Internal Discovery ‘Low-Touch’

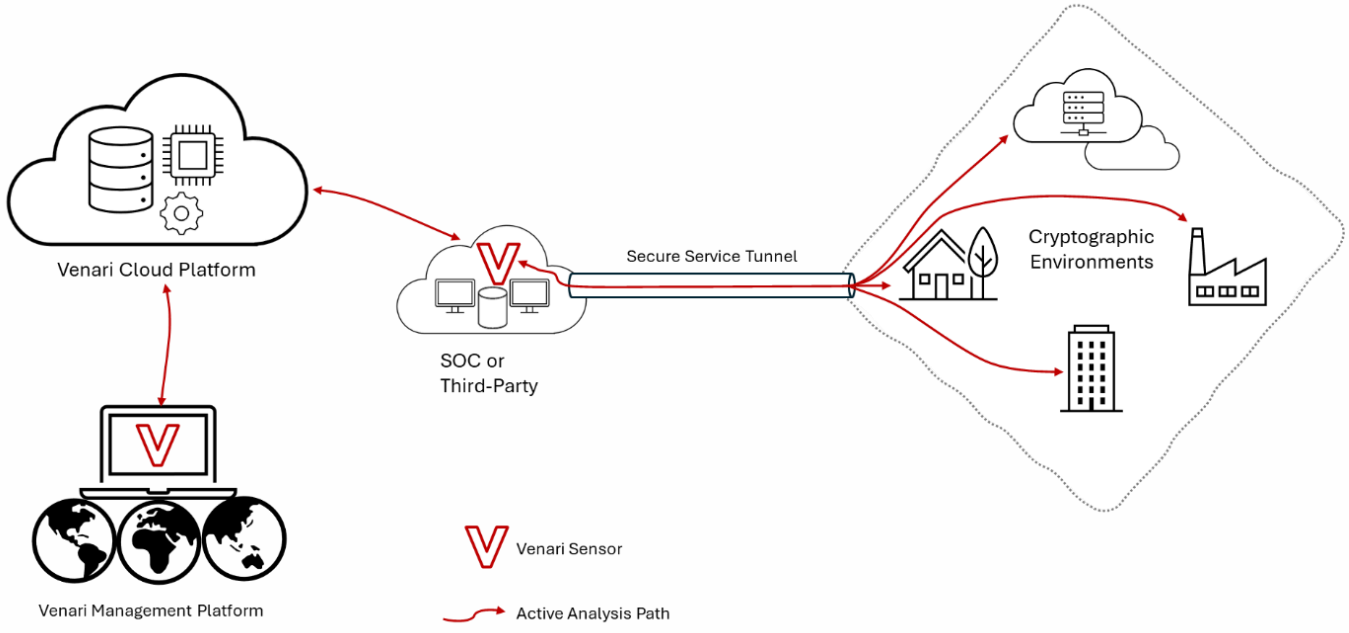
Technical Brief for PQC Readiness Assessment

The Venari Adaptive Cryptographic Intelligence Platform is an AI-powered, automated, real-time cryptographic monitoring and PQC readiness solution. It employs a low-touch assessment methodology by deploying active and passive sensors within Third-Party Service Provider infrastructure that leverage existing connections to your systems.

Sensors passively monitor network traffic relayed by mirrors or span ports over secure links, to access encrypted traffic across the entire organisational infrastructure. Sensors undertake active assessments to target specific networks or systems, The solution supports on-premises, cloud, and hybrid environments — without requiring agent installations, traffic decryption, or performance-impacting interventions.

This enables continuous TLS/SSL session analysis, IPsec or SSH inspection, asset discovery and inventory, vulnerability detection, and compliance orchestration, supporting frameworks including NIST SP 800-57, PCI DSS 4.0, HIPAA, and NCSC-NL guidelines. The solution's core innovation lies in its TLS-first crypto-agility focus, providing a scalable foundation for PQC transitions.

Deployment Architecture: Low-Touch System Integration



contact@venarisecurity.com

venarisecurity.com

Venari's Low-Touch approach minimises deployment complexity

Sensor Deployment:
Lightweight, virtual sensors positioned within management infrastructure of Third-Party Service Providers communicate via secure tunnels to key termination destinations of your organisation. The sensors ingest mirrored traffic via protocols like ERSPAN or TAP aggregation and combine with lightweight assessment capabilities ensuring full-spectrum visibility without inline processing

Data Flow Pipeline:

a. Traffic Ingestion: Sensors capture encrypted sessions in real-time, parsing metadata (e.g., cipher suites, key exchange methods) combined with active scanning of assets within the sensor.
b. Entity Normalization: Traffic is correlated to assets (e.g., endpoints, applications) using Venari's entity resolution engine.
c. Artificial Intelligence Contextual Analysis: Advanced LLM models classify applications, prioritize risk, help in guided migration, and score PQC exposure.
d. Insight Generation: Outputs feed into CBOM databases, compliance engines, and alerting systems.

