proofpoint.

RESUMEN DE LA SOLUCIÓN

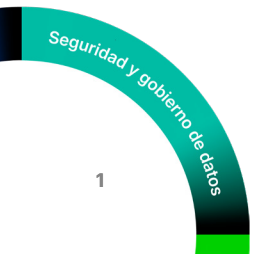
# Proofpoint Insider Threat Management

Proteja su organización contra los usuarios internos de riesgo

## Ventajas principales

- Protección contra daños financieros y a la marca causados por usuarios internos negligentes, maliciosos y comprometidos
- Detección proactiva de comportamientos de riesgo con visibilidad detallada de los indicadores de comportamiento
- Aceleración de las investigaciones con pruebas irrefutables
- Colaboración eficaz con RR. HH., el departamento legal y otras partes interesadas
- Protección de la privacidad de los usuarios y garantía de objetividad durante las investigaciones
- Rápida rentabilización, gracias a la facilidad de despliegue y a un agente de endpoint ligero

Este conjunto de soluciones forma parte de la plataforma Human-Centric Security de Proofpoint, que mitiga las cuatro áreas clave de riesgos basados en las personas.




Las plantillas modernas y distribuidas trabajan desde absolutamente cualquier lugar. Tanto los empleados como el personal externo y los contratistas tienen acceso a más datos que nunca, ya sea en sus dispositivos, en el correo electrónico o en la nube. Los cambios corporativos, como las fusiones y adquisiciones, las desinversiones y las reestructuraciones, causan incertidumbre que puede desencadenar amenazas internas. Además, las tensiones geopolíticas y económicas fomentan el ciberespionaje por parte de usuarios internos.

Estas dinámicas aumentan el riesgo de amenazas internas que podrían acabar en robo de secretos comerciales y propiedad intelectual, fraude, espionaje y sabotaje del sistema. Todos estos resultados pueden provocar daños materiales, financieros, de reputación y estratégicos a una organización. Para afrontar con eficacia las amenazas internas, los equipos de seguridad necesitan información del contexto de los comportamientos de riesgo.

Proofpoint Insider Threat Management (ITM) ofrece una visibilidad integral de los usuarios negligentes, maliciosos y comprometidos, y ayuda a los equipos de seguridad a identificar comportamientos de riesgo e investigar incidentes de origen interno de manera eficiente. Proofpoint ITM facilita un enfoque centrado en las personas, con información detallada sobre el comportamiento y las intenciones del usuario. Permite configurar políticas, filtrar alertas, buscar amenazas y responder a los incidentes desde una consola centralizada. Gracias a las pruebas forenses, puede investigar las vulneraciones de seguridad internas de manera rápida y eficaz. Cuanto más rápido se resuelva un incidente, menor será el impacto en la empresa, así como en su reputación y sus ganancias.

## Reducción proactiva del riesgo de seguridad

### Visión integral del riesgo humano

Las amenazas internas pueden venir de cualquier lugar y en cualquier momento. Por eso son una de las principales preocupaciones de ciberseguridad para los CISO a nivel mundial. Si usa Proofpoint Human Risk Explorer (HRE) con Proofpoint ITM, puede ver la puntuación de las señales de riesgo correlacionadas con el fin de descubrir y mitigar de forma proactiva los riesgos emergentes. Proofpoint HRE proporciona un conocimiento integral de los riesgos asociados a las personas, ya que analiza varias dimensiones en un solo lugar. Estos riesgos incluyen las vulnerabilidades, comportamientos, exposición a ataques, manejo de datos sensibles, concienciación en seguridad e identidad de cada empleado.

Proofpoint HRE también utiliza conocimientos basados en datos para hacer recomendaciones. Por ejemplo, si un usuario muestra un comportamiento que entraña riesgos, como descargar grandes volúmenes de información sensible, puede tomar medidas inmediatas, como aplicar controles de seguridad más estrictos, asignarle una formación específica o elevar el nivel de supervisión. Al concentrarse primero en los usuarios de alto riesgo, reduce significativamente la probabilidad de incidentes y mejora su postura de riesgo global.

