Proofpoint Insider Threat Management

Gestión de amenazas internas centrada en las personas para las empresas modernas

VENTAJAS PRINCIPALES

- Detección de actividades internas de riesgo y prevención de pérdida de datos desde el endpoint
- Simplificación de la respuesta a amenazas y la pérdida de datos de origen interno
- Reducción del tiempo hasta alcanzar la rentabilidad gracias a un despliegue SaaS muy escalable, a través de un moderno backend nativo cloud
- Productividad de los usuarios garantizada gracias a un agente ligero en el endpoint

CASOS DE USO PRINCIPALES DE ITM

- Identificación del riesgo asociado a los usuarios
- Protección frente a la pérdida de datos desde el endpoint
- Aceleración de la respuesta a los incidentes causados por usuarios
- Desarrollo de programas de gestión de amenazas internas

Insider Threat Management (ITM) de Proofpoint aplica un enfoque centrado en las personas para proteger su empresa contra la pérdida de datos, los actos maliciosos y los daños a la marca imputables al personal interno. Le protegemos frente a la malicia, negligencia o desconocimiento de usuarios autorizados. Asimismo, correlacionamos la actividad de los usuarios y el movimiento de datos para protegerle de fugas de datos provocadas por usuarios internos. Además, detectamos comportamientos de riesgo en tiempo real para que cuente con pruebas irrefutables de actos maliciosos.

Detección y prevención de comportamientos de riesgo en tiempo real

Proofpoint ITM permite establecer una correspondencia en tiempo real entre comportamientos de riesgo a nivel de aplicaciones, archivos, equipos de sobremesa, servidores y entornos virtualizados en tiempo real, y no cuando el incidente ya se ha producido. Ofrecemos una visibilidad en tiempo real que le proporciona nuevas formas de correlacionar, detectar y resolver incidentes debidos a amenazas internas.

Escenarios de amenazas reales y colaborativos

Puede detectar, en tiempo real, comportamientos de riesgo, tales como

- Filtración de datos
- Desplazamiento lateral peligroso de datos
- Abuso de privilegios
- Uso indebido de aplicaciones
- Acceso no autorizado
- Acciones accidentales peligrosas

Gracias a nuestro generador de reglas basado en lógica booleana, es fácil crear reglas y activadores adaptados a su entorno. Puede partir de cero o de escenarios de amenazas preconfigurados. Nuestra amplia variedad de reglas de detección de amenazas internas aprovecha el conocimiento del CERT de la universidad Carnegie Mellon, NITTF, NIST y de nuestros clientes.

Caza de amenazas simplificada

La caza de amenazas no se limita a las amenazas externas. Gracias a ITM, puede identificar a usuarios internos que asumen riesgos innecesarios o malintencionados. Nuestra interfaz de tipo apuntar y hacer clic permite explorar y buscar fácilmente los comportamientos anormales de forma proactiva.

Con la caza de amenazas simplificada puede:

- Estudiar las actividades y los comportamientos de riesgo dentro de su entorno
- Utilizar grupos inteligentes para filtrar los miles de actividades que no tienen importancia y centrarse en las relevantes
- Contextualizar los comportamientos anormales gracias a una vista cronológica de las actividades y a pruebas basadas en capturas de pantalla

Compatibilidad con la clasificación de datos

Nuestras soluciones se integran con Microsoft Information Protection (MIP). Nuestro agente de ITM lee las etiquetas de confidencialidad en tiempo real mientras que el usuario interacciona con el archivo. Puede definir reglas de detección y prevención basadas en la etiqueta de sensibilidad de MIP, el origen, tipo y destino del archivo.

Prevención de la pérdida de datos

Proofpoint ITM permite prevenir la filtración de datos confidenciales a través de los canales habituales, como son los dispositivos USB, incluidas carpetas de sincronización locales, dispositivos de almacenamiento conectados a la red, unidades flash, dispositivos multimedia y teléfonos. La solución funciona incluso cuando el usuario no está conectado.

Puede gestionar las actividades USB por usuario, grupo y host, de las formas siguientes:

- Bloquear la escritura de datos en USB
- Poner los dispositivos USB seguros en una lista segura
- Bloquear los archivos que siguen determinados patrones de nombre de archivo
- Bloquear tipos de archivos
- Bloquear fuentes de archivos
- Implementar reglas de prevención globales

La suite Proofpoint Enterprise DLP puede ampliar la protección al correo electrónico y las apps cloud.

Aceleración de la respuesta a incidentes

Muchas empresas llevan a cabo iniciativas frente a amenazas internas a raíz de un incidente de seguridad. Y en su mayoría descubren que los flujos de trabajo genéricos de sus herramientas de seguridad no son eficaces contra las amenazas internas. Los datos internos son sensibles y requieren de un mayor grado de colaboración con los equipos que no se ocupan de la ciberseguridad.

Contexto inmediato y pruebas irrefutables

Nuestros flujos de trabajo están específicamente adaptados a los eventos generados por los usuarios. Además, puede buscar los eventos de seguridad gracias a palabras clave y filtros entre todos los metadatos recopilados y todas las capturas de pantalla realizadas. Dicho de otro modo, no hay que aprender un nuevo lenguaje de consulta. Los filtros se pueden guardar para utilizarlos en la caza proactiva de amenazas y para investigaciones futuras.

A medida que identifica las alertas y eventos críticos relacionados con las investigaciones, puede etiquetarlos y categorizarlos. Si necesita compartir pruebas, puede encontrar las alertas y los eventos pertinentes gracias a estas etiquetas, y después exportarlos a formatos de archivo habituales, como PDF. Estos informes incluyen capturas de pantalla y contexto asociado a los detalles de las alertas y eventos ("quién, por qué, dónde y cuándo"). Esto facilita su gestión por parte del equipo de ciberseguridad y su compresión por parte de los equipos jurídico, de RR. HH. y cumplimiento de normativas, así como de los investigadores.

Ventajas de la arquitectura de ITM

Nuestra arquitectura basada en la nube está diseñada para ofrecer escalabilidad, facilidad de uso, seguridad y capacidad de ampliación. Utiliza nuestros agentes de endpoints ligeros y líderes del sector para recopilar los datos de actividad. Usted consigue así una visibilidad inigualable e independiente de las aplicaciones de las actividades de los usuarios a nivel de sistemas, sin interferir en su trabajo.

Despliegue totalmente SaaS

Proofpoint Endpoint DLP es una moderna plataforma SaaS diseñada para facilitar la escalabilidad, el análisis, la seguridad, la privacidad y la capacidad de ampliación. De esta forma, reduce el tiempo de instalación y el coste del backend, y simplifica la gestión continua a los administradores de la seguridad en toda la organización. El resultado es una visibilidad instantánea de la actividad de los datos.

Dos problemas, una solución ligera

Proofpoint Endpoint DLP e Proofpoint Insider Threat Management utilizan un mismo agente ligero y una moderna arquitectura SaaS. Cuando se usan juntos, Endpoint DLP protege frente a los riesgos de pérdida de datos entre los usuarios habituales, mientras que ITM amplía esa protección a todos los comportamientos de riesgo de usuarios malintencionados o que entrañan un mayor peligro.

MÁS INFORMACIÓN

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