QuantumGate

White Paper | February 2025

The Discovery Tools as a fundamental step towards the Transition to the PQC cryptography

Introduction

In today's digital landscape, cryptography forms the backbone of secure communication and data protection. However, the advent of quantum computing poses a significant threat to current cryptographic methods. This white paper explores the transition from classical to post-quantum cryptography (PQC) and highlights the crucial role of discovery tools in this process.

> Quantum Computing isn't just a threat to current encryption; it's fundamentally altering the landscape of confidentiality and integrity.

Understanding Post-Quantum Cryptography

Quantum computers pose a serious threat to classical cryptographic systems due to their ability to solve complex mathematical problems much faster than traditional computers. The primary concern lies in quantum algorithms that can efficiently break widely used asymmetric encryption methods:

Shor's Algorithm: This quantum algorithm can quickly factor large numbers and solve discrete logarithm problems, which form the basis of many public-key cryptosystems, including:

RSA Encryption: Traditionally considered secure due to the difficulty of factoring large numbers, RSA could be broken within hours by a sufficiently powerful quantum computer.

Diffie-Hellman & Elliptic Curve Cryptography (ECC): These widely used asymmetric cryptographic methods are also vulnerable to quantum attacks.

Google demonstrated "quantum supremacy" in 2019 when their Sycamore processor solved a specific problem in 200 seconds that would have taken the world's fastest supercomputer 10,000 years.

Impacts of Quantum Computing on Cryptography

Public Key Infrastructure (PKI) Vulnerability

Encryption and key exchange mechanisms that rely on RSA, DH, or ECC will no longer be secure once quantum computers reach a practical level of power.

Blockchain and Cryptocurrency Risks

Public-key cryptography underpins many blockchain technologies, making cryptocurrencies susceptible to quantum attacks.

"Store Now, Decrypt Later" (SNDL) Attacks

Adversaries may store encrypted data today, anticipating that future quantum computers will allow them to decrypt it once they become powerful enough. This poses a long-term threat to sensitive information.

The Need for Post-Quantum Cryptography

To counter these risks, the cybersecurity community is actively developing **post-quantum cryptographic (PQC) algorithms**, also known as **quantum-resistant cryptography**. These algorithms are designed to resist attacks from both classical and quantum computers, ensuring long-term data protection across critical industries.

These algorithms rely on mathematical problems that are believed to be difficult for both classical and quantum computers to solve.

As quantum computing advances, traditional public-key cryptographic solutions—such as classic digital signatures and key exchange mechanisms—will become obsolete, impacting secure communications, e-commerce, web security, and various other applications. The development and implementation of quantum-resistant cryptographic standards will be crucial in safeguarding sensitive information in the post-quantum era.

Preparing for the Transition

The transition to new cryptographic standards will take many years, depending on the size and complexity of an organization. As a result, industry experts and government officials recommend starting the process now to protect sensitive data.

Regulators in several Western countries have released requirements or recommendations urging organizations to commence the migration process immediately.

The Transition to Post-Quantum Cryptography

Discovery Tools: The Foundation of Cryptographic Transition

The first step in transitioning to PQC is understanding your organization's current cryptographic landscape. This involves identifying all cryptographic assets used across your infrastructure, including:

- Cryptographic keys and certificates
- Encryption algorithms
- Cryptographic protocols
- Hardware security modules (HSMs)
- Cloud-based cryptographic assets

Discovery tools play a pivotal role in the transition to PQC. These tools, often paired with professional services, help organizations create a comprehensive inventory of cryptographic assets, analyse vulnerabilities, and assess associated risks.

Comprehensive Asset Inventory

Modern IT environments are complex and hybrid, making manual discovery of cryptographic assets impractical. Automated discovery tools can scan across diverse platforms, including on-premises servers, cloud environments, and containerized applications. These tools identify cryptographic assets stored in:

- Certification Authorities (CAs)
- Servers and databases
- Hardware Security Modules (HSMs)
- Network traffic
- Cloud providers
- Containers and microservices

This comprehensive inventory provides the necessary context for managing risks and planning the transition to PQC.

Risk Assessment and Analysis

Discovery tools go beyond simple identification. They analyse the collected data to:

- Identify outdated algorithms and other vulnerable cryptographic assets
- Assess the potential impact of quantum attacks on each asset
- Prioritize assets for remediation based on risk level

This analysis is crucial for developing a targeted and efficient PQC transition strategy.

