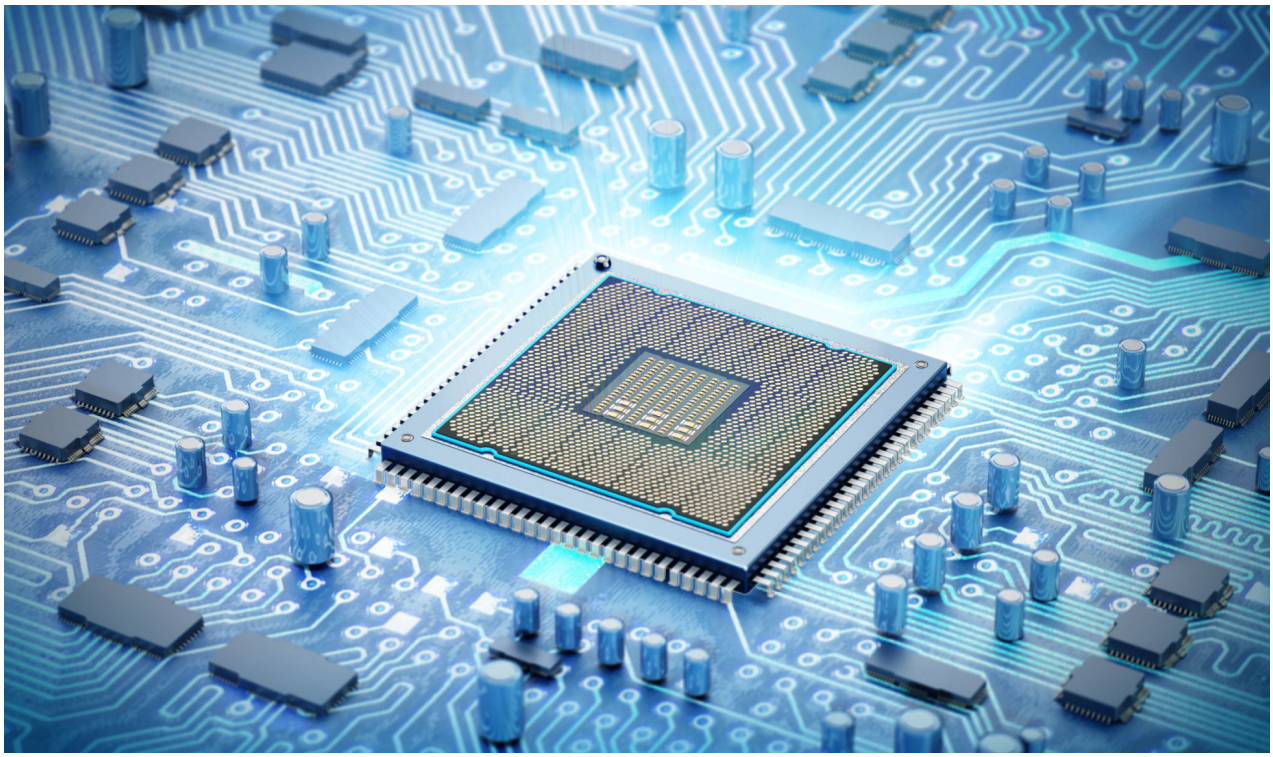
WIRELESS
AIRSPACE
DEFENSE

LOCH
TECHNOLOGIES

EMI Attack Surface

www.loch.io



Wireless Airspace Defense for EMI Risks and Threats

Electromagnetic Interference (EMI) attacks, particularly in cybersecurity and electronic warfare, involve the intentional use of electromagnetic energy to interfere with or damage electronic equipment. These attacks can be highly sophisticated and are often associated with military or espionage activities. However, due to the increasing pressures for better supply chain audits, tampered hardware and counterfeit products are finding their way onto the motherboard, creating new vulnerabilities and covert communications, resulting in EMI attacks going unmonitored. This report highlights the risks and threats associated with the EMI attack surface and what can be done now to help detect, assess, and prevent risk.

Understanding the Implications of EMI on Business Operations

EMI attacks can compromise the integrity and confidentiality of your data and systems. Without proper monitoring and mitigation measures, your business could become vulnerable to cyber threats, including data breaches, espionage, and sabotage.

EMI interference could disrupt the operational functionality of electronic equipment critical to your business operations. If customers are affected by service interruptions, this could lead to downtime, delays in production, loss of revenue, and damage to your reputation.

Furthermore, dealing with the aftermath of EMI attacks, such as repairing or replacing damaged equipment, investigating the source of the interference, and implementing security measures, can incur significant financial costs for your business based on the knee-jerk reaction to gaining back control.

