Akamai

WHITE PAPER

De WAF a WAAP: Enfoque de Akamai para una solución integral de seguridad de API y aplicaciones

Contenido

Introducción

Con superficies de ataque cada vez más grandes y diversas, una fricción y unos costes cada vez mayores, y amenazas multidimensionales y evasivas en constante evolución, los equipos de seguridad necesitan visibilidad más allá del tradicional firewall de aplicaciones web (WAF). En concreto, necesitan más herramientas automatizadas para aumentar la eficiencia y protecciones más profundas en el ecosistema de aplicaciones e interfaces de programación de aplicaciones (API). La terminología más moderna para estas protecciones es la protección de aplicaciones web y API (WAAP). Las organizaciones más exigentes que priorizan la seguridad de su empresa y la de sus clientes demandan una protección completa contra varias amenazas en todo su patrimonio digital. Además de proteger las aplicaciones de ataques conocidos, desconocidos y de día cero, estas protecciones incluyen:

- Detección adaptable de amenazas
- Actualizaciones automatizadas de políticas
- Sólida protección frente a DDoS
- Detección y protección de API
- Visibilidad y mitigación de bots
- Integración sencilla de los ciclos de vida de desarrollo

Este documento analiza la tecnología WAF tradicional, el paso de WAF a WAAP y la continua demanda del mercado que está transformando las soluciones WAAP. Como líder consolidado en el ámbito de la seguridad, Akamai centra su enfoque en tecnologías de seguridad innovadoras que potencien y protejan la experiencia online de los usuarios finales.

Definición tradicional de un WAF

Un WAF tradicional se encuentra en el centro del flujo de tráfico entre los usuarios finales y una aplicación web. El WAF inspecciona el tráfico HTTP no cifrado o cifrado que pasa a través de él en busca de cualquier ataque, en función de una lista de reglas.

La mayoría de los WAF se basan en una lista predefinida de reglas para identificar las solicitudes HTTP maliciosas que se intercalan con el tráfico HTTP legítimo y proteger contra miles de posibles vulnerabilidades conocidas. Además, los nuevos vectores de ataque y sus variantes evolucionan continuamente y son explotados por los atacantes. Aquí es donde un WAF tradicional necesita continuamente actualizar y ajustar sus reglas según las características legítimas del tráfico, que variarán en función de la aplicación y cambiarán con el tiempo.

A medida que los usuarios finales han exigido más protección y rendimiento, los WAF han ampliado su alcance para incluir tecnologías y servicios de seguridad adyacentes, como la mitigación de ataques distribuidos de denegación de servicio (DDoS), seguridad de API y capacidades de mitigación de bots. Esta evolución continua justifica una nueva definición y una nueva terminología.

Desafíos de un WAF tradicional

Las organizaciones que cuentan con un WAF suelen coincidir en que no cumple las expectativas iniciales en términos de eficacia, facilidad de gestión e impacto en las aplicaciones y API protegidas. Debido a los problemas de rendimiento que a menudo se producen al analizar miles de millones de solicitudes web y de API en busca de código malicioso, los WAF han sido a menudo una fuente de fricción dentro de la organización, degradación del rendimiento y obstrucción a la implementación debido a los protocolos de seguridad.

Algunos de los desafíos de implementación más importantes de los WAF tradicionales tienen las siguientes causas:

- La inexactitud en las detecciones y el gran número de falsos positivos generan saturación por el volumen de alertas y riesgos adicionales.
- Los WAF se basan en tareas manuales de revisión, ajuste y mantenimiento.
- La falta de controles detallados lleva a políticas de denegación pesadas que interrumpen la experiencia del usuario final y los procesos empresariales.
- Una inteligencia sobre amenazas desfasada aumenta las vulnerabilidades.
- El rendimiento y la cobertura disminuyen debido a las restricciones y la falta de flexibilidad.
- Su capacidad para proteger un entorno digital cada vez más amplio es limitada.

Los WAF tradicionales son una potente herramienta de seguridad. Sin embargo, a menudo pueden dar lugar a problemas operativos y riesgos sin mitigar en las organizaciones que se abordarán en este documento.

Las organizaciones que deseen actualizar su tecnología WAF con una solución WAAP deben asegurarse de que la solución ofrezca tanto valor empresarial como sólidas protecciones de seguridad. La transición de WAF a WAAP combina el poder de protección con funcionalidad, eficiencia y facilidad de uso para satisfacer las necesidades de las empresas, para cualquier equipo, no solo los de seguridad.

Principios de diseño: de WAF a WAAP

Dado que los WAF tradicionales se centran en la creación de reglas de usuario final, cualquier proveedor puede crear una solución WAF y comercializarla con relativa facilidad, como demuestra la prevalencia de ofertas comerciales basadas en el conjunto de reglas básicas de ModSecurity del proyecto de código abierto de seguridad de aplicaciones web OWASP (OWASP CRS).

Sin embargo, es difícil para un proveedor diseñar una solución WAAP integral que cumpla los siguientes requisitos:

- Se implemente en línea para proteger las aplicaciones y las API a medida que surjan nuevas vulnerabilidades.
- Se adapte a las prácticas modernas de desarrollo de aplicaciones.
- Proporcione capas igualmente sólidas de defensa contra DDoS, mitigación de bots, protección de API y protección de aplicaciones web del cliente.

A medida que en Akamai nos acercábamos al diseño final de nuestra solución WAAP, resultaba evidente que debía ser más que "suficientemente buena". App & API Protector se creó para hacer frente a los riesgos de seguridad sin que las organizaciones de nuestros clientes desviaran el foco de sus principales objetivos empresariales. Para crear nuestro diseño, partimos de la base de que una solución WAAP ideal debería tener las siguientes características:

Seguridad eficaz
Las aplicaciones dirigen todos los aspectos de las empresas. Protegerlas frente a acciones malintencionadas es el objetivo fundamental de un equipo de seguridad corporativa. Los equipos de seguridad se enfrentan al reto de encontrar una solución WAAP que ofrezca las mejores detecciones de su clase. La herramienta de seguridad ideal prioriza la eficacia de la detección, ya que es el aspecto más importante de una solución WAAP, y tiene un historial excelente de protección frente a ataques de día cero, exploits, y vulnerabilidades y exposiciones comunes (CVE), además de un impresionante historial de disponibilidad.

Precisión
Los equipos de seguridad deben encontrar el equilibrio adecuado para mitigar los riesgos y, al mismo tiempo, respaldar el avance rápido de la empresa. Las soluciones ideales deben tener mecanismos de ajuste automático que ayuden a reducir los falsos positivos sin comprometer la experiencia del usuario final ni los procesos empresariales.

Protecciones modernas

Las organizaciones deben actualizar continuamente (y a menudo manualmente) las protecciones con las reglas más recientes para abordar las nuevas vulnerabilidades a medida que se descubren. Para ello, necesitan dos capacidades clave: acceso a la información más reciente sobre vectores de ataque y recursos de seguridad cualificados que puedan adaptar la estrategia de defensa para hacer frente a los ataques modificables. Una solución ideal será líder en la comunidad de inteligencia sobre amenazas y proporcionará capacidades que simplifiquen las operaciones de seguridad en todas las protecciones de la infraestructura.

Capacidad de adaptación

El panorama de amenazas evoluciona a un ritmo acelerado. Ante la inminente llegada de los ataques basados en IA, los equipos de seguridad deben ser más eficientes que nunca en sus operaciones de seguridad. Las soluciones WAAP ideales deben combinar la automatización avanzada, el aprendizaje automático y la inteligencia global profunda para ofrecer actualizaciones automáticamente y proporcionar sugerencias de modificación de reglas personalizadas que se implementan con un solo clic.

Visibilidad

Las soluciones WAF tradicionales suelen emitir un flujo interminable de alertas que los profesionales de la seguridad deben analizar individualmente, y esto supone una pesada carga para los recursos internos. Una solución WAAP óptima proporciona visibilidad de varias soluciones y un contexto proactivo en torno a los ataques, notificando a la organización cuándo, dónde y cómo se produjeron con el fin de aliviar la carga de trabajo.

Escalabilidad

Una solución sin suficiente capacidad para gestionar el tráfico entrante puede convertirse fácilmente en un cuello de botella que aumenta la latencia web y tiene el potencial de fallar ante una sobrecarga. Un enfoque WAAP eficaz se adapta a la perfección y automáticamente a las demandas de tráfico y a los ataques, así como a sus variaciones con el tiempo, y proporciona protección continua sin interrupciones ni reducción del rendimiento.

