurs non autorisés.

Windows / macOS / Linux

Principaux avantages

Facile à installer et à gérer

Endpoint Protector peut être opérationnel en 30 minutes. Il est facile à utiliser par le personnel technique comme par le personnel non technique.

Des profiles de conformité prédéfinis

Grâce aux politiques de protection des données prédéfinies, il est facile de trouver les données réglementées et de garantir les conformité du GDPR, de l'ACCP, de l'HIPAA, de PCI DSS et plus encore.

Une Protection multi-plateforme

La solution offre les mêmes fonctions de sécurité et le même niveau de protection pour les ordinateurs Windows, macOS et Linux. Elle prend également en charge les appareils Apple équipés de processeurs M1 basés sur Arm.

Rapports détaillés sur l'activité des utilisateurs

Avec Endpoint Protector, il est possible de suivre, de rapporter et d'obtenir des informations précieuses sur les données sensibles transférées, où et par qui. .

Options de déploiement flexibles

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

Politiques granulaires

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

DLP pour les Enterprises

À l'ère de la transformation numérique et des plateformes de travail collaboratif (WSC), faire face aux risques de perte de données et de non-conformité sont une nécessité pour les entreprises, car les répercussions des violations de données engendrent de lourdes amendes, des problèmes juridiques et une atteinte à la réputation.
Endpoint Protector Entreprise est livré avec une solution de sécurité des données la plus efficace du marché, permettant aux entreprises d'identifier, de surveiller et de contrôler en permanence les données qu'elles doivent protéger, où qu'elles soient.

Remédiation des utilisateurs

Endpoint Protector Enterprise ajoute plus de flexibilité aux politiques de sécurité. Grâce à la fonction de remédiation de l'utilisateur, les utilisateurs finaux sont autorisés à s'auto-réparer, ce qui signifie qu'après avoir justifié de leur activité, le transfert d'informations sensibles spécifiques est autorisé pendant une durée définis.

La console de gestion

Les politiques de prévention des pertes de données peuvent être facilement définies pour l'ensemble du réseau à partir du tableau de bord centralisé d'Endpoint Protector qui offre une expérience utilisateur améliorée.

Une intégration sans faille

Notre solution offre une intégration avec Active Directory (AD) et la technologie de gestion des informations et des événements de sécurité (SIEM). L'intégration avec SIEM permet de transférer les événements d'activité vers un serveur SIEM pour l'analyse et la création de rapports. Avec AD, les grands déploiements peuvent être plus simples.

Protection en fonction du contenu

Pour Windows, macOS et Linux

Email Clients: Outlook / Thunderbird / Apple Mail / Web Browsers: Internet Explorer / Firefox / Chrome / Safari / Instant Messaging: Skype / Slack / WhatsApp / Cloud Services & Sharing: Dropbox / iCloud / OneDrive / BitTorrent / AirDrop / Other Applications: iTunes / FileZilla / SFTP / Total Commander / TeamViewer / OTHERS

Points de sortie Denylists
Des filtres peuvent être définis sur la base d'une large liste d'applications surveillées. Les périphériques de stockage USB, les partages réseau et autres points de sortie peuvent être surveillés.

Listes de refus de types de fichiers
Les filtres de type de fichier peuvent être utilisés pour bloquer les documents en fonction du véritable type de fichier, même si les utilisateurs modifient l'extension.

Reconnaissance optique des caractères
Inspectez le contenu des photos et des images, en détectant les informations confidentielles des documents numérisés et autres similaires.

Listes de refus de contenu prédéfinies et personnalisées
Des filtres peuvent être créés sur la base de contenus prédéfinis tels que les numéros de carte de crédit ou les numéros de sécurité sociale et de contenus personnalisés tels que des mots-clés ou des expressions.

Nom du fichier Denylists
Des filtres basés sur les noms de fichier peuvent être créés. Ils peuvent être définis sur la base du du fichier et de l'extension, juste le nom ou juste l'extension.

