Cryptographic Bill of Materials & Infrastructure Platform

Discover, inventory, and govern every cryptographic asset — from certificates to quantum readiness.

QCecuring provides a unified platform for cryptographic infrastructure management. Our CBOM engine discovers all algorithms, keys, certificates, and protocols across your enterprise, while integrated modules automate certificate lifecycle, SSH key governance, code signing, PKI, and HSM management.

7	100+	6+	PQC	4
Integrated Modules	Platform Integrations	Discovery Methods	Quantum Ready	Deployment Models

Prepared For

RITES Vendor Assessment | Cryptographic Infrastructure & CBOM Evaluation

The Industry Problem

Organizations face an unprecedented cryptographic visibility crisis. With quantum computing advancing rapidly, regulatory mandates tightening, and certificate sprawl growing exponentially, enterprises cannot answer fundamental questions about their cryptographic posture.

2033	~70%	65%	Active
CNSA 2.0 DEADLINE	QUANTUM-VULNERABLE	UNMANAGED CERTS	HNDL ATTACKS

Critical Challenges

No Cryptographic Visibility
Most organizations cannot identify where RSA, ECDSA, or deprecated algorithms are deployed. Without a CBOM, PQC migration is guesswork.

Certificate Outages
80% of organizations experienced certificate-related outages in the past 2 years. Average cost: $300K per hour of downtime.

SSH Key Sprawl
40%+ of SSH keys are orphaned — belonging to d eparted employees or decommissioned systems. Each i s a persistent backdoor.

Harvest Now, Decrypt Later
Nation-state adversaries are collecting encrypted data today, waiting for quantum computers to break it. Data with 10+ year confidentiality requirements is already exposed.

Regulatory Pressure
CNSA 2.0 mandates PQC by 2033. PCI DSS 4.0 requires cipher inventory. NIST SP 800-131A deprecates weak algorithms. Compliance requires visibility.

Fragmented Tooling
Separate tools for certificates, SSH keys, code signing, and HSMs create gaps, inconsistencies, and operational overhead.

Platform Overview

QCecuring is a unified cryptographic infrastructure management platform with seven integrated modules. At its core, the CBOM engine provides complete cryptographic discovery and quantum risk assessment, while specialized modules automate the full lifecycle of certificates, keys, and signing operations.

Cryptographic Discovery & CBOM (Core)

Multi-method discovery of all cryptographic assets — algorithms, keys, certificates, protocols, and libraries. CycloneDX CBOM output, per-asset quantum risk scoring, CNSA 2.0 / PCI DSS 4.0 compliance evaluation, and PQC migration roadmap generation.

SSL Certificate Lifecycle Management

Automated discovery, renewal, and deployment of SSL/TLS certificates across hybrid infrastructure. Multi-CA support (DigiCert, Sectigo, Let's Encrypt, AD CS, Vault). Policy-driven automation with zero-outage guarantee.

SSH Key Lifecycle Management

Complete SSH key inventory, trust relationship mapping, automated rotation, orphan key remediation, and compliance enforcement across all server platforms.

Code Signing

Centralized, HSM-backed signing for all software artifacts (Authenticode, JAR, Docker, NuGet, macOS, Android). CI/CD integration with approval workflows and tamper-proof audit trails.

PKI-as-a-Service

Fully managed PKI with complete CA hierarchy, multi-protocol enrollment (ACME, SCEP, EST, CMP), FIPS 140-2 Level 3 HSM protection, and 1M+ certificates/day throughput.

HSM Management

Unified control plane for multi-vendor HSM fleets (Thales Luna, Entrust nShield, AWS CloudHSM, Azure Managed HSM). Health monitoring, key lifecycle, and compliance reporting.

Cloud-Native Security

Kubernetes-native certificate management, automatic service mesh mTLS, ephemeral certificates, SPIFFE/SPIRE workload identity, and cert-manager integration.

Discovery Architecture

The QCecuring CBOM engine uses six complementary discovery methods to achieve complete cryptographic visibility. Each method targets a different layer of the technology stack, ensuring no blind spots.

1. Source Code Analysis
Static analysis of crypto API calls across Java, Python, Go, C/C++, .NET, and Rust. Identifies algorithm usage, key generation patterns, and deprecated function calls.

2. Binary & Container Scanning
Analyze compiled binaries, shared libraries, and container image layers without source code access. Detects compiled-in cryptography and third-party library versions.

