proofpoint

RESUMEN DE LA SOLUCIÓN

La IA en Proofpoint

La IA está permitiendo nuevas e innovadoras formas de ayudar a las personas a realizar su trabajo. De igual forma, la IA está ayudando a los ciberdelincuentes a aumentar su propia productividad. Sus tácticas, técnicas y procedimientos (TTP) se ven potenciados por la IA, lo que les permite llevar a cabo ataques multietapa y multicanal a escala global. Estas amenazas suelen eludir los sistemas de seguridad tradicionales y son más difíciles de detectar por parte de los propios usuarios.

Pero los riesgos no provienen únicamente de ataques externos. Las filtraciones de datos tienen cada vez más su origen en el comportamiento cotidiano de los usuarios dentro de la propia organización. La IA puede ayudar a supervisar el flujo de datos e identificar comportamientos de riesgo en contexto. Esto puede reducir considerablemente la carga de trabajo de los equipos de los centros de operaciones de seguridad (SOC).

Mientras que las repercusiones de la IA en el mundo laboral no dejan de evolucionar, Proofpoint se sitúa a la vanguardia del sector en lo que respecta al uso de la IA para proteger a sus clientes. Al combinar la innovación continua basada en la IA con una inteligencia de amenazas inigualable, nuestras soluciones se adelantan a los ciberdelincuentes, protegen los datos sensibles y ayudan a las empresas a mantenerse seguras en un mundo cada vez más impulsado por la IA.

Cómo utilizan los ciberdelincuentes la inteligencia artificial para intensificar sus ataques

Proofpoint ha podido comprobar de primera mano las consecuencias del uso de la IA por parte de los ciberdelincuentes. En 2025, Proofpoint observó un aumento del 94 % en el número de amenazas por correo electrónico dirigidas a los clientes en comparación con el año anterior. Esto da lugar a un panorama de amenazas más sofisticado, que incluye la inyección de prompts de IA, el envío masivo de correo electrónico y los ataques mediante el desvío de servicios legítimos.

Los ciberdelincuentes aprovechan la IA para ganar terreno de varias maneras:

- **Multiplicador de fuerza.** La IA permite a los ciberdelincuentes llevar a cabo ataques más sofisticados en una superficie de ataque más amplia. Este año hemos detectado miles de correos electrónicos destinados a hacer que los agentes de IA actúen en nombre del ciberdelincuente.
- **Barrera de entrada reducida.** La IA permite automatizar entre el 80 % y el 90 % de la cadena de ataque. De este modo, los ciberdelincuentes disponen de más tiempo para dedicarse a ataques más complejos. Hemos observado un repunte de los ataques multifase y a través de múltiples canales, que implican el envío de miles de mensajes no deseados.
- **Segmentación avanzada.** Antes de la llegada de la IA, los ciberdelincuentes se basaban en patrones genéricos y predecibles para llevar a cabo sus ataques. Gracias a la IA, pueden crear ataques personalizados para cada víctima.

Este año hemos observado un aumento de los ataques personalizados que se hacen pasar por servicios legítimos.

Todos estos cambios han complicado la identificación precisa de las amenazas por correo electrónico.

El análisis semántico y otros métodos basados en grandes modelos de lenguaje pueden resultar útiles.

En 2025, Proofpoint observó un aumento del

94%

en el número de amenazas por correo electrónico dirigidas a los clientes en comparación con el año anterior.

