

FICHA TÉCNICA

Proofpoint Communications Insights for Insider Threat Management

Información sobre los riesgos relacionados con los usuarios para una detección proactiva



Ventajas principales

- Identificación de señales de alerta tempranas antes de que se produzcan acciones perjudiciales.
- Visibilidad completa de las intenciones y el comportamiento de los usuarios.
- Aceleración de la toma de decisiones gracias a resúmenes generados por IA y a información contextual.
- Intervención proactiva para prevenir nuevos daños y adoptar las medidas adecuadas.
- Protección de la privacidad de los empleados mediante la generación de alertas extremadamente fiables sin revelar el contenido completo de las comunicaciones.

Las amenazas internas comienzan con una intención

Las amenazas internas rara vez comienzan con una acción; comienzan con una intención. Sin embargo, la mayoría de los programas de gestión de riesgos internos se basan principalmente en señales de comportamiento. Solo detectan las violaciones de las políticas después de que se haya producido la actividad de riesgo. Sin embargo, las señales de alerta críticas (como el resentimiento, la coacción, los agravios o la malicia) suelen aparecer primero en las comunicaciones profesionales cotidianas. Entre ellas se incluyen el correo electrónico, la mensajería y las plataformas de colaboración.

Sin visibilidad sobre las señales de comunicación, los equipos de seguridad carecen del contexto necesario para anticiparse a los riesgos internos. Resultado: la detección se retrasa y las investigaciones se llevan a cabo de forma reactiva. Los equipos pierden oportunidades de intervenir antes de que se filtren datos sensibles o se produzcan daños en los sistemas y las redes.

¿Por qué adoptar Proofpoint Communications Insights for ITM?

Proofpoint Communications Insights for Insider Threat Management ofrece una visión más detallada de las intenciones de los usuarios mediante el análisis de las comunicaciones profesionales en busca de indicadores de comportamientos maliciosos o de riesgo. Al combinar la información sobre las comunicaciones con la actividad de los usuarios en el endpoint, la solución ayuda a los equipos internos de gestión de riesgos a detectar antes las posibles amenazas. Es importante que los equipos comprendan no solo lo que hacen los usuarios, sino también lo que podrían estar pensando o planeando.

Una comprensión integral de las motivaciones y las acciones permite intervenir de forma más rápida y proactiva antes de que se produzcan daños. De este modo, se obtiene un programa de gestión de riesgos internos más sólido que reduce la exposición, mejora el tiempo de respuesta y favorece el cumplimiento normativo.

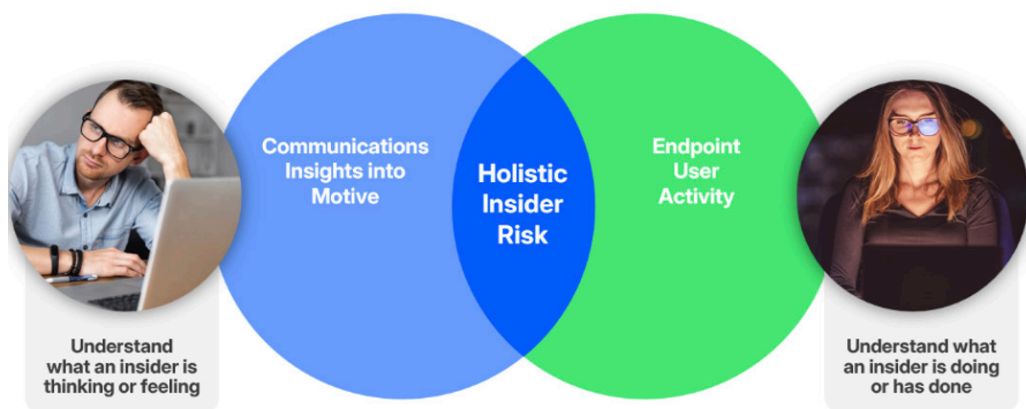


Figura 1: Proofpoint Communications Insights for ITM combina información sobre las comunicaciones de los usuarios y su actividad en los endpoints.

