proofpoint.

GUÍA DE COMPRA

Cómo elegir la mejor solución de protección del correo electrónico para su organización

Funciones principales

Estas son las funciones clave que debe tener en cuenta cuando piense en adoptar una solución moderna de protección del correo electrónico:

1. Protección frente a la mayor variedad de amenazas
2. Detección y respuesta automatizadas
3. Opciones de despliegue flexibles
4. Una excelente experiencia de usuario
5. Protección más allá del correo electrónico

Descripción general

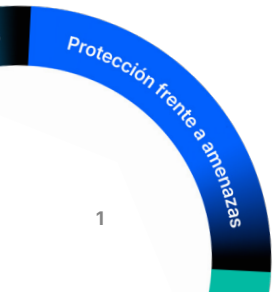
El correo electrónico sigue siendo uno de los principales vectores de ciberamenazas. En los últimos años, sin embargo, la superficie de ataque se ha ampliado más allá del correo electrónico, ya que los usuarios utilizan ahora múltiples canales digitales para comunicarse y colaborar. Así que no es de extrañar que los ciberdelincuentes sigan su ejemplo y se aprovechen de esta tendencia. De hecho, tienen más éxito que nunca en la distribución de una amplia variedad de amenazas centradas en las personas a través de todos los canales digitales.

Para responder, las organizaciones aglutinan una amalgama de productos aislados y especializados para neutralizar estas amenazas.

Por desgracia, esta estrategia deja lagunas en la defensa y pasa por alto muchos riesgos. Además, gestionar e integrar distintas herramientas de seguridad es complicado y costoso. Para evitar estos escollos, las organizaciones necesitan una solución integral de protección del correo electrónico, capaz de defenderlas frente a las amenazas actuales y emergentes centradas en las personas, en forma de plataforma única.

En esta guía, destacamos las características clave que son esenciales para una solución de protección del correo electrónico de alto rendimiento, y por qué son tan importantes.

Figura 1: Distribución de los tipos de amenazas enviadas por correo electrónico.



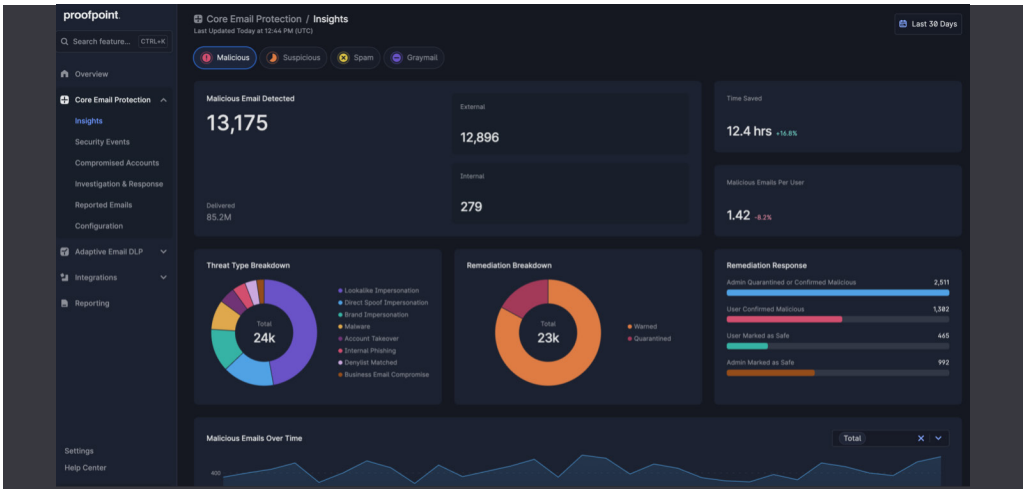


Figura 2: Vista completa de las amenazas por correo electrónico bloqueadas por Proofpoint Core Email Protection.

55 000 M$

Pérdidas por ataques BEC entre 2013 y 2023 en todo el mundo[2].

60 segundos

Tiempo medio que tarda un usuario en caer en la trampa de un correo electrónico de phishing[3].

1: Protección frente a la mayor variedad de amenazas

El coste medio de una fuga de datos causada por un ataque de phishing o Business Email Compromise (BEC) es de 4,88 millones de dólares[1]. Se trata del segundo mayor coste de incidente, después de los ataques de usuarios internos malintencionados. Y cada amenaza que consigue superar las defensas de la red genera pérdidas financieras y afecta negativamente la imagen de la empresa.

