Bastille

Wireless Threat Intelligence

EXECUTIVE SOLUTION BRIEF

Cloud Infrastructure Wireless Security

BASTILLE.NET

Wireless Threats Pierce Even the Most Secure Data Centers

Every application has a dependency on infrastructure in today’s cloud environments. “The Cloud” has evolved into a superset of enterprise data-centers, co-location facilities, hosting environments, network exchanges, and SaaS platforms. Securing cloud infrastructure from both physical and wireless threats is crucial.

To protect these assets, the industry has spent billions to make data centers amongst the most physically secure locations on the planet. Physical security of Cloud Infrastructure 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; however, wireless threats don't care about guards and gates. Wi-Fi, Cellular, Bluetooth and other protocols can be used to take control of systems inside a data center from beyond the perimeter fence, or to exfiltrate data, voice and video.

Modern data center locations which drive today’s Cloud Infrastructure need their security to be enhanced to encompass Wireless Security for Cloud Infrastructure to detect and mitigate all threats.

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 the physical network. To ensure your data center is free of unknown wireless threats; you must continuously scan for wireless threat activity.

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

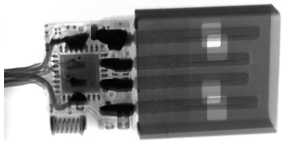
Any one of these threats can impact system stability, deny access to or steal data from applications, or compromise the integrity of the cloud infrastructure.

Threats Are Camouflaged

Advanced data exfiltration threat devices are often designed to look like cables and components that are normally present in your facility; the only way to know if a true threat is present is to monitor the wireless spectrum for transmissions that violate security policy.

Physical inspection will not identify these threats.

EXAMPLE: The O.MG Cable™



The O.MG Cable is a hacking tool which is designed to look exactly like common vendor-issued cables, but includes a miniature computer and Wi-Fi network interface. The O.MG Cable enables a hacker to insert payloads into the target computer, remotely trigger payload delivery, perform keystroke logging, and establish Wi-Fi connectivity for command & control as well as data exfiltration.

These cables are physically identical and undetectable unless you are continuously monitoring for wireless activity.

The O.MG Cable, and many others like them, are broadly available online and cost around one hundred dollars. Multiple customers have reported finding O.MG Cables using Bastille’s solution.

Threats Are Often Unintentional

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

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 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, if improperly configured or not fully updated, may allow unauthorized persons to link to and modify server configurations to impact availability or exfiltrate system data.

Intelligent Wireless Threat Security

To detect these wireless threats and enable a modern security policy, an improved approach to cloud infrastructure security is required. 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 cloud infrastructure locations. 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.

Sensor Arrays

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.

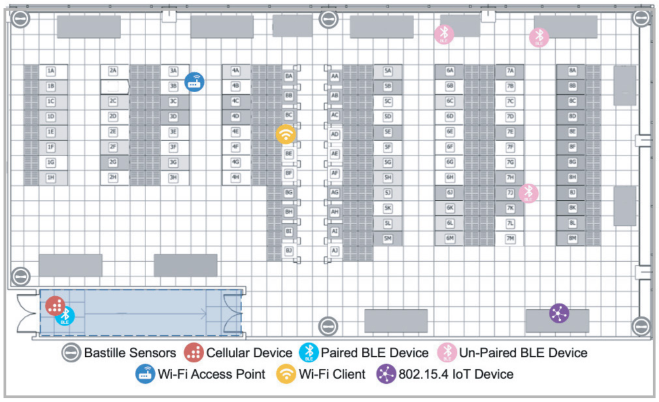
Concentrator

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.



Bastille's Solution for Cloud Infrastructure Wireless Security

Cloud Infrastructure Wireless Security

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 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.

