Proofpoint Email Protection

Detección y bloqueo de amenazas del correo electrónico maliciosas y sin malware

VENTAJAS PRINCIPALES

- Bloqueo en el punto de entrada de estafas BEC, ataques de phishing y malware avanzado
- Llamada de atención del usuario con etiquetas de advertencias de correo electrónico
- Mejora de la productividad con seguimiento rápido de los mensajes e higiene del correo electrónico
- Adaptación para grandes empresas gracias a su total flexibilidad
- Eficiencia operativa a través de la automatización de las operaciones de seguridad y la respuesta a amenazas
- Ampliación de la protección con autenticación y cifrado del correo electrónico integrados, DLP en el correo electrónico y Targeted Attack Protection, entre otras funcionalidades
- Acuerdos de nivel de servicio (SLA) líderes del sector cuando se despliega en cloud:
  - Disponibilidad de servicio del 99,999 %
  - Protección frente a virus del 100 %
  - Menos de 1 minuto de latencia del correo electrónico
  - 99 % de spam bloqueado o redirigido

Proofpoint Email Protection ayuda a proteger y controlar el correo electrónico entrante y saliente. Esta solución emplea aprendizaje automático y técnicas de detección multicapa para identificar y bloquear el correo electrónico malicioso. Además, clasifica de forma dinámica las amenazas actuales y otros incidentes habituales, y ofrece control granular sobre una amplia variedad de correo electrónico, como los mensajes fraudulentos, el phishing, el malware, el spam o el correo masivo, entre otros. También ofrece una flexibilidad total, con políticas de seguridad personalizadas y reglas de enrutamiento del correo. Es la solución de seguridad del correo electrónico más desplegada en empresas Fortune 1000, ya que se escala incluso para las empresas más grandes. Además, admite instalaciones cloud, locales e híbridas.

El correo electrónico es el principal vector de ataque: más del 96 % de las amenazas que aprovechan la ingeniería social (probadas o sospechosas) llegan por correo electrónico[1]. Además de las amenazas más habituales para el correo electrónico, como el phishing y el malware, las estafas Business email compromise (BEC) representan una nueva amenaza para las empresas. Proofpoint Email Protection detecta las amenazas, tanto conocidas como desconocidas, que pasan desapercibidas para otras soluciones. Proofpoint procesa miles de millones de mensajes al día, por lo que observa más amenazas, las detecta más rápidamente y le protege mejor contra amenazas que no emplean malware, como el correo electrónico fraudulento. Con Email Protection, puede detener una gran mayoría de amenazas antes de que lleguen a la bandeja de entrada de sus empleados.

Detección de amenazas emergentes que otras soluciones pasan por alto

Detección de mensajes phishing, de impostores y fraudulentos

Email Protection detecta las amenazas emergentes antes de que lleguen a la bandeja de entrada de sus empleados. Proofpoint Advanced BEC Defense, optimizada por NexusAI, está diseñada para bloquear eficazmente una amplia variedad de estafas por correo electrónico, como el redireccionamiento de pagos y el fraude de facturas de proveedores desde cuentas comprometidas. Estas amenazas requieren técnicas de detección más sofisticadas, ya que normalmente no tienen payload maliciosa que detectar.

1 Data Breach Investigations Report (Informe de investigaciones de fugas de datos), Verizon, 2020

Proofpoint Advanced BEC Defense es nuestro motor de detección basado en aprendizaje automático e inteligencia artificial. Está especialmente diseñado para detectar y bloquear ataques BEC. Detecta de forma dinámica estos ataques mediante el análisis de varios atributos de los mensajes. Por ejemplo:

- Datos del encabezado del mensaje
- Dirección IP del remitente (dirección IP origen, reputación)
- Cuerpo del mensaje (urgencia, palabras o frases específicas)

Determina si el mensaje constituye una amenaza BEC. Y detecta varias tácticas utilizadas por los autores de ataques BEC, como:

- Cambios de la dirección de respuesta
- Uso de direcciones IP maliciosas
- Uso de dominios de proveedores cuya identidad ha sido usurpada

Advanced BEC Defense también proporciona visibilidad pormenorizada de los detalles de un ataque BEC (tema, timos de las tarjetas regalo, redirección de nóminas, facturación, señuelo, tarea, etc.). Explica por qué el mensaje es sospechoso y ofrece ejemplos de mensajes. De esta forma, su equipo de seguridad puede comprender y comunicar mejor el ataque. Los datos recopilados por NexusAI se integran en el gráfico de amenazas Nexus de Proofpoint. Este analiza y correlaciona información sobre amenazas a nivel de correo electrónico, nube y redes sociales de todos nuestros clientes. Esto le ofrece una protección que le permite ir un paso por delante de las amenazas.

