



Autumn 2026

Product Release Datasheet



[Quantum readiness](#) can't be a one-time discovery exercise. [Harvest-now, decrypt-later](#) attacks put long-lived encrypted data at risk today, and public TLS certificate lifetimes are shrinking to 47 days.

[The Autumn 2026 release](#) makes quantum readiness continuous.

[Quantum Trust Hub](#) discovers cryptographic assets, prioritizes exposure by business impact, and routes remediation to your existing processes. [AppViewX CLM](#), [PKI](#), [SSH](#), and [Code Signing](#) then put that into action with post-quantum cryptography (PQC) and hybrid certificates, renewal automation for 47-day lifetimes, short-lived SSH certificates, and certificate actions triggered from AI assistants and agents.

See and Prioritize Quantum Risk

Build a continuously updated [cryptographic bill of materials \(CBOM\)](#) from tools you have in place, and route remediation to the people who own it.

Feature	Description	Why It Matters
Agentless Qualys Integration	Analyze the output of the Qualys scans you already schedule to discover PQC-relevant protocols, cipher suites, certificates, and library metadata.	Keep your crypto inventory and compliance reporting current with no new agent to deploy or manage. Qualys joins Tenable as a source for agentless discovery.

See and Prioritize Quantum Risk

Build a continuously updated cryptographic bill of materials (CBOM) from tools you have in place, and route remediation to the people who own it.

Feature	Description	Why It Matters
CBOM / SBOM Upload	Import Cryptographic and Software Bills of Materials from EDRs, CSPMs, and third-party scanners directly into Quantum Trust Hub.	See cryptography across applications, dependencies, and the supply chain in a single dashboard, with version-aware, prioritized remediation guidance.
ServiceNow Integration	Create ServiceNow tickets from PQC inventory findings, grouped as one ticket per remediation scope, with ticket ID, status, and action tracked in Quantum Trust Hub.	Remediation runs through the ITSM workflows application owners already use, so migration doesn't stall at the handoff between security and IT. Quantum Trust Hub tracks every ticket from discovery to closure.

Migrate to PQC and Hybrid Certificates

Issue NIST-standardized ML-DSA and SLH-DSA certificates and hybrid composite certificates from AppViewX PKI, then manage and sign with post-quantum keys across CLM and Code Signing.

Feature	Description	Why It Matters
Post-Quantum Certificate Lifecycle Management	Discover PQC certificates, generate PQC CSRs, enroll with PQC-capable CAs, and automate deployment to endpoints.	PQC certificates get the same automated lifecycle as classical certificates, so the platform that finds quantum risk also fixes it.
HSM-Backed PQC Key Generation	Generate and protect post-quantum keys across supported HSM integrations for CA creation, certificate issuance, and code signing.	Build a clear path to test and operationalize quantum-safe PKI hierarchies, hybrid certificate strategies, and signing workflows.

Built for 47-Day Certificate Lifetimes

Keep renewals reliable as certificate lifetimes shrink and renewal volume multiplies.

Feature	Description	Why It Matters
ACME ARI Support	Support ACME Renewal Information (RFC 9773), so clients renew within a server-suggested window instead of too early or too late.	Reduce renewal-related outages, and rotate certificates quickly without manual intervention when a CA needs to revoke and reissue.
DCV Automation	Check requested domains against Domain Control Validation status before submission and revalidate multiple domains in a single bulk action.	Domain validation data can be reused for only 10 days from March 2029, so revalidation becomes continuous. Remove that bottleneck and catch validation errors before they surface later in the lifecycle.
AWS Certificate Coverage	Automatically discover certificates stored in Amazon S3 buckets, track expiry, and push renewals back to the same buckets, with controlled, auditable private key export for exportable AWS ACM certificates.	Bring AWS certificates under automated lifecycle management across regions and accounts, so unmanaged certificates don't hide in S3 or ACM as renewals multiply.
MCP-Enabled CLM Actions	Renew, regenerate, or revoke certificates from AI assistants and agents through natural language, using the Model Context Protocol (MCP).	Extend certificate lifecycle automation into the AI-driven workflows your teams already use.

Modernize PKI and Retire Long-Lived Credentials

Enforce CA policy, retire Microsoft AD CS at scale, and stay compatible with legacy validation paths.

Feature	Description	Why It Matters
CA Policy Management	Define reusable CA policies manually or by uploading a Certification Practice Statement (CPS) and reviewing the extracted values, then apply them consistently during CA creation and renewal.	Turn CPS requirements into enforceable CA settings, reduce configuration drift, and onboard CAs faster with reusable policies.

Modernize PKI and Retire Long-Lived Credentials

Enforce CA policy, retire Microsoft AD CS at scale, and stay compatible with legacy validation paths.

Feature	Description	Why It Matters
AD CS Migration	Track, resume, and audit multiple AD CS migration runs from one view, with safeguards against duplicate migrations for the same CA.	Retire Microsoft AD CS in large environments with clear progress visibility and fewer operational errors.
SSH Short-Lived Certificates	Replace unmanaged, long-lived SSH keys with short-lived certificates that expire automatically. Track every user and host certificate in an inventory, with expiry tiles on the SSH dashboard.	Move SSH access off never-expiring keys without interrupting sessions or making users replace their private keys and remove the standing access risk of unmanaged keys.
HTTP CRL Publishing	Publish CRLs over HTTP and embed port 80 CRL Distribution Point (CDP) URLs in issued certificates where network, proxy, or relying-party requirements call for it.	Stay compatible with legacy validation paths and reduce deployment friction, while existing secure endpoint configurations keep working.
GCP Workload Identity Federation	Authenticate to Google Cloud with workload identity federation instead of long-lived service account keys.	Stop creating, distributing, rotating, and revoking static keys. Lower credential-leak risk, fewer audit findings, and an authentication model aligned with zero trust.
Automated Code Signing in Azure DevOps	Install the AppViewX signing package dynamically inside Azure DevOps CI/CD pipelines, register signing certificates securely, and trigger signing as part of each build.	Consistent, secure signing across every build and release, with less manual setup and more reliable signing workflows.

Get your quantum readiness baseline.

Request a 30-day Quantum Trust Hub assessment for a complete CBOM, your first Quantum Readiness Score, and a prioritized remediation plan, built with your data.



165 Broadway, 23rd Floor
New York, NY 10006

info@appviewx.com
www.appviewx.com

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