PERCEPTION POINT

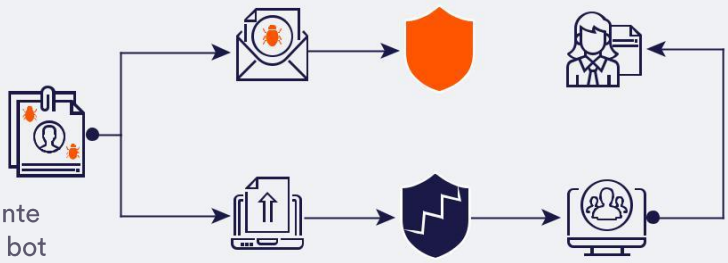
SOLUTION PAPER

Protección avanzada contra amenazas para aplicaciones web

La brecha de seguridad de contenido de las aplicaciones web

El intercambio de contenido y la carga de archivos se han convertido durante mucho tiempo en una función vital en las organizaciones digitalizadas. Es un elemento esencial en la colaboración y la productividad de la fuerza laboral, así como en la realización de negocios y la prestación de servicios. Las aplicaciones y servicios web comerciales y desarrollados internamente ayudan a las organizaciones a conectarse fácilmente con clientes, socios e incluso usuarios en línea no regulados. Al permitir que el contenido externo se comparta en el entorno empresarial, estos canales también representan un riesgo de seguridad, ya que crean una superficie de ataque adicional para que los actores de amenazas maliciosos apunten y comprometan. Si bien las empresas invierten mucho en sus arquitecturas de seguridad de red y correo electrónico, las aplicaciones web siguen estando protegidas de manera inadecuada y constituyen un punto ciego de seguridad.

> Un malware evasivo está incrustado en un CV Y está destinado a llegar a Gina, la reclutadora de recursos humanos de la empresa. Cuando se envía a gina.hr@your.company.com, su solución avanzada de seguridad de correo electrónico puede detectarlo a tiempo, pero ¿qué sucede si el currículum se carga directamente en un portal de "carreras" o se envía a través del bot de chat en su sitio web?



La detección tradicional es inadecuada

Los motores antivirus individuales pueden ser rápidos para emitir un veredicto y pueden manejar grandes alcances de cargas, pero no brindan una detección suficiente contra amenazas evasivas o desconocidas. Además, las soluciones que integran la tecnología sandbox tradicional pueden ser más eficaces contra los ataques avanzados, pero su falta de escalabilidad y su latencia adicional (minutos hasta el veredicto) las hacen inaceptables para la mayoría de las empresas. Otros enfoques como CDR pueden ser una buena opción para algunos casos, pero están limitados en cuanto a tipos de archivos y usabilidad de contenido.

Se recomienda que evalúe sus riesgos y exposición a ataques y agregue la protección requerida que sirva a la organización a cualquier escala sin afectar el negocio, e independientemente del tipo de contenido compartido.

Se requiere una solución de seguridad moderna.

PERCEPTION POINT

Perception Point: intercepte cualquier amenaza mientras mantiene el negocio como de costumbre

La solución nativa de la nube de Perception Point está diseñada para asegurar herméticamente cualquier flujo comercial que involucre flujos de archivos externos o contenido generado por el usuario; protección contra phishing, malware, ransomware, amenazas persistentes avanzadas, intentos de explotación de 0-days y más.

La galardonada plataforma emplea algoritmos avanzados de detección de amenazas de varias capas que identifican incluso los ataques más evasivos. Cada pieza de contenido se inspecciona a través de todas las capas de detección, incluido un sandbox de próxima generación que escanea dinámicamente el 100 % del tráfico (incluidos los archivos incrustados y las URL) en sus aplicaciones web en segundos para evitar que el contenido malicioso se infiltre en la organización.

Protección sin precedentes
Evitar la transmisión de cualquier archivo malicioso, URL o ataque de ingeniería social con > 99,95 % de tasa de detección comprobada

Despliegue rápido
Implemente en minutos en cualquier fuente de contenido o aplicación web

Velocidad inigualable
Escanee dinámicamente el 100% del tráfico en segundos

Privacidad y Cumplimiento
Cumpla con todas las regulaciones de datos: RGPD, HIPAA y SOC-2 TIPO II

Escala ilimitada
Analice millones de archivos sin latencia; con mecanismos de seguridad integrados

Respuesta a incidentes gestionada
Ahorre recursos con un equipo de IR todo incluido, un multiplicador de fuerza 24/7 para cualquier SOC

Asegure cualquier flujo de intercambio de contenido

Los portales web para usuarios externos, los foros de atención al cliente, las interfaces de administración de socios, los formularios de solicitud de empleo, las aplicaciones de chat y las soluciones de intercambio de contenido de terceros son solo algunos ejemplos de las herramientas que su empresa puede usar para comunicarse y colaborar de manera efectiva con usuarios fuera de la organización.

