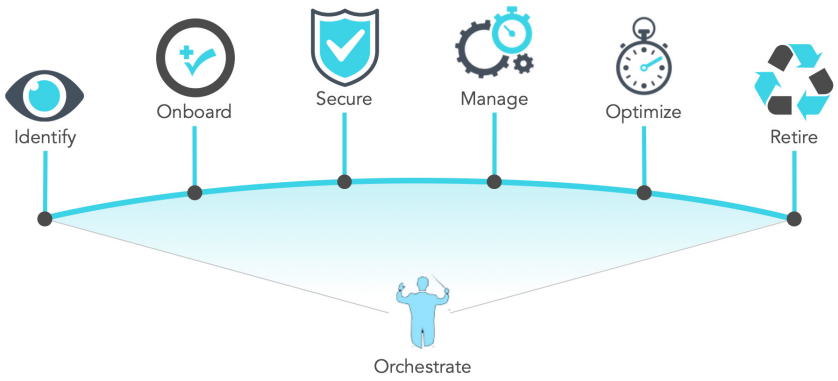
Zingbox Enables Network Access Control with IoT Device Visibility and Security

Introduction

Zingbox is the first to introduce the industry's only solution that orchestrates management of the entire IoT device lifecycle. The Zingbox IoT Guardian platform complements organizations' existing NAC (network access control) by augmenting it with deep IoT visibility and intelligence.



The integration between Zingbox and NAC technologies represents the true integration between IoT and IT and eliminates the need to administer multiple, disparate systems.

ABOUT ZINGBOX

75,000+ licensed beds under contract

1,100+ deployments

11.2+ Million IoT devices

1.6+ PB IoT data analyzed each day

HHS, FDA, NIST Contributing towards defining IoT regulations

11 offices worldwide (U.S. and Japan)

Enterprises have been deploying network firewall solutions to help protect from external malicious actors. NAC solutions help enterprises do the following:

- Ensure the right level of network access for its users and applications
- Implement best security practices (e.g., the least-access principal) and compliance requirements (e.g., access based on device type, OS, and the presence of endpoint security)
- Mitigate network threats by enforcing security policies that block, isolate, and repair noncompliant machines without administrator attention

However, when enterprises deploy NAC solutions to get these benefits, they quickly become overwhelmed and fall short of fully benefiting from them. These are some of the ways that happens:

- Networks that serve the applications are dynamic and often changing (e.g., device movement, application software changes).
- Application and device network access is not locked down due to ongoing requests to adjust access—undermining the primary reason the NAC solution was purchased in the first place!
- Lack of true device identity and the applications it hosts are the underlying reasons for lax network policies and for not deploying airtight networks with zero-trust policies.

Actionable Deep Device Context and Use Cases

A key component of Zingbox philosophy is to provide actionable deep device context. Zingbox IoT Guardian feeds this deep device context to NAC systems which can then be involved in orchestrating a rich set of use cases across the entire IoT device lifecycle. Zingbox sends NAC several deep device context attributes that enable a virtually unlimited number of use cases across the entire IoT device lifecycle.

The following is a sample of the actions NAC systems can enforce based on attributes from Zingbox:

	Onboard	Provision	Authorize	Remediate	Retire
Action:	Staging VLAN	Segmentation	Policy Enforcement	Quarantine	Quarantine
Condition – Based on attributes from Zingbox:	· New Device · Low Confidence · Risk Score	· Device Category · Device Profile · Confidence Score · Custom Tag · Risk Score	· Risk Score · Device Category · Device Profile · Confidence Score · Custom Tag · OS Status · AV Status · Unmanaged · Physical Location	· Risk Score · In-Use · Highest Severity Alert · Confidence Score · Custom Tag · OS Status · Physical Location	· CMMS · Inactive for X days

The remaining sections of this document describe the use cases that Zingbox IoT Guardian enables and that a NAC solution delivers.

