ENDPOINT PROTECTOR | by CoSoSys

DATASHEET 5.0.0.0

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

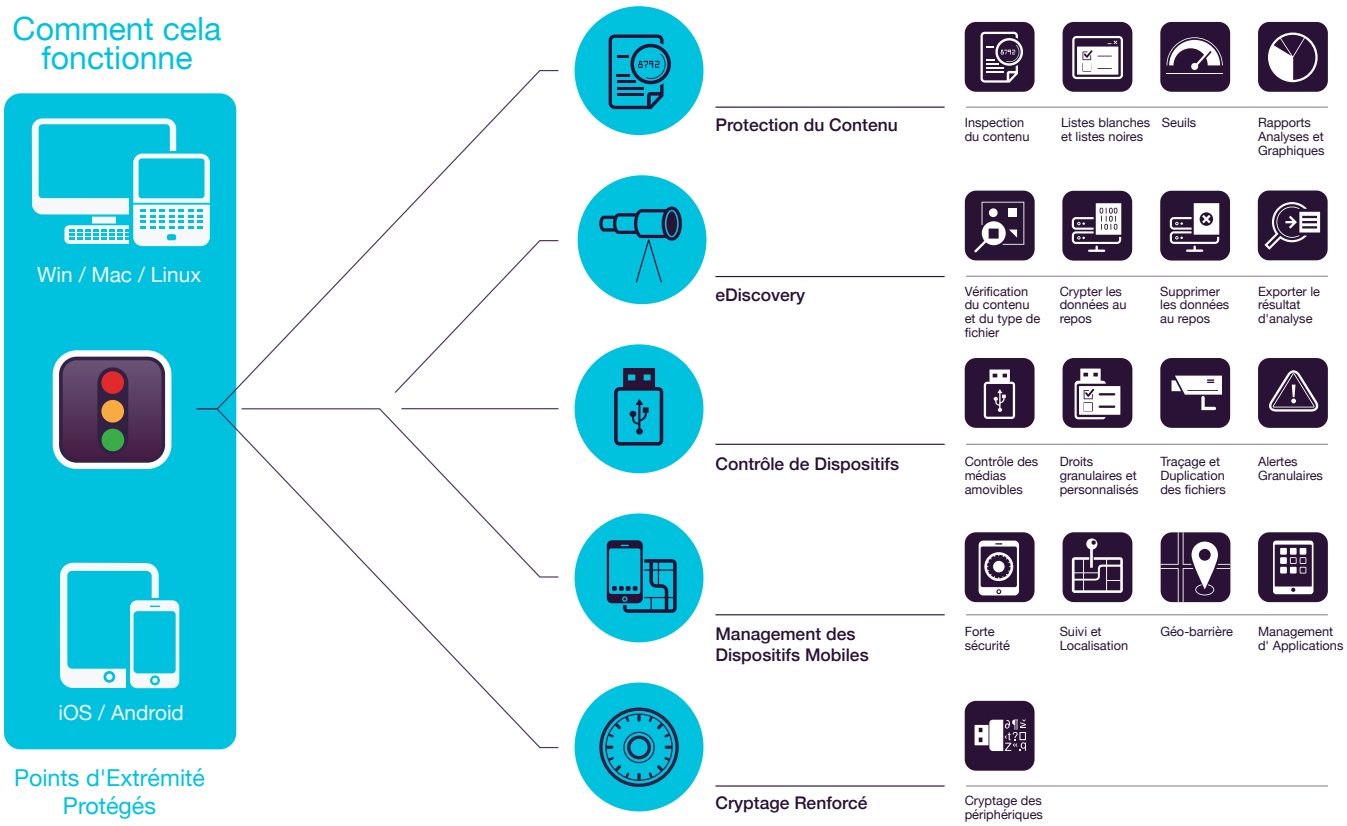
ENDPOINT PROTECTOR

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 cela 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.

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.

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.

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..

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.

Protection de Contenu

Surveillez les éléments confidentiel Pour Windows, macOS et Linux

Clients Email: Outlook / Thunderbird / Lotus Notes • Navigateurs: Internet Explorer / Firefox / Chrome / Safari • Messageries instantannées: Skype / Microsoft Communicator / Yahoo Messenger • Cloud Services & File Sharing: Dropbox / iCloud / SkyDrive / BitTorrent / Kazaa • Autres applications: iTunes / Samsung Kies / Windows DVD Maker / Total Commander / Team Viewer

Filtres de 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.

