WHITEPAPER

Why Every Organisation Needs a CBOM

You cannot secure — or migrate — cryptography you cannot see. A Cryptography Bill of Materials is the foundation every post-quantum programme is built on.

The Inventory Problem Underneath the Quantum Problem

Most conversations about post-quantum readiness start with algorithms: which one to adopt, when to switch, what it replaces. That conversation is premature for almost every organisation, because it assumes something that usually isn't true — that the organisation already knows where its cryptography lives.

In practice, cryptographic decisions accumulate silently over years: a TLS configuration set once and never revisited, a signing key generated for a project that outlived its original owner, a third-party library with an embedded algorithm nobody chose deliberately. Quantum risk isn't solved by picking the right algorithm. It's enabled by visibility into what you actually have — and that visibility has a name: a Cryptography Bill of Materials, or CBOM.

What a CBOM Actually Is

A CBOM is a structured, machine-readable inventory of every cryptographic asset in use across a system or organisation — extending the same logic that a Software Bill of Materials (SBOM) applies to software dependencies, but focused specifically on cryptography. A complete CBOM captures:

- Algorithms and key lengths in use (e.g. RSA-2048, ECC P-384, ML-KEM-768)
- The libraries implementing them, and their versions
- Certificate details and where key material is stored (HSM, software keystore, etc.)
- Protocols and configurations in use — TLS versions, cipher suites, signing workflows

The industry is converging on **OWASP CycloneDX** as the standard machine-readable format for expressing this — the same ecosystem already widely used for software bills of materials

— which means a CBOM built to that standard is portable across tooling, auditors, and regulators, not locked into one vendor's proprietary format.

Why "We'll Discover It During Migration" Doesn't Work

It's tempting to treat discovery as something that happens organically once a migration project starts. In practice this produces exactly the outcome you'd expect: a migration team finds new cryptographic assets throughout the project, timelines slip, and the organisation never has a moment where it can say with confidence "we've found everything that matters."

A CBOM built ahead of migration — and kept continuously current, not refreshed as a one-off audit — turns that uncertainty into a known, bounded scope. It's the difference between planning a migration and discovering one as you go.

From Inventory to Exposure

A CBOM by itself is a list. Its value comes from what it enables next: mapping each cryptographic asset to the business service it actually protects, so exposure can be assessed in terms that matter — not "we have 4,000 certificates using RSA-2048" but "our customer payment gateway depends on twelve of those certificates, and three are due to expire this quarter."

This is the difference between a compliance artefact and an operational one. Enterprise Cryptographic Exposure Management (ECEM) treats the CBOM as a living foundation — continuously updated as infrastructure changes — that every later stage of the lifecycle (assessment, prioritisation, migration planning, monitoring) builds directly on top of.

Building One Without a Six-Month Project

Building a CBOM does not require instrumenting every application by hand. Agentless, read-only discovery — scanning network protocols, querying PKI and HSM systems, inspecting source repositories and cloud configurations — can establish a credible first-pass inventory in weeks, not quarters, without deploying agents to production systems or touching the cryptographic material itself.

Quantum Sentinel builds and maintains this inventory automatically as part of Enterprise PQC Discovery, presenting it as a living Enterprise CBOM rather than a static report that's out of date the day it's generated.

Registered as a limited company in England and Wales under company number: 17317113. Registered office: 71-75 Shelton Street, Covent Garden, London, WC2H 9JQ, United Kingdom.