CLOUDFLARE

A situação da segurança e do gerenciamento de APIs

As interfaces de programação de aplicativos (APIs) impulsionam novas experiências de aplicativos, desde o rastreamento de dados de saúde até a personalização de jogos on-line. Elas também alimentam inúmeras vantagens para as empresas: análise de clientes, integrações SaaS, recursos de IA generativa e muito mais.

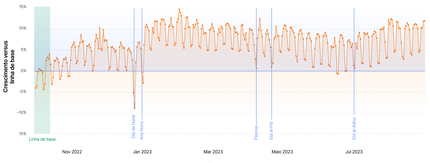
Ao mesmo tempo, as APIs são complexas de gerenciar e estão constantemente sob ataque. Dê uma olhada nas tendências de segurança e gerenciamento no tráfego de APIs, que agora representa **mais da metade (57%) de todo o tráfego dinâmico da internet*.**

30,7%

Quase 31% a mais de endpoints de API REST foram descobertos por meio de aprendizado de máquina do que por meio de identificadores de sessão fornecidos pelo cliente

Um mundo centrado em APIs

Como um todo, o tráfego total de APIs em todo o mundo cresceu de forma constante ao longo de 2023.



de Resposta

Os dez principais setores com a maior parcela de tráfego de APIs em relação ao tráfego geral da web:

1. Plataformas da comunidade IoT
2. Trem, ônibus e táxi
3. Serviços jurídicos
4. Multimídia, jogos e software gráfico
5. Logística, cadeia de suprimentos e transporte
6. Eletrônicos de consumo
7. Software financeiro
8. Segurança e investigações
9. Bancos, serviços financeiros e seguros
10. Dispositivos médicos

APIs desprotegidas

Organizações que não possuem um inventário de APIs abrangente correm o risco de ter "APIs ocultas", superfícies de ataque essencialmente ocultas:

59,2%

Fornecer acesso de "gravação" de APIs à pessoa errada pode levar a riscos de segurança. Muitas organizações (59,2%) permitem acesso de "gravação" (a capacidade de enviar atualizações) a pelo menos metade de suas APIs.

mais de 15.000

Mais de 15.000 contas que usam a Cloudflare tiveram endpoints de API descobertos apenas por meio de métodos de aprendizado de máquina

Vulnerabilidades comuns de APIs

A demanda do mercado por segurança e gerenciamento de APIs disparou paralelamente ao crescimento do tráfego, erros e ataques a APIs.

Ameaça nº 1 às APIs
Anomalias HTTP, a ameaça mais frequente às APIs, são sinais comuns de solicitações maliciosas de APIs.

Erro nº 1 de tráfego de APIs
Mais da metade (51,6%) dos erros de tráfego provenientes de origens de APIs incluíam códigos de erro "**429: "Excesso de solicitações".**

Método de mitigação nº 1
Um terço das mitigações de APIs consistiu no bloqueio de ataques de negação de serviço distribuída (DDoS)

O desafio de proteger APIs versus aplicativos web

Um aplicativo web

- É **visível** para o usuário final.
- É **acessado pelos usuários finais** por meio de um navegador web.
- **Visualiza dados** do back-end (usando HTML, CSS e JavaScript) com interações variadas do usuário.
- Normalmente é protegido por um modelo de "**segurança negativa**" que bloqueia tráfego malicioso conhecido.

Uma API

- É **invisível** para o usuário do aplicativo.
- Permite que **sistemas e aplicativos** troquem dados.
- **Transporta dados** acessando servidores e aplicativos usando um formato definido (mais comumente RESTful JSON, gRPC, XML, GraphQL).
- É protegida de forma mais eficaz por meio de um modelo de "**segurança positiva**" que permite apenas tráfego validado e autenticado.

As três principais maneiras de defender APIs

Avançar em direção a um modelo de "segurança positiva" versus "segurança negativa"

Em um modelo de segurança positiva, você aceita apenas o tráfego de APIs que é considerado "bom conhecido" (conforme definido pelos esquemas de APIs). Isso é mais eficaz do que a segurança negativa, que se concentra apenas em restringir o tráfego de APIs considerado "ruim conhecido".

Aplicar o aprendizado de máquina para liberar recursos e reduzir custos

O aprendizado de máquina pode descobrir todo o tráfego de APIs (incluindo variações de ataques), diferenciar entre picos de tráfego legítimos e tráfego de bots maliciosos e gerenciar outras tarefas de gerenciamento de APIs que consomem muitos recursos.

Unificar o desenvolvimento, a visibilidade, o desempenho e a segurança de aplicativos

Uma nuvem de conectividade, que permite conectividade any-to-any entre redes, nuvens, aplicativos e usuários, fornece tecido conjuntivo crítico entre o desenvolvimento de aplicativos e serviços detalhados de defesa de APIs.

CLOUDFLARE

Quer saber mais?

Acesse o relatório completo sobre segurança e gerenciamento de APIs de 2024 da Cloudflare

Leia o relatório

*As conclusões de dados neste infográfico são baseadas em padrões de tráfego agregados observados pela rede global da Cloudflare (incluindo o firewall de aplicativos web, proteção contra DDoS, gerenciamento de bots e serviços de gateway de API da Cloudflare) entre 1º de outubro de 2022 e 31 de agosto de 2023.