VigilWatch

SECURITY • VIGILANCE • PROTECTION

The Tactical Intelligence Briefing

Professional-grade protection against tech-facilitated stalking and surveillance.

The Threat Landscape is Invisible, But Ubiquitous

7.5M

People stalked annually in the US (13.5M lifetime).

80%

Stalking victims reporting technology involvement (tracking devices, apps).

40%

US adults who have encountered private data compromise via public Wi-Fi.

$16B+

Cybercrime losses reported to the FBI in 2024.

The tools for surveillance—a $29 AirTag, a $99 WiFi Pineapple—have never been cheaper. The attacker needs five minutes; the defender needs constant vigilance.

The Fragmentation of Personal Defense

Current detection tools are locked inside single-vendor ecosystems, delayed by hours, or nonexistent for 3 billion Android users. VigilWatch bypasses vendor lock-in by reading raw BLE advertisements directly.

The Ecosystem Bypass Diagram

VigilWatch: A Multi-Layered Intelligence System

Layer 1: Passive Environmental Scanning

Continuous BLE & WiFi Discovery.

Layer 2: Behavioral Analytics

Route Contamination & Threat Scoring.

Layer 3: Active Response

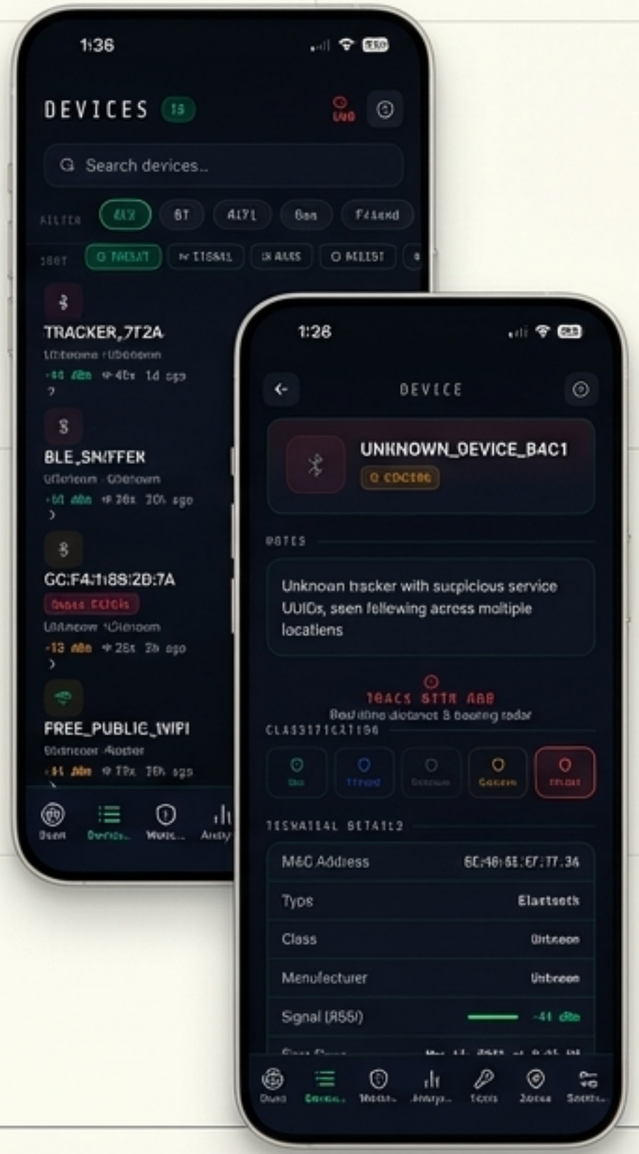
UWB Hardware Pinpointing.

