Bastille

EXECUTIVE SOLUTION BRIEF

Bastille Networks: A Comprehensive Wireless Intrusion Detection System

Executive Summary

Wireless threats increasingly undermine enterprise security as organizations adopt Wi-Fi, Bluetooth, cellular, and IoT technologies. Bastille Networks offers a 100% passive, broadband Wireless Intrusion Detection System (WIDS) that delivers real-time monitoring, detection, analysis, investigation, and response capabilities. Covering 100 MHz to 7.125 GHz, Bastille provides enterprises with critical visibility into wireless activity, allowing rapid identification and mitigation of threats across all major wireless communication protocols.

Challenges in the Wireless Threat Landscape

Modern enterprises face multiple challenges in securing the radio frequency (RF) environment:

- **Wi-Fi Vulnerabilities:** Organizations are susceptible to various threats, including rogue access points, Evil Twin attacks, MAC spoofing, interception of unencrypted data transmission, and protocol-level exploits such as KRACK. Devices connecting to unsanctioned Wi-Fi networks may expose corporate credentials and sensitive data.
- **Bluetooth Exploits:** Bluetooth connections often come configured with minimal security controls. Attacks such as BlueBorne or KNOB exploit protocol flaws to spread malware or gain access to a device's data and communication channels.
- **Cellular Risks:** Mobile phones and hotspots can act as covert data connections that bypass existing security controls. This capability is particularly dangerous in secure facilities where mobile phones are restricted and in manufacturing environments where cellular interference can disrupt critical operations.
- **IoT Device Proliferation:** Many IoT devices lack fundamental security protections and use obscure wireless protocols. These devices often bypass traditional network security controls, creating blind spots and backdoors that can compromise the enterprise network.

Traditional wired intrusion detection systems (IDS) and basic Wi-Fi monitoring tools fail to address these threats, leaving organizations blind to risks in the RF spectrum. Additionally, many current solutions are reactive, providing limited context or forensic value.

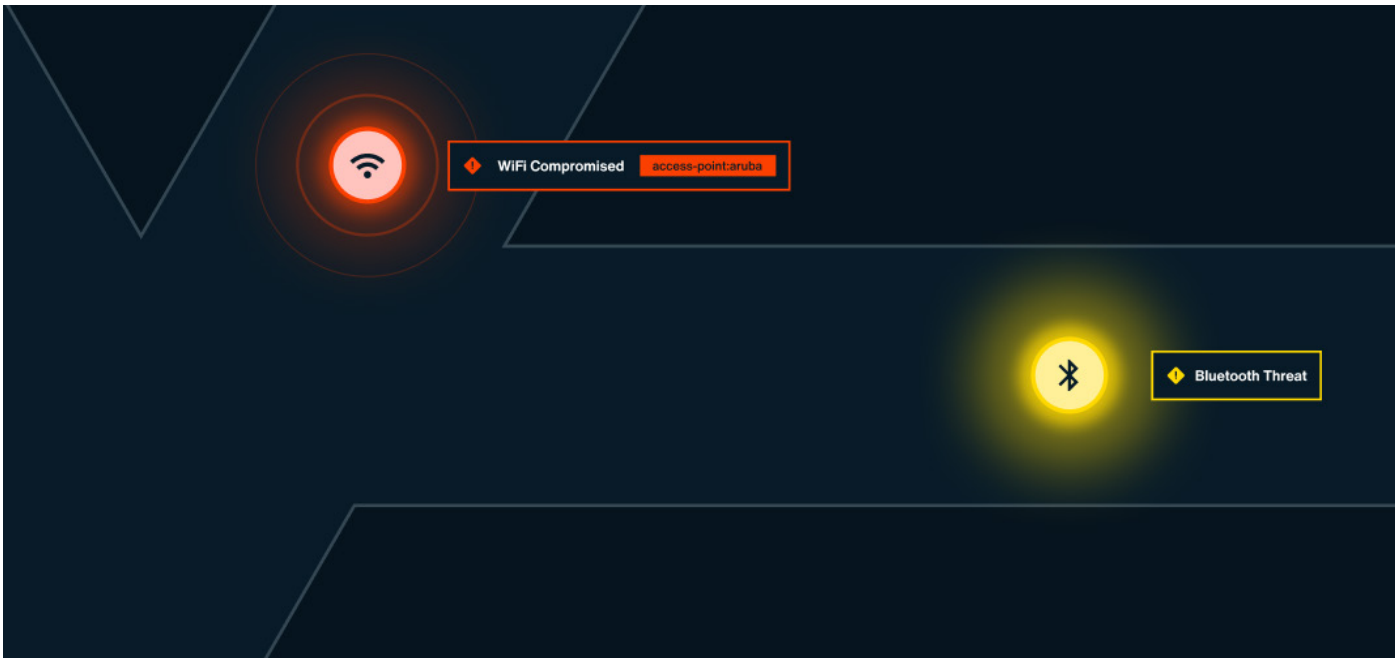

Figure 1: Bastille Wireless Intrustion Detection System

Bastille's WIDS Capabilities

Bastille's solution is purpose-built to address the full spectrum of wireless threats with the following features:

