ManageEngine
DataSecurity Plus

Perfeccione su estrategia de DLP

Guía para elaborar un plan efectivo de prevención de la pérdida de datos

www.datasecurityplus.com

Índice

1. Introducción

Un estudio de 2018 realizado por descubrió que, para una organización típica, los datos no estructurados crecen un 23% anualmente, lo que significa que cada 40 meses duplicarán su tamaño. En el mismo estudio, alrededor de una cuarta parte de las empresas estudiadas citaron tasas de crecimiento de datos superiores al 40 por ciento, lo que significa que sus datos totales no estructurados se duplicaron cada dos años.

Teniendo en cuenta este crecimiento exponencial de los datos, las empresas necesitan una forma sencilla de clasificar, evaluar y proteger continuamente sus almacenes de datos que no dejan de crecer. Esta necesidad se ve agravada por el hecho de que la mayoría de estos datos son probablemente confidenciales, información personal identificable o alguna otra forma de datos sensibles que deben ser protegidos a toda costa.

Sin embargo, ¿son las empresas capaces de garantizar la protección de datos a gran escala?

En esta nueva era de software de seguridad informática integrada, la necesidad del momento es examinar detenidamente todas las soluciones disponibles para identificar la mejor manera de proteger los datos. Al fin y al cabo, un enfoque único no sirve para todos, y aferrarse a enfoques anticuados de protección de datos nunca es aconsejable.

A medida que los datos proliferan, el software tradicional de protección de datos ha dado un paso atrás para permitir que las soluciones integrales de prevención de pérdida de datos ocupen el lugar que les corresponde: Encabezando el objetivo de todo CISO de garantizar la completa visibilidad y seguridad de los datos en reposo, en uso y en movimiento.

1.1 El enfoque de "aceptación del riesgo" para la seguridad de los datos

El **68%** de los líderes empresariales considera que sus riesgos de seguridad informática están aumentando. - Accenture

El tiempo medio para identificar una brecha en **2019 fue de 206 días** - IBM

Hoy en día, la seguridad de TI ya no consiste únicamente en prevenir los ataques, ni en bloquear totalmente las amenazas que puedan surgir. La mejor manera de describir la mentalidad de los CISO hoy en día es la aceptación del riesgo.

Después de todo, con la evolución de las tendencias de los robos cibernéticos, evitar las infracciones es prácticamente imposible. Una vez que las empresas aceptan que ya están siendo atacadas, o que podrían ser atacadas por los ciberdelincuentes en cualquier momento, pueden centrarse en lo que deben hacer a continuación para salvaguardar sus datos críticos.

Anticipando un ataque a la vuelta de cada esquina y preparándose para diferentes tipos de escenarios, las empresas no se verán sorprendidas cuando un ataque atraviese sus defensas. En cambio, estarán preparados para afrontar y mitigar los daños que una violación pueda causar en sus almacenes de datos.

1.2 ¿Qué es la prevención de la pérdida de datos?

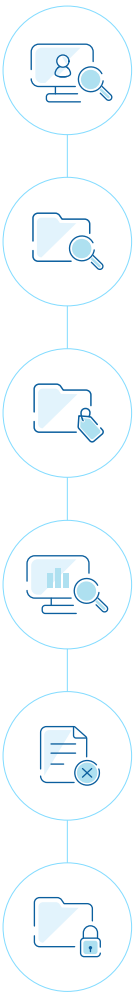
La prevención de la pérdida de datos (DLP) es el proceso de identificar, clasificar, catalogar, monitorear el acceso y controlar el uso de los datos críticos para la empresa, con el objetivo de garantizar que no salgan de la red sin la debida autorización. El aumento de sofisticados ataques cibernéticos y amenazas a la seguridad de los datos, junto con el establecimiento de estrictas normas y reglamentos de seguridad de los datos, ha aumentado la importancia de adoptar prácticas y herramientas de DLP.

Los métodos tradicionales de protección de datos tienen un enfoque estrecho con visibilidad de datos y software de seguridad en silos que impide la correlación entre el contexto de los datos y los detalles de acceso. Esta correlación, que es un componente necesario de las estrategias efectivas de prevención de la pérdida de datos, está integrada en el software de DLP y se le da la debida importancia en las estrategias de prevención de la pérdida de datos.

1.3 Funciones del software de prevención de pérdida de datos

La implementación de un software de DLP puede proporcionar información detallada sobre el uso que los interesados hacen de los datos de la empresa. Para proteger la información sensible, las organizaciones deben saber primero que existe, descubrir dónde está y averiguar quién la utiliza y con qué fines. Además, el software debe ser capaz de controlar el uso de los datos sensibles y protegerlos tanto de los atacantes externos como de los internos.