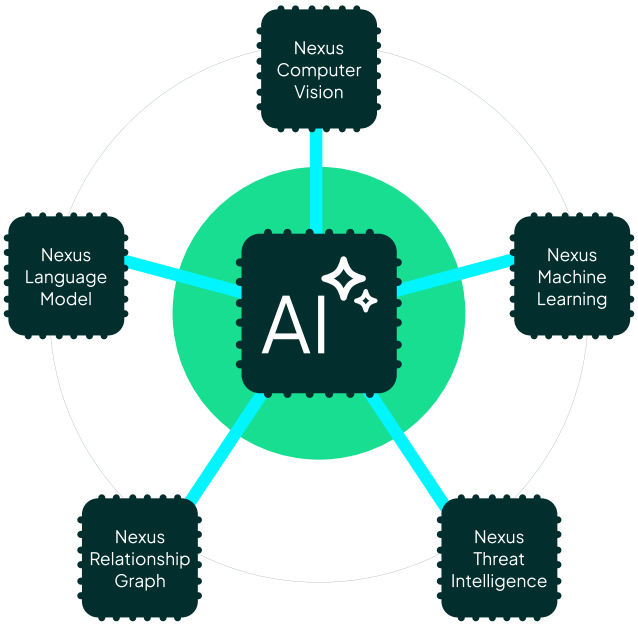
Proofpoint Nexus AI para la seguridad de la colaboración

Las soluciones de seguridad de la colaboración de Proofpoint Collaboration Security Prime se basan en nuestra plataforma Nexus™ AI, que utiliza un enfoque multicapa para la detección de amenazas.

Cómo utilizan los ciberdelincuentes la inteligencia artificial para intensificar sus ataques

Proofpoint Nexus es un conjunto de motores optimizados mediante IA que funcionan de forma conjunta para ofrecer una eficacia de detección del 99,999 %. Combina el aprendizaje automático, la visión artificial, los gráficos de relaciones, la inteligencia de amenazas y los modelos de lenguaje para detectar y bloquear los ataques con precisión.

Los modelos de Proofpoint Nexus AI procesan **2,1 billones de correos electrónicos** al año, con el apoyo de un equipo de inteligencia de amenazas que supervisa **más de 100 grupos de ciberdelincuentes distintos** y más de **8900 campañas de amenazas**.



Nexus LM™ (Language Model) detecta los ataques de BEC y las amenazas sofisticadas de phishing, basándose en un análisis avanzado del lenguaje (en particular, el lenguaje transaccional, el sentido de urgencia, el contexto y la intención) para sacar a la luz las amenazas ocultas y los riesgos desconocidos que pesan sobre los datos.

Nexus RG™ (Relationship Graph) identifica los cambios sutiles en el comportamiento de tus usuarios durante sus comunicaciones, detectando desviaciones respecto al comportamiento habitual, variaciones en el volumen y el intercambio de datos corporativos sensibles con el fin de reducir el riesgo de fugas de datos, y le protege contra los ciberriesgos relacionados con el comportamiento.

Nexus TI™ (Threat Intelligence) analiza las tácticas de los ciberdelincuentes y protege de forma proactiva contra las nuevas ciberamenazas, utilizando datos en tiempo real para identificar las nuevas tácticas de los ciberdelincuentes y las vulnerabilidades del sistema, y activar una emulación en un entorno aislado (sandbox) para las URL y los archivos adjuntos sospechosos.

Nexus CV™ (Computer Vision) identifica y neutraliza las amenazas basadas en la visión. Gracias a una tecnología avanzada de visión artificial, Nexus CV detecta las amenazas ocultas en elementos visuales, como en sitios de phishing, códigos QR, archivos adjuntos maliciosos y mensajes falsificados.

Nexus ML™ (Machine Learning) utiliza técnicas de aprendizaje dinámicas y adaptativas, como el aprendizaje supervisado, el aprendizaje no supervisado y los métodos de ensamblaje. Combina estas técnicas con capacidades de detección predictiva de amenazas que permiten identificar los patrones de ataque conocidos, así como con técnicas no supervisadas para detectar anomalías desconocidas.

