proofpoint.

RESUMEN DE LA SOLUCIÓN

Proofpoint Collaboration Security Prime

Protección contra ataques de IA a gran escala en el correo electrónico y otros canales

Características principales

- Bloquea la mayor variedad de amenazas con una eficacia del 99,999 %.
- Amplía la protección para las personas en el correo electrónico y otros canales.
- Fortalece la resiliencia humana con orientación e información basadas en riesgos.
- Minimiza el impacto del compromiso de cuentas internas y de proveedores.
- Simplifica las operaciones con una plataforma unificada que automatiza los flujos de trabajo.
- Elimina el coste y la complejidad de las soluciones fragmentadas a través de la consolidación.

Esta suite de soluciones forma parte de la plataforma integrada Human-Centric Security de Proofpoint, que protege a las personas y los datos en los entornos de trabajo agénticos.

Descripción general

A medida que las organizaciones entran en la era agéntica, adoptan herramientas y asistentes impulsados por la IA para ayudar a las personas a trabajar de forma más eficaz. Estos agentes de IA ya forman parte integral de la fuerza laboral e interactúan con empleados, aplicaciones y otros agentes a través del correo, la mensajería, las aplicaciones cloud y mucho más. A medida que se amplía el entorno de trabajo, también crece la superficie de ataque, y los atacantes ya explotan estos canales de comunicación de confianza.

Ante esta situación, muchas organizaciones se ven obligadas a adoptar un enfoque de seguridad fragmentado, basado en soluciones aisladas. Pero esto crea más brechas en las defensas, aísla a los equipos y aumenta la complejidad operativa.

Frente a los ataques impulsados por IA multicanal y multifase, y para proteger las interacciones de confianza entre personas, IA y aplicaciones cloud, las organizaciones requieren un enfoque más integral. Proofpoint Collaboration Security Prime puede ayudarle. Proofpoint Prime unifica la detección y respuesta ante amenazas en todo el entorno de trabajo agéntico.

Además, le ayuda a:

- Protegerse frente los ataques multicanal y multifase con una precisión incomparable.
- Minimizar el impacto del compromiso de cuentas de empleados y de proveedores.
- Proteger las comunicaciones empresariales confidenciales con proveedores, partners y clientes.
- Fortalecer la resiliencia humana con una formación específica centrada en los riesgos y en las personas.
- Optimizar las operaciones de seguridad mediante la automatización.

Protección de las personas en todos los canales de colaboración, incluido el correo electrónico

A medida que el trabajo sigue evolucionando hacia un entorno más conectado y asistido por IA, Proofpoint Collaboration Security Prime protege a las personas independientemente de dónde trabajen. Bloquea los ataques multicanal por correo electrónico, así como a través de herramientas de colaboración y mensajería como Microsoft Teams, Slack, redes sociales y aplicaciones cloud, sin alterar los métodos de trabajo.

Proofpoint Prime protege a los empleados en este entorno de trabajo ampliado contra una amplia gama de amenazas, entre las que se incluyen:

- Phishing avanzado
- Fraude por correo electrónico (Business Email Compromise o BEC)
- Ataques por teléfono o TOAD
- Envío masivo de correo electrónico
- Ransomware
- Usurpación de cuentas
- Ataques generados por IA y técnicas de explotación de la IA, como la inyección de prompts

Además, detiene los ataques en todas las etapas del ciclo de vida de la amenaza: desde antes de la entrega hasta después de la entrega, y desde el momento del clic hasta el inicio de sesión.

Optimizada por la tecnología de IA Proofpoint Nexus®, Proofpoint Prime ofrece una protección inigualable contra las amenazas con una eficacia del 99,999 %. Combina nuestra rica inteligencia sobre amenazas, modelos lingüísticos avanzados, gráficos relacionales, análisis del comportamiento y visión artificial. Todas estas tecnologías trabajan juntas para detectar y bloquear las amenazas antes de que causen daños.

Los modelos Nexus ® AI se entrenan con uno de los conjuntos de datos más amplios y diversos del sector de la ciberseguridad.

Protección frente al compromiso de cuentas

Los ciberdelincuentes utilizan identidades comprometidas para acceder a cuentas legítimas y lanzar ataques multifase. Aprovechan las cuentas comprometidas de sus empleados y proveedores de confianza. En un entorno de trabajo guiado por la colaboración y asistido por agentes, es esencial reducir al mínimo el impacto de estas amenazas.