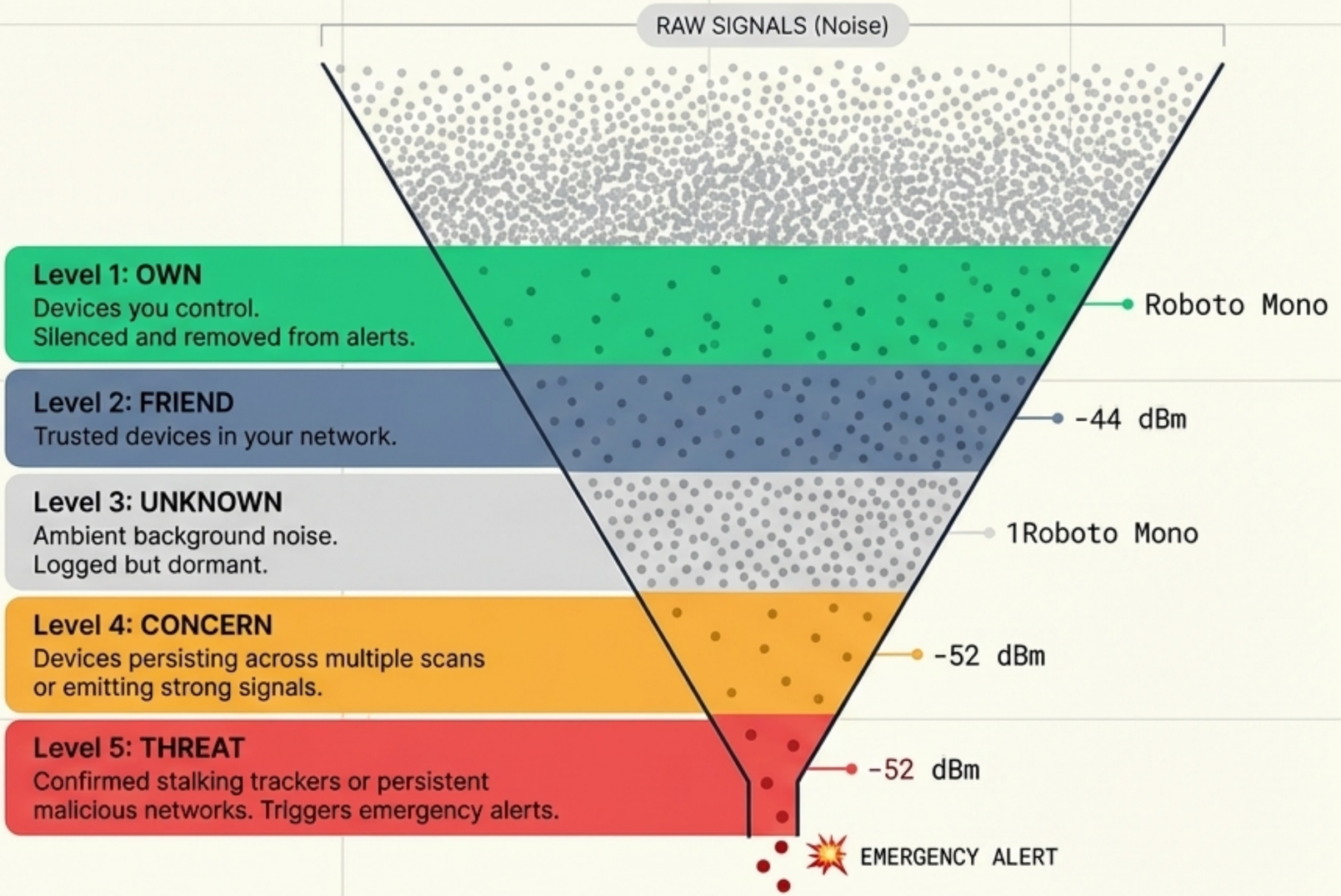
Layer 4: Legal Action

Court-Ready Evidence Export.

Not a delayed notification. A real intelligence system running continuously to build a picture of every device in your world.

Filtering Noise into Actionable Intelligence





Layer 1: Comprehensive Signal Acquisition

BLE Stalking Detection

Scans Classic and BLE signals. Surfaces AirTags, Tiles, custom beacons, and skimmers. Reads raw `MAC addresses` and `signal strength (RSSI)` to determine physical proximity.

