

WAF de Cloudflare

Un WAF que garantiza la seguridad de las aplicaciones modernas

Desafíos de la seguridad de las aplicaciones

Las aplicaciones son más imprescindibles que nunca para las empresas. Esto supone una superficie de ataque ampliada, por lo que son constantemente el objetivo de los atacantes.

Las preocupaciones resultantes abarcan desde cómo garantizar la protección contra las explotaciones de vulnerabilidades de día cero a la detección de los intentos de evasión, pasando por la reducción del riesgo de relleno de credenciales que lleva a la usurpación de cuentas, así como la detección de la pérdida de datos, e incluso la exploración en busca de cargas de malware a las aplicaciones.

Estas cuestiones van emparejadas con la necesidad de garantizar la protección de las aplicaciones como parte de una postura de seguridad más amplia y unificada, que también proteja las API, detenga los bots y reduzca los riesgos del lado del cliente. Y es importante lograr este objetivo sin cargar a los equipos con problemas de administración innecesarios.



WAF de Cloudflare

El firewall de aplicaciones web (WAF) de Cloudflare es el pilar de nuestra cartera de soluciones de seguridad avanzada para aplicaciones, que ofrece servicios que garantizan la seguridad y la productividad de las aplicaciones. Solo el WAF de Cloudflare proporciona una visibilidad integral de la seguridad y protección por capas contra los ataques de OWASP y las nuevas explotaciones de vulnerabilidades, detecta las evasiones y los nuevos ataques gracias al aprendizaje automático, bloquea la usurpación de cuentas, detecta la pérdida de datos y mucho más, protegiendo las aplicaciones dondequiera que se alojen. Nuestras eficaces funciones de seguridad para aplicaciones (como nuestros servicios de seguridad de las API y de gestión de bots) están completamente integradas en nuestro WAF. Llamamos al mismo potente motor de reglas que ofrecemos 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 instantánea del panorama de las amenazas ofrece una rentabilidad tangible, ya que los equipos pueden comprender su tráfico de ataque y las protecciones que deben implementar inmediatamente tras cada incorporación.



Protección rápida contra los ataques emergentes

Con decenas de miles de vulnerabilidades por año, nuestro WAF añade rápidamente nuevas reglas administradas para bloquear la explotación de las nuevas vulnerabilidades descubiertas (de día cero). Complementadas con WAF Attack Score (nuestras puntuaciones de ataques del WAF basadas en el aprendizaje automático), nuestras reglas administradas bloquean la explotación de vulnerabilidades para detectar las evasiones.



Un sistema de información sobre amenazas basado en una vasta red global

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

Desafíos de la seguridad de las aplicaciones

Cloudflare protege de forma más eficaz.

Ofrecemos una seguridad de WAF más eficaz con protecciones por capas:

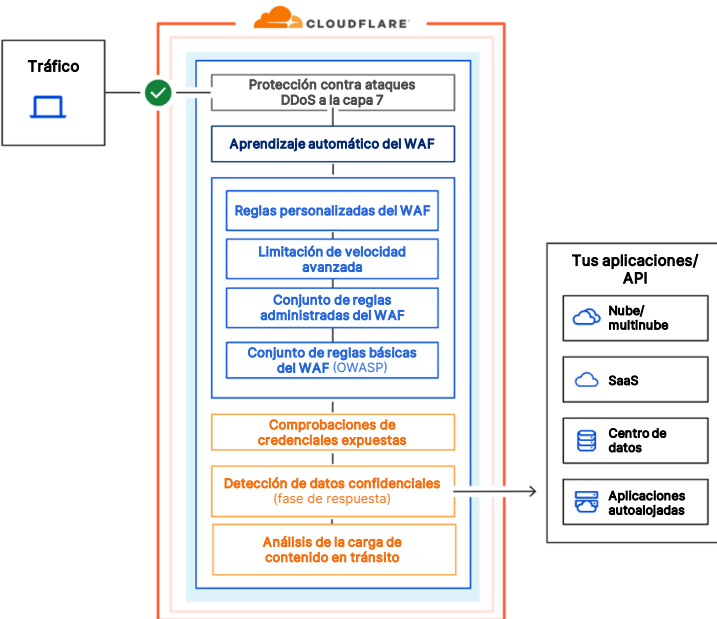
- Análisis de seguridad
- Varios conjuntos de reglas administradas
- Reglas personalizadas
- Detecciones basadas en el aprendizaje automático
- Detección de datos confidenciales
- Comprobaciones de credenciales robadas
- Limitación de velocidad avanzada
- Análisis de la carga para la protección contra el malware

Cloudflare responde más rápido.

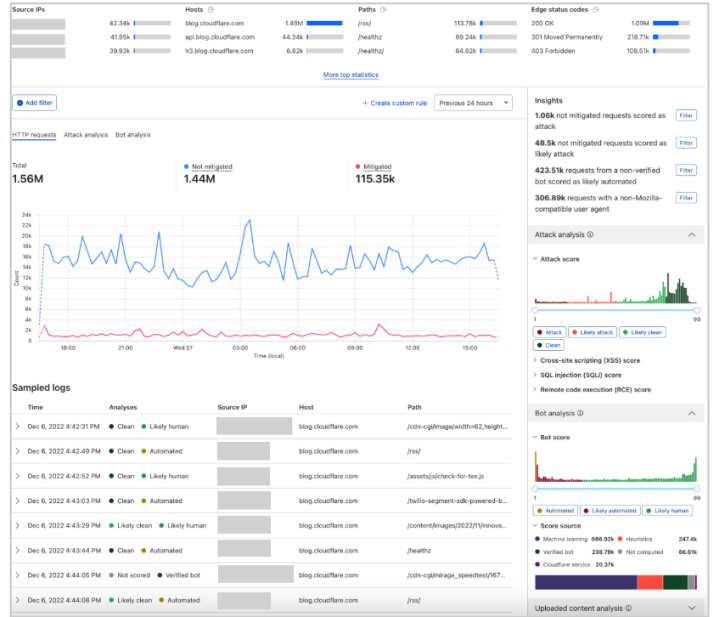
Te protegemos contra las vulnerabilidades a una velocidad inigualable. Para las principales vulnerabilidades, como HTTP/2 Rapid Reset, Log4j y muchas otras, implementamos varias reglas administradas un día laborable antes que otros proveedores de WAF.

