Akamai

WHITE PAPER

Simplifique la seguridad de las aplicaciones web

Ataques a las aplicaciones web

Las aplicaciones web modernas se han vuelto complejas, especialmente con la creciente adopción de arquitecturas basadas en microservicios. La gran dependencia de las API para prácticamente todas las interacciones online contribuye a esta complejidad y conlleva la posibilidad de que se creen nuevos puntos de entrada para los hackers. Por otra parte, las vulnerabilidades web conocidas siguen presentes y cada nueva generación de programadores vuelve a introducirlas en las aplicaciones. Los atacantes de hoy en día usan métodos más desarrollados, como bots, ataques distribuidos de denegación de servicio (DDoS) de alquiler y ataques multivectoriales dirigidos a aplicaciones web, API e incluso vulnerabilidades del lado del cliente.

Sin embargo, los ataques oportunistas siguen siendo el tipo más común de ataque web: no tienen como objetivo una empresa concreta, pero no dudarán en atacarla en cuanto descubran una vulnerabilidad. Los escáneres utilizan bots automatizados para escrutar constantemente sitios web al azar, en busca de cualquiera de los miles de vulnerabilidades. En cuanto detectan una, el atacante puede hacer que se revelen los secretos de una base de datos, se carguen archivos maliciosos en un servidor web o se sobrecargue un sitio con una inmensa ráfaga de tráfico.

Riesgos asociados a los ataques web

Las organizaciones con una tolerancia baja al riesgo necesitan una seguridad sólida para construir una cadena de confianza, tanto interna (entre sistemas, cadena de suministro, operaciones, etc.) como externa (con partners, clientes, organismos gubernamentales, etc.). Las API, desde los flujos internos sencillos entre las partes de una aplicación de microservicios hasta grandes transacciones de empresa a empresa, son especialmente importantes porque son el vínculo digital que conecta diversos sistemas y ecosistemas de partners, y permiten ofrecer experiencias digitales y omnicanal a los clientes.

Por desgracia, los cibercriminales tienen un arsenal casi ilimitado de métodos de ataque web diseñados para causar el máximo daño. Un pirateo exitoso que resulte en una exfiltración de datos confidenciales o un ataque DDoS que haga que sus sitios web no estén disponibles pueden acabar con esa confianza y causar daños considerables debido a la pérdida de la lealtad de los clientes, a multas normativas, a demandas o a un deterioro de la reputación de la marca.

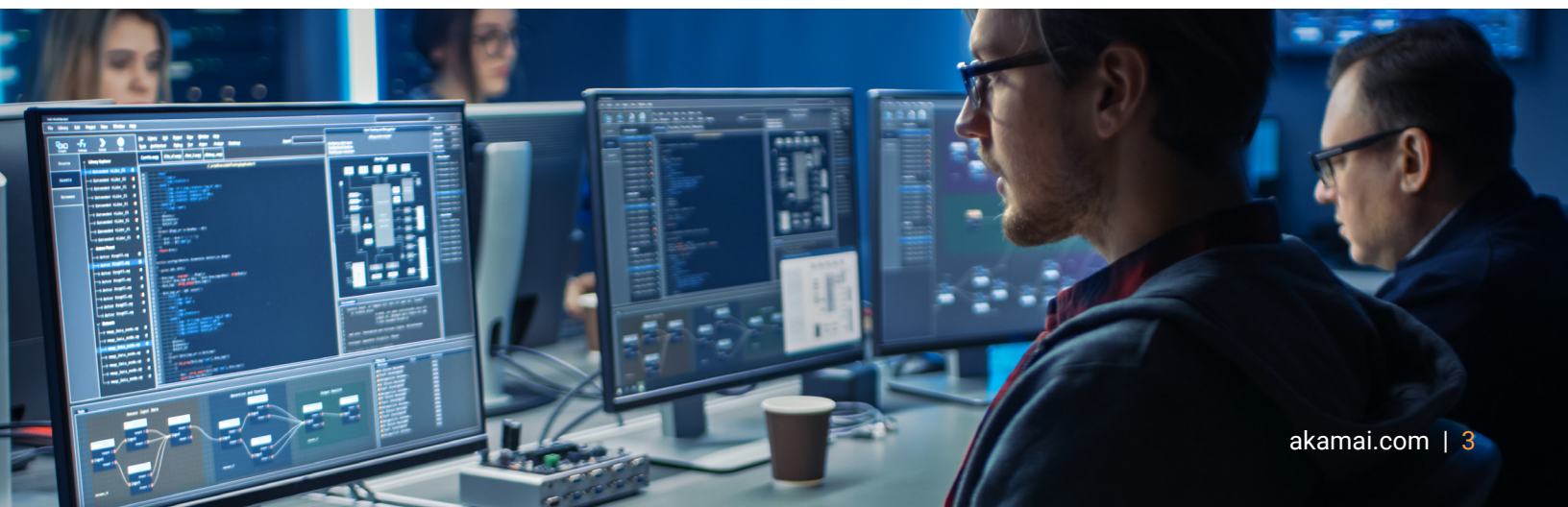
Desafíos de la seguridad de las aplicaciones web

