proofpoint.

RESUMEN DE LA SOLUCIÓN

Proofpoint Active Exploits Protection

Bloquee los exploits desde el primer momento, antes de que se ejecuten

Ventajas principales

- Protección de primer nivel contra exploits en el buzón de correo: identifica y bloquea la actividad maliciosa antes de que se ejecute la payload o se comprometa el endpoint.
- Priorización de vulnerabilidades basada en exploits activos en entornos reales.
- Reducción de la exposición antes del despliegue de parches, con protección frente a malware basado en exploits y actividades de comando y control.
- Aceleración de las investigaciones gracias a datos contextuales sobre amenazas actuales y pasadas e inteligencia de detección actualizada de forma continua.
- Preparación para los flujos de trabajo de seguridad basados en IA y en agentes.

Descripción general

La velocidad de aprovechamiento de vulnerabilidades y el volumen de ataques siguen en aumento El número de vulnerabilidades reveladas alcanza niveles sin precedentes, y los ciberdelincuentes las explotan más rápido que nunca. Las soluciones tradicionales se basan en puntuaciones de gravedad, no en lo que los ciberdelincuentes están explotando en este momento.

Proofpoint Active Exploits Protection supone un punto de inflexión.

Gracias a su visibilidad sobre la distribución de exploits en el correo electrónico y el tráfico de red, Proofpoint ayuda a las organizaciones a detectar actividades maliciosas antes de que se ejecute la payload. La solución combina inteligencia sobre vulnerabilidades activas, priorización orientada a las tácticas de los ciberdelincuentes y protección instantánea para que los equipos de seguridad reduzcan su exposición donde más importa. El resultado es un enfoque más proactivo de la protección contra los exploits, basado en la prevención de los ataques en una fase más temprana de la cadena de ataque.

La solución: inteligencia sobre vulnerabilidades desde el primer momento y protección inmediata

Proofpoint Active Exploits Protection transforma la inteligencia sobre vulnerabilidades activas en protección práctica y en una respuesta priorizada. La solución combina inteligencia sobre exploits basada en los ciberdelincuentes, detección de amenazas en correo electrónico y red, e integraciones operativas para identificar y detener la actividad de exploits antes de su ejecución.

Gracias a una visibilidad de primer orden sobre los exploits distribuidos por correo electrónico (principal vector de los ataques modernos), Proofpoint identifica los intentos de distribución de exploits y el comportamiento real de los ciberdelincuentes desde las primeras fases de la cadena de ataque, antes de la ejecución de la payload, el compromiso de endpoints o el desplazamiento lateral.

Proofpoint Active Exploits Protection aprovecha esta inteligencia única sobre vulnerabilidades y la amplia cobertura de amenazas basadas en la red y exploits para ayudar a las organizaciones a priorizar las vulnerabilidades en función de su explotación activa, reducir su exposición mientras se aplican los parches y acelerar las investigaciones gracias a una inteligencia de amenazas útil.

Priorice las vulnerabilidades confirmadas frente a los riesgos teóricos

Centre los esfuerzos de corrección en las vulnerabilidades que los ciberdelincuentes explotan activamente, no solo en las puntuaciones CVSS altas.

Proofpoint Active Exploits Protection correlaciona la inteligencia sobre los ataques y el comportamiento de los ciberdelincuentes observados a través de fuentes de telemetría de todo el mundo para ayudar a las organizaciones a identificar rápidamente las vulnerabilidades que suponen un riesgo operativo inmediato.

Este enfoque centrado en los ciberdelincuentes ayuda a los equipos de seguridad a reducir el ruido, establecer mejores prioridades y concentrar los recursos en las vulnerabilidades con mayor probabilidad de explotación.

