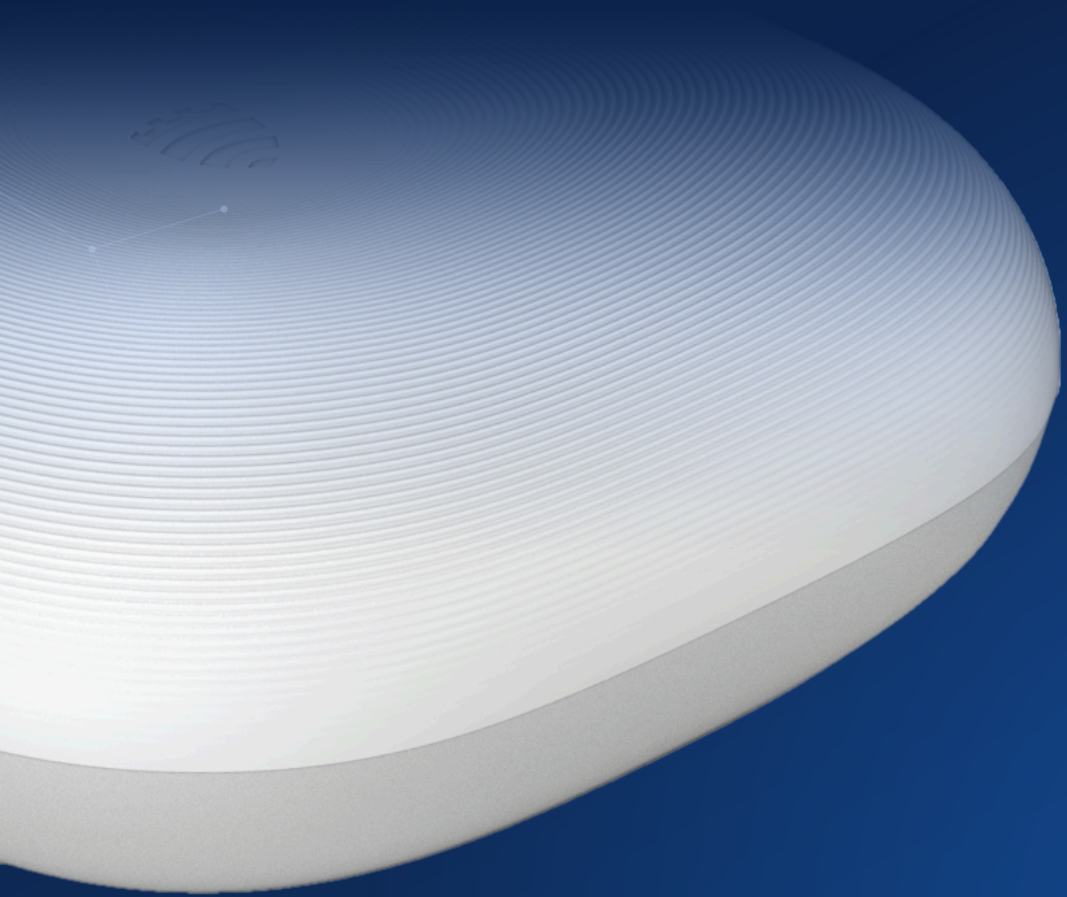
LOCH TECHNOLOGIES

AirShield

WIRELESS AIRSPACE DEFENSE

Invisible Threats. Visible Protection.

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



WI-FI | BLUETOOTH | CELLULAR | IoT / LPWAN | GPS / GNSS | ZERO TRUST

LOCH TECHNOLOGIES

www.loch.io

Wireless is the new network and attack surface that most security teams cannot see — the invisible threat.

The Wireless Airspace Defense Problem

Wi-Fi, Bluetooth, cellular and low-power IoT radios now carry critical traffic through every facility, yet they sit outside the wired, IP-based controls that security programs are built on.

230×
rise in wireless vulnerabilities disclosed per year since 2010

20×
faster growth than software vulnerabilities overall

2.5 / day
new wireless CVEs published during 2025

80%
of IoT devices now connect wirelessly

CVE figures: NIST National Vulnerability Database analysis, 2010–2025 · IoT figure: LOCH Technologies

Why existing defenses miss it

- **No IP address, no visibility.** Scanners, NAC and agents never see off-network radios.
- **One flaw, many vendors.** Bugs in shared chipsets and stacks hit whole device classes.
- **Proximity is the only credential.** Attackers need to be near the building, not inside it.
- **Unmanaged by design.** Personal, contractor and transient devices escape central control.
- **Unpatchable for years.** IoT, IoMT and OT devices rarely get fixes, so exposure compounds.
- **Attacks are scaling.** AI-assisted reconnaissance and nation-states now work the RF layer.



