



From Noise to Clarity: Adding Intelligence to the PQC Migration

James Howe
Head of Cryptography

Presentation outline

1

- **The 'Haystack' Challenge**

Why traditional discovery methods can result in noisy inventories.

2

- **A New Approach**

Integrated discovery and management, utilizing existing infrastructure.

3

- **Real-World Insights**

Practical lessons learned.

4

- **Achieving Agility**

Outcomes and the path forward.

The Global Mandate for PQC Readiness

Governments and security agencies worldwide have issued a clear and urgent mandate: **prepare for the quantum threat**



Following [NSM-10](#), the goal is to mitigate quantum risk by 2035, starting with a complete inventory.



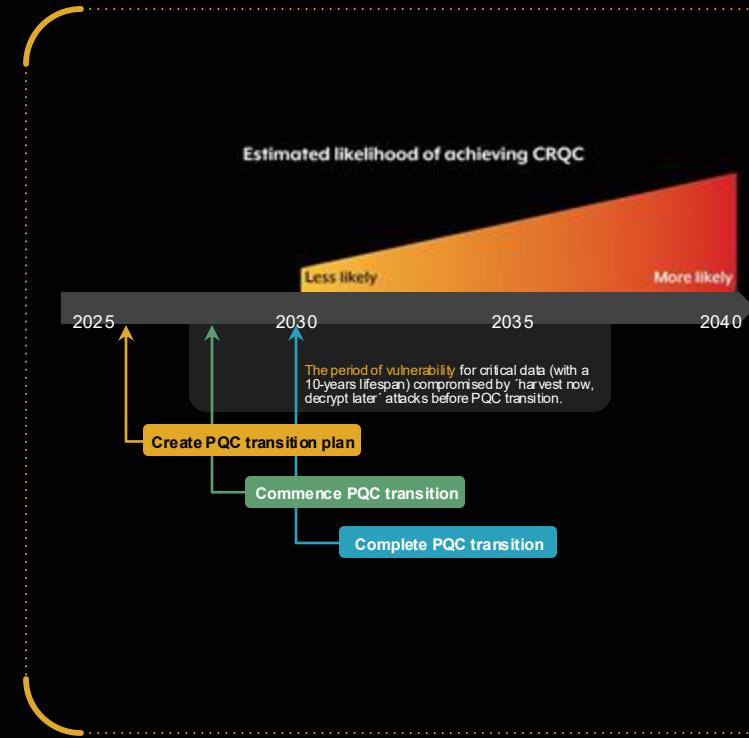
The [NCSC](#) has also set a 2035 target date for completing the PQC transition.



[ACSC](#) has issued guidance for organizations to begin planning their migration, starting with a complete cryptographic inventory.



The [EU](#) roadmap calls a cryptographic inventory an "essential step and 'no-regret' move" for every organization.



The PQC Migration Imperative

The quantum threat and the urgent need for PQC.

PQC migration

A complex, multi-faceted challenge for large enterprises.



Vast, distributed IT environments



Numerous legacy systems and cryptography



Fragmented software ecosystem



Disparate and diverse hardware



The PQC Migration Imperative

The quantum threat and the urgent need for PQC.

PQC migration

A complex, multi-faceted challenge for large enterprises.



