WHITE PAPER

Future-Proofing Your Security

A Guide to Implementing Quantum-Safe Cryptography

Executive Summary

Quantum computing is reshaping the security landscape. With the ability to solve complex mathematical problems far faster than traditional computers, quantum technologies pose a direct challenge to the cryptographic standards that protect data today.

Widely used encryption algorithms, such as RSA, ECC, and Diffie-Hellman, are based on problems considered computationally infeasible—until now. Shor's algorithm, for example, can already break these standards, while Grover's algorithm makes brute-force attacks against symmetric encryption significantly more efficient. Meanwhile, state-backed adversaries have begun implementing "harvest now, decrypt later" tactics—capturing encrypted data now for future decryption once quantum computing matures.

This paper outlines the urgency of the quantum threat and presents two strategic approaches to mitigating it: Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD). It details the algorithms being standardized, the global efforts underway, and the risks of waiting to act. And finally, a six-step roadmap offers a practical starting point for organizations seeking to secure long-lived data and critical systems before quantum disruption occurs.

"A quantum computer of sufficient size and sophistication... could jeopardize civilian and military communications, undermine supervisory and control systems for critical infrastructure, and defeat security protocols for most internet-based financial transactions."[1]

The Dawn of the Quantum Age

Quantum computing represents a fundamental shift in how problems are solved. Unlike classical bits, which exist as either 0 or 1, quantum bits (qubits) can exist in multiple states simultaneously through superposition. Combined with entanglement and interference, this enables quantum systems to evaluate a vast number of possibilities simultaneously, achieving speeds that far surpass those of traditional computing.

While these capabilities are opening doors in research and optimization, they are simultaneously dismantling long-standing security assumptions. The same mathematical principles that underpin today's encryption standards become vulnerable in the face of scalable quantum computation, so problems that were once practically unsolvable, like factoring large numbers or solving discrete logarithms, become tractable with quantum algorithms.

Critically, common encryption protocols like RSA, ECC, and Diffie-Hellman—once considered unbreakable—are now within reach of quantum attack. And while large-scale quantum computers capable of cracking encryption are still in development, the timeline is narrowing, with industry experts projecting that the cryptographic disruption known as "Q-Day" could arrive within the next decade. Organizations with long-term data sensitivity, such as those in government, finance, healthcare, and telecommunications, cannot afford to wait.

The Impact of Shor's and Grover's Algorithms

Quantum computing poses a serious threat to today's digital security by targeting the core assumptions underlying modern cryptographic systems. Two specific quantum algorithms—Shor's and Grover's—demonstrate the need for urgent action.

Impact of Shor's Algorithm on Cybersecurity

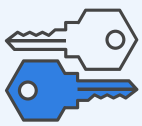
Undermines the security of many existing cryptographic systems, including secure communication, and digital signatures

Shor's algorithm: a direct threat to public-key cryptography

Shor's algorithm can efficiently factor large numbers and compute discrete logarithms, tasks considered infeasible for classical computers. This poses a direct risk to widely adopted public-key cryptosystems, including RSA, Diffie-Hellman Key Exchange, and Elliptic Curve Cryptography (ECC).

These algorithms protect everything from HTTPS connections to VPNs, digital signatures, and cryptocurrency wallets. Once quantum systems reach a sufficient scale, Shor's algorithm will enable adversaries to decrypt secure internet communications, forge digital signatures and impersonate trusted entities, and compromise banking systems and blockchain transactions.

The result would be a collapse in the confidentiality, authenticity, and integrity of data across virtually all sectors.



Impact of Grover's Algorithm on Cybersecurity:

Weakens the security of authentication mechanisms, data encryption, and password-based systems

Grover's algorithm: weakening symmetric encryption

Grover's algorithm doesn't break symmetric keys, but it cuts their effective strength in half by accelerating brute-force attacks. This impacts:

- **Password-based authentication:** Faster brute-force attacks increase the risk of credential compromise.
- **Encrypted data at rest:** Shorter key lengths become more vulnerable over time.
- **Authentication protocols:** Protocols relying on shared secrets or symmetric algorithms will require stronger protections.