Cooperación
Una solución de seguridad eficaz debe integrarse fácilmente en la pila actual, ser fácil de programar y usar, y no provocar fricciones. La solución ideal debería servir de puente entre los equipos de seguridad y desarrollo.

Asistencia
Durante los eventos de seguridad más exigentes, las organizaciones suelen verse abrumadas por la cantidad de habilidades y recursos que se necesitan para proporcionar una resolución oportuna. Una solución ideal contará con opciones de servicios gestionados ofrecidos de forma periódica o bajo demanda, que proporcionen las competencias y recursos de mitigación necesarios en situaciones comunes, como ataques en curso, problemas en los servicios, rotación de personal, carencias de habilidades internas y mucho más.

Con estos principios de diseño en mente, vamos a explorar el enfoque que Akamai propone al crear su solución WAAP líder, App & API Protector, empezando por la tecnología principal. Nuestra solución combina muchos productos de seguridad en uno para afrontar de forma integral los desafíos que plantea la protección de las aplicaciones, la defensa contra ataques DDoS volumétricos, la protección de las API en toda la infraestructura y el control del tráfico de bots.

Enfoque proactivo de Akamai para WAAP

Más allá de los conjuntos de reglas

A pesar de que el mercado ha pasado de los principios de diseño de WAF tradicionales a la solución de seguridad moderna y eficaz de WAAP, la tecnología eficaz de detección y mitigación nunca ha dejado de ser el objetivo principal.

Akamai presentó por primera vez en 2009 su WAF, el primero del mundo basado en el Edge. En aquel momento, los proveedores de seguridad ofrecían WAF basados en conjuntos de reglas estáticas como fundamento para las detecciones. Akamai se diferenció entonces gracias a la creación de un motor patentado basado en reglas llamado Kona Rule Set, que empleaba un pequeño número de reglas flexibles (en lugar de reglas estáticas) junto con un modelo de puntuación de anomalías para mejorar la precisión y la visibilidad de los ataques.

Posteriormente, en 2017, Akamai introdujo grupos de ataque automatizados, lo que eliminó la necesidad de que las organizaciones configuraran y actualizaran continuamente las reglas con protecciones gestionadas por Akamai. Los grupos de ataques automatizados fueron una revolución y se implementaron rápidamente en miles de políticas activas de WAF de clientes de Akamai con el fin de aprovechar las ventajas de este nuevo enfoque.

Akamai continuó desarrollando su enfoque de seguridad de las aplicaciones, dando prioridad a la protección combinada de aplicaciones y API, incluidas las capacidades de defensa contra bots, con el lanzamiento de App & API Protector en 2021, una solución WAAP destinada a sustituir el WAF de Kona Site Defender para grandes empresas y compañías globales en crecimiento. App & API Protector ha cambiado la forma en que Akamai aborda las operaciones de seguridad mediante la modernización de la tecnología Kona Rule Set para crear Adaptive Security Engine.

Modernización de la protección frente a DDoS en la capa de aplicación más allá de la limitación de velocidad

Cuando se trata de DDoS, la limitación de velocidad es una herramienta probada y eficaz. Sin embargo, el aumento de los sofisticados ataques DDoS a la capa 7, los ataques multivectoriales y la explotación de las API han hecho que las defensas frente a DDoS tradicionales tengan dificultades para mantenerse al día. Las defensas estáticas, que se basan en umbrales fijos y firmas predefinidas, son reactivas y propensas a generar falsos positivos, especialmente debido a que los atacantes combinan cada vez con más frecuencia tráfico malicioso con solicitudes legítimas. Aquí es donde Akamai cambió el enfoque de la protección frente a DDoS e introdujo importantes innovaciones, como la protección de URL y el motor de DDoS conductual.

El motor Behavioral DDoS Engine es una revolucionaria incorporación a Akamai App & API Protector y se une a Adaptive Security Engine como una de sus tecnologías principales. Juntos, estos motores ofrecen una protección sin precedentes contra las amenazas modernas, lo que convierte a Akamai en líder en WAAP. Este enfoque de doble motor diferencia a Akamai al ofrecer actualizaciones automatizadas, capacidades de ajuste automático y detección basada en contexto, liberando a los usuarios de las tareas manuales.

Solución única para una protección completa

Hoy en día, el cambio sigue redefiniendo la seguridad de las aplicaciones con prácticas de desarrollo modernas a través del uso de edge computing sin servidor, arquitecturas basadas en microservicios, aplicaciones de una sola página y enfoques SaaS/IaaS/PaaS/FaaS.

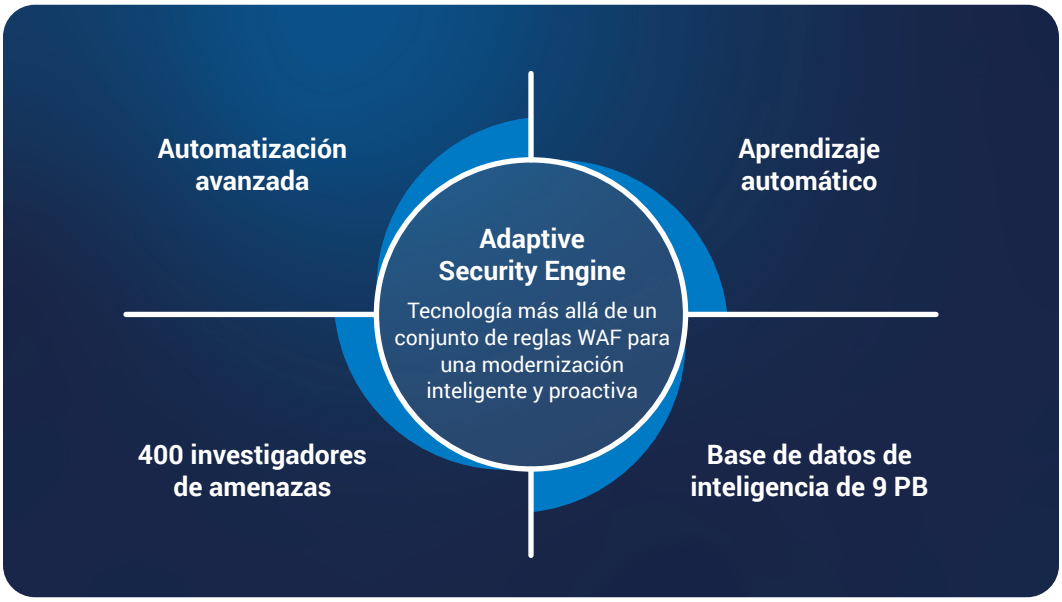
Para proteger las aplicaciones y API modernas en entornos de TI complejos, Akamai ha rediseñado su tecnología de seguridad de las aplicaciones con un enfoque más adaptable, flexible e integral. Durante el proceso de migración de la solución WAAP de Akamai desde Web Application Protector y Kona Site Defender a App & API Protector, se incorporaron nuevas funciones de seguridad y herramientas.

App & API Protector ahora proporciona muchas mejoras de seguridad adicionales, todas ellas visibles y controladas a través de una única interfaz. La solución de WAAP de Akamai combina:

1. Un motor de seguridad adaptable
2. Seguridad de las aplicaciones con controles detallados
3. Defensa contra DDoS, incluida la protección avanzada frente a ataques DDoS a la capa 7
4. Protección de API, incluidas las funciones de detección y protección de PII
5. Capacidades de visibilidad y mitigación de bots
6. Una plataforma que respalda la escalabilidad global, la inteligencia sobre amenazas y la resiliencia

Adaptive Security Engine

Adaptive Security Engine es una solución de protección de nueva generación que combina aprendizaje automático (ML) con inteligencia sobre seguridad en tiempo real, competencias de expertos en ciberseguridad y automatización avanzada. Como tecnología principal de Akamai en materia de detección y protección, Adaptive Security Engine ofrece un enfoque automatizado para proteger aplicaciones web completas y activos de API. También se suma a los avances de la migración de Akamai de WAF a WAAP, que incluyen soluciones de seguridad correlacionadas, como gestor de bots, protección frente a DDoS, integraciones de DevOps y mucho más.



Adaptive Security Engine es una solución única, ya que 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. Utiliza la misma inteligencia e información de la plataforma para reducir los falsos positivos mediante recomendaciones de ajuste. Esta función de ajuste automático facilita el trabajo a los equipos de seguridad y desarrollo, ya que incluye protecciones adaptables frente a las amenazas en forma de actualizaciones proactivas.

Detección adaptable de amenazas

El motor emplea un modelo multidimensional de puntuación de amenazas que combina la inteligencia de esta plataforma con datos/metadatos de cada solicitud. Estos datos se procesan con lógica de toma de decisiones para identificar con precisión los ataques reales.

