IDC MarketScape

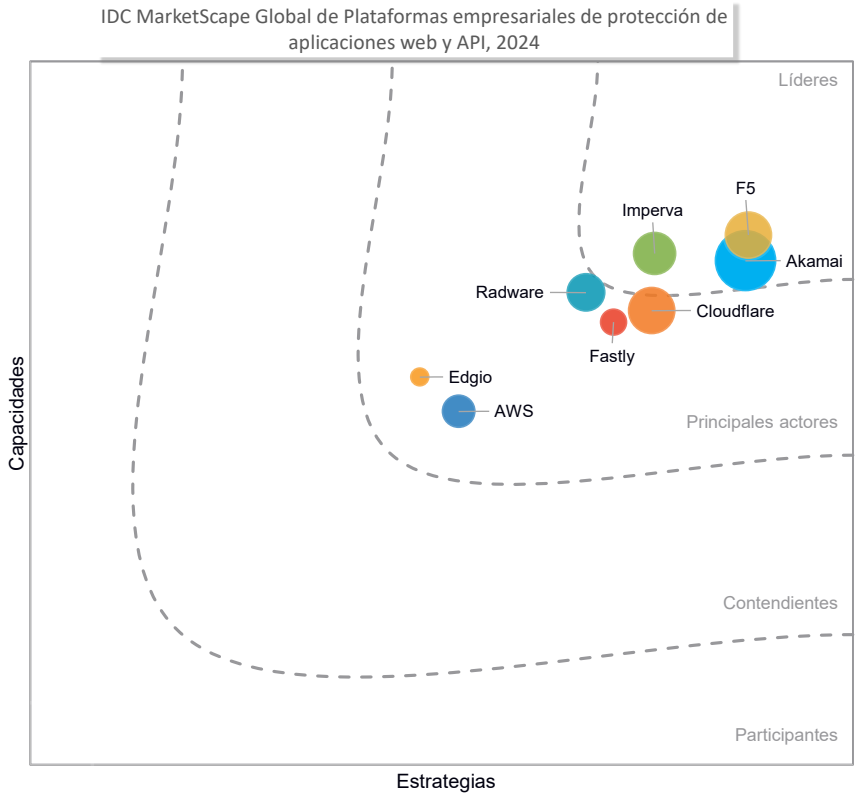
IDC MarketScape: Evaluación de proveedores globales de plataformas empresariales de protección de aplicaciones web y API 2024

Christopher RodríguezESTE EXTRACTO DEL MARKETSCAPE DE IDC PRESENTA A Akamai

FIGURA DE IDC MARKETSCAPE

FIGURA 1

Evaluación de IDC MarketScape sobre proveedores globales de plataformas empresariales de protección de aplicaciones web y API



Fuente: IDC, 2024

Consulte el Apéndice para obtener la metodología detallada, la definición del mercado y los criterios de evaluación empleados.

EN ESTE EXTRACTO

El contenido de este extracto se ha obtenido directamente de IDC MarketScape: Evaluación de proveedores globales de plataformas empresariales de protección de aplicaciones web y API 2024 (Doc n.º US51795524). Se incluyen las secciones siguientes, en parte o en su totalidad: Opinión de IDC, Criterios de inclusión de proveedores en IDC MarketScape, Orientación esencial, Perfil resumido del proveedor, Apéndice y Más información. También se incluyen las Figuras 1 y 2.

OPINIÓN DE IDC

Las aplicaciones web son componentes fundamentales de la empresa digital moderna, ya que proporcionan la funcionalidad necesaria para interactuar con clientes y clientes potenciales, socios e invitados, además de empleados y proveedores. Los atacantes examinan de forma constante estas aplicaciones y las interfaces de programación de aplicaciones (API) relacionadas en busca de oportunidades para robar datos, obtener acceso no autorizado o defraudar a las empresas para obtener beneficios ilícitos. Los ataques dirigidos a aplicaciones web y API han provocado filtraciones de datos de gran repercusión, costosos tiempos de inactividad e impactos en el mundo real, incluido el robo. Los usuarios finales y los clientes suelen llevarse la peor parte del impacto debido a pérdidas financieras. A la larga, esto puede provocar una pérdida de confianza de los clientes y una menor disposición a efectuar operaciones en línea.

La ciberdelincuencia en línea es algo más que una simple molestia. Tiene el potencial de degradar y perturbar los resultados empresariales. A lo largo de los años, las empresas han adoptado numerosas herramientas de seguridad para hacer frente al flujo constante de nuevas tácticas de amenaza y a la ampliación de las superficies de ataque posible. El firewall de aplicaciones web (WAF) proporciona una protección esencial frente a vulnerabilidades conocidas y nuevas en la capa de aplicaciones. Las empresas han incorporado numerosas soluciones especializadas, como la mitigación de DDoS (Ataque de Denegación de Servicio Distribuido, por sus siglas en inglés) la gestión de bots y, más recientemente, la seguridad de las API.

