AppViewX Quantum Trust Hub | Solution Overview

Move from Cryptographic Inventory to Quantum Readiness with Quantum Trust Hub

Challenge

Harvest-now, decrypt-later attacks put RSA- and ECC-protected data at risk today. NIST's final transition guidance deprecates these quantum-vulnerable algorithms after 2030 and disallows them after 2035. Critical federal systems face earlier deadlines under Executive Order 14412: 2030 for key establishment and 2031 for signatures. With the threat already active and the deadlines now set, quantum readiness can't wait.

Your crypto inventory stops at the certificate

Certificates are only the top layer. Cryptography also lives in TLS configurations, protocols, cipher suites, and libraries hard-coded into application code. An inventory that stops at certificates misses much of your quantum exposure.

Every vulnerable asset looks equally urgent

Thousands of quantum-vulnerable RSA certificates need remediation, and they can't all be fixed at once. Without business context, you can't tell whether the customer-facing payment API or the internal app comes first, or who owns the fix.

Remediation is manual, and progress doesn't hold

Migration runs as a one-off project, not a program tracked from discovery to closure. Without continuous policy enforcement, even migrated systems can fall back to classical crypto through a misconfiguration or a malicious downgrade.

Migration progress is invisible to auditors and the board

Auditors want evidence of where every quantum-vulnerable asset stands, and the board wants to know when you'll be PQC compliant. Without compliance reporting or migration status tracked against a timeline, there's nothing credible to show either.

AppViewX Quantum Trust Hub

See Your Crypto. Score Your Risk. Build Your Migration Path.

AppViewX Quantum Trust Hub is a cryptographic posture management solution that discovers cryptographic assets, prioritizes quantum exposure by business impact, and routes remediation into your existing workflows, with custom PQC policies and audit-ready reporting built in. It turns quantum readiness from a one-time discovery exercise into continuous crypto posture management, with board-level proof of where you stand.

Discovery and Inventory

Find certificates, TLS configurations, cipher suites, protocols, and crypto libraries in one continuously updated inventory, with every asset mapped to its application and owner from your CMDB.

Risk-Based Prioritization and Remediation

Rank every quantum-vulnerable asset by the business application it supports, so migration starts where exposure would hurt most. Route remediation through the ITSM workflows, tracked to closure.

Governance and Policy Enforcement

Check every crypto asset against custom PQC policies continuously, catch fallbacks to classical crypto, and track quantum readiness against your migration timeline, with audit-ready reports.

What It Delivers

Know Your Quantum Exposure. Prove Your Readiness.

Agentless Discovery

Discover cryptographic assets by analyzing the output of Qualys and Tenable scans, without rolling out new agents. Generate a continuously updated cryptographic bill of materials (CBOM), or import one from existing EDR and CSPM tools, for centralized analysis.

Business Context Risk Scoring

Map every asset to its application, host, business context, and owner from your CMDB (ServiceNow). Risk scoring ranks findings by business impact, not just algorithm type or key size, so high-value assets move first.

ITSM Remediation Through ServiceNow

Create ITSM (ServiceNow) tickets directly from PQC findings, scoped by remediation area, with status tracked in Quantum Trust Hub. Remediation steps point to NIST-standardized alternatives such as ML-KEM and ML-DSA.

Post-Quantum Certificate Lifecycle Management

Discover PQC certificates from any CA, generate PQC CSRs, enroll with PQC-capable CAs, and automate deployment and renewal, building crypto-agility into your migration.

Custom PQC Policies

Apply custom PQC policies across every cryptographic asset with continuous compliance checks, so a migrated system that falls back to classical crypto gets caught early.

Executive Dashboard and Reporting

An organization overview dashboard spans certificates, code, and configurations, with drill-down reports by certificate, library, or service and audit-ready compliance reports that track migration against your timeline.

What Security Leaders Get

Continuous PQC posture, not a one-time inventory	See quantum exposure across certificates, configurations, protocols, and code in one inventory that stays current, instead of a discovery exercise you repeat every time something changes.
Fix your highest quantum risk first	Start migration where exposure would hurt most, not where the algorithm looks weakest, with every quantum risk assigned to an owner accountable for fixing it.
Show the board real PQC progress	Measure quantum readiness as a score and track migration against your timeline, so the board gets a clear status and auditors get the evidence behind it.
Find and replace quantum-vulnerable certificates on one platform	Discover risk in Quantum Trust Hub, then issue PQC and hybrid composite certificates with AppViewX PKI and automate their lifecycle with AppViewX CLM, all on the same platform.

Get a complete picture of your crypto estate.

Schedule a quantum readiness assessment and see where you stand across certificates, configurations, and code.

AppViewX
info@appviewx.com
www.appviewx.com
+1 (212) 400-7541