State of Apps and API Security 2025

How AI Is Shifting the Digital Terrain

As organizations continue to invest in AI-powered applications, thereby introducing new vulnerabilities, threat actors are simultaneously using AI to automate the entire kill chain. The result has been a rise in both the volume and sophistication of attacks on web apps and APIs.

6 ways AI is helping attackers

- AI-enhanced malware
- AI-powered vulnerability scanning
- Attacks on LLM-based applications (prompt injection, data poisoning, jailbreaking techniques)
- Sophisticated web scraping
- Automated distributed denial-of-service (DDoS) attacks
- Low and slow attacks

Web attacks

33%

Increase in global web attacks year over year

⚠ Impact

AI is feeding the attack surge

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.

Web attack industry trends

230 billion+

web attacks

Commerce was the industry most impacted by web attacks, seeing nearly triple the number of attacks as the second highest industry (high tech).

API attacks

32%

Increase in OWASP API Security Top 10–related incidents*

⚠ Impact

AI-powered APIs are less secure

The majority of AI-powered APIs are externally accessible and many rely on inadequate authentication mechanisms, a vulnerability compounded by the growing array of AI-driven attacks targeting them.

30%

Growth in security alerts related to the MITRE security framework*

⚠ Impact

The MITRE framework remains crucial for providing insights into attacker techniques targeting APIs

As attackers use automation and AI to exploit APIs, the MITRE framework can help defenders more quickly and accurately identify these attacks.

Layer 7 DDoS attacks

94%

Growth in monthly Layer 7 DDoS attack volumes Top 10–related incidents

⚠ Impact

Attacks growing in both sophistication and strength

Layer 7 DDoS attacks surged as attackers refined their techniques to exploit specific vulnerabilities in web application logic or APIs. Meanwhile, increasingly sophisticated bot-driven attacks' traffic patterns closely emulated legitimate API use.

Layer 7 DDoS attack industry trends

7 trillion

The number of Layer 7 DDoS attacks targeting the high technology industry from January 2023 through December 2024, making it the most-affected industry.

Mitigation strategies

- Employ shift-left and DevSecOps API security plans
- Use adaptive security engines
- Apply API testing tools
- Implement OWASP security guidelines
- Develop specialized DDoS protections
- Monitor security frameworks
- Employ layered ransomware defenses
- Use AI-powered firewalls and bot defense solutions

*Over a 30-day period

Get the full report for exclusive insights into attack trends.

Download report