10 mitos sobre la selección de firewalls de aplicaciones web

Proteger las aplicaciones web puede ser una tarea ardua, especialmente sin personal de seguridad dedicado a ello o formación sobre el tema. Un firewall de aplicaciones web (WAF) mantiene las amenazas a raya, al tiempo que salvaguarda el rendimiento de las aplicaciones. Sin embargo, con tantas soluciones en el mercado, decantarse por una no es tan simple. Desmintamos algunos mitos sobre los WAF para discernir qué es lo realmente importante, de forma que pueda preocuparse menos por los ataques y más por el crecimiento de su negocio.

MITO 1: **Manejar un WAF es complicado.**

No tiene por qué. El WAF de Akamai simplifica la seguridad de la capa de aplicación y ante ataques distribuidos de denegación de servicio (DDoS) gracias a conjuntos de reglas fáciles de gestionar. Las reglas de WAF se actualizan automáticamente para proteger el entorno contra las amenazas de ciberseguridad más recientes, de modo que sus defensas siempre estén al día. Estas reglas se prueban exhaustivamente para impedir el paso de amenazas y permitir el de usuarios legítimos, sin que se produzcan sorpresas. Y, si alguna vez necesita la ayuda de un experto en seguridad, puede recurrir al servicio de asistencia de Akamai, disponible de forma ininterrumpida.

MITO 2: **Las reglas más personalizables ofrecen más seguridad.**

Cuando se trata de facilidad de uso, menos es más. Tener más reglas que personalizar genera una complejidad innecesaria, especialmente si el personal de su organización no cuenta con la experiencia en seguridad que requiere profundizar en los detalles de las dependencias e interacciones entre reglas. Los conjuntos de reglas de WAF automatizados de Akamai se agrupan en ocho categorías. Todo lo que tiene que hacer es activarlos. Con menos botones que tocar, menor es el riesgo de causar algún problema al ajustarlos.

MITO 3: **Las interrupciones son un precio que hay que pagar por llevar un negocio.**

Las interrupciones del servicio ya no pueden tolerarse como un simple gaje de los negocios online. Según *Network World*, una hora de inactividad puede suponer pérdidas de hasta 8000 dólares para empresas pequeñas y, para empresas medianas, de hasta 74 000 dólares. Akamai, que proporciona escala y resiliencia con una disponibilidad del 100 % en más de 130 países y 1700 redes en todo el mundo, cuenta con la confianza de los sectores donde la disponibilidad es vital, incluidas ocho de las diez mayores empresas de tecnología financiera del mundo y 91 de los principales retailers de Internet de los Estados Unidos.

MITO 4: Una actualización de reglas más rápida se traduce en una defensa de aplicaciones más rápida.

No si esas reglas no se han revisado correctamente. Cuando se precipita la fase de producción, las reglas de WAF nuevas pueden ser contraproducentes. Para proteger a nuestros clientes, probamos las nuevas reglas en dos fases. En primer lugar, en laboratorio, comprobamos la respuesta ante tráfico legítimo y malicioso conocido; después, pasamos a la plataforma para analizar el cambio de falsos positivos y negativos respecto al tráfico real de Internet. No cambie velocidad por calidad solo por experimentar con nuevas reglas en su negocio.

MITO 5: El análisis de amenazas basado en la participación colectiva proporciona protección suficiente.

El análisis que depende exclusivamente de la participación colectiva carece de precisión, validación y contexto para el comportamiento, y no tiene en cuenta los falsos positivos. Dado que distribuye más de 95 exabytes de datos en miles de millones de dispositivos para más de 6000 de las principales empresas online, Akamai tiene una gran visibilidad de una enorme cantidad de tráfico, tanto legítimo como malicioso, en todo el mundo y en los distintos sectores. Examinando este tráfico, los expertos en seguridad de Akamai pueden ver cómo evolucionan los ataques y el tráfico legítimo. Esta información beneficia a la precisión de las reglas en todos los sectores.

MITO 6: Cuanto mayor sea el número de activaciones de reglas, mejores serán los resultados.

