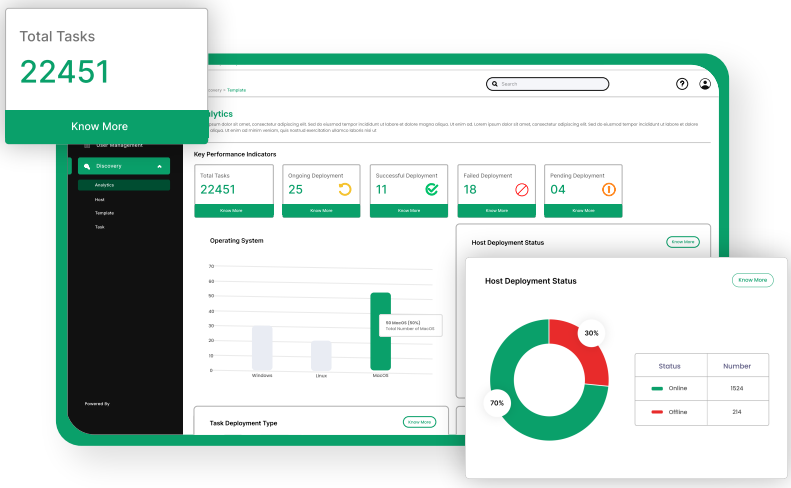
# Deterministic Cryptographic Visibility with Continuous Control

Cryptographic debt and manual audits shouldn't be this complex. CBOM automates cryptographic management, ensuring every algorithm, key, and library is discovered and compliant.

## Introduction

Cryptography is a critical infrastructure, yet it remains hidden and vulnerable. Most organizations lack visibility into where their cryptography lives, creating risks from aging algorithms and hardcoded keys. CBOM solves this by scanning core systems and code to build a centralized inventory of all cryptographic assets. By uncovering hidden risks and ensuring compliance with emerging PQC mandates, we enable a secure, quantum-safe migration. Transform your undocumented cryptography into a governed, audit-ready security control.




## Benefits

- **Post-Quantum Readiness:** Identify and track quantum-vulnerable cryptography to support dependency-aware migration planning.
- **Compliance Evaluation:** Maintain continuously updated, exportable cryptographic inventories aligned with regulatory and security frameworks.
- **Unified Crypto Normalization:** Normalize cryptographic metadata across diverse environments to ensure consistent analysis and governance.
- **Incident Response Acceleration:** Reduce investigation time by correlating cryptographic assets to affected systems and services.
- **Scalable Governance:** Apply cryptographic policies consistently across teams, applications, and technology stacks.
- **Operational Risk Reduction:** Prevent outages and security failures caused by undocumented or deprecated cryptographic usage.

## Deployment Options

CBOM is designed to adapt to diverse enterprise environments, supporting secure deployment models aligned with organizational, regulatory, and data residency requirements.

**On-Premises**

Retain full ownership of cryptographic data for maximum control in isolated or highly regulated environments.

**Cloud-Based**

Leverage elastic scalability and rapid deployment to accelerate visibility without managing infrastructure.

**SaaS**

Simplify your journey with a fully managed service that reduces operational overhead and provides instant insights.

**Hybrid**

Simplify your journey with a fully managed service that reduces operational overhead and provides instant insights.

## Use Cases

**Quantum Exposure Identification:**

Locate quantum-vulnerable algorithms and map their execution dependencies to prioritize PQC migration.

**Audit-Ready Compliance:**

Instantly generate structured, point-in-time inventories to satisfy regulatory reviews and internal security audits.

**Incident Impact Scoping:**

Rapidly identify every application and service affected by a compromised certificate, algorithm, or library for precise containment.

**Supply Chain Risk Assessment:**

Inspect third-party vendor software and open-source components for hidden cryptographic risks before they enter your production environment.

**Legacy Debt Identification:**

Find deprecated algorithms and weak configurations during platform reviews to eliminate outdated cryptographic implementations.

## With CBOM, Organizations Gain Deterministic Cryptographic Control

**Establish Cryptographic Ground Truth:** Create a single, normalized system of record for cryptographic algorithms, keys, certificates, protocols, and libraries across code, binaries, dependencies, and runtime environments.

**Differentiate Presence from Execution:** Identify which cryptographic components are merely present versus those actively executed in production, eliminating false positives and incomplete risk assessments.

**Correlate Cryptography to Systems and Flows:** Map cryptographic assets to applications, services, and data paths to understand operational dependencies, impact radius, and downstream risk.

**Accelerate Cryptographic Incident Response:** Rapidly assess exposure during algorithm deprecations, certificate failures, or vulnerability disclosures by understanding exactly where and how cryptography is used.

**Enable Structured Cryptographic Modernization:** Identify legacy, weak, and quantum-vulnerable cryptography and prioritize remediation based on execution context, dependency criticality, and business impact.

*CBOM delivers continuous cryptographic intelligence that reduces uncertainty, shortens response cycles, and supports long-term cryptographic resilience.*

## Key Capabilities

- **Cryptographic Asset Discovery :** Identify algorithms, keys, and libraries across code, binaries, and runtime environments in real time.
- **Metadata Normalization:** Standardize fragmented data into a unified schema for consistent analysis across teams and tools.
- **Dependency Correlation:** Map assets to active execution paths to pinpoint real-world usage and potential blast radius.
- **Policy-Based Evaluation:** Instantly flag weak or deprecated cryptography against internal policies and global standards.
- **Quantum Risk Identification :** Surface quantum-vulnerable assets to build a data-driven, prioritized PQC migration roadmap.
- **Governance and Reporting :** Generate exportable, audit-ready inventories for rapid compliance and incident response.

ENCRYPTION CONSULTING

## Get in Touch

Get in Touch Ready to take control of your cryptographic supply chain? Contact us today to learn how Encryption Consulting's CBOM can transform your enterprise with a secure, scalable, and compliant discovery solution tailored to your business requirements. Drop us an email at info@encryptionconsulting.com or call us at +1-469-815-4136