Filtres de 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.

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

Filtres par 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.

Liste Blanche
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 électronique.

Désactiver Capture d'écran
Désactivé les fonctions de captures d'écrans afin de s'assurer qu'aucune donnée précieuse affichée sur l'écran n'est divulgué hors du réseau protégé.

Surveillance du Presse-papiers
Éliminer les fuites de données de contenu sensible par copier/coller et couper/coller, renforcer la politique de sécurité des données.

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.

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

Active Directory
Profiter de l'AD ou d'outils similaires, pour simplifier les déploiements. Importer et synchroniser tous les groupes et entités.

Seuil Global et Régulier pour les filtres
Des seuils peuvent être définis sur chaque filtre permettant en fonction du nombre de violations, une autorisation de transfert, une alerte plus une autorisation, une alerte majeure plus un blocage de transfert. Les filtres s'appliquent sur les types de contenus ou sur la somme des violations.

Traçage des Fichiers
Enregistrement de tous les transferts ou tentatives, vers les diverses applications en ligne et des services « cloud », avec une information claire des actions de chaque utilisateur.

Duplication des Fichiers
Enregistrement d'une copie des fichiers qui ont été transférés à des dispositifs connectés ou des e-mails, ou stocké sur le « Cloud » ou d'autres applications.

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 liées aux faits les plus importants et aux transferts confidentiels.

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.

Politiques de Protection HIPAA
Permet une analyse approfondie des documents avant que le transfert soit effectué pour les informations PHI, les médicaments approuvés par la FDA, les codes ICD-9, etc.

DLP pour les Clients Légers
Protéger les données sur les Terminal Serveur et prévenir la perte de données dans des environnements Client Légers comme dans tout autre type de réseau.

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

eDiscovery

Recherche active multi-supports de données confidentielles. Pour Windows, macOS et Linux

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

Trouver des contenus et des fichiers sur votre réseau

Créer des politiques personnalisées pour eDiscovery définissant quel contenu est sensible pour votre entreprise selon les critères: type de fichier, contenu prédéfini, contenu personnalisé, nom de fichier, contenu protégé par Regex ou HIPAA. Scanner sur votre réseau les données sensibles en fonction du contenu sélectionné.

Crypter les Données en veille

Une fois les données confidentielles trouvées, l'option de cryptage avec une solution de chiffrement AES 256 est disponible afin d'empêcher l'accès des employés non autorisés et d'arrêter la possibilité de fuites de données.

Supprimer les Données en veille

Sécuriser les données et assurer la conformité aux règles appliquées dans l'entreprise en supprimant les informations sensibles immédiatement dès qu'elles sont identifiées si elles violent la politique de l'entreprise.

Exporter les Résultats d'Analyse

Les résultats de la vérification sont exportable aux formats de fichiers Excel, PDF ou CSV. Ils peuvent être utilisés comme rapports de gestion ou comme documents de vérification. Les résultats de l'analyse fournissent les détails sur les données sensibles trouvées dans les ordinateurs, le chemin d'accès, l'heure de la découverte, si elles ont été cryptées, supprimées ou signalées et bien autres informations précieuses.

Liste Noire par Type de Fichier

La liste noire par Type de fichier peut être utilisée pour détecter des documents spécifiques stockés dans les postes connectés au réseau: fichiers graphiques, fichiers Office, fichiers d'archive, fichiers de programmation et bien d'autres encore.

Liste Noire par Contenu Prédéfini

Ajouter des informations sur la liste noire a contenu prédéfini telles que: les numéros de carte de crédit, les numéros de sécurité sociale, les informations d'identification personnelles et d'autres données. Identifier les informations sur tous les périphériques, s'assurer du respect de la politique de l'entreprise. Cette liste noire peut aider à assurer la conformité aux réglementations telles que PCI DSS, HIPAA et autres.

Liste Noire par Contenu Personnalisé

Créer une liste noire en fonction de contenus personnalisés tels que des mots clés et des expressions. Différents dictionnaires de liste noire peuvent être créés par copiers/coller, saisie ou importation.

Liste noire par Nom de Fichier

Rechercher des fichiers spécifiques en fonction de leur nom et leur lieu de stockage. Les résultats sont affichés dans les résultats de l'analyse eDiscovery avec la liste des fichiers trouvés et des actions comme supprimer, crypter ou décrypter peuvent être effectuées

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.

