

Akamai obtiene la puntuación más alta en 2 de 3 casos de uso en el informe Gartner Critical Capabilities for Cloud Web Application Firewall Services de 2019



Gartner evaluó a 12 de los principales proveedores de soluciones WAF basadas en la nube. Akamai obtuvo las puntuaciones más altas en los casos de uso de aplicaciones empresariales fundamentales a escala web (3,68/5) y seguridad de API (3,49/5).

Para ser competitivas en la economía digital actual en constante cambio, las organizaciones necesitan que sus aplicaciones empresariales estén disponibles a través de sitios web y API. Esta necesidad está fomentando una implementación rápida y creciente de aplicaciones web, API, aplicaciones móviles basadas en API, dispositivos IoT y otras aplicaciones orientadas al público. Todos estos casos de uso aumentan la complejidad y el riesgo, y amplían la superficie de ataque.

Cada vez hay más en juego.

Ataques como la inyección SQL, la ejecución de archivos maliciosos y las secuencias de comandos en sitios cruzados pueden disminuir o incluso paralizar el rendimiento de un sitio web. De manera más insidiosa, pueden reenviar la lógica de las aplicaciones a una base de datos. Una vez allí, los agentes maliciosos pueden utilizarla para sustraer y filtrar los datos de la empresa.

Para protegerse contra este panorama de amenazas en constante evolución, muchas empresas implementan firewalls de aplicaciones web (WAF).

Implementación de WAF basados en la nube para la protección contra una amplia gama de amenazas

A diferencia de los firewalls tradicionales, que solo proporcionan protección de servidor a servidor, los WAF se sitúan entre los clientes web y los servidores. Están diseñados para inspeccionar el tráfico HTTP antes de que llegue a la aplicación.

Los WAF están disponibles como dispositivos en las instalaciones propias y como servicios basados en la nube. Sin embargo, las tendencias indican que las empresas, cuando es posible, están migrando a WAF basados en la nube.

Según Gartner: "En 2023, los servicios de protección de API y de aplicaciones web (WAAP) en la nube protegerán más del 30 % de las API y las aplicaciones web públicas mediante la combinación de medidas de protección contra ataques de denegación de servicio (DDoS), mitigación de bots, protección de API y firewalls de aplicaciones web (WAF). Esta cifra supone un aumento considerable respecto al porcentaje actual de menos del 10 %".¹

Los WAF basados en la nube suelen ofrecer mayor escalabilidad y flexibilidad que los dispositivos ubicados en un centro de datos. Por lo general, tienen una amplia visibilidad del tráfico de Internet y pueden identificar rápidamente las amenazas emergentes y adaptar las medidas de protección en consecuencia.

El WAF de Akamai logra la puntuación más alta en 2 de 3 casos de uso principales:

- Puntuación más alta en la categoría de aplicaciones empresariales fundamentales a escala web (3,68 de 5)
- Puntuación más alta en la categoría de seguridad de API (3,49 de 5)
- Tercera puntuación más alta en la categoría de aplicaciones web orientadas al público (3,60 de 5)

Akamai obtiene la puntuación más alta en 2 de 3 casos de uso

Protección de sitios y aplicaciones web frente al tiempo de inactividad y al robo de datos

Kona Site Defender, la solución WAF de nivel empresarial de Akamai, aprovecha un conjunto de herramientas de varios niveles siempre activas para proteger los sitios web y las API contra sofisticados ataques DDoS y a las aplicaciones web, así como de ataques directos contra el origen.

Implementada en la plataforma de distribución en la nube más grande del mundo, con más de 260 000 servidores en 131 países, Kona Site Defender autentica el tráfico válido en el borde de Internet y es capaz de detener los ataques a una escala inigualable.

Este tipo de protección del rendimiento se ha diseñado para permitir a los clientes ofrecer una experiencia de usuario final óptima, incluso durante un ataque. Además, permite a las organizaciones innovar de forma acelerada en sus ofertas web y móviles, sin muchas de las distracciones de seguridad que impiden la comercialización rápida.

Funciones de Kona Site Defender:

Plataforma global en la nube

Al estar integrada en la plataforma de distribución en la nube más grande del mundo, Kona Site Defender se ha diseñado para detener los ataques en el borde de Internet, antes de que puedan llegar a sus aplicaciones.

Protección contra DDoS

Kona Site Defender minimiza el tiempo de inactividad potencial, incluso cuando defiende sus aplicaciones de los ataques DDoS de mayor tamaño.

Firewall de aplicaciones web

Le protege de las amenazas a la capa de aplicación con un conjunto de reglas automatizado y altamente personalizable.