Vast, distributed IT environments



Numerous legacy systems and cryptography



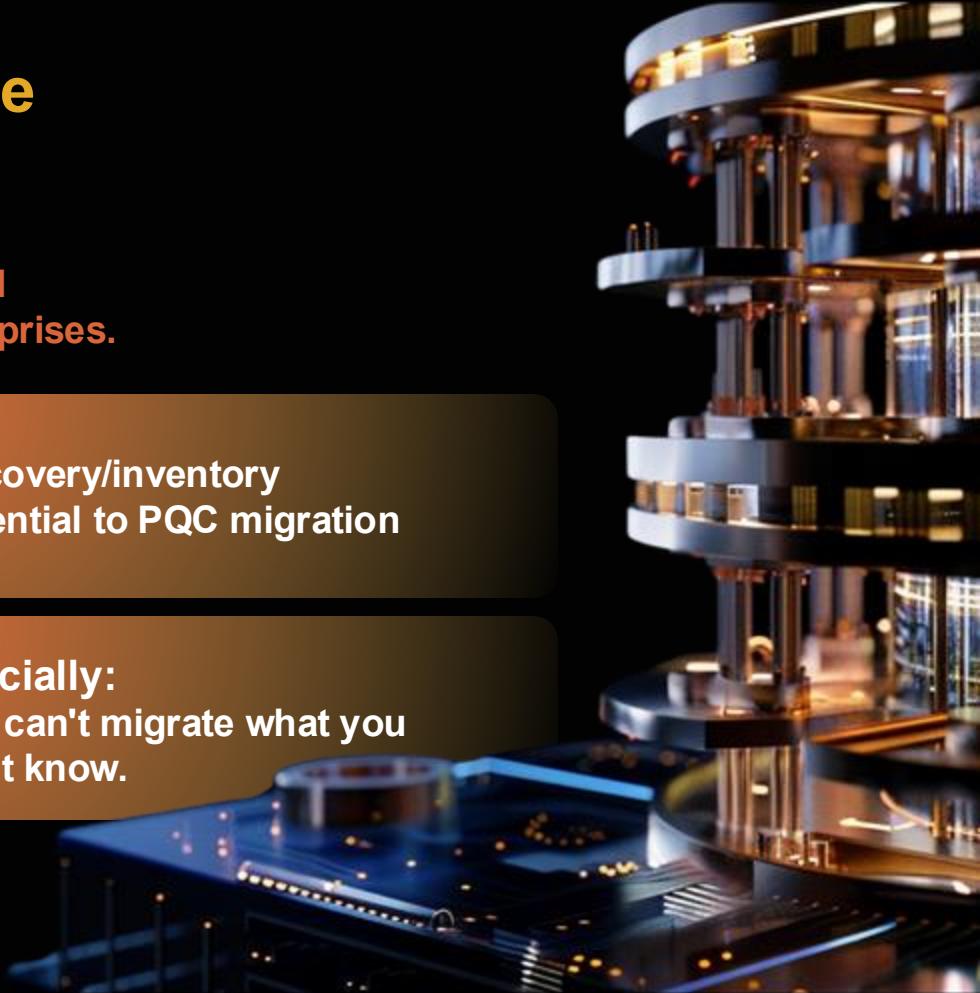
Fragmented software ecosystem



Disparate and diverse hardware

**Discovery/inventory
essential to PQC migration**

**Crucially:
You can't migrate what you
don't know.**



Deepening Insight

Practical Integrations with Key Tools



Holistic approach

Bridges data silos for unparalleled cryptographic visibility.



Creates overall data landscape map, leveraging CMDBs and other tool insights.



Import certificate, secrets & TLS configs to analyze potential crypto. vulnerabilities & misconfigurations



Orchestrates filesystem scanning to enable seamless scanning of remote hosts.



Ingest certificate/asset data from its CMDB capabilities for centralized management & enhanced security posture



Ingest data to enhance key management and security monitoring.



Ingest and analyze TLS handshake data from Next-Generation Firewall log files.



Cryptography Bill of Materials

Upload/analyze CBOMs for comprehensive insight.

Lessons from the Field

Customer-Driven Innovation



Customer feedback revealed key pain points

- High operational overhead managing numerous, siloed security agents.
- Drove the development of 3rd party ingestion for faster time-to-value, optimizing sensor deployment.
- Reduced alert fatigue via unique alerts.
- Enabled flexible asset profiling.



This feedback loop was critical for refining the solution.



