PATERO
QUANTUM SECURE COMMUNICATIONS

CHALLENGE

To withstand modern cyberattacks, including quantum threats, today's cryptographic products, protocols, and services need to be updated, replaced, or significantly altered. Cryptographic libraries, however, can be difficult to inventory.

SOLUTION

As part of a structured cryptographic migration strategy, NIST and other government agencies (e.g. DHS, CISA) recommend:

- Defining vulnerabilities in operational networks
- Characterizing cryptographic libraries in hardware, software, applications and services
- Assessing vulnerabilities to build a remediation playbook

PATH FORWARD

Patero cryptographic migration suite enables organizations to create and execute crypto-migration strategies that align with NIST recommendations and remediate vulnerabilities creating risk to operational resilience. Patero technologies are dual-use and designed to work across a broad range of compute options.

PANOQOR™

Cryptographic Inventory and Quantum Risk Assessment

CISA, NSA, and NIST - DRIVING QUANTUM SECURITY

The Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the National Institute of Standards and Technology (NIST) are pushing planning for migration to postquantum cryptographic standards — especially for organizations in Critical Infrastructure Sectors.

CREATING AND MAINTAINING A CRYPTOGRAPHIC INVENTORY

- Become quantum-ready — a state where a CRQC is not a threat,
- Prepare a transition to zero trust architecture,
- Identify outside access to dataset and at higher risk, and
- Identifying data at risk for "steal now and decrypt later" attacks

Meets all CISA Requirements

- Discovery
- Inventory
- Harvest Now, Decrypt Later vulnerabilities
- Visibility of all cryptography
- Identify embedded cryptography
- Correlate cryptographic inventory
- Prioritization of key assets

Why Is this Important?

- Organizations may not be aware of the breadth and scope of their
- dependencies on public key infrastructure
- Cryptography is embedded or hard-coded in products and services
- Many organizations do not have the personnel to execute these tasks

Business Benefits

PanoQoR combines network scanning with analytic capabilities to help organizations structure cryptographic migration strategies through a data-driven framework. PanoQoR technologies enable:

- Complete inventory of cryptography algorithms within specified domains without taxing current staff
- Accelerated compliance with government mandates and directives
- Alignment of cryptographic migration strategy with organizational risk and priorities

Solution Approach

NIST is recommending a structured process that consists of concrete and achievable steps organizations can take now to reduce immediate vulnerability and prepare for the transition to post-quantum cryptography. Patero solutions comply with NIST, CISA and Federal directives and reduce time and cost of executing recommended processes.

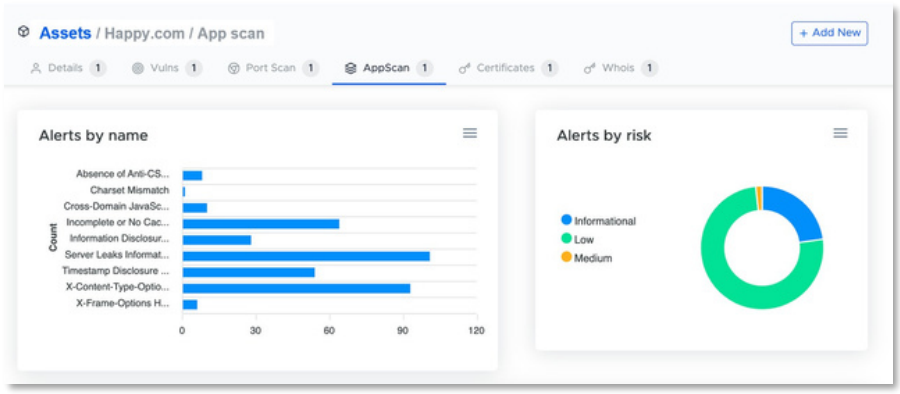


Figure 2 Sample dashboard of alerts and alert categories

PanoQoR is a cryptographic inventory and risk analysis tool that helps companies inventory cryptographic libraries, assess the cryptographic security posture and quantify the quantum-based risk to networks, information systems and assets.

Five Pillars of Cryptographic Discovery, Inventory, and Reporting

Internal	External	IT Assets	Databases	Code
Understand what encryption is visible externally from your infrastructure	Identify internal encryption within your network, how, and where it communicates	Recognize how endpoints, IoT devices, and servers use encryption and for what purposes	Pinpoint the location of databases and understand how they are encrypted	Search for and inventory the encryption used within your code and code libraries

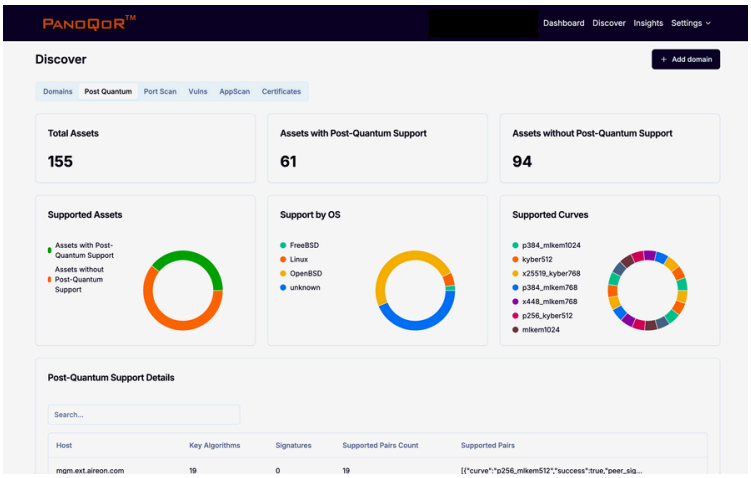
PanoQoR starts by discovering and cataloging network domains and subdomains. Once domains and subdomains have been enumerated, PanoQoR begins port scans, app scans, and pulls SSL certificate information for network endpoints. From there, PanoQoR analyzes the network for vulnerabilities such as expired or near-expired certificates, open ports, and configuration risks. Identified vulnerabilities can be associated with the criticality of specific assets and information systems as well as the cost to shape and execute remediation strategies. Finally, PanoQoR includes analysis that scores cryptographic risk to direct quantum computing attacks.

Cryptographic inventory, specific vulnerabilities, and quantum risk scores are delivered in report format delivered by Patero staff.

Conclusion

Cyber actors routinely exploit poor security configurations, weak controls, and other poor cyber hygiene practices to gain initial access to enterprise information systems. CISA reports that open ports and misconfigured services exposed to the internet are one of the most common vulnerability findings. PanoQoR is an easy way to identify both network and cryptographic vulnerabilities that create immediate and long-term risk to organization priorities and resilience.

Whether or not your organization is starting to plan a post-quantum cryptographic migration, understanding specific cryptographic and network vulnerabilities and is an easy way to prioritize remediation strategies to mitigate enterprise risk and ensure organizational resilience.



North America

Patero Inc.
7757 Baltimore Ave, Suite 1603
College Park, MD 20742
U.S.A
+1 650-641-0678
quantumsafe@patero.io
www.patero.io

EMEA

Patero GmbH
Feldstraße 15
29386 Hankensbüttel
GERMANY
+49 151-16246830
quantumsafe@patero.de
www.patero.de