Sus principales funciones son las siguientes:

- Priorización de parches basada en vulnerabilidades CVE con actividad de explotación real.
- Distinción entre amenazas urgentes y riesgos de menor prioridad.
- Priorización de las correcciones basada en un contexto claro y útil sobre las amenazas, incluyendo flujos de reputación de direcciones IP y dominios en tiempo real.
- Ajuste de prioridades según la actividad real de los ciberdelincuentes para mejorar la orientación operativa.

Protección inmediata mientras se aplican los parches

La aplicación de parches lleva tiempo. Proofpoint Active Exploits Protection ayuda a las empresas a reducir su exposición durante este periodo, proporcionando información constantemente actualizada sobre las vulnerabilidades y ofreciendo protección inmediata para el correo electrónico y el tráfico de red.

Ofrece una lógica de detección fiable y oportuna para amenazas avanzadas, entre las que se incluyen:

- Distribución del malware
- Comunicaciones de mando y control
- Kits de exploits
- Phishing de credenciales
- Propagación del ataque
- Ransomware, redes de bots
- Anomalías de protocolos y aplicaciones
- Minería de monedas
- Ataques de denegación de servicio distribuidos (DDoS)
- Ataques contra los sistemas de control de supervisión y adquisición de datos (SCADA)

Sus principales funciones son las siguientes:

- Inteligencia sobre exploits que se actualiza constantemente y diseñada para mejorar la protección en una fase más temprana de la cadena de ataque.
- Reglas de detección basadas en la red para sistemas IDS, IPS y NGFW, y controles de seguridad asociados.
- Firmas fiables para devoluciones de llamadas de malware, droppers (instaladores de malware), comunicaciones de comando y control, ofuscación, amenazas relacionadas con kits de explotación y filtración.
- Actualizaciones diarias de las reglas para seguir la evolución del panorama de amenazas.
- Cobertura de las principales familias de malware, campañas de ataque y vectores de amenazas basados en la red.
- Compatibilidad con los formatos IDS e IPS más utilizados, incluidos despliegues compatibles con Suricata y Snort.

Amplíe sus herramientas de seguridad con inteligencia global de amenazas

Proofpoint Active Exploits Protection proporciona inteligencia útil que se integra con una amplia gama de herramientas de seguridad, entre las que se incluyen firewalls, soluciones IDS, IPS, NGFW, UTM y SIEM, sistemas de autenticación, plataformas de caza de amenazas, flujos de trabajo de respuesta a incidentes y herramientas de seguridad personalizadas.

La solución proporciona inteligencia sobre la reputación y las amenazas relacionadas con direcciones IP, dominios, malware, firmas y campañas sospechosas y maliciosas, así como sobre las actividades de ataque asociadas.

Sus principales funciones son las siguientes:

- Información de amenazas actual e histórica relativa a direcciones IP, dominios, hash de malware, firmas y contenido de los mensajes
- Fuentes de reputación IP y de dominio organizadas por categoría de amenaza y puntuación de confianza
- Actualizaciones frecuentes de los flujos con envejecimiento acelerado para reflejar la actividad actual
- Base de datos mundial de amenazas consultable que permite la navegación, la exploración en profundidad y la investigación
- Compatibilidad con múltiples formatos de flujo de datos para la integración operativa, incluidos los formatos TXT, CSV, JSON, IDS y comprimidos
- Enriquecimiento basado en API para herramientas SIEM, TIP, de respuesta a incidentes y herramientas internas

Mejore la precisión de la detección y reduzca el ruido

Proofpoint Active Exploits Protection se basa en observaciones de amenazas reales, análisis de malware, información de sensores de todo el mundo e investigaciones sobre amenazas. Este enfoque contribuye a una detección extremadamente fiable, al tiempo que reduce los falsos positivos en las herramientas de seguridad de red existentes.

Sus principales funciones son las siguientes:

- Contenido de las detecciones basado en las investigaciones y en las amenazas observadas.
- Análisis de malware en un entorno aislado (sandbox) para capturar el comportamiento de red tras su ejecución.
- Datos procedentes de sensores de todo el mundo para aumentar la precisión de la detección.
- Descripciones de firmas, referencias y documentación para respaldar los flujos de trabajo de los analistas.
- Aplicación de las políticas basada en categorías y alineada con las prioridades de la empresa.