Cloudflare integra completamente la seguridad de las aplicaciones.

Nuestro WAF está totalmente integrado con el resto de nuestra cartera de soluciones de seguridad para aplicaciones (que incluye API Gateway y nuestro servicio de gestión de bots), todo ello entregado en un paso único desde la conectividad cloud de Cloudflare.



Análisis de seguridad del WAF



Un 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 te permiten integrar fácilmente la plataforma SIEM que elijas o respaldar tus centros de operaciones de seguridad (SOC) gracias a la información que ofrece Cloudflare.

DevSecOps más fácil

Gracias a nuestra integración con Terraform, que no requiere configuración, la incorporación de la seguridad de las aplicaciones en los enfoques de DevOps es algo automático.

Con el respaldo de Cloudforce One

La seguridad para aplicaciones de Cloudflare recibe información sobre amenazas de Cloudforce One, nuestro equipo dedicado a las operaciones de respuesta a amenazas, y bloquea las amenazas mediante nuevas detecciones basadas en la nueva información sobre amenazas y sobre las tácticas, las técnicas y los procedimientos.

Seguridad de aplicaciones web

Protección por capas gracias a varios conjuntos de reglas del WAF	Evita las cargas malintencionadas en cualquier componente de solicitud con varios conjuntos de reglas: 1. Reglas administradas por Cloudflare 2. Conjunto de reglas básico de OWASP 3. Reglas personalizadas para detener cualquier ataque. Nuevas reglas administradas probadas 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 basadas en el aprendizaje automático	Evita los intentos de omisión con modelos de aprendizaje automático para complementar los conjuntos de reglas en capas. Hay disponibles 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 las principales plataformas CMS y de comercio electrónico	Benefíciate de protección lista para usar y sin coste adicional para plataformas como WordPress, Joomla, Plone, Drupal, Magento e IIS, entre otras.
Configuración de reglas personalizadas	Cuando implementes tus reglas o conjuntos de reglas, crea un modelo de seguridad positivo o negativo utilizando las siguientes acciones: BLOQUEAR, DESAFÍO GESTIONADO, DESAFÍO JS, OMITIR, REGISTRAR, CAPTCHA HEREDADO, RESPUESTAS PERSONALIZADAS.
Limitación de velocidad avanzada	Evita el abuso, los ataques DDoS y los intentos por fuerza bruta dirigidos a las aplicaciones y las API limitando la velocidad de las direcciones IP individuales o en función de un atributo de encabezado (p. ej., clave, cookie, token), de un ASN o de un país.
Detección de datos confidenciales	Detecta las respuestas que contengan datos confidenciales, como información de identificación personal, información financiera, números de tarjetas de crédito o secretos como claves API.
Comprobaciones de credenciales expuestas	Detecta los ataques de relleno de credenciales con credenciales robadas antes de que se produzca la usurpación de cuentas de los usuarios finales.
Análisis de la 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 creando reglas personalizadas.
SSL/TLS	Descarga y configura completamente el tráfico SSL para tu aplicación.
Menos falsos positivos	Nuevas reglas probadas en grandes cantidades de tráfico para garantizar el menor número de falsos positivos.
Compatibilidad con gRPC y WebSocket	Proxy y tráfico seguro para los puntos finales de gRPC y WebSocket.
Páginas de bloqueo personalizables	Personaliza las páginas de bloqueo con los detalles adecuados para los visitantes.
Completa integración con el conjunto de productos de Cloudflare	Mejora el rendimiento de las aplicaciones, enruta el tráfico por ubicación geográfica y aprovecha el proceso 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	Consigue visibilidad para ajustar el WAF; realiza un análisis exhaustivo que incluya todas las solicitudes del WAF.
Registro de cargas	Registra y encripta las cargas malintencionadas para el análisis de incidentes.
Integraciones con plataformas SIEM	Transfiere o exporta registros directamente en tus plataformas SIEM existentes.
Integración con Terraform	Incorpora la seguridad de las aplicaciones en los flujos de trabajo de CI/CD.
Gestión	
Gestión desde una sola consola	Gestión optimizada con una única consola para implementar y gestionar la seguridad y el rendimiento de las aplicaciones en todo el mundo.
Gestión a nivel de cuenta	Ahorra tiempo en la gestión del WAF gracias a una configuración única 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 sanciones económicas si se incumplen los acuerdos de nivel de servicio.
No requiere hardware, software ni configuración	La implementación solo requiere un simple cambio de DNS.
Certificación de PCI (Industria de tarjetas de pago)	Cloudflare tiene la certificación de proveedor de servicios de primer nivel.
Servicio con la autorización de FedRAMP	Nuestro paquete Cloudflare for Government, que incluye seguridad para aplicaciones, tiene la autorización de FedRAMP.



¿Quieres saber más? Regístrate en nuestra [serie de demostraciones sobre la seguridad de las aplicaciones.](#)