LOCH TECHNOLOGIES

Retail Solutions

Managing Cyber Security
In The MarketPlace

loch.io

Retailers around the globe are continuously orchestrating a complex series of events. Digital transformation is revolutionizing every aspect of the retail industry and infiltrating every stage of the process, such as:

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

In order to win in today's environment, where a retailer's nearest competitor for share of wallet is as far away as their customer's phone, companies must provide a hyper-coordinated digital experience that drives value to the shopper at every step of the buyer's journey. Retailers must have the right product, in the right place, at the right price, at the right time, or they lose.

When they do these things, not only can they win, but they can start to take the wheel for the rest of the consumer journey and make recommendations and up-sales that drive increased basket sizes stickiness through hyper relevance, support, and repeat business for products and services.

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

> "Having responsibility for all aspects of information security across a retail environment today is a challenging task. With more devices embracing IoT wireless, it's hard to know what data is being transmitted without purpose-built, full-spectrum wireless monitoring. This is one of several reasons why we're evaluating LOCH's solution to help provide wireless IoT visibility, asset discovery and risk analysis for actionable data in securing our infrastructure."
>
> — Terrence Weekes, Chief Information Security Officer

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.

Receiving: Inventory is processed at the receiving dock using wireless handheld inventory scanners and mobile computing devices leveraging embedded Wi-Fi or 4G/5G. Scanning those items into inventory triggers inventory availability alerts to the merchandising or planning team and initiates the workflow for stocking or shelving. Often, these products are RFID tagged to help accelerate the intake process.

Inventory Management: Once received, items become inventory and are placed into stock for merchandising planogram coordination. Traditionally, work orders are generated and broadcast to store associates through handheld mobile devices or forklift-mounted tablets via Wi-Fi or 900MhZ. Workers use these soft orders to pick up pallets and products from the receiving dock and backstock and place them in their pre-assigned locations on the store floor.

Advantages of Digital Transformation for Retail:

- Lasting customer relations, in-store or online
- Optimized operations, from supplier to cart
- Multi-dimensional convenience — faster offerings and new ways to shop
- Higher revenue — one local click to a global marketplace

Video surveillance: Back-of-house intake and stocking processes, front-of-house cash lanes, and the store floor are all monitored with video surveillance cameras to minimize shrinkage, enforce OSHA policies, and verify inventory receipt and shelf stowage locations. These video systems operate on a variety of different radio frequencies. Protecting the consumer's privacy and also the brand of the retailer while enforcing video surveillance requires protecting the cameras from hijacking and quickly eliminating rogue devices.

Locationing: Location-based services can drive guided shopping experiences and optimize the capabilities of in-store associates by tracking the locations of products, customers, and associates and their individual routes through the store, at all times. When these three elements come together, customer satisfaction tends to increase dramatically, while driving greater in-store sales or basket sizes. In-store, location-based services are rooted in wireless technologies such as BLE, ZigBee, Wi-Fi, Bluetooth, and others.

Payment: Retailers are finding that, by offering more payment options to customers, they can improve the customer experience, increase the likelihood of developing repeat customers, and accelerate the check-out process. Mobile Point of Sale (mPOS) solutions are the cornerstone of the field of emerging payment options — enabling POS terminals to move to new/seasonal and random line busting locations or providing mobile device-based payment options at the point of product selection.

Energy Management & Building Automation Systems: As the entire retail brick and mortar environment becomes highly sophisticated, hyper-connected energy management and building automation controls systems are driving operational expense savings in the store. Facilities of retail size and scale burn a tremendous amount of energy, and intelligent systems can maximize retailers' savings and conserve energy spent on heating, ventilation, refrigeration, cooling, and lighting. These systems are typically wirelessly enabled for ease of installation and movement to optimal locations, leveraging a variety of technologies and protocols.

Wireless devices, often known as **IoT** (Internet of Things), **IIoT** (Industrial Internet of Things), and **OT** (Operational Technology), comprise broad and comprehensive sets of tools and systems that are pervasive across many areas of the retail ecosystem:

Know immediately if an adversary has compromised one of your IoT devices

The Challenge and the Opportunity

Today, it is more common than not that associate workflow and customer facing systems, tools, and devices are wirelessly enabled. Moreover, most of these technologies have a low-level of intelligence attributed to their network interface.

