Bastille

PRODUCT BRIEF

Cellular & RF Based Threat Detection, Location and Alerting for the Enterprise

Cellular & RF Threat Remediation

Discover: Detect and Locate

The core and multi-patented technology of our sensor arrays and analytics continuously scans your airspace and detect wireless emitters, digitally demodulate those signals, identify protocols and individual unique devices. This allows Bastille to put an accurate dot on a floor plan map of your facility to show the location of each individual device.

Analyze: Classify and Alert

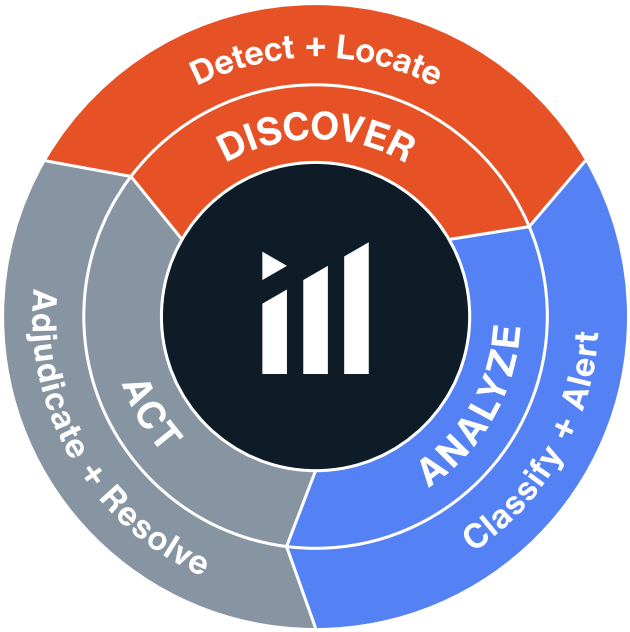
Bastille provides context information about the devices it locates. This allows you to tell whether the device that is represented by the dot is connected with other devices, what kind of data it is streaming, or if it's being actively attacked in certain cases. Rule-based alerts can be established that interact with your incident response workflow. Using integrations, Bastille alerts can be used to send emails, text message, phone calls, or to instantiate tickets in an external incident response system like PagerDuty, ServiceNow, or Lenel OnGuard.

Act: Adjudicate and Resolve

You can undertake various levels of investigation. For example, if you click through a Bluetooth device, Bastille might be able to tell you that it's a Sony device and give you a model number that corresponds to a television. With that information, you might infer that somebody has just put a television in your space and it has an active Bluetooth connection. From there, you may choose to physically intervene to remove the device, or decide to use one of the Bastille integrations to your other network systems to disable the device automatically.

Similarly, you can use Bastille's DVR feature to go back in time and see a given device's presence and location history. Through this forensic analysis, it may become clear that the device has been in or near restricted areas, or that the device has been present during off-business hours in a way that is indicative of involvement in a malicious event.

Continuous Enterprise Monitoring



Bastille allows you to accurately **discover** devices, **analyze** if a certain device is permitted in an area and if it presents a threat, then **act** to resolve the incident and record the actions taken.

Bastille Finds Real World RF & Cellular Threats in Real Time

Bastille provides corporations and agencies the ability to discover, locate, and mitigate radio borne threats to their assets, facilities and networks. These threats arise from managed, unmanaged and rogue wireless, IoT and Cellular devices. Bastille does this protection by using Software Defined Radios (SDRs) to passively observe the entire radio space in a facility from 60 MHz to 6GHz. More than 70% of devices connected to the network today are connected via RF & Cellular and that percentage is growing. Equally important are the radio-enabled and cellular devices in your facility which are NOT connected to your network; those which enter daily with employees and visitors, and those installed by contractors into your buildings. These devices are the ones which can be used to exfiltrate voice, video, and computer data right past your firewalls and into the unsecure world outside.

Example: A laptop legitimately connected to your network right now could also be tethered to a cell phone via Bluetooth and that cellphone can be connected via a 40 Mbps 4G Cellular data connection to a server in China which is capturing your company secrets in real time

Covert, rogue and vulnerable wireless and cellular devices are inside your enterprise today. Suspicious equipment includes SmartTVs, security cameras, printers and peripherals, medical devices, building controls and of course, cell phones.

Only Bastille can deliver:

- **Complete Visibility:** Detect all the wireless/cellular devices and connections in your facilities whether or not they have connected to your network
- **Threat Detection:** Detect that a device such as one with a Bluetooth or cellular connection is transmitting data (and is not just an employee listening to music)
- **Accurate Threat Location:** Locate both offending devices on your floor plan.

The whole Bastille threat detection process takes just seconds from when the wireless/cellular device first transmits until your Security team receives an Alert in your existing alerting system.

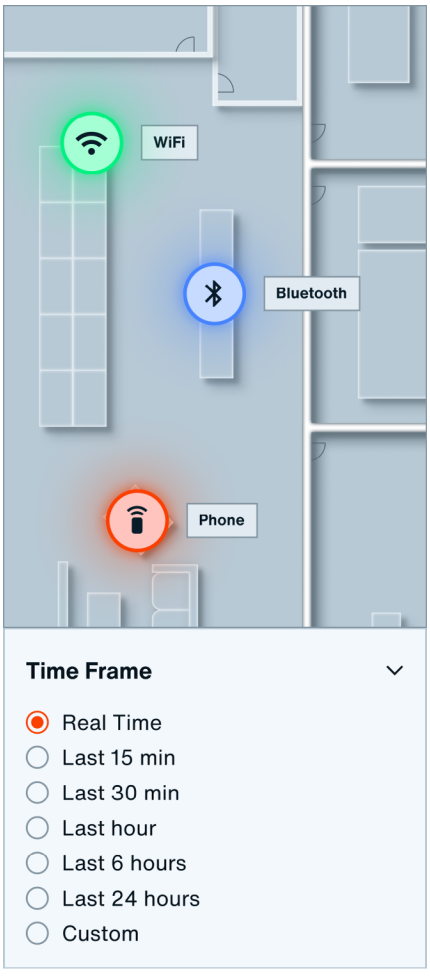


Figure 1: Bastille UI shows the office floor plan with location of Cellular, Wi-Fi and Bluetooth devices

Comprehensive Device & Network Visibility

Government Only Technology Now Available for Enterprise

Bastille has been doing RF and Cellular Intrusion Detection and research for the Government for years. Only in 2020 did Bastille finally receive FCC approval for its Civilian cellular sensor array. This allows Bastille for the first time to offer accurate Cellular Intrusion Detection to the Enterprise. Now corporations can have the RF security that the DoD and Intelligence Community rely on to protect the nation's secrets.