Données protégées HIPAA

Permet une analyse approfondie des points d'extrémité pour les informations PHI, les médicaments approuvés par la FDA, les codes ICD-10 et ICD-9, etc. Respecter la conformité avec la détection HIPAA où réside l'information confidentielle sur les soins de santé et appliquez des actions d'assainissement si nécessaire.

Seuils

Éviter la numérisation redondante à l'aide des options des seuils. Vous pouvez spécifier lorsque l'inspection doit s'arrêter en fonction d'un nombre spécifique de violations. Ou quels fichiers doivent être recherchés en fonction d'une taille de fichier minimale.

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. Gérer efficacement les politiques de eDiscovery.

Liste blanches de Fichiers autorisés

Téléchargez les fichiers dans les listes blanches comme des exceptions des politiques de numérisation que vous avez définies dans eDiscovery. Peu importe si la politique est basée sur le type fichiers, le contenu prédéfini, contenu personnalisé, etc etc., la liste blanche des fichiers seront exclus de l'analyse.

Caractéristiques supplémentaires

Beaucoup d'autres fonctionnalités sont également disponibles.

info@endpointprotector.com

Contrôle de Dispositifs

Surveillez tous les ports E/S pour Windows, Mac OS X et Linux

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

Définir des Droits Globaux
Par défaut, les droits des périphériques s'appliquent globalement via le réseau. Cependant, le module est extrêmement granulaire.

Définir les Droits par Groupe
Les droits des dispositifs peuvent être configurés de manière détaillée en fonction de groupes, ce qui permet aux différents services d'accéder aux différents accès.

Définir les Droits par Ordinateur
Les droits de périphérique peuvent être configurés par ordinateur. Utile lorsque les ordinateurs jouent un rôle unique dans l'organisation.

Définir les Droits par Utilisateur
En fonction de leurs rôles et de leurs tâches, chaque utilisateur peut recevoir différents droits d'accès aux périphériques selon les règles de l'entreprise.

Définir les Droits par Périphérique
La granularité des droits peut être réduite au niveau de l'appareil, en fonction de l'ID du fournisseur, de l'ID du produit et du numéro de série.

Classes Personnalisées
Les droits peuvent être créés en fonction des classes de périphériques rendant la gestion plus facile pour les produits du même fournisseur.

Dispositifs de Confiance
Pour les dispositifs cryptés, différents droits d'accès peuvent être configurés en fonction du niveau de cryptage (logiciel, matériel, 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 les transferts de fichiers sensibles vers des ordinateurs non connectés au 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

Pour Windows et Mac OS X

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

Forts Mécanismes de Sécurité
AES 256bit approuvé par le gouvernement, la protection par mot de passe et des techniques anti-falsifications pour assurer l'intégrité de l'application.

Mot de Passe Principal
La création d'un mot de passe principal va assurer la continuité dans diverses circonstances, comme la réinitialisation du mot de passe de l'utilisateur.

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 macOS

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 eet 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.

Appliance Materielle

Appliance Virtuelle

Instance d'Amazon

Solution Cloud

Modules

		Terminaux Clients protégés					
Windows	Windows XP / Windows Vista	(32/64 bit)	●	●	●	●	
	Windows 7 / 8 / 10	(32/64 bit)	●	●	●	●	
	Windows Server 2003 - 2016	(32/64 bit)	●	●	●	●	
macOS	macOS 10.6	Snow Leopard	●	●	●	●	
	macOS 10.7	Lion	●	●	●	●	
	macOS 10.8	Mountain Lion	●	●	●	●	
	macOS 10.9	Mavericks	●	●	●	●	
	macOS 10.10	Yosemite	●	●	●	●	
	macOS 10.11	El Capitan	●	●	●	●	
	macOS 10.12	Sierra	●	●	●	●	
Linux	Ubuntu		●	●	●	n/a	
	OpenSUSE		●	●	●	n/a	
	CentOS / RedHat		●	●	●	n/a	
iOS	iOS 4, iOS 5, iOS 6, iOS 7, iOS 8, iOS 9, iOS 10						●
Android	Jelly Bean (4.1+), KitKat (4.4+), Lollipop (5.0+), Marshmallow (6.0+), Nougat (7.0+)						●

* 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