Bastille

EXECUTIVE SOLUTION BRIEF

# Intelligent Wireless Airspace Defense For Classified Areas

# Mission Security Is Critical

Securing classified areas and Sensitive Compartmented Information Facilities (SCIFs) requires a suite of security tools, protocols, and personnel to ensure the broadest and most comprehensive solution is in place. Each mission has different security requirements, the strictest of which include securing locations from wireless threats.

The world has moved on from a simple 100% wireless device exclusion policy. Wireless electronic device policy has evolved to keep pace with employment law, attract and retain talent, and embrace sensor-rich mission support technologies. Today, allowing personal medical devices, performance-enhancing wearables, and supporting a broader personnel profile is a reality. An intelligent wireless threat security system is more than device detection; it must support rapid geolocation, device assessment, and simplified adjudication workflows.

# Physical Security Has Limits

Physical security of classified areas is a well-refined practice involving identity scanners, physical blockades, trained guards, motion detectors, and comprehensive camera systems. It focuses entirely on what can be seen and touched and will always fail to detect invisible, wireless threats.

Wireless Airspace Defense, by contrast, focuses on identifying and locating the invisible threats present in today's classified facilities.

Bastille's solution can ensure your classified area is continuously monitored for wireless activity and identify threats before they reach the sensitive data your mission is handling.

