LOCH TECHNOLOGIES

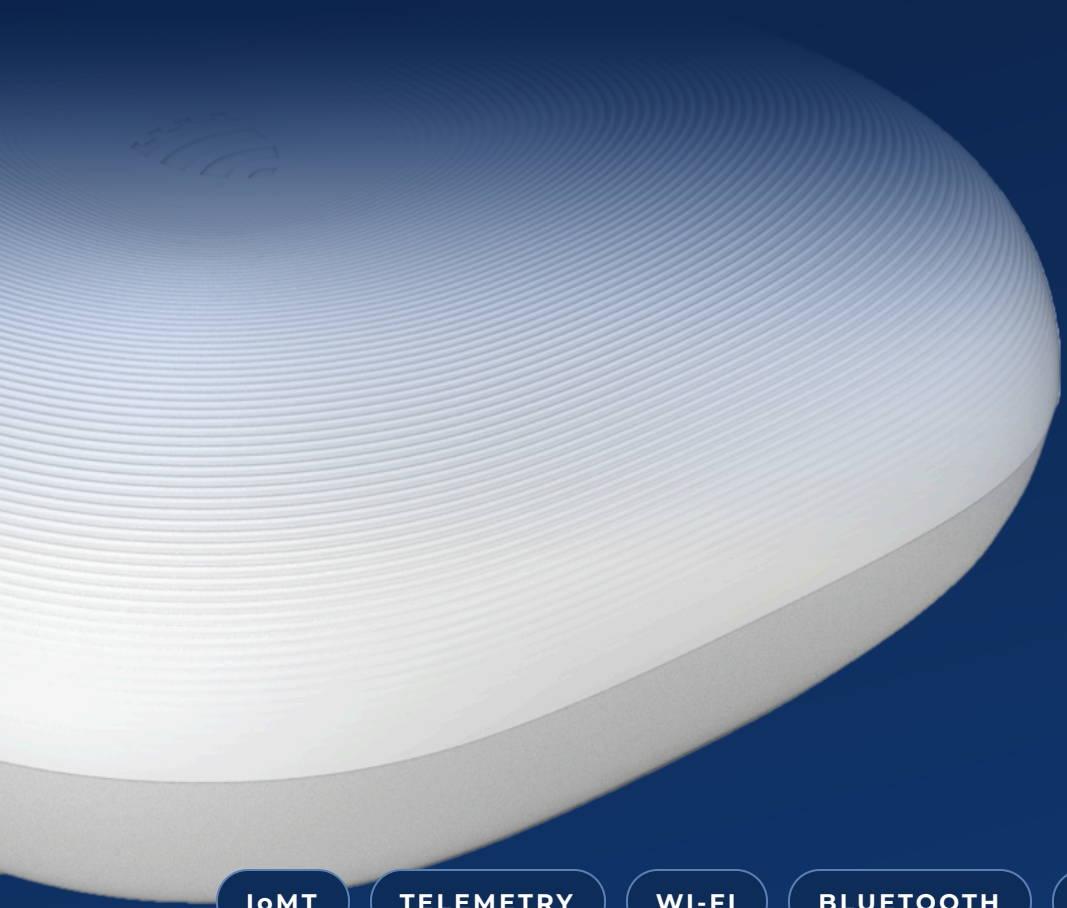
AirShield

WIRELESS AIRSPACE DEFENSE FOR HEALTHCARE

Patient care runs on wireless.
Who is watching the airspace?

Use Case · Healthcare Delivery Organizations and the Internet of Medical Things

Software-Defined RF Sensor · 300 MHz – 6 GHz · Zero Trust for the Airspace



IoMT | TELEMETRY | WI-FI | BLUETOOTH | CELLULAR | 24/7

LOCH TECHNOLOGIES

www.loch.io

The hospital went wireless faster than security could follow. The attack surface is now in the air.

The Growing Problem Space

Hospitals now run on radio. Infusion pumps, patient monitors, telemetry, beds, pagers and staff devices all connect wirelessly, alongside thousands of phones carried by patients and visitors. Network-based IoMT tools see only the devices that pass traffic through a monitored VLAN. Everything else is invisible.