APLICACIONES INTERNAS	SOLUCIONES DE TERCEROS (APOYADAS POR ICAP)	
	Dispositivos de seguridad	Aplicaciones comerciales
Cargas a soluciones SaaS	WAF	SAP, MICRO FOCUS
Canales de soporte	CASB	Akamai, citrix
Interfaces cliente/proveedor	Gateways	Kiteworks
Herramientas de colaboración ad hoc	Proxies Web	ORACLE, ISILON SYSTEMS
Foros		
Aplicaciones de chat		
Portales de reclamos		

PERCEPTION POINT

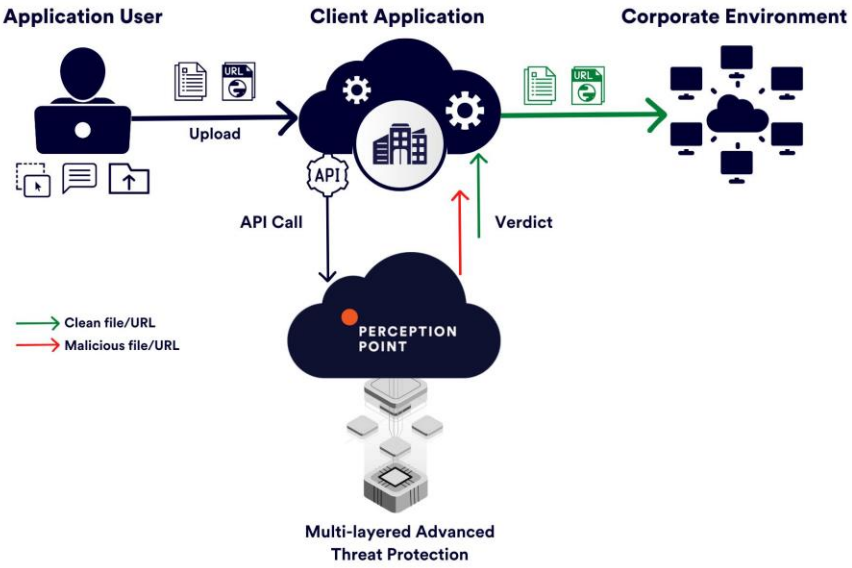
Implemente en minutos con cualquier aplicación web

Perception Point se integra fácilmente con cualquier aplicación web o proxy de seguridad a través de la API REST o la implementación de ICAP para mejorar su postura y prueba de seguridad.

API REST

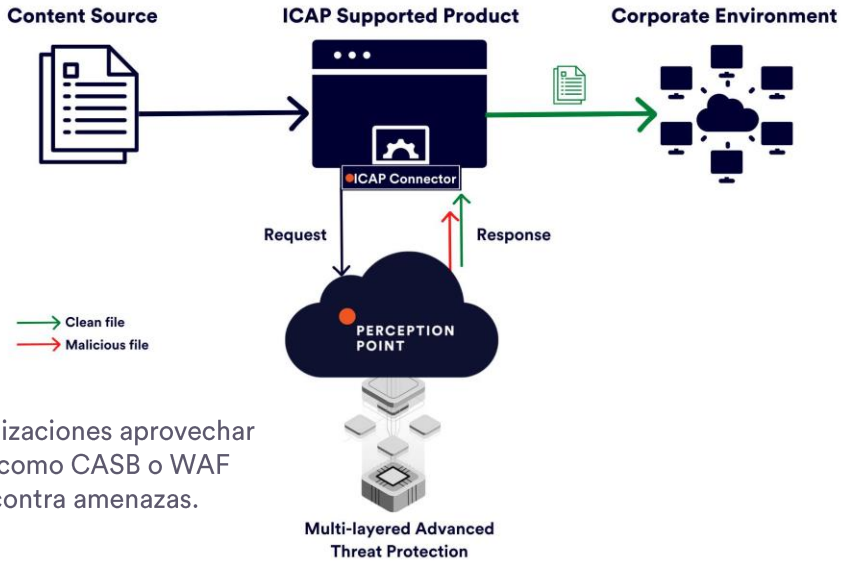
El uso de la API REST garantiza una escalabilidad y disponibilidad sin igual, se comparte contenido en tus aplicaciones se sube a Perception Point para un análisis profundo y analítico.

En segundos, Perception Point proporciona un veredicto limpio o malicioso, el cual, a su vez, elimina cualquier contenido malicioso.



ICAP

Perception Point puede conectarse sin problemas con cualquier aplicación o infraestructura que admita el Protocolo de adaptación de contenido de Internet (ICAP) y emplear la detección de múltiples capas. La integración se realiza a través de una instalación sencilla del conector ICAP de Perception Point en el entorno del cliente.

