detect. correct. protect.
Cybr IQ

CYBRIQ • FOR SECURITY LEADERSHIP

SpacesIQ

If your CMDB is wrong about 30% of what's plugged into your buildings, your security program is making decisions on a fiction.

"What's actually on the network right now?" SpacesIQ is the answer that doesn't take three tools and four people.

Printers in hallways. Sensors on the warehouse floor. Badge readers, kiosks, HVAC controllers, contractor laptops on a live port — invisible to NAC and asset inventory until the moment they aren't, and by then the audit is already in motion. **SpacesIQ extends CybrIQ's patented Device DNA™ to every switch port** on every floor, in every building. Same engine as RoomIQ. 100× the footprint.

THE QUESTIONS YOU CAN'T ANSWER CLEANLY TODAY

- **Inventory accuracy** — when did your CMDB last reconcile against ground truth?
- **Shadow networks** — what does facilities have plugged in that IT was never told about?
- **Agent coverage** — what fraction of your inventory can't run an EDR agent?
- **Contractor access** — how many third-party laptops are on a live port right now?
- **OT / medical / IoT** — what's sitting on flat networks waiting for a regulator to ask?

WHAT SPACESIQ GIVES THE CISO

- **Live single source of truth** for every device on every port — including those NAC was never told about
- **Trust scoring** driving allow / quarantine / investigate workflows you already operate
- **Anomaly detection** at first electrical change — before the device speaks IP
- **Audit-defensible evidence** tied to place, port, owner, policy
- **Stack-native integration** — SIEM/XDR, NAC, ITSM, your existing investment

CONTROL ALREADY IN YOUR STACK	WHAT IT SEES	WHAT SPACESIQ ADDS
NAC	Authenticated devices on managed ports	Every device on every port — including the ones NAC was never told about
Asset inventory / CMDB	What you bought, last reorg	What's plugged in, right now, and how it differs from your records
EDR / XDR	Endpoints with the agent installed	The 30–50% of inventory that can't run an agent
Vulnerability mgmt	Devices the scanner can find and identify	Devices the scanner can't see — and the ones lying about themselves

PROOF — REGIONAL HEALTHCARE NETWORK

A regional healthcare network ran a SpacesIQ pilot across multiple buildings. Within the first **2 weeks**, the discovery alone surfaced thousands of unmanaged medical devices the CMDB had never recorded — including HIPAA-relevant exposures that would have failed the next audit cycle. SecOps got visibility. Compliance got audit evidence. The board got an honest answer to "what's actually on the network."

WHERE THIS LANDS IN YOUR PROGRAM

- **Zero-trust foundations** — you can't enforce policy on devices you can't see
- **Audit posture** — HIPAA, PCI, SOC 2, NIST, CMMC require evidence, not assertions
- **M&A diligence** — true device inventory of an acquired environment in days, not quarters
- **Operational risk reporting** — quantified hardware-attack-surface metrics for the board

WHERE IT LANDS FIRST

- **Healthcare** — unmanaged medical devices, shared clinic networks
- **Financial services** — regulator scrutiny on third-party hardware exposure
- **Manufacturing** — OT, sensors, automation gear on flat networks
- **Retail** — POS, kiosks, store-level IoT, contractor access

- **Corporate campuses** — facilities-deployed IoT outside IT's line of sight

Deployment signal: Standard pilot completes in **2 weeks**. Full campus rollout typically **30–60 days**. Agentless. No port reconfiguration.

Book a CISO walkthrough
shai.moshe@cybriq.io

Get the threat-model brief
Layer 1 attack surface, control mappings, integration spec