
Akamai
Desmontamos los
5 mitos sobre los firewalls
de aplicaciones web

Para las organizaciones que realizan operaciones empresariales esenciales online, el firewall de aplicaciones web (WAF) debe ser la primera línea de defensa que frene el tráfico malicioso y permita el paso del tráfico legítimo. La tecnología WAF ha estado disponible durante muchos años, pero la definición original de WAF es demasiado simplista para los actuales casos de uso, más evolucionados y modernos. Esto hace que muchos directivos empresariales y profesionales de la seguridad sigan aferrados a percepciones y mitos obsoletos.

Estos mitos pueden llevar a las organizaciones a subestimar y desaprovechar la potencia del WAF que probablemente ya forma parte de su pila, lo que abre la puerta a los atacantes y aumenta el riesgo operativo. La necesidad de una seguridad digital integral en el ámbito de la tecnología WAF es cada vez mayor. Para mejorar las estrategias de seguridad y aprovechar lo último en protección de la tecnología WAF, primero debemos abordar los mitos más frecuentes.

Observamos 9930 millones de ataques a aplicaciones web en el tercer trimestre de 2023.

Los ataques diarios durante el tercer trimestre de 2023 alcanzaron un máximo de aproximadamente 327 millones.

Fuente: Investigación de Akamai sobre amenazas

Mito n.º 1

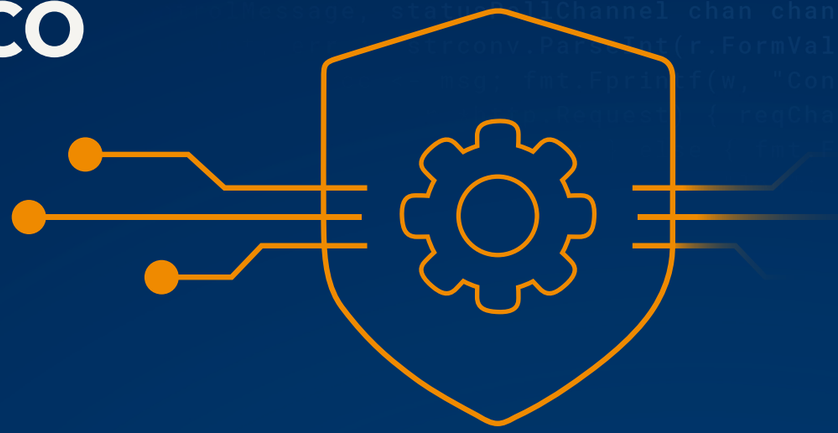
Los WAF necesitan actualizaciones manuales constantes para mantener su eficacia

Si bien es cierto que las últimas actualizaciones proporcionan las protecciones más recientes, existen algunos mitos en torno a esta afirmación que es preciso aclarar. En la actualidad, muchas organizaciones no cuentan con los recursos o la experiencia en seguridad suficientes para actualizar y ajustar continuamente las reglas de WAF. Los beneficios para la empresa de las actualizaciones automatizadas y adaptables no se limitan al ahorro de tiempo y la facilidad de uso; además, se reducen los riesgos. Al analizar las empresas que optaron por actualizar manualmente, observamos que más del 77 % tenían un retraso de cinco o más versiones en las actualizaciones de conjuntos de reglas. Akamai envía automáticamente actualizaciones de WAF de forma continua, lo que ahorra a su organización tiempo, inversión en recursos y riesgos innecesarios.

Mito n.º 2

Los WAF solo controlan el tráfico

Donde un WAF heredado se interponía entre los usuarios y una aplicación web para analizar el tráfico HTTP en relación con una lista definida de reglas, la solución de Akamai aportó rápidamente una serie de innovaciones destacadas que van más allá del WAF tradicional y proporcionan otras capacidades y protecciones, incluidas la mitigación de DDoS, la seguridad de API, la mitigación de bots, la detección de malware, la detección de datos confidenciales y la aceleración del rendimiento. Además, con el lanzamiento de App & API Protector, su solución de seguridad WAF ahora incluye aún más tecnologías muy valoradas por los clientes, como Site Shield, mPulse Lite, EdgeWorkers, Image & Video Manager y API Acceleration, entre muchas otras. La ejecución de una solución WAF por parte de Akamai implica una tecnología multifunción que proporciona a los profesionales de la seguridad una visibilidad y un control plenos de las protecciones de seguridad en los distintos entornos.