"By 2029, advances in quantum computing will make most conventional asymmetric cryptography unsafe to use."[2]

"I estimate a 1-in-7 chance that fundamental public-key cryptography will be broken by 2026—and a 50% chance by 2031."[3]

While symmetric algorithms can be hardened (such as using AES-256 instead of AES-128), systems must be evaluated for their exposure and upgraded accordingly.

Harvest Now, Decrypt Later: A Quiet Arms Race

Even though production-scale quantum computers aren't yet available, the threat posed by such systems is already active. State-backed adversaries are already executing Harvest Now, Decrypt Later (HNDL) attacks, capturing encrypted data with the intention of decrypting it once quantum capabilities mature.

This approach is especially dangerous for long-lived sensitive data, such as classified records, legal files, health data, and financial histories, critical infrastructure, including power grids, telecom backbones, and transportation control systems, and government and defense systems, including secure communications, encrypted archives, and authentication mechanisms.

The risk is not theoretical. Encrypted data stolen today can be safely stored for years before it is eventually compromised.

The HDNL strategy makes it clear: Waiting for quantum computers to become widespread before deploying countermeasures is not an option. Organizations must secure their long-term data now.

Understanding Quantum-Safe Cryptography

As quantum computing advances, organizations must adopt cryptographic systems that can withstand quantum-enabled attacks. Two primary approaches form the foundation of quantum-safe security: PQC and QKD. Each offers distinct advantages and implementation pathways.

PQC

PQC algorithms are designed to resist attacks from both classical and quantum computers. Unlike traditional public-key algorithms, PQC is built on mathematical problems that remain computationally difficult even for quantum systems.

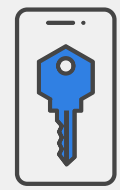
These algorithms are structured into four major families:

Algorithm Family	Description	Examples
Lattice-based	Based on hard problems in high-dimensional lattices	CRYSTALS-Kyber (ML-KEM), Dilithium, Frodo, NTRU
Code-based	Leverages the difficulty of decoding error-correcting codes	BIKE, HQC
Multivariate	Involves solving systems of multivariate polynomial equations	Rainbow, UOV
Hash-based	Uses one-way hash functions to create secure digital signatures	XMSS, SPHINCS+

Highlights from NIST's PQC standardization effort

- **ML-KEM (CRYSTALS-Kyber)**
  A lattice-based key encapsulation mechanism selected by NIST for FIPS standardization. Efficient and secure, it is a leading choice for quantum-resistant key exchange.
- **BIKE and HQC**
  These code-based alternative algorithms under consideration by NIST provide redundancy and resilience by offering different mathematical underpinnings than lattice-based systems.
- **Frodo**
  Another lattice-based scheme that avoids structured lattices, providing higher theoretical security at the cost of larger keys and slower performance—ideal where security outweighs efficiency.

These algorithms are currently being evaluated and implemented by security vendors across the ecosystem. Fortinet is actively integrating these standards into our roadmap to support long-term cryptographic resilience.



"Most organizations don't know how cryptography works within their environment, where keys and algorithms are used, or how secrets are stored and managed. Swapping them for new algorithms will be challenging."[4]

QKD

QKD takes a fundamentally different approach: Instead of relying on mathematical difficulty, it uses the laws of quantum mechanics to establish a secure key exchange.

In QKD systems, quantum particles (such as photons) are transmitted between two parties. Any eavesdropping attempt disturbs the quantum state of those particles, instantly alerting the parties and preserving the integrity of the key.

QKD advantages

- **Unconditional security**
  Based on physical laws, not mathematical assumptions.
- **Forward secrecy**
  Keys are never transmitted directly and cannot be cloned.

Challenges and limitations

- **Distance constraints**
  Quantum signals degrade over long distances, limiting range.
- **High cost**
  QKD systems require specialized hardware and infrastructure.
- **Integration complexity**
  Existing systems are not designed to support QKD natively, making deployment nontrivial.

In short, QKD looks promising for ultra-high-security applications but remains impractical for broad use. PQC, by contrast, is scalable, software-driven, and deployable across today's digital infrastructure.