3. Network Traffic Analysis
Passive TLS/SSH traffic inspection captures cipher suite negotiations, protocol versions, certificate chains, and key exchange parameters in real-time.

4. Cloud & KMS Enumeration
API-driven discovery of AWS KMS, Azure Key Vault, GCP Cloud KMS, and cloud certificate services. Maps all cloud-managed cryptographic resources.

5. Configuration & Store Scanning
Scan TLS configs (Nginx, Apache, IIS), Java KeyStores, Windows Certificate Stores, AD CS templates, and SSH server configurations.

6. Runtime Tracing
eBPF-based kernel tracing captures actual cryptographic operations at runtime. Identifies crypto that is actively executing vs. merely configured.

CBOM Output & Standards

Output Format	CycloneDX CBOM v1.6+ (JSON/XML) — industry standard
Asset Types Discovered	Algorithms, Keys, Certificates, Protocols, Libraries
Quantum Risk Scoring	Per-asset: CRITICAL / HIGH / MEDIUM / LOW / NONE
Risk Factors	Algorithm vulnerability × Data sensitivity × Retention period × HNDL exposure
Compliance Profiles	CNSA 2.0, PCI DSS 4.0, FIPS 140-2/3, NIST SP 800-131A
Scanning Mode	Continuous (scheduled) + On-demand + CI/CD pipeline
Remediation	Integrated triggers to CLM, SSH KLM, Code Signing modules

Platform Capabilities

Cryptographic Discovery & CBOM

- Multi-method discovery: code, binary, network, cloud, config, runtime
- CycloneDX CBOM v1.6+ output for interoperability with SBOM/GRC tools
- Per-asset quantum risk scoring with HNDL exposure analysis
- Continuous scanning with drift detection and alerting
- Pre-built compliance profiles (CNSA 2.0, PCI DSS 4.0, FIPS)
- PQC migration roadmap generation with prioritized remediation

Certificate Lifecycle Management

- Automated discovery: network scan, cloud API, agent, CT logs, store enumeration
- Multi-CA support: DigiCert, Sectigo, Let's Encrypt, AD CS, EJBCA, Vault, AWS Private CA
- Policy-driven renewal at configurable thresholds (90/60/30/7 days)
- Automated deployment to Nginx, IIS, JKS, K8s secrets, cloud load balancers
- Service reload/restart after deployment with rollback on failure
- Immutable audit trail with actor attribution and compliance reporting

SSH Key Lifecycle Management

- Agentless and agent-based discovery of all SSH keys across servers
- Trust relationship mapping: who can access what, transitive paths
- Automated zero-downtime key rotation with pre-verification
- Orphan key detection and remediation (departed employees, decommissioned systems)
- Policy enforcement: algorithm, key size, age, passphrase requirements
- Support for Linux, Unix, macOS, Windows OpenSSH, network devices

Code Signing, PKI, HSM & Cloud-Native

- HSM-backed signing: Authenticode, JAR, Docker, NuGet, macOS, Android, firmware
- CI/CD plugins: Jenkins, GitHub Actions, GitLab CI, Azure DevOps
- Full CA hierarchy with ACME, SCEP, EST, CMP enrollment protocols
- Multi-vendor HSM fleet management (Thales, Entrust, AWS, Azure, GCP)
- Kubernetes-native: CRDs, cert-manager, service mesh mTLS, SPIFFE/SPIRE
- Ephemeral certificates (<50ms issuance) for cloud-native workloads

Supported Integrations

QCecuring integrates with 100+ enterprise systems across certificate authorities, cloud platforms, infrastructure, DevOps toolchains, and IT service management.

Certificate Authorities

- DigiCert CertCentral
- Sectigo / Comodo
- GlobalSign Atlas
- Entrust Certificate Services
- Let's Encrypt (ACME)
- Microsoft AD CS (DCOM + REST)
- EJBCA Enterprise
- HashiCorp Vault PKI
- AWS Private CA
- Azure Key Vault (CA)
- Google Cloud CAS
- Venafi (interop)

Cloud & Infrastructure

- AWS (ACM, KMS, CloudHSM, EC2, EKS, ALB)
- Azure (Key Vault, HSM, AKS, App Gateway)
- GCP (Cloud KMS, CAS, GKE, Cloud LB)
- Kubernetes (EKS, AKS, GKE, OpenShift, Rancher)
- Docker / Container registries
- Terraform / Pulumi providers
- Nginx, Apache, IIS, HAProxy, F5
- Java KeyStores (JKS/PKCS#12)
- Windows Certificate Store
- Linux servers (RHEL, Ubuntu, CentOS, Debian)
- Network devices (Cisco, Juniper, Palo Alto)
- HSMs (Thales Luna, Entrust nShield, Securosys)