Many of these smart devices communicate outside of retailers' primary production network — meaning, over cellular or other LPWAN near field communications — to transmit stateful maintenance and supply information to their manufacturer or their service partner company. As a result, retailers have little to no visibility control over the smart device, wireless IoT, or third-party communication segment of the retail environment.

> "The threats are obviously becoming more sophisticated... the way we work is very different than other industries, and the way we worked a decade ago. While that presents great opportunities, it also raises the stakes of the game. That's why we need to work together."
>
> ~ Alison Kenney Paul,
> Vice Chairman and US Retail & Distribution Leader, Deloitte LLP

So, what's the big deal? Simply put, you can't manage what you can't see. When a device is broadcasting and receiving information about your environment, whether it sits on your production network, your payment network, or over cellular, it is sharing critical data about you — information that can be used against your company, your suppliers, and your customers. If that same vulnerable device is also connected to your network, you could be in real trouble.

Despite the ubiquity of these new and non-standard wireless devices, the vast, overwhelming majority of organizations view network security through the traditional lens of network and endpoint. Organizations put technology in the rack to filter data and protect network infrastructure. They invest in endpoint products to protect the Windows, Mac, Android, and iOS-based devices with which they are familiar.

What they miss, however, is the rapidly increasing number of third-party devices that lack either the computing horsepower or the OS to run an endpoint protection application. Furthermore, these devices are not considered part of the wireless infrastructure, because they are tethered to, or embedded in, commercial equipment and operating on alternate frequencies with non-standard protocols. The result is that retail organizations simply can't see, manage, or control these devices.

$6 TRILLION
Global cybercrime damage by 2021

156 MILLION
Phishing emails sent every day

91%
Cyberattacks are seeded by phishing emails

36%
Increase in ransomware attacks in 2017

44%
Cyberattacks go unnoticed

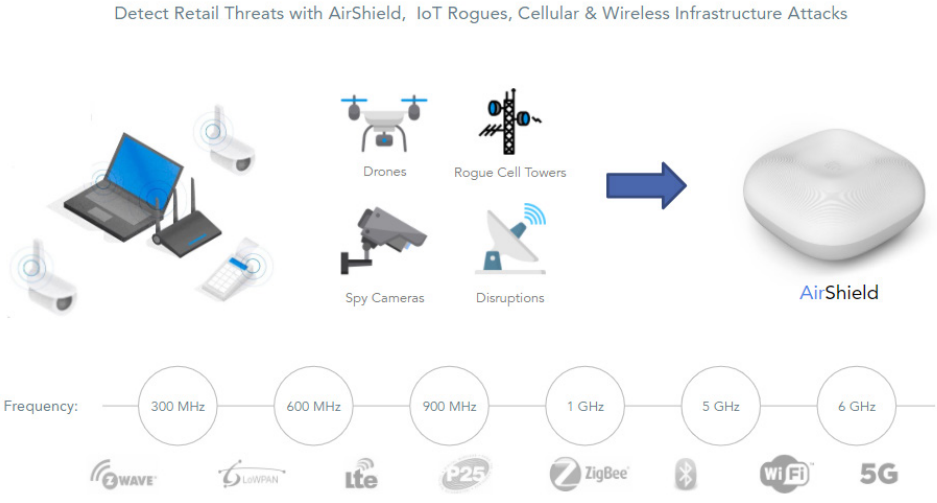
For example, if a wireless video camera operating over Wi-Fi is plugged into the network on the managed wire, but also has an embedded 4G/5G connection to a monitoring service, this is a security "blind spot" for the organization that nonetheless presents a real cybersecurity vulnerability. Other examples: a traffic counter or an energy management system that is plugged into the network, but which also has an embedded Bluetooth radio broadcasting for ease of integration with a third-party service app. In any of these scenarios, the organization faces a potentially critical risk.

Frequency of Cyber Attacks in Retail

The Verizon DBI Report, an authoritative source on retail cyber attacks, noted 234 incidents of breaches against retail companies in 2019, with 139 confirmed cases of data disclosure. Web application attacks and misuse of privileges were the two leading attack categories. Perhaps unsurprisingly, 81% of the threat actors were external to the affected companies, and the motivation was financial in 97% of all cases. All in all, 64% of compromised data was payment information.