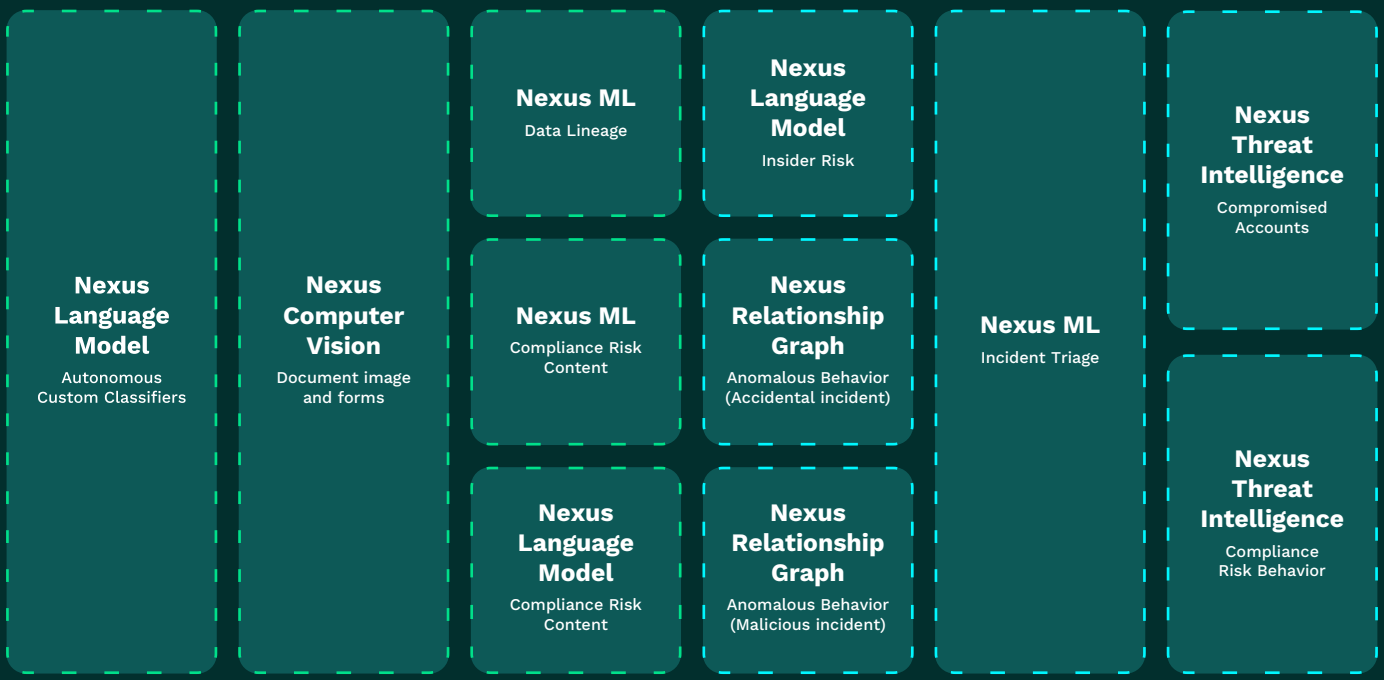
Proofpoint Nexus AI para la seguridad y el gobierno de los datos

Proofpoint utiliza los mismos motores Nexus, potentes y líderes en el mercado, para optimizar sus soluciones de seguridad y gobierno de los datos.

La IA para prevenir las fugas de datos

Nexus clasifica y realiza un seguimiento del recorrido de los datos, así como de su flujo. No importa si los destinatarios pertenecen a la organización o son externos.

- **Nexus LM™ (Language Model)** aprende a identificar los tipos de documentos profesionales que se utilizan en su organización, como los documentos de negociación, las previsiones o los diseños de productos. Transforma estas clases aprendidas en un conjunto de reglas aplicables que permiten detectar, priorizar y proteger rápidamente los datos sensibles sin necesidad de intervención manual.
- **Nexus RG™ (Relationship Graph)** analiza las relaciones entre los datos con el fin de prevenir pérdidas de datos accidentales o intencionadas derivadas de correos electrónicos enviados al destinatario equivocado o de situaciones de filtración de datos.
- **Nexus TI™ (Threat Intelligence)** protege contra las cuentas comprometidas que envían correos electrónicos de phishing, tanto a nivel interno como externo.
- **Nexus CV™ (Computer Vision)** detecta contenidos sensibles presentes en las imágenes de los correos electrónicos y los documentos.
- **Nexus ML™ (Machine Learning)** ofrece una visibilidad completa sobre cómo se crean, copian, renombran, comparten y mueven los archivos entre los repositorios y los destinos. Esta actividad se vincula a un historial trazable que permite agilizar las investigaciones, establecer controles basados en el origen y proporcionar pruebas listas para presentarse en auditorías de programas de protección de datos.



