



Introduction

For four consecutive years, Akamai has tracked the state of API security across successive waves of enterprise innovation — digitization, cloud growth, and now AI adoption — each accompanied by rapid API growth. Across these phases, proliferating APIs have expanded the attack surface faster than organizations have strengthened API testing, visibility, and resilience against threats.

This year’s findings confirm a clear pattern: API growth is outpacing API resilience, and AI adoption is amplifying the risk exposure.

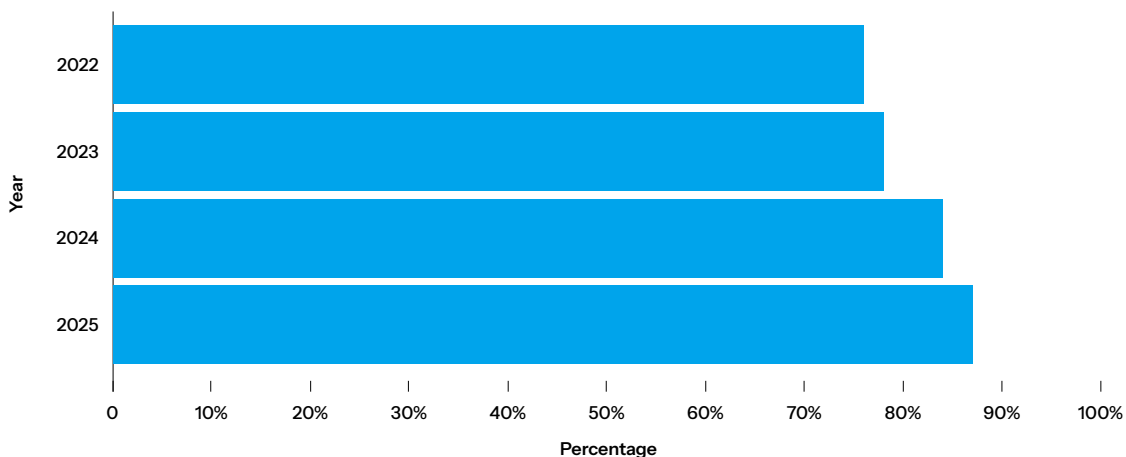
Global enterprises now manage sprawling API estates. The global median inventory per enterprise exceeds 5,900 APIs while the top quartile exceeds 29,400. As estates expand, the sightline into API risk and security coverage has not kept pace, and reported API security incidents have risen steadily over the four years of our research.

In our 2026 study, 87% of respondents reported experiencing at least one API-related security incident in the past 12 months, up from 76% in 2022.

Our 2026 study is based on a global survey reflecting insights from 1,840 security professionals across six industries and 10 countries in Asia-Pacific, the Americas, and EMEA. Respondents were evenly distributed between C-suite executives with a security focus and DevSecOps and AppSec professionals, allowing us to compare leadership and technical perspectives.

More organizations are impacted by API security incidents

The percentage of organizations experiencing API-related incidents has risen steadily for four consecutive years.



Author’s note: Each of the annual API Security Impact Study editions that we reference reflect the prior 12 months of data (for example, our 2026 report covers findings from 2025).