LOCH TECHNOLOGIES

Securing the Stadium of the Future: RF Defense for Fans, Players, and Infrastructure.

LOCH helps NFL stadiums turn invisible risk into visible control.
By detecting threats before they escalate, documenting RF activity for compliance, and neutralizing drones and rogue devices in real time, AirShield and SkyShield protect fans, players, infrastructure, and reputation across the wireless frontier.

Stadiums are “digital cities” and must prepare for deliberate disruption, RF espionage, and nation-state tactics now migrating to civilian targets.

Real-world parallels:

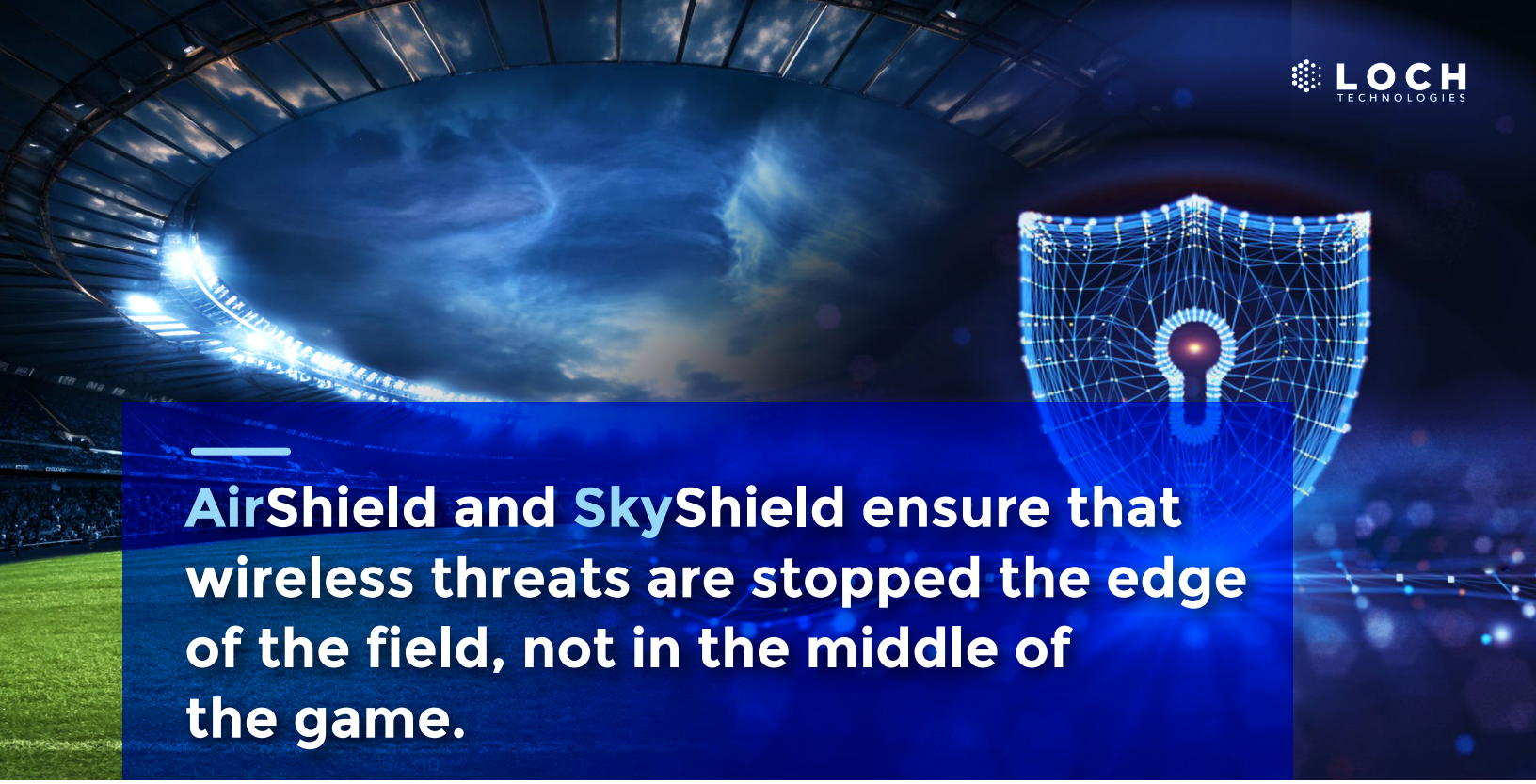
- Super Bowl LIII: A drone incident delayed the game-day flyover; stricter FAA enforcement followed.
- Fake Amber Alerts/Presidential Alerts: Spoofed mobile alerts during mass gatherings caused confusion at concerts and rallies—could happen during a game.
- Las Vegas drone jamming (2022): A drone interfered with nearby aviation signals, highlighting jamming risk to stadium GPS systems.
- Credential spoofing at DEFCON: AirShield currently detects 1,000+ RF threats per day during high-profile events.

