



**ENDPOINT
PROTECTOR**

by CoSoSys

HOJA DE DATOS 4.4.0.9

Prevención de Pérdida de Datos & Gestión de Dispositivos Móviles

Adecuado para cualquier tamaño de red y cualquier industria



DLP para Windows, Mac y Linux.

Protegiendo toda la red





ENDPOINT PROTECTOR

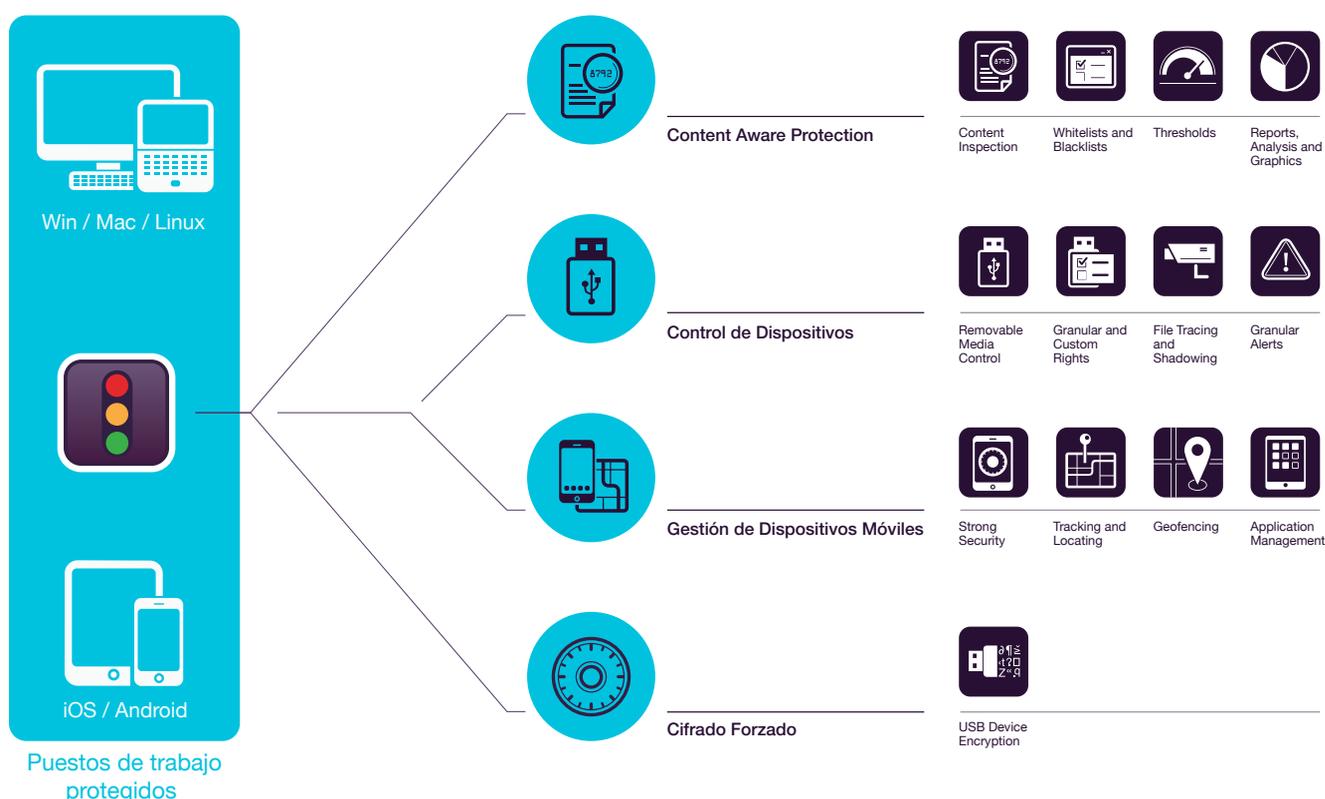
by CoSoSys

Solución "out of the box" que protege los datos confidenciales y sensibles contra las amenazas existentes para los dispositivos de almacenamiento, los servicios en la nube y los dispositivos móviles.