Device Onboarding and Provisioning

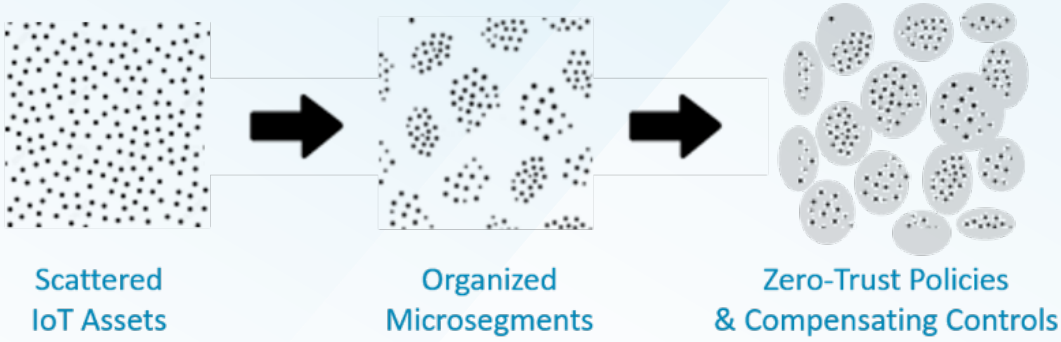
Onboarding specialized network-enabled equipment such as medical devices can be a challenging task. Industry security best practices suggest that medical devices be placed in their appropriate VLAN along with their own class of devices. A complete inventory of non-traditional IT assets is often missing, which makes it 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:

Device discovery, identification, and classification: Having full visibility and identification of network-connected medical and IoT assets is the first step for any security program. Employing machine-learning algorithms, Zingbox autogenerates device profiles and analyzes network behavior. During the planning phase of a NAC rollout, Zingbox passively listens to network traffic and discovers all network-connected medical and IoT assets including their network locations, such as the port number and IP address of their connecting switches.

Microsegmentation: A proper network segmentation plan requires listing device identity profiles and their interactions. Zingbox autogenerated device profiles and network behaviors can then be used for the planning phase of a NAC rollout. By integrating with NAC, 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.

Ongoing management: Nothing in an enterprise network stays static. Zingbox automatically feeds device identities and profiles into the NAC system for automatic and ongoing enforcement.

The following is a pictorial representation of Zingbox-orchestrated device segmentation:



Authorization

A NAC can provide role-based network access to the devices and the applications running on them.

ACL rules generation: Zingbox has deep visibility into device roles (e.g., a general-purpose iPad vs. an iPad used as a DICOM viewer) and can automatically generate ACL rules that allow the required access and required/trusted behavior.

Remediation

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

Device network isolation: By submitting alerts to NAC, Zingbox Inspector can trigger authorization profiles that isolate and quarantine affected devices in real time.

Reduce the risk from lateral movement: Zingbox IoT Guardian's *AI-powered anomaly detection* can identify in real-time any malicious activity (e.g., Ransomware spreading from one system to the other) and generate alerts. Alerts can automatically trigger policy enforcement actions via NAC APIs, e.g., to quarantine infected devices.

Retirement

Medical devices may contain Patient Health Information (PHI) or Personal Identification Information (PII). It is important to properly retire such medical devices:

Identify devices with private information: Zingbox IoT Guardian can identify devices that handle sensitive private information so that the data on such devices can be deleted to ensure compliance and protect patient privacy.

HEALTHCARE SECURITY CONCERNS

Most attacked industry since 2015

90% of hospitals are cyberthreat victims

75% of network traffic in a hospital is unmonitored

73% of hospitals do not have a security strategy for medical devices

17% of confirmed attacks originate from connected medical endpoints

Conclusion

Zingbox provides a highly complementary IoT security and management solution for NAC. Its enhanced device identity, profiling, security anomaly detection, and enforcement can also greatly accelerate the NAC rollout. Zingbox is pre-integrated with many leading NAC systems such as Cisco ISE/ pxGrid and Aruba ClearPass.

With these integrated solutions, organization across industries no longer need to deploy separate solutions and resources to manage their IT and IoT infrastructures. They can expand the devices they manage while continuing to use tools with which they are already familiar.