La protección de aplicaciones Web y API (WAAP) combina estas tecnologías de seguridad esenciales en una plataforma integrada y coherente para garantizar un nivel fiable de protección frente a las grandes amenazas en línea. Las plataformas consolidadas e integradas ayudan a reducir las lagunas de seguridad, disminuyen la

complejidad de la gestión y agilizan las inspecciones. La investigación de IDC muestra que el 77 % de las empresas califican la integración entre soluciones de seguridad como «importante» o de «importancia crítica». Las aplicaciones se enfrentan cada día a toda una serie de amenazas, y los atacantes aprovechan intencionadamente múltiples tácticas para identificar puntos débiles en las defensas. En consecuencia, las estrategias de seguridad de las aplicaciones que se centran en silos de seguridad especializados están abocadas al fracaso. La convergencia y la consolidación de la seguridad son un paso fundamental para lograr una postura de seguridad más sólida, ya sea mediante la mejora de la precisión de la detección, la disminución de los falsos positivos o la detección precisa de las amenazas avanzadas y de día cero.

Sin embargo, la convergencia también aporta muchas ventajas para el negocio, como la reducción del tiempo y los recursos necesarios para la implantación y la gestión, la mejora de la experiencia del usuario y la mejora de los análisis. Además, la realización de todas las funciones de seguridad en un solo servicio reduce la latencia introducida por el enrutado del tráfico a múltiples puntos de inspección de seguridad.

Al mismo tiempo, las empresas deben adoptar un enfoque realista a la hora de adoptar toda la gama de tecnologías de protección de aplicaciones de forma gradual, según sea necesario, o a medida que el tiempo y los recursos lo permitan. Para los clientes, es esencial disponer de una plataforma modular e integrada que permita implantar WAAP con facilidad a lo largo del tiempo. Para los proveedores, el reto consiste en identificar la combinación precisa de capacidades integradas en las principales áreas funcionales de seguridad que deben incluirse en los distintos niveles de productos.

Aunque el WAF es un componente fundamental, la protección moderna de las aplicaciones es imposible sin una estrategia coherente de API's. Las API's desempeñan ahora un papel fundamental en la era moderna de la empresa digital, ya que proporcionan un proceso ágil y eficiente para integrar aplicaciones y ofrecer una funcionalidad potente y nueva en la red. Sin embargo, las API's cambian la superficie de ataque de modos totalmente novedosos. Las API's son vulnerables a errores de configuración, exposición de datos sensibles y ataques de denegación de servicio. Es importante destacar que, aunque las API's son vulnerables a muchos de los mismos ataques dirigidos a las interfaces de usuario, también introducen amenazas específicas de las API's, como la autorización rota a nivel de objeto (BOLA, de sus siglas en inglés). Las API's también facilitan la comunicación entre aplicaciones, que puede no estar cubierta por soluciones de protección perimetral como el WAF. Esto puede dar lugar a un punto ciego de seguridad que los atacantes aprovechan para moverse lateralmente, detrás de las defensas basadas en la red.

La combinación de WAF y seguridad de API es esencial para garantizar una cobertura completa de las aplicaciones web en todas las interfaces y superficies de ataque. La

propuesta de valor de WAAP se completa con tecnologías diseñadas para hacer frente a tipos de amenazas especializadas, como los ataques DDoS y las actividades de bots no deseados. Estas amenazas varían ampliamente en términos de facilidad de detección, dificultad de mitigación, frecuencia de ocurrencia y gravedad del impacto. En última instancia, una pila completa de protección de aplicaciones requiere seguridad WAF y API, mitigación de DDoS y gestión de bots. Sin embargo, los requisitos técnicos únicos de las API's y los requisitos especializados de los ataques DDoS y las actividades de los bots hacen que la evolución hacia WAAP sea un camino largo y complejo.

CRITERIOS DE INCLUSIÓN DE PROVEEDORES EN IDC MARKETSCAPE

WAAP es una solución de seguridad convergente para la protección activa de aplicaciones con WAF en su núcleo. IDC ha identificado los atributos clave que se presentan en esta sección y que deben estar presentes en la solución considerada para optar a su inclusión en este análisis IDC MarketScape para plataformas empresariales WAAP.

Los proveedores deben ofrecer una solución WAAP convergente que combine dos más de los siguientes elementos en una plataforma de seguridad unificada:

- Seguridad de la API`s
- Gestión de bots
- Mitigación de DDoS
- Cortafuegos de aplicaciones web

Es importante señalar que el WAF se considera esencial y debe estar integrado para ser reconocido como parte de una solución WAAP. Además, las ventas puntuales de componentes WAAP como soluciones independientes no se contabilizarán como WAAP.

Asimismo, este análisis de IDC MarketScape contempla los siguientes requisitos para la participación y presencia en el mercado:

- **Participación en el mercado:** El proveedor ofreció funciones críticas de WAAP como solución unificada a partir de 2023. Las funciones básicas o ampliadas específicas pueden ofrecerse como parte de un paquete o plataforma diferente, o como soluciones independientes, siempre que las funciones no se ofrecieran únicamente como productos independientes o separados. Consulte la sección Definición del mercado para obtener una descripción completa y detallada de las funciones obligatorias y opcionales.

- **Representación del mercado:** El proveedor alcanzó una participación mínima de ingresos en el mercado competitivo de WAAP en 2023, según lo verificado en el Security Products Tracker de IDC.
- **Presencia mundial:** El proveedor cuenta con una distribución mínima de ingresos en cada una de las principales regiones globales, incluidas Norteamérica, Latinoamérica, EMEA y Asia/Pacífico, a partir de 2024, según lo confirmado en el Security Products Tracker de IDC.

IDC observa que ciertos proveedores de nube y seguridad que ofrecen algunos componentes de una solución WAAP quedaron fuera del análisis debido a su enfoque en productos específicos, en lugar de una solución WAAP completamente integrada. Del mismo modo, algunos de los que ofrecen WAAP no alcanzaron los requisitos mínimos de representación en el mercado global.

