# Proofpoint Endpoint DLP y Proofpoint ITM

## Protección centrada en las personas frente a pérdida de datos y amenazas internas

### Productos

- Proofpoint Endpoint Data Loss Prevention
- Proofpoint Insider Threat Management

### Ventajas principales

- Reducción del riesgo de pérdida de datos confidenciales y de amenazas internas
- Simplificación de la respuesta a incidentes de origen interno e incumplimiento de las políticas
- Aceleración del período de rentabilización de los programas de prevención de la pérdida de datos y amenazas internas

En la actualidad, las plantillas distribuidas trabajan en todas partes y desde cualquier lugar. Tanto empleados como personal externo y contratistas tienen acceso a más datos que nunca, ya estén en el portátil, en el correo electrónico o en la nube. El riesgo de pérdida de datos es, por tanto, muy alto. Sin embargo, los datos no se pierden solos. Son los usuarios quienes los pierden.

Los usuarios que filtran datos pueden clasificarse en tres tipos: negligentes, malintencionados o comprometidos por un ataque. Para implantar políticas adecuadas, es preciso conocer el contexto del comportamiento de los usuarios. Esto también le ayudará a determinar mejor la respuesta más conveniente cuando se produzca un incidente de origen interno.

Proofpoint Endpoint Data Loss Prevention (DLP) y Proofpoint Insider Threat Management (ITM) ofrecen un enfoque centrado en las personas para gestionar las amenazas internas y prevenir la pérdida de datos en los endpoints.

Ayudan a los equipos de TI y ciberseguridad a:

- Identificar comportamientos de riesgo asociados a los usuarios e interacciones con datos confidenciales.
- Detectar e impedir los incidentes de seguridad provocados por usuarios internos y las pérdidas de datos desde los endpoints.
- Responder más rápidamente a los incidentes provocados por los usuarios.

Proofpoint Endpoint DLP protege frente a la pérdida de datos causada por los usuarios habituales. Proofpoint ITM incluye la misma protección, pero además, al ofrecer una visibilidad profunda de la actividad de los usuarios, defiende frente a las amenazas de los usuarios de riesgo. Ambos productos forman parte de la plataforma Proofpoint Information Protection and Cloud Security, una completa plataforma contextualizada y nativa de la nube que proporciona visibilidad e información en todos los canales. Permite configurar políticas, filtrar alertas, cazar amenazas y responder a incidentes desde una sola consola centralizada. Ayuda a detener la pérdida de datos e investigar las infracciones internas con rapidez y eficacia. Y cuanto más rápido se resuelva un incidente, menor será el impacto en la empresa, así como en su reputación y su cuenta de resultados.

# Supervisión de usuarios habituales y de riesgo

## Flexibilidad con un único agente para endpoints

En el entorno competitivo actual es fundamental poder gestionar las amenazas internas y las pérdidas de datos basadas en los endpoints. Sin embargo, la mayoría de las organizaciones no necesitan (y posiblemente no deberían) recopilar telemetría de endpoints sobre todas las actividades de todos los usuarios en todo momento. Nosotros, en cambio, recomendamos un enfoque más adaptable y basado en riesgos. Eso implica obtener información sobre algunas actividades de todos los usuarios y sobre todas las actividades de los que presentan mayor riesgo.

Para satisfacer esta necesidad, Proofpoint ha desarrollado un agente de endpoints ligero que protege frente a la pérdida de datos y proporciona una visibilidad profunda de la actividad de los usuarios. Con un sencillo cambio en la configuración de las políticas, puede ajustar la cantidad y el tipo de datos que se obtienen para cada usuario o grupo de usuarios. Este enfoque adaptable le ayuda a investigar y a responder a las alertas de forma más eficaz sin necesidad de recopilar grandes volúmenes de datos.

Los usuarios habituales suelen ser los que utilizan la empresa a diario. Dado su bajo nivel de riesgo, puede supervisarlos con Proofpoint Endpoint DLP para informarse de la actividad de los datos y el contexto de los usuarios. Por ejemplo, puede configurar reglas para que se genere una alerta cuando un usuario intente filtrar datos sensibles, ya sea copiándolos en una unidad USB o subiéndolos a una carpeta de sincronización en la nube.

