RoomIQ

Cybr IQ
detect. correct. protect.

The blind spot nobody audits

Executive Conference rooms look immaculate: pro cameras, big screens, sleek touch panels. Under the table? A tangle of dongles, hubs, extenders, and USB gadgets that quietly **bypass traditional security checks**. If you trust what a device *claims* to be (its MAC, driver, or label), you're trusting the attacker. Traffic analysis and NAC see "a camera." Attackers see a doorway.

Where attackers hide

- USB impostors that pretend to be keyboards or network cards
- Tampered cameras/mics with hidden implants
- Rogue wireless/HDMI adapters slipped in "just for the meeting"
- Unmanaged hubs/switches behind displays and podiums

Trust the language of electricity

Instead of asking a device who it is, CybrIQ.io measures how it behaves electrically. Every device has a unique, low-level "Device DNA"—a physical fingerprint that can't be spoofed with software tricks.

- Identify every device at the physical layer (even MACless/quiet ones)
- Allow / alert / block at first contact—before a device participates on your network
- Prove what connected, where, when, and why you allowed or blocked it

Real Life Examples

A global enterprise rolled out hundreds of identical conference kits. Paperwork, serials, and images all looked legit. CybrIQ.io flagged one camera whose electrical fingerprint didn't match the fleet. It wasn't a quirk—it was a supply-chain implant built to capture more than meeting minutes. Without physical-layer validation, it would've blended in forever.

What we catch the moment it appears

- Cameras & mics: spot tampering *before* a conversation is compromised
- Wireless dongles: recognize and block unknown connectors on plug-in
- Displays & controllers: verify they are genuine, not modified hardware
- USB accessories: stop HID/USB-NIC impostors before damage is done

Outcomes your execs will care about

- Prevent eavesdropping in boardrooms and deal rooms
- Cut risk at the door: block unapproved hardware automatically
- Shrink incident time: precise room/port/device evidence in seconds
- Hand auditors proof: inventory, policies, events, and exception logs tied to place and owner
- Fit your stack: integrates with SIEM/XDR, NAC/EDR, and ITSM for tickets and automated response

How to start (fast)

- Pick 3–5 high-trust rooms (board, trading, ops).
- Connect CybrIQ.io to your environment and policies.
- Run a baseline pass and review findings with your room techs and security.

Bottom line:

Conference rooms look polished—and are often the weakest place in your building. CybrIQ.io exposes the truth at Layer 1, turning shiny spaces into secure spaces.

LET'S SECURE YOUR MOST IMPORTANT ROOM

Cybr IQ
detect. correct. protect.

www.cybriq.io