Bastille

EXECUTIVE SOLUTION BRIEF

Securing Data Centers Against Wireless Threats

Wireless Airspace Defense with Bastille Networks

Executive Summary

Data centers form the critical foundation of digital operations across industries, hosting sensitive information, enabling cloud services, and powering essential business functions. While data center operators have invested in strong perimeter and network defenses, wireless communication remains a largely unmonitored and highly exploitable attack surface. As wireless protocols and IoT devices proliferate across operational and IT environments, organizations require a new layer of defense: Wireless Airspace Defense. Bastille Networks provides the visibility, detection, and response capabilities to protect data centers from wireless threats, without disrupting operations or introducing network risk.

Evolving Wireless Threats to Data Centers

The risk profile of data centers has changed significantly with the rise of unmanaged wireless communications. Even in controlled environments with stringent policies, the following threats frequently emerge:

- **Unauthorized Devices:** Employees or contractors may inadvertently introduce mobile hotspots, Wi-Fi access points, USB modems, or wearable devices that bypass firewall protections and provide backdoors into secure systems.
- **Wireless Bridging:** Devices connected simultaneously to secure corporate networks and unsecured wireless networks (e.g., LTE, 5G, or guest Wi-Fi) create unintended data exfiltration paths. These “soft breaches” often go unnoticed by traditional network monitoring tools.
- **IoT and Embedded Systems:** Printers, security cameras, HVAC systems, environmental sensors, and smart lighting often communicate over Bluetooth Low Energy (BLE), Zigbee, or proprietary radio frequency (RF) protocols. Misconfigurations or vulnerabilities in these systems open up additional attack vectors.
- **SDR and Rogue Transmission Tools:** Inexpensive software-defined radios (SDRs) allow threat actors to scan, spoof, or jam RF signals across various frequencies. These tools can emulate authorized devices or exploit unmonitored spectrum ranges.

The Case for Wireless Airspace Defense

The wireless airspace is a security blind spot in many data centers. Traditional firewalls, NAC systems, and endpoint agents effectively secure digital pathways but offer no visibility into the physical-layer RF activity that permeates data center environments.

Bastille enables data center operators to:

- **Continuously Monitor the Entire Spectrum:** Gain visibility across 100 MHz to 7.125 GHz, including Wi-Fi, LTE, 5G, BLE, Zigbee, and proprietary wireless protocols.
- **Detect Rogue and Unknown Devices:** Identify unauthorized transmissions from wireless devices that violate policy or introduce risk.
- **Locate Devices Precisely:** Determine the physical location of transmitting devices to enable rapid physical investigation and remediation.
- **Correlate Wireless Activity with Network Events:** Link RF emissions to potential bridging, lateral movement, or anomalous behavior.
- **Support Compliance and Risk Governance:** Document and enforce wireless policy as part of broader compliance mandates (such as NIST, ISO/IEC 27001, SOC 2, PCI DSS, and others).

Bastille Solution Architecture

Bastille's wireless airspace defense platform is ideal for enterprise-scale data center deployments. It provides:

- **100% Passive Sensor Network:** Bastille sensors listen to the wireless environment without emitting any signals. This feature results in zero disruption to critical infrastructure and supports covert monitoring of high-security areas.
- **Advanced Signal Processing and Analytics:** Bastille identifies, classifies, and tracks wireless transmissions using advanced algorithms and machine learning models. It distinguishes between authorized, unknown, and malicious behavior in real time.
- **Wide Protocol and Frequency Coverage:** Bastille provides visibility to protocols from 100 MHz to 7.125 GHz, capturing RF emissions from IoT devices, WI-Fi, Bluetooth, and cellular devices.
- **Device Localization:** Bastille calculates device location based on signal attributes using patented proprietary techniques. The solution provides one to three meters of accuracy when locating any transmitting device and visualizes its location on the facility's floor plan.
- **Integration with SOC Tools:** Bastille integrates with SIEM platforms, ticketing systems, and incident response tools, enabling alerts for wireless threats to flow into existing security workflows for triage and investigation.
- **Global scale:** The Bastille solution scales globally across the enterprise, so operators with multiple sites can manage and monitor their deployment centrally.

Deployment Models for Data Center Environments

Bastille supports flexible deployment models to accommodate different facility types and risk profiles:

- **Corporate Data Centers:** Full-facility coverage for RF zoning, alerting, and policy enforcement.
- **Colocation Environments:** Segmented monitoring to protect shared space while supporting customer tenancy rules.
- **Cloud-Adjacent Facilities:** Provide administrators with prebuilt dashboards that provide an instantaneous view into RF devices, including activity, threats, abnormal behavior, and sensor performance.

Deployment scales with floor space and threat tolerance, with sensor density tailored to visibility and resolution needs.

Strategic Business Impact

Deploying Bastille in your data center environment delivers measurable outcomes:

Outcome	Description
Reduced Risk of Wireless Breach	Detect and mitigate rogue devices and bridging activity before exploitation occurs.
Improved Incident Response	Enable rapid identification and physical location of transmitting devices.
Increased Compliance Confidence	Demonstrate proactive wireless monitoring to meet audit and certification requirements.
Enhanced Operational Resilience	Monitor wireless threats without interrupting core IT or facility operations.

Conclusion

Wireless threats are no longer theoretical but operational realities in modern data centers. Without wireless airspace visibility, critical infrastructure remains vulnerable to unseen attack vectors.

Bastille closes this gap with passive, continuous wireless monitoring, helping security leaders extend Zero Trust principles into the physical layer and reduce risk in high-value environments.

To schedule a demo or wireless risk assessment, visit bastille.net or contact your account representative.

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

linkedin.com/company/bastille-networks/

x.com/bastillenet

youtube.com/@Bastille