LOCH TECHNOLOGIES

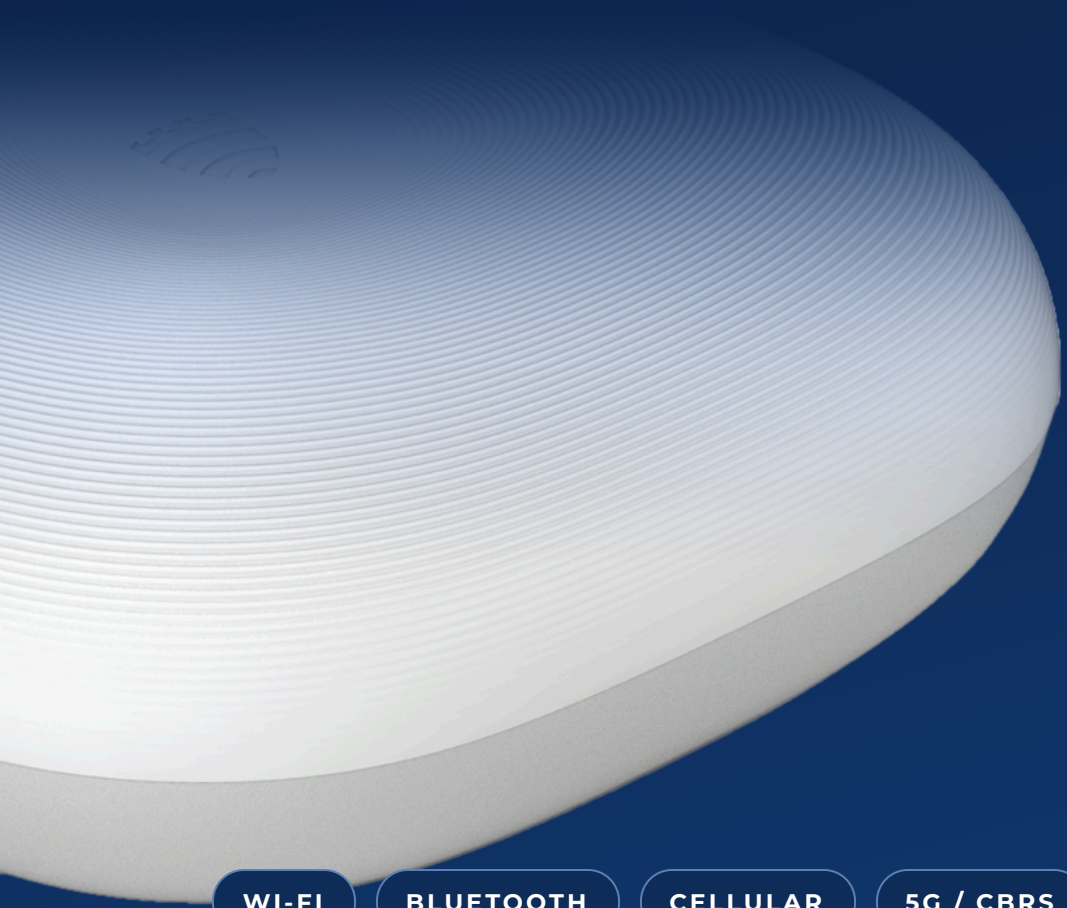
AirShield

WIRELESS AIRSPACE DEFENSE FOR SMART CASINOS

The house watches every hand.
Who is watching the airspace?

Use Case · Casinos, Integrated Resorts and Gaming Operators

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



WI-FI | BLUETOOTH | CELLULAR | 5G / CBRS | IoT | DRONES

LOCH TECHNOLOGIES

www.loch.io

Casinos watch every table, door and dollar.
Almost none can see the radio spectrum.

The Smart Casino Wireless Problem

A modern resort runs on wireless: cashless wagering, mobile check-in, connected slot machines, kiosks, digital signage, door locks and staff radios. Thousands of guest devices arrive every day. Surveillance covers the floor on video and the SOC covers the wire. The airspace between them is unmonitored.

$100M
earnings impact MGM Resorts estimated from its September 2023 cyberattack

10 GB
of data taken from a casino through a connected fish tank

3 months
the longest PCI DSS allows between rogue access point checks

24 hours
Nevada's deadline to notify regulators of a cybersecurity incident

MGM Resorts Form 8-K, Oct 2023 · Darktrace, 2017 · PCI DSS v4.0.1 Req. 11.2.1 · NGC Regulation 5.260, amended Jan 2026

Why casinos are uniquely exposed

- **Open by design.** Anyone can walk the floor or book a room. Proximity is the only credential a wireless attacker needs.
- **Everything is connected.** Slots, signage, cameras, locks and HVAC add IoT devices faster than IT can inventory them.
- **High-value targets.** Cash, card data, loyalty databases and VIP guests concentrate in one building.
- **Money moves over the air.** Cashless wagering, mobile wallets, kiosks and point of sale all depend on wireless.
- **A crowd to hide in.** A covert transmitter is one signal among thousands of guest phones, watches and earbuds.
- **Wi-Fi tools see only Wi-Fi.** Bluetooth, cellular and IoT radios sit outside what network security monitors.

