



LIBRO ELECTRÓNICO

Protección del correo electrónico más rápida e inteligente

5 razones por las que Proofpoint es la principal opción para reforzar la seguridad del correo electrónico de Microsoft 365 mediante API



Introducción

El correo electrónico es desde hace mucho tiempo el principal vector de amenazas. Y los ataques avanzados, como las estafas Business Email Compromise (BEC), los riesgos para la cadena de suministro, el ransomware y el compromiso de cuentas van en aumento.

Esto ha llevado a firmas de análisis como Gartner y Forrester a recomendar el refuerzo de las seguridad de Microsoft 365.^{1,2}

Para ofrecer una protección completa del correo electrónico, la nube y los datos, han surgido soluciones de seguridad del correo electrónico cloud integrada (ICES) basadas en API. Estas soluciones se despliegan rápidamente para hacer frente de manera proactiva a estos ataques avanzados.

Cuando los clientes de Microsoft quieren reforzar rápidamente su seguridad, recurren en su gran mayoría a Proofpoint. El 85 % de las empresas Fortune 100 (y más de 1,8 millones de clientes en todo el mundo) nos han elegido como su partner de seguridad. Somos líderes del sector en protección del correo electrónico y la nube.

La API Proofpoint Core Email Protection establece un nuevo estándar para soluciones ICES. No solo ofrece un nivel superior en la detección de amenazas con una eficacia del 99,99 %, sino que también proporciona a los equipos herramientas de gestión sin fisuras. Se trata de una plataforma preparada para el futuro que se nutre de las revolucionarias tecnologías de IA de Proofpoint Nexus y de nuestra incomparable inteligencia global de amenazas. Proofpoint le permitirá:

- Bloquear la más amplia variedad de amenazas con la solución basada en IA líder.
- Optimizar la eficacia de su centro de operaciones de seguridad (SOC).
- Preparar su arquitectura de seguridad para el panorama de amenazas del futuro.

Pero estas son solo algunas de las razones. Aquí tiene una lista completa de por qué debería elegir la API Proofpoint Core Email Protection para reforzar la seguridad de Microsoft 365.



1. Mark Harris, Peter Firstbrook, et al. (Gartner). "Market Guide for Email Security" (Market Guide para la seguridad del correo electrónico), octubre de 2021.

2. Jess Burn, Joseph Blankenship, et al. (Forrester). "Best Practices: Phishing Prevention" (Mejores prácticas: prevención del phishing), noviembre de 2021.

Razón 1

Bloquee una amplia gama de amenazas

La información de amenazas es un elemento clave para detectarlas y detenerlas. Cuando los algoritmos tienen más datos con los que trabajar, son más capaces de encontrar anomalías.

Proofpoint cuenta con una combinación única de información de amenazas. Nuestra pila de detección multicapa, Nexus AI, está entrenada por billones de puntos de datos globales que se han recopilado durante más de 20 años de miles de clientes. Combinamos esta información con los conocimientos de nuestro equipo de investigación de amenazas para maximizar la protección de nuestros clientes frente a las amenazas.

Gane en precisión

La mayoría de las soluciones basadas en API solo aplican una técnica de detección, como la detección de anomalías. Esto significa que a menudo pasan por alto amenazas reales o impiden que lleguen mensajes legítimos. En cambio, Proofpoint combina técnicas de IA y aprendizaje automático con inteligencia de amenazas y análisis en entorno aislado (sandbox) para que nuestros motores de detección sean más precisos. Dado que nuestros conjuntos de datos son exhaustivos, no solo somos capaces de detectar más amenazas, sino que también generamos menos falsos positivos.

Razón 1 ●

Razón 2

Razón 3

Razón 4

Razón 5

Trabaje con un líder del sector

Los pasos siguientes

Proteja a su organización en todos sus flancos

Proofpoint Nexus AI integra seis potentes núcleos para contrarrestar una amplia variedad de amenazas basadas en IA.

