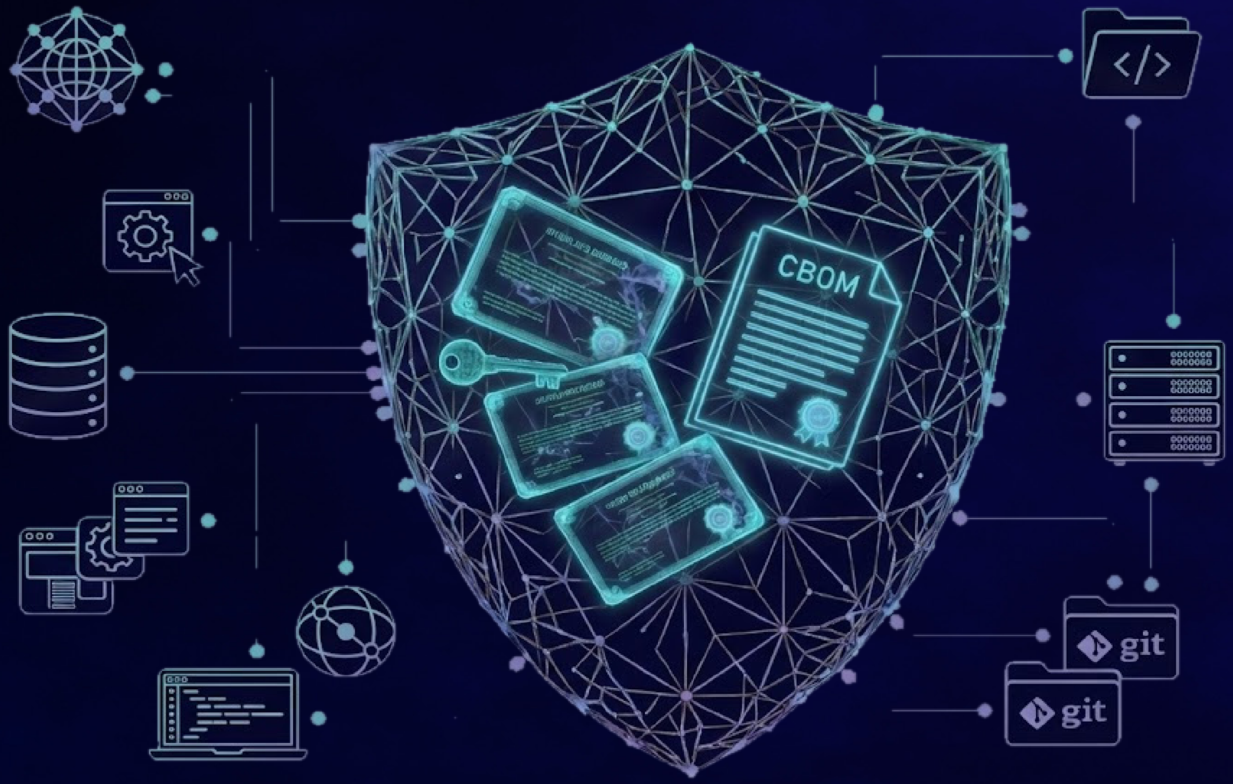
Cryptographic Posture Management

Securing the Digital Foundation for a Quantum-Ready Future.



insight | Public Edition | December 2025

Table of Contents

01. Executive Summary

Cryptography acts as the invisible bedrock of digital trust, securing everything from employee identities and customer authentication and authorization to private APIs and the software supply chain. Yet, in most modern enterprises, this critical infrastructure is managed through a patchwork of fragmented tools, manual processes and siloed ownership models.

This fragmentation creates a "blind spot" that generates two distinct classes of risk. First, Traditional Crypto Debt: immediate operational risks stemming from expired certificates, weak keys, and misconfigurations that lead to outages, breaches, and compliance failures. Second, Quantum-Era Vulnerability: the looming threat posed by powerful enough quantum computers. While Cryptanalytically Relevant Quantum Computers (CRQC) are a future milestone, the risk is active today through "Harvest Now, Decrypt Later" (HNDL) attacks, where adversaries collect encrypted traffic to decrypt once quantum capabilities mature.

