ENDPOINT PROTECTOR | by CoSoSys

HOJA DE DATOS 5.2.0.8

Solución de Prevención de Pérdida de Datos (DLP) Líder en la Industria

Solución de seguridad de nivel empresarial para cualquier industria

DLP para Windows, macOS y Linux

Protegiendo toda la red

ENDPOINT PROTECTOR | by CoSoSys

Una solución de Prevención de Pérdida de Datos (DLP) avanzada que pone fin a las fugas y al robo de datos ofreciendo al mismo tiempo un control para los dispositivos de almacenamiento portátiles y garantizando el cumplimiento de las normas de protección de datos.
La solución está diseñada para proteger los datos confidenciales de las amenazas internas, manteniendo la productividad y haciendo que el trabajo sea más conveniente, seguro y agradable.
Endpoint Protector es una solución DLP de nivel empresarial para Windows, macOS, Linux, Thin Clients y soluciones de Desktop-as-a-service (DaaS). Esta solución es una opción ideal para las empresas que operas con redes multiplataformas y tiene un formato modular que permite mezclar y combinar las herramientas adecuadas para satisfacer necesidades específicas. Haciendo el despliegue de la solución, las organizaciones pueden salvaguardar la información personal y cumplir con los requerimientos de las regulaciones cómo GDPR, HIPPA, CCPA, PCI DSS etc. Endpoint Protector ofrece también protección para la propiedad intelectual de la empresa y los secretos comerciales.

Beneficios Clave

Fácil de instalar y gestionar

Endpoint Protector puede estar en funcionamiento en 30 minutos. La solución es fácil de ejecutar tanto por personal técnico, cómo no técnico.

Perfiles de cumplimiento predefinidos

Con las políticas de protección de datos predefinidas, es fácil encontrar datos regulados y asegurar los requerimientos de cumplimiento con GDPR, CCPA, HIPPA, PCI DSS y otras.

Protección multiplataforma

La solución ofrece las mismas características de seguridad y nivel de protección para computadoras en los sistemas operativos Windows, macOS y Linux.

Informes detallados de la actividad del usuario

Con Endpoint Protector es rastrear, reportar y obtener información valiosa sobre qué datos sensibles están transferidos a dónde y por quién.

Opciones de implementación flexibles

Endpoint Protector se puede implementar de múltiples maneras, dependiendo de las necesidades y la infraestructura existente de la empresa.

Políticas granulares

Se pueden definir derechos de acceso granulares para los dispositivos extraíbles y puertos periféricos, así como políticas de seguridad para usuarios, equipos y grupos.

Control de Dispositivos
para Windows, macOS y Linux

Monitorear y Controlar los USB y los puertos periféricos. Establecer Derechos por Dispositivo, Usuario, Equipo, Grupo o de manera Global.

Content Aware Protection
para Windows, macOS y Linux

Monitorear y Controlar datos en movimiento, decidiendo qué datos confidenciales puedan o no salir de la empresa via varios puntos de salida. Los Filtros se puede configurar por Tipo de Archivo, Aplicaciones, Contenido Predefinido y Personalizado, Expresiones Regulares y más.