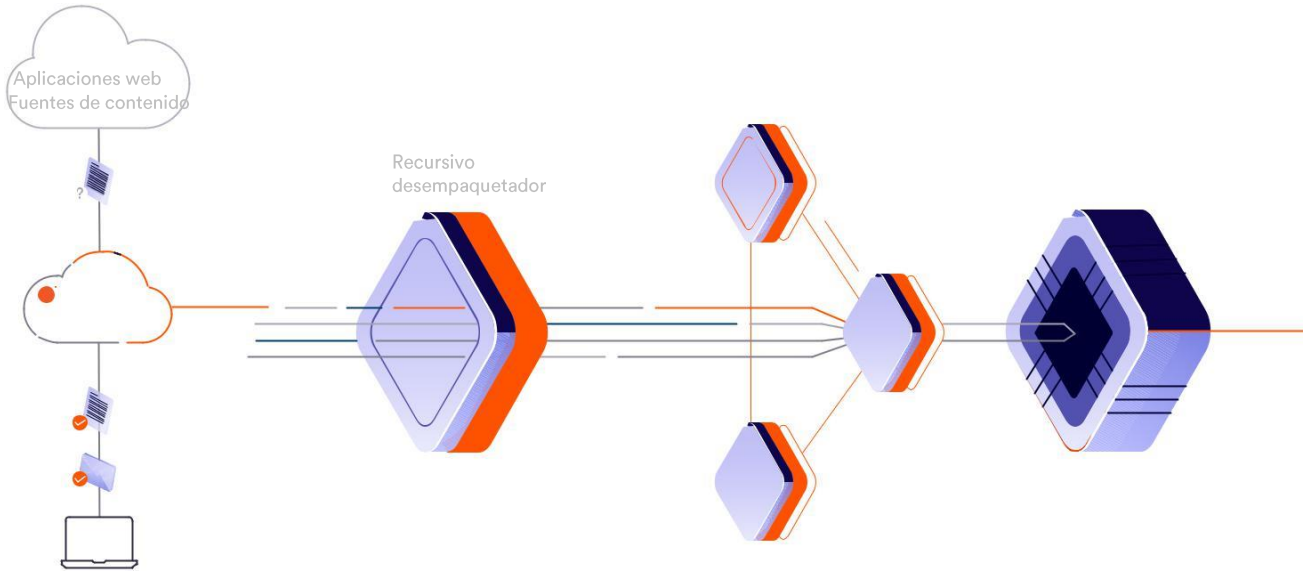


Además, el protocolo ICAP permite a las organizaciones aprovechar su inversión en soluciones de proxy existentes como CASB o WAF y agregarles fácilmente protección avanzada contra amenazas.

PERCEPTION POINT

Detección de amenazas avanzada galardonada y sin precedentes

Perception Point es pionera en la detección avanzada de amenazas y ha sido calificada como la número 1 en pruebas de laboratorios independientes por sus capacidades de detección una y otra vez. Los diferentes motores aprovechan algoritmos de detección de última generación que utilizan visión por ordenador, aprendizaje automático y varios métodos dinámicos y estáticos para interceptar todo tipo de amenazas, desde ataques básicos hasta amenazas avanzadas desconocidas.



1

"Recursive unpacker"

Descomprime el contenido en unidades más pequeñas (archivos y URL) para identificar ataques maliciosos incrustados. Todos los componentes extraídos recursivamente luego pasan individualmente a través de las siguientes capas de detección.

2

Firmas estáticas

Combina los mejores motores antivirus de la industria para identificar ataques maliciosos junto con tecnología patentada para la detección de firmas altamente complejas.

3

Motores antiphishing

Integra nuevos algoritmos de IA, como el reconocimiento de imágenes y el análisis léxico, con los mejores motores de reputación de su clase.

4

Inteligencia de amenazas

Combina múltiples fuentes de inteligencia de amenazas con un motor propio que escanea URL y archivos para aprender sobre ataques actuales y potenciales.

7

HAP™

Motor sandbox patentado de próxima generación que se compone de algoritmos de software que utilizan datos a nivel de CPU para acceder a toda la ejecución del procesador, para interceptar de forma determinista cualquier tipo de ataque desconocido o evasivo en entornos Windows y macOS. Esta capa propietaria brinda una detección sin precedentes contra la ejecución de código malicioso en scripts y ejecutables, vulnerabilidades de 0-days y N-days, errores lógicos, explotaciones de última generación y más.

Acerca de Perception Point

Perception Point es una empresa de prevención como servicio para el aislamiento, la detección y la remediación rápida y precisa de todas las amenazas en los principales vectores de ataque de una organización: correo electrónico, navegadores web y aplicaciones de colaboración en la nube. El servicio de respuesta a incidentes integrado de forma nativa y completamente administrado actúa como fuerza multiplicadora para el equipo SOC, reduciendo los gastos generales de administración, mejorando la experiencia del usuario y brindando información continua; proporcionando la mejor protección.

Implementado en minutos, sin cambios en la infraestructura de la empresa, el servicio patentado, nativo de la nube y fácil de usar reemplaza los engorrosos sistemas heredados para evitar bien el phishing, BEC, spam, malware, zero-day, ATO y otros ataques avanzados. antes de que lleguen a los usuarios finales. Las empresas y organizaciones de la Fortune 500 de todo el mundo están evitando ataques a través de su correo electrónico, navegadores web y canales de colaboración en la nube con Perception Point.

Para obtener más información sobre Perception Point, visite nuestro sitio web o síganos en LinkedIn, Facebook y Twitter.

© 2022 Perception Point. Reservados todos los derechos.

Visítenos: www.perception-point.io

Contáctenos: info@perception-point.io

PERCEPTION POINT