SEGURIDAD CENTRADA EN LAS PERSONAS

Un multiplicador de fuerza en las arquitecturas de ciberseguridad modernas

Por qué la seguridad centrada en las personas es el elemento crítico de una estrategia de defensa moderna: adapta, conecta y refuerza sus inversiones existentes en ciberseguridad

proofpoint.

Resumen ejecutivo

Una responsabilidad clave de los CISO actuales es determinar las inversiones estratégicas críticas para la arquitectura de ciberseguridad de su empresa. Y hay algunos pilares de seguridad ampliamente reconocidos, como la arquitectura SASE (Secure Access Service Edge), la detección y respuesta ampliadas (XDR) y la identidad, que deben ocupar un lugar central en la estrategia de defensa de una organización. Estos tres pilares no pueden funcionar de manera independiente. En una arquitectura de ciberseguridad moderna, es esencial que todos los componentes trabajen de forma coordinada para hacer frente a las amenazas actuales y preparar a la organización para los desafíos del futuro. No obstante, aunque cada uno de estos pilares es clave, ninguno aborda el mayor riesgo de todos: las personas y sus acciones.

La seguridad centrada en las personas cierra el círculo: de la bandeja de entrada a los endpoints, de las identidades a las amenazas internas. Porque detrás de cada incidente hay un ser humano: comprometido, negligente o malicioso.

Este documento técnico analiza cómo la seguridad centrada en las personas constituye el elemento crítico (y transformador) de una arquitectura de ciberseguridad moderna.

Este documento técnico:

- **Explica cómo la seguridad centrada en las personas desempeña un papel fundamental** dentro de la arquitectura general, al eliminar puntos ciegos en la protección actual y detectar los riesgos de origen humano en el entorno digital de trabajo actual.
- **Presenta la plataforma Human-Centric Security de Proofpoint.** Este documento describe cómo Proofpoint actúa de eje estratégico que refuerza sus inversiones en seguridad existentes y protege a su organización contra las amenazas centradas en las personas.

Más allá de perímetros y productos individuales: qué está fallando

Muchos CISO siguen combatiendo amenazas modernas con modelos antiguos. Esto significa controles aislados, información fragmentada y herramientas que no pueden adaptarse con la suficiente rapidez. Pero la superficie de ataque ha cambiado, y nuestra respuesta también debe hacerlo.

Esta es la nueva realidad: el objetivo de los ciberdelincuentes actuales son las personas, no los puertos de red. Con la ampliación de los entornos de trabajo digitales, los ciberdelincuentes centran sus ataques en las personas a través del correo electrónico y otros muchos canales digitales, como las herramientas de colaboración y mensajería, las plataformas de medios sociales, las aplicaciones cloud, los grandes modelos de lenguaje (LLM) y los servicios de uso compartido de archivos. Además, los ciberdelincuentes pueden secuestrar comunicaciones empresariales de confianza, lo que afecta a las relaciones con proveedores y clientes.

Al mismo tiempo, los datos no se pierden por arte de magia: cada incidente tiene su origen en una decisión o acción humana. Los usuarios negligentes descuidan los datos sensibles o críticos. Los usuarios maliciosos se los llevan al abandonar la empresa. Los hackers comprometen las cuentas de usuarios para robarlos. Los usuarios que no cumplen las políticas los usan de forma indebida.

Elegir soluciones líderes sigue siendo fundamental, pero los CISO actuales también deben centrarse en diseñar una arquitectura inteligente y cohesionada, capaz de evolucionar con el panorama de amenazas y de garantizar que todas las herramientas trabajen de forma coordinada para ofrecer una defensa eficaz.

En Proofpoint, hemos creado algo único en el sector: una completa plataforma de seguridad centrada en el ser las personas (Human-Centric Security) que actúa como multiplicador de fuerza, potenciando sus inversiones en seguridad para el correo electrónico, la identidad, los datos y el acceso.

