Zingbox

aruba
a Hewlett Packard
Enterprise company

Zingbox IoT Guardian – Aruba ClearPass Integration

Introduction

Zingbox IoT Guardian compliments existing NAC solutions such as Aruba ClearPass by augmenting it to include deep IoT visibility and intelligence. IoT Guardian does this by first discovering the IoT devices on the network, identifying and profiling them with a patented three-tier machine learning algorithm, and then reporting them to the ClearPass system. IoT Guardian next checks for security risks and anomalous behavior, and when it discovers any, it sends alerts to ClearPass for automated policy enforcement. In sum, IoT Guardian provides ClearPass with accurate IoT device identities and notifies it whenever a security threat arises and device behavior veers from what is expected and safe.

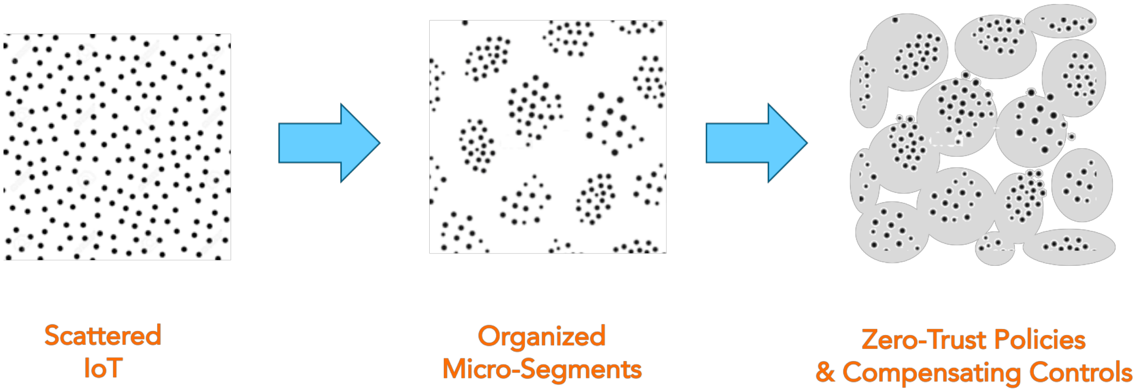
Let's look more closely at two benefits from a Zingbox IoT Guardian – Aruba ClearPass integration: device provisioning and policy enforcement.

Device Provisioning

Onboarding specialized network-enabled equipment such as medical devices can be a challenging task. Industry security best practices suggests that medical devices be placed in their appropriate VLAN along with its own class of devices. A complete inventory of non-traditional IT assets is often missing, which makes it rather difficult to design a network with VLANs for all the device types and then onboard devices into their appropriate VLAN segments. Zingbox provides several key features that enable VLAN segmentation:

- Discovery: Zingbox discovers all network-connected medical and IoT assets.
- Identification and classification: Zingbox identifies device makes and models, and understands their context of use.
- Segmentation: By integrating with Aruba ClearPass, Zingbox can provide it with device identities and profiles that you can then use to create security groups for defining network segments and access policies.

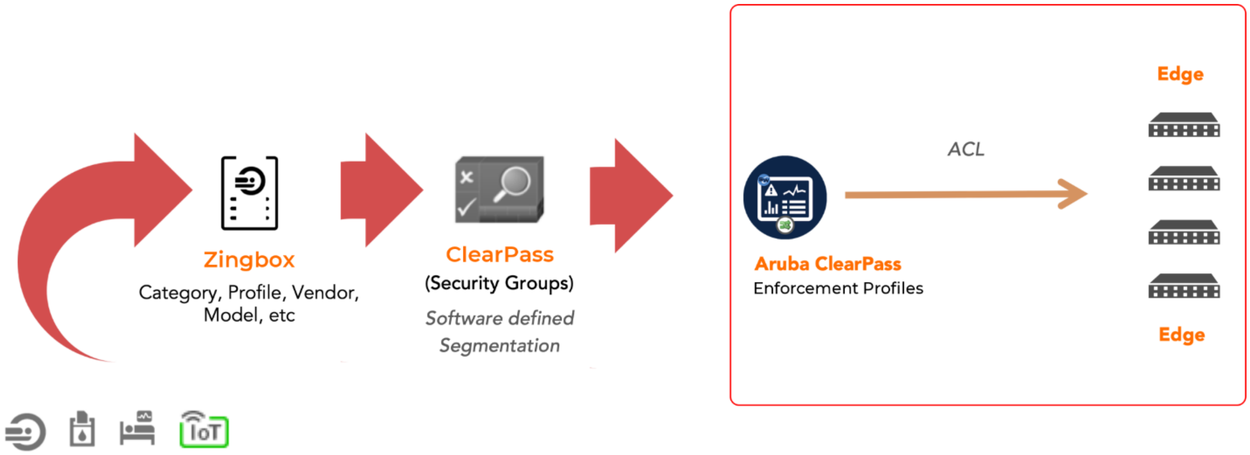
  Following is a pictorial representation of Zingbox orchestrated device segmentation:



Policy Enforcement

While manually defining policies and mitigating threats is feasible in the initial stages of a network, employing automation eventually becomes not only expedient but essential as the network expands in size and complexity. A Zingbox-Aruba integration can reduce risk by facilitating remediation and enforcing trusted behaviors:

- Device network isolation: By submitting alerts to Aruba ClearPass, Zingbox Inspector can trigger authorization profiles that isolate and quarantine affected devices in real-time.
- Only allow trusted behaviors: Through machine learning, Zingbox develops a baseline for the acceptable and trusted behaviors of each device, including its communication patterns with other devices. This behavioral data is available for export as ACL rules that can be programed as dACL (downloadable ACLs) to restrict all other communications. Aruba ClearPass can also use Zingbox device profiles for policy definition and enforcement.



Conclusion

Zingbox IoT Guardian provides Aruba ClearPass with Zingbox-learned IoT device identities to help with VLAN segmentation, and device profiles and alerts for use in NAC policy rules. By integrating Zingbox IoT Guardian with Aruba ClearPass, you can confidently expand your NAC coverage to include IoT devices among the many non-IoT devices you already secure.