El número de activaciones de reglas es un detalle banal. Lo que realmente importa es la correlación y la puntuación de los activadores, que determinan el número de ataques que detecta el WAF. Akamai procesa más de 2 billones de interacciones en Internet e interactúa con más de 100 millones de direcciones IP a diario, lo que nos proporciona un volumen de información y estadísticas incomparable. La mayoría de los ataques comienza en un sector antes de pasar a otros. Con cientos de millones de ataques web detectados en diferentes sectores cada semana, la perspectiva única de Akamai le ayuda a mantenerse por delante de las amenazas y a protegerse de los ciberataques antes de que se propaguen.

MITO 7: No hace falta proteger las API.

En un mundo digital cada vez más conectado, no basta con proteger las páginas web. Una seguridad de API adecuada reduce la superficie de ataque. El WAF de Akamai puede proteger las API contra ataques DDoS y dirigidos a aplicaciones web bloqueando el tráfico de API en función de la dirección IP, la geolocalización, el acceso anómalo o un número excesivo de solicitudes. Asimismo, inspecciona automáticamente las solicitudes de API (incluidos los formatos JSON y XML) en busca de contenido malicioso, lo que otorga un alto nivel de protección tanto en sitios web como en API.

MITO 8: Un WAF puede proteger contra todos los ataques de día cero.

Por definición, un ataque de día cero es todavía desconocido, por lo que ningún proveedor puede hacer esa promesa; aunque eso no significa que un WAF no pueda servir de ayuda. Por ejemplo, el WAF de Akamai utiliza reglas basadas en anomalías para detectar ataques de día cero que comparten características con otros casos conocidos. Diseñado como un mecanismo de puntuación de anomalías, el WAF de Akamai ha identificado ataques que explotan las vulnerabilidades de día cero sin necesidad de ajustes adicionales. Asimismo, las reglas WAF de Akamai se actualizan automáticamente, por lo que no tiene que preocuparse de estar al día de los cambios constantes del panorama de amenazas.

MITO 9: Un WAF mitiga todos los bots.

Si bien es cierto que un WAF convencional proporciona una importante capa de protección contra bots, el WAF de Akamai bloquea los bots conocidos y también aquellos que envían mucho tráfico. Si no se les pone remedio, los bots ruidosos ralentizan los sistemas y afectan al tráfico legítimo. Emplear un WAF es una forma fácil de gestionar bots que desperdician recursos sin causar daños adicionales. Por otro lado, si una organización está en el punto de mira de bots más sofisticados, estos encontrarán una forma de burlar el WAF. En estos casos, Akamai también ofrece soluciones de gestión de bots especializadas, que detectan y protegen en casos de amenazas avanzadas, como el robo de credenciales.

MITO 10: Las soluciones puntuales individuales funcionan mejor en sus áreas de especialización.

En lo que a la protección contra las amenazas de ciberseguridad más recientes se refiere, la transferencia de conocimiento que conlleva contar con un amplio abanico de soluciones de seguridad (y el volumen de incidentes observados con estas) favorece una protección automatizada más eficaz, una mejor detección de anomalías y unos conjuntos de reglas de mayor calidad. Una estrategia de seguridad que utiliza soluciones puntuales de varios proveedores suele ser más difícil de gestionar, requiere más formación y plantea retos de integración.

Para obtener más información sobre cómo el WAF de Akamai facilita la seguridad gracias a la protección contra los ataques DDoS y a la capa de la aplicación, visite Akamai.com/Security.

Akamai garantiza experiencias digitales seguras a las empresas más importantes del mundo. La plataforma perimetral inteligente de Akamai llega a todas partes, desde la empresa a la nube, lo que permite a nuestros clientes y a sus negocios ser rápidos, inteligentes y seguros. 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 perimetral, rendimiento web y móvil, acceso empresarial y distribución de vídeo de Akamai está respaldada por un servicio de atención al cliente, análisis y una supervisión ininterrumpida durante todo el año sin precedentes. Para descubrir por qué las marcas más importantes del mundo confían en Akamai, visite **www.akamai.com/es/es/** o **blogs.akamai.com/es/**, o siga a **@Akamai** en Twitter. Puede encontrar los datos de contacto de todas nuestras oficinas en **akamai.com/es/es/locations.jsp**. Publicado en abril de 2019.