HARMONY IoT

Cyber Of Things

# Harmony IoT vs. WIPS

# Products compression

October 28th, 2019

By ORCHESTRA

Confidential

The comparison between Harmony IoT solution and WIPS is not really a comparison as they are completely different solutions.
Harmony IoT delivers an enterprise-grade defense for your airspace that protects valuable digital assets from IoT-born attacks.

WIPS is a simple solution that protects only against a few known Wi-Fi attacks that are interfering with the Wi-Fi protocol. These are very naive kind of attacks and no serious attacker would even use these known attacks. Regardless, WIPS doesn't really do the job but even if it were successful (it is not, and we will explain why below) this is a very small subset of the protection required by today's enterprises in the world where we have billions of IoT and connected devices.

All of these devices (IoT and connected devices) that surrounds the enterprise pose a real threat, an attacker can (and we already have real examples) easily gain access to them through their cloud service or by connecting to their management interface or through neighboring public wireless networks or directly to them without going through the enterprise network at all. They can even come from the factory infected!!

Once the attacker gains access, he can penetrate the network (no need for any "Wi-Fi" attack) and can for example, infect other devices in the network or start to leak data out of the organization through public networks while still "adhering" to the standard Wi-Fi Protocols. Not to mention that now modern IoT and connected devices have more protocols such as Bluetooth and can use those to gain access to company assets.

In today's smart connected world, you need to continuously monitor all devices, build a behavioral profile over time and based on sophisticated analysis to detect malicious pattern behavior which you can't know ahead of time (zero day) and most importantly they might not interfere with the standard Wi-Fi protocol.

That being said, WIPS protection (like its "cousin" IDS/IPS) is still lacking which is derived from how its built and results in high number of false alarms.
In today's noisy wireless and connected world (everything today talks wireless) WIPS simply creates so much alerts (due to its simple rules that aren't updated) that it would be turned off and most importantly it doesn't cover attacks that aren't "interfering" with the Wi-Fi protocol.

The threats that Harmony IoT will keep you safe from are outside the scope of the WIPS domain.

Harmony IoT solution protects the enterprise from any malicious activity done by an offending device and not only on the integrity of the protocol it uses. It continuously monitors behavior through the wireless and employs A.I logic to all historical data of the organization. Furthermore, the technology and patents developed by Harmony IoT provides

the organization with a 360◦visibility of the organization airspace including every device and network belonging or not to the organization. Harmony IoT cloud service is another important aspect as it learns malicious activities and patterns from millions of devices and sensitive organizations all around the world and updates all of its sensors with new models instantly.

**You need a different solution that would keep your enterprise safe in today's smart connected world. YOU NEED Harmony IoT.**

Below are a few more attributes of Harmony IoT solution and how WIPS is lacking:

1. **Coverage** – The ability to cover the enterprise airspace and its surrounding so that there are no blind spots.
+ Harmony IoT's solution is able to cover 100% of the wireless airspace in and around the enterprise.
- WIPS are integrated into the access point, and so they are only installed to cover access point reception. This gives extremely limited coverage of wireless defense and leaves the organization blind-sided to attacks it can't see.
2. **Location** – The ability to localize where the threat is. So that response can happen in a pinpoint accuracy and also for the IT/SOC team to be able to locate the offending device.
    + Harmony IoT's solution deploys it sensors to cover the entire airspace in and around the enterprise. They are able to locate the threat and provide accurate detection of the attacking device due to Harmony IoT patent-pending Wi-Fi-based localization algorithm.
    - WIPS – No Support
3. **Independency** – no dependency on existing IT infrastructure, agentless and out of band.
    + Harmony IoT operates completely independent of the enterprise existing infrastructure (out of band). It provides end-to-end solution including smart visibility, proactive threat detection and real-time attack mitigation without any dependency on existing customer IT infrastructure.
    - WIPS are part of the enterprise existing infrastructure; usually they run over high-end access point equipment (requiring multiple antennas) which also makes the solution expensive and creates high-load over these access-points.

4. **Intelligence** – The ability to understand and learn each specific environment including being able to detect new emerging threats and zero-day malicious behaviors.
    + Harmony IoT's solution uses advanced behavioral analysis and anomaly detection algorithms in order to detect sophisticated attacks, both known and unknown. The solution embeds distributed machine-learning technology allowing each of the deployed sensors to continuously learn and adapt to their environment. In today's world, each enterprise air-space is very 'noisy' (devices carried by employees, guests, contractors, neighbor's offices, public transportation, passing-by pedestrians etc.). Many enterprises have millions of devices in their environments and therefore need a solution that can see, learn, understand and most impotently protect from any of those devices. Harmony IoT solution combines

distributed machine-learning (sensors) and big-data analytical engine in order to do just that, i.e. keeping the enterprise safe in a smart-connected world.
    - WIPS relies on signatures to detect only known attacks. This is a highly ineffective defense mechanism, as changing a single bit in the attack vector can bypass them with ease. Furthermore, WIPS has no learning capability and therefore will only see "noise" in today's world effectively leaving the enterprise blind and unprotected.

5. **Accurate Detection** – Detecting Attacks, Malicious behavior and Policy breaches with high accuracy.

+ Harmony IoT's solution produces high-fidelity alerts relying on its unique data-science engines and algorithms and combining positive and negative security models which combines known attacks models with known malicious behavior to provide the most accurate threat detection solution. The solution combines location information, profiling of device behavior (connectivity, data transfer patterns etc…), known attacks, known malicious behaviors, abnormal deviation from device norm and many other factors to accurately detect whether the device is now attacking or under attack.

- WIPS inherently produces a high rate of false-positives. Cisco's own documentation has a section called "Alarms to turn off or ignore"(1). This causes a lot of customers to not only ignore potential breaches, but also to turn off automatic mitigation features due to the device mistaking the corporate network as malicious for example, and actively blocking it, causing business downtime. WIPS only looks at management and control W-Fi frames (Connectivity only) and therefore is limited to only recognize certain attacks that use these frames (e.g. RTS Flood).

6. **Protocols** – In today's Smart Connected world we have lots of devices (and growing as by the end of the year there would be more than 30 billion) "speaking" in different protocols.

+ Harmony IoT's solution support Wi-Fi , Bluetooth , BLE and will extend to more wireless protocols.

- WIPS support Wi-Fi only.

7. **Visibility** – One of the most important aspects in today's enterprise environment is lack of visibility to the devices that are inside the airspace and not only connected to the organization network.

+ Harmony IoT's solution, is able to extract information from many sources and protocols which allows building the most comprehensive air-space visibility. The solution comes with a large base of known types of IoT devices, such as: mobile devices, smart TVs, smart outlets, smart lights, smart coffee-machines, wearables etc. The solution uses this base to visualize and map the environment (in and around the enterprise).

- WIPS provides MAC Addresses visibility and in most cases provides only information on devices that connect to the enterprise network only.

(1) https://www.cisco.com/c/en/us/td/docs/wireless/technology/wips/deployment/guide/WiPS_deployment_guide.html