iViu Insights

CONFIDENTIAL

PLATFORM DOCUMENTATION

The iViu SIGINT Platform

A passive signal-intelligence layer that detects WiFi devices hundreds of feet before they reach a perimeter — turning physical security from reactive response into proactive prevention, and integrating cleanly with the systems you already run.

Critical-Infrastructure SIGINT | Safety & Bad-Actor Detection | Consumer Journey Analytics

DOCUMENT	AUDIENCE	VERSION
Platform Overview	Customers · Partners · Consultants	2026.06

CONTENTS

EXECUTIVE SUMMARY

Cameras, guards, and fencing are the proven core of physical security — and they perform at their best the moment a threat is in range. The iViu SIGINT Platform extends that protection earlier in time. Patented iDTag sensors passively detect the WiFi signals that virtually every person carries, identifying an approaching device **600+ feet beyond the perimeter** and **three to five minutes before** it reaches camera or guard range.

That advance warning is delivered through a single sensor that simultaneously powers three capabilities — infrastructure perimeter protection, bad-actor detection, and consumer journey analytics — and feeds the case-management, video-management, and incident-management systems you already operate. This document explains what the platform does, how it works end to end, where it fits, and the value it creates.

Live detection — anonymous devices identified **600+ ft beyond** a substation perimeter, well ahead of camera range.

iPS · LIVE

AN ADDED LAYER — THAT FITS WHAT YOU RUN

iViu is built to **strengthen the security you already trust** — cameras, guards, access control, and your video-management system. It adds an early-warning layer in front of them, then hands off rich context the instant a threat reaches their range.

Extends Reach

600+ ft of detection with no line-of-sight requirement — covering ground beyond camera range.

Adds Time

3–5 minutes of advance warning turns response into prevention.

Works With Your Cameras

Hands detections to your VMS, CMS, and incident tools — no rip-and-replace.

600ft+	<1m	3–5min	Zero
Outdoor detection radius	Indoor positioning accuracy	Earlier than camera detection	PII collected or stored

1

SECTION ONE

Platform Overview

Adding Time to the Security You Already Trust

Cameras, guards, and access control are the backbone of physical security, and they excel the moment a threat is in range. What no line-of-sight system can do is see a threat *forming* hundreds of feet out. iViu adds exactly that — a complementary early-warning layer that gives your team more time to act and richer context to act on.

TODAY · RESPOND ON ARRIVAL

- Threat identified once it is in range
- Response begins as the event unfolds
- Limited awareness beyond line-of-sight range
- Evidence assembled after the fact

→

WITH IVIU · ACT EARLIER

- Devices detected 600+ ft before the fence
- Operators gain minutes of advance time
- No line-of-sight required — full-radius coverage
- Continuous, time-stamped forensic record

Three Pillars, One Sensor

A single iDTag sensor deployment powers three capabilities at once, from the same hardware investment. A customer who installs the platform for perimeter protection also receives bad-actor detection and retail-grade analytics at no additional hardware cost.

01

Critical-Infrastructure SIGINT

Detect approaching devices at substations, water treatment plants, pipelines, cell towers, and government facilities — well beyond camera range, complementing existing coverage, over an encrypted uplink that never touches the facility network. Patented identity-resilience defeats device randomization.

02

Safety & Bad-Actor Detection

Identify persons of interest by anonymously tracking the WiFi signals their devices emit. The instant a watchlisted device enters an enrolled location, the platform escalates automatically — security staff, corporate security, then law enforcement — in seconds.

03

Consumer Journey Analytics

Under-1-meter indoor positioning delivers heatmaps, journey playback, dwell-time analysis, and conversion dashboards — turning existing floor space into a data-generating asset. Fully GDPR- and CCPA-compliant by design.

2

SECTION TWO

How It Works

Process Flow — From Signal to Intelligence

The platform handles every layer automatically — from physical detection at the edge to decision-ready intelligence in an operator's hands. Four stages, end to end:

STEP 01

Sensor Deployed

iDTag installed at site, indoor or outdoor. PoE or USB-C powered. No facility network required.

→

STEP 02

Signals Detected

Every 10 ms the sensor sweeps for WiFi devices in range — anonymous, <1 m accurate.

→

STEP 03

Platform Processes

Data transports via MQTT over an encrypted uplink to Azure; Go services correlate in real time.