PQC vs. QKD: a practical comparison

While QKD offers theoretical perfection, PQC offers practical protection immediately, and at scale. Both are part of a quantum-safe future, but only PQC is ready for enterprise deployment today. Here is a side-by-side comparison:

Feature	Post-Quantum Cryptography (PQC)	Quantum Key Distribution (QKD)
Operating principle	Quantum-resistant algorithms	Secure key exchange via quantum mechanics
Deployment	Software-based upgrades	Requires dedicated quantum hardware and channels
Use cases	Encryption, authentication, digital signatures	Limited to secure key exchange
Scalability	High, easy to integrate with existing systems	Low, constrained by infrastructure and distance
Cost	Low to moderate	High
Maturity	Actively being standardized and implemented	Still in early research and commercial rollout

The Impact of Quantum Computing on Cybersecurity

Quantum computing will not merely challenge today's encryption—it will upend foundational elements of cybersecurity. The shift will impact every sector that relies on digital trust, from communication and finance to defense and infrastructure.

Disruption of cryptographic standards

Shor's algorithm directly threatens the integrity of public-key systems. These algorithms underpin secure communication (HTTPS traffic, VPN tunnels, and secure email), digital signatures (software updates, certificates, and transaction validation), and data encryption (stored files, cloud backups, and distributed ledgers).

If these systems are compromised, attackers could intercept traffic, impersonate trusted services, or decrypt sensitive data long after it was originally transmitted.

Risks to critical infrastructure

Public-key cryptography is deeply embedded in operational systems deployed across the digital infrastructure, from energy grids and transportation networks to satellite communications and financial markets. Quantum attacks could disrupt power distribution, sabotage supply chains, and exfiltrate proprietary industrial controls.

As a result, quantum-readiness must extend beyond IT teams to operational technology (OT), where encryption plays an increasingly critical role.

Acceleration of brute-force threats

Grover's algorithm weakens symmetric-key systems by reducing the search space from 2^n to $2^{n/2}$. While this doesn't break encryption outright, it does require organizations to reevaluate key sizes (upgrade to AES-256), strengthen password hashing mechanisms, and reassess authentication protocols using shared secrets. These shifts, while manageable, must be executed deliberately and at scale across every system that relies on symmetric keys.

Implications for authentication

Authentication frameworks, including TLS, Kerberos, and federated identity models, often rely on public-key validation. These models must be re-architected to incorporate PQC or hybrid mechanisms that remain secure even under quantum conditions.

Standards and Global Efforts

Successfully navigating the quantum transition requires not only technical readiness but also effective coordination among governments, vendors, and standards bodies.

NIST's role in PQC standardization

The U.S. National Institute of Standards and Technology (NIST) has led the global effort to define, vet, and standardize PQC algorithms. Its multi-year competition has already produced significant milestones:

- **July 2022:** NIST selects four algorithms for standardization:
  - CRYSTALS-Kyber for key encapsulation
  - CRYSTALS-Dilithium, Falcon, and SPHINCS+ for digital signatures
- **August 2024:** NIST finalizes the first post-quantum Federal Information Processing Standards (FIPS):
  - **FIPS 203:** Lattice-based key agreement
  - **FIPS 204:** Lattice-based digital signatures
  - **FIPS 205:** Hash-based signatures (SPHINCS+)

These form the core of the emerging quantum-safe ecosystem and guide vendor implementation worldwide.

International standards efforts

Multiple global bodies are driving alignment on PQC:

- **ETSI:** Advancing telecom-specific standards for PQC
- **ISO/IEC:** Defining interoperable global standards
- **IETF:** Developing Internet Protocol support for PQC
- **ITU:** Promoting quantum awareness and infrastructure readiness

These bodies collaborate with NIST to ensure consistency and interoperability across use cases and geographies.