La detección adaptable es muy eficaz para identificar ataques furtivos, evasivos y dirigidos, en los que los atacantes dedican más tiempo y esfuerzo. A medida que los atacantes escudriñan en busca de vulnerabilidades y errores de configuración, Adaptive Security Engine recopila y correlaciona pruebas sobre sus tácticas para que resulte más fácil identificar su rastro histórico.

Además de la carga útil real y su ubicación dentro de la solicitud, otros ejemplos de las dimensiones del ataque que evalúa para cada cliente incluyen los siguientes:

- Un historial de reconocimiento o ataques (por ejemplo, frecuencia, magnitud, gravedad)
- Cualquier señal asociada a herramientas maliciosas de ataque y automatización.
- Correlación con fuentes conocidas de tráfico de ataques.

Además, Adaptive Security Engine se ha mejorado con dos tecnologías patentadas: Smart Detect, que crea una huella con los datos de entrada para mejorar notablemente la precisión de la detección, y Smart Sniff, que detecta el tipo correcto de contenido en el cuerpo de la solicitud para evitar la manipulación del contenido y la elusión de las medidas de protección. Los investigadores de amenazas de Akamai aprovechan la amplia infraestructura y los sistemas de Akamai para ejecutar de forma pasiva nuevas detecciones en todo el tráfico de producción y, a continuación, analizar los resultados aplicando modelos de aprendizaje automático.

Actualizaciones automáticas

En la actualidad, muchas organizaciones no disponen de recursos ni de conocimientos de seguridad suficientes para realizar un seguimiento continuo de las amenazas en desarrollo, actualizar las configuraciones y volver a evaluar su tráfico web con el fin de optimizar las políticas. Como respuesta, Akamai actualiza continuamente el motor Adaptive Security Engine mediante un marco de pruebas automáticas de IA/ML para dar cuenta de las amenazas cambiantes, al tiempo que mantiene un alto nivel de precisión. A menudo, estas actualizaciones han protegido frente a ataques de día cero antes de que se anunciaran.

Marco de pruebas para garantizar la precisión

La prueba de una solución WAAP se basa en una premisa sencilla: probar diferentes vectores de ataque y detener los ataques web. Sin embargo, deben tenerse en cuenta los siguientes factores:

- Los entornos reales son más complejos que los entornos de prueba y suelen dar lugar a falsos positivos y falsos negativos.
- El diseño de un marco de pruebas teniendo en cuenta la precisión requiere una verificación adicional, no centrarse únicamente en la detección de ataques, sino hacerlo sin generar de forma inadvertida falsos positivos o falsos negativos.
- Las pruebas requieren el uso de tráfico web real, tanto legítimo como malicioso.

Las actualizaciones de Adaptive Security Engine constan de varias etapas para garantizar que el tráfico legítimo no se vea afectado negativamente:

- Todas las detecciones se someten a pruebas de laboratorio con tráfico sintético para garantizar que captan correctamente los ataques sin introducir falsos positivos.
- A continuación, se prueban las actualizaciones en el tráfico de producción en directo para garantizar que la muestra sea válida para el tráfico actual de la plataforma. Este proceso implica ejecutar la actualización en modo "en la sombra" en el tráfico real de los clientes. La ejecución "en la sombra" garantiza que no se produzca ningún impacto en el tráfico de los clientes, a la vez que se sigue ejecutando la detección de pruebas con precisión.
- Una vez que una actualización ha pasado la fase dos, el aprendizaje automático identifica patrones o desencadenantes que el análisis humano puede haber pasado por alto, tras lo cual el equipo de investigación de amenazas revisa manualmente los resultados.
- Solo cuando se superan estas comprobaciones en cada fase, un cambio puede pasar a la siguiente fase y desplegarse en un segmento más grande de la red. Tras una implementación del 100 %, las capacidades de ajuste automático eliminarán los falsos positivos restantes, causados por los patrones de tráfico específicos de los clientes.

Ajuste automático

El ajuste automático alivia la carga del ajuste manual, que puede dar lugar a políticas obsoletas y errores humanos, para proporcionar una experiencia en la que usuario prácticamente no debe intervenir. Adaptive Security Engine aplica aprendizaje automático, modelos estadísticos y heurística en todos los activadores de cada política de seguridad para diferenciar con precisión entre ataques reales y tráfico de usuario final identificado erróneamente como malicioso. No se trata de una comprobación genérica de toda la plataforma que se aplica solo durante la incorporación, sino de un proceso de ajuste continuo que tiene lugar todos los días de la semana, durante todo el año, sin necesidad de configuración ni intervención por parte del usuario final.

El ajuste automático es sencillo y sin fricciones. Los administradores de seguridad pueden revisar y aceptar fácilmente las recomendaciones con un solo clic a través de la interfaz de usuario, o bien automatizarlas mediante las API de AppSec, la interfaz de línea de comandos (CLI) o Terraform. Para una mayor transparencia, un enlace prefiltrado a Web Security Analytics muestra todas las solicitudes consideradas como falsos positivos y proporcionamos nuestra justificación para cada recomendación.

Flexibilidad en la configuración y la automatización

Cuando un proveedor de soluciones WAAP deja atrás la tecnología tradicional de conjuntos de reglas, la configuración y la automatización se vuelven más flexibles. Adaptive Security Engine permite lo siguiente:

- Tener diferentes tipos de actualizaciones de WAF (automáticas frente a manuales) para diferentes aplicaciones y su propensión asociada al riesgo.
- Controlar la acción por grupo de ataque y la regla necesaria para la personalización si el comportamiento de la aplicación/el tráfico no es estándar.
- Configurar condiciones simples y complejas para diferentes características de solicitud, como IP, ubicación geográfica, encabezado, carga útil, etc.
- Mitigar de forma proactiva las fuentes de amenazas que se han detectado llevando a cabo ataques o análisis sospechosos de WAF en las aplicaciones, con Penalty Box.
- Modificar el encabezado de depuración.
- Modificar el tamaño de la inspección de la carga útil de la solicitud o la configuración del registro de carga útil del ataque.
- Ejecutar simulaciones de cambios en la lógica de detección para aplicar con confianza estos cambios en la fase de producción.

Aplicación en el mundo real

El modo de evaluación proporciona a los clientes de Akamai flexibilidad y granularidad a la hora de configurar versiones específicas de Adaptive Security Engine y de probar actualizaciones o nuevas reglas/políticas. Los clientes pueden ver las nuevas actualizaciones o los cambios antes de elegir habilitarlos según sea necesario o apropiado para su entorno de aplicaciones web específico. Para una modernización eficaz de la seguridad, Akamai cree que las pruebas con tráfico en tiempo real ofrecen mejores resultados que las pruebas con tráfico antiguo. El modo de evaluación es similar a aplicar una regla en la sombra donde se pueden ver los resultados en tiempo real como si se aplicara la política, pero sin ningún impacto para los usuarios finales. Las organizaciones pueden optar por este modo de funcionamiento manual/de evaluación para minimizar el impacto inesperado de falsos positivos y falsos negativos.

Integración de protecciones modernizadas

Los equipos de seguridad y de DevOps también pueden manejar aspectos de seguridad integrando llamadas a API de Akamai mediante la CLI, Akamai Terraform o scripts en su canal de automatización de integración e implementación continuas (CI/CD). La velocidad en el desarrollo no se verá afectada por la seguridad gracias a la flexibilidad en la configuración y la automatización. Estas integraciones pueden lograr lo siguiente:

- Incorporación rápida de aplicaciones
- Gestión uniforme de las políticas de seguridad en grandes carteras de aplicaciones
- Centralización de la aplicación de la seguridad en infraestructuras híbridas y multinube
- Mejora de la colaboración entre los equipos de DevOps y seguridad en un flujo de trabajo de GitOps para una cobertura óptima

Además, la gestión de eventos e información de seguridad (SIEM) permite recopilar eventos de seguridad que tienen lugar en la plataforma de Akamai. A su vez, nuestra solución de integración SIEM proporciona una forma de distribuir eventos SIEM a herramientas de análisis SIEM locales y basadas en la nube, como Splunk y QRadar. Esto le permite incorporar eventos de seguridad de Akamai a su infraestructura general de seguridad y eventos en cuatro sencillos pasos.