Los usuarios de riesgo necesitan más atención. Puede tratarse de empleados que vayan a incorporarse a la empresa o a abandonarla, contratistas externos, titulares de cuentas con privilegios o usuarios que suelen ser blanco de ataques, como los altos directivos. Para entender sus motivaciones e intenciones, debe reunir información más detallada. Su supervisión debe basarse en su comportamiento o sus circunstancias. Proofpoint ITM recopila datos en profundidad sobre la actividad de estos usuarios, datos que pueden proporcionar información contextual sobre sus intenciones antes, durante y después de un evento.

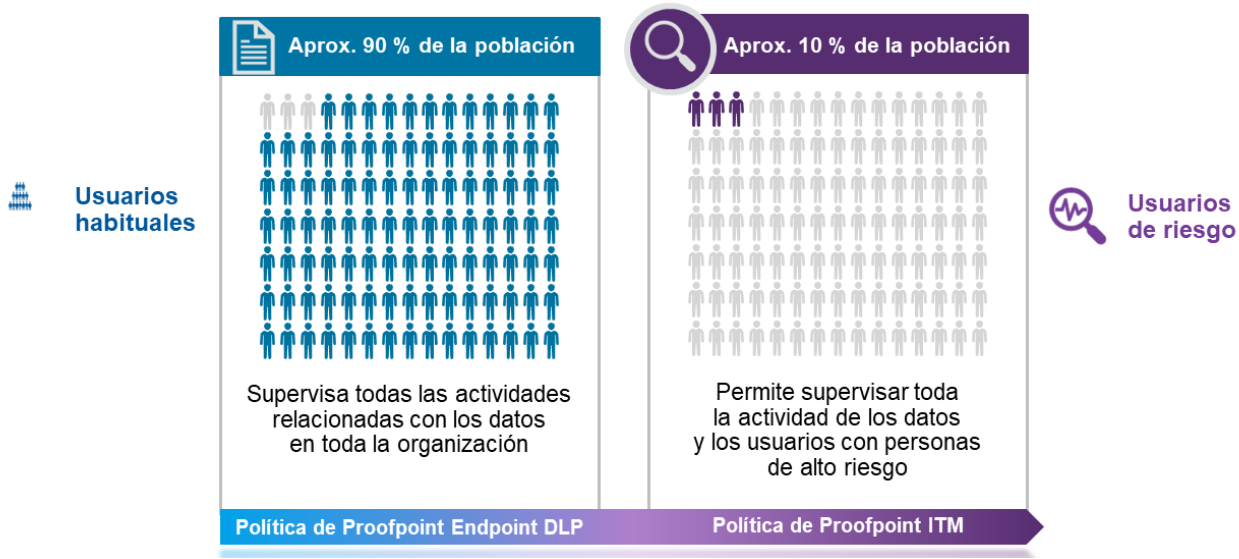


Figura 1: Un único agente ligero para endpoints proporciona flexibilidad para supervisar a los usuarios habituales y de riesgo.

La información en profundidad de Proofpoint ITM ayuda a responder al "quién, qué, dónde y porqué" de la actividad de riesgo. Con contexto y perspectiva, estará en mejor posición para discernir la intención del usuario cuando se produzca una pérdida de datos o un comportamiento al margen de las políticas.

### Listas de vigilancia de usuarios

Las listas de vigilancia inteligentes le ayudan a organizar y priorizar los usuarios por tolerancia al riesgo en función de su perfil. Estas listas pueden basarse en criterios tales como la confidencialidad del cargo y los datos a los que acceden los usuarios. También pueden girar en torno a la vulnerabilidad del usuario al phishing y a otras amenazas que utilizan ingeniería social. Además, pueden emplear criterios basados en la ubicación del usuario, los cambios en su categoría profesional y otros factores jurídicos y relacionados con Recursos Humanos.

## Visibilidad y contexto de la actividad de los usuarios y los datos

### Visibilidad de usuarios habituales y de riesgo

Tanto Proofpoint Endpoint DLP como Proofpoint ITM proporcionan visibilidad de la interacción de los usuarios con los datos. Sin embargo, difieren en el tipo y el volumen de datos que recopilan.

