Productos de Proofpoint

Proofpoint le ofrece visibilidad y protección para su recurso más importante y el mayor riesgo para su seguridad: las personas. Ofrecemos las herramientas más eficaces para proteger contra las amenazas dirigidas a las personas, con objeto de proteger tanto la información que crean y a la que acceden, como a los propios usuarios.

Nuestras soluciones de ciberseguridad y cumplimiento de normativas incluyen el correo electrónico, las redes sociales, la Web, las redes y las plataformas de la nube, incluida Microsoft Office 365. Además disponemos de integraciones estratégicas de tecnología con los mejores proveedores de seguridad de la industria. De esta forma, le ayudamos a proteger mejor a sus empleados, sus datos y su marca.

PROTECCIÓN DEL CORREO ELECTRÓNICO

Defiéndase de las amenazas por correo electrónico, garantice la continuidad de las comunicaciones por este canal e implemente políticas para el correo entrante y saliente.

Email Protection

Proofpoint Email Protection protege a los usuarios frente a los mensajes de correo electrónico malicioso y no deseados, tanto si son amenazas de malware como si no contienen malware, como el correo de impostores o las estafas de tipo business email compromise (BEC). Para ello, proporcionamos visibilidad granular y continuidad del negocio a organizaciones de todos los tamaños. Mediante el control de los aspectos del correo entrante y saliente y la configuración de políticas, ayudamos a sus equipos de seguridad y de TI a proteger a sus usuarios frente a las amenazas del correo electrónico y a mantener activas las comunicaciones por correo electrónico en caso de fallo general.

Email Fraud Defense (EFD)

Proofpoint Email Fraud Defense (EFD) protege a sus empleados, clientes y partners comerciales frente a toda forma de fraude por correo electrónico, deteniendo los ataques de impostores incluso antes de que los mensajes lleguen a la bandeja de entrada. Desde un único portal, puede autorizar los mensajes legítimos, bloquear los mensajes fraudulentos y ver todas las amenazas, sea cual sea la táctica empleada o la víctima elegida. Mediante el empleo de autenticación del correo electrónico, aprendizaje automático y políticas, así como con la implementación de autenticación DMARC, EFD le ayuda a bloquear todas las tácticas de fraude que emplean los delincuentes para lanzar ataques avanzados.

Threat Response Auto-Pull (TRAP)

Proofpoint Threat Response Auto-Pull (TRAP) usa funciones de orquestación y automatización para retirar los mensajes maliciosos que ya se han entregado en la bandeja de entrada de un usuario. Esta versión básica de Threat Response identifica y elimina los mensajes maliciosos basándose en alertas de TAP. A continuación, utiliza lógica empresarial para seguir su rastro hasta el grupo más grande de destinatarios, y localizar y retirar los mensajes correspondientes. TRAP también genera informes que muestran los intentos de cuarentena, las amenazas que consiguen y no consiguen sus objetivos, y una lista de los usuarios que reciben más ataques, lo que reduce la carga de trabajo de su equipo de seguridad.

Internal Mail Defense

Proofpoint Internal Mail Defense emplea un eficaz enfoque multicapa para proteger el correo electrónico interno de su empresa y ayudar a detectar las cuentas comprometidas. Esta solución analiza todo el correo interno para detectar spam y direcciones URL o archivos adjuntos maliciosos. Si se marca el correo interno enviado, se elimina y se pone en cuarentena automáticamente. Además, los equipos de seguridad tienen visibilidad de las cuentas desde las que se enviaron las URL maliciosas, de forma que se pueden localizar las posibles cuentas comprometidas y aplicar las medidas oportunas.

Essentials para pequeñas empresas

Proofpoint Essentials adapta las funciones de Email Protection a las necesidades de las pequeñas empresas. Esta solución ofrece filtrado de spam, detección de phishing, antivirus multicapa, análisis de URL en entorno aislado, un robusto motor de reglas de filtrado, continuidad del correo electrónico, cifrado mediante políticas, archivado del correo electrónico y protección de cuentas de redes sociales. Y lo mejor de todo, se gestiona desde una interfaz de usuario sencilla e intuitiva, lo que facilita su uso a las pymes que normalmente tienen equipos de seguridad más reducidos.