EMI attacks can also be used to exfiltrate sensitive information or intellectual property from your organization covertly. Without proper monitoring, you may not detect these unauthorized transmissions, leading to the loss of valuable assets and competitive advantage. Failure to address EMI risks could result in non-compliance with industry regulations and standards related to cybersecurity and data protection, leading to legal repercussions, fines, and damage to your company's reputation.

Finally, EMI attacks are entering the supply chain via stealthy rogue, tampered hardware, and/or counterfeit products posing additional risks to the business. Without monitoring for EMI threats against systems standards or baselines, you may inadvertently incorporate compromised components into your network, exposing your business to potential exploitation. The goal of EMI monitoring and baselining is to detect non-compliant chipsets before an IP is assigned and placed onto the network.

Why does it matter?

Neglecting to monitor EMI risks exposes your business to various threats, including cybersecurity breaches, operational disruptions, financial losses, and regulatory non-compliance. Implementing effective monitoring and mitigation strategies is crucial to safeguarding your organization's assets, reputation, and long-term viability.

EMI is an expanding attack surface of electromagnetic interference that presents risks such as data loss, disrupted transmissions, battery wear, and failures in critical systems. Different types of signals each contribute uniquely to the spectrum of threat.

Signal Category	EMI Threats
Analog Voice Signals	Cross-talk. Harmonic Interference. Amplitude modulation
Digital Data Signals	Bit errors. Signal attenuation. Timing errors
Video Signals	Image Distortion, Ghosting, Signal loss
Control Signals	Misinterpretation of signals. Delayed response. Loss of control
Satellite Signals	Atmospheric interference. Scintillation, Solar flares
Cellular Signals	Intermodulation. Tower interference, Multipath fading
WiFi Signals	Channel interference. Bandwidth saturation, Encryption vulnerabilities
Bluetooth Signals	Eavesdropping, Bluejacking. Bluesnarfing
GPS Signals	Jamming. Spoofing, Multipath errors
RFID/NFC Signals	Reader collision, Tag collision, Eavesdropping
Tampered Hardware	Counterfeit products/chips on motherboard

Detecting EMI (Layer 0) threats is critical in tackling these issues. EMI pertains to the most fundamental layer of electromagnetic activity, encompassing any ‘intended’ or ‘unintended’ emanations. Every device that uses electricity emits electromagnetic emanations - radio waves and is susceptible to attack.

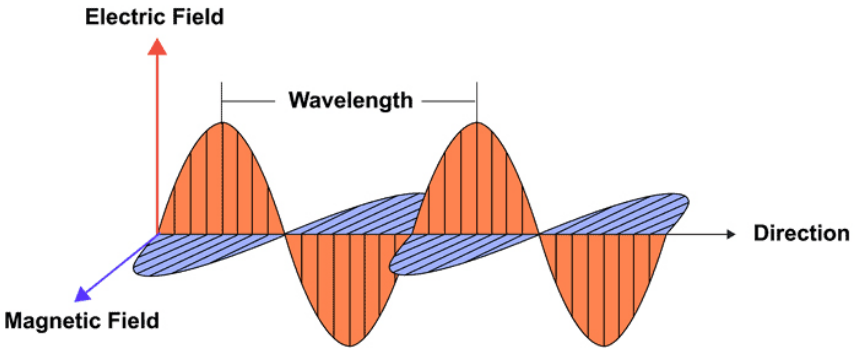
EMI Detection: Safeguarding the Wireless Airspace

- **Early Detection:** EMI (Layer 0) threat detection involves monitoring and analyzing electromagnetic emissions at their source. This allows businesses to detect potential interference, tampered hardware, counterfeit products, or unusual emissions before disrupting communications.

- **Mitigation:** Businesses can mitigate these issues by identifying and locating sources of interference or vulnerabilities in the spectrum. This might involve adjusting the placement of antennas, implementing shielding, or employing frequency manipulation techniques.

- **Enhancing Security:** EMI (Layer 0) threat detection improves the overall security posture of IoT, IIoT, IT, and wireless networks. It helps in identifying potential weaknesses and vulnerabilities that can be exploited by attackers using attacks such as:

  - PowerHammer - used to exfiltrate data through the power lines
  - aIR-Jumper - takes sensitive data through infrared CCTV
  - USBee - steal data using RF transmissions from USB
  - DiskFiltration - steal data using sound signals
  - AirHopper -turns a video card into an FM transmitter
  - Fansmitter- uses noise from a fan to transmit data
  - GSMem - an attack that relies on cellular frequencies
  - POWER-SUPPlay - turns Power-Supplies into Speakers
  - xLED - uses router or switch LEDs to exfiltrate data
  - HVACKer - uses an HVAC system to control
  - CTRL-ALT-LED - steal data using keyboard LEDs
  - BRIGHTNESS - stealth using screen brightness variations



Enterprises that depend on cellular 4G or 5G, GPS, and broad-spectrum IoT technologies are vulnerable to various risks, including security breaches, disruptions, and unauthorized access, stemming from RF vulnerabilities. To mitigate these risks effectively, it's crucial to implement EMI (Layer 0) threat detection mechanisms. By detecting and addressing these threats at their source, businesses can significantly enhance the reliability and security of their wireless communications and IT infrastructure. This proactive approach helps safeguard business operations from potential RF-related risks, ensuring uninterrupted functionality and protection against malicious activities.