Con los siguientes elementos, podrá proteger y controlar su fuente de datos:

- **Filtrado de eventos**
  Utilice la configuración y la política de seguridad para centrarse en amenazas reales.
- **Retención de datos**
  El recopilador almacena datos durante 12 horas para que pueda capturar eventos pasados por alto.
- **Protección contra sobrecarga de SIEM**
  En el conector de SIEM, puede definir el número máximo de eventos de seguridad obtenidos en cada solicitud. Esto ayuda a evitar sobrecargar la aplicación SIEM.
- **Intervalo de obtención**
  Puede definir la frecuencia con la que los conectores de SIEM realizan una llamada a la API de SIEM para obtener datos de eventos de seguridad.

Seguridad de aplicaciones y protección frente a DDoS

La seguridad de las aplicaciones es un aspecto crucial de la ciberseguridad moderna, ya que garantiza que las aplicaciones sean resistentes a una amplia gama de amenazas y vulnerabilidades. Su importancia radica en varias áreas clave. La integridad y confidencialidad de los datos son primordiales, ya que la seguridad de las aplicaciones garantiza la protección de los datos confidenciales contra el acceso no autorizado y la manipulación. También desempeña un papel fundamental en la continuidad del negocio, ya que protege las aplicaciones de las interrupciones causadas por incidentes de seguridad, lo que garantiza una disponibilidad constante del servicio. Además, la seguridad de las aplicaciones es esencial para la gestión de la reputación, ya que evita las vulneraciones que pueden dañar la reputación de una organización y erosionar la confianza de los clientes. Por último, ayuda a las organizaciones a cumplir los requisitos normativos, evitando así sanciones legales y financieras.

Funcionalmente, una solución WAAP filtra y supervisa el tráfico HTTP entre las aplicaciones web e Internet. Esto protege contra ataques web comunes, como XSS, inyección SQL y DDoS.

La solución App & API Protector es reconocida por su protección frente a DDoS líder del mercado, diseñada para contrarrestar los ataques volumétricos cuyo objetivo es saturar los recursos. La solución combate los ataques DDoS de las siguientes formas:

- **Mitigación de DDoS basada en el Edge**
  Al aprovechar la plataforma en el Edge globalmente distribuida de Akamai, App & API Protector puede bloquear instantáneamente ataques DDoS antes de que lleguen al origen de la aplicación. Este enfoque centrado en el Edge garantiza una latencia mínima y una protección máxima sin que ello afecte al rendimiento de la aplicación.

- **Limitación de velocidad**
  App & API Protector incluye limitación de velocidad adaptativa para defenderse de ataques DDoS distribuidos en la capa de aplicación. Estos controles se pueden configurar para limitar la tasa de solicitudes entrantes en función de varios criterios, incluidos, entre otros, la IP, la ubicación geográfica, controles de reputación de IP, varios encabezados HTTP y condiciones de coincidencia.

- **Protección de URL con deslastre de carga inteligente**
  Adopta un enfoque diferente para la limitación de velocidad. Con la protección de URL, puede proteger su origen de solicitudes excesivas en función de la tasa de solicitudes aceptable (RPS máximo) dependiendo de la capacidad del origen. Se ha diseñado específicamente para proteger direcciones URL con un alto volumen de procesamiento, terminales de API, etc. frente a los ataques DDoS de nivel de aplicación altamente distribuidos.

- **Behavioral DDoS Engine**
  Behavioral DDoS Engine, una novedad en App & API Protector, es una potente herramienta para una estrategia de defensa en profundidad. Introduce un enfoque automatizado para la gestión y mitigación de los eventos DDoS, utilizando el aprendizaje automático para establecer niveles de tráfico estándar e identificar anomalías con respecto a las normas. El motor funciona comprendiendo los cambios en los patrones de tráfico y permite a los usuarios definir cómo reacciona el sistema a las diferentes anomalías sin establecer umbrales explícitos, lo que reduce la carga operativa de la gestión y el ajuste del sistema.

- **Actualizaciones automáticas y ajuste automático adaptable**
  Gracias a la estrategia de Akamai de dos motores, Adaptive Security Engine y Behavioral DDoS Engine, App & API Protector se adapta continuamente a las nuevas amenazas mediante actualizaciones automáticas y un autoajuste basado en el aprendizaje automático para reducir la carga operativa.

Behavioral DDoS Engine: cómo funciona

En el núcleo de Behavioral DDoS Engine se encuentra un modelo de aprendizaje automático avanzado que supervisa continuamente el tráfico en tiempo real, estableciendo líneas de referencia para el comportamiento normal y detectando instantáneamente las desviaciones que indican un ataque. Mediante el análisis de patrones de tráfico en múltiples dimensiones dinámicas, como el país de procedencia, los patrones y las huellas digitales de TLS, y la dirección IP, este motor puede identificar rápidamente anomalías y tomar medidas.

Los componentes clave de Behavioral DDoS Engine incluyen los siguientes:

- **Supervisión del comportamiento en tiempo real**
  El motor analiza continuamente el tráfico para establecer líneas de referencia de la actividad normal y detecta instantáneamente las desviaciones que indican posibles ataques DDoS.

- **Aprendizaje automático para una mayor precisión**
  Los modelos de aprendizaje automático avanzados respaldan la capacidad del motor para identificar anomalías sutiles en los patrones de tráfico, lo que garantiza una mitigación precisa sin bloquear a los usuarios legítimos.

- **Mitigación proactiva**
  Al aprovechar la información de la red global de Akamai (1056 TB de tráfico al día), el motor predice y neutraliza los ataques, a menudo antes de que puedan afectar a las empresas.

- **Análisis multidimensional**
  El tráfico se evalúa en múltiples dimensiones, incluidos los patrones de IP, país y TLS, lo que proporciona una sólida protección adaptada a las necesidades de cada aplicación.

Arquitectura avanzada para una defensa superior
El motor Behavioral DDoS Engine funciona a través de una arquitectura sofisticada que incluye varios componentes críticos:

- **Motor de detección**
  Utiliza dimensiones dinámicas y datos históricos de ataques para identificar ataques DDoS en tiempo real.
- **Motor de mitigación**
  Contrarresta automáticamente los ataques mediante la inteligencia del generador de líneas de referencia y señales de amenazas, lo que reduce la sobrecarga operativa de los equipos de seguridad.
- **Reducción de ruido/falsos positivos**
  Los modelos de aprendizaje automático filtran los datos irrelevantes, lo que garantiza que se utilice un tráfico limpio para el análisis y la mitigación.
- **Generador de líneas de referencia**
  Perfecciona continuamente los perfiles de tráfico mediante el procesamiento de datos limpios durante un periodo de dos semanas, lo que permite al motor mantenerse al día de las estrategias de ataque más recientes.
- **Validador estándar**
  Con la ayuda de la IA, este componente crucial evalúa cientos de ataques DDoS cada mes para ajustar la solución.

Este marco automatizado garantiza que los equipos de seguridad puedan confiar en el motor para ajustar dinámicamente las defensas sin intervención manual. La solución detecta la actividad de tráfico anómala, como el tráfico generado por bots o los intentos de DDoS, y la filtra para proteger las aplicaciones de forma eficaz.

Precisión de la seguridad de las aplicaciones

Una solución de seguridad de las aplicaciones (WAF o WAAP) que no sea precisa requiere más recursos internos para gestionar el creciente número de alertas diarias. La inexactitud puede generar un gran número de falsos positivos (una solicitud se marca como maliciosa cuando no lo es) y falsos negativos (una solicitud se marca como no maliciosa cuando lo es), lo que supone una pérdida de tiempo y de los recursos que se dedican a la investigación y el análisis de este tipo de alertas.

Las organizaciones a menudo se ven saturadas por el volumen de alertas, pero siguen sin una solución debido a una variedad de controles o funciones que corrigen en exceso o no lo hacen suficientemente. Esto suele llevar a la organización a desconectar su WAF, o peor aún, a ignorar las alertas y las actualizaciones de versiones. Aunque esto alivia muchas preocupaciones de la organización sobre el bloqueo accidental de usuarios legítimos, también protege contra menos ataques web y de API. Muchas organizaciones también carecen de controles detallados, lo que les impide lograr un buen equilibrio entre permitir el tráfico legítimo y bloquear el malicioso.

La ventaja de una solución WAAP eficaz es que reduce tanto los falsos positivos como los falsos negativos para aumentar la precisión y minimizar el impacto en los usuarios legítimos con un conjunto completo de controles y capacidades WAAP.

Qué es la precisión

La precisión mide la capacidad de un WAF o WAAP para detener simultáneamente ataques sin bloquear inadvertidamente a los usuarios legítimos. Tiene en cuenta cuatro variables:

- **Verdaderos positivos (VP):** ataques reales que se identifican correctamente como maliciosos.
- **Falsos positivos (FP):** solicitudes legítimas que se identifican incorrectamente como maliciosas.
- **Verdaderos negativos (VN):** solicitudes legítimas que se pasan a la aplicación.
- **Falsos negativos (FN):** ataques reales que se transfieren incorrectamente a la aplicación.