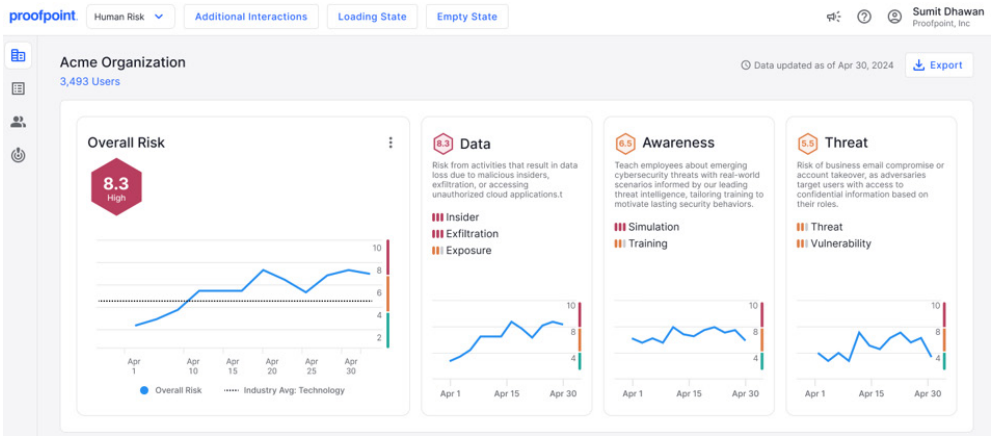



**Figura 1:** Con Proofpoint Human Risk Explorer, puede conocer fácilmente el riesgo general para su organización y compararlo con la media del sector. Si profundiza más, puede obtener información sobre riesgos de origen interno, filtraciones de datos y exposición de datos.

### Enfoque adaptativo basado en los riesgos

Para mitigar los riesgos internos, la mayoría de las organizaciones identifican grupos de riesgo comunes. Se trata de individuos o equipos que, debido a sus funciones, comportamientos o circunstancias, pueden representar un mayor riesgo para la integridad de los sistemas y datos. Los grupos de riesgo más habituales son los de empleados que abandonan la empresa, nuevos empleados, usuarios con acceso privilegiado, ejecutivos, contratistas o personas propensas a hacer clic, entre otros.

¿Pero qué pasa con los usuarios de riesgo desconocidos? La mayoría de las organizaciones no necesitan (y posiblemente no deberían) recopilar telemetría de endpoints sobre todas las actividades de todos los usuarios en todo momento. En cambio, Proofpoint facilita un enfoque adaptativo y basado en el riesgo. Esto implica que las políticas estáticas y manuales se sustituyen por otras que se ajustan automáticamente en tiempo real, en función del comportamiento del usuario.

En un enfoque adaptativo, las políticas dinámicas ajustan la supervisión del usuario en función de los comportamientos, no de características de riesgo predeterminadas. Por ejemplo, pensemos en un usuario que no forma parte de ningún grupo de riesgo. Cuando comienza a copiar datos sensibles en una unidad USB, Proofpoint ITM genera una alerta, lo que activa un nivel de supervisión elevado. Esta política obtiene metadatos detallados y capturas de pantalla durante un tiempo determinado. La supervisión solo se lleva a cabo cuando es necesario. De esta forma, se garantiza la privacidad y se optimizan las alertas para los analistas de seguridad. Con un enfoque adaptativo basado en el riesgo, ahorra tiempo y mejora la precisión de la detección.

### Agente de endpoint extremadamente estable y flexible

Para facilitar el enfoque adaptativo basado en el riesgo, Proofpoint utiliza un único agente de endpoint ligero que protege contra la pérdida de datos y proporciona un profundo conocimiento del comportamiento de los usuarios. Puede ajustar la cantidad y los tipos de datos recopilados para cada usuario o grupo de usuarios. Esto le ayuda a detectar amenazas a tiempo e investigar y responder a las alertas de manera eficaz, con un menor coste de procesamiento y almacenamiento. El agente en modo usuario de Proofpoint no entra en conflicto con otras soluciones ni requiere mucha capacidad de procesamiento, lo que garantiza la estabilidad, la productividad y el rendimiento de los usuarios.