Una solución integral de DLP puede:



Descubra datos personales sensibles
como la información personal identificable y la información de salud protegida electrónicamente (PII y ePHI) almacenada en los repositorios de almacenamiento de la empresa.

Evalúe los riesgos
asociados a los datos mediante el análisis de los permisos, la ubicación de almacenamiento, el tipo de datos, etc.

Clasifique y catalogue archivos
que contienen PII y ePHI para permitir a los administradores controlar el movimiento de datos a través de servidores de archivos y endpoints.

Monitoree la actividad de los usuarios
en archivos que contienen información sensible y clasificada, y alerte a los administradores de actividades sospechosas.

Detecte el movimiento de archivos restringidos
a dispositivos de almacenamiento externo y aplicaciones web.

Evite las pérdidas de datos
utilizando políticas de DLP adaptadas para detectar y bloquear los intentos de transferencia de archivos dañinos.

Aparte de esto, las mejores herramientas de DLP también pueden proporcionar informes detallados para demostrar el cumplimiento de los mandatos normativos actuales y en evolución, como el GDPR, PCI DSS, HIPAA, ISO 27001, SOX, CCPA, y más.

2. Elija la herramienta de DLP adecuada

En promedio, sólo el cinco por ciento de las carpetas de las empresas están debidamente protegidas. - Varonis

La ciberdelincuencia costará al mundo **6 billones** de dólares anuales en 2021. - Cybersecurity Ventures

Algunos softwares de DLP son notoriamente complejos para los casos de uso básicos a los que se enfrentan las pequeñas y medianas empresas (PYMES). Los analistas de lo reiteraron, y continuaron destacando la importancia de tener en cuenta ciertos factores clave a la hora de elegir el software de DLP.

Los responsables de la toma de decisiones deben tener en cuenta el tamaño de la empresa, el volumen de datos almacenados, el software existente, los requisitos normativos aplicables, los objetivos empresariales y los recursos humanos y financieros disponibles para operar y mantener la solución de DLP. Con una cuidadosa consideración, las empresas pueden evitar la compra e instalación de software que finalmente termina siendo ineficaz o una mala opción.

De todos los factores que hay que tener en cuenta, estos son los tres principales parámetros que hay que considerar a la hora de elegir una herramienta de DLP.

2.1 Identifique los datos que necesitan más protección

Comprender el tipo, el contenido y el contexto de los datos almacenados y obtener información sobre el nivel de protección necesario es el primer paso de la evaluación. Para proteger los datos críticos, los responsables de seguridad deben localizarlos, monitorear quién accede a ellos y controlar cómo y dónde se utilizan.

Con una solución completa de DLP, pueden descubrir y clasificar automáticamente los datos sensibles en todo el almacenamiento de la empresa. También puede proporcionar una profunda visibilidad del uso y movimiento de datos, con información sobre las tendencias de acceso de los empleados. A su vez, esto ayudará a comprender mejor el nivel de protección necesario, dónde deben aplicarse las salvaguardias, así como a identificar cualquier deficiencia en los procesos de seguridad de datos existentes.

2.2 Flexibilidad de las políticas de DLP proporcionadas

La mayoría de las soluciones de DLP tienen una multitud de políticas de prevención de pérdida de datos integradas. Sin embargo, los responsables de la toma de decisiones deben analizar si son realmente útiles y lo suficientemente capaces de proteger las puertas de entrada más vulnerables de una empresa al robo de datos: los endpoints.

El software de DLP debe ser capaz de monitorear toda la actividad de los archivos en los endpoints y los puertos externos, hacer seguimiento a las acciones de copiar y pegar, detectar las transferencias de datos injustificadas y detener instantáneamente los intentos de robo de datos sensibles a través de USB e impresoras. Hay que dar confianza a los empleados para que manejen los datos sensibles de forma segura, con una combinación de avisos educativos en pantalla sobre las acciones que violan las políticas de uso de datos y una lista de acciones de respuesta activa disponibles.

Además, estas políticas deben permitir a los CISO adaptarlas en función de las necesidades y deseos de la empresa, y el software debe permitir la creación de políticas adicionales para casos de uso muy específicos.

2.3 Recursos necesarios para la implementación del software

Las herramientas de DLP son mucho más que un costoso check verde en una lista de verificación de cumplimiento. Los precios de muchos proveedores de DLP de gran prestigio suelen estar fuera del alcance de las PYMES, porque también tienen que tener en cuenta los costes asociados al tiempo y la mano de obra necesarios para elegir, implementar y mantener el software.

A la hora de elegir el software, los responsables de la toma de decisiones deben analizar la facilidad de implementación, funcionamiento y mantenimiento; qué nivel de formación proporciona el proveedor; y si la herramienta es fácil de ajustar a las necesidades de la empresa.

Al tener en cuenta estos tres criterios clave en el proceso de toma de decisiones, los CISO pueden identificar el mejor software de prevención de pérdida de datos más rápidamente y analizar su efectividad para satisfacer sus necesidades.

