WHITEPAPER

Understanding Enterprise Cryptographic Exposure Management (ECEM)

A practical guide to the discipline of discovering, understanding, and reducing cryptographic exposure — and why it matters before the quantum era, not after it.

Executive Summary

Every organisation relies on cryptography to secure data, identities, applications and communications. Yet very few organisations can confidently answer where cryptography is used, which algorithms protect their critical systems, which certificates and keys are nearing end of life, which systems rely on quantum-vulnerable cryptography, or which business services should be prioritised first.

Without these answers, quantum readiness becomes guesswork. This is the gap that Enterprise Cryptographic Exposure Management (ECEM) closes.

Enterprise Cryptographic Exposure Management (ECEM) is the discipline of discovering, understanding, and reducing cryptographic exposure — the business risk created by unknown, weak, outdated, or quantum-vulnerable cryptography across an organisation. Just as Vulnerability Management helps organisations identify and prioritise software vulnerabilities, ECEM helps organisations identify, measure and reduce cryptographic exposure.

Why Cryptographic Exposure Matters Now

Quantum computing may still be years away. Cryptographic exposure already exists today.

Every day, organisations continue to deploy cryptographic algorithms, certificates, keys and libraries across applications, cloud platforms, databases, APIs and infrastructure. Over time, these cryptographic assets become difficult to track, understand and manage. The longer cryptography remains invisible, the harder — and more expensive — the transition to post-quantum cryptography becomes.

You can't prepare for tomorrow if you don't understand today's cryptographic exposure. Encrypted data intercepted and stored today can potentially be decrypted once sufficiently capable quantum computers exist — a risk commonly referred to as "harvest now, decrypt later." For any organisation handling data with a

multi-year sensitivity window, that risk is already active, regardless of when large-scale quantum computers actually arrive.

How ECEM Fits Alongside Existing Security Disciplines

Yesterday	Today	Tomorrow
Vulnerability Management	Exposure Management	**Enterprise Cryptographic Exposure Management**
Applications	Infrastructure	**Cryptography**
CVEs	Attack Paths	**Cryptographic Exposure**
Patch Systems	Reduce Exposure	**Prepare for the Quantum Era**

ECEM is not simply cryptographic discovery. It is the continuous discipline of discovering, assessing, prioritising and reducing cryptographic exposure across the enterprise — building on the same operational maturity that Vulnerability Management and Exposure Management brought to applications and infrastructure, and applying it to cryptography specifically.

The Five Questions Every Organisation Should Be Able to Answer

Most organisations know their vulnerabilities. Very few know their cryptographic exposure. ECEM starts by making these five questions answerable with evidence, not assumption:

- Where is cryptography being used?
- Which algorithms protect our critical systems?
- Which certificates and keys are nearing end of life?
- Which systems rely on quantum-vulnerable cryptography?
- Which business services should be prioritised first?

The ECEM Lifecycle

A continuous cycle for managing cryptographic exposure and preparing for the quantum era.

01 · Discover

Discover cryptographic assets across your enterprise — endpoints, servers, applications, databases, PKI, HSMs, cloud environments and source code repositories.

02 · Inventory

Build a comprehensive inventory of all cryptographic assets: a living Enterprise CBOM (Cryptography Bill of Materials).

03 · Assess

Assess cryptographic exposure and business impact using business context and recognised industry guidance, including NIST and CNSA 2.0.

04 · Prioritise

Prioritise risks and focus remediation where it delivers the greatest reduction in cryptographic exposure.

05 · Transition

Plan and execute migration to post-quantum cryptography with a practical, phased roadmap.

06 · Monitor

Continuously monitor and improve cryptographic posture as the environment changes.

Standards This Discipline Draws On

ECEM is not a proprietary framework invented in isolation — it operationalises a set of standards that already define what "quantum-safe" and "cryptographically sound" mean in practice:

- FIPS 203 (ML-KEM) — the NIST standard for module-lattice-based key encapsulation, the primary post-quantum key-establishment algorithm.
- FIPS 204 (ML-DSA) and FIPS 205 (SLH-DSA) — NIST's module-lattice and stateless hash-based digital signature standards.
- NIST SP 800-131A — guidance on transitioning cryptographic algorithm and key-length usage.
- CNSA 2.0 — the NSA's Commercial National Security Algorithm Suite 2.0 timeline for national security systems.

Where to Start

ECEM does not require a big-bang programme. Most organisations begin with discovery — simply establishing where cryptography exists across the environment — before moving into assessment, prioritisation, and migration planning. The discipline is designed to be continuous: exposure changes as infrastructure changes, so ECEM is a standing capability, not a one-time audit.

Quantum Sentinel is the Enterprise Cryptographic Exposure Management platform built around this exact lifecycle — deployed on-premises or within your private infrastructure, collecting cryptographic metadata only, and never copying private keys, certificates, sensitive files, or application data.

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.