detect. correct. protect.

CYBRIQ • AV INTEGRATOR PARTNER PROGRAM

RoomIQ

Conference-room hardware is now a board-oversight item. AV integrators are the supplier of record.

The Layer 1 security answer becomes part of your bid.

AV integrators are the only suppliers who know what hardware is actually in the room. CISOs are starting to ask.

Every conference room you ship contains dozens of devices that bypass the customer's security stack. USB hubs, HDMI extenders, wireless presenters, contractor laptops, vendor-managed cameras and microphones. NAC reads VLAN identity. EDR runs on the host operating system. Neither tool reads the device itself. RoomIQ adds a Layer 1 reading: a patented electrical fingerprint (**Device DNA™**) that is unique per device and cannot be spoofed in software.

WHAT YOUR CUSTOMER'S STACK DOES NOT SEE

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

WHAT ROOMIQ ADDS AT LAYER 1

- **Identifies** every device at the physical layer, including MACless and quiet ones that never authenticate
- **Allows, alerts, or blocks** at first contact, before the device exchanges a single packet
- **Logs** what connected, where, when, and who approved it (per port, per minute)
- **Integrates** with the customer's stack: SIEM and XDR, NAC and EDR, ITSM (ServiceNow, Jira)

Why it is on board agendas now: Conference-room hardware moved into board-oversight territory after the supply-chain compromises of 2025. Reference points the customer's CISO is reading: the FCC review of TP-Link, the renewed CISA Volt Typhoon advisories, the CISA AA22 hardware-implant series, and the SEC disclosure rule that treats undocumented hardware as a material-misstatement risk.

THE CONTROL ALREADY IN THE CUSTOMER'S STACK	WHAT IT SEES (AND WHAT IT MISSES)	WHAT ROOMIQ ADDS
NAC (ISE / ClearPass)	MAC + 802.1X identity. Both are software-set and spoofable.	**Layer 1 fingerprint set in silicon, un-spoofable**
EDR (CrowdStrike / SentinelOne)	Behavior on the host OS. No agent on a hub, codec, or unmanaged adapter.	**A read of the device at the wire, before any OS runs**
Asset inventory	What was purchased and when. Not what is plugged in right now.	**Continuous per-port record of currently connected devices**

PROOF — SUPPLY-CHAIN IMPLANT CAUGHT BEFORE FIRST USE

A Fortune 500 enterprise rolled out 200+ identical conference kits across a multi-site refresh. Paperwork, serial numbers, and acceptance photos all matched. RoomIQ identified **one camera** whose Layer 1 fingerprint did not match the rest of the fleet. The mismatch surfaced in **under 20 minutes** of the appliance going live, before the device joined the network. It was not a manufacturing variation. It was a supply-chain-stage implant. Without a Layer 1 reading, the device would have stayed in the asset register indefinitely, indistinguishable from its 199 siblings.

WHY THIS WINS YOU DEALS

- **Security-justified bids.** Average ticket lift in partner-led deals: **18–32%** vs. the same room without a security SKU.
- **Recurring revenue.** Per-room monthly SKU, 36-month default term. Partner GM envelope: **35–50%** by tier and volume.
- **Reduced churn at CISO transitions.** Evidence packs are durable; the new CISO inherits the relationship.
- **Engineering moat.** Layer 1 fingerprinting is US-patented (US 11,528,162 B2). Commodity vendors cannot copy the engine.

DISCOVERY QUESTIONS TO OPEN THE DOOR

- ? *"How do you know the camera installed last quarter is still the same camera you installed?"*
- ? *"Who signs off when a contractor plugs a hub into the boardroom for a vendor demo?"*
- ? *"Which devices were in the room during the last earnings call or M&A discussion?"*
- ? *"How would you show evidence on inventory completeness if the auditor asked tomorrow?"*

Pilot: two weeks end-to-end. **Day 1** appliance racked, no new cabling. **Week 1** first per-port inventory. **Week 2** evidence pack plus SIEM and ITSM integration verified.

Apply to the Partner Program
shai.moshe@cybriq.io

Schedule a co-sell briefing
30 min · CISO playbook + indicative SKU and margin sheet