Retail Solution Brief

Zero Trust Security for Retail Multi-Access Edge

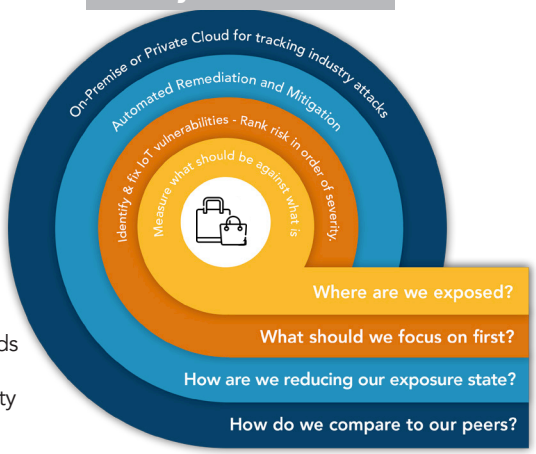
Retail is all about grabbing your fair share of the wallet. Digital transformation is revolutionizing every aspect of the retail industry and infiltrating every stage of the process, such as:

- Supply chain & logistics and Real-time inventory (scaling ahead of demand)
- Marketing (smart digital signage) and Associate enablement and communications
- Omni-channel customer engagement and customer behavior marketing
- Cyber-physical systems security
- Payment processing (self-service kiosks, interactive POS)
- Contactless pickup and delivery

In taking this systematic, digitized approach to sales and loyalty, retailers have built complicated webs of connected people, machines, and devices. What was once a transactional business process has transformed into a modern, highly digitized, real-time science serving customer needs for information, availability, assistance, security, privacy, and pricing. But even as these technologies drive optimizations in knowledge, logistics, velocity, and economics, they have also introduced pervasive security gaps and vulnerabilities throughout the product journey — particularly among wireless IoT devices.

IoT has created the world's largest attack surface, the scope of which is only broadening with exponential growth in deployment of 5G/LTE. Today's networks and organizations were never built to handle this extraordinary volume, velocity, and hyperconnectivity of IoT technologies in the Retail environment.

4 Key Questions...



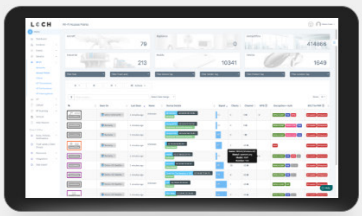
The LOCH Wireless Machine Vision™ platform provides next-generation wireless AI driven threat intelligence across 3G/4G and 5G deployments, broad-spectrum wireless IoT, Citizens Broadband Radio Service (CBRS) as well as 802.11/Bluetooth WiFi environments by providing customers with full IoT discovery, asset classification, risk analysis and actionable remediation capabilities based on a Zero Trust framework.

Cyber Threats Impacting Retail

- POS Attacks
- Inadequate Network Segmentation
- Rogue Cell Towers – covert data exfiltration
- Man In The Middle Attacks
- IoT Spyware

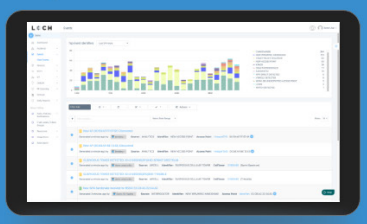
Solution Benefits

DETECT



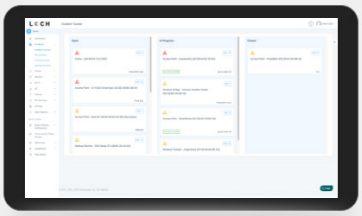
- Detect, identify and classify all broad spectrum RF emitting devices in range
- Device and network pairing communication map analysis and correlation
- Risk assessment threat ranking for Zero Trust network access control
- Mobile App for hunting rogues even if mobile

TRACK



- Wireless deep packet inspection
- Behavioral baselining, analysis and anomaly detection/alerts
- DVR-like capabilities for forensics, including geo-positioning
- Carrier integration with cellular devices for anomaly detection, fraud/ theft and cost management

REMEDIATE



- List and map devices on dashboard or directly into SIEMs.
- Interact with MDM and EMM assets for correlation and feedback on exceptions
- Rectify network segmentation via interactions with SOAR, FW and/or NAC systems
- Automate response and closure via collaboration with ITSM/ITSL and CMDBs

Rogue Cell Tower Detection - Prevent authorized devices from connecting to unauthorised cell towers

Detect and Prevent Evil Twin Attacks - Prevent authorized devices from connecting to unauthorised Wi-Fi Access Points

Roaming - prevent increase in data usage and excessive billing. Monitor potential data exfiltration against traffic base line to flag malware and bots.

