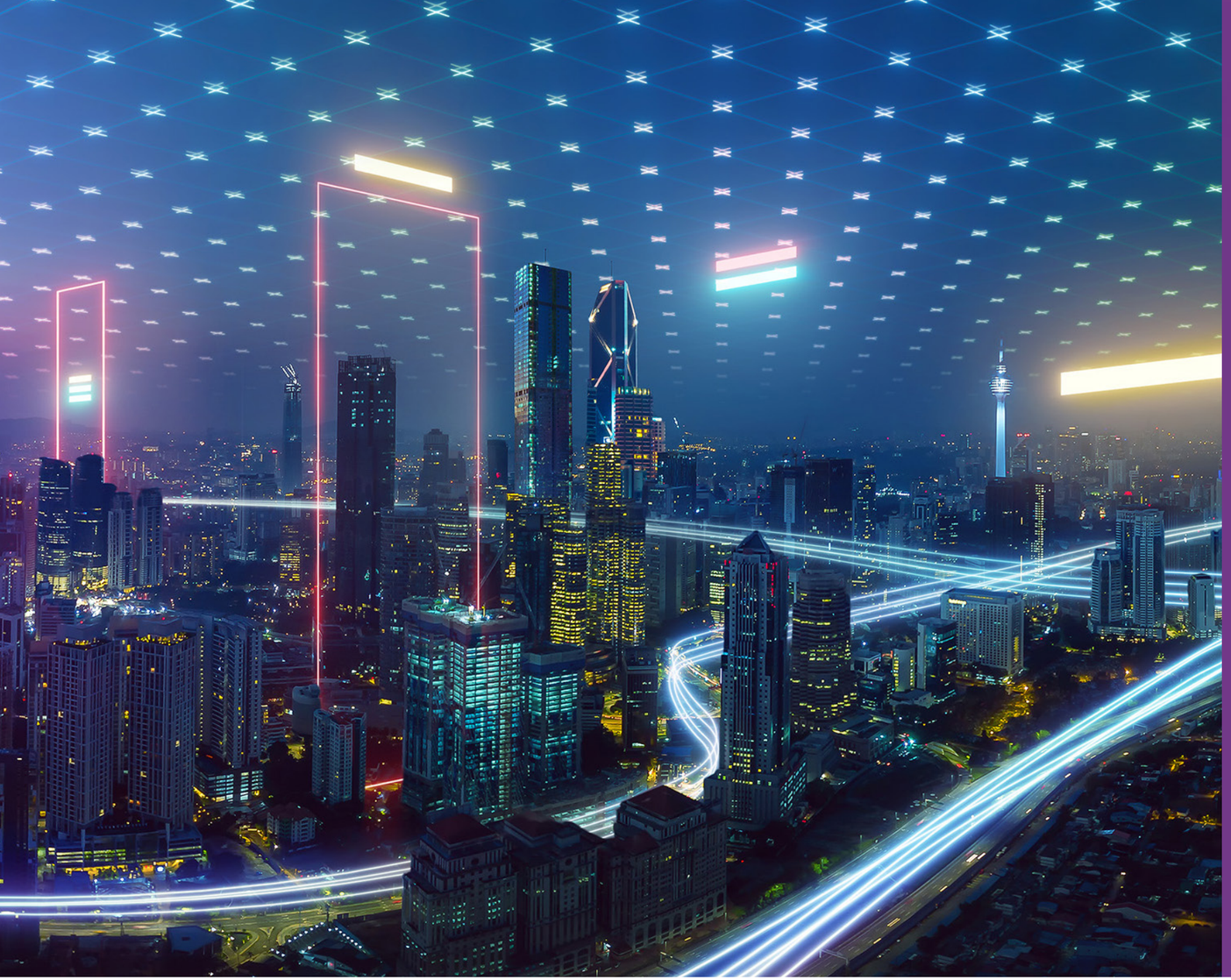


EBOOK

Why HSMs Are the Key to Quantum-Safe Security

ENTRUST

SECURING A WORLD IN MOTION

INTRODUCTION

A Shifting Data Security Landscape

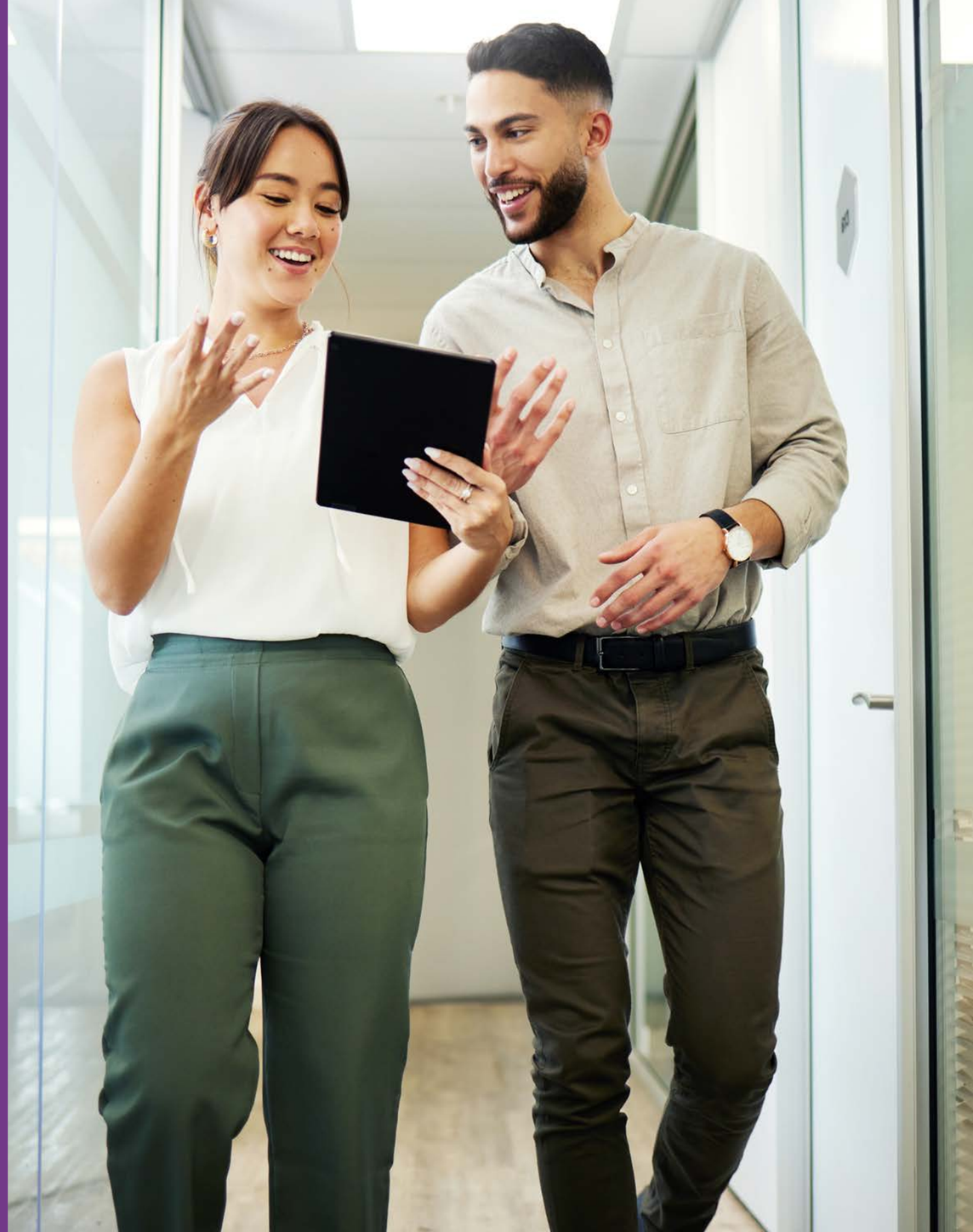
The foundations of digital trust are being tested like never before. Cyberattacks are growing more sophisticated, regulatory requirements are expanding, and the cryptographic methods we've relied on for decades are under pressure from a new threat: quantum computing.