CONSEJOS PARA EMPRESAS QUE BUSCAN ADQUIRIR ESTAS TECNOLOGÍAS

Consideraciones clave sobre las capacidades de los proveedores

El análisis de IDC MarketScape sobre plataformas empresariales WAAP toma en cuenta el nivel de protección que los compradores de TI exigen y esperan, así como el grado de integración, la simplicidad de uso, los servicios profesionales y gestionados adicionales, y el coste total. En el entorno empresarial, una solución WAAP debe proporcionar una protección sólida, reducir al máximo el impacto en el rendimiento y afectar lo menos posible la experiencia del usuario final. El análisis también hace hincapié en el objetivo principal del WAAP, que consiste en combinar múltiples tecnologías de seguridad esenciales en una única plataforma integrada y coherente. La extensibilidad y la oferta de múltiples modelos de precios también son necesarias para permitir la adopción de WAAP de la manera que mejor se adapte a las necesidades de protección coherente contra las grandes amenazas en línea, junto con el foco en el valor para el negocio.

Las expectativas de los usuarios siguen aumentando. Las empresas continúan incorporando nuevas tecnologías para crear experiencias de usuario más innovadoras y atractivas. Las aplicaciones dependen cada vez más de infraestructuras complejas y distribuidas. Los equipos de DevOps trabajan de forma más rápida e inteligente para lanzar nuevas funcionalidades al mercado. Las empresas deben evaluar con atención las funciones especializadas que los proveedores podrían no ofrecer de manera nativa o por defecto. Estas capacidades pueden estar disponibles como complementos propios, productos separados o mediante integraciones con terceros u OEM. Además:

- **WAF del lado del cliente.** El WAF del lado del cliente, también llamado protección del lado del cliente, es una tecnología de seguridad emergente diseñada para hacer frente a un vector de amenazas especializado: el código de las aplicaciones web que se ejecuta en los dispositivos de los usuarios finales. Este código incluye scripts que se ejecutan en el navegador para realizar diversas funciones en el dispositivo en lugar de en el servidor web.
- **Prevención ante fraudes y abusos.** Las capacidades de prevención de fraudes y abusos en línea suelen basarse en capacidades de gestión de bots ajustadas específicamente para abordar los patrones únicos indicativos de actividades fraudulentas específicas, como la apropiación de cuentas o el fraude de cuentas nuevas (también llamado fraude de cuentas falsas). Se necesita información sobre la identidad de los usuarios, la telemetría a nivel de clientes y dispositivos y el comportamiento de los usuarios para detectar plenamente el fraude y otras acciones que indiquen un uso indebido de aplicaciones y API que funcionen correctamente. Esto genera diferencias significativas entre las soluciones WAAP, tanto en su capacidad para detectar fraudes como en la manera en que estas funcionalidades se presentan y se ofrecen a los compradores.
- **Proxies residenciales.** Las soluciones WAAP difieren en su capacidad para identificar atacantes que utilizan proxies residenciales u otras técnicas de ocultación, como la rotación de IP.
- **WebSockets.** Incluye compatibilidad con aplicaciones que usan WebSockets, un protocolo que facilita comunicaciones en tiempo real mediante una conexión bidireccional continua. La compatibilidad con WebSockets es cada vez más importante, ya que los usuarios en línea esperan aplicaciones interactivas y en tiempo real.
- **WebAssembly (WASM).** Es un lenguaje de bajo nivel que proporciona un formato de código binario portátil. La principal ventaja del WASM hasta la fecha ha sido su capacidad para admitir fácilmente una amplia gama de lenguajes de desarrollo. La importancia del soporte para WASM en las soluciones WAAP crece a medida que aumenta su adopción.
- **Autoprotección de aplicaciones en tiempo de ejecución (RASP).** RASP es una función de seguridad avanzada que protege el entorno de ejecución de las aplicaciones y supervisa las entradas de datos para identificar, detectar y bloquear los ataques. RASP puede ser una opción útil para la seguridad de aplicaciones en profundidad, si se comprenden adecuadamente las expectativas de complejidad de despliegue e impacto en el rendimiento.
- **Tokens de acceso privado (PAT).** Apple y otras empresas tecnológicas han incrementado su atención a la privacidad del usuario final, ofreciendo métodos que certifican la autenticidad y fiabilidad de los dispositivos que solicitan acceso, sin exponer detalles personales identificables. La compatibilidad de WAAP con

PAT de Apple puede ayudar a reducir la dependencia de CAPTCHAS u otras técnicas de detección de bots que introducen incomodidad o incertidumbre en la experiencia del usuario. Apple PAT forma parte de una iniciativa más amplia en la industria para desarrollar tecnologías que protegen la privacidad, permitiendo compartir y procesar datos de usuarios con terceros seleccionados sin revelar información de identificación personal (PII de sus siglas en inglés).

- **Automatización.** La aplicación automática de actualizaciones mejora la facilidad de uso y añade valor empresarial.
- **Pruebas de simulación.** Permite probar las actualizaciones de las reglas antes de aplicarlas en el entorno de producción. Las pruebas de simulación son más eficaces cuando pueden efectuarse con tráfico real.
- **eBPF.** Es una función de Linux que permite ejecutar programas aislados en el núcleo del sistema operativo, lo que tiene importantes implicaciones para mejorar la observabilidad de la seguridad, especialmente en entornos nativos en la nube.