Proofpoint Collaboration Security Prime le ayuda a detectar, investigar y neutralizar las cuentas de los empleados que han sido comprometidas. Lo hace en todas las plataformas, como Microsoft 365, Google Workspace, Okta, etc., al correlacionar señales de identidad y actividad en todo el ecosistema de Proofpoint.

En el caso de amenazas procedentes de proveedores, Proofpoint Prime protege a sus empleados contra el riesgo de explotación por parte de ciberdelincuentes que utilizan cuentas de terceros comprometidas. Identifica las actividades sospechosas procedentes de las cuentas de proveedores. Además, implementa medidas de protección adaptativas, como indicadores de advertencia y aislamiento de URL, para reducir los riesgos sin interferir en las comunicaciones empresariales legítimas.

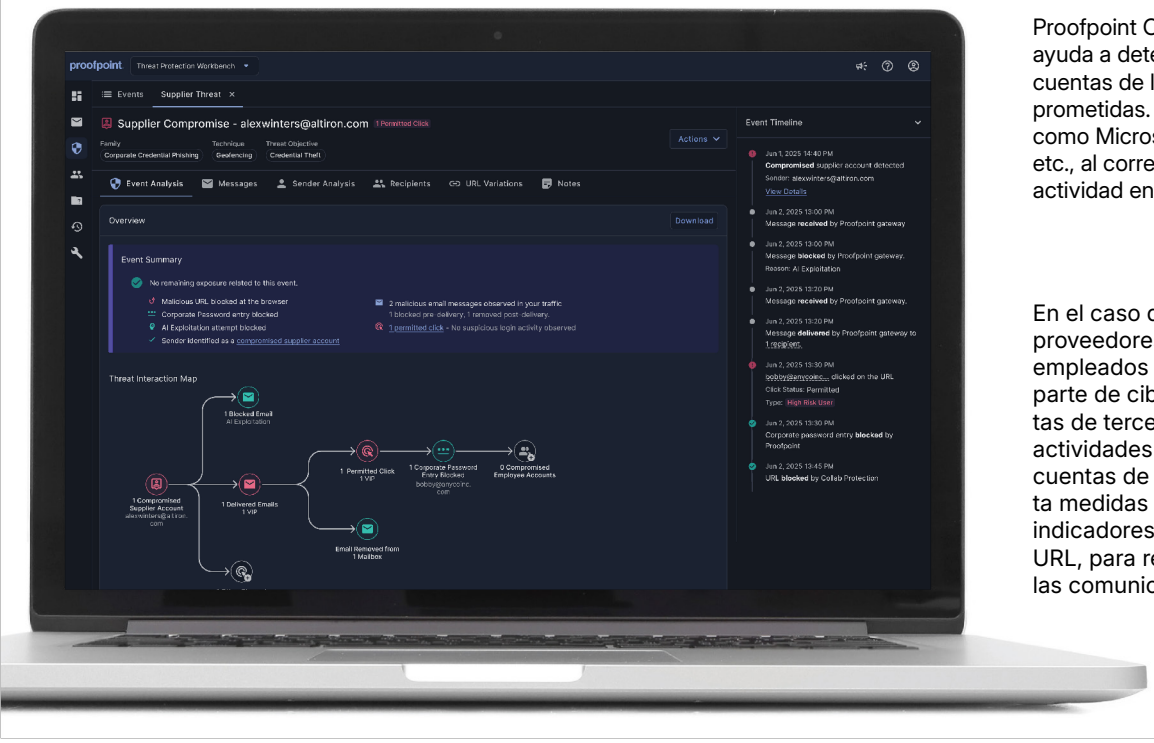

Figura 1. Proofpoint Collaboration Security Prime detiene y correlaciona las amenazas en el correo electrónico, las herramientas de mensajería y colaboración, la nube y los proveedores.