1. Full Spectrum Visibility: Bastille sensors monitor signals across the entire 100 MHz to 7.125 GHz range. This broad visibility includes:

- Wi-Fi (2.4 GHz, 5 GHz, and 6 GHz bands)
- Bluetooth Classic and BLE
- Cellular protocols (LTE, 5G)
- IoT RF technologies (Zigbee, Z-Wave, and others)

This capability enables the detection of wireless activity regardless of manufacturer, protocol tack, or encryption level.

2. 100% Passive Monitoring: Bastille's WIDS platform passively listens to RF emissions and is FCC-certified as 100% passive. It does not transmit any signals, eliminating regulatory risk and avoiding interference with operational wireless systems. This passive architecture is crucial in environments such as healthcare, defense, or manufacturing, where organizations must tightly control wireless emissions. It also allows Bastille to deploy in secure or classified environments, where rules and regulations require full passive operations.

3. Advanced Threat Detection: Using machine learning and rule-based analytics, Bastille detects:

- Rogue access points and unauthorized SSIDs
- Misconfigured devices
- Bluetooth enumeration and pairing attempts
- Signal anomalies
- IoT device impersonation or unexpected protocol usage

Threats are correlated across the environment and enriched with device metadata, behavioral patterns, and historical context.

4. Device Localization: Bastille utilizes signal characteristics and a network of distributed sensors to pinpoint the location of wireless devices with high precision, achieving an accuracy of 1-3 meters. This capability supports:

- Physical security and threat hunting
- Rapid interdiction of rogue devices
- Compliance validation for restricted zones

Localization is achieved through patented Bastille technologies and does not require cooperation from the device. It is the only solution that can actively track Bluetooth devices before AND after pairing.

5. Policy Enforcement: Security teams can define and enforce granular wireless usage policies. Bastille continuously monitors for policy violations, including:

- Connection of unauthorized BYOD or IoT devices
- Bluetooth peripherals in high-security areas
- Unexpected cellular activity in air-gapped or SCIF environments
- Wi-Fi hotspots violating company or regulatory policies

Alerts are prioritized based on severity, threat category, and impact.

6. Integration with Enterprise Systems: Bastille integrates with SIEM and SOAR platforms through standard APIs and syslog. This capability allows:

- Centralized alert management
- Automated response workflows
- Correlation with other security telemetry
- Long-term threat intelligence aggregation and compliance reporting

Popular integrations include widely used solutions like Splunk, Aruba, PagerDuty, and Lenel OnGuard.

Benefits of Bastille WIDS

- **Comprehensive Risk Mitigation:** Bastille eliminates wireless blind spots and provides a unified view across all wireless technologies, supporting proactive threat detection and incident prevention.
- **Operational Efficiency:** Security analysts receive actionable alerts with device type, behavior, and location context, thereby reducing the mean time to detection (MTTD) and the mean time to response (MTTR).
- **Regulatory Support:** Organizations subject to HIPAA, PCI DSS, NERC CIP, or FedRAMP benefit from Bastille's auditing and compliance monitoring capabilities.
- **Protection of Critical Environments:** Bastille is uniquely suited for high-stakes environments such as:
  - **Data centers:** Prevent rogue Wi-Fi or Bluetooth risks to sensitive infrastructure
  - **Hospitals:** Enforce radio silence zones and monitor RF emissions from medical devices
  - **Manufacturing:** Detect unauthorized wireless transmissions that could disrupt industrial control systems
  - **Government and military:** Identify RF intrusions in SCIFs or restricted facilities

Conclusion

Wireless threats will continue to evolve as enterprises adopt new technologies. Bastille's broadband, 100% passive WIDS solution uniquely positions organizations to detect, monitor,and respond to wireless threats across Wi-Fi, Bluetooth, cellular, and IoT protocols. By delivering unmatched RF visibility, contextual intelligence, and actionable alerting, Bastille enables enterprises to protect their wireless environments with confidence. Security leaders seeking to close the wireless gap and operationalize RF security benefit from Bastille's purpose-built, scalable platform.

For more information, visit www.bastille.net or contact Bastille Networks today.

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