Consideraciones estratégicas

Además, dada la rápida evolución de las tecnologías de aplicaciones web y API, los cambios en las prácticas empresariales y el nivel constante de adaptación e innovación por parte de los protagonistas de las amenazas, los compradores de seguridad deben ser muy conscientes de la capacidad de la solución para satisfacer sus necesidades en los próximos tres a cinco años. Además:

- **Detección de ocultación.** Los ciberdelincuentes son cada vez más audaces en sus esfuerzos por robar datos y productos, cometer fraudes y acosar o extorsionar a las empresas. Las herramientas sofisticadas y las tácticas inteligentes suelen reservarse para los objetivos lucrativos. Cuando las empresas de seguridad identifican y bloquean los ataques, los ciberdelincuentes inician entonces un proceso de adaptación. Los proveedores de WAAP deberían invertir significativamente en ocultar la naturaleza de las detecciones para garantizar la longevidad de sus esfuerzos de mitigación. Además, las estrategias de mayor éxito evitan que los atacantes sepan cuándo han sido detectados, y les obligan a malgastar sus recursos. Se han implementado mitigaciones avanzadas contra bots y fraudes, que incluyen el uso de tecnologías de engaño para evitar que los atacantes finalicen el proceso de desarrollo de sus herramientas cibernéticas.
- **Plataformización.** Las plataformas están transformando las industrias al simplificar procesos y proporcionar funcionalidades especializadas mediante una interfaz fácil de usar, que evita la necesidad de efectuar un desarrollo técnico desde cero. Por ejemplo, Shopify es una plataforma de comercio electrónico que simplifica el proceso de creación de un nuevo negocio en línea.

Funciones como la información de clientes, el inventario y el procesamiento de pagos se ofrecen como un SaaS completo y personalizado. La seguridad, incluidas las protecciones WAF y DDoS básicas, se incluye como funcionalidad integrada en la plataforma. Esto cambiará las necesidades y expectativas de los compradores respecto a las soluciones WAAP, y para los proveedores de soluciones será necesario realizar adaptaciones estratégicas.

- **Estrategias de «desplazamiento a la izquierda».** La necesidad de aplicar pruebas y prácticas de seguridad en una fase más temprana del ciclo de vida de desarrollo del software no es nueva. Detectar vulnerabilidades antes de la puesta en producción evita que los atacantes tengan la oportunidad de descubrirlas y explotarlas. La detección y corrección tempranas también son más eficaces y rentables. No obstante, en los últimos años ha surgido el concepto de *shift left* (desplazamiento a la izquierda), que alcanza estos objetivos integrando las herramientas tradicionales de postproducción en los flujos de trabajo y herramientas de los desarrolladores. Por ejemplo, gracias al uso de API's para invocar pruebas dinámicas de seguridad de aplicaciones (DAST) en DevOps pueden detectar y corregir amenazas de forma rápida y sencilla. Además, a medida que los equipos de DevOps trabajan más rápido y utilizan microservicios, código modular, infraestructura como código (IaC) y otros medios para acortar los ciclos de desarrollo, la necesidad de apoyar estrategias de desplazamiento a la izquierda se hace inevitable.
- **Cambio de personas:** Las tendencias de plataformización, las estrategias de desplazamiento a la izquierda y un aumento general de la cultura de concienciación sobre la seguridad (todo el mundo es responsable de la seguridad) están impulsando un cambio en los compradores y los responsables de la toma de decisiones. En el proceso de compra de WAAP participan desarrolladores, equipos de nube y redes, e incluso compradores de las líneas de negocio. Los proveedores de WAAP necesitan enfocarse más en la simplificación, automatización, una protección robusta desde el inicio y la educación del mercado para atender de manera más eficaz a un amplio espectro de compradores y responsables de decisiones.
- **Inteligencia artificial generativa (GenAI).** La introducción de la GenAI suscitó preocupación por los nuevos riesgos potenciales que esta tecnología puede generar en los entornos empresariales. La investigación de IDC sobre compradores reveló que, como consecuencia de ello, las organizaciones se plantean la necesidad de aumentar los presupuestos destinados a la seguridad de las aplicaciones. Los vendedores de WAAP varían mucho en cuanto a la atención y planificación que prestan a los posibles riesgos relacionados con la GenAI en función de múltiples factores como:

- Nuevas amenazas potenciales que aprovechan la GenAI para eludir las defensas con mayor eficacia
- Posibles aplicaciones de las tecnologías emergentes (por ejemplo, GenAI para mitigar las actividades de los bots, asaltar, ralentizar o sabotear las operaciones de los bots).
- La posible necesidad de desplegar funciones o productos especializados, o la posibilidad de confiar en las defensas existentes, a medida que las empresas crean capacidades de LLM, o aprovechan LLM de terceros, en sus estrategias de aplicación.
- Posibles aplicaciones de la GenAI para mejorar la eficacia y productividad de las operaciones de seguridad
- Posibles aplicaciones de la IA para mejorar la detección de vulnerabilidades en materia de seguridad

En general, a pesar de la gran amplitud de funcionalidades requeridas e implícitas en la definición de WAAP, IDC observó un alto nivel de capacidades en las soluciones consideradas en este IDC MarketScape. Se espera que la definición de WAAP siga cambiando, dadas las tecnologías emergentes y las amenazas cambiantes. Sigue habiendo margen de mejora en algunas áreas funcionales, y los proveedores tienen trazadas amplias hojas de ruta. Aunque en determinados casos de uso o para requisitos excepcionales pueden ser necesarios productos puntuales especializados, los proveedores de WAAP han avanzado mucho en el camino hacia plataformas completas y potentes con la funcionalidad profunda necesaria para garantizar una protección y un rendimiento sólidos de las aplicaciones.