Funcionamiento de Proofpoint Communications Insights for ITM

Proofpoint Communications Insights for ITM puede supervisar las comunicaciones de los usuarios en Microsoft 365 y Google Workspace. La supervisión de Microsoft 365 incluye Copilot, Mail, OneDrive, SharePoint, Teams y Viva Engage. La supervisión de Google Workspace incluye correos electrónicos, llamadas de voz, mensajes SMS, grabaciones de llamadas y Google Chat.

El análisis de riesgos relacionado con las comunicaciones de los usuarios, impulsado por IA, identifica indicadores alineados con el modelo Insider Threat Matrix™, un marco industrial abierto y público para detectar y prevenir amenazas internas. Este análisis identifica el estado de ánimo de los usuarios, incluyendo sentimientos más matizados como el resentimiento, el descontento o la coacción. El análisis de las comunicaciones de los usuarios mediante IA está disponible en más de 100 idiomas y dialectos.

Cuando Proofpoint Communications Insights for ITM identifica comunicaciones de usuarios que suponen un riesgo, se envía una alerta a Data Security Workbench, la consola unificada de Proofpoint Insider Threat Management. A partir de ahí, los analistas de seguridad pueden examinar los resúmenes generados por la IA que ponen de relieve intenciones potencialmente preocupantes. Los analistas solo pueden ver todas las conversaciones de los usuarios cuando sea necesario. Esto garantiza un acceso controlado a los datos sensibles y protege la privacidad de los usuarios.

La solución conserva las comunicaciones de los usuarios durante 90 días.

Detección proactiva de riesgos internos

Proofpoint Communications Insights for ITM permite a los equipos de seguridad pasar de las investigaciones reactivas a la detección proactiva de amenazas internas. Unifica la motivación y el comportamiento en una visión única y útil de los riesgos.

La combinación de un análisis de las comunicaciones basado en IA y los datos telemétricos de los endpoints de Proofpoint ITM ofrece a los equipos de seguridad una visión general de las intenciones y el comportamiento de los usuarios. Un contexto más detallado permite realizar investigaciones más rápidas y fiables. Las funciones de detección mejoradas protegen la privacidad de los empleados.

Con Proofpoint Communications Insights for ITM, podrá beneficiarse de una detección proactiva de riesgos internos con:

- **Detección temprana de riesgos** – Obtenga información sobre las intenciones de los usuarios gracias a la captura continua y al análisis inteligente de las comunicaciones profesionales. Detecta las posibles amenazas antes y con mayor precisión.
- **Información sobre el "porqué"** – Comprenda por qué se producen los riesgos añadiendo un contexto y una intención humana a las señales técnicas.
- **Aceleración de las investigaciones** – Gracias a la visibilidad de las señales de comunicación y del comportamiento de los endpoints, obtén una perspectiva más detallada que te permita realizar investigaciones más rápidas.
- **Detección mejorada** – Libere a los analistas de seguridad de la tarea de revisar las comunicaciones no intencionadas. Céntrese en alertas extremadamente fiables, lo que reduce la carga operativa.
- **Controles de privacidad** – Proteja la privacidad de los usuarios notificando los riesgos únicamente mediante alertas, sin mostrar el contenido completo de las comunicaciones de los usuarios.

proofpoint®

Acerca de Proofpoint, Inc. Proofpoint, Inc. es un líder global en ciberseguridad centrada en las personas y en agentes, protegiendo la forma en que las personas, los datos y los agentes de IA se conectan a través del correo electrónico, la nube y las herramientas de colaboración. Proofpoint es un socio de confianza para más del 80 % de las empresas Fortune 100, más de 10 000 grandes empresas y millones de organizaciones más pequeñas, ya que ayuda a detener amenazas, prevenir la pérdida de datos y fortalecer la resiliencia en las personas y en los flujos de trabajo de IA. La plataforma de seguridad de colaboración y de datos de Proofpoint ayuda a organizaciones de todos los tamaños a proteger y empoderar a su personal mientras adoptan la IA de forma segura y con confianza. Para obtener más información, consulte www.proofpoint.com/es.

Conecte con Proofpoint: [LinkedIn](#)

Proofpoint es una marca registrada o nombre comercial de Proofpoint, Inc. en Estados Unidos y/o otros países. Todas las demás marcas registradas contenidas aquí son propiedad de sus respectivos propietarios.

DESCUBRA LA PROOFPOINT PLATAFORMA →