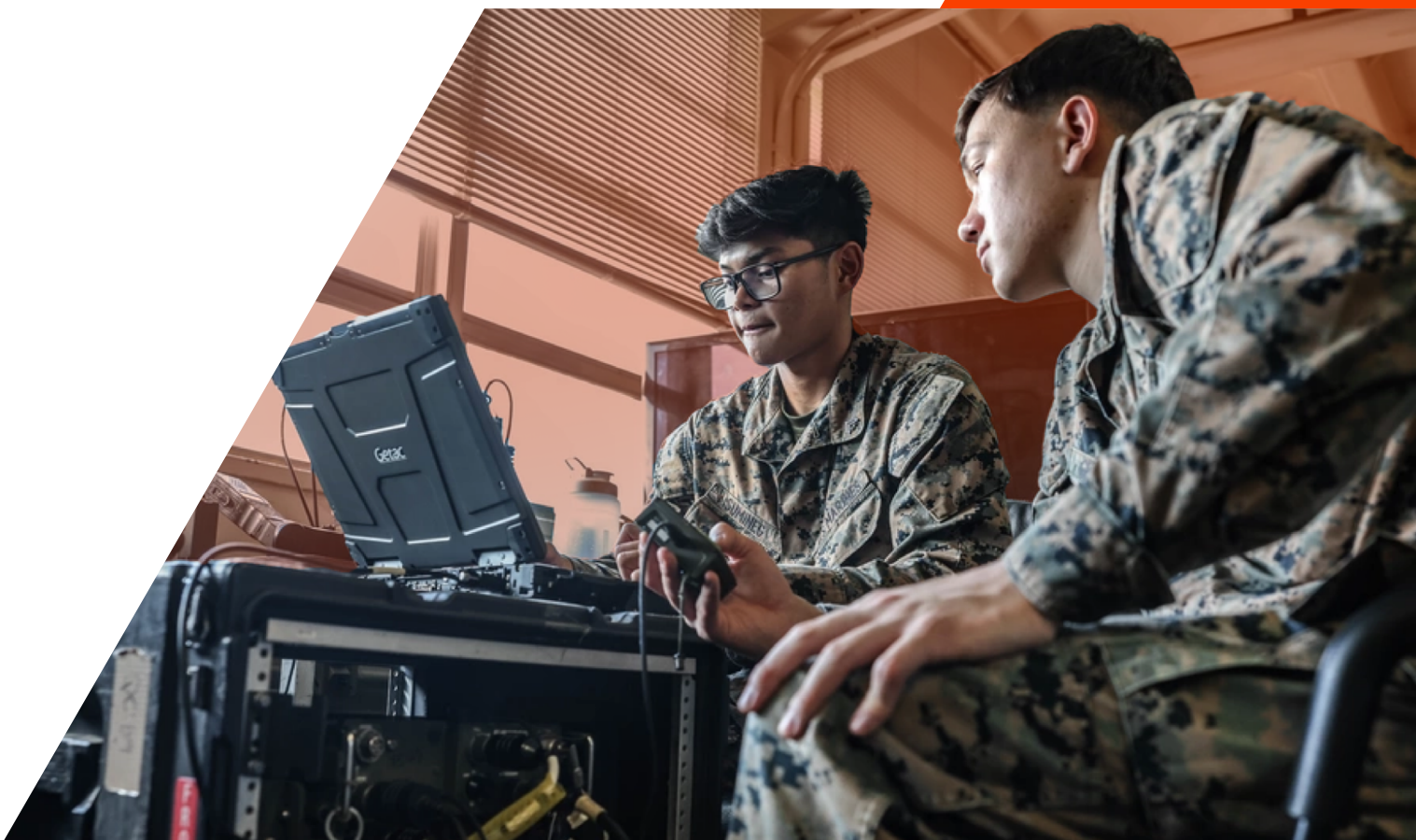
Bastille

EXECUTIVE DATASHEET

# Bastille Public Sector



# Enforce Device Policy with 24x7 Wi-Fi, Cellular and Bluetooth Detection, Location and Alerting

Bastille's real-time Cellular, Bluetooth, BLE and Wi-Fi detection and location system locates all authorized and unauthorized devices within a campus or forward deployed location. Bastille accurately places dots on a floor-plan for device location and sends alerts when a device is found where it should not be or doing what it should not do.

