RESUMEN DE PRODUCTO

Cloudflare WAF

Un WAF que garantiza la seguridad de las aplicaciones modernas

Desafíos de la seguridad de las aplicaciones

Las aplicaciones son más importantes que nunca para las empresas, por lo tanto, son un blanco constante para los atacantes, y eso supone una mayor superficie de ataques.

Las cuestiones centrales son mantener la protección contra las explotaciones de vulnerabilidades de día cero, detectar los intentos de evasión, reducir el riesgo de relleno de credenciales que lleva a la usurpación de cuentas, detectar la pérdida de datos, e incluso el análisis de cargas de malware en las aplicaciones.

A lo anterior, se le suma la necesidad de garantizar la protección de las aplicaciones como parte de una estrategia de seguridad más amplia y unificada, que también proteja las API, detenga los bots y reduzca los riesgos del lado del cliente. Y todo esto debe lograrse sin cargar a los equipos con excesivos problemas de administración.

WAF de Cloudflare

El firewall de aplicaciones web (WAF) de Cloudflare es el pilar fundamental de nuestro conjunto de soluciones de seguridad avanzada para aplicaciones, un modo de mantenerlas seguras y productivas. Cloudflare WAF es el único que brinda visibilidad total de la seguridad: ofrece protección por capas contra ataques OWASP y vulnerabilidades emergentes, detecta evasiones y nuevos ataques con aprendizaje automático, bloquea la usurpación de cuentas, detecta la pérdida de datos y mucho más, mientras protege las aplicaciones dondequiera que estén alojadas. Nuestras funciones sólidas de seguridad para aplicaciones, como la seguridad de las API y la mitigación de bots, están totalmente integradas con nuestro WAF, y recurren al mismo motor de reglas sólido, que se brinda desde una de las primeras conectividades cloud del mundo.

Visibilidad de los ataques e incorporación sencilla

Ofrecemos análisis de seguridad diferenciados para visualizar todo el tráfico, mitigado o no. La visibilidad inmediata del panorama de amenazas ofrece un retorno de la inversión tangible, lo que permite a los equipos comprender su tráfico de ataque y las protecciones que deben implementar luego de la incorporación.

Protección rápida para los ataques nuevos

Debido a las decenas de miles de vulnerabilidades que aparecen cada año, nuestro WAF añade rápidamente nuevas reglas administradas para bloquear los posibles riesgos de explotación de vulnerabilidades recientes (día cero). Para detectar las evasiones, nuestras reglas administradas bloquean la explotación de vulnerabilidades, complementadas con WAF Attack Score obtenidas del aprendizaje automático.

Información sobre amenazas que impulsa una gran red global

La eficacia de la seguridad comienza con tener los mejores datos, y nuestra red global extensa redirecciona mediante proxy el 20 % de Internet, lo que nos brinda una visión inigualable del panorama de amenazas. Estos datos impulsan los modelos de aprendizaje automático que empleamos junto con las detecciones tradicionales basadas en firmas para encontrar y mitigar los intentos de ataque con alta precisión.

Desafíos de la seguridad de las aplicaciones

Cloudflare protege de manera más eficaz.

Ofrecemos una seguridad WAF más eficaz con protecciones en capas:

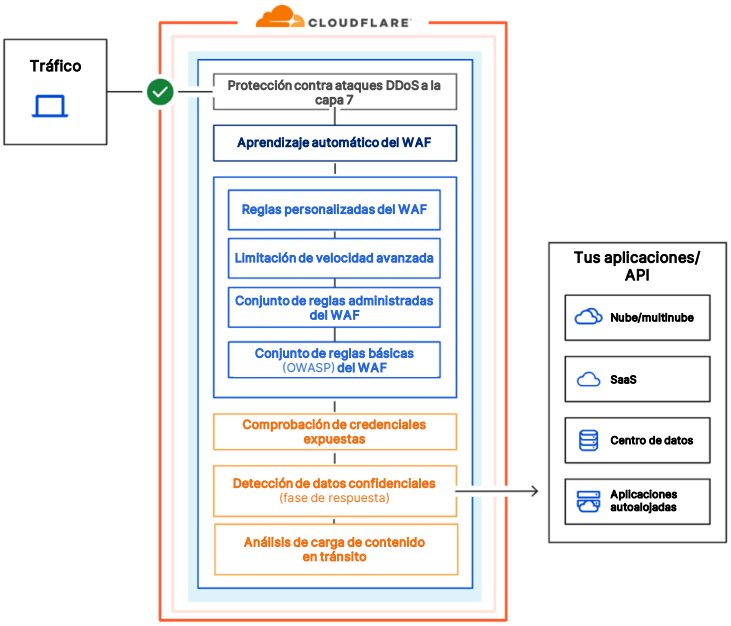
- Análisis de seguridad
- Múltiples conjuntos de reglas administradas
- Reglas personalizadas
- Detecciones a partir del aprendizaje automático
- Detección de datos confidenciales
- Comprobaciones de credenciales robadas
- Limitación de velocidad avanzada
- Análisis de carga antimalware