Listes de refus et d'autorisation d'emplacement de fichier
Filtres basés sur l'emplacement des fichiers sur le disque dur local. Ceux-ci peuvent être définis pour inclure ou exclure des sous-dossiers.

Expressions régulières Denylists
Un outil puissant pour identifier une séquence de caractères qui définis un motif de recherche.

En dehors des heures et du réseau
Définit des politiques de repli qui s'appliqueront en dehors des heures de travail ou en dehors du réseau.

Autorisations de domaines et d'URL
Appliquez les politiques de l'entreprise tout en laissant aux employés la flexibilité dont ils ont besoin pour faire leur travail. Activez la fonction DPI et créez des portails d'entreprise ou des adresses électroniques autorisés.

Contrôle de l'impression de l'écran et du presse-papiers
Révoquer les capacités de capture d'écran. Éliminez les fuites de données de contenu sensible grâce aux fonctions Copier & Coller / Couper & Coller, ce qui renforce la politique de sécurité des données.

Remédiation utilisateur
Permet aux utilisateurs d'outrepasser en toute sécurité une politique DLP et offre des options pour justifier les transferts de données. Aide à accroître la responsabilité de l'utilisateur final et la sensibilisation aux transferts de données sensibles dans l'organisation.

Intégration SIEM
Exploiter les produits de gestion des informations et des événements de sécurité en externalisant les journaux. Assurez une expérience transparente entre les produits de sécurité.

Seuil pour les filtres
Règles avancées de détection de contenu Définе des conditions complexes pour l'analyse de contenu en combinant plusieurs critères (PII, mots du dictionnaire, expressions régulières, etc.) à l'aide d'opérateurs logiques (ET/OU).

Limite de transfert
Définissez une limite de transfert dans un intervalle de temps specifi . Elle peut être basée soit sur le nombre de , soit sur la taille des fi . Des alertes par e-mail lorsque la limite est atteinte sont disponibles.

Analyse contextuelle du contenu
Activez un mécanisme d'inspection avancé pour une détection plus précise des contenus sensibles tels que les DPI. La personnalisation du contexte est disponible.

Mot de passe temporaire hors ligne
Autorisez temporairement les transferts de fichiers sur les ordinateurs déconnectés du réseau. Assurez la sécurité et la productivité.

Tableaux de bord, rapports et analyses
Surveillez l'activité liée aux transferts de fichiers grâce à un puissant outil de rapport et d'analyse. Obtenez des rapports graphiques pour les cadres de niveau C.

Conformité (GDPR, HIPAA, etc.)
Devenez conforme aux règles et réglementations du secteur telles que PCI DSS, GDPR, HIPAA, etc. Évitez les amendes et autres sanctions.

DLP pour les imprimantes
Des politiques pour les imprimantes locales et réseau afin de bloquer l'impression de documents confidentiels et d'empêcher la perte et le vol de données.

DLP pour les clients légers
Protégez les données sur les serveurs de terminaux et prévenez les pertes de données dans les environnements de clients légers, comme dans tout autre type de réseau.

Des fonctionnalités supplémentaires sont disponibles. Pour en savoir plus, demandez une démo sur EndpointProtector.com.

eDiscovery

for Windows, macOS and Linux

fichier type: Graphic Files / Office Files / Archive Files / Programming Files / Media Files / etc. / Predefined Content: Credit Cards / Personally Identifiable Information / Addresses / SSNs / IDs / Passports / Phone Numbers / Tax IDs / Health Insurance Numbers / etc. / Custom Content / fichier Name / Regular Expression / HIPAA / OTHERS

Cryptage et décryptage des données

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

Supprimer les données

En cas de violation manifeste de la politique interne, supprimez les informations sensibles dès qu'elles sont détectées sur des terminaux non autorisés.

Listes de dénombrement des lieux de balayage

Des filtres peuvent être créés sur la base d'emplacements prédéfinis. Évitez les analyses redondantes des données au repos grâce à des inspections ciblées du contenu.