Los equipos de seguridad trabajan intensamente para minimizar al máximo la exposición de la empresa a ciberriesgos. La única manera de lograr este objetivo es bloquear el mayor número posible de amenazas.

Estos son los criterios que debe cumplir una solución de protección del correo electrónico:

- **Uso de inteligencia de amenazas en tiempo real.** La inteligencia de amenazas actualizada al minuto permite identificar y anticipar las amenazas emergentes con mayor rapidez y precisión. Sin embargo, la inteligencia de amenazas no se limita a los datos, también debe contar con la participación de equipos de investigación con un alto nivel de especialización. Si una solución cuenta con estos dos aspectos clave, es capaz de identificar y analizar tendencias a gran escala con mayor velocidad y eficacia. Por ejemplo, puede detectar y rastrear ciberdelincuentes y agentes estatales sofisticados, e identificar cambios en el panorama de amenazas.
- **Uso de la IA para detectar amenazas.** Para bloquear los ataques por correo electrónico que se basan en la manipulación combinada con payloads es esencial una pila de detección multicapa impulsada por IA. Esto incluye grandes modelos de lenguaje (LLM), gráficos relacionales y de comportamiento, aprendizaje automático y capacidad de análisis de imágenes. Estas funciones ayudan a bloquear las amenazas a gran escala.
- **Supervisión continua de amenazas.** Es fundamental contar con la capacidad de analizar URL y archivos adjuntos en entorno aislado, pero el *momento* en el que se realiza el análisis es igual de importante. Para identificar los ataques que han eludido las defensas o las amenazas con activación retardada, es necesario adoptar una solución que detecte y bloquee las amenazas durante todo su ciclo de vida: antes de la entrega, después de la entrega y en el momento de hacer clic.
- **Visibilidad de los usuarios atacados.** Debe identificar a las personas a las que se dirigen los ataques y los métodos que utilizan los ciberdelincuentes, así como determinar si han caído en la trampa. Igualmente, es importante conocer la forma en que son objetivo de los ataques, a qué datos tienen acceso y si suelen caer en la trampa de estos ataques. Con esta información, podrá adoptar las medidas de protección adecuadas en el momento oportuno.

Cuanto antes se detecten las amenazas, más segura estará su organización. Además, sus equipos de TI y de seguridad ya no tendrán que dedicar su valioso tiempo a la respuesta y corrección de incidentes.

1. IBM. "Cost of a Data Breach Report" (Informe sobre el coste de las fugas de datos), 2024.
2. FBI. "Business Email Compromise: The $55 Billion Scam" (Business Email Compromise: el timo de los 55 000 millones de dólares), septiembre de 2024.
3. Verizon. "Data Breach Investigation Report"(Informe sobre las investigaciones de fugas de datos). 2024.

2: Detección y respuesta automatizadas

Los mensajes maliciosos que llegan a las bandejas de entrada o que denuncian los usuarios pueden acaparar el tiempo de los equipos de seguridad y afectar negativamente a su productividad. El análisis y la eliminación manual de estas amenazas requieren mucho tiempo. Es esencial detectar y responder rápidamente a estas amenazas. Esta rápida actuación puede marcar la diferencia entre un incidente menor y un compromiso a gran escala.

Estos son los criterios que debe cumplir una solución de protección del correo electrónico:

- **Buzón de correo malicioso optimizado por IA.** Los mensajes denunciados por los usuarios deben examinarse lo antes posible. Cuando se dirigen automáticamente a una bandeja de entrada supervisada por una máquina, pueden ser analizados por la IA y neutralizados sin ninguna intervención de su equipo de TI o de seguridad. También debe haber un sistema de respuesta automática que informe los usuarios de que se han recibido sus denuncias. De esta forma se cierra el ciclo de retroalimentación y se refuerza el comportamiento positivo.
- **Orquestación y corrección automatizadas.** En ningún caso debe permitirse que correos electrónicos maliciosos permanezcan en las bandejas de entrada de los usuarios; deberían eliminarse automáticamente de las bandejas de entrada de toda la organización. También debe asegurarse de que la solución se integra fácilmente con sus herramientas SIEM/SOAR existentes. Esto le proporciona una visión más unificada de su ecosistema de seguridad.
- **Flujos de trabajo simplificados.** Las herramientas de seguridad deben facilitar el trabajo de los analistas. Por lo tanto, los flujos de trabajo intuitivos y los resúmenes claros de amenazas generados por IA son esenciales para optimizar la productividad. Funciones como la búsqueda integrada y las alertas priorizadas pueden ayudarles a localizar rápidamente las amenazas. Lo mismo ocurre con las herramientas que agilizan las medidas correctivas que deben aplicarse tras las acciones automatizadas.

