Palo Alto Networks Introduces Next-Generation Trust Security to Automate and Future-Proof Digital Resilience

March 23, 2026

Certificate lifecycle automation prevents outages and accelerates post-quantum readiness

SANTA CLARA, Calif., March 23, 2026 /PRNewswire/ -- Palo Alto Networks (NASDAQ: PANW), the global cybersecurity leader, today defined a new standard for operational resilience with the launch of Next-Generation Trust Security (NGTS). As the industry moves toward a mandatory 47-day certificate renewal cycle, NGTS transforms cryptographic trust from a manual, human error prone process to an automated network control, eliminating service outages and dramatically improving operational efficiency.

For decades, digital certificates - the "passports" of the digital economy - lasted years and changed rarely. Today, however, the enterprise has entered a period of continuous cryptographic reset: certificate lifetimes are shrinking by over 90%, encryption standards are shifting for a post-quantum world, and sudden decertification of global trust authorities can now force the immediate replacement of thousands of certificates.

Anand Oswal, Executive Vice President of AI & Network Security, Palo Alto Networks
"When digital trust breaks, the business stops. Expired or non-compliant certificates trigger outages that take business-critical applications, infrastructure, and cloud services offline. Managing updates manually takes considerable time and coordination across several teams, and with increased scale and speed requirements, a manual approach is no longer viable. With NGTS, and our quantum-safe security solution, the network becomes the ultimate control point to automate the cryptographic reset."

NGTS is the industry's first network-native platform that unifies certificate lifecycle management (CLM) with real-time network visibility and enforcement. Available today, this unified defense enables businesses to:

- **Gain Increased Visibility:** Discover where trust lives across all network services and applications, eliminating the "shadow" certificates and blind spots that lead to security gaps.
- **Facilitate Operational Resilience:** Protect the business from certificate-related outages and trust failures by automatically identifying and refreshing credentials before they disrupt customer transactions or internal services.
- **Build Cryptographic Agility:** Accelerate the transition to a post-quantum future with automated lifecycle management built to handle faster renewal cycles and evolving encryption standards without manual effort.

Emanuel Figueroa, Senior Research Analyst, Identity and Access Management Security, Worldwide, IDC
"For years, the industry relied on a checkpoint model of trust — authenticate once and assume safety. But in a post-quantum world with shrinking certificate lifecycles, that assumption no longer holds. Trust now has to adjust as quickly as the environment it protects. By moving certificate lifecycle management out of manual spreadsheets and into a network-native platform, Palo Alto Networks is turning cryptographic maintenance into a continuous automated process rather than a periodic task. This isn't only about avoiding outages; it's about creating a unified security fabric where cryptographic agility is built in, keeping the business resilient even as encryption standards evolve beneath the stack."

While legacy tools manage certificates in a vacuum, Palo Alto Networks is the only provider that embeds trust directly into the network layer. By integrating CyberArk's best-in-class machine identity intelligence into the network, NGTS closes the gap between the teams managing certificates and the teams responsible for uptime.

Learn more about how NGTS is redefining operational resilience.

Follow Palo Alto Networks on X, LinkedIn, Facebook and Instagram.

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 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 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 services marks used or mentioned herein belong to their respective owners.

View original content to download multimedia:https://www.prnewswire.com/news-releases/palo-alto-networks-introduces-next-generation-trust-security-to-automate-and-future-proof-digital-resilience-302722225.html

SOURCE Palo Alto Networks, Inc.

Press@paloaltonetworks.com.