3. Desarrolle una estrategia de DLP

La creación de una estrategia efectiva de prevención de la pérdida de datos comienza con las mejores prácticas que se enumeran a continuación.

Implemente su solución de DLP por fases

Antes de la implementación, haga una lista y priorice todos los archivos que deben ser protegidos. Cree un calendario para garantizar que la implementación se realice por fases. Tratar de implementar medidas de DLP en los endpoints, la nube y los servidores a la vez conduce a una enorme cantidad de falsos positivos, lo que puede conducir rápidamente a la fatiga de las alertas.

Empiece con el descubrimiento y la clasificación de datos

Saber qué datos hay que proteger y dónde se encuentran es el primer paso de la DLP. Las funciones de descubrimiento y clasificación de datos proporcionan visibilidad del almacenamiento de datos sensibles y de las medidas de protección asociadas a ellos. Una vez establecidas las categorías, las soluciones de DLP pueden operar sobre los contenidos clasificados.

Cree, ajuste y actualice sus políticas de riesgo

Realice pruebas durante su implementación inicial utilizando un pequeño subconjunto de políticas para construir una línea de referencia, y luego amplíe a partir de ahí. Ajuste regularmente los perfiles de riesgo, las políticas y las reglas para reducir los falsos positivos, mejorar la efectividad y adaptarse a las necesidades cambiantes de la empresa.

Registre todos los incidentes identificados

Mantenga una documentación clara y concisa de todas las políticas infringidas y los incidentes detectados. Utilice un dashboard informativo para analizar los principales incidentes de pérdida de datos, las puntuaciones de riesgo y los incidentes de seguridad, y emplee la corrección activa o pasiva adecuada.

Ejecute pruebas con un agente de endpoint de DLP

Antes de implementar la solución en toda la organización, realice pruebas exhaustivas con su agente de DLP para endpoints para garantizar que esté correctamente configurado, funcione de forma satisfactoria, ejecute las políticas según sus requisitos y sea compatible con las aplicaciones de las estaciones de trabajo existentes.

Integre con gestores de seguridad de acceso a la nube

Identificar y proteger la información sensible en las aplicaciones en la nube es también una parte esencial de una solución efectiva de DLP. La integración de los gestores de seguridad de acceso a la nube (CASB) con su solución de DLP extiende la seguridad de los datos también a las plataformas en la nube.

4. Enriquezca su enfoque de DLP

Con la información disponible sobre las desventajas de utilizar varios software y con el DLP en mente como objetivo final, estos son los puntos clave a tener en cuenta.

4.1 Las ventajas de implementar un software de DLP integral

Las principales lecciones aprendidas por los CISO en su viaje hacia la identificación de las mejores herramientas de prevención de pérdida de datos son:

- La evaluación del riesgo de los datos y la DLP no son mutuamente excluyentes.
- La auditoría de archivos y la DLP no son mutuamente excluyentes.

La combinación de las funciones de visibilidad de los datos y de las herramientas de seguridad de los datos dentro de un software de DLP da a las organizaciones la ventaja de identificar las amenazas, y reaccionar ante ellas rápidamente con mayor precisión.

4.2 Obtenga la ventaja de DataSecurity Plus

Como siempre, ManageEngine pretende satisfacer todas estas necesidades con un software DLP integral, DataSecurity Plus. Proporciona auditoría de archivos, monitoreo de la integridad de los archivos, detección y respuesta a ransomware, respuesta a incidentes de seguridad, descubrimiento de datos, clasificación de datos y funciones de DLP, y es realmente una solución integral para garantizar que los datos de su organización permanezcan seguros dentro de su red.

5. Prevención de la pérdida de datos con DataSecurity Plus

Con las funciones combinadas de análisis de archivos y evaluación de riesgos de datos, usted puede identificar los datos sensibles, evaluar toda la información asociada y analizar si está en riesgo debido a la ubicación de almacenamiento, la titularidad o los permisos de seguridad asignados. Luego, implemente un proceso de clasificación de datos para etiquetar los datos con información contextual, como el tipo de datos que son, su sensibilidad, su nivel de confidencialidad y su valor para la organización.

Con esta información contextual a la mano, puede implementar controles de seguridad apropiados para proteger los datos de cambios accidentales, eliminaciones y robos. Esto garantizará el cumplimiento de varios mandatos de privacidad y seguridad, y también demostrará que todos sus datos están seguros dentro de su red, cumpliendo así los objetivos del proceso de DLP.

