New Report Warns of Looming Security Crisis as AI Agents Proliferate

Salt Security Unveils Groundbreaking Research Urging Organisations to Prioritise API Security to Unlock the True Potential of Agentic AI

LONDON, UNITED KINGDOM, August 13, 2025 /EINPresswire.com/ -- A new Salt Security report, Securing the Future of Agentic AI: Building Consumer Trust through Robust API Security highlights a critical warning: without proper Application Programming Interface (API) discovery, governance and security, the very technology meant to drive smarter customer engagement could open the door to cyber attacks or data leakage. The research also reveals an increasing trust gap between businesses deploying agentic AI for external communications and consumers wary of sharing personal information due to security concerns.

Because APIs power AI agents, with the ability to make requests, retrieve data and interact across different platforms, the common thread towards improving confidence in agentic AI interactions is API security. The report proposes that once security is strengthened, consumer trust will follow and allow agentic AI to reach its full business potential.

The unique report delved into both sides of the agentic AI equation - those organizations already using it and consumers that are encountering it.

Key Highlights from Businesses Using Agentic AI:

- Over half (53%) of organisations using agentic AI say they are already deploying it, or plan to, for customer-facing roles
- Nearly half (48%) of organizations currently use between 6 and 20 types of AI agents and 19% deploy between 21 and 50; 37% of organisations report that 1–100 AI agents are currently active within their systems; and almost a fifth (18%) host between 501–1000 agents
- Only 32% conduct daily API risk assessments
- 37% have a dedicated API security solution
- Just 37% have a data privacy team overseeing AI initiatives
- 7% assess API risk monthly or less

Key Highlights from Consumers:

- 64% of consumers have interacted with AI chatbots more frequently in the past year

- 80% of those consumers have shared personal information during these interactions
- 44% say they've felt pressured to share information just to complete a task
- Only 22% of consumers are comfortable sharing data with AI agents, compared to 37% who trust interactions over the phone and 54% in person
- 62% believe AI agents are easier to trick than humans

AI Agent Use is Exploding, But Consumers Aren't Convinced

The report revealed that over half of organisations already using agentic AI say they deploy it or plan to for customer-facing tasks. Meanwhile, 64% of consumers report encountering AI chatbots more frequently than a year ago, and four in five who interact with them have shared personal details in the process.

Yet, trust remains a significant hurdle. Just 22% of consumers feel comfortable sharing data with chatbots, compared to 54% in person and 37% over the phone. Alarmingly, 44% say they've felt pressured into providing information to AI agents just to complete a task. The discomfort is compounded by perceptions of vulnerability, with 62% believing AI agents are more easily tricked by hackers than humans.

"Agentic AI is changing the way businesses operate, but consumers are clearly signalling a lack of confidence," said Michael Callahan, CMO at Salt Security. "What many organisations overlook is that the safety and success of AI depends on APIs that power it and they must be effectively discovered, governed and secured. Otherwise, the trust gap will widen, and the risks will escalate."

APIs form the digital foundation for AI agents, enabling them to retrieve data, trigger actions, and interact across platforms. However, each connection adds a potential attack surface. As AI agents automate more tasks and handle sensitive information, weaknesses in API authentication, input validation and access control become high-risk vulnerabilities.

The Security Shortfall: API Risk Is Underestimated

Despite the growing risk, security practices remain uneven. Only 32% of organisations conduct daily API risk assessments, while 7% report doing so monthly or less. Meanwhile, only 37% say they use dedicated API security solutions, and the same proportion have a dedicated data privacy team overseeing AI initiatives.

The report outlines key best practices, including:

- Continuous API monitoring and anomaly detection using AI tools
- Strong authentication frameworks and least-privilege access
- Encryption for data in transit and at rest
- Regular security testing and developer training

“As AI agents become more autonomous and embedded in business operations, securing the APIs that power them should be an urgent priority as this is a problem that will just keep compounding until it’s out of control,” Michael Callahan concluded. “Securing API infrastructure needs to happen now to reduce risk, improve trust, bolster innovation and increase overall cyber resilience.”

Download the full report, Securing the Future of Agentic AI, here to see the complete findings and recommended security actions.

Methodology:

Censuswide carried out a survey on behalf of Salt Security of 1000 US-based consumers and 250 organisations with 250+ employees who are already using agentic AI

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 centralized 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.

Charley Nash, Account Manager
Eskenzi PR Limited
charley@eskenzipr.com