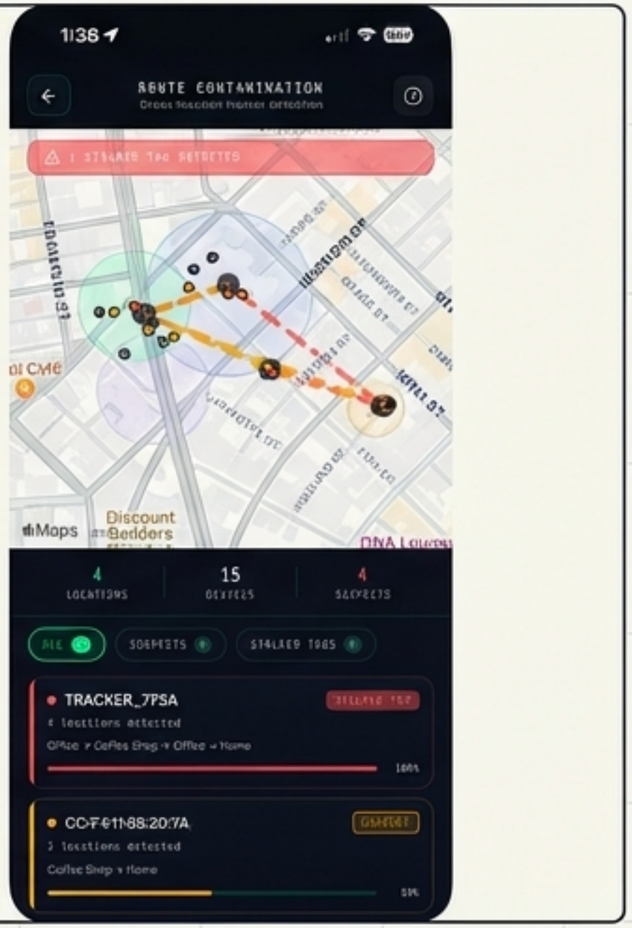
WiFi Surveillance Detection

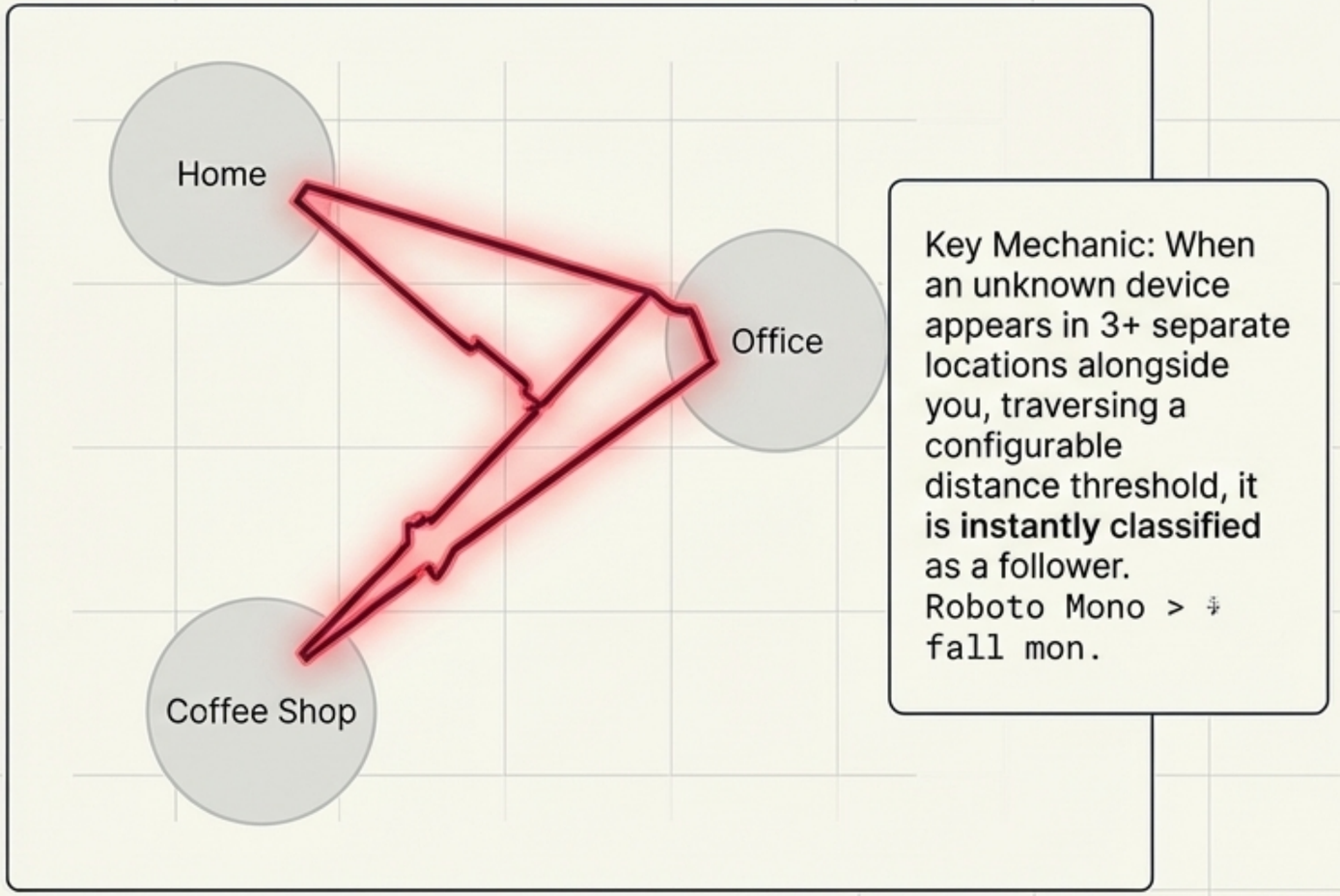
Identifies persistent rogue access points and evil twin networks used to harvest credentials in travel hubs and cafes.