10+
connected devices per hospital bed, and rising

80%
of new IoT deployments connect wirelessly

230×
rise in wireless vulnerabilities disclosed per year since 2010

2.5 / day
new wireless CVEs published during 2025

LOCH IoMT white paper · LOCH Technologies · NIST National Vulnerability Database analysis, 2010–2025

Why hospitals are exposed

- **Devices that cannot be patched.** Clinical devices run for years, cannot take agents and are hard to update without disrupting care.
- **An open campus.** Patients, visitors, vendors and contractors bring unmanaged devices into every unit.
- **Legacy radio leaks PHI.** Unencrypted analog pagers still carry patient information over the air.
- **Blind spots off the VLAN.** Network-based tools miss devices on the wrong subnet, or not on the network at all.
- **More than Wi-Fi.** Medical telemetry, MedRadio, Bluetooth and cellular sit outside Wi-Fi security tools.
- **Interference is a safety issue.** A noisy device can disrupt monitoring and telemetry with no attacker involved.



Why it matters

Patient safety
A compromised or jammed device is a clinical event. Research links ransomware to higher in-hospital mortality.

Patient privacy
Health records are among the most valuable data a criminal can steal, and every exposure is reportable.

Continuity of care
Hospitals hit by ransomware lose 17 to 25% of patient volume in the first week.

A healthcare breach costs more than any other.
Time to detect is the cost you can control.

The Cost of a Breach

$6.64M
average cost of a healthcare data breach, the highest of any industry for 13 years running

247 days
average time to identify and contain a breach, across all industries

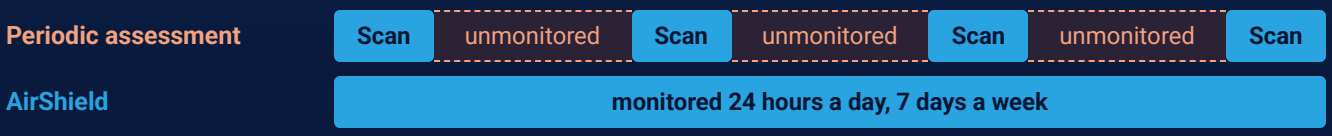
$3.1B
cost UnitedHealth Group reported from the 2024 Change Healthcare attack

192.7M
people whose data was exposed in that one attack

IBM Cost of a Data Breach Report 2026 · UnitedHealth Group · HHS Office for Civil Rights

- **Care is disrupted.** Diverted ambulances, cancelled procedures and paper charting.
- **Penalties follow.** Notification, regulatory, legal and forensic costs.
- **Revenue falls.** Volume drops 17 to 25% in the first week of a ransomware attack.
- **Trust erodes.** Patients choose where to go, and they remember.

The Value of Continuous 24/7 Monitoring



	PERIODIC ASSESSMENT	CONTINUOUS MONITORING
Coverage in time	A few days a year	Every hour of every day
A rogue device appears at 2 a.m.	Found at the next assessment	Flagged when it first transmits
Intermittent interference	Gone before anyone looks	Captured with time and location
Nights, weekends, holidays	Unwatched	Watched the same as any weekday
Evidence	A point-in-time report	A continuous record with playback

Why it matters. The longer a threat goes unseen, the more it costs. AirShield detects wireless threats at the radio layer, before they reach the wired network.

Top 10 use cases: know every device, protect the critical ones.

01 Inventory Every Wireless Medical Device

IoMT VISIBILITY

A typical hospital has more than ten connected devices per bed, bought by different departments and managed by biomed, IT and vendors. Network-based tools find only the devices that pass traffic through a monitored VLAN. A pump on the wrong subnet, or a device that never joins the network, is not in the inventory.

WITHOUT AIRSHIELD

Inventory depends on what the network can see.

Misconfigured and off-network devices are missed.

Biomed, IT and security hold different lists.

WITH AIRSHIELD

Every RF-emitting device is found and classified.

Each device is fingerprinted and risk-scored.

Inventory syncs to the CMDB and SIEM.

USES Passive discovery · Device fingerprinting · Risk scoring · CMDB integration

Why it matters. You cannot protect a device you do not know you have. Inventory is the first step of every risk analysis.

02 Protect Life-Critical Devices

INFUSION PUMPS · PATIENT MONITORS

Infusion pumps, syringe pumps and patient monitors are the devices patients depend on most, and among the hardest to secure. They cannot run security agents, and a device on the wrong network segment can be reached by anyone nearby.

WITHOUT AIRSHIELD

Segmentation errors go unnoticed.

Unauthorized connections are not seen.

Problems surface at the bedside.

WITH AIRSHIELD

Devices on the wrong network are flagged.

