Akamai

WHITE PAPER

8 Do's and Don'ts of API Security

Critical factors for a robust API security posture

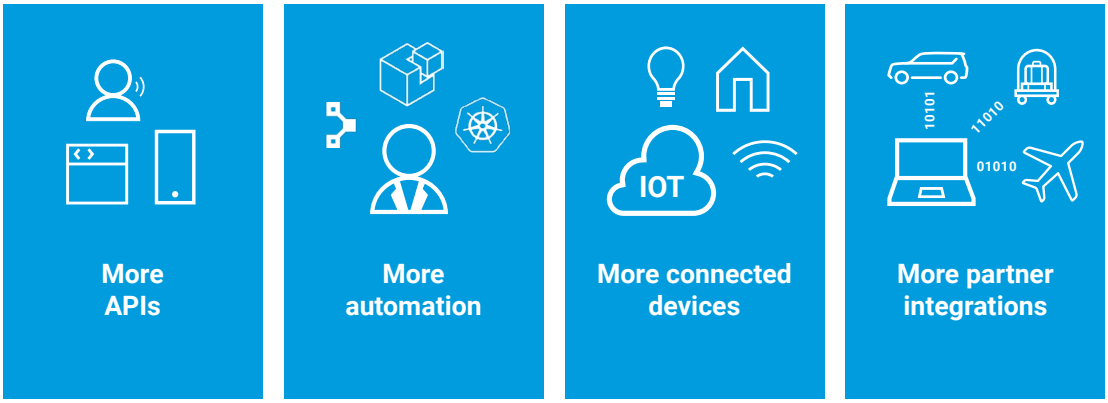
What's so complicated about protecting APIs?

API security is topping the priority list for many IT executives — and with good reason. Consider the following:

"The explosion of APIs provides an attractive attack surface, and API security continues to flummox security leaders."

— The Eight Components Of API Security, Forrester Research, Inc., September 28, 2023

Factors in API risk growth



In response to these risks, organizations must understand the following before they begin to implement effective API security:

APIs are a moving target	
Internal API awareness	**External API exposure**
Fast-moving DevOps processes create and decommission APIs continuously, leading to an incomplete API inventory	Immature API practices lead to unintended exposure of sensitive APIs to external parties, including many shadow APIs

APIs are vulnerable to two different types of threats	
Technical vulnerabilities	**Misuse and abuse**
Attackers can exploit software vulnerabilities and misconfigurations, including the OWASP API Security Top 10	Business logic abuse and other behaviors, like aggressive data scraping, can happen regardless of a technical vulnerability

Addressing the complex challenge of API security requires a well-considered approach that includes:

Incorporating the latest technology advances

Breaking down organizational barriers

Addressing the complete API threat landscape

The following are some essential strategies to implement — and pitfalls to avoid — as you develop a more sophisticated API security strategy for your organization.