As guidance and requirements by standards bodies and regulators on Post-Quantum Cryptography (PQC) are accelerating, organizations can no longer afford to guess where their cryptography resides. This operational imperative has driven the emergence of a new category of enterprise security platforms: Cryptographic Posture Management (CPM).

61% of organizations plan to migrate to post-quantum cryptography in the next 5 years.[1]

At the heart of CPM platforms lies Automated Cryptographic Discovery and Inventory (ACDI), the foundational capability that enables continuous mapping of cryptographic assets across clouds, networks, and code. This metadata is then enriched with org-level context and ownership details and analyzed to assess both traditional and quantum risk. This data can then be used by security and DevOps teams to remediate the highest priority vulnerabilities to improve overall security posture.

This white paper outlines the roadmap to crypto agility. It details how CPM can be leveraged to identify immediate and future risks, automate governance, and transition from a reactive stance to a proactive, quantum-secure posture.

02. The Complexity of Modern Cryptography

Cryptography used to be concentrated in a small number of systems: perimeter VPNs, a few certificate authorities, and well-defined server fleets. Today it is everywhere. Cloud-native architectures introduce ephemeral infrastructure and auto-scaling services. Development teams embed cryptographic libraries into applications. Certificates are minted and rotated by multiple platforms. Secrets and tokens move through CI/CD pipelines, service meshes, and third-party SaaS tools.

The cryptographic estate changes constantly. A quarterly spreadsheet-based inventory is outdated the moment it is produced. Manual audits cannot keep pace with certificate issuance, key rotation, and configuration drift across large fleets. At the same time, critical business functions depend on cryptography

[1] Entrust PKI and Post-Quantum Trends Survey (4,052 respondents)

being correct and consistent; small changes can create availability incidents as easily as they can create security failures.

Ownership is also fragmented. PKI teams manage some certificates, cloud teams manage others, application teams manage libraries, and security teams manage policies. Without a shared, continuously updated system of record, responsibility for remediation is unclear and posture improvements are difficult to measure.

03. The Dual Risk: Crypto Debt and Quantum Vulnerability

Effective Cryptographic Posture Management must address two parallel timelines of risk: the immediate operational threat and the strategic quantum horizon.

3.1 The Immediate Threat: Crypto Debt

Most organizations suffer from accumulated 'crypto debt,' the result of years of deferred maintenance, evolving threats, and shifting cryptographic standards. This manifests as active vulnerabilities—such as expired certificates that cause sudden outages, developers hard-coding secrets into applications, or servers negotiating weak TLS versions. These are not theoretical problems; they are immediate reliability and compliance issues that adversaries can exploit today.

3.2 The Looming Threat: Quantum Computing

Overlaying this is the strategic threat of the quantum era. The public-key algorithms (RSA, ECC) that underpin the modern internet are mathematically vulnerable to future quantum computers. While a stable CRQC is expected in the 2030s, the threat timeline is compressed by HNDL attacks. Adversaries are already scraping encrypted traffic with the intent of decrypting it later, putting long-lifespan data—such as PII, trade secrets, and health records—at risk immediately. Furthermore, transitioning an enterprise to PQC is a multi-year endeavor. Organizations that fail to inventory and plan now will find themselves struggling to meet impending regulatory deadlines.

Cryptographic Risk Types, Examples and Impact

Risk Type	Examples	Typical Impact
• Traditional Weaknesses	• Deprecated protocols (SSL, TLS 1.0/1.1), weak keys (RSA <2048), unencrypted endpoints, expired certs.	• Data breaches, service outages, compliance failures (PCI-DSS, HIPAA).
• Supply-Chain Exposure	• Unsigned artifacts, unmanaged or improperly rotated code signing keys and pipeline secrets.	• Release tampering risk; integrity loss.
• Quantum-era Vulnerability	• RSA/ECC usage where long-term confidentiality is required (e.g., trade secrets, PII).	• “Harvest Now, Decrypt Later” – Future decryption of data captured today.
• Crypto Agility Gaps	• Hard-coded algorithms, unknown dependencies, inflexible libraries.	• Slow, costly migration; high risk of downtime during updates.