En un mundo donde los dispositivos portátiles y la nube han transformado la manera en que vivimos y trabajamos, Endpoint Protector 4 ha sido diseñado para proteger la información, mantener la productividad y hacer el trabajo más cómodo, seguro y agradable.

El concepto de las Listas Negras prohíbe el uso de dispositivos específicos, la carga de archivos en URLs y nombres de dominios específicos para ciertos equipos/ usuarios/ grupos, aumentando la productividad mientras se mantiene el control de los dispositivos y de la información. Endpoint Protector 4, disponible tanto como Appliance Virtual o como Hardware, se instala en unos minutos y reduce drásticamente los riesgos que plantean las amenazas internas y que pueden determinar la fuga y el robo de datos. Asimismo, permite el cumplimiento de las normas y de las regulaciones de la industria.

Como funciona



Content Aware Protection
para Windows, Mac OS X y Linux

Monitoree y controle qué datos confidenciales pueden o no pueden salir de la red a través de varios puntos de salida. Los filtros se pueden definir por tipo de archivo, aplicación, contenido predefinido y contenido personalizado, regex y más.

Control de Dispositivos
para Windows, Mac OS X y Linux

Gestione, controle y configure el nivel de seguridad en smartphones y tabletas. Despliegue los ajustes de seguridad, la configuración de la red, de las aplicaciones, etc.

Gestión de Dispositivos Móviles
Para Android, iOS y Mac OS X

Gestione, controle y configure el nivel de seguridad en smartphones y tabletas. Despliegue los ajustes de seguridad, la configuración de la red, de las aplicaciones, etc.

Cifrado Forzado
Para Windows y Mac OS X

Proteja de forma automática los datos copiados a dispositivos USB con cifrado AES de 256 bit. Multiplataforma, basada en contraseña fácil de utilizar y muy eficiente.



Content Aware Protection

para Windows, Mac OS X y Linux

Clientes de E-mail: Outlook / Thunderbird / Lotus Notes • Navegadores Web: Internet Explorer / Firefox / Chrome / Safari • Mensajería Instantánea: Skype / Microsoft Communicator / Yahoo Messenger • Servicios en la Nube / Compartir Archivos: Dropbox / iCloud / SkyDrive / BitTorrent / Kazaa • Otras aplicaciones iTunes / Samsung Kies / Windows DVD Maker / Total Commander / Team Viewer • OTROS



Filtros de Contenido Predefinido

Los filtros se pueden crear a base de contenido predefinido como números de tarjeta de crédito, números de Seguridad Social, y otros.



Filtros de Contenido Personalizado

Permite crear filtros en base a contenido personalizado como palabras clave y expresiones. Se pueden crear múltiples listas negras de diccionarios.



Filtros de Expresiones Regulares

Permite crear filtros personalizados avanzados para encontrar una cierta recurrencia en los datos transferidos a través de la red protegida.



Filtros de Tipo de Archivo

Los filtros de tipo de archivo se pueden utilizar para bloquear documentos específicos por sus extensiones, sin importar si han sido modificadas de forma manual por el usuario.



Lista Blanca de Archivos

Mientras que todos los otros intentos de transferencia de archivos están bloqueados, las listas blancas pueden ser creadas para evitar redundancia y aumentar la productividad.



Lista Blanca de Dominio y URL

Permite aplicar las políticas de la empresa a la vez que permite a los empleados la flexibilidad que les hace falta para cumplir el trabajo. Pueden incluirse en la lista blanca los portales o correos electrónicos corporativos.



Desactivar la Impresión de Pantalla

Revoque la opción de hacer captura de pantalla y asegúrese de que la información confidencial mostrada en la pantalla no pueda salir de la red protegida.



Monitorización del Portapapeles

Elimine la fuga de datos sensibles a través de la acción de cortar y pegar, mejorando aún más la política de seguridad de datos.