PERFIL RESUMIDO DEL PROVEEDOR

En esta sección se recogen brevemente las observaciones clave de IDC que dan como resultado la posición de un proveedor en el IDC MarketScape. Aunque cada proveedor se evalúa en función de cada uno de los criterios descritos en el Apéndice, la descripción que figura aquí ofrece un resumen de los puntos fuertes y los retos del proveedor.

Akamai

Akamai es Líder en este IDC MarketScape 2024 para plataformas empresariales WAAP mundiales.

Se trata de un proveedor mundial de redes y seguridad suministradas desde la Nube Conectada de Akamai, una plataforma distribuida en la nube que acerca las aplicaciones y experiencias a los usuarios y aleja las amenazas. Akamai se ha especializado en el mercado empresarial, con una fuerte penetración en la lista Fortune

500. La cartera de seguridad de Akamai incluye una solución WAAP integrada llamada App & API Protector (AAP), así como soluciones dedicadas en las categorías de seguridad API, mitigación de DDoS, gestión de bots, protección de cuentas, WAF, protección y cumplimiento del lado del cliente, DNS y protección de marca. Akamai se ha expandido a la seguridad empresarial con soluciones para ZTNA, microsegmentación, cortafuegos DNS, caza de amenazas y MFA.

Puntos fuertes

Capacidades

- El motor de seguridad adaptable (ASE, por sus siglas en inglés) ofrece autoajuste para un uso fiable de las reglas preestablecidas. ASE proporciona una mayor protección contra ataques de día cero, duplica la eficacia de las detecciones (según Akamai) y reduce hasta cinco veces los falsos positivos (según Akamai), además de habilitar actualizaciones automáticas para garantizar un uso fluido y constante. ASE está impulsado por la inteligencia de seguridad de Akamai.
- Con ASE es posible marcar los falsos positivos para facilitar y agilizar su corrección; según la propia empresa, más del 50 % al cabo de un día y el 75 % en una semana.
- La suite WAAP completa ofrece una experiencia de compra única para disfrutar de una seguridad simplificada y completa. Hay un único SKU WAAP, con complementos para funciones avanzadas o especializadas.
- Los complementos extensivos y soluciones especializadas permiten adaptarse a requisitos específicos de casos de uso, como la protección contra la toma de control de cuentas (ATO), la protección de marca y la protección contra scrapers en eventos de alta demanda.
- Akamai ofrece una infraestructura Edge/CDN a gran escala. Ofrecer protección cercana al usuario garantiza el rendimiento.
- La compatibilidad con los flujos de trabajo DevOps respalda las estrategias de *shift left* de los clientes empresariales. La compatibilidad con la gestión y el despliegue a través de API, CLI y Terraform mejora la postura de seguridad sin ralentizar a los desarrolladores.
- Las integraciones actuales con herramientas de seguridad relacionadas facilitan su integración en una arquitectura más completa y mejoran los resultados de protección. La solución incluye conectores predefinidos para Splunk, Qradar y ArcSight.
- Se ofrece un enfoque multimodal de la seguridad de las API's. que ofrece protección inmediata para el tráfico API conocido en la plataforma y protección completa de la API más adelante, según sea necesario.

- La diversidad de las funciones relacionadas adicionales que se ofrecen junto con WAAP garantiza que la seguridad no obstaculice el rendimiento. La cartera de soluciones incluye algunas como SiteShield, mPulse Lite, EdgeWorkers, Image & Video Manager y API Acceleration.
- Akamai introdujo recientemente nuevas capacidades para la mitigación de DDoS en la capa de aplicación, incluida la detección de ráfagas cortas y la limitación de velocidad personalizable basada en pistas contextuales granulares. Estas soluciones abarcan todo el espectro de ataques DDoS, incluidas las necesidades específicas de los ataques a la capa de aplicación.
- Se incluye una vista unificada de la telemetría de seguridad que proporciona un amplio análisis y visibilidad de la seguridad, con capacidades de desglose. Web Security Analytics se incluye con todos los productos de seguridad de aplicaciones.
- El modo de evaluación ofrece la oportunidad de revisar los efectos de los cambios en las reglas basándose en el tráfico en tiempo real antes de aplicar los cambios. Esta característica permite la implementación de nuevas reglas sin el riesgo de un impacto desconocido en el tráfico de producción.

Estrategia

- Akamai señaló planes para la integración de WAAP con herramientas de seguridad adyacentes como la microsegmentación, que complementará las herramientas de seguridad y proporcionará defensa en profundidad.
- Akamai está desarrollando estrategias para proteger el aumento del uso de LLM. El uso de las herramientas existentes para las nuevas prácticas de seguridad mejora el valor para el cliente; sin embargo, las protecciones específicas de GenAI pueden seguir siendo más especializadas.
- La empresa tiene planes agresivos de expansión hacia la computación de borde (edge computing). Las opciones para proteger las transacciones en el borde pueden ayudar a evitar que las amenazas lleguen a los servidores de origen.
- Se observaron indicios de ejecución de la estrategia, especialmente en materia de seguridad de las API's. La estrategia de seguridad de las API's está a punto de completarse tras las adquisiciones de Noname Security y Neosec.
- Hay un sólido historial de adquisiciones estratégicas, que transforman productos concretos como Cyberfend, Neosec, Noname Security y Prolexic en una plataforma coherente. Las inversiones son indicadores de la dedicación a la seguridad de los clientes.
- Akamai aprovecha la telemetría para realizar un seguimiento del progreso estratégico, como el uso y aceptación de políticas, el modo automático y el

estado de mitigación. Así se garantiza que las estrategias de desarrollo se ajusten a la realidad del cliente.

