detect. correct. protect.
Cybr IQ

CYBRIQ • FOR COMPLIANCE & AUDIT

SpacesIQ

Real evidence for HIPAA, PCI, SOC 2, NIST, and CMMC — for every device on every port in every building.

Auditors no longer accept "trust the spreadsheet." SpacesIQ produces the device evidence they're now asking for.

Printers, displays, badge readers, kiosks, HVAC controllers, contractor laptops, IoT sensors, medical devices, OT gear — quietly invisible to NAC and CMDB until the audit asks where they are. **SpacesIQ extends CybrIQ's patented Device DNA™** to every switch port, on every floor, in every building — and produces audit-defensible evidence at the layer regulators are now probing.

THE AUDIT FINDINGS YOU KEEP GETTING

- **Inventory inaccuracy** — CMDB and ground truth diverge faster than your reconciliation cycle
- **Unmanaged devices on regulated networks** — POS, medical, contractor laptops, IoT
- **Missing access logs** — devices that connected without being recorded
- **Unsubstantiated attestations** — claims your controls work, no evidence the auditor accepts
- **Stale documentation** — last network diagram is from a previous reorg

WHAT SPACESIQ PRODUCES

- **Live authoritative inventory** — every device on every port, fingerprinted at Layer 1
- **Real-time anomaly evidence** — when a known device behaves differently, when an unknown one connects
- **Place-port-owner-policy attribution** — every record tied to where, what, who, why
- **Exportable evidence** — CSV, SIEM correlation, ITSM ticket trail, regulator-ready reports
- **Continuous attestation** — daily verification that the regulated network is what you said it was

FRAMEWORK	CONTROL AREA	EVIDENCE SPACESIQ PRODUCES
HIPAA Security Rule	§164.308 Administrative; §164.310 Physical; §164.312 Technical	Live device inventory, access workflow, anomaly alerts, audit-trail exports
PCI DSS 4.0	2.x Configure Components; 9.x Physical Access; 12.5.1 Inventory	Per-port device record, unauthorized-device detection, time-stamped access logs
SOC 2 (CC)	CC6.1 Logical & Physical Access; CC7.2 Monitoring	Continuous-monitoring evidence, anomaly alerts, exportable trail across all locations
NIST 800-53	CM-8 Component Inventory; PE-3 Physical Access; SI-4 System Monitoring	Layer 1 component inventory, location attribution, anomaly evidence
CMMC 2.0	CM.L2-3.4.1 Hardware Inventory; AC.L2-3.1.1 Access Control	Authoritative live hardware inventory across regulated facilities

PROOF — REGIONAL HEALTHCARE NETWORK

A regional healthcare network ran a SpacesIQ pilot across multiple buildings. Within the first **2 weeks**, the discovery alone surfaced thousands of unmanaged medical devices the CMDB had never recorded — including HIPAA-relevant exposures that would have failed the next regulator review. Findings surfaced first internally, on the compliance team's timeline, with exportable evidence ready for the auditor.

WHERE THE EVIDENCE IS MOST OFTEN MISSING

- **Healthcare** — HIPAA §164.310 Device & Media Controls across clinics
- **Retail / payments** — PCI 9.x and 12.5.1 across stores
- **Federal contractors** — CMMC CM.L2-3.4.1 across regulated facilities

WHY THIS IS ON THE AUDIT RADAR NOW

- 2025 wave of supply-chain hardware compromises drove regulator focus to physical-layer evidence
- HIPAA Security Rule updates require continuous device inventory, not point-in-time

- **Financial services** — SOC 2 CC6/CC7 across multi-tenant offices
- **Manufacturing** — NIST 800-53 CM-8 / PE-3 across plant floors

- SOC 2 Trust Services Criteria emphasize ongoing monitoring of CC6/CC7 controls
- CMMC 2.0 explicitly demands authoritative hardware inventory across regulated environments

Deployment signal: Standard pilot completes in **2 weeks** — typically before the next quarterly attestation cycle.

Book a compliance walkthrough
shai.moshe@cybriq.io

Download the audit-evidence sample
Anonymized log export · ready for auditor review