According to Gartner, traditional public key cryptography (based on classical cryptographic algorithms) could be unsafe as early as 2029 — and fully breakable by 2034.[1] The National Institute of Standards and Technology (NIST) has taken this a step further, stating that it will begin deprecating traditional algorithms by 2030. And, with threat actors already harvesting encrypted data for later decryption, the transition to post-quantum cryptography (PQC) cannot wait.

For organizations across every industry, the implications are clear. Sensitive data — from financial transactions to healthcare records — is at risk of long-term exposure. The security systems that protect identities, payments, and digital services will need to evolve.

Hardware security modules (HSMs) are the root of trust for enterprise security. Entrust nShield HSMs are production-ready for PQC, helping organizations prepare today for the cryptographic challenges of tomorrow. This eBook explores why PQC readiness matters, the role HSMs play, and how organizations can get started today.

1. https://www.isaca.org/about-us/newsroom/press-releases/2025/organizations-lack-a-quantum-computing-roadmap-isaca-finds



The Importance of HSMs

Every digital interaction relies on trust. Behind the scenes, HSMs are what generate, store, and safeguard the cryptographic keys that secure this trust. They sit at the heart of identity systems, payment networks, and online services, ensuring that sensitive data is protected and transactions are authentic.

Think about the daily flow of information: when a customer checks their bank balance, makes a card payment, or logs into a secure website, keys located in an HSM work to encrypt data and verify identities. Without that root of trust, the confidentiality and integrity of digital services would collapse.

Global standards reinforce this role. Certifications like FIPS 140-3 and Common Criteria validate HSMs as the highest assurance option for key protection. They also support compliance with a growing list of mandates, from the Payment Card Industry Data Security Standards (PCI DSS) to the General Data Protection Regulation (GDPR) and Network and Information Security Directive 2 (NIS2).

> “HSMs provide the trust backbone enterprises need to operate securely and help meet the expectations of regulators, partners, and customers alike.”

The Post-Quantum Challenge

Quantum computing promises breakthroughs in science, medicine, and technology. But it also carries a disruptive consequence: the ability to break the cryptographic algorithms that protect today's digital world.

This will be the most complex cryptographic transition in history. Every asymmetric cryptographic system and infrastructure in use today must ultimately be re-engineered to become quantum-safe — a process that will touch every layer of IT and require significant time and resources.

Despite these risks, organizational preparedness remains alarmingly low. According to the Information Systems Audit and Control Association (ISACA), only 5% of CISOs say PQC is a high business priority.[2] Meanwhile, 63% of leaders believe quantum computing will increase cybersecurity risks, and half expect it will create regulatory challenges.

Adoption is lagging too — research shows that just 3% of banking websites currently support PQC, even though financial data is among the most targeted.[3] And, according to the Ponemon Institute, only 41% of organizations are preparing for the post-quantum world.[4]

The takeaway is clear: the quantum threat is no longer theoretical, and waiting to act only increases long-term exposure.