04. From Inventory to Posture

Automated Cryptographic Discovery and Inventory (ACDI) represents the mechanism of collection. It is the process of continuously scanning networks, file systems, cloud environments, databases, key management service (KMS), Hardware Security Module (HSM), code repositories and more to identify every instance of cryptography. This process produces a Cryptographic Bill of Materials (CBOM), a machine-readable standard that enumerates algorithms, key lengths, libraries, and dependencies. CBOMs can be generated for each source type, and typically follow a standardized format such as CycloneDX v1.6/1.7.

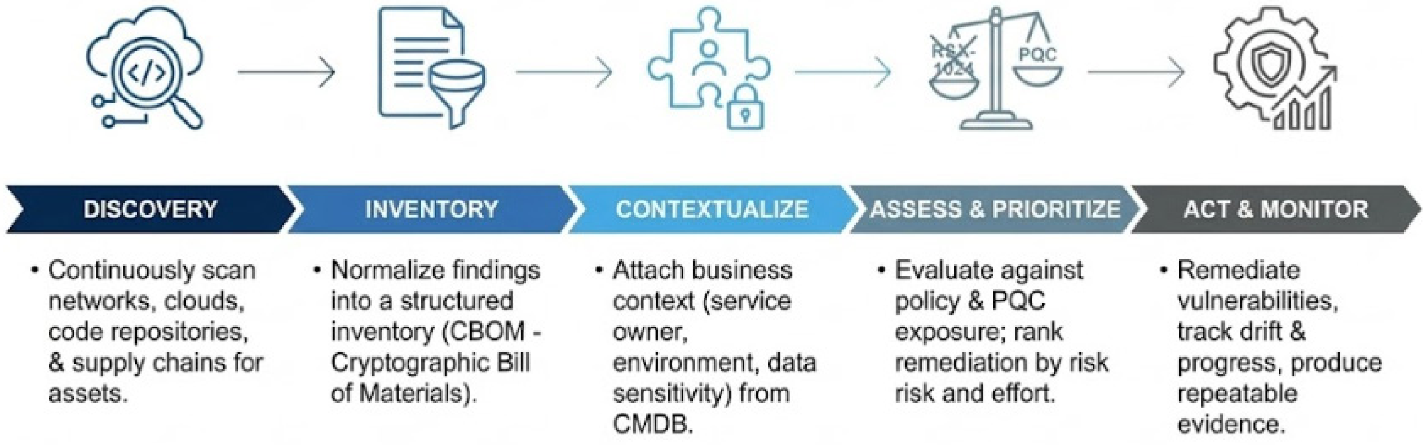
Just as the industry adopted Cloud Security Posture Management (CSPM) to secure cloud infrastructure and Data Security Posture Management (DSPM) to protect sensitive data assets, Cryptographic Posture Management (CPM) has emerged as a necessary tool to secure the fundamental 'trust layer' that underpins them both. CPM platforms provide an end-to-end solution that not only discovers and inventories cryptography but also enriches and analyzes the entire cryptographic estate to turn raw data into actionable insights and ensures continuous compliance.

05. The Scope of Inventory: Beyond the Certificate

A common misconception is equating "Cryptographic Inventory" solely with the discovery of external SSL/TLS certificates. While certificates are critical, they represent only the surface of the cryptographic estate. True CPM requires deep visibility across the entire technology stack to identify "shadow crypto," hard-coded dependencies, and unmanaged secrets.

A comprehensive inventory must segment cryptographic risk across three critical domains: Data in Motion, Data at Rest, and the Software Supply Chain.

Cryptographic Posture Management Workflow



DISCOVERY

- Continuously scan networks, clouds, code repositories, & supply chains for assets.

INVENTORY

- Normalize findings into a structured inventory (CBOM - Cryptographic Bill of Materials).

CONTEXTUALIZE

- Attach business context (service owner, environment, data sensitivity) from CMDB.

ASSESS & PRIORITIZE

- Evaluate against policy & PQC exposure; rank remediation by risk risk and effort.

ACT & MONITOR

- Remediate vulnerabilities, track drift & progress, produce repeatable evidence.

5.1 Data in Motion (Network Cryptography)

This domain encompasses the cryptographic protocols and handshakes that secure communications between users, servers, and services. It is often the most visible layer but also the most prone to configuration drift and legacy protocol support.