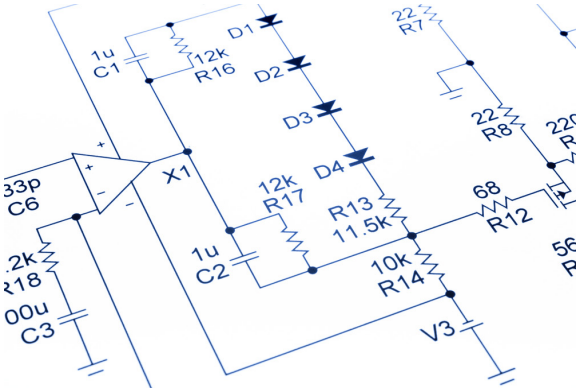
EMI Dangers and Vulnerabilities

- **Radio Frequency Interference (RFI):** This is a common form of EMI where radio frequency signals are intentionally used to disrupt the normal operation of electronic devices. RFI can be targeted at specific frequencies to interfere with communication systems, navigation systems, or other RF-dependent technologies.

- **HERF (High-Energy Radio Frequency) Attacks:** These involve directing high-energy RF pulses at electronic targets to cause damage or disruption. HERF devices can be used to disable electronic components, erase data on magnetic storage, or interfere with computer systems.

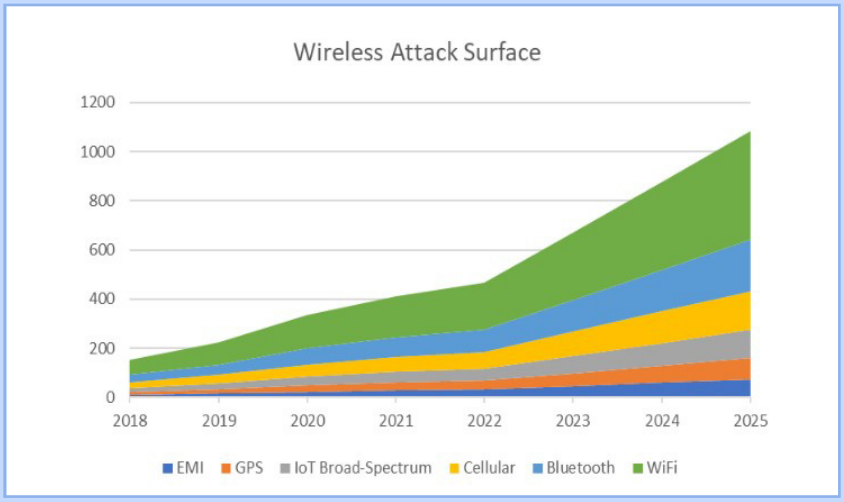
- **Microwave Weapons:** These devices use microwaves to heat and potentially damage electronic components. Directed-energy microwave weapons can disable electronics without causing physical damage to the targeted device, making them a subtle tool for electronic warfare.

- **TEMPEST Attacks:** This refers to a type of spying technique that involves eavesdropping on the electromagnetic emissions from computing devices. While not an "attack" in the traditional sense, it is a form of EMI exploitation used to gather information without direct physical access to the target.