Continuous Monitoring

The cryptographic landscape is not static. Discovery tools provide ongoing monitoring capabilities, allowing organizations to:

- Track progress towards quantum readiness
- Identify new vulnerabilities as they emerge
- Ensure compliance with evolving standards and regulations

The Value of Discovery Tools

Informed Decision Making

Leaders can prioritize resources, allocate budgets, and develop targeted strategies based on concrete and comprehensive data rather than assumptions.

Risk Mitigation

Discovery tools help organizations identify and address cryptographic vulnerabilities before they can be exploited.

Compliance and Audit Readiness

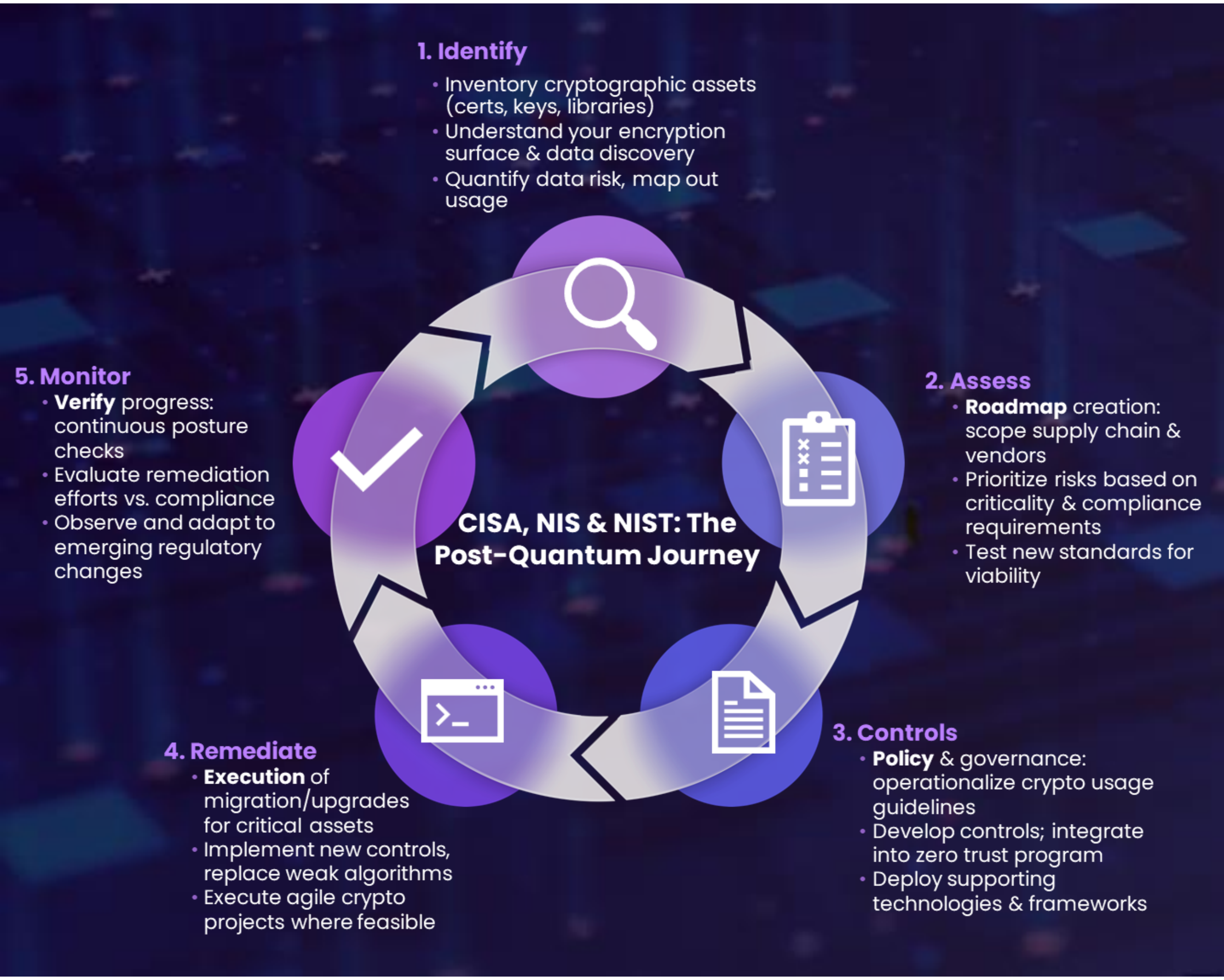
As regulations around cybersecurity and data protection evolve, discovery tools help organizations stay compliant. They provide the documentation and insights needed to demonstrate due diligence in cryptographic practices.

