PERCEPTION POINT

Seguridad de correo electrónico avanzada

Prevención de amenazas para la empresa moderna

Puntos principales.

Prevención en tiempo real
Bloquea el contenido malicioso antes de que llegue al usuario final.

Visibilidad del X-Ray
Nuestra consola para cualquier código ejecutado por el sistema para una visibilidad del 100% de las intenciones maliciosas.

Escaneo profundo
Descomprime los archivos y siga las URL para detectar intenciones maliciosas evasivas.

Retraso cero
Los motores en línea funcionan en cuestión de segundos.

Implementación con un solo clic
Implementación fácil y rápida en la nube. Sin cambios en los procesos existentes.

Escala ilimitada
Escanea el 100 % del tráfico de correo electrónico, independientemente del volumen.

Servicios de correo electrónico
Office 365, Gmail, cualquier servicio de correo electrónico en la nube, Exchange.

Privacidad y cumplimiento
Cumple con SOC2. No hay datos almacenados en los servidores.

Respuesta a amenazas 24/7
Equipo de inteligencia experto monitoreando continuamente los incidentes.

Contáctanos

www.perception-point.io
info@perception-point.io

Estamos en Boston | Tel Aviv

La necesidad urgente de seguridad de correo electrónico de última generación.

El correo electrónico es la fuente del 91 % de los ataques dirigidos y, a pesar de que existen muchas soluciones de correo electrónico, la mayoría de las empresas siguen estando muy expuestas. Por un lado, los hackers sofisticados están continuamente innovando y ahora pueden evadir las tecnologías AV, Sandbox y CDR.

Por otro lado, múltiples implementaciones han dado como resultado un caos de soluciones que genera mayores costes, complejidad y demoras. Existe una necesidad urgente de tecnología de próxima generación que sea mucho más efectiva contra el panorama completo de amenazas, al mismo tiempo que se alinea con la empresa moderna en la nube.

NUESTRA SOLUCIÓN:

Intercepción más rápida + protección holística.

Nuestra seguridad de correo electrónico avanzada combina la prevención de amenazas de vanguardia con la velocidad, la escala y la flexibilidad de la nube. Hemos incorporado múltiples motores de análisis e inteligencia de amenazas para una protección mejorada contra ataques como phishing, spam, malware básico y BEC.

Para las amenazas avanzadas, hemos inventado una tecnología de vanguardia que combina la visibilidad del hardware con la agilidad del software para ver lo que pasan por alto las soluciones líderes. Escaneo a nivel de CPU para interceptar ataques en la etapa más temprana posible, el exploit, incluso antes de que se entregue el malware.

Nuestra seguridad de ciberseguridad como servicio se implementa con un solo clic, se analiza en segundos y tiene una escala ilimitada para escanear siempre el 100 % de su tráfico.

Cobertura de 0-days, N-days y amenazas diarias.

Nuestra plataforma protege su negocio de toda la gama de ataques

Amenazas cotidianas	Amenazas N-Days	Amenazas 0-Days
Basado en firmas + ataques payload less	Ataques enmascarados y software sin parches	Vulnerabilidades desconocidas
Spam, phishing, malware, BEC y ATO	Exploits aprovechando vulnerabilidades conocidas.	Exploits que aprovechan vulnerabilidades desconocidas en Office, Adobe y navegadores.
	Las firmas alteradas impiden la detección.	

Lo que dicen nuestros clientes:

> *"La integración de la plataforma de Perception Point en nuestro Offce365 fue rápida y sin problemas y no tuvo ningún impacto en nuestros niveles de servicio de correo electrónico. En menos de un mes, ya bloquearon un ataque potencialmente dañino que podría haber engañado fácilmente a nuestros usuarios y causado una interrupción grave. Es raro ver retornos inmediatos tan rápido".*
>
> – CISO, sector sanitario

Solución en capas inherente

Capas estándar mejoradas + protección APT de última generación para la defensa de mayor rendimiento del mercado.

Amenazas típicas | phishing, malware, suplantación de identidad, BEC, etc.

1

Filtro spam

recibe el correo y aplica filtros de reputación y antispam para rápidamente saber si se trata de un email malicioso.

2

Recursive Unpacker.

Divide el contenido en unidades más pequeñas (archivos y URLs) para identificar ataques maliciosos ocultos, extrayendo URLs y archivos incrustados de forma recursiva. Todos los componentes extraídos pasan por separado a través de nuestras múltiples capas de seguridad.

3

Threat Intelligence.

Combina múltiples fuentes de inteligencia de amenazas con nuestro producto desarrollado internamente para escanear URLs y archivos, y así identificar ataques.

4

Filtros phishing

1.Combina los mejores filtros de reputación de URLs y de análisis de imágenes (desarrollados internamente) para identificar técnicas de suplantación de identidad y phishing.

5

Firmas estáticas

Combina los mejores motores antivirus junto con tecnología patentada para identificar firmas complejas.

6

BEC y ATO

Previene ataques payload-less que no necesariamente incluyen archivos/URL maliciosos e intentos de apropiación de cuentas.

N-Days / 0-Days

Primera plataforma asistida por hardware (HAP™)

La exclusiva tecnología a nivel de CPU actúa antes en la cadena de destrucción que cualquier otra solución. Bloqueo de ataques en la fase de explotación (lanzamiento previo al malware) para una verdadera prevención de APT.

7

HAP™ (Dropper).

Emplea un motor avanzado basado en heurística para detectar errores lógicos y manejar macros y scripts.

8

HAP™ (CFG).

Registra la CPU mientras procesa la entrada (archivos y URL) e identifica exploits examinando todo el flujo de ejecución, detectando cualquier desviación del flujo normal de un programa para identificar de manera determinista la actividad maliciosa

9

HAP™ (FFG).

Detecta técnicas avanzadas, como exploits, que se escriben para eludir los algoritmos CFI comunes. Los gráficos de flujo de control conscientes de la semántica patentados desarrollados para cada aplicación identifican las desviaciones del flujo de ejecución durante el tiempo de ejecución

Prueba de 30 días gratuita y fácil

Simplemente contacta a sales@perception-point.io.

PERCEPTION POINT