NAC Integration

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

ABOUT ZINGBOX

75,000 licensed beds under contract

1,100+ deployments

11.2 Million IoT devices

1.6+ PB IoT data analyzed each day

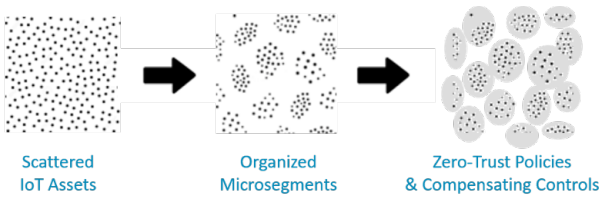
HHS, FDA, NIST Contributing towards defining IoT regulations

11 offices worldwide (U.S. and Japan)

Zingbox is the first to introduce the industry's only IoT lifecycle management solution that complements organizations' existing Network Access Control (NAC) such as Cisco ISE. The integration between Zingbox and Cisco technologies represents the true integration between IT and IoT and eliminates the need to administer multiple, disparate systems.

Use Cases of Zingbox and NAC Integration

- Context aware device micro-network segmentation
- Malicious device quarantine / unquarantined
- Device network location identification, such as port # and switch IP
- Real-time risk notification and policy enforcement



How does the Zingbox-Cisco ISE integration work?

- Zingbox IoT Guardian discovers, identifies, and inventories IoT devices through its always-on machine-learning algorithm and shares its contextually enriched actionable device data through Cisco pxGrid with Cisco ISE.
- Cisco ISE uses the actionable information about device context to organize devices more effectively into "security groups" and organize the network into IoT context-aware micro-segments.
- Zingbox IoT Guardian continuously monitors and learns real-time behaviors of IoT devices and generates profiles, tags and ACLs within ISE and TrustSec to implement automatic IoT device onboarding and dynamic access control.
- Using AI-learned normal behaviors of IoT devices, Zingbox IoT Guardian can detect any deviations or compromises, and integrate with ISE, TrustSec or DNA Center for real-time threat detection and containment.

Asset Discovery & Tracking

- Identify, classify and inventory IoT assets
- Enrich asset records with contextual data
- Relay IoT context to ISE

Micro-segmentation

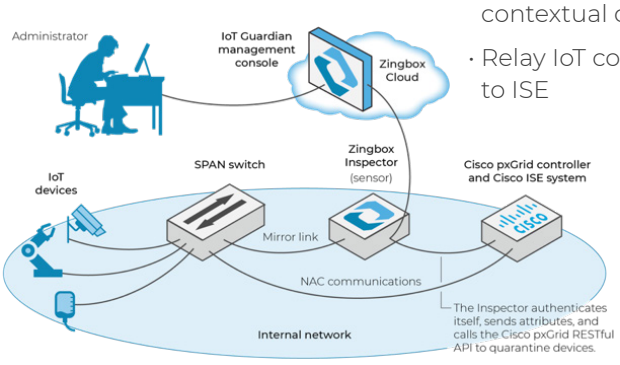
- Define security groups in ISE using IoT context
- Network admission policies based on IoT security groups
- Organize assets dynamically in context-aware micro-segmentation

Policy Definition

- Learn normal device behaviors
- Apply principles of least privilege to IoT assets
- Generate ACLs to only allow trusted behaviors

Security Enforcement

- Detect deviation from expected baseline
- Surgically block malicious connections
- Isolate and quarantine the device



With the integration of Zingbox and Cisco ISE, 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.