Harmony IoT: Wireless Airspace Security for Smart Retail

Harmony IoT – Securing Smart Retail

Harmony IoT is a complete airspace security solution that delivers visibility, continuous monitoring and real time attack mitigation. What makes it different from standard NAC and MDM is it monitors the airspace rather than devices. This gives Harmony IoT the power to see all devices (store owned, customer owned, managed or unmanaged) and take action based on what the devices are doing or attempting to do. It has a policy engine that protects customers from connecting to malicious hotspots and can ensure in-store devices are configured to meet wireless security standards.

Finally, Harmony IoT is non-invasive: It is an out-of-band solution that requires no changes to the network. That means rapid time to implementation and low TCO, and its cloud based central management makes it ideal for single or multiple store deployments.

The retail business is highly competitive. Retailers are under constant pressure to find cost efficiencies but they also must adopt new ways of making the customer experience more appealing and engaging. Smart, wireless technologies are transforming retail operations to meet these challenges. However, this transformation is exposing retail businesses to new, wireless based cyber-attacks. Traditional security tools do not monitor or control activity over the airspace, leaving smart retail exposed to data breaches and ransomware. Harmony IoT is a comprehensive wireless airspace security solution that delivers visibility, policy control and attack defense for the smart retail environment.

OPEN AIRSPACE, OPEN APPLICATIONS

Most businesses control who may enter their premises and limit what devices visitors can use. Retailers on the other hand are fully open to the public. In smart retail, customers are encouraged to interact with multiple wirelessly enabled applications that enhance the shopping experience. Wireless applications are also key to automation and cost control, such as inventory management and point of sale.

The open airspace makes it easy for customers to check prices, get in-store promotions and use free Wi-Fi. It also makes it easy for attackers to compromise customer devices as well as the IoT and other devices that support smart retail. Attackers also have access to the IoT devices that manage store operations (HVAC systems, printers, PoS, asset and inventory tracking). Some of the largest data breaches in retail history started with IoT devices.

Current security tools such as traditional NAC (network access control) systems and MDM (mobile device management) were not designed to solve these security issues. They lack visibility into unmanaged devices operating in the airspace, are unable to monitor airspace traffic and cannot detect and stop many airspace attacks.

Harmony IoT: Comprehensive Airspace Security

Visibility
- Device discovery
- Device type
- Manufacturer

Monitoring
- Connections
- Disconnections
- Location
- Anomaly detection

Policy
- Authentication
- Encryption
- White list
- Black list

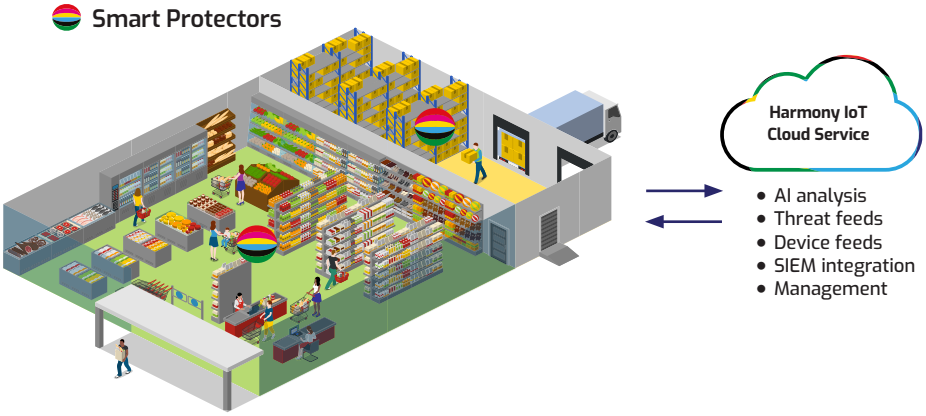
Enforcement
- Events
- Alerts
- Sensitive area protection

Audit and Reporting
- Event logs
- Compliance and audit reporting
- Airspace security hygiene

HOW IT WORKS

Harmony IoT is a cloud managed solution comprising small sensors (Smart Protectors) that monitor the retail airspace. The sensors use information from the data link layer to monitor and secure the airspace. They do not collect any sensitive or confidential information. Each Smart Protector processes large amounts of data locally and sends a much smaller volume of meta-data to the Harmony IoT cloud service for analysis and reporting.

The Harmony IoT cloud service is an AI/big data system that continuously learns from all Smart Protector deployments. Harmony IoT identifies what is normal/suspicious in terms of device type as well as what is normal/abnormal behavior in the context of each customer environment. Unlike signature-based systems which are easy to defeat, Harmony IoT identifies and mitigates attacks even as attackers evolve their methods to escape detection by traditional WIPS (wireless intrusion prevention systems).



Hackers have a variety of techniques for compromising in store devices like PoS kiosks

Harmony IoT policy enforcement (e.g. whitelisting, attack detect/block) prevents tampering with PoS and other in-store devices.

FEATURES AND BENEFITS

Full Visibility
Detects what devices (device type, manufacturer, model) are present in the airspace - regardless of what network they belong to, or even if they are attached to a network.

Continuous Monitoring
Records when devices appear and disappear from the airspace, attempts to attach to a network (SSID), attempts to establish an access point or network, suspicious activity, and anomaly detection.

Policy management
Set and enforce security standards such as Wi-Fi encryption and authentication standards, what is allowed by location, device type, time of day/day of week. Device white and blacklisting.

Restricted Area Policy
Only known, trusted devices are allowed in designated areas such as warehouses.

Alerts and Mitigation
Mitigate attacks in real time. Mitigations can be automated or under operator control. Mitigations are immediate and target only the offending device.

Location Sensing
Harmony IoT reports on the location of every device operating in the airspace. This makes it easy to pinpoint the location of any offending device, drastically reducing the time to fully mitigate.

Compliance Reporting
Harmony IoT generates compliance reports that expose issues needing attention and provide assurance that compliance policies and security mandates for the airspace are being met.

Out-of-Band
Harmony IoT passively monitors activity in the airspace and weeeeeeeeneeds no connection or resoureeeeeeeeeeeeeces from the host network. It requires no internal resources (IP addresses, DNS, software updates etc.) from IT operations staff.

Orchestra Group is a privately held company led by top cybersecurity and data-science experts. Our Harmony IoT solution protects retail, financial institutions, banks, data centers, governments, healthcare organizations, manufacturing facilities, defense contractors, and SCADA companies. Visit us at www.orchestragroup.com