La oferta integral de prevención de pérdida de datos de ManageEngine DataSecurity Plus, le permite:

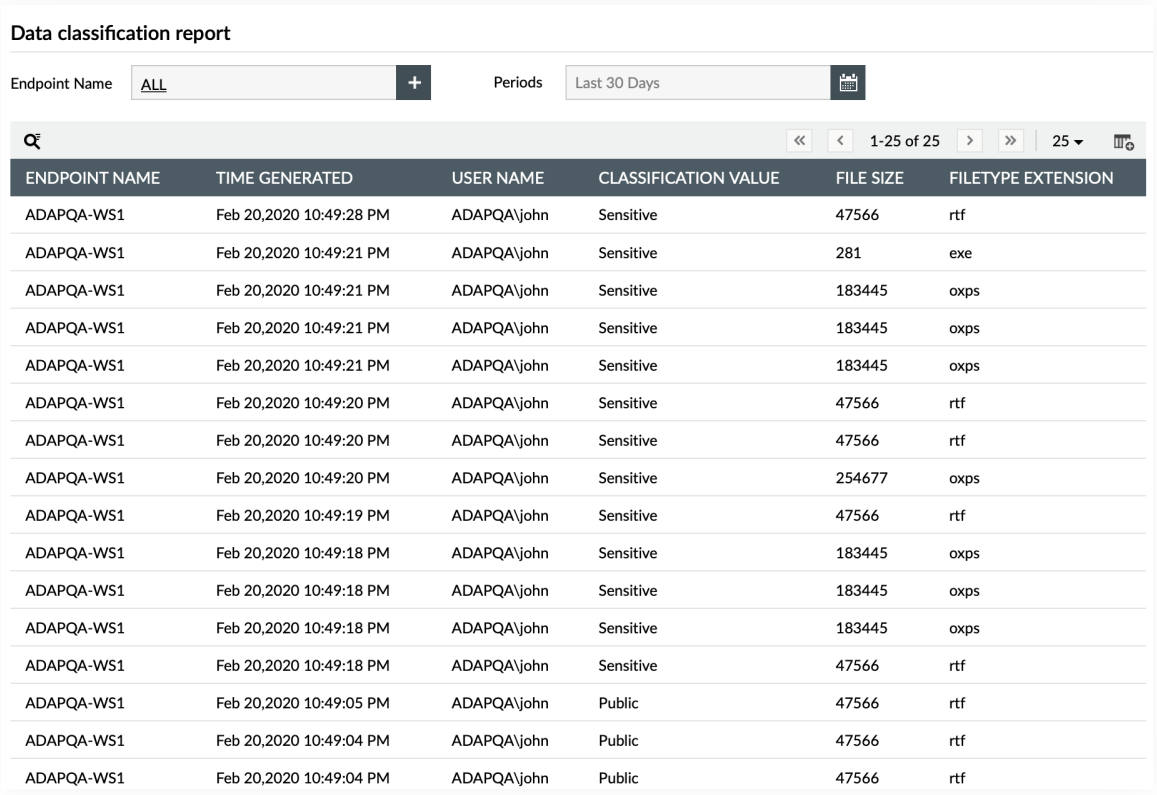
Descubrir datos sensibles

- Examine el servidor de archivos de Windows y los entornos de failover cluster en busca de PII, PCI y ePHI utilizando la.
- Reciba informes sobre el volumen, el tipo y las tendencias observadas en el almacenamiento de datos sensibles.
- Busque números de pasaporte, direcciones de correo electrónico, números de tarjetas de crédito y muchos otros tipos de datos personales con políticas de descubrimiento de datos preconfiguradas y personalizables.
- Analice varios tipos de archivos, como los de correo electrónico, texto, comprimidos, etc.
- Cree y mantenga un inventario de los datos más sensibles de su organización programando análisis de detección de datos a intervalos regulares.

Clasifique los archivos sensibles

- Analice el riesgo asociado a los archivos viendo los detalles de los permisos efectivos, la titularidad, la ubicación de los archivos y mucho más.
- Clasifique manualmente los archivos que contienen información personal identificable (PII) e información de salud protegida electrónicamente (ePHI) con.
- Automatice la clasificación de los archivos con puntuaciones de alto riesgo para comprender mejor qué archivos necesitan medidas de seguridad de datos elevadas.

- Catalogue los archivos sensibles en las estaciones de trabajo y evite el robo de datos a ravés de los correos electrónicos de Outlook, las aplicaciones web y los medios de almacenamiento externos.