In response to the increased IoT attack surface and the costs relating to data breach analysis and resolution — approximately $3.86M per incident — retailers are now looking for new ways to detect, assess, and prevent risk, before any data loss or incident occurs.

The new security challenge is that, unlike traditional network infrastructure and endpoints, today's retail environment may contain hundreds or thousands of somewhat known or unknown wireless probes, sensors, and transmitters — none of which are owned, operated, or managed by the networking team, but all of which may represent a potential entry point onto the network.



The fly in the ointment is that, in order to gain unwarranted access, all a bad actor has to do is steal the credentials of a low-end service radio, associate with the equipment and pretend to be that device, and tunnel their way through the equipment's wired connection to your network. These hacks can be perpetrated in-person, with a small leave-behind device, or, for instance, from an adjacent facility or parking lot.

Protecting Retail IoT with the LOCH Wireless Machine Vision™ Platform

We built the LOCH Wireless Machine Vision™ Platform to help organizations find and remediate these risks and vulnerabilities. The LOCH platform monitors everything in the RF environment and makes all of the previously invisible activity surrounding your corporate assets and facilities visible. Once we reveal these devices and threats, you can begin to manage them — creating and enforcing policies to protect your most critical assets, while ensuring that you suffer no unplanned production downtime due to nefarious wireless activities.

Moreover, as cellular performance increases and costs decrease, many of these wireless devices are now cellularly enabled. With the hyper-proliferation of 4G/5G devices now entering retail environments, unplanned and unexpected behavior anomalies through policy violations and/or security breaches are beginning to have a significant impact on unplanned date overages as a result of device abuse.

The LOCH platform is able to baseline expected device usage through zero trust policy mapping and by providing alerts for deviations to policy or excess usage abuse. As a result, organizations can take proactive action to adjust their data plans and avoid unexpected cost overages.

Digital Threats Impacting Retail

POS Attacks - POS or "point-of-sale" attacks are especially popular with cyber criminals, because the POS system contains some of the most sensitive data possible — the card numbers and PINs of the company's customers.

Web Application Attacks - Attackers will attempt to breach a company's online payment application, then install malicious code designed to steal the customer's credit card information as they enter it.

Insider Threats - As always, these are a common threat to retail companies, as employee turnover can be high and there are points of vulnerability.

Cookie Theft / Sidejacking / Session Hijacking - A cookie theft is exactly what it sounds like: a hacker exploits an insecure connection to steal your cookie and pretend that they're you on the website you're visiting.

Fake/Rogue Cell Tower - As wireless devices may have cellular access, an attacker may want to ensure cellular access is unavailable while performing Wi-Fi attacks. To accomplish this, they create fake cell towers and deny authentication to the network.

Downgrade Cellular Network: Attacks against weaker cellular networks require disabling more secure networks, allowing for man-in-the-middle attacks or enabling them to install trojans.

Evil Twin AP: Here, an attacker creates an access point and draws devices towards it through a higher signal power and/or existing network deauthentication. Connected devices may either expose their credentials or be directed to malicious services for system compromise.

Weak Authorization: Retail networks may be set up to use (WPS) WiFi Protected Setup. As a result, access codes to many devices are well known or easily brute-forceable, which allows an attacker access to the network.

Weak Encryption: Retail networks may not follow strong and required network security practices by using common/easily recovered WPA/WPA2 passphrases, or unencrypted or known weak networks.

Rogue Devices: A rogue device, such as a spy camera, wireless-enabled USB drive, or an open printer may put the remote home user/network at risk.

Misconfiguration - Excessive data usage can lead to uncontrollable costs.

IoT Rogue - Rogue communication and data exfiltration.

SIM Port Hijack - Loss of control over your SIM connectivity.

Cellular Attacks - Malware, DDoS, and BOTNETs can lead to excessive device utilization and data exploitation.

Roaming - Increases data usage and billing costs.

Thinking About Cybersecurity

LOCH enables retail companies seeking to protect themselves from cyber attacks to implement the following strategies:

Asset Discovery - You can't defend what you don't know, so continuous, non-intrusive asset discovery is key.

Risk Analysis - Identify and fix vulnerability exposure states, prior to loss or incident occurring.

Risk Mitigation - Implement a solution that is dynamically in-tune with the ever- changing retail environment.

Event Detection and Response - Project your threat feed into adjacent security ecosystems.

