QuSecure | QuProtect R3: Cryptographic Command & Control

QuSecure

Capability Statement

QuSecure, Inc. is a post-quantum cybersecurity company delivering QuProtect™ R3, a distributed cryptographic command-and-control platform that enables federal agencies to discover, inventory, enforce, and report on cryptographic posture across their networks without requiring application redesign or hardware replacement.

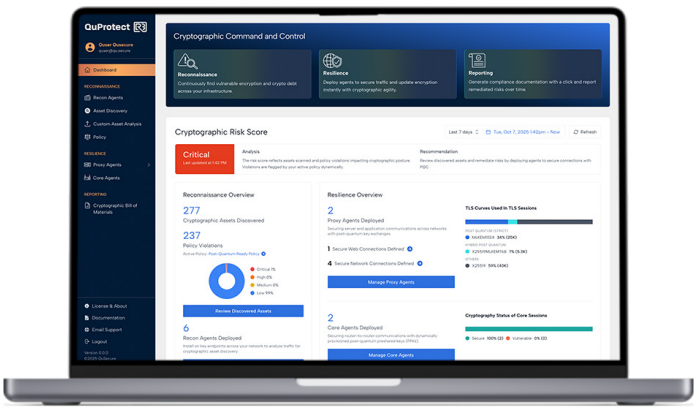
QuProtect R3 operates as a centralized orchestration layer paired with deployable enforcement and discovery agents. The Orchestrator functions as a cryptographic control plane: it maintains authoritative policy definitions, distributes enforcement rules to distributed agents, aggregates cryptographic posture telemetry, and evaluates compliance status through a policy engine. The Orchestrator does not perform application processing; it governs cryptographic behavior across networked systems.

The platform addresses two immediate federal imperatives: (1) protecting data-in-transit today against "Store Now, Decrypt Later" attacks by enforcing post-quantum key exchange (ML-KEM, FIPS 203) at the application layer; and (2) providing the cryptographic visibility and agility required to execute a structured, policy-driven migration to NIST PQC standards without waiting for every application vendor to independently implement PQC.

A core differentiator of QuProtect R3 is automated certificate discovery, visibility, and lifecycle management. QuProtect R3 continuously discovers certificates across the environment — including those of unknown provenance, expired certificates, self-signed certificates, and certificates not rooted in approved PKIs — inventories them in CycloneDX CBOM format and can automatically provision and rotate certificates via integrated PKI providers. This capability directly addresses one of the most persistent operational pain points in federal networks: certificate management is largely manual, certificate lifetimes are too long, and non-PKI-enrolled certificates are commonplace — representing prime targets for

QuProtect R3™ Reconnaissance, Resilience, Reporting

QuProtect R3 is organized around three integrated capability pillars — Reconnaissance, Resilience, and Reporting — delivered through a central Orchestrator and a mesh of three distinct distributed agent types. Two of the three pillars (Reconnaissance and Reporting) were developed with input from the U.S. Army C5ISR Center.auditability for quantum security at layers 2 and 3, and easily integrates into existing infrastructure.



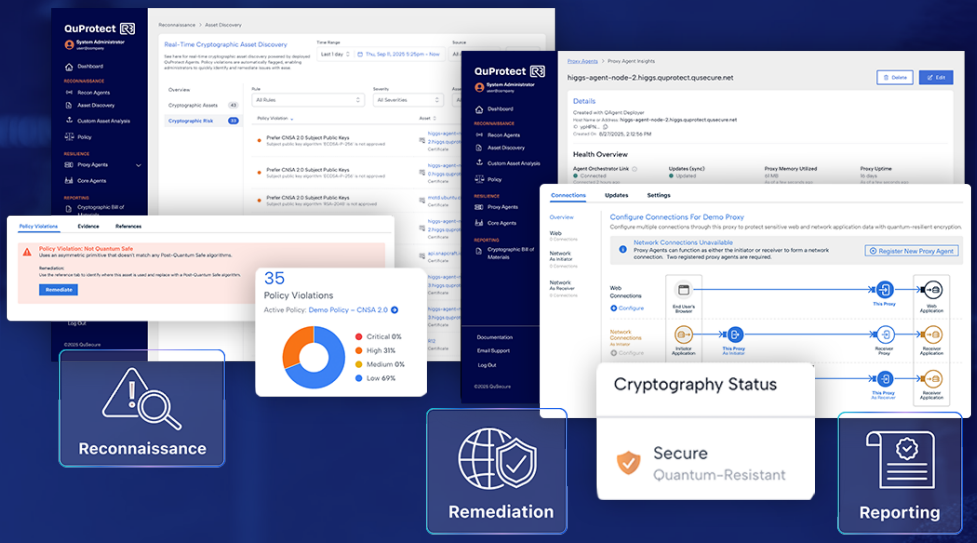
Federal Traction

- SBIR Phases I–III (Army, Air Force)
- SPARTN + TACFI Transition Pathways
- Integrated into Second Front's Game Warden
- Built for tactical and enterprise networks at scale.

Differentiators

- Only crypto-agile platform field-ready today
- No rip-and-replace: overlays existing infrastructure
- Zero-code deployment across on-prem, edge, and cloud
- Designed with and for warfighters at classified and tactical edge levels

QuSecure



QuProtect R3: Key Components

Orchestrator	**Cryptographic Control Plane** The Orchestrator is the central management layer. It aggregates cryptographic inventory data from distributed agents, hosts policy engine with pre-loaded and customizable compliance policy templates, generates risk scores, surfaces real-time alerts on non-compliant or vulnerable assets, manages PKI integrations for automated certificate distribution and rotation, and exposes a CBOM API for third-party SIEM and compliance tool integration.
Recon Agents	**Continuous Discovery & Policy-Based Risk Reporting** Dynamically build up a cryptographic inventory sourced from operational data by monitoring network traffic Find TLS servers with soon-to-expire certificates or supporting outdated TLS versions Discover TLS clients offering weak ciphersuites or probing servers for weak configurations Identify non-quantum-safe assets to build a remediation plan Statically generate a CBOM
Proxy Agents	**Secure Connections For Quantum-Resistant Data In Transit** Secure web (PQ TLS), network (PQ TLS and Secure TCP), and router traffic on networks Introduce a crypto-agile overlay at the ntwork layer to reduce risk and costs of application code changes Automate certificate provisioning and rotation of client and server certificates for protected applications Enforce a zero-trust architecture by requiring mutual authentication with cryptographically strong service identities

Policy Engine

For Drop-In & Custom Compliance Templates

The Orchestrator policy engine comes with three pre-loaded, read-only policy templates provide immediate compliance baselines:

Secure Baseline **CNSA 2.0**

Post-Quantum Ready **Custom Policy**

Policy evaluation occurs continuously producing real-time compliance status and measurable deltas between baseline and post-enforcement posture. Policy changes propagate from the Orchestrator to all agents centrally; no per-application reconfiguration is required.

PQC Readiness

Alignment With Latest Standards & Mandates

NIST FIPS 203 (ML-KEM)

NSA CNSA 2.0

FIPS 140-validated cryptography | CMVP #4694

CycloneDX CBOM

OMB M-22-09 / M-23-02

DoD IL2 / IL5 / IL6 | Under active USAF TACFI contract.

CISA PQC Product Categories (Jan 2026)

Company Information

UEI: WBKKDF2LAMV9
CAGE Code: 8GGT0
NAICS: 541715, 541511, 511210, 423430

www.qusecure.com

info@qusecure.com |
+1 (650) 356-8001