- **Nexus Language Model (LM)** reconoce sutiles patrones lingüísticos e indicios de comportamiento para identificar los ataques BEC antes de que puedan causar daños.
- **Nexus Generative AI** analiza los datos del correo electrónico, la nube y los endpoints para identificar patrones sutiles en los intentos de phishing y filtración.
- **Nexus Threat Intelligence (TI)** enriquece los modelos de detección de amenazas proporcionando actualizaciones en tiempo real sobre tácticas, técnicas y vulnerabilidades de los atacantes.
- **Nexus Relationship Graph (RG)** supervisa el comportamiento de los usuarios en todos los sistemas, en busca de anomalías que indiquen amenazas internas o compromiso de cuentas.
- **Nexus Machine Learning (ML)** potencia nuestra detección predictiva de amenazas.
- **Nexus Computer Vision (CV)** detecta y neutraliza las amenazas ocultas en elementos visuales, como en sitios de phishing, códigos QR, archivos adjuntos maliciosos y mensajes falsificados.

Razón 2

Consiga el SOC más eficiente

Cuanto más tiempo permanezca una amenaza en su entorno de Microsoft 365, mayor será el daño que puede provocar. Esa es la razón por la que una respuesta rápida y eficaz es absolutamente fundamental para garantizar la seguridad de Microsoft 365.

La API Proofpoint Core Email Protection automatiza la protección del correo electrónico y proporciona flujos de trabajo de alta eficacia para los equipos de los SOC. Esto garantiza que puedan centrarse en sus tareas más importantes.

Así es como Proofpoint agiliza el SOC:

- **Automatiza la detección, corrección y respuesta a las amenazas por correo electrónico.** Esto reduce el volumen de amenazas por correo electrónico que los equipos tienen que investigar.
- **Proporciona avisos contextuales y formación en tiempo real.** Los mensajes de advertencia y la orientación ayudan a los usuarios a tomar decisiones de seguridad informadas. Los administradores ahorran tiempo al reducir el número de eventos que hay que analizar y corregir.
- **Presenta breves resúmenes de las amenazas.** Los equipos obtienen un resumen intuitivo de los puntos más importantes de cada amenaza, creado por IA generativa.
- **Acelera la caza de amenazas y su corrección.** La búsqueda integrada y los flujos de trabajo basados en alertas ayudan a los equipos a detectar rápidamente las amenazas adecuadas y a corregirlas antes de que puedan causar daños.
- **Se despliega rápidamente.** Nuestra solución está integrada con la API de Microsoft Graph y tiene un período de aprendizaje automatizado de menos de 48 horas.

