Key insights of the report

AI-powered APIs are more unsecure than their counterparts.
The majority of artificial intelligence (AI)–powered APIs are externally accessible and many rely on inadequate authentication mechanisms — a vulnerability that's compounded by the growing array of AI-driven attacks that are targeting them.

AI fuels technical advancement for threat actors.
This includes advancements like AI-driven malware, vulnerability scanning, attacks on AI-integrated systems, and sophisticated web scraping capabilities.

32%

The percentage of increase in OWASP API Security Top 10–related incidents

API security incidents are rising, with Open Worldwide Application Security Project (OWASP) API Security Top 10 issues revealing authentication and authorization flaws that expose sensitive data and functionality.

30%

The growth in security alerts related to the MITRE security framework

Attackers are using advanced techniques, including automation and AI, to exploit APIs. The MITRE framework can help defenders more quickly and accurately identify these attacks.

33%

The percentage of increase in global web attacks year over year

The surge in attacks directly correlates with the rapid adoption of cloud services, microservices, and AI applications, which expand attack surfaces and introduce new security challenges.

230 billion+

The number of web attacks that hit commerce organizations,

making it the most impacted industry with nearly triple the number of attacks experienced by high technology (the second most attacked industry).