A lot more than Cellular Intrusion Detection

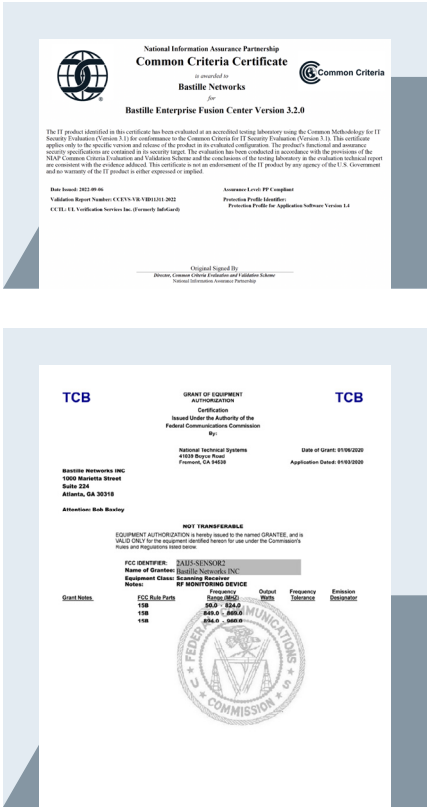
Though commonly thought of as Cellular Intrusion Detection, Bastille does a lot more than merely detecting the presence of cell phones. Customers can set up alerts based on wireless device behavior. Examples include:

- **Compromised Devices:** Bastille baselines facilities, all wireless devices (including Cellular, Wi-Fi, Bluetooth and BLE) and their typical behavior and can alert when a device is compromised and exhibits abnormal behavior
- **Secure Area Data Breaches:** Alert when an allowed Bluetooth hearing aid performs an unallowed BLE pairing with a device outside the secure area. Or detect when a Company phone at a desk is joined by a personal phone at the same desk.
- **MDM Enhancement:** Alert when a phone which is not under Mobile Device Management is turned on
- **Insider Threats:** Alert when a device is seen in an area where it is not allowed, or forensically investigate to understand the devices and their behavior from weeks or months ago

> We are excited to see the final development of Bastille's technology to provide security by monitoring the RF and cellular spectrum.

Anil John

SVIP Technical Director, U.S. Department of Homeland Security Press Release


National Information Assurance Partnership

Common Criteria Certificate

is awarded to

Bastille Networks

for

Bastille Enterprise Fusion Center Version 3.2.0

TCB

GRANT OF EQUIPMENT AUTHORIZATION

Certification

Issued Under the Authority of the Federal Communications Commission

By:

TCB

Bastille Networks INC

1000 Marietta Street

Suite 224

Atlanta, GA 30318

Attention: Bob Bouley

NOT TRANSFERABLE

EQUIPMENT AUTHORIZATION is hereby issued to the named GRANTEE, and is VALID ONLY for the equipment identified hereon for use under the Commission's Rules and Regulations listed below.

FCC IDENTIFIER: 2AIJ5-SENSOR2

Name of Grantee: Bastille Networks INC

Equipment Class: Scanning Receiver

Notes: RF MONITORING DEVICE

Grant Notes	FCC Rule Parts	Frequency Range (MHz)	Output Watts	Frequency Tolerance	Emission Designator
	15B	50.0 - 824.0			
	15B	849.0 - 869.0			
	15B	894.0 - 960.0			

Figure 2: 100% Passive-Only FCC Certification

Bastille Enterprise Capabilities

The basic Bastille Enterprise set up provides real-time visibility and situational awareness into the Big 4 protocols operating in your facility: Cellular, Bluetooth, Bluetooth Low Energy, and Wi-Fi.

Bastille's Intelligence Community customers tell us that even Nation States are now using these common protocols for spying. There are so many of these signals bouncing around even your most secure areas that it's easy for spy radios to hide in the traffic. However, not with Bastille. Bastille locates every radio emitter in your facility and determines what devices each is connected to, whether on your network or going around your network. This includes the detection of live Bluetooth paired devices, and not just devices attempting to establish a Bluetooth connection.

As an organization, you want to protect your Company secrets from competitors, from criminals and from technical espionage by foreign governments. You have spent a fortune locking down the 200 Mbps of traffic going in and out of your facilities over your internet connections. Isn't it time to start watching the 5 Gbps which are leaving your facilities over unmonitored and unchecked radio waves?

Bastille's Patented Software-Defined Radio (SDR) Technology

Bastille's software-defined sensor arrays scan from 60 MHz to 6 GHz. Within that range, Bastille has more than a dozen protocol decoders, including Cellular, Wi-Fi, Bluetooth, Bluetooth Low Energy (BLE), ZigBee, DECT and others. Using software-defined radios we see all the emitters distinctly, and then by using protocol decoders in the arrays we digitally demodulate the protocols.

Bluetooth's Inherent Security Issues

Bluetooth flaw in native security can subject a user to threat vectors: default configuration, theft and loss, eavesdropping and impersonation, person-in-the-middle attack, piconet/ service mapping, and denial-of service attacks.

SANS

Hackers show off long-distance Wi-Fi radio proxy at DEF CON

The device uses the 900MHz band, but hides the data in the background radio noise.

PC World

Researchers Find Major Security Flaw with ZigBee Smart Home Devices

By making it easier to have smart home devices talk to each other, many companies also open up a major vulnerability with ZigBee that could allow hackers to control your smart devices.

Engadget

Protocol Demodulation and Dots-on-a-map

For example, BLE, Bluetooth and Wi-Fi are in the 2.4 GHz band. But we are not just looking for power signals in the 2.4GHz band, as some other companies do. Instead Bastille demodulates the BLE, Bluetooth, and Wi-Fi protocols, and decodes the unencrypted header packets. Bastille does not decode encrypted data payload but we do see the header packets and from this can associate all the emissions with this specific BLE, Bluetooth or Wi-Fi device, allowing us to put a protocol specific dot on the map.

This is in contrast to other companies that are not doing digital demodulation, but instead are only looking for energy in the RF spectrum. By only looking for energy in a certain spectral band, it is impossible for these competing products to differentiate multiple co-located devices that are transmitting at the same time. The best they can do is to provide heatmaps of activity that do not differentiate devices and have very coarse time resolution (seconds instead of microseconds). By demodulating each packet, Bastille is able to differentiate devices, and even emissions, to provide device-level visibility.