Razón 1

Razón 2 ●

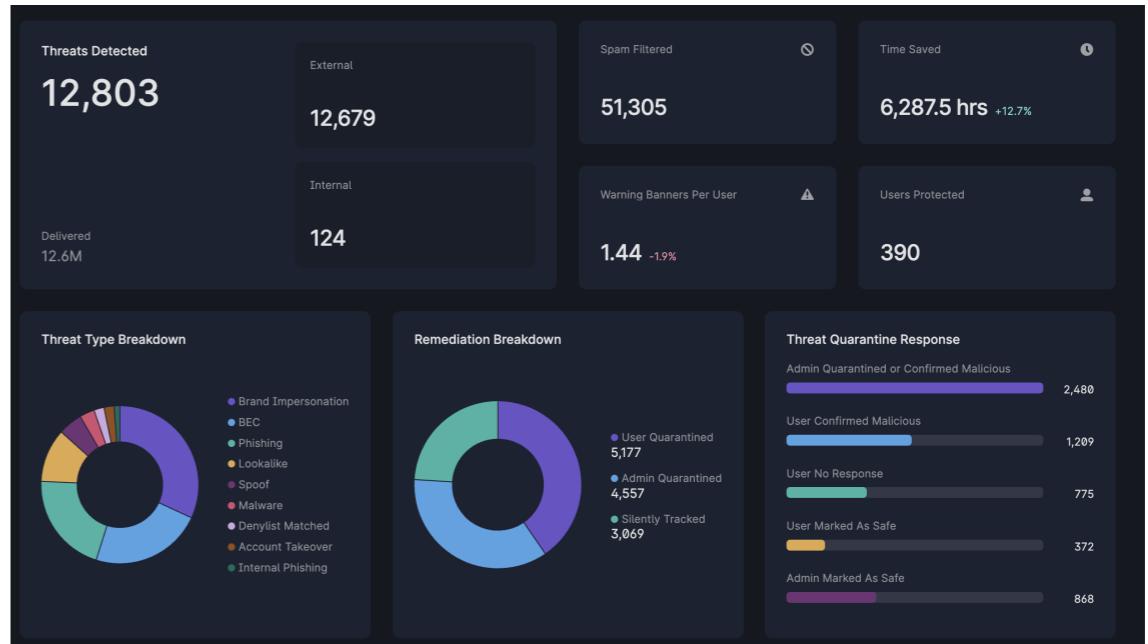
Razón 3

Razón 4

Razón 5

Trabaje con un líder del sector

Los pasos siguientes



Cuando elige Proofpoint

El **99,99 %** de las amenazas por correo electrónico se detienen antes de que se conviertan en un peligro

El SOC debe gestionar un **30 %** menos de amenazas por correo electrónico

Razón 3

Protéjase contra las amenazas actuales más evasivas

Las amenazas por correo electrónico evolucionan constantemente y son difíciles de defender. Por eso, proteger a sus empleados es una tarea de enormes proporciones, incluso para las empresas más sofisticadas. Afortunadamente, Proofpoint puede ayudarle.

Gracias a la API de Proofpoint Core Email Protection, puede identificar y bloquear amenazas conocidas y desconocidas en toda la empresa. Esto significa que las amenazas avanzadas se detienen en la puerta de entrada, no después de que lleguen. Estas amenazas son:

Phishing, URL maliciosas y malware

Los ciberdelincuentes siguen enviando un aluvión de enlaces y archivos adjuntos maliciosos por correo electrónico, que solo pueden detenerse con protecciones avanzadas del correo electrónico.

Proofpoint utiliza el análisis en entorno aislado (sandbox), la extracción de URL, la detección de evasiones, el aislamiento del navegador y una amplia variedad de las técnicas avanzadas para lograr la máxima eficacia en la defensa contra payloads maliciosas.

Ataques BEC

Los ataques de suplantación sin carga útil, como los ataques BEC se encuentran entre los más difíciles de detectar debido a su aparente legitimidad.

Los motores Proofpoint Nexus AI analizan las relaciones y el lenguaje de los usuarios, además de buscar otros indicadores de amenazas potenciales. Los desajustes en los atributos de los encabezados, los bucles de retroalimentación DMARC y el comportamiento de los remitentes proporcionan información valiosa que utilizamos para detener en seco las amenazas BEC.

Amenazas TOAD

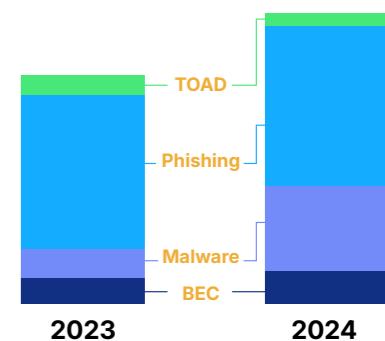
En los ataques por teléfono o TOAD (Telephone-Oriented Attack Delivery), también conocidos como phishing de devolución de llamadas, los ciberdelincuentes envían correos electrónicos que intentan persuadir a los destinatarios para que llamen a un falso centro de llamadas. Estas amenazas pueden ser difíciles de detectar, ya que rara vez contienen cargas virales maliciosas.

Los motores Proofpoint Nexus AI utilizan el aprendizaje automático y la visión por ordenador para buscar indicadores de amenazas conocidas con el fin de bloquearlas (números de teléfono y códigos QR maliciosos, suplantaciones de identidad basadas en imágenes, etc.).

