Palo Alto Networks Report Reveals AI Is Driving a Massive Cloud Attack Surface Expansion

December 16, 2025

99% of organizations have experienced an attack against AI apps and services in the past year; Security teams can't keep pace with the surging volume of insecure code

SANTA CLARA, Calif., Dec. 16, 2025 /PRNewswire/ -- The rapid adoption of enterprise AI is fueling an unprecedented surge in cloud security risks. To help organizations understand and combat escalating threats, Palo Alto Networks (NASDAQ: PANW), the global cybersecurity leader, today released its annual "State of Cloud Security Report 2025," exposing how AI is driving a massive expansion of the cloud attack surface.

As cloud infrastructure grows to host the influx of AI workloads, it has become a critical target, with 99% of respondents reporting at least one attack on their AI systems within the past year. Simultaneously, the rise of GenAI-assisted vibe coding, used by 99% of respondents, is generating insecure code faster than security teams can review it. Of the 52% of teams that ship code weekly, only 18% are able to fix vulnerabilities at that pace, leaving unaddressed risks compounding rapidly across cloud environments.

Elad Koren, Vice President of Product Management, Cortex
"As organizations aggressively scale cloud investments to power AI initiatives, they are inadvertently opening the door to sophisticated new attack vectors. Our research confirms that traditional approaches to cloud security are inadequate, leaving security teams to fight machine-speed threats with fragmented tools and slow, manual fix cycles. Teams need more than just dashboards highlighting risks they can never burn down; they must transform with an agentic-first platform that spans code to cloud to SOC to finally operate faster than the adversary."

Palo Alto Networks State of Cloud Report Highlights
Based on a survey of over 2,800 security executives and practitioners across 10 countries, the report reveals critical shifts driven by AI in the cloud, including:

New frontiers of cloud risk: Attackers are rapidly pivoting to exploit the foundational layers of the cloud, targeting API infrastructure, identity and lateral network movement, overwhelming already strained security teams.

- **API attacks jump 41%:** As agentic AI relies heavily on APIs to operate, this explosion in usage has greatly expanded the attack surface, turning APIs into a primary entry point for sophisticated threats.
- **Identity remains the weakest link:** Among respondents, 53% indicate lenient identity and access management (IAM) practices as a top challenge, confirming that insufficient access controls are now a leading vector for credential theft and data exfiltration.
- **Lateral movement risks persist:** 28% of respondents point to unrestricted network access between cloud workloads as a growing threat, allowing attackers to pivot freely across environments and turn minor compromises into major incidents.

The growing imperative for cloud and security operations (SOC) unification: Multivendor complexity and tool sprawl are compounding risk, making unification of cloud security and the SOC a strategic necessity.

- **Tool sprawl creates blind spots:** Managing an average of 17 cloud security tools from five vendors creates fragmented data and context gaps, slowing incident response. Consequently, 97% of respondents prioritize consolidating their cloud security footprint.
- **Siloes slow resolution:** Disjointed workflows and isolated data sources between cloud and SOC teams stall remediation, with 30% of teams taking more than a full day to resolve an incident.
- **Cloud and SOC must merge:** The consensus is clear: 89% of organizations believe cloud and application security must be fully integrated with the SOC to be effective.

End-to-end defense at machine speed: As adversaries weaponize AI to further accelerate attacks, static visibility and siloed tools are leaving cloud environments exposed. The report emphasizes that, to stay ahead, organizations need an end-to-end solution that merges proactive risk reduction with reactive incident response. Meeting this demand, Palo Alto Networks Cortex® Cloud ™ unifies industry-leading CNAPP with best-in-class CDR in an agentic-first platform that spans from code to cloud to SOC to secure cloud innovation at the speed of AI.

Read the blog and download the full "State of Cloud Security Report 2025."

About Palo Alto Networks
As the global AI and cybersecurity leader, Palo Alto Networks (NASDAQ: PANW) is dedicated to protecting our digital way of life via continuous innovation. Trusted by more than 70,000 organizations worldwide, we provide comprehensive AI-powered security solutions across network, cloud, security operations and AI, enhanced by the expertise and threat intelligence of Unit 42®. Our focus on platformization allows enterprises to streamline security at scale, ensuring protection fuels innovation. Explore more at www.paloaltonetworks.com.

View original content to download multimedia:https://www.prnewswire.com/news-releases/palo-alto-networks-report-reveals-ai-is-driving-a-massive-cloud-attack-surface-expansion-302642980.html

SOURCE Palo Alto Networks, Inc.

Caren Auchman, cauchman@paloaltonetworks.com