Internal Discovery ‘Low-Touch’

Datasheet for
PQC Readiness Assessment

At a Glance

Product: Venari Low-Touch Sensor

Deployment time: <4 hours

Coverage: 100% of relayed internal encrypted traffic (on-prem, cloud, hybrid) plus 100% of targeted cryptographic assets

Decryption: None – zero privacy impact

PQC Score delivered: Within 30 minutes of first traffic and / or assessment

Frameworks auto-mapped: NIST, PCI DSS 4.0, HIPAA, DORA, NCSC-NL, GDPR

Solution Summary

A single lightweight sensor hosted by a strategic Third-Party Service Provider, turns existing traffic mirrors into a cryptographic observatory and becomes a strategic probe to Identify cryptographic assets. In one ‘low-touch’ deployment you gain:

- Real-time TLS/SSL inventory (CBOM)
- 0–100 Post-Quantum Readiness Score
- Continuous drift alerts
- Board-ready compliance reports in plain English

No agents. No inline appliances. No decryption.

contact@venarisecurity.com
venarisecurity.com

The Enterprise Crypto Blind-Spot

Segment	Typical Visibility Gap
Legacy Data Centers	Unknown Ciphers and Protocols
Cloud VPCs	No-Span Port Mirroring
Branch and IOT	Slioed Firewalls
M&A Networks	Zero Baseline

How ‘Low-Touch’ Works – 4 Steps

1. Our sensor, hosted by a Third-Party Service Provider connects into any environment—on-premises, cloud, or third-party data centers.

2. Redirect your current SPAN, TAP, or ERSPAN ports toward the Third-Party Service Provider sensor. Zero network reconfiguration required.

3. Active assessment of TLS, SSH & IPsec across all reachable assets, plus real-time traffic analysis for complete coverage.

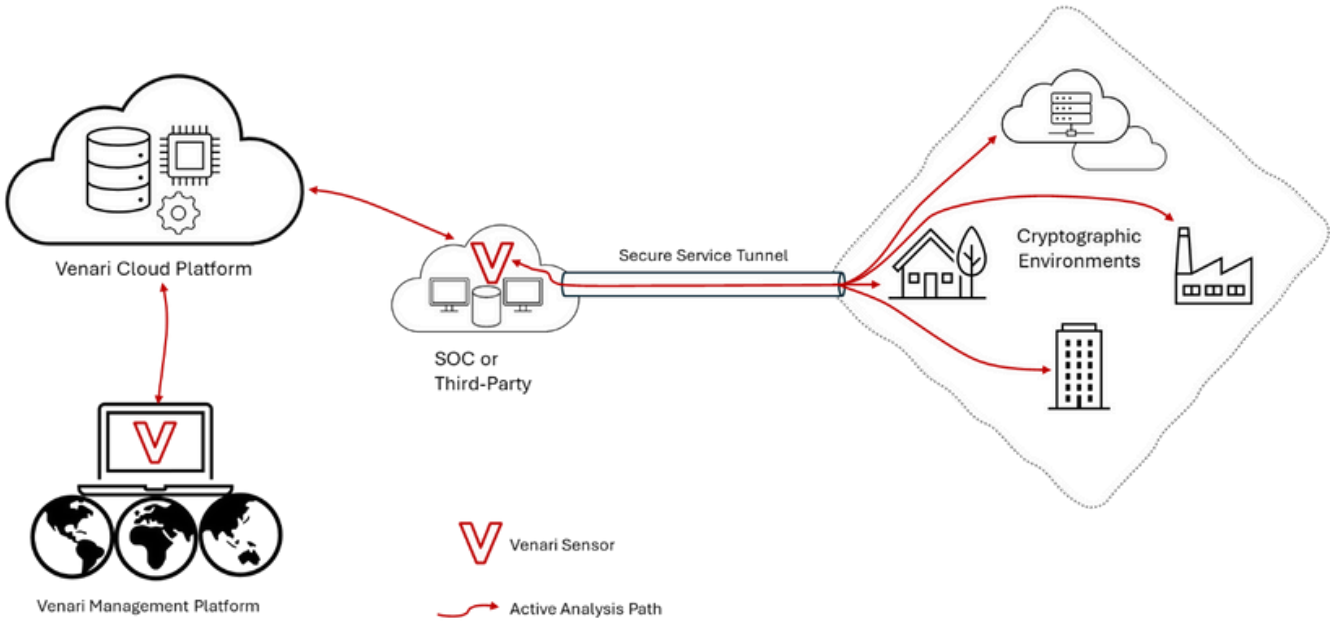
4. In-memory processing delivers instant visibility into your cryptographic posture. See vulnerabilities immediately.

The Result: Complete Cryptographic Visibility

contact@venarisecurity.com
venarisecurity.com

VENARI SECURITY

Deployment Architecture: Low-Touch System Integration



Leveraging existing connections from trusted Third-Party Service Providers, Venari sensors ingest relayed traffic from cryptographic environments and undertake assessments toward targets, to identify cryptographic assets, quantify risks and report findings, either against compliance frameworks or regulatory standards. Guided remediation provides usable insights to users, helping drive migration to post-quantum safe security practices and illustrate at an executive levels, the cryptographic posture of networked assets within an organisation.

Product:

Low-touch sensor

Deployment time:

<6 hours

Coverage:

100% of internal encrypted traffic + targeted crypto assets.

Decryption:

Zero data. Zero privacy impact.

PQC score:

in <30 minutes.

Auto-mapped:

NIST, PCI, HIPAA, DORA, NCSC-NL, GDPR.

contact@venarisecurity.com
venarisecurity.com

VENARI SECURITY

Sample 24-Hour Output

Cryptographic Bill of Materials (CBOM) Auto-generated, SBOM-compatible JSON/CSV with every algorithm, library, and endpoint.
PQC Readiness Score 0–100 weighted index:

- **40 % Vulnerable algorithms (RSA<3072, ECC<256)**
- **30 % Certificate hygiene**
- **20 % Protocol downgrade risk**
- **10 % Migration feasibility**

Compliance Map One-click evidence packs for 6 frameworks.

Drift Alerts SIEM webhook the moment a TLS 1.0 session appears.

Sample 24-Hour Output

CBOM excerpt

1.2 M TLS sessions analysed

14% still negotiating RSA-1024

42 applications using ECC-P-256

Top offender: legacy SAP gateway (10.11.4.0/24)

PQC Score: 61/100 Recommendation:

"Replace 3,400 certs with Kyber hybrids in <90 days."

TRY FREE TODAY

Step 1: Engage trusted Third-Party Service Provider

Step 2: Redirect traffic and identify target assets

Step 3: Receive executive report + remediation playbook

Step 4: Review guided remediation and reports

contact@venarisecurity.com

venarisecurity.com

VENARI SECURITY