+45,8 %

de aumento interanual de las amenazas* enviadas a los usuarios

*Mensajes maliciosos, detectados por Proofpoint



Razón 1

Razón 2

Razón 3 ●

Razón 4

Razón 5

Trabaje con un líder del sector

Los pasos siguientes

124 M

Número de ataques BEC que blokea Proofpoint al mes

45 %

Aumento anual de las amenazas por correo electrónico enviadas a los usuarios finales

9 M

Número de ataques TOAD que blokea Proofpoint al mes

Razón 4

Obtenga la mejor experiencia de usuario

Cuando se trata de proteger el correo electrónico, la mejor experiencia que se puede ofrecer a los usuarios es que sea invisible. Nuestra tasa de detección es del 99,99 %. Proofpoint minimiza las distracciones de los usuarios ante amenazas, spam y correo gris.

Con la API de Proofpoint Core Email Protection, puede proporcionar a los usuarios:

- Una experiencia de usuario nativa de Outlook para el spam y el correo gris.
- Menos interrupciones gracias a una eficacia de detección líder en el sector y una reparación rápida.
- Advertencias contextuales para formar a los usuarios en tiempo real.

Ofrezca experiencias de usuario nativas de Outlook

Los usuarios de hoy en día están abrumados por el volumen de correos electrónicos que reciben

a diario. Proofpoint reduce el ruido moviendo automáticamente el spam y el correo gris de la bandeja de entrada a la carpeta de correo no deseado predeterminada de Microsoft.

Los usuarios pueden arrastrar y soltar los mensajes que deseen a su bandeja de entrada. Esto evita que los correos electrónicos de esos remitentes se marquen como spam o correo gris en el futuro.

Garantice la productividad de los usuarios y de los equipos de seguridad

La API de Proofpoint Core Email Protection ayuda a los empleados a mantener su productividad enviando correos electrónicos de riesgo bajo-medio de forma segura. Estos mensajes incluyen formación en tiempo real para ayudar a los usuarios a tomar decisiones de seguridad informadas y aprender de sus errores. El resultado es una reducción del número de eventos que hay que analizar y corregir.

Action required: your email is quarantined [TS-Alert ID: 64788ac0cb864956-x]

AS Acme Security To: Frederick Price Fri 2024-02-16 15:37

Be careful: possible impersonation detected

- Possible impersonation: The sender's domain, "@firstcorp-mail.com", looks like "firstcorp.com", which your organization interacts with
- Sense of urgency: Common technique used in email fraud
- Financial request: Common technique used in email fraud

Report and Delete **Release to Inbox**

SUSPICIOUS EMAIL PREVIEW - LINKS AND ATTACHMENTS DISABLED

Sent Feb 16 2024 15:37
Sender lisa.williams@firstcorp-mail.com
Recipient(s) Frederick Price <frederick.price@rotepads.com>
Subject Important: Bank Details Changed!
Attachments account_details.pdf