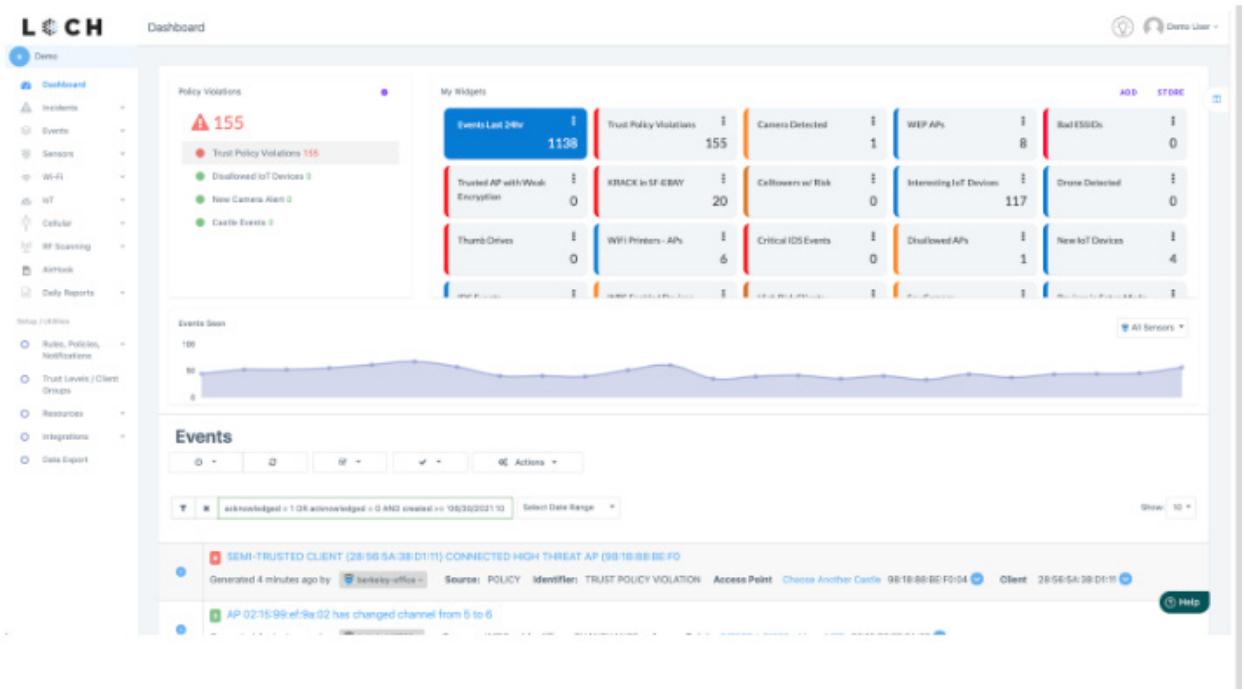


Wireless Airspace Defense

Wireless and RF-based communications play a pivotal role in enabling IT, IoT, and OT functionalities, positioning them at the forefront of technological advancement. However, the proliferation of internet-enabled devices has expanded the attack surface, introducing new vulnerabilities. While established technologies like 802.11 and Bluetooth benefit from mature security models, the emergence of numerous protocols and frequencies for communications lacks adequate protection.



AirShield AI: Zero Trust Enforcement for all things Wireless/RF



AirShields detection capabilites extend to indentifyng events in cellular, broad-spectrum IoT, GPS, Bluetooth, CBRS, GPS, and EMI.

Although solutions exist to safeguard classified facilities such as government buildings and SCIFs, there remains a gap in cost-effective solutions that offer continuous 24/7 assessment at an affordable price point.

Furthermore, ensuring the integrity of the supply chain for microelectronics, devices, and systems is paramount in the face of rapid commercial progress and the proliferation of Commercial Off-The-Shelf (COTS) devices. State-sponsored adversaries further compound this challenge.

Addressing these complexities requires innovative solutions like the LOCH AirShield platform. By leveraging AirShield, organizations can effectively mitigate risks by capturing, analyzing, and continuously monitoring both 'intended' and 'unintended' emissions. This proactive approach enhances security measures, offering comprehensive protection against evolving threats in the dynamic landscape of wireless communication and IT infrastructure.

Wireless/RF & Supply Chain Threats

Conventional 'network-based' security measures are inadequate in safeguarding against RF/Wireless or Cellular connectivity-based attacks. Moreover, they lack the capability to identify compromised equipment within the supply chain, where altered software, firmware, or microelectronics embed backdoors for initial infiltration.

As with any cyber assault, malicious actors continually target vulnerable victims, exploiting a vast attack surface that offers multiple entry points and evades detection.

The three emerging attack surfaces that have become prime targets are:

Wide-Spectrum RF/Wireless

Broad-Spectrum Wireless encompasses the expansive range (300MHz to 6GHz) of unseen radio frequencies utilized by devices for communication. While some of these devices eventually transition to wired networks, allowing traditional security tools to detect abnormalities and mitigate threats, many solely rely on RF/Wireless connectivity, operating beyond the purview of network security solutions.

Cellular Interception

LTE, 4G, and more recently, 5G networks have surged in popularity, driven by the promise of enhanced bandwidth and network segmentation offered by 5G technology. However, such connectivity evades traditional security measures, lacking firewalls or endpoint agents, thus creating a susceptible target for interception.

Hardware Tampering

Hardware tampering involves the insertion of malware or trojans into communication devices, servers, or other network equipment during manufacturing or supply chain processes. These alterations, whether in software, firmware, or microelectronics, can be exploited to establish backdoors for initial access and subsequent network infiltration.