## Información en tiempo real sobre comportamientos de riesgo

### Visibilidad granular de los usuarios de riesgo

Para ayudarle a detectar comportamientos de riesgo, Proofpoint proporciona una vista detallada de la actividad de los endpoints que incluye a los usuarios que intentan mover datos sensibles, como subirlos a sitios web no autorizados o copiarlos en carpetas de sincronización en la nube.

Asimismo se muestran los usuarios que manipulan tipos de archivos (por ejemplo, cambiando las extensiones de archivo) o que cambian el nombre a archivos que contienen datos sensibles. Estas actividades podrían ser indicio de que los usuarios intentan ocultar sus huellas. Cuando van unidas a determinados contextos, como un empleado que presenta su renuncia y se va a una empresa de la competencia, podrían señalar a un usuario de alto riesgo que requiere más investigación.

Proofpoint también proporciona visibilidad del uso de las aplicaciones y la navegación web. Las señales de comportamiento de riesgo incluyen la instalación y ejecución de herramientas no autorizadas, la realización de actividades de administración de seguridad, la manipulación de los controles de seguridad o la descarga de software malicioso. Proofpoint proporciona información detallada (quién, qué, dónde y cuándo) sobre las actividades de riesgo. Con contexto y datos, puede discernir mejor la intención del usuario cuando se produce un comportamiento inusual.

## Análisis de contenido y clasificación de datos

Los datos sensibles están más expuestos cuando se comparten o transfieren. Proofpoint analiza los datos en movimiento e interpreta las etiquetas de clasificación, como Microsoft Information Protection (MIP), para garantizar que se apliquen las políticas correctas.

Aprovechando la inversión ya realizada en clasificación de datos, puede identificar la información confidencial de la empresa, como la propiedad intelectual, sin crear flujos de trabajo independientes para los equipos de seguridad y los usuarios. Sin embargo, en algunos casos, es posible que no pueda usar la clasificación de datos para identificar datos regulados y datos de clientes. En tal caso, puede aprovechar los excelentes detectores de Proofpoint, como el de concidencia exacta de datos (EDM) para los datos estructurados y el de coincidencia de documentos indexados (IDM) para el contenido no estructurado, como la propiedad intelectual. Estos métodos avanzados mejoran la precisión de la detección y protegen su información más crítica.

## Motor de reglas flexible y biblioteca de alertas

Con Proofpoint ITM, puede crear nuevas reglas y activadores adaptados a su entorno o adaptar nuestros escenarios de amenazas prediseñados. Estos escenarios pueden modificarse por grupos de usuarios, aplicaciones y fechas y horas, además de según el grado de sensibilidad de los datos, las etiquetas de clasificación, el origen y destino, los canales de movimiento y los tipos.

| ACTIVIDAD DE DATOS | ACTIVIDAD DE COMPORTAMIENTOS |
|---|---|
| Alertas relacionadas con la interacción y la filtración de datos, incluidas las siguientes:<br>• Carga de archivos en la web<br>• Copia de archivos en dispositivos USB<br>• Copia de archivos para sincronización con la nube local<br>• Impresión de archivos<br>• Copiar/pegar archivos/carpetas/texto<br>• Actividades con archivos (renombrar, copiar, mover, eliminar)<br>• Seguimiento de archivos (de web a USB, de web a web, etc.)<br>• Descarga de archivos desde la web<br>• Envío de archivos como adjuntos de correo electrónico<br>• Descarga de archivos desde el correo electrónico/endpoint | Alertas relacionadas con comportamientos, incluidas las siguientes:<br>• Ocultación de información<br>• Acceso no autorizado<br>• Elusión de controles de seguridad<br>• Comportamientos negligentes<br>• Creación de una puerta trasera<br>• Violación de derechos de autor<br>• Herramientas de comunicación no autorizadas<br>• Tareas de administración no autorizadas<br>• Actividades no autorizadas del administrador de bases de datos<br>• Preparación de un ataque<br>• Sabotaje informático<br>• Elevación de privilegios<br>• Robo de identidad<br>• Actividades de Git sospechosas<br>• Uso inaceptable |

Proofpoint ITM también incluye bibliotecas de alertas listas para usar que facilitan la configuración y permiten obtener valor más rápidamente. Estas alertas le avisan de movimientos de datos o interacciones arriesgadas en los endpoints. Proofpoint puede alertar asimismo de una gama más amplia de comportamientos internos de riesgo. La biblioteca de amenazas internas incluye más de 150 reglas basadas en directrices del centro CERT e investigaciones basadas en comportamientos, lo que ofrece un medio rápido y fácil de detectar comportamientos de riesgo.