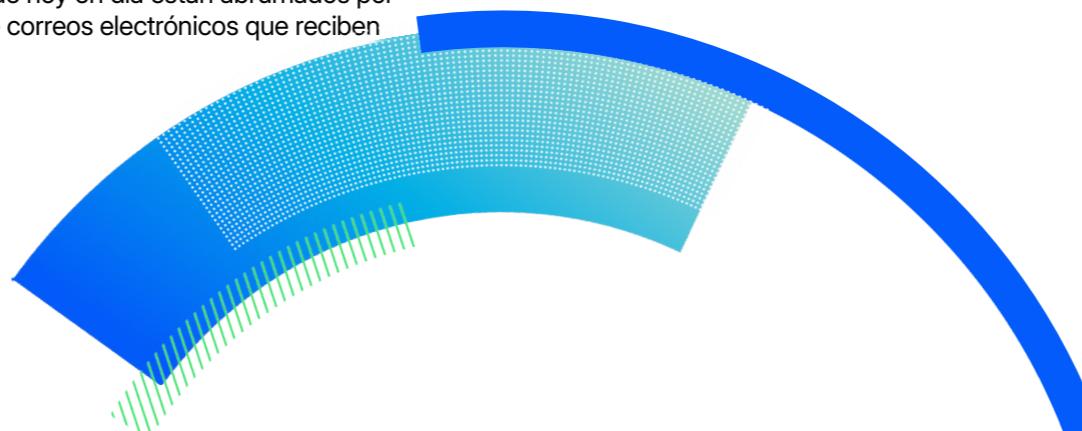
Hi Fred,

We'd like to inform you that our bank details have changed. Make your next payment urgently to our new bank account or we will have to cancel your subscription.

Best,
Lisa Williams, CEO, FirstCorp

Reply **Forward**

Formación de usuarios en tiempo real sobre mensajes sospechosos



Razón 5

Diseñe una arquitectura de seguridad atemporal

Proofpoint le ayuda a reducir el riesgo en todos los lugares en los que interactúan sus empleados, hoy y en el futuro. Protegemos su organización de los atacantes que suplantan la identidad de sus empleados, partners y proveedores, y evitamos la pérdida de datos tanto

accidental como intencionada. Además, nos integramos con una amplia gama de herramientas para ayudarle a automatizar y consolidar toda su pila de seguridad.

Nuestra plataforma se integra con los mejores proveedores de seguridad, como Palo Alto Networks, Okta, CrowdStrike y muchos más.

Razón 1

Razón 2

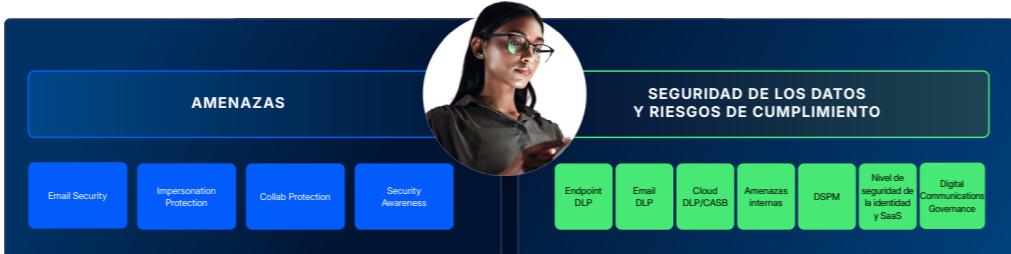
Razón 3

Razón 4

Razón 5 ●

Trabaje con un líder del sector

Los pasos siguientes



Consolide proveedores para mejorar su rentabilidad

Cuando elige Proofpoint para reforzar la seguridad de Microsoft 365, también obtiene acceso a nuestras soluciones integrales que no solo se limitan a la protección de su organización frente a los ataques por correo electrónico. Esto significa que puede proporcionar a su equipo herramientas de vanguardia para agilizar sus flujos de trabajo.

Con Proofpoint, obtendrá una seguridad que se extiende a su personal, sus datos y toda su organización.

Bloquee amenazas contra los usuarios

- Proteja el correo electrónico contra malware, phishing y ataques BEC.
- Impida los ataques de suplantación de la identidad y de compromiso de proveedores.
- Proteja las herramientas de colaboración contra los ataques de robo credenciales y el malware.

Proteja sus datos y las comunicaciones digitales

- Evite que sus usuarios pongan en peligro los datos por error.
- Detecte actividades internas maliciosas y reciba alertas en tiempo real.
- Controle todas sus comunicaciones digitales.

Oriente a sus empleados para elegir mejores opciones de seguridad

- Ofrezca formación personalizada basada en los riesgos.
- Simule ataques para evaluar la resiliencia de sus usuarios.
- Fomente el comportamiento adecuado con sugerencias en tiempo real a través del correo electrónico y la web.