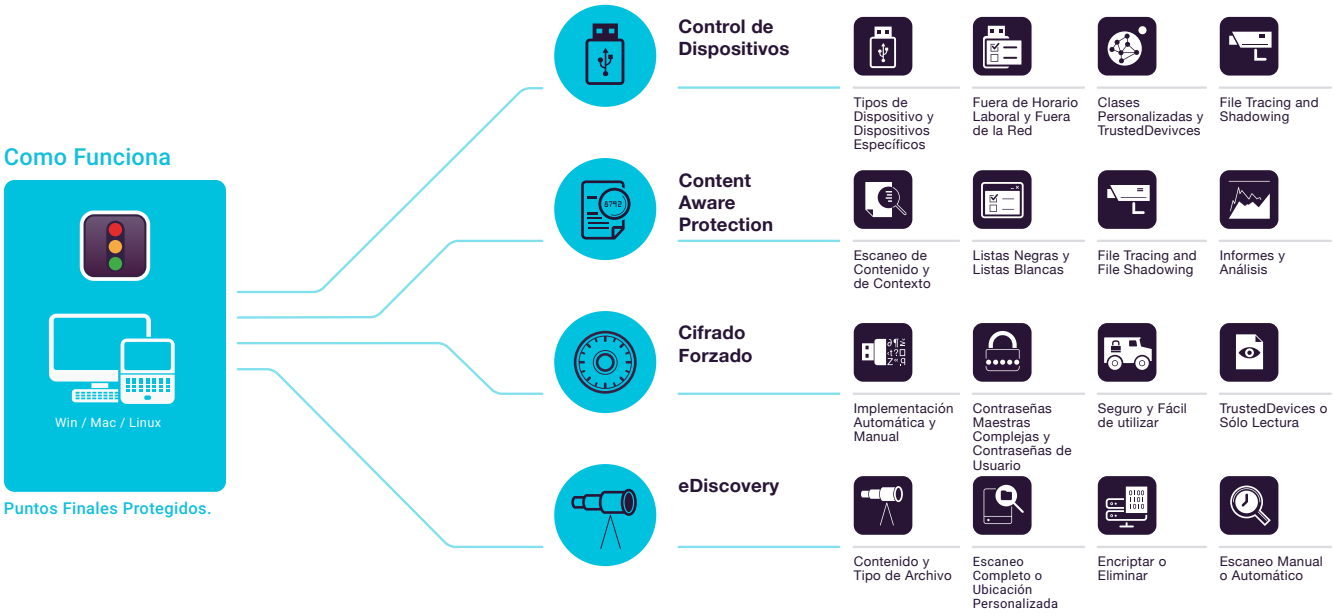
Cifrado Forzado
para Windows, macOS y Linux

Proteger de manera automática los datos copiados a dispositivos USB de almacenamiento con encriptación AES 256bit. Multiplataforma, basado en contraseña, fácil de utilizar y muy eficiente.

---

eDiscovery
para Windows, macOS y Linux

Escanear datos en reposo en los puntos finales de la red y aplicar acciones de remediación, cómo encriptar o eliminar en el caso de que los datos confidenciales están identificados en equipos no autorizados.

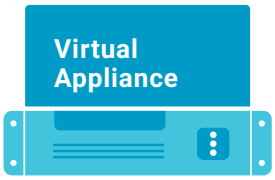


Salud | Educación | Fabricación | Financiero | Media

100% Flexibilidad de Implementación

Nuestros productos son de nivel empresarial y están en una continua evolución para poder servir mejor a cualquier tipo de red e industria. Con una arquitectura cliente-servidor, el despliegue y la administración se realizan fácilmente y de manera centralizada desde la interfaz web. Además del Virtual Appliance, el servidor puede ser almacenado por nosostros y en las principales infrastructuras de nube, cómo Amazon Web Services, Microsoft Azure y Google Cloud.

Control de Dispositivos, Content Aware Protection, Cifrado Forzado y eDiscovery están disponibles para equipos que tienen diferentes versiones de Windows, macOS y Linux.



Virtual Appliance

Servicios en la Nube

Amazon Web Services
Microsoft Azure
Google Cloud

Almacenado en Nube

Control de Dispositivos

para Windows, macOS y Linux

Unidades USB/ Impresoras / Dispositivos Bluetooth / CD & DVD / HDDs Externos / Teensy Board / Cámaras Digitales / Cámaras Web / Thunderbolt / Wifi / Network Share / FireWire / iPhones / iPads/ iPods / Unidades ZIP / Lectores de Tarjeta / Smartphones Android / Modems USB / OTROS

Establecer 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 Dispositivo y Dispositivos Específicos

Establecer permisos – denegar, permitir, solo lectura etc. Los permisos se pueden aplicar para un tipo de dispositivo o puede ser para dispositivos específicos (basado en FID, PID y Número de Serie).

Clases Personalizadas

Aplicar permisos para dispositivos basados en el ID del Fabricante y el ID del Producto para para una gestión más fácil de los productos del mismo fabricante.

Políticas Fuera del Horario Laboral

Las Políticas de Control de Dispositivos se pueden configurar para aplicarse fuera de las horas normales de trabajo. Se pueden establecer la hora de inicio y finalización, y los días laborales.

Políticas Fuera de la Red

as políticas Fuera de la Red se pueden configurar para aplicarse fuera de la red de la empresa. La aplicación está basada en las direcciones FODN y DNS IP.

Sincronización del Directorio Activo

Aprovechar el DA para hacer despliegues grandes de forma más simple. Mantenga las entidades actualizadas, reflejando el grupo de red, equipos y usuarios.

