Securing Critical IoT Infrastructure

Zingbox

A PALO ALTO NETWORKS® COMPANY

paloalto NETWORKS®

All Enterprises have an IoT Problem

IOT Represent

Over 50% of endpoints

Unmanaged, shadow assets

New devices joining each day

A growing attack surface

IOT Assets are

Non-standard devices

Diverse – OS, firmware, apps

Often shipped with vulnerabilities

Impossible to control patching – risk exposure

Growing Risk Exposure

Unpatched, unmanaged, yet connected

Useful life is longer than it's cyber life

Growing risks and vulnerabilities

Weakest links in enterprise network

IT workflows may not work anymore

Critical Infrastructure Owner Goals

Visibility

Inventory Tracking

Monitoring

Service Continuity

Operational Efficiency

Safety

Maintenance

Asset Maintenance

Cyber Maintenance - patching

Cybersecurity Challenges

Lack security expertise in the team

Outside the jurisdiction of security experts

Traditional security tools do not work

What's Unique about Critical Infrastructure?

Purpose-built Systems

Business necessity that introduces risk

Convergence of Digital and Physical Domains

Severe Impact of a Security Breach

Useful Life is Longer than the Cyber Life

IoT Security Needs a New Solution

Today's IT Environment

Homogeneous Infrastructure

2016

Future IoT Environment

- Diverse and heterogeneous
- Specific-purpose hardware
- Unique malware for each device
- Reactive approach not effective

Future

Malware Behavior

Malware portable across homogeneous platforms

Malware Signatures
Attack Behaviors
Payload Analysis

< The common thread >

IoT Personality

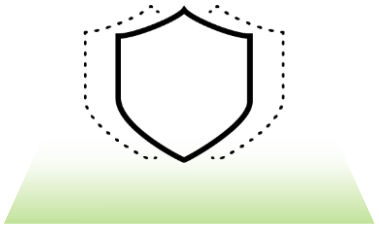
Similar device behaviors across various deployments

Machine Learning driven context and behavior recognition
to detect zero-day threats

IoT Security Capabilities

Device Discovery & Identification

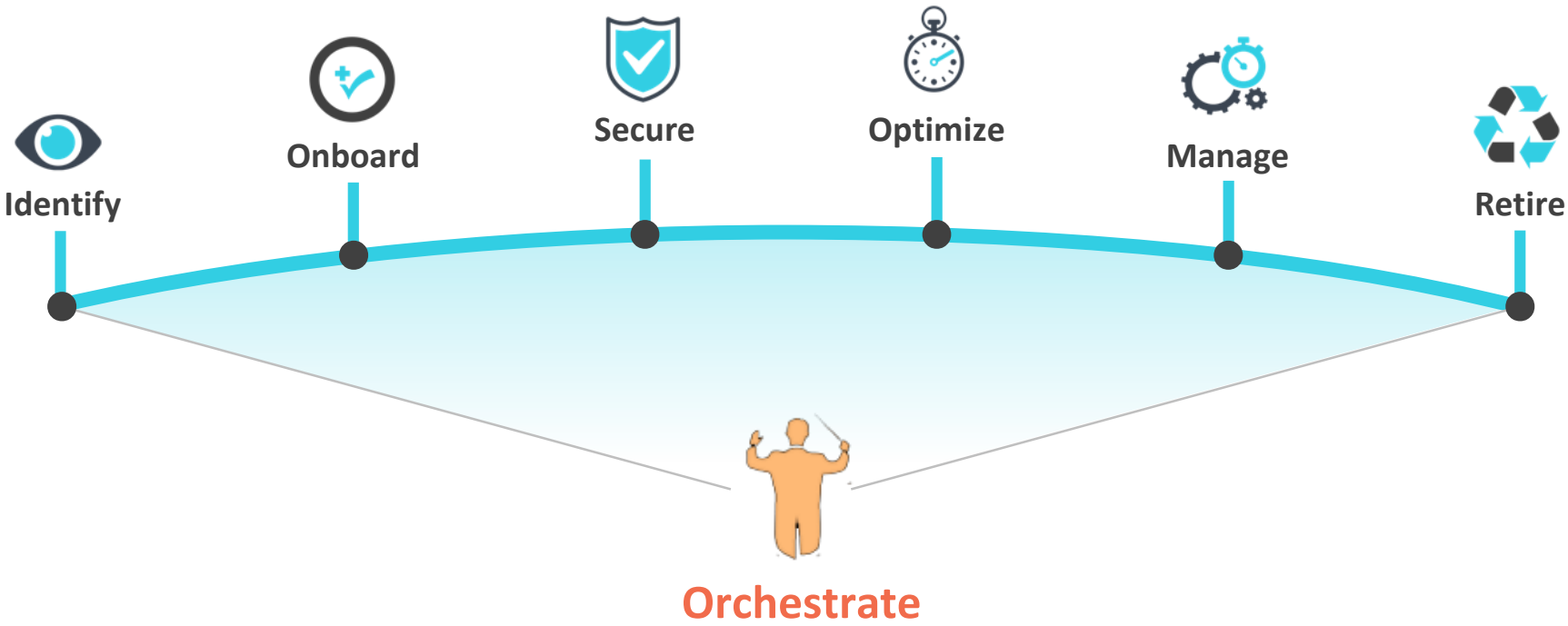
- Dynamic device inventory
- Automated device provisioning and authorization