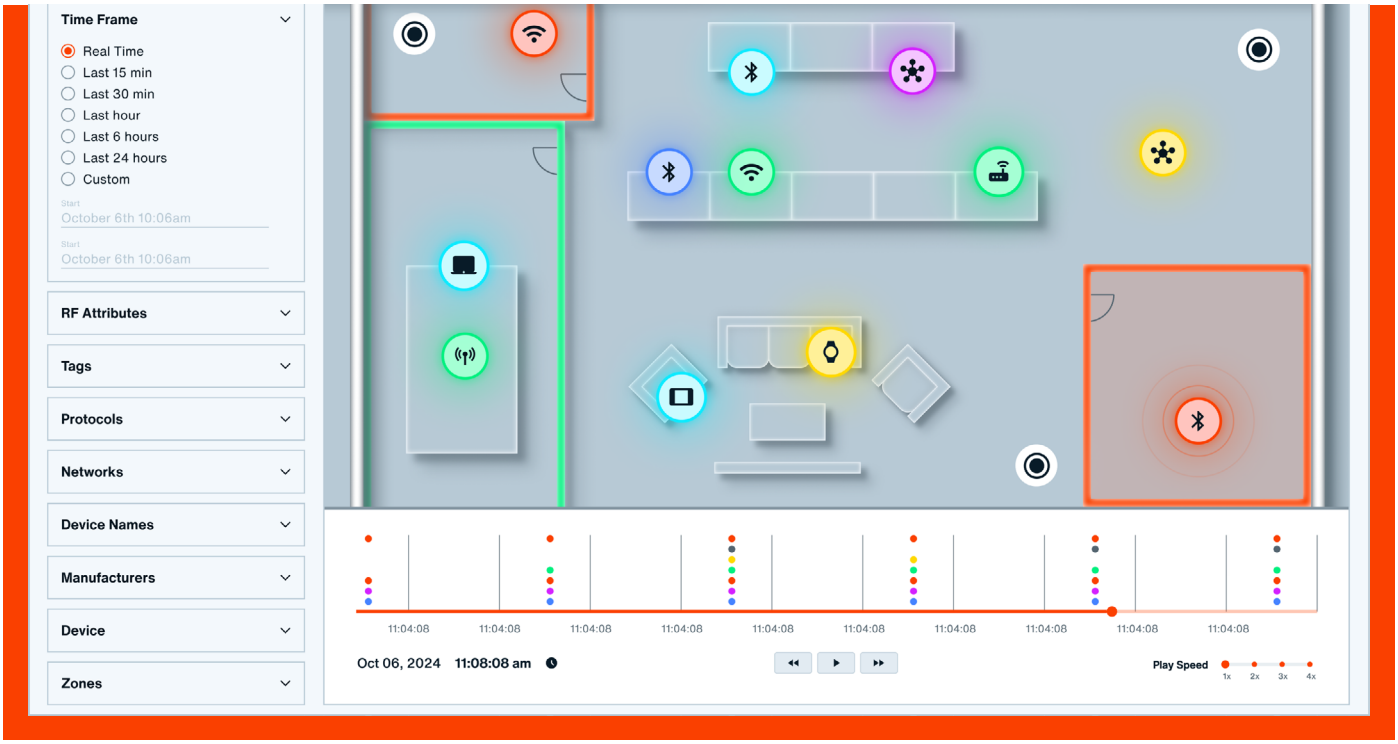



**Figure 1:** Bastille's Solution For Intelligent Wireless Airspace Defense For Classified Areas

# Wireless Threats

Wireless threats, like network-borne vulnerabilities and malware, are evolving rapidly. However, they have a distinct advantage over network-centric attacks: They are not detectable on managed networks. Wireless threats can exfiltrate data out-of-band from even the most complex firewall, intrusion detection, and malware scanning systems on a physical network. You must continuously monitor for wireless threat activity to ensure your classified space is free of unknown wireless threats.

**Wireless threats manifest themselves in forms such as:**

- Cellular voice, data and video ex-fil devices, which can bridge physical networks
- Rogue Wi-Fi access points and data ex-fil devices
- Rogue video and still-image cameras
- Bluetooth-based data harvesting devices
- Industrial Control System jammers, blockers and signal interfering devices

These threats can compromise the security of the spaces where you hold sensitive discussions, process critical information, or have compliance obligations regarding the security of the wireless airspace.

# Cellular Phones

Most SCIFs have a set of lockers outside, and everyone entering the SCIF knows they should have left their phone in their vehicle or in one of those lockers. And yet, many of us have been in a classified meeting when we heard a phone ring! Was that phone also compromised by spyware, unbeknownst to the user? Cell phones are notoriously hard to detect just by their cellular signal. The cellular signals phones emit are just not as “chatty” as expected. Bastille has the unique ability to locate cell phones just by their cellular signal, separate multiple such phones, and put an accurate location dot on a floor plan map to tell you the exact whereabouts of each phone.

Whether a person maliciously or accidentally brought a cell phone into your SCIF is secondary to your need to know precisely and immediately where it is, where it’s been, and as much attribute data about the device as possible.

# Threats Are Evasive

Wireless devices used for eavesdropping or data exfiltration would be ineffective if they were easy to find. They often attempt to avoid detection by transmitting during busy times (to blend in) or off-hours (fewer observers). A continuous monitoring wireless TSCM system, like Bastille, will detect threat devices whenever they transmit.

# Threats Are Camouflaged

Advanced data exfiltration threat devices look precisely like cables and components usually present in your facility. The only way to detect the threat is to monitor the wireless spectrum for transmissions that violate security policy.

Physical inspection can not identify these threats.

# A Hearing Aid is a Listening Device

Under employment law, SCIFs must allow employees with a medical need for hearing aids access to the facility. They sit in classified meetings as needed. However, if the hearing aid connects over Bluetooth to a compromised phone in the parking lot, then that is an audio exfiltration risk. The wearer may not even know they are connected or that attackers have compromised their phones.
But YOU need to know!

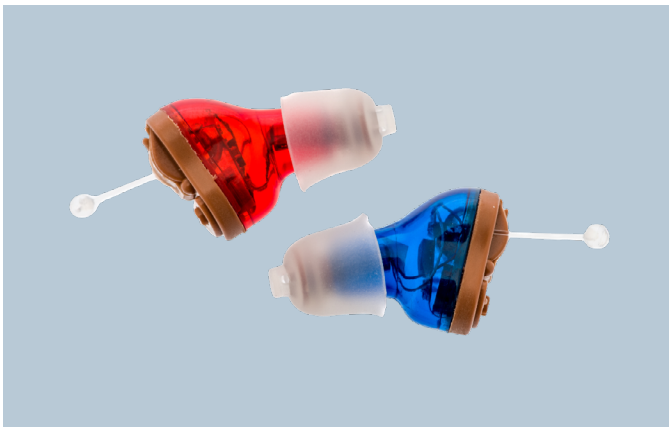


**Figure 2:** Hearing Aid Listening Device

# Intelligent Wireless Threat Security

The threat of unknown wireless devices in classified areas will be ever-present; monitoring for these threats must match the mission security parameters AND the personnel supporting them. This refined approach is:

- Intelligent
- Comprehensive
- Integrated
- Future Focused

Bastille Networks makes this refined approach available.