Informes y Análisis

Monitoree la actividad relacionada con la transferencia de archivos con una potente herramienta de informes y análisis. Los registros y los informes se pueden exportar también a soluciones SIEM.



Panel de Control y Gráficos

Permite una rápida visión de los eventos y las estadísticas más importantes gracias a los gráficos y tablas disponibles.



Directorio Activo

Permite realizar un despliegue más sencillo e importar y sincronizar todos los grupos y entidades aprovechándose del AD o de herramientas similares.



“Threshold “Global y Regular para Filtros

Permite definir un número máximo de intentos de violación permitido en la transferencia de archivos. Puede aplicarse en base a cada tipo de contenido o en base a la suma de todos los forzamientos.



File Tracing

Registre todos los intentos o las transferencias de archivos a varias aplicaciones online y servicios en la nube, ofreciendo así una visión completa de las acciones de los usuarios.



File Shadowing

Guarde una copia de los archivos que han sido transferidos a dispositivos o a través de correo electrónico, de soluciones en la nube u otras aplicaciones.



Contraseña Temporal

Permita la transferencia temporal de archivos a los equipos desconectados de la red. Garantice la seguridad y la productividad.



Crear Alertas por E-mail

Las alertas por e-mail predefinidas o personalizadas pueden ser configuradas para ofrecer información de los eventos más importantes relacionados con la transferencia de datos confidenciales.



DLP para Impresoras

Establezca políticas para impresoras locales y de red para bloquear la impresión de documentos confidenciales y prevenir así la fuga y la pérdida de datos.



Políticas HIPAA de Content Aware

Permite un escaneo en profundidad de los contenidos que incumplen las políticas legales de los documentos antes de que se efectúe la transferencia.



DLP para Thin Clients

Proteja los datos en Terminal Servers y prevenga la pérdida de datos en entornos con Thin Clients igual que en cualquier otro tipo de red.

Características adicionales

Muchas otras características también están disponibles.

info@endpointprotector.com



Control de Dispositivos

para Windows, Mac OS X y Linux

Unidades USB / Impresoras / Dispositivos Bluetooth / MP3 Players /HDDs Externos / Teensy Board / Cámaras Digitales / Cámaras Web / Thunderbolt / PDAs / Network Share / FireWire /iPhones / iPads iPods / Unidades ZIP / Puerto Serie / Dispositivos de almacenamiento PCMCIA / Dispositivos Biométricos / OTROS



Configurar Permisos Globales

Los permisos de dispositivos se aplican globalmente a través de la red por defecto. No obstante, el módulo es extremadamente



Configurar Permisos por Grupo

Los permisos de dispositivos pueden configurarse de modo granular en función de los grupos, permitiendo diferentes derechos de acceso para varios departamentos.



Configurar Permisos por Equipos

Los permisos de dispositivos se pueden configurar por equipo. Es útil cuando un equipo tiene un papel único en la organización.



Configurar Permisos por Usuario

En función de su puesto y sus tareas, cada usuario puede recibir diferentes niveles de acceso de acuerdo con las políticas de la empresa.



Configurar Permisos por Dispositivos

La granularidad de los permisos permite una clasificación hasta el nivel de dispositivo, basado en el ID del fabricante, ID del producto y número de Serie.



Clases Personalizadas

Los permisos pueden ser creados en base a las clases de dispositivos, haciendo la gestión más fácil para productos del mismo fabricante.



Trusted Device (Dispositivo de Confianza)

Para dispositivos cifrados, se pueden establecer diferentes permisos de acceso basados en el nivel de cifrado (software, hardware, etc.).



File Tracing

Registra todos los intentos o las transferencias de datos a dispositivos de almacenamiento USB, ofreciendo una completa visión de las acciones de los usuarios.



File Shadowing

Guarde una copia de los archivos que han sido transferidos a dispositivos controlados.



Contraseña Temporal

Permita acceso temporal de los dispositivos a los equipos fuera de la red local. Garantiza seguridad y la productividad y permite la transferencia temporal de archivos a los equipos desconectados de la red.