Moved from "what we thought was needed" to **"what customers actually need."**

The screenshot shows a dark-themed user interface for managing data sources. It features a grid of cards, each representing a different data source provider. Each card includes the provider's logo, name, a brief description, and a 'DETAILS' button. Some cards also have an 'UPLOAD' or 'LEARN MORE' button. The providers listed are Qualys, CrowdStrike, ServiceNow, AWS KMS, Palo Alto Networks, CBOM, AQG Network Analyzer, AQG Java Tracer, and File System Scanner.

Data Sources		
Qualys	CrowdStrike	ServiceNow
Import Qualys data for secrets, certificates, and TLS handshakes for vulnerability management and security monitoring.	Import CrowdStrike data and deploy AQG sensors for unified endpoint monitoring and advanced threat intelligence.	Import ServiceNow data for centralized certificate management and enhanced security posture.
DETAILS	DETAILS	DETAILS
AWS Amazon Web Services KMS	Palo Alto Networks	CBOM
Import AWS KMS data for enhanced key management and security monitoring.	Import network logs to monitor TLS handshakes and security posture.	Import Cryptographic Bill of Materials (CBOM) 1.4 and 1.6 for cryptographic static code analysis of applications.
DETAILS	DETAILS	DETAILS
AQG Network Analyzer	AQG Java Tracer	File System Scanner
Identifies the encryption methods used to secure data during network transmission.	Logs cryptographic calls made by a Java application running on a JVM.	Scans the filesystem or a container image for cryptographic objects and formats the information for analysis by AQGuard.
LEARN MORE	UPLOAD	UPLOAD

The Next Challenge: A High-Fidelity Haystack



While integration achieves comprehensive discovery, it introduces the challenge:

actionable intelligence by filtering out the noise.

We now have all the data, but it's still just data. A unified inventory can contain hundreds of thousands of cryptographic objects.



Endpoints

A clean Windows installation alone contains **200-300** keys & certs.



Applications

Each application adds another **1-10** objects.



Infrastructure

Devices like load balancers and firewalls generate **5-10** objects per node.



Supply Chain

A typical enterprise starts with thousands of third-party objects *before counting a single asset generated for its own internal applications.*

The Next Challenge: A High-Fidelity Haystack

This massive scale leads to the critical question:

"How do I see from this haystack the things that I need to change?"

Inventories are full of noise, this isn't a discovery issue but a contextual one.

Some examples:

Weak keys in a developer's sample code.

Deprecated CAs in a standard Linux trust store.

Certificates managed by a third-party application you can't control.

A legacy root cert in a standard OS trust store that uses a deprecated signature algorithm.

A weak TLS cipher suite offered by a third-party API your organization consumes.

The Solution: From Haystack to Actionable Insight

So, how do we find the needles in this high-fidelity haystack?

- ◆ The answer isn't more data; it's **more intelligence**.
- ◆ We can solve this problem with intelligent triage, powered by an enrichment engine.
- ◆ This engine is powered by a database built from millions of publicly known assets from OSs, containers, and applications
- ◆ This is the baseline, and can be further enriched by path, location, common CAs, etc.

Example:
The Weak Key Problem

A scanner finds a weak 512-bit RSA key.
Is this a Critical threat?

