High-Touch Technical Brief

VENARI SECURITY

Technical Brief for
PQC Readiness Assessment

High-Touch Objectives

The High-Touch deployment option is specifically engineered to deliver visibility and continuous governance of the only three protocols that matter for enterprise cryptographic risk in 2025–2030:

- TLS/SSL (including TLS 1.3, QUIC, DTLS)
- SSH (all versions, key-exchange, and host-key algorithms)
- IPec/IKE (IKEv1 & IKEv2, ESP/AH, pre-shared keys and certificate-based)
-

No other protocols are in scope – this focused approach guarantees depth, accuracy, and performance where it matters most without having to decrypt communications.

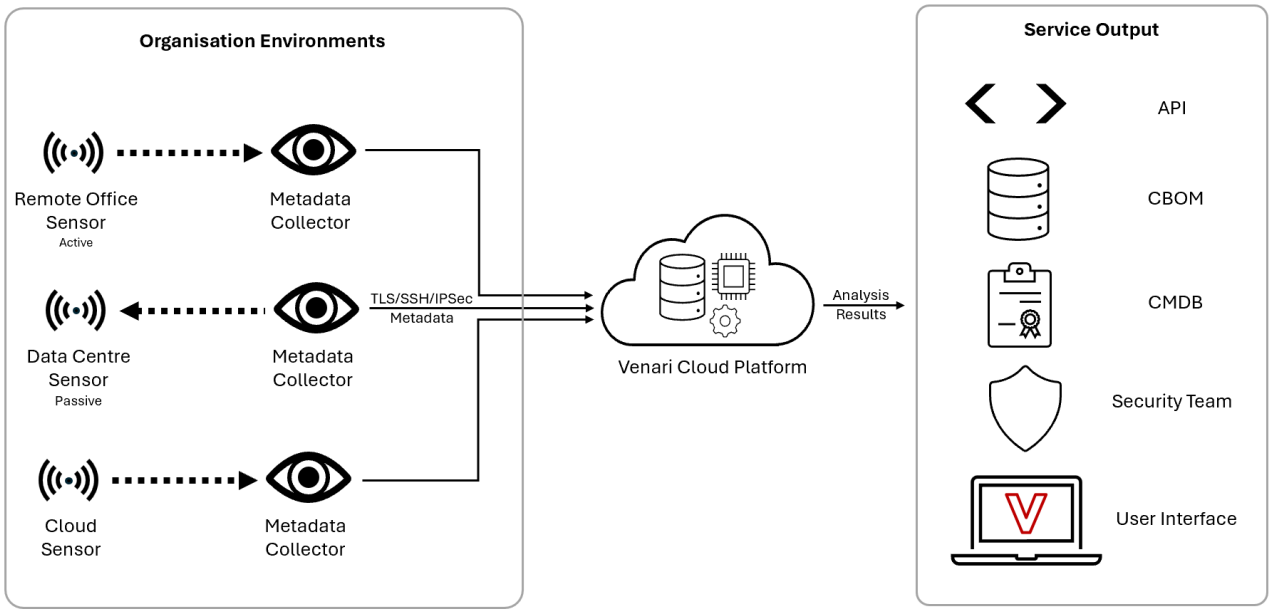
Specific High-Touch Objectives

1. **TLS/SSL** – Capture every handshake even when traffic never crosses a central mirror point (e.g., east–west, container overlay, endpoint-to-endpoint).
2. **SSH** – Discover every host key, user key, and key-exchange algorithm (RSA-SHA1, ECDSA P-256, ed25519, etc.) across servers, network devices, jump hosts, and Git/CI systems.
3. **IPsec** – Inventory every IKE policy, transform set, certificate, and pre-shared key in site-to-site, remote-access, and mesh VPNs – including tunnels that terminate on firewalls, routers, and cloud VPN gateways.
4. **PQC Readiness at Binary Level** – Identify every instance of quantum-vulnerable RSA ≤ 2048, ECC ≤ P-256, and RSA-SHA1 SSH keys, regardless of whether they ever appear in live traffic.
5. **Zero Blind Spots Guarantee** – Prove 100% coverage of all TLS, SSH, and IPSec implementations across air-gapped, OT, mainframe, and highly segmented environments.

