HARMONY IoT
BY ORCHESTRA GROUP

Harmony IoT: Complete Wireless Airspace Security

Industries We Protect

Manufacturing
Auto manufacturer uses Harmony IoT to protect IT/OT assembly plant.

Health Care
A major health care provider protects clinics and medical devices from wireless attacks with Harmony IoT

Government
Harmony IoT protects embassies from wireless surveillance, bugs and data theft.

Travel/Hospitality
Harmony IoT protects visitors to trade shows, airports, and other public venues from wireless attacks.

Financial Services
Harmony IoT protects banks, insurance companies and other financial institutions from wireless threats.

The use of IoT devices has exploded in recent years. Because IoT devices are often connected to both the wired and wireless worlds of private networks, they create a bridge from one to the other. This bridge is easily exploited, giving attackers enterprise-wide access to critical systems, sensitive data and processes. Most enterprises lack adequate network security in their wireless airspace. Harmony IoT plugs that gap. Harmony IoT is a non-invasive, light footprint solution that establishes strong security safeguards in the wireless airspace.

THE NEED FOR WIRELESS AIRSPACE SECURITY

The security architecture of most enterprise networks is "wired centric". This architecture, comprising firewalls, IPS and end point security, comes from an era before widespread use of wireless technology. Today, wireless is pervasive. Wireless and IoT are central to critical business processes (industry 4.0, medical IoMT, logistics, etc.). Many enterprises now host more wireless end points and IoT devices than wired, but security has not kept up with this change.

Security tools such as traditional NAC (network access control) and MDM (mobile device management) lack visibility into many IoT devices and do not monitor activity in the airspace. They also lack policy and enforcement controls over airspace activity. Harmony IoT monitors and protects the airspace. It prevents attacks from disrupting critical business processes, and it stops wireless attacks from breaching the wired network.

Harmony IoT: COMPREHENSIVE AIRSPACE SECURITY

To be effective, airspace security must be comprehensive. It must provide visibility into all devices (managed and unmanaged) operating in the airspace, continuously monitor all activity, and like a firewall, provide policy management, enforcement, and reporting. It must mitigate attacks in real time, before damage is done. Harmony IoT does all that, and it is intuitive and easy to use. 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.

Visibility
- Device discovery
- Device type
- Manufacturer

Monitoring
- Connections
- Disconnections
- Location
- Anomaly detection

Policy
- Authentication
- Encryption
- White list
- Black list

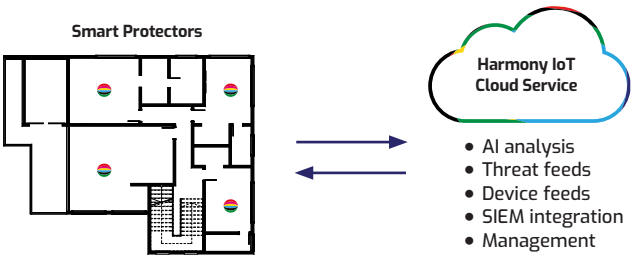
Enforcement
- Events
- Alerts
- Sensitive area protection

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

HOW Harmony IoT WORKS

Harmony IoT is a cloud managed solution* comprising small sensors (Smart Protectors) that monitor the airspace and send data to the Harmony IoT cloud. The sensors use information from the data link layer to secure the airspace. They do not collect information from the higher layers of the network stack that contain sensitive/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 for analysis and reporting.

The Harmony IoT cloud is an AI/big data system that continuously learns from all Smart Protector deployments. Harmony IoT identifies what is normal/suspicious based on device type as well as what is abnormal within the specific 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).



SECURITY CAPABILITIES AND ATTACK PROTECTIONS

- Evil Twin, Karma, Dogma attack detection and prevention
- Unauthorized hot spot prevention
- Rogue or suspicious AP detection
- Man-in-the-Middle prevention
- Detects use of open connections and weak encryption
- Detects weak authentication
- Detects unknown devices
- Vulnerability detection
  Insecure configuration detection
- Device whitelists, blacklists
- Location reporting
- Protects high-sensitive areas

FEATURES AND BENEFITS

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 corporate network.

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

Anomaly Detection
Reports and alerts on suspicious and unusual activity.

Policy Management
Sets and enforces security standards for encryption, authentication standards, device type, what is allowed by location, device type, time of day/day of week. Enables device whitelists and blacklists.

Restricted Area Policy
Only known, trusted devices are allowed in designated areas such hospital operating rooms, manufacturing floors, high security office spaces.

Attack Mitigation
Mitigates attacks in seconds. Mitigations can be automated or under operator control. Mitigations target only the offending device with no impact on other devices or processes.

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 and reduces time to fully mitigate.

Compliance Reporting
Harmony IoT generates SS-019 wireless security standard compliance reports. It highlights issues needing attention and enables assurance that security policies and mandates for the airspace are being met.

Out-of-Band
Harmony IoT passively monitors activity in the airspace and needs no connection or resources from the host network. It needs no network administration overhead for set up and operation.

*on prem available

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