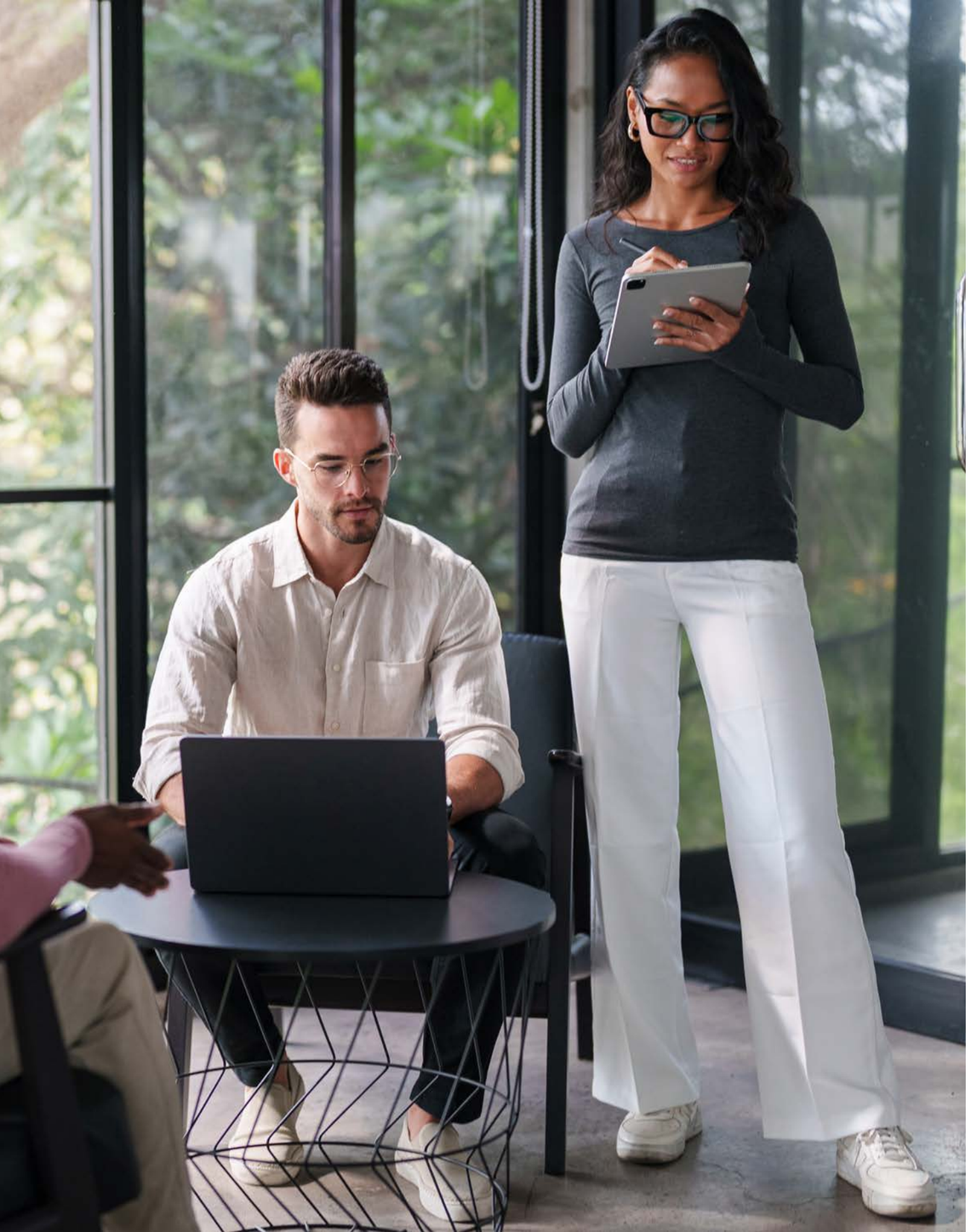
2. https://www.isaca.org/about-us/newsroom/press-releases/2025/organizations-lack-a-quantum-computing-roadmap-isaca-finds
3. https://www.f5.com/labs/articles/threat-intelligence/the-state-of-pqc-on-the-web
4. https://www.entrust.com/cybersecurity-institute/reports/2024-pki-and-post-quantum-trends-study

63%

of leaders believe quantum computing will increase cybersecurity risks, and half expect it will create regulatory challenges.

41%

of organizations are preparing for the post-quantum world.[4]



How HSMs Enable PQC Readiness

Preparing for the post-quantum era isn't just about identifying new algorithms — it's about ensuring they can be adopted, deployed, and managed at scale. That's where HSMs play a critical role.