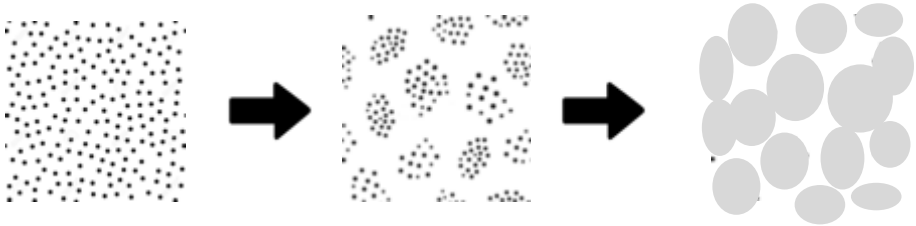
Risk Detection & Prevention

- AI driven behavioral analytics
- Least privilege with Zero-trust policies
- Vulnerabilities, recalls, security advisories

Orchestration of IoT Assets



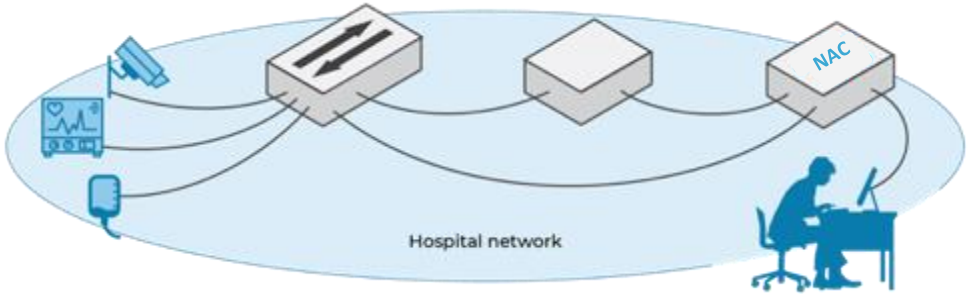
Orchestration of IoT Assets



Scattered IoT Assets

Organized Micro-segments

Zero-Trust Policies & Compensating Controls



Zero-touch, Non-disruptive deployment

NAC Administrator

IoT orchestration

asset discovery & tracking

- identify, classify and inventory IoT assets
- enrich asset records with contextual data
- relay IoT context to NAC

micro-segmentation

- define ‘security groups’ in NAC using IoT context
- network admission policies based on IoT ‘security groups’
- organize assets dynamically in context-aware micro-segments