Puntuaciones de Client Reputation

Client Reputation utiliza un sofisticado motor de análisis de riesgos para calcular un conjunto de “puntuaciones de riesgo” para cada dirección IP que intenta acceder a su sitio. Analiza las direcciones IP entrantes y utiliza varios factores, como la persistencia del atacante, el número de aplicaciones objetivo, la gravedad del ataque, la magnitud, el sector y los ataques anteriores dirigidos a las aplicaciones de un cliente para determinar una puntuación que especifica la probabilidad de que esta dirección IP participe en un ataque web, entre los que se incluyen:

- **DOSATCK**
  Utiliza botnets para lanzar ataques de denegación de servicio (DoS). El objetivo de un ataque DoS es inundar un sitio con tantas solicitudes falsas que el sitio se vuelve insoportablemente lento o incluso se bloquea. En un ataque distribuido de denegación de servicio (DDoS), estas solicitudes proceden de miles de ubicaciones (normalmente ordenadores o teléfonos infectados por malware), lo que hace imposible detener el ataque simplemente bloqueando una dirección IP determinada.

- **SCANTL**
  Las herramientas de análisis pueden identificar posibles riesgos de seguridad, como la inyección SQL, la falsificación de solicitudes entre sitios (CSRF), redirecciones no válidas y otras vulnerabilidades. Ejecutar una herramienta de análisis web en su propio sitio es una buena idea. Que un malhechor ejecute una herramienta de análisis en su sitio web no lo es.

- **WEBATCK**
  Utiliza técnicas como la inyección SQL, la inclusión remota de archivos o los ataques de scripts entre sitios para realizar tareas como instalar malware o robar datos de usuario. Un hacker podría hacerse con todos sus datos de usuario, incluyendo contraseñas, números de tarjetas de crédito, números de la Seguridad Social y cualquier otra información que usted pudiera haber almacenado en la base de datos de usuarios.

- **WEBSCRP**
  Utiliza herramientas automatizadas para descargar una copia de una página web y luego "raspar" (es decir, copiar) todo el contenido de esa página. Este contenido podría reutilizarse para usos ilegales o poco éticos.

Con Client Reputation, puede proteger de forma proactiva a su organización de fuentes de amenazas sospechosas gracias a la inteligencia acumulada sobre amenazas de Akamai Connected Cloud.

Protección contra malware

El malware es una práctica de ataque habitual de los cibercriminales. Para una protección completa de las aplicaciones, Akamai cuenta con una solución contra el malware. Por motivos de mejora de la eficiencia, tanto interna como externa, las organizaciones de todos los tamaños permiten la carga de archivos. Entre los usos más comunes se incluyen los siguientes:

- Currículos para solicitudes de empleo
- Contratos de trabajo, documentación de incorporación, E-Verify, establecimiento de domiciliaciones bancarias, etc.
- Solicitudes, incluyendo préstamos, configuración de cuentas y solicitudes de crédito
- Estimaciones de seguros o reparaciones de automóviles, hogares, etc.
- Registros médicos para la configuración de cuentas de pacientes o aseguradoras
- Reseñas de productos o experiencias de clientes que incluyan imágenes

La protección contra malware en el entorno de la seguridad de aplicaciones y API detecta y aísla las amenazas en el Edge antes de que lleguen al sistema corporativo al que se dirigen. Las organizaciones pueden proteger el tiempo, el presupuesto y la productividad, así como los datos internos y de los clientes, aprovechando las ventajas de la protección contra malware para aplicaciones y API:

- **Detecta y bloquea el malware en el Edge.**
  Evite los riesgos del análisis en los servidores, pues el malware ya podría haberse propagado en ellos en el momento en que se realiza.
- **Evita la complejidad y libera tiempo.**
  Analice los archivos solo una vez, en lugar de configurar la protección en cada sistema de forma individual, como en el caso de los analizadores ICAP y basados en agentes.
- **Establece la estrategia de seguridad para favorecer el crecimiento.**
  Al elegir un enfoque preventivo y por capas, las organizaciones pueden ampliar la protección a medida que crece la empresa, lo que proporciona una protección adicional en el Edge, además de la opción de volver a escanear en el origen.
- **Proporciona coherencia a las aplicaciones.**
  No es necesario que las empresas configuren ni cambien el código de aplicación. La protección contra malware se aloja completamente en Akamai Connected Cloud.

Análisis de la seguridad de las aplicaciones

App & API Protector incluye el producto preferido (y más utilizado) de Akamai: Web Security Analytics. Esta solución WAAP le permite capturar los eventos de seguridad que tienen lugar en su aplicación web y sus API en la plataforma de Akamai y visualizarlos en las herramientas de análisis de seguridad proporcionadas.

Web Security Analytics es un componente vital de la ciberseguridad moderna, ya que ofrece información completa sobre el tráfico web y las posibles amenazas. Al analizar una amplia variedad de puntos de datos, incluidos patrones de tráfico, el comportamiento de los usuarios y eventos de seguridad, proporciona una visibilidad detallada del estado de seguridad de las aplicaciones web. Este enfoque proactivo permite a las organizaciones detectar y responder a las amenazas de forma más eficaz, mitigando los riesgos antes de que puedan causar daños importantes. Web Security Analytics no solo ayuda a identificar actividades maliciosas, como ataques de bots, inyecciones SQL y scripts entre sitios, sino que también ayuda a comprender y abordar las vulnerabilidades dentro de las aplicaciones web. Además, apoya las iniciativas de cumplimiento mediante la generación de informes que demuestran la conformidad con las políticas de seguridad y los requisitos normativos.

Detección y creación de perfiles de API

Las API permiten a las organizaciones ofrecer potentes experiencias web y móviles, a menudo mediante la exposición de datos y lógica de back-end para desarrollar ofertas nuevas e innovadoras. Pero las API también amplían la superficie de ataque. Las organizaciones necesitan conocer bien cuáles son los terminales de API en su entorno, las funciones de API y sus perfiles de tráfico. La capacidad de detección y creación de perfiles de API de Akamai hace precisamente eso y más, de forma automática y continua.

La función de detección de API alerta a los equipos de seguridad cuando hay API y aplicaciones nuevas y, a menudo, no protegidas, que están conectadas en distintas líneas de negocios dentro de una organización. Esta tecnología de detección automatizada es una nueva característica de la solución WAAP de Akamai para mantener alineados a los equipos de desarrollo, los responsables de las distintas líneas de negocio y los equipos de seguridad.

El motor de seguridad adaptable detecta automáticamente las API cada 24 horas en función de un mecanismo de puntuación que tiene en cuenta el tipo de contenido de respuesta, las características de la ruta y los patrones de tráfico. Los datos de detección incluyen información sobre la especificación API observada con detalles como los siguientes:

- Nombre de host
- Ruta de acceso base
- Ruta de acceso de recurso
- Parámetros y su tipo de datos
- Métodos
- Formato de la API

Las rutas de acceso base y de recursos se determinan en función de un algoritmo que tiene en cuenta la profundidad de la ruta, y el recuento de elementos secundarios y del mismo nivel del tráfico observado para un nombre de host específico con tráfico de API. En la ruta de acceso al recurso, si se observa un parámetro para un método específico, se marca y se identifica el tipo de datos de ese parámetro.

El perfil de tráfico de los terminales de la API contiene información sobre el propósito de la API y el nivel de amenaza actual. Algunos de los puntos de datos incluidos son:

- Total de solicitudes desde que se detectó la API por primera vez, tanto en las últimas 24 horas como viendo la tendencia que siguen con el paso del tiempo.
- Fecha en la que se detectó la API por primera vez y se vio por última vez.
- Número de solicitudes en distintos métodos como GET, PUT, POST, DELETE y OPTIONS.
- Número de solicitudes que generan respuestas 2xx, 3xx, 4xx y 5xx.
- Identificación del cliente final basada en el agente de usuario.
- Errores de respuesta como el porcentaje de tráfico que genera errores del lado del cliente y del lado del servidor.
- Coincidencias de atacantes conocidos, incluido el porcentaje de tráfico total procedente de atacantes conocidos a la plataforma de Akamai, clasificados en atacantes web, analizadores web, scrapers y atacantes DoS.