**Sample devices located include:**

- **Cellular Phones:** Individual phones located in real-time just by their cellular signal
- **Bluetooth/BLE:** Detect paired, active pairing and unpaired devices
- **Wearables:** e.g. Smart watches such as Garmin Fenix, FitBit and Biometric Human Performance Monitors and other tactical gear
- **Personal Medical Devices:** e.g. Hearing aids
- **Laptops & Tablets**
- **Any device emitting cellular, Wi-Fi, Bluetooth or BLE**

## Precise Real-Time Accurate Individual Device Location – Not Misty Heat Maps

Earlier solutions and even some existing solutions detect power in a certain frequency in an area, and therefore cannot tell you if there is one device or 10 devices in a room. Bastille's multi-patented solution recognizes individual devices, including individual cellular signals, and places a real-time dot on your floor plan to show where the device is located... which eliminates false positives.

## Deploy and GEOFENCE (in/out) for SCIF and Open Secret Environments

Bastille is FCC certified as 100% passive and can be deployed where no transmitters are permitted. Bastille can set geo-fences to include or exclude areas where devices are/not allowed and send real-time alerts when devices are located and/or policies are violated.

> We are excited to see the final development of Bastille's technology to provide security by monitoring the RF and cellular spectrum.

**Anil John**

SVIP Technical Director, U.S. Department of Homeland Security Press Release

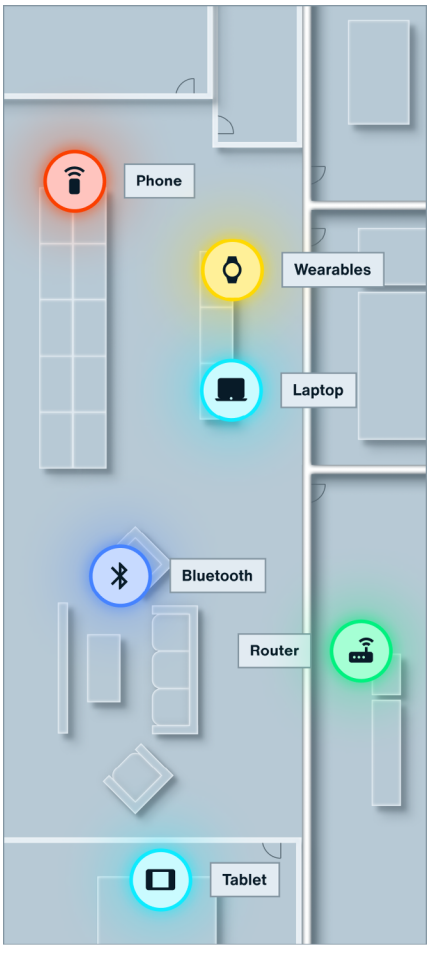



**Figure 1:** Bastille provides real-time Cellular, Bluetooth, BLE and Wi-Fi device detection, location and alerts

## Authorized vs Unauthorized Devices

Commands want to permit only certain authorized devices in SCIF/Open Secret areas, and Bastille makes this possible. Bastille takes feeds from other systems, such as Aruba, where a device has been authorized, and gives the ability to tag specific devices as authorized for a given location and/or time.

## Bastille's Unique Bluetooth Detection – Device Pairing Red Alerts

Bastille detects and Red Alerts if device pairing ever happens e.g. a Garmin Fenix pairs with a phone in a locker or car outside the Open Secret area. Even BLE devices can pair up to 100 metres or more! In other systems, once a Bluetooth/ BLE device is paired, the devices become invisible to the system. This is exactly when you don't want them to be invisible. If you need to understand where Bluetooth devices are, what they are connected to and how active they are, then Bastille has the only way to do it.

