

# Proteja sus datos confidenciales con **DataSecurity Plus**

Proteja sus datos en reposo, en uso y en movimiento ante robos, exposiciones y filtraciones.



# Soluciones que ofrece DataSecurity Plus



## Auditoría de servidor de archivos

Audita e informa sobre todos los accesos y modificaciones de archivos con alertas en tiempo real y respuestas automáticas a amenazas para actividades de archivo de alto riesgo.



## Análisis de archivos

Analiza el uso de espacio en disco, gestiona datos no deseados, identifica datos en riesgo, analiza permisos de archivos y más mediante el análisis de seguridad y almacenamiento de archivos.



## Evaluación de riesgo de datos

Descubre y clasifica archivos que contienen datos personales sensibles, como PII o ePHI, basados en su vulnerabilidad, usando información de contenido y contexto.



## Prevención de fugas de datos

Detecta y evita fugas de datos sensibles a través de dispositivos USB, correos electrónicos, aplicaciones web y más mediante monitoreo de seguridad de endpoints en tiempo real.



## Protección en la nube

Supervisa el tráfico web de tu organización, examina el uso de aplicaciones web no autorizadas y aplica políticas para bloquear contenido web inapropiado o malicioso.

Instale, configure y ejecute **DataSecurity Plus** en cuestión de minutos.

**Descargue ahora**

una prueba gratuita  
de 30 días



# Auditoría de Servidores de Archivos con DataSecurity Plus

Planes anuales desde:  
**\$745 para servidores de archivos Windows**  
**\$595 para servidores CIFS de NetApp**

**Descargar ahora**

Prueba gratuita  
de 30 días

[Más información sobre la Auditoría de Servidores de Archivos](#)

#### Entornos compatibles:

Servidores de archivos Windows, clústeres de conmutación por error, grupos de trabajo y entornos de servidor CIFS de NetApp.



**Audite todas las actividades de archivos**, incluyendo creación, eliminación, cambio de nombre y de permisos, junto con detalles sobre quién modificó cada archivo, cuándo y desde dónde.



**Informe sobre actividades de copiar y pegar archivos** cuando se hayan copiado mediante sesiones directas o remotas en el servidor de archivos.



**Garantice la integridad de los archivos** monitoreando modificaciones no deseadas y transferencias de datos sospechosas con notificaciones en tiempo real y capacidades de respuesta.



**Detecte y detenga ataques de ransomware** rápidamente identificando su origen y aislando máquinas infectadas del resto de la red.



**Rastree actividades de alto riesgo**, como intentos fallidos repetidos de acceder a archivos críticos o aumentos repentinos en cambios de permisos de archivos.



**Acelere el análisis forense** utilizando nuestra extensa colección de informes precisos y listos para auditoría.



# Análisis de Archivos con DataSecurity Plus

Plan anual desde \$95

[Descarga ahora](#)

Prueba gratuita  
de 30 días

[Más información sobre el Análisis de Archivos](#)

## Entornos compatibles:

Servidores de archivos de Windows, clústeres de conmutación por error y entornos de grupos de trabajo.



**Analice el uso del espacio en disco** y active alertas cuando el espacio libre caiga por debajo de valores preconfigurados.



**Identifique acumuladores de datos** revisando las tasas de consumo de almacenamiento de tus empleados a lo largo del tiempo.



**Gestione datos ROT (Redundantes, Obsoletos y Triviales)**, encontrando y eliminando datos duplicados, obsoletos, sin valor comercial y otros datos innecesarios en tus repositorios de almacenamiento.



**Elimine archivos duplicados** y recupere espacio en disco. Compare nombre, última modificación y tamaño para identificar copias idénticas con precisión.



**Localice archivos huérfanos**, como los de usuarios deshabilitados, eliminados o expirados, para reducir el riesgo de robo de datos.



**Analice permisos de seguridad de archivos** y entienda quién tiene qué niveles de acceso sobre archivos críticos para el negocio.



**Identifique datos en riesgo**, como archivos con permisos rotos o heredados de manera incorrecta y archivos corrompidos por variantes conocidas de ransomware.



**Ubique datos sobreexpuestos**, es decir, archivos con acceso abierto para todos y aquellos con niveles de permisos de control total.



**Obtenga información detallada sobre el almacenamiento de archivos**, incluyendo datos de propiedad, tipo y ubicación de los archivos. Realice un seguimiento selectivo de archivos actualmente abiertos, ocultos y más.



# Evaluación de Riesgo de Datos con DataSecurity Plus

Plan anual desde \$395

[Descarga ahora](#)

Prueba gratuita  
de 30 días

[Más información sobre la Evaluación  
de Riesgo de Datos](#)

## Entornos compatibles:

Compartidos basados en SMB y  
entornos de Microsoft SQL  
Server.



**Descubra datos personales sensibles**, como PII, ePHI y PCI, usando expresiones regulares y coincidencia de palabras clave.



**Habilite la protección consciente del contenido** mediante la creación de perfiles de datos críticos según su puntuación de riesgo calculada.



**Use clasificación automática o manual** para etiquetar archivos sensibles con etiquetas predefinidas, como Público, Interno, Restringido y Sensible.



**Identifique y asegure datos críticos** usando reglas predefinidas de descubrimiento y clasificación de datos, y cumple con normativas como el GDPR, la CCPA, HIPAA y PCI DSS.



**Active el escaneo de proximidad** para reducir falsos positivos y aumentar la precisión en la detección de información crítica para el negocio.



**Facilite la clasificación en tiempo real** al analizar y catalogar archivos cuando se crean, modifican y más.



**Acelere su respuesta a incidentes** con opciones para mover, eliminar o poner en cuarentena datos sensibles usando scripts personalizados.