### Prevención de filtraciones de datos desde el endpoint no autorizadas

No siempre basta con detectar a los usuarios de riesgo y las actividades de datos sospechosas. También hay que bloquear las fugas de datos en tiempo real. Con nuestra solución, puede evitar que los usuarios interactúen con datos sensibles de maneras que contravengan las políticas, como que transfieran datos desde y a dispositivos USB, sincronicen archivos con carpetas en la nube, carguen datos en la web, los copien y los peguen, los impriman o los copien en dispositivos móviles, tarjetas SD, recursos compartidos de red y otros recursos. También puede impedir que los usuarios envíen datos sensibles a través de sitios de IA generativa (GenAI).

Puede personalizar su prevención según usuarios, grupos de usuarios, grupos de endpoints, nombres de procesos, dispositivos USB, números de serie de USB, proveedores de USB, etiquetas de clasificación de datos, URL de origen y resultados de análisis de contenido.

## Simplificación y aceleración de las investigaciones

### Consola unificada

Proofpoint le ayuda a agilizar las investigaciones y la respuesta a los incidentes de origen interno. Para obtener visibilidad multicanal, puede obtener telemetría de los endpoints, el correo electrónico y la nube de manera centralizada. Esta consola unificada, denominada Data Security Workbench, ofrece visualizaciones claras que permiten supervisar actividades, correlacionar alertas, gestionar investigaciones, buscar amenazas y coordinar la respuesta a incidentes. Esta visión centralizada le permite reducir los costes operativos.

Las potentes funciones de búsqueda y filtrado de Proofpoint le ayudan a identificar de manera proactiva riesgos internos mediante exploraciones de datos personalizadas. Puede buscar los comportamientos y actividades de riesgo que afectan a su organización o responder ante nuevos riesgos.

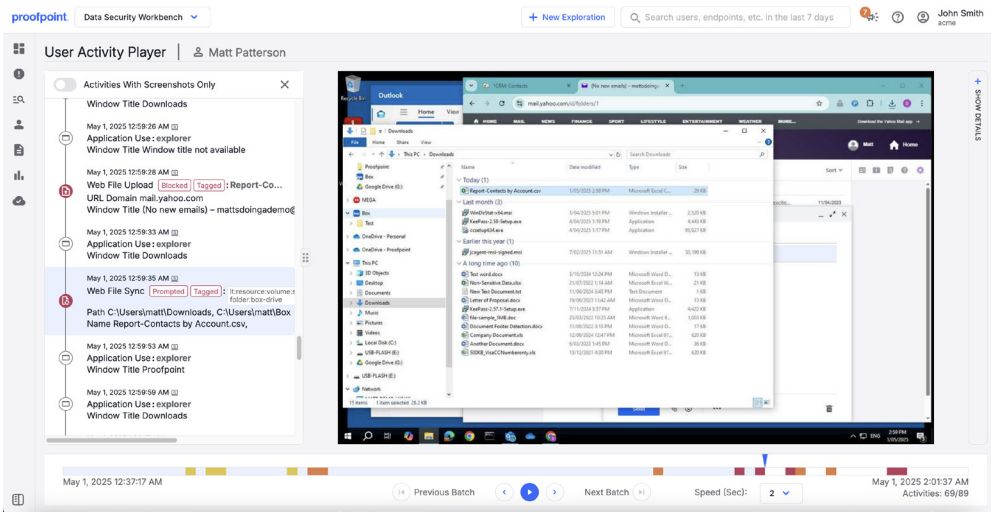



**Figura 2:** Desde el Data Security Workbench, puede ver lo que sucedió antes, durante y después de un incidente interno en una vista cronológica. Además, puede consultar fácilmente las capturas de pantalla para obtener más contexto y pruebas forenses.

Puede acelerar las investigaciones con la búsqueda asistida por IA utilizando prompts en lenguaje natural. Como ocurre con nuestras funciones de detección, puede adaptar una de las plantillas de exploración de amenazas que se incluyen o bien crear la suya propia.

