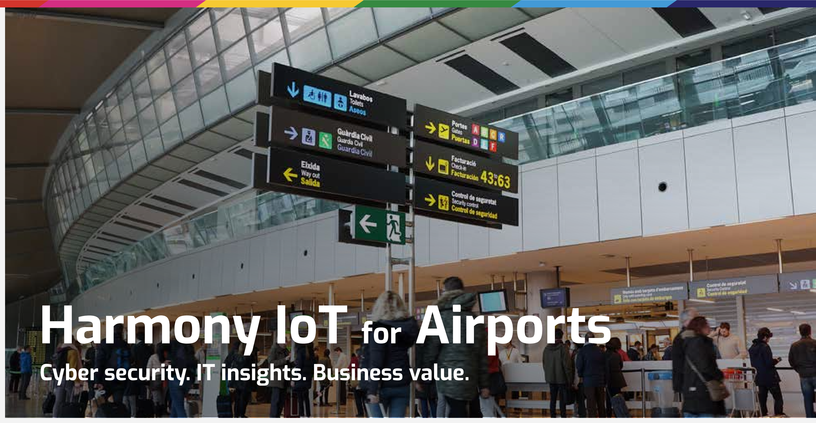


Harmony IoT for Airports

Cyber security. IT insights. Business value.

Wireless networks are both invisible and ubiquitous. Most organizations are blissfully oblivious to the activity in their airspace, but no other on-premise technology is as vulnerable and risky as wireless.

No matter whether the network access point provides corporate or guest-only access, is on-premise or across the street – employee and guest mobile devices are exposed. As the PCI guidelines explain, organizations need to protect against attacks by rogue or unknown wireless access whether or not the wireless technology is part of the corporate network.

These issues are compounded for airports – businesses that host thousands or hundreds of thousands of visitors every day, each with their own devices and vulnerabilities. Many offer guests free or paid access through their own facilities or third-party providers. Whether the access is in-house or outsourced, managing the airspace provides both challenges and opportunities for airports:

1. CYBER SECURITY
- Protect guests and employees from wireless (wifi and bluetooth) attacks that deny service, extort money, spread panic and misinformation, or steal credentials.

2. IT INSIGHTS
- Visibility and control over networks and devices in the airspace.
- Compliance with Wireless PCI guidelines for organizations that store, process or transmit cardholder data – a PCI guideline even when there are no wireless access points directly connected to the cardholder data environment.

3. BUSINESS VALUE
- De-personalised data from mobile can provide statistical guest flow information including locations and movement to improve customer service and generate revenue.

Harmony IoT provides the most robust solution for airspace threat prevention.
Contact us at info@orchestra.group for more information or a demo.

HIGHLIGHTS OF THREATS DETECTED ON CUSTOMERS SITES

Example 1: Incident Cy-INC-932

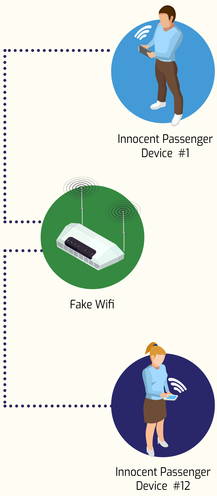
"ROGUE ACCESS POINT" ATTACK

The network "FreeWiFi" (c4:72:05:81:28:71 ; Cisco device ; OPN) is a network operating on-premise. It appears to be a legitimate access point offered by a Mobile Operator for its customers, like in many places in North America, except this one isn't a legitimate Mobile Operator access point. It is a malicious hotspot disguising itself as a legitimate access point to get people to connect to it. "FreeWiFi" is a very well known network in North America and is used by millions of people.

It is also a saved network in many devices and is specifically saved on every mobile device sold by the Mobile Operator in North America. This makes every device that sees that network to automatically connect to it. In the case of a legitimate network, that is great.

In this case however this network is malicious and any device connected to it is under great risk. The system detected 12 victim devices connected to this access point.

We have confirmed with the Mobile Operator that this is not their network, but a malicious one.



THREATS & CONSEQUENCES
- Sensitive data theft from devices through network sniffing
- Privileged credentials theft through phishing and man-in-the-middle network attacks to be used to access high priority assets
- Malware infection of devices through network exploits for complete remote control over the device

Example 2: Incident HiT-INC-857

POSSIBLE MALICIOUS DEVICES

Three suspicious Wi-Fi antennas were detected on-premise. These external antennas, made by Alfa and Panda, are a favorite among wireless hackers as they allow for special operation modes that facilitate wireless attacks, alongside extended wireless signal.

These devices are marked by Harmony IoT as high-risk as they are usually used by hackers and are closely monitored by our sensors. No malicious activity was detected from these devices at those times.

THESE DEVICES ARE:
- 00:c0:ca:63:e6:d6 (Alfa device) connected to 16 different access points.
- 00:c0:ca:91:c8:dd (Alfa device) connected to 38 different access points.
- 9c:ef:d5:a8:81:7c (Panda device) connected to a single access point.

THREATS & CONSEQUENCES
- These devices facilitate many wireless attacks and should be tracked closely.