Scans automatiques

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

Résultats de l'analyse

Surveillez les journaux pour analyser les données au repos et prenez des mesures correctives si nécessaire. Les journaux et les rapports peuvent également être exportés vers des solutions SIEM.

État du balayage

Vérifiez facilement l'état actuel de votre scan. L'état de la numérisation est affiché dans le format 0-100%.

Seuil pour les filtres

Definir le nombre de violations de politique qu'un fichier peut contenir pour que la politique de sécurité soit appliquée et que le fichier soit signalé au serveur.

Conformité (GDPR, HIPAA, etc.)

Devenir conforme aux règles et réglementations du secteur telles que PCI DSS, GDPR, HIPAA, etc. Évitez les sanctions et autres amendes.

Listes de refus de types de fichiers

Les filtres de type de fichier peuvent être utilisés pour découvrir des documents en fonction du véritable type de fichiers, même si les utilisateurs modifient l'extension.

Listes de refus de contenu prédefinis

Des filtres peuvent être créés sur la base de contenus predefinis tels que les numéros de carte de crédit, les numéros de sécurité sociale et bien d'autres.

Listes de refus de contenu personnalisé

Des filtres peuvent également être créés sur la base de contenus personnalisés tels que des mots-clés et des expressions. Divers dictionnaires de listes de refus peuvent être créés.

Nom du fichier Denylists

Des filtres basés sur les noms de fichier peuvent être créés. Ils peuvent être définis sur la base du nom de fichier et de l'extension, juste le nom ou juste l'extension.

Expressions régulières Denylists

Un outil puissant pour identifier les séquences de caractères qui définie un motif de recherche.

Autorisations de fichiers

Alors que toutes les autres tentatives de transfert de fichier sont bloquées, des listes d'autorisations peuvent être créées pour éviter la redondance et augmenter la productivité.

Type MIME Allowlists

Évitez les analyses redondantes au niveau mondial en excluant l'inspection du contenu pour certains types MIME.

Intégration SIEM

Exploiter les produits de gestion des informations et des événements de sécurité en externalisant les journaux. Assurez une expérience transparente entre les produits de sécurité.

Flexibilité de déploiement à 100%

Nos produits sont de qualité professionnelle et évoluent en permanence pour servir au mieux tout type de réseau et d'industrie.z Avec une architecture client-serveur, ils sont faciles à déployer et sont gérés de manière centralisée à partir de l'interface web.z Outre l'appliance virtuelle, le serveur peut être hébergé par nos soins et dans les principales infrastructures de cloudz computing comme Amazon Web Services, Microsoft Azure ou Google Cloud.

Plusieurs options de connexion, notamment les comptes locaux, l'authentification Active Directory (AD) sur site, Azure AD etz OKTA Single Sign-on (SSO) sont disponibles, en permettant un contrôle plus simple et plus facile pour leszadministrateurs. L'authentification multifactorielle (MFA) est également possible. Contrôle des dispositifs, protection du contenu, cryptage renforcé, etc.

Appliance virtuelle

Services Cloud

Amazon Web Services
Microsoft Azure
Google Cloud

Hébergement Cloud

Gartner peerinsights™

Très bien noté par Gartner Peer Insights pour les solutions de prévention des pertes de données en entreprise.

Protected Endpoints

Windows	Windows 7 / 8 / 10	(32/64 bit)	●	●	●	●
	Windows Server 2003 - 2019		●	●	●	●
	Windows XP / Windows Vista	(32/64 bit)	●	●	●	●
macOS (kext and kextless agent)	Apple Silicon M1		●	●	●	●
	macOS 12.00	(32/64 Monterey bit)	●	●	●	●
	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

*Des fonctionnalités supplémentaires sont disponibles. Pour en savoir plus, demandez une démo sur EndpointProtector.com.

Partenaire officiel

COSOSYS

Distribué officiellement
en France par

IPSTEEL

cybersécurité & réseau

contact@ipsteel.com

www.ipsteel.com