Cuando la eficacia de su equipo de seguridad mejora, también lo hacen sus defensas. Además, podrá sacar el máximo partido de sus recursos e inversiones en seguridad.

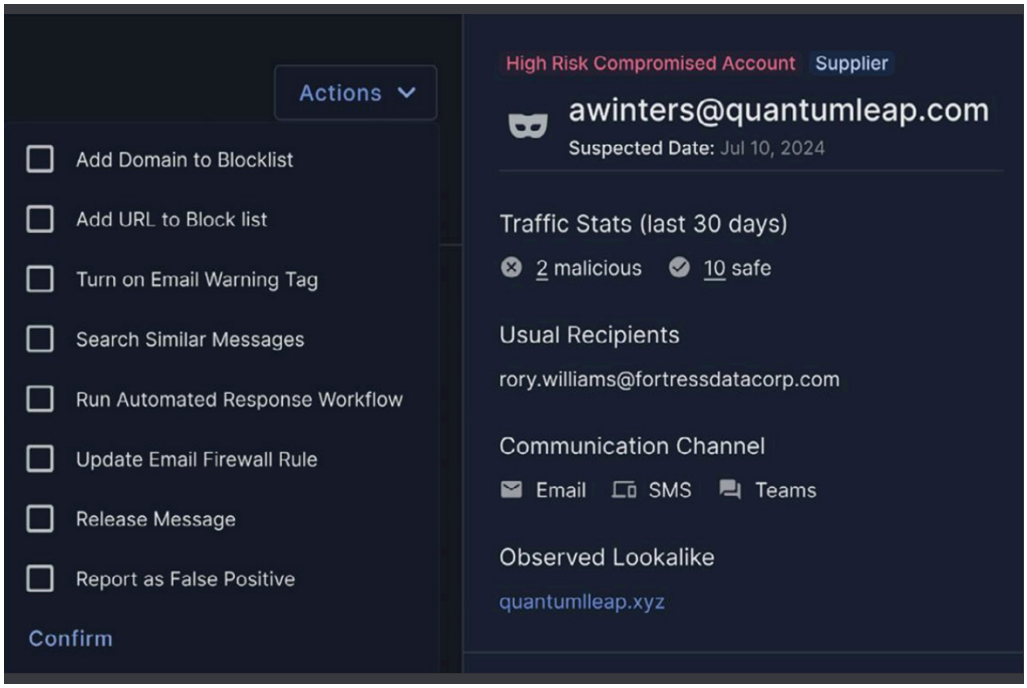


Figura 3: Ejemplo de flujos de trabajo automatizados de detección y respuesta de Proofpoint Core Email Protection.