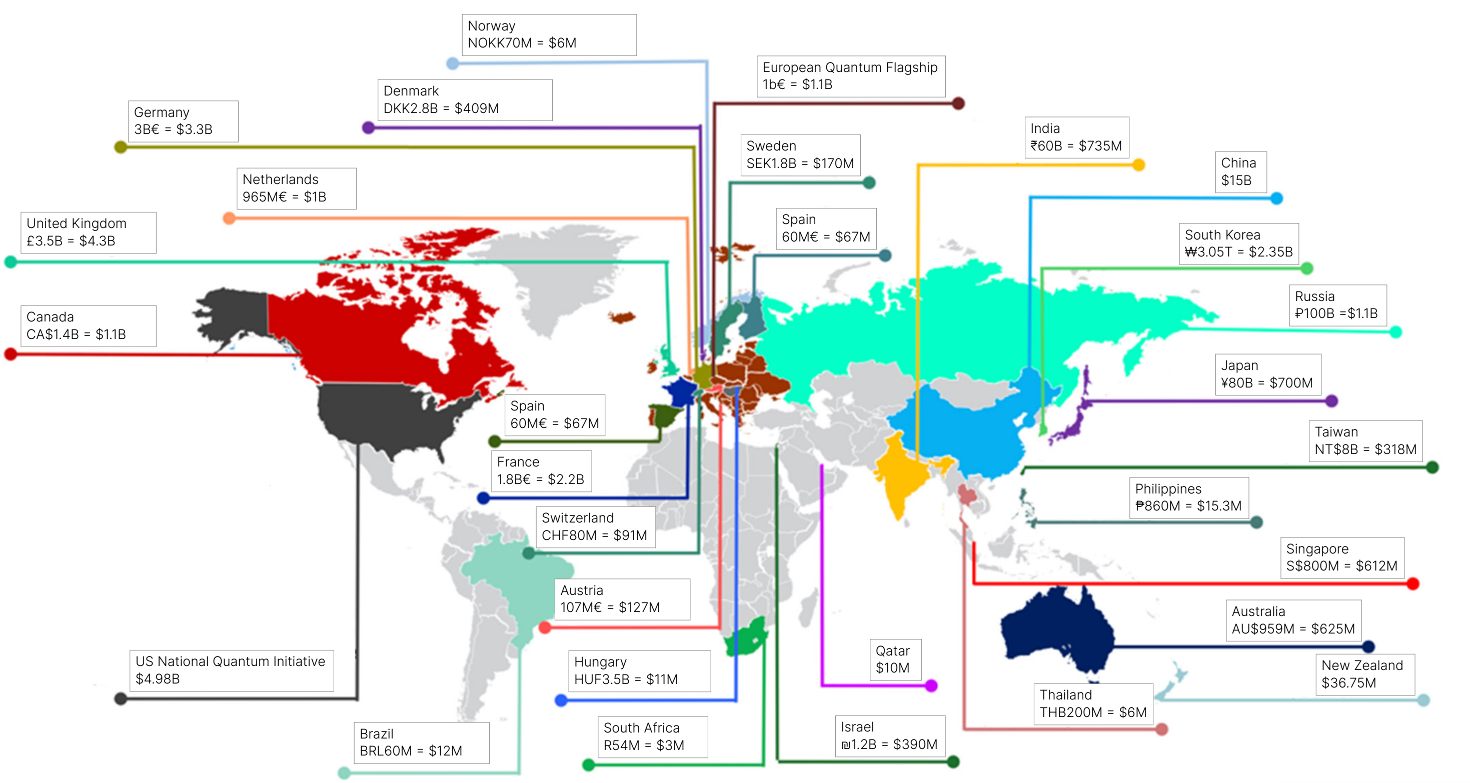


Figure 1. Global quantum efforts worth $42 billion (estimate)

Government investment in quantum readiness

Governments worldwide are backing quantum security with strategic investments and national roadmaps:

- **U.S.:** National Quantum Initiative Act and NSM-10 transition strategy and the 6 June 2025 Executive Order "Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144" directing near term actions by the US Government
- **EU:** Quantum Flagship program
- **UK:** National Quantum Strategy
- **Other nations:** Initiatives in Canada, China, Australia, India, Brazil, South Africa, and Spain

The race to secure quantum infrastructure is well-funded and already underway, with over $42 billion invested globally in the development and defense of quantum technology.

Industry collaboration and Fortinet's role

Major technology firms, including IBM, Google, and Microsoft, are also heavily investing in quantum-safe platforms. Fortinet is contributing directly through the integration of PQC into Fortinet solutions, participation in standards organizations, and co-founding roles in global alliances such as the World Economic Forum's Center for Cybersecurity, the Cyber Threat Alliance, and the Cloud Security Alliance. These partnerships support industrywide adoption and rapid operationalization of quantum-safe measures.

The Need for Quantum-Safe Security

For most organizations, the move to quantum-safe cryptography will not be optional. It will be essential to preserving trust, continuity, and compliance in the face of disruption. The transition is not just a security upgrade—it's a foundational shift in digital resilience.