Futureproof Solution with Software Defined Radio

The benefit of using Software Defined Radio is that it future proofs deployments. If new protocols are released or existing protocols evolve, a firmware upgrade to the Bastille sensors is all that is needed to gain visibility of the devices using the new/evolved protocol.

Figure 3: Bastille's sensor array, which is now in its fourth generation, is entirely passive (does not emit any radio signals) and was designed and built in the USA.

Differentiated & Patented Technology

Advanced Cellular, Wi-Fi, Bluetooth and Bluetooth Low Energy (BLE) Network and Device Detection

The focus for most customers is obtaining visibility into devices using the Big Four protocols: Cellular, Wi-Fi, Bluetooth and Bluetooth Low Energy. Bastille detects and locates them all of the time. Other vendors cannot detect cellular at all or can only detect cellular when the phone sends a RACH to rejoin the network. Bastille tracks every transmission in cellular frequencies to give you the most up to date location.

Other vendors claim “Bluetooth detection” but they are actually only detecting Bluetooth Low Energy devices and they are only detecting them when the devices are in “advertising mode.” Once the BLE device finds a partner and pairs with it, those devices disappear from the competitors’ screens. Only Bastille continues to locate both ends of the BLE device throughout the connection.

Bastille’s Accurate Cellular and RF Device Location

Core to the Bastille solution is the accurate localization of cell phones and other RF emitters within the area under observation. Previous generations of solutions based on spectrum analyzer approaches or basic SDRs with limited analytics have only been able to present clouds of cellular energy which may contain one or ten devices, one meter or ten meters away.

Bastille’s breakthrough and patented work provides Bastille the ability to disambiguate multiple cell phones and accurately locate those individual devices in real-time.

Bastille US Patents		
9485266: Security measures based on signal strengths of radio frequency signals	**9625564:** Blind signal classification and demodulation in a multimodal radio frequency environment	**9945928:** Computational signal processing architectures for electromagnetic signature analysis
9485267: Anomalous behavior detection using radio frequency fingerprints and access credentials	**9635044:** Electromagnetic Persona Generation Based on Radio Frequency Fingerprints	**10104098:** Electromagnetic threat detection and mitigation in the internet of things
9551781: Efficient localization of transmitters within complex electromagnetic environments	**9736175:** Anomalous Behavior Detection Based on Behavioral Signatures	**10122736:** Ground And Air Vehicle Electromagnetic Signature Detection And Localization
9560060: Cross-modality electromagnetic signature analysis for radio frequency persona identification	**9739868:** Electromagnetic signature analysis for threat detection in a wireless environment of embedded computing devices	**10338191:** Sensor Mesh And Signal Transmission Architectures For Electromagnetic Signature Analysis
9591013: Radio frequency fingerprint detection	**9880256:** Diverse Radio Frequency Signature, Video, and Image Sensing for Detection and Localization	**10473749:** Localization Of Mobile High-speed Wireless User Equipment From Uplink Channels

Cellular Localization: Heatmaps versus Dots

Bastille conducts a real-time emitter differentiation of all cellular emitters, which contributes to our industry-leading LTE localization performance. This is in contrast to others that can only provide a “mist” or heatmap of LTE energy. Heatmaps of RF energy require a sophisticated signals intelligence operator to determine if there is one phone or 10 in a space, do not provide actionable deterministic alerts, and do not provide the discrete position estimate for each LTE emitter in the space.

Industry Leading Bluetooth and BLE Device Location

Bastille is the only solution to detect both Bluetooth and Bluetooth Low Energy as distinct device protocols and then to show which of these devices are paired with each other. Bastille has several patents issued and pending for visibility into these protocols covering what kinds of data those protocols are communicating and what kinds of network connections they have.

Bluetooth uses 79 channels, at 1 MHz wide each, Bluetooth Low Energy uses 40 channels that are 2 MHz wide each, and they have very different characteristics. When your phone goes into Bluetooth ready-to-pair mode, it starts transmitting on an advertising channel, and in that state, it’s meant to be highly visible. Even your laptop could pick up that kind of transmission. However, when the Bluetooth device enters a piconet, i.e. pairs with another device, it starts using the data channels and it stops using advertising channels. If you are relying on a less sophisticated or older generation sensor solution, it probably uses a hardware Bluetooth decoder that can only see one channel at a time, and will not see all the data traffic for that Bluetooth device.

This means that with other solutions, once a Bluetooth or a Bluetooth Low Energy device enters into a network with other devices, it becomes invisible to them because it stops transmitting on the advertising channel. This is exactly when you don’t want them to be invisible! Bastille’s proprietary SDRs see all the channels all the time, and understand which devices, such as wrist worn fitness devices and phones, are communicating with each other. Bastille puts a dot on a map for all the Bluetooth and Bluetooth Low Energy devices in your space.

If you want to understand where ALL Bluetooth devices are, what they are connected to and how active they are, then Bastille has the only solution.

Bluetooth and BLE Based Voice and Data Exfiltration

Bastille not only shows device location, but also network state connection. This is important because if you have a facility where you allow a health monitoring wristband or watch into the secured area, but not cell phones, you expect that all cell phones are left outside or turned off and placed in a locker at the door. However, if the cell phone is not powered down, the connection between the phone and the fitness device can still be active. Since Bluetooth connections can persist for over 300 feet, you can have a live data connection from a secure area to an unsecured cell phone outside the secure area. Bastille can detect that happening, and can detect the difference between a connected device and unconnected device and give you an alert that you can adjudicate.

Figure 4: Bastille UI screenshot showing accurate real time location on a floor plan of cellular, Wi-Fi and Bluetooth devices

Seamless Integration with Your Existing Security Infrastructure

Integrates with Existing Cyber and Physical Security Infrastructure

Bastille ties into your existing infrastructure such as Security Information and Event Management (SIEM) systems such as Splunk, Wireless Access Points (APs) such as those from Aruba, Cisco Meraki or Fortinet, MDM systems like VMware, MobileIron or IBM, plus offers integration with physical security products such as Point Tilt Zoom (PTZ) Security Cameras and Access Management Control Systems line LENEL OnGuard.

APIs and Extensibility

Bastille's APIs are designed to allow for integration with the entire constellation of existing tools and systems that exist in your enterprise.