How AirShield closes the gap

01 Discover
Passive software-defined radios see every RF-emitting device from 300 MHz to 6 GHz, on or off your network.

02 Classify
Each device is fingerprinted, typed, tagged with a trust level and given a risk score.

03 Analyze
Behavioral analytics and wireless intrusion detection flag policy violations in real time.

04 Enforce
Locate devices to within 1 inch, terminate unacceptable connections and open tickets in SIEM, SOAR and ITSM.

Eight ways security teams put AirShield to work.

Secure Facilities & SCIFs

Enforce no-wireless zones with evidence. Alert on handsets, hotspots and Bluetooth or Wi-Fi emitters entering restricted space, then walk responders to the device.

Cellular UE · Hotspots · Bluetooth · Wi-Fi

Rogue Access Points & Wi-Fi Attacks

Catch rogue APs, Wi-Fi Pineapples and bad ESSIDs, see which trusted clients connected to them, and use AirTerminate to break unacceptable connections.

Rogue AP · Deauth flood · KRACK · Bad ESSID

Rogue Cell Towers

Baseline every tower by carrier, band, tower ID and signal strength. New, unclassified or suspicious towers and unexpected band changes raise an alert.

AirCell · New tower · Suspicious tower · Band change

Covert Surveillance & RF Espionage

Sweep continuously, not once a quarter. Hidden spy cameras, Bluetooth trackers, planted hotspots and unexplained transmitters are detected, logged and located.

Spy camera · BT tracker · Unknown emitter

Shadow IoT & Unmanaged Devices

Build the wireless inventory your CMDB is missing: Wi-Fi Direct printers, cameras, thermostats, IoT gateways and devices left in setup mode, ranked by risk.

WPS · Open / WEP · Default config · Setup mode

OT, IoMT & Industrial Wireless

Map 802.15.4, Zigbee, Z-Wave and LPWAN networks node by node, and give long-lived devices that cannot be patched a passive compensating control.

802.15.4 · Zigbee · Z-Wave · LoRa · LPWAN

Drones & Vehicles at the Perimeter

Detect the radio signatures of drones and vehicles approaching protected sites, adding RF awareness to cameras, guards and perimeter sensors.

Drone detected · Vehicle detected

Government, Defense & Remote Sites

Baseline the RF environment around installations and unattended sites, then cue analysts to change. LTE backhaul and on-prem hosting suit restricted networks.

RF baseline · Change detection · LTE backhaul

One sensor, the whole spectrum

Most wireless security stops at Wi-Fi. AirShield listens from 300 MHz to 6 GHz, GPS included.



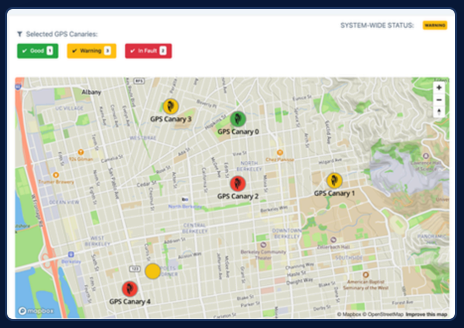
GPS is a radio signal too, and it can be jammed, spoofed or replayed.

AirShield GPS Canary

JAMMING · SPOOFING · MEACONING DETECTION

Navigation, timing and tracking systems trust whatever their GPS receiver reports. A GPS Canary is a fixed reference sensor, so any deviation in its position or time is an attack indicator.

- **Jamming.** Noise on GPS frequencies drowns out the satellites. Canary reports signal loss and lost lock.
- **Spoofing.** Counterfeit signals fake position or time. Canary flags shifts in its location and clock.
- **Meaconing.** Real signals are rebroadcast with a delay. Canary detects the time and position deviation.



Canary health by location

Benefits of GPS attack detection

- **Early warning.** Alerts fire as signal state changes, before operations feel it.
- **Where and when.** Epoch-based history narrows the affected area and time window.
- **Multi-constellation.** GPS, QZSS, GLONASS, BeiDou, Galileo and SBAS on L1.
- **Attack or fault?** Compare Canaries to rule out a bad receiver or blocked sky.
- **Timing protected.** Catch clock shifts that upset synchronized comms and surveillance.
- **Evidence on record.** Logged events feed SIEM, SOAR and incident reports.

Military & Defense

Protect installations, flight lines, ranges and forward sites where navigation, timing and unmanned systems depend on GNSS, with early warning of jamming or spoofing near the perimeter.

Bases · Flight lines · Ranges · UAS operations

Commercial & Critical Infrastructure

Airports, seaports, utilities and fleets rely on GPS for approaches, vessel and vehicle tracking, and network timing. Detect interference before it becomes delays, safety hazards or compliance findings.

