

# KONA SITE DEFENDER

PROTEJA SUS SITIOS Y APLICACIONES WEB FRENTE AL TIEMPO DE INACTIVIDAD Y AL ROBO DE DATOS



Seguridad de aplicaciones adaptada a su negocio, su estrategia de seguridad y su superficie de ataque, avalada por Akamai Intelligent Platform™. Disfrute de la protección más reciente contra amenazas con un rendimiento, escala y experiencia de usuario final incomparables, incluso durante un ataque.

## Acerca de Kona Site Defender

Para prosperar en la rápida e hiperconectada economía digital actual, sus aplicaciones empresariales están diseñadas para que los usuarios y los partners comerciales accedan a ellas de forma sencilla, masiva y a alta velocidad, a través de sitios web y API. Sin embargo, también suponen un atractivo punto de entrada para acceder a datos valiosos, por lo que son el principal objetivo de ataques graves. Kona Site Defender ofrece una amplia protección a los sitios web y las aplicaciones frente a los tiempos de inactividad y al robo de datos que causan los ataques web sofisticados y oportunistas, así como los ataques distribuidos de denegación de servicio (DDoS). Las organizaciones que utilizan Kona Site Defender tienen la capacidad de centrar sus esfuerzos en implementar innovaciones importantes en su oferta web para mejorar el rendimiento de distribución sin la distracción de un número creciente de ataques dirigidos.

## Descripción general de Kona Site Defender

Kona Site Defender protege los sitios web y las API contra todo tipo de sofisticados ataques DDoS, ataques a aplicaciones web y ataques directos contra el origen, con un conjunto de herramientas multicapa siempre activo. Se despliega por toda la plataforma Akamai Intelligent Platform™, compuesta por más de 200 000 servidores, presentes en más de 3500 ubicaciones en 1600 redes de 131 países. Esta solución bloquea los ataques a gran escala en el perímetro de la red de Akamai y lejos de su servidor web y aplicaciones.

## Protección contra DDoS siempre activa

El firewall de aplicaciones web de Kona Site Defender absorbe los ataques DDoS dirigidos a la capa de aplicación y autentica el tráfico válido en el perímetro de la red. Los controles automatizados incorporados responden a los ataques en cuestión de segundos. Para los ataques realmente nuevos y sofisticados que requieren una respuesta más específica, los expertos en seguridad de los clientes pueden crear reglas personalizadas basadas en firmas individuales. Además, la arquitectura de Akamai Intelligent Platform™ está diseñada como un proxy inverso, solo acepta tráfico en los puertos 80 y 443 y contrarresta automáticamente todos los ataques DDoS a la capa de red. Con una capacidad de distribución de más de 61 Tbps de tráfico, tenemos la capacidad de absorber los mayores ataques dirigidos a la capa de red sin ni siquiera pestañear. Los ataques DDoS contra la infraestructura DNS pueden mitigarse con la solución complementaria Fast DNS.

## Firewall de aplicaciones web

El firewall de aplicaciones web incluye una completa colección de reglas de firewall de capa de aplicación predefinidas y configurables. El equipo de investigación de amenazas de Akamai mantiene esta colección al día con actualizaciones regulares basadas en la inteligencia interna ante amenazas derivada de la visibilidad en múltiples categorías de entre el 15 % y el 30 % del tráfico de Internet global. Así se aumenta la precisión general en la disminución de falsos positivos y negativos. Las personalizaciones de reglas pueden servir de parches virtuales para mitigar rápidamente las nuevas vulnerabilidades de los sitios web, a la vez que se actualiza la aplicación según el proceso de ciclo de vida normal.

## Protección de API

Kona Site Defender utiliza modelos de seguridad positivos y negativos para proteger las API de llamadas maliciosas. Los clientes pueden definir qué tipos de solicitudes y llamadas están permitidos. Kona Site Defender inspecciona los parámetros de las API RESTful con referencia a una lista blanca de valores esperados, además de comprobar que no haya contenido peligroso en los parámetros de ruta y de cuerpo de JSON. Se usan controles de frecuencia para mitigar los ataques DDoS lanzados a través de las API. Kona Site Defender ofrece la elaboración de informes y análisis a nivel de API.

## Seguridad de DevOps

Las empresas están adoptando cada vez más las tecnologías de cloud computing, la automatización y las prácticas de desarrollo y operaciones (DevOps), y necesitan integrar la seguridad en sus ágiles procesos de desarrollo. Con Kona Site Defender, las organizaciones tienen una manera de actualizar regularmente los controles de seguridad e incluirlos en sus procesos de desarrollo. Kona Site Defender ofrece a las empresas diversas API de gestión que permiten a los desarrolladores y los administradores integrar tareas de configuración de seguridad comunes en el proceso de CI/CD.