Prevent Device Threats - Malware, Firmware Hacks, Sensor IoT Compromises, Man In the Middle Attacks, Device Tampering

Key Differentiators

- **Single pane of glass** to manage ALL wireless threats across cellular 3G/4G/5G, broad-spectrum wireless, CBRS and 802.11/ Bluetooth Wi-Fi devices
- **Early Warning System** - detecting threats before they hit the wired network
- **Edge IoT Vulnerability Scanning** to detect open ports and services to identify exposed threats before they are abused
- **Monitor Enforce Zero-Trust** Policies and "No Phone" Zones
- **Deployable** in air-gapped environments as well
- **API driven integration** with wide ecosystem for automated remediation and collaboration

Invisible Threats. Visible Protection

LOCH TECHNOLOGIES

Detect, Track and Secure IoT devices within your environment

LOCH Security for Retail IoT

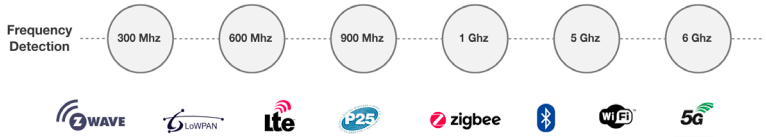
- **Wireless IoT Deployments:** In environments where Wireless/ RF is used for connectivity, LOCH is the single truth for device inventory. Any device that is emitting an RF signal, will be identified and located..
- **IoT Security:** Cybersecurity tools that manage such devices are based on network side solutions that use deep packet inspection and protocol dissection of flows from the subnets/ VLANs. LOCH's auto discovery will find devices that were missed due to incorrect subnet/VLAN configuration.
- **IoT Device Scanning:** LOCH solutions includes an 'outside-in', continuous edge vulnerability management solution to provide security validation of devices preventing misconfigurations of open ports, services and threats..
- **4G/5G Security:** In addition to traffic monitoring against established baselines for anomalies, LOCH can sense the presence of adjacent RF channels to thwart man-in-the-middle hijack attempts.
- **LTE Connectivity:** LOCH delivers the ability to monitor traffic from SIMs to alert on excessive use and changes in Device/SIM association.

Wireless IoT in Retail Environments

Wireless
The new invisible attack surface

LOCH Core Competencies for Retail IoT

- Software defined radios to detect broad spectrum RF
- Comprehensive classification of all assets in the environment and continuous Intrusion Detection
- Wireless Security Threat Research for rapid anomaly detection
- Decoding of IoT protocols
- Zero-Trust Policy Enforcement
- Rogue Cellular Tower and Stingray Detection
- API integrations for threat mitigation and remediation



Security Posture and Operational Efficiency for IoT Devices

- **Infrastructure** - Supplier to Warehouse to Shelf - Crucial for delivering the products, resources & services. Full RF protection.
- **Point of Sale Systems** - critical for productivity and efficiency. Ensure network segmentation and scan against loss of PII.
- **Digital Signage** – Ensure proper network segmentation and scan for unprotected side channel WiFi connections.
- **Network Infrastructure** – wired and wireless network correlation for misconfigurations that create blind spots for cybersecurity initiatives.
- **Sensors** – critical for facility and asset maintenance and customer experience tracking. Ensure proper segmentation and access.
- **Surveillance Cameras** – Ensure proper segmentation and eliminate potential exploitable backdoors that can lead to lateral attacks.
- **Rogue Cell Towers** – Validate 4G/LTE/5G or Private LTE communications for exfiltration and/or malware/process injection.

info@loch.io | 1-888-725-9434 | www.loch.io