Información de Usuarios y Equipos

Obtener una mejor visibilidad con informaciones como por ejemplo el ID de los Empleados, Equipos, Ubicación, detalles de contacto correctos y más (direcciones IP, MAC etc.)

File Tracing

Registrar todos los intentos o las trasferencias de datos a dispositivos de almacenamiento USB, ofreciendo una visión más clara de las acciones de los usuarios.

File Shadowing

Crear instantáneas de archivos transferidos a dispositivos autorizados para auditorías detalladas.

Contraseña Temporal Offline

Permitir el acceso temporal de los dispositivos a los equipos fuera de la red local. Garantice la seguridad y la productividad.

Crear Alertas via Correo Electrónico

Recibir alertas por correo en tiempo real para varios eventos relacionados al uso de medios extraíbles en las computadoras de la empresa.

Panel de Control y Gráficos

Son disponibles gráficos y tablas para una perspectiva general rápida de los eventos y las estadísticas más importantes.

Informes y Análisis

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

Límite de trasnferencia

Limitar el número de archivos o el tamaño del archivo que se pueden transferir dentro de un intervalo de tiempo. Incluir o excluir las transferencias por dispositivos, aplicaciones online y redes compartidas.

Cifrado Forzado

para Windows, macOS y Linux

Cifrado de grado militar 256bit AES / Técnicas antisabotaje / Gestión de contraseña centralizada/ Enviar mensajes a los usuarios / Borrado remoto / Configuración de política de contraseña / OTROS

Cifrado forzado de dispositivos USB

Autorizar solamente el uso de dispositivos USB cifrados y asegurar que todos los datos copiados en estos dispositivos son cifrados automáticamente.

Despliegue automático y Solo Lectura

Están disponibles tanto el despliegue automático, cómo el despliegue manual. Está también disponible la opción de permitir Acceso de Solo Lectura hasta que la encriptación sea necesaria.

Contraseñas Maestras y de Usuario Complejas

La complejidad de la contraseña se puede establecer según se necesita. La Contraseña Maestra proporciona continuidad en circunstancias cuando la contraseña de usuarios se reestablece.

Gestión de contraseña y borrado remoto

Cambiar las contraseñas de los usuarios de forma remota y borrar los datos cifrados en caso de dispositivos comprometidos.

Content Aware Protection

para Windows, macOS y Linux

Clientes de E-mail: Outlook / Thunderbird / Apple Mail • Navegadores Web: Internet Explorer / Firefox / Chrome / Safari • Mensajería Instantánea: Skype / Slack / WhatsApp • Servicios en la Nube & Compartir Archivos: Dropbox / iCloud / OneDrive /BitTorrent / AirDrop • Otras aplicaciones: iTunes / FileZilla / SFTP/ Total Commander / Team Viewer / OTROS

Lista Negra de Puntos de Salida

Autorizar solamente el uso de dispositivos USB cifrados y asegurar que todos los datos copiados en estos dispositivos son cifrados automáticamente.

Lista Negra de Tipo de Archivo

Los filtros por Tipo de Archivo se pueden utilizar para bloquear documentos basados en el tipo del archivo real, aunque los usuarios cambien la extensión.

Listas Negras 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.

Listas Negras de Contenido Personalizado

Los filtros se pueden crear también basados en contenido personalizado como palabras clave y expresiones. Se pueden crear Múltiples Diccionarios de Listas Negras.

Listas Negras de Nombre de Archivo

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

Listas Negras y Listas blancas 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 las subcarpetas.

Listas negras de Expresiones Regulares

Una herramienta poderosa que permite identificar una secuencia de características que definen un patrón de búsqueda.

Fuera de Horario y Fuera de la Red

Definir políticas de reserva que van a funcionar fuera de las horas laborales o fuera de la red.

Lista Blanca de Dominio y URL

Hacer cumplir las políticas de la compañía, pero permita a los empleados la flexibilidad que necesitan para hacer su trabajo. Habilitar la función DPI y la lista blanca de portales de empresa o direcciones de correo electrónico.

Monitorización de la Captura de Pantalla y Portapapeles

Desactivar la opción de hacer capturas de pantalla. Eliminar 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)

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

Integración con SIEM

Aprovechar la Información de Seguridad y los Productos de Gestión de evento mediante la externalización de registros. Garantizar una experiencia fluida a través de los productos de seguridad.

Límite para Filtros

Definir el número de violaciones de política que puede contener un archivo para que se aplique la política de seguridad y se informe / bloquee la transferencia del archivo.

