detect. correct. protect.

Cybr IQ

CYBRIQ • BUILDING-WIDE LAYER 1 VISIBILITY

# SpacesIQ

*If it plugs in anywhere in your building, SpacesIQ knows.*

## SpacesIQ sees what your CMDB misses — every device on every port, in every building.

Printers in hallways. Displays in cafeterias. Sensors on the warehouse floor. Badge readers, kiosks, HVAC controllers, contractor laptops on a live port — all quietly invisible to NAC and asset spreadsheets. **SpacesIQ extends CybrIQ's patented Device DNA™** to every switch port, on every floor, in every building.

### WHERE THE VISIBILITY GAP LIVES

- **Unknown devices** connecting silently — contractor laptops, unmanaged switches, temp gear
- **Shadow networks** from facilities-deployed displays, badge readers, controllers
- **Asset spreadsheets** that haven't been accurate since the last reorg
- **Unmanaged medical devices, POS, IoT & OT** on flat networks
- **BYOD churn** in classrooms, retail, manufacturing, warehouses

### WHAT SPACESIQ DELIVERS

- **Real-time fingerprinting** of every device — even unmanaged or quiet ones
- **Continuous port-level monitoring** across floors, buildings, campuses
- **Trust scoring** driving allow / quarantine / investigate workflows
- **Instant anomaly alerts** when a known device behaves differently
- **Audit-ready evidence** tied to place, port, owner, and policy

| THE CONTROL ALREADY IN YOUR STACK | WHAT IT SEES | WHAT SPACESIQ ADDS |
|---|---|---|
| **NAC** | Authenticated devices on managed ports | Every device on every port — including those NAC was never told about |
| **Asset inventory (CMDB)** | What you bought, last reorg | What's plugged in, right now |
| **EDR** | Endpoints with the agent installed | The 30–50% of inventory that can't run an agent |

### 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 existing CMDB had never recorded — including HIPAA-relevant exposures that would have failed their next audit cycle. The discovery alone justified the rollout.

### WHERE SPACESIQ LANDS

- **CISO** — single source of truth for what's actually on the network, right now
- **Compliance** — audit evidence tied to port, place, owner, policy
- **Facilities & operations** — accountable inventory without becoming security analysts
- **SecOps** — anomaly detection on devices NAC and EDR can't see

### WHERE TO LAND IT FIRST

| | |
|---|---|
| **Healthcare** | Unmanaged medical devices, shared clinic networks |
| **Retail** | POS, kiosks, store-level IoT, contractor access |
| **Manufacturing** | OT, sensors, automation gear |
| **Education** | BYOD churn, lab equipment, rotating classrooms |
| **Corporate** | Facilities-deployed IoT outside IT's line of sight |

### IN ONE SENTENCE

SpacesIQ closes the visibility gap between **what's on your network** and **what's plugged into your building** — with a live device map, real-time verification, faster audits, and zero unseen entry points from facilities, contractors, or IoT vendors.

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

**Request a demo**
shai.moshe@cybriq.io

**Download the technical brief**
Layer 1 visibility architecture & integrations