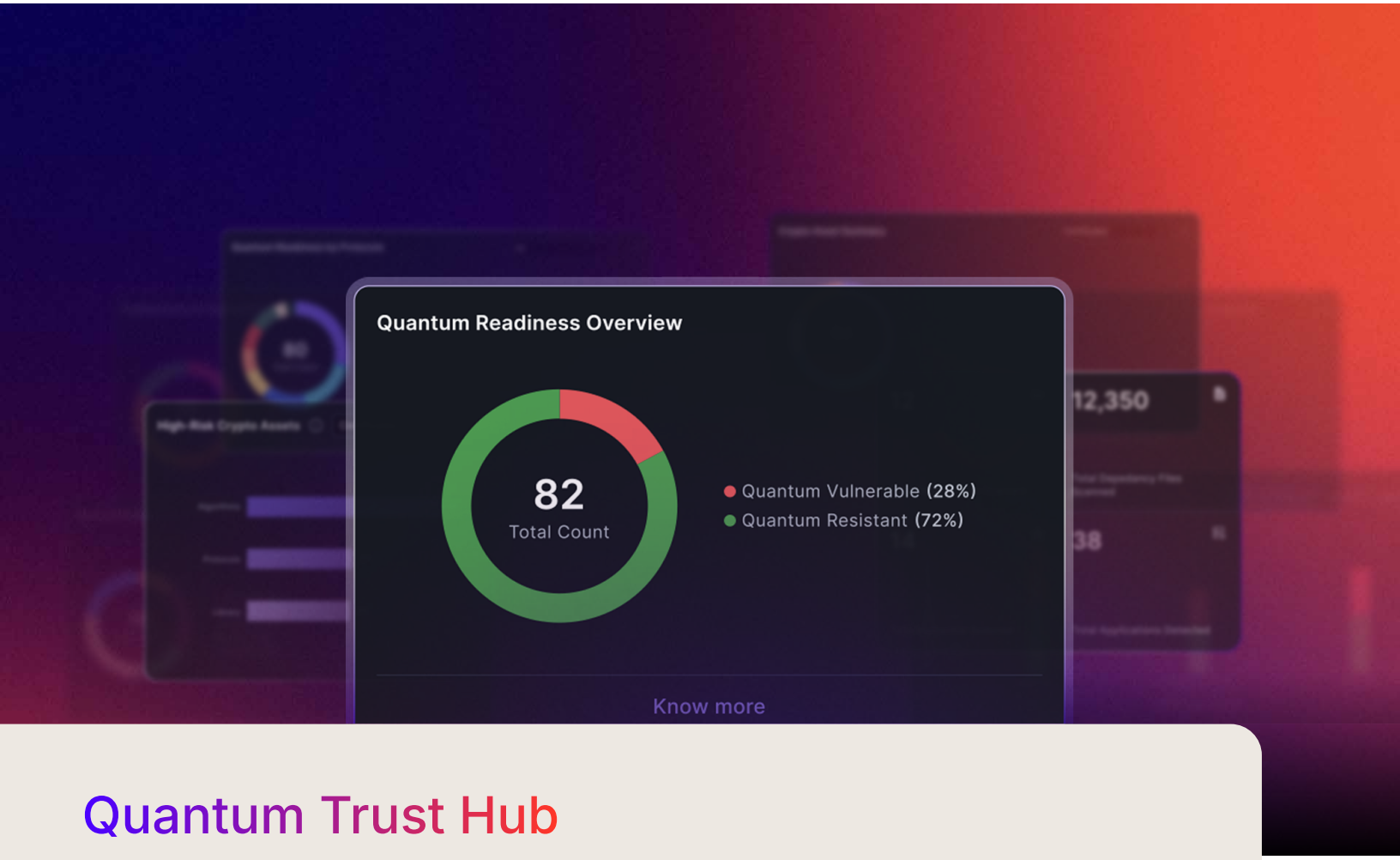
Solution Brief

AppViewX



Quantum Trust Hub

Know your quantum exposure. Prove your readiness.