## Detailed Device Information

Bastille passively determines more than 150 fields of information from devices including manufacturer, model, name, network connection, frequency, and transmitter ID among other fields. This data provides valuable context for both forensic and real-time device determination and adjudication.

## Forensics

Bastille provides accurate locations and device information in DVR format for a year or longer to permit detailed investigations for insider threat. Exports to Splunk, Tableau or any other system via standard APIs.

## Canned Splunk, aruba & Other Enterprise Integrations

Bastille's standards based APIs allow simple integration with all your existing systems like Splunk, SIEMs, Incident Response Platforms, Wi-Fi WIDS and Access Points without the need for additional modules.

## Key Bastille Features

- LoAuthorized vs. unauthorized devices
- Works for SCIF/Open Secret areas
- Bluetooth / BLE pairing, paired, unpaired alerts
- Detailed device information
- DVR for forensics
- Device location within 3 meters
- SIEMS integrations, including Splunk
- NAC Integrations with Aruba, Cisco/Meraki
- Standards-based APIs
- On-premise deployment
- FCC certified 100% passive
- MDM integrations with VMWare and MobileIron

**Figure 2:** Sensor Arrays

## MDM and Access Control

Use Bastille's integrations to disconnect a device from the network via your NAC system if a device breaches a geofenced area or breaks a policy. Bastille integrates with MDM solutions to provide location information to the MDM solution, which then can disable apps on the device, such as the camera app when the device enters a geofenced or restricted area.

## Device Adjudication Workflow

Bastille allows you to accurately **Detect** and **Locate** all devices, **Evaluate** if a certain device is permitted in an area and if it presents a threat, send an **Alert** to **Investigate** the device with detailed device information and **Resolve** the incident and record the actions taken.

## About Bastille

Launched in 2014, Bastille is the leader in enterprise threat detection through software-defined radio. Bastille provides full visibility into the known and unknown mobile, wireless and Internet of Things devices inside an enterprise's corporate airspace–together known as the Internet of Radios. Through its patented software-defined radio and machine learning technology, Bastille senses, identifies and localizes threats, providing security teams the ability to accurately quantify risk and mitigate airborne threats that could pose a danger to network infrastructure.

NTS

Test Certificate

A sample of the following product received on January 17, 2018 and tested on January 17, 23 and 26 and February 2, 2018 complied with the requirements of,

- Subpart B of Part 15 of FCC Rules for Class A digital devices
- Innovation, Science and Economic Development Canada Interference Causing Equipment Standard ICES-003, "Information Technology Equipment (ITE) – Limits and methods of measurement", Issue 6, dated January 2016 (Class A)

given the measurement uncertainties detailed in National Technical Systems report FR-060661.01-FCC Rev 0.

Bastille Networks
Model Sensor-2

Deniz Demirci
Senior Wireless / EMC Engineer

David Guidotti
Report Preparer

Gary Izzell
Quality Assurance Delegate

**Figure 3:** 100% Passive-Only FCC Certification

Bastille

## About us

Bastille specializes in providing security solutions for wireless environments. Bastille uses a network of Software-Defined Radios (SDRs) to continuously monitor a facility's entire wireless environment, including cellular, Bluetooth Classic, Bluetooth Low Energy (BLE), Wi-Fi, Zigbee, and other protocols. Our sensors detect, analyze, and localize transmissions in real time, providing a comprehensive view of wireless activity.

Bastille's system goes beyond just identifying signals; it analyzes data to uncover real-time and long-term threats. By capturing the entire wireless spectrum, Bastille offers unparalleled visibility into potential security risks, empowering organizations to proactively safeguard their wireless infrastructure.

## Learn more

To learn more please visit
[www.bastille.net](http://www.bastille.net)

Or follow us on