NIST has already released the first three standardized post-quantum algorithms (ML-DSA, ML-KEM, and SLH-DSA), a milestone that marks the beginning of the industry-wide transition to quantum-safe cryptography. Additional standardized PQC algorithms are expected in the coming months and years, but this first tranche is significant — and the ones enterprises are preparing to implement.

To take advantage of these new standardized algorithms, organizations need infrastructure that can support them without requiring disruptive hardware refreshes. Entrust nShield HSMs are engineered for crypto-agility and can be reprogrammed while deployed in the field through software updates to support the latest cryptographic standards. This ensures enterprises can deploy PQC methods in production environments with confidence as soon as they are validated, while continuously strengthening resilience against quantum computing threats.

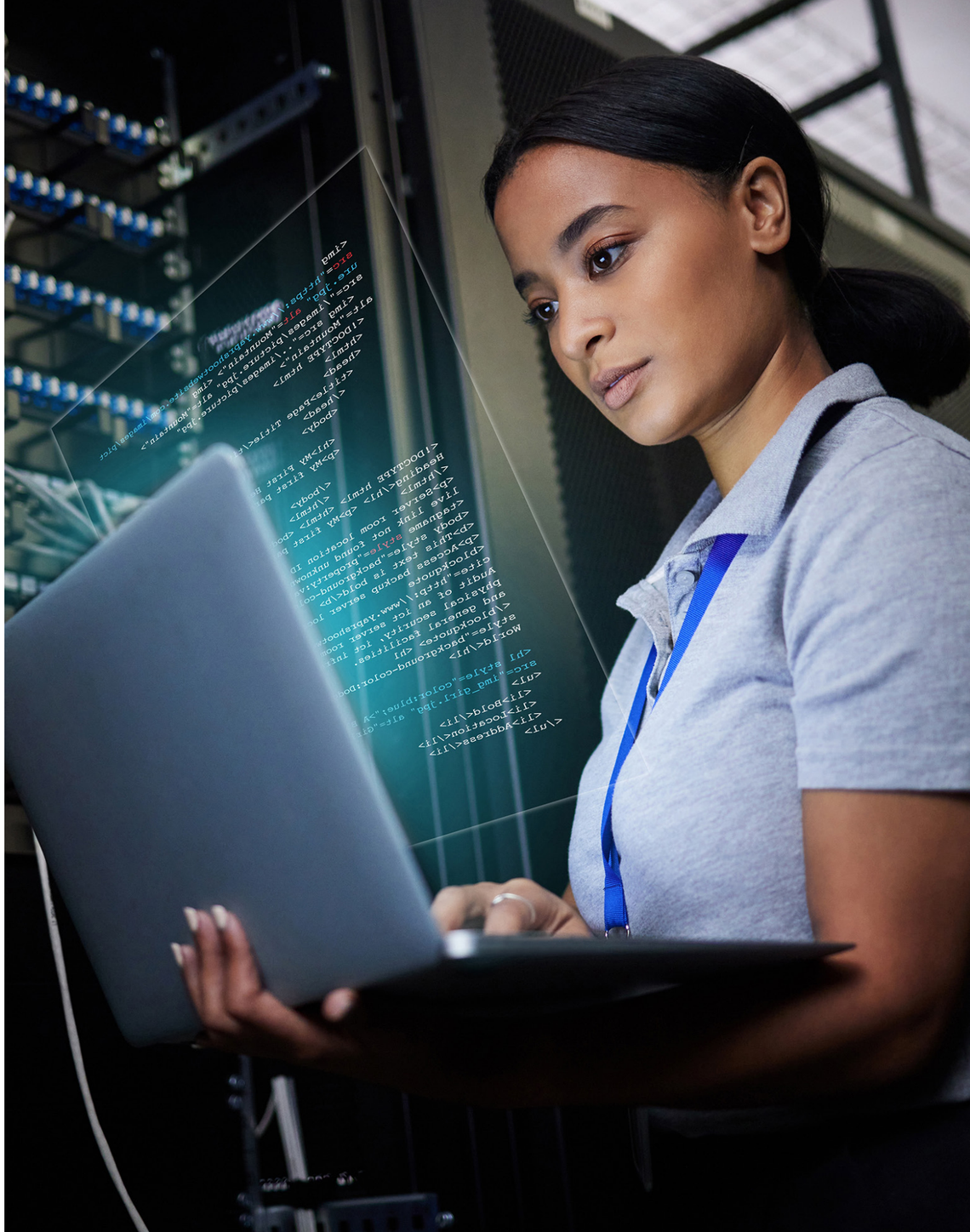
Bottom line: PQC readiness isn't a future promise — it's something enterprises can operationalize now with the right HSMs in place.

