Lista definitiva para evaluar soluciones WAF

Una guía para elegir la solución adecuada a sus necesidades de seguridad de aplicaciones y API

Encuentre fácilmente al proveedor idóneo de firewall de aplicaciones web (WAF) o de protección de API y aplicaciones web (WAAP). Con esta completa lista podrá evaluar qué soluciones se adaptan a sus necesidades financieras, operativas, de seguridad y de rendimiento.

Funciones de seguridad

Seguridad de aplicaciones

- Asegúrese de que ofrece **cobertura frente a las 10 principales vulnerabilidades establecidas por OWASP**, como la inyección SQL, los ataques de scripts entre sitios (XSS), la inyección de archivos locales (LFI) y la falsificación de solicitudes en el servidor (SSRF). Compruebe si puede personalizar la protección e implementarla automáticamente.
- Evalúe si su solución controla de forma proactiva el tráfico procedente de **direcciones IP con mala reputación** y le advierte si **se está haciendo un uso indebido de una excepción previa**.
- Compruebe la **flexibilidad de las listas de autorización y bloqueo**: ¿Puede establecer relaciones entre distintos atributos, como la dirección IP, la ubicación geográfica, el número de sistema autónomo (ASN) y las huellas digitales de TLS, para crear políticas eficaces?

Protección contra DDoS

- Compruebe que el proveedor ofrece **protección contra ataques DDoS multicapa** para aplicaciones y API, incluidos el sistema de nombres de dominio (DNS), y las capas 3, 4 y 7.
- Asegúrese de que la solución **proporciona detección de DDoS basada en el comportamiento** para proteger las aplicaciones.
- Evalúe la granularidad de los controles de **limitación de velocidad**. ¿Se configuran automática o manualmente? ¿Cuenta con protección ante los ataques volumétricos y de POST lento?
- Revise las funciones para **reducir la carga** durante los ataques DDoS y mejorar el rendimiento.
- Conozca los posibles **costes adicionales** debidos al aumento de tráfico durante los ataques DDoS.
- Asegúrese de que **la protección contra ataques DDoS a la capa 7 está automatizada** para no desaprovechar el tiempo ni los conocimientos de su equipo. **¿Las protecciones se adaptan** a su perfil de tráfico específico o a su tolerancia al riesgo?

Protección frente a vulnerabilidades de día cero

- Asegúrese de que el WAF cuenta con **las protecciones existentes para las CVE conocidas** y que puede ajustarse rápidamente para defenderle ante nuevas vulnerabilidades de día cero. Investigue el **historial de defensa en ataques de día cero** y los tiempos de respuesta de la solución.
- Descubra si cuenta con **protecciones contra CVE específicas** como cliente.

Protección de API

- Asegúrese de que la solución **protege los terminales de API** frente a los ataques de inyección, ataques de denegación de servicio (DoS) e infracciones de especificación.
- Compruebe **su capacidad de detección de API**: ¿detecta API nuevas o modificadas automáticamente? ¿Puede protegerlas fácilmente?
- Asegúrese de que dispone de **alertas y mecanismos de detección de información de identificación personal (PII)** para proteger los datos confidenciales y evitar filtraciones.

Protección contra bots

- Compruebe si el WAF **detecta y mitiga las amenazas automatizadas** mediante definiciones y un directorio de bots. ¿Cuál es el tamaño del directorio? ¿Con qué frecuencia se actualiza con bots nuevos y modificados?
- Examine **las definiciones de bots** de la herramienta. ¿Puede **crear sus propias** definiciones?
- Compruebe si la solución incluye un **CAPTCHA o un mecanismo de verificación humana** que no perturbe la experiencia del usuario. ¿Deben los usuarios finales interactuar con el sistema de verificación para avanzar?

Inteligencia sobre amenazas y automatización

Inteligencia sobre amenazas

- Asegúrese de que la inteligencia sobre amenazas del proveedor se basa en **datos propios** para evitar retrasos por terceros o posibles manipulaciones.
- Investigue el tamaño del **equipo de búsqueda de amenazas del proveedor** y de su red global de expertos en seguridad que supervisan los riesgos emergentes.
- Evalúe el **volumen y la pertinencia de los datos** que procesa su base de datos de inteligencia. ¿Ofrece información sobre sectores similares al suyo o sobre empresas que suelen recibir ciberataques?

Automatización

- Compruebe si el WAF funciona mediante **una solución tecnológica obsoleta basada en conjuntos de reglas**. ¿Cuenta con mecanismos complejos y modernos, como actualizaciones automatizadas a través de modelos avanzados heurísticos y aprendizaje automático?
- Asegúrese de que los conjuntos de reglas se actualizan automáticamente para **eliminar la intervención manual**. ¿Se aplican actualizaciones automáticas a nivel global? ¿Cómo se elimina una actualización o **se prueba con tráfico en tiempo real**?
- Examine si la solución adapta las medidas de protección a su entorno sin intervención. ¿**Se ajusta de forma automática y continua** a las políticas de seguridad en función del perfil de tráfico en tiempo real de su empresa?
- Compruebe cómo controla la solución los **falsos positivos**. ¿Cómo logra reducir los falsos positivos **sin perturbar el tráfico válido**?

