ENDPOINT PROTECTOR | by CoSoSys

FICHA TÉCINCA

Prevención de Pérdida de Datos & Gestión de Dispositivos Móviles

DLP para Windows, Mac y

Protegiendo toda la red

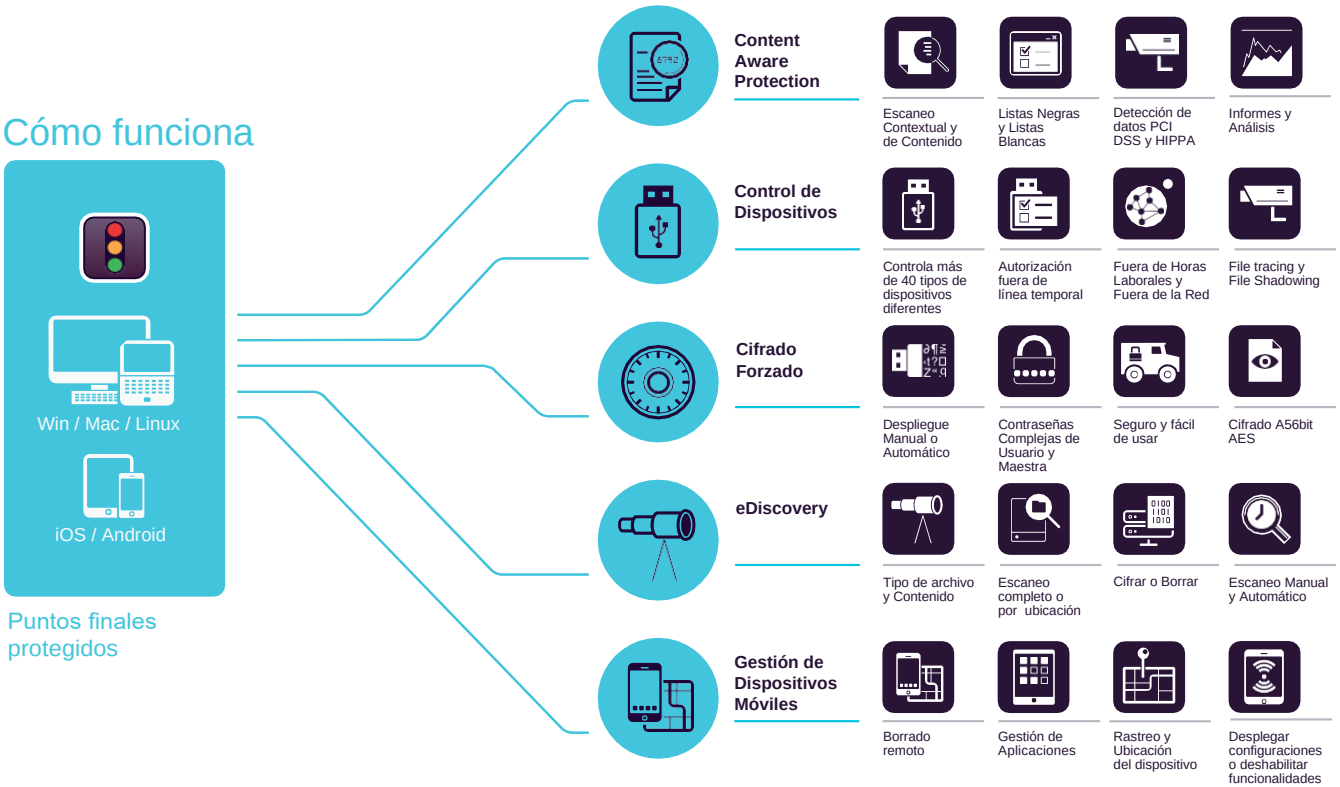
ENDPOINT PROTECTOR | by CoSoSys

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 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 dispositivos iOS y Android. Esta solución está disponible como Virtual Appliance, Hardware Appliance y como instancia en Amazon Web Services, Google Cloud y Microsoft Azure. La solución es fácil de utilizar e instalar sin la necesidad de conocimientos tecnológicos muy avanzados. Se puede gestionar por los administradores o por un solo Panel de Control.

