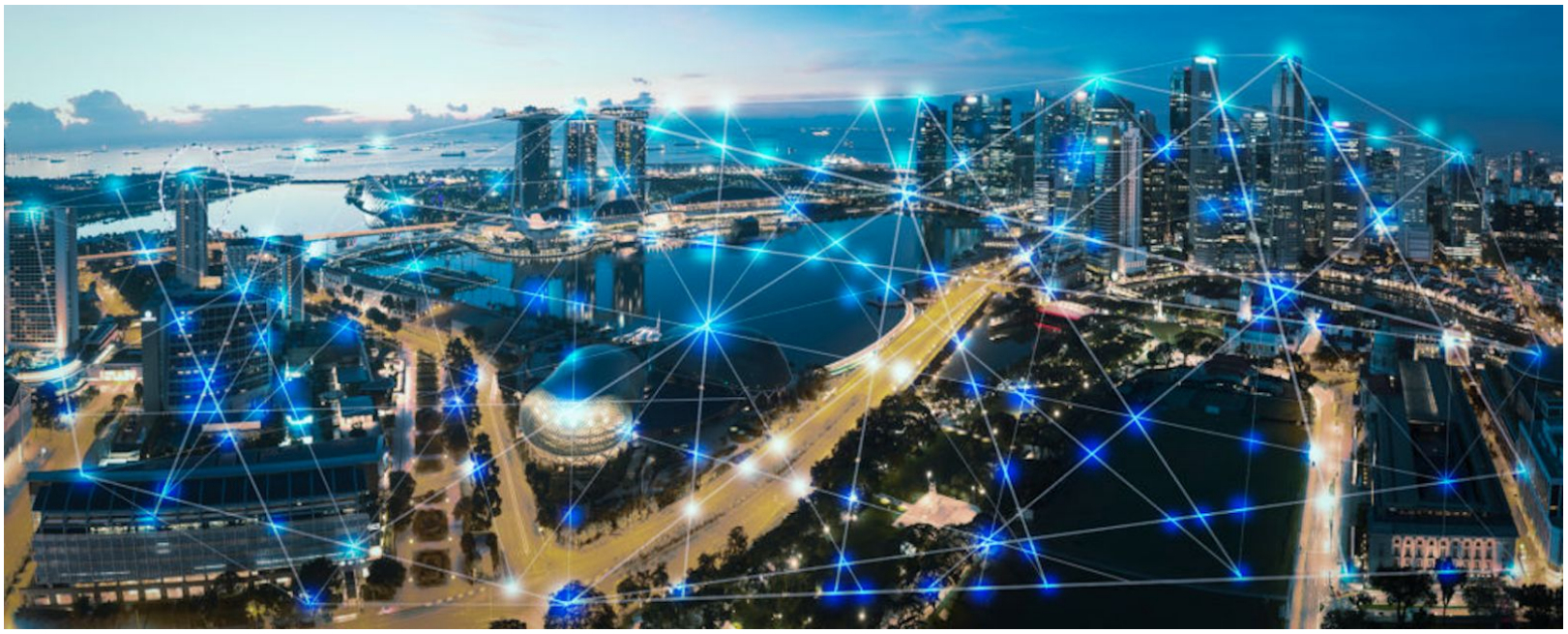
802secure

Fortifying IT & OT Networks from IoT Risks



Solution Brief

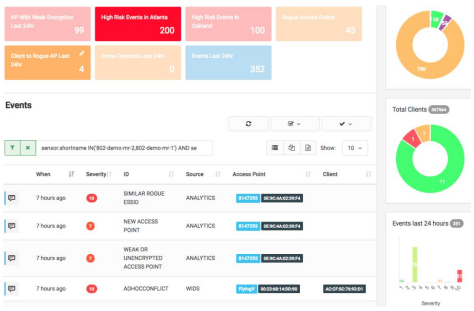
Bridging the Cyber Physical Security Gap

802secure

Fortifying IT & OT Networks from IoT Risks

Cyber Physical Security through non-intrusive wireless monitoring and protection that provides IoT asset visibility and cyber protection for both IT and OT networks.

Propelled by the need to consolidate management and create efficiencies, organizations are converging information technology (IT) and operational technology (OT) networks, thereby increasing the risk and complexity of these previously isolated OT networks. This convergence is referred to as **Cyber Physical Security.**



Combined with the the introduction of IoT-enabled devices with wireless capabilities, this evolution creates new risks to our buildings, infrastructure, and delivery of modernized services across healthcare, hospitality, critical infrastructure, manufacturing, and numerous other industries.