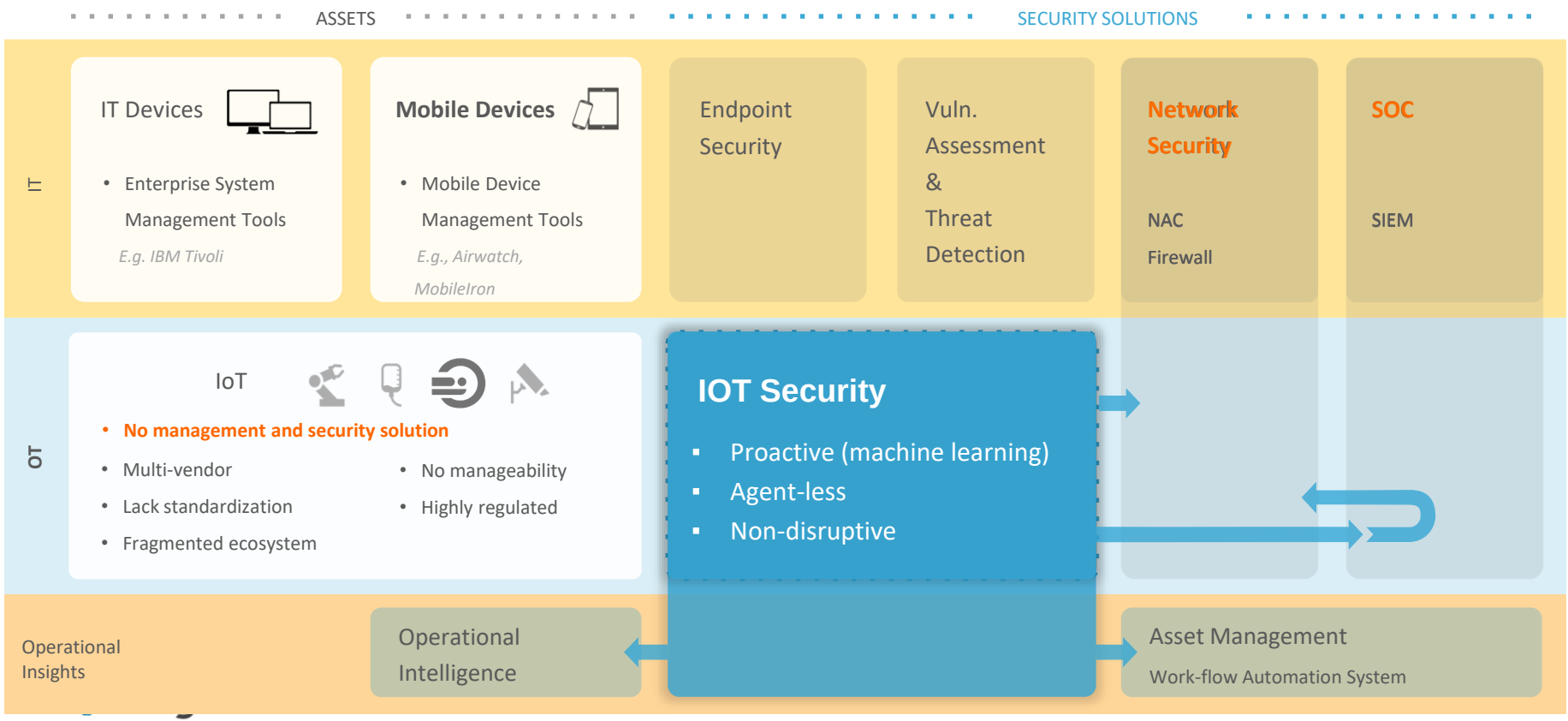
policy definition

- learn normal device behaviors
- apply principles of least privilege to IoT assets
- generate ACLs to only allow trusted behaviors

security enforcement

- detect deviations from expected baseline
- surgically block malicious connections
- isolate and quarantine the device

IoT Security Positioning



The IoT Maturity Model

Zingbox

IoT Security is a journey

Take baby steps in the right direction!

Thank You!

Zingbox in action...

2.5 PB+
IoT Data/Day

850M+
IoT Events/Day

11.2 M+
IoT Devices

1,100+
Deployments

Enabling the Internet of *Trusted* Things

Contact us: info@zingbox.com