BROADKORE

Passive SIGINT and Wireless Device Detection for Secure Facilities

Spectrum Operations | SIGINT | Electronic Warfare | Aerospace Engineering

CAPABILITY BRIEFING | 2026

BROADKORE builds passive, zero-emission RF sensing that helps authorized operators of correctional and secure facilities find unauthorized cellular, Wi-Fi, Bluetooth and IoT devices in the spaces they are responsible for. The platform never transmits, never disrupts authorized networks, requires no FCC transmit authorization, and works alongside existing cellular Managed Access Systems (MAS).

SIGINT Platform: Core Capabilities

SIGINT and RF detection. Detects cellular and wideband transmitters within a defined site from a distributed network or a single sensor, customized to power and size requirements. Direction finding and geolocation are in development.

Authorized equipment recognition. Learns the RF characteristics of a facility's own authorized equipment so unknown devices stand out.

Cell-site simulator detection. Protects staff and visitors by detecting rogue base stations (IMSI catchers) near a protected site.

Passive Wi-Fi, Bluetooth and IoT sensing. Extends protection beyond cellular to 2.4, 5 and 6 GHz Wi-Fi, Classic Bluetooth and Bluetooth Low Energy (BLE).

Spectrum operations and EW. Spectrum operations, detection of RF and acoustic weapons, and electromagnetic pulse (EMP) and counter-UAS (C-UAS) systems.

Wireless Interdiction Augmentation

- **Rogue hotspot and unauthorized device detection:** unauthorized access points, tethering and hotspots, peer-to-peer links and prohibited wireless peripherals.
- **Device association mapping:** which devices connect to which access points inside the restricted area.
- **Device location (in development):** direction finding and geolocation, indoors and along the perimeter.
- **MAS integration:** Wi-Fi and Bluetooth detections combined with cellular MAS data, with automated alerts.

Device or link	MAS alone	MAS + BROADKORE
Cellular handsets	Covered	Covered
Wi-Fi-only phones and tablets	Blind spot	Covered
Hotspots and tethered devices	Partial	Covered
Rogue Wi-Fi access points	Blind spot	Covered
Bluetooth and BLE peripherals	Blind spot	Covered
Cell-site simulators	Blind spot	Covered

Mission Environments

Correctional facilities

Find contraband phones, hotspots and Bluetooth devices that cellular interdiction misses, with distributed or single-sensor coverage.

SCIFs and defense installations

Continuous checks for prohibited personal electronic devices without adding any emitter to a controlled space.

Border and perimeter security

Detect unauthorized wireless activity along a defined fence line or port of entry with distributed or single sensors sized to the site.

Responsible by Design

- **Defined boundaries:** sensing is configured for a specific facility or perimeter.
- **Signals, not content:** works with signal characteristics and device metadata, not the content of communications.
- **Operator controlled:** deployed by authorized facility operators under their own policies and applicable law.

Aerospace Technology and Reverse Engineering

Consulting, design and prototyping for emerging aerospace systems: counter-UAS, radar, 4G LTE and 5G systems engineering, radio propagation and antenna array analysis, embedded systems for UAVs, reverse engineering and analysis, product design and engineering services.

0 W	2.4 / 5 / 6 GHz	1 or many sensors	No jamming
RF energy transmitted	Wi-Fi bands monitored	Sized to power and size needs	No FCC transmit license needed

HEAD OFFICE
Huntsville, Alabama
United States

EMAIL
ci@broadkore.com

WEB
broadkore.com

Request a capability briefing: broadkore.com/sigint.html#contact

(c) 2026 BROADKORE. All rights reserved.