PROTECCIÓN FRENTE A AMENAZAS AVANZADAS

Detecte, investigue y responda a las amenazas con mayor rapidez, precisión y confidencialidad.

Targeted Attack Protection (TAP)

Proofpoint Targeted Attack Protection (TAP) ayuda a detectar, mitigar y bloquear amenazas avanzadas que contengan direcciones URL y archivos adjuntos maliciosos dirigidos a personas a través del correo electrónico y las apps en la nube, como Microsoft Office 365 y Google G Suite. TAP le ofrece visibilidad de las personas muy atacadas (VAP, Very Attacked People) de su organización. Además, le permite reescribir todas las URL incrustadas con el fin de proteger a sus usuarios en cualquier dispositivo y seguir el rastro a los clics en enlaces maliciosos.

Email Isolation

Proofpoint Email Isolation permite a sus equipos de TI y de seguridad autorizar a los usuarios para acceder a su correo web personal desde dispositivos corporativos sin tener que preocuparse por la seguridad. Puede integrarse con TAP para proporcionar una capa adicional de seguridad para sus VAP, protegiendo al mismo tiempo a todos los usuarios contra los sitios web desconocidos o peligrosos. Para ello, evita que cualquier malware o contenido malicioso afecte al usuario o al dispositivo. Nuestro servicio en la nube separa el contenido web, de los datos y redes de la empresa. Además, simplifica la gestión de riesgos y costes operativos, mejorando su estado general de seguridad.

Browser Isolation

Proofpoint Browser Isolation amplía las funciones de Proofpoint Email Isolation para proteger todas las actividades de navegación web para todos los usuarios, incluidas las personas muy atacadas, o VAP. Esta solución ofrece un servicio de navegación web seguro y anónimo, fácil de implementar, gestionar y mantener para su equipo de TI. De esta forma, sus usuarios disponen de privacidad cuando acceden a sitios como su correo web. Y no tienen que preocuparse por si introducen nuevos riesgos para su organización.

Threat Response

La solución Proofpoint Threat Response ha sido diseñada para los equipos de operaciones de seguridad que trabajan en pos de la madurez de la seguridad. Le proporciona una vista práctica de las amenazas de su red y alertas de todo tipo, y automatiza la recopilación y comparación de datos forenses. También elimina el trabajo manual y de investigación en relación a la respuesta a los incidentes. De esta forma, su equipo de seguridad puede corregir las amenazas más rápidamente y con más eficacia. Y, a diferencia de los procesos tradicionales de respuesta a incidentes, Threat Response confirma de forma automática las infecciones de malware, verifica las pruebas de infecciones anteriores, y enriquece las alertas de seguridad añadiendo automáticamente el contexto y la inteligencia internos y externos.

Emerging Threats Intelligence

Proofpoint Emerging Threats Intelligence (ET) es el estándar de referencia para los investigadores de amenazas, ya que aporta inteligencia de amenazas 100 % verificada de una de las fuentes de datos de malware más grande el mundo. Además, ayuda a entender el contexto histórico más detallado del origen y el autor de una amenaza, integrándose perfectamente con sus herramientas de seguridad. A diferencia de otras fuentes de inteligencia que solo informan de los dominios o las direcciones IP, nuestra inteligencia incluye un historial de diez años, pruebas de su detección, y más de 40 categorías de amenazas con las direcciones IP, dominios y muestras correspondientes.

Emerging Threats Pro Ruleset

Proofpoint Emerging Threats (ET) Pro Ruleset es un grupo de reglas destinadas a detectar y bloquear las amenazas de manera inmediata y con precisión, utilizando sus dispositivos de seguridad de la red actuales, incluidos los firewalls y sistemas IDS/IPS de red. Actualizada a diario en formato SNORT y Suricata, la solución ET Pro Ruleset cubre más de 40 categorías diferentes de comportamientos de red, infraestructuras de mando y control de malware, ataques DoS, redes de bots, exploits, vulnerabilidades, protocolos de red SCADA y actividad de kits de exploits, entre otras. Gracias a la ejecución de actualizaciones diarias y al uso de un entorno aislado automatizado, su equipo de seguridad tiene la tranquilidad de saber que todas las amenazas se han evaluado convenientemente.