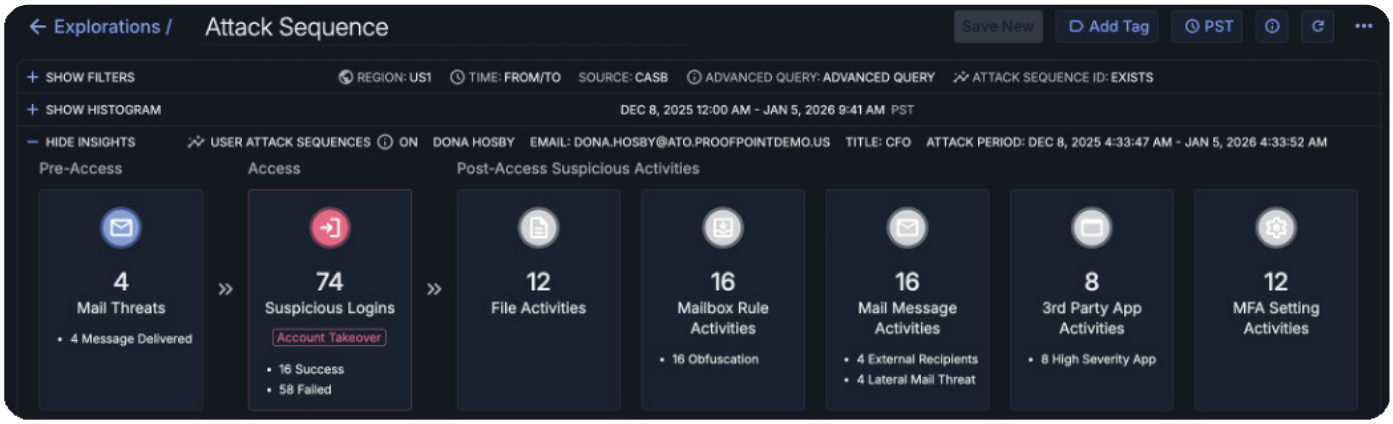

Figura 2. Proofpoint Collaboration Security Prime ofrece visibilidad sobre las secuencias de ataque y automatiza la contención.

Protección de sus comunicaciones empresariales de confianza

Los ciberdelincuentes suelen utilizar tácticas de suplantación de la identidad para acceder a comunicaciones corporativas de confianza. La suplantación de la identidad de su empresa, ya sea mediante la suplantación directa de dominios (domain spoofing) o el registro de dominios parecidos (lookalike domains), pone en peligro a sus empleados, clientes y partners. Además, puede ser muy perjudicial para su marca.

Proofpoint Collaboration Security Prime puede ayudarle a reducir estos riesgos de suplantación de la identidad de forma proactiva. Le ofrece una visibilidad completa de todos los correos electrónicos salientes enviados desde sus dominios de confianza, incluidos los de terceros. Tendrá acceso a potentes herramientas y a consultores expertos que le guiarán en cada paso del proceso de implementación de la autenticación del correo electrónico. Esto garantizará el cumplimiento de DMARC y evitará que los ciberdelincuentes suplanten sus dominios.

Nuestra protección se extiende más allá de los correos electrónicos generados por los usuarios para incluir un entorno seguro dedicado a retransmitir los mensajes generados por las aplicaciones, así como los correos electrónicos enviados por proveedores SaaS externos en su nombre.

Proofpoint Prime también ofrece funciones avanzadas para detectar dominios parecidos. Supervisa dinámicamente Internet para identificar dominios muy similares al suyo. Además, proporciona información detallada sobre su registro y sobre cualquier posible uso indebido.

No nos limitamos a la detección. Podemos desactivar las URL y los dominios maliciosos en su nombre gracias a las estrechas relaciones que mantenemos con los registradores, los proveedores de alojamiento web y los proveedores de dominios de nivel superior. Nuestros profesionales gestionan el proceso de principio a fin, para que sus equipos puedan centrarse en su actividad principal.