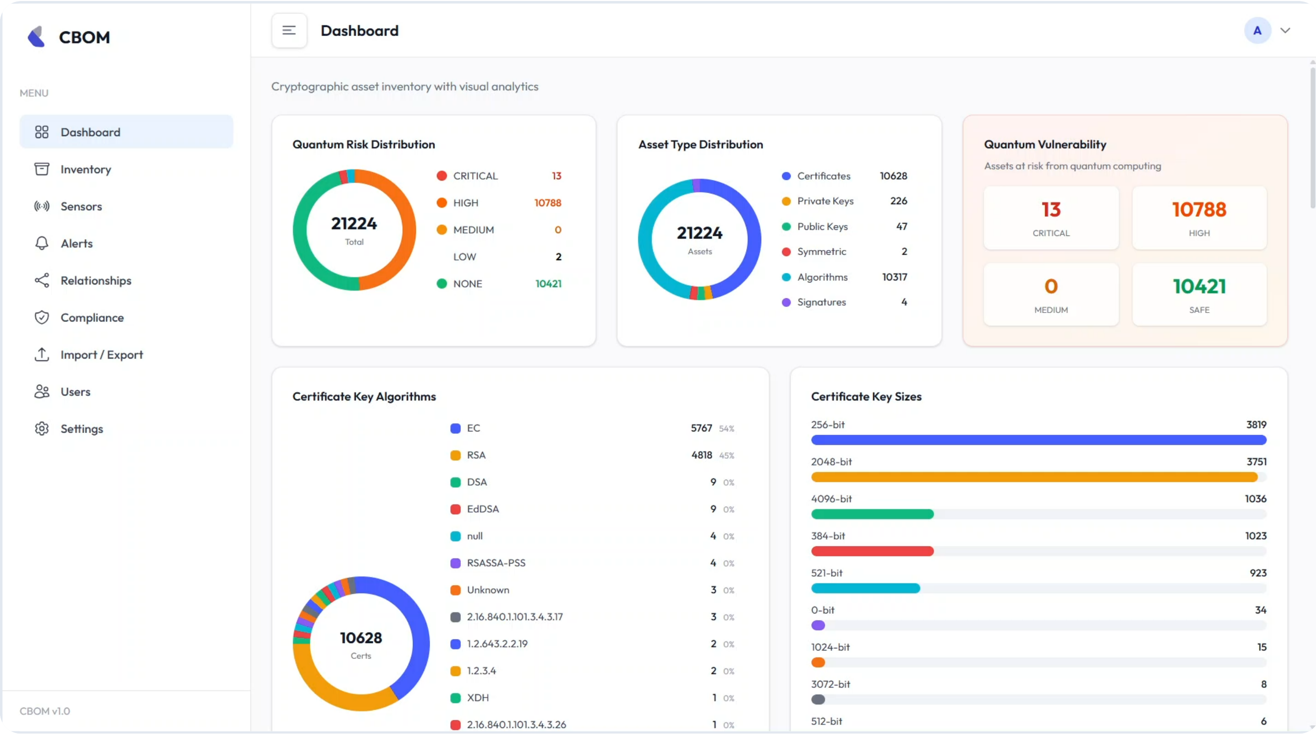
DevOps & ITSM

- Jenkins, GitHub Actions, GitLab CI
- Azure DevOps, CircleCI, ArgoCD
- cert-manager (Kubernetes)
- Istio / Linkerd / Consul (service mesh)
- SPIFFE/SPIRE (workload identity)
- Sigstore / cosign (container signing)
- ServiceNow (ITSM integration)
- Jira (ticket creation)
- Slack / Microsoft Teams (alerting)
- PagerDuty / OpsGenie (escalation)
- Splunk / Elastic (SIEM export)
- Prometheus / Grafana (observability)