Unauthorized pairings and access raise alerts.

NAC and firewall integrations close the gap.

USES Pairing map analysis · Zero Trust policy · NAC and SOAR integration

Why it matters. When a device is delivering medication or watching a heartbeat, a security failure is a patient safety event.

Use cases 3 to 5: clean spectrum, safe connections, private data.

03 Detect RF Interference Before It Disrupts Care PATIENT SAFETY

Medical telemetry and patient monitoring depend on clean spectrum. Wi-Fi-connected beds and other chatty devices cause interference through constant probing and reconnects, and the result looks like a failing monitor.

WITHOUT AIRSHIELD

Dropouts are blamed on the equipment.

Biomed has no way to find the source.

WITH AIRSHIELD

Spectrum and power views show the interference.

The source is located and removed.

Why it matters. A dropped vital-signs feed is a clinical risk even when nobody is attacking.

04 Stop Rogue Access Points and Evil Twins WI-FI

Clinicians, patients and visitors connect to hospital Wi-Fi all day. A rogue access point, or an evil twin that copies the hospital's network name, can capture credentials and sit between a device and the record system.

WITHOUT AIRSHIELD

A look-alike network goes unnoticed.

Devices connect to it automatically.

WITH AIRSHIELD

Rogue APs and evil twins are detected live.

AirTerminate breaks the unsafe connection.

Why it matters. A stolen clinician login opens the systems that hold patient records.

05 Protect PHI Over the Air HIPAA · PRIVACY

Patient information travels over radio in ways no data-loss tool inspects. Unencrypted analog pagers broadcast PHI. Personal hotspots and Bluetooth links carry data past the firewall.

WITHOUT AIRSHIELD

Unencrypted PHI is broadcast unnoticed.

Off-network transfers leave no log.

WITH AIRSHIELD

Unencrypted and unauthorized links are flagged.

Forensic playback shows what, when and where.

Why it matters. Every exposure of PHI is reportable. Finding the leak first costs less than explaining it later.

Use cases 6 to 8: the devices nobody is managing.

06 Find Rogue and Hidden Devices

SKIMMERS · CAMERAS · TRACKERS

Hospitals are public buildings. Card skimmers can appear at pharmacy, cafeteria and parking payment points. Hidden cameras and trackers can be planted in patient and staff areas. Each is small, cheap and wireless.

WITHOUT AIRSHIELD

Devices are found by chance, if at all.

No way to search a whole campus.

WITH AIRSHIELD

Unknown transmitters are flagged by zone.

Threat Hunting app locates them within 1 inch.

Why it matters. Patients are at their most vulnerable in a hospital. Their privacy deserves the same protection as their records.

07 Secure Cellular and Private 5G

LTE · 5G · CBRS

Cellular now connects telehealth carts, remote monitoring, ambulances and medical devices with built-in SIMs. Private 5G and CBRS are arriving on campus. A rogue cell tower or a hijacked SIM bypasses every network control.

WITHOUT AIRSHIELD

A fake tower looks like any carrier tower.

Cellular devices bypass firewalls and NAC.

WITH AIRSHIELD

AirCell rates towers known, unknown or suspicious.

Cellular devices on campus are inventoried.

Why it matters. Care is moving beyond the hospital walls, and the cellular link is now part of the clinical network.

08 Protect the Devices You Cannot Patch

LEGACY DEVICES

Many medical devices stay in service for a decade or more, running software that no longer receives fixes. Taking them offline to patch means taking care offline. One flaw in a shared wireless chipset can expose a whole device class.

WITHOUT AIRSHIELD

Known flaws stay exposed for years.

Attempts against them go unseen.

WITH AIRSHIELD

Vulnerable devices are flagged and risk-ranked.

Monitoring acts as a compensating control.

Why it matters. Monitoring is the protection available today for devices that cannot be changed.

Use cases 9 and 10: policy, proof and compliance.

09 Extend Zero Trust to the Wireless Edge

ZERO TRUST · SEGMENTATION

Zero Trust programs focus on users and managed endpoints. Wireless medical and IoT devices have no user, no agent and often no place in the policy. Pharmacies and operating rooms may also need device-free zones.

WITHOUT AIRSHIELD

Wireless devices sit outside Zero Trust policy.

Restricted areas rely on signage.

WITH AIRSHIELD

Trust levels and policies apply to every device.

No-phone zones alert on violations.