Crear Alertas por E-mail

Las alertas por e-mail predefinidas o personalizadas pueden ser configuradas para ofrecer información de los eventos más importantes relacionados con la transferencia de datos confidenciales.



Panel de Control y Gráficos

Permite una rápida visión de los eventos y las estadísticas más importantes gracias a los gráficos y tablas disponibles .



Informes y Análisis

Monitoree la actividad relacionada con la transferencia de archivos con una potente herramienta de informes y análisis. Los registros y los informes se pueden exportar también a soluciones SIEM.

Características adicionales

Muchas otras características también están disponibles.

info@endpointprotector.com



Cifrado Forzado

para Windows y Mac OS X



Cifrado forzado de dispositivos USB

Autorice solamente el uso de dispositivos USB cifrados y asegúrese de que todos los datos copiados en los dispositivos de almacenamiento son cifrados automáticamente.



Contraseña Máster

La creación de una "Contraseña Máster" proporcionará continuidad en diferentes circunstancias como por ejemplo, el reseteo de la contraseña de un usuario.



Fuertes Mecanismos de Seguridad

Cifrado de 256 bits, con protección basada en contraseña y técnicas anti-manipulación para asegurar la integridad de la aplicación.

Características adicionales

El cifrado está disponible también para Almacenamiento en la Nube, Carpetas Locales, CDs & DVDs

info@endpointprotector.com



Gestión de Dispositivos Móviles

para Android, iOS y Mac OS X



Registro inalámbrico para iOS & Android

Los dispositivos pueden ser registrados en remoto a través de SMS, e-mail, enlace URL o Código QR. Elija la forma más conveniente para su red.



Registro masivo

Para un proceso de despliegue eficiente, hasta 500 smartphones y tabletas pueden ser registrados al mismo tiempo.



Bloqueo Remoto

Active en un instante el bloqueo remoto del dispositivo móvil en caso de incidencias, evitando así la fuga de datos debida a dispositivos perdidos o extraviados.



Seguimiento y Localización

Monitoree de cerca los dispositivos móviles de la empresa y manténgase informado en todo momento de dónde se encuentran los datos sensibles de la empresa.



Desactivar funcionalidades incorporadas

Controle los permisos de las funcionalidades incorporadas como la cámara para evitar violaciones y la pérdida de datos sensibles.



Reproducción de sonido fuerte para la localización de dispositivos perdidos

Localice un dispositivo extraviado mediante la activación remota de un sonido fuerte hasta que se encuentre el dispositivo (soportado en Android).



Gestión de Aplicaciones Móviles

Gestione las aplicaciones según las políticas de seguridad de la organización. Permite el despliegue en remoto e instantáneo de aplicaciones gratuitas o de pago en los dispositivos registrados.



Despliegue de configuración de red

Despliegue la configuración de la red para e-mail, Wi-Fi, VPN, Bluetooth, modo de timbre, etc., o desactívelos.



Alertas

Disponibilidad de alertas predefinidas del sistema al igual que la posibilidad de configurar alertas personalizadas.



Informes y Análisis

Monitoree la actividad relacionada con la transferencia de archivos con una potente herramienta de informes y análisis. Los registros y los informes se pueden exportar.



Modo Kiosk con Samsung Knox

Bloquee el dispositivo móvil en una aplicación específica. Aplique la seguridad de forma en remoto a toda la flota de dispositivos móviles y conviértelos en dispositivos dedicados.



Gestión de Mac OS X

Para extender las funcionalidades de DLP, los Macs se pueden registrar también en el módulo de MDM aprovechando de opciones de configuración adicionales.



Aplicación de Contraseña

Protección proactiva de los datos sensibles de la empresa guardados en dispositivos móviles aplicando fuertes políticas de contraseñas.



Borrado Remoto

Borrado en remoto de manera sencilla para las situaciones críticas en las que la única forma de prevenir la fuga de datos es borrando el contenido del dispositivo.



