




The Quantum Countdown

*Why federal agencies must act now
to secure a post-quantum future.*



A decorative graphic in the top right corner consisting of numerous vertical orange bars of varying heights and widths, creating a stylized, abstract pattern that resembles a barcode or a data visualization.

Emerging technologies are quickly shaping how the federal government acts. With the advent of a cryptographically relevant quantum computer (CRQC) on the horizon, a new threat emerges, one that poses a significant risk to the integrity of government data.

CRQCs will disrupt traditional public-key encryption models; in response, federal agencies must act now to build resilient, future-ready systems.

Adversarial nation-states are already engaged in a strategy known as "**harvest now, decrypt later**," where threat actors collect vast stores of information with the express intent of unlocking it once a powerful CRQC comes online.

Agencies that postpone network security today will end up putting mission-critical information at risk, because CRQCs aren't a far-off possibility:

"CRQCs are a computer that's fast enough to use [Shor's Algorithm](#) to break some of the cryptography that we're using today. If you look at the different experts who are weighing in on when a CRQC will be available, some say it'll be within three years, others say five years, but most agree that it will probably be by the end of 2030," said Jim Smid, principal architect for the Department of War the intelligence community at Palo Alto Networks.

With this in mind, Palo Alto Networks is helping agencies implement next-generation safeguards by working with teams to address multi-layer encryption and deliver upgraded firewalls in anticipation of quantum-driven attacks.

Securing our nation's foundations

Zero Trust rests on a single, fragile assumption: that the underlying encryption securing an agency's data is unbreakable. "You can do a lot with Zero Trust, but if the encryption itself is broken, you don't have a good foundation," Smid explained.

Faced with this challenge, agency leaders should adopt a pragmatic, strategic approach that focuses on three core areas:

1. Visibility: The first step starts with achieving visibility into your organization's current cryptographic landscape. "All cyber starts with visibility," Smith advised. "Make sure that you have an inventory of every place you're deploying cryptographic algorithms and what encryption you have in place — including VPNs and SSL/TLS connections."

Generating an inventory of what's active in your environment allows for effective triage and prioritization when "harvest now" tactics emerge.

2. Standardization: Quantum theory is complex. "A lot of people get wrapped around the axle when they hear quantum, and they want to start down these pretty sophisticated conversations around the physics of it," Smid said. But in order to mount an effective defense, "you don't really have to understand how it works."

Focus instead on practical concerns — and solutions. “We have the capabilities built into our products to start turning on better encryption that will withstand quantum attacks. And we’ve made it very simple for you to do that,” he said.

Palo Alto Networks offers built-in capabilities that support [NIST 800-133](#), [FIPS 203](#), [204](#) and [205](#) — helping agencies align with federal mandates, ensure compliance and *avoid* vendor lock-in and bolt-on security solutions.

“We recognized that customers were overburdened by managing numerous network tools, and our response was to consolidate these functions into a single, unified solution. It’s this foundational approach that continues to guide our strategy in zero trust and quantum resiliency,” Smid said.

3. Phased Modernization: On Palo Alto Networks’ platform, agencies have the option to enable a “phased roll-out” without disrupting existing operations.

Post Quantum Cryptography (PQC) can be set as a default preference while still maintaining the ability to revert to legacy encryption if required. Once systems are ready, users can switch to mandatory PQC. Under this option, NIST standards apply to all data, in-rest and in-transit.

IMPORTANT NOTE

For workloads that may require extra scrutiny, [hybrid encryption](#) can be applied to reduce and defend against flawed PQC algorithms.



A Call to Partnership

Quantum technologies will change the very nature of how we live, work and play. It’s a problem of immense scale and complexity, yet agencies don’t have to “go at it alone,” Smid explains. Palo Alto Networks works with its federal partners to promote true quantum resiliency.



“Don’t feel like you need to solve the quantum readiness problem on your own. Reach out to industry,” Smid said. Tomorrow’s post-quantum foundations will take time to implement, especially in complex, federal IT environments.

To get started on that journey, and ensure you’re ready to face the quantum threat, look toward partners like Palo Alto Networks. “We’re building the standards into the overall platform to make it simple and manageable for our customers,” Smid said.

And with the right platform, you can gain visibility into agency vulnerabilities, “and have the tools at their disposal to quickly and effectively address them,” he said.

Start your post-quantum journey today.

[Learn more →](#)