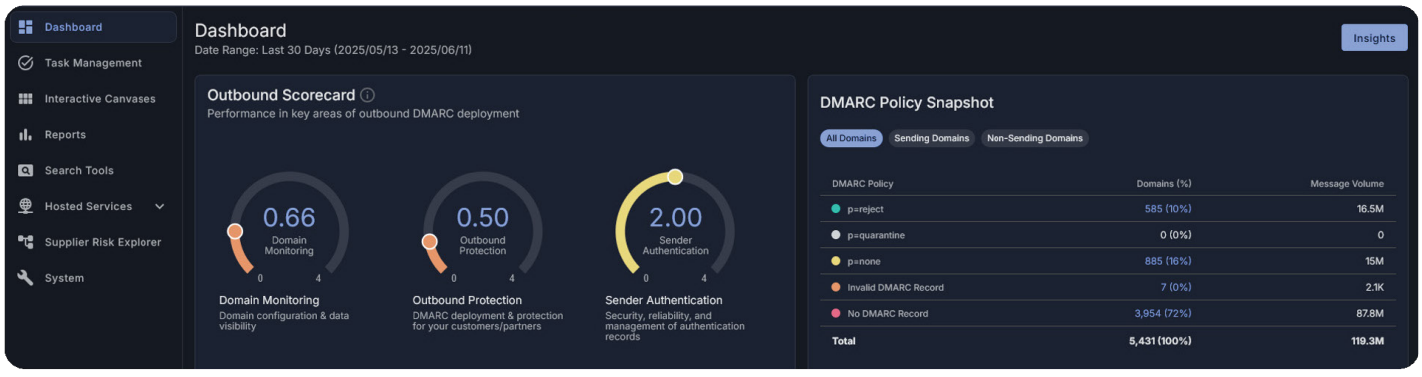

Figura 3. Proofpoint Collaboration Security Prime ofrece una visibilidad sobre las amenazas de suplantación de la identidad, como la suplantación de dominios y el registro de dominios parecidos.

Refuerzo de la resiliencia de los usuarios mediante consejos basados en riesgos

A medida que el trabajo se vuelve más colaborativo y dinámico, es esencial que los empleados sean más resilientes frente a los ciberataques. Esto requiere ir más allá de una formación centrada en el cumplimiento normativo para abarcar la gestión de los riesgos relacionados con los usuarios, es decir, una formación en tiempo real que refleje la forma en que trabajan los usuarios y los riesgos reales a los que se enfrentan..

Proofpoint Collaboration Security Prime ayuda a su organización a llevar a cabo este cambio de rumbo animando a sus empleados a tomar decisiones más seguras. Ofrece formación automatizada, específica y basada en los riesgos asociados a las personas, adaptada al comportamiento, el rol, la exposición a los ataques y el perfil de riesgo único de cada usuario. Gracias a la IA, Proofpoint Prime convierte las amenazas del mundo real en simulaciones instantáneas con un solo clic. Las formaciones se ajustan a los indicios de riesgo activas con el fin de provocar cambios de comportamiento cuantificables y duraderos.

Los módulos de formación no solo se adaptan a las señales de riesgo individuales, sino que se ofrecen en el marco de experiencias atractivas y gamificadas. Esto motiva a los usuarios a participar, lo que refuerza la adopción de comportamientos más seguros con el paso del tiempo. Los alumnos pueden seguir fácilmente su progreso gracias a un panel de control intuitivo, que les mantiene informados y garantiza que asuman sus responsabilidades.

Al mismo tiempo, los administradores pueden adaptar fácilmente los programas en función de las prioridades de la empresa en materia de riesgos. Los resultados hablan por sí solos: mayor compromiso, cambio de comportamiento cuantificable y una cultura de seguridad más sólida dentro de su organización.

Figura 4. Proofpoint Collaboration Security Prime ofrece visibilidad sobre el comportamiento real de los usuarios, lo que permite ofrecer formación específica y basada en los riesgos.

Simplificación de las operaciones de seguridad

A medida que las amenazas se expanden más allá del correo y alcanzan herramientas de colaboración, plataformas cloud y ecosistemas de proveedores, los equipos de seguridad deben hacer cada vez más con menos recursos. En este contexto, las soluciones puntuales y desconectadas no facilitan las cosas. No solo aumentan la complejidad, sino que también ralentizan los tiempos de respuesta y aumentan los costes operativos. Todo esto complica enormemente la reducción de riesgos a gran escala.

Proofpoint Collaboration Security Prime simplifica las operaciones de seguridad al unificar la detección y la investigación de amenazas, y al automatizar los flujos de trabajo y la respuesta. Gracias a las integraciones nativas, el Threat Protection Workbench puede recopilar información de detección y análisis detallados de ataques procedentes de plataformas de correo electrónico, mensajería instantánea y colaboración, cuentas cloud y ecosistemas de proveedores. De este modo, los equipos pueden investigar los incidentes y tomar medidas decisivas, todo ello desde un entorno de trabajo unificado para lograr la máxima eficacia.