Why it matters

Revenue
The floor earns around the clock. Every hour of disrupted gaming, payments or check-in is lost win.

The license
Regulators expect risk assessments, records and fast incident reports. Game integrity is the license.

Guest trust
High-value guests expect discretion. A leaked database or a filmed high-limit room is hard to repair.

Six problems AirShield solves for casinos, and why each one matters.

From Blind Spot to Visible Airspace

	THE PROBLEM	WHAT AIRSHIELD DOES	WHY IT MATTERS
01	**Cheating devices on the floor**	Flags unknown transmitters near tables and machines and guides security to them	Game integrity protects the win and the license
02	**Skimmers and rogue access points**	Detects them continuously at the cage, kiosks, ATMs and points of sale	Card data stays safe and PCI evidence is always current
03	**Unmanaged IoT**	Discovers, classifies and risk-scores every connected device on the property	No forgotten device becomes the next fish tank
04	**Rogue cell towers**	AirCell rates every tower known, unknown or suspicious	VIP and executive communications stay private
05	**Bugs in sensitive rooms**	Alerts the moment an unauthorized device transmits in a restricted zone	The count room, cage and boardroom stay confidential
06	**Drones overhead**	Detects and geolocates unauthorized drones in the same console	Guests and events are protected from above

Where wireless risk lives in a smart casino

Gaming floor
Connected slots and tables, cashless wagering, thousands of guest devices.

Cage and count room
Cash, card data, kiosks and ATMs. The first target for skimmers and bugs.

Hotel tower
Smart locks, in-room IoT and VIP suites where privacy is the product.

Convention and events
Temporary networks, exhibitor equipment and crowds that change every week.

Back of house
Surveillance room, data center, building systems and vendor access.

Rooftop and perimeter
Pool decks, outdoor venues, parking structures and the airspace above.

Use cases 1 and 2: the game and the money.

01 Protect the Integrity of the Game GAMING FLOOR

Cheating teams use concealed cameras, Bluetooth earpieces and miniature transmitters to read cards, signal partners and probe gaming machines. Surveillance watches hands and faces. It does not see radio, and a covert device is one signal among thousands of guest phones.

WITHOUT AIRSHIELD

Covert devices operate unnoticed at tables and machines.

Investigations start after the loss, from video alone.

No record of which devices were present, or when.

WITH AIRSHIELD

Unknown transmitters are flagged by zone and behavior.

The Threat Hunting app guides security to within 1 inch.

RF events correlate with cameras; playback shows the timeline.

USES Zone-based alerts · Behavioral analytics · Threat Hunting app · Fused sensor detection

Why it matters. Game integrity is the license. One cheating ring costs the win and the regulator's confidence.

02 Guard the Cage, Kiosks and Card Data PAYMENTS · PCI DSS

A resort runs thousands of payment points: the cage, ATMs, kiosks, restaurants, retail and hotel desks. A Bluetooth skimmer or rogue access point near any of them puts card data at risk. PCI DSS requires detecting authorized and unauthorized wireless access points at least every three months, even where wireless is prohibited.

WITHOUT AIRSHIELD

Quarterly walk-through scans leave months of dwell time.

Bluetooth and cellular skimmers are invisible to Wi-Fi tools.

Evidence for assessors is compiled by hand.

WITH AIRSHIELD

Rogue access points are detected continuously, with alerts.

Skimmers and other unauthorized emitters are found and located.

Reports and device history are ready for the assessor.

USES Rogue AP detection · Bluetooth visibility · AirTerminate · Audit reports

Why it matters. A card breach brings fines, forensic costs and lost guest trust. Continuous detection cuts exposure from months to minutes.

Use cases 3 and 4: connected devices and cellular.

03 Inventory Every Connected Device

IoT · SMART BUILDING

Smart casinos connect slot machines, kiosks, digital signage, cameras, door locks, HVAC and even aquarium sensors. Vendors and departments add devices faster than IT can track them. In one widely reported case, attackers reached a casino's high-roller database through a connected fish tank thermometer.

WITHOUT AIRSHIELD

Devices added by vendors never reach the inventory.

Default settings and setup modes go unnoticed.

Unpatchable devices have no compensating control.

WITH AIRSHIELD

Every RF-emitting device is discovered, classified and risk-scored.

Misconfigured and vulnerable devices are flagged for action.

CMDB, NAC and SIEM integrations keep the inventory current.

USES Device fingerprinting | Risk scoring | CMDB and NAC integration

Why it matters. You cannot defend what you do not know. A complete inventory is also the starting point of every regulator's risk assessment.

04 Expose Rogue Cell Towers and Cellular Backdoors

LTE · 5G · CBRS

High-value guests, hosts and executives carry phones worth intercepting. An IMSI catcher in a hotel room or a parked vehicle can pose as a carrier tower. A cellular modem hidden in equipment bypasses the network entirely. Resorts also depend on in-building cellular and private networks for their own operations.

