Akamai

WHITE PAPER

API Security Fundamentals

Table of Contents

Introduction

API security fundamentals

API security is one of the fastest-growing priorities for security executives. But it's also arguably one of the least understood. The evolution of application programming interfaces (APIs) from implementation detail to strategic enabler of innovation has been a rapid one. As a result, many security teams are scrambling to increase the sophistication of their API security strategies and practices.

APIs are enabling business operations, but they also carry the crown jewels of an organization's data. Even perfect APIs can be abused by hackers, so it's essential to know the fundamentals of API security to protect your business from evolving threats. As more customer interactions and business processes use APIs, enterprise security teams are reworking their security strategies to put API risks at the forefront.

Whether you're looking to touch up on your basics or unsure of what questions to ask, read our guide for everything you need to know about API security threats, trends, and best practices. You'll get an in-depth look at:

- The different types of APIs
- What API security means for businesses today
- Best practices for mitigating API security risks
- Common API attacks and abuse methods

API Basics

What is a web API?

A web API is a programmatic interface consisting of one or more endpoints to a defined request–response message system, typically expressed in JSON or XML, which are publicly exposed via the web — most commonly by means of an HTTP-based web server.

In other words, a web API is what most people think of when they hear "API." It's a collection of endpoints. Endpoints consist of resource paths, the operations that can be performed on these resources, and the definition of the resource data (in JSON, XML, protobuf, or another format).

The term is useful to differentiate web APIs from other APIs, such as those exposed by the operating system or by libraries to applications running on the same machine. But we all understand "APIs" to mean HTTP-based (web) APIs when we talk about the enterprise digital transformation and API security.

What are the most common types of APIs and API terms?

It is helpful for security teams to be familiar with the following terms that refer to different usage models and technology approaches for API implementations. Web APIs are defined as being based on HTTP, and the four main types of web APIs seen today are RESTful, SOAP, GraphQL, and gRPC. The following table defines these four common types, among others.