Controle la proliferación de aplicaciones SaaS e identidades

- Detecte y responda rápidamente a las usurpaciones de cuentas.
- Siga y comprenda de forma proactiva las rutas de ataque a través de Active Directory.
- Detecte cuentas de software como servicio (SaaS) y revierta desviaciones en el nivel de seguridad.

Razón 1

Razón 2

Razón 3

Razón 4

Razón 5

Trabaje con un ●
líder del sector

Los pasos siguientes

Trabaje con un líder del sector

Con Proofpoint, no tiene que elegir entre la mejor tecnología y una solución totalmente integrada. Somos líderes reconocidos del sector en ciberseguridad, prevención de la pérdida de datos (DLP) y cumplimiento de normativas.

Reconocimiento de los analistas del sector de Proofpoint Core Email Protection

GARTNER
Líder
Magic Quadrant 2024 para plataformas de protección del correo electrónico

N.º 1 en 4 de los 5 casos de uso
En el Magic Quadrant 2024 para plataformas de protección del correo electrónico:
- Protección básica del correo electrónico - Seguridad del correo saliente
- Plataformas de seguridad - Usuarios avanzados

FORRESTER®
El informe The Forrester Wave™:
Enterprise Email Security, 2.º trimestre de 2023 | Líder

FROST & SULLIVAN
Frost Radar™ 2023:
Email Security, 2023: Líder en crecimiento e innovación en el mercado de la seguridad del correo electrónico en el Frost Radar™ por 9º año consecutivo

2024 Frost & Sullivan
Premio a la empresa del año | Sector de la seguridad del correo electrónico global y a la excelencia en las mejores prácticas

Frost & Sullivan 2025
Premio a la empresa del año | Sector de la seguridad del correo electrónico australiano y excelencia en las mejores prácticas

GIGAOM
GigaOm Radar 2023 para Anti-Phishing:
Incluido como líder y agente de cambio acelerado (Fast Mover)

GigaOm Radar 2024 para detección y respuesta a amenazas para la identidad:
Incluido como líder y agente de cambio acelerado (Fast Mover)

GigaOm Radar 2024 para tecnología de engaño:
Incluido como líder y agente de cambio acelerado (Fast Mover)

KUPPINGERCOLE ANALYSTS
Leadership Compass 2023 en seguridad para el correo electrónico:
Liderazgo en las cuatro categorías: general, producto, innovación y mercado

OMDIA
Omdia Universe 2024 - Seguridad del correo electrónico:
Líder

RAIDATI
Market Quadrant de Radicati 2024 para seguridad del correo electrónico:
Actor principal (Top Player)

© 2025 Proofpoint, Inc.



Los siguientes pasos

Razón 1

La mejor ciberdefensa es la que detiene las amenazas donde se inician. Esa es la razón por la que más de 1,8 millones de clientes en todo el mundo nos han elegido como su partner de seguridad.

Razón 2

La API Proofpoint Core Email Protection bloquea el 99,99 % de las amenazas distribuidas por correo electrónico, spam y correo gris. Nuestra pila de detección multicapa Proofpoint Nexus combina gráficos relacionales, aprendizaje automático, visión por ordenador y análisis semántico. Se optimiza mediante los datos sobre amenazas de más de 3 billones de correos electrónicos analizados cada año. Por lo tanto, puede prevenir la mayoría de las amenazas avanzadas actuales.

Razón 4

La API Proofpoint Core Email Protection hace algo más que bloquear amenazas. También ayuda a los equipos de seguridad, que se benefician de flujos de trabajo optimizados basados en alertas y de la búsqueda integrada. Además, los mensajes de correo electrónico notificados por los usuarios se corrigen automáticamente, y los usuarios reciben formación en tiempo real cada vez que informan de un correo electrónico sospechoso.

