ENDPOINT PROTECTOR | by CoSoSys

HOJA DE DATOS 5.2.0.5

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

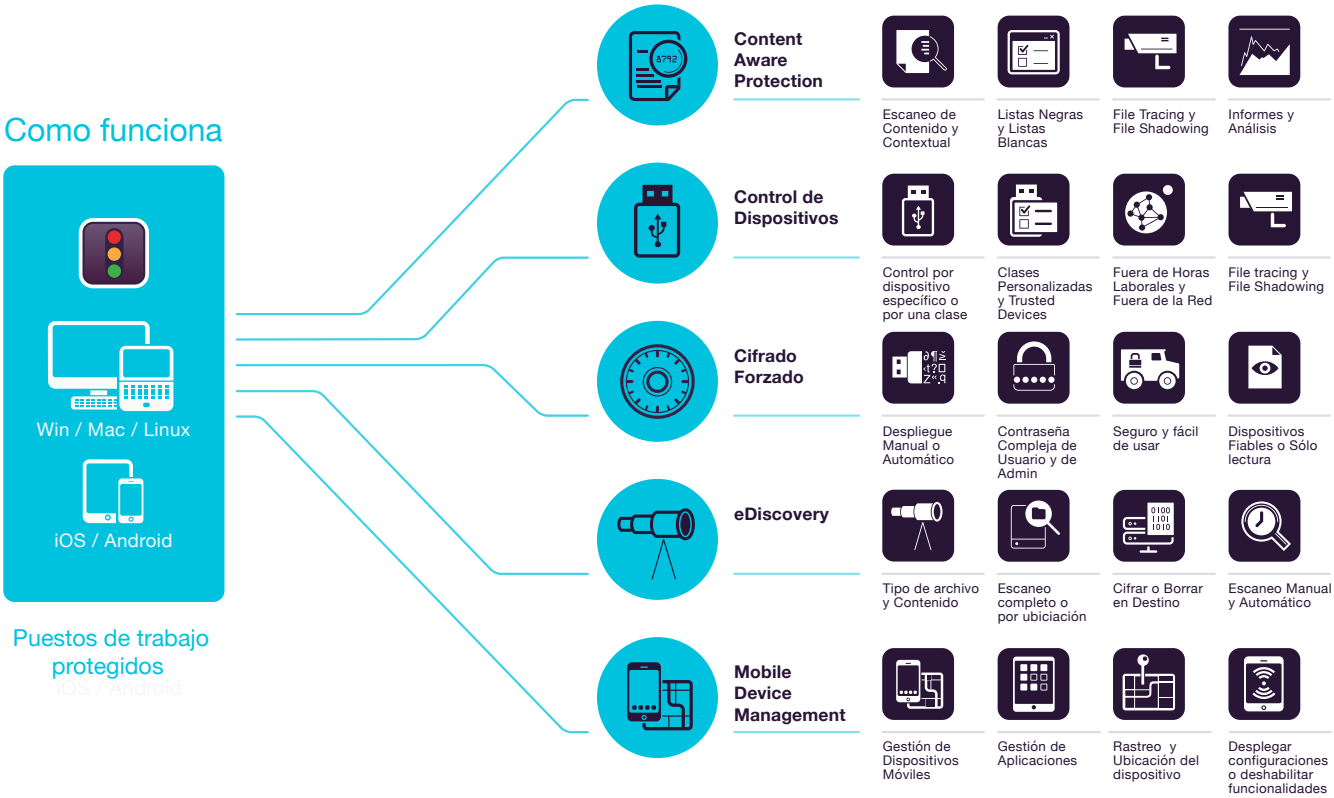
ENDPOINT PROTECTOR

by CoSoSys

Solución “out of the box” que protege los datos confidenciales contra las amenazas plateados por dispositivos portátiles de almacenamiento, servicios en la nube y dispositivos móviles.

En un mundo donde los dispositivos portátiles y de estilo de vida y la nube están transformado la manera en que vivimos y trabajamos, Endpoint Protector ha sido diseñado para proteger la información contra las amenazas internas, al mismo tiempo que mantiene la productividad y hace que el trabajo sea más cómodo, seguro y agradable.
El enfoque en las Listas Negras y Listas Blancas otorga flexibilidad en la creación de políticas. Las organizaciones tienen la opción de prohibir el uso de dispositivos extraíbles específicos, la transferencia de datos a aplicaciones de compartir archivos en la nube y otros servicios online, de escanear ciertos PII, pero permitir transferencias a URLs y nombres de dominios específicos para ciertos ordenadores/usuarios/grupos, evitando la interrupción de tareas.
Con Endpoint Protector siendo disponible como Hardware o Virtual Appliance, se puede configurar en cuestión de minutos. Además, la interfaz de gestión adaptable permite administrar políticas y verificar informes desde cualquier dispositivo, desde ordenadores a tabletas.
Endpoint Protector reduce drásticamente los riesgos planteados por las amenazas internas que pueden determinar la fuga y el robo de datos. Asimismo, permite el cumplimiento con las normas y las regulaciones de la industria.

