Bastille

EXECUTIVE SOLUTION BRIEF

# Wireless Airspace Defense

# Wireless Dangers to the Connected Enterprise

In today's connected environments, wireless threats pose an invisible risk to organizations across various sectors. Comprehensive wireless security is more critical than ever, from corporate data centers and cloud infrastructure to classified areas. Wireless devices, often unmonitored, can serve as gateways for data breaches, eavesdropping, and unauthorized access.

Wireless security presents unique challenges, as traditional measures primarily focus on wired networks and physical threats. However, the rapidly expanding use of wireless technologies such as Wi-Fi, Bluetooth, and cellular devices leaves organizations vulnerable to threats that conventional security tools cannot detect.

The proliferation of IoT devices, wearables, and personal electronics further complicates this landscape. Devices like the USB Ninja Cable and O.MG Cable™ can exfiltrate sensitive data over wireless connections, while compromised personal devices may unknowingly introduce risks to high-security environments. Wireless threats often involve rogue Wi-Fi access points, Bluetooth-based data harvesting tools, cellular jammers, or hidden surveillance equipment.

These threats are hazardous because they can bypass traditional security protocols. In many cases, they operate out-of-band, making them difficult to detect and allowing attackers to exfiltrate data or disrupt operations without alerting security teams.

# 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 enterprise has no unknown threats.

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

- Rogue Wi-Fi access points and data ex-fil devices
- Rogue video and still-image cameras
- Bluetooth-based data harvesting devices
- Cellular voice, data, and video ex-fil devices, which can bridge physical networks
- 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.

# Threats are Camouflaged

Advanced data exfiltration threat devices often resemble cables and components typically present in your facility. The only way to identify an actual threat is to monitor the wireless spectrum for transmissions that violate the security policy.

Physical inspection will not identify these threats.

EXAMPLE

## USB Ninja Cable

The USB Ninja Cable hacking tool looks like a standard vendor-issued cable. However, it includes a miniature computer, controllable by Bluetooth, which can gather and exfiltrate all the data it sees, including logging keystrokes. These cables are undetectable unless you are scanning for wireless activity.  The USB Ninja cable, and many others like it, are broadly available online and cost less than one hundred dollars. For an extra $50, you can buy the wireless trigger device for the USB Ninja, which can trigger two different payloads from hundreds of yards away via toggle buttons!  Multiple customers have found USB Ninja cables using Bastille in the last year.

Here's a video about the USB Ninja Cable: https://www.youtube.com/watch?v=UhBK-M2iXwA

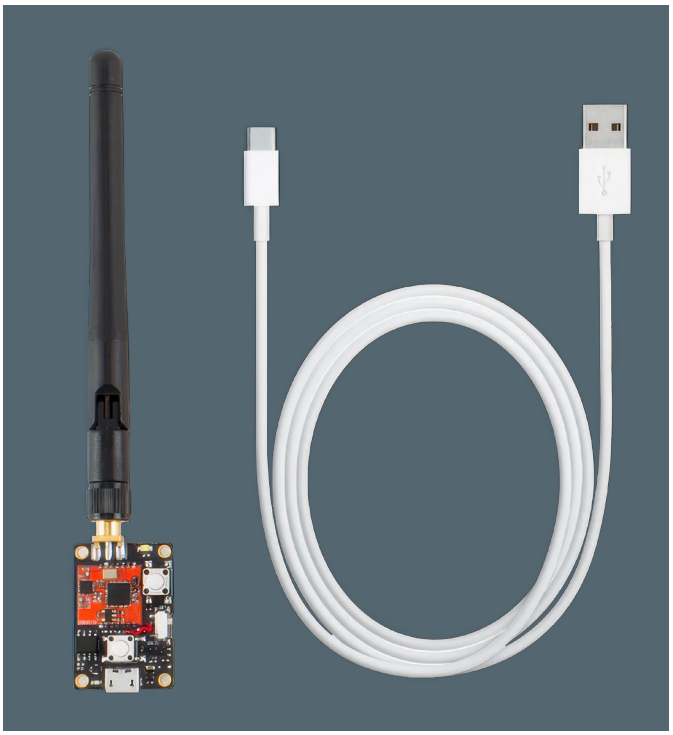

**Figure 1:** USB Ninja Bluetooth Remote and Cable

EXAMPLE

## The O.MG Cable™

The O.MG Cable hacking tool looks precisely like standard vendor-issued cables. It includes a miniature computer, controllable by Wi-Fi, that can gather and exfiltrate all the data that it sees, including logging keystrokes. These cables are undetectable unless you are scanning for wireless activity. Like many others, they are broadly available online and cost around one hundred dollars. Multiple customers have reported finding O.MG Cables using Bastille's solution.

Thousands of inexpensive devices are available online, and sophisticated adversaries build their own. And let's not forget cell phones, laptops, and other everyday devices that are compromised, misconfigured, or left for nefarious purposes.

## Threats are Often Unintentional

Wireless technology has proven to be a boon for convenience and adaptability in all aspects of the modern world. This convenience creates additional vectors for malicious use and requires continuous monitoring to detect threats immediately.

EXAMPLE

## Dell Quick Sync

Dell Technologies has implemented Bluetooth Low Energy (BLE) and Wi-Fi capabilities into their Quick-Sync 2 remote server management cards. This capability enables users to access system management functions while in range of the server after going through a few configuration steps, which only require being physically near the server. While convenient, this functionality may allow unauthorized persons to link to and modify server configurations to impact availability or exfiltrate system data if improperly configured or not fully updated.