→

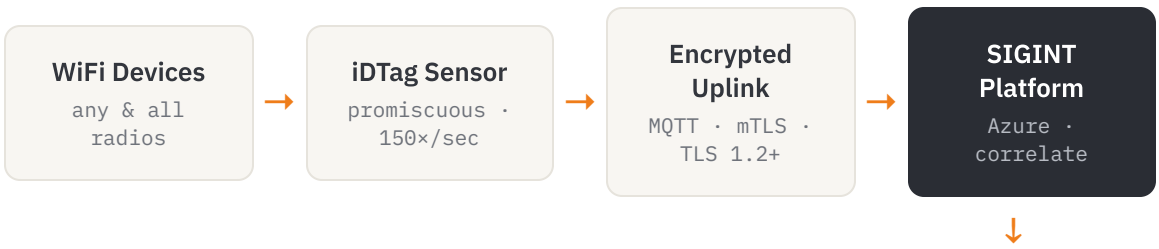
STEP 04

Intelligence Delivered

Dashboards, heatmaps, alerts, and API feeds surface decision-ready intelligence to ops & security.

Information Flow — Edge to Cloud to Action

Every detection follows the same encrypted path. WiFi signals are captured at the edge, packaged as anonymous records, and streamed to the cloud — where three services turn raw signal into alerts, intelligence, and operator tools.



Integration Service

Email & SMS
Teams channel
MQTT · Webhook
REST API · CLI

SIGINT Monitor

Bad-actor matching
Incident triggers
Heuristic learning
SOC integration

Platform UI

System management
Configuration
Data retrieval
Investigation tool

↳ outputs route to your security teams, dashboards, and connected systems

Operational Lifecycle — Detect → Deter → Protect → Record

Four operational pillars cover the full threat response — from invisible early detection through encrypted forensic record.

01
Detect

See it 600+ ft before the fence.

Passive WiFi scan 150×/sec, resilient to identity randomization, <1 m accuracy.

02
Deter

Make bad actors leave first.

Trigger lighting, PA, sirens, and access systems on confirmed approach. Tiered escalation.

03
Protect

Alert & lock down in seconds.

Multi-level alerts via SMS, email, API. Security in <1 s; law enforcement in <5 s.

04
Record

Every signal, time-stamped.

Encrypted, auditable log — anonymous fingerprint, time, location. Forensics-ready, no PII.

3

SECTION THREE

The Sensor & Architecture

The iDTag Sensor

The iDTag is a compact, ruggedized indoor/outdoor positioning sensor — roughly 4 × 2.5 × 0.7 inches. It performs a passive, promiscuous sweep of the WiFi spectrum 150 times per second. Crucially, its encrypted independent uplink means the sensor **never touches the facility network** — essential for utility, government, and DoD deployments where network access is restricted.

ACCURACY **< 1 m**	SCAN RATE **10 ms**	RANGE **–40 / +85°C**
POWER **PoE / USB-C**	CONNECTIVITY **Encrypted Uplink**	FIRMWARE **FOTA · OTA**

Architecture — Edge to Cloud in Four Layers

Each layer is independently scalable and communicates exclusively over encrypted channels with mutual-TLS authentication. Signal data flows left to right; no layer is ever exposed to the public internet without encryption.

LAYER 1

Edge Sensors

iDTag passive WiFi sensor · 150×/sec · 600+ ft · PoE/USB-C · AES-256 on-device · MQTT client

LAYER 2

Secure Transport

EMQX broker cluster · per-device mTLS certs · TLS 1.2/1.3 · MQTT 3.1.1/5.0 · QoS 1 delivery

LAYER 3

Cloud Processing

Azure IoT Hub + VMs · Go microservices · iViu UDID resolution · patented positioning · REST APIs

LAYER 4

Data & Analytics

MySQL analytics DB · React partner portal · admin dashboard · ORC tools · summary data feed API

Listener · MCDR

Ingests telemetry; the patented de-randomizer resolves rotating identities into persistent UDIDs.

Positioning

Sub-1 m fingerprinting & multi-sensor fusion with per-site zone assignment.

Alerts · API · ORC

Watchlist alerts, partner REST API, and organized-retail-crime investigation tooling.

4

SECTION FOUR

Safety & Bad-Actor Detection

Process Flow — Bad-Actor Monitoring

Sensors at entrances and key points continuously compare detected devices against an operator-controlled watchlist. A match triggers an incident — and every detection feeds back to refine the person-of-interest and bad-actor lists.