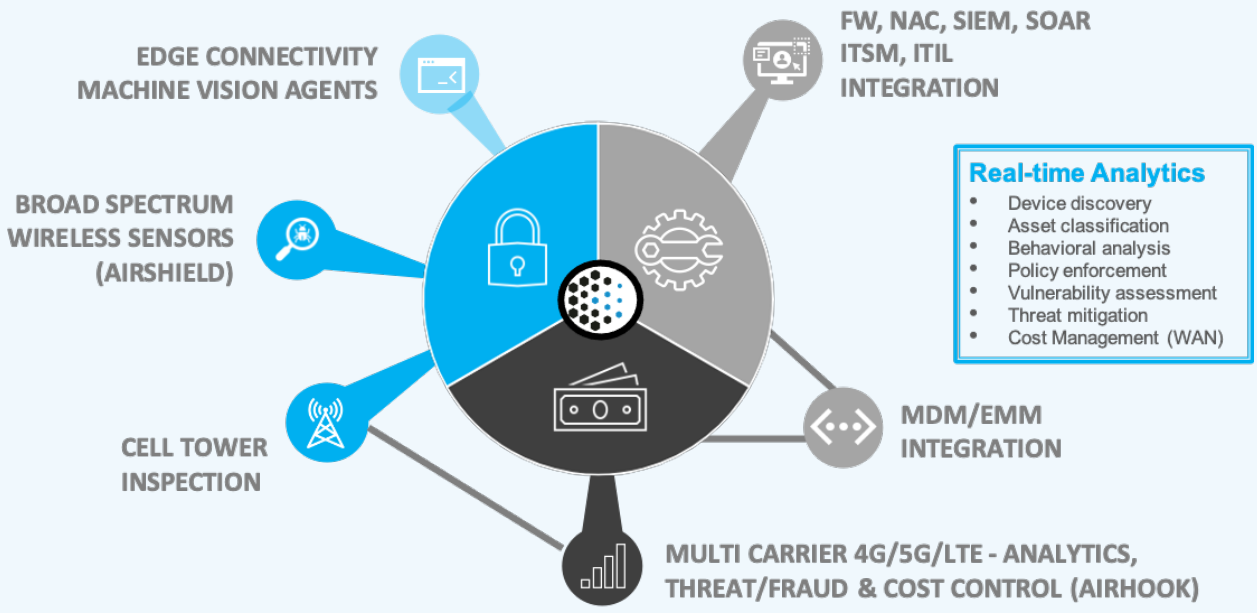
Device Analytics - Monitor your cybersecurity performance.

Bringing Wireless Security to Retail Environments

LOCH helps bring order to this world of wireless chaos. With its patented **Wireless Machine Vision™** platform, LOCH provides full proactive management and security for all 5G and IoT environments. Every connected device needs to be visible, manageable, and secure, regardless of the type of device, the protocol it uses, and who owns it.

Whether for 4G/5G, broad-spectrum IoT wireless, or private LTE environments, LOCH helps customers manage security, performance, and cost for the full range of wireless devices.

By providing full visibility and actionable intelligence on all devices, LOCH enables organizations to confidently embrace the new world of wireless innovation that is driving the next generation of digital transformation.



Support for Hyper-WAN (5G) Environments

Without real-time visibility, monitoring, and active management for 5G wireless devices, enterprises have no way of managing the risk and costs associated with them. There is no way, for example, to predict data usage, monitor device policy and behavior, or detect and remediate real-time threats to the environment.

To address this, the LOCH AirHook service provides real-time visibility and comprehensive security, performance, and cost management for 5G cellular devices across all carriers. AirHook feeds discovered information into the LOCH platform.

The AirHook service reports into the LOCH Wireless Machine Vision Platform™ for centralized management and reporting.

About LOCH Technologies, Inc.

LOCH is a global leader of next-generation wireless threat monitoring. The company provides actionable intelligence on all 5G cellular and wireless IoT devices to help organizations improve their security posture, reduce risk, and manage wireless data usage across the enterprise.

Every wireless device needs to be visible and secure, regardless of what type of device it is, what protocol it uses, and who owns it.

This guides everything we do and why LOCH aims to secure and enable the new world of wireless innovation that will drive the next generation of digital transformation.
For additional information, please visit us at www.loch.io

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