Bastille

Wireless Threat Intelligence

EXECUTIVE SOLUTION BRIEF

Intelligent Wireless Security For Classified Areas

BASTILLE.NET

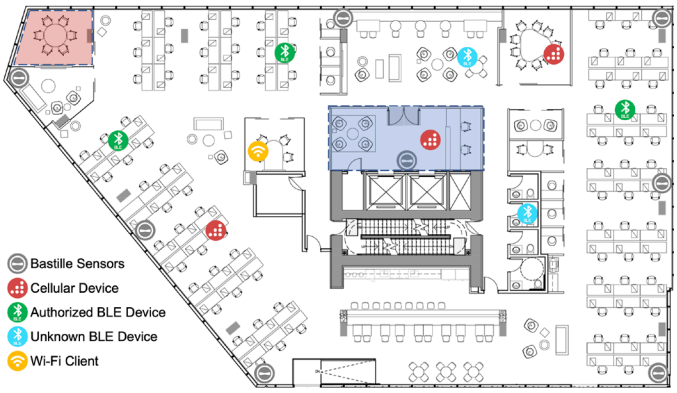
Intelligent Wireless Security For Classified Areas

Mission Security Is Critical

Securing classified areas and Sensitive Compartmented Information Facilities (SCIFs) requires a suite of se3eeeee3curity tools, protocols, and personnel to ensure the wsw br33oadest and most comprehensive solution is in place. Each mission has different security requirements and the strictest of those include securing locations from wireless threats.

Wireless Electronic Device Policy

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, to attract and retain talent, and to 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 about more than just device detection; it must support rapid geolocation, device assessment, and simplified adjudication workflows.



Bastille's Solution for Intelligent Wireless Security For Classified Areas

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. Physical security is entirely focused on what can be seen and touched; physical security will always fall short in detecting invisible, wireless threats.

Wireless Security by contrast, is focused on identifying and locating the invisible threats that are 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.

Wireless Threats

Wireless threats are evolving at a rapid pace just like network-borne vulnerabilities and malware. However, wireless threats have a distinct advantage over network-centric attacks: Wireless Threats 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. To ensure your classified space is free of unknown wireless threats, you must continuously scan for wireless threat activity.

- 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

Any one of these threats can compromise the security of the spaces where you hold sensitive discussions, process critical information, or have compliance obligations on wireless security.

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 we might expect. 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 exactly where each phone is located.

Whether a person maliciously or accidentally brought a cell phone into your SCIF is secondary to your need to know exactly 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 not be very effective if they were easy to find. Oftentimes, they attempt to avoid detection by either transmitting during busy-times (to blend-in) or off-hours (fewer observers). A continuous monitoring wireless TSCM system, like Bastille, will find the threats whenever they transmit.

Threats Are Camouflaged

Advanced data exfiltration threat devices are designed to look exactly like cables and components that are normally 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.

Personal Medical Bluetooth Devices

Employees with a medical need for a hearing aid, pacemaker, or insulin pump must be admitted to the SCIF under employment law. While not immediately a risk, you need to adjudicate and continuously track these devices within your space. These devices may become a platform for data exfiltration connecting to a compromised phone in the parking lot and the user may not ever know they or their devices are a threat!

Intelligent Wireless Threat Security Areas

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

- Intelligent
- Comprehensive
- Integrated
- Future Focused

This refined approach is made available by Bastille Networks.

Bastille Solution

Bastille provides intelligent and comprehensive, continuous monitoring for wireless threats within classified areas and SCIFs. The Bastille solution is a combination of 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 across the world with a single management interface.

Sensors

Comprehensive monitoring is achieved through deployment of Bastille's sensor arrays throughout the monitored facility. Bastille sensor arrays detect wireless emitter activity from 25 MHz to 6 GHz and this RF traffic is decoded, processed and sent to the Bastille 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 are based on Software Defined Radio (SDR) technology which allows them to receive in-place upgrades ensuring future protocol support and decoding.

Concentrator

The Bastille Concentrator receives data from all of the sensor arrays in a facility, refines and consolidates the data into events, and sends them to the Fusion Center. The Premium Concentrator is used to gather additional data from cellular device transmissions.

Fusion Center

Bastille's Fusion Center platform is the only NIAP certified product in this market and provides you 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. Any detected wireless device is clearly overlayed on your facility floor plan, including current device location to within 3m accuracy and a playback capability to show the historical location of each wireless device as it moved through your space. This playback functionality allows correlation with other systems to determine who brought the device in, along with 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.

Common Criteria

Bastille is the only NIAP Compliant Cellular Intrusion Detection Product

Intelligent Wireless Security For Classified Areas

Examples of Bastille's Differentiation

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

Threat Signatures & Event Intelligence

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

Individual Cellular Device Detection

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

Advanced Bluetooth Device Detection

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

Device Location plotted on your floor plan

To find out how Bastille can detect Wireless Threats in your Classified Areas, visit **bastille.net**

Follow us on Twitter **@bastillenet** and on **LinkedIn**.

INFO@BASTILLE.NET
800.530.3341

Bastille
Wireless Threat Intelligence