Las soluciones de protección de API y aplicaciones web (WAAP) basadas en la nube se diseñan para mitigar cualquier tipo de ataque contra aplicaciones web, DDoS o basado en API. Sin embargo, uno de los principales desafíos que conllevan los firewalls es que los equipos responsables de la seguridad de las aplicaciones deben analizar y ajustar constantemente las reglas a medida que esas aplicaciones cambian, las amenazas evolucionan y las actualizaciones pasan a estar disponibles. Ampliar o consolidar la plantilla con profesionales de la seguridad experimentados sigue siendo un reto y, a menudo, las personas cualificadas cambian de puesto cada dos años. Este proceso suele ser manual, requiere mucho tiempo, debe ser realizado por operarios cualificados y no es escalable para la mayoría de las organizaciones debido a la rotación, los ciclos de aprendizaje y las arquitecturas de integración de tecnología especializadas.

Unas políticas de seguridad obsoletas pueden convertirse en una fuente de frustración, ya que la fatiga de la exposición a alertas disminuye drásticamente la capacidad de diferenciar con precisión los falsos positivos de los ataques reales. También es posible que los equipos de seguridad que no sean capaces de ajustar de forma eficaz las reglas desactiven sus protecciones y acepten intencionalmente una exposición mayor al riesgo por temor a que los usuarios legítimos se vean afectados y a interrumpir la actividad.

¿Por qué Akamai WAAP?

Akamai App & API Protector es una solución WAAP basada en la nube, con visibilidad y mitigación de bots, diseñada para proteger sus aplicaciones y API a escala ante un sinfín de amenazas en las capas de red y de aplicación con menos esfuerzo y coste. Gracias al asistente para la incorporación en modo de autoservicio de Akamai, no hay que tener conocimientos previos, ya que proporciona orientación e información para proteger los recursos rápida y fácilmente. En la configuración automatizada se analizan las alertas de seguridad y el comportamiento de las aplicaciones para ajustar las protecciones automáticamente y ahorrar así recursos. App & API Protector elimina muchos de los problemas actuales de firewall que sufren las empresas y que generan carga de trabajo adicional y obstáculos para las implementaciones.



Las protecciones automatizadas, que pueden ser completamente gestionadas por Akamai, están implementadas en la plataforma más distribuida del mundo, por lo que no será necesario que intervenga directamente para garantizar la seguridad de las aplicaciones y proteger las API. La protección automática contra ataques web, como la inyección SQL, los scripts entre sitios y la inclusión de archivos locales, proporciona una amplia cobertura que apenas requiere mantenimiento. Al aplicar aprendizaje automático y capacidades heurísticas, podemos mejorar la identificación de patrones de falsos positivos en el tráfico fijándonos en cada política de forma individual, en lugar de realizar una verificación genérica de toda la red, para obtener resultados más relevantes y prácticos.