Distinctive Features of LOCH AirShield: Setting a New Standard in Security

As the landscape of data transmission expands with the adoption of numerous protocols, frequencies, and operating systems beyond traditional WiFi channels, the threat of over-the-air attacks has surged, growing in both frequency and sophistication while often evading detection.

In response to this evolving cybersecurity challenge, LOCH AirShield has redefined next-generation defense strategies with its groundbreaking Wireless Airspace Defense platform™. This platform, comprising AirShield™, AirCell™, and AirShield-GPS™ capabilities, is engineered to detect, assess, and mitigate risks arising from the emerging attack vectors of cellular, wide-spectrum IoT, EMI emissions, GPS, and WiFi networks.

Unlike conventional security measures, AirShield offers non-intrusive, passive monitoring, providing 24/7 continuous surveillance of the airwaves. This enables real-time visibility into every RF-emitting device within the premises, empowering organizations to proactively identify and neutralize potential threats before they escalate.

AirShield AI for Far Field and Mid Field RF Detection

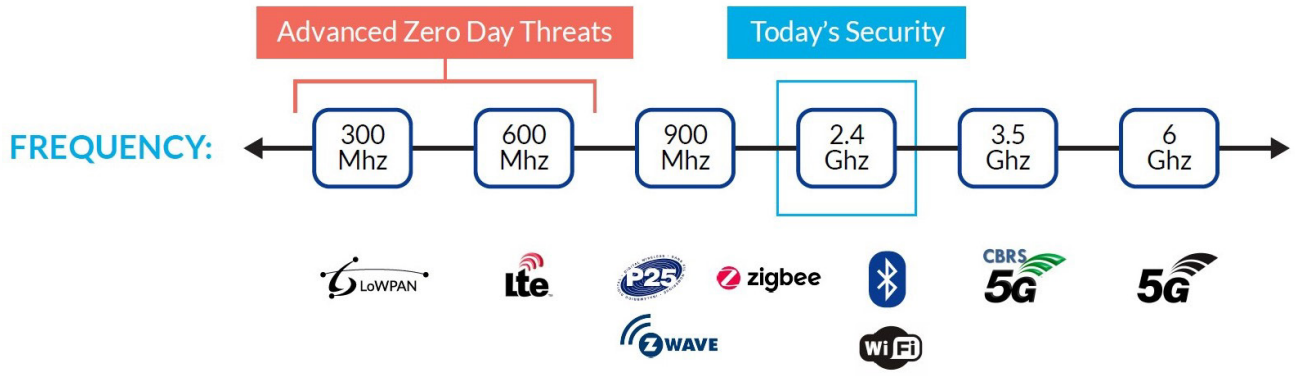
LOCH's AirShield smart sensor is equipped with state-of-the-art software-defined radios (SDR) that possess the unique capability to "listen" to RF emissions spanning from 300MHz to 6GHz. This broad frequency range empowers the sensor to detect intended emissions from various sources, including broad-spectrum RF, WiFi, Cellular, Bluetooth, and other protocols.

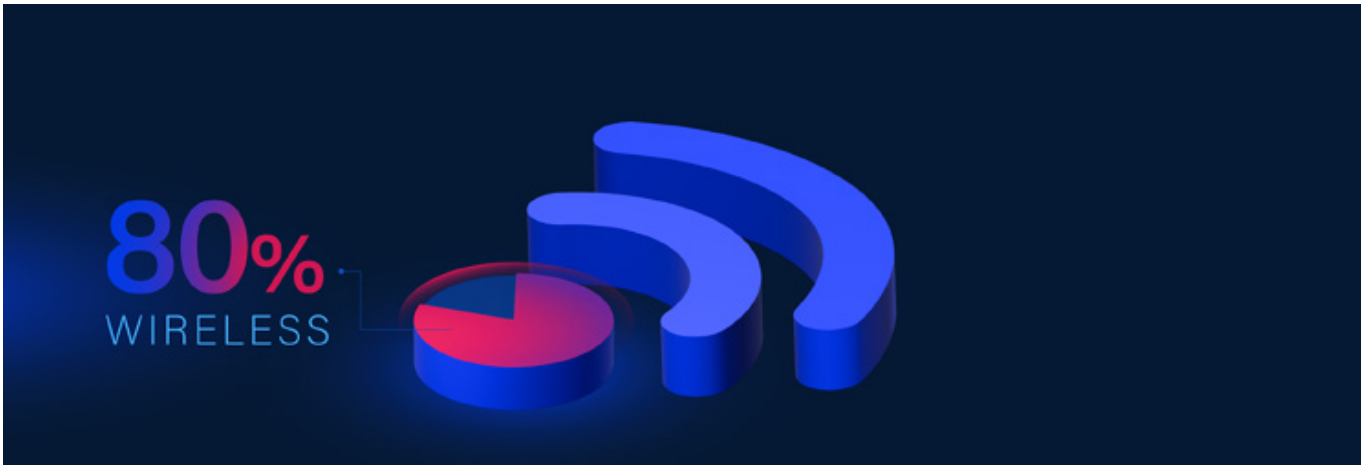
What sets the AirShield sensor apart is its remarkable field programmability, ensuring adaptability to emerging technologies and applications. This future-proof feature enables seamless integration with new protocols and functionalities as they emerge, safeguarding against obsolescence.

