PERCEPTION POINT

Seguridad de colaboración avanzada

Intercepción rápida de cualquier ataque en forma de contenido en todos los canales

Puntos principales

Cobertura de amenazas
Ataques avanzados persistentes
Days/N-Days-0
Phishing
Malware
Suplantación de identidad
BEC

Prevención en tiempo real
Block malicious content Bloquea el contenido malicioso antes de que llegue al usuario final

Visibilidad del X-Ray
CPU-level visibility seesDesempaqueta y sigue las URL para detectar intentos maliciosos evasivos

Escaneo profundo
Desempaqueta y sigue las URL para detectar intentos maliciosos evasivos

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

Escala ilimitada
Escanea el 100% del contenido, independientemente del volumen

Retraso cero
In-line engines work inLos motores en línea funcionan en segundos

Aplicaciones de oficina y de colaboración en la nube: Un creciente punto ciego de seguridad en toda la empresa

La necesidad de comunicarse y colaborar a nivel global ha creado una proliferación de herramientas alojadas en la nube dentro de las organizaciones. **Correo electrónico. Aplicaciones de almacenamiento en la nube. Plataformas de mensajería. Redes sociales. CRMs.** Hasta 20 aplicaciones por empresa

Pero con los nuevos canales surgen nuevas brechas para hackers y nuevos puntos ciegos de seguridad, haciéndose indispensable la visibilidad completa de las amenazas en todos los canales en una única solución

NUESTRA SOLUCIÓN

Detección de amenazas ágil y unificada para cualquier canal

Perception Point es una empresa de ciberseguridad -prevención como servicio-, implementada en minutos sin cambios en la infraestructura empresarial ni en las políticas cibernéticas. Brindamos la mejor protección a la empresa moderna contra ataques como BEC, phishing, spam, malware, 0-days & N-days, en todos los canales de comunicación

Además de la plataforma, el servicio incluye un eq1uipo de respuesta a incidentes que sirve como la extensión de vuestro equipo SOC. El equipo de IR optimiza los motores de detección de amenazas, proporciona la gestión de falsos positivos, monitoreo de incidentes, etc., lo que garantiza que la .plataforma funcione para tu organización y no al revés

Email

G Suite
Exchange
Office 365

Any web-based email service

Cloud Storage

OneDrive
Dropbox
Google Drive
box
SharePoint

Cloud Collaboration

Salesforce
slack

API

Integration with any other application where files or URLs are exchanged.

Custom development per client needs.

Prueba gratuita de 30 días

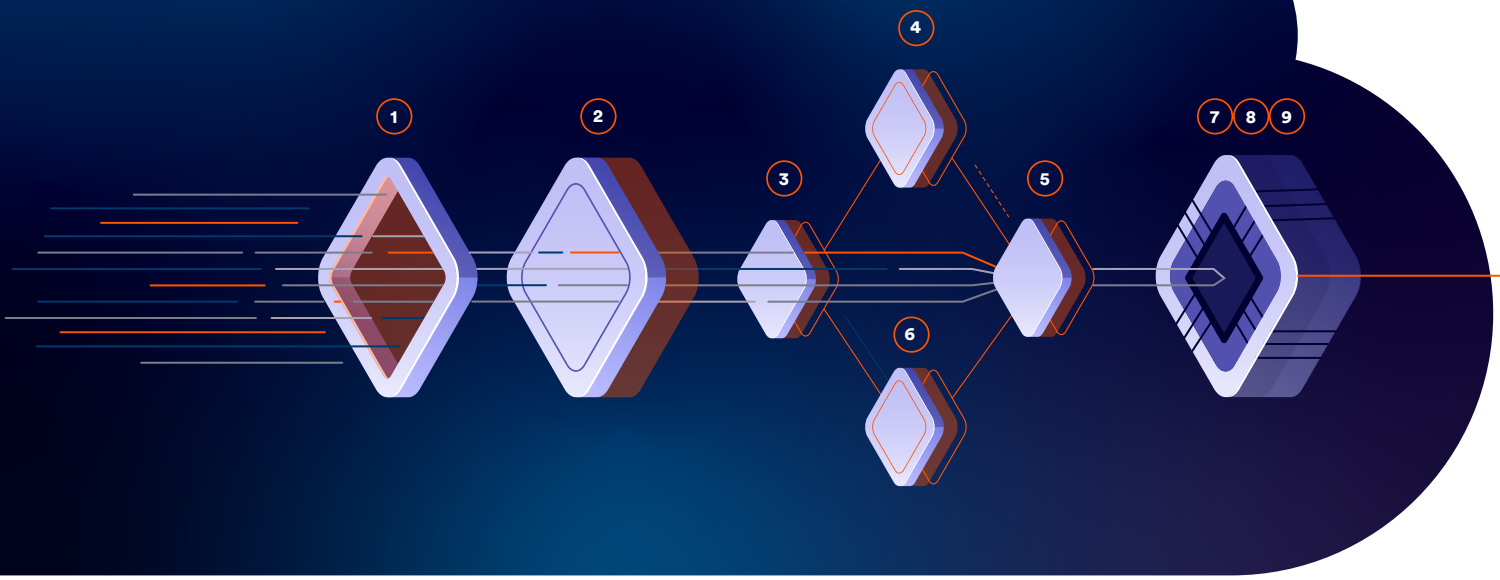
Configura una POC en menos de una hora, sin interferencias ni molestias para el usuario final o la organización. No se almacena ningún contenido y .todos los datos están encriptados

PERCEPTION POINT

Contáctanos

Inherent Layered Solution

Enhanced standard layers + cutting-edge APT protection for the most high-performance defense on the market.



Everyday Threats | Phishing, Malware, Impersonation, 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

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

Combines best-in-class signature based anti-virus engines to identify malicious attacks. In addition, we've developed a tool that acts to identify highly complicated signatures.

6

BEC y ATO

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

Primera plataforma asistida por hardware HAP™

UniqLa 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

Proteja múltiples canales con nuestra plataforma completa de seguridad de colaboración avanzada
Correo electrónico, mensajería, almacenamiento en la nube, CRM + API para cualquier canal de intercambio de contenido

PERCEPTION POINT