- **Protocol & Cipher Negotiation:** Inventorying not just the presence of encryption, but the quality of the connection. This includes detecting deprecated protocols (TLS 1.0/1.1, SSL v3), weak cipher suites (e.g., those using CBC mode or RC4), and insecure key exchange parameters.
- **Internal & East-West Traffic:** Moving beyond the perimeter to inventory internal API traffic, Service Mesh (mTLS) configurations, and SSH key usage for administrative access.
- **Non-Web Protocols:** capturing cryptography in database connections, VPNs (IPsec), and file transfer protocols (SFTP/FTPS), which often escape standard web scanners.

5.2 Data at Rest & Managed Infrastructure

Cryptography at rest involves the protection of inactive data and the secure management of the keys that protect it. This area is critical for preventing data breaches and ensuring the long-term integrity of sensitive records.

- **Managed Cryptography (KMS & HSMs):** This involves inventorying keys residing in Key Management Systems (KMS), Hardware Security Modules (HSMs), and cloud vaults. This includes tracking key rotation policies, usage logs, and the hardware root-of-trust configurations.
- **Storage & Database Encryption:** Identifying encryption configurations for cloud storage buckets, block storage volumes, and database-level encryption (TDE).
- **Keystores & Trust Stores:** Locating scattered cryptographic artifacts such as Java Keystores (JKS), PKCS#12 files, and local trust stores on servers, which are frequent hiding spots for unmanaged private keys and expired root certificates.

5.3 The Software Supply Chain (Application Cryptography)

Perhaps the most opaque and risky domain, this covers the cryptography embedded directly into the applications and libraries that power the business. This is where "crypto debt" accumulates most heavily in the form of hard-coded secrets and obsolete algorithms.

- **Cryptographic Libraries:** Identifying which libraries (e.g., OpenSSL, Bouncy Castle) are linked to software, including their specific versions. This is vital for rapidly identifying vulnerability exposure (e.g., Heartbleed-style events).
- **Embedded Algorithms & Calls:** Scanning source code and compiled binaries to detect specific calls to cryptographic primitives (e.g., AES-256, RSA-1024). This enables teams to flag quantum-vulnerable algorithms hard-coded by developers.
- **Code Signing & CI/CD Secrets:** Inventorying the keys and certificates used to sign software artifacts and securing the secrets used within build pipelines. Unmanaged signing keys represent a critical supply chain risk that can lead to release tampering.

Note: The domains outlined above are not an exhaustive catalog of every possible cryptographic instance. Instead, they serve as a strategic framework—a way to bucket and conceptualize the vast, often invisible, cryptographic dependencies that exist across a modern digital estate.

06. Risk and Prioritization: Context is King

An inventory containing thousands of cryptographic assets provides little value without context. A CPM provides a risk-based prioritization model, where assets are evaluated not just on their technical specifications, but on their business impact and implementation context. A weak key on an isolated test server is merely a hygiene issue, whereas the same weak key on a payment gateway represents a critical incident.

Prioritization must therefore account for several interdependent dimensions:

Data Sensitivity & Exposure. Evaluating whether the asset protects high-value targets like PII or IP, and determining if the system is internet-facing or air-gapped.

Usage & Mode of Operation. Risk is not binary; it depends on how a key is applied. A strong algorithm (e.g., AES-256) is rendered insecure if implemented in a vulnerable mode (e.g., ECB vs. GCM). Similarly, the impact of compromise varies by usage: a compromised signing key undermines trust and integrity, potentially allowing code tampering, while a compromised encryption key results in immediate confidentiality loss.

HNDL Relevance. Assessing the specific "Harvest Now, Decrypt Later" risk for data with a long lifespan (e.g., health records or trade secrets) versus ephemeral session data.

Crypto-Agility. Whether a key can be rotated automatically or requires complex code refactoring plays a major role in determining the urgency and cost of remediation.