Moreover, the AirShield sensor goes beyond mere detection by incorporating advanced demodulation capabilities. This allows AirShield to decipher the transmitted protocols and extract valuable information from the emitting assets, enhancing situational awareness and enabling informed decision-making in response to detected threats or anomalies.

Wireless /RF Attack Surface

With 80% of devices now wirelessly connected, wireless has quickly become the new network and attack surface - the invisible threat.





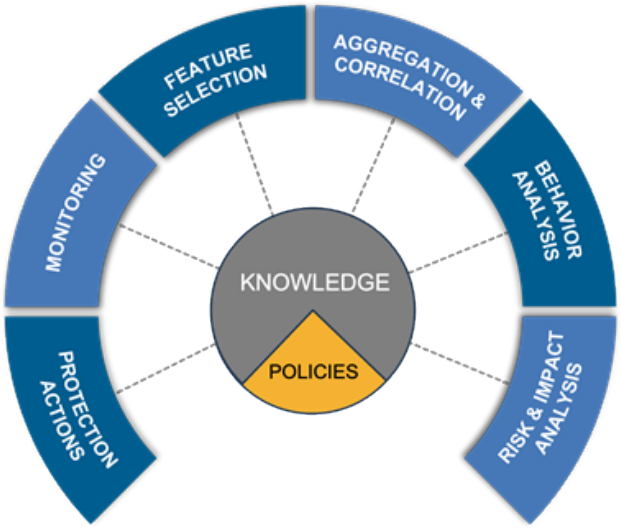
Wireless Airspace Defense - a new era in cybersecuirty

LOCH's AirShield AI smart sensor employs cutting-edge technology to accurately pinpoint, identify, and continuously monitor devices across a wide spectrum of RF frequencies. By meticulously analyzing "intended" as well as "unintended" emissions, the platform gains RF insights into the behavior of devices.

Through monitoring control plane beacons, probes, authentication, and association frames, AirShield constructs a comprehensive inventory of all assets within the network and their communication patterns. This meticulous approach not only facilitates device identification but also provides valuable insights into their operational characteristics and communication behaviors.

Wireless Airspace Defense for:

- enforcing zero-trust - measure what should be against what is,
- Asset Classification - Rank all RF Vulnerabilities in order of severity,
- Mitigate risk through the use of Air Termination.



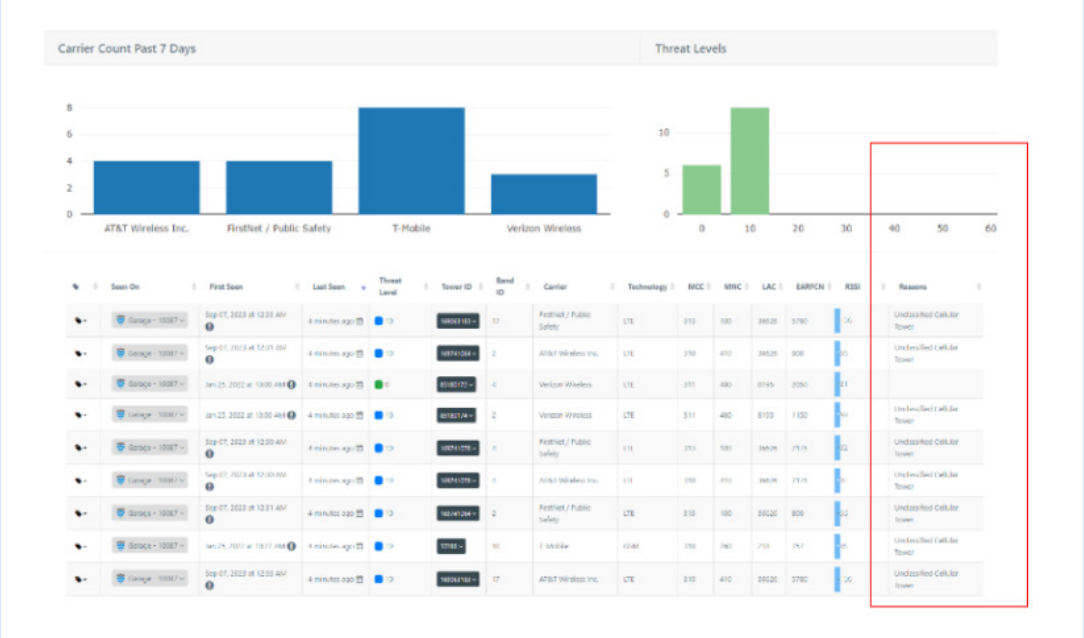
Zero-Trust Enforcement for all wireless communications