Proofpoint Endpoint DLP recopila telemetría de las interacciones de los usuarios con los datos en los endpoints. Señala si los usuarios manipulan algún tipo de archivo, por ejemplo, modificando su extensión o cambiando su nombre si contiene datos sensibles. También registra si intentan trasladar datos confidenciales subiéndolos a un sitio web no autorizado o copiándolos en una carpeta de sincronización en la nube.

Proofpoint ITM presenta una visión más completa de la actividad basada en el endpoint, lo que permite supervisar a usuarios de riesgo. Capta las mismas interacciones de datos que Proofpoint Endpoint DLP, pero además proporciona visibilidad del uso de las aplicaciones y captura pantallas de la actividad en los endpoints y de otros comportamientos peligrosos. Este tipo de comportamientos pueden incluir la instalación y ejecución de herramientas no autorizadas o la realización de actividades asignadas al administrador de seguridad. La información en profundidad de Proofpoint ITM ayuda a responder al "quién, qué, dónde y porqué" de la actividad de riesgo. Con contexto y perspectiva, estará en mejor posición para discernir la intención del usuario cuando se produzca una pérdida de datos o un comportamiento al margen de las políticas.

El enfoque centrado en las personas de Proofpoint proporciona una visibilidad más granular de las interacciones de sus usuarios con los datos confidenciales que la ofrecida por las herramientas tradicionales de DLP para endpoints. Además, estas últimas no informan del desplazamiento de los datos, a menos que la acción genere una alerta. Tampoco relacionan a los usuarios con las acciones. Son omisiones con las que puede pasar desapercibida una actividad de datos aparentemente lícita que, analizada en contexto, demuestra formar parte de un comportamiento de riesgo más amplio.

### Análisis de contenido y clasificación de los datos

Puede identificar los datos confidenciales que se desplazan, en el momento de mayor riesgo, gracias al análisis de contenido en movimiento y la lectura de etiquetas de clasificación de datos, como las de Microsoft Information Protection.

Aprovechando la inversión ya realizada en clasificación de datos, puede identificar información confidencial de la empresa, como propiedad intelectual, sin crear flujos de trabajo separados para equipos de seguridad y usuarios finales. En algunos casos, quizá no pueda confiar en la clasificación de datos para distinguir datos sometidos a normativas y datos de clientes, pero sí hacer uso de los excelentes detectores de contenido de eficacia demostrada de Proofpoint Cloud App Security Broker (CASB) y Proofpoint Email DLP. Y Proofpoint Intelligent Classification and Protection (antes Dathena) le permite descubrir y clasificar datos automáticamente en tiempo real con inteligencia artificial.

Para detectar y prevenir comportamientos de riesgo, puede configurar reglas de análisis de contenido. Cuando un comportamiento no cumple las políticas, se genera una alerta que proporciona información práctica en tiempo real. El análisis de contenido se activa cuando un usuario realiza una actividad peligrosa, como cargar o descargar datos de la web, copiar datos en USB, sincronizar o compartir datos en la nube y abrir documentos.

# Detección en tiempo real de comportamientos de usuarios e interacciones con datos que comportan riesgos

## Motor de reglas flexible

Puede crear desde cero reglas y activadores adecuados para su entorno o bien adaptar nuestros escenarios de amenazas prediseñados. Estos escenarios pueden modificarse por grupos de usuarios, apps, fecha/hora, así como por confidencialidad de los datos, etiquetas de clasificación, orígenes y destinos, canales de desplazamiento y tipos de datos. Para favorecer la coherencia y ayudarle a ahorrar tiempo, las reglas configuradas para ITM pueden aplicarse a otros canales, como el correo electrónico, la nube y la web, a través del administrador de políticas unificado de la plataforma.