Data classification report

Endpoint Name: ALL

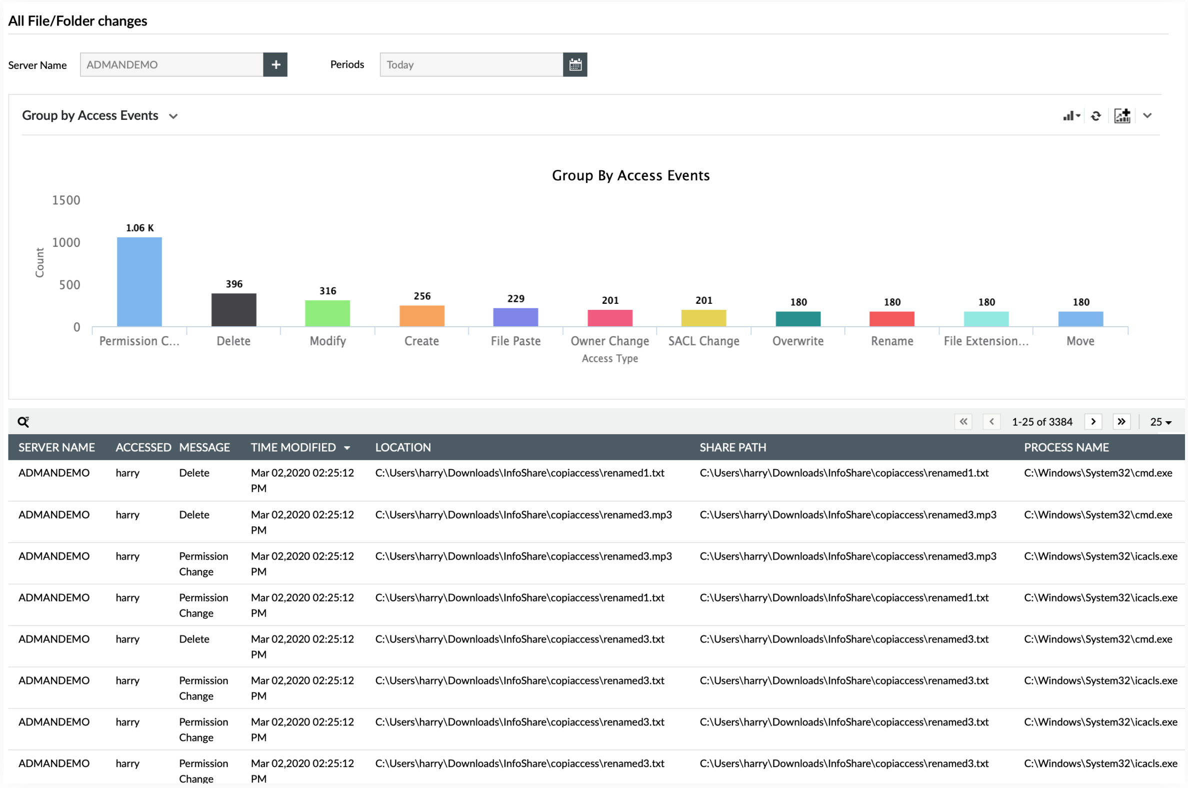
Periods: Last 30 Days

1-25 of 25 | 25

ENDPOINT NAME	TIME GENERATED	USER NAME	CLASSIFICATION VALUE	FILE SIZE	FILETYPE EXTENSION
ADAPQA-WS1	Feb 20,2020 10:49:28 PM	ADAPQA\john	Sensitive	47566	rtf
ADAPQA-WS1	Feb 20,2020 10:49:21 PM	ADAPQA\john	Sensitive	281	exe
ADAPQA-WS1	Feb 20,2020 10:49:21 PM	ADAPQA\john	Sensitive	183445	oxps
ADAPQA-WS1	Feb 20,2020 10:49:21 PM	ADAPQA\john	Sensitive	183445	oxps
ADAPQA-WS1	Feb 20,2020 10:49:21 PM	ADAPQA\john	Sensitive	183445	oxps
ADAPQA-WS1	Feb 20,2020 10:49:20 PM	ADAPQA\john	Sensitive	47566	rtf
ADAPQA-WS1	Feb 20,2020 10:49:20 PM	ADAPQA\john	Sensitive	47566	rtf
ADAPQA-WS1	Feb 20,2020 10:49:20 PM	ADAPQA\john	Sensitive	254677	oxps
ADAPQA-WS1	Feb 20,2020 10:49:19 PM	ADAPQA\john	Sensitive	47566	rtf
ADAPQA-WS1	Feb 20,2020 10:49:18 PM	ADAPQA\john	Sensitive	183445	oxps
ADAPQA-WS1	Feb 20,2020 10:49:18 PM	ADAPQA\john	Sensitive	183445	oxps
ADAPQA-WS1	Feb 20,2020 10:49:18 PM	ADAPQA\john	Sensitive	183445	oxps
ADAPQA-WS1	Feb 20,2020 10:49:18 PM	ADAPQA\john	Sensitive	47566	rtf
ADAPQA-WS1	Feb 20,2020 10:49:05 PM	ADAPQA\john	Public	47566	rtf
ADAPQA-WS1	Feb 20,2020 10:49:04 PM	ADAPQA\john	Public	47566	rtf
ADAPQA-WS1	Feb 20,2020 10:49:04 PM	ADAPQA\john	Public	47566	rtf