Platform Interface

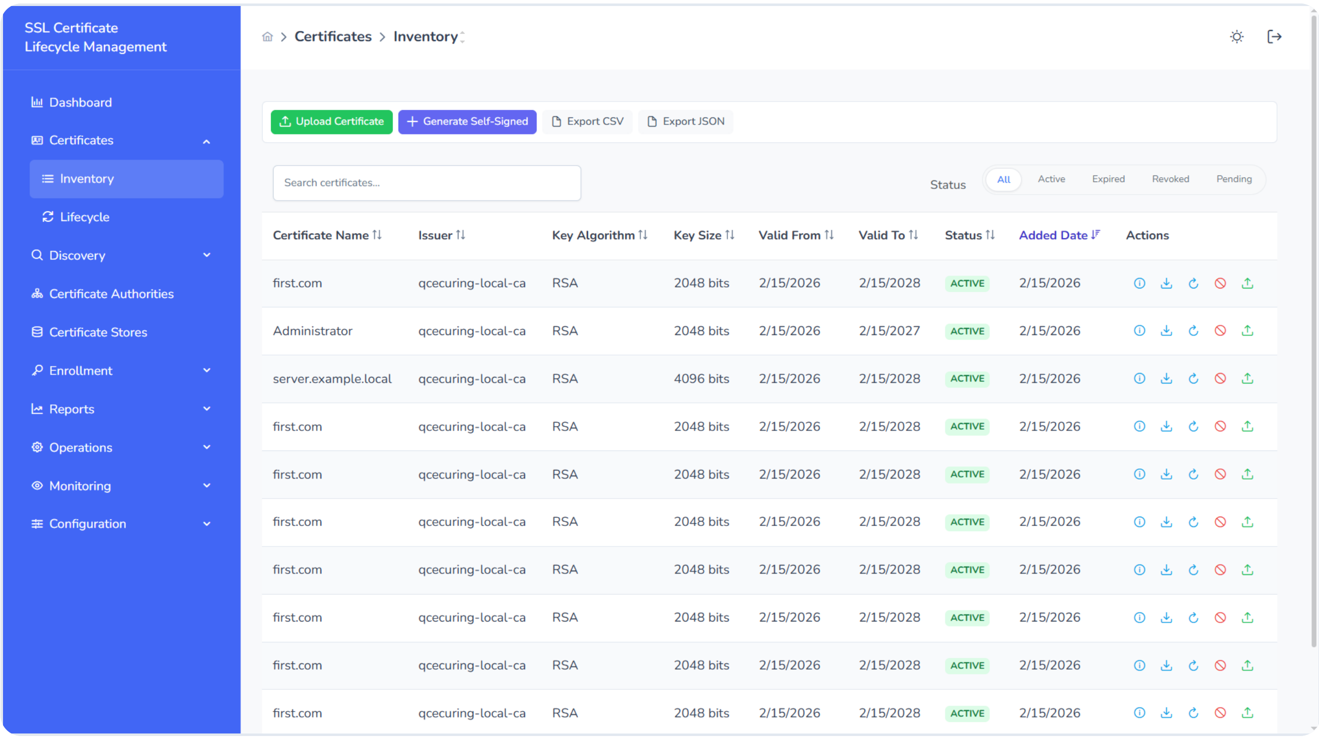
The QCecuring platform provides a unified web-based interface for managing all cryptographic assets. Below are representative views of the platform dashboard and key modules.