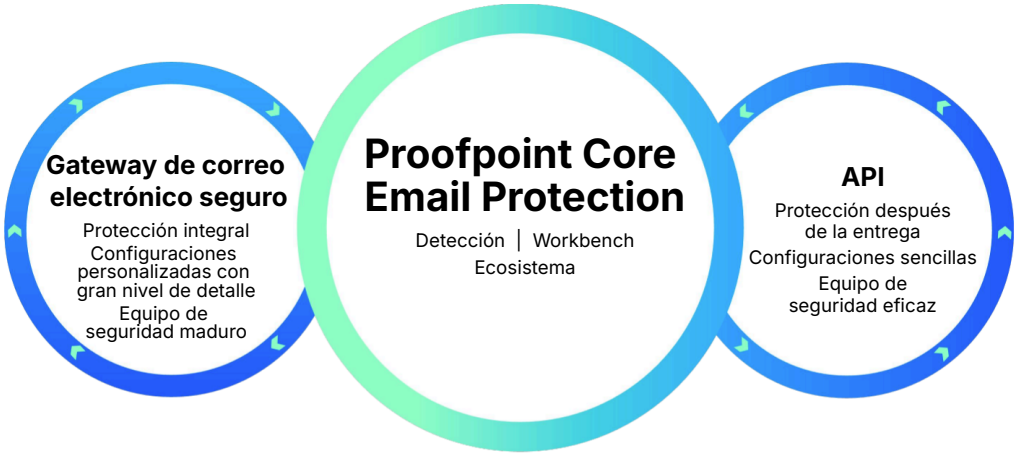


Figura 4: Ventajas del despliegue mediante API y gateway del correo electrónico seguro con Proofpoint Core Email Protection.

3: Opciones de despliegue flexibles

Su arquitectura, prioridades de seguridad y requisitos de cumplimiento están en constante evolución. Una solución de seguridad para el correo electrónico debe poder evolucionar y ajustarse a sus necesidades. Aunque el despliegue de API es actualmente el mejor enfoque, puede que no lo sea en el futuro. No limitarse a un único enfoque de despliegue permite optimizar la cobertura de seguridad adaptándola eficazmente a los distintos riesgos.

Cuando sus equipos de TI y seguridad tienen la libertad de elegir, pueden evolucionar y fortalecer sus defensas, asegurando que sigan siendo efectivas a largo plazo. Y su empresa seguirá contando con una protección robusta y adaptada a su crecimiento.

Estas son las características a tener en cuenta:

- **Despliegue de gateway de correo electrónico seguro (SEG).** Los gateway de correo electrónico seguros ofrecen una protección completa para muchos tipos de entornos. Esta es la opción recomendada para quienes desean una protección del correo electrónico totalmente personalizable. Los gateway de correo electrónico seguros le permiten maximizar su protección de extremo a extremo con protección antes de la entrega, después de la entrega y al hacer clic. Ofrecen opciones de configuración flexibles, así como visibilidad de los riesgos relacionados con las personas.
- **Despliegue basado en API.** Esta opción ofrece una incorporación sencilla y controles predefinidos dentro de plataformas de nube como Microsoft 365. El despliegue puede completarse en solo unos minutos. Esta es la opción ideal si busca una protección potente para el correo electrónico que requiera mínima configuración, junto con una gestión muy automatizada que ofrece información clara sobre amenazas y acciones correctivas automáticas.

Si elige un proveedor que ofrezca opciones de despliegue flexibles, contará con el tipo de detección que necesita, al mismo tiempo que asegura la durabilidad y evolución de su sistema de seguridad.

74 %

Porcentaje de CISO que consideran que el factor humano es la mayor vulnerabilidad de su empresa[4].

40 %

La concienciación en materia de seguridad puede reducir la tasa de clics sobre amenazas reales en más de un 40 % en menos de seis meses[5].

4: Una excelente experiencia de usuario

Hay un dicho que afirma que el mayor riesgo y la mejor detección se encuentran en el mismo lugar: entre la silla y el teclado. Para bloquear los mensajes maliciosos, los usuarios necesitan las herramientas adecuadas.

Si se sienten abrumados, es más probable que ignoren las amenazas reales o cometan errores. El spam, el correo gris y las constantes falsas alertas aumentan este riesgo. Los empleados necesitan advertencias claras y prácticas, herramientas de información intuitivas y simulaciones de phishing bien diseñadas para reforzar los comportamientos de seguridad positivos.

Estos son los criterios que debe cumplir una solución de protección del correo electrónico:

