CLOUDFLARE

El estado de la seguridad y la gestión de las API

Las interfaces de programación de aplicaciones (API) permiten crear nuevas experiencias para aplicaciones, desde el seguimiento de los datos de estado hasta la personalización de videojuegos en línea. También ofrecen innumerables ventajas empresariales, tales como análisis de clientes, integraciones de SaaS, funciones de IA generativa y mucho más.

Al mismo tiempo, la gestión de las API es compleja y siempre son objeto de ataque. Echa un vistazo a las tendencias en materia de seguridad y gestión del tráfico de las API, que ahora comprende **más de la mitad (57 %) de todo el tráfico dinámico de Internet***.

30,7 %

Los modelos de aprendizaje automático detectaron más puntos finales de la API REST de los que se detectaron a través de identificadores de sesión facilitados por los clientes, en concreto casi un 31 % más.

Un mundo centrado en las API

En conjunto, el tráfico total de las API en todo el mundo creció de forma progresiva a lo largo de 2023.

Los 10 principales sectores con mayor proporción de tráfico de API respecto a su tráfico web total:

1. Plataformas comunitarias de IoT
2. Tren, autobús y taxi
3. Servicios legales
4. Multimedia, videojuegos y software gráfico
5. Logística, cadena de suministro y transporte
6. Electrónica de consumo
7. Software financiero
8. Seguridad e investigación
9. Banca, servicios financieros y seguros
10. Dispositivos médicos

API no protegidas

Las organizaciones que carecen de un inventario completo de sus API corren el riesgo de tener "API paralelas", que son esencialmente superficies de ataque ocultas:

59,2 %

Otorgar acceso de "escritura" a la API al usuario equivocado puede amenazar la seguridad. Muchas organizaciones (59,2 %) permiten el acceso a operaciones de "escritura" (la capacidad de enviar actualizaciones) al menos a la mitad de sus API.

+15 000

Los modelos de aprendizaje automático identificaron puntos finales de la API de más de 15 000 cuentas que utilizan Cloudflare.

Vulnerabilidades comunes de las API

La demanda de soluciones de seguridad y gestión de las API se ha disparado en paralelo al crecimiento del tráfico, los errores y los ataques a las API.

Principal amenaza contra las API

Las anomalías HTTP, la amenaza más frecuente contra las API, son señales comunes de solicitudes API maliciosas.

Principal error del tráfico de las API

Más de la mitad (51,6 %) de los errores de tráfico procedentes de los servidores API incluía **códigos de error http 429: "demasiadas solicitudes"**.

Principal método de mitigación

Un tercio de las medidas de mitigación de API incluyó el bloqueo de ataques de denegación de servicio distribuido (DDoS).

El desafío de proteger las API vs. las aplicaciones web

vs.

Una aplicación web

- Es **visible** para el usuario final.
- Es **accesible** a través de un navegador web.
- **Visualiza datos** desde el backend (utilizando HTML, CSS y JavaScript) con diversas interacciones del usuario.
- Se suele proteger mediante un modelo de **"seguridad negativo"** que bloquea el tráfico malicioso conocido.

Una API

- Es **invisible** para el usuario de una aplicación.
- Permite que **sistemas y aplicaciones** intercambien datos.
- **Transporta datos** mediante el acceso a servidores y aplicaciones utilizando un formato definido (lo más habitual es RESTful JSON, gRPC, XML, GraphQL).
- Su protección es más eficaz mediante un modelo de **"seguridad positivo"** que solo permite el tráfico validado y autenticado.

3 formas clave de proteger las API

Avanza hacia un modelo de "seguridad positivo" vs. un modelo de "seguridad negativo"

En un modelo de seguridad positivo, solo aceptas el tráfico de la API validado como "bueno conocido" (según lo establecido por los esquemas de API). Este enfoque es más eficaz que un modelo de seguridad negativo, que solo se centra en restringir el tráfico de la API validado como "malo conocido".

Aplica el aprendizaje automático para liberar recursos y reducir costes

El aprendizaje automático puede detectar todo el tráfico de las API (incluidas las variaciones de los ataques), diferenciar entre los picos de tráfico legítimo frente al tráfico de bots maliciosos, y gestionar otras tareas de gestión de las API que requieren un gran cantidad de recursos.

Unifica el desarrollo, la visibilidad, el rendimiento y la seguridad de las aplicaciones

Una conectividad cloud, que permite una conectividad universal entre redes, nubes, aplicaciones y usuarios, proporciona un tejido conectivo esencial entre el desarrollo de las aplicaciones y los servicios de protección integral de las API.

CLOUDFLARE

¿Quieres saber más?

Accede al informe completo de Cloudflare sobre seguridad y gestión de las API 2024

Leer informe

*Las conclusiones de esta infografía se basan en los patrones de tráfico agregado observados por la red global de Cloudflare entre el 1 de octubre de 2022 y el 31 de agosto de 2023. Se incluyen los servicios del firewall de aplicaciones web, protección contra DDoS, gestión de bots y puerta de enlace API de Cloudflare.