ENDPOINT PROTECTOR | by CoSoSys

DATASHEET 5.2.0.0

Prévention de Perte des Données & Management des Dispositifs Mobiles

Convient à toute taille de réseau et tous types d'entreprises

DLP pour Windows, Mac et Linux

La protection de l'ensemble du réseau

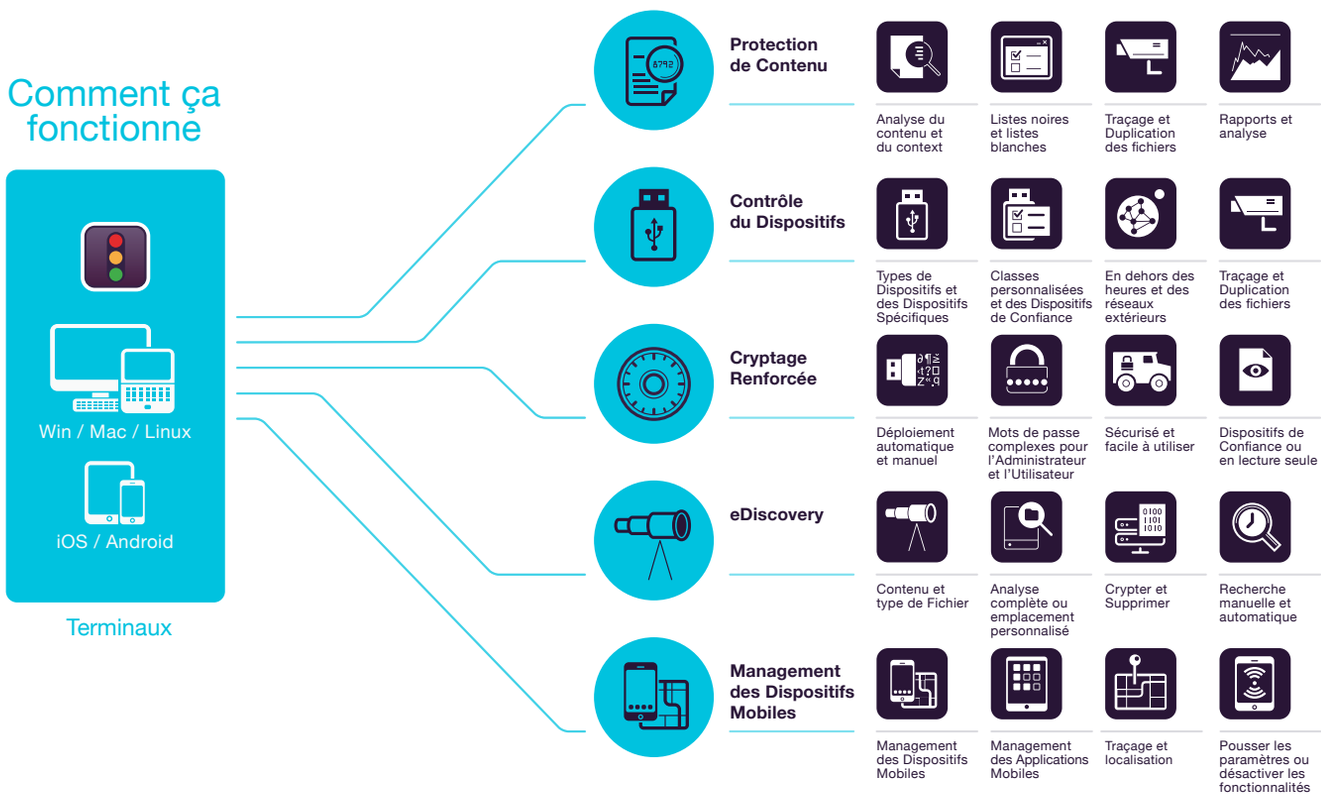
ENDPOINT PROTECTOR

by CoSoSys

Solution « Out of the Box » pour sécuriser les données sensibles contre les menaces posées par les dispositifs de stockage portables, les services « Cloud » et les appareils mobiles

Dans un monde où la vie devient « connectée », les périphériques portables et le Cloud transforment notre façon de travailler et de vivre, Endpoint Protector est conçu pour protéger les données confidentielles des menaces internes, tout en maintenant dans le travail la productivité et l'efficience.
L'approche basée sur la liste blanche et la liste noire offrent une certaine souplesse dans la construction de politiques sécuritaires. Les sociétés ont la possibilité d'interdire l'utilisation de périphériques amovibles spécifiques ainsi que les transferts de données vers les applications de stockage et partage sur le « Cloud ». Il en est de même pour tous les services en ligne permettant la recherche d'informations personnelles. Pour des ordinateurs / utilisateurs / groupes spécifiques, il est possible d'autoriser les transferts d'informations vers des URL spécifiques et des noms de domaines identifiés, cela permet une utilisation simple pour les taches courantes.
Avec l'Appliance Matérielle ou Virtuelle de Endpoint Protector, la mise en route de votre protection peut être réalisée en quelques minutes. En outre, l'interface de gestion interactive permet de gérer les politiques et de vérifier les rapports à partir de n'importe quel périphérique, du bureau à la tablette. Endpoint Protector réduit considérablement les risques et les menaces internes qui pourraient conduire à des fuites, des vols ou autres délits sur vos données.

