**API security risks**

APIs are a critical part of modern business, powering mobile, IoT, and web applications. Companies use them to interact with partners and to share data both publicly and internally. APIs can expose application logic or share sensitive data, which is why APIs are now a key target for attackers.

As part of its API Security Project, OWASP published its list of top security risks for APIs, the **API Security Top 10**. These API risks are real - Cloudflare now sees API endpoints globally receive more malicious requests compared to standard web applications.

**Key risk: Improper Assets Management (Shadow APIs)**

It is common for organizations not to track the APIs in production, leading to Shadow APIs with no visibility into API endpoints in use -- or the activity occurring on them.

**Key risk: Authentication and authorization**

Authentication and authorization have long been issues for applications and remain so for APIs. Authenticated users may be able to gain illicit access to sensitive data — even worse, data might not be authenticated at all.

**Key risk: Lack of resources**

This is when API backends are overwhelmed because no rate limits are in place or restrictions on the size or number of resources that can be requested. This can take API endpoints offline.

The dedicated API security of API Gateway keeps customers APIs safe from OWASP API security risks.

**Key Cloudflare API protections**

- **API Discovery**: Automatically discovers API endpoints to prevent “shadow APIs” through an always up-to-date API inventory.
- **Mutual TLS**: Provides strong authentication by issuing and validating client certificates.
- **Schema Validation**: Use of OpenAPI schemas to validate incoming traffic for a positive security model.
- **Volumetric Abuse Detection**: Cloudflare-suggested rate limits for each endpoint and path based on observed traffic to deter abuse.