Como funciona



Content Aware Protection para Windows, macOS y Linux	Monitorice 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, macOS 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.
Cifrado Forzado para Windows y macOS	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.
eDiscovery para Windows, macOS y Linux	Escanee datos en reposo en los puntos finales de la red y aplique acciones de remediación tales como encriptar o borrar datos en caso de identificación de datos confidenciales en ordenadores no autorizados.
Gestión de Dispositivos Móviles para Android, iOS y macOS	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.

Content Aware Protection

para Windows, macOS 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

Lista negra de puntos de salida

Los filtros se pueden configurar en base a una gran lista de aplicaciones monitorizadas. Dispositivos de almacenamiento USB, recursos compartidos de red y otros puntos de salida pueden ser monitorizados por contenido.

Lista negra por tipo de archivo

Los filtros por tipo de archivo se pueden utilizar para bloquear documentos basados en su extensión, incluso si éstos son modificados de forma manual por el usuario.

Lista negra de contenido predefinido

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

Lista negra de diccionario personalizado

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

Lista negra por nombre de archivo

Se pueden crear filtros basados en nombres de archivos. Éstos se pueden configurar en función del nombre y la extensión del archivo, solo el nombre o solo la extensión.

Lista negra y lista blanca de ubicación de archivo

Se pueden crear filtros basados en la ubicación del archivo en el HDD local. Se puede definir para incluir o excluir conteniendo subcarpetas.

Lista negra de expresiones regulares

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

Lista blanca de archivos permitidos

Mientras todos los intentos de transferencia de archivos están bloqueados, se pueden crear listas blancas para evitar redundancia y aumentar la productividad.

Lista blanca de dominio y URL

Permite aplicar las políticas de la empresa a la vez que le da a los empleados la flexibilidad que necesitan para cumplir con su trabajo. Pueden incluirse en la lista blanca portales o correos electrónicos corporativos.

Monitorización de impresión de pantalla y portapapeles

Desactive la opción de hacer capturas de pantalla. Elimine la fuga datos sensibles a través de la acción de copiar/cortar y pegar, mejorando aún más la política de seguridad de datos.

Reconocimiento Óptico de Caracteres (OCR)

Inspeccione el contenido de fotos e imágenes, detectando información confidencial desde documentos escaneados y otros archivos similares.

File tracing y file shadowing

Registre todos los intentos o las trasferencias de archivos a varias aplicaciones online y otros puntos de salida. Para una mejor investigación, guarde una copia de los archivos que han sido transferidos.

Límite para filtros

Permite definir un número máximo de intentos de violación en la transferencia de archivos. Puede aplicarse en base a cada tipo de contenido o en base a la suma de todas las violaciones.

Límite de transferencia

Establezca un límite de transferencia dentro de un intervalo de tiempo específico. Eso puede basarse en una cantidad de archivos o tamaño de archivo. Dispone de alertas por correo electrónico cuando se alcanza el límite.

Escaneo de contenido y contextual

Habilite un mecanismo de inspección avanzada para una detección más precisa de contenido sensible como PIIs. Disponible la personalización de contexto.

Contraseña temporal

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

Panel de control, informes y análisis

Monitorice 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.

Cumplimiento (GDPR, HIPAA, etc.)

Cumplir con las reglas de la industria y regulaciones como PCI, DSS, GDPR, HIPAA, etc. Evite las multas y otros prejuicios.

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.

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, macOS 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

Permisos de forma granular

Los permisos del dispositivo se pueden configurar de forma global, por grupo, equipo, usuario y dispositivo. Use los ajustes por defecto o configure según sea necesario.

Tipos de dispositivos y dispositivos específicos

Establece permisos (denegar, permitir, solo lectura, etc.) para tipos de dispositivos o dispositivos específicos (utilizando VID, PID 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.

Políticas fuera del horario laboral

Las políticas de control de dispositivos se pueden configurar para aplicarse cuando se encuentra fuera de las horas normales de trabajo. Se puede establecer la hora de inicio y finalización, y los días hábiles.

Políticas fuera de la red

Las políticas de control de dispositivo se pueden configurar para aplicarse cuando se encuentra fuera de la red de la compañía. La configuración está basada en nombres de dominio DNS y direcciones IP.

Sincronización de Active Directory

Aproveche AD para hacer grandes despliegues de forma más simple. Mantenga a las entidades actualizadas, reflejando el grupos de red, computadoras y usuarios.

Información de Usuarios y Equipos

Obtenga una mejor visibilidad con información tal como ID de empleados, equipos, ubicación, detalles de contacto y más (direcciones IP, MAC, etc.)

File tracing

Registre todos los intentos o las trasferencias 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 el acceso temporal de los dispositivos a los equipos fuera de la red local. Garantice 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.

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

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

Características adicionales

Muchas otras características también están disponibles.
info@endpointprotector.com

Cifrado Forzado

para Windows y macOS

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.

Despliegue automático y solo lectura

El despliegue se puede hacer de forma automática y manual. existe la posibilidad de dar permisos de solo lectura hasta que el cifrado sea necesario.

Usuarios complejos y contraseña maestra

La complejidad de la contraseña se puede configurar según sea necesario. La contraseña maestra proporciona continuidad en circunstancias como el restablecimiento de la contraseña de los usuarios.