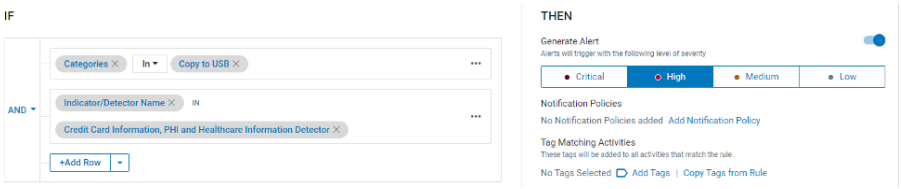


Figura 2: Configuración de alertas con instrucciones condicionales simples.

## Biblioteca de alertas

Proofpoint Endpoint DLP y Proofpoint ITM incluyen bibliotecas de alertas listas para utilizar que facilitan la configuración y aceleran la rentabilidad. Tanto Proofpoint Endpoint DLP como Proofpoint ITM pueden alertarle del desplazamiento y las interacciones de riesgo de los datos que se producen en el endpoint. Proofpoint ITM también puede enviar alertas sobre una amplia variedad de comportamientos relacionados con amenazas internas.

## Biblioteca de alertas de Proofpoint Endpoint DLP y Proofpoint ITM

### ACTIVIDAD DE LOS DATOS

Alertas relacionadas con actividades de interacción y filtración de datos, como las siguientes (más de 40 alertas):

- Subida de archivos a la web
- Copia de archivos en dispositivos USB
- Copia de archivos para sincronización de nube local
- Impresión de archivos
- Actividades con archivos (cambiar nombre, mover y eliminar)
- Seguimiento de archivos (web a USB, web a web, etc.)
- Descarga de archivos desde la web
- Envío de archivos como adjuntos de correo electrónico
- Descarga de archivos desde el correo electrónico/endpoint

### ACTIVIDAD DE LOS USUARIOS (SOLO PROOFPOINT ITM)

Alertas relacionadas con toda la variedad de actividades de usuarios en los endpoints (más de 100 alertas):

- Ocultación de información
- Acceso no autorizado
- Omisión de controles de seguridad
- Comportamiento imprudente
- Creación de una puerta trasera
- Infracción del copyright
- Herramientas de comunicaciones no autorizadas
- Tareas de administración no autorizadas
- Actividad de administrador de bases de datos no autorizada
- Preparación de un ataque
- Sabotaje de tecnologías de la información
- Elevación de privilegios
- Robo de identidad
- Actividad GIT sospechosa
- Uso inaceptable

Muchas veces los usuarios no saben que su comportamiento es peligroso, pero con las notificaciones puede ayudarles a aprender.

## Prevención de filtraciones de datos no autorizadas desde el endpoint

No siempre basta con detectar las actividades de riesgo asociadas a usuarios y datos: en ocasiones, debe bloquear la fuga de datos en tiempo real. Con nuestra plataforma puede evitar interacciones de los usuarios con los datos confidenciales contrarias a las políticas.

Este tipo de interacciones incluye:

- Transferir datos a y desde dispositivos USB.
- Sincronizar archivos con carpetas cloud.
- Subir archivos a sitios web no autorizados.
- Imprimir archivos.

Personalice la prevención por usuarios, grupos de usuarios, grupos de endpoints, nombres de procesos, dispositivo USB, número de serie USB, proveedor de USB, etiquetas de clasificación de datos, URL de origen y resultados del análisis de contenido. Puede ampliar las funciones de DLP a aplicaciones de correo electrónico, cloud y web con el resto de nuestra plataforma Proofpoint Information Protection and Cloud Security.

## Concienciación sobre comportamientos de riesgo

Muchas veces los usuarios ignoran que su comportamiento es peligroso, pero con las notificaciones puede ayudarles a aprender. Por ejemplo, si un usuario intenta trasladar archivos sensibles, recibirá una notificación que le informará de que esa acción infringe la política corporativa y le solicitará una justificación. La notificación irá acompañada de un enlace a la política de la empresa. Concienciar a los empleados sobre su comportamiento contribuye a mantener su productividad y a la vez refuerza los controles de seguridad. Las notificaciones pueden personalizarse según el riesgo, la función o la ubicación del usuario.