**Use escaneos incrementales** para reducir la carga de CPU al escanear solo archivos nuevos o modificados.



**Audite actividades de archivos sensibles** con detalles sobre quién accedió a qué archivo, qué políticas se violaron, cuándo y desde dónde.



# Prevención de Fugas de Datos con DataSecurity Plus

Plan anual desde \$345

**Descarga ahora**

Prueba gratuita de 30 días

[Más información sobre la Prevención de Fugas de Datos](#)

#### Entornos compatibles:

**Endpoints:** Windows OS cliente

**Aplicaciones:** Outlook

**Navegadores:** Chrome, Firefox, Internet Explorer y más

**Auditoría y bloqueo de almacenamiento extraíble:** Dispositivos USB

**Escritorios virtuales:** Citrix y VMware (con Windows 7 o superior)

**Máquinas distribuidas:** Laptops y escritorios

**Otros:** Unidades internas, impresoras, portapapeles, unidades compartidas, Wi-Fi y adaptadores Bluetooth.



**Evite fugas de datos** detectando y bloqueando el flujo no autorizado de archivos críticos a través de dispositivos USB, correos electrónicos, impresoras, Wi-Fi y más.



**Audite dispositivos de almacenamiento removibles** y obtenga información sobre quién transfirió qué archivo al dispositivo, cuándo y desde dónde.



**Refuerce el control de dispositivos externos** al limitar las funciones de los dispositivos USB, como denegar acceso de lectura, escritura o ejecución.



**Habilite la protección contra copias de archivos** para detectar y deshabilitar actividades de copia de archivos de alto riesgo en compartidos locales y de red.



**Use el control de aplicaciones** para impedir que los empleados ejecuten archivos no autorizados o potencialmente maliciosos mediante listas de bloqueo.



**Fomente prácticas seguras en el uso del correo electrónico** escaneando adjuntos en busca de archivos confidenciales y evitando que los usuarios los compartan.



**Active mensajes instantáneos** en pantalla para advertir a los empleados sobre posibles violaciones a las políticas de prevención de fugas de datos (Outlook).



**Automatice su respuesta a incidentes** ejecutando scripts personalizados que pueden desconectar sesiones de usuarios no autorizados, apagar máquinas comprometidas y más.



**Use monitoreo de seguridad en endpoints** para detectar anomalías repentinas en los patrones de transferencia de datos y acceso a archivos.



# Protección en la Nube con DataSecurity Plus

**\*Complemento gratuito del módulo de Prevención de Fugas de Datos**  
[Más información sobre Protección en la Nube](#)

## Entornos compatibles:

**Aplicaciones en la nube:** Box, Dropbox, Microsoft 365 (OneDrive, Sharepoint y Exchange Online) y más

**Protocolos de red:** HTTP y HTTPS

**Navegadores:** Chrome, Firefox, Internet Explorer y más.



**Audite el tráfico web** en toda su organización junto con detalles sobre qué sitio web fue accedido, cuándo y desde dónde.



**Aproveche la capacidad de inspección profunda de paquetes** para examinar solicitudes web que contengan parámetros cifrados.



**Use el descubrimiento de aplicaciones en la nube** para obtener información detallada basada en aplicaciones, dominios y usuarios sobre los accesos realizados en tu red.



**Filtre URLs** al aprobar o bloquear aplicaciones directamente desde la interfaz de informes o utilizando parámetros personalizados, reduciendo así el riesgo general.



**Audite las cargas de archivos** realizadas en varias aplicaciones de almacenamiento, como Microsoft 365, Google Workspace, Zoho Suite y Dropbox.



**Implemente políticas de prevención de fugas de datos en la nube (Cloud DLP)** para bloquear de manera granular cargas de archivos riesgosas basadas en dominios, URLs, suites de aplicaciones y otros parámetros.



**Examine servicios en la nube no autorizados (shadow IT)** según la categoría de aplicaciones accedidas y la puntuación de riesgo, y correlacione esta información con los principales usuarios que las utilizan.



**Bloquee dominios inapropiados**, como redes sociales, comercio electrónico y otros sitios de baja reputación o que disminuyen la productividad y se consideren inseguros para su organización.



**Evalúe las puntuaciones de reputación** de dominios en función de datos en tiempo real obtenidos de análisis de amenazas integrados y asegúrate de que solo las aplicaciones críticas para el negocio estén aprobadas para su uso.

# ManageEngine DataSecurity Plus

Una plataforma unificada de visibilidad y seguridad de datos  
Una solución de doble enfoque para combatir amenazas internas, prevenir la pérdida de datos y cumplir con los requisitos de cumplimiento.



**Descarga ahora**

Prueba gratuita  
de 30 días

## Información de contacto



### Sitio web

[www.manageengine.com/latam/data-security/](http://www.manageengine.com/latam/data-security/)



### Demo personalizada

[www.manageengine.com/latam/data-security/solicitud-demo-gratis.html](http://www.manageengine.com/latam/data-security/solicitud-demo-gratis.html)



### Detalles de precios

[www.manageengine.com/latam/data-security/obtener-cotizacion.html](http://www.manageengine.com/latam/data-security/obtener-cotizacion.html)



### Demo en vivo

[demo.datasecurityplus.com](http://demo.datasecurityplus.com)



### Soporte técnico

[support@datasecurityplus.com](mailto:support@datasecurityplus.com)



### Consultas de ventas

[latam-sales@manageengine.com](mailto:latam-sales@manageengine.com)



### Llame gratis

+1.408.916.9891

## Recursos adicionales

Presentación

Arquitectura

Centro de ayuda

Guía de inicio rápido

Centro de recursos