HUMAN-CENTRIC SECURITY

Implementar seguridad centrada en las personas en el entorno de trabajo digital actual

Cómo la plataforma de protección integral y multicapa de Proofpoint da vida a la seguridad centrada en las personas en la era de la transformación digital.

proofpoint®

Resumen ejecutivo

El entorno de trabajo digital moderno ha cambiado radicalmente la forma de trabajar. Las organizaciones han adoptado la nube y ahora los empleados colaboran en una compleja combinación de entornos. Entre ellas figuran el correo electrónico, las herramientas de colaboración y mensajería, las plataformas de redes sociales, las aplicaciones de software como servicio (SaaS), los grandes modelos de lenguaje (LLM) y los servicios de intercambio de archivos.

Este cambio ha permitido una innovación más rápida y una mayor flexibilidad. Pero también ha introducido muchas nuevas superficies de riesgo que pueden explotar los ciberdelincuentes. Los trabajadores del conocimiento generan, almacenan y acceden hoy a los datos de formas para las que no están preparadas las estrategias de seguridad tradicionales, centradas en proteger redes y endpoints. Estos cambios exigen una arquitectura moderna, alineada con la forma en que trabajan las organizaciones y las personas. Una arquitectura que responda a la realidad de que los usuarios, y no la infraestructura, son los principales objetivos de las ciberamenazas.

Este documento técnico analiza cómo Proofpoint ha logrado un hito en el sector: la plataforma Human-Centric Security, que responde a estas nuevas realidades situando a los usuarios en el centro de la estrategia de defensa moderna.

Este documento:

- **Explica por qué proteger a las personas es más importante** que nunca en el entorno digital actual.
- **Describe los problemas centrados en el factor humano** que la plataforma Proofpoint fue diseñada para resolver.
- **Analiza las tecnologías clave** que sustentan una arquitectura capaz de detectar amenazas de forma proactiva, guiar y proteger a los usuarios en tiempo real, y agilizar la investigación y la respuesta.

Las personas como nuevo perímetro: por qué es fundamental la seguridad centrada en las personas

En el centro del desafío actual de la ciberseguridad está el individuo. Las amenazas centradas en las personas, como el phishing, la usurpación de cuentas, los riesgos internos y la filtración de datos, son ahora responsables de la mayoría de los incidentes. La mayoría de los ataques modernos no explotan las vulnerabilidades técnicas, sino a las personas. Ya sea mediante el engaño, la distracción o la manipulación, las amenazas se dirigen a los usuarios en espacios de trabajo digitales cada día más complejos.

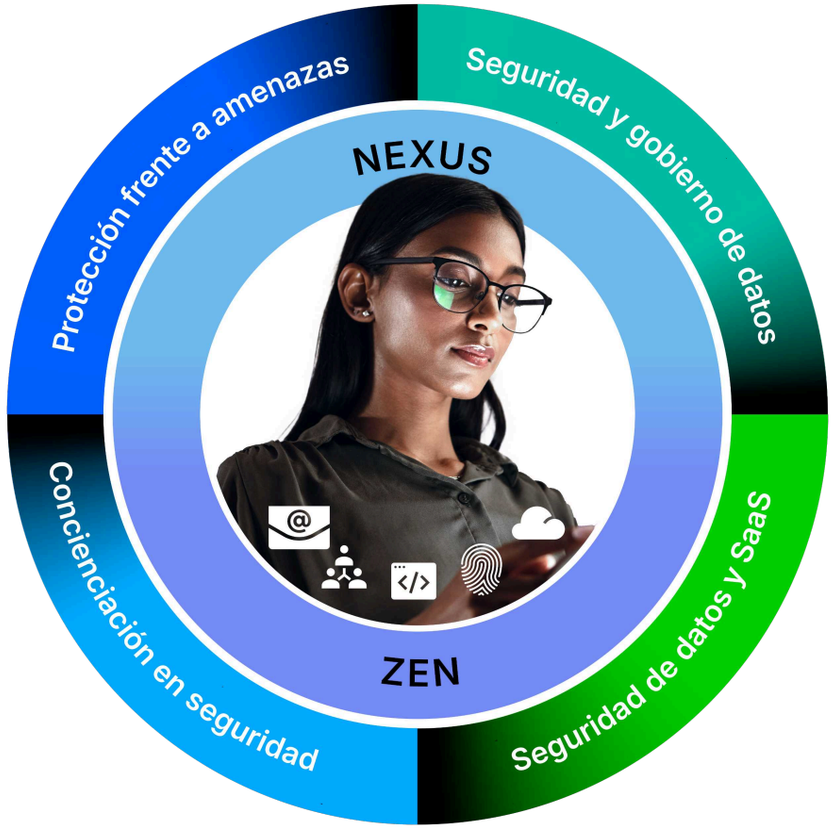
Los modelos de seguridad tradicionales se han centrado en proteger las redes y los endpoints. Pero las amenazas modernas se centran en las vulnerabilidades humanas. Con la plataforma de ciberseguridad de Proofpoint, las organizaciones pueden proteger a los empleados y los datos con un enfoque centrado en las personas. Nuestra plataforma proporciona las mejores soluciones para cubrir cuatro necesidades críticas: detener las amenazas, proteger la información, orientar a los empleados, y fortalecer el nivel de la seguridad de datos y aplicaciones SaaS.