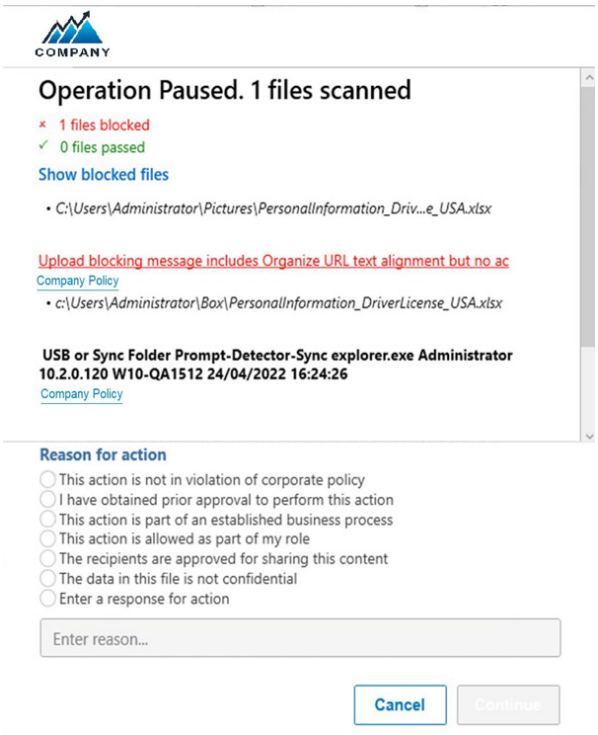


Figura 3: Notificación a un usuario final de su comportamiento de riesgo y solicitud de justificación.

# Mayor agilidad en la investigación y la respuesta a incidentes

## Consola unificada

Proofpoint Endpoint DLP y Proofpoint ITM aprovechan la plataforma Proofpoint Information Protection and Cloud Security para ayudarle a acelerar la investigación y la respuesta a incidentes de origen interno. La plataforma recopila telemetría de los endpoints, el correo electrónico y la nube para proporcionar visibilidad multicanal en un mismo lugar. Su consola unificada ofrece visualizaciones intuitivas que permiten supervisar actividades, correlacionar alertas, gestionar investigaciones, cazar amenazas y coordinar la respuesta a incidentes.

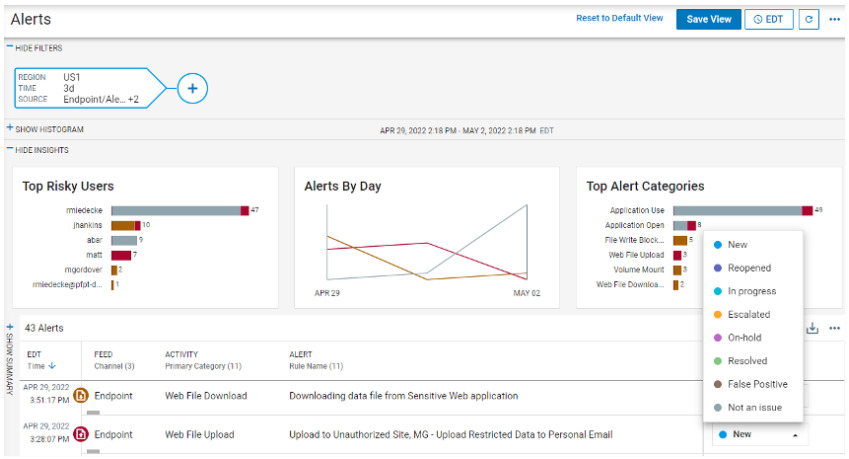


Figura 4: Visualización de todos los eventos y alertas desde una consola unificada.

## Caza de amenazas simplificada

Nuestras potentes funciones de filtrado y búsqueda le ayudan a identificar las amenazas de manera proactiva con exploraciones de datos personalizadas. Puede buscar los comportamientos y actividades de riesgo que afectan a su organización o responder ante nuevos riesgos. Al igual que con nuestras funciones de detección, puede adaptar una de las plantillas de exploración de amenazas listas para utilizar o crear la suya propia.

