detect. correct. protect.

Cybr IQ

CYBRIQ • CONFERENCE-ROOM SECURITY AT LAYER 1

RoomIQ

Your boardroom looks safe. The hardware in it isn't.

Pro cameras. Big displays. Sleek touch panels. Underneath: a doorway.

Under every modern boardroom lives a tangle of dongles, hubs, extenders, and USB gadgets that quietly bypass NAC, EDR, and asset inventory. **NAC sees "a camera." Attackers see a doorway.** RoomIQ closes the door at Layer 1 — using a patented **Device DNA™** fingerprint that can't be spoofed in software.

WHAT'S INVISIBLE IN EVERY CONFERENCE ROOM

- **USB impostors** posing as keyboards or NICs
- **Tampered cameras and microphones** with hidden implants
- **Rogue HDMI / wireless adapters** dropped in "just for the meeting"
- **Unmanaged hubs and switches** behind displays and podiums
- **Supply-chain swaps** matching the paperwork but not the silicon

WHAT ROOMIQ DOES ABOUT IT

- **Identifies** every device at the physical layer (including MACless / quiet ones)
- **Allows, alerts, or blocks** at first contact — before the device ever talks
- **Logs** what connected, where, when, and who approved it
- **Integrates** with your SIEM/XDR, NAC/EDR, and ITSM stack

Why now: After the wave of supply-chain hardware compromises in 2025 — TP-Link, the CISA AA22 alerts, the renewed Volt Typhoon advisories — boards have made conference-room hardware an explicit oversight category. The question is no longer if Layer 1 evidence is required. It's whether you have it.

THE CONTROL ALREADY IN YOUR STACK	WHAT IT SEES	WHAT ROOMIQ ADDS
NAC	MAC + 802.1X identity (spoofable)	**Layer 1 electrical fingerprint (un-spoofable)**
EDR	Behavior on the host OS	**Behavior at the wire — before any OS exists**
Asset inventory	What you bought, when	**What's plugged in, right now**

PROOF — SUPPLY-CHAIN IMPLANT CAUGHT BEFORE FIRST USE

A Fortune 500 enterprise rolled out 200+ identical conference kits. Paperwork, serials, and photos all matched. RoomIQ flagged **one camera** whose electrical fingerprint didn't match the fleet — in **under 20 minutes**, before it joined the network. Not a quirk; a supply-chain implant. Without Layer 1 validation, it would have blended in forever.

WHERE ROOMIQ LANDS

- **CISO** — board-reportable evidence of every device that joined every meeting
- **Security operations** — first-contact detection, integrated with your existing stack
- **Compliance** — audit-ready logs for HIPAA, PCI, SOC 2, NIST, CMMC reviews
- **Executive protection** — verified hardware in M&A and regulated meetings

THREE QUESTIONS TO ASK IN YOUR NEXT ROOM REVIEW

- ? *"How do you know the camera installed last quarter is still the same camera?"*
- ? *"Who signs off when a contractor plugs a hub into the boardroom?"*
- ? *"Can your security team prove what was in the room during the M&A call?"*

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

Request a demo

Download the technical brief

shai.moshe@cybriq.io

Layer 1 Device DNA™ architecture & integrations