Salt Security Research: As AI Agents Outpace Security, Most Organizations Face an Unsecured API Surge

PALO ALTO, CA, UNITED STATES, April 8, 2026 /EINPresswire.com/ -- The latest State of AI and API Security Report Finds Almost Half of Organizations Have Delayed AI Deployments Due to API Security Concerns; and Nearly All Attacks Now Originate from Authenticated Sources

Salt Security, the leading API and agentic security company, today released its 1H 2026 State of AI and API Security: Navigating the Agentic Era report, revealing a widening gap between the rapid deployment of AI agents and the security programs designed to protect them. The research finds that while autonomous AI agents are being deployed at enterprise scale, 92% of organizations lack the advanced security maturity required to defend these environments.

In order to work properly and carry out autonomous actions, AI is reliant on APIs, which are becoming the execution layer for AI systems, powering every action taken by agents, large language models (LLMs), and Model Context Protocol (MCP) servers. Because of this, the number of APIs in use in organisations today have exploded, with two-thirds (66%) reporting growth of over 50% in the last year.

However, as organizations scale AI-driven automation, security is failing to keep pace, creating what Salt defines as the Agentic Security Gap. The security of modern AI environments now requires visibility and control across the entire agentic stack, not just individual APIs.

“You cannot secure AI agents without securing every layer they touch, including the APIs they call, the MCP servers they route through, and the data they access,” explained Roey Eliyahu, Co-Founder and CEO at Salt Security. “Risk in the agentic era doesn’t sit in one place. It lives in how all of those pieces interact in real time.”

AI Adoption is Accelerating and Security is Falling Behind

The research, based on a survey of 327 security leaders, shows that while AI adoption is accelerating, security maturity is lagging:

- Almost half (47%) of organizations have delayed production releases due to API security concerns
- Almost one third (32%) experienced an API security incident in the past year

- Only 8% report advanced API security maturity, leaving most organizations underprepared
- Two-thirds (66%) reported API growth of more than 50% in the past year, driven by automation and AI adoption

Additionally, 79% of boards and executive teams have increased scrutiny of AI security risks, yet only 18% are extremely confident in their ability to detect attacks leveraging Generative AI, a confidence gap that reflects the inadequacy of legacy tools in agentic environments.

A notable reason for this confidence gap, is lack of visibility, which remains a critical weakness:

- Less than one in four (24%) have a fully automated API inventory, while the majority rely on partial or manual tracking
- Nearly 90% of organizations are already using or planning to use GenAI in API development, introducing new security risks into the software lifecycle

The findings also point to a marked change in the threat landscape where attackers are no longer breaking in, they are operating inside trusted systems, often through AI-driven processes.

- Nearly all (99%) of attack attempts analyzed by Salt Labs originate from authenticated sources, increasingly rogue agents operating with legitimate credentials but no human oversight, no rate limiting, and no behavioral guardrails.
- Almost two-thirds (65%) of attacks exploit Security Misconfiguration (OWASP API8), a vulnerability dramatically amplified when over-permissioned APIs are connected to AI agents that can query, chain, and exfiltrate data at machine speed.

API Security Emerges as the Fourth Pillar of Cybersecurity

The report concludes that API security is no longer a subset of application or cloud security, but a foundational discipline in its own right. As APIs now account for the majority of web traffic and power all AI agent activity, they represent a distinct and critical attack surface that existing security pillars were not designed to protect.

To address this shift, Salt Security is advancing a new model for enterprise security called the Agentic Security Graph, which maps the relationships between:

- LLMs (reasoning layer)
- MCP servers (execution layer)
- APIs (action layer)

Together, these components form the agentic stack, providing the context needed to understand not just what AI systems generate but also what they do across enterprise environments.

“Salt Security was founded on the belief that APIs are the most critical and most overlooked attack surface in the enterprise. As AI agents have emerged, it has become clear that APIs are just one pillar in a much larger, deeply connected system,” said Roey Eliyahu, Co-Founder and CEO at Salt Security. “Today, we secure the entire agentic environment, the llm, agents, MCP servers, APIs, and the data they access. Our 1H 2026 research confirms that this isn’t a future problem, it’s happening now, and most organizations are not ready.”

The 1H 2026 State of AI and API Security: Navigating the Agentic Era is available for download
The report is based on a survey of 327 security professionals conducted in early 2026, spanning technology, financial services, healthcare, manufacturing, and other industries.
About Salt Security

Salt Security is the leading API and agentic security company, protecting the world’s most innovative enterprises from API and AI agent attacks. The Salt Security API Protection Platform secures the full agentic ecosystem—discovering all APIs, agents, and MCP connections; stopping attacks in real time; and eliminating vulnerabilities before they reach production. Salt Security was founded in 2016 and is backed by Sequoia Capital, S Capital, Tenaya Capital, Salesforce Ventures, Advent International, and other leading investors. For more information, visit www.saltsecurity.com or follow Salt Security on LinkedIn and X.

Dr. Karl Bateson
Salt Security
karlb@salt.security