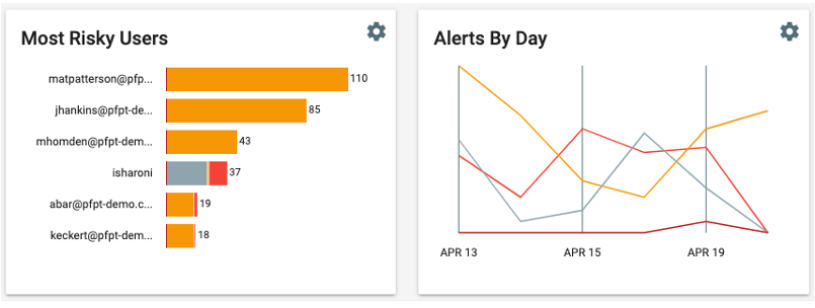


Figura 5: Identificación de comportamientos potencialmente peligrosos o fuera de lo normal.

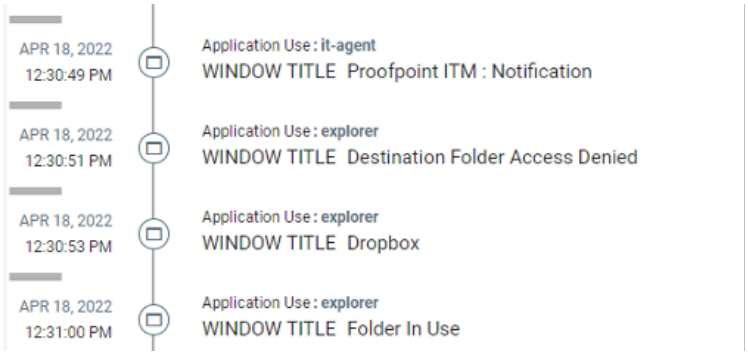


**Figura 6: Vista cronológica fácil de entender con el historial de interacciones del usuario con los datos.**

## Triaje de alertas

La investigación y la resolución de las alertas de seguridad de origen interno no siempre es fácil y puede convertirse en un proceso largo y costoso. Además, a menudo requiere la participación de departamentos no técnicos, como el de Recursos Humanos, cumplimiento de normativas, legal y gestión de línea de negocio.

Con Proofpoint Endpoint DLP y Proofpoint ITM puede analizar a fondo cada alerta, ya que ambas soluciones le permiten ver los metadatos y reunir información contextualizada en vistas cronológicas. Los equipos de seguridad pueden ver rápidamente qué eventos se deben investigar en profundidad y cuáles se pueden cerrar de forma inmediata. Las etiquetas para agrupar y clasificar las alertas facilitan la coordinación.

Las funciones de flujo de trabajo básico y uso compartido de información optimizan la colaboración multifuncional. Puede exportar registros de actividades de riesgo sobre múltiples eventos en formatos de archivos habituales, como PDF. Con Proofpoint ITM, estas exportaciones de PDF desde la plataforma incluyen pruebas con capturas de pantalla, así como datos del contexto relacionado. Todo ello ayuda a los equipos no técnicos, como Recursos Humanos, a interpretar fácilmente los datos para las investigaciones forenses.

## Capturas de pantalla para usuarios de riesgo

Una imagen vale más que mil palabras. Proofpoint ITM puede realizar capturas de pantalla de la actividad de los usuarios. Disponer de pruebas claras e irrefutables de los comportamientos maliciosos o negligentes ayuda a los directivos y a los departamentos jurídico y de RR. HH. a tomar decisiones informadas.