Shift post-quantum readiness from a one-time discovery exercise into continuous crypto posture management, with audit-ready reporting built in.

© 2026 AppViewX, Inc. All rights reserved.

Certificate health isn’t the same as cryptographic resilience.

The quantum threat is already here. Bad actors are exfiltrating encrypted traffic today and storing it until a quantum computer can decrypt it. Financial records, health data, IP, and government secrets taken now stay exposed for as long as they stay sensitive.

Most PQC programs start with certificates because they're visible. But certificates are only the identity layer. Most of the cryptographic attack surface lives below it: TLS configuration policies, negotiated cipher suites, protocol versions, crypto libraries embedded in application code, firmware signing keys, and HSM key material. A server with a valid PQC certificate can still negotiate classical RSA key exchange, leaving the session quantum-vulnerable.

Quantum readiness migration is unlike Y2K, because no single patch fixes it. Migration touches every system that uses cryptography, so it must start now. Most teams start with:

No crypto inventory	**Certificates, ciphers, and libraries scattered across cloud, on-prem, and code repos.**
No way to prioritize risk	**No way to compare RSA-2048 vs. SHA-1 vs. hard-coded RC4, or which matters most.**
No business context	**A vulnerability on a marketing app is treated the same as one on a payments system.**
Audit and compliance gaps	**No artifact for NIST, NSM-10, CNSA 2.0, PCI DSS, eIDAS, ETSI, or regulators.**
Manual remediation	**Each algorithm replaced is a one-off project, with no policy, no scorecard, and no end state.**
No story for the board	**Executives need a single number that improves quarter over quarter.**

47 days

Public TLS certificate lifetimes drop to **47 days in March 2029.** At that pace, manual renewal stops being viable. The automation that handles 47-day renewals is the same foundation PQC migration runs on. Build it once and it covers both.

2029

Google’s target for bringing PQC to its own systems, products, and services. The largest players aren’t waiting for the mandates.

2030

The deadline Executive Order 14412 sets for federal agencies to move high-value assets and high-impact systems to post-quantum key establishment. Digital signatures follow by **December 31, 2031.**

2035

NIST’s final transition guidance sets the end date: quantum-vulnerable RSA and ECC algorithms are deprecated after 2030 and disallowed after 2035. NIST urges all organizations to treat PQC migration as a current operational priority.

© 2026 AppViewX, Inc. All rights reserved.

Which of these do I fix first, and who owns it?

Without business context	With business context
 **4,200** RSA-2048 Certificates The security team drowns in undifferentiated findings with no remediation path.	**AppViewX Quantum Trust Hub** Asset: **14 Customer-facing payment APIs** Finding: **RSA key exchange on TLS 1.2** Owner: **Payments Engineering** Priority: CRITICAL **The CISO has a board-ready action plan.**

Security, application, and PKI teams spend their time on the applications where exposure would hurt the most.

Move From Crypto Inventory To Quantum Readiness

Discovery and Inventory

See your entire crypto estate and assign every asset an owner.

What it delivers

- Certificate, configuration, and code scanning that detects quantum-vulnerable algorithms (such as RSA, ECC, and DH) in source code and dependencies, weak libraries, TLS protocols, cipher suites, and key sizes across endpoints and services
- Agentless certificate and network discovery, plus crypto findings from Tenable and Qualys, so there are no new agents to deploy
- A continuously updated CBOM of algorithms, protocols, libraries, and certificates, with import of CBOMs and SBOMs from existing tools
- CMDB data that maps every asset to its application, host, business context, and owner

Risk-Based Prioritization and Remediation

Prioritize risk by business impact, then migrate to PQC and hybrid certificates.