No nos limitamos a resolver fallos de seguridad. Gracias a integraciones avanzadas con partners como CrowdStrike, Okta, Zscaler, Microsoft, Palo Alto Networks y otros, minimizamos el tiempo de permanencia, neutralizamos los ataques antes y devolvemos un tiempo valioso a su equipo de seguridad.

Si hasta ahora solo ha utilizado nuestras soluciones para la protección del correo electrónico, le aseguramos que esto no es más que el principio. Bienvenido a la era de las plataformas.

proofpoint.

Los pilares básicos de una arquitectura de ciberseguridad moderna

Todos los CISO los reconocen. Constituyen los pilares básicos y reconocidos de una arquitectura de ciberseguridad moderna: **SASE, XDR, identidad, y SecOps y automatización.** Como se describe a continuación, cada uno es esencial y responde a preocupaciones importantes en materia de gestión de riesgos. Pero aquí está el problema, ninguno de ellos tiene en cuenta el mayor riesgo del panorama actual de la seguridad: las personas. **Esto convierte a la seguridad centrada en las personas en el pilar más crítico de todos.**

SecOps y automatización

Optimiza la detección, investigación y respuesta eliminando el esfuerzo manual y los flujos de trabajo aislados. Además, soluciona los retrasos en la respuesta, la fatiga de alertas y la ineficacia operativa. Proofpoint automatiza el triaje de amenazas y la aplicación de políticas mediante estrategias integradas, información enriquecida sobre riesgos humanos y API flexibles. Esto permite a los equipos del centro de operaciones de seguridad (SOC) actuar con mayor rapidez y precisión.

SASE

Proporciona un acceso seguro y optimizado a aplicaciones y datos, independientemente de la ubicación del usuario o del dispositivo que esté utilizando. Admite plantillas distribuidas, acceso a la nube y aplicación coherente de políticas en entornos de teletrabajo. Cuando se basa en indicios de riesgo centrados en las personas, SASE puede dar prioridad a la protección de usuarios o comportamientos de alto riesgo.

Seguridad centrada en las personas

Sitúa a las personas en el centro de la protección, ya que los usuarios, y no las infraestructuras, son los principales objetivos de las ciberamenazas. La plataforma Human-Centric Security de Proofpoint combate el phishing, la pérdida de datos y el compromiso de cuentas combinando la detección de amenazas basada en IA y la formación de usuarios en tiempo real. Para reducir los riesgos centrados en las personas, nuestras tecnologías Nexus y Zen identifican de forma única y precisa a los usuarios, comportamientos y exposiciones de riesgo.