### Clasificación de alertas

Investigar y resolver las alertas de seguridad de origen interno no siempre es fácil. Puede ser un proceso largo y costoso. Además, a menudo implica a otros departamentos no técnicos, como los de RR. HH., cumplimiento de normativas, legal y de dirección de línea de negocio.

Con Proofpoint, puede profundizar en cada una de las alertas y ver metadatos e información contextualizada, con vistas cronológicas. Los equipos de seguridad pueden identificar qué eventos necesitan investigar más a fondo y cuáles pueden cerrar de inmediato. La información contextualizada recibida antes, durante y después de un incidente provocado por un usuario interno ofrece contexto sobre sus intenciones. Saber si un usuario es negligente, malicioso o comprometido es fundamental para decidir los próximos pasos.

El flujo de trabajo y las funciones de intercambio de información agilizan la colaboración entre equipos. Puede exportar registros de actividades peligrosas para varios eventos, en formatos de archivo habituales, como PDF. Estas exportaciones incluyen pruebas con capturas de pantalla y el contexto relacionado. Todo ello ayuda a los equipos no técnicos, como el de Recursos Humanos y el departamento legal, a interpretar fácilmente los datos con fines de investigaciones forenses y a tomar decisiones fundamentadas.

### Capturas de pantalla para pruebas forenses

Una imagen vale más que mil palabras y Proofpoint puede obtener capturas de pantalla de la actividad de los usuarios. Disponer de pruebas claras e irrefutables de los comportamientos maliciosos o negligentes ayuda a los directivos y a los departamentos legal y de RR. HH. a tomar decisiones informadas.

En caso de infraestructuras de seguridad complejas, quizá sea necesario mantener una única fuente de información en todos los sistemas. Esto puede implicar la retención de capturas de pantalla, fragmentos de texto o archivos para llevar a cabo la investigación en su propio espacio de almacenamiento. Con Proofpoint es fácil, gracias a que ofrece la exportación automática de datos al almacenamiento gestionado en AWS S3, Microsoft Azure y Google Cloud Platform que posee.

## Equilibrio entre controles de privacidad y seguridad

Un programa eficaz de gestión de riesgos internos debe ofrecer un equilibrio entre la privacidad del usuario y la seguridad de los datos, según estipulan las normativas de privacidad de los datos. Proofpoint adopta un enfoque que integra la privacidad en el diseño del producto. Esto le ayuda a proteger los derechos de los empleados, cumplir con las leyes de privacidad y evitar sesgos durante las investigaciones.

### Residencia y almacenamiento de los datos

Proofpoint ofrece data centers en varias regiones, lo que facilita el cumplimiento de los requisitos de privacidad y residencia de los datos. Actualmente tenemos data centers en Estados Unidos, Canadá, Europa, Emiratos Árabes Unidos, Australia y Japón.

Puede controlar el almacenamiento de los datos de los endpoints mediante agrupaciones de endpoints. Cada agrupación, o dominio, puede asignarse a un data center para el almacenamiento. De esta forma, los clientes pueden separar fácilmente los datos por ubicación geográfica.

### Controles de acceso basados en atributos

Para cumplir los requisitos de privacidad, es preciso tener flexibilidad y control del acceso a los datos. Con Proofpoint, puede asegurarse de que los analistas de seguridad solo vean los datos que necesitan. Por ejemplo, puede dar acceso a un analista solo a los datos de un usuario específico o limitar cuánto tiempo tiene acceso.

### Anonimización y enmascaramiento de datos

La anonimización de la información personal garantiza la privacidad del usuario y elimina los sesgos durante las investigaciones. Proofpoint anonimiza los datos recopilados de los usuarios y no almacena el nombre completo ni el identificador de empleado de los usuarios que activan alertas, sino que los analistas investigan las alertas en función de identificadores únicos y anonimizados. Si se debe conocer la identidad de un usuario, el analista de seguridad puede solicitar la desanonimización y el administrador puede concederla.