Características adicionales

El cifrado está disponible también para Almacenamiento en la Nube, Carpetas Locales, CDs & DVDs
info@endpointprotector.com

eDiscovery

para Windows, macOS y Linux

Tipo de archivos: Archivos Gráficos / Archivos Office / Archivos comprimidos / Archivos de programación / Archivos de medios, etc • Contenido predefinido: Tarjetas de Crédito / Información de Identificación Personal / Dirección / SSN / DNI / Pasaporte / Número de Teléfono / DNI / Seguro Médico, etc • Contenido Personalizado / Nombre de Archivo / Expresiones Regulares / HIPAA

Cifrar y descifrar archivos

Los datos en reposo que contienen información confidencial pueden estar encriptado para evitar el acceso de los empleados no autorizados. Las acciones de descifrado también están disponibles.

Borrar archivos

Si se dan violaciones claras de la política interna, borre la información sensible tan pronto como sea detectado en endpoints no autorizados.

Lista negra de ubicaciones a escanear

Los filtros se pueden crear en base a ubicaciones predefinidas. Evite el escaneo redundante de datos en reposo con inspecciones específicas.

Escaneo automático

Además del escaneo “Clean” y del escaneo “Incremental”, se pueden programar escaneos automáticos, ya sea cada X tiempo o por repetición (semanal o mensual).

File tracing

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

Informes y análisis

Monitorice 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.

Límite para filtros

Permite definir un número máximo de intentos de violación permitida en la transferencia de archivos. Puede aplicarse en base a cada tipo de contenido o en base a la suma de todas las violaciones.

Cumplimiento (GDPR, HIPAA, etc.)

Cumplir con las reglas de la industria y regulaciones como PCI DSS, GDPR, HIPAA, etc. Evite las multas y otros prejuicios.

Integración con SIEM

Aproveche las soluciones de Seguridad de la Información y Gestión de Eventos mediante la externalización de registros. Asegura una experiencia única para los productos de seguridad.

Lista negra por tipo de archivo

Los filtros por tipo de archivo se pueden usar para bloquear documentos basados en su extensión, incluso si estos son modificados manualmente por los usuarios.

Lista negra de contenido predefinido

Los filtros se pueden crear en base a un contenido predefinido como números de tarjetas de crédito, DNI números de seguridad y muchos más.

Lista negra de diccionario personalizado

También se puede crear una lista negra basada en contenido personalizado, como palabras clave y expresiones. Se pueden crear múltiples diccionarios de listas negras.

Lista negra por nombre de archivo

Se pueden crear filtros basados en nombres de archivos. Éstos se pueden configurar en función del nombre y la extensión del archivo, o solo el nombre o solo la extensión.

Lista negra y lista blanca de ubicación de archivos

Se pueden crear filtros basados en la ubicación del archivo en el HDD local. Estos se pueden definir para incluir o excluir conteniendo subcarpetas.

Lista negra de expresiones regulares

Se pueden crear listas negras personalizadas avanzadas para encontrar cierta recurrencia en los datos almacenados en la red protegida.

Lista blanca de archivos permitidos

Mientras todos los otros intentos de transferencias de archivos son bloqueados, se pueden crear listas blancas para evitar redundancia y aumentar la productividad.

Lista blanca de dominio y URL

Permite aplicar las políticas de la empresa a la vez que le da a los empleados la flexibilidad que necesitan para cumplir con su trabajo. Pueden incluirse en la lista blanca portales o correos electrónicos corporativos.

Lista blanca por tipo de archivo MIME

Evite el escaneo redundante a nivel global excluyendo la inspección de contenido para ciertos tipos de archivos MIME.

Características adicionales / Muchas otras características también están disponibles. / info@endpointprotector.com

Gestión de Dispositivos Móviles

para Android, iOS y macOS

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

Monitorice 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

Monitorice 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 Samung 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, eDiscovery, Control de Dispositivos y Cifrado están disponibles para equipos con diferentes versiones de Windows, macOS 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 7 / 8 / 10	(32/64 bit)	●	●	●	●
	Windows Server 2003 - 2016	(32/64 bit)	●	●	●	●
	Windows XP / Windows Vista	(32/64 bit)	●	●	●	●
macOS	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	●	●	●	●
	macOS 10.7	Lion	●	●	●	●
Linux	Ubuntu		●	●	●	n/a
	OpenSUSE / SUSE		●	●	●	n/a
	CentOS / RedHat		●	●	●	n/a
	Fedora		●	●	●	n/a

*Por favor consulte los detalles relacionados con las versiones y distribuciones soportadas en endpointprotector.es/linux

iOS	iOS 4, iOS 5, iOS 6, iOS 7, iOS 8, iOS 9, iOS 10, iOS 11, iOS 12	●
Android	Jelly Bean (4.1+), KitKat (4.4+), Lollipop (5.0+), Marshmallow (6.0+), Nougat (7.0+), Oreo (8.0+), Pie (9.0+)	●

COSOSYS

HQ (Romania)

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

Germany

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

Korea

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

North America

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

Official Partner