Authentication for Automatic Adjudication

Bastille has API integrations that interface with a variety of network access systems including systems by Cisco/Meraki, Aruba and MDM vendors like VMware and MobileIron. With these integrations, Bastille users can ingest the list of authenticated on-network devices that are allowed in their facility. These devices get tagged in Bastille's system so that if you wish, they can be auto-adjudicated thereby automating your device adjudication workflows.

Network Access Control

For devices that breach a geofence or otherwise subvert the facility's security policy, Bastille provides integrations to network access control (NAC) systems such that the device can be removed from the network.

Integrations

aruba

ArcSight

AXIS COMMUNICATIONS

cisco

FORTINET

Genetec

mobileiron

OnGuard

PagerDuty

paloalto NETWORKS

splunk>

vmware

MDM Enhancement

Devices that violate location policy and are managed by MDM or UEM, can be automatically turned off or otherwise disabled using rules in Bastille's system.

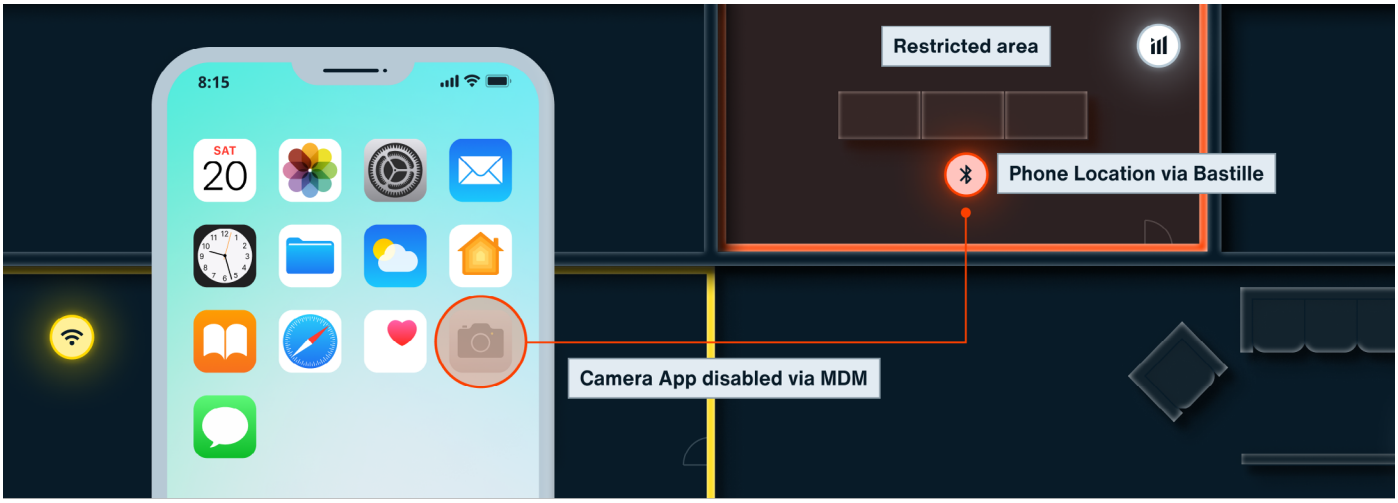


Figure 5: Bastille's MDM integration enables device location to be sent back to the MDM to trigger rules such as "Disable the cell phone camera when the phone is in a restricted area"

Unified Management and Data Aggregation

SIEMs like Splunk are excellent for viewing aggregate data and offer sophisticated rules engines tied into your other sources of data. Using our Splunk API Integration you can push your Bastille data to your Splunk instance, supply your Splunk rules, run Splunk alerting and Splunk aggregate analysis. If Splunk is your source of record for all your security systems, then by having Bastille data in Splunk using the Splunk Bastille App, you can do correlations across other systems.

We support campus wide and worldwide deployments back to one central location, so you can do worldwide management and alerting of all your systems.

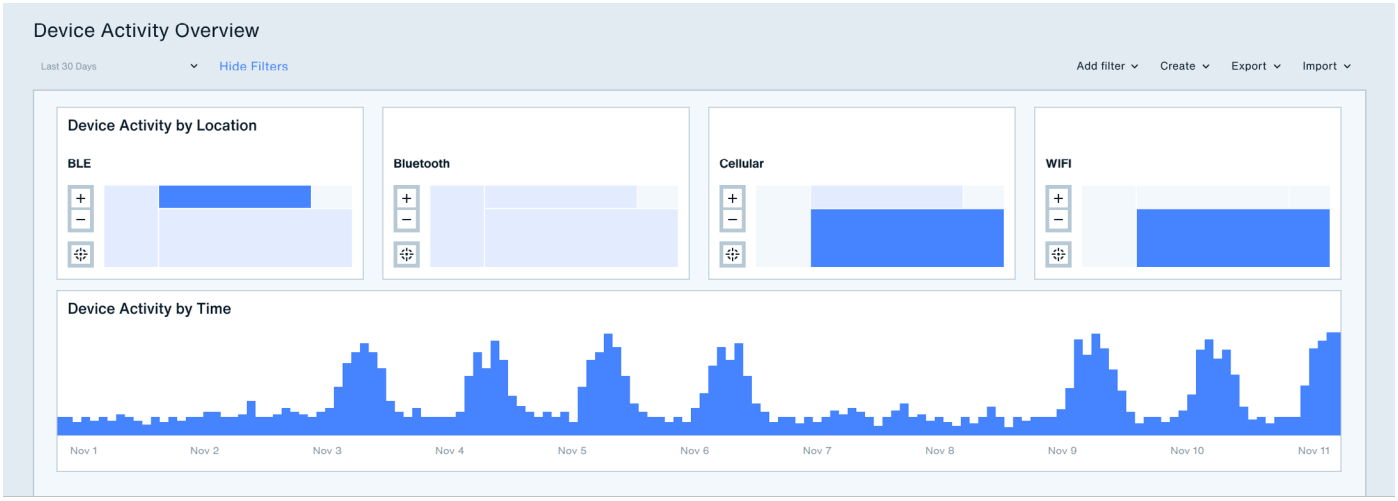


Figure 6: Bastille's Splunk App allows you to ingest data from Bastille, correlating with additional network data and applying analytics and rulesets from Splunk

Adjudication Workflow

To maintain security in a facility, you must establish the baseline of which devices are allowed in the facility. Then, as devices come and go from a facility, they need to be adjudicated to maintain the security of the space.

Bastille offers a streamlined workflow to keep track of which devices are allowed in your environment and how you keep your environment pristine from disallowed or unauthorized devices.

Bastille Enterprise Architecture

The Bastille architecture can be deployed 100% on premise or include cloud components if preferred.