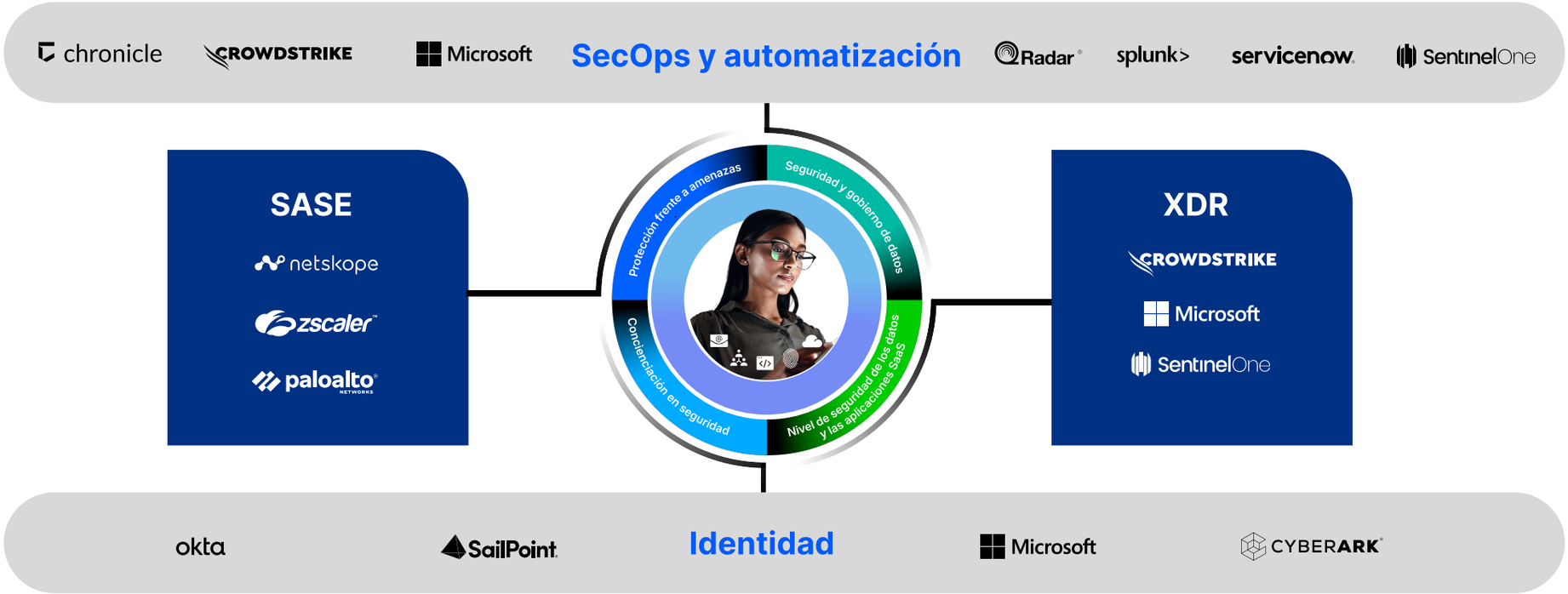
XDR

Unifica los datos telemétricos del correo electrónico, los endpoints, la nube y las redes para agilizar la detección, el análisis y la neutralización de amenazas. Reduce los problemas de los silos de visibilidad y los tiempos de respuesta prolongados. Los datos de telemetría centrados en las personas de Proofpoint, incluida la información sobre usuarios específicos y en riesgo, pueden optimizar la XDR con inteligencia contextual temprana y procesable.

Identidad

Protege las identidades y el acceso de los usuarios en la nube y en entornos locales mediante la detección de la usurpación de cuentas, el uso indebido de credenciales de inicio de sesión y la configuración incorrecta de aplicaciones SaaS. Reduce el riesgo de ataques a la identidad y accesos no autorizados mediante la supervisión continua de las autorizaciones, los comportamientos de inicio de sesión y las configuraciones de las aplicaciones de alto riesgo. Como Proofpoint sabe quién tiene acceso a qué y por qué, los equipos de seguridad pueden evitar los desplazamientos laterales y aplicar el principio de privilegios mínimos.

La seguridad centrada en las personas, un multiplicador de fuerza



La plataforma Human-Centric Security de Proofpoint actúa como un plan de control estratégico en su arquitectura de ciberseguridad. Se integra con sus inversiones en seguridad existentes proporcionando señales de riesgo centradas en las personas, que potencian su eficacia.

Nuestra plataforma permite conocer la clasificación de datos, la intención de los usuarios y el contexto de las amenazas. Utiliza IA, aprendizaje automático e inteligencia de amenazas en tiempo real para obtener información y tomar decisiones automatizadas sobre políticas.

Estas son algunas de las muchas maneras en que la **plataforma Human-Centric Security de Proofpoint** se integra con los demás pilares de su arquitectura, para transformar su protección global:

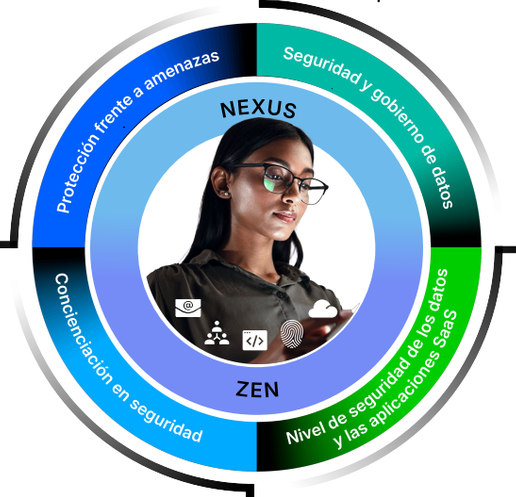
SASE y control adaptable de acceso

En colaboración con partners como Zscaler y Palo Alto Networks, Proofpoint integra inteligencia sobre amenazas y comportamiento para influir en las políticas de acceso en tiempo real. Los usuarios objetivo están sujetos a un nivel más de autenticación o tienen su acceso bloqueado a través de Zscaler o Palo Alto Prisma Access. La actividad maliciosa desencadena la aplicación inmediata de políticas.

Se trata de una arquitectura SASE informada por personas, no solo por paquetes.

Respuesta acelerada y automatizada

Proofpoint se integra con sistemas de administración de información y eventos de seguridad (SIEM) y plataformas de orquestación, automatización y respuesta de seguridad (SOAR) para reducir el tiempo medio de detección, análisis y neutralización de amenazas mediante la activación de alertas centradas en las personas y la automatización de las acciones de respuesta. Los indicios de riesgos de Proofpoint activan estrategias automatizadas en Cortex XSOAR o Splunk SOAR que ponen en cuarentena a los usuarios o restablecen las credenciales de inicio de sesión. Las alertas enriquecidas en Splunk o Microsoft Sentinel reducen los falsos positivos y aceleran el triaje. Los datos de amenazas y la telemetría de comportamientos de Proofpoint se comparten entre sistemas para permitir flujos de trabajo unificados.



XDR que se aplica en el punto de entrada

El phishing sigue siendo el principal punto de entrada. Nuestra asociación con CrowdStrike, Microsoft Sentinel y SentinelOne nos permite cerrar el círculo. La notificación de un correo electrónico desencadena el aislamiento del endpoint en CrowdStrike o SentinelOne en cuestión de segundos, no de horas. La asignación de una puntuación de riesgo a los usuarios y la información contextual específica sobre amenazas de Proofpoint enriquecen las alertas en Microsoft Sentinel.

Proofpoint proporciona visibilidad desde el mismo punto de entrada, por lo que su solución XDR se beneficia de una información exhaustiva.

Protección de identidades y accesos privilegiados

Compartimos el contexto de riesgo con Okta, CyberArk y SailPoint para configurar el control de acceso de forma dinámica. Identificamos a sus usuarios de mayor riesgo y compartimos esa información con nuestros partners. ¿Un comportamiento sospechoso? Aplicamos la autenticación multifactor. ¿Un usuario de alto riesgo? Aplicamos políticas y controles adaptables. ¿Una cuenta comprometida? Revocamos el acceso. Juntos, hacemos realidad el modelo Zero Trust (de confianza cero) mediante una aplicación adaptable y consciente de la identidad.

proofpoint.

Sus próximas acciones deben ser estratégicas, no tácticas

La cuestión no es qué herramienta utilizar a continuación, sino cómo desarrollar una plataforma que pueda adaptarse a sus inversiones existentes, conectarse a ellas y optimizarlas.

