detect. correct. protect.

Cybr IQ

CYBRIQ • FOR COMPLIANCE & AUDIT

RoomIQ

Audit-defensible evidence of every device in every meeting room.

The auditor asks what was in the room. RoomIQ has the answer, time-stamped, attributed, and exportable.

HIPAA, PCI, SOC 2, NIST, and CMMC reviews increasingly probe physical-layer controls in meeting spaces — especially after the 2025 supply-chain hardware incidents. NAC and EDR don't generate evidence at the layer auditors are asking about. **RoomIQ does** — using a patented **Device DNA™** fingerprint that produces audit logs tied to device identity, location, time, and approval workflow.

WHAT AUDITORS ARE ASKING

- **Hardware inventory accuracy** — does what's installed match what's recorded?
- **Unauthorized device detection** — when something new connects, who sees it?
- **Approval and access workflow** — who authorized the device, and is that documented?
- **Tamper evidence** — can you prove a device hasn't been substituted?
- **Supply-chain integrity** — does the camera you bought match the camera that's running?

WHAT ROOMIQ PRODUCES

- **Per-device audit log** — Layer 1 fingerprint, port, location, time, owner, approval status
- **Tamper-evident records** — electrical fingerprint of each device through its lifecycle
- **Authorization workflow** — allow / alert / block actions tied to named approver
- **Exportable evidence** — CSV, SIEM correlation, ITSM ticket trail
- **Continuous attestation** — daily verification that installed devices haven't been swapped

FRAMEWORK	CONTROL AREA	EVIDENCE ROOMIQ PRODUCES
HIPAA Security Rule	§164.310(d)(1) Device & Media Controls	Per-device fingerprint log, location attribution, authorization workflow
PCI DSS 4.0	9.x Physical Access; 12.5.1 Inventory	Real-time inventory, unauthorized-device detection, time-stamped access logs
SOC 2 (CC)	CC6.1 Logical & Physical Access	Continuous-monitoring evidence, anomaly alerts, exportable activity trail
NIST 800-53	CM-8 Information System Component Inventory; PE-3 Physical Access	Layer 1 component inventory, tamper evidence, named-approver records
CMMC 2.0	CM.L2-3.4.1 Authoritative Hardware Inventory	Authoritative live hardware inventory at the physical layer

PROOF — SUPPLY-CHAIN IMPLANT CAUGHT BEFORE AUDIT CYCLE

A Fortune 500 enterprise rolled out 200+ identical conference kits. Paperwork, serials, photos all matched the procurement record. RoomIQ flagged **one camera** whose electrical fingerprint didn't match the fleet — in **under 20 minutes**, before it joined the network. Without Layer 1 verification, the audit-period attestation would have been wrong, and the next regulator review would have found it.

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