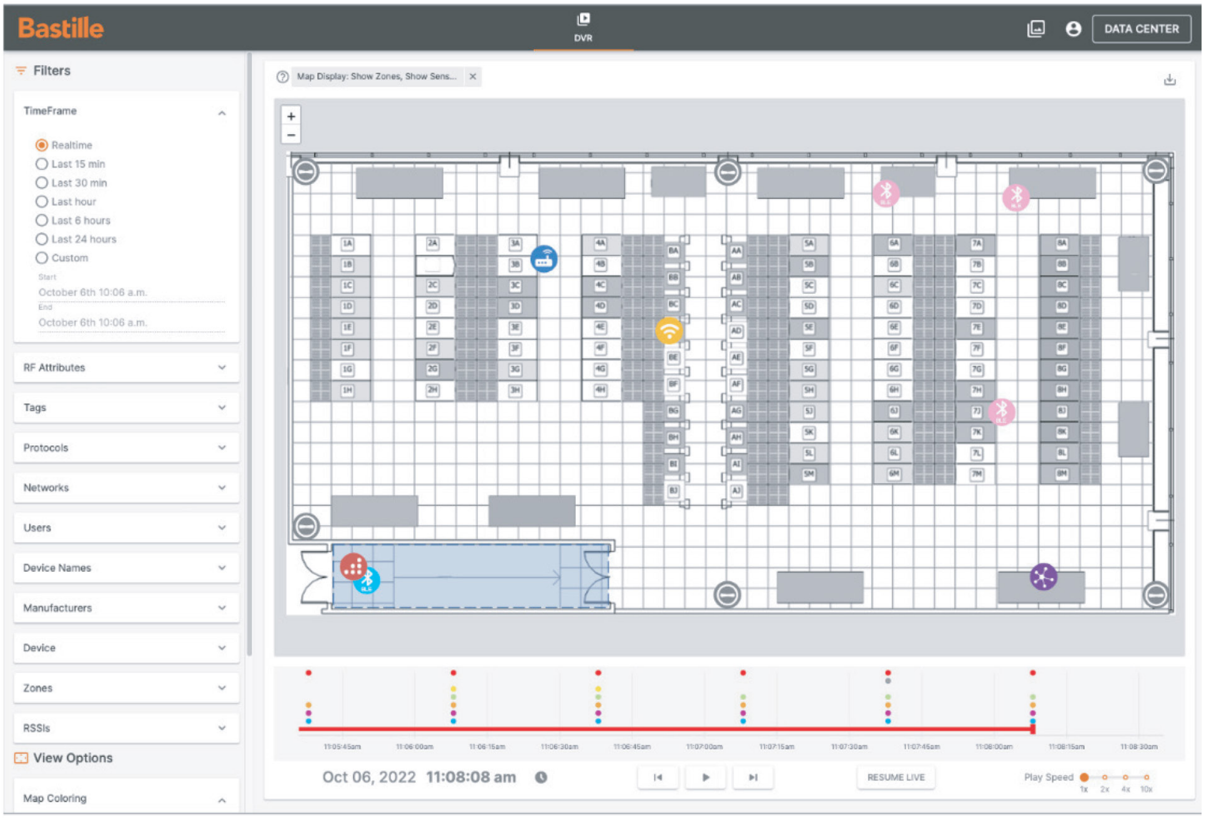
Bastille's comprehensive categorization capabilities allow you to rapidly detect new RF emitters and assess their threat posture while maintaining visibility to approved devices such as cellphones, bluetooth devices, and Wi-Fi clients used by your personnel.

Advanced Bluetooth Device Detection

Bastille's unique approach simultaneously monitors all 79 Bluetooth channels 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. 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 surveillance threats.

Individual Cellular Device Detection

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



● Realtime
○ Last 15 min
○ Last 30 min
○ Last hour
○ Last 6 hours
○ Last 24 hours
○ Custom

Start
October 6th 10:06 a.m.
End
October 6th 10:06 a.m.

Oct 06, 2022 11:08:08 am

Device locations plotted on your floor plan

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

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

INFO@BASTILLE.NET
800.530.3341

Bastille
Wireless Threat Intelligence