



Endurion

Digital Force Protection (DFP)

July 2026

Turning Tactical RF Collection into Operational Intelligence

Digital Force Protection requires visibility into the electromagnetic environment surrounding personnel, facilities, vehicles, and mission activity. As operators move through contested digital environments, adversaries can exploit wireless emissions, rogue infrastructure, Bluetooth trackers, drone activity, GNSS interference, and cellular anomalies to monitor, track, or compromise operations.

Integrated Mission Technology

Signal Hardware

Serves as tactical-edge RF collection hardware, passively capturing Wi-Fi, Bluetooth, GNSS, and other signal telemetry from the operating environment.

Pathfinder Software

Ingests, enriches, analyzes, visualizes, and operationalizes that data into actionable intelligence.

Together, the technology enables teams to detect digital exposure, identify anomalous RF activity, monitor persistent emitters or co-travelers, assess technical surveillance risk, and maintain a shared understanding of the digital threat environment.

The Alert Lifecycle

[1] Ingest

Signals ingest via MQTT into WiFi, cellular, Bluetooth, GNSS, and Remote ID tables for analysis.

[3] Detect

Active detectors run against each enriched event, with compound escalation, scoring, and alerting.

[5] Persist

Alerts are deduplicated, stored, and incremented when repeat observations occur.

[2] Enrich

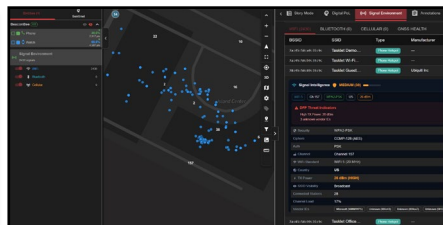
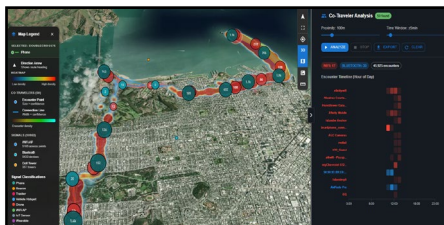
Signals gain OUI, geofence, device, and scan context to separate noise from mission-relevant indicators.

[4] Fuse

Results are scored, grouped, and adjusted based on geography, confidence, and operational context.

[6] Resolve

Stale alerts are automatically resolved based on severity-specific suppression windows.





Digital Coverage

Wi-Fi Threat Detection

- Rogue AP, Open Non-IoT AP, Foreign Country AP, Hidden + High Power
- IE Open Network, Evil Twin, Multichannel Honeypot, Connection Downgrade

Cellular Threat Detection

- Unknown PCI, Foreign MCC, Null Cell Tower ID
- Unlicensed ARFCN, Unregistered Operator

Bluetooth Threat Detection

- Known Tracker OUI, Unknown Persistent Device
- MAC Anomalies, Signal Strength, Close Proximity Alerts

GNSS Threat Detection

- GNSS Jamming, SV Exclusion Spoofing
- Clock Coherence Spoofing, Time-of-Week Patterns

Drone & Behavioral Detection

- RemoteID Broadcast, BLE + WiFi Drone Signature
- Co-Travelers, Abnormal Signal Presence

Operational Value

Enabling faster investigations, proactive response, and visualization of potential DFP threats

Persistent Awareness Across Locations

- Captures local RF activity as operators move across mission-relevant locations.
- Supports awareness across hotels, airports, vehicles, partner facilities, training sites, and mission areas.
- Connects RF observations across multiple locations instead of treating each site as an isolated event.

Geofence-Aware Threat Scoring

- Applies location-based context to RF detections.
- Elevates anomalous activity when it occurs near sensitive facilities, lodging, event venues, convoy routes, restricted areas, or operating locations.
- Distinguishes routine background RF activity from indicators that carry greater operational risk.

Multi-Node and Multi-Phone Positioning

- Uses observations from multiple RF + Signal detection sets and operator devices to support emitter localization.
- Combines signal strength, timing, and position data to estimate where suspicious emitters may be located.
- Supports detection of access points, BLE trackers, cell towers, and additional RF sources within the operating environment.



Enhanced Digital Force Protection Through Integrated Mission Technology

Endurion's technology provides a differentiated Digital Force Protection capability by connecting tactical-edge RF collection, anomaly detection, geospatial context, and operational intelligence within a single platform. Beluga captures passive signal telemetry at the edge, while Pathfinder enriches, fuses, visualizes, and operationalizes that data into actionable intelligence. Together, they enable organizations to detect technical surveillance indicators, map the digital environment around personnel and mission locations, identify rogue or persistent signal activity, correlate RF observations with movement and geofences, escalate compound indicators into higher-confidence alerts, and build historical baselines across locations, events, routes, and recurring operations.

The Future of Mission Advantage.