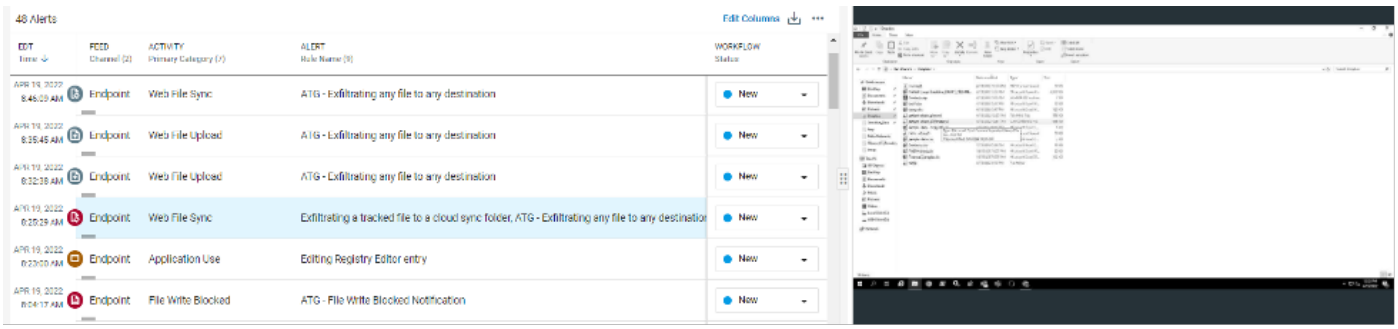


**Figura 7: Vista cronológica de las actividades de los usuarios con captura de pantalla del endpoint del usuario.**

### Facilidad de integración en entornos de seguridad complejos

Lo que impulsa la plataforma Proofpoint Information Protection and Cloud Security son los microservicios. Con los webhooks de nuestra plataforma, sus herramientas SIEM y SOAR pueden ingerir las alertas de Proodpoint Endpoint DLP e Proodpoint ITM, lo que facilita la identificación y la clasificación rápida de los incidentes.

En caso de infraestructuras de seguridad complejas, quizá sea necesario mantener una única fuente de información en todos los sistemas. Facilitamos esta tarea con exportaciones automáticas de datos de Proofpoint Endpoint DLP y Proofpoint ITM al almacenamiento de AWS S3 que posea y opere.

## Necesidades resueltas de privacidad y cumplimiento

### Administración de la residencia y el almacenamiento de los datos

La plataforma Proofpoint Information Protection and Cloud Security cuenta con el respaldo de nuestros centros de datos en varias regiones, lo cual le permite cumplir los requisitos de protección y residencia de los datos. Actualmente tenemos centros de datos en Estados Unidos, Europa, Australia y Japón.

El almacenamiento de datos de los endpoints puede controlarse agrupando endpoints y asignando cada grupo o dominio a un centro de datos. Esta función permite a los clientes separar fácilmente los datos por zona geográfica. Por ejemplo, los datos de endpoints en EE. UU. pueden agruparse en un dominio estadounidense y enviarse al centro de datos de Estados Unidos.

### Privacidad con controles de acceso basados en atributos

Para cumplir los requisitos de privacidad, es preciso tener flexibilidad y control del acceso a los datos. Con Proofpoint Endpoint DLP y Proofpoint ITM, puede administrar los accesos con facilidad para garantizar que los analistas de seguridad solo vean los datos que necesitan. Por ejemplo, puede elaborar políticas granulares para asignar los accesos de tal forma que los analistas de seguridad establecidos en Europa solo puedan ver datos europeos, no de Estados Unidos ni de la región de Asia-Pacífico. Y dispone de flexibilidad para dar a un analista únicamente acceso a los datos de un determinado usuario y limitar cuánto tiempo podrá acceder a ellos.

## Visibilidad y contexto multicanal

Proofpoint Endpoint DLP y Proofpoint ITM aprovechan toda la potencia de la plataforma Proofpoint Information Protection and Cloud Security. Adoptan un enfoque centrado en las personas sobre contenido, comportamientos y amenazas para impedir la pérdida de datos e investigar las amenazas. A través de una consola unificada, ofrecen visibilidad e información contextualizada de múltiples canales, incluidos los endpoints, el correo electrónico, la nube y la web.

Permiten, desde una única consola, configurar políticas, cazar amenazas e investigar y responder a alertas, sea cual sea el canal, sin necesidad de pasar de una herramienta a otra para cada actividad. También permiten analizar a fondo los metadatos de las alertas y, de este modo, averiguar qué ha ocurrido antes, durante y después de un evento. Además, la solución nativa de la nube puede desplegarse con rapidez, lo que contribuye a agilizar su rentabilización.

Trabaje con más eficacia, ahorre tiempo valioso y minimice las interrupciones de la actividad empresarial causadas por la pérdida de datos y las amenazas internas gracias a la visibilidad y el contexto que proporciona la plataforma Proofpoint Information Protection and Cloud Security.

## MÁS INFORMACIÓN

Para obtener más información, visite **http://proofpoint.com/es**.