Operational Modes:
Manual, Continuous, and Interval (5, 30, or 60 minutes) background scanning.

Layer 2: Route Contamination Mapping

VigilWatch transforms historical scan data into an active threat intelligence layer. A stalker's tracker becomes visible not through a single scan, but through the undeniable geographic pattern it leaves behind.





The Science of Follow-Me Detection

Haversine Clustering

Groups raw GPS coordinates into 50m semantic zones to prevent false positives from slight GPS drift.

`50m ZONE`

5-Dimension Follow Score

Calculates confidence (0-100) based on time, distance, frequency, and a stationary penalty algorithm.

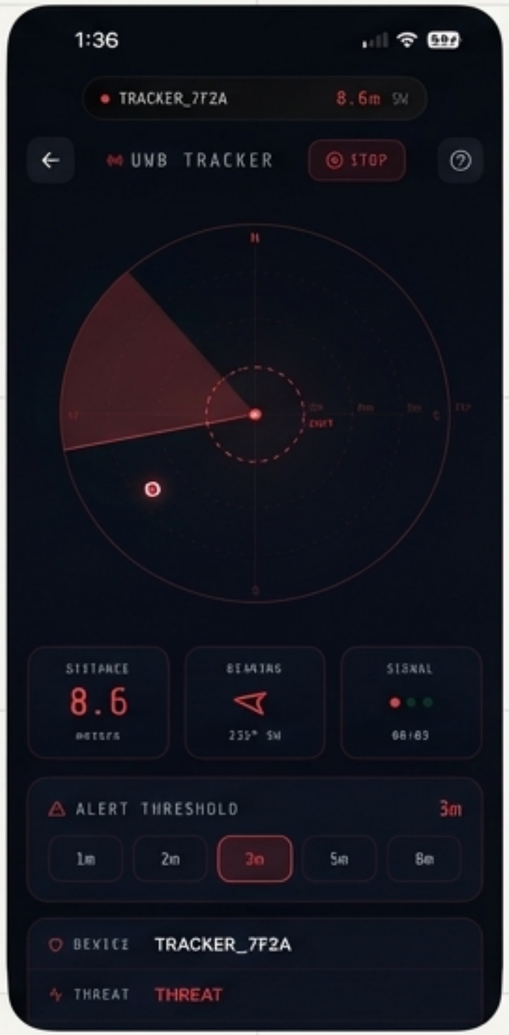
`CONFIDENCE: 0-100`

Threat Trigger

High confidence Follow-Me across 4+ locations provides undeniable proof of physical tracking.

`4+ LOCATIONS`

Layer 3: Precision Proximity Tracking



Active Search Protocol

Turn passive detection into an active physical search. Find the hidden device before you drive away.