Protección de API

Protección centrada en las API contra ataques DDoS y ataques basados en parámetros, con la capacidad de configurar las defensas y generar informes sobre eventos de seguridad según la API.

Actualizaciones de reglas

Con una visibilidad inigualable de los ataques más recientes, Akamai actualiza de forma continua y transparente los conjuntos de reglas de seguridad y permite al cliente controlar su activación.

Parches virtuales

Las reglas personalizables le permiten proporcionar un parche virtual para proteger rápidamente las aplicaciones o personalizar la protección del tráfico de su sitio web.

Disponibilidad y tiempo de actividad del 100 %

Una plataforma altamente resistente y con capacidad de recuperación automática que incluye un acuerdo de nivel de servicio (SLA) que garantiza un tiempo de actividad del 100 % y conmutación por error del sitio (failover) para mantener su sitio web activo, incluso si los servidores se quedan fuera de servicio.

SureRoute

Mitiga los problemas de red que escapan a su control para mejorar el rendimiento y la disponibilidad, y proporciona a los usuarios una ruta óptima a su sitio web.

Rendimiento mejorado

El almacenamiento en caché, las capacidades de descongestión avanzada y la optimización de TCP están diseñados para mejorar el rendimiento del sitio web para los usuarios, incluso durante los ataques de mayor tamaño.

API de gestión

Integre los controles de seguridad en el proceso de desarrollo de software y entrega.

Análisis avanzado de la seguridad web

Ayuda a mantener una configuración de seguridad óptima adaptada a sus necesidades empresariales específicas.

Akamai obtiene la puntuación más alta en 2 de 3 casos de uso

Acceda al informe completo, por cortesía de Akamai

El informe Gartner Critical Capabilities for Cloud Web Application Firewall Services de 2019 contiene información valiosa para los responsables de la seguridad que están planteándose adoptar la protección WAF para sus aplicaciones web y móviles. En él, se incluyen resultados clave, recomendaciones, supuestos de planificación estratégica y mucho más.

El informe también incluye la calificación (1-5) asignada por Gartner a los distintos proveedores según su capacidad para ejecutar 11 funciones esenciales WAF. Para calcular las puntuaciones de los casos de uso, Gartner evaluó cada una de las funciones en términos de importancia relativa.

En el informe completo, puede consultar la puntuación de cada proveedor para cada función esencial. También podrá leer explicaciones detalladas de la capacidad de cada proveedor para ofrecer las cinco funciones esenciales que Gartner considera más importantes a la hora de evaluar los servicios WAF. El informe ya está disponible por cortesía de Akamai.



Obtenga ahora el informe Gartner Critical Capabilities for Cloud Web Application Firewall Services. **Descargar informe.**

1. Informe Gartner Critical Capabilities for Cloud Web Application Firewalls Services de 2019

Gartner Research, Critical Capabilities for Cloud Web Application Firewall Services, 29 de octubre de 2019. Jeremy D'Hoinne, Adam Hils, Rajpreet Kaur y John Watts

Gartner no respalda a ningún proveedor, producto o servicio representado en sus publicaciones de investigación y no recomienda a los usuarios de tecnología la selección de forma exclusiva de aquellas tecnologías con las mejores valoraciones u otras designaciones. Las publicaciones de investigación de Gartner consisten en las opiniones de la empresa de investigación Gartner y no deben interpretarse como declaraciones de hechos. Gartner renuncia a todas las garantías, expresas o implícitas, con respecto a esta investigación, incluidas las garantías de comerciabilidad o adecuación con un fin específico.



Akamai garantiza experiencias digitales seguras a las empresas más importantes del mundo. La plataforma inteligente de Akamai en el Edge llega a todas partes, desde la empresa a la nube, para garantizar a nuestros clientes y a sus negocios la máxima eficacia, rapidez y seguridad. Las mejores marcas del mundo confían en Akamai para lograr su ventaja competitiva gracias a soluciones ágiles que permiten destapar todo el potencial de sus arquitecturas multinube. En Akamai mantenemos las decisiones, las aplicaciones y las experiencias más cerca de los usuarios que nadie; y los ataques y las amenazas, a raya. La cartera de soluciones de seguridad en el Edge, rendimiento web y móvil, acceso empresarial y distribución de video de Akamai está respaldada por un servicio de atención al cliente y análisis excepcional, y por una supervisión ininterrumpida, durante todo el año. Para descubrir por qué las marcas más importantes del mundo confían en Akamai, visite www.akamai.com o blogs.akamai.com, o siga a [@Akamai](https://twitter.com/Akamai) en Twitter. Puede encontrar los datos de contacto de todas nuestras oficinas en www.akamai.com/locations. Publicado en noviembre de 2019.