Cloudflare responde más rápido.

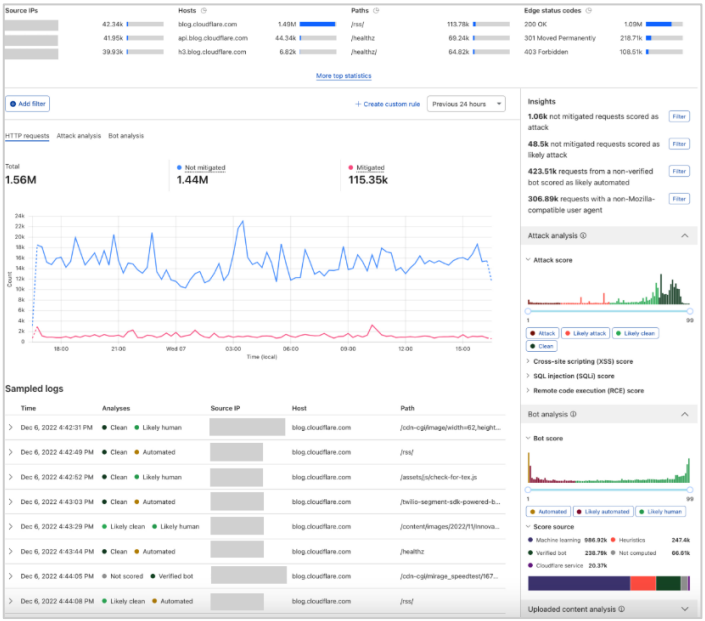
Brindamos una protección más rápida contra las vulnerabilidades. Para vulnerabilidades importantes como HTTP/2 Rapid Reset, Log4j y muchas otras, implementamos varias reglas administradas un día hábil más rápido que otros proveedores de WAF.

Cloudflare integra por completo la seguridad de las aplicaciones.

Nuestro WAF está totalmente integrado con el resto de nuestro conjunto de soluciones de seguridad para las aplicaciones, incluida API Gateway y la gestión de bots, todo en un solo paso desde la conectividad cloud de Cloudflare.



Análisis de seguridad del WAF



WAF para la seguridad empresarial

Integración con las plataformas SIEM y compatibilidad con los SOC

Las API de Cloudflare y las integraciones de registros sin procesar facilitan la integración con tu SIEM o permiten a tus centros de operaciones de seguridad (SOC) aprender de la información que brinda Cloudflare.

DevSecOps más fácil

Nuestra integración con Terraform, que no requiere configuración, hace que la incorporación de la seguridad de las aplicaciones en los enfoques de DevOps sea algo automático.

Con el respaldo de Cloudforce One

La seguridad para aplicaciones de Cloudflare recibe información sobre amenazas de Cloudforce One, nuestro equipo dedicado, y bloquea las amenazas mediante nuevas detecciones basadas en la información que va incorporando y en las nuevas tácticas, técnicas y procedimientos.