Universal UWB Simulation

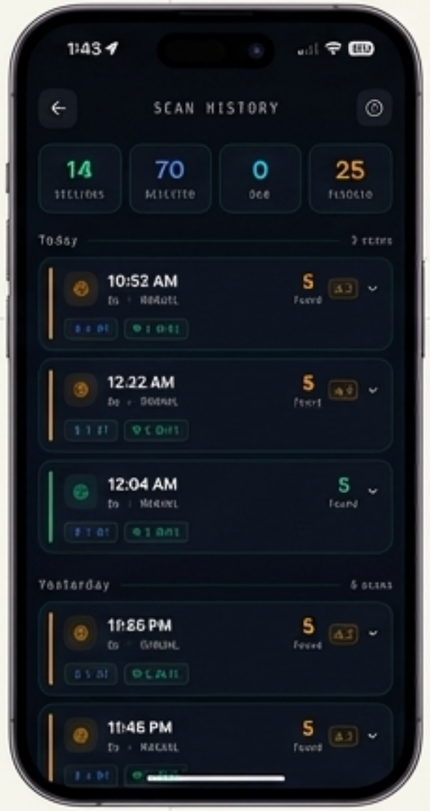
Simulates ultra-wideband (UWB) ranging for non-Apple trackers, displaying real-time estimated distance in meters and signal strength to the exact threat device.

Configurable Perimeters

Set physical alert thresholds (`1m to 8m`) that trigger immediate haptic and visual warnings when the hardware perimeter is breached.

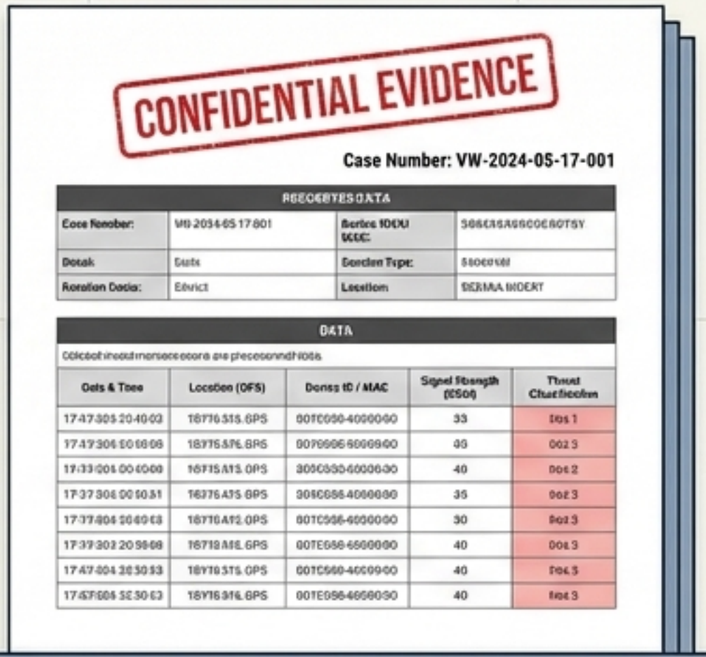
Layer 4: Legal-Grade Evidence Export

Standard built-in alerts vanish. VigilWatch remembers. It transforms your phone's scan history into a structured, court-ready evidence package.



Raw Environmental Capture

Structured Data Export



Includes:
- Unique Case Number
- Exact Timestamps & Geolocation
- RSSI Signal Logs
- Threat Classifications
- COMMUTE PATTERN + ESCALATING trends

The Defense Gap: Market Comparison

Capabilities	VigilWatch	Apple / Google OS	AirGuard	Kaspersky	Generic Scanners
Combined WiFi + BLE Scanning	✅	❌	❌	✅	✅
Route Contamination Analytics	✅	⚠️	❌	❌	❌
UWB Proximity Radar (All Brands)	✅	⚠️	✅	❌	❌
Legal-Grade Evidence Export	✅	❌	❌	⚠️	❌
100% Local Privacy (No Servers)	✅	⚠️	✅	⚠️	✅

VigilWatch is the only holistic intelligence system, not just a branded tracker alarm.

The VigilWatch Defense Loop

DETECT

Layer 1: Continuous, passive environmental sweeping for BLE/WiFi fingerprints.