Límite de Trasnferencia

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

Escaneo de Contenido y Contextual

Habilitar un mecanismo de inspección avanzada para una detección más precisa de contenido sensible como PII. Está disponible la personalización de contexto.

Contraseña Temporal Offline

Permitir la transferencia temporal de archivos a los equipos desconectados de la red. Garantizar la seguridad y la productividad.

Panel de control, Informes y Análisis

Monitorizar la actividad relacionada con la transferencia de archivos con una potente herramienta de informes y análisis. Obtener informes gráficos para los ejecutivos de nivel C.

Cumplimiento (GDPR, HIPAA etc.)

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

DLP para Impresoras

Establecer 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

Protejer los datos en Terminal Servers y prevenir la pérdida de datos en entornos de Thin Clients cómo en cualquier otro tipo de red.

eDiscovery

para Windows, macOS y Linux

Tipo de archivo: Archivos Gráficos / Archivos Office / Archivos Comprimidos / Archivos de programación / Archivos Multimedia / etc • Contenido predefinido: Tarjetas de Crédito / Información de Identificación Personal / Dirección / SSN / DNI / Pasaporte / Número de Teléfono / Identificación fiscal / Seguro Médico / etc • Contenido Personalizado / Nombre de Archivo / Expresiones Regulares / HIPAA / OTROS

Cifrar y Descifrar Datos

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

Eliminar Datos

Si ocurren violaciones claras de la política interna, se puede borrar la información sensible tan pronto como se detecte en puntos finales no autorizados.

Listas Negras de Ubicación del Escaneo

Los filtros se pueden crear teniendo como base ubicaciones predefinidas. Evitar el escaneo redundante de datos en reposo con inspecciones específicas.

Escaneos Automáticos

Además del Escaneo “Clean” y del Eescaneo “Incremental”, se pueden programar Escaneos Automáticos, ya sea cada X tiempo o por repetición (semanal o mensual).

Resultados del Escaneo

Gestionar los registros para escanear los datos en reposo y tomar acciones para remediar los problemas encontrados. Los registros también se pueden exportar a las soluciones SIEM.

Estado del Escaneo

Revisar fácilmente el estado actual del escaneo. El estado del escaneo aparece en el formato 0-100%.

Límite para Filtros

Definir el número de violaciones de política que puede tener un archivo para que la política de seguridad se pueda aplicar y el servidor este informado.

Cumplimiento (GDPR, HIPPA etc.)

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

Listas Negras de Tipo de Archivo

Los filtros por Tipo de Archivo se pueden usar para bloquear documentos basados en el tipo real del archivo, incluso si los usuarios cambian la extensión.

Listas negras de Contenido Predefinido

Los filtros se pueden crear basados en un contenido predefinido como Números de Tarjetas de Crédito, Números de Seguridad Social etc.

Listas Negras de Contenido Personalizado

Los filtros se pueden crear también basados en contenido personalizado, como palabras clave y expresiones. Se pueden crear varios Diccionarios de Listas Negra.

Listas Negras de 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.

Listas Negras de Expresiones Regulares

Una herramienta poderosa para poder identificar la secuencia de características que definen un patrón de búsqueda.

Lista Blanca de Archivos Permitidos

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

Listas Blancas por Tipo MIME

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

Integración con SIEM

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

Miles de empresas aseguran sus datos con Endpoint Protector.

AON

"Encontramos que Endpoint Protector es mejor que otras soluciones DLP, especialmente en el rastreo de archivos - características de Content Aware Protection, así como en los Detalles y Control de la Actividad de los usuarios finales"

Prialaksana Januaresza,
Assistant VP & IT Head

Spectrum of HOPE

"Endpoint Protector agrega una fuerte capa de seguridad de datos. Además, el servicio al cliente de CoSoSys es excelente."

Josh McCown,
IT Director

AspirePharmaceuticals

"Nuestra empresa se creó en cuestión de horas y el soporte y el servicio que ofrece CoSoSys son excelentes."

Jay Patel,
Accounts Manager

Gartner peerinsights™

Altamente calificado en **Gartner Peer Insights** para soluciones de prevención de pérdida de datos empresariales.

Puntos Finales Protegidos

Windows	Windows 7 / 8 / 10	(32/64 bit)	●	●	●	●
	Windows Server 2003 - 2019	(32/64 bit)	●	●	●	●
	Windows XP / Windows Vista	(32/64 bit)	●	●	●	●
macOS	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

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