detect. correct. protect.
Cybr IQ

CYBRIQ • FOR SECURITY LEADERSHIP

RoomIQ

Conference-room hardware just became a board-oversight category. Here's what to put in your next quarterly review.

The board is asking what's actually in the room. RoomIQ is what you bring to that conversation.

Boardrooms host M&A discussions, executive-protection sessions, regulated meetings, and material-information conversations. Underneath each one — dongles, hubs, USB devices, and contractor-installed gear that bypass NAC and EDR. **NAC sees "a camera." Attackers see a doorway.** RoomIQ closes the door at Layer 1 with a patented **Device DNA™** fingerprint that can't be spoofed in software.

WHAT YOU CAN'T ANSWER TODAY

- **USB impostors** presenting as keyboards, NICs, or storage — invisible to EDR until they act
- **Tampered cameras and microphones** with hidden implants the supply chain didn't catch
- **Rogue HDMI / wireless adapters** dropped in by contractors "just for the meeting"
- **Unmanaged hubs and switches** behind displays — no MAC, no agent, no telemetry
- **Supply-chain swaps** that match the paperwork but not the silicon

WHAT ROOMIQ GIVES THE CISO

- **Board-reportable evidence** — every device that joined every meeting, by name, time, location, approval
- **First-contact detection** — allow / alert / block before the device transmits a packet
- **Stack-native integration** — SIEM/XDR, NAC/EDR, ITSM workflows already in production
- **Audit-defensibility** — physical-layer logs that hold up under regulator review

Why this is on your desk now: The 2025 wave of supply-chain hardware compromises — TP-Link, the CISA AA22 alert series, the renewed Volt Typhoon advisories — has turned conference-room hardware into an explicit board-oversight category. Audit committees are asking for Layer 1 evidence. AV integrators don't have it. NAC and EDR don't generate it. The CISO who walks into the next quarterly review with this question already answered controls the conversation.

CONTROL ALREADY IN YOUR STACK	WHAT IT SEES	WHAT ROOMIQ ADDS
NAC	MAC + 802.1X identity (spoofable)	**Layer 1 electrical fingerprint (un-spoofable)**
EDR / XDR	Behavior on the host OS, after the agent runs	**Behavior at the wire — before any OS exists**
Asset inventory / CMDB	What you bought, last reorg	**What's plugged in, right now, and how it differs from intended**
SIEM correlation	Activity across devices the SIEM was told about	**The devices the SIEM was never told about**

PROOF — SUPPLY-CHAIN IMPLANT CAUGHT BEFORE FIRST USE

A Fortune 500 enterprise rolled out 200+ identical conference kits. Paperwork, serials, photos all matched. RoomIQ flagged **one camera** whose electrical fingerprint didn't match the fleet — in **under 20 minutes**, before it joined the network. A supply-chain implant. Without Layer 1 validation, it would have entered production and stayed invisible until exfiltration was already happening.

WHERE THIS LANDS IN YOUR PROGRAM

- **Board reporting** — quantified evidence of executive-meeting hardware integrity

THREE QUESTIONS FOR YOUR NEXT QUARTERLY REVIEW

- **M&A diligence** — verified room hygiene during deal-stage conversations
- **Executive protection** — Layer 1 verification of devices in principal-attended meetings
- **Compliance posture** — HIPAA, PCI, SOC 2, NIST, CMMC audit-evidence material

? *"How do we know the camera installed last quarter is still the same camera?"*

? *"Who signs off when a contractor plugs a hub into the boardroom?"*

? *"Can we prove what was in the room during the M&A call?"*

Deployment signal: Standard pilot completes in **2 weeks**. Stack-native. No new cabling, no rip-and-replace.

Book a CISO walkthrough
shai.moshe@cybriq.io

Get the threat-model brief
Layer 1 attack surface, controls map, integration spec