CBOM Discovery & Cryptographic Inventory Dashboard



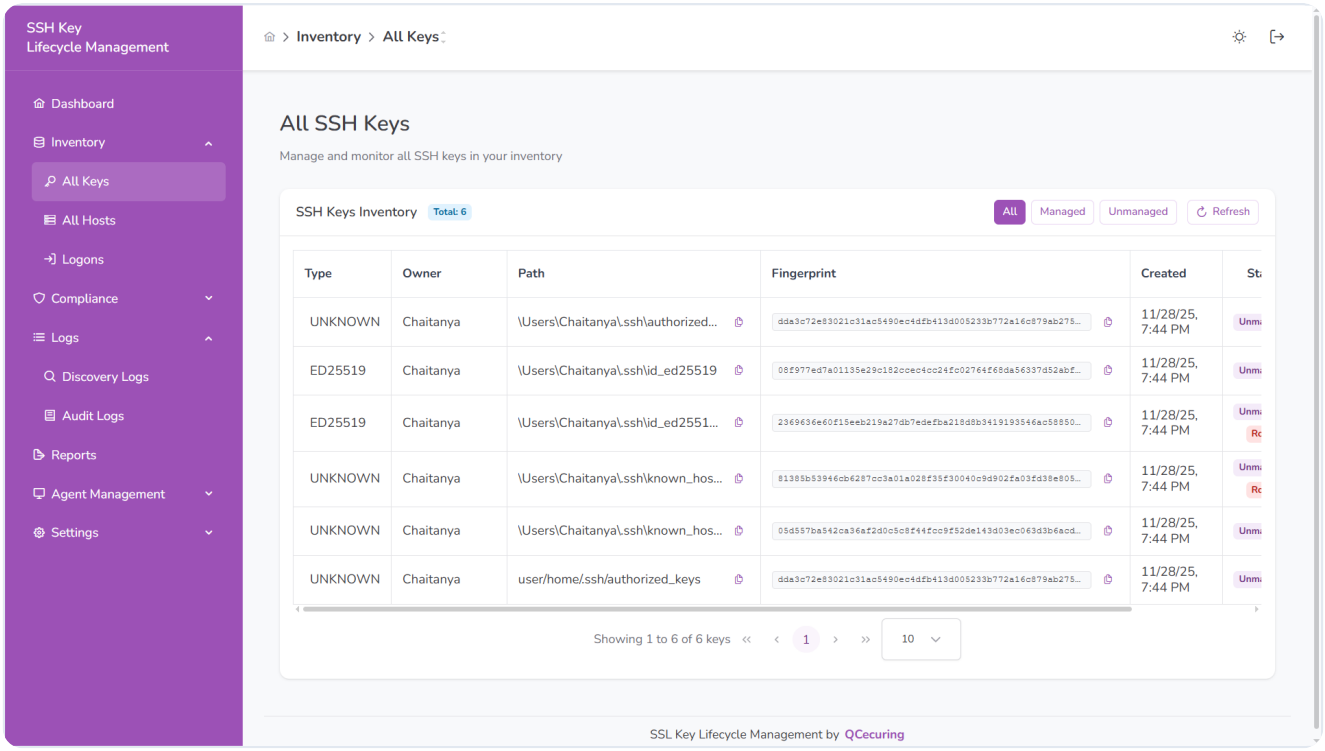
Cryptographic asset inventory with quantum risk scoring, algorithm distribution, and compliance status.

SSL Certificate Lifecycle Management



Certificate inventory with expiry tracking, CA distribution, automated renewal status, and deployment targets.