07. Strategic Benefits and Operational ROI

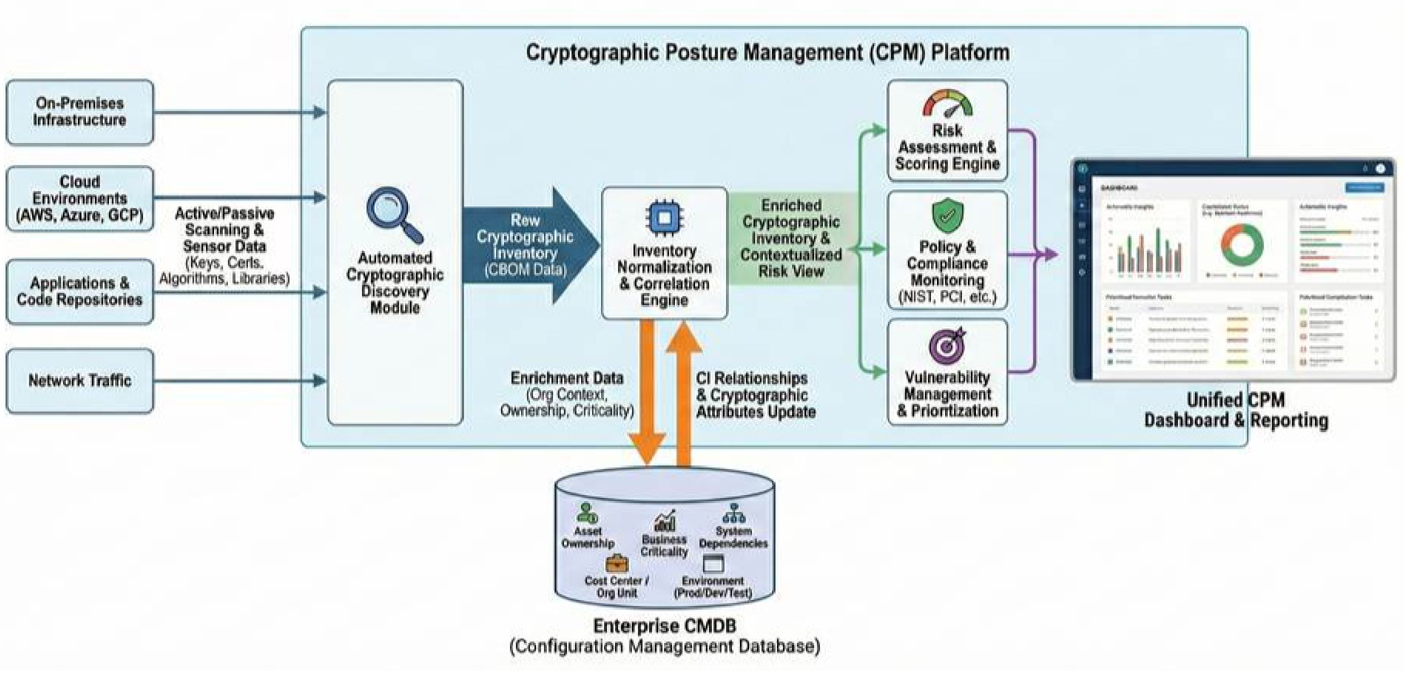
Implementing CPM delivers immediate value far beyond future quantum preparation. By transforming cryptography from an opaque technical dependency into a managed, measurable capability, organizations can secure their digital foundation today while building the roadmap for tomorrow.

This operational maturity drives ROI across four critical pillars:

7.1 Operational Resilience & Agility

The primary driver for most organizations is the elimination of "self-inflicted" outages and the acceleration of development velocity.

- **Zero-Downtime Operations:** Automated discovery eliminates the common causes of outages, such as expired certificates or broken trust chains. It moves the organization from a manual or fragmented posture to an operational capability that handles key and certificate rotations safely at scale.


Cryptographic Posture Management (CPM) Platform
On-Premises Infrastructure
Cloud Environments (AWS, Azure, GCP)
Applications & Code Repositories
Network Traffic
Active/Passive Scanning & Sensor Data (Keys, Certs, Algorithms, Libraries)
Automated Cryptographic Discovery Module
Rew Cryptographic Inventory (CBOM Data)
Inventory Normalization & Correlation Engine
Enriched Cryptographic Inventory & Contextualized Risk View
Risk Assessment & Scoring Engine
Policy & Compliance Monitoring (NIST, PCI, etc.)
Vulnerability Management & Prioritization
Unified CPM Dashboard & Reporting
Enrichment Data (Org Context, Ownership, Criticality)
CI Relationships & Cryptographic Attributes Update
Asset Ownership
Business Criticality
System Dependencies
Cost Center / Org Unit
Environment (Prod/Dev/Test)
Enterprise CMDB (Configuration Management Database)

- **Agility in Software Development:** CPM platforms treat cryptography as a core software supply chain dependency. By identifying embedded crypto libraries and hard-coded algorithms early, engineering teams can modernize code without breaking builds, effectively treating "crypto debt" like technical debt.

