ENDPOINT PROTECTOR | by CoSoSys

ntrs ecurity

HOJA DE DATOS 5.0.0.0

# 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

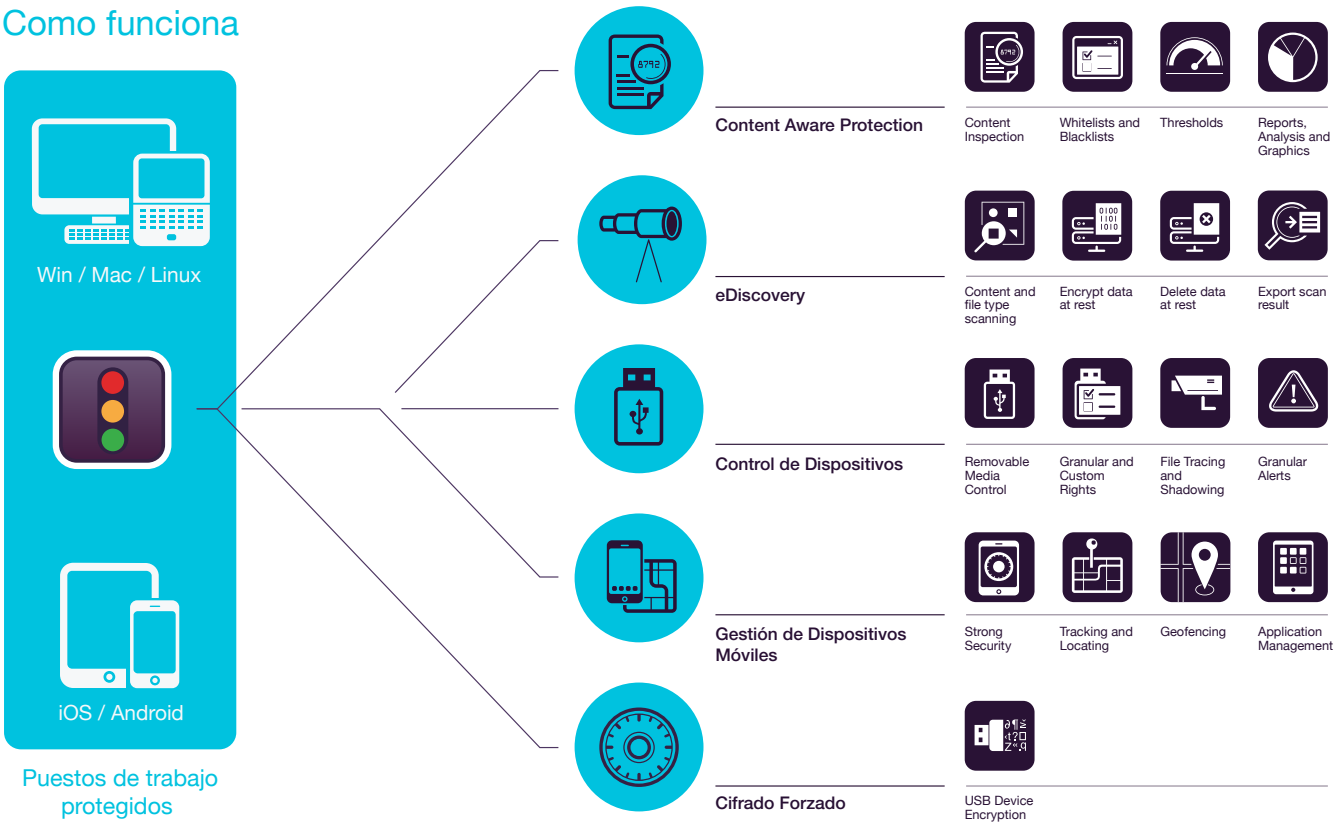
# ENDPOINT PROTECTOR

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**<br>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. |
| **eDiscovery**<br>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. |
| **Control de Dispositivos**<br>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. |
| **Gestión de Dispositivos Móviles**<br>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. |
| **Cifrado Forzado**<br>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. |

# 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

### Filtros de Contenido Predefinido
Los filtros se pueden crear a base de contenido prefinido 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 datos sensibles a través de la acción de cortar y pegar, mejorando aún más la política de seguridad de datos.

