Harmony IoT and Network Segmentation as Security Boundary in the World of IoT

October 28th, 2019

By ORCHESTRA

Confidential

Network segmentation is a good methodology for some organizations, but is highly limited by design and does not provide a sufficient security boundary in today's smart and connected world.
Below are three key examples for how Harmony IoT complements it:
1. Once you have configured network segmentation, how do you know it is actually working properly? We have seen countless examples with our clients were they were sure one part of the company was completely segmented from the rest, only to discover with our help cross-connecting devices all over the place. This was due to human error, configuration mistakes and lack of understanding. Harmony IoT gives you full visibility into your wireless airspace and helps you maintain proper network hygiene. Thanks to Harmony IoT's advanced analytics engine you get better identification to assist you in asset management, along with individual risk scores to help you secure your premises and tackle whats most important.
2. You can configure network segmentation for the devices that you know about, but what about all of the devices you don't know about? The ones being brought in by employees, contractors and guests? You have no control over them. Moreover, the entire world of IoT and smart devices (anything from wearables to smart printers and TVs) is unmanageable. You can't install an agent on them or monitor them in any way. Harmony IoT sees everything, and gives you power to control who connects where. With Harmony IoT you can actually enforce network segmentation.
3. Network segmentation only works for.. networks. In today's world there are many ways devices can communicate with one another (e.g. Bluetooth, BLE) that are not inside a network, but peer-to-peer. These communications happen in a completely separate layer from where the network segmentation is configured. You can instruct a specific computer to only connect to a certain network, but you can't tell it who it can connect to via Bluetooth for example (and all laptops and smartphones have Bluetooth today. Even coffee machines). Also, say all of the organization's important data is stored on a network that is segmented from the rest, so you can't get to it from any other computer on the network. Attackers can remotely, from across the street and using nothing more than a laptop and an antenna, disconnect those computers from their network and connect them to another, malicious wireless network, where the attackers can talk to them freely. Harmony IoT understands all of these protocols, accurately detects malicious activities and cyber attacks around your premises and mitigates them automatically and in real-time.

To sum up, network segmentation is a valid strategy, and could improve security. The problem is it is not able to handle today's threats. With every device manufactured today coming out with wireless interfaces, it substantially increases their attack surface, so a much broader security solution is needed in order to keep you safe in today's smart and connected world.

©Orchestra Group 2019 | All Rights Reserved | Confidential