SpacesIQ

Cybr IQ

detect. correct. protect.

If it plugs in, SpacesIQ knows it.

SpacesIQ extends CybrIQ's electrical-signature visibility beyond the conference room. It continuously scans, identifies, and verifies every device connected to the network — anywhere in the building.

Whether it's a printer in a hallway, a display in a cafeteria, a sensor in a warehouse, or a rogue laptop in a shared space, SpacesIQ knows it's there, confirms it's authorized, and alerts teams before a potential breach or compliance issue occurs.

SpacesIQ builds on the same real-time Layer-1 intelligence that powers RoomIQ, but at scale across every space, every switch port, and every connected environment.

RoomIQ secures the meeting room.   SpacesIQ secures everywhere else.

The Problem It Solves

Modern enterprise networks extend far beyond the conference room. Printers, cameras, sensors, kiosks, access points, HVAC controllers, and countless IoT devices sit quietly on the network, often without proper visibility or management.

Common pain points include:

- Unknown devices connecting silently.
  Guest laptops, unmanaged switches, or temporary contractor equipment can connect to a live port without being seen by traditional network tools.

- Shadow networks forming organically.
  Facilities and operations teams plug in smart displays, badge readers, or controllers without notifying IT — leaving them invisible to monitoring systems.

- Asset lists that are never accurate.
  Spreadsheets and discovery scans can't keep up with the constant movement of physical devices.

How SpacesIQ Fixes It

SpacesIQ operates as a continuous verification layer that bridges the gap between network visibility and physical device awareness.

- Electrical-signature detection
  Each device connected to the switch draws a unique electrical pattern. SpacesIQ learns that fingerprint, recognizes it instantly, and flags anything new or abnormal.

- Port-level awareness
  It maps every switch port in real time, showing exactly what is connected, where, and when — even across multiple floors or buildings.

- Instant anomaly detection
  When an unrecognized device connects or an existing one behaves differently, SpacesIQ triggers alerts before the device can communicate or spread.

- Automated trust scoring
  Every device receives a trust score based on its signature, behavior, and connection history, helping IT teams decide what to allow, quarantine, or investigate.

Why It Matters

- SpacesIQ closes the visibility gap between what's on your network and what's actually plugged in.
- It gives IT and security teams:
- A live map of every device across every space.
- Real-time verification that no rogue or misconfigured equipment is active.
- Fewer false alarms and faster audits.
- Assurance that facilities, contractors, and IoT vendors can't create unseen entry points.
  Use Cases
- Corporate offices and campuses
- Hospitals and clinics with unmanaged medical devices
- Retail stores and POS systems
- Manufacturing and warehouse facilities
- Education environments with rotating equipment and BYOD devices

Key Benefits

Capability	What It Delivers
Real-time device fingerprinting	Detects every device instantly, even unmanaged ones.
Continuous port monitoring	Identifies what's connected, when, and where.
Trust scoring and alerts	Flags unauthorized or suspicious behavior automatically.
Scalable visibility	Extends RoomIQ coverage across every building and network segment.
Compliance assurance	Provides verifiable data for security and audit teams.

Cybr IQ
detect. correct. protect.

www.cybriq.io