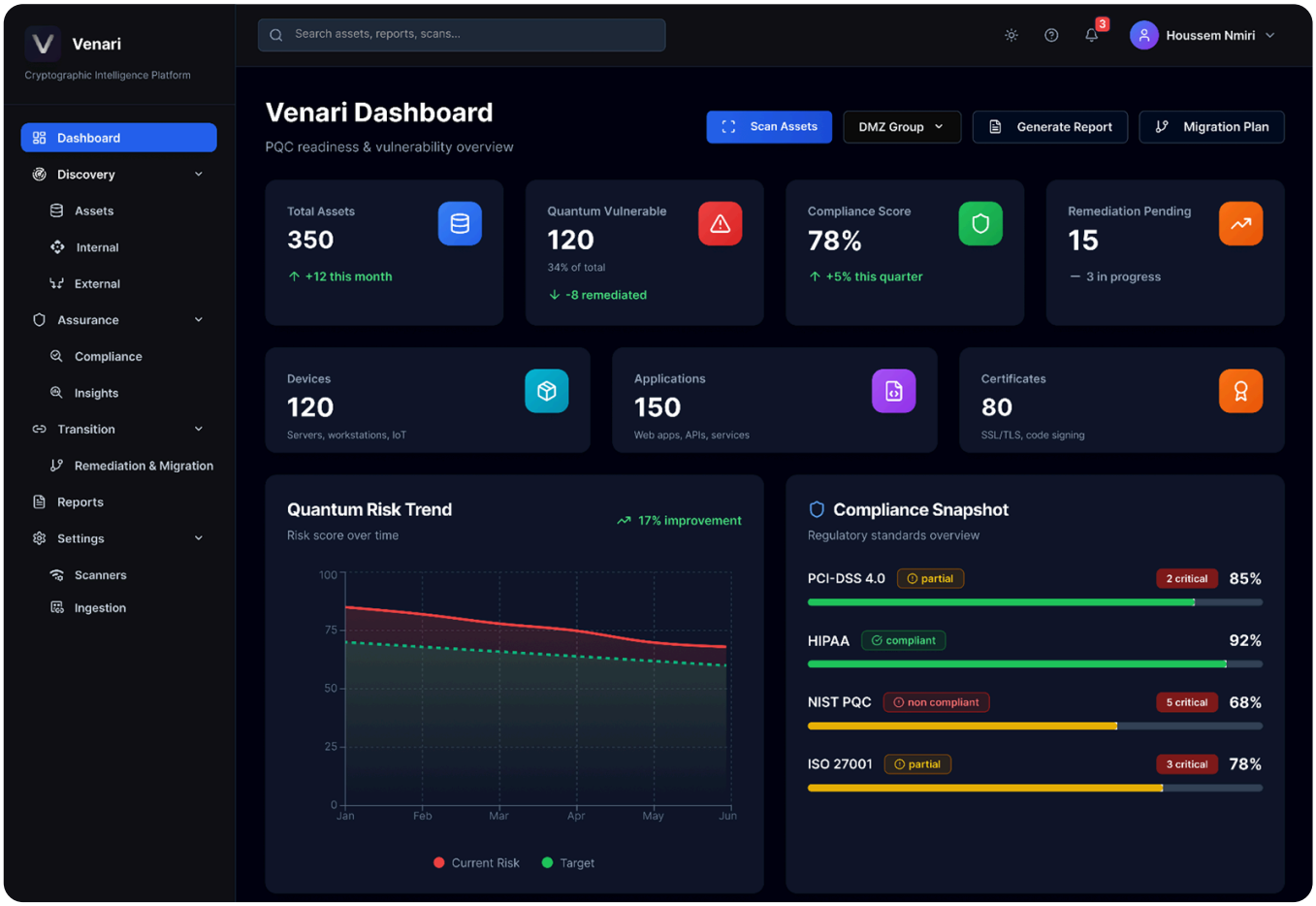
contact@venarisecurity.com
venarisecurity.com

High-Touch Internal Discovery Architecture and Dashboard

The following diagram illustrates the High-Touch example comprising sensors covering offices, Data and Cloud environments, to cover a variety of different networks found within an organisation:



The Venari Platform illustrates the cryptographic posture of an organisation; engage with Venari to request your demonstration.



contact@venarisecurity.com

venarisecurity.com

Added Value for Technical & Security Engineering Teams

Benefit	Technical
Single Source of Truth	One platform now owns TLS, SSH, and IPec inventory no more spreadsheet chaos across network, server, and endpoint teams
SSH Host-Key Risk Elimination	Auto-discovers every RSA-SHA1 and 1024-bit DSA host key on network devices and jump hosts – immediate remediation tickets created.
IPSec PSK Discovery	Extracts, detects and analyse every key across all the environments
PQC Migration Confidence	now exactly how many RSA-2048 certificates, ECC P-256 keys, and SSH ed25519-vs-RSA ratios exist before choosing Kyber/Dilithium hybrids
Audit Proof Evidence	Cryptographic Dependency Graph exports signed JSON evidence for every TLS, SSH, and IPec instance – accepted by ECB, FCA, and NYDFS examiners.

Proof Of Concept

Obtain the sensor by downloading a virtual version, which is operational within minutes.

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

Review the results in an executive report, which includes a prioritised remediation playbook.

contact@venarisecurity.com
venarisecurity.com

VENARI SECURITY