Consolide su estrategia en materia de seguridad con nuestra herramienta de detección de "vulnerabilidades y exposiciones comunes" (CVE), que proporciona información detallada de las mismas, incluidos los niveles de amenaza y datos sobre las protecciones actuales de Akamai, lo que le ayudará a guiar sus estrategias de seguridad y desarrollo interno. Además, puede mejorar la coordinación interna y acelerar el tiempo de comercialización con las integraciones predefinidas por Akamai en SecDevOps, incluidas las integraciones de Akamai como código, API, CLI y Terraform.

Estándares más altos con protecciones adaptables

¿Cómo logra Akamai App & API Protector ofrecer simplicidad y precisión? Akamai Adaptive Security Engine, la tecnología principal de App & API Protector, es única 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. Esta tecnología facilita las operaciones de seguridad, ya que tiene en cuenta todos los puntos de datos anómalos o sospechosos y asigna una puntuación de amenaza a cada solicitud. Cuanto mayor es la puntuación de la amenaza, más agresivas son las protecciones y, al modificar estas últimas de forma dinámica para adaptarlas al nivel de amenaza detectado, podemos identificar incluso los ataques más evasivos a la vez que mantenemos un nivel de falsos positivos muy bajo.

Los ataques a aplicaciones suelen implicar algún tipo de reconocimiento, pero, mientras los atacantes buscan vulnerabilidades, Akamai recopila pruebas de sus técnicas y tácticas. De esta forma, no solo es posible identificarlos rápidamente, sino que también dejan una huella digital histórica en el tráfico específico en caso de que regresen. Cuanto mayor sea la frecuencia de un ataque, más fuerte será la protección.

Akamai tiene información sobre:

Más de 780 millones
de alertas diarias de ataques a aplicaciones web

Más de 26 000 millones
de solicitudes de bots

Más de 932 TB
de datos analizados diariamente

Inteligencia colectiva sobre amenazas de seguridad

Muchos de los sitios web más atacados en Internet son clientes de Akamai, entre ellos, 9 de las 10 principales empresas de retail, los 10 bancos más importantes, 9 de las 10 principales empresas de atención sanitaria, las 6 ramas del ejército de EE. UU., y muchos otros. Podemos observar más de 780 millones de ataques diarios a aplicaciones web y 26 000 millones de solicitudes de bot. Cientos de expertos en detección de amenazas y científicos de datos analizan en Akamai más de 932 TB de datos de nuevos ataques diariamente en busca de amenazas. Gracias a toda esta información global, junto con el aprendizaje automático avanzado, la inteligencia artificial (IA) y los análisis humanos, podemos detener de forma proactiva y predictiva tanto ataques comunes como otros altamente sofisticados.

Akamai ha mitigado ataques a aplicaciones durante más de una década y ha protegido a sus clientes y mantenido la disponibilidad de sus infraestructuras, resistiendo algunos de los mayores ataques. Seguimos investigando y elaborando informes sobre amenazas emergentes y, a medida que los ataques continúan evolucionando, creciendo y volviéndose más sofisticados, nosotros perseveramos en nuestra innovación y adaptamos nuestras soluciones para adelantarnos a los cibercriminales. Además, dado que App & API Protector está construido sobre la plataforma de Akamai, integra una serie de funciones diseñadas para garantizar que sus sitios web, aplicaciones web y API ofrezcan el máximo rendimiento.

Revise sus necesidades de protección de aplicaciones web y API, y descubra los beneficios de Akamai App & API Protector con esta prueba gratuita.

Akamai protege la experiencia de sus clientes, su personal, sus sistemas y sus datos, ayudándole a integrar la seguridad en todo lo que crea, dondequiera que lo cree o distribuya. La visibilidad de las amenazas globales que ofrece nuestra plataforma nos permite adaptar y desarrollar su estrategia de seguridad para integrar el enfoque Zero Trust, detener el ransomware, proteger las aplicaciones y las API o combatir los ataques DDoS, y le proporciona la confianza necesaria para innovar, crecer y transformar todo su entorno. Para obtener más información acerca de las soluciones de cloud computing, seguridad y distribución de contenido de Akamai, visite akamai.com y akamai.com/blog, o siga a Akamai Technologies en X, antes conocido como Twitter, y LinkedIn. Publicado en junio de 2024.