The Connected Industry: Cloud Security The Backbone for Internet of Things

Dharminder Debisarun
Cybersecurity strategist

Cyber Evolution Trends

Data Is Everywhere

Virtualization, IoT, BYOD and SaaS adoption has increased the threat vector

25B+

connected devices will be in use by 2021

Advanced Threats

Attacks are becoming more pervasive and sophisticated

300M+

never before seen samples every month

32%

increase in malware delivered over encrypted traffic YoY

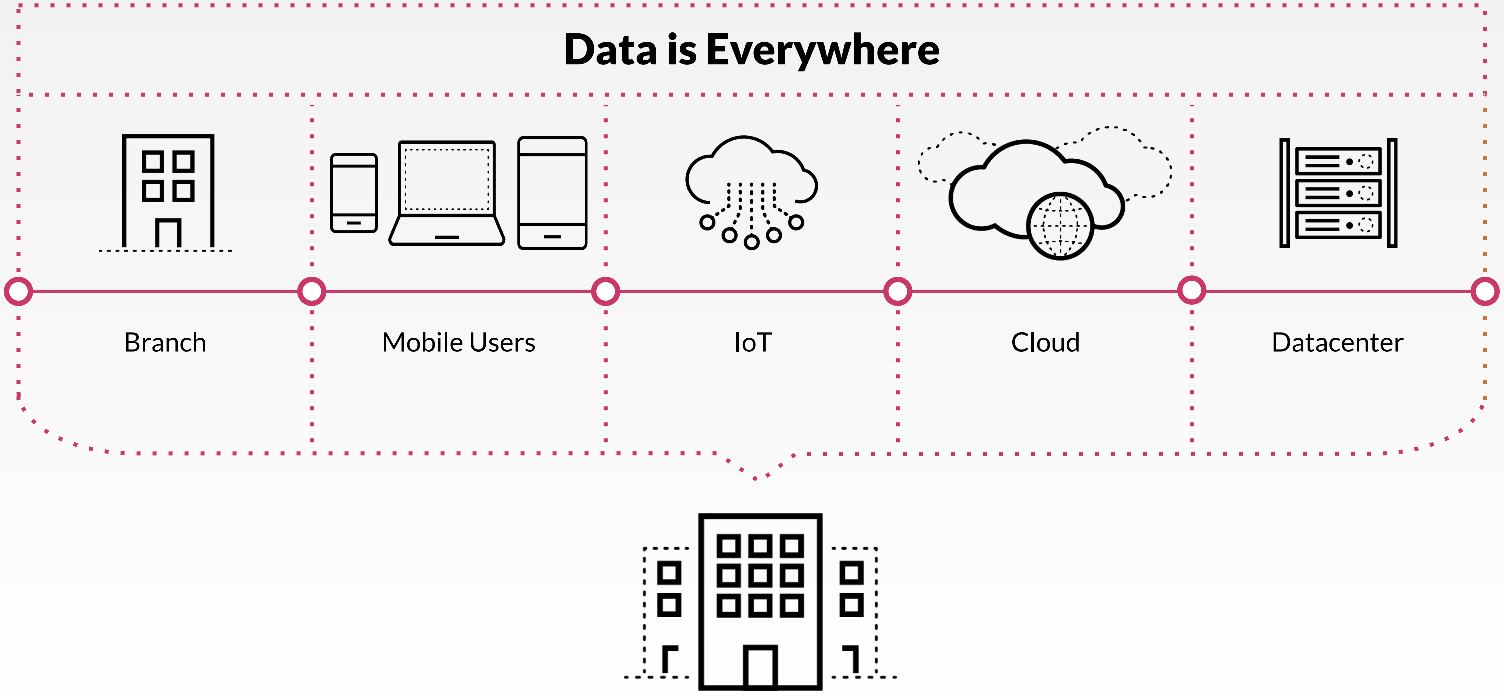
Security Skills Shortage

Cybersecurity skills shortage leaves organizations at risk

53%

of organizations report a shortage of cybersecurity skills

Cyber Evolution: Enterprise



Data is Everywhere

Branch

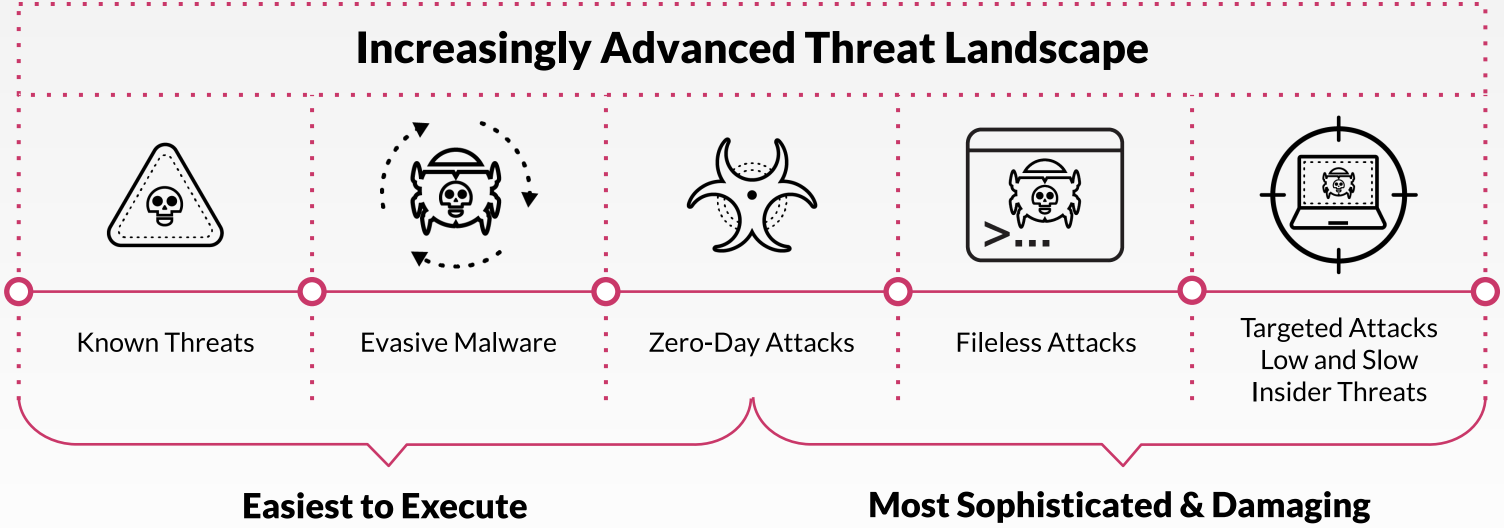
Mobile Users

IoT

Cloud

Datacenter

Cyber Evolution: Threats



Increasingly Advanced Threat Landscape

Known Threats

Evasive Malware

Zero-Day Attacks

Fileless Attacks

Targeted Attacks
Low and Slow
Insider Threats

Easiest to Execute

Most Sophisticated & Damaging

I(IOT) Enables Industry 4.0

Operation IoT → IT – OT Convergence ← Information IoT

- Connected HVAC
- Smart Lighting
- Surveillance Camera