Las filtraciones de contenido de Endpoint Protector, tanto para datos en reposo como para datos en movimiento, varían desde el tipo de archivo hasta el contenido predefinido basado en diccionarios, expresiones regulares o regulaciones de protección de datos como GDPR o HIPAA. La Detección Contextual ofrece una forma avanzada de revisión de datos confidenciales centrándose en el contenido y en el contexto. La transferencia de datos importantes no autorizada a personas o aplicaciones externas es monitorizada y los administradores reciben una alerta en el caso de una violación de la política. La solución tiene un enfoque DLP modular, políticas y configuraciones granulares.

Cómo 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, conteni- do predefinido y contenido personalizado, regex etc.

Control de Dispositivos
para Windows, macOS y Linux

Gestione y controle los dispositivos USB o los puertos periféricos. Establezca derechos por dispositivo, usuario, equipo, grupo o a nivel global.

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 eficaz.

eDiscovery
para Windows, macOS y Linux

Escanee datos en reposo en los puntos finales de la red y aplique acciones de remediación tales como cifrar o borrar datos en caso de identificación de datos confidenciales en equipos 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 / Apple Mail • Navegadores Web: Internet Explorer / Firefox / Chrome / Safari • Mensajería Instantánea: Skype / Slack / WhatsApp • Servicios enla Nube / Compartir Archivos: Dropbox / iCloud / BitTorrent / AirDrop • Otras aplicaciones: iTunes / FileZilla / SFTP/ Total Commander / Team Viewer / OTROS

Lista negra de puntos de salida
Los filtros se pueden configurar teniendo como base una amplia lista de aplicaciones monitorizadas.Dispositivos de almacenamiento USB, recursos compartidos de red y otros puntos de salida pueden ser monitorizados.

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

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 contenido personalizado Permite crear filtros basados 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. Estos 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 las subcarpetas.

Lista negra de expresiones regulares
Una herramienta poderosa que permite identificar una secuencia de características que definen un patrón de búsqueda.

Fuera de Hora y Fuera de la Red
Le permite establecer políticas que van a funcionar fuera de las horas laborales o fuera de la red.

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 de la empresa.

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.

Integración SIEM
Aproveche la información de seguridad y los productos para gestionar el evento mediante la externalización de registros. Garantice una experiencia fluida a través de los productos de seguridad.

Límite para filtros
Establezca un límite de transferencia dentro de un intervalo de tiempo específico. Esto puede basarse en la cantidad de archivos o en el tamaño. Ahora están disponibles alertas por correo electrónico cuando se alcanza el límite.

Límite de transferencia
Establezca un límite de transferencia dentro de un intervalo de tiempo específico. Esto 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. Está disponible la personalización de contexto.

Contraseña temporal offline
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. Puede tener 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. Evite las multas y otros problemas.

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.

Existen más características adicionales. Para más información puede solicitar un demo en: EndpointProtector.com

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

Establezca 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
Se pueden establecer permisos (denegar acceso, permitir acceso, acceso de solo lectura, etc.) para tipos de dispositivos o dispositivos específicos (utilizando VID, PID y número de serie).

Clases personalizadas
Los permisos pueden ser creados a partir del VID y el PID para una gestión más fácil para 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
Reciba alertas a su correo sobre varios eventos que tienen que ver con el uso de medios extraíbles que han tenido lugar en los equipos de la empresa.

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

Información de Usuarios y Equipos
Obtenga una mejor visibilidad con informaciones como por ejemplo el ID de los 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 visión completa de las acciones de los usuarios.

File Shadowing
Guarde una copia de los archivos que han sido transferidos a dispositivos autorizados.

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

Crear alertas por correo
Las alertas por correo pueden ser configuradas para ofrecer información de los eventos más importantes relacionados con la transferencia de datos confidenciales en los equipos de la empresa.

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

Cifrado Forzado
para Windows y macOS

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
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 se necesite el cifrado.

