

Bundles de soluciones de Proofpoint

Proteger a las personas. Defender los datos.

Proofpoint proporciona una estrategia exclusiva de ciberseguridad centrada en las personas, que comienza por saber quiénes son sus VAP (Very Attacked People™, o personas muy atacadas) y evaluar el riesgo que presenta cada uno para su organización. Nuestros bundles Proofpoint Threat Protection y Proofpoint Information Protection proporcionan soluciones globales que responden al panorama actual de amenazas, refuerzan sus recursos y evolucionan al ritmo de su estrategia de seguridad. Este documento ofrece una vista del conjunto de bundles y explica cómo pueden ayudarle a proteger a sus empleados y sus datos.

Inteligencia artificial y aprendizaje automático optimizadas mediante el gráfico de amenazas Nexus

Proofpoint utiliza inteligencia artificial (AI) y aprendizaje automático (ML) para proteger a las personas y los datos. La inteligencia artificial y el aprendizaje automático forman parte de nuestra suite de productos para ofrecer a los clientes protección completa y permanentemente actualizada frente a una amplia variedad de amenazas externas. Contamos con casi dos décadas de experiencia en materia de inteligencia artificial, aprendizaje automático y tratamiento de datos (ciencia de datos) en la plataforma de inteligencia artificial que optimiza los productos de Proofpoint. Esto permite a las soluciones eliminar un amplio espectro de riesgos de ciberseguridad y cumplimiento normativo.

Nuestra inteligencia de amenazas y nuestra tecnología de detección de amenazas destacan por utilizar modelos de aprendizaje automático entrenados por el gráfico de amenazas Nexus de Proofpoint, que está formado por más de un billón de nodos. El gráfico de amenazas Nexus tiene acceso a enormes conjuntos de datos de ciberseguridad que cubren el correo electrónico, la nube, las redes, los dominios, y mucho más. Nuestro equipo interno de tratamiento de datos está formado por profesionales de los sectores público y académico, así como por expertos con titulaciones superiores en ciberseguridad. Hemos colaborado con importantes universidades para estar a la vanguardia en tratamiento de datos. Este equipo trabaja en nuestros productos de protección frente a amenazas, de protección de la información y de cumplimiento normativo en colaboración con investigadores de amenazas. La colaboración maximiza la eficacia de nuestro aprendizaje automático.

Bundles Proofpoint Threat Protection — Proteger a las personas

Proteja a sus empleados frente a las amenazas que se dirigen contra ellos. Gracias a la integración de múltiples controles en el correo electrónico, la nube, los usuarios y los proveedores, la plataforma Proofpoint Threat Protection ofrece una protección completa contra el phishing, las estafas BEC, el malware y el ransomware. Esta plataforma integrada, optimizada por inteligencia artificial, ofrece una visibilidad inigualable de su superficie de ataques, una protección más eficaz frente a las amenazas modernas y resultados operativos positivos. Todos los bundles pueden desplegarse fácilmente gracias a las opciones Inline+API o basadas en registros MX. Y todas ofrecen la misma calidad de protección.

Presentación de Proofpoint Threat Protection

FUNCIONES	COMPONENTE	PX	P0	P1	P1+
Despliegue y administración	<ul style="list-style-type: none"> En modo local, híbrido o en la nube Inline+API o basado en registros MX 	<ul style="list-style-type: none"> Clientes cloud de Microsoft 365 solamente Inline+API solamente 	✓	✓	✓
Estafas Business Email Compromise (BEC)	Análisis de comportamiento y reputación, inteligencia artificial/aprendizaje automático	✓	✓	✓	Panel de riesgos asociados a proveedores
Phishing, ransomware y malware	Análisis de comportamiento y reputación, inteligencia artificial/aprendizaje automático	✓	✓	✓	✓
	Reescritura de URL y análisis en entorno aislado (sandbox) al hacer clic		✓	✓	✓
	Análisis en aislado (sandbox) de adjuntos		✓	✓	✓
Usurpación de cuentas	Visibilidad de la usurpación de cuentas	✓	✓	✓	✓
	Investigación después del acceso en vista cronológica	+	+	+	+
	Corrección de los entornos de correo electrónico y de nube	+	+	+	+
Denuncia de mensajes de correo electrónico y corrección	Herramienta mSOAR automatizada	✓	✓	✓	✓
	Buzón de correo malicioso automatizado	✓*	✓	✓	✓
	Denuncia de mensajes por parte de los usuarios	✓		Etiquetas de advertencias de correo electrónico	
Panel de amenazas y de usuarios	Información de amenazas, incluidos los VAP	✓	✓	✓	✓
	Panel de riesgos asociados a los usuarios		✓	✓	✓
Higiene del correo entrante y configuración	Antispam, antivirus y contra el correo gris		✓	✓	✓
	Funciones para directivos/VIP		✓	✓	✓
	Políticas personalizadas		✓	✓	✓
Defensa en profundidad de usuarios	Aislamiento de clics en mensajes modificados	+		VAP	Todo
	Formación para concienciar en materia de seguridad	+	+	✓	✓
Autenticación del correo electrónico y protección interna	Implementación de DMARC, información práctica	+	+	+	✓
	Protección frente a mensajes internos maliciosos	+	+	+	<5000 usuarios

