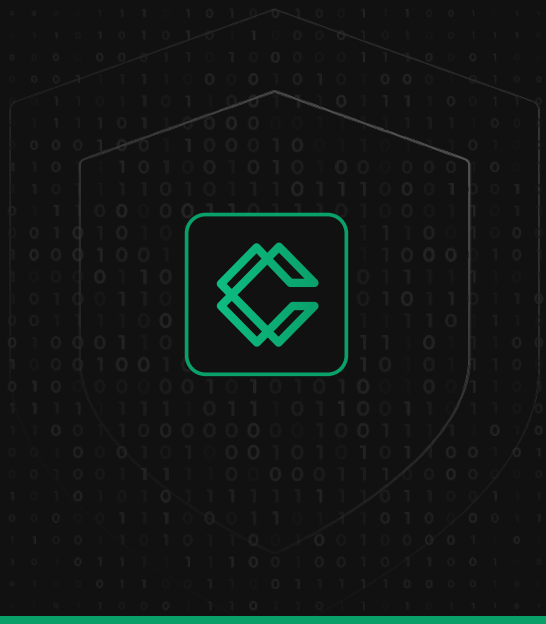
Enterprise Cryptographic Posture Management

Every key, certificate, and algorithm across cloud, on premises, hardware, applications, and source code, in one continuously updated CycloneDX inventory built for the quantum safe era.



20+	***50+***	***30+***
Production Sensors	Dashboard KPIs	Widgets
7+	***70+***	***880+***
Code Languages	Crypto Libraries	API Patterns

The Problem

You Can’t Protect Cryptography You Can’t See

- **Two questions you can’t answer:** are we compliant with current cryptographic standards, and are we ready to migrate to post quantum cryptography? Neither works without knowing what cryptographic assets you own and where they live.
- **Invisible assets:** keys, certificates, and algorithms sit scattered across cloud accounts, on premises servers, HSMs, databases, application code, and developer workstations, invisible until something breaks.
- **The cost compounds:** expired certificates cause outages, outdated algorithms create silent compliance gaps, and audits drag on for weeks because the evidence isn’t in one place.
- **The clock is running:** NIST has finalized its post quantum standards, NSA CNSA 2.0 mandates full adoption by 2030, and NSM-10 and the EU Cyber Resilience Act are already in effect. Without a current inventory you can neither prove compliance today nor migrate in time.