Usuarios complejos y contraseña maestra La complejidad de la contraseña se puede configurar según sea necesario. La contraseña maestra proporciona continuidad en casos como por ejemplo el restablecimiento de la contraseña de los usuarios.

Gestión de contraseña y borrado remoto Le permite cambiar las contraseñas de los usuarios de forma remota y borrar los datos cifrados en el caso de los dispositivos con problemas.

eDiscovery

para Windows, macOS y Linux

Tipo de archivos: 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

Cifrar y descifrar archivos
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.

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

Lista negra de ubicaciones a escanear
Los filtros se pueden crear teniendo como base 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).

Resultados del escaneo
Gestione los registros para escanear los datos en reposo y tome acciones para remediar los posibles problemas encontrados. Los registros e informes también se pueden exportar a las soluciones SIEM.

Estado del escaneo
Revise fácilmente el estado actual de su escaneo. El estado del escaneo aparece en el formato 0-100%.

Límite para filtros
Permite 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, HIPAA, etc.)
Cumplir con las reglas de la industria y regulaciones como PCI DSS, GDPR, HIPAA, etc. Evite las multas y otros problemas.

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 basados en un contenido predefinido como números de tarjetas de crédito, DNI, números de seguridad etc.

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 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.

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.

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.

Existen más características adicionales. Para más información puede solicitar un demo en:

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 eficaz 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 incidentes, evitando así la fuga de datos por culpa de los 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. Esta característica permite el despliegue en remoto e instantáneo de aplicaciones gratuitas o de pago en los dispositivos registrados.

Despliegue de configuración de red
Despliegue o desactive la configuración de la red para correos, Wi-Fi, VPN, Bluetooth, configure un modo de timbre,etc.

Alertas
Disponibilidad de alertas predefinidas del sistema, se pueden recibir correos con notificaciones sobre los eventos relacionados con el monitoreo de los dispositivos móviles.

Modo Kiosk con Samsung Knox
Bloquee el dispositivo móvil en una aplicación específica. Aplique la seguridad de forma remota a todos los dispositivos móviles y conviértalos en dispositivos dedicados.

Gestión de macOS
A parte de los dispositivos iOS y Android, las características MDM se pueden aplicar también a los equipos macOS para una gestión más fácil.

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

Borrado Remoto
Destinado a 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 específico.

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 sus empleados pueden contactar rápidamente con las personas adecuadas.

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, números de teléfono etc.

Crear Alertas por correo
Las alertas por correo se pueden configurar para ofrecer información acerca de los eventos más importantes relativos al uso de los dispositivos móviles.

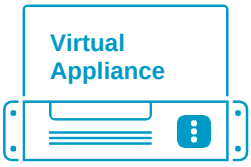
Panel de Control y Gráficos
Permite una rápida visión de los eventos y las estadísticas más importantes gracias a los gráficos y tablas disponibles.

Existen más características adicionales. Para más información puede solicitar un demo en:

100% Flexibilidad de Despliegue

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 Hardware Appliance y del Virtual Appliance, el servidor puede ser almacenado por nosostros en Amazon Web Services, Microsoft Azure y Google Cloud.

Content Aware Protection, Control de Dispositivos, Cifrado Forzado y eDiscovery están disponibles para equipos que tienen diferentes versiones de Windows, macOS y Linux. Gestión de Dispositivos Móviles y Mobile Application Management también están disponibles para iOS y dispositivos móviles Android.



Virtual Appliance

Hardware Appliance

Cloud Services

Amazon Web Services Microsoft Azure Google Cloud

Almacenado en la Nube

Módulos

			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
iOS	iOS 8, iOS 9, iOS 10, iOS 11, iOS 12, iOS 13					●
Android	KitKat (4.4+), Lollipop (5.0+), Marshmallow (6.0+), Nougat (7.0+), Oreo (8.0+), Pie (9.0+), Andoid 10 (10.0+)					●

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

HQ (Rumanía)

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

Alemania

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

America del Norte

E-mail sales.us@endpointprotector.com
Sales +1 888 271 9349
Support +1 877 377 6475

Korea del Sur

contact@cososys.co.kr
+82 70 4633 0353
+82 20 4633 0354

Official Partner