- El WAAP de origen aborda las limitaciones de la seguridad de las CDN y protege el tráfico este-oeste, el tráfico no relacionado con CDN y los entornos multicloud. Esta capacidad es inminente y se observan signos de progreso.
- Se ofrecen múltiples vías para la participación de los clientes, como conferencias de clientes, reuniones periódicas del consejo asesor o procesos ad hoc.

Desafíos

Capacidades

- Los motores AI/ML no favorecen un ajuste fácil por los clientes (es decir, no pueden cambiar el orden de las reglas). Esto puede crear retrasos en la respuesta a falsos positivos y requerir la colaboración con Akamai para resolverlo. Las excepciones temporales y las soluciones provisionales son una opción posible para sortear las complejidades del orden de las normas.
- Los factores de forma limitados, como los contenedores y serverless, limitan la compatibilidad para los clientes que desean controlar la infraestructura de seguridad. En la actualidad, el soporte para Terraform y los controles basados en API es el enfoque de Akamai para el despliegue y la automatización.
- El WAAP de Akamai tiene un precio de producto premium, que puede resultar prohibitivo para decisores de compra. Sin embargo, las opciones de precios de Akamai incluyen la protección Zero Overhead Fixed Fee (ZOFF), precios basados en solicitudes y la Tarifa de Protección DDoS que incluye un sobrecoste cero para los picos de tráfico debidos a actividades DDoS.
- No se soporta gRPC, que puede ser preferible en casos de uso especializado o en sectores específicos.

Estrategia

- Las funciones especializadas y los complementos opcionales pueden implicar costos adicionales, lo que puede elevar el costo total de propiedad (TCO) y limitar la implementación completa. El tráfico fuera de la CDN (por ejemplo, el tráfico de la pasarela API) supone un coste añadido.
- La estrategia de desarrollo de WAAP actualmente contempla una mínima integración con la solución de confianza cero Akamai Enterprise Application Access (EAA). Las aplicaciones web permiten impulsar la transformación del entorno laboral, y una mayor integración entre líneas de productos es clave para respaldar la amplia variedad de casos de uso de acceso seguro.

- La multiplicidad de soluciones (por ejemplo, Account Protector, Brand Protector y Content Protector) da lugar a una estrategia contra el fraude fragmentada, lo que puede aumentar la complejidad de los mensajes.

Aspectos para decidirse por Akamai

Akamai proporciona un conjunto completo de funciones de entrega, rendimiento y seguridad, diseñadas para funcionar de manera integrada como un servicio único y cohesivo. Akamai concede licencias para capacidades avanzadas y especializadas como complementos opcionales. La estrategia permite a las empresas invertir en la solución a medida que mejor satisfaga sus necesidades de seguridad y suministro. En conjunto, la solución WAAP de Akamai cubre la amplia gama de requisitos de seguridad, disponibilidad, integridad y cumplimiento necesarios para empresas digitales modernas a gran escala.

APÉNDICE

Lectura de un gráfico IDC MarketScape

A efectos de este análisis, IDC dividió las posibles medidas clave para el éxito en dos categorías principales: capacidades y estrategias.

La posición en el eje Y refleja las capacidades actuales del proveedor y su menú de servicios, así como su grado de adaptación a las necesidades del cliente. La categoría de capacidades se centra en las capacidades de la empresa y el producto hoy, aquí y ahora. En esta categoría, los analistas de IDC se fijan en el grado en que un proveedor está creando u ofreciendo capacidades que le permitan ejecutar la estrategia elegida en el mercado.

La posición en el eje x, o eje de estrategias, indica hasta qué punto la estrategia futura del proveedor se ajusta a lo que los clientes necesitarán en un plazo de tres a cinco años. La categoría de estrategias se centra en decisiones de alto nivel e hipótesis subyacentes sobre ofertas, segmentos de clientes y planes de negocio y salida al mercado para los próximos tres a cinco años.

El tamaño de los marcadores de proveedores individuales en el IDC MarketScape representa la cuota de mercado de cada proveedor individual dentro del segmento de mercado específico que se está evaluando.

Para cada criterio específico, los proveedores fueron evaluados en una escala del uno al cinco, donde tres representa el punto de referencia que indica una evaluación promedio, cinco representa la mejor y más excepcional evaluación, y uno es la más baja y también igualmente rara. A continuación, se ponderaron los criterios en función de la perspectiva de los analistas y la comprensión de las tendencias generales del

mercado para informar mejor la toma de decisiones de los compradores de TI. Las evaluaciones para cada criterio también se ponderaron entre una evaluación «cuantitativa» y una evaluación «cualitativa», según fuera más apropiado y pertinente para el criterio específico.