7.2 Risk Reduction & Security Architecture

Visibility is the precursor to security. A unified inventory allows security teams to validate their architecture and respond to threats faster.

- **Enabling Zero Trust Architecture:** Zero Trust relies entirely on strong machine identity (mTLS, certificates) and pervasive encryption. CPM provides the essential verification that these identities are valid, compliant, and under control—turning "Verify, Never Trust" from a slogan into an enforceable reality.
- **Faster Vulnerability Response:** When new vulnerabilities emerge, teams can instantly identify which systems, protocols, or certificates are affected. This intelligence feeds directly into vulnerability management, drastically reducing Mean Time to Remediate (MTTR).
- **Proactive Weakness Identification:** Continuous monitoring detects weak configurations—such as legacy protocol versions (TLS 1.0/TLS 1.1) or unencrypted endpoints—allowing for remediation before they result in a breach or compliance failure.

7.3 Strategic Governance & Future Readiness

Long-term resilience requires aligning internal posture with external mandates and future technology shifts.

- **Audit Velocity & Compliance:** Organizations can replace weeks of manual evidence gathering with instant, exportable CBOMs. As regulators publish new guidance, a current inventory becomes a repeatable source of truth for internal assurance.
- **Supply Chain Accountability:** Inventory-driven controls allow enterprises to hold vendors accountable. Organizations can validate supplier practices, request Cryptographic Bills of Materials (CBOMs), and enforce shared responsibility models.
- **Foundation for PQC Transition:** Visibility grounds PQC planning in reality. By quantifying where quantum-vulnerable mechanisms protect high-value data, organizations can build a phased migration plan based on actual business risk.

7.4 The Financial Case: ROI & Cost Avoidance

Data indicates that a proactive approach to cryptographic management is significantly more cost-effective than reactive modernization.

- **The "Cost of Inaction" Multiplier:** Financial modeling based on the PQFIF[2] suggests that delaying cryptographic modernization leads to exponential cost increases. Early implementation costs are estimated to be a fraction of reactive migration costs (projected at 5x higher) or emergency response scenarios (projected at 50x higher) following a cryptographic breakthrough.
- **The Automation Dividend:** Manual cryptographic discovery is labor-intensive and error-prone. Industry analysis indicates that automated discovery and planning tools can reduce total migration costs by 30-50% compared to manual methods, while simultaneously freeing up engineering resources for high-value tasks.
- **Preventing Remediation Costs:** Beyond direct savings, CPM avoids the catastrophic costs associated with "Harvest Now, Decrypt Later" (HNDL) attacks. Furthermore, with new SEC cybersecurity rules, verifying cryptographic posture reduces potential Director & Officer (D&O) liability for failing to mitigate known risks.

Together, these benefits turn cryptography from an opaque technical dependency into a managed, measurable capability—supporting both day-to-day resilience and long-horizon quantum readiness.

[2] Estimate based on the U.S. Crypto Assets Task Force (SEC): Post-Quantum Financial Infrastructure Framework (PQFIF) (2025).

08. Aligning CPM to Governance and PQC Roadmaps

CPM is most effective when treated as a strategic governance capability rather than a standalone technical project. True governance is the bridge between written policy and technical reality. By aligning cryptographic posture with enterprise risk frameworks, organizations transition from reactive cleanup to proactive assurance.

Governance in a CPM context operates as a continuous cycle of Validation, Customization, and Assurance:

8.1 Establishing the Baseline (Validation)

Before policy can be enforced, the environment must be measured. You cannot govern what you cannot see. Teams use the inventory to establish a trusted baseline—validating where encryption is enforcing critical services and quantifying the exact spread of quantum-vulnerable mechanisms. This creates the evidence foundation required to justify remediation budgets and track progress.

