ThreatBlocker
GPS Jamming and Spoofing Data, Detection, and Protection

The Problem
- The world has become dependent on GPS to maintain our way of life
- Jamming and spoofing hardware/open source software is more accessible than ever before
- New solutions require system overhauls, changing all GPS components and antennas
- Solutions that protect the integrity of our GPS systems are required today

The Solution
ThreatBlocker provides GPS jamming and spoofing data, detection, and protection; leveraging Orolia Defense & Security’s patented BroadShield software and The Aerospace Corporation's BLISS (Blind Interference Signal Suppression) algorithms. It is configurable to meet your requirements and is designed to be installed in-line with your existing hardware. Install ThreatBlocker in-between a FRPA (Fixed Radiation Pattern Antenna) and GNSS receiver/system. Threatblocker has LED status indicators for real-time awareness, robust API for data output, and an intuitive web user interface to view real-time and historical data.

WHAT IS BROADSHIELD?
Patented GPS jamming and spoofing detection algorithms.

WHAT IS BLISS?
A digital processing technique to suppress jamming signals.

NEW CAPABILITIES
- L1 & L2 anti-jam (AJ) capabilities
- L1 & L2 jamming detection
- L1 & L2 J/S measurements
- Ideal for common jammers
Specifications

**Size, Weight and Power**

- **Size:** 144 x 164 x 32mm (WxDxH)
- **Weight:** 840 grams
- **Power:** 10 Watts (Peak)

**Data output via Light Weight Ethernet (LWE)**

- Built-in API
- RaptorX plugin
- WebUI

**Ruggedization and Compliance Certifications**

- Wide voltage input: 9-36V
- Operating temp: -40°C to +85°C
- EMI/EMC EN 55032, FCC 47 CFR PART 15/EN 55024/2014/30/EU

**STANDARD CONFIGURATION**

**PLOT - LIVE FIRE FIELD TEST**

Data output from ThreatBlocker is compatible with an existing RaptorX plugin, allowing for a GPS jamming heat map. Blue corresponds to low J/S while red corresponds to high J/S.

**J/S MEASUREMENTS - LIVE FIRE FIELD TEST**