LEYENDA

- ✓ Incluido en el bundle
- + Disponible con coste adicional

*Próximamente, nube solamente

Descripciones de los bundles Proofpoint Threat Protection

BUNDLE	PRESENTACIÓN	DESCRIPCIÓN	FUNCIONES INCLUIDAS
PX	<p>Protección rápida y fácil del correo electrónico basada en IA para Microsoft 365.</p> <p>Ideal para organizaciones pequeñas que busquen fortalecer la seguridad nativa de Microsoft 365 y simplificar al mismo tiempo la administración de la seguridad con ajustes predefinidos. Se despliega en minutos con la opción Inline+API.</p>	<p>Proofpoint PX solo está disponible para instancias cloud de Microsoft 365. Es la forma más rápida y fácil de disfrutar de la mejor protección del correo electrónico y la nube del sector. Gracias al empleo conjunto de aprendizaje automático, análisis de comportamientos e inteligencia sobre amenazas, PX detecta, bloquea y neutraliza con precisión el phishing, las estafas Business Email Compromise (BEC), y los ataques de ransomware y contra la cadena de suministro que consiguen sortear los controles de seguridad de Microsoft.</p>	<p>Detección y reparación automatizadas optimizada por inteligencia artificial para complementar las defensas nativas de Microsoft</p>
P0	<p>Protección avanzada del correo electrónico y la nube.</p> <p>Ideal para organizaciones con amenazas más dirigidas y aquellas que necesitan personalización y configuración adicionales.</p>	<p>Neutralice las amenazas que llegan a través del correo electrónico en toda la cadena de ataque, desde la detección hasta la respuesta. Esto incluye la capacidad de automatizar la administración del buzón de correo malicioso mediante la eliminación de los mensajes de phishing denunciados por el usuario que sean maliciosos. Esto permite hacer frente a amenazas como el phishing, las estafas Business Email Compromise (BEC), el fraude de proveedores, el ransomware y otros tipos de malware. Esta solución le ayuda a conseguir visibilidad de los objetivos de los ataques y de las técnicas empleadas, así como a determinar si los usuarios atacados hacen clic en mensajes de phishing o los denuncian, y si son comprometidos.</p>	<p>Todas las funciones de PX y:</p> <ul style="list-style-type: none"> • Opciones de despliegue más flexibles (híbrido y local) • Administración del flujo de correo con personalización mediante una consola de administración completa • Protección avanzada al hacer clic en caso de ataques con adjuntos y URL, incluido TAP URL Isolation for VAP • Etiquetas de advertencia de HTML con funciones para denunciar mensajes sospechosos • Higiene de correo electrónico de los usuarios, incluido antispam, antivirus y correo gris, así como otros controles • Panel de riesgos asociados a los usuarios con controles recomendados (Nexus People Risk Explorer)
P1	<p>Protección frente a amenazas avanzadas.</p> <p>Ideal para organizaciones que necesitan formar a los usuarios con funciones adicionales e integradas de defensa en profundidad.</p>	<p>Forme a los usuarios para reforzar su resiliencia frente a las amenazas que reciben. Refuerce la protección frente a amenazas con un sólido programa de formación para concienciar en materia de seguridad que se integra con sus controles de seguridad del correo electrónico e incluye simulaciones de phishing, evaluaciones culturales y de conocimientos, y formación completa y material de concienciación.</p> <p>Adapte el programa de formación propuesto a sus usuarios en función de las amenazas reales que reciben. Utilice todo el catálogo de cursos de formación y herramientas interactivas diseñadas para modificar el comportamiento de los usuarios. Entre las funciones se incluyen simulaciones de amenazas que ponen a prueba la respuesta de los usuarios a los ataques de phishing mediante miles de plantillas, en más de 40 idiomas y 13 categorías. Esto puede ayudar a establecer una base de referencia de seguridad, formar a los empleados para que eviten los riesgos para la seguridad e informar de los progresos. El avance de su programa puede verse en un panel especial para CISO. En él se destacan los indicadores que más interesan a los responsables de seguridad.</p>	<p>Todas las funciones de P0 y Proofpoint Security Awareness Training Enterprise</p>