Customer Site

Figure 7: Bastille's Sensors Arrays & Concentrators

Customer Site, Private Customer Cloud, Secure AWS or GovCloud

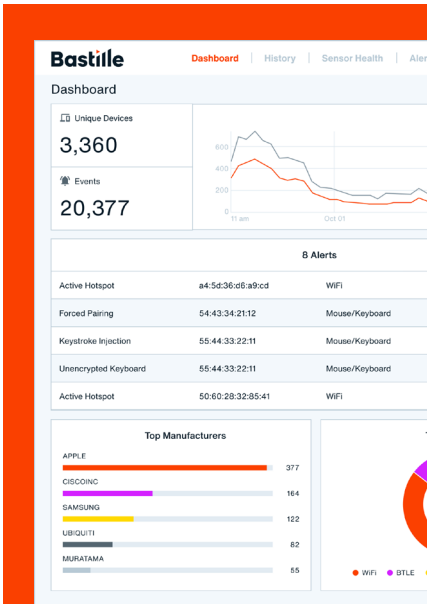


Figure 8: Bastille's Fusion Center (Analytics / Machine Learning)

Integrations

Figure 9: Bastille's Integrations

Patented Cellular Intrusion Detection

Cellular Intrusion Detection

Cellular phones are a ubiquitous productivity tool, but they are also the most prolific security and compliance threat faced by organizations. Cell phones have cameras, recording devices, the ability to become out-of-network hotspots, and they can tether to laptops and computers in the building for data-exfiltration. Companies and government agencies can best protect themselves by monitoring both authorized and unauthorized phones that enter and move around their environments. This functionality can directly alert organizations to potential security threats and compliance issues in real time.

Cell phone location has been historically difficult because a comprehensive cell phone detection and location product must be able to discover a cell phone even when the Wi-Fi and Bluetooth are not active. After four years of intense R&D and more than a dozen patents, Bastille has created the solution.

Accurately Locate Cell Phones Inside Your Facility Using Just Their Cellular Signals

Other solutions claim to 'detect smartphones' when all they can do is detect Bluetooth and Wi-Fi signals, not cellular signals. Still other companies claim to detect cellular phones when all they can do is detect cellular energy. Those systems cannot tell the difference between one phone close to a sensor and 10 phones farther away. Bastille's Cellular Intrusion Detection is the first system which accurately detects, counts, and locates cellular devices inside your facility. Sure, we can track devices via Bluetooth and Wi-Fi like the other companies but the bad guys turn off those signals when they plan to do bad things. To know that your facility is locked down from unauthorized devices you need to detect and locate cellular signals.

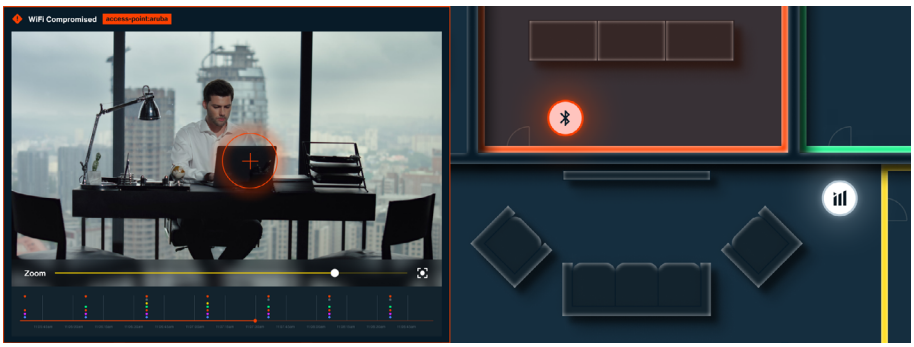


Figure 10: Bastille locates a cell phone in a geo-fenced area and triggers a 3rd party video camera

Cellular Intrusion Detection for Regulatory Compliance

- **Unauthorized cell phone detection:** Detecting when an unauthorized cell phone becomes active.
- **Insider threat:** Real time alerting and forensic "DVR" replay of cell phone locations.
- **Broker and Trading Compliance:** Monitor all cell phones for complete trade communications surveillance monitoring.
- **Secure Processing and Manufacturing:** Exclude Cell Phones from Facilities engaged in activities such as: Financial Services Lockbox Processing, Credit Card Manufacturing, Passport Application Processing.
- **Any place where cell phones are not allowed by contract:** Detect and remediate infractions. Keep an audit trail of Radio Events to prove that your firm is complying with the "no cell phone rule.

Cellular Intrusion Detection for Industrial Safety

- **Manufacturing and Logistics Cell Phone Policy Enforcement:** Enforce no cell phone policy inside a warehouse, at a machine, or on a vehicle.

Know What the Phone is Doing?

You want to know what those phones are doing. Does somebody sitting in the board meeting have an open cellular connection where he is streaming the entire meeting to an accomplice outside? The Chairman of the Board wants to know that right in the meeting and to know which seat that active phone is sitting in. Has someone brought his personal cell phone into a facility in “Off” mode and then secretly turned it on?

You need to be alerted that that happened and you want to know where that device is before the individual can use the device illicitly. Has someone forgotten she has a cell phone in her pocket and entered a “no cell phone” area? You need to be alerted and perhaps even have the right video camera highlight the intrusion so that you can see who made the error and then remind them to take their cell phone back outside.

Don’t Be Fooled by Misty Clouds of Cellular Energy

Distinguishing and locating individual cell phones, and placing an accurate dot on a map to show you exactly where a cell phone is right now, is a very hard problem. Technologies based on spectrum analyzers just alert you when they detect energy in a cellular frequency. They cannot distinguish between one phone being close to a sensor or 10 phones being farther away, resulting in false positives and wasted time.

Constant Cell Phone Monitoring

It’s not sufficient to spot a cell phone only when it is first turned on or taken out of airplane mode. For accurate location, you need to continuously monitor for cell phones, update their location and alert when they enter a restricted area.