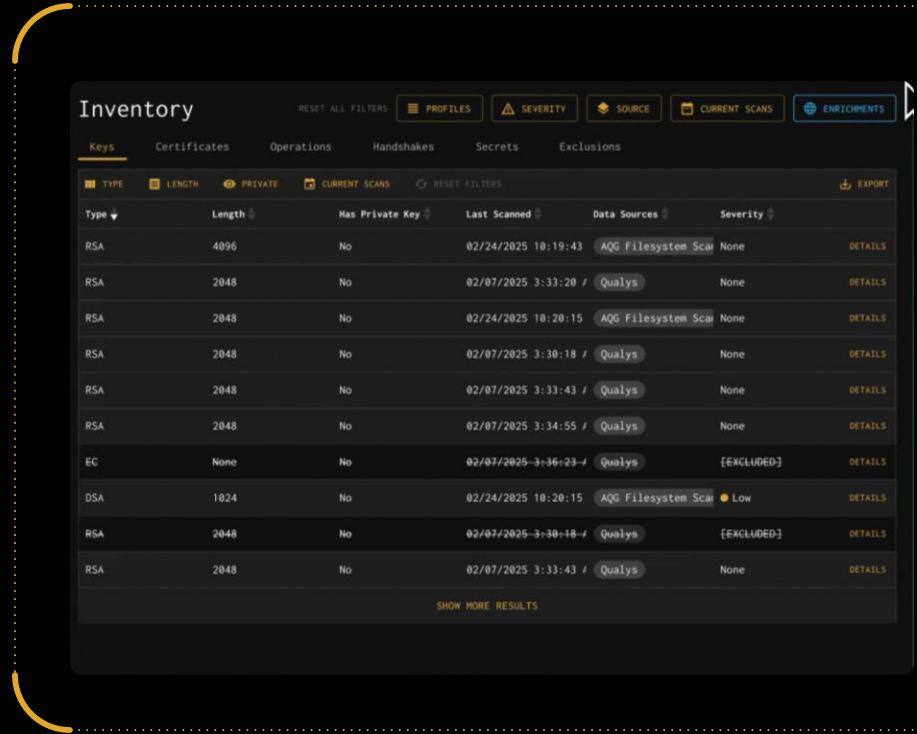
Enrichment could show this in developer sample code, gets removed.

But that same key found in a production environment is a huge issue!

The Impact of Enrichment

So, how do we find the needles in this high-fidelity haystack?

- ◆ The answer isn't more data; it's **more intelligence**.
- ◆ We can solve this problem with intelligent triage, powered by an enrichment engine.
- ◆ This engine is powered by a database built from millions of publicly known assets from OSs, containers, and applications.
- ◆ This is the baseline, and can be further enriched by path, location, common CAs, etc.



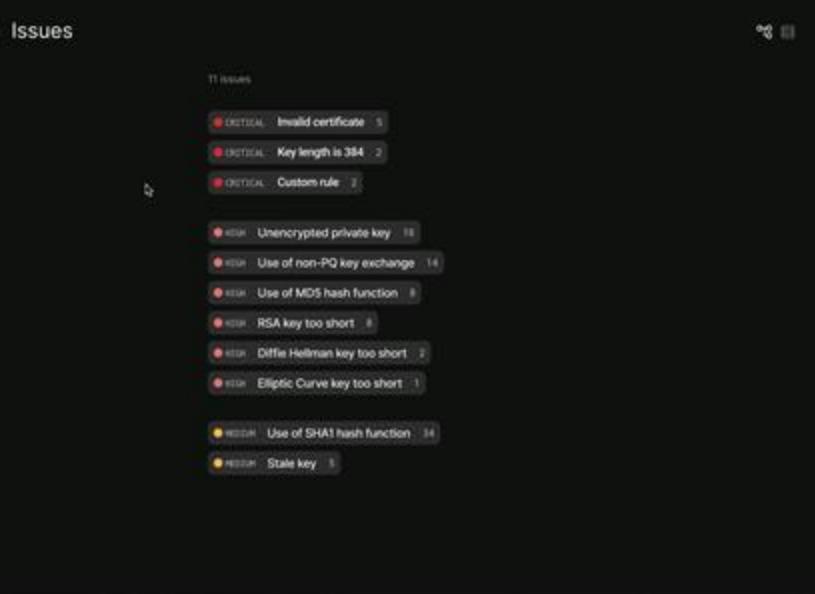
The screenshot shows a "Inventory" page with a table of assets. The columns include Type, Length, Has Private Key, Last Scanned, Data Sources, and Severity. The table lists various RSA keys and one EC key, with details like scan times (e.g., 02/24/2025 10:19:43) and sources (e.g., AQG Filesystem Scan). Some rows have a "Qualys" status indicator. A "DETAILS" link is visible next to each row. At the bottom, there's a "SHOW MORE RESULTS" button.

