

Bastille

EXECUTIVE SOLUTION BRIEF

Data Centers Wireless Airspace Cybersecurity



Wireless Threats Pierce Even the Most Secure Data Centers

In today's data-driven environments, enterprises depend on storage infrastructure, whether enterprise data centers, co-location facilities, hosting environments, network exchanges, or SaaS platforms. Securing data center infrastructure from both physical and wireless threats is crucial.

The industry has spent billions to make data centers among the most physically secure locations on the planet. Data center infrastructure features well-refined physical security measures, including identity scanners, physical barriers, trained guards, motion detectors, and comprehensive camera systems. Physical security focuses on tangible threats, but wireless threats don't care about guards and gates. Attackers can use Wi-Fi, cellular, Bluetooth, and other protocols to control systems inside a data center from beyond the perimeter fence or exfiltrate data, voice, and video.

Modern data centers should implement Wireless Airspace Cybersecurity solutions, such as Bastille, to detect and mitigate these threats.

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 undetectable in 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 wireless threat activity to confirm your data center is free of 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

Any of these threats can impact system stability, deny access to or steal data from applications, or compromise the integrity of the data center infrastructure.

Threats Are Camouflaged

Advanced data-exfiltration threat devices often resemble cables and components commonly found 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 via Bluetooth, that can gather and exfiltrate all data it sees, including keystroke logging. These cables are undetectable unless you are scanning for wireless activity. The USB Ninja cable, and many others like it, are widely available online and cost less than \$100. 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>

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.



Figure 1: USB Ninja Bluetooth Remote and Cable

Threats Are Often Unintentional

Wireless technology has proven a boon for convenience and adaptability across 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 its Quick-Sync 2 remote server management cards. This capability enables users to access system management functions while within range of the server after completing a few configuration steps that require only physical proximity to the server. While convenient, this functionality may allow unauthorized persons to access and modify server configurations, impacting availability or exfiltrating system data if improperly configured or not fully updated.

Intelligent Wireless Threat Security

An improved approach covering data center 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 of wireless threats across data center infrastructure. 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 enables in-place upgrades and future protocol support and decoding.



Figure 2: Sensor Arrays

Concentrator

The Bastille Concentrator receives data from a facility's sensor arrays, refines and consolidates it into events, and sends the events 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. The Fusion Center receives wireless data from the Concentrator(s), compiles and analyzes it, 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 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 enables correlation with other systems to determine who brought the device in, 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, including the sensor arrays, for the life of the subscription.

Bastille's Differentiation

Bastille has 35 wireless detection patents 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 into your security policy, enabling you to evolve it 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.

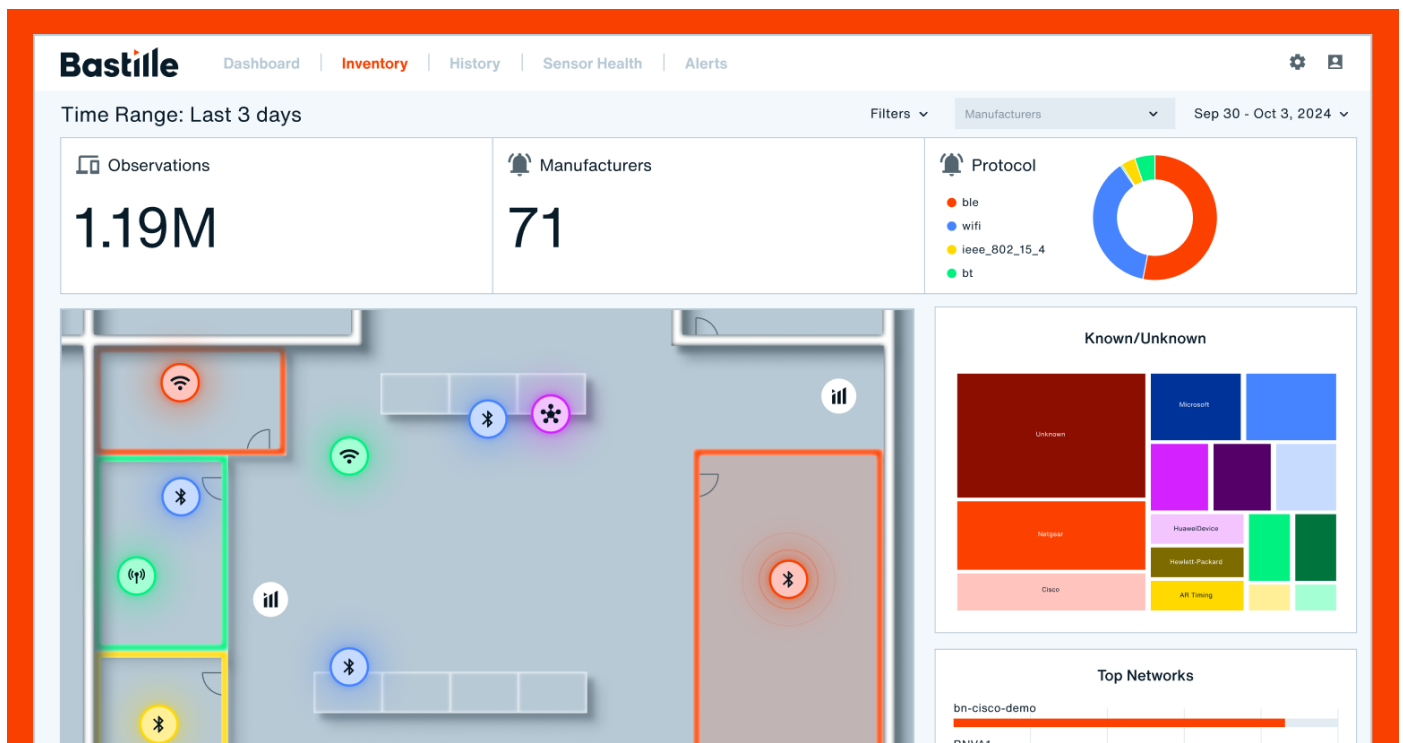


Figure 3: Bastille's Solution for Cloud Infrastructure Wireless Security

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 detect 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 ensuring data privacy.

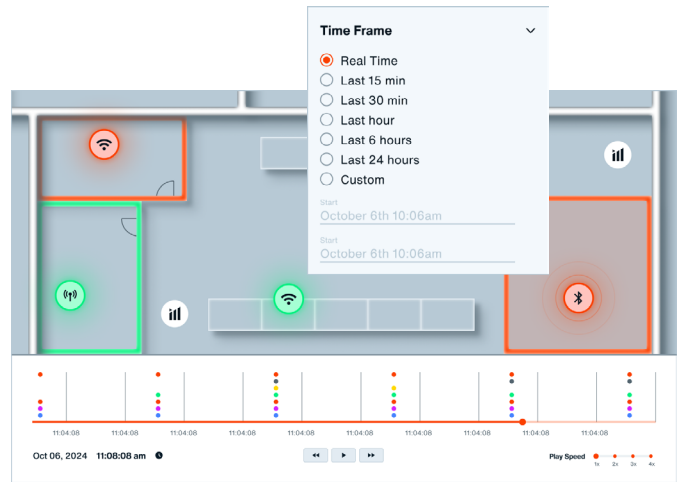


Figure 4: Device locations plotted on your floor plan

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