↺ Closed loop — every recorded event sharpens detection. A device flagged once becomes high-priority everywhere on the network.

Automated Alert Escalation Ladder

L1 — **Security Staff**
On-site officers receive an immediate alert as a person-of-interest UDID enters the perimeter. **< 1s**

L2 — **Corporate Security**
Regional and corporate teams notified with full event context, location, and historical actor profile. **< 3s**

L3 — **Law Enforcement**
For confirmed threats, the monitoring center or SOC dispatches with structured intel for response. **< 5s**

L4	**Site Lockdown** Trigger door access, lighting, and PA lockdown protocols on confirmed alerts.	`manual`

Four Operating Modes

Each mode triggers independently — configurable per sensor, interior zone, or site. Combine modes on one deployment for layered coverage.

Restricted-Area Presence

Alerts when any device enters an off-limits zone — back office, server room, employee-only — at any hour.

After-Hours Detection

Triggers on devices during operator-defined closed hours — perimeter, parking, and rooftop included.

Bad Actor / Person of Interest

Known watchlist UDID detected at site or zone level. Triggers on first detection — no dwell time.

Rule-Based Escalation

Multi-factor trigger: proximity, dwell time, bad-actor match, cluster size, or perimeter crossing.

PRIVACY iViu only tracks anonymous device identifiers (UDIDs). No names, emails, phone numbers, or PII is ever collected or stored. The UDID is not reversible to its origin and the watchlist is operator-controlled and fully auditable — GDPR- and CCPA-compliant by design.

FIELD SCENARIOS

Use Cases by Market Segment

The same platform adapts to radically different environments. Below, representative scenarios across four market segments — each drawn from iViu's deployment simulations.

RETAIL & COMMERCE

Big-Box Retail — Interior & Exterior

Layered sensors detect after-hours parking-lot loitering and vehicles of interest outside, while interior sensors flag known bad actors and unauthorized signals in restricted zones.

`Loss prevention · ORC · analytics`

Small Store / Store Interior

A single-sensor deployment delivers bad-actor alerts on entry plus traffic, dwell, and conversion analytics — no separate hardware for security and marketing.

`First-detection alerting · journey data`

CRITICAL INFRASTRUCTURE

Border / Substation Perimeter

Outdoor sensors detect approaching devices 600+ ft beyond the fence line — providing advance warning ahead of camera range — over an uplink isolated from the facility network.

`Early warning · network-isolated`

Cell Site / Remote Asset

Unattended tower sites gain unauthorized-access detection with PoE power and no on-site staff — alerts route directly to a remote monitoring center.

`Unmanned · remote alerting`

LOGISTICS & INDUSTRIAL

Distribution Center

Perimeter and dock-door monitoring detects unauthorized presence around high-value inventory and after-hours yard activity across a large footprint.

`Yard security · cargo theft`

Construction Site

Temporary, network-free deployment protects equipment and materials on an active site, flagging after-hours intrusion where no fixed infrastructure exists.

`Rapid deploy · theft deterrence`

PROPERTY & VENUES

Apartment Complex

Common-area and entry monitoring detects trespassers and repeat offenders across a multi-building property, with privacy preserved through anonymous UDIDs.

`Resident safety · trespass`

Shopping Center / Car Dealership

Large open lots gain after-hours coverage and tenant-level traffic intelligence — protecting inventory while quantifying visitor flow.

`Lot coverage · tenant analytics`

5

SECTION FIVE

An Added Layer — That Fits What You Run

A Complementary Layer, Not a Replacement

The SIGINT Platform pairs naturally with the cameras, guards, and access control you already run — it sits *in front* of them, extending the detection envelope hundreds of feet outward and adding situational awareness in the minutes *before* an event reaches their range. You keep what works and extend it earlier in time.

✓ Extends Reach

600+ ft detection with no line-of-sight requirement covers ground beyond camera range.

✓ Adds Time

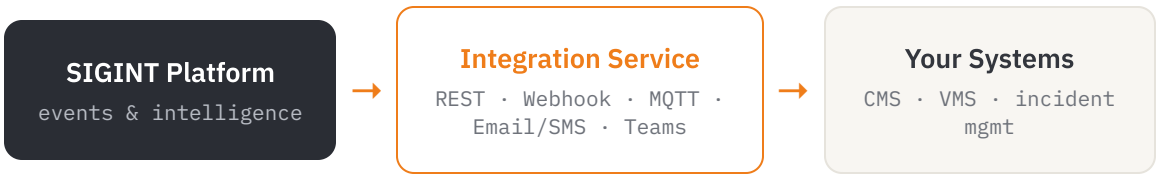
3–5 minutes of advance warning turns response into prevention.