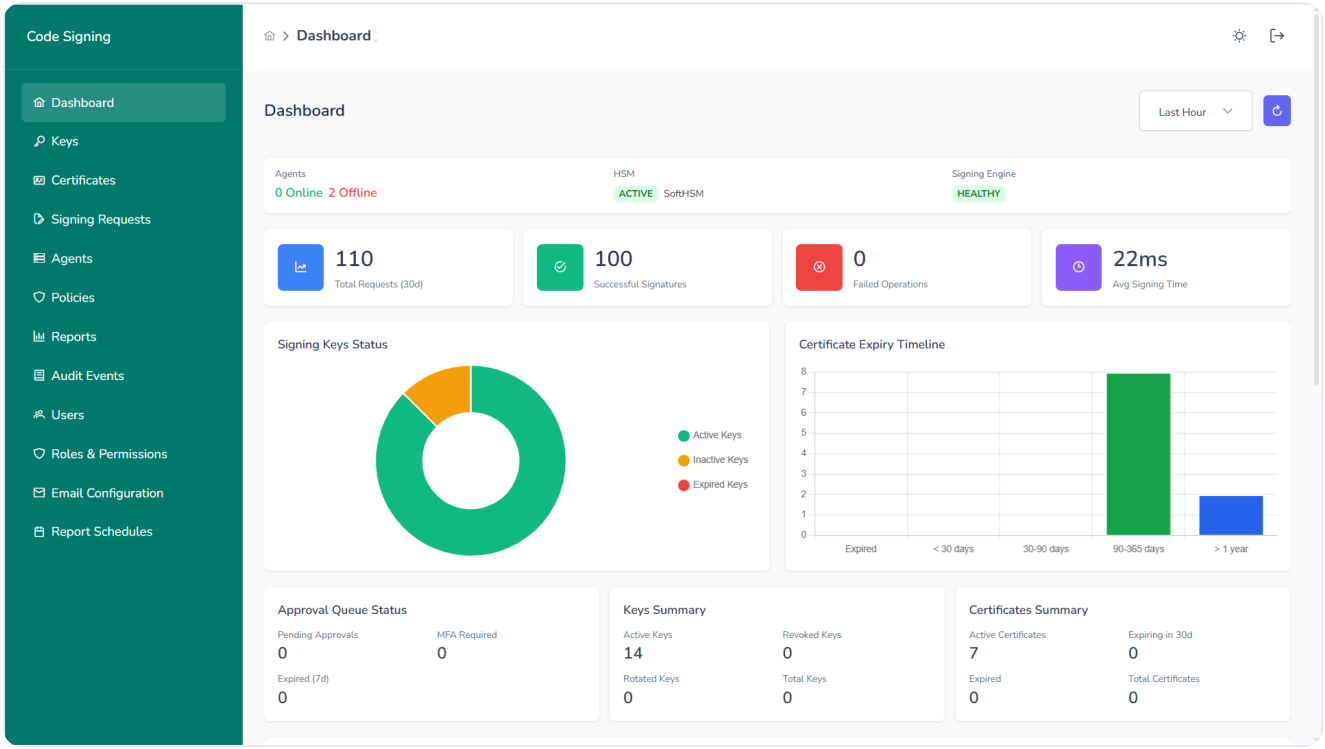
SSH Key Lifecycle Management



SSH key inventory with trust relationship mapping, rotation status, and orphan key identification.

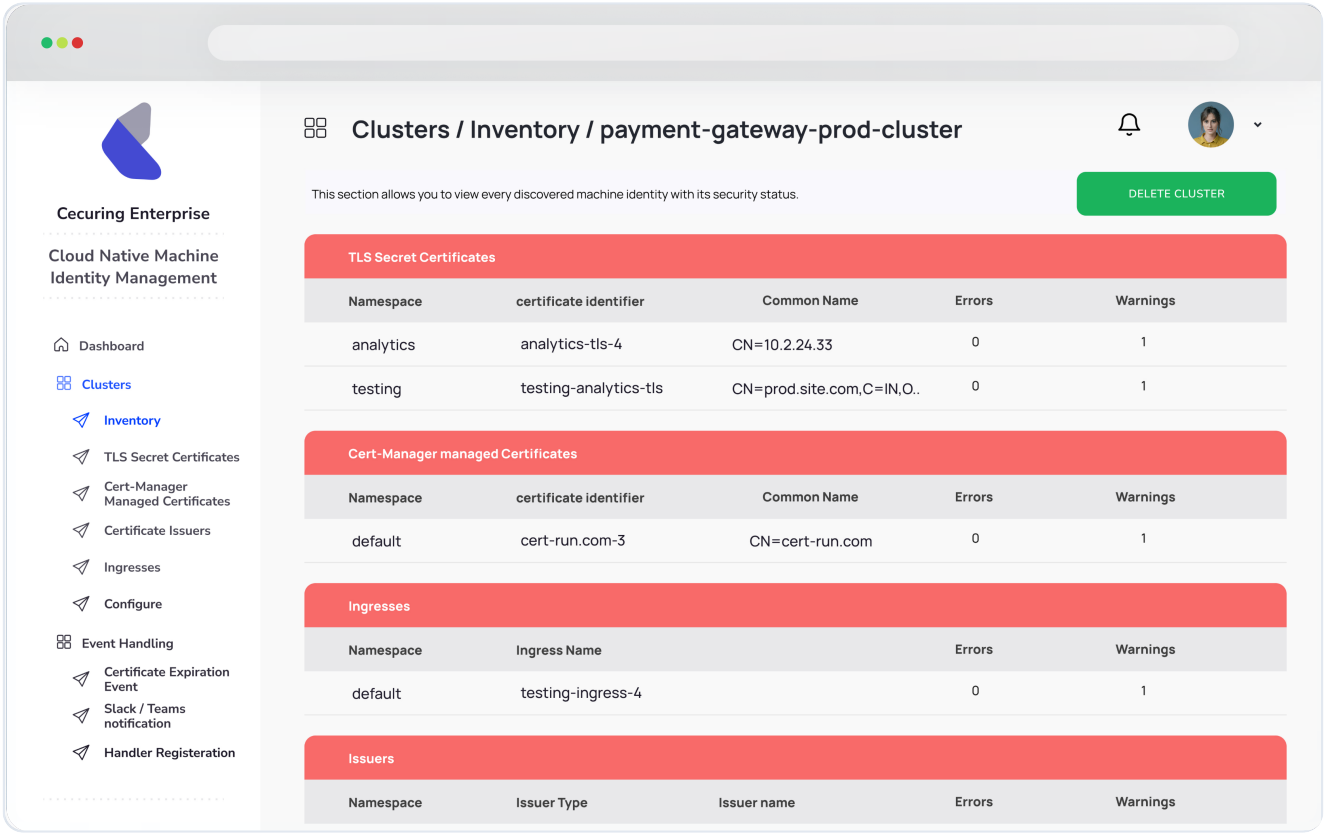
Platform Interface (continued)

Code Signing Management



Signing operations dashboard with HSM key management, approval workflows, and CI/CD pipeline integration.

