INFORMACIÓN SOBRE EL PRODUCTO DE AKAMAI

App & API Protector

En el mundo interconectado actual, proteger las aplicaciones web y las API de una amplia variedad de amenazas emergentes y en constante evolución es fundamental para tener éxito en los negocios. Sin embargo, con los procesos de migración a la nube, las modernas prácticas de DevOps y las aplicaciones en constante cambio, la protección de las interacciones digitales presenta nuevas complejidades y desafíos.

Implantar una solución integral para la protección de aplicaciones web y API (WAAP) refuerza su estrategia de seguridad, ya que actualiza las protecciones de manera adaptable y ofrece información sobre las vulnerabilidades objetivo de forma proactiva.

Akamai App & API Protector es una solución única que agrupa numerosas tecnologías de seguridad, como firewall de aplicaciones web (WAF), mitigación de bots, protección de API y protección ante ataques distribuidos de denegación de servicio (DDoS). App & API Protector está reconocida como la solución líder de WAAP, capaz de identificar y mitigar rápidamente las amenazas más allá del WAF tradicional para proteger toda la infraestructura contra los ataques multidimensionales. La plataforma es fácil de implantar y usar, ofrece una visibilidad integral e implementa automáticamente protecciones actualizadas y personalizadas mediante el motor de seguridad adaptable Adaptive Security Engine de Akamai.

El poder de la seguridad adaptable

App & API Protector va más allá de los conjuntos de reglas gracias a Adaptive Security Engine. Con esta innovadora tecnología, el sistema de protección se actualiza de forma continua y automática, y las recomendaciones de políticas personalizadas se implementan con tan solo un clic. Adaptive Security Engine proporciona una protección moderna que combina el aprendizaje automático (ML), la información sobre seguridad en tiempo real, la automatización avanzada y los conocimientos de más de 400 profesionales de la seguridad e investigadores de amenazas. Este motor de seguridad adaptable es único por los siguientes motivos:

- Analiza las características de cada solicitud en tiempo real en el Edge para una detección más rápida.
- Aprende los patrones de ataque sirviéndose de datos tanto locales como globales para adaptar el sistema de protección a las exigencias específicas del cliente.
- Se adapta a las amenazas futuras, lo que garantiza una protección actualizada incluso a medida que estas evolucionan.

Adaptive Security Engine aligera la pesada carga de trabajo asociada a los ajustes manuales gracias a actualizaciones automatizadas para ofrecer una experiencia que apenas requiere la intervención humana. En el momento del lanzamiento, se demostró que esta tecnología duplicaba las detecciones y quintuplicaba la reducción de falsos positivos. Las actualizaciones recientes de nuestros algoritmos basados en ML han cuadriplicado adicionalmente la reducción de falsos positivos. Los profesionales de la seguridad pueden volver a sacar la capa de héroes, ya que dispondrán de más tiempo para dedicarlo a garantizar unas operaciones empresariales digitales seguras y orientadas al cliente.

Ventajas para su empresa

Detección fiable de ataques
Evolucione a medida que lo hace el panorama de amenazas y protéjase contra amenazas ya establecidas y emergentes, como DDoS, botnets y ataques de inyección y a las API, entre otros.

Un producto, varias protecciones
Maximice su inversión en seguridad con una solución que incluye WAAP, visibilidad y mitigación de bots, protección frente a DDoS, conectores de seguridad de la información y gestión de información y eventos de seguridad (SIEM), optimización web, cloud computing, aceleración de API y mucho más.

Seguridad sin intervención
Aligere la carga asociada al mantenimiento manual que tanto tiempo requiere con actualizaciones automáticas y recomendaciones proactivas de ajustes automáticos de Akamai Adaptive Security Engine.

Facilidad de uso
Con el diseño mejorado de la interfaz de usuario se simplifica la puesta en marcha y se ofrecen unas operaciones de seguridad completas. Además, se incluye asistencia para la configuración y guías de resolución de problemas.

Visibilidad unificada
Analice todos sus datos de seguridad desde un único panel y acceda al informe de detección proactiva a través de la telemetría compartida de las soluciones de seguridad de Akamai.

Novedad: Motor basado en el comportamiento para DDoS

El nuevo motor basado en el comportamiento para DDoS refuerza y simplifica la defensa ante ataques de ese tipo mediante ML. Los algoritmos de detección basados en el comportamiento y las anomalías analizan varias dimensiones del tráfico, como el país de origen, la huella digital de red y otros atributos de solicitud HTTPS para crear protecciones personalizadas y proporcionar un enfoque no intervencionista contra los ataques DDoS a la capa de aplicación.

El uso de ML mejora su eficacia y toma de decisiones respecto a las dimensiones del tráfico para su uso en la creación de perfiles de tráfico o referencias. El mecanismo de puntuación para los diferentes niveles de sensibilidad tiene en cuenta la propensión al riesgo de su empresa para detectar ataques y minimizar los falsos positivos.