La Figura 1 ofrece una representación visual de varios factores que se traducen en un posicionamiento a lo largo de cada eje. Las características y funcionalidades específicas del producto existente son un componente importante del eje «capacidades», pero también se tienen en cuenta muchos más factores. Del mismo modo, el eje «estrategias» tiene muy en cuenta los planes del vendedor para el desarrollo futuro de sus productos. Sin embargo, también se tienen en cuenta varios factores, como la solidez de la empresa en general y los planes de comercialización. Estos factores pueden tener un impacto a largo plazo en la solución, por lo que IDC ha ajustado en consecuencia la ponderación de estos criterios. En general, en la evaluación de cada proveedor intervienen varios factores, por lo que se recomienda tener en cuenta la Figura 1 en el contexto proporcionado en los perfiles de los proveedores.

Metodología de IDC MarketScape

La selección de criterios, las ponderaciones y las puntuaciones de los proveedores de IDC MarketScape representan el juicio bien documentado de IDC sobre el mercado y los proveedores específicos. Los analistas de IDC ajustan el conjunto de características estándar por las cuales se evalúa a los proveedores mediante discusiones estructuradas, encuestas y entrevistas con líderes del mercado, participantes y usuarios finales. Las ponderaciones de mercado se basan en entrevistas con usuarios, encuestas a compradores y la aportación de los expertos de IDC en cada mercado. Los analistas de IDC asignan las puntuaciones de los proveedores, y sus posiciones en el IDC MarketScape, a partir de encuestas detalladas, entrevistas con los proveedores, información pública y experiencias de usuarios finales. El objetivo es ofrecer una evaluación precisa y homogénea de las características, el desempeño y las capacidades de cada proveedor.

Definición del mercado

WAAP es una solución de seguridad convergente para la protección activa de aplicaciones con WAF en su núcleo. Las soluciones WAAP combinan múltiples funciones en una plataforma de seguridad unificada que incluye WAF, gestión de bots, seguridad de API, mitigación de DDoS y otras tecnologías de seguridad. Sin embargo, el WAF se considera fundacional y debe ser un componente integral para ser considerado WAAP. Además, las ventas puntuales de componentes WAAP como soluciones independientes no se contabilizarán como WAAP.

Componentes esenciales de WAAP

Cortafuegos de aplicaciones web (WAF)

Los productos WAF supervisan, filtran o bloquean las comunicaciones en tránsito hacia y desde una aplicación web. Un WAF puede ejecutarse desde la red o en la nube y suele desplegarse a través de un proxy delante de una o varias aplicaciones web. WAF es el componente central de una solución WAAP.

Seguridad de la API

Las soluciones de seguridad para API están creadas específicamente para proteger las comunicaciones de API frente a usos indebidos, manipulaciones y vulnerabilidades. Estas soluciones ofrecen capacidades esenciales, ya sea de forma parcial o completa. Entre ellas se incluyen la ingesta, validación y aplicación de esquemas de API; la monitorización dinámica y adaptativa del tráfico, así como el análisis de patrones. También permiten detectar y prevenir amenazas como malware, vulnerabilidades, inyecciones de código, bots, ataques DDoS, fraudes y usos indebidos.

Algunas capacidades de protección de API pueden estar incluidas de forma predeterminada en la oferta de un WAAP, como las inspecciones del tráfico de API que pueden completarse en el mismo punto de inspección que un WAF. Sin embargo, un despliegue completo de seguridad de la API puede requerir sensores y componentes adicionales para garantizar la visibilidad y el inventario de todos los puntos finales de la API y, en última instancia, la protección de todas las comunicaciones de la API.

Gestión de bots

La gestión de bots es la práctica de garantizar la integridad de las comunicaciones en línea limitando el acceso solo a usuarios humanos auténticos y actividades de bots deseables en condiciones controladas y aprobadas. Las soluciones de gestión de bots aprovechan numerosas señales y conocimientos sobre el cliente, el dispositivo, el navegador, la identidad del usuario y el comportamiento, combinados con análisis avanzados para detectar los bots más sofisticados y escurridizos. Estas soluciones también proporcionan una categorización granular y un control sobre todo el ecosistema de bots basado en perfiles de riesgo, tipos de bots o para bots específicos.

El mercado más amplio de gestión de bots incluye soluciones específicas diseñadas para abordar los requisitos de seguridad específicos que imponen los bots no deseados. Hay varios niveles de integración entre las soluciones WAAP. Una solución WAAP suele ofrecer un nivel mínimo de detección y control de bots, mientras que las funciones avanzadas se ofrecen a través de una suscripción adicional o actualización.

Mitigación de DDoS

El mercado de mitigación DDoS incluye soluciones que detectan y filtran los ataques distribuidos de denegación de servicio. Aunque los cortafuegos, los IPS y otros productos de seguridad pueden incluir funciones de defensa DDoS, las soluciones de mitigación de DDoS específicas están diseñadas para hacer frente a los ataques más grandes, complejos y novedosos. Estos productos pueden ser locales o en la nube, o un híbrido de ambos.

Dependiendo de la naturaleza de la solución o del despliegue de WAAP, pueden incluirse libremente varios niveles de protección en la solución. Las protecciones ampliadas en forma de capacidad adicional o cobertura de tipos de ataque especializados pueden ofrecerse como suscripción adicional o de actualización.

Componentes ampliados, avanzados y opcionales de WAAP

WAF del lado del cliente

El WAF del lado del cliente (CSWAF) amplía la visibilidad y el control de la seguridad de las aplicaciones a los scripts que se ejecutan en los navegadores de los usuarios finales. Las soluciones CSWAF varían drásticamente en cuanto al alcance de sus capacidades. Las funciones básicas suelen incluir visibilidad, evaluación e inventario de scripts y comunicaciones. El mercado está más dividido en lo que respecta a funciones de seguridad avanzadas, como la detección de vulnerabilidades, el cifrado, la protección del código, la identificación de anomalías y amenazas, y la aplicación de políticas.