Safety

- Device and Employee safety

Operation

- Operational quality & efficiency

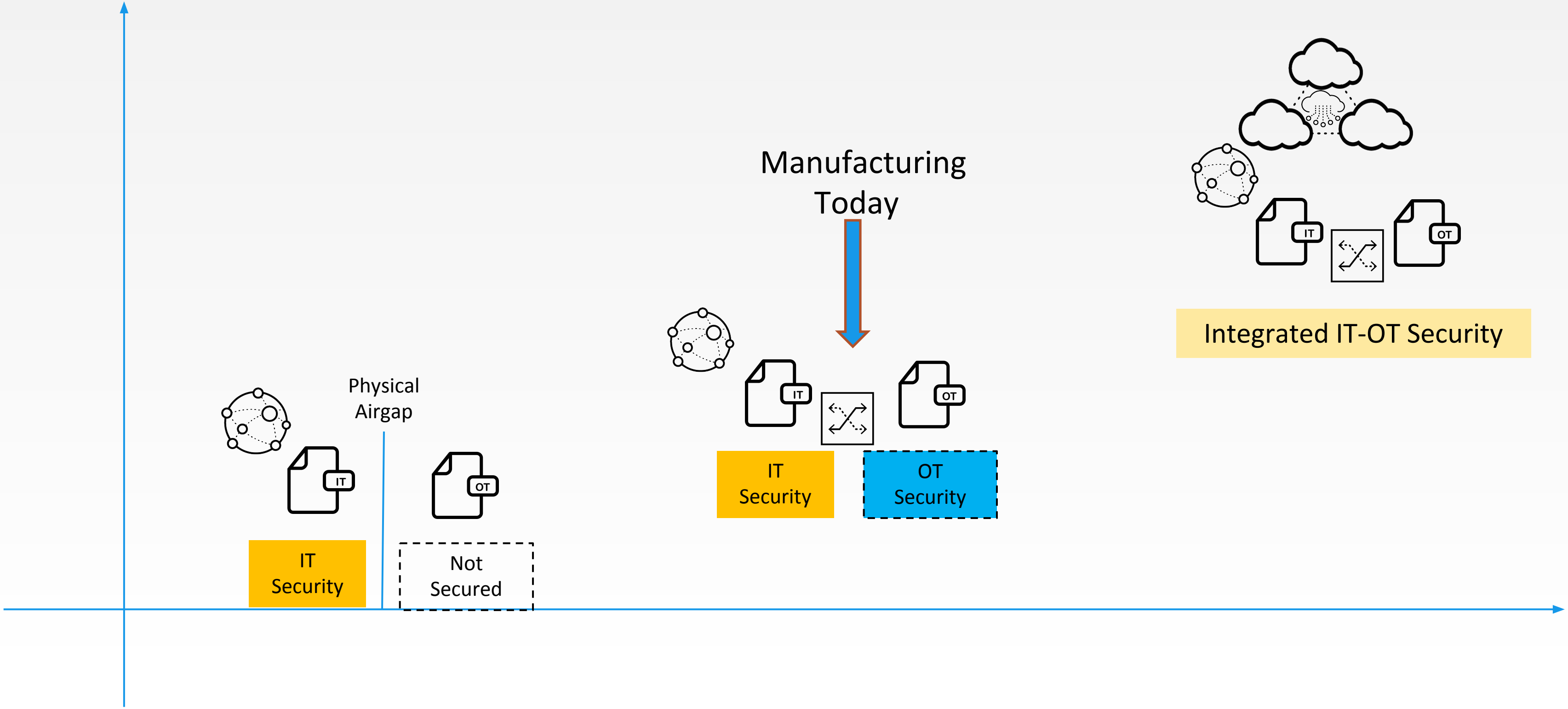
Security

- Data and equipment security

Continuity

- Life cycle continuity & integrity

OT Cybersecurity Evolution



A Shift in the Market

IT Department

- IoT device discovery & visibility
- Agent-less, signature-less, proactive security
- Context-aware policy enforcement

Security & Risk Assessment

OT Department

- IoT device inventory tracking
- Utilization monitoring
- Operation continuity & efficiency

Business Efficiency & Continuity

Rapidly Evolving IoT Botnet Attacks

Unique IoT Botnets

Evolving rapidly to specifically leverage IoT devices (Mirai, Rakos)

IoT related DDoS

Attacks targeting various host sites & network infrastructure - launched by compromised IoT Devices

Growing Volume

Over 1gbps attacks leveraging as many as 500,000 IoT Devices at once

Networks Targeted

Service providers seeing attacks targeting their infrastructure – launched from compromised things attached to their network

IoT Introduces Security Risks

Unpatched Vulnerabilities

Patching IoT hard or impossible