PROTECCIÓN FRENTE A AMENAZAS

Bloquee las amenazas que se dirigen contra sus empleados

CONCIENCIACIÓN EN SEGURIDAD

Ofrezca orientación continua a sus empleados



SEGURIDAD Y GOBIERNO DE DATOS

Prevenga la pérdida de datos y gobierne las comunicaciones

SEGURIDAD DE DATOS Y SAAS

Evite la exposición de datos y SaaS

Figura 1: La plataforma de seguridad centrada en las personas de Proofpoint ofrece las mejores soluciones en cuatro áreas clave.

Una completa plataforma de protección multicapa

La plataforma integral de Proofpoint se basa en una arquitectura multicapa que:

- **Detecta amenazas de forma proactiva** en todo el entorno de trabajo digital mediante el uso de funciones como IA avanzada, aprendizaje automático e inteligencia de amenazas en tiempo real.
- **Proporciona un amplio conjunto de puntos de control de usuarios** que protegen a las personas y los datos, independientemente de dónde se realice el trabajo.
- **Alerta, orienta y capacita a los usuarios** para resistir los ataques dirigidos contra las personas.
- **Optimiza la investigación de la respuesta a incidentes.**

Estas capacidades son posibles gracias a tres tecnologías fundamentales: Nexus, Zen y Threat Protection Workbench. En las secciones siguientes se analizan estas tecnologías.

Nexus

Detección basada en IA e inteligencia de amenazas

Proofpoint Nexus® es la capa de detección de la arquitectura Proofpoint. Se trata de una plataforma de detección unificada impulsada por IA, aprendizaje automático e inteligencia de amenazas en tiempo real.

Nexus integra múltiples tipos de modelos de IA. Cada uno de ellos está diseñado para analizar señales de riesgo específicas en todas las formas de trabajar de las personas.
Por ejemplo, el correo electrónico, las aplicaciones cloud, las herramientas de colaboración y los navegadores.

Componentes clave de la plataforma de detección de Nexus

Nexus Threat Intelligence (TI) recibe continuamente señales de agentes, campañas e infraestructuras ciberdelincuentes conocidos y desconocidos para proporcionar a los productos de Proofpoint detecciones ricas en contexto y la capacidad de adaptarse a la evolución constante de las técnicas de amenazas.

Nexus Language Model (LM) aprovecha la potencia de los modelos de lenguaje de IA avanzados para evaluar el tono, la urgencia y la estructura lingüística de los mensajes utilizados en los ataques de ingeniería social, como las estafas Business Email Compromise (BEC).

Nexus Relationship Graph (RG) correlaciona la actividad de los usuarios, el historial de comportamiento y la sensibilidad a los roles para evaluar la probabilidad de comportamientos de riesgo o ataques dirigidos a personas de alto riesgo.

Nexus Machine Learning (ML) detecta comportamientos inusuales de los usuarios en las herramientas de comunicación y colaboración, identificando indicios sutiles pero relevantes de cuentas comprometidas o de uso indebido de usuarios internos.

Nexus Computer Vision (CV) reconoce la suplantación de marcas y las tácticas de fraude visual mediante el análisis de la disposición, la colocación del logotipo y la imitación del diseño. Gracias a una tecnología avanzada de visión por ordenador, detecta las amenazas ocultas en elementos visuales, como en sitios de phishing, códigos QR, archivos adjuntos maliciosos y mensajes falsificados.

Nexus detecta ataques avanzados de phishing, robo de credenciales, intentos de suplantación de identidad y campañas de ransomware. En un caso real, Nexus identificó un compromiso de un proveedor que condujo a un fraude de facturas dirigido a un departamento financiero. Bloqueó el ataque antes de su ejecución al identificar lenguaje inusual y discrepancias visuales, y al aplicar inteligencia de amenazas existente de su conjunto de datos mundial.