Why implement quantum-safe now?

Proactive risk mitigation: Deploying quantum-safe encryption now protects long-lived and high-value data from HNDL attacks already in progress.

Improved security posture: PQC solutions do not just resist future quantum attacks. They also provide enhanced security that strengthens defenses against today's advanced threats.

Competitive advantage: Organizations that prioritize quantum resilience signal a long-term commitment to security and compliance—a position that is essential for regulators, customers, and partners alike.

Innovation catalyst: Preparing for quantum security often leads to broader modernization: asset inventory, key life-cycle management, and crypto-agility.

Implementation Challenges

Transitioning to post-quantum cryptography is not a simple software patch. It will require technical, operational, and organizational change across IT, OT, and vendor ecosystems. These challenges include:

Complexity of transition

While cryptographic functions are deeply embedded in infrastructures, organizations often lack complete visibility, including where cryptography is used, which protocols depend on vulnerable algorithms, and how cryptographic assets are stored and managed.

Interoperability and integration

Introducing PQC into legacy systems and vendor stacks can create compatibility issues. Not all tools, devices, or platforms are ready for PQC integration. Hybrid strategies—combining classical and quantum-safe algorithms—may be required during the transition.

Resource constraints

Deploying and maintaining quantum-safe solutions requires specialized knowledge. But with many organizations already facing staffing and skill gaps in cybersecurity, execution will be more challenging without the right partners.

Cost considerations

The cost of transition may involve upgrading hardware to support longer keys or new libraries, retooling authentication and encryption protocols, training security and DevOps teams, and working with vendors to replace or augment existing crypto modules.

Vendor readiness

Not all vendors have integrated PQC into their roadmaps. Delaying adoption until incumbent vendors catch up can leave organizations exposed. Vendors ready now with solutions designed to adapt to changing requirements should be prioritized.

Sustaining long-term security

Quantum readiness is not a one-time project. Standards, threats, and technologies will continue to evolve. Security strategies must stay agile and adaptive to remain effective through the decade ahead.

Implementing Quantum-Safe Security: A Six-Step Strategy

Fortinet recommends the following phased approach to quantum resilience:

1. Use quantum-resistant cryptography now

Prioritize the protection of sensitive and long-term data using NIST-approved PQC algorithms. Transition to quantum-safe encryption, signatures, and key exchanges wherever feasible.

2. Select quantum-safe-ready solutions

Engage vendors who already offer quantum-safe options or have committed to the NIST roadmap. Fortinet is actively integrating PQC into its products and platform, enabling rapid adoption.

3. Transition gradually using hybrid models

For legacy environments, adopt hybrid cryptographic mechanisms that pair classical and quantum-safe algorithms. This ensures backward compatibility while preparing for the future.

4. Assess risk across systems and workflows

Conduct a detailed cryptographic inventory. Identify algorithms in use, where they live, and where they interact. This includes everything from VPNs and certificates to authentication systems, DevOps pipelines, and OT endpoints.

5. Monitor advancements and stay agile

Track updates from NIST, ETSI, and other global bodies. Keep an eye on cryptographic libraries, product updates, and vulnerabilities that could impact your rollout plan.

6. Ensure standards compliance

Align with industry best practices and evolving standards to demonstrate readiness and maintain regulatory compliance. Fortinet solutions are designed to support current FIPS and emerging PQC standards.

This approach will help ensure your organization is protected against present-day hackers who aim to exploit your data once quantum-computers are available (often referred to Y2Q or Qday).

6 Steps to Prepare for Quantum Cyber Threats

1

Adopt Quantum-Resistant Cryptography

Protect sensitive data with post-quantum encryption.

2

Invest in Quantum-Ready Solutions

Future-proof systems and partner with quantum-safe vendors.

3

Transition Gradually

Use a hybrid approach combining traditional and quantum-safe methods.

4

Assess Risks and Update Policies

Identify vulnerabilities and align policies with quantum threats.

5

Stay Informed

Monitor advancements in quantum computing and cryptography.

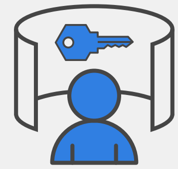
6

Ensure Compliance

Follow emerging standards and adopt best practices.