Evolucione con flujos de trabajo impulsados por la IA

Proofpoint Active Exploits Protection está diseñada para gestionar las operaciones de seguridad modernas basadas en la inteligencia de amenazas. Se prevé que las funciones futuras permitan el acceso a la inteligencia de amenazas a través del protocolo MCP y de flujos de trabajo basados en agentes, lo que facilitará los casos de uso impulsados por API e IA.

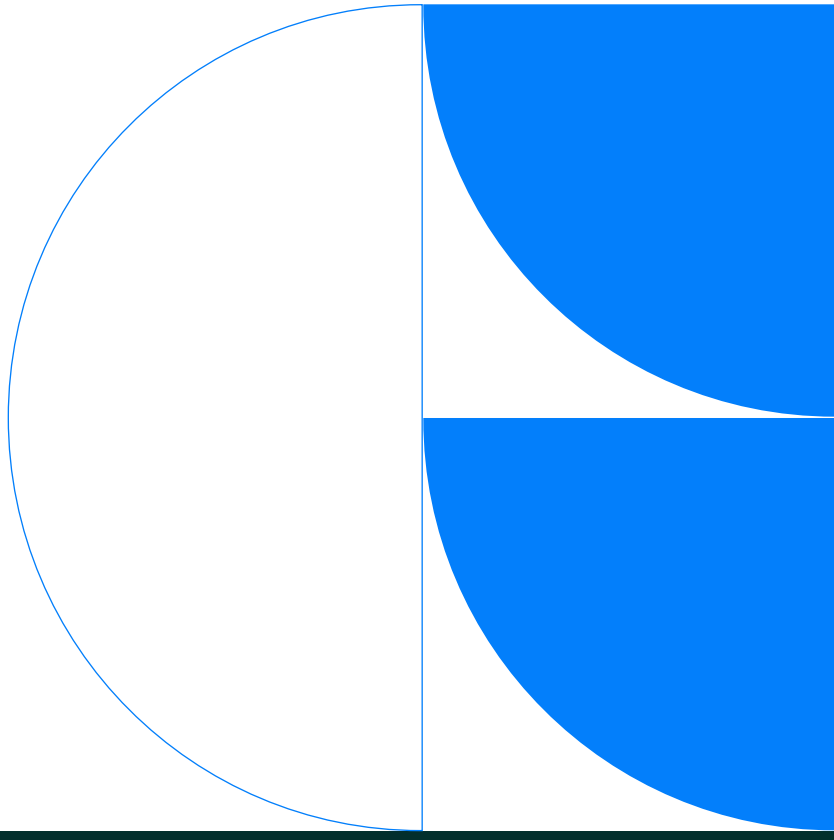
Estos flujos de trabajo tienen como objetivo ayudar a los equipos a integrar directamente la inteligencia de amenazas priorizada en las operaciones de seguridad automatizadas, acelerar la toma de decisiones y reducir la clasificación manual.

Resumen

Proofpoint Active Exploits Protection ayuda a las organizaciones a prevenir ataques basados en vulnerabilidades antes de que se produzcan brechas, combinando visibilidad de primer nivel sobre exploits en correo electrónico, inteligencia de vulnerabilidades consciente del adversario y protección instantánea.

En lugar de basarse únicamente en las puntuaciones de gravedad de las vulnerabilidades o en modelos teóricos de exposición, Proofpoint Active Exploits Protection permite a los equipos de seguridad establecer prioridades en función de los objetivos reales de los ciberdelincuentes.

Al unificar la definición de prioridades, la protección y la investigación, Proofpoint Active Exploits Protection ayuda a los equipos de seguridad a centrarse en lo que realmente importa, a ofrecer protección inmediata y a investigar con mayor rapidez.



proofpoint.