What it delivers

- Risk scoring that ranks crypto assets by business application context from CMDB
- Downstream dependency mapping that assesses PQC readiness across the full communication path, so silent fallbacks to classical crypto don't cause outages or security gaps
- Clear remediation steps that point to NIST-standardized alternatives such as ML-DSA and SLH-DSA
- ServiceNow tickets created directly from PQC findings, one per remediation scope, with ticket status tracked in Quantum Trust Hub
- ML-DSA, SLH-DSA, and hybrid composite certificates issued by AppViewX PKI, with CLM automating their lifecycle from PQC CSR generation and enrollment with PQC-capable CAs to deployment and renewal

Governance and Policy Enforcement

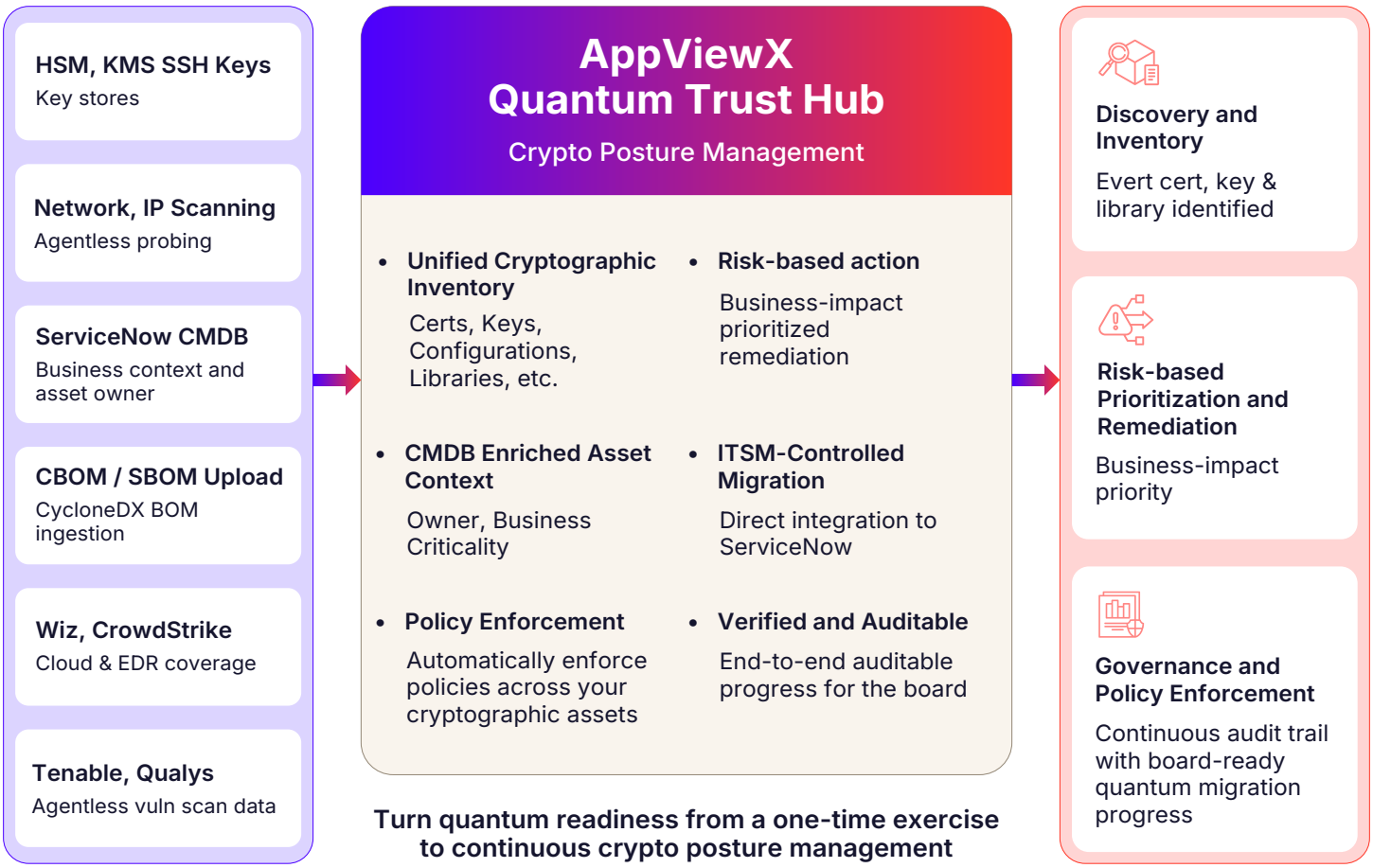
Enforce audit-ready policy and show the board real progress.