Mito n.º 3

Los WAF generan fatiga en los defensores por la saturación de alertas

Pregunte a cualquier defensor de primera línea y escuchará de primera mano que los equipos de seguridad se encuentran colapsados por el gran volumen de alertas y activadores que deben investigar, especialmente los generados por las defensas WAF. La solución de este problema es exactamente la razón por la que Akamai desarrolló Adaptive Security Engine, la tecnología principal que impulsa la solución WAF de Akamai. Con este motor de seguridad adaptable, su organización cuenta con una protección moderna que combina el aprendizaje automático, la información sobre seguridad en tiempo real, la automatización avanzada y los conocimientos de más de 400 investigadores de amenazas de Akamai. Diseñado para proteger entornos de aplicaciones web y API por completo, Adaptive Security Engine es único porque aprende los patrones de tráfico y ataque específicos de cada cliente, analiza las características de cada solicitud en tiempo real y utiliza esos conocimientos para interceptar las amenazas futuras y adaptarse a ellas. Al confiar en ASE, los defensores pueden despedirse de la fatiga causada por las alertas, a la vez que ahorran un tiempo valioso y reducen el nivel de esfuerzo necesario para mantener protegidas las aplicaciones y las API.

Se ha demostrado que, gracias a las recomendaciones de ajuste de ASE, los falsos positivos se reducen

x 5

Mito n.º 4

Las reglas de WAF más personalizables ofrecen más seguridad

Más reglas pueden significar más configuración, más pruebas y más análisis. Si bien más reglas no siempre significan una mayor seguridad, esta tampoco mejora necesariamente con menos. Si es usted un profesional de la seguridad que cree que "más es más", no se preocupe. Nuestro WAF incluye un número ilimitado de reglas personalizadas, y proporcionamos nuestras actualizaciones de reglas proactivas y adaptables independientemente de cuántas tenga. Gracias a las actualizaciones y el ajuste automáticos, su equipo puede verificar de forma eficaz y eficiente la configuración de WAF según las necesidades en toda su infraestructura digital. ¿Desea agregar una nueva regla? El modo de evaluación le permite analizar el impacto que las reglas nuevas y modificadas tendrán sobre el tráfico real; esto permite ver los efectos en tiempo real en los paneles del portal de clientes. Este método de prueba "en la sombra" garantiza que, al implementarla, la nueva regla protegerá exactamente como se espera.

Mito n.º 5

Los WAF solo se interponen en el camino de los desarrolladores

Los desarrolladores generan un valor reconocido por el cliente para las organizaciones modernas. Cuando la seguridad se interpone en el camino, la innovación se ralentiza, los ciclos de lanzamiento se retrasan y la velocidad de obtención de valor disminuye. Sin embargo, las versiones no probadas podrían tener efectos devastadores en la seguridad que obliguen a interrumpir las operaciones empresariales. En Akamai, defendemos la causa de los desarrolladores y los profesionales de la seguridad. Creemos que las defensas WAF (las que protegen las aplicaciones, las API y mucho más) pueden favorecer una cultura de DevSecOps que impulse la velocidad, la agilidad y la colaboración. Por eso, todas nuestras funciones de WAF se pueden gestionar a través de una API abierta de seguridad de aplicaciones o Terraform, que permite a su equipo automatizar la incorporación de aplicaciones y API, además de gestionar las configuraciones de seguridad. Y cuando necesite un poco de ayuda, en Akamai TechDocs encontrará funciones modernas, interactivas e intuitivas diseñadas específicamente para desarrolladores.

Cómo puede ayudar Akamai

Debido a la rápida expansión de las superficies de ataque y a la constante evolución de las amenazas, combinado con unos atacantes muy motivados, los defensores necesitan visibilidad más allá de las protecciones de WAF tradicionales. App & API Protector de Akamai es una única solución que agrupa numerosas tecnologías de seguridad, como firewall de aplicaciones web, mitigación de bots, seguridad de API y protección contra DDoS. En App & API Protector, las protecciones de seguridad se actualizan de forma continua y automática, y las recomendaciones de políticas personalizadas se implementan con tan solo un clic. Adaptive Security Engine (ASE), el motor de seguridad adaptable de Akamai y tecnología central de App & API Protector, ofrece una protección moderna porque combina aprendizaje automático, inteligencia de seguridad en tiempo real, automatización avanzada e información de más de 400 expertos en amenazas.

Inicie una prueba gratuita o descubra cómo Akamai protege sus activos web más importantes para reducir el riesgo y la fricción operativa en su organización.