ANALYZE

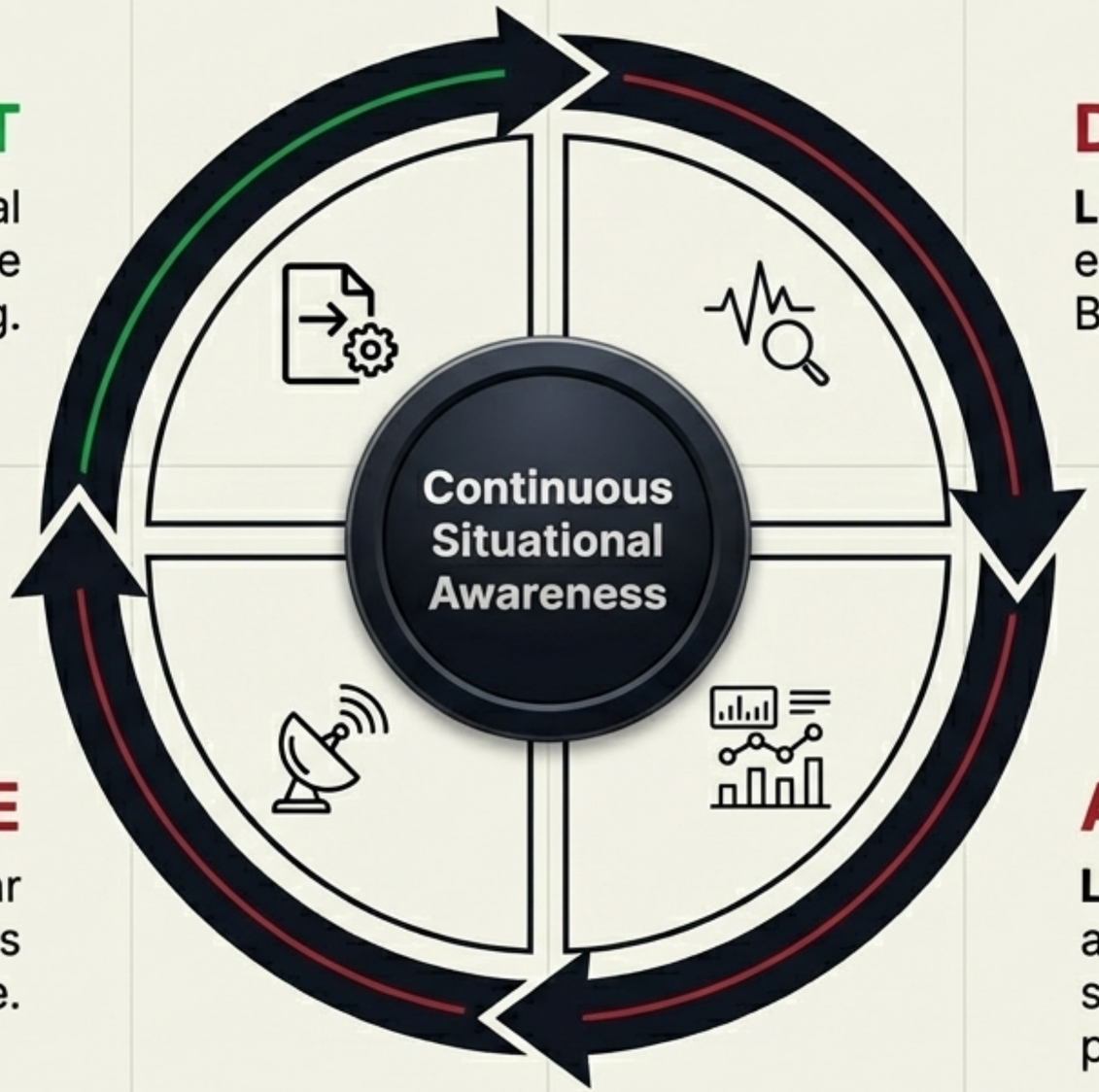
Layer 2: Haversine clustering and Follow Score algorithms surface invisible geographic patterns.

LOCATE

Layer 3: UWB radar pinpointing actively hunts the physical hardware.

ACT

Layer 4: Exportable legal evidence breaks the cycle of stalking.



Absolute Local Privacy & Operational Control

100% Local Storage

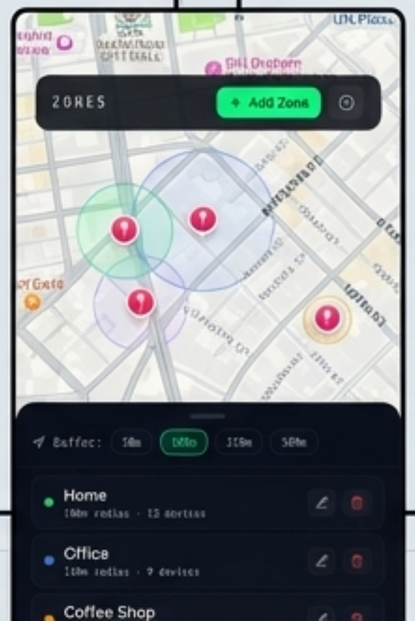
No accounts, no cloud servers, no off-device data sharing. The intelligence stays entirely on your hardware.