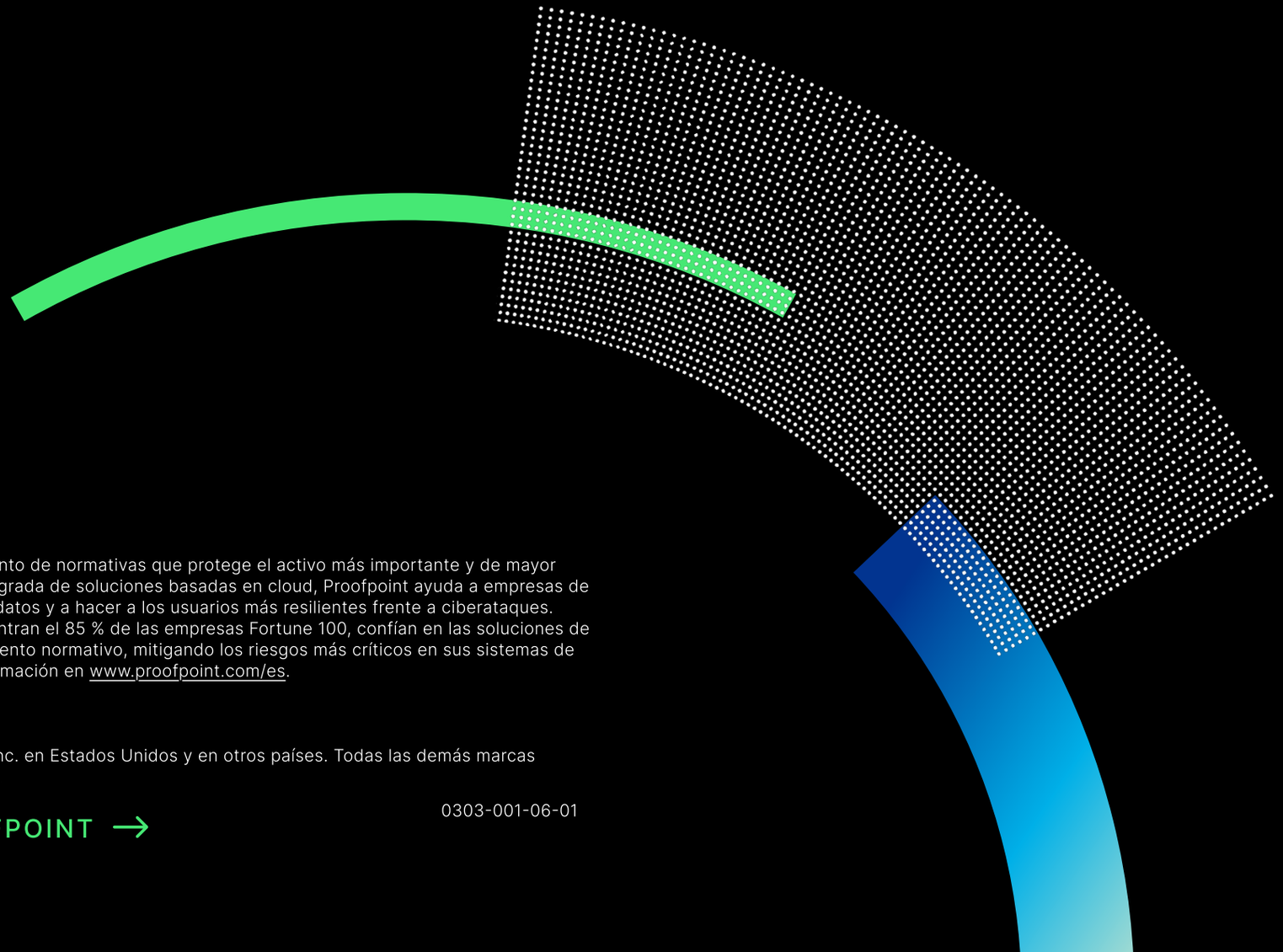
Más información sobre nuestras integraciones

Descubra más casos de uso de integración entre Proofpoint y otros componentes de su arquitectura de ciberseguridad.
Visite proofpoint.com/use/partners/technology-alliance-partners.

Hable con Proofpoint hoy mismo

- **Evalúe** si su arquitectura de seguridad está preparada para gestionar las amenazas centradas en las personas.
- **Determine** cómo pueden optimizarse sus inversiones actuales (XDR, SASE e identidad) con nuestra inteligencia unificada de riesgos asociados en las personas.
- **Descubra** cómo es realmente la seguridad basada en plataformas y cuáles son los primeros pasos para conseguirla. Le mostraremos cómo convertir la información centrada en las personas en una seguridad transformadora.

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

0303-001-06-01

DESCUBRA LA PLATAFORMA DE PROOFPOINT →