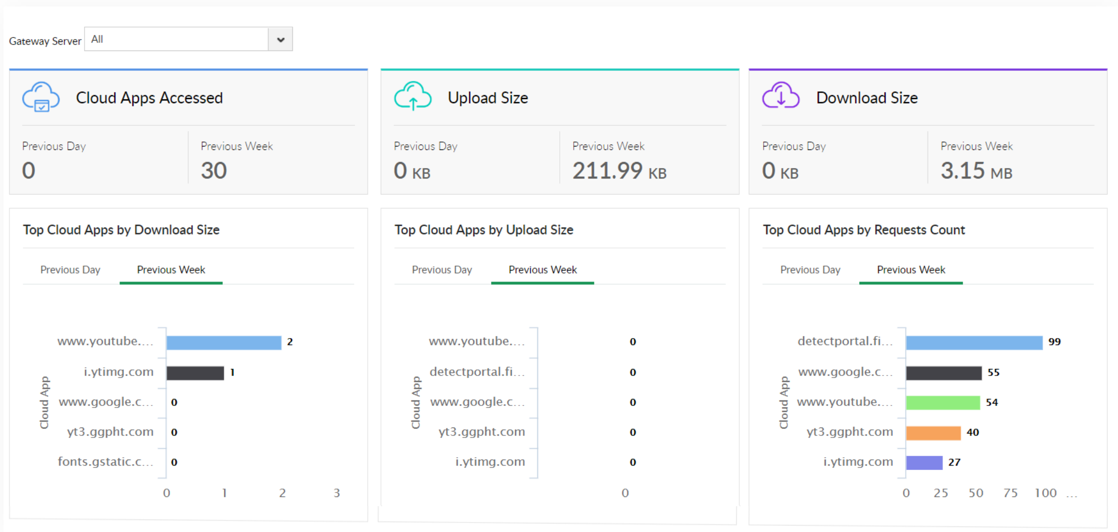
Monitoree la actividad de los usuarios

- e informe sobre los usuarios que acceden a los archivos para saber quién, qué, cuándo y dónde está detrás de toda la actividad crítica de los archivos.
- Examine detalladamente en los eventos más importantes, como los cambios repentinos de permisos, los eventos de copiar y pegar, las eliminaciones de archivos y los eventos de cambio de nombre.
- Verifique la integridad de los archivos críticos con informes en tiempo real sobre la actividad de los archivos sospechosos.
- Active alertas instantáneas siempre que haya un pico repentino de eventos de acceso o modificación de archivos o carpetas, o múltiples intentos de acceso fallidos.
- mediante perfiles de alerta basados en umbrales y una biblioteca actualizada de tipos de archivos de ransomware conocidos. Ejecute scripts personalizados para apagar los equipos infectados y detener el progreso del malware, mitigando así los daños.