Prevención del fraude en línea

La prevención del fraude abarca una amplia gama de soluciones que funcionan de forma independiente o conjunta para proteger los sistemas digitales de actividades fraudulentas o no deseadas. La prevención del fraude en línea puede suponer el uso de soluciones de gestión de identidad, autenticación fuerte, comprobación de identidad, protección contra el fraude en los pagos, detección del fraude en las transacciones, prevención del fraude en las empresas y soluciones dedicadas de prevención del fraude en línea.

En el contexto de WAAP, las capacidades para prevenir fraudes y usos indebidos en línea suelen estar basadas en la gestión de bots. Estas soluciones se ajustan específicamente para detectar patrones únicos que indican actividades fraudulentas, como la toma de control de cuentas o la creación de cuentas falsas. Se necesita información sobre la identidad de los usuarios, la telemetría a nivel de clientes y dispositivos y el comportamiento de los usuarios para detectar plenamente el fraude y otras acciones que indiquen un uso indebido de aplicaciones y API que funcionen correctamente. Esto genera diferencias significativas entre las soluciones WAAP, tanto

en su capacidad para detectar fraudes como en la manera en que estas funcionalidades se presentan y se ofrecen a los compradores.

MÁS INFORMACIÓN

Investigación relacionada

- *Presentación de la encuesta sobre seguridad de aplicaciones web y API, 2024* (IDC n.º US52509324, agosto de 2024)
- *Identificación y medición de los costes de los ciberataques dirigidos a aplicaciones web y API* (IDC #US52025924, abril de 2024)
- *Perspectiva de análisis del mercado: Mercado mundial de la seguridad activa de las aplicaciones, 2023* (IDC #US51332023, noviembre de 2023)
- *IDC TechBrief: WAF del lado del cliente* (IDC #US51199423, septiembre de 2023)
- *Previsión mundial de protección y disponibilidad de aplicaciones, 2023-2027: Escalada de amenazas y nuevas fronteras* (IDC #US51178423, septiembre de 2023)
- *Cuotas del mercado mundial de protección y disponibilidad de aplicaciones, 2022: Las plataformas compiten con las tecnologías emergentes* (IDC #US51204923, septiembre de 2023)
- *Comparativa: WAF y protección de API emergen como elementos esenciales de seguridad* (IDC #US51187923, septiembre de 2023)

Sinopsis

Este estudio de IDC ofrece una visión general de las soluciones WAAP disponibles por méritos propios, al tiempo que tiene en cuenta las ventajas de una cartera de proveedores más amplia, las asociaciones estratégicas y técnicas, la propiedad intelectual, las adquisiciones, el coste total de propiedad, la satisfacción del cliente y los diferenciadores competitivos. WAAP es un enfoque integrado para permitir un acceso seguro y eficaz a importantes aplicaciones web y API relacionadas. El mercado evoluciona rápidamente más allá de la capacidad de los productos puntuales para mitigar suficientemente el riesgo. Por ello, los compradores de productos de seguridad deben tener en cuenta una amplia gama de capacidades y enfoques.

Según Christopher Rodríguez, director de investigación del equipo de Seguridad y Confianza de IDC, «el mercado de WAAP se encuentra en un momento crítico, ya que los proveedores compiten para protegerse contra la próxima generación de amenazas en línea, al tiempo que se defienden de los incesantes ataques de la era moderna. Al mismo tiempo, los compradores empresariales están enfocando su planificación de WAAP en el contexto de tecnologías que cambian rápidamente».

ACERCA DE IDC

International Data Corporation (IDC) es el principal proveedor mundial de inteligencia de mercado, servicios de asesoramiento y eventos para los mercados de las tecnologías de la información, las telecomunicaciones y la tecnología de consumo. Con más de 1300 analistas en todo el mundo, IDC ofrece conocimientos globales, regionales y locales sobre tecnología, evaluación comparativa y contratación de TI, y oportunidades y tendencias del sector en más de 110 países. El análisis y la visión de IDC ayudan a los profesionales de TI, a los ejecutivos empresariales y a la comunidad inversora a tomar decisiones tecnológicas basadas en hechos y a alcanzar sus objetivos de negocio clave. Fundada en 1964, IDC es una filial propiedad al cien por cien de International Data Group (IDG, Inc.).

Sede mundial

140 Kendrick Street
Building B
Needham, MA 02494
EE. UU.
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com

Aviso sobre derechos de autor y marcas registradas

Este documento de investigación de IDC se publicó como parte de un servicio de inteligencia continua de IDC, que proporciona investigación escrita, interacciones de analistas y actas de conferencias y eventos de conferencias en la web. Visite www.idc.com para obtener más información sobre los servicios de suscripción y consultoría de IDC. Para consultar la lista de oficinas de IDC en todo el mundo, visite www.idc.com/about/worldwideoffices. Póngase en contacto con el departamento de ventas de informes de IDC en el +1.508.988.7988 o en www.idc.com/?modal=contact_repsales para obtener información sobre cómo aplicar el precio de este documento a la compra de un servicio de IDC o para obtener información sobre copias adicionales o derechos web.

Copyright 2024 IDC. Prohibida su reproducción salvo autorización expresa. Todos los derechos reservados.