El enmascaramiento de datos también garantiza la privacidad de los datos. Puede enmascarar datos sensibles, como la información sanitaria (PHI) y los datos de identificación personal (PII). Al hacerlo, los datos no se pueden identificar en la interfaz de usuario y solo las personas que necesitan acceder a ellos pueden verlos en su totalidad.

## Mejora de la agilidad empresarial con un enfoque moderno

### Escale rápida y fácilmente

Proofpoint es una solución nativa de la nube que se escala fácilmente y se adapta a la evolución de las necesidades de su negocio. Admite cientos de miles de usuarios por suscriptor. Además, se despliega rápidamente y es fácil de mantener. Esto garantiza una rápida rentabilización. Además, Proofpoint se integra fácilmente en su ecosistema existente con un enfoque basado en API "API-first". Los webhooks facilitan la ingestión de alertas para sus herramientas de administración de información y de eventos de seguridad (SIEM) y de orquestación, automatización y respuesta de seguridad (SOAR), lo que le ayuda a identificar y clasificar los incidentes rápidamente.

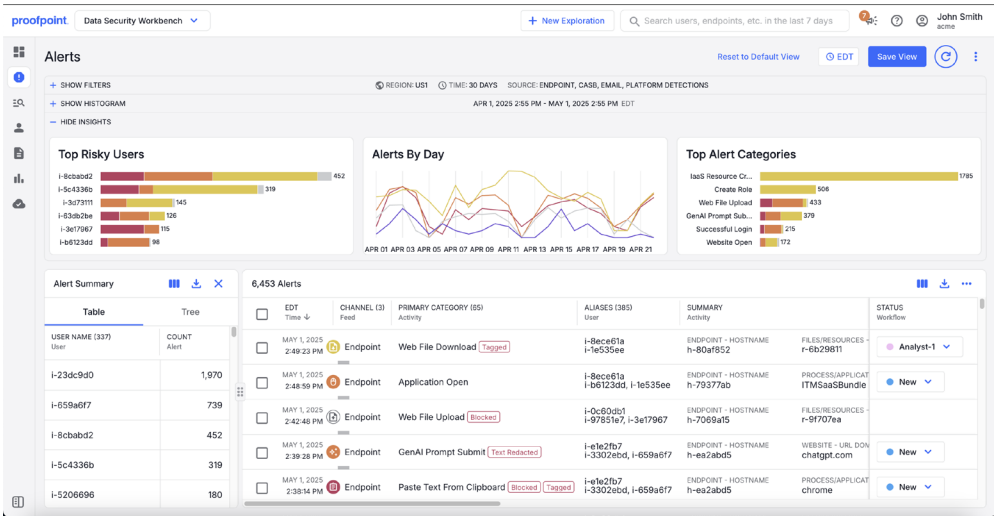



**Figura 3:** La anonimización protege la identidad del usuario, ayudando a garantizar la privacidad, además de eliminar los sesgos durante las investigaciones.

## Gestione sin riesgos los cambios a nivel empresarial

Los cambios organizativos en la empresa pueden suscitar dudas e incertidumbre, lo que deja el terreno abonado para las amenazas internas. Las fusiones y adquisiciones, los despidos inminentes o las nuevas tecnologías, como la IA generativa, pueden hacer que un riesgo de origen interno se convierta en una amenaza. Los equipos de gestión de riesgos internos necesitan visibilidad y controles para gestionar los cambios cuando se produzcan. Con Proofpoint esto es posible, gracias a un enfoque adaptativo basado en el riesgo que ofrece detección y prevención proactivas.

## Desarrolle y consolide su programa

Un programa eficaz de gestión de riesgos internos es una combinación de personas, procesos y tecnología. Proofpoint puede ser su partner de confianza para garantizar el éxito de su programa. Nuestros servicios Premium proporcionan la experiencia que necesita para optimizar su programa, aprovechar sus inversiones en tecnología y garantizar el compromiso y la participación de las partes interesadas. Los servicios Advisory proporcionan asesoramiento estratégico y servicios continuos durante la creación y mejora de su programa. Los servicios Applied le ayudan a optimizar su inversión tecnológica, garantizar la continuidad de las operaciones y madurar su programa de gestión de riesgos internos.

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: X | LinkedIn | Facebook | YouTube



**DESCUBRA LA PLATAFORMA DE PROOFPOINT →**