Efficient Resource Allocation

By identifying the most critical vulnerabilities and high-risk assets, discovery tools allow organizations to focus their resources where they're needed most. This targeted approach can significantly reduce the overall cost and complexity of the PQC transition.

The transition to post-quantum cryptography is not just a technical upgrade; it's a strategic imperative for organizations worldwide

Organizations and Governments are urged to prepare for this transition to maintain data security in the quantum era. NIST, NIS and CISA have already identified the journey to quantum-resistant cryptography, which is a complex one, but with the right tools and expertise, organizations can navigate this transition successfully, ensuring their data remains secure in the quantum era.



CISA, NIS & NIST: The Post-Quantum Journey

1. Identify
- Inventory cryptographic assets (certs, keys, libraries)
- Understand your encryption surface & data discovery
- Quantify data risk, map out usage

2. Assess
- **Roadmap** creation: scope supply chain & vendors
- Prioritize risks based on criticality & compliance requirements
- Test new standards for viability

3. Controls
- **Policy** & governance: operationalize crypto usage guidelines
- Develop controls; integrate into zero trust program
- Deploy supporting technologies & frameworks

4. Remediate
- **Execution** of migration/upgrades for critical assets
- Implement new controls, replace weak algorithms
- Execute agile crypto projects where feasible

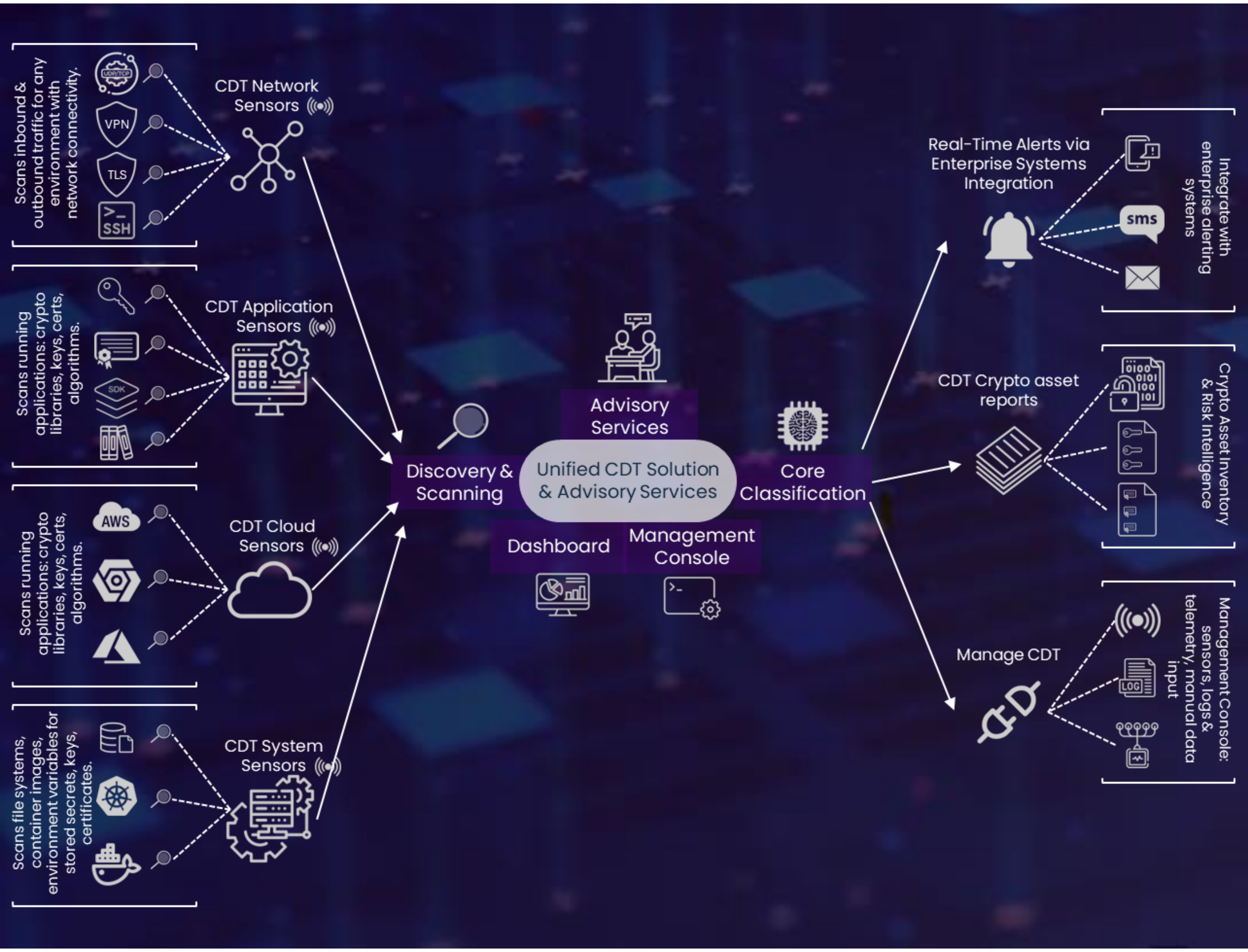
5. Monitor
- **Verify** progress: continuous posture checks
- Evaluate remediation efforts vs. compliance
- Observe and adapt to emerging regulatory changes