Nexus también destaca en la protección de datos. En otro caso real, cuando un empleado pegó datos de un cliente en una herramienta de IA generativa no autorizada, Nexus detectó el patrón de datos sensibles, elevó la puntuación de riesgo y bloqueó la acción.

Nexus analiza más de **2600 millones de correos electrónicos al día, inspecciona más de 450 millones de URL diarias** y correlaciona señales de cientos de ciberdelincuentes. Esta enorme escala mejora tanto la precisión como la capacidad de respuesta en todo el panorama de amenazas.

proofpoint.

Zen

Puntos de control y orientación contextual del usuario

Proofpoint Zen™ es la capa de aplicación y orientación al usuario de la arquitectura de Proofpoint. Aplica las políticas de seguridad allí donde trabajan los usuarios. Los puntos de control de la suite Zen convierten la inteligencia en protección en tiempo real y en formación en base a las políticas. Esto ayuda a los usuarios a tomar decisiones más seguras sin ralentizar su trabajo.

Componentes principales de la suite Zen

Zen for Outlook capacita a los usuarios como defensores de primera línea integrando herramientas de seguridad en sus flujos de trabajo de correo electrónico. Gracias a la inteligencia de amenazas en tiempo real de Nexus, muestra a los usuarios advertencias online cuando reciben correos electrónicos sospechosos y permite denunciar fácilmente. Proporciona avisos inteligentes para comportamientos de riesgo y alertas para datos confidenciales en correos electrónicos salientes.

ZenWeb es una extensión ligera para navegadores basados en Chromium que protege las actividades web en aplicaciones SaaS, el intercambio de archivos y las herramientas de IA generativa, y protege a los usuarios frente a los sitios de phishing. Gracias a las detecciones en tiempo real de los modelos de amenazas de Nexus, proporciona detección y prevención de amenazas inmediatas sin interrumpir la productividad de los usuarios.

Zen Endpoint DLP/Insider Threat Management proporciona protección a nivel de dispositivo contra la pérdida de datos y las amenazas internas mediante la supervisión del comportamiento de los usuarios en el endpoint. Supervisa el uso del llaves USB, la actividad del Portapapeles, las operaciones de sincronización de archivos y el comportamiento de las aplicaciones. Hace capturas de pantalla de acciones sospechosas de los usuarios y elabora una cronología de actividades de los usuarios.

Zen Cloud API Connectors amplía la seguridad a plataformas SaaS basadas en la nube como Microsoft 365, Google Drive, Slack y Box. Supervisa las cargas de archivos y detecta comportamientos inusuales, como los excesos a la hora de compartir información. También permite flujos de trabajo personalizados en Okta y herramientas de organización, automatización y respuesta a incidentes de seguridad (SOAR).

Zen Communications Connectors captura las comunicaciones en plataformas reguladas, como Microsoft Teams, Zoom y Slack, para archivarlas y supervisarlas. Ingesta mensajes de varios canales en un formato de archivo unificado y se integra con herramientas de supervisión para flujos de trabajo de recursos humanos y jurídicos.