The Time Is Now: Securing the Stadium of the Future

NFL stadiums are no longer just venues—they are high-density, high-value digital cities vulnerable to invisible wireless threats that evolve by the minute. From spoofed alerts and drone incursions to RF jamming and rogue device surveillance, threat actors are shifting from state-sponsored targets to civilian icons like live sports.

The time to act is now—before one RF-driven disruption impacts fan safety, halts a nationally televised game, or threatens critical infrastructure.

LOCH's AirShield and SkyShield platforms give NFL stadiums total control of the wireless frontier. By detecting and classifying every RF-emitting device, intercepting drones before they enter the airspace, and delivering forensic-grade compliance reporting, LOCH helps stadiums detect, assess, and prevent risk in real time—not after the damage is done.



AirShield and SkyShield ensure that wireless threats are stopped the edge of the field, not in the middle of the game.

Use Case 1

Crowd Safety and Incident Prevention (AirShield + SkyShield)

The Problem:

In high-density stadium environments, attackers can exploit wireless vectors to trigger panic, confusion, or diversion. Threats include:

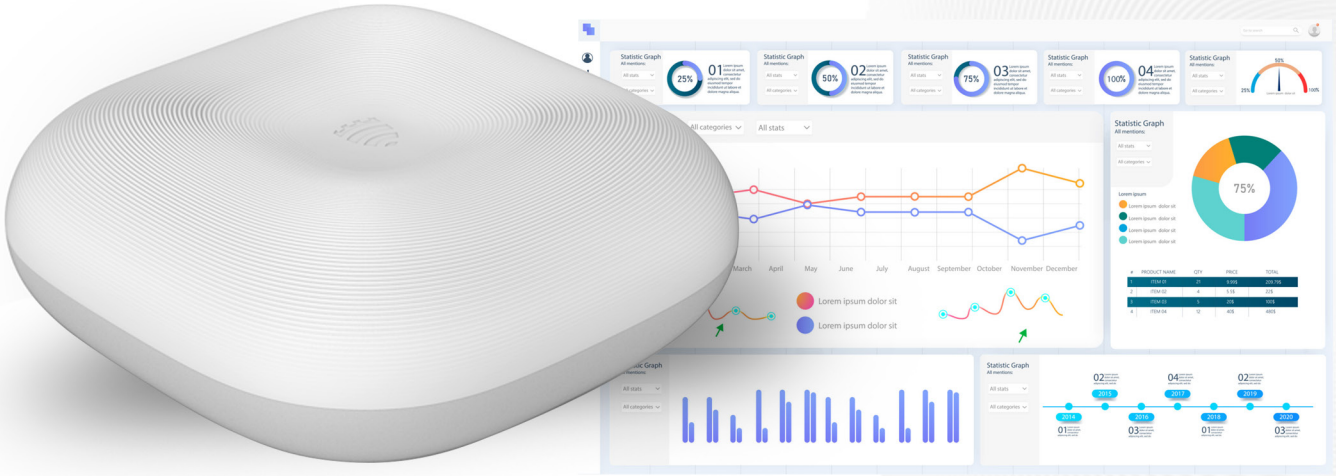
- Drones flying over fans or players, triggering fear.
- Fake cellular towers or spoofed alerts are disrupting fan communications.
- RF interference disrupts emergency radios or PA systems during a crisis.

Why it matters:

Panic can escalate quickly in tightly packed crowds, and traditional security often lacks visibility into RF-based attack methods.

Benefit:

LOCH's **AirShield** monitors for RF anomalies across fan zones, while **SkyShield** secures the airspace. Both systems are cloud-connected for **real-time alerting**, mobile response coordination, and **automated incident logging**—giving teams time and data to act decisively before threats impact safety or reputation.



AirShield

From Locker Room to End Zone—AirShield Owns the Wireless Field

Use Case 2

Wireless Threat Monitoring (AirShield)

The Problem:

Stadiums are flooded with personal and unauthorized RF devices—rogue hotspots, Bluetooth skimmers, fake access points, and embedded surveillance tools. These can be exploited for:

- **Credential theft via spoofed Wi-Fi portals.**
- **Bluetooth-based contact tracing manipulation.**
- **Hidden RF bugs streaming locker room or VIP conversations.**

Why it matters:

These unmanaged devices often evade traditional security tools and create blind spots that can compromise privacy, compliance, and safety.

Benefit:

AirShield provides continuous, passive visibility across Wi-Fi, Bluetooth, LoRa, ZigBee, cellular (4G/5G), and more, identifying both managed and rogue devices. The system logs threat behaviors and integrates with SIEM/SOAR platforms for **automated response**, giving security teams actionable intel to eliminate wireless vulnerabilities without disrupting the fan experience.

Top 5 Reasons AirShield Is Your Stadium's First Line of Wireless Defense

Unmanaged Wireless Devices Are Everywhere: With 20,000+ personal devices and IoT assets inside a stadium, AirShield identifies rogue hotspots, skimmers, and unauthorized RF activity invisible to traditional security systems.