La IA agéntica en Proofpoint

En lo que respecta al ámbito de la IA agéntica, Proofpoint invierte en dos áreas clave.

1: Proofpoint Satori™ Agents

Desarrollamos agentes de IA destinados a integrarse en las soluciones existentes de Proofpoint. Proofpoint Satori Agents automatizará las tareas y reducirá la carga de trabajo manual de sus equipos del SOC.

- **Abuse Mailbox Agent** automatiza la revisión manual de los mensajes denunciados. De este modo, aligera la carga de trabajo de los SOC encargados de distinguir las amenazas reales de los correos electrónicos inofensivos.
- **DLP Triage Agent** gestiona las alertas y la supervisión de la actividad de su solución de prevención de la pérdida de datos (DLP).
- **Phishing Simulation Agent** utiliza la automatización basada en la IA para poner en marcha tus programas de concienciación en materia de seguridad y reforzar la resiliencia humana.

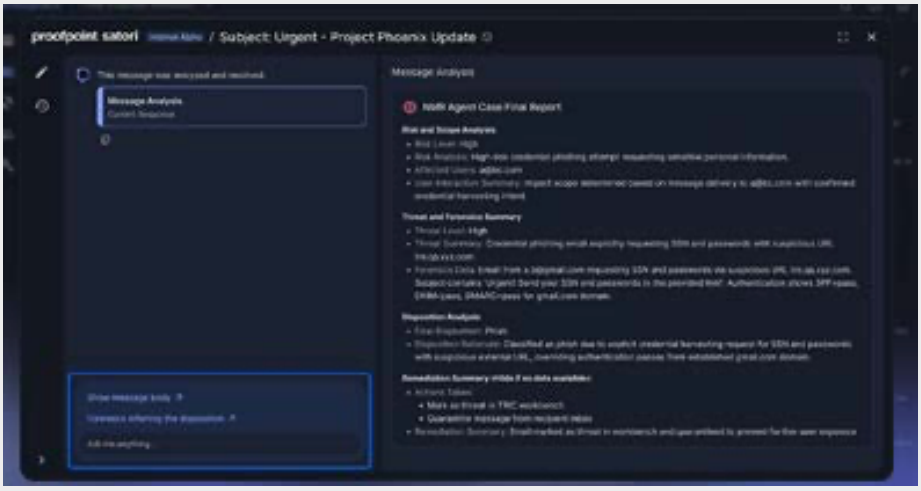


Figura 2: Proofpoint Satori Abuse Mailbox Agent en acción.

2: Proofpoint AI Security

La rápida adopción de la IA entre usuarios, agentes y sistemas empresariales trae consigo nuevos riesgos de seguridad. Por eso hemos ampliado nuestra plataforma de seguridad centrada en las personas (Human-Centric Security) para proteger todo el entorno de trabajo agéntico de su organización.

Proofpoint AI Security ofrece visibilidad, control y protección unificados en todas las interacciones con la IA, lo que garantiza un uso seguro y conforme a la normativa de las tecnologías de IA.

- **Protege la forma en que usuarios, agentes y sistemas interactúan con la IA** en toda la empresa.
- **Ofrece visibilidad y gobierno integrales** sobre el uso de la IA, los agentes y las interacciones con modelos.
- **Previene la fuga de datos, el uso indebido de herramientas y los accesos con permisos excesivos** en flujos de trabajo de IA.

proofpoint.