Proofpoint Prime también ayuda a los equipos a establecer prioridades de manera eficaz. El Threat Interaction Map correlaciona las amenazas y los eventos de seguridad en todos los puntos de control, y proporciona un mapa visual de las vías de ataque. Esto permite a los analistas identificar rápidamente los incidentes más críticos.

Al mismo tiempo, inspecciona automáticamente los mensajes denunciados por los usuarios, neutraliza el contenido malicioso y proporciona comentarios a los usuarios. Esto permite reducir las intervenciones manuales y reforzar los comportamientos seguros de los usuarios.

¿El resultado? Una respuesta más rápida y una menor complejidad operativa. Además, su equipo de seguridad puede hacer más con menos, sin sacrificar la protección.

Elección del nivel adecuado de protección

Proofpoint Collaboration Security Prime está disponible en varios niveles, lo que le permite adaptar la protección al perfil de riesgo y las necesidades operativas de su organización. Cada nivel se basa en el anterior. La cobertura abarca desde amenazas básicas por correo electrónico hasta canales de colaboración, pasando por el compromiso de cuentas, la reducción de riesgos relacionados con las personas y la protección avanzada de la marca.

Descubra las funciones disponibles en la página siguiente.

proofpoint.

Acerca de Proofpoint, Inc. Proofpoint, Inc. es líder mundial en ciberseguridad centrada en las personas y los agentes, que protege 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 partner de confianza para más de 80 empresas Fortune 100, más de 10 000 grandes empresas y millones de pequeñas organizaciones. Les ayuda a bloquear amenazas, prevenir la pérdida de datos y reforzar la resiliencia de las personas y los flujos de trabajo de IA. La plataforma de colaboración y seguridad de datos de Proofpoint ayuda a organizaciones de todos los tamaños a proteger y empoderar a su

Conecte con Proofpoint: LinkedIn

	Funciones disponibles	Proofpoint Core Email Protection	Proofpoint Collaboration Security Tier 2	Proofpoint Collaboration Security Tier 3	Proofpoint Collaboration Security Prime
Seguridad del correo electrónico	Protección contra ataques BEC, phishing, phishing de devolución de llamadas y malware.	●	●	●	●
	Pila de detección multicapa optimizada por Nexus AI	●	●	●	●
	Datos sobre amenazas incomparables procedentes de más de 2,8 millones de clientes.	●	●	●	●
	Análisis en entorno aislado (sandbox) de archivos adjuntos y URL	●	●	●	●
	Reescritura de URL y análisis en entorno aislado (sandbox) al hacer clic	SEG	SEG	SEG	SEG
	Aislamiento de clics sospechosos en URL reescritas	(VAP)*	Todos los usuarios*	Todos los usuarios*	Todos los usuarios*
	Antispam y detección de correo gris	●	●	●	●
	Etiquetas de advertencias contextuales en caso de correos electrónicos sospechosos	●	●	●	●
	Herramientas adaptativas de integridad del correo electrónico con autoaprendizaje basado en el comportamiento de los usuarios	●	●	●	●
	Políticas de enrutamiento de correo electrónico configurables	SEG	SEG	SEG	SEG
	Corrección automatizada de mensajes	●	●	●	●
	Automatización del buzón de denuncia de abusos	●	●	●	●
	Personas muy atacadas (VAP)™, ciberdelincuentes e inteligencia de amenazas global	●	●	●	●
Protección contra amenazas multicanal y multifase	Detección y corrección de cuentas en la nube comprometidas		●	●	●
	Bloqueo de URL maliciosas enviadas a través de aplicaciones de mensajería y colaboración		●	●	●
	Protección frente a cuentas de proveedores comprometidas		●	●	●
Resiliencia humana y concienciación en seguridad	Automatización de la formación basada en el nivel de riesgo			●	●
	Refuerzo de la concienciación de los empleados mediante simulaciones basadas en amenazas reales			●	●
	Conversión de amenazas activas en simulaciones seguras			●	●

SEG = despliegue de un gateway de correo

***Disponible solo para despliegues**