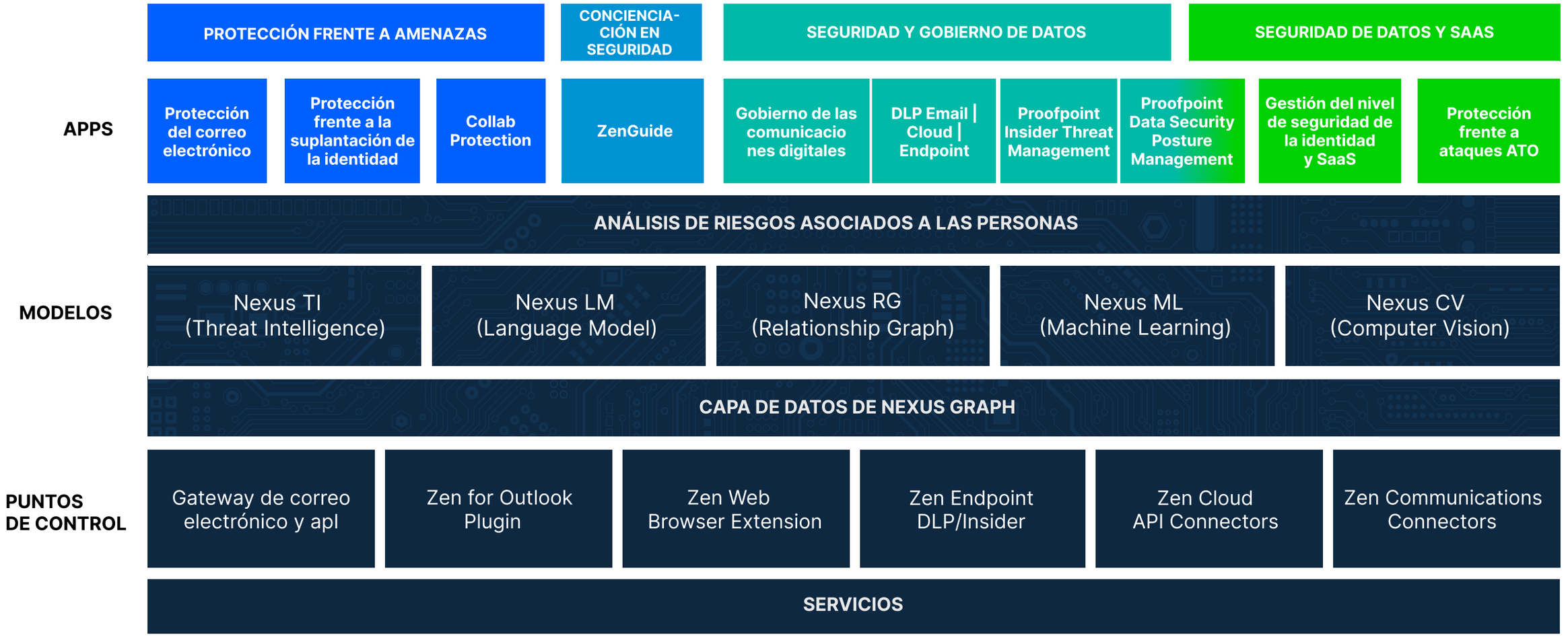


Figura 2: La plataforma Human-Centric Security de Proofpoint se basa en una arquitectura multicapa. Las soluciones de Proofpoint (en nuestras cuatro áreas clave: Protección frente a amenazas, concienciación en seguridad, seguridad y gobierno de los datos y nivel de seguridad de aplicaciones SaaS) utilizan directamente las capacidades de nuestras principales tecnologías Nexus y Zen

Proofpoint Threat Protection Workbench

Investigación rápida y corrección automatizada

Cuando se detecta una amenaza o se señala una infracción, la rapidez y la claridad son fundamentales. Para los equipos de los centros de operaciones de seguridad (SOC), la multiplicidad de consolas, el exceso de clics y la dependencia de otros equipos ralentizan los tiempos de respuesta y aumentan los riesgos de éxito de los ataques.

Proofpoint Threat Protection Workbench es la capa de investigación y automatización de la arquitectura de Proofpoint. Al proporcionar una consola intuitiva y centralizada, agiliza la investigación y corrección de las amenazas. Permite a los equipos de seguridad clasificar, analizar y responder a las amenazas sin los retrasos causados por el cambio de herramientas o los datos fragmentados.

Los equipos de seguridad utilizan Threat Protection Workbench para procesar los envíos de buzones abusivos, escalar señales sobre usuarios de alto riesgo e investigar campañas de amenazas. Al correlacionar la información de amenazas de Nexus con el comportamiento de los usuarios y los activadores de políticas, Threat Protection Workbench proporciona alertas de alta fidelidad en lugar de ruido no deseado.

Ejemplos de casos de uso de Threat Protection Workbench

- Respuestas automatizadas para las investigaciones de usurpaciones de cuentas.
- Visualizaciones de rutas de clics para usuarios específicos.
- Resumen de las complejas amenazas multicanal.

Todas estas funciones reducen la carga de trabajo de los analistas y el tiempo de permanencia de las amenazas. Para responder a las amenazas, los analistas pueden activar directamente las estrategias o utilizar API para escalarlos a otros componentes integrados en sus pilas de seguridad más amplias.