Cloud-Native Security



Kubernetes certificate management with service mesh mTLS, workload identity, and ephemeral certificate issuance.

Deployment Models

QCecuring supports four deployment models to meet diverse enterprise requirements — from fully managed SaaS to air-gapped government environments.

SaaS (Multi-Tenant)
Fully managed cloud deployment. Zero infrastructure overhead. Automatic updates, scaling, and maintenance. 99.99% SLA with active-active multi-region architecture.

Hybrid
SaaS control plane with on-premises agents. Sensitive operations stay local while management is cloud-hosted. Best of both worlds for regulated industries.

On-Premises
Deploy within your own data center. Full data sovereignty. Docker/Kubernetes-based deployment. Customer-managed infrastructure with vendor support.

Air-Gapped
Fully disconnected deployment for classified/government environments. No internet dependency. Offline updates via secure media. FIPS 140-2 validated.

Technical Architecture

Architecture	Microservices, containerized, Kubernetes-native
Scalability	Horizontal auto-scaling, 1M+ certs/day, 10K+ concurrent operations
High Availability	Active-Active clustering, multi-region, automatic failover
Database	PostgreSQL (primary), Redis (cache), Elasticsearch (search/analytics)
API	REST API, GraphQL, gRPC, Webhooks, CLI tool
Authentication	SAML 2.0, OIDC, LDAP/AD, MFA, API tokens, mTLS
Authorization	Fine-grained RBAC, team-based access, approval workflows
Encryption	TLS 1.3 in transit, AES-256 at rest, HSM-protected platform keys
Audit	Immutable audit log, SIEM export, compliance reporting
Agent	Lightweight agent (< 50MB), mTLS authenticated, auto-update

Professional Services

Our engineering team works directly with your security and infrastructure teams to design, deploy, assess, and migrate cryptographic infrastructure. Scoped engagements with clear deliverables.

PKI Establishment (2-Tier / 3-Tier)	2-4 weeks. Design and deploy complete enterprise PKI hierarchy — offline Root CA with HSM, online Issuing CA, certificate templates, key ceremony, CP/CPS documentation, and operational runbooks.
PKI Health Assessment	1-2 weeks. Comprehensive audit of existing PKI — misconfigurations, ESC vulnerabilities, CA security, CRL/OCSP health, compliance gap analysis, and prioritized remediation roadmap.
Certificate Discovery & Inventory	1-2 weeks. Network-wide TLS scan, cloud certificate inventory (AWS/Azure/GCP), Kubernetes enumeration, SSH key discovery, CT log analysis, and ownership mapping.
CLM Platform Deployment	2-4 weeks. Deploy QCecuring CLM — CA integrations, discovery agents, automation workflows, monitoring dashboards, RBAC setup, team training, and ITSM integration.
Post-Quantum Readiness Assessment	2-3 weeks. Build complete CBOM, quantum risk classification per asset, CNSA 2.0 gap analysis, HNDL exposure mapping, and phased migration roadmap (2026-2033).
Microsoft AD CS Migration	4-8 weeks. Migrate from AD CS to modern PKI — architecture design, parallel operation, phased certificate migration, auto-enrollment replacement, and decommission plan.
SSH Key Audit & Remediation	2-4 weeks. Complete SSH key inventory, ownership mapping, orphan identification, key rotation execution, SSH hardening, and certificate migration roadmap.

Engagement Process

1. Discovery Call
Understand your environment, requirements, and goals. 30-minute call, no commitment.

2. Scoping & Proposal
Define scope, deliverables, timeline, and pricing. Clear SOW before any work begins.

3. Execution
Our engineers work alongside your team — on-site or remote. Regular progress updates throughout.

4. Handoff & Support
Documentation, training, and 30-day post-engagement support included with every engagement.

Training & Certification Programs

Hands-on training programs for enterprise teams. Learn PKI deployment, certificate management, post-quantum readiness, and SSH security from practitioners who build these systems daily. All courses include labs, certificate of completion, and post-training support.