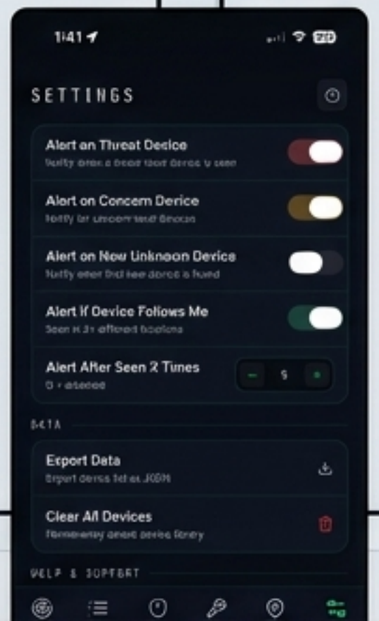
Passive Detection

Scans the environment without ever attempting to connect to or ping the threat devices. The attacker never knows they are being monitored.

Contextual Zones

Users establish custom geofenced buffer zones (e.g., Home, Office at 100m radius) to intelligently contextualize background noise and eliminate false positives.





Who Needs Professional-Grade Detection?

Domestic Abuse Survivors & Advocates

Bypassing notification delays and hardware lock-in to provide immediate, documented safety.

Travelers & Executives

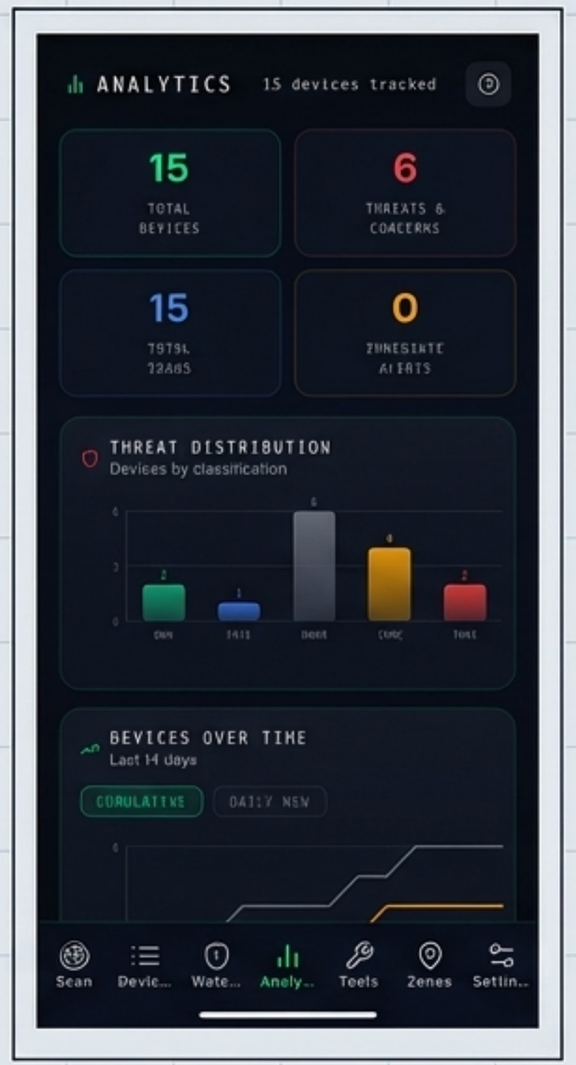
Securing the ambient environment against rogue WiFi and passive data harvesting in hotels and transit hubs.

Privacy-Conscious Individuals

Making the invisible RF spectrum visible, enabling proactive situational awareness.

Security Professionals & First Responders

Utilizing the Analytics Dashboard and Evidence Export for forensic documentation of wireless surveillance.



Scan. Detect. Document. Protect.

The tools to track you are cheap, accessible, and already deployed. VigilWatch is the comprehensive countermeasure that ensures your privacy remains yours to protect.

Your world. Your frequency.