Geofencing

Defina un perímetro geográfico virtual para conseguir el control de las políticas de MDM aplicadas en un área específica.



Restricciones iOS

Asegúrese de que el dispositivo es utilizado únicamente para cuestiones laborales. Si no cumplen con las políticas de la empresa, desactive iCloud, Safari, App Store, etc.



Despliegue de vCards en Android

Agregue y despliegue contactos en dispositivos móviles Android asegurándose de que su fuerza de trabajo móvil puede estar en contacto rápidamente con los contactos adecuados.



Monitorización de Aplicaciones

Manténgase informado con respecto a las aplicaciones que los empleados se descargan en los dispositivos móviles, manteniendo el equilibrio necesario entre el trabajo y el ocio.



Gestión de Activos

Obtenga una visión de los dispositivos móviles administrados con detalles como el nombre del dispositivo, tipo, modelo, capacidad, versiones S.O, operador, IMEIs, MACs, etc.



Crear Alertas por E-mail

Las alertas por e-mail se pueden configurar para ofrecer información acerca de los eventos más importantes relativos al uso de los dispositivos móviles.



Panel de Control y Gráficos

Permite una rápida visión de los eventos y las estadísticas más importantes gracias a los gráficos y tablas disponibles.

Características adicionales

Muchas otras características también están disponibles.

info@endpointprotector.com

100% Flexibilidad de Despliegue

Adecuados para cualquier tipo de red, nuestros productos pueden ser utilizados por grandes empresas, PYMES e incluso usuarios domésticos. Con una arquitectura cliente-servidor, el despliegue y la administración se realizan fácilmente y de manera centralizada desde su interfaz basada en web. Además del Hardware Appliance y del Virtual Appliance, la Instancia de Amazon Web Services y la versión basada en la nube, existe una versión autónoma para aquellos que están buscando las funcionalidades más básicas.

Endpoint Protector

Content Aware Protection, Control de Dispositivos y Cifrado están disponibles para equipos con diferentes versiones de Windows, Mac y distribuciones de Linux. La Gestión de Dispositivos Móviles y la Gestión de Aplicaciones Móviles están asimismo disponibles para dispositivos móviles iOS y Android.

My Endpoint Protector

Content Aware Protection, Control de Dispositivos y Cifrado están disponibles para equipos con diferentes versiones de Windows y Mac OS X. La Gestión de Dispositivos Móviles y la Gestión de Aplicaciones Móviles están asimismo disponibles para dispositivos móviles iOS y Android.



Hardware Appliance



Virtual Appliance



Instancia de Amazon



Solución en la Nube

Módulos

Puestos de trabajo protegidos



Windows	Windows XP / Windows Vista (32/64 bit)	●	●	●
	Windows 7 / 8 / 10 (32/64 bit)	●	●	●
	Windows Server 2000 - 2016 (32/64 bit)	●	●	●
Mac OS X	Mac OS X 10.6 Snow Leopard	●	●	●
	Mac OS X 10.7 Lion	●	●	●
	Mac OS X 10.8 Mountain Lion	●	●	●
	Mac OS X 10.9 Mavericks	●	●	●
	Mac OS X 10.10 Yosemite	●	●	●
	Mac OS X 10.11 El Capitan	●	●	●
Linux	Ubuntu	●	●	n/a
	OpenSUSE	●	●	n/a
	CentOS / RedHat	●	●	n/a
*Por favor consulte los detalles relacionados con las versiones y distribuciones soportadas en endpointprotector.com/linux				
iOS	iOS 4, iOS 5, iOS 6, iOS 7, iOS 8, iOS 9			●
Android	Jelly Bean (4.1+), KitKat (4.4+), Lollipop (5.0+)			●



HQ (Romania)

E-mail: sales@cososys.com
Sales: +40 264 593 110 / ext. 103
Support: +40 264 593 113 / ext. 202

Korea

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

Germany

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

North America

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

Official Partner

www.endpointprotector.es