Premium Threat Information Service (PTIS)

Proofpoint Premium Threat Information Service (PTIS) le permite priorizar sus decisiones de seguridad, ya que le proporciona un conocimiento más profundo y contextualizado del panorama actual de las amenazas en cada momento. Incluye tres componentes: acceso directo a nuestros investigadores de amenazas, líderes en el sector, informes personalizados sobre amenazas con una periodicidad mensual, así como avisos avanzados de amenazas emergentes, a través del acceso a los documentos de registro de nuestros analistas. Este servicio puede ayudar y retener a los analistas de seguridad, personal que es difícil de encontrar, ya que reduce los procesos manuales, de manera que les permite centrarse en los asuntos más críticos.

FORMACIÓN PARA CONCIENCIAR EN MATERIA DE SEGURIDAD

Convierta a sus usuarios en una última línea de defensa sólida contra el phishing y otros ciberataques permitiéndoles identificar y denunciar las amenazas.

Anti-Phishing Suite

Proofpoint Anti-Phishing Suite le ayuda a identificar y reducir hasta un 90 % la vulnerabilidad de sus empleados ante los ataques de phishing y las infecciones de malware. Si un usuario cae en la trampa de un ataque de phishing simulado de ThreatSim, se le presenta un "momento para aprender" con sugerencias sobre cómo mantenerse a salvo en el futuro.

Los usuarios que se dejan engañar en un ataque simulado pueden inscribirse en uno de nuestros 8 módulos de formación antiphishing automáticamente o por separado. Además, con este paquete, los administradores tienen acceso al botón de denuncia PhishAlarm® y a las herramientas de análisis de PhishAlarm Analyzer. Estas herramientas son el principio de nuestra solución Closed Loop Email Analysis and Response (CLEAR), que facilita la denuncia directa y la respuesta automática cuando se detectan ataques de phishing activos.

Formación para concienciar en materia de seguridad para grandes empresas

El paquete de Formación para concienciar en materia de seguridad para grandes empresas incluye la suite Anti-Phishing Suite y añade ThreatSim para simulaciones USB, las evaluaciones de conocimientos de CyberStrength®, nuestra biblioteca completa de módulos de formación, y la totalidad de material de concienciación, incluidos los vídeos. Este paquete es ideal para los clientes que tienen intención de administrar el programa de formación para concienciar en materia de seguridad más eficaz y completo. Con acceso a más herramientas para identificar el riesgo, cambiar el comportamiento y reducir la exposición, puede aplicar una estrategia más efectiva de reducción de riesgos centrados en las personas.

SEGURIDAD DE APLICACIONES EN LA NUBE

Proteja a sus empleados y sus datos frente a amenazas, pérdidas de datos y riesgos de incumplimiento en las aplicaciones en la nube.

Cloud Account Defense (CAD)

Proofpoint Cloud Account Defense (CAD) ofrece protección automática contra el compromiso de cuentas y los archivos maliciosos en Office 365 y G Suite. El compromiso de cuentas suele comenzar por el phishing, el malware de robo de credenciales o el relleno de credenciales (*credential stuffing*) de fuerza bruta. Las cuentas comprometidas se utilizan normalmente para lanzar otros ataques, como los de fraude del CEO o phishing, tanto desde dentro como desde fuera de las organizaciones. CAD ayuda a detectar, investigar y defenderse rápidamente frente a los ciberdelincuentes que acceden a sus datos sensibles y a sus cuentas de confianza. Esta solución le proporciona detección de amenazas centradas en las personas, correlación de actividad de amenazas, análisis forense granular con inteligencia detallada de amenazas, y políticas flexibles para aplicar una respuesta automática.