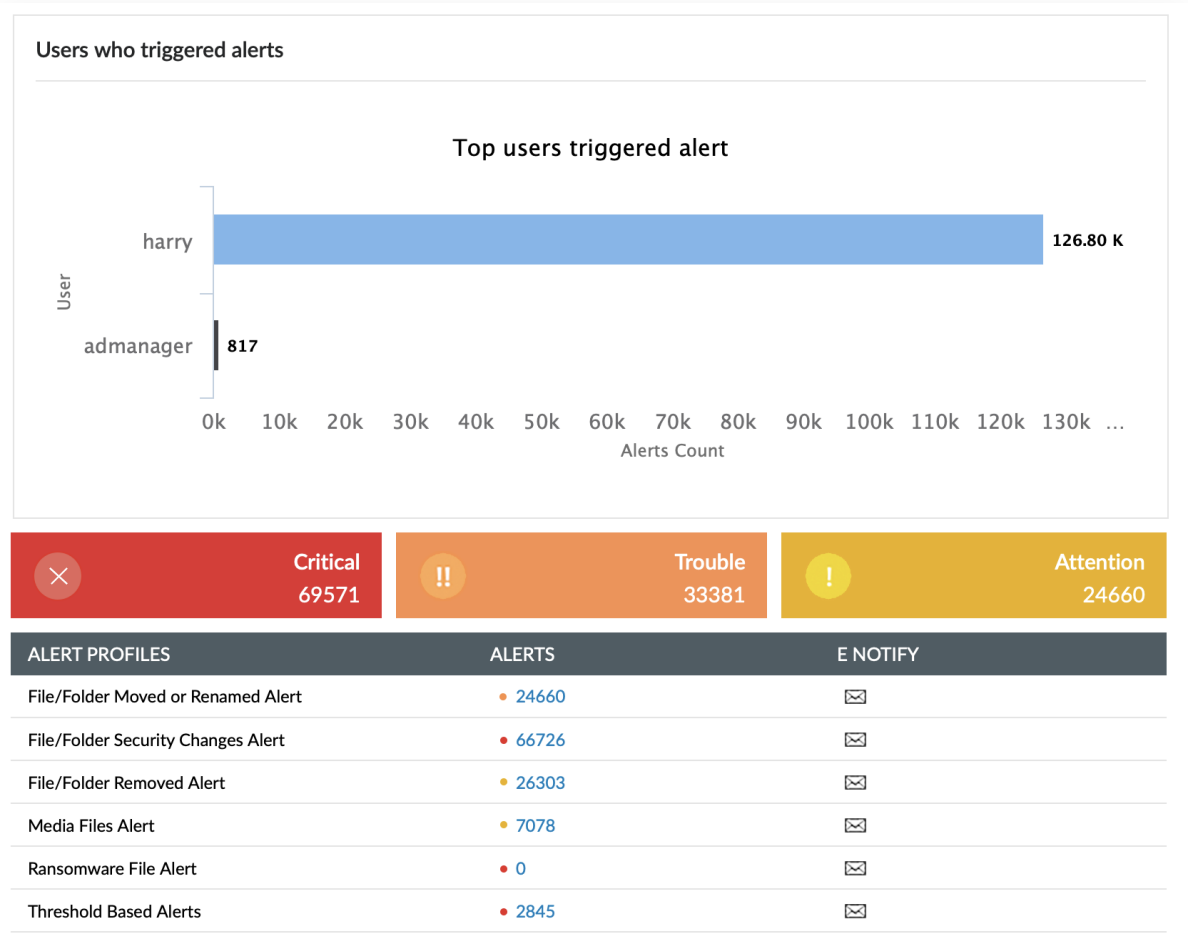
Habilite la protección en la nube

- Audite el tráfico web de su organización para supervisar el uso de aplicaciones de alto riesgo.
- Implemente un control centralizado sobre el uso de las aplicaciones sancionadas y no sancionadas.
- Controle las actividades de los usuarios en millones de sitios web dañinos y bloquee su visita a secciones dañinas u oscuras de la web.
- Supervise y analice qué recursos sensibles de su empresa se suben a la nube.



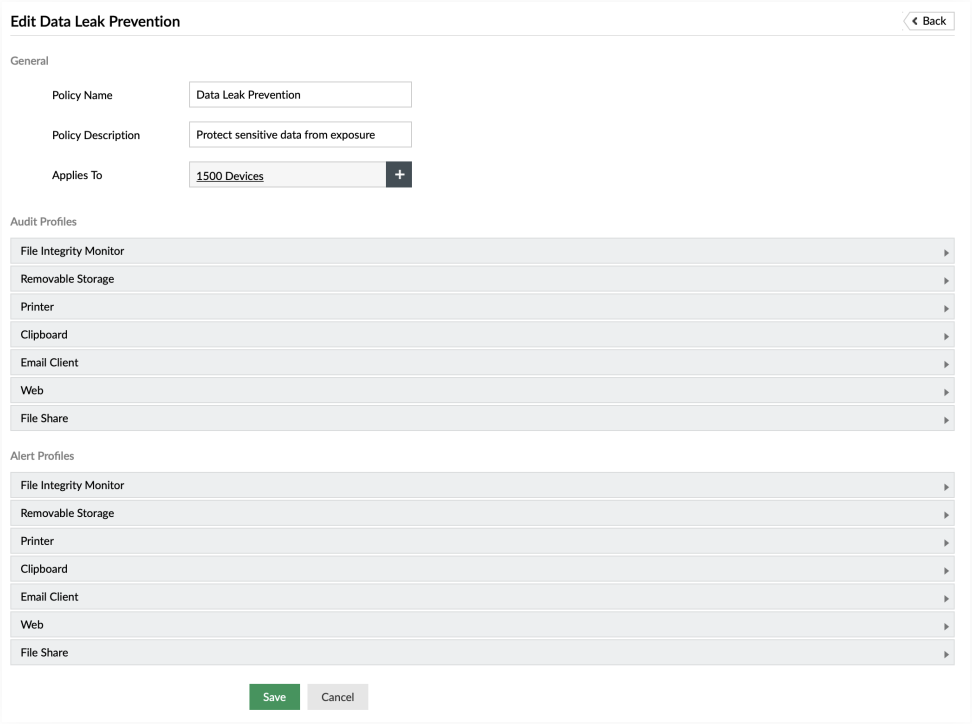
Detecte las amenazas a la seguridad

- Reduzca la superficie de los ataques detectando las vulnerabilidades de los permisos, como las herencias rotas, los archivos que permiten un acceso no restringido y mucho más con el análisis de archivos.
- Minimice el riesgo de incumplimiento correlacionando el análisis de almacenamiento y la detección de datos para descubrir los datos sensibles que se han almacenado más allá de su período de limitación.
- Reciba alertas en tiempo real para eventos de acceso a archivos sospechosos y actividad inusual de los usuarios, como los archivos a los que se accede después de un período prolongado de inactividad, o durante horas no laborables.
- Notifique a los administradores los cambios de archivos críticos y automatice las respuestas a las amenazas de seguridad, como las intrusiones de ransomware y las acciones de copia de archivos.
- Monitoree a los usuarios sospechosos, los archivos importantes y las ubicaciones no seguras para detectar la actividad de los archivos no autorizados.