## VENTAJAS



Protección de los ingresos, la fidelidad de los clientes y la imagen de la marca



Mantenimiento del rendimiento de las aplicaciones incluso en caso de ataque



Reducción de los costes generados durante picos del tráfico de ataques



Integración avanzada con infraestructura de TI y DevOps



Aplicación de los conocimientos de los mejores expertos en materia de seguridad de aplicaciones



Obtención de una profunda visibilidad y percepción de las amenazas con el análisis de la seguridad web

# Kona Site Defender

## Características



### Plataforma global en la nube

Al estar integrado en la plataforma de distribución en la nube más grande del mundo, Kona Site Defender extiende la infraestructura de seguridad a la nube y detiene los ataques antes de que puedan llegar a sus aplicaciones.



### Protección contra DDoS

Kona Site Defender protege sus aplicaciones de los mayores ataques DDoS, eliminando automáticamente los ataques a la capa de red en el perímetro y respondiendo a los ataques a la capa de la aplicación en cuestión de segundos, lo que reduce al mínimo el tiempo de inactividad potencial.



### Firewall de aplicaciones web

Kona Site Defender incluye un firewall de aplicaciones web de alta escalabilidad que protege su empresa contra amenazas a la capa de aplicación gracias a un conjunto de reglas automatizado y con grandes posibilidades de personalización.



### Protección de API

Kona Site Defender proporciona protección centrada en las API contra ataques DDoS y ataques basados en parámetros. Así, las organizaciones pueden definir las API que desean proteger y configurar y generar informes sobre eventos de seguridad según la API.



### Actualizaciones de reglas

Gracias a la visibilidad de los ataques más recientes contra las organizaciones online más grandes y que sufren ataques con mayor frecuencia, Akamai actualiza de manera continua y transparente el conjunto de reglas de seguridad de Kona Site Defender, lo que le permite controlar la activación.



### Parches virtuales

Su equipo de seguridad personaliza las reglas y le proporciona un parche virtual para sus aplicaciones. De esta forma, se abordan rápidamente las nuevas vulnerabilidades o simplemente se personaliza la protección del tráfico de su sitio web.



### Disponibilidad permanente

Kona Site Defender está integrado en una plataforma altamente resistente y de recuperación automática respaldada por un acuerdo de nivel de servicio (SLA) que garantiza una disponibilidad permanente. Además, incluye funciones de conmutación por error del sitio que utilizan la plataforma para mantener su sitio web siempre activo, incluso si sus servidores se vienen abajo.



### SureRoute

Kona Site Defender incluye la tecnología SureRoute de Akamai para que los usuarios encuentren siempre la ruta más adecuada a su sitio web, con lo que se logra mitigar los problemas de red que escapan a su control y mejorar el rendimiento y la disponibilidad.



### Rendimiento mejorado

Saque partido a las capacidades de rendimiento integradas en la red de distribución de contenido (CDN) de Akamai, como el almacenamiento en caché, las capacidades de descarga avanzada y la optimización de TCP, para que los usuarios disfruten de un mejor rendimiento en su sitio web incluso durante los ataques de mayor tamaño.



### API de gestión

Las API de gestión para tareas de configuración comunes permiten integrar los controles de seguridad en el proceso de desarrollo de software y entrega de la empresa.



### Análisis avanzado de la seguridad web

Con una evaluación detallada de los eventos, su equipo de seguridad podrá determinar mejor los cambios necesarios para mantener una configuración de seguridad óptima que se adapte a sus necesidades empresariales específicas.

## Opciones adicionales para aumentar la protección



### Client Reputation

Este módulo optativo puede mejorar las decisiones de seguridad en un entorno difícil, al proporcionarle la capacidad de filtrar clientes maliciosos en función de su comportamiento y puntuación de riesgo.



### Seguridad gestionada

Delegue la gestión y la supervisión de la seguridad, así como la mitigación de amenazas, en los expertos en seguridad de Akamai. Está diseñada para ayudarle a esbozar una estrategia ágil de seguridad en la nube.



Akamai, la mayor plataforma de entrega en la nube del mundo y en la que confían más usuarios, ayuda a los clientes a ofrecer las mejores y más seguras experiencias digitales en cualquier dispositivo, en cualquier momento y en cualquier lugar. La plataforma masivamente distribuida de Akamai no tiene parangón en términos de escala, con más de 200 000 servidores repartidos en 130 países, lo que ofrece a los clientes un excelente rendimiento y protección contra las amenazas. La cartera de soluciones de rendimiento web y móvil, seguridad en la nube, acceso empresarial y distribución de vídeo de Akamai está respaldada por un servicio de atención al cliente excepcional y una supervisión ininterrumpida. Para descubrir por qué las principales instituciones financieras, líderes de retail online, proveedores de contenidos multimedia y de entretenimiento, y organizaciones gubernamentales confían en Akamai, visite [www.akamai.com/es/es](http://www.akamai.com/es/es) y [blogs.akamai.com/es/](http://blogs.akamai.com/es/), o siga a @Akamai en Twitter. Encontrará nuestra información de contacto global en [www.akamai.com/locations](http://www.akamai.com/locations); también puede llamar al +34 91 793 32 43. Publicado en abril de 2018.