Benefits of HSMs

Enterprises face constant pressure to secure data, satisfy regulators, and maintain business continuity. HSMs address these needs by providing a trusted foundation for cryptographic operations — alongside a host of notable advantages:

- **Stronger security:** HSMs safeguard the most sensitive keys inside a tamper-resistant environment, protecting against insider threats and advanced attacks.
- **Compliance support:** Certifications like FIPS 140-3 and Common Criteria help organizations demonstrate compliance with PCI DSS, GDPR, NIS2, and other mandates.
- **Operational efficiency:** Consolidating key management in HSMs reduces complexity, eliminates risky workarounds, and lowers the burden on security teams.
- **Scalability and agility:** From securing a handful of applications to supporting enterprise-wide public key infrastructure (PKI), HSMs can adapt to diverse environments and evolving standards.
- **Business continuity:** Crypto-agility helps ensure that when new algorithms emerge — including PQC — organizations can adopt them without disrupting operations.

By combining high assurance with flexibility, HSMs provide a resilient backbone that enables secure growth in an increasingly complex threat and regulatory landscape.



HSMs in Action: Real-World Use Cases

HSMs aren't theoretical safeguards — they're already securing some of the most critical systems in the world. Their applications span industries and use cases, and PQC readiness ensures they can continue doing so as cryptographic standards evolve.

PKI: HSMs protect the keys that issue and manage digital certificates, enabling secure authentication across hybrid and cloud environments.

Financial services: From securing payment card data to protecting high-speed trading platforms, HSMs safeguard transactions at the core of global commerce. This is especially critical in a landscape where 80% of consumers prefer to do their banking online.[5]

Cloud deployments: Support for Bring Your Own Key and Hold Your Own Key models gives organizations control over data sovereignty and compliance in cloud environments. This matters because regulations increasingly require that sensitive keys stay under enterprise control, not solely with the cloud provider. For organizations that want maximum flexibility and assurance, Entrust offers nShield as a Service — a cloud-based HSM solution that delivers the same high-assurance protection without the complexity of managing hardware.

Beyond these established applications, HSMs are also expanding into emerging areas. They protect code signing processes to ensure software integrity, secure IoT ecosystems where millions of devices must each have unique identities, and provide the crypto-agility enterprises need to adopt PQC algorithms at scale.

5. https://www.entrust.com/company/newsroom/8-out-of-10-consumers-prefer-full-digital-banking-experience

How HSMs Protect the World Around You

HSMs aren't just behind-the-scenes hardware — they play a role in services and systems people rely on every day. To understand the real-world impact of quantum-ready HSMs, consider how they already protect billions of interactions across industries:

- **Securing connections:** Entrust nShield HSMs help protect more than 300 million wireless subscribers across America and another 57 million subscribers in the UK.
- **Protecting the power grid:** Leading U.S. electric utilities use nShield HSMs to safeguard services for more than 90 million customers.
- **Smarter, safer transport:** nShield HSMs provide the root of trust for Germany's first Cooperative Intelligent Transport System (C-ITS) on the Autobahn, enabling secure Vehicle-to-Everything connectivity with millions of digital certificates.
- **The root of trust for retail innovation:** Square chose nShield HSMs to secure its mobile point-of-sale card readers, protecting customer transactions and streamlining PCI DSS compliance.
- **The foundation of financial data security:** Banks and payment providers rely on HSMs for encryption, digital signing, and secure key management — essential for PCI DSS, NIS2, DORA, and eIDAS compliance.'
- **Security built in:** From device provisioning to code signing, HSMs secure manufacturing supply chains, ensuring products and software are trusted from the factory to the field.

These examples show how deeply HSMs are embedded in modern life. As quantum threats emerge, making these systems PQC-ready is critical to protecting not just enterprises — but the millions of consumers who depend on them every day.

Entrust Advantage: A Trusted Partner for the Future

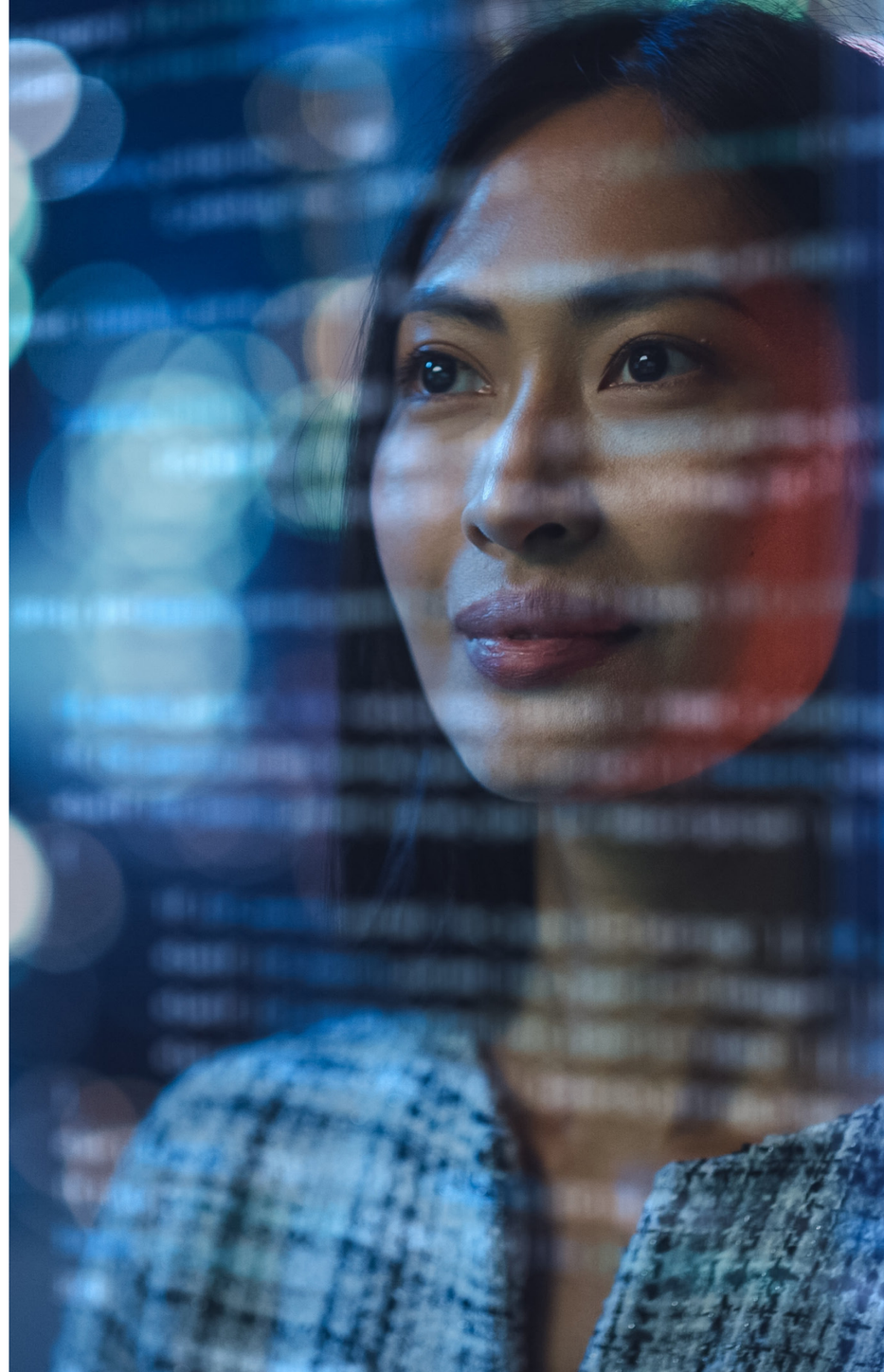
Entrust has been advancing cryptographic security for decades, helping organizations safeguard their most critical systems and data. With the nShield family of HSMs, Entrust continues to deliver innovation and assurance that enterprises can rely on.

