Enterprise Strategy Group

BRIEF

AUGUST 2025

Preparing Legacy Apps for a Post-quantum World

Todd Thiemann, Principal Analyst

Abstract: Enterprises need to plan for a post-quantum world and face the daunting task of enabling post-quantum support for legacy apps. As organizations plan for quantum computing and need a solution to modernize their cryptography approach for data in motion, they can look to Palo Alto Networks for a path to the post-quantum world for apps that cannot be upgraded or support Post-Quantum Cryptography (PQC).

Key Highlights

- 51% of enterprises have started their journey toward a post-quantum world.[1]
- Organizations have legacy applications that are difficult or impossible to update for PQC.
- Palo Alto Networks PAN-OS 12.1 Orion provides a path to post-quantum readiness for legacy applications that are difficult to patch.

Cryptographic Agility and Preparing for a Post-quantum Computing World

Quantum computing's progress is expected to solve complex problems radically faster than today's classical computers. That progress should eventually yield cryptographically relevant quantum computing (CRQC), at which point quantum systems can break today's public key cryptography. In anticipation of this expected change, governments around the world are developing new national quantum readiness strategies, including requirements to migrate to new quantum resistant PQC standards.

While the timeline for a capable quantum computer remains uncertain, enterprises are moving toward achieving cryptographic agility so they can adapt their inventory of cryptographic algorithms and practices without significantly disrupting the overall business operations. Cryptographic agility addresses the "brittleness" of today's cryptographic infrastructure by enabling organizations to upgrade different cryptographic algorithms across applications, infrastructure, and hardware as standards, threats, and requirements change. There is no guarantee that today's approved PQC algorithms or tomorrow's future algorithms will provide the necessary security over time. And there are multiple PQC algorithms for different purposes. Crypto agility enables organizations to smoothly adapt without interrupting operations as the cryptography evolves.

Enterprises need to consider expected changes in evolving from classical public-key cryptographic algorithms to standardized PQC. The U.S. National Institute of Standards and Technology (NIST) released an Initial Public Draft (IPD) report in November 2024 detailing the NIST roadmap for the PQC adoption, which includes aggressive timelines for deprecating (2030) and disallowing (2035) a broad range of currently used algorithms. NIST subsequently published the finalized PQC standards (FIPS 203, FIPS 204, and FIPS 205), which provide a clear framework as well as requirements. Commercial enterprises will eventually need to consider deploying updated cryptographic algorithms in anticipation of quantum threats targeting classic encryption algorithms. This upcoming change is particularly relevant to public sector and regulated industries like financial services and healthcare.

Enterprises recognize the need to prepare for a PQC world, and the first step is getting visibility to their cryptographic inventory used for data in transit. Cryptographic assets permeate an enterprise environment, and

[1] Source: Enterprise Strategy Group Research Report, *Operationalizing Encryption and Key Management*, April 2024.

organizations frequently struggle to identify all elements of their cryptographic technology. They then need to prepare to migrate that cryptographic infrastructure to emerging PQC standards for data in transit.

Palo Alto Networks Prepares Enterprises for Post-quantum World

Palo Alto Networks announced a new cryptography inventorying tool, quantum-optimized firewalls, and an update to its PAN-OS operating system (PAN-OS 12.1 Orion) to facilitate quantum readiness. The solution portfolio provides visibility to cryptographic assets, agility in adapting algorithms, and remediation capabilities to deliver enterprise quantum readiness.

Analyst Insight

Enterprises need to focus on gaining visibility into their cryptographic estate in preparation for impending changes needed to prepare for PQC and plan for accommodating hybrid and cryptographically agile implementations of PQC. Not all IT systems will be able to accommodate the expected compute and memory requirements of PQC software updates. The Palo Alto Networks announcement provides a smooth path for organizations dependent on legacy systems to combine PQC readiness with operational continuity.

Palo Alto Networks has applied an old concept to a new problem in taking a “virtual patching” approach to facilitating PQC readiness. Virtual patching has historically provided protection against vulnerabilities without modifying the code or system. In this case, Palo Alto Networks is providing a performance-optimized encryption proxy using the latest next-generation firewalls (NGFW), which are performance-optimized for PQC algorithms. Combining these NGFW with the latest update to PAN-OS introduces a "cipher translation proxy" that provides a bridge for web applications that must be protected but cannot be upgraded. This proxy adapts to a PQC world by translating classical cryptographic communications into quantum-safe ones and vice versa.

The exact timing for a cryptographically capable quantum computer is unknown, but the challenges are engineering challenges rather than physics challenges. It is not if quantum computers will arrive, but rather when cryptographically relevant quantum computers will arrive. Palo Alto Networks is providing a path for enterprises to understand their cryptographic exposure and options for legacy infrastructure that cannot be updated to achieve PQC readiness.

The Palo Alto Networks solution is a major piece of PQC readiness that complements enterprise initiatives to prepare digital certificate infrastructure for the upcoming changes caused by quantum computing.

Conclusion

As organizations start planning and executing to achieve PQC readiness, it’s time to prioritize crypto agility and improve their overall crypto hygiene. Improving crypto agility with necessary processes and solutions in place to evolve and future-proof their cryptographic infrastructure will enable enterprises to turn a potential quantum catastrophe into a minor bump in the road.

Information contained in this publication has been obtained by sources Informa TechTarget considers to be reliable but is not warranted by Informa TechTarget. This publication may contain opinions of Informa TechTarget, which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent Informa TechTarget’s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, Informa TechTarget makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

About Enterprise Strategy Group
Enterprise Strategy Group, now part of Omdia, provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com
www.esg-global.com