Scalability and Resilience:
The platform auto-scales horizontally in containerised environments (e.g., Kubernetes), with zero-downtime updates. Integration with existing SOC tools (e.g., Splunk, ELK Stack) via RESTful APIs and syslog ensures seamless data export for SIEM correlation.

This architecture guarantees <1% overhead on monitored traffic, enabling rapid rollout (typically <24 hours) across global environments.

Core Technical Features

Venari's toolkit addresses cryptographic assurance holistically:

Feature	Technical Description	PQC/Compliance Integration
Combination of Real-Time TLS/SSL, SSH & IPsec monitoring and assessment	Passively monitored session handshakes and responses from active assessments are monitored for protocol versions (TLS 1.0–1.3), cipher strengths (e.g., AES-256-GCM), and certificate chains using libraries like OpenSSL. Flags deprecated ciphers (e.g., RC4, SHA-1) via pattern matching.	Identifies quantum-vulnerable primitives (RSA <2048-bit, ECC <256-bit) per NIST IR 8413; triggers PQC migration alerts.
Cryptographic Bill of Materials (CBOM) Generation	Dynamically builds asset inventories from traffic and response-derived metadata, exporting in SBOM-compatible formats (e.g., CycloneDX JSON). Includes algorithm mappings and dependency graphs.	Catalogs PQC gaps; automates NIST CSF 2.0 mappings for crypto inventory requirements.
Multi-Framework Compliance Mapping	Rule-based engine aligns observed cryptographic usage against framework controls (e.g., PCI DSS Req. 4.1 for TLS 1.2+). Supports custom policy extensions via YAML configs.	Validates PQC readiness against NCSC-NL quantum guidelines; generates audit trails with EVIDENCE tags for HIPAA.
PQC Readiness Scoring	The proprietary algorithm computes a 0–100 score based on vulnerability heatmaps (e.g., % of RSA-dependent sessions). Uses weighted factors like algorithm entropy and migration feasibility.	Benchmarks against ETSI QS standards; simulate quantum attack vectors (e.g., Shor's algorithm impact on ECC).

Core Technical Features

Venari's toolkit addresses cryptographic assurance holistically:

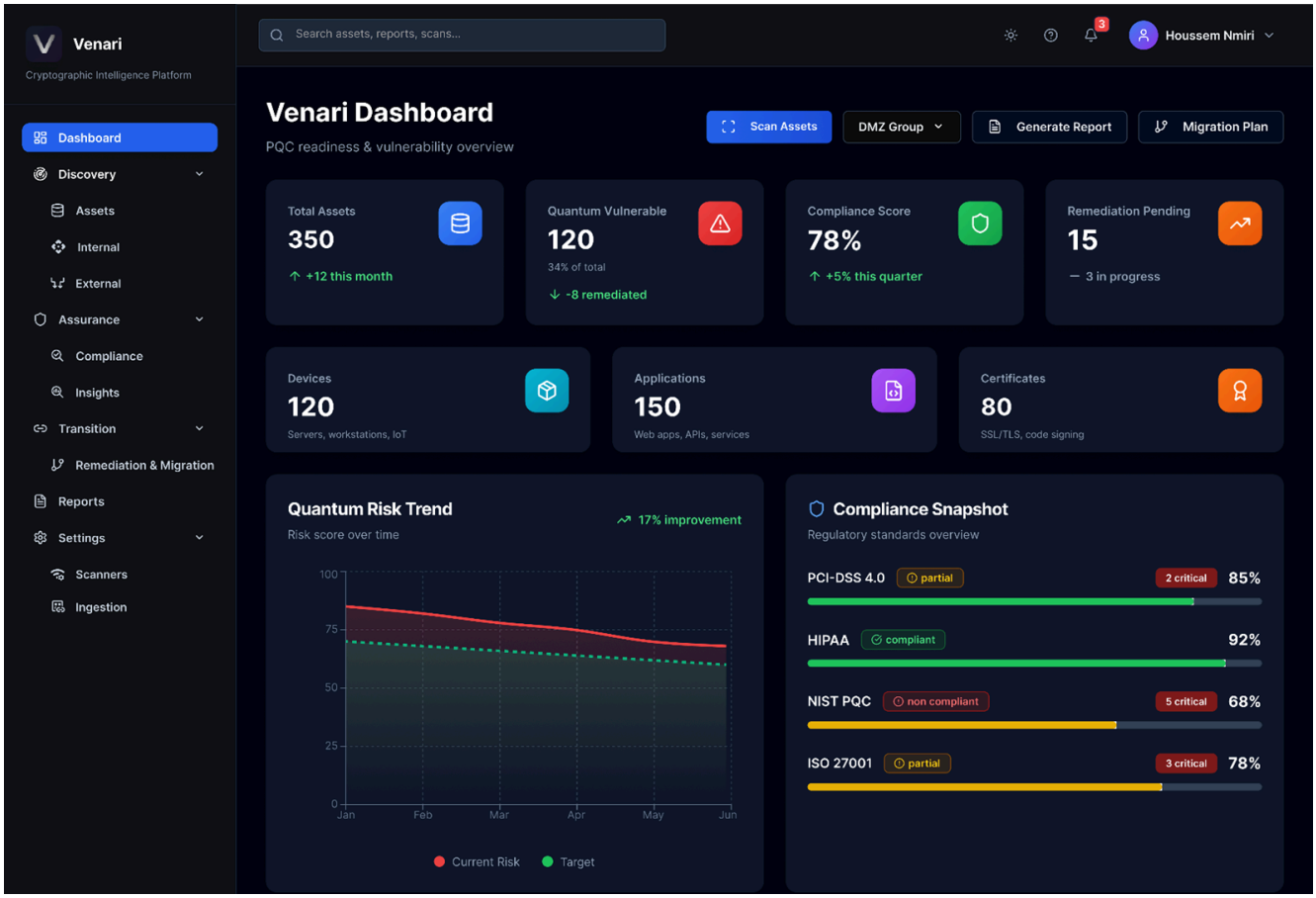
Feature	Technical Description	PQC/Compliance Integration
AI Automation	Use Artificial Intelligence to help summarise the key information from billions of collected data points, recognise business applications and create remediation recommendations	CBOM by business application and guided remediation plan to reduce risk and prepare for PQC
Executive Dashboards and Reports	Grafana-based visualizations with NLG (natural language generation) via models like GPT-4 for summaries. Exports PDFs/CSV with embedded metrics.	PQC trend reports (e.g., "45% of sessions vulnerable; recommend Kyber hybrid in 6 months").
API & SIEM Integrations	OpenAPI 3.0 endpoints for query/pull (e.g., /cbom/export), with webhook support for push alerts. Native connectors where required.	Enables SOC playbook automation, e.g., auto-ticketing PQC issues in ServiceNow.

Benefits for Technical Teams

- **Zero-Decryption Privacy:** Maintains data-in-transit integrity, compliant with GDPR/CCPA.
- **Easy to Deploy:** Deploy the service via partners and have access to the different segments of the organisation.
- **Extensibility:** Modular design allows custom PQC plugins (e.g., integrating CRYSTALS-Kyber validation).

Minimum System Requirements :

The Venari Adaptive Cryptographic Intelligence Platform redefines cryptographic assessments by embedding PQC readiness into Third-Party Service Provider operations, delivering low-touch visibility that scales with your infrastructure.



Engage with Venari now to explore the Adaptive Cryptographic Intelligence Platform.

contact@venarisecurity.com

venarisecurity.com

VENARI SECURITY

Sample 24-hour Output

Example 24-hour discovery
- 1.2 million TLS sessions
- 3,400 SSH connections
- 86 IPsec tunnels were assessed

Within 24 hours, the dual-engine methodology, which integrates active scanning of TLS, SSH, and IPSec configurations with real-time traffic analysis, produced these findings from a single enterprise network. Venari identified:

- **14% of cryptographic assets were still negotiating RSA-1024**
- **42 applications were using ECC-P-256**
- **The top offender, a legacy SAP gateway**

This process required no agents and caused no operational disruption, providing immediate results.

Proof Of Concept

Engage your Third-Party Service Provider to establish connectivity and define assessment routines.

Connect and assess by directing the sensor at the core switch mirror and designated endpoints. The remaining processes are automated.

Review the results as an executive report, which includes a prioritised remediation playbook. or download a CycloneDX-compatible CBOM.

contact@venarisecurity.com
venarisecurity.com

VENARI SECURITY