Future Trends and Considerations

The quantum era is approaching faster than many anticipated. While full-scale quantum computers are still in development, the surrounding ecosystem is maturing rapidly. Those organizations that track and anticipate emerging trends will be better positioned to adapt and lead.



"Security and risk leaders need to begin planning for post-quantum cryptography now due to the wide and deep impact of replacing cryptographically dependent systems."[5]

Quantum-AI synergy

The convergence of quantum computing and AI will accelerate defensive and offensive capabilities.

- **Real-time threat intelligence:** Quantum-enhanced AI could analyze massive datasets at unprecedented speeds, improving anomaly detection and threat correlation.
- **Adaptive defenses:** AI trained on quantum datasets may develop self-healing, autonomous cybersecurity systems capable of responding to complex attacks.
- **More sophisticated adversaries:** Threat actors will use quantum-AI tools to automate attacks, identify vulnerabilities at scale, and develop novel evasion techniques.

Hybrid quantum-classical systems

Rather than replace classical computing, early-stage quantum processors will augment it. These hybrid systems will accelerate threat detection workflows, improve the performance of PQC algorithms, and deliver better performance for simulation, modeling, and analytics

Enterprises should prepare for hybrid environments where security systems leverage both classical and quantum resources.

Quantum-safe hardware innovation

Custom processors and chips optimized for post-quantum cryptography are already being developed. These purpose-built components will reduce the latency associated with PQC operations, enable secure deployment in constrained environments (IoT, mobile, edge, and improve performance and energy efficiency. Organizations should expect increased availability of quantum-resistant endpoints and cloud-enabled cryptographic modules in the years ahead.

Quantum-safe cloud adoption

Major cloud providers are introducing services that support PQC-enabled key management, quantum-resilient storage, and secure communication frameworks built on NIST standards. These services will enable faster rollout of quantum-safe architectures, especially for distributed enterprises and DevOps-centric teams.

Securing the Future: A Call to Action

The quantum threat is no longer hypothetical. While the timeline for "Q-Day" remains uncertain, the preparation window is closing. Nation-states are expected to develop cryptographically relevant quantum computers (CRQC) before the private sector. Their use will likely expand from initial espionage activities to other applications over time. Additionally, early commercial CRQCs will probably have limited uptime and error correction capabilities, restricting their immediate impact.

Quantum computing doesn't just change the future of cybersecurity—it redefines what it means to be secure. Organizations must act now to protect high-value data, secure critical infrastructure, and maintain digital trust in the decade ahead. Those organizations that prepare now will lead tomorrow.

Key takeaways

- **The threat is already here:** HNDL attacks are occurring now, targeting data that may remain sensitive for years to come.
- **PQC is practical and available:** NIST-approved algorithms provide a ready pathway for adoption.

- **QKD is promising, but niche:** It is valuable for specific high-security environments, but limited in scalability.
- **Standards are solidifying:** Governments, vendors, and alliances are aligning to support global migration.
- **Fortinet is ready:** Our platform strategy and product roadmap are built for a quantum-resilient future.

What to Do Next

To prepare for the quantum era, organizations should begin by assessing their current cryptographic landscape, identifying where sensitive data resides, and how it is protected. It's critical to prioritize the protection of long-lived, regulated, and mission-critical data that may be vulnerable to future quantum decryption. Selecting vendors that align with NIST standards and demonstrate a clear commitment to post-quantum cryptography (PQC) is equally important. Implementing hybrid cryptographic strategies now and evolving them over time will help ensure long-term resilience.

Fortinet is already building toward that future. Our portfolio is grounded in strong security foundations and engineered to adapt alongside the emerging demands of quantum-safe networking.

[1] Biden, Joseph R. National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems. The White House, 4 May 2022.

[2] Gartner. Top Strategic Technology Trends for 2025: Postquantum Cryptography. Gartner, 2024.

[3] Mosca, Michele. Cybersecurity in an Era with Quantum Computers: Will We Be Ready? Cryptology ePrint Archive, Paper 2015/1075, 2015.

[4] Gartner. Top Strategic Technology Trends for 2025: Postquantum Cryptography. Gartner, 2024.

[5] Gartner. Postquantum Cryptography: The Time to Prepare Is Now! Gartner, 2023.

www.fortinet.com

August 1, 2025 9:40 PM / MKTG-1657-0-0-EN