Post-Quantum Security for Providers

Cisco empowers service providers to secure their networks and protect sensitive customer data against emerging quantum threats by delivering innovative, integrated post-quantum cryptographic solutions. By enabling cryptographic agility, maintaining regulatory compliance, and collaborating with industry leaders, Cisco helps ensure resilient, future-ready digital infrastructure—enabling providers to uphold trust, meet evolving security demands, and lead confidently into the quantum era.

Benefits

- **Future-proofs network security**
  By integrating post-quantum cryptographic algorithms—such as those recommended by NIST—Cisco helps ensure that provider networks remain secure against the emerging threat of quantum-enabled attacks.
- **Enables cryptographic agility**
  Cisco's emphasis on cryptographic agility allows networks and routers to seamlessly adopt new cryptographic standards, helping ensure ongoing protection as security requirements and algorithms evolve.
- **Supports regulatory compliance and data sovereignty**
  With features designed to manage and protect data in line with local and regional regulations, Cisco helps providers uphold legal obligations and maintain customer trust in complex regulatory environments.
- **Delivers immediate protection and smooth transitions**
  Quantum Key Derivation Services (e.g., Session Key Service [SKS] and Secure Key Integration Protocol [SKIP]) and proactive software upgrades empower providers to implement quantum-safe measures today, while preparing infrastructure for future standards with minimal disruption.
- **Enhances operational integrity and customer trust**
  By safeguarding sensitive data and helping ensure uninterrupted service even as quantum threats develop, Cisco helps providers differentiate themselves as resilient and forward-thinking partners.

Overview

Quantum computing, while offering revolutionary advances, also poses a critical risk to current cryptographic systems that secure data across the internet and private networks. As quantum capabilities develop, threat actors are already harvesting encrypted data with the intent to decrypt it in the future, exposing sensitive sectors like government, finance, and critical infrastructure to potential breaches, financial fraud, and loss of confidential information.

Service providers, who transmit and manage vast volumes of sensitive data, face unique challenges in safeguarding their infrastructure and ensuring compliance with evolving regulatory requirements.

Cisco's post-quantum security solutions help service providers proactively address these risks by integrating quantum-safe cryptographic algorithms and enabling cryptographic agility across their networks. By adopting and testing next-generation algorithms and delivering software upgrades and quantum-safe key management tools, Cisco empowers providers to maintain data confidentiality, comply with regulations, and ensure operational integrity as quantum threats emerge. This comprehensive approach helps customers secure their networks today while preparing for the challenges of tomorrow's quantum era.

Trends and challenges

The quantum threat is imminent

Quantum computing is rapidly advancing, promising to solve complex problems at speeds impossible for today's computers. However, this innovation poses a critical challenge to current cryptographic systems, as quantum-enabled attacks could break widely used protocols like TLS, SSH, and MACsec. Threat actors are already exploiting this future risk through tactics such as "harvest now, decrypt later," where they collect encrypted data today, intending to decrypt it when quantum computers become viable. This creates an urgent need for quantum-resistant security, especially for sectors where data must remain confidential for a decade or more.

Regulatory and compliance pressure is increasing

Service providers are under intense scrutiny from regulators and must comply with a growing set of data privacy and sovereignty laws. The dependence of national infrastructure and critical services on provider networks elevates the risk of a breach, potentially resulting in national security incidents or public safety threats. Providers must demonstrate leadership in security to win and retain trust amid evolving regulatory requirements.

Forward-thinking providers have a market opportunity

As quantum threats move closer to reality, providers who adopt post-quantum security measures will stand out as resilient and future-ready partners. Cisco's integrated, agile approach enables customers to confidently address these challenges while capturing new opportunities in a quantum-driven future.

How it works

Quantum-safe cryptographic algorithms

Cisco's solution centers on integrating next-generation, post-quantum cryptographic algorithms—such as those recommended by NIST (e.g., ML-KEM-1024)—across its networking portfolio. These algorithms are designed to withstand attacks from quantum computers, helping ensure that critical data in transit remains secure even as cryptographic threats evolve. Customers benefit from Cisco's ongoing testing and validation of these algorithms, which are being incorporated into protocols like SSH, TLS, and MACsec.

Quantum Key Derivation Services

To provide immediate quantum-safe protection, Cisco offers Quantum Key Derivation Services, including:

- **Session Key Service (SKS):** Enables secure, quantum-safe key management for encrypted communications.
- **Secure Key Integration Protocol (SKIP):** Facilitates the integration of quantum-safe key exchange mechanisms into existing network infrastructures.