Bloqueo del correo electrónico malicioso y no deseado

Hemos integrado técnicas de detección multicapa en Proofpoint Email Protection para defender contra las amenazas que evolucionan continuamente. Con la detección basada en firmas, esta solución bloquea las amenazas conocidas, como los virus, los troyanos y el ransomware. Además, emplea análisis de reputación dinámicos para evaluar de forma continua las direcciones IP locales y globales con el fin de determinar si deben aceptarse las conexiones por correo electrónico. Nuestro exclusivo clasificador de correo electrónico clasifica de forma dinámica una amplia variedad de mensajes de correo electrónico, como los fraudulentos, de phishing, malware, spam, correo masivo, contenido para adultos y del círculo de confianza. Además, pone en cuarentena el correo entrante por tipo. En conjunto, estas funciones le ayudan a protegerse ante los primeros signos de actividad maliciosa.

Seguimiento de los mensajes en cuestión de segundos

Proofpoint Email Protection dispone de la función de búsqueda más potente. Con esta función inteligente, puede identificar fácilmente datos de registros difíciles de encontrar, en base a decenas de criterios de búsqueda. Asimismo, puede controlar rápidamente de dónde vienen los mensajes y a dónde se dirigen. Email Protection proporciona detalles específicos de los resultados de las búsquedas, como metadatos con más de cien atributos.

Las búsquedas se realizan en segundos, no en minutos. Puede descargar y exportar los resultados de su búsqueda (hasta un millón de registros). Además, el producto integra varios informes en tiempo real, lo que ofrece visibilidad detallada del flujo y las tendencias del correo. Con estos datos, puede abordar de forma proactiva los problemas a medida que surgen.

Adaptación para grandes empresas gracias a su total flexibilidad

Proofpoint Email Protection satisface las exigencias de las empresas más grandes del mundo. Permite crear reglas de firewall a nivel global, de grupos y de usuarios. Puede crear las políticas de seguridad y las reglas de enrutamiento del correo que mejor se adapten a sus necesidades, e implementarlas con facilidad. Email Protection ofrece las mismas ventajas y una mayor flexibilidad, con múltiples opciones de despliegue, como hardware local, máquina virtual y SaaS.

Concienciación del usuario sobre seguridad

Las etiquetas de advertencia en el correo electrónico permiten a sus empleados tomar decisiones más fundamentadas sobre los mensajes cuando se desconoce si están limpios o son maliciosos. Estas etiquetas ofrecen una breve descripción del riesgo asociado con un mensaje concreto e indican el nivel de exposición con distintos colores, lo que facilita su identificación a sus empleados. De esta forma pueden denunciar los mensajes sospechosos directamente cuando ven la etiqueta de advertencia, incluso si acceden al correo electrónico desde dispositivos móviles. Esta función reduce el riesgo de ataque potencial, ya que los empleados serán más cautos cuando se trate de mensajes no seguros.

Proofpoint Email Protection permite también a los administradores del correo electrónico ofrecer a los usuarios la posibilidad de gestionar mensajes cifrados y de baja prioridad, como el correo masivo, o revisar los mensajes en cuarentena y tomar las medidas oportunas directamente en el panel de tareas de Outlook. Las opiniones de los usuarios se transmiten a Proofpoint y esto nos ayuda a mejorar la precisión global en la clasificación del correo masivo.

Administración centralizada de Email Encryption e Email DLP

Puede ampliar su protección con facilidad agregando Proofpoint Targeted Attack Protection, Email Fraud Defense, Email Encryption o Email Data Loss Prevention (DLP). Email Protection proporciona funciones básicas de DLP y cifrado del correo electrónico, pero puede disfrutar de soluciones más avanzadas a través de la misma consola de administración. Esta estrecha integración le ayuda a gestionar los datos confidenciales que se envían por correo electrónico. Además, evita la fuga o pérdida de datos a través del correo electrónico. Por último, cumple varios requisitos de cumplimiento regulatorio.

MÁS INFORMACIÓN

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