Cloud App Security Broker

Proofpoint Cloud App Security Broker (PCASB) protege a las empresas frente al compromiso de cuentas en la nube, el exceso de datos confidenciales compartidos y los riesgos de incumplimiento de normativas en la nube. PCASB proporciona una vista granular centrada en las personas, del acceso a las aplicaciones y la gestión de los datos. Nuestra solución combina detección de cuentas comprometidas, control de acceso, prevención de la pérdida de datos (DLP), control de aplicaciones de terceros y análisis, para ayudarle a proteger Microsoft Office 365, G Suite, Box, etc. Nuestros potentes análisis le ayudan a conceder a los usuarios y a las aplicaciones en la nube los niveles de acceso adecuados en función de los factores de riesgo relevantes para usted.

PROTECCIÓN DE LA INFORMACIÓN

Encuentre, investigue y proteja los datos en el correo electrónico, las aplicaciones en la nube, los archivos de recursos compartidos localmente y SharePoint

Email Data Loss Prevention (DLP)

Proofpoint Email DLP evita los descuidos de los empleados en las comunicaciones salientes, para impedir la pérdida de información privada y confidencial. En lugar de obligar a los usuarios a tomar decisiones de políticas sobre el tipo y el nivel de protección del contenido que envían (lo que puede incrementar su carga de trabajo y el tiempo), puede dejarles que trabajen con normalidad mientras nuestra solución implementa políticas de comunicación por correo electrónico de manera centralizada y automática. Con más de 80 políticas configuradas específicamente, que localizan, clasifican y bloquean automáticamente los mensajes confidenciales, puede estar seguro de que las posibilidades de que se produzca una fuga de datos son reducidas.

Email Encryption

Proofpoint Email Encryption utiliza cifrado basado en políticas para que la comunicación segura a través de mensajes y archivos adjuntos sea automática y simple para sus usuarios. Los servicios de cifrado del correo electrónico tradicionales pueden presentar dificultades para los usuarios, sin embargo con Email Encryption no necesitan cifrar de forma manual los mensajes que envían y reciben, ya que esto se realiza en segundo plano. Con nosotros, puede proteger los mensajes de correo electrónico confidenciales garantizando al mismo tiempo que sus colaboradores, partners comerciales y usuarios puedan seguir accediendo sin problema a los mensajes protegidos desde sus ordenadores o dispositivos móviles.

Data Discover

Proofpoint Data Discover descubre, supervisa y protege los datos confidenciales en archivos de recursos compartidos, almacenes de datos (data stores) y sitios de SharePoint. Para ello, automatiza el análisis de contenido para seguir el rastro de la información por la red local de su organización. A continuación identifica automáticamente los datos confidenciales —incluida la información sanitaria y de identificación personal (PHI y PII)— que esté en riesgo de exposición no autorizada, y facilita la reparación en tiempo real mediante la puesta en cuarentena, copia o eliminación.

Meta

Proofpoint Meta es la nueva generación de acceso seguro a aplicaciones empresariales. Meta, una solución centrada en las personas, garantiza que los empleados, contratistas y partners tengan acceso basado en la identidad, con confianza cero, a los recursos de la empresa en el centro de datos y en cualquier nube.

ObserveIT Insider Threat Management

Proofpoint adquirió ObserveIT en noviembre de 2019. Insider Threat Management ofrece una solución para endpoints ligera que ayuda a las organizaciones a identificar y mitigar el riesgo de amenazas internas. La solución proporciona detección y prevención para defender los datos frente al comportamiento malintencionado y negligente de empleados, usuarios con privilegios y terceros.

Con Insider Threat Management, las organizaciones pueden reducir considerablemente el riesgo de incidentes de seguridad, mediante la supervisión del comportamiento de los usuarios y ofreciendo formación y disuasión en tiempo real. ObserveIT reduce el tiempo de investigación de días a minutos y ofrece una reproducción completa de los incidentes de seguridad para mejorar los tiempos de respuesta y simplificar el cumplimiento de normativas.

PROTECCIÓN FRENTE A RIESGOS DIGITALES

Proteja su marca y a sus clientes de las amenazas de redes sociales, dominios web y la Internet oscura (Dark Web).