Protect Critical Infrastructure: Scoreboards, access control, HVAC, and cameras rely on wireless protocols—AirShield detects RF interference or hijacking attempts before systems fail on game day.

Stop Attacks Before They Escalate: From credential spoofing to rogue access points, AirShield enables real-time alerting, automated response, and forensic tracking to contain threats in seconds.

Zero-Trust for the Wireless Edge: AirShield extends zero-trust principles to the RF layer—detecting and classifying every emitting device, whether it's on the network or not.

Compliance, Audit, and Insurance Readiness: With Critical Path to Exposure™ reporting, stadiums can demonstrate due diligence for legal defense, cyber insurance, and league compliance

Use Case 3

Cyber-Physical Infrastructure Protection (AirShield + SkyShield)

The Problem:

Stadium operations now depend on wireless-controlled infrastructure—scoreboards, lighting, HVAC, camera feeds, and concession systems. RF interference or compromise could cause:

- **Unauthorized scoreboard takeovers or lighting disruptions.**
- **RF jamming that disables IP security cameras.**
- **Drone-initiated payloads targeting Wi-Fi access points or GPS receivers used in logistics.**

Why it matters:

Cyber-physical sabotage during live events risks safety, game continuity, and public trust.

Benefit:

AirShield detects anomalous behaviors and interference across all RF layers—including hidden IoT or OT signals—while **SkyShield** defends against aerial vectors targeting those systems. Together, they form a **zero-trust wireless perimeter** around the stadium, preserving operational uptime, incident traceability, and coordinated response readiness.

Use Case 4

Drone Threat Detection (SkyShield)

The Problem:

Stadiums are prime targets for unauthorized drones used for surveillance, livestream piracy, or even malicious payload delivery. Scenarios include:

- **Drones hovering over player tunnels or press boxes** for espionage or media leaks.
- **Unauthorized aerial footage** was broadcast to pirate streaming platforms.
- **Drones dropping propaganda leaflets, pathogens, smoke devices, or triggering panic during high-attendance games.**

Why it matters:

The NFL bans drones near stadiums during events. A single airborne intrusion can compromise safety, intellectual property, or even halt gameplay.

Benefit:

LOCH's **SkyShield** detects drones up to 4.5 miles away using 360° RF monitoring, classifies 450+ drone types (including DIY), and uses **selective jamming** to neutralize threats without affecting adjacent RF systems. **Real-time alerts and drone flight-path tracking** give stadium operators control of their airspace and crowd confidence in their security response.

Use Case 5

Compliance, Liability Protection, and Insurance Readiness

The Problem:

Stadium operators must prove due diligence in threat monitoring to maintain league compliance, limit liability, and secure insurance coverage. RF-related incidents can lead to:

- **League sanctions or fines for unmitigated security failures.**
- **Increased insurance premiums due to lack of active surveillance.**
- **Litigation following a drone breach, jamming incident, or wireless data leak.**

Why it matters:

Without RF visibility, operators lack forensic evidence and cannot demonstrate proper risk controls during audits or claims.

Benefit:

AirShield's Critical Path to Exposure™ reporting and **SkyShield's flight-path and signal telemetry logs** deliver **forensic-grade data** to validate incident handling, threat prevention, and infrastructure resilience. This supports compliance with league protocols and strengthens liability coverage during legal or insurance assessments.

Securing the Skies: Mitigating Threats From Drones - Detect, Identify and Take Down

Up to
7 km

Up to 7 km detection distance :
SkyShield detected drones 4.5 miles away with consistent and strong direction tracking.

Selective Jamming

Selective Jamming:
Selective jamming (a.k.a smart defense) jams a specific drone target without disrupting other DRONES within WI-FI, Bluetooth, or other RF frequencies within the same band (2.4GHz and 5.8GHz bands).

Up to
14

Drone swarm detection and multi-object tracking:
SkyShield detected 14 out of 14 different DRONE types flown at the same time from various distances and locations, with accurate direction finding (DF).

100%
Detection coverage

100% Detection coverage:
SkyShield detected 100% of the DRONES, including commercial off-the-shelf (COTS), Do-It-Yourself (DIY)/Hobbyist quadcopters, and fixed-wing drones.

100%
Defeat coverage

100% Defeat coverage:
SkyShield defended/jammed 100% of the tested drones, including the DJI Mavic drone, which we know is difficult to defeat using jammers.

LOCH TECHNOLOGIES

LOCH's **AirShield** and **SkyShield** solutions deliver critical RF visibility and control that physical security alone cannot provide. For NFL stadiums, this means preventing drone incursions, wireless attacks, and operational disruptions before they escalate. These platforms support compliance with NIST, FEMA, and DHS frameworks, reduce cyber liability insurance exposure, and protect against multi-million dollar losses tied to safety breaches, game delays, or media violations. **LOCH empowers stadiums to secure fans, players, and infrastructure across the wireless frontier.**