Cellular & CBRS Attack Surface Management

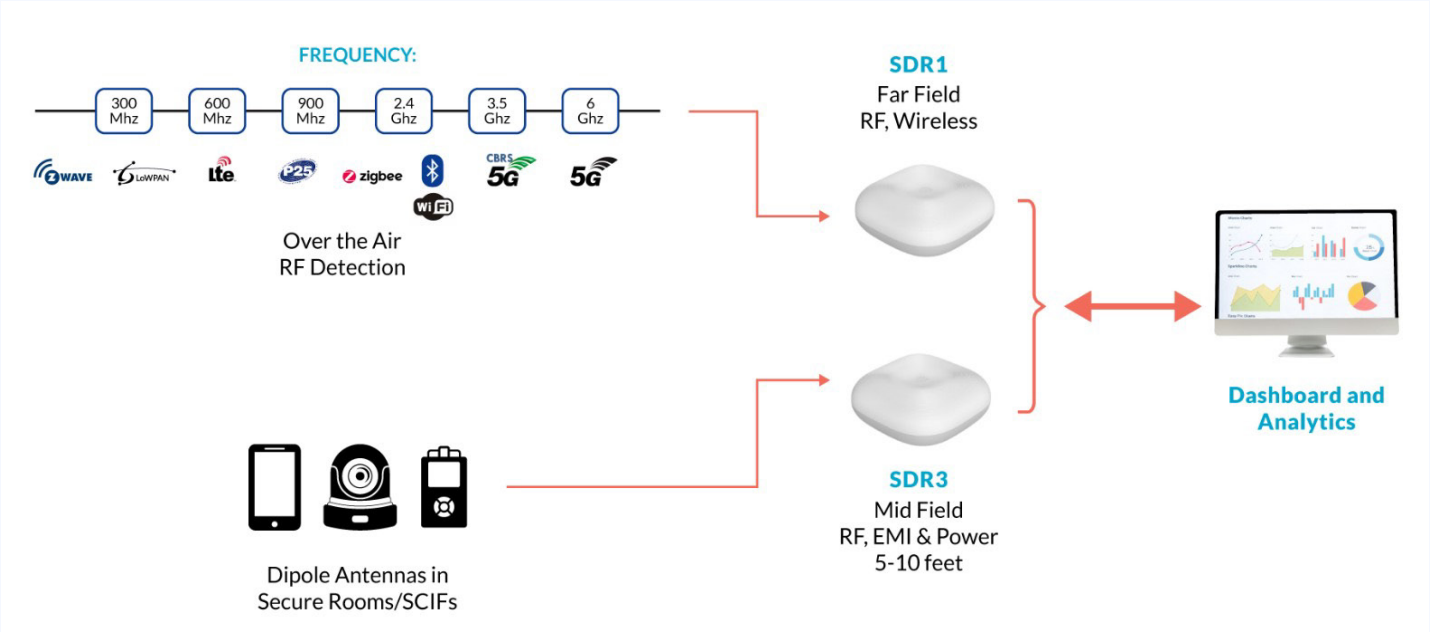
The LOCH AirShield platform offers uninterrupted surveillance of eNodeB and gNodeB advertisements, enabling the comprehensive collection, inventorying, and monitoring of data from cellphone towers. This data undergoes rigorous analysis against an internal repository of known attributes sourced from carriers, identifying legitimate cellphone towers and assigning them a trust score ranging from known to suspicious.

Additionally, users have the flexibility to contribute their own data, such as CBRS and private cellular networks, to enrich the internal dataset for further analysis and refinement.

Central to AirShield's capabilities is its patented antenna board equipped with seven antennae, facilitating the collection of RF data across various frequencies, including cellular 3G/4G/5G, broad-spectrum RF (ranging from 300 MHz to 6.0 GHz), and 802.11 Wi-Fi/Bluetooth. This comprehensive data collection empowers the platform to deliver robust protection and security enforcement measures in both Far Field (building-level) and Mid Field (room-level) deployments, ensuring comprehensive coverage and defense against potential threats.