8.2 Policy Customization

Governance is not "one size fits all." Policies must be tuned to the specific regulatory landscape and data sensitivity of the organization:

- **Financial Services:** Policies heavily prioritize strict key rotation schedules and HSM usage to prevent fraud and meet payment card standards.
- **Healthcare:** Governance focuses on long-term data confidentiality (e.g., 20+ years), ensuring patient records remain unreadable to unauthorized parties—a critical defense against "Harvest Now, Decrypt Later" attacks.
- **Government & Defense:** The priority shifts toward strict adherence to federally approved algorithms and explicit mandates for PQC migration timelines.

8.3 Continuous Compliance.

Traditional audits are point-in-time snapshots that often miss configuration drift. CPM enables "Continuous Compliance," where the distance between Policy (what you say you do) and Posture (what is actually running) is monitored in real-time. This allows teams to detect non-compliant instances—such as a developer accidentally deploying a self-signed certificate to production—the moment they appear.

Strategic Alignment Frameworks

Framework / Standard	Governance Objective	CPM Action
• NIST Security Outcomes	• Tie security posture to standardized federal metrics.	• Map inventory coverage and remediation progress directly to NIST categories (Identify, Protect, Detect).
• Audit & Control Evidence	• Move from manual sampling to continuous validation.	• Use automated inventory exports and posture checks as repeatable artifacts for key management controls.
• CNSA 2.0 (U.S. NSS)	• Mandate PQC migration for National Security Systems.	• Deadline 2025: Ensure no new quantum-vulnerable crypto is deployed. • Deadline 2030: Complete migration of all vulnerable encryption.
• EU PQC Roadmaps	• Coordinate readiness across member states and industries.	• Sequence readiness activities (inventory -> pilots -> hybrid transition) with milestone-based reporting.

09. Qinsight Atlas: Modern Cryptographic Posture Management

Qinsight Atlas moves beyond static inventory to provide dynamic CPM. It helps security teams eliminate immediate crypto debt—such as weak encryption, deprecated algorithms, and unencrypted endpoints—while simultaneously architecting the defense against quantum-era threats. By treating cryptography as a managed asset rather than invisible infrastructure, Atlas transforms compliance from a burden into a continuous assurance capability.

9.1 What Differentiates Qinsight Atlas

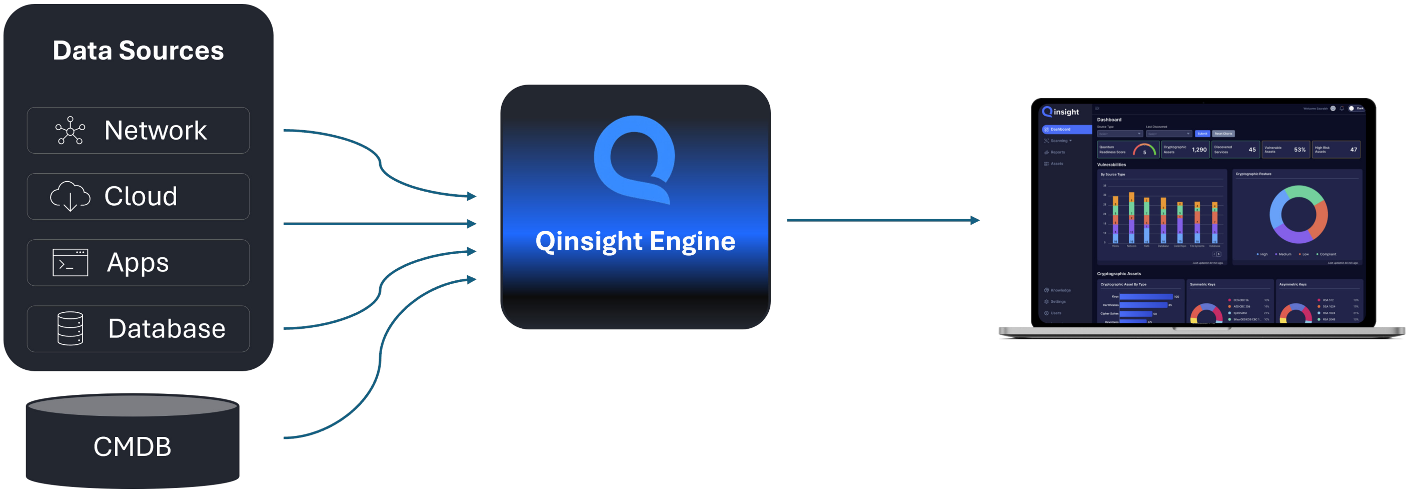
Deep Context & Automated Enrichment. Raw inventory data is often noisy and disconnected from business reality. Atlas solves this by integrating with your CMDB, cloud tags, and directory services to automatically enrich every cryptographic finding. It correlates a technical artifact (e.g., an RSA-2048 key) with its business context—identifying the System Owner, Data Sensitivity Level, and Application Criticality. This ensures remediation teams aren't just chasing files; they are securing business processes.