Type	Length	Has Private Key	Last Scanned	Data Sources	Severity	
RSA	4096	No	02/24/2025 10:19:43	AQG Filesystem Scan	None	DETAILS
RSA	2048	No	02/07/2025 3:33:20	Qualys	None	DETAILS
RSA	2048	No	02/24/2025 10:20:15	AQG Filesystem Scan	None	DETAILS
RSA	2048	No	02/07/2025 3:38:18	Qualys	None	DETAILS
RSA	2048	No	02/07/2025 3:33:43	Qualys	None	DETAILS
RSA	2048	No	02/07/2025 3:34:55	Qualys	None	DETAILS
EC	None	No	02/07/2025 3:36:23	Qualys	[EXCLUDED]	DETAILS
DSA	1024	No	02/24/2025 10:20:15	AQG Filesystem Scan	Low	DETAILS
RSA	2048	No	02/07/2025 3:38:18	Qualys	[EXCLUDED]	DETAILS
RSA	2048	No	02/07/2025 3:33:43	Qualys	None	DETAILS

Enhancing Insight

Advanced Intelligence & Actionable Filtering

-  Intelligent filtering reduces noise, delivering advanced insights with broader context.
-  Deep enrichments provide rich context to: "Is this crypto mine? Do I care?"
-  Transforms raw data into a clear, prioritized action plan for PQC migration.
-  Eliminates days/weeks of manual investigation by providing rich context.
-  Alleviates alert fatigue by focusing security teams on a clear, prioritized list of issues.



The screenshot shows a user interface titled "Issues" with a subtitle "11 issues". The list is organized into four columns based on severity:

Severity	Description	Count
CRITICAL	Invalid certificate	5
CRITICAL	Key length is 384	2
CRITICAL	Custom rule	2
HIGH	Unencrypted private key	10
HIGH	Use of non-PQ key exchange	14
HIGH	Use of MD5 hash function	1
HIGH	RSA key too short	1
HIGH	Diffie Hellman key too short	2
HIGH	Elliptic Curve key too short	1
MEDIUM	Use of SHA1 hash function	34
LOW	Stale key	1

Announcing: *OpenCryptography.com*

Today, we're excited to launch a new initiative for the security and developer communities.



What It Is: A new public website providing open access to a searchable database of cryptographic issues found within public software artifacts.



The Mission: To provide a central, public resource for security professionals, developers, and researchers to search and analyze the cryptographic security of the tools they use every day.



Launching with: An analysis of the cryptographic security of the most popular images on Docker Hub.

A screenshot of the OpenCryptography.com homepage. The page features a header with the logo 'OPEN CRYPTOGRAPHY' and 'Powered by AQteve.Guard'. It includes a search bar and navigation links for 'About', 'Learn', 'Feedback', and 'Book a demo'. The main content area has a light blue background with large, overlapping orange and blue circles. The text 'Uncover the Internet's cryptographic DNA' is prominently displayed. Below it, a subtext reads: 'Explore our free public database of 10,000+ unique Docker image scans for hidden cryptographic assets and critical implementation flaws that traditional scanners often miss.' A 'Learn more' link is provided. At the bottom, logos for 'alpine' (Linux), 'debian', 'NGINX', and 'Ubuntu' are shown.

From Clarity to Agility: Accelerating the PQC Transition

Achieving a clear, prioritized inventory isn't the end goal; **it's the catalyst that makes a successful PQC migration possible.**



Transforms the Timeline: turns the PQC migration from a multi-year "archeological dig" into a focused, manageable engineering project. **You can now scope, plan, and execute in months, not years.**



Enables Prioritized Remediation: removes chaos by enabling you to surgically target your highest-risk systems and dependencies first.



Establishes Long-Term Readiness: Builds the visibility and control needed to defend against the quantum threat and all future cryptographic challenges.



Thanks for listening!

Any questions?