Visibilidad y generación de informes

Visibilidad precisa

- Asegúrese de que el WAF proporciona **una visibilidad detallada de las amenazas** y el rendimiento, con paneles e informes personalizables sobre los entornos de distintas soluciones.
- Al utilizar un WAF, los equipos de seguridad pasan la mayor parte del tiempo en la consola de datos. Explore las **opciones de personalización**, las funciones de análisis proactivo y **la granularidad de los informes** a las que tendrá acceso.
- Evalúe la capacidad de la solución para **supervisar el tráfico de API** y de las aplicaciones de forma eficaz, detectar usos indebidos y proporcionar información detallada sobre la proliferación de API.

Alertas en tiempo real y análisis proactivo

- Compruebe las funciones **de alerta casi en tiempo real** que avisan a su equipo de las amenazas críticas. Las alertas se deben personalizar en función de criterios específicos, como la gravedad, el origen o el tipo de ataque, para facilitar su comprensión y ofrecer una respuesta rápida.
- Busque una solución que **preanalice la información** sobre el lugar, el momento y la forma en que se producen los ataques para reducir la carga de trabajo de su equipo de seguridad. La solución también debe **recomendar los siguientes pasos** para mejorar su estrategia de seguridad.

Plataforma y arquitectura

Alcance global

- Compruebe si el WAF proporciona acceso al Edge de la red global o a servicios de CDN para mejorar el rendimiento y la seguridad. Investigue **la cobertura de la solución a nivel global** para saber si cubre sus principales centros y los de sus clientes.

Compatibilidad con entornos híbridos y en la nube

- Compruebe que la solución es **independiente de la nube** y que es compatible con sus entornos multinube, híbridos y locales. Si se basa en una CDN, asegúrese de que también ofrece protección más allá del Edge de la red.

Resiliencia y failover

- Evalúe la **resiliencia de la solución**: ¿puede realizar un failover automáticamente para mantener la protección durante interrupciones e incidencias?
- Revise las **últimas interrupciones del servicio del proveedor y sus respuestas**.
- Compruebe si los **acuerdos de nivel de servicio** (SLA) satisfacen sus necesidades empresariales.

Asistencia y servicios gestionados

Opciones de asistencia y acceso a servicios incluidos

- Examine las **opciones de asistencia incluidas** y las disponibles con costes adicionales que ofrece la solución de WAF.
- Compruebe si cuenta con **respuesta ininterrumpida ante incidentes** y si podrá acceder directamente al centro de operaciones de seguridad (SOC) durante los ataques.
- Asegúrese de que el proveedor ofrece **servicios de seguridad totalmente gestionados** para cubrir las posibles deficiencias de sus recursos internos, como la falta de experiencia en la gestión de los ataques, la configuración o la rotación de personal.

Integración y compatibilidad con DevSecOps

API, CLI y automatización de la infraestructura

- Compruebe las integraciones de **las API, la interfaz de línea de comandos (CLI) y Terraform** para automatizar e integrar la seguridad en sus flujos de trabajo de desarrollo. La compatibilidad con GitOps y otros marcos de infraestructura como código es fundamental para aplicar las medidas de seguridad de forma coherente en todos los entornos.

Integración con SIEM

- Asegúrese de que el WAF **se integra a la perfección con herramientas de gestión de información y eventos de seguridad (SIEM)**, como Splunk o QRadar, para mejorar la supervisión, la generación de informes y la respuesta a incidentes.

Resultados empresariales y eficiencia

Escalabilidad y rendimiento

- Compruebe la capacidad de la solución para **escalar automáticamente** cuando haya que gestionar picos de tráfico sin bajar el rendimiento. ¿En qué momento se genera latencia o surgen vulnerabilidades por cargas pesadas?
- Compruebe que los SLA garantizan una **disponibilidad del 100 %** y evalúe si la solución también ofrece mejoras de rendimiento para sus aplicaciones, como el almacenamiento en caché o la aceleración del tráfico.

Gestión unificada

- Investigue si puede **gestionar las políticas de seguridad en todos los entornos** (nube, local e híbrido) desde una única interfaz. Asegúrese de que la solución es compatible con su pila tecnológica actual para que los equipos de seguridad y desarrollo puedan utilizarla sin complicaciones.

Rentabilidad

- Evalúe si la solución **puede unificar la gestión del WAF, los DDoS, los bots y la protección de API** para controlarlo todo con un único proveedor, lo que reduce la complejidad y los costes de gestión. Determine el valor general de la solución comparando la eficacia de su seguridad y su coste operativo.

Confianza en el proveedor y su fiabilidad

Historial de servicio y estabilidad

- Revise el **historial de interrupciones e incidentes** del proveedor durante los últimos 5 años.
- Asegúrese de que la empresa cuenta con **estabilidad financiera**. ¿Es rentable? ¿Desde cuándo opera? ¿Cuáles son las características y el tamaño de sus clientes?

Reputación y reseñas

- Revise reseñas y testimonios fidedignos de los clientes para saber si otras empresas de su sector **confían en el proveedor**. ¿Los casos de uso de sus clientes actuales están en línea con sus necesidades?
- Compruebe si **los analistas del sector**, como Gartner y Forrester, valoran positivamente sus soluciones de protección de API y aplicaciones.
- Tras ponerse en contacto con el proveedor, **debe confiar** en su capacidad de respuesta y asistencia en caso de que surjan problemas cuando lo contrate. Pregúntele quién le ofrecerá asistencia después de su incorporación inicial.

¿Desea obtener más información sobre la solución WAAP de Akamai?
Comience una prueba gratuita de App & API Protector.

| Publicado en: 12/24