Obtenga más información sobre cómo Proofpoint puede ayudarle a reforzar la seguridad del correo electrónico y web de Microsoft 365.

proofpoint.com/es/products/threat-defense

Trabaje con un
líder del sector

Los pasos siguientes ●

Acerca de Proofpoint

Protección de las personas

3,4 billones	>1,4 billones	124 M	>183 M		
de mensajes analizados al año	de SMS/MMS analizados al año	de ataques BEC detenidos al mes	de simulaciones de phishing al año		
0,8 billones	21 billones	177 M			
de adjuntos analizados al año	de URL analizadas al año	de ataques TOAD detenidos al año			

Adopción en el mercado

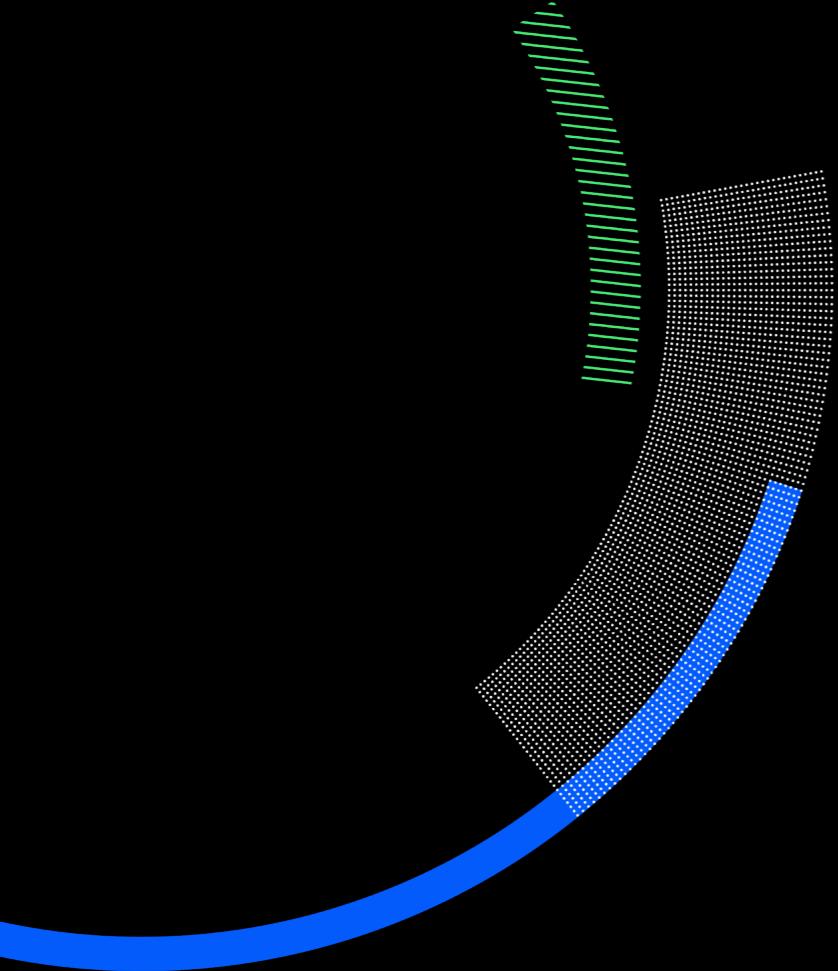
+1,88 M +150
de clientes

ISP y operadoras móviles en todo el mundo

85 %
de empresas F100 protegidas por Proofpoint

50 %
de empresas F100 usan Proofpoint DLP

> 60 %
de empresas F1000 protegidas por Proofpoint



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. Organizaciones líderes de todos los tamaños, entre las que se encuentran el 85 % de las empresas Fortune 100, confían en las soluciones de Proofpoint para su seguridad centrada en las personas y su cumplimiento normativo, mitigando los riesgos más críticos en sus sistemas de correo electrónico, cloud, redes sociales y web. Encontrará más información en www.proofpoint.com/es.

Conecte con Proofpoint: [LinkedIn](#)

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

DESCUBRA LA PLATAFORMA DE PROOFPOINT →