

Cloudflare API Shield

Gestiona y protege las API que impulsan el negocio

Desafíos de las API modernas

En la mira de los atacantes

Las API mueven el mundo. El 58 % del tráfico HTTP dinámico en la red de Cloudflare está relacionado con las API.

Las API presentan interesantes oportunidades de negocio que permiten ofrecer productos más rápido y mejorar la experiencia del cliente. En la actualidad, los líderes de informática y seguridad tienen que equilibrar la seguridad de sus API, además de la de sus aplicaciones web, sin desacelerar la innovación.

Los equipos de seguridad y de informática necesitan proteger los datos confidenciales de sus clientes y, al mismo tiempo, activar las operaciones empresariales en las aplicaciones web y las propiedades de las API.

Al fin y al cabo, la confianza de los clientes está en juego.



Cloudflare API Shield

Los clientes pueden identificar, proteger y simplificar la seguridad y la gestión de sus API públicas mediante la consolidación de la protección de sus aplicaciones web y API en el perímetro de Cloudflare.

API Shield forma parte del conjunto de soluciones de seguridad de las aplicaciones de Cloudflare, que también detiene a los bots, impide los ataques DDoS, bloquea los ataques a las aplicaciones y supervisa los ataques a la cadena de suministro.



Riesgos de las API paralelas

Los equipos de desarrollo suelen publicar nuevas API sin dar conocimiento al equipo de informática, por lo que estas API se ejecutan en paralelo, sin gestión ni seguridad.



Preocupaciones relacionadas con la autenticación, la pérdida de datos y el uso abusivo

Una vez que se identifican las API, se deben proteger contra ataques y abuso de API con autenticación, validación de esquemas, protecciones contra el abuso de las APIs y detecciones de exfiltración de datos.



Supervisión del rendimiento de las API

Dado que las API impulsan el negocio, una vez que se supervisan y protegen las API, las empresas deben vigilar su rendimiento: comprender los volúmenes de solicitudes por punto final, las tasas de error y la latencia.

Cloudflare API Shield

Gestiona y protege las API que impulsan el negocio

Capacidades clave	
Detección y gestión de las API	
Identificación y aprendizaje de esquemas	Identifica los puntos finales de las API en uso activo y sus esquemas asociados a través de modelos basados en el aprendizaje automático y la heurística.
Análisis de secuencia y rendimiento	Identifica las secuencias más importantes del comportamiento de las llamadas API y analiza el rendimiento de los puntos finales de las API (p. ej. latencia, tasa de error, tamaño de respuesta, etc.).
Gestión y portal para desarrolladores	Gestiona la documentación interactiva de las API y alójala en tu dominio con Cloudflare Pages.
Postura de seguridad de las API	
Detección de ataques BOLA	
Postura de autenticación	Ejecuta análisis de riesgos que identifican y alertan sobre configuraciones erróneas de autenticación en las API, como la ausencia de autenticación o la autenticación mixta (donde solo algunas llamadas API a un punto final requieren derechos de acceso).
Detección de datos confidenciales	Detecta datos confidenciales en las respuestas de la API procedentes de tu origen y recibe alertas por punto final.
Protección en tiempo de ejecución de las API	
Validación de autenticación	Autentica y valida el tráfico de la API con certificados mTLS, tokens web JSON (JWT), claves API y tokens OAuth 2.0 para bloquear las solicitudes de clientes ilegítimos.
Validación de esquemas	Utiliza esquemas de API para aceptar solicitudes de API válidas y bloquear solicitudes con formato incorrecto y anomalías HTTP. Esto complementa el modelo de seguridad negativa de Cloudflare WAF para una seguridad integral.
Protección contra el ataque de REST y GraphQL	Evita el ataque volumétrico y secuencial con sugerencias de la limitación de velocidad basadas en sesiones por punto finales. Amplía las protecciones contra la denegación de servicio (DoS) a los puntos finales de GraphQL.

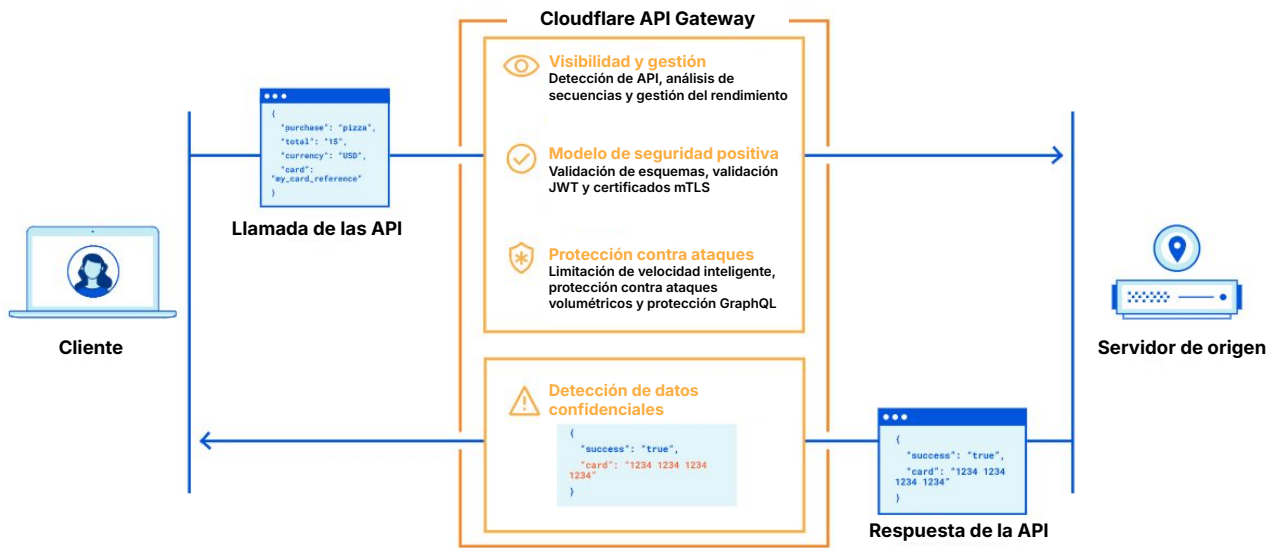


Figura 1: arquitectura de Cloudflare API Shield

Liderazgo de Cloudflare

El conjunto de soluciones de seguridad de las aplicaciones de Cloudflare ha recibido numerosos elogios por su solidez y amplitud. Cloudflare fue reconocida como empresa líder en el último informe de Forrester Wave: Web Application Firewalls. Gartner reconoció a Cloudflare como líder en soluciones de mitigación de DDoS según los clientes en el informe de 2023 de Gartner® Peer Insights™ “Voice of the Customer”: DDoS Mitigation Solutions. Forrester reconoció a Cloudflare como un competidor de rendimiento sólido en el informe The Forrester Wave™: Bot Management Software, Q3 2024. IDC nombró a Cloudflare un competidor fundamental en el informe 2024 IDC MarketScape for Web Application and API Protection (WAAP) Enterprise Platforms.