Salt Security Report Shows API Security Blind Spots Could Put AI Agent Deployments at Risk

Insecure APIs Threaten the Resilience and Security of AI Projects

Salt Security Logo

LONDON, UNITED KINGDOM, October 8, 2025 /EINPresswire.com/ -- Salt Security has today released its semi-annual State of API Security Report that exposes an alarming disconnect between rapid API adoption and immature security practices, which threatens the success of critical AI and automation initiatives. The H2 2025 State of API Security Report shows that, as enterprises race to capitalise on the emerging AI Agent Economy, API security has emerged as a systemic vulnerability in the digital backbone that powers it.
The findings from a study of responses from 386 professionals tasked with managing APIs in their organisations reveal:

- 80% of organisations lack continuous, real-time API monitoring, leaving them blind to active threats targeting AI agents.
- 1 in 3 companies (33%) experienced an API security incident in the past year, while 50% had to delay a new application rollout due to API security concerns.
- Only 19% are “very confident” in the accuracy of their API inventory, while more than half (54%) rely on error-prone developer documentation to identify sensitive data exposure.

“APIs are now central to digital transformation and AI, yet security controls remain inconsistent, reactive, and dangerously behind the curve,” said Eric Schwake, Director of Cyber Security Strategy at Salt Security. “AI without API security is like driving a car blindfolded - if you can’t govern APIs, you can’t govern AI. Without immediate action, the unmonitored API attack surface will continue to expand, putting both innovation and resilience at risk.”

AI Adoption Fuels Complexity

Generative AI is adding new layers of complexity to API security. While 62% of organisations have already adopted GenAI in API development, more than half (56%) view it as a growing security concern, particularly due to vulnerabilities in AI-generated code. At the same time, 59% are

leveraging GenAI within their security operations, creating a dynamic that introduces both defensive opportunities and offensive risks.

API Growth Accelerating

The study highlights explosive growth in API adoption, with 41% of organisations reporting increases of 51–100% over the past year and a further 13% experiencing growth of 101–200%. Remarkably, 6% saw their API volumes more than triple, surging by over 301% in just 12 months. This rapid expansion is mirrored in portfolio size, as 42% of organisations now manage between 101 and 500 APIs, while 14% oversee more than 1,000, further demonstrating the accelerating scale and complexity of today's API ecosystems.

Barriers to Effective Security

Despite rising investment in API security, significant challenges remain. Nearly 80% of organisations increased their budgets over the past year, yet most of these boosts were modest at under 15%. Budget limitations were cited as the top barrier by 25% of respondents, followed by resource shortages (16%). Beyond funding, structural concerns persist, with 15% citing inadequate runtime security, 14% highlighting poor manageability, and 12% noting underinvestment in pre-production security, signs that many programs are still struggling to mature.

Shifting Security Strategies

The report urges organisations to pivot from fragmented, reactive defences to a holistic strategy built on continuous API discovery, stronger governance, runtime protection, and GenAI-specific safeguards.
"AI adoption is rampant, but security is not keeping up. Existing tools miss the API execution layer, which means attackers can hijack entire AI agents via APIs," added Eric Schwake.
"Enterprises that master API security will be able to unlock AI-driven innovation safely at scale. Those that don't are at risk of falling behind."

About the Report

The H2 2025 State of API Security Report is based on a survey of 386 security professionals responsible for API security across industries. It examines the risks, practices, and challenges that shape API security in the era of AI-driven digital transformation. The full report can be downloaded here.

About Salt Security

Salt Security secures the APIs that power today's digital businesses. Salt delivers the fastest API discovery in the industry—surfacing shadow, zombie, and unknown APIs before attackers find them. The company's posture governance engine and centralised Policy Hub automate security

checks and enforce safe API development at scale. With built-in rules and customisable policies, Salt makes it easy to stay ahead of compliance and reduce API risk. Salt also uses machine learning and AI to detect threats early, giving companies a critical advantage against today's sophisticated API attacks. The world's leading organisations trust Salt to find API gaps fast, shut down risks, and keep their businesses moving. Learn more at https://salt.security

Charley Nash
Eskenzi PR
email us here