Comment ça fonctionne



Protection de Contenu
pour Windows, macOS et Linux

Surveillez et contrôlez les dossiers confidentiels qui peuvent ou ne peuvent pas être transférés via les divers points de sortie. Les filtres peuvent être définis par type de fichier, application, Contenu prédéfini et personnalisé, Regex et plus encore.

Contrôle de Dispositifs
pour Windows, macOS et Linux

Surveillez et contrôlez tous les ports et les périphériques USB. Définir les droits d'entrée / Sortie par: Dispositif, Utilisateur, Ordinateur, Groupe ou Global.

Cryptage Renforcé
pour Windows, macOS

Encrypter automatiquement les données copiées sur les périphériques de stockage USB avec un Cryptage AES 256bit. Cryptage Multiplateformes, basé sur le mot de passe, simple d'utilisation et très efficace.

eDiscovery
pour Windows, macOS et Linux

Scannez les données stockées sur ses postes ou périphériques connectés au réseau et appliquez les actions correctives telles que le cryptage si des données confidentielles sont identifiées sur des ordinateurs non autorisés.

Management des Dispositifs Mobiles
pour Android, IOS et macOS

Gérer, contrôler et régler le niveau de sécurité sur les Smartphones et Tablettes. Poussez sur les périphériques : des paramètres de sécurité, des paramètres réseau, des applications .etc..

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.

Caractéristiques supplémentaires
Beaucoup d'autres fonctionnalités sont également disponibles. / info@endpointprotector.com

Contrôle de Dispositifs

pour Windows, macOS et Linux

Dispositifs USB / Imprimantes / Appareils Bluetooth / Lecteurs MP3 / Disques durs externes / Teensy Board / Appareils photo numériques / Webcams / Thunderbolt / PDA / Partage Réseau / FireWire / iPhones / iPads / iPods Disques ZIP / Serial Port / PCMCIA Périphériques de stockage / Dispositifs biométriques / 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 réseau extérieur

Les stratégies de contrôle de dispositifs peuvent être configurées pour s'appliquer en dehors du réseau de l'entreprise. L'application est basée sur les noms de domaine DNS et les adresses IP.

Importation et synchronisation Active Directory

Profitez de l'AD pour simplifier les déploiements de grande envergure. Tenez les entités à jour, en reflétant les groupes 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.

Caractéristiques supplémentaires

Beaucoup d'autres fonctionnalités sont également disponibles.
info@endpointprotector.com

Cryptage Renforcé

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.

Fonctions supplémentaires

Le chiffrement est également disponible pour le stockage en nuage, les dossiers locaux, les CD et
info@endpointprotector.com

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 / etc.
• Contenu personnalisée / Nom du fichier / Expression Régulier/ HIPAA/ etc.

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.

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.

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.

Listes noires et listes blanches du location

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

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 des Domaine ou des URL

Appliquer la politique de l'entreprise mais permettre aux employés la flexibilité dont ils ont besoin pour faire leur travail. Portails de la liste blanche ou adresses e-mail.

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.

Caractéristiques supplémentaires

Beaucoup d'autres fonctionnalités sont également disponibles. / info@endpointprotector.com

Management de Dispositifs Mobiles

Pour Android, iOS et Mac OS X

Inscription en direct pour iOS et Android

Les appareils peuvent être enregistrés à distance via SMS, E-mail, lien URL ou code QR. Choisissez le moyen le plus pratique pour votre réseau.

Inscription en masse

Pour un processus de déploiement efficace, jusqu'à 500 smartphones et tablettes peuvent être enrôlés en même temps.

Verrouillage à distance

Activer à distance le verrouillage instantané du périphérique mobile en cas d'incident connexe. Éviter les fuites de données en raison de dispositifs perdus ou égarés.

Suivi et Localisation

Surveiller de près les appareils mobiles de l'entreprise et connaître en tout temps les données sensibles de votre entreprise.

Désactiver les fonctionnalités intégrées

Contrôler l'autorisation des fonctions intégrées telles que la caméra, en évitant les brèches de données et la perte de données sensibles.

Emettre un son pour localiser des dispositifs perdus

Localiser un périphérique mobile égaré en activant une sonnerie à distance jusqu'à ce qu'il soit trouvé (supporté uniquement par Android).

Management des Applications Mobiles

Gérer les applications en fonction des stratégies de sécurité de l'organisation. Appuyez instantanément sur les applications gratuites et payantes pour les appareils mobiles enregistrés

Pousser les paramètres réseau

Pousser les paramètres réseau comme les paramètres E-mail, Wi-Fi et VPN ou désactivez-les, notamment Bluetooth, définir le mode de sonnerie, etc.