BUNDLE	PRESENTACIÓN	DESCRIPCIÓN	FUNCIONES INCLUIDAS
P1+	<p>Protección completa contra amenazas que llegan a través del correo electrónico y en la nube.</p> <p>Ideal para grandes empresas que necesitan protección avanzada del correo electrónico y la nube a través de funciones de defensa en profundidad y de información práctica</p>	<p>Refuerce la protección frente al fraude de dominios y de correo electrónico, incluidas las estafas BEC, para bloquear los ataques de suplantación de identidad en el correo electrónico entrantes y salientes que se envían en nombre de su organización. Los ataques BEC pueden utilizar diversas tácticas de suplantación de identidad. Necesita un enfoque de seguridad multicapa que proteja a sus empleados, clientes y partners comerciales. La solución BEC integrada de Proofpoint cubre todas las tácticas de las amenazas, le proporciona visibilidad de todo el ecosistema de correo electrónico y le ofrece controles para detener estos ataques antes de que lleguen a la bandeja de entrada. Vaya más allá de la implementación de DMARC para identificar los riesgos de estafa que presentan sus proveedores. Proofpoint proporciona esta visibilidad única de los riesgos asociados a los proveedores para ayudarle a combatir los ataques complejos contra la cadena de suministro. Identifique automáticamente a sus proveedores y evalúe el nivel de riesgo de los dominios que utilizan para enviar mensajes de correo electrónico a sus usuarios. Gracias a la integración de datos en la plataforma de protección, revelamos el volumen de mensajes, las amenazas detectadas procedentes de los dominios de los proveedores, así como los mensajes bloqueados procedentes de dominios parecidos a los de sus proveedores. Además, las organizaciones con menos de 5000 usuarios también pueden beneficiarse de visibilidad en tiempo real de las amenazas internas enviadas por correo electrónico desde cuentas comprometidas y neutralizarlas automáticamente. Puede identificar rápidamente qué cuentas están comprometidas y los usuarios afectados.</p>	<p>Todas las funciones de P1 y:</p> <ul style="list-style-type: none"> • Proofpoint Email Fraud Defense (EFD) • Proofpoint Supplier Risk Explorer • Proofpoint TAP URL Isolation para todos los usuarios • Internal Mail Defense para organizaciones con menos de 5000 usuarios

Bundle Proofpoint Information Protection — Defender los datos

Modernice su solución de prevención de la pérdida de datos (DLP) con nuestro bundle Proofpoint Enterprise DLP. Este bundle adopta una estrategia centrada en las personas, que reúne contexto detallado sobre el contenido, los comportamientos y las amenazas para disponer de datos prácticos y prevenir la pérdida de datos. Dote a sus equipos de seguridad y cumplimiento con telemetría del correo electrónico, la nube y los endpoints. Esto les permite abordar toda la gama de casos de pérdida de datos centrados en las personas. Todo en una única solución.

Proofpoint Enterprise DLP incluye:

- **Proofpoint Email DLP.** Proporciona protección de la pérdida de datos con políticas integradas, huellas digitales de archivos y la función de autocorrección Smart Send.
- **Proofpoint Cloud App Security Broker (CASB).** Ofrece protección frente a amenazas en la nube y previene la pérdida de datos, incluido el exceso de datos confidenciales compartidos, el control de aplicaciones de terceros y la gestión de las aplicaciones no aprobadas o shadow IT.
- **Proofpoint Endpoint DLP y Proofpoint Insider Threat Management (ITM).** Para el 3 % de los usuarios. Mitigación de riesgos internos con un agente ligero para endpoints. Prevención frente al comportamiento malintencionado y negligente de empleados, usuarios con privilegios y personas externas.

MÁS INFORMACIÓN

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

ACERCA DE PROOFPOINT

Proofpoint, Inc. es una compañía líder en ciberseguridad y cumplimiento de normativas que protege el activo más importante y de mayor riesgo para las organizaciones: las personas. Gracias a una suite integrada de soluciones basadas en cloud, Proofpoint ayuda a empresas de todo el mundo a detener las amenazas dirigidas, a salvaguardar sus datos y a hacer a los usuarios más resilientes frente a ciberataques. Compañías líderes de todos los tamaños, entre las que se encuentra el 75 % del Fortune 100, confían en las soluciones de Proofpoint para su seguridad centrada en personas y su cumplimiento regulatorio, mitigando los riesgos más críticos en sus sistemas de correo electrónico, cloud, redes sociales y web. Encontrará más información en www.proofpoint.com/es.

©Proofpoint, Inc. Proofpoint es una marca comercial de Proofpoint, Inc. en Estados Unidos y en otros países. Todas las marcas comerciales mencionadas en este documento son propiedad exclusiva de sus respectivos propietarios.