Cryptographic Discovery — How do we break away from the pack?

Response to Customer Inquiry: How Venari's Approach to Cryptographic Discovery is Different

Unlike traditional discovery tools that rely on active polling, agent-based scanning, or scheduled probes, Venari passively monitors all TLS traffic at the network layer—seeing every cryptographic exchange across all endpoints and servers, without requiring agents, scans, or predefined targets.

The Problem with Traditional Cryptographic Discovery

Most discovery tools use active scanning, which introduces several limitations:

- Requires prior knowledge of endpoints and servers—You can only scan what you already know, meaning blind spots remain for unmanaged, unknown, or misconfigured assets.
- Creates network noise—introducing synthetic traffic that can interfere with operations.
- Relies on scheduled polling—capturing only snapshots of cryptographic posture, leaving gaps between scans.
- Requires endpoint agents—adding complexity, increasing operational overhead, and requiring ongoing maintenance.
- Introduces operational friction—requiring change control processes and impact assessments before deployment, increasing deployment time and risk.

How Venari is Different

Venari operates passively at the network layer, monitoring all TLS sessions, certificate exchanges, and cipher negotiations in real time via a tap, mirror port, or packet broker in AWS or Azure—without requiring prior knowledge of endpoints or servers, agents, or scans. This enables:

- Visibility into all cryptographic activity across the network—capturing everything, everywhere, all the time across both known and unknown endpoints and servers.
- No dependency on asset inventories—unlike active tools, which require preconfigured targets, Venari automatically discovers all cryptographic endpoints dynamically.
- No operational friction—no extra load, no security risks, no endpoint dependencies, and no need for change control approvals that delay implementation.

Turning Insight into Actionable Compliance & Risk Management

Venari doesn't just observe cryptographic activity—it translates insights into actionable intelligence by:

- Mapping acquired data against NIST, NCSC, and custom compliance policies to validate regulatory adherence.
- Organizing cryptographic risks using a RAG (Red, Amber, Green) priority system, providing an immediate risk posture overview.
- Providing suggested remediations, enabling security teams to proactively mitigate cryptographic vulnerabilities before they become threats.
- Offering protocol and asset intelligence, giving organizations a clear understanding of real-world cryptographic usage to inform future PQC migration strategies.

Why This Matters for You

Comparison: Active Scanning vs. Venari's Passive Cryptographic Observation

The table below highlights the key differences between traditional active scanning and Venari's passive cryptographic observability, illustrating why Venari provides a more comprehensive, real-time, and frictionless approach to cryptographic discovery.

Feature	Active Scanning (Traditional Discovery Tools)	Venari Passive Observation (Network-Layer TLS Monitoring)
Visibility Scope	Limited to known endpoints and servers	Captures all endpoints and serversacross the network in real time
Discovery Method	Periodic, scheduled scans	Continuous, passive monitoring of all TLS traffic
Coverage Gaps	Misses unknown, unmanaged, or misconfigured assets	No blind spots—sees everything, everywhere, all the time
Impact on Performance	Generates network noise, adds scan-related overhead	Zero impact—no extra traffic or performance degradation
Change Control & Friction	Requires approval and assessment before deployment	No operational friction—no changes needed to endpoints or infrastructure
Data Collection Method	Uses synthetic requests or endpoint agents	Monitors real-world cryptographic usage passively
Compliance & Risk Management	Snapshots at predefined intervals	Real-time risk posture with RAG prioritization and suggested remediations
Cryptographic Intelligence	Limited to what the scan captures at a given moment	Continuous insight into TLS sessions, certificate exchanges, and ciphers
Regulatory Mapping	Requires manual correlation with compliance frameworks	Automatically maps to NIST, NCSC, and custom cryptographic policies
Adaptability to PQC Migration	Requires frequent manual updates for evolving standards	Seamless, ongoing validation of cryptographic changes with PQC readiness insights

Key Takeaway

Venari removes the limitations of active scanning, offering unmatched cryptographic visibility across all endpoints and servers—without impact, friction, or operational blind spots. By passively monitoring network-layer TLS activity, Venari delivers continuous discovery, real-time risk analysis, and compliance validation that traditional tools cannot match.

Bridge your knowledge gap.
Visit: www.venarisecurity.com

Venari Security Ltd.

16 Great Queen Street, London,
WC2B 5AH, United Kingdom
+44 (0)20 7294 7749
info@venarisecurity.com

About Venari Security

Venari Security provides organisations with advanced visibility into their encrypted attack surface, ensuring regulatory compliance and privacy adherence through our cryptographic discovery tool.

Our focus is on crypto agility which helps you assess both external and internal cryptographic risks, preparing your business now and for the quantum future.