✓ Adds Memory

Repeat-offender identification and a forensic record existing tools rarely capture.

Integration With Your Existing Systems

The platform's built-in Integration Service pushes alerts and intelligence into the systems you already operate — whether off-the-shelf vendor products or homegrown tools. Standard, well-documented interfaces mean integration is a configuration exercise, not a development project.



Case Management

Auto-create cases and attach actor history, location, and timestamps via REST or webhook.

Video Management (VMS)

Cue cameras to a detection zone and bookmark footage the moment an alert fires.

Incident Management

Open and escalate incidents in your SOC tooling through MQTT,

API, or Teams notifications.

A dedicated *Master Files Integration* interface also supports machine-to-machine configuration of customer, location, and tag records. See the companion **SIGINT Platform & Master Files Integration Guide** for full schemas and message formats.

6

SECTION SIX

Return on Investment

The platform's economics rest on three levers: one sensor serving three functions, prevention that avoids loss rather than documenting it, and clean integration that avoids rip-and-replace. The drivers below are qualitative — model them against your own loss, labor, and incident data.

One investment, three returns. Because a single iDTag deployment simultaneously serves SIGINT, safety, and analytics, the hardware cost is amortized across security *and* revenue-generating functions.

An added layer, not a forklift upgrade. iViu complements the cameras and VMS you already run rather than replacing them — so the spend is incremental, the rollout is fast, and the systems you trust keep working, now extended earlier in time.

Where the Savings Come From

LEVER	HOW VALUE IS CREATED
Loss prevention	Early detection & repeat-offender identification deter theft before it occurs, reducing shrink and ORC losses.
Labor efficiency	Automated alerting and unmanned remote-site coverage reduce reliance on continuous guarding and manual monitoring.
Hardware consolidation	One sensor replaces separate security and analytics systems — a single install, cable run, and maintenance contract.
Faster resolution	Structured forensic records and actor history shorten investigation time and strengthen evidence quality.
Low integration cost	Standard APIs into existing CMS/VMS/incident systems avoid rip-and-replace and custom development.

MODEL A · RETAIL

Shrink reduction + revenue lift

- Reduced shrink from deterred theft & ORC
- Recovered margin on prevented loss events
- Analytics-driven conversion & layout gains at no extra hardware cost
- Lower guard hours via automated alerts

Anchor metrics: capture rate, dwell, conversion, repeat-visitor rate, incident count.

MODEL B · INFRASTRUCTURE

Breach avoidance + coverage

- Avoided cost of a single perimeter breach or outage
- Coverage of remote/unmanned sites without added staff
- Reduced false-alarm dispatch via confirmed multi-factor triggers
- Network-isolated deployment avoids IT/OT integration cost

Anchor metrics: sites covered per FTE, mean time-to-detect, breach/incident rate.

7

SECTION SEVEN

Security, Privacy & Rollout

Security Architecture

mTLS Client Authentication

Every sensor carries a unique iViu-CA-signed certificate. The broker rejects any connection without one — no password fallback.

End-to-End Encryption

TLS 1.2+ in transit, AES-256 at rest. Internal services run on a private Azure VNet with no public exposure.

Zero-PII Architecture

The anonymous iViu UDID is derived from signal characteristics and cannot be reverse-mapped to a person or device owner.

Network Segmentation

Outbound-only sensor traffic on an isolated VLAN means zero inbound attack surface on the customer network.

Getting Started

01
Site Survey
RF survey & coverage map

→

02
Install
PoE/USB-C, no facility network

→

03
Burn-In
2–3 wk environmental learning

→

04
Go Live
Same-day; OTA from then on

READY TO SEE IT LIVE?

Schedule a briefing or request an evaluation unit.

Whether you are protecting critical infrastructure or optimizing a retail footprint, iViu's team will scope a deployment to your environment and integration needs.

SALES & SUPPORT
support@iviutech.com

PHONE
(949) 536-8441

PARTNER PORTAL
partner.iviuinsights.com

CORPORATE HQ
Burr Ridge, IL 60527

COMPLIANCE
GDPR · CCPA · UL · FCC

WEB
iviuinsights.com