AirShield AI Smart sensor



AirShield AI Smart sensors for Far-Field (building-level) and Mid-Field (room-level) RF visivility and detection

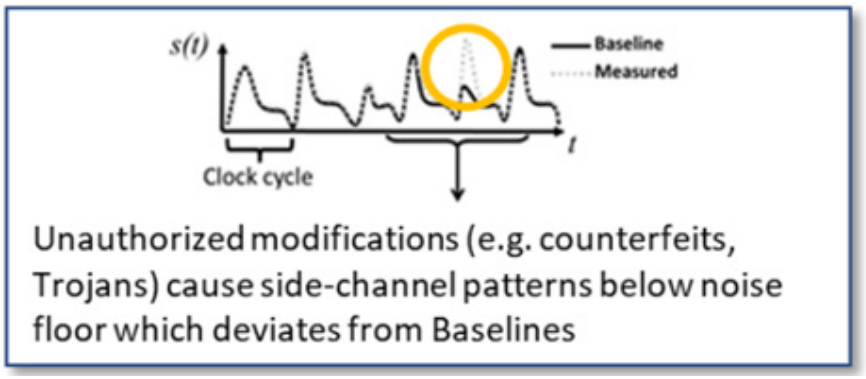
AirShield AI for Near Field and EMI Emanation Detection

LOCH's AirShield EMI fingerprinting employs an innovative out-of-band approach to identify alterations and intrusions within microelectronic components and systems. This technique relies on precise anomaly detection of unintended analog emissions or near-field emanations, such as power consumption or electromagnetic radiation.

AirShield's EMI fingerprinting methodology facilitates non-destructive screening and verification of microelectronics, particularly for cutting-edge devices, on a scalable basis. Every electronic device emits unique unintended emissions or emanations, stemming from variations in manufacturing processes and specific firmware configurations.

By harnessing the power of machine learning, AirShield's EMI fingerprinting establishes a baseline of standard emission patterns and utilizes it to pinpoint tampering in hardware or firmware introduced at various stages of the supply chain. This advanced approach enhances security measures by enabling proactive detection of unauthorized modifications, safeguarding against potential threats and ensuring the integrity of electronic systems.

Detecting Hardware Trojans, Counterfeit Products/Microchips, and Tampered Hardware



Every Device that Uses Electricity is Susepticial to Attack

By using machine learning to establish power fingerprint "attack" emissions baselines from electronic devices, this process aims to detect any unauthorized modifications to motherboards or any tampering within the electronic systems itself.

Essentially, EMI power fingerprinting development comprises a suite of analytical tools and machine learning models designed for extraction methodologies applicable to various targets. While existing EMI fingerprinting solutions offer analytical tools for sensor configuration and data management, AirShield AI/ML employs distinct training algorithms and real-time assessment mechanisms, resulting in heightened accuracy.

AirShield EMI fingerprinting offers flexibility in terms of side-channel signal collection devices, supporting multiple low-cost digitizers and software-defined radios. Furthermore, it accommodates test equipment from various vendors, such as Keysight, known for its high-end devices featuring exceptional sensitivity and minimal noise levels. These capabilities enable AirShield to capture even the faintest near-field side channel patterns, facilitating the detection of hidden intrusions within the supply chain.

The LOCH AirShield EMI fingerprinting system is capable of evaluating the integrity of digital devices to identify any unauthorized modifications in both hardware and software components. This capability has been successfully demonstrated across various platforms, including industrial control systems, network infrastructure, and UAV flight computers.

The primary goal of AirShield EMI fingerprinting is to establish a novel protection framework that distinctively separates security-monitoring functions from the protected system itself. This approach targets low-resource, embedded, and Internet of Things (IoT) devices, aiming to enhance security measures without imposing significant resource burdens on the protected systems.

In essence, AirShield EMI fingerprinting introduces a proactive security paradigm that allows for continuous monitoring and detection of tampering without compromising the performance or functionality of the underlying digital devices. By focusing on scalability and efficiency, it addresses the evolving security needs of modern digital ecosystems while minimizing overhead and complexity.

Conclusion

The LOCH AirShield AI Wireless Airspace Defense Platform, offers comprehensive protection against a myriad of threats, ranging from rogue actors and devices to misconfigurations and covert data exfiltration pathways via EMI emissions. Acting as a vigilant sentinel, AirShield continuously monitors the airspace, promptly detecting and alerting against policy deviations or unacceptable exposure states before any loss or incident occurs.

This proactive approach to security is indispensable in today's interconnected world, whereby wired and wireless connections intersect, posing unseen risks. With AirShield AI, organizations gain heightened vigilance and control, allowing them to navigate this invisible threat landscape with confidence and assurance of robust protection.

By proactively addressing these challenges and implementing comprehensive security measures, organizations can reduce the risks posed by hardware-based attacks, counterfeit products, and tampered hardware, thereby safeguarding the integrity and security of their electronic devices and systems along with any covert wireless "unseen" transmissons within the environment.