Unit 42 Report: AI and Attack Surface Complexity Fuel Majority of Breaches

February 17, 2026

Adversaries leverage AI to accelerate attacks, exploiting identity weakness and enterprise complexity

SANTA CLARA, Calif., Feb. 17, 2026 /PRNewswire/ -- The *Unit 42 2026 Global Incident Response Report*, released today by Palo Alto Networks (NASDAQ: PANW), reveals an era of accelerated attacks where AI, sprawling attack surfaces, and identity fuel the majority of breaches. Based on Unit 42® analysis of over 750 high-stakes incidents, adversaries are leveraging AI throughout the attack lifecycle, accelerating attack speeds by 4x over the past year. Enterprise complexity is working in the attackers' favor — identity weaknesses were exploited in 89% of investigations, while 87% of attacks involved multiple attack surfaces.

Sam Rubin, SVP of Unit 42 Consulting & Threat Intelligence, Palo Alto Networks
"Enterprise complexity has become the adversary's greatest advantage. This risk is compounded as attackers increasingly target credentials, utilizing autonomous AI agents to bridge human and machine identities for independent action. To mitigate these threats, organizations must reduce complexity and move to a unified platform approach that relentlessly eliminates implicit trust."

2026 Global Incident Response Report Highlights

- **AI bolsters attack speeds:** As threat actors increasingly leverage AI and advanced automation, the time from initial access to data exfiltration has plummeted to just 72 minutes in the fastest attacks — a 4x increase in speed over the past year.
- **Attack complexity is growing:** 87% of attacks span two or more attack surfaces, blending activity across endpoints, cloud, SaaS platforms and identity systems. Unit 42 tracked activity across as many as 10 different fronts simultaneously.
- **Identity drives initial access:** 65% of initial access is driven by identity-based techniques, like social engineering and credential misuse, while vulnerabilities account for initial access in 22% of all attacks.
- **The browser is a primary battleground:** 48% of attacks involve the browser, reflecting how routine web sessions are weaponized to harvest credentials and bypass local controls.
- **SaaS supply chain attacks increase:** Attacks involving third-party SaaS applications have surged 3.8x since 2022, accounting for 23% of all attacks as threat actors abuse OAuth tokens and API keys for lateral movement.

Bridging the Critical Gaps in Defense

Unit 42 links 90% of data breaches to misconfigurations or security gaps, with complexity, poor visibility and excessive trust acting as systemic attack enablers.

To counter the collapse of the attack lifecycle, the report recommends that defenders move beyond traditional perimeter security and adopt a unified platform approach that:

- **Moves at machine speed:** Empower SOCs with AI and automation to detect and contain high-velocity attacks in minutes rather than hours.
- **Secures the build pipeline:** Embed security directly into the software and AI development lifecycle to block vulnerabilities before they reach the cloud.
- **Modernizes identity defense:** Centralize management of human, machine and agentic identities to close governance gaps and stop credential-based exploits.
- **Protects the human interface:** Use secure browser technology and active exposure management to defend the modern workspace and unmanaged devices.
- **Eliminates implicit trust:** Adopt zero trust to continuously verify every interaction, neutralizing an attacker's ability to move laterally.

To download the full 2026 Unit 42 Global Incident Response Report and Executive Resource Kit, visit https://www.paloaltonetworks.com/resources/research/unit-42-incident-response-report.

About Unit 42

Palo Alto Networks Unit 42 brings together world-renowned threat researchers, elite incident responders and expert security consultants to create an intelligence-driven, response-ready organization that's passionate about helping you proactively manage cyber risk. Together, our team serves as your trusted advisor to help assess and test your security controls against the right threats, transform your security strategy with a threat-informed approach, and respond to incidents in record time so that you get back to business faster. Visit paloaltonetworks.com/unit42.

About Palo Alto Networks

Palo Alto Networks (NASDAQ: PANW), the global AI cybersecurity leader, protects our digital way of life with a comprehensive portfolio of cybersecurity solutions and platforms across Network, Cloud, Security Operations, AI and Identity. Trusted by over 70,000 customers and powered by Unit 42 threat intelligence, our AI-driven platforms eliminate complexity, empowering enterprises to modernize with confidence and securing the speed of innovation. Explore the future of security at www.paloaltonetworks.com.

Palo Alto Networks, Unit 42, and the Palo Alto Networks logo are registered trademarks of Palo Alto Networks, Inc. in the United States and in jurisdictions throughout the world. All other trademarks, trade names, or service marks used or mentioned herein belong to their respective owners.

View original content to download multimedia:https://www.prnewswire.com/news-releases/unit-42-report-ai-and-attack-surface-complexity-fuel-majority-of-breaches-302689259.html

SOURCE Palo Alto Networks, Inc.

MEDIA CONTACT: Press@paloaltonetworks.com