# Bastille Solution

Bastille provides intelligent, comprehensive, continuous monitoring for wireless threats within classified areas and SCIFs. The Bastille solution combines Sensor Arrays deployed throughout your facility, Concentrators to aggregate and process sensor data, and the Fusion Center platform, which analyzes and augments the wireless data and enables integrations with your existing security systems. This tiered architecture allows the Bastille solution to scale from monitoring a single room to many campuses worldwide with a single management interface.

# Sensors

Bastille achieves comprehensive monitoring by deploying its sensor arrays throughout the monitored facility. Bastille sensor arrays detect wireless emitter activity from 25 MHz to 6 GHz, and Bastille decodes, processes, and sends this RF metadata traffic to the Concentrator for further event correlation. The sensor arrays are 100% passive, which means they never transmit, are plenum-rated, are available for indoor and outdoor use, and are manufactured in the United States. The sensors capture all available attributes of the wireless devices, including dozens of identifiers such as vendor name, Bluetooth network definitions, Wi-Fi device characteristics, and Cellular network information.

Bastille's Sensor Arrays use Software-Defined Radio (SDR) technology, which allows them to receive in-place upgrades and ensures future protocol support and decoding.

Bastille's Sensor Arrays are nondescript and can be concealed above false ceilings or left in the open and labeled with harmless designations to reduce suspicion or inspection.

**Figure 3:** Sensor Arrays

# Concentrator

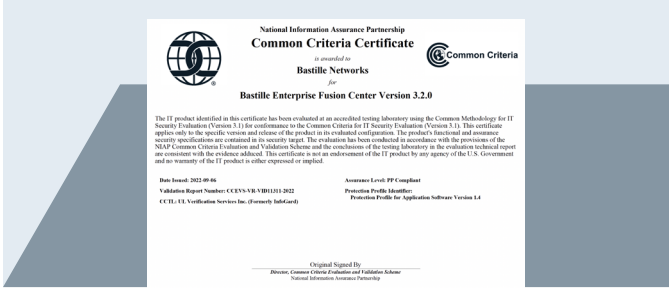
The Bastille Concentrator receives data from a facility's sensor arrays, refines and consolidates the data into events, and sends them to the Fusion Center.
The Premium Concentrator gathers additional data from cellular device transmissions.

# Fusion Center

Bastille's Fusion Center platform is the only NIAP-certified product in this market and provides additional assurances on the quality and security of the Bastille solution. Fusion Center receives wireless data from the Concentrator(s), compiles and analyzes the data, and displays all data on current and historical wireless device activity. The Fusion Center overlays any detected wireless device clearly on your facility floor plan, including the current device location to within 3m accuracy and a playback capability to show the historical position of each wireless device as it moves through your space. This playback functionality allows correlation with other systems to determine who brought the device in and when and where they traveled within the facility.

Bastille's Fusion Center automatically detects known wireless threats from its curated database of threats discovered by Bastille's Threat Research team and industry-disclosed vulnerabilities. The Fusion Center platform offers highly customizable reports, provides rich API capabilities for integration with SIEM/SOAR systems, and is fully maintained and supported by Bastille along with the sensor arrays for the life of the subscription.

Data from Bastille's Fusion Center will help accelerate compliance audits of your facility and detect unauthorized wireless devices before they enter your secure space.