Digital Risk Protection

Proofpoint Digital Risk Protection protege a sus clientes y sus marcas frente a los riesgos para la seguridad digital que albergan los dominios web, las redes sociales y la Internet profunda (Deep Web). Esto implica defender los dominios corporativos contra el fraude de marcas; proteger y supervisar las cuentas de redes sociales con el fin de detectar el phishing, la usurpación de cuentas y el spam; controlar la actividad en la Internet profunda (Deep Web) y oscura (Dark Web) para descubrir amenazas contra directivos de la empresa, filtraciones de credenciales, ubicaciones de ataques físicos y eventos cercanos de gran impacto. Gracias al aprendizaje automático, nuestra solución le permite anticiparse a las amenazas, ya estén planificadas, sean inminentes o se estén produciendo en tiempo real.

ARCHIVADO Y CUMPLIMIENTO DE NORMATIVAS

Conserve, descubra y supervise los datos en todas las plataformas de comunicación para garantizar el cumplimiento de las normativas.

Enterprise Archive

Proofpoint Enterprise Archive usa inteligencia en la nube y aprendizaje automático para conservar y descubrir información esencial para la empresa de una forma que sea fácil de encontrar. Aborda tres retos fundamentales: descubrimiento legal, cumplimiento de normativas y reducción de costes y dificultad. Y lo hace sin el esfuerzo que supone para el equipo de TI gestionar el archivado de forma interna en la empresa. Nuestra arquitectura escalable en la nube, el resultado garantizado de las búsquedas, el excepcional nivel de satisfacción del cliente y el cifrado más sofisticado de la industria le otorgan un control total de las cuestiones legales y el cumplimiento de normativas.

Enterprise Collaboration Archive

Proofpoint Enterprise Collaboration Archive aplica controles basados en políticas para capturar el contenido de las redes sociales Salesforce Chatter, Jive, Skype Enterprise, LinkedIn, Twitter y otras plataformas, con el fin de facilitar su revisión o gestión como cualquier otro recurso de datos crítico de su plataforma de supervisión o su archivo de cumplimiento de normativas. De esta manera puede garantizarse el cumplimiento de las normativas relevantes para su caso. Además, le proporciona funciones avanzadas que automatizan y simplifican las tareas de cumplimiento fundamentales,

Intelligent Supervision

Proofpoint Intelligent Supervision ayuda a las compañías de servicios financieros a simplificar el cumplimiento de las normativas más exigentes y complejas del mundo, como FINRA, SEC e IIROC. Esta solución está totalmente integrada con Enterprise Archive y emplea aprendizaje automático para facilitar una captura, revisión y generación de informes eficaces y conformes con los requisitos normativos. De esta forma disfruta de visibilidad total de todo su correo electrónico, mensajes instantáneos, herramientas de colaboración, voz, SMS y redes sociales.

E-Discovery Analytics

Proofpoint E-Discovery Analytics ofrece un intuitivo flujo de trabajo de descubrimiento electrónico para los equipos del departamento legal. Gracias al empleo de aprendizaje automático con resultados de búsquedas en tiempo real y análisis anticipados integrados, aumenta la información obtenida. Le ayudamos a estar preparado para los procesos de litigio, lo que redunda en una mejora del control y una reducción de los riesgos.

Cumplimiento de normativas en redes sociales

Proofpoint permite garantizar el cumplimiento de las normativas actuales en las prácticas de marketing en redes sociales para que los usuarios no corran riesgos de incumplimiento en este ámbito. Digital Risk Protection se integra perfectamente con las principales soluciones de archivado para recopilar y clasificar el contenido de las redes sociales con el fin de facilitar las búsquedas y procedimientos de e-discovery en el futuro. Todo esto le permitirá ahorrar tiempo y dinero durante una auditoría.

MÁS INFORMACIÓN

Para obtener más información, visite **proofpoint.com/es**.

ACERCA DE PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) es una compañía líder en ciberseguridad 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. Compañías líderes de todos los tamaños, entre las que se encuentran más de la mitad del Fortune 1000, confían en las soluciones de Proofpoint para su seguridad centrada en personas y su cumplimiento regulatorio, mitigando los riesgos más críticos en sus sistemas de correo electrónico, cloud, redes sociales y web. Encontrará más información en **www.proofpoint.com/es**.

proofpoint.

1201-002-01-01 02/20