These services allow customers to implement quantum-resistant key management today, reducing risk from "harvest now, decrypt later" attacks and preparing their organizations for future quantum capabilities.

Cryptographic agility and software upgrades

Recognizing the dynamic nature of cryptographic standards, Cisco emphasizes cryptographic agility—the ability for network devices to support new cryptographic algorithms as they are standardized. This capability is delivered through:

- **Software upgrades:** Regular updates occur across Cisco's portfolio, providing access to the latest quantum-safe cryptographic protocols and algorithms.

- **Router configuration flexibility:** Network infrastructure can be easily reconfigured to adopt new standards, balancing security with network performance and minimizing operational disruption.

Customers can schedule upgrades and plan for hardware refreshes as needed (with a focus on 2027 and beyond), helping ensure that their infrastructure evolves alongside quantum-safe standards.

Integration with existing infrastructure

Cisco's solutions are designed to be integrated seamlessly into existing provider networks. Quantum-safe features and tools are available as software enhancements and upgrades, allowing customers to enhance their security posture without the need for disruptive overhauls. This approach supports a phased transition, letting organizations adopt quantum-safe measures at a pace that fits their unique operational requirements.

Standards-based industry collaboration

Cisco is a leader in collaborating with industry bodies and standards organizations such as NIST, IETF, Trusted Computing Group, and IEEE. This helps ensure that Cisco solutions remain interoperable, future-ready, and aligned with the latest global security standards. Customers benefit from Cisco's active participation in standardization efforts, which speed the adoption and maturity of quantum-safe technologies across the industry.

Proactive guidance and best practices

Beyond technology, Cisco provides customers with expert guidance on transitioning to quantum-safe security. This includes:

- **Assessment of confidentiality requirements:** Helps customers identify which data sets and communications require long-term protection.
- **Migration planning:** Provides advice on software upgrade cycles, hardware refresh timelines, and phased integration of quantum-safe features.
- **Cryptographic agility strategies:** Helps ensure that networks remain adaptable as standards evolve and new threats emerge.

Use cases and applicability

Cisco's post-quantum security solutions are particularly suited for:

- **Service providers:** Telecommunications carriers, cloud operators, and managed network service providers transmitting and storing large volumes of sensitive data.
- **Sectors with long-term confidentiality needs:** Military, government, financial services, and critical infrastructure organizations facing regulatory requirements for data protection lasting a decade or longer.

Product and solution variations

While the core approach is consistent—integrating post-quantum cryptography and agility across the portfolio—customers may encounter:

- **Support for different protocols:** Quantum-safe enhancements are being added to widely used protocols (SSH, TLS, EAP-TLS for MACsec) based on customer deployment needs.
- **Hardware and software options:** Depending on the current generation of Cisco® routers and network devices, some customers may require hardware refreshes or may be able to adopt quantum-safe measures through software upgrades alone.

> "By prioritizing post-quantum cryptographic solutions, service providers can protect their customers' data, ensure data sovereignty, maintain regulatory compliance, and safeguard their own operational integrity as quantum threats emerge."

"This underscores the urgent need to adopt quantum-resistant security measures, ensuring that encryption remains robust against future quantum threats and that the security of critical data is preserved."

Cisco Capital

Financing to help you achieve your objectives

Cisco Capital® can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. Learn more.

The Cisco Advantage

Cisco is uniquely positioned to help providers achieve quantum-safe security through its integrated approach—combining advanced, standards-based cryptographic solutions, proven expertise in securing critical infrastructure, and deep industry collaboration. By offering agile, future-ready tools that seamlessly fit existing networks and guiding customers through every step of the transition, Cisco empowers organizations to confidently protect sensitive data and maintain regulatory compliance as quantum computing threats rapidly evolve.

Learn more

Secure Your Future with Cisco Post-Quantum Security

Protect your service provider infrastructure from emerging quantum threats today. Cisco's advanced post-quantum cryptography solutions help safeguard your network and customer data against future quantum attacks. Visit Cisco's Post-Quantum Cryptography Trust Center at https://www.cisco.com/site/us/en/about/trust-center/post-quantum-cryptography.html to learn more and connect with a Cisco Services sales representative or authorized channel partner.

C22-5650385-00 01/26