What it delivers

- Custom PQC policies applied across every crypto asset, with continuous compliance checks that catch a migrated system falling back to classical crypto, whether through an operational mistake or a malicious downgrade.
- An organization overview dashboard with an enterprise-wide view of cryptographic assets across certificates, code, and configurations, plus drill-down reports by certificate, library, or service to speed up investigation and remediation
- A quantum readiness score and audit-ready compliance reports, with migration progress tracked against a defined timeline

© 2026 AppViewX, Inc. All rights reserved.

Crypto Posture: The Command Center for Every PQC Decision



Turn quantum readiness from a one-time exercise to continuous crypto posture management

Measurable progress towards quantum readiness every quarter

Results	Business value
Discovery to remediation on a single platform	Quantum Trust Hub replaces a stack of CLM, PKI, SSH, Code Signing and crypto-inventory tools.
A Quantum Readiness Score in days, not months	Agentless cert scan delivers a baseline in days, not the months a services-led engagement requires.
Fewer certificate outages	Continuous discovery and automated certificate lifecycle management remove the late-night expired-certificate fire drill.
Board-ready PQC posture	A Quantum Readiness Score that climbs quarter over quarter, gives auditors and the board defensible evidence.

© 2026 AppViewX, Inc. All rights reserved.

Where Quantum Trust Hub applies

Map every certificate and its trust chain

Most teams have no complete inventory of certificates across public and internal trust, from root to leaf. Quantum Trust Hub finds them through agentless TLS handshake scans, agent-based scans of local stores, and managed CA and load balancer integrations. It classifies each as classical, hybrid, or PQC-only and scores it on a NIST-aligned severity scale, including trust-hierarchy risk, since a weak root or intermediate puts every issued leaf certificate at risk.

See what's protecting every data flow

Each connection's protocols, libraries, and cipher suites decide whether its data is quantum-safe. Quantum Trust Hub inspects TLS, SSH, and IPsec for protocol versions, fallback behavior, key sizes, deprecated ciphers like RC4 and 3DES, and PQC or hybrid support. It scores readiness by crypto library, protocol, key exchange, and authentication, and tracks each application's posture over time.

Find the crypto buried in your code

Code can last for years, so quantum-vulnerable crypto inside applications outlives every certificate rotation. Quantum Trust Hub scans Java, Python, and C/C++ source, build artifacts such as JARs, DLLs, and binaries, embedded certificates, and libraries such as OpenSSL, BouncyCastle, and WolfSSL. It flags weak algorithms, including MD5, SHA-1, DES, 3DES, and RSA under 2048, and recommends NIST-approved replacements.

Why AppViewX

Agentless-first discovery that works with your existing security stack. Certificate and network discovery require no new agents, Quantum Trust Hub pulls crypto findings from the vulnerability and management tools you already run, like Qualys and Tenable, instead of deploying a net-new sensor fleet.

Risk prioritized by business impact, not algorithm type. CMDB integration maps every crypto asset to its application, host, business context, and owner, so remediation starts with the customer-facing API, instead of the internal dev environment, and the fix lands with the right owner.

Posture and remediation on one platform. Quantum Trust Hub identifies and prioritizes what needs to move. AppViewX PKI issues ML-DSA, SLH-DSA, and hybrid certificates and AppViewX CLM automates their lifecycle, from CSR generation and enrollment to deployment, renewal, and mass rotation.

> **"AppViewX is the key enabler for our post-quantum readiness."**
>
> \- Senior VP of Data Protection, Financial Services

302%	<6	200+
Return on Investment	months payback	Integrations

Find out where your quantum exposure is.

Talk to an AppViewX expert about your environment and quantum priorities.

AppViewX

165 Broadway, 23rd Floor,
New York, NY 10006

info@appviewx.com
www.appviewx.com

+1 (212) 400 7541
+1 (929) 955 0055