WITHOUT AIRSHIELD

A fake base station looks like any carrier tower.

Cellular hotspots and modems bypass firewalls and NAC.

No baseline of the property's normal cellular environment.

WITH AIRSHIELD

AirCell inventories every tower by carrier, band and tower ID.

Each tower is rated known, unknown or suspicious.

Unauthorized cellular devices are detected in restricted areas.

USES AirCell | Tower risk rating | LTE, 5G and CBRS coverage

Why it matters. Discretion is part of what a casino sells. Intercepted calls or a hidden cellular backdoor put guests, deals and data at risk.

Use cases 5 and 6: private rooms and open sky.

05 Keep Sensitive Rooms Free of Bugs

COUNT ROOM · SURVEILLANCE · VIP

Money and confidential information concentrate in the count room, cage, surveillance room, boardroom and high-limit salons. Hidden cameras, audio bugs, keyloggers and trackers can be planted by insiders, vendors or guests. A periodic bug sweep shows one moment in time.

WITHOUT AIRSHIELD

A device planted the day after a sweep goes unseen.

No-device policies cannot be verified.

Insider activity leaves no wireless record.

WITH AIRSHIELD

Zone alerts fire when an unauthorized device transmits.

Monitoring is continuous, not a quarterly sweep.

Device history ties activity to a time and place.

USES Zone-based alerts | Trust levels | Historical playback

Why it matters. These rooms hold what the property cannot afford to leak: cash procedures, surveillance coverage, deals and guest identities.

06 One Platform for Drones and Signals

DRONES · SIGNALS

Resorts host pool decks, outdoor concerts, sporting events and rooftop venues. A drone can film guests, survey the property or carry a wireless device onto a roof. Physical security and cyber teams use separate tools, so nobody links the drone to the device it delivered.



WITHOUT AIRSHIELD

No awareness of drones over crowds and venues.

Separate consoles for drones, Wi-Fi and cellular.

Cyber and physical teams work from different data.

WITH AIRSHIELD

Unauthorized drones are detected and geolocated.

One console shows drones beside every wireless finding.

Alerts reach the SOC and security through SIEM and SOAR.

USES Drone detection | Single console | SIEM and SOAR integration

Why it matters. Guest safety and privacy extend to the sky. One platform retires overlapping tools and gives both teams the same picture.

Ten ways AirShield protects the house.

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 wireless inventory

Discovers every RF-emitting device on the property, whether or not it ever joins your network.

Zero impact on gaming operations

Passive monitoring with no agents and no network changes. Nothing touches gaming or payment systems.

Zone-based policy

Different rules for the floor, the cage and the count room, with trust levels and alerts for each zone.

Real-time threat detection

Wireless intrusion detection and behavioral analytics flag rogue devices and policy violations as they happen.

Find it and fix it

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

Works with surveillance

Fused sensor detection correlates RF events with cameras and physical sensors for faster response.

Cellular assurance

AirCell scores every tower across LTE, CBRS and 5G, exposing rogue towers and protecting private networks.

Risk you can rank

Each device is fingerprinted, typed and risk-scored, so teams act on the worst exposures first.

Audit-grade evidence

Historical playback, incident tracking and reports give regulators and PCI assessors a continuous record.

Fits the SOC, deploys anywhere

SIEM, SOAR, ITSM, CMDB and NAC integrations. PoE powered, with on-prem hosting for restricted networks.

One sensor, the whole spectrum

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

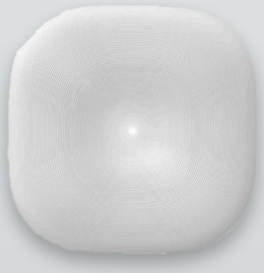
300 MHz	600 MHz	900 MHz	1.5 GHz	2.4 GHz	3.5 GHz	5 GHz	6 GHz
LPWAN	LTE	Z-Wave LoRa	GPS L1	Wi-Fi BT	CBRS	Wi-Fi	5G

The house should never play blind.
AirShield makes the airspace visible.

Summary: The Odds Without Visibility

CAPABILITY	LOCH AIRSHIELD	WI-FI WIDS AND PERIODIC SWEEPS
Protocol coverage	Wi-Fi, Bluetooth, LTE/5G, CBRS, 802.15.4, LPWAN	Wi-Fi only
Monitoring	Continuous, property-wide	Quarterly scans and scheduled sweeps
Device inventory	Every RF emitter, on or off the network	Only devices that join the network
Skimmers and covert devices	Detected and located	Found only if a sweep happens to catch them
Rogue cell tower detection	Included	Not supported
Drone detection	Included, in the same console	Separate system or none
Device location	To within 1 inch	Not available
Zone-based policy	Rules and alerts for each area of the property	Not available
Regulator and PCI evidence	Continuous logs, playback and reports	Manual and point-in-time

Casinos lead every industry in physical surveillance. The wireless layer grew up beside it, unwatched. One passive sensor and one console protect the integrity of the game, the payment environment, connected devices, guest privacy and the airspace above the property.



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