PKI Fundamentals & Enterprise Deployment	2-3 days | Intermediate. Hierarchy design, CA deployment, certificate templates, key ceremonies, HSM integration, CRL/OCSP, CP/CPS documentation, and DR procedures.
Certificate Lifecycle Management	1-2 days | Intermediate. Discovery, monitoring, ACME automation, cert-manager for Kubernetes, renewal at scale, incident response, and 47-day certificate readiness.
Post-Quantum Cryptography Readiness	1 day | Advanced. NIST PQC standards (ML-KEM, ML-DSA), CNSA 2.0 requirements, CBOM, crypto-agility assessment, hybrid deployment, and migration roadmap development.
SSH Key Management & Certificate-Based Access	1 day | Intermediate. Key discovery, rotation automation, SSH CA setup, short-lived certificates with SSO, principal-based access, and compliance requirements.
PKI for DevOps: cert-manager, Vault & ACME	1 day | Advanced. cert-manager deep dive, Vault PKI secrets engine, mTLS with Istio/Linkerd, Infrastructure as Code for PKI, and multi-cluster management.

Training Delivery

- Instructor-led workshops (on-site or virtual)
- Hands-on labs with real infrastructure
- Custom curriculum for teams of 5+
- Certificate of completion for all participants
- Post-training Q&A support (30 days)
- Practitioner-led (not academic instructors)
- Corporate packages for 5-50 participants
- Flexible scheduling (weekday/weekend)
- Lab environments provided (no setup needed)
- Compliance evidence for audit requirements

Support & SLA

Support Tiers	Standard (8x5), Premium (24x7), Enterprise (dedicated TAM)
Response Time	P1: 15 min | P2: 1 hour | P3: 4 hours | P4: 1 business day
Uptime SLA	99.99% (SaaS) | 99.9% (on-premises with HA)
Channels	Portal, Email, Phone, Slack/Teams integration

Compliance & Industries

SOC 2 Type II · ISO 27001 · FIPS 140-2/3 · PCI DSS · HIPAA · eIDAS · CNSA 2.0 · WebTrust

Financial Services · Healthcare · Government & Defense · Technology · Manufacturing · Energy & Utilities · Telecom · Retail

Security

QCecuring is built with security-first architecture. The platform itself is hardened, audited, and certified to meet the most stringent enterprise and government requirements.

Platform Security

- TLS 1.3 enforced for all communications
- AES-256 encryption at rest (all data stores)
- HSM-protected platform signing and encryption keys
- mTLS authentication for all agent communication
- Zero-trust internal architecture (service-to-service mTLS)
- Immutable audit logs with tamper detection
- Role-based access control (RBAC) with least privilege
- Multi-factor authentication (MFA) enforced
- API rate limiting and DDoS protection
- Secrets management (no plaintext credentials)
- Regular penetration testing and vulnerability scanning
- Secure SDLC with code review and SAST/DAST

Industries We Serve

Financial Services & Banking
Certificate management for payment gateways, trading platforms, and core banking. PCI DSS compliance, HSM integration for transaction signing, and PQC readiness for long-lived financial data.

Technology & SaaS
Cloud-native PKI for microservices, automated mTLS for service mesh, code signing for software supply chain, and DevOps-integrated certificate automation at scale.

Government & Defense
Air-gapped deployments, FIPS 140-2/3 validated, CNSA 2.0 compliant. PKI for classified networks, CBOM for national security cryptographic inventory, and post-quantum migration planning.

Telecommunications
Certificate management for 5G infrastructure, SIM/eSIM provisioning PKI, network equipment identity, and subscriber authentication certificate lifecycle.

Healthcare & Life Sciences
HIPAA-compliant certificate management, device identity for medical IoT, S/MIME for protected health information, and cryptographic governance for clinical trial data.

Manufacturing & Automotive
Device identity certificates for IoT/connected products, firmware signing, supply chain integrity verification, and factory provisioning PKI.

Energy & Utilities
OT/ICS certificate management, SCADA system identity, NERC CIP compliance, and cryptographic protection for critical infrastructure control systems.

Retail & E-Commerce
TLS certificate automation for web properties, payment processing certificate governance, PCI DSS compliance, and customer data encryption management.

Ready to See Your Cryptographic Posture?

QCecuring discovers every algorithm, key, certificate, and protocol in your enterprise — then automates remediation with integrated lifecycle m anagement.

Request a Demo

QCecuring Technologies

info@qcecuring.com

www.qcecuring.com