La protección de las API puede ser todo un desafío si se carece de la visibilidad necesaria. ¿Cómo protege una organización lo que no puede ver? Akamai permite a las empresas detectar y clasificar de forma automática y continua las API, incluidos sus terminales, las definiciones y las características de los recursos y el tráfico. Una vez identificadas las API, Akamai proporciona una amplia protección para hacer frente a ataques DoS, inyecciones maliciosas, ataques de abuso de credenciales, así como contra infracciones de especificación de API. El enfoque de Akamai, independiente del origen y de la nube, permite una fácil detección de las API en todas las aplicaciones sin que el usuario final tenga que llevar a cabo ninguna configuración adicional. Esta visibilidad permite a los desarrolladores, a los propietarios de aplicaciones y a los equipos de seguridad anticiparse a las API nuevas, desconocidas o en constante cambio, así como registrarlas fácilmente para protegerlas.

Visibilidad y mitigación de bots

Dado que los bots contribuyen a más de la mitad del tráfico en los sitios web, puede resultar difícil saber qué bots ayudan a una organización a alcanzar los objetivos y cuáles tienen la intención de perjudicar. Los bots buenos aumentan la eficiencia de una organización al automatizar evaluaciones, conversaciones o recomendaciones. Los bots maliciosos pueden obstruir las rutas de tráfico y afectar a la experiencia operativa y del cliente, lo que repercute negativamente en los ingresos. En App & API Protector, las funciones asociadas a la visibilidad y mitigación de bots ofrecen potentes mecanismos para detectar bots buenos y dejarlos pasar, al tiempo que bloquean los maliciosos. Esto permite lo siguiente a las organizaciones:

- **Ver los bots y comprender su impacto**
  La visibilidad del tráfico de bots es fundamental para las empresas digitales modernas, dado el uso generalizado de bots para operaciones como la búsqueda, la comprobación del rendimiento del sitio y la interacción con partners empresariales.
- **Mejorar el control operativo**
  El bloqueo de los bots maliciosos mejora la eficiencia, reduce los riesgos empresariales y financieros, y ayuda a controlar el gasto en TI.
- **Adoptar mejores decisiones basadas en datos**
  Los análisis e informes detallados ayudan a tomar decisiones creativas y eficaces sobre la trayectoria del cliente, la estrategia de seguridad, la tolerancia al riesgo y las operaciones de TI.

Visibilidad y mitigación de bots intrínsecas a App & API Protector

App & API Protector ofrece funciones de detección y control del tráfico de bots que pueden afectar negativamente al rendimiento y la seguridad de las propiedades web. Proporciona visibilidad temprana para supervisar de forma proactiva las anomalías y amenazas relacionadas con bots que se desarrollan a lo largo del tiempo.

Uso de la solución de control de bots de Akamai distribuida en App & API Protector:

- Acceso a más de 1700 bots definidos conocidos por Akamai
- Visibilidad en tiempo real del tráfico de bots
- Creación de definiciones de bots personalizadas
- Permitir los bots buenos y bloquear los maliciosos
- Consulta de la visibilidad de bots y los informes de tendencias

Para sitios con problemas avanzados de bots, Akamai ofrece Bot Manager, que incluye un sofisticado sistema de protección contra bots para optimizar el comercio electrónico y la seguridad digital. Bot Manager proporciona acciones más detalladas para bots persistentes y maliciosos, como los que se utilizan para ataques como:

- Credential Stuffing
- Acaparamiento de inventario
- Scraping de contenido y precios
- Abuso de la lógica empresarial

Funciones clave en relación con los bots

Akamai es consciente de la creciente necesidad de gestionar los bots a través de un sistema WAAP y ha mejorado sus herramientas de visibilidad y mitigación para incluir nuevas funciones integradas, como las siguientes:

- **Detección de suplantación del navegador**
  Esta funcionalidad de Akamai Bot Manager, una de las favoritas de los clientes, utiliza modelos de puntuación dinámicos y aprendizaje automático para identificar y contrarrestar las actividades de bots en el navegador, y se incluye en App & API Protector.
- **Acciones de respuesta condicional**
  Ahora, los clientes conocen mejor las actividades de los bots en el navegador y pueden responder con acciones condicionales para aplicar diferentes estrategias de respuesta contra bots maliciosos.
- **Acciones desafiantes**
  Enfréntese a los bots con una variedad de diferentes acciones desafiantes, como desafíos intercalados que, si no se resuelven, ofrecen la posibilidad de bloquear el acceso al contenido.

Más que un WAF: ventajas de la solución de Akamai

El enfoque de Akamai con respecto a WAAP dio como resultado la solución App & API Protector. Sin embargo, hay más de un producto que beneficia a nuestros clientes de WAAP. Akamai Connected Cloud, que se basa en la plataforma global más distribuida y está respaldada por cientos de expertos en amenazas, ofrece rendimiento, disponibilidad, inteligencia, experiencia y seguridad.

Inteligencia y detección de amenazas

Contar con una solución interna de inteligencia sobre amenazas sólida mejora la capacidad de un proveedor de WAAP para responder a las cambiantes amenazas. Sin embargo, la calidad, la puntualidad y la utilidad de la información proporcionada determinarán el impacto en la eficacia de la seguridad de las aplicaciones. Akamai analiza continuamente los datos disponibles a través de Akamai Connected Cloud para identificar las tendencias actuales en el panorama de amenazas, los nuevos vectores de ataque a medida que se observan por primera vez y los atacantes actualmente activos. A continuación, Akamai incorpora esa inteligencia a su solución WAAP de varias formas.

El motor Adaptive Security Engine de Akamai, descrito anteriormente en este documento, combina dos niveles de inteligencia sobre amenazas en un potente motor capaz de gestionar automáticamente las protecciones más recientes para nuestros clientes. Además del aprendizaje automático y la adopción de reglas automatizadas, Adaptive Security Engine está respaldado por la inteligencia frente a amenazas de la plataforma global de Akamai y un gran equipo de investigadores de amenazas expertos.

Inteligencia de la plataforma de Akamai

Contar con una de las plataformas globales más grandes proporciona a Akamai el mecanismo necesario para analizar a escala global el tráfico de ataque dirigido contra cada uno de sus clientes. Nuestra base de datos de inteligencia incluye una media de 1056 TB de datos sobre ataques al día. La solución aprovecha la visibilidad de Akamai sobre el tráfico web de miles de las empresas online más grandes, con más tráfico y atacadas con más frecuencia para adquirir datos relevantes y de alta calidad de cuyo análisis se encarga el equipo de investigación de amenazas:

- **Activadores WAAP**
  Recopila datos directamente de las implementaciones de WAAP globales de Akamai, mediante la captura de eventos de ataque reales dirigidos a todos los clientes que utilizan nuestras soluciones de seguridad.

- **Registros de CDN**
  Incorpora análisis offline realizados en registros de eventos de todos los clientes de Akamai, incluidos aquellos que no han implementado su solución WAAP.

La base de datos de inteligencia de Akamai alberga uno de los conjuntos de datos más grandes del mundo (9 PB). Para las organizaciones que priorizan la seguridad de sus empresas y clientes, la inteligencia sobre amenazas de Akamai está a la cabeza de cualquier otro proveedor de soluciones WAAP.

Investigación de amenazas y respuesta a incidentes

Las organizaciones dedicadas a la investigación de amenazas y la respuesta a incidentes proporcionan inteligencia humana y análisis para complementar y ampliar la cobertura de ataques que ofrecen las soluciones WAAP. Akamai cuenta con varios equipos con diferentes misiones para ayudar a nuestros clientes de WAAP, así como para identificar nuevos vectores de ataque que pueden requerir protecciones adicionales.

Investigación de amenazas

El equipo de investigación de amenazas realiza análisis periódicos de las tendencias de ataques web en toda la base de clientes de Akamai, además de análisis personalizados para clientes individuales según sea necesario. El equipo también diseña e implementa la heurística en busca de información útil que permita crear y actualizar la lógica principal de reglas de WAF y Client Reputation.