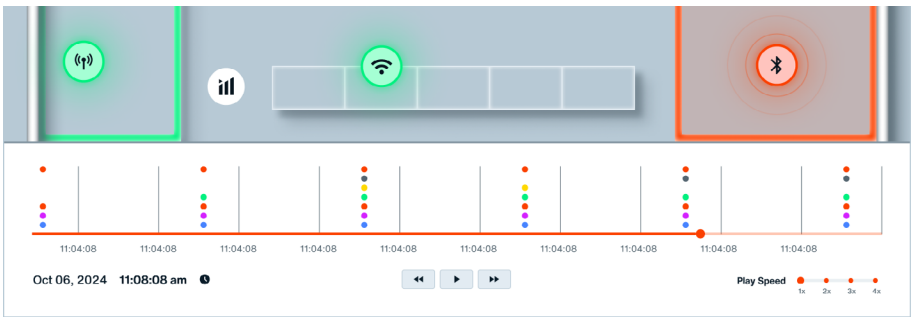


Figure 11: Bastille’s DVR functionality records historic cell phone, Wi-Fi and Bluetooth device location for forensic investigations

Cellular Intrusion Detection for Security (physical and information)

- **Secure area protection:** Detect and alert to cell phones in and around: C-Suite Meeting rooms, Government SCIFs.
- **Video camera surveillance enhancement:** Cue and Slew a camera to an individual target of interest in real time and alert. Use Outside the Frame Analytics to select and display a suspect on video.
- **Cellular intrusion alarm:** Alert when an unauthorized cell phone just entered a building or protected area inside or outside regular hours.
- **Visitor device monitoring:** Both authorized and unauthorized devices can be tracked without invading visitors’ privacy. Policies requiring visitors to leave cell phones outside a facility can now be enforced.

Top RF & IoT Vulnerabilities

Wireless Threat	Top Internet of Radios Vulnerabilities of 2019
Rogue Wi-Fi Hotspots (and Wi-Fi pineapples)	Can someone in your building by-pass all your Wireless Intrusion Detection Systems by opening a Wi-Fi hotspot which detours your data around your expensive Wi-Fi anomaly detection?
Wi-Fi Pineapples	Wi-Fi Pineapples can insert themselves into legitimate Wi-Fi networks, and can be used for Man-In-The-Middle attacks to sniff network traffic and steal credentials.
Bluetooth Data Exfiltration (tethering)	Bluetooth tethering can be used to pair a network device with a cellular data path (e.g. 4G LTE) which bypasses your traditional network security. How do you detect when someone starts Bluetooth tethering in your building? How do you avoid false alarms when the Bluetooth is only being used to connect a headset?
Eavesdropping / Surveillance Devices (e.g. conference room bugs)	Voice and motion-activated bugs cost as little as $20 on eBay.® These devices are getting smaller, yet with ever more sophisticated capabilities. They can exfiltrate voice and video across multiple radio bands, using FM, cellular and/or Wi-Fi.
Vulnerable Wireless Peripherals (mice/keyboards)	Low-end wireless keyboards, even from top manufacturers, allow sniffing of keystrokes out of the air from 250 feet away because they do not implement encryption. A vulnerable wireless mouse dongle can expose the computer to an external attack through keystroke injection. Once the computer is itself compromised, it can expose the larger network to insider attacks.
Unapproved Cellular Device Presence	Many organizations have a “no cell phones in this area” policy to comply with regulations. Ensuring that policies are maintained is key for security.
Unapproved Wireless Cameras (using Wi-Fi and other protocols)	Inexpensive wireless cameras are great for security when your security department installs them. But if someone else installs them then they can be used to plan security breaches. Know every camera operating in your facility and whether it works for your security team or someone else.
Vulnerable Wireless Building Controls (e.g. default credentials)	Many new pieces of equipment ship with two consoles: Ethernet and “Radio Ready” Consoles. You know about your Ethernet console but is there another console on your equipment set up with default configuration and broadcasting for instructions?
Unapproved IoT Emitters	New thermostats and building sensors often have multiple data radios. Wi-Fi is the one you know about. But is your sensor also transmitting on other frequencies like ZigBee (short range) or LoRa (up to 1 mile range)? What data is beaming down the street that you don’t know about?
Vulnerable Building Alarm Systems	Many Window, Door and Motion detectors can be ordered to “pay no attention to the man climbing in the window” by someone carrying a $10 radio jammer, or $300 Software Defined Radio, which can also simulate any alarm event. Security professionals need to be alerted when someone attempts to jam any part of their alarm system.

Customer Testimonial

Visibility

At Cylance, we've been using Bastille for a little over a year now. For me, the promise of Bastille to Cylance was visibility. We were going through quarterly audits of our corporate headquarters looking for covert listening devices, rogue access points, anything that could be used by an attacker to bridge the gap between the physical and the data layer and extract information out of our enterprise. The reason that we went with Bastille was that Bastille gave us the ability to do real time inspection of that space, and instead of dealing with something after it's been there for a while and you find it. We can detect it and remediate it the second it gets turned on.

Bastille gives Cylance the ability to, in real time, detect something that is potentially malicious or unwanted on our network and remediate it before we have to worry about the threat of exfiltration.

Radio (RF) is the New Frontier

As enterprises continue to grow and we're getting new smart devices, the boundaries are essentially eroding on a traditional perimeter. A firewall's not going to protect you from an RF based attack and Bastille is the only tech on the market that gives an enterprise the ability to not only monitor but protect all of the RF airspace at the same time.

Advantage Over Sophisticated Attackers

One of the reasons that I'm very fond of Bastille is normally when you're dealing with a sophisticated attacker, they're not going to attack you with the same attack that's been around for 10 years. They're funded, they're skilled. They can infiltrate things like supply chains. They can infiltrate corporate networks. And having that next generation of technologies where the attackers themselves don't realize that you're doing protection or monitoring there, essentially gives you a leg up. It gives you the ability to detect an attacker via a vector that they're not aware that you have capabilities to protect.

Trade-Secrets can be Exfiltrated by Voice and Data

Any type of covert listening device that could monitor our data science team or bridge the gap between our network and start to ex-filtrate trade secrets out over RF is a major, major concern. Not just from a customer privacy perspective, but from a competitive advantage. If you can't keep a hold of your company's intellectual property, it's gonna start popping up in competitive products."

Bastille was actually able to identify a bunch of vulnerable RF devices in our network on the initial POC, and we were able to go around and get everything replaced.

Jon Miller
Chief Research Officer

CYLANCE™

"

The Internet of Things will give superpowers to a new class of entrepreneurs able to forge the future of connected communications. Unfortunately, some of them will be criminals.

Internet of Things security has been a pressure point among researchers for a while. In an effort to keep costs low and the learning curve lower for neophyte consumers, manufacturers have rushed connected things to the market. Many have generic firmware and, worse, default passwords. Creepy hackers have easily commandeered everything from home security cameras to baby monitors. The jump to using connected devices as weaponry was just a matter of time.