At the core is the Entrust Security World architecture, which provides proven, scalable management of cryptographic assets across diverse environments. This foundation enables organizations to manage keys with consistency, resilience, and efficiency — whether they operate a single HSM or an enterprise-wide deployment.

Entrust also leads the way in PQC readiness. Most recently, the nShield HSM implementation of three NIST standardized post-quantum algorithms has been validated by NIST's Cryptographic Algorithm Validation Program (CAVP).[6] This demonstrates that enterprises can begin adopting PQC algorithms today with confidence, supported by production-ready solutions.

But Entrust's leadership extends beyond HSMs. We are active members of the Internet Engineering Task Force (IETF) and the NIST National Cybersecurity Center of Excellence (NCCoE) PQC Migration Project, helping shape global standards for the quantum era. Entrust also launched the industry's first commercially available PQC-ready PKI, giving organizations a proven path to manage certificates and identities with post-quantum assurance.

In parallel, Entrust continues to maintain and extend its portfolio of global certifications, including FIPS 140-3, Common Criteria, and eIDAS. While certification of PQC-enabled firmware is in process, these longstanding validations underscore Entrust's commitment to delivering solutions that meet the highest assurance standards.



6. https://www.entrust.com/company/newsroom/entrust-nshield-hsms-achieve-validation-from-nist-cryptographic-algorithm-validation-program

Ready for the Future of Cryptography?

Quantum computing is no longer a distant possibility — it's a coming reality that threatens the cryptographic systems protecting today's digital world. The risks are clear, but so is the path forward.

HSMs remain the backbone of digital trust, and **Entrust nShield HSMs** are production-ready to help organizations navigate the transition. With support for NIST-validated post-quantum algorithms, they give enterprises the confidence that their sensitive data, transactions, and services will remain secure — not only today, but in the quantum era ahead.

Existing nShield customers can take advantage of these capabilities by simply upgrading their HSM firmware in the field, avoiding the need for a complex migration process.

Organizations that act now can avoid costly disruptions later, ensuring resilience against future threats while supporting compliance with evolving regulations. Entrust provides the technology, expertise, and assurance to make that journey possible.

The time to prepare is now. Contact Entrust today to start your PQC readiness journey with a strong cryptographic foundation.

ABOUT ENTRUST

Entrust fights fraud and cyber threats with comprehensive identity-centric security that protects people, devices, and data. Our solutions help enterprises and governments safeguard critical systems from every angle, enabling secure onboarding and issuance, providing everyday identity protection, and empowering them with 360-degree visibility and orchestration across keys, secrets, and certificates so they can transact and grow with confidence. Building on our decades as a pioneer and innovator in establishing trust, Entrust has a global partner network and supports customers in over 150 countries.

For more information, visit entrust.com.

ENTRUST

SECURING A WORLD IN MOTION