Key insights of the report

APIs have become the dominant attack surface for modern enterprises, with the average number of daily API attacks up by 113% year over year.

- Approximately 61% of API attacks in 2025 involved unauthorized workflows and abnormal activity, up from 30% in 2024. This shift shows that attackers are moving away from traditional web attacks toward behavior-based threats.
- An average of 3,000 APIs per customer contained sensitive data, and 12% showed security weaknesses; 24% of those issues pertained to sensitive data exposure. The growth of agentic AI amplified this trend, reinforcing that securing AI means securing APIs.

Web attacks (including attacks that target API endpoints and web applications) increased by 73% between 2023 and 2025, underscoring the continued importance of strong cyber hygiene and security fundamentals in today's evolving threat landscape.

Layer 7 DDoS attacks surged by 104% over the last 2 years (2023–2025).

Super botnets like Aisuru and Kimwolf (TurboMirai variants) enable accessible DDoS as a service, making sophisticated attacks available to anyone.

AI is a force multiplier.

- AI reinforces existing weaknesses rather than creating new categories. Organizations that chase narrow AI-specific fixes miss the fundamentals. AI-assisted code generation (vibe coding) is introducing new vulnerabilities and misconfigurations that often reach production untested.
- Agentic AI vulnerabilities are expanding the modern attack surface. A new Open Worldwide Application Security Project (OWASP) framework identifies 10 threats specific to AI agents that make autonomous decisions (goal hijacking, tool misuse, memory poisoning, etc.).