National Information Assurance Partnership

Common Criteria Certificate

is awarded to

Bastille Networks

for

Bastille Enterprise Fusion Center Version 3.2.0

Common Criteria

**Figure 4:** 100% Passive-Only FCC Certification

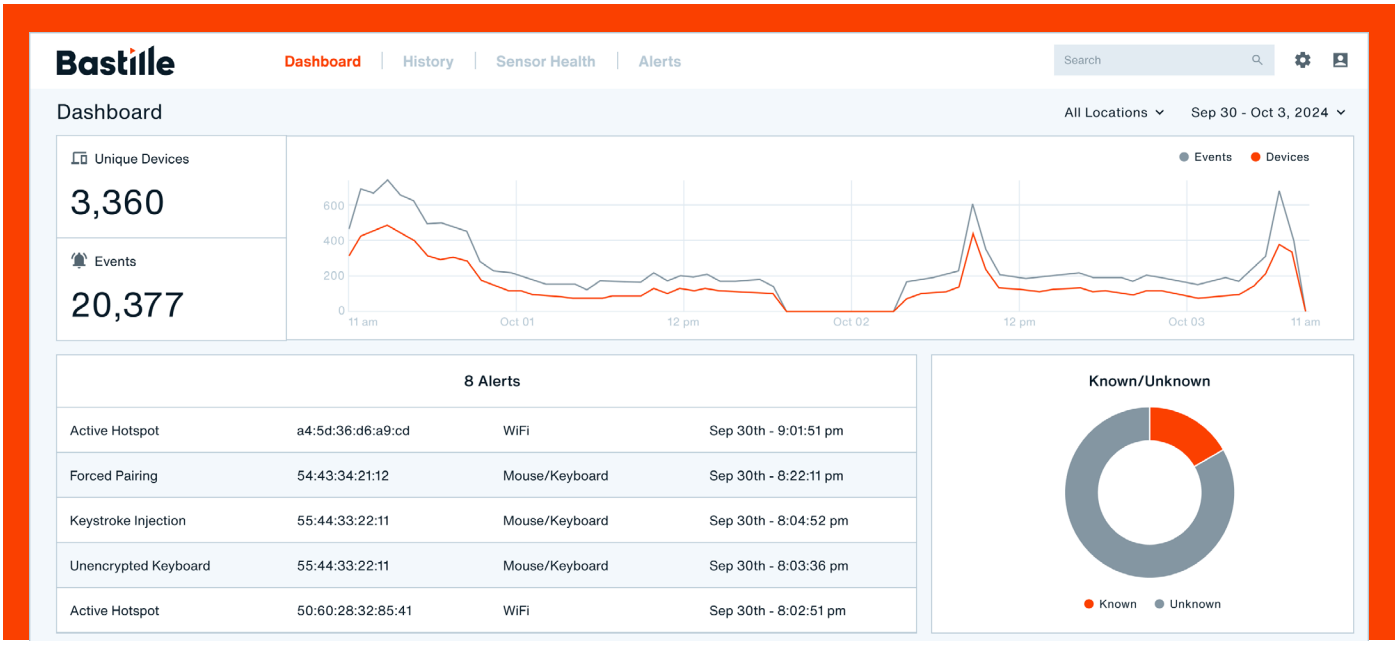



**Figure 5:** Bastille's Fusion Center

# Bastille's Differentiation

Bastille has 30 patents in the wireless detection space and maintains a significant advantage in detecting wireless threats.

**EXAMPLE**

## Threat Signatures & Event Intelligence

Bastille's Threat Signatures filter through all detected devices and apply categorizations to them so you can focus your resources on the critical threats. Bastille's solution brings wireless data to your security policy enabling you to evolve your policy to match the reality of your environment.

Bastille's comprehensive categorization capabilities allow you to rapidly detect new RF emitters and assess their threat posture while maintaining visibility to approved devices such as performance wearables and medical devices used by your personnel.

**EXAMPLE**

## Individual Cellular Device Detection

Bastille provides comprehensive data on individual cellular devices that transmit in the monitored space. With Bastille's technology, you can track each cellular device's location, carrier, and specific attributes as it moves through the monitored facility.

**EXAMPLE**

## Advanced Bluetooth Device Detection

Bastille uniquely monitors all 79 Bluetooth and 40 Bluetooth Low Energy channels simultaneously. This approach identifies Bluetooth-paired devices, explicitly noting the paired network endpoints and their attributes. Other vendors only show when Bluetooth devices are looking to pair; after they've paired, they become invisible. After a device has paired, it can exfiltrate data and cause disruption; you need this visibility to protect against Bluetooth threats.


**Figure 6:** Bastille's Solution For Intelligent Wireless Airspace Defense For Classified Areas

# Protecting The Most Secure Locations

**U.S. Department of Defense**


**U.S. Department of Energy**


**U.S. Department of Homeland Security**


**U.S. Department of The Air Force**


**U.S. Intelligence Community**


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

or follow us on