QuantumGate's Crypto Discovery Tool

QuantumGate is offering a comprehensive tool for Crypto discovery, inventory and monitoring platform, as well as Advisory services to catalog all crypto assets and highlight cryptographic vulnerabilities and protocol weaknesses.

	Capabilities	Value Proposition
Network Sensor	Scans inbound & outbound traffic for ciphers, handshake parameters, SSL/TLS versions, SSH usage, IPsec settings. Works with AWS, GCP, on-prem HPC, Kubernetes, or any environment with network connectivity	**End-to-End Visibility**: Unified scanning covers network, application, and storage layers
Application Sensor	Examines running applications. Identifies embedded crypto libraries, hardcoded keys, or obsolete algorithms. Flags library versions missing critical patches.	**Reduced Crypto Risk**: Immediately find weak keys (RSA-1024), outdated ciphers (MD5, SHA-1), ECC vulnerabilities and expired certificates. Surfaces misconfigured TLS/SSH protocols
System Sensor Engine	Searches file systems, container images, environment variables for stored secrets, keys, certificates, or config files. Integrates with HSM/KMS solutions for hardware or cloud-based key management	**Streamlined Reporting**: Central dashboard with risk summaries; exportable to DevOps, SIEM, or compliance teams. Helps IT/Sec teams plan next steps efficiently
All sensors	Feed into the unified platform which, together with our Advisory Services, provides transparency of your cryptographic posture and sets you on a path to post-quantum readiness.	**Post-Quantum Readiness**: Identifies which components require upgrades to meet quantum-safe standards. Lays the foundation for a seamless crypto migration

CDT High Level Architecture


Scans inbound & outbound traffic for any environment with network connectivity.
UDP/TCP
VPN
TLS
SSH
CDT Network Sensors
Scans running applications: crypto libraries, keys, certs, algorithms.
SDK
CDT Application Sensors
Scans running applications: crypto libraries, keys, certs, algorithms.
AWS
CDT Cloud Sensors
Scans file systems, container images, environment variables for stored secrets, keys, certificates.
CDT System Sensors
Advisory Services
Discovery & Scanning
Unified CDT Solution & Advisory Services
Core Classification
Dashboard
Management Console
Real-Time Alerts via Enterprise Systems Integration
sms
Integrate with enterprise alerting systems
CDT Crypto asset reports
Crypto Asset Inventory & Risk Intelligence
Manage CDT
LOG
Management Console: sensors, logs & telemetry, manual data input

QuantumGate's Crypto Discovery Tool automates scanning of network protocols, applications, key storage solutions, operating systems and edge platforms to provide a view of cryptographic usage and identify potential vulnerabilities that need to be addressed.

Final Take Aways

Strategic Readiness is Key: The transition to post-quantum cryptography (PQC) is no longer a distant possibility but a pressing necessity. Organizations must recognize this shift as a strategic imperative, integrating quantum readiness into their broader cybersecurity framework.

Begin Your Journey Now: The path to quantum-resistant security is extensive and requires a long-term commitment—often five years or more. Starting early provides a competitive advantage, allowing for careful planning, resource allocation, and the minimization of potential disruptions.

Leverage Expert Tools and Services: Successfully navigating the complexities of PQC demands more than just awareness. Organizations should proactively adopt cryptographic discovery tools and partner with expert service providers to gain visibility into their current cryptographic landscape, assess vulnerabilities, and implement robust migration strategies.

The time to act is now – every step taken today is an investment in a safer, quantum-resistant tomorrow.

quantumgate.ae

contact@quantumgate.ae