API Gateway Security

A centralized way to manage APIs

APIs are everywhere today, allowing various software systems to communicate in ways that power our increasingly connected world. APIs, or application programming interfaces, provide a set of rules and tools that enable diverse software programs written in different languages to exchange information and share functionality. API gateways provide a centralized point for managing, securing, and optimizing API calls — both requests and responses.

Because they are critical to so many processes and often connect to sensitive data, APIs have become a favorite target of malicious actors. As a result, security teams must adopt protocols, practices, and measures that ensure API gateway security and protect the underlying microservices and back-end services that APIs support.

What is an API?

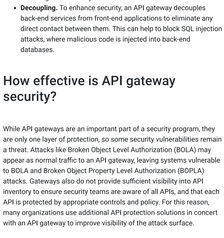
An API is a set of protocols and definitions that allow software components from different systems or written in different languages to nevertheless communicate easily and share information. By standardizing the way that applications communicate, APIs allow one application to access and incorporate data and functions provided by another application. For example, when developers want to include the latest weather information on a website, they can use an API to access data from a weather-related source rather than creating their own separate application to collect and interpret weather data. APIs are involved in almost every online action and transaction, from ecommerce and mobile payments to social media platforms and cloud services, which means they create a large attack surface.

What are threats to APIs?

Hackers now target APIs because they often provide access to sensitive data or may allow attackers unauthorized access to larger systems. With the rapid proliferation of APIs, security teams often are unaware of all the APIs in their organization's digital ecosystem, making it more difficult to adequately protect each API with security controls and regular patches and updates. API security can be jeopardized by a variety of risks, including vulnerability exploits, authorization errors, authentication issues, and denial-of-service attacks.

What is an API gateway?

An API gateway is a layer of software that serves as a single entry point for managing API calls or client requests and returning responses from API endpoints. API gateways route incoming requests to the appropriate microservice or back-end service, combining multiple requests into a single request or splitting single requests into multiple requests to fulfill a client's need most efficiently. API gateways also translate protocols between different apps and microservices and may serve as a load balancer to optimize API performance.



How an API gateway works

What is API gateway security?

An API gateway can perform a broad range of security functions to prevent API abuse and attacks, and enhance an organization's security posture.

- **Authentication**. API gateways may validate credentials such as ID tokens to authenticate the identity of all API requests.
- **Rate limiting and throttling.** API gateway security measures include the ability to limit the number of times an API can be called within a specific period of time to ensure that processing capacity is not exceeded or overwhelmed. This helps prevent denial-of-service attacks, as well as brute-force attacks and trial-and-error attacks, where hackers attempt to access systems by repeatedly trying various credentials.
- **Policy enforcement.** API gateways can enforce policies and rules — especially around authentication, authorization, and access control — to be followed when accessing microservices and back-end services.
- **Signature-based protection.** APIs can block certain threats by recognizing the signatures and patterns of known attacks.
- **Logging and monitoring.** API gateways enable continuous monitoring of API traffic and metrics around API usage. Gateways may also maintain a log of all transactions that provides insight into usage and security issues.
- **Decoupling.** To enhance security, an API gateway decouples back-end services from front-end applications to eliminate any direct contact between them. This can help to block SQL injection attacks, where malicious code is injected into back-end databases.

How effective is API gateway security?

While API gateways are an important part of a security program, they are only one layer of protection, so some security vulnerabilities remain a threat. Attacks like Broken Object Level Authorization (BOLA) may appear as normal traffic to an API gateway, leaving systems vulnerable to BOLA and Broken Object Property Level Authorization (BOPLA) attacks. Gateways also do not provide sufficient visibility into API inventory to ensure security teams are aware of all APIs, and that each API is protected by appropriate controls and policy. For this reason, many organizations use additional API protection solutions in concert with an API gateway to improve visibility of the attack surface.

What are API gateway security best practices?

Organizations and their security teams can improve API gateway security by adhering to these best practices.

- **Centralize authentication.** By centralizing API authentication at the gateway, organizations can minimize the risk of each microservice attempting independently to manage access, token verification, and other elements of the authentication process, which can lead to complexity and security gaps.
- **Implement rate limiting.** Controlling the number of API requests can prevent excessive requests — both malicious or legitimate — from overwhelming services and from succumbing to DoS or DDoS attacks.
- **Monitor continuously.** Continuous monitoring and analytics can help to detect potential threats and solve client access and request issues.
- **Remove unused and deprecated APIs.** Security teams can enhance API gateway security by keeping track of all APIs and removing APIs that are no longer used or that no longer support the latest security measures.
- **Enable a web application firewall (WAF).** Deploying a WAF in networking and API security programs can block common threats like injection attacks and cross-site scripting by limiting access to APIs based on defined rules and conditions.
- **Leverage behavioral analytics.** A SaaS-based behavioral analytics solution can record all API activity to determine a baseline for normal behavior. Then it can alert potential threats and recommend defensive or proactive responses.

Frequently Asked Questions (FAQ)

- What is OpenAPI security?
- What is BOLA?
- What is BOPLA?

Why customers choose Akamai

Akamai is the cybersecurity and cloud computing company that powers and protects business online. Our market-leading security solutions, superior threat intelligence, and global operations team provide defense in depth to safeguard enterprise data and applications everywhere. Akamai's full-stack cloud computing solutions deliver performance and affordability on the world's most distributed platform. Global enterprises trust Akamai to provide the industry-leading reliability, scale, and expertise they need to grow their business with confidence.

Take me there

Related Products

API Security

Gain full visibility into your entire API estate with continuous detection and monitoring.

Learn more

App & API Protector

One-stop, zero-compromise security for websites, applications, and APIs.

Learn more

Additional Resources

State of Apps and API Security 2025: How AI Is Shifting the Digital Terrain

AI is introducing new vulnerabilities to businesses and new tools for attackers as threats grow, new Akamai research finds.

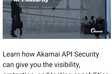
Download report

API Security Fundamentals

As API security becomes more important, you need to be sure you know the fundamentals.

Learn more

How Akamai Can Protect Your APIs and Data



Learn how Akamai API Security can give you the visibility, protection, and testing capabilities for preventing API abuse and attacks.

Watch the video

Related Pages

Learn more about related topics and technologies on the pages listed below.

- Read the latest API security blog posts
- What Is API Performance?
- What Is API Abuse?
- How Do APIs Work?
- What Is Credit Card Security?
- What Is Tokenization?
- What Is API Sprawl?
- What Is API Protection?
- What are API Security Breaches?
- What Is An API Security Provider?
- What Is API Gateway Security?
- What Is An API Security Audit?
- What Is API Discovery?
- What Are API Security Risks?
- What Is API Security for Mobile Applications?
- How to Assess Your API Security
- What Is API Threat Hunting?
- What Is API Security?
- What Is OpenAPI Security?
- What Are API Security Threats?
- What Are API Attacks?
- What Is BOLA?
- What Is BOPLA?
- What Are API Vulnerabilities?
- What Are API Security Endpoints?
- What Is the API Lifecycle?
- What Is an API Gateway?