Alertes

Des alertes systèmes prédéfinis étendues sont disponibles, ainsi que l'option de configuration des alertes systèmes personnalisés.

Rapports et analyses

Surveiller l'activité de tous les utilisateurs liés à l'utilisation de périphériques avec un puissant outil de rapportage et d'analyse. Les journaux et les rapports peuvent également être exportés

Mode Kiosque avec Samsung Knox

Verrouiller ou contenez l'appareil mobile dans des applications spécifiques. Appliquer à distance la sécurité sur la flotte mobile et les transformer en périphériques dédiés.

Gestion Mac OS X

Pour étendre les fonctionnalités DLP, les Mac peuvent également être enrôlés dans le module MDM, en profitant d'options de gestion supplémentaires.

Application de mot de passe

Protection proactive des données essentielles de l'entreprise stockées sur les appareils mobiles en imposant des stratégies de mots de passe solides.

Effacement à distance

Pour les situations critiques où le seul moyen d'éviter les fuites de données est en essuyant le dispositif, ce qui peut facilement être effectuée à distance.

Géo-barrière

Définir un périmètre virtuel d'une zone géographique, en obtenant un meilleur contrôle des politiques MDM qui s'appliquent uniquement dans un domaine spécifique.

Restrictions iOS

Assurez-vous que l'utilisation commerciale est possible. Si ce n'est pas conforme aux règles de l'entreprise, désactivez iCloud, Safari, App Store, etc.

Pousser vCards sur Android

Ajouter et appuyer sur les contacts pour les appareils mobiles Android, en veillant à ce que votre personnel mobile peut obtenir rapidement en contact avec les bonnes personnes.

Surveillance des applications

Savoir quelles applications vos employés téléchargent sur leurs appareils mobiles, en gardant une ligne discrète entre le travail et les loisirs.

Management d'actifs

Obtenir un aperçu de l'appareil mobile et sur les noms de périphériques, Types, Modèles, Capacité, Versions OS, les transporteurs, IMEI, MAC, etc.

Créer des alertes par e-mail

Des alertes par courrier électronique peuvent être configurées pour fournir des informations sur les événements les plus importants liés à l'utilisation des appareils mobiles.

Tableau de bord et graphiques

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

Caractéristiques supplémentaires

Beaucoup d'autres fonctionnalités sont également disponibles.
info@endpointprotector.com

100% Flexibilité du déploiement

Adaptés à tout type de réseau, nos produits peuvent être utilisés par des Groupes Internationaux, des ETI, des PME et TPE des artisans et même des particuliers. Pourvu d'une architecture client-serveur, Endpoint Protector est facile à déployer et gérer grâce à son interface de centralisation Web: Appliance Matériel ou Virtuelle, Services d'Instance Amazon ou la Version Cloud, une version autonome est également disponible pour ceux qui recherchent des fonctionnalités de base.

Endpoint Protector

La Protection de Contenu, eDiscovery, le Contrôle des Dispositifs et le Cryptage sont disponibles pour les ordinateurs fonctionnant sur différentes versions et distributions Windows, Mac et Linux. Le Mangement des Dispositifs Mobiles et le Management des Applications Mobiles sont également disponibles pour les dispositifs mobiles iOS et Android.

My **Endpoint Protector**

La Protection de Contenu, le Contrôle de Dispositifs et le Cryptage sont disponibles pour les ordinateurs fonctionnant sous Windows et Mac. Le Management des Dispositifs Mobiles et le Management des Applications Mobiles sont disponibles pour les dispositifs mobiles iOS et Android.

Hardware Appliance

Virtual Appliance

Amazon Instance

Cloud Solution

Modules

		Terminaux Clients protégés					
Windows	Windows 7 / 8 / 10	(32/64 bit)	●	●	●	●	
	Windows Server 2003 - 2016	(32/64 bit)	●	●	●	●	
	Windows XP / Windows Vista	(32/64 bit)	●	●	●	●	
macOS	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	●	●	●	●	
	macOS 10.7	Lion	●	●	●	●	
Linux	Ubuntu		●	●	●	n/a	
	OpenSUSE / SUSE		●	●	●	n/a	
	CentOS / RedHat		●	●	●	n/a	
	Fedora		●	●	●	n/a	
iOS	iOS 4, iOS 5, iOS 6, iOS 7, iOS 8, iOS 9, iOS 10, iOS 11						●
Android	Jelly Bean (4.1+), KitKat (4.4+), Lollipop (5.0+), Marshmallow (6.0+), Nougat (7.0+), Oreo (8.0+)						●

* Vérifier les détails concernant les versions et les distributions prises en charge sur: endpointprotector.fr/linux

COSOSYS

Siège (Roumanie)

E-mail sales@cososys.com
Ventes +40 264 593 110 / ext. 121
Support +40 264 593 113 / ext. 202

Allemagne

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

Corée

E-mail contact@cososys.co.kr
Ventes +82 70 4633 0353
Support +82 20 4633 0354

Amérique du Nord

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

Partenaire official