# Intelligent Wireless Threat Security

An improved approach to cloud infrastructure security is required to detect these wireless threats and enable a modern security policy. 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 cloud infrastructure locations. 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 sensor arrays throughout the monitored facility. Bastille sensor arrays detect wireless emitter activity from 25 MHz to 6 GHz. Bastille decodes, processes, and sends this RF traffic to the Concentrator for further event correlation. The sensor arrays are 100% passive, meaning they never transmit, are plenum-rated, are available for indoor and outdoor use, and Bastille manufactures them 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.

# 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.

**Figure 2:** Sensor Arrays

# 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. Fusion Center overlays any detected wireless device clearly on your facility floor plan, including 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.

# Use Cases

The Bastille solution is essential for organizations with diverse security needs.

In cloud infrastructure environments, where physical security is highly developed, wireless threats can still bypass perimeter defenses and compromise sensitive systems. Bastille's solution provides the visibility to detect unauthorized devices that could threaten cloud-based data and infrastructure.

In classified areas and SCIFs, where even a single compromised device can lead to significant data breaches, Bastille ensures continuous monitoring to detect and neutralize any wireless threats before they can cause harm.

For organizations focused on technical surveillance countermeasures (TSCM), Bastille's continuous monitoring of RF activity detects unauthorized listening devices and surveillance equipment, providing actionable intelligence to thwart espionage efforts.

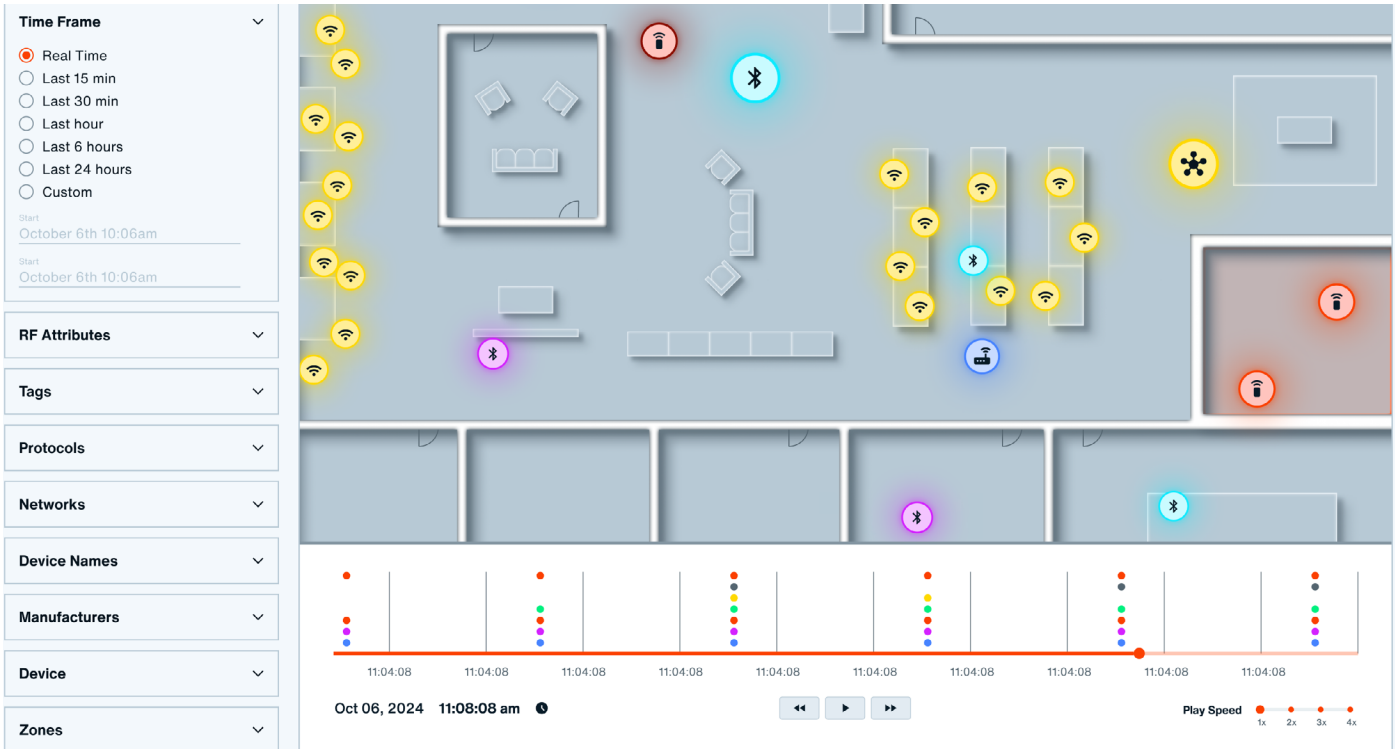


**Figure 3:** Bastille's Solution for Cloud Infrastructure Wireless Security

# Examples of Bastille's Differentiation

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

**EXAMPLE**

## Threat Signatures & Event Intelligence

Bastille's Threat Signatures filter through all detected devices and categorize them so you can focus your resources on 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 devices and assess their threat posture while maintaining visibility to approved devices used by your personnel.

**EXAMPLE**

## Advanced Bluetooth Device Detection

Bastille's unique approach simultaneously monitors all 79 Bluetooth and 40 Bluetooth Low Energy channels. This approach identifies Bluetooth-paired devices, explicitly noting the paired network endpoints, attributes of both ends of the pairing, and Bluetooth devices performing inquiries or scans. Other vendors only show when Bluetooth devices are looking to pair; after they've paired, they become invisible. A paired device can exfiltrate data and cause disruption; you need this visibility to protect against Bluetooth surveillance threats.

**EXAMPLE**

## Individual Cellular Device Detection

Bastille provides comprehensive data on all 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 while adhering to data privacy concerns.

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