Multi-Dimensional Risk Scoring. Most tools stop at identifying the algorithm. Atlas goes deeper, evaluating risk based on Usage and Mode of Operation. It distinguishes between a key used for encryption (confidentiality risk) versus digital signing (integrity risk) and flags dangerous implementations—such as strong algorithms used in weak modes (e.g., AES in ECB mode). This granular scoring prevents false positives and focuses engineering effort on the vulnerabilities that actually threaten the organization.

Industry-Adaptive Policy Frameworks. Governance is pre-built, not starting from scratch. Atlas includes tailored policy packs designed for highly regulated industries. Whether you need to enforce PCI-DSS key rotation schedules in FinTech, long-lifespan data protection for Healthcare (HNDL defense), or CNSA 2.0 compliance for Government, Atlas automatically maps your inventory against sector-specific mandates, highlighting violations the moment they occur.

Unified "Dual-Risk" Visibility. The only platform designed to manage the timeline of cryptographic transition. Atlas provides a unified dashboard that quantifies traditional crypto debt (expired certificates, TLS 1.0) alongside Quantum-Era Exposure (HNDL risk). This allows leaders to visualize their PQC migration readiness without losing sight of today's hygiene requirements.

Integration-First Ecosystem. Built for the complex enterprise, Atlas utilizes an API-first architecture that connects seamlessly with existing scanning infrastructure, HSMs, and CI/CD pipelines. This ensures comprehensive visibility without the need for disruptive agent deployments or architectural overhaul.



10. Conclusion

The transition to Post-Quantum Cryptography represents one of the largest security migrations in history, and it cannot be managed with spreadsheets. The risk is no longer theoretical; between the immediate operational drag of "crypto debt" and the strategic threat of "Harvest Now, Decrypt Later," the cost of inaction is rising daily.

The safest path forward is also the most logical: know what you have. By implementing Cryptographic Posture Management (CPM) today with Qinsight Atlas, organizations can secure their digital foundation for the quantum era without disrupting business velocity.

Glossary & References

Glossary

ACDI: Automated Cryptographic Discovery and Inventory. Continuous identification and documentation of cryptographic assets and configurations.

CBOM: Cryptographic Bill of Materials. Structured representation of cryptographic mechanisms present in software and/or environments.

CPM: Cryptographic Posture Management. Assessing crypto strength/compliance, prioritizing remediation, and tracking progress.

CRQC: Cryptanalytically Relevant Quantum Computing. Quantum capability sufficient to break widely used public-key cryptography.

Crypto agility: Ability to change cryptographic algorithms/configurations without major redesign or prolonged downtime.

HNDL: Harvest Now, Decrypt Later.

NSS: National Security Systems

PQC: Post-Quantum Cryptography. Algorithms designed to resist known quantum attacks.

References

- NIST NCCoE: *Migration to Post-Quantum Cryptography (PQC), CSWP 48* (Initial Public Draft, 2025).
- NIST: *FIPS 203, 204, and 205, Post-Quantum Cryptography Standards* (Finalized August 2024).
- White House: *National Security Memorandum 10 (NSM-10), Promoting United States Leadership in Quantum Computing.*
- NSA: *Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) policy guidance* (2024-2025).
- European Union: *Digital Operational Resilience Act (DORA), Regulatory Standards* (2025).
- U.S. Crypto Assets Task Force (SEC): *Post-Quantum Financial Infrastructure Framework (PQFIF)* (2025).
- FS-ISAC: *Post-Quantum Cryptography: A Guide for the Financial Sector* (2025).