Conclusión

Una arquitectura específica para la seguridad centrada en las personas

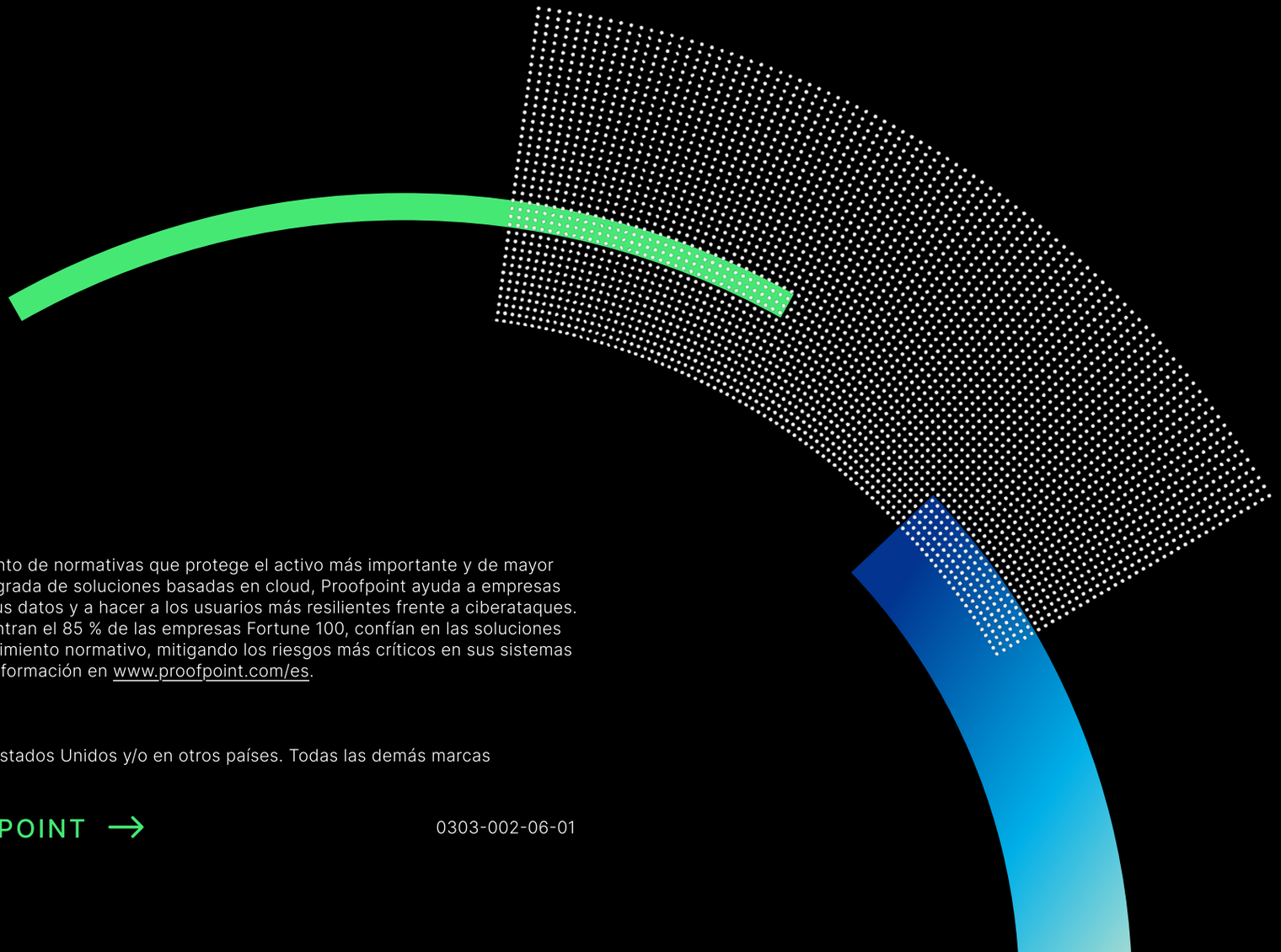
La naturaleza de los ciberriesgos ha cambiado. Las amenazas no solo afectan a los sistemas, sino también a las personas. Y la complejidad del espacio de trabajo digital ha superado las defensas construidas para protegerlo. A medida que los usuarios se mueven con fluidez entre el correo electrónico, los navegadores, las herramientas de colaboración y las aplicaciones cloud, el antiguo modelo de seguridad, basado en perímetros estáticos y controles uniformes, ya no puede seguir el ritmo.

La plataforma de Proofpoint resuelve este reto alineando la arquitectura de seguridad con la forma de trabajar de las personas. A través de Nexus, las organizaciones obtienen visibilidad impulsada por IA de las amenazas centradas en las personas, basada en inteligencia de amenazas y análisis de comportamiento sin igual. Con Zen, nuestra plataforma protege y asesora a los usuarios en el momento, sin fricciones. Y con Workbench, los equipos de seguridad responden más rápido, con información más clara y menos sobrecarga operativa.

Esto no es teórico. Nuestra plataforma es una arquitectura probada a escala de producción que reduce el riesgo y crea resiliencia a largo plazo. Las organizaciones pueden proteger los flujos de trabajo actuales y prepararse para la próxima evolución del riesgo centrado en las personas.

Combinando una detección de primer nivel, controles de comportamiento integrados y una respuesta rápida e integrada, podemos ayudar a su organización a reducir el riesgo donde más importa: en la intersección de personas, datos y amenazas.

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 →

0303-002-06-01