corelight

White paper

Post-quantum readiness and the mandate for automated cryptography discovery and inventory

The critical challenge of post-quantum cryptography

The impending arrival of cryptographically relevant quantum computers (CRQCs) presents a profound security challenge to federal agencies. Much of the cryptographic infrastructure protecting sensitive government data, communications, and critical infrastructure today relies on public-key algorithms that are vulnerable to quantum attack. This transition—known as the post-quantum cryptography (PQC) migration—is now formally driven by federal mandates and national security policy, including NSM-10, OMB M-23-02, CNSA 2.0, the Department of War (DoW) PQC strategies, and CNSS Policy #15. Collectively, these directives impose immediate and material requirements on agencies to inventory cryptographic dependencies, plan for algorithm transition, and achieve cryptographic agility across enterprise and operational environments.

The foundational first step in PQC readiness—and the most significant hurdle for large, complex federal environments—is comprehensive cryptographic discovery and inventory. Agencies cannot protect what they cannot see. They must accurately inventory all existing cryptographic assets, including algorithms, key lengths, cipher suites, certificates, and protocols, across their diverse network and application landscape. Without this visibility, a PQC migration plan cannot be properly scoped, budgeted, or executed, leaving federal systems exposed to future "harvest now, decrypt later" attacks and increasing the risk of non-compliance with federal policy mandates.

The power of network visibility drives PQC readiness

This initial phase demands a non-disruptive, highly scalable, and accurate solution that can provide a single source of truth for cryptographic asset inventory across on-premises, cloud, and air-gapped environments. While the challenge of automated cryptography discovery and inventory (ACDI) spans multiple approaches—CI/CD, SDLC, vulnerability management, asset and certificate inventory, application development, and more—the power of network data provides a unique and comprehensive means of identifying and capturing cryptographic details across complex environments.

Corelight Open Network Detection and Response (Open NDR) provides the foundational data federal agencies need to successfully execute the PQC inventory phase and track migration progress over time. By leveraging deep packet inspection (DPI) and full metadata extraction from on-premises and cloud network traffic, Corelight enables comprehensive ACDI through completely passive monitoring. Corelight transforms raw network traffic into rich, structured data (logs) that deliver a definitive, real-time inventory of cryptographic usage. This inherently scalable and non-invasive approach is well suited for mission-critical federal networks and helps agencies operationalize the discovery and continuous visibility requirements outlined in CNSS Policy #15, CNSA 2.0, and broader DoW and federal post-quantum cryptography strategies, providing the data foundation needed to plan, prioritize, and execute PQC migration with confidence.

Key ACDI capabilities Corelight supports

Federal requirement	Corelight capability
Comprehensive cryptographic discovery across the enterprise *CNSS Policy #15; CNSA 2.0 transition planning*	**Full-spectrum protocol visibility** Corelight's deep packet inspection (DPI) identifies protocols independent of port number through dynamic protocol detection, ensuring visibility into cryptographic usage that traditional port-based monitoring misses. This includes PQC-relevant protocols such as SSL/TLS, SSH, and SMB across on-premises, cloud, and hybrid environments.
Accurate inventory of cryptographic algorithms and parameters *PQC readiness, algorithm transition planning*	**Granular cryptographic metadata extraction** For every observed connection, Corelight extracts and logs critical cryptographic metadata, including negotiated cipher suites and elliptic curves, RFC-compliant key exchange algorithms, certificate (X.509) attributes, and detailed SSH parameters. This data provides the authoritative technical foundation required for ACDI.
Attribution of cryptographic usage to systems and applications *Asset ownership, remediation prioritization*	**Application and service identification** Using advanced network fingerprinting techniques, Corelight identifies and logs applications and services in use. Unique connection identifiers (UIDs) enable correlation of cryptographic details to specific applications, services, and infrastructure components.
Ongoing visibility, reporting, and compliance tracking *Continuous monitoring; audit readiness*	**Actionable dashboards and reporting** Extracted cryptographic data feeds directly into inventory and compliance dashboards, enabling agencies to assess PQC readiness, identify unmanaged or non-compliant cryptographic usage, and generate scheduled ACDI reports to support internal governance and external compliance validation.
Integration with existing security and data architectures *Enterprise-scale implementation; long-term compliance and trending*	**Seamless integration and long-term data retention** Corelight's flexible export options and compact data formats integrate seamlessly with federal security ecosystems, including SIEM, data lakes, and XDR platforms. This supports custom logging, long-term storage, and historical tracking of cryptographic changes required for sustained PQC compliance.

Federal civilian agencies and the DoW are being directed to establish a usable inventory of cryptographic assets to understand the scope, scale, and complexity of PQC migration. Corelight not only delivers a proven, operational NDR dataset for defenders protecting today's networks, but also serves as the foundational data source for both real-time and historical visibility into cryptographic usage. This visibility enables agencies to baseline current-state risk, prioritize remediation, and chart a defensible path toward full cryptographic agility and PQC migration. Corelight's Open NDR platform itself is planned to transition to PQC-aligned cryptography beginning in 2026.

To learn more about post-quantum readiness, request a demo at

https://corelight.com/contact

info@corelight.com | 888-547-9497