### 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.

### 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 trasferencias 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
Si quiere ampliar información

www.ntrsecurity.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

### Escaneo por contenido y tipo de archivo

Cree políticas de eDiscovery personalizadas definiendo que contenido es sensible para su organización en función del tipo de archivo, contenido predefinido, contenido personalizado, nombre de archivo, Regex o contenido protegido de HIPAA. Comience a escanear datos según el contenido seleccionado.

### Cifrar Datos en Reposo

Una vez que se detectan datos confidenciales, el Administrador tiene la opción de cifrarlos con la solución de encriptación AES 256 para evitar el acceso de los empleados no autorizados y además tener la posibilidad de filtrar datos.

### Borrar Datos en Reposo

Proteja los datos y asegure el cumplimiento con las regulaciones de la industria eliminando la información confidencial inmediatamente después de que se identifica si viola la política de la compañía.

### Exportar Resultados de Escaneo

Los resultados del escaneo están disponibles para exportar en Excel, PDF o CSV y pueden utilizarse como informes para la gestión o como documentos de auditoría. Los resultados del escaneo proporcionan los detalles sobre los equipos donde se encontraron los datos confidenciales, qué datos confidenciales, la ruta, hora de descubrimiento, si fueron cifrados, borrados o reportados y otra información valiosa.

### Lista Negra por Tipo de Archivo

Lista Negra por tipo de archivo se puede utilizar para detectar documentos específicos almacenados en puntos finales de red: archivos gráficos, archivos de office, archivos de programación y muchos otros.

### Lista Negra de Contenido Predefinido

Agregue en la Lista Negra de Contenido Predefinido información como números de tarjeta de crédito, números de seguro social, información de identificación personal y otros y descubra la información almacenada y si la misma viola la política de la empresa. Esta lista negra puede ayudar a asegurar el cumplimiento de regulaciones como PCI DSS, HIPAA y otros.

### Lista Negra de Diccionario Personalizado

También puede crear una lista negra basada en contenido personalizado, como palabras clave y expresiones. Se pueden crear varios Diccionarios de Listas Negras mediante Copiar / Pegar, Escribir o Importar.

### Lista Negra por Nombre de Archivo

Busque archivos específicos basados en su nombre y rastree su ubicación. Los resultados se muestran en Resultados de Escaneo de eDiscovery con la lista de archivos encontrados y la posibilidad de ejecutar acciones como eliminar, cifrar o descifrar.

### Lista Negra de Expresiones Regulares

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

### Datos protegidos de HIPAA

Permite un análisis profundo de los puntos finales para detectar información de PHI, los medicamentos aprobados por la FDA, Códigos ICD-10 e ICD-9, etc. Alcance el cumplimiento de HIPAA para detectar dónde reside la información confidencial de salud y aplicar acciones de remediación si es necesario.

### Límites de amenazas y tamaño de archivo

Evite el escaneado redundante utilizando las opciones Umbral. Puede especificar cuándo debe detenerse la inspección según un número determinado de infracciones o que archivos se deben escanear de acuerdo con un tamaño de archivo mínimo.

### Lista Blanca por Tipo de archivo

Seleccione el contenido y los archivos que desea que se escaneen y se publiquen, pero agregue en listas blancas los tipos de archivo que desea excluir de la exploración para evitar la redundancia y aumentar la productividad.

### Lista Blanca de Archivos Permitidos

Suba archivos a las listas blancas como excepciones de las políticas de escaneo que ha definido en eDiscovery. Independientemente de si las políticas están basadas en tipo de archivo, contenido predefinido, contenido personalizado, los archivos de las listas blancas estarán excluidas del escaneo.

**Características adicionales**

Si quiere ampliar información

www.ntrsecurity.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

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

### 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 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 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
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.

**Características adicionales**

Si quiere ampliar información

www.ntrsecurity.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.

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

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

# 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.

# 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 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+) | | | | | | ● |

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

Fabricante

COSOSYS

Distribuido

Tel. +34 93 6110817
Plataforma Movil +34 671452874
Mail ntrs@ntrs.es
http://www.ntrs.es