- **Detección de spam y correo gris.** El spam y los correos masivos atascan las bandejas de entrada y distraen a los usuarios. Incluso el correo gris, como los mensajes comerciales no solicitados, puede afectar negativamente a la productividad. La protección del correo electrónico garantiza la integridad y mantiene las bandejas de entrada limpias, optimizando la experiencia del usuario y facilitando que los empleados mantengan la concentración.
- **Avisos a los usuarios de mensajes sospechosos.** Los correos sospechosos pueden ser tanto maliciosos como legítimos, y solo el usuario está capacitado para discernir entre ambos. Las notificaciones con vista previa contextual alertan a los usuarios de los indicios de amenaza identificados en los mensajes. Al mismo tiempo, neutralizan de forma automática cualquier adjunto o enlace URL malicioso vinculado al mensaje sospechoso, requiriendo que el usuario interactúe con la notificación antes de acceder al contenido del correo electrónico.
- **Protección al hacer clic.** Incluso los empleados bienintencionados pueden cometer el error de hacer clic en una amenaza cuando están muy ocupados. Las protecciones al hacer clic, como los banners de advertencia, permiten a los usuarios pararse y pensar antes de actuar. Además, las ventanas virtuales del navegador añaden una capa adicional de protección para evitar el robo de datos de acceso y la descarga de programas maliciosos.
- **Concienciación personalizada en materia de seguridad.** Las simulaciones de phishing y la formación en concienciación suelen ser el principal punto de contacto entre los empleados y las soluciones de protección del correo electrónico. Las herramientas de formación más eficaces ofrecen aprendizaje en tiempo real cuando los usuarios hacen clic en un mensaje de phishing. También ofrecen módulos pequeños interactivos, adaptados al nivel de conocimientos de cada usuario. Este enfoque personalizado fortalece la concienciación y promueve comportamientos seguros a largo plazo.

Una experiencia de usuario coherente ayuda a sus usuarios a mantenerse alerta mientras realizan sus tareas.

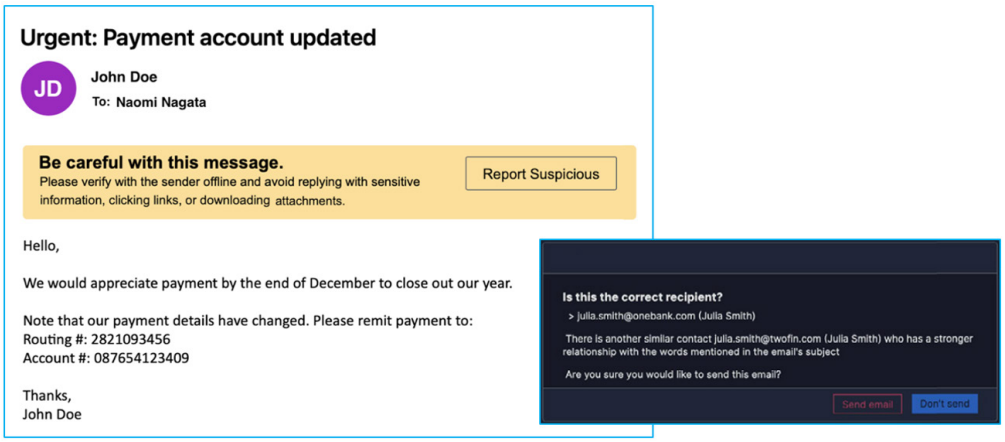


Figura 5: Ejemplo de un mensaje de alerta que indica un posible error del destinatario y el correspondiente banner de advertencia de correo electrónico que aparece.

4. Proofpoint. *Voice of the CISO.* 2024.
5. Investigación de Proofpoint ZenGuide.

2524 %

Aumento del número de URL maliciosas distribuidas mediante phishing en mensajes SMS en los últimos tres años[6].

5: Protección más allá del correo electrónico

Con la ampliación de los espacios de trabajo digitales, es importante contar con una plataforma adaptable. Debe ser capaz de proteger no solo el correo electrónico, sino también los nuevos canales de comunicación digital. Los ciberdelincuentes ya no limitan sus ataques al correo electrónico. Han seguido a los usuarios hasta plataformas como Microsoft Teams, Slack, Zoom, LinkedIn y WhatsApp, que son nuevos vectores de ataque.

Para que una solución esté preparada para el futuro, debe incluir protecciones avanzadas adicionales, como la autenticación de correo electrónico DMARC, la detección fiable de cuentas cloud comprometidas y la visibilidad de las amenazas del correo electrónico de los proveedores.