Evite las pérdidas de datos

- Configure y empiece a proteger sus datos fácilmente con las políticas de alerta y respuesta integradas en la.
- Monitoree la actividad de los archivos en los medios de almacenamiento extraíbles e interrumpa las transferencias de datos sensibles a las unidades USB.
- Monitoree la actividad de los archivos adjuntos de Outlook y bloquee a los usuarios para que no adjunten datos críticos del negocio a los correos electrónicos.
- Utilice mensajes emergentes en pantalla para advertir a los empleados sobre las violaciones de la política de uso de datos.
- Maneje las infracciones críticas de las políticas mediante scripts personalizados y una serie de opciones de corrección disponibles para eliminar o poner en cuarentena los archivos y bloquear las transferencias de archivos.



Cumpla con la normativa

- Aborde los requisitos de PCI DSS, HIPAA, GDPR, SOX, CCPA y otras normativas con en tiempo real.
- Configure suscripciones a informes para recibir periódicamente informes listos para la auditoría sobre la actividad de los archivos, el almacenamiento de datos sensibles, los incidentes de seguridad detectados, etc.
- Identifique la causa raíz de los incidentes de seguridad utilizando datos forenses, y genere pistas de auditoría claras y concisas para garantizar la responsabilidad de toda la actividad de los archivos.

6. Conclusión

La prevención de la pérdida de datos es un proceso continuo que se enriquece cuando se ponen en marcha las herramientas, los procedimientos y la gestión adecuados. Reiterando los hechos discutidos anteriormente, un enfoque único no sirve para todos, y se debe tener mucho cuidado, precaución y tiempo al elegir el software de DLP. Al hacerlo, los CISO pueden tomar una decisión informada, y también aprovechar al máximo las funciones del software elegido para proteger efectivamente los datos de su empresa contra los ataques internos y externos.

Próximos pasos

- Configure y evalúe las funciones de DataSecurity Plus con una prueba gratuita y totalmente funcional de 30 días.
- Vea una instancia en línea de DataSecurity Plus (disponible sin necesidad de registrarse).
- Programe una demostración para que un experto en el producto le enseñe el software y responda a sus preguntas.
- Vea los detalles de los precios y solicite un presupuesto personalizado.

DataSecurity Plus

ManageEngine DataSecurity Plus es una solución de visibilidad y seguridad de datos. Supervisa y alerta sobre las modificaciones y el movimiento de archivos críticos en servidores de archivos, failover clusters, estaciones de trabajo y USB. Los usuarios pueden localizar y analizar los archivos que contengan PII/ePHI almacenados en servidores de archivos de Windows, failover clusters y entornos de OneDrive mediante reglas de detección de datos integradas. Su función de prevención de pérdida de datos (DLP) ayuda a detectar y responder al robo de datos sensibles a través de USB, correo electrónico, impresoras y más. También proporciona informes de auditoría detallados que ayudan a las organizaciones a agilizar el cumplimiento de múltiples normativas de TI.

Para explorar estas funciones y ver DataSecurity Plus en acción, .
Para saber más sobre DataSecurity Plus, visite www.datasecurityplus.com.

Download free trial $ Get a quote

Explore **las soluciones de DataSecurity Plus**

Auditoría del servidor de archivos

Audite e informe sobre los accesos y modificaciones de los archivos, con alertas en tiempo real y respuestas automatizadas para las actividades críticas de los archivos.

Learn more

Análisis de archivos

Analice la seguridad y el almacenamiento de los archivos, gestione los archivos basura, optimice el uso del espacio en disco e identifique las vulnerabilidades de los permisos.

Learn more

Evaluación del riesgo de los datos

Descubra y clasifique los archivos que contienen datos confidenciales, como PII, PCI y ePHI, combinando la inspección de contenidos y el análisis contextual.

Learn more

Prevención de la pérdida de datos

Detecte e interrumpa las pérdidas de datos a través de los USB, el correo electrónico, las aplicaciones web y las impresoras; monitoree la actividad de los archivos en los endpoints; y mucho más.

Learn more

Protección en la nube

Supervise el tráfico web de la empresa y aplique políticas para bloquear el uso de aplicaciones web inapropiadas, de riesgo o maliciosas.

Learn more