Respuesta ante incidentes

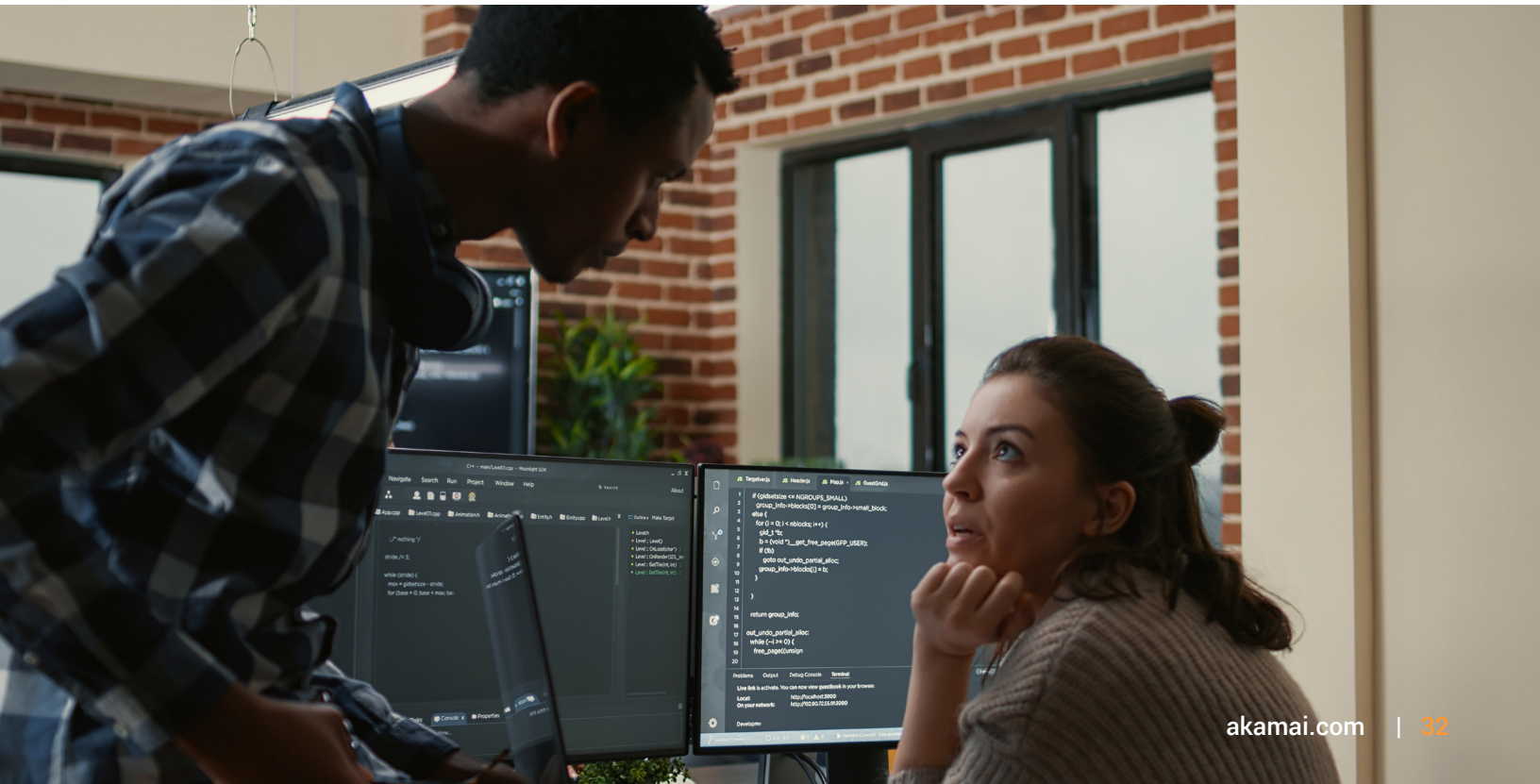
Akamai opera dos equipos de respuesta ante incidentes, el equipo de respuesta a incidentes de seguridad informática (CSIRT) y el equipo de respuesta a incidentes de inteligencia de seguridad (SIRT), que trabajan con el centro de operaciones de seguridad (SOC) global de Akamai y proporcionan análisis y respuesta a incidentes a clientes individuales cuando sufren un ataque. Además, el CSIRT supervisa a los clientes de Akamai que sufren ataques con frecuencia y que representan una amplia gama de sectores para identificar nuevos vectores o tendencias de ataque.

Detección rápida de amenazas

Nuestras nuevas capacidades permiten una rápida implementación de protecciones contra amenazas emergentes y CVE destacados. Las actualizaciones automáticas y la opción de implementar acciones “gestionadas por Akamai” le permiten gestionar sus defensas con agilidad.

Protección contra CVE

El equipo de investigación de amenazas de Akamai supervisa continuamente las vulnerabilidades y exposiciones comunes, y garantiza que la solución WAAP se actualice para proteger las aplicaciones de los clientes y proporcionar la confirmación necesaria a través de la herramienta de búsqueda de CVE de Akamai. Esta herramienta ayuda al proporcionar información detallada sobre las CVE, incluidos los niveles de amenazas y datos sobre las protecciones actuales de Akamai. El catálogo de protección contra CVE le proporciona la visibilidad necesaria para priorizar las estrategias de seguridad de acuerdo con las protecciones de Akamai. Además, le permite buscar en la base de datos de CVE para identificar las medidas de protección activas de Akamai contra una vulnerabilidad, así como evaluar el nivel de amenaza y acceder a los datos de las CVE.



Plataforma en el Edge distribuida globalmente

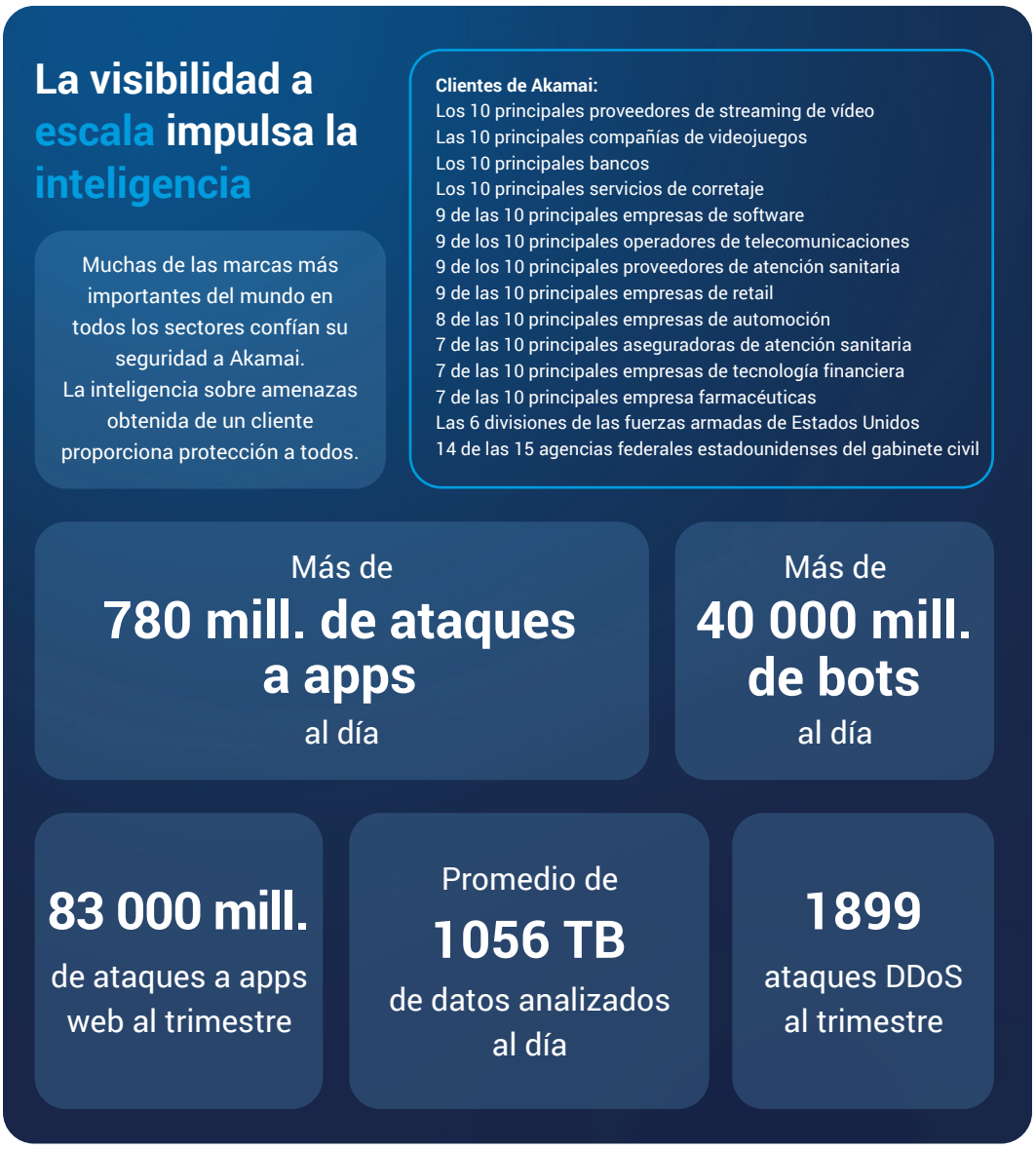
Fiabilidad y resistencia

Las soluciones WAAP prémium se basan en redes amplias y potentes que no limitan el tráfico legítimo de los clientes ni siquiera en el caso de los ciberataques más grandes. La probada calidad, capacidad y facilidad de uso de la plataforma global de un proveedor de WAAP deben tener la misma importancia que las funciones de la solución. Cuando un proveedor de WAAP no logra distribuir un tráfico legítimo durante un ataque, los clientes deben plantearse si han invertido en una solución o simplemente en una herramienta.