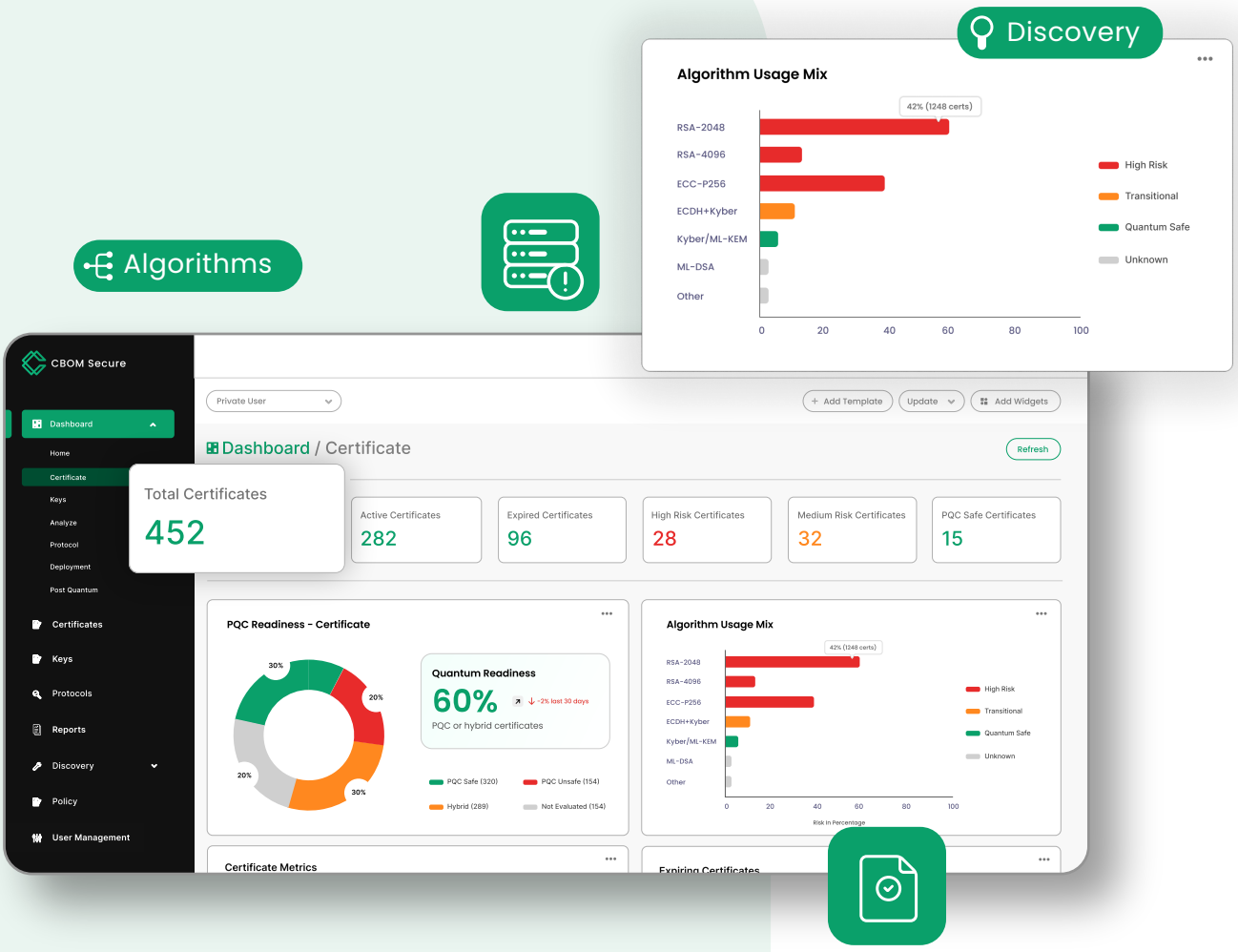
The Solution

One Inventory. Every Cryptographic Asset

- **Continuous by design:** inventories every cryptographic asset across the enterprise, then keeps doing it. Automated discovery, risk analysis, and compliance evaluation run across cloud, hardware, network, files, databases, source code, and key management infrastructure.

- **Standard output:** findings normalize into the vendor neutral CycloneDX 1.6 cryptographic bill of materials standard, surfaced through role based dashboards, time series analytics, and integrated alerting.

- **Beyond certificates:** where competitors stop at certificates and network endpoints, CBOM Secure scans application source code and correlates it with runtime infrastructure, mapping the cryptography hardcoded in your repos to the keys it actually uses in production.



Capability Pillars

Five pillars mapped to the questions security, compliance, and engineering teams need to answer.

Comprehensive Discovery

Eighteen production sensors, ten coverage categories, one inventory. Keys, certificates, and algorithms discovered continuously; clouds, HSMs, databases, source code, binaries, PKI managers. Agents for depth, agentless for reach. Most deployments run both.

Quantum Ready Posture Management

Full NIST quantum-safe coverage: ML-KEM, ML-DSA, SLH-DSA (FIPS 203–205), plus Falcon. Readiness tracked across keys, certificates, and cipher suites — hybrid TLS (X25519MLKEM768) detected in production. Migration runs on live inventory, not spreadsheets.

Crypto Agility Scoring

Every host receives a crypto agility score: a quantified measure of how quickly its algorithms can be swapped when standards change, vulnerabilities surface, or quantum safe migration begins. Foundational for NSM-10, the EU Cyber Resilience Act, and emerging agility frameworks, and measurable today.

Continuous Compliance

Compliance moves from periodic to continuous. Every asset is evaluated against active policies (NIST SP 800-131A, FIPS 140-3, PCI DSS 4.0, CMMC 2.0, and custom policies), with pass and fail rates tracked over time. Time series analytics show posture daily, not at audit time. Audits become a download, not a fire drill.

Risk Intelligence

Four risk bands: Critical, High, Low, Safe. Scoring weighs algorithm strength, expiry, key reuse, cipher mode, IV/nonce handling, KDF parameters, quantum exposure. publicKeySha256 collisions catch reuse; weak signatures flagged; hardware and software keys tracked separately.

Coverage

Production Coverage Across the Cryptographic Surface

Category	Production Coverage	Notes
Cloud Platforms	AWS, Microsoft Azure, and Google Cloud (ACM, IAM, KMS, Key Vault, Cloud KMS)	Native SDK
Hardware Security Modules	Any PKCS#11 HSM or token (Entrust nShield, SoftHSM2, Yubico, and others)	Standards-based
Key Management	Any KMIP server (1.0-2.1), HashiCorp Vault, and Encryption Consulting CertSecure	Native PKI
Network / TLS	Live TLS handshake with certificate, protocol, and cipher enumeration	Live discovery
Directory Services	Microsoft Active Directory and LDAP directories	Standards-based
Database TDE	Oracle, SQL Server, and MySQL encryption state and keys	Native DB
File Systems & Keystores	PEM/CRT files, Java keystores, and ZIP archives across Windows and Linux	Cross-platform
Source Code	7 languages and 70+ cryptographic libraries (GitHub, Git, ZIP)	Static analysis
Binary Scanning	Windows PE and Linux ELF binaries and code-signing certificates	Static analysis

Output & Integration

CycloneDX 1.6 and 1.7:

The open industry standard for cryptographic bill of materials.

Source code outputs:

File level findings, project summaries, and call graph JSON.

REST API:

OpenAPI documented endpoints for every dashboard widget and KPI.

Alerting:

Email and Microsoft Teams notifications before incidents escalate.

Deployment Models

Deploys Into the Infrastructure You Already Run

- **Agentless:** cloud platforms, KMIP servers, network endpoints, databases, and HSMs via standards based APIs.
- **Air gapped:** bootstrap keys generated by the Collector Server and encrypted in advance enable deployment in disconnected environments common to federal, defense, and critical infrastructure customers .
- **Hybrid:** most production deployments combine both modes.
- **With agents**: file systems, OS trust stores, source code repositories, and system discovery.
- **Multi-tenant:** native isolation for multiple organizations on a single deployment, sized for MSSPs and enterprises with separate business units.

COMPLIANCE & REGULATORY ALIGNMENT

CBOM Secure produces the cryptographic inventory evidence current and emerging regulatory frameworks require.

- NIST SP 800-131A
- NIST IR 8547
- FIPS 140-3
- PCI DSS 4.0
- CMMC 2.0
- ISO 27001
- SOC 2
- FedRAMP
- NSM-10
- EU CRA
- DORA

ENCRYPTION CONSULTING

Get in Touch

Encryption Consulting LLC has guided cryptographic strategy at Fortune 500 enterprises. CBOM Secure brings years of advisory practice into a single platform for discovering, scoring, and governing enterprise cryptography.

Schedule A Demonstration →

info@encryptionconsulting.com

www.encryptionconsulting.com