Airports · Seaports · Utilities · Transportation

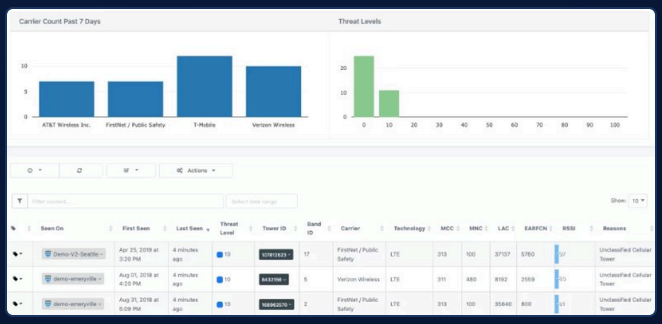
Deployment: one PoE connection and an external antenna in an IP65 outdoor enclosure, with a view of at least four satellites. Alerts by email, syslog, Slack or webhook; OpenAPI for SIEM and SOAR. Works in tandem with AirShield sensors.

Phones join the strongest signal. A fake cell tower only has to be louder.

AirCell ROGUE CELL TOWER DETECTION · 4G · 5G · CBRS

Stingrays, IMSI catchers and DIY fake base stations cost under $1,000 and put themselves between your phones and the network. AirCell inventories every tower in your airspace and scores its trust.

- **Inventory.** Every tower advertising to devices is logged by carrier, band, tower ID and signal.
- **Score.** Each tower is checked against known carrier attributes and rated known, unknown or suspicious.
- **Your networks.** Add your CBRS or private cellular towers so they are recognized as legitimate.



Tower list: carrier, band, tower ID and threat level

Benefits of rogue tower detection

- **Stop silent interception.** Know when a tower appears that no carrier operates.
- **Signal, not noise.** Threat levels separate suspicious towers from new legitimate ones.
- **Every sub-6 GHz band.** Decodes LTE, CBRS and 5G in both NSA and SA modes.
- **Close the blind spot.** Cellular traffic never crosses your firewall or Wi-Fi security.
- **Private 5G assured.** Watch the integrity and availability of your own cellular network.
- **Evidence on record.** Tower history by sensor and site feeds SIEM and investigations.

Military & Defense

Detect fake base stations near bases, command posts and secure facilities before personnel devices attach. Baseline the legitimate towers around a site and alert on anything new or suspicious.

Bases · Command posts · Embassies · SCIF perimeters

Commercial & Critical Infrastructure

Protect executives, trading floors, airports, utilities and venues from cellular eavesdropping, and keep the private 5G and CBRS networks that run operations trusted and available.

Airports · Utilities · Finance · Venues · Private 5G

One console: tower data sits beside Wi-Fi, Bluetooth, IoT and GPS findings in the LOCH console, with the same trust policies, alerts and SIEM, SOAR and ITSM integrations. Works in tandem with AirShield sensors.

Sensor

- Software-defined radios monitor 300 MHz – 6 GHz
- Wi-Fi, Bluetooth, 4G / LTE / 5G, 802.15.4 and LPWAN
- Passive monitoring: no agents, no network changes
- More than 25,000 sq ft of detection per sensor

Detection & Analytics

- Device discovery, classification and risk scoring
- Wireless intrusion detection with trust-level policies
- AirCell rogue cell tower and cellular UE detection
- GPS jamming and spoofing detection with GPS Canary
- Spectrum waterfall and power spectral density views
- Historical playback for forensic deep-dives

Response & Threat Hunting

- Threat Hunting app tracks devices to within 1 inch
- Incident tracking with photos and full history
- AirTerminate breaks unacceptable connections
- Automated daily alerts and summary reports

Integration & Deployment

- LOCH Cloud results in minutes, or an on-prem server
- SIEM, SOAR, ITSM, CMDB, FW and NAC integrations
- PoE, or optional LTE backhaul for off-network sites
- API for ticketing, tracking and remediation tools



10.2 × 10.2 in · PoE powered
Mounting ring included

AirShield at a glance

Frequency	300 MHz – 6 GHz
Coverage	25,000+ sq ft
Backhaul	GbE PoE · LTE optional
Power	PoE 60 W · DC 10–19 V
Vehicle power	12 V DC direct, optional
Dimensions	10.2 × 10.2 × 6 in
Weight	2.5 lb
Operating temp.	0 to +55 °C
Vibration	5.0 G, 5–500 Hz
Local config	RJ45 serial · reset button

Internal antennas: 2× 2.4 / 5 GHz omni (5 dB), wideband 100 MHz – 6 GHz, Bluetooth ceramic, optional LTE

See your airspace

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