Why it matters. Zero Trust that stops at the wired network leaves the largest device population unwatched.

10 Prove Compliance Continuously

HIPAA · PCI DSS · AUDIT

The HIPAA Security Rule requires a risk analysis of everything that touches ePHI, and the proposed update would add a written asset inventory and network map. Payment areas fall under PCI DSS, which requires rogue access point detection at least every three months.

WITHOUT AIRSHIELD

Evidence is gathered by hand before audits.

Wireless is a gap in the risk analysis.

WITH AIRSHIELD

A current wireless inventory is always on hand.

Reports and history are ready for auditors.

Why it matters. Regulators are moving from policies on paper to proof of control. Continuous records provide it.

How AirShield supports healthcare security frameworks

Framework	What it asks for	AirShield capability
HIPAA Security Rule	Risk analysis and safeguards for ePHI	Wireless asset discovery, risk scoring and monitoring
Proposed HIPAA update	Asset inventory and network map; not yet final	Continuous inventory of every RF-emitting device
HHS Performance Goals	Voluntary goals such as asset inventory and segmentation	Device classification and segmentation checks
PCI DSS 11.2.1	Detect authorized and unauthorized wireless access points	Continuous rogue access point detection

Framework summaries are for orientation. Confirm applicability with your compliance team.

Ten reasons healthcare organizations choose AirShield.

A software-defined RF sensor passively monitors 300 MHz to 6 GHz and reports to a single LOCH console, in the cloud or on-premises.

Complete IoMT inventory

Discovers every RF-emitting device, including the ones network-based tools miss.

Zero impact on patient care

Passive monitoring with no agents. Nothing is installed on clinical devices or networks.

Continuous 24/7 monitoring

Always on through nights, weekends and holidays, with real-time alerts to the right team.

Early warning

Detects wireless threats at the radio layer, before they reach the wired network.

Find it and fix it

The Threat Hunting app locates devices to within 1 inch. AirTerminate breaks unsafe connections.

Interference visibility

Spectrum and power views help biomed find what is disrupting telemetry and monitoring.

Cellular assurance

AirCell scores every tower across LTE, CBRS and 5G and exposes rogue towers.

A compensating control

Continuous monitoring protects legacy devices that cannot be patched or replaced.

Audit-grade evidence

Historical playback, incident tracking and reports support HIPAA and PCI reviews.

Fits the hospital stack

SIEM, SOAR, ITSM, CMDB, NAC and MDM integrations, with cloud or on-prem hosting.

One sensor, the whole spectrum

Medical telemetry, MedRadio, Bluetooth and cellular all sit inside the 300 MHz to 6 GHz range.

400 MHz	608 MHz	900 MHz	1.4 GHz	2.4 GHz	3.5 GHz	5 GHz	6 GHz
MedRadio	WMTS	Z-Wave LoRa	WMTS	Wi-Fi BT	CBRS	Wi-Fi	5G

Patient care runs on wireless. AirShield makes it visible, around the clock.

Summary: Why Healthcare Looks to AirShield

CAPABILITY	LOCH AIRSHIELD	NETWORK-BASED IoMT TOOLS AND WI-FI WIDS
Protocol coverage	Wi-Fi, Bluetooth, LTE/5G, CBRS, 802.15.4, LPWAN	Wi-Fi and wired traffic only
Device discovery	Every RF emitter, on or off the network	Only devices on a monitored VLAN
Impact on clinical devices	None. Fully passive	Varies. Active scans can disrupt devices
Monitoring	Continuous, 24/7	Periodic assessments
RF interference	Located by source	Not visible
Rogue cell tower detection	Included	Not supported
Rogue and hidden devices	Detected and located to within 1 inch	Found by chance
Legacy devices	Monitored as a compensating control	Unprotected until replaced
Audit evidence	Continuous logs, playback and reports	Manual and point-in-time

Healthcare breaches are the most expensive of any industry, and wireless is the part of the hospital that security tools see least. One passive sensor and one console give healthcare delivery organizations a complete wireless inventory, early warning of threats and interference, and continuous evidence for regulators, without touching a single clinical device.



10.2 × 10.2 in · PoE powered

AirShield at a glance

Frequency	300 MHz – 6 GHz
Coverage	25,000+ sq ft per sensor
Backhaul	GbE PoE · LTE optional
Hosting	LOCH Cloud or on-prem

See your airspace

www.loch.io
info@loch.io
1-888-725-9434