Akamai App & API Protector, que va más allá de los conjuntos de reglas, cuenta con la tecnología de Adaptive Security Engine.

La mejor detección de ataques: a medida que su entorno digital va creciendo, también aumenta la profundidad y la amplitud de las soluciones de protección de las que disfruta como cliente de Akamai. Además de las actualizaciones automáticas y del ajuste automático adaptable que ofrece Adaptive Security Engine, App & API Protector proporciona una detección líder de ataques DDoS, de bots y de malware, entre otros vectores, que cuenta con el reconocimiento de los analistas. Compruebe las protecciones de Akamai frente a las vulnerabilidades y exposiciones comunes (CVE) emergentes y avanzadas con nuestra herramienta de investigación de amenazas.

Seguridad de las aplicaciones: App & API Protector cuenta con un conjunto completo de defensas y opciones de personalización que permiten adaptar la estrategia de seguridad a las necesidades de su organización. Funciones eficaces como Client Reputation, listas de redes y detección de nuevos ataques, entre otras, le ofrecen una ventaja frente a los adversarios, a la vez que simplifican las operaciones de seguridad. Las defensas avanzadas de la capa de aplicación de la solución WAAP de Akamai neutralizan los ataques DDoS, de inyección SQL, de scripts entre sitios, de inclusión de archivos locales y de falsificación de solicitudes en el servidor, así como otros vectores de ataque.

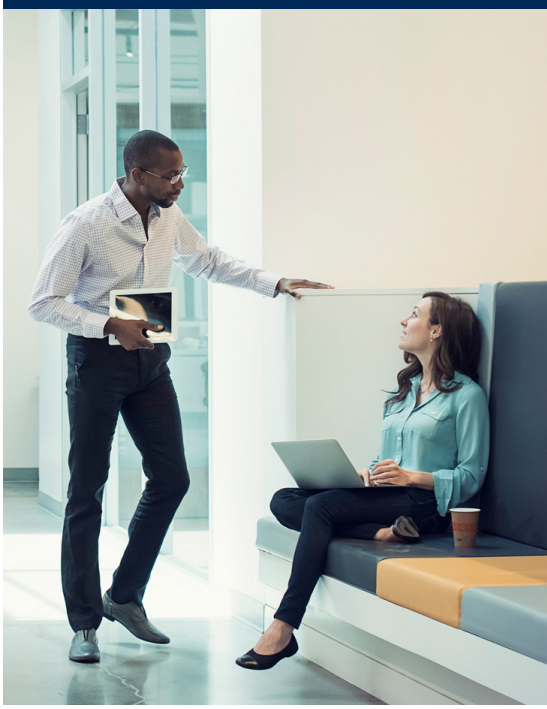
Seguridad ante DDoS y controles de frecuencia detallados: reconocida como una solución ante DDoS líder del mercado, App & API Protector proporciona protección en varios frentes. Para empezar, bloquea instantáneamente los ataques DDoS dirigidos a la capa de red en el Edge para mitigar los riesgos y ahorrar recursos. A continuación, detecta y neutraliza automáticamente los sofisticados ataques DDoS a la capa 7 en el Edge para proporcionar una protección automática y en tiempo real ante el panorama cambiante de estas amenazas. Los controles de frecuencia detallados elaboran una estrategia de defensa acorde con el tráfico y los perfiles de ataque.

Visibilidad y mitigación de bots: adquiera visibilidad en tiempo real de su tráfico de bots con acceso al directorio de Akamai, que cuenta con más de 1750 bots conocidos. Investigue los análisis web sesgados, evite la sobrecarga de origen y cree sus propias definiciones de bots para permitir el acceso a bots de terceros y partners sin ningún impedimento. App & API Protector ahora incluye controles de bots ampliados, como la función Detección de suplantación del navegador, las acciones condicionales y los desafíos criptográficos.

10 principales vulnerabilidades según OWASP

Akamai mitiga los riesgos expuestos en las listas "10 principales vulnerabilidades según OWASP" y "10 principales riesgos de seguridad de API según OWASP". Obtenga más información sobre cómo App & API Protector y la seguridad de Akamai protegen a los clientes ante amenazas importantes, comunes o emergentes.

Para obtener más información sobre las protecciones de Akamai contra los riesgos expuestos en la lista "10 principales vulnerabilidades según OWASP", descargue el white paper.



Protección de las API: la seguridad de API líder del sector de Akamai mejora la protección mediante visibilidad del tráfico en toda la infraestructura, detección proactiva de vulnerabilidades, identificación de cambios en el entorno y protección ante ataques ocultos. Con las características de API de App & API Protector, podrá:

- Detectar automáticamente una gama completa de API conocidas, desconocidas y en constante cambio dentro de su tráfico web, incluidos sus terminales, definiciones y perfiles de tráfico.
- Registrar fácilmente las API recién detectadas con tan solo unos clics.
- Garantizar la protección contra ataques DDoS, de inyección y de abuso de credenciales, así como contra infracciones de especificación de API.
- Controlar el tratamiento de datos confidenciales gracias a la función de notificación de información de identificación personal que ofrece App & API Protector para cumplir las normativas.