Akamai tiene como objetivo ofrecer a sus clientes un rendimiento y una protección líderes en el sector. Esta misión solo es posible si los servicios se construyen sobre la base más sólida: Akamai Connected Cloud Akamai ha creado la plataforma en la nube más distribuida del mundo, compuesta por más de 4200 puntos de presencia en más de 130 países.

Entre los clientes de Akamai se incluyen los 10 principales servicios de corretaje, los 10 principales bancos, los 10 principales servicios de streaming de vídeo y las 10 principales empresas de videojuegos. Nuestra base de clientes abarca desde la mayoría de las principales empresas de automoción, proveedores de atención sanitaria, retail y operadores de telecomunicaciones hasta un número significativo de agencias gubernamentales y las fuerzas armadas.

Estos clientes confían en las capacidades de Akamai para respaldarlos y protegerlos de los 40 mil millones de bots por día, los 780 millones de ataques de aplicaciones por día y los 1889 ataques DDoS por trimestre que amenazan con derribar sus redes. Akamai proporciona sus soluciones de seguridad con éxito porque la información sobre amenazas recopilada de un cliente se utiliza también para proteger al resto de clientes. La escala de la plataforma global de Akamai ofrece tanto la cantidad como la calidad de los datos que se necesitan para proteger a las organizaciones que están entrando en la era de la IA.



Escala mundial

En el caso de un WAF, el problema de la escalabilidad gira tanto en torno a su capacidad para inspeccionar el volumen necesario de tráfico web, inicialmente y a medida que aumenta con el tiempo, como al número de reglas necesarias para evaluar dicho tráfico. Las soluciones WAF tradicionales basadas en hardware suelen carecer de la escala suficiente porque están limitadas a los recursos de CPU y memoria disponibles en el dispositivo y pueden tener que competir con otras soluciones en el mismo dispositivo.

La implementación de una solución WAAP integrada en la plataforma en la nube de Akamai elimina el problema de la escala al aprovechar los recursos de servidor distribuidos de Akamai para inspeccionar el tráfico web entrante. Los usuarios y los atacantes se conectan a sitios web protegidos a través del servidor de Akamai más cercano, que analiza el tráfico en busca de ataques y bloquea cualquier solicitud maliciosa detectada. Gracias a esto, la solución WAAP de Akamai puede ampliarse sin problemas cada vez que aumenta el volumen de tráfico de aplicaciones web (tanto picos repentinos de tráfico como crecimiento a largo plazo), así como con las nuevas ubicaciones de usuarios en todo el mundo.

Rendimiento

Un bajo rendimiento puede dificultar la implementación de una solución de seguridad, especialmente una solución WAAP que se implemente en línea delante de una aplicación. Una reducción del rendimiento de los sitios web esenciales para la empresa puede dar lugar a la disminución de la productividad, una experiencia de usuario deficiente, un tiempo de comercialización más lento y la caída de los ingresos.

La escala global de la plataforma en la nube de Akamai hace posible que la solución WAAP proteja las aplicaciones web sin reducir el rendimiento. Una solución WAAP distribuida globalmente inspecciona el tráfico HTTP a medida que entra en la plataforma, distribuyendo los recursos de CPU y memoria necesarios para analizar dicho tráfico entre todos los servidores de la plataforma. Esto elimina la cuestión del rendimiento como fuente de fricción dentro de la organización y obstáculo para el despliegue.

Plataforma en el Edge que optimiza la protección

Las soluciones de seguridad de aplicaciones web independientes de la nube de Akamai funcionan a la perfección en toda la plataforma para proteger de una amplia gama de ataques basados en API y aplicaciones. La siguiente imagen ilustra la pila completa de mecanismos y controles de seguridad por capas de Akamai que se utilizan para mantener las amenazas lejos del origen, al tiempo que mejora el rendimiento y el acceso de los usuarios legítimos.

Akamai App & API Protector incluye una amplia gama de mecanismos y controles de seguridad integrados automáticamente (en azul) para proporcionar una defensa integral inmediata, además de añadir productos y servicios adicionales de Akamai que ofrecen una protección completa de la capa 7.

Asistencia gestionada en caso de ataque

Además de la gestión continua de WAAP, Akamai también proporciona a los clientes asistencia gestionada en caso de ataque: supervisión ininterrumpida de los sitios web protegidos y respuesta gestionada ante cualquier ataque detectado.

El equipo de asistencia gestionada en caso de ataque emplea al personal del SOC global de Akamai para responder a los incidentes de seguridad a medida que se producen mediante las siguientes acciones:

- Responde a las alertas de WAAP y a las solicitudes de los clientes y realiza una investigación adicional de los problemas.
- Determina la firma de ataque correspondiente e implementa medidas de mitigación adicionales.
- Trabaja con los equipos de aplicaciones del cliente para medir la eficacia y precisión de las medidas de mitigación implementadas, ajustándolas según sea necesario.
- Revisa la respuesta general con los equipos de aplicaciones del cliente tras el incidente.
- Proporciona botones de alerta de ataque en la interfaz para iniciar una solicitud de asistencia de emergencia.

Centro de control de operaciones de seguridad (SOCC)

El SOCC de Akamai lleva más de 10 años ayudando a mitigar muchos de los ataques más grandes del mundo, protegiendo a los clientes de un panorama de amenazas global en constante evolución.

La supervisión y mitigación de un ataque malicioso requiere cuatro funcionalidades:

- Visibilidad global
- Supervisión proactiva y alertas
- Mitigación ágil de los ataques
- Servicio continuo de asesoramiento por parte de un equipo de seguridad experimentado

El SOCC de Akamai ofrece estas capacidades, pues opera la infraestructura de seguridad más grande del mundo. Todo el tráfico de red se ejecuta en nuestra plataforma de seguridad unificada, que recopila inteligencia en tiempo real. Por ejemplo, Akamai recopila tendencias de seguridad, como el reciente gran aumento de los ataques de inyección SQL.

Todo esto ayuda al equipo de seguridad de Akamai a mitigar rápidamente las amenazas que sufren sus clientes con la máxima eficacia y el mínimo impacto.

Conclusión

Además de la protección frente a DDoS en el nivel de red y de aplicación, las nuevas formas de bots automatizados y ataques dirigidos a través de API y componentes del lado del cliente implican que las organizaciones deben proteger todas sus aplicaciones web, terminales de API, navegadores e infraestructura con un enfoque de seguridad integral de defensa en profundidad. Los responsables y los profesionales de la seguridad necesitan soluciones de seguridad de las aplicaciones web que identifiquen y mitiguen rápidamente las amenazas de numerosos vectores de ataque, y que extiendan las protecciones tradicionales más allá del firewall a las tecnologías de seguridad adyacentes para obtener una protección óptima.

El enfoque de Akamai respecto a WAAP consiste en ofrecer un conjunto de soluciones sin igual en cuanto a cobertura y eficacia, ya que proporciona todas las tecnologías de seguridad necesarias para una estrategia de seguridad moderna. Creemos que la solución de seguridad líder no debería ser solo para las marcas más grandes o populares del mundo. Nuestra cartera multicapa para protección de aplicaciones y API pone la seguridad de las aplicaciones web a disposición de cualquier organización que dé prioridad a este aspecto.

Con una solución que evoluciona y se adapta continuamente, y aprovechando su amplia y profunda inteligencia sobre ataques, Akamai colabora con empresas globales para modernizar y mejorar continuamente la seguridad. Nuestro objetivo es dotar a los equipos de seguridad de su organización de la inteligencia, la visibilidad, la automatización y la orientación necesarias para impulsar las iniciativas internas y, al mismo tiempo, mantener a los atacantes alejados de sus sistemas corporativos. Por eso, las marcas más exigentes confían en nosotros para proteger sus actividades en el universo online.

La seguridad de Akamai protege las aplicaciones que impulsan su negocio en cada punto de interacción sin comprometer el rendimiento ni la experiencia del cliente. Gracias a la escala de nuestra plataforma global y su visibilidad de las amenazas, colaboramos con usted para prevenirlas, detectarlas y mitigarlas, de forma que pueda generar confianza en la marca y cumplir su visión. 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 el 25 de febrero.