Seguridad de las aplicaciones web	
Protecciones por capas de varios conjuntos de reglas WAF	Evita las cargas malintencionadas en cualquier componente de solicitud con numerosos conjuntos de reglas. 1. Reglas administradas por Cloudflare 2. Conjuntos de reglas básicas de OWASP 3. Reglas personalizadas para detener cualquier ataque. Nuevas reglas administradas que se probaron en una gran cantidad de tráfico para garantizar el menor número de falsos positivos.
Reglas actualizadas para las protecciones de día cero	Reglas que los equipos de seguridad de Cloudflare actualizan continuamente para garantizar la protección contra los nuevos ataques y la explotación de vulnerabilidades de día cero antes de que las revisiones o actualizaciones estén disponibles.
Detecciones a partir del aprendizaje automático	Evita los intentos de omisión con modelos de aprendizaje automático para complementar los conjuntos de reglas en capas. Hay cuatro puntuaciones de ataque distintas para las reglas: puntuación de ataque de WAF global, puntuación de ataque XSS, puntuación de ataque SQLi y puntuación de ataque RCE.
Conjuntos de reglas específicas para plataformas grandes de comercio electrónico y sistemas de gestión de contenidos	Recibe una protección lista para aplicar sin costo adicional para plataformas como WordPress, Joomla, Plone, Drupal, Magneto, IIS, entre otras.
Configuración de reglas personalizadas	Crea un modelo de seguridad positivo o negativo al implementar las reglas o los conjuntos de reglas con las siguientes acciones: BLOQUEO, DESAFÍO ADMINISTRADO, DESAFÍO JS, OMISIÓN, REGISTRO, CAPTCHA HEREDADO, RESPUESTAS PERSONALIZADAS.
Limitación de velocidad avanzada	Evita el abuso, los ataques DDoS y los intentos por fuerza bruta dirigidos a aplicaciones y las API limitando la velocidad de las direcciones IP individuales o por atributos de encabezado (p. ej., clave, cookie, token), ASN o país.
Detección de datos confidenciales	Detecta respuestas que contienen datos confidenciales, como la información de identificación personal, la información financiera, los números de tarjetas de crédito o información confidencial como claves de API.
Comprobación de credenciales expuestas	Detecta ataques de relleno de credenciales con credenciales robadas antes de que se apropien de las cuentas de los usuarios finales.
Análisis de carga de contenido	WAF Content Scanning analizará los archivos cargados en busca de malware, y puedes combinar sus señales con otros parámetros de la solicitud mediante la creación de reglas personalizadas.
SSL/TLS	Descarga y configura completamente el tráfico SSL para tus aplicaciones.
Menos falsos positivos	Nuevas reglas probadas en grandes cantidades de tráfico para garantizar el menor número de falsos positivos.
Compatibilidad con gRPC y Websocket	Redireccionamiento y protección del tráfico para los puntos finales de gRPC y Websocket.
Páginas de bloqueo personalizables	Personaliza las páginas de bloqueo con los detalles adecuados para los visitantes.
Integración total con el conjunto más amplio de productos de Cloudflare	Mejora el rendimiento de las aplicaciones, el enrutamiento del tráfico por ubicación geográfica y aprovecha el procesamiento perimetral.

Visibilidad, informes y programabilidad	
Análisis de seguridad	Visualización de todos los ataques potenciales, según la puntuación del aprendizaje automático.
Registro en tiempo real y acceso a archivos de registro sin procesar	Obtén visibilidad para configurar el WAF, realiza un análisis exhaustivo que cubra todas las solicitudes del WAF.
Registro de cargas	Registra y cifra las cargas maliciosas para el análisis de incidentes.
Integraciones de SIEM	Envía o extrae registros directamente a tus SIEM existentes.
Integración con Terraform	Incorpora la seguridad de las aplicaciones en los flujos de trabajo de CI/CD.
Gestión	
Gestión desde un solo panel	Gestión optimizada con un único panel para implementar y gestionar la seguridad y el rendimiento global de las aplicaciones.
Gestión a nivel de cuenta	Ahorra tiempo en la gestión del WAF mediante una única configuración del WAF a nivel de cuenta para todos los dominios.
Alta disponibilidad, con acuerdos de nivel de servicio	Garantía del 100 % de tiempo activo, incluidas las sanciones económicas si se incumplen los acuerdos de nivel de servicio.
No requiere hardware, software ni configuración	Implementación con un simple cambio de DNS.
Certificación PCI	Cloudflare tiene la certificación de proveedor de servicios de primer nivel.
Autorización de FedRAMP	Nuestro paquete Cloudflare for Government, que incluye la seguridad para las aplicaciones, está aprobado por FedRAMP.

¿Quieres más información? Regístrate en nuestra serie de demostraciones sobre la seguridad de las aplicaciones.