In the [James] Bond films, despite villain superpowers, the forces of good always win. Then again, there is usually just one villain and they can't rent superpowers for just $30 a month. Cyber security trouble is not going away."

Forbes

Bastille Enterprise

Bastille Enterprise: Permanent System for Single Room to Global Enterprise Deployment

Fusion Center

The Fusion Center is available in several options to permit on-site/premise or cloud deployment as required. The Bastille Fusion center can be installed on-site as a second appliance, installed as a virtual appliance in a private cloud such as Pivotal Cloud Foundry (PCF), or can function as a SaaS client in the Bastille AWS Cloud or AWS GovCloud. The Fusion Center hosts Bastille APIs and can be accessed using HTTP Rest commands. A single Fusion center is horizontally scalable and can support multiple sites.

Sensor Arrays

Bastille's Sensor Arrays are 100% passive, they do not transmit, and are certified to be compliant with FCC standards. Earlier solutions to market relied on emitting RF signals to ping/poll devices. This is not suitable for any non-government customer or government customers where transmitters are not permitted in sensitive and classified spaces. Even though Bastille is entirely passive, we still gather 150+ data-fields from the devices we discover.

The Bastille Sensor Array is the 4th-generation Software Defined Radio (SDR) sensor array from Bastille. It contains two scanning 802.11ac Wi-Fi receivers, two SDR receiver front ends that can each sample at 61.44 MSps and sense from 25 MHz to 6 GHz. An array of bespoke internal antennas have been optimized to maximize detection and localization performance.

Each Sensor Array can cover an area of approximately 1,800 – 3,300 sq. ft. They are typically deployed at a client site, one every 50 ft along the perimeter of thee Area Under Observation (AOU). The Bastille Sensor Array is fully UL 2043 certified to operate in the building plenum. Given their plenum certification, Bastille sensors can be, and are typically installed above the ceiling tiles. Alternatively they can be suspended from a ceiling or placed on top of shelves.

Bastille Enterprise can protect a single room in one building or scale to protect hundreds of buildings within a global enterprise. Sensor Arrays are installed at each site and connect to the global Fusion Center.

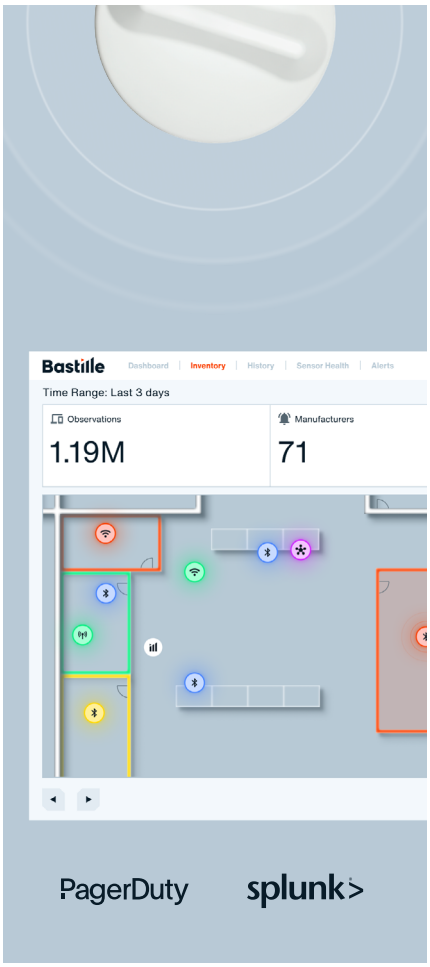


Figure 12: The Bastille architecture can be deployed 100% on premise or include cloud components if preferred.

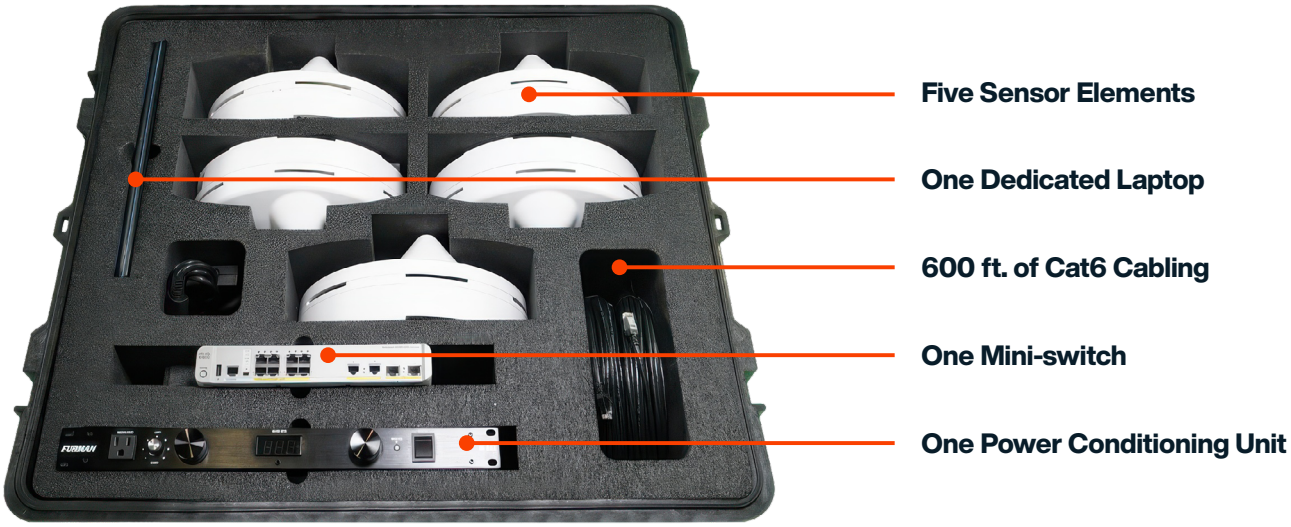
Bastille FlyAway Kit & Bastille Express

Portable Systems for Rapid Deployment at Meetings, Events and Remote Offices

Standalone Systems

The Bastille FlyAway Kit and Bastille Express are designed to work as standalone systems which can be moved from location to location and deployed rapidly. Typical use cases include providing security at meetings, events and at other remote offices/ locations. The sensor arrays are identical to the Enterprise solution and can detect and locate all the same devices and protocols. The server or cloud based Fusion Center from the Enterprise solution is delivered on a laptop. For both the Bastille FlyAway Kit and Bastille Express, the entire kit is delivered in two Pelican cases which can be shipped on a plane or transported in the back of an SUV or similar.