IT and OT Wireless Risks

1

OT networks are comprised of wireless Industrial IoT (IIoT) systems

802secure

802 Secure's AirShield

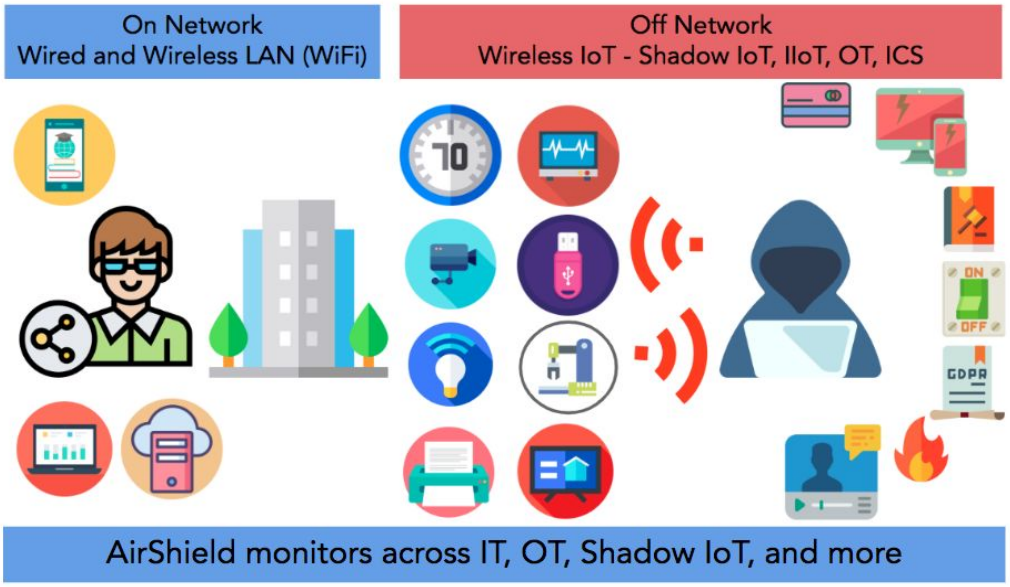
802 Secure's AirShield is an autonomous and non-intrusive wireless monitoring and protection solution that provides immediate visibility and cyber protection for both IT and OT networks.

AirShield provides scans across multiple wireless protocols and frequencies to detect wireless devices and networks and protect against misconfigurations, Shadow IoT, unknown and unmanaged IoT devices, and previously undetected wireless attacks.

AirShield protects the infrastructure from wireless and IoT wireless threats using wireless deep packet inspection, situational awareness, zero trust, anomaly detection, and behavioral analysis.

What makes it different

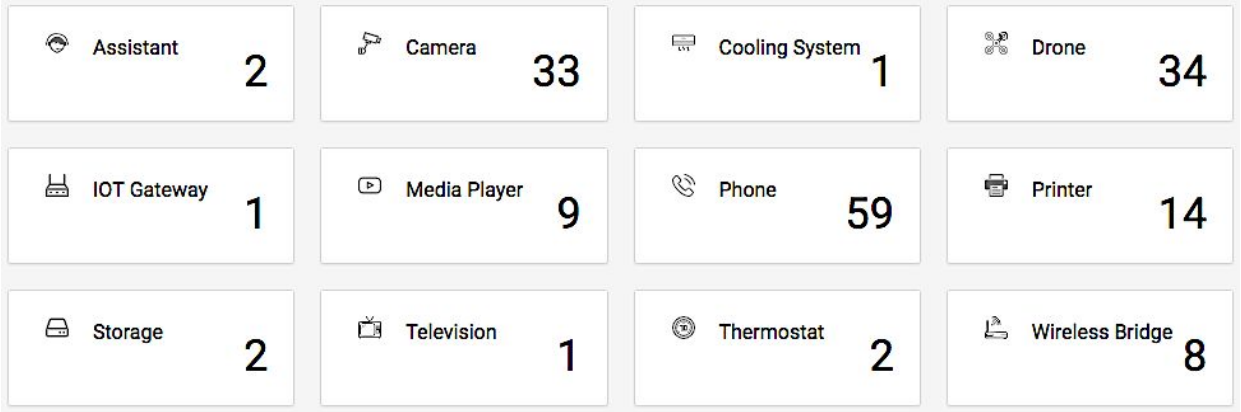
Beyond the network - Traditional WiFi vendors are focused on protecting their networks, not OT networks or Shadow IoT problems. This inflection point suggests that most organizations are blind to the IoT risks surrounding them. AirShield scans and identifies wireless devices and networks in your airspace to bring out the needles in the haystack and stack-rank the risks across IT and OT networks, as well as Shadow IoT.