Otros factores a tener en cuenta:

- **Autenticación simplificada del correo electrónico.** Una de las formas más eficaces de combatir los correos electrónicos fraudulentos es utilizar la autenticación del correo electrónico tanto en los mensajes entrantes como en los salientes. Para proteger su imagen de marca, busque un proveedor que ofrezca servicios gestionados o alojados para agilizar el despliegue de la autenticación. El asesoramiento de expertos puede ser de gran ayuda cuando se trata de la autenticación DMARC.
- **Detección de cuentas comprometidas.** La combinación de la visibilidad de las amenazas del correo electrónico (como los clics reales en los mensajes de phishing) con las alertas CASB garantiza una detección más precisa de las cuentas comprometidas. Esto reduce el número de falsos positivos y permite aplicar respuestas automatizadas, como obligar a restablecer las contraseñas o impedir que se compartan archivos confidenciales.
- **Protección contra el phishing más allá del correo electrónico.** Las URL maliciosas son ahora el vector de ataque más común, en parte porque pueden enviarse a través de cualquier canal, incluida la mensajería instantánea, las herramientas de colaboración y los medios sociales. Opte por una solución capaz de analizar las URL en tiempo real, para que los enlaces maliciosos se bloqueen donde y cuando los usuarios intenten acceder a ellos.
- **Limitación del riesgo asociado a los proveedores.** Sin una visibilidad adecuada, resulta complicado identificar las amenazas presentes en su cadena de suministro. Las soluciones de protección del correo electrónico que integran la evaluación del riesgo asociado a los proveedores pueden asignar puntuaciones precisas y detectar cuentas comprometidas, fortaleciendo así la defensa contra el fraude y mejorando la seguridad general del sistema. Combinado con la autenticación, este enfoque proactivo fortalece la protección frente a uno de los vectores de ataque más complejos de detectar.

Gracias a estas funciones, sus equipos podrán gestionar eficazmente las amenazas nuevas y emergentes, sea cual sea su origen.

6. Investigación de Proofpoint

Conclusión

Más del 94 % de las amenazas dirigidas contra sus empleados se distribuyen a través del correo electrónico[7], por lo que es esencial una protección sólida de este vector prevalente.

Para optimizar su defensa contra las amenazas, busque una solución completa de protección del correo electrónico, que incluya medidas básicas y avanzadas. Debe ser capaz de detectar y responder a las amenazas automáticamente, además de ofrecer una experiencia de usuario óptima. Lo ideal es que la solución ofrezca opciones de despliegue flexibles que se adapten a sus necesidades cambiantes. También debe proteger otros canales digitales además del correo electrónico, como las herramientas de colaboración, las plataformas de mensajería instantánea y las aplicaciones cloud.

¿Utiliza un mosaico de soluciones especializadas y fragmentadas? Si es así, puede mejorar la protección de su correo electrónico. Ha llegado el momento de evaluar la eficacia de sus dispositivos de seguridad actuales frente a todas las amenazas centradas en las personas, para el correo electrónico y para muchos otros vectores.

Proofpoint ofrece seguridad centrada en las personas

Proofpoint Core Email Protection Proofpoint permite a su organización reducir los riesgos en todos los puntos de interacción con personas, ahora y en el futuro.

Proofpoint Core Email Protection detiene el 99,99 % de las amenazas del correo electrónico antes de que se conviertan en un peligro. Basada en nuestra avanzada pila de detección impulsada por inteligencia artificial Proofpoint Nexus, líder del sector, esta solución identifica y neutraliza amenazas avanzadas en el correo electrónico, incluyendo phishing, estafas BEC, malware, ransomware, usurpación de cuentas, suplantaciones de identidad, ingeniería social y mucho más. Con su consola moderna e intuitiva, los analistas de seguridad ganan en eficacia gracias a la visibilidad completa de las amenazas y a los flujos de trabajo de corrección automatizados. La solución cuenta con una arquitectura diseñada para adaptarse al panorama de amenazas futuras, ofreciendo opciones de despliegue flexibles, como API y gateway del correo electrónico seguro, que garantizan un despliegue ágil y escalable.

Por eso, más de dos millones de clientes, incluido el 85 % de la lista Fortune 100, confían en las soluciones de seguridad centradas en las personas de Proofpoint para proteger a sus usuarios y su empresa.

Para obtener más información, póngase en contacto con nuestro equipo de ventas en la dirección sales@proofpoint.com.

7. Investigación de 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

DESCUBRA LA PLATAFORMA DE PROOFPOINT →

0203-010-06-02