The Bastille FlyAway Kit and Bastille Express include all necessary components for field use:



From Pelican Case to Discovering and Analyzing in around 30 minutes

Figure 13: The Bastille Fly Away Kit

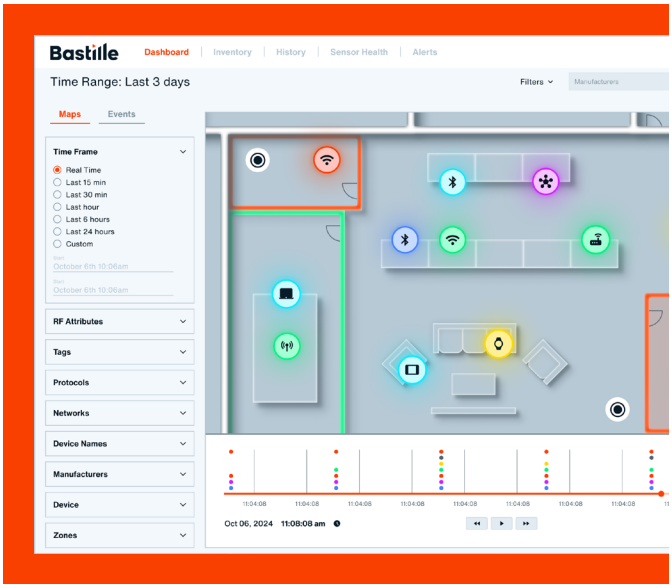


Figure 14: The Bastille Fusion Center

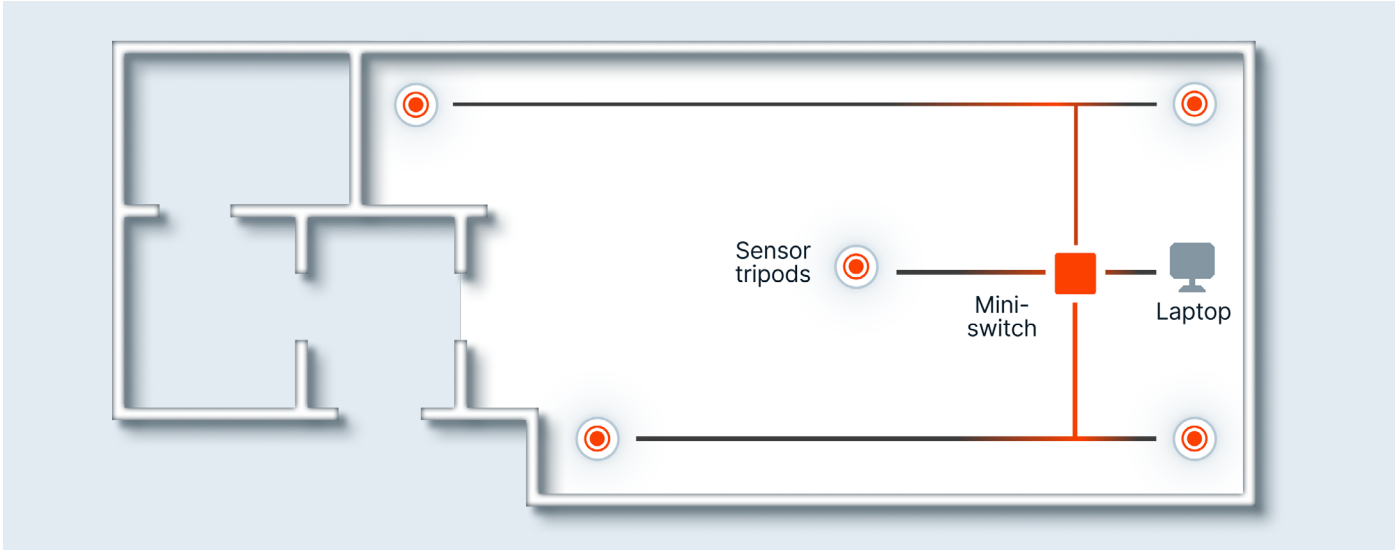


Figure 15: Use the power of Bastille to detect, locate and alert on WI-FI, BLE, Bluetooth and Cellular devices in remote and temporary locations.

Bastille Solutions for Commercial Customers

Bastille is available as a permanent installation or as a mobile tactical kit, with a variety of deployment scenarios. Many customers buy multiple products to satisfy their varying needs across their global environments. All Bastille products have the same GUI, Sensor Arrays and can detect the same protocols and devices. Below is a brief summary of the key features by product version for non-government customers. Please note that government customers have different products.

Key Features	Bastille Enterprise	Bastille Express XLE	Bastille Express
Passive FCC Certified Software Defined Radio Sensor Arrays	✓	✓	✓
Wi-Fi, BT, BTLE, 802.15.4 and Cellular Visibility	✓	✓	✓
DVR (Playback of Historical Data)	✓	✓	✓
Tagging and Adjudication Workflow	✓	✓	✓
Same Intuitive Easy-to-use Graphical User Interface	✓	✓	✓
Real-Time Enterprise Infrastructure Integrations	✓	✓	✓
API Module	Option	Included	✗
Number of Sensors	Unlimited	12 – Expandable to 50	5
Coverage	Millions of sq. ft.	Up to 20,000 sq. ft. Per Deployment – Expandable	Up to 5,000 sq. ft. Per Deployment
Simultaneous Areas Covered	Unlimited	Three	One
Typical Installation	Above or Below Ceiling	Tripod	Tripod
Use Case Type	Permanent	Portable/Tactical	Portable/Tactical

Bastille Versions

Bastille is available in two versions, both of which detect, locate and alert Cellular, Wi-Fi, Bluetooth and Bluetooth Low Energy devices and networks.

Bastille Enterprise

Supports deployments from one building to hundreds of buildings on a global basis. Sensor Arrays are installed above the ceiling in a building for persistent monitoring. The Fusion Center can be physically on-premise at the customer site, or housed within the customer's private cloud or within the Bastille Secure Cloud.

Bastille Express

Originally developed for the DoD, Bastille Express is a portable, self-contained, five-sensor version of Bastille using the same interface as Bastille Enterprise. Designed for temporary deployment (a few hours to a few months) and to be highly portable, the system ships in two Pelican cases and has all the equipment required to set up and monitor areas of up to 5,000 square feet within hours of the kit arriving on site.

Figure 16: Bastille's sensor array, which is now in its fourth generation, is entirely passive (does not emit any radio signals) and was designed and built in the USA.

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