802secure

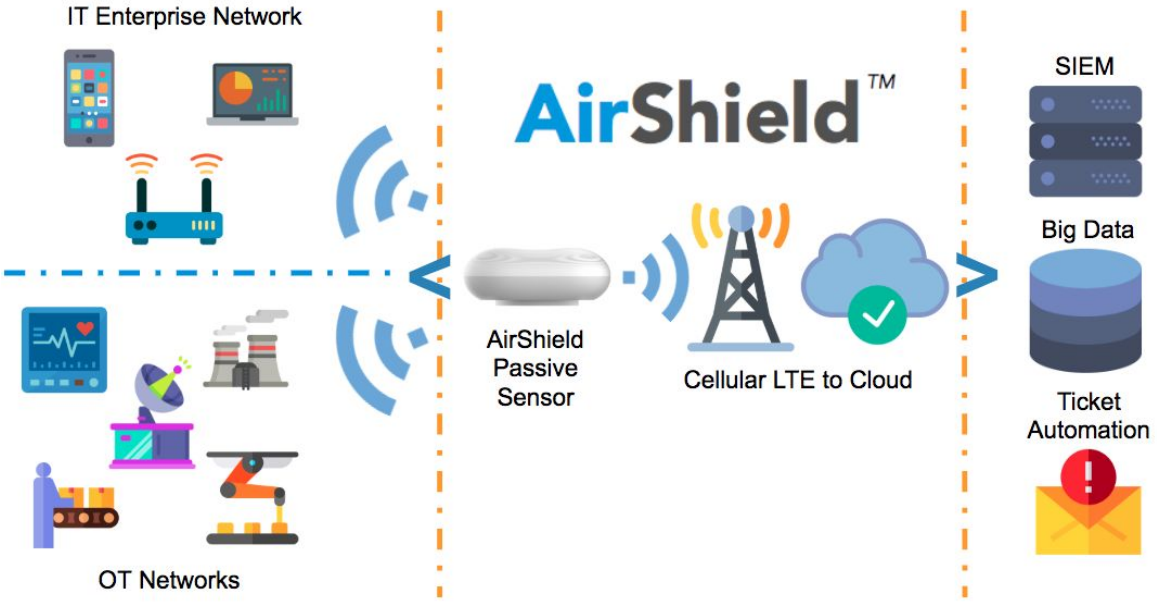
Beyond WiFi - Most IT organizations support WiFi today with their Wireless LAN. But now protocols such as Bluetooth, BLE, Cellular, Zigbee, and more have entered Manufacturing, Logistics, Building Automation, Security Surveillance, and Critical Infrastructure. 80% of IoT is wireless, therefore gaining visibility into these wireless IoT devices requires looking more broadly across the Radio Frequency (RF) spectrum and deeper into the protocols. AirShield looks at both the traditional IT WiFi networks for Rogues, but also Bluetooth, Cellular, and more to identify wireless devices and risks across other protocols and frequencies to bring visibility to IoT and IIoT wireless networks.

IoT Fidelity - Whether it's Shadow IoT and consumer devices or wireless-enabled IIoT, fidelity is key to identifying the type of IoT device or network so the information security team can assess risk. While traditional network monitoring products provide long lists of MAC addresses, Wireless Deep Packet Inspection (WDPI) is necessary to determine the actual device. For example, distinguishing between a Surveillance Camera vs. a Spy Camera greatly impacts the ranking of a risk within an organization. Where others leave off, AirShield's Wireless Deep Packet Inspection (WDPI) provides clear insights into the device thereby allowing categories of devices and networks sorted by Consumer IoT, IIoT, Automotive, Aircraft, and more. This uncovers "needles in the haystack" to uncover the high risk and unmanaged devices in the organization.



802secure

How it Works



Complete Wireless IT and OT Network Visibility Use-Cases

AirShield maps the Critical Path to Exposure™ to uncover IoT wireless devices, networks, and machine-to-machine communication risk. This industry-leading Wireless Deep Packet Inspection provides visibility, classification, and fidelity and enumerates risks including:

- Asset Visibility and Classification
- Asset Configuration Management and Security Posture Monitoring
- Remote Wireless Performance and Reliability Troubleshooting and Alerting
- Risk Management and Compliance including PCI, HIPAA, and NIST
- Data Loss Protection and protection against breaches
- Attack Detection and Zero Trust Policy Violations
- Threat Mitigation through Air Isolation and Deceptive Networking
- Incident Response and Forensics through DVR-like capabilities

Bottomline Benefits of IT & OT Asset Wireless Visibility

Airshield directly improves the bottomline of an organization through Cyber Physical Security visibility across IT and OT. Here's how we've helped customers deliver intrinsic value with AirShield:

- Identified data-center risk from new wireless thermostats following unbeknownst HVAC upgrades prior to exploit and potential for overheating entire data-center. Avoided potential for more than $1 million in losses per day.
- Automated remote wireless troubleshooting at an International Airport uncovering bandwidth issues, root cause, and missed SLAs by service provider. Money paid back by service provider for missed SLAs paid for AirShield within 3 months.
- Uncovered multiple risks for hospitality casino including spy cameras, drones, misconfigured Smart TVs, and unconfigured wireless thermostats and surveillance cameras. Reduced fraud, improved safety, and prevented public humiliation risks by an amount far to large to quantify.
- Enumerated multiple risks for a large hospital allowing the institution to ensure ongoing HIPAA and GDPR compliance and prevent a breach. AirShield uncovered employee wireless thumb drives and misconfigured wireless medical devices.
- Demonstrated immediate value to critical infrastructure customer with a drone issue, when AirShield revealed the drone, mobile device flying drone, and nearby Smart Vehicle allowing security to identify the perpetrator.

(1) Gartner, "IoT Solutions can't be trusted and out to destroy our enterprise", approved stats

Headquarters
802 Secure, Inc.
1285 66th St
Emeryville, CA 94608

More Information:
Web: www.802secure.com
Email: sales@802secure.com
Phone: 1-888-725-9434