Rendimiento y mucho más de la mayor red global: estar en la plataforma de Akamai proporciona a los clientes una ventaja competitiva gracias a su inigualable escala mundial, que ofrece visibilidad en tiempo real de una parte significativa del tráfico global de Internet. Estos enormes volúmenes de datos permiten a Akamai ofrecer inteligencia útil sobre las amenazas para ayudar a las organizaciones a ir siempre un paso por delante de los ataques en constante evolución y proporcionar un servicio de detección y mitigación más rápido en los diversos entornos. La plataforma también proporciona un aumento demostrado del rendimiento y un acuerdo de nivel de servicio (SLA) con disponibilidad del 100 %.

Protector contra malware: este módulo complementario puede analizar los archivos antes de cargarlos en el Edge para detectar el malware e impedir que entre en sus sistemas corporativos en forma de cargas maliciosas. Dado que no es necesario configurar ninguna aplicación ni API adicional, no tendrá que invertir tiempo en ajustar la protección en cada sistema de forma individual.

Incorporación sencilla: las herramientas de seguridad solo funcionan si se usan. Akamai tiene como objetivo crear una plataforma fácil de usar que promueva la productividad y haga posible una protección eficaz. Podrá ponerlas en marcha rápidamente con el proceso de incorporación sencilla o directamente aplicar la protección a las aplicaciones nuevas con unos pocos clics.

Paneles, alertas y herramientas de generación de informes: el análisis de seguridad web de Akamai ofrece un panel de telemetría detallada sobre los ataques. Desde él, podrá analizar los eventos de seguridad, crear alertas de correo electrónico en tiempo real mediante umbrales y filtros estáticos, y usar las herramientas de presentación de informes personalizables que supervisan y evalúan continuamente la eficacia de sus protecciones en la plataforma de Akamai.

Integraciones de DevOps: integre perfectamente la seguridad en los flujos de trabajo de DevOps con GitOps, lo que garantiza que la seguridad se adapte a un desarrollo rápido. Las API de Akamai, disponibles a través de CLI o Terraform, permiten la gestión completa de App & API Protector a través del código y se corresponden con todas las acciones disponibles en la interfaz de usuario.

Integraciones con SIEM: hay disponibles API de SIEM, y en App & API Protector se incluyen automáticamente los conectores preintegrados para Splunk, QRadar y ArcSight, entre otros.

Funciones incluidas: para aumentar la visibilidad y el rendimiento, App & API Protector ahora cuenta con muchos de los productos preferidos de los clientes de Akamai, por ejemplo:

- Site Shield: evite que los atacantes eludan las protecciones basadas en la nube y dirijan sus ataques a su infraestructura de origen.
- mPulse Lite: adquiera visibilidad detallada del comportamiento de los usuarios, solucione problemas de rendimiento en tiempo real y mida la repercusión que tienen los cambios digitales en los ingresos.
- EdgeWorkers: descubra las ventajas de los procesos informáticos sin servidor, entre las que se incluyen la mejora del plazo de comercialización y la posibilidad de ejecutar la lógica más cerca de los usuarios finales.
- Image & Video Manager: optimice de manera inteligente las imágenes y los vídeos con la combinación óptima de calidad, formato y tamaño.
- API Acceleration: aumente el rendimiento de las API gestionando fácilmente el acceso, adaptándose a los picos de demanda y mejorando la seguridad de las API.

Es posible que las ofertas de nivel gratuito tengan restricciones de uso. Póngase en contacto con Akamai para obtener más información.

Advanced Security Management

El módulo opcional Advanced Security Management ofrece una gran flexibilidad en la configuración y la automatización para aquellos clientes con entornos de aplicaciones más complejos y necesidades de seguridad avanzada. La opción Advanced Security Management incluye configuraciones de seguridad adicionales, políticas de velocidad y de seguridad, controles de ataques DDoS a la capa de la aplicación, reglas WAF personalizables, seguridad de API positiva y acceso a inteligencia sobre amenazas basada en la reputación de IP (Client Reputation) disponible de forma inmediata.

Managed Security Service

A todos los clientes de Akamai se les ofrece soporte estándar las 24 horas del día, todos los días de la semana durante todo el año. Además de los servicios profesionales a la carta de consultoría o para proyectos individuales, Akamai ofrece niveles de servicios gestionados: un servicio de WAAP totalmente gestionado, asistencia gestionada ante ataques y asistencia del centro de operaciones de seguridad.

Descubra App & API Protector y solicite una prueba gratuita en akamai.com/aap.