Many IoT vendors—especially consumer IoT--do not automatically update products

Cloud-based Management

Many IoT devices offer cloud-based management, exposing the devices to exploits and brute force password attacks

Weak Authentication

Mirai botnet recruited bots by finding IoT devices with one of **61 common passwords**

Lack of Host-based Security

Organizations often cannot install traditional endpoint protection or host IPS on IoT

Existing Security Risks Of OT Devices

Unpatched Vulnerabilities

Patching / System updates few and far between if ever. Most because of required system uptime requirements.

Patching/updating could take system out of spec

No Central Management

Many devices have been added to network via COTS

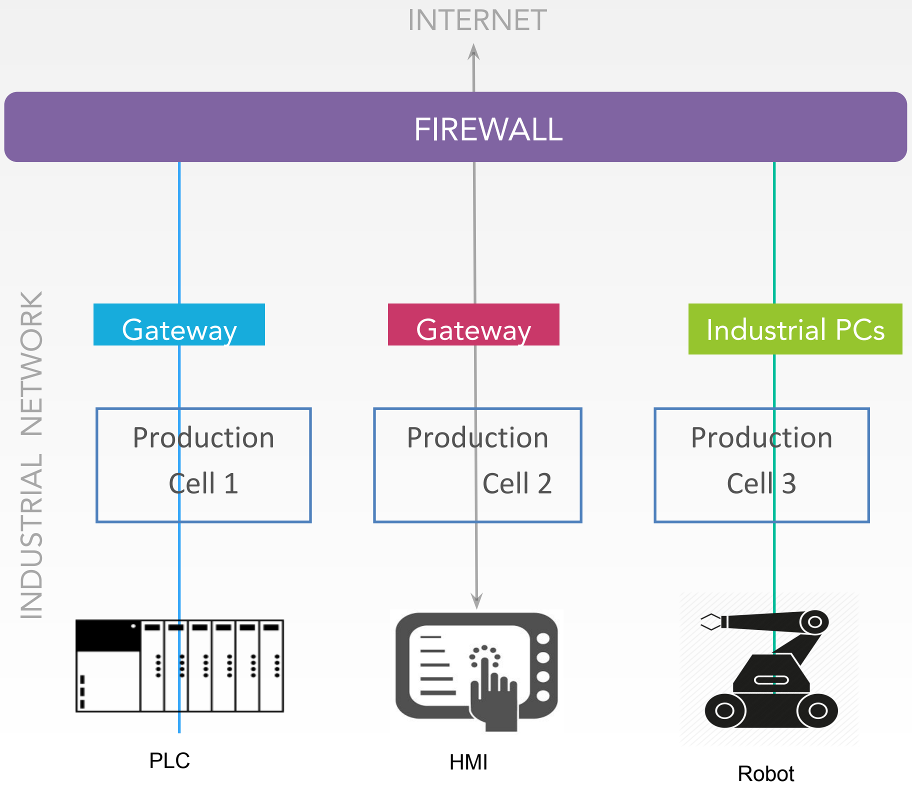
Weak Authentication or Password

Older devices that do not support strong authentication or passwords. Many just left on default password

Lack of Host-based Security

Many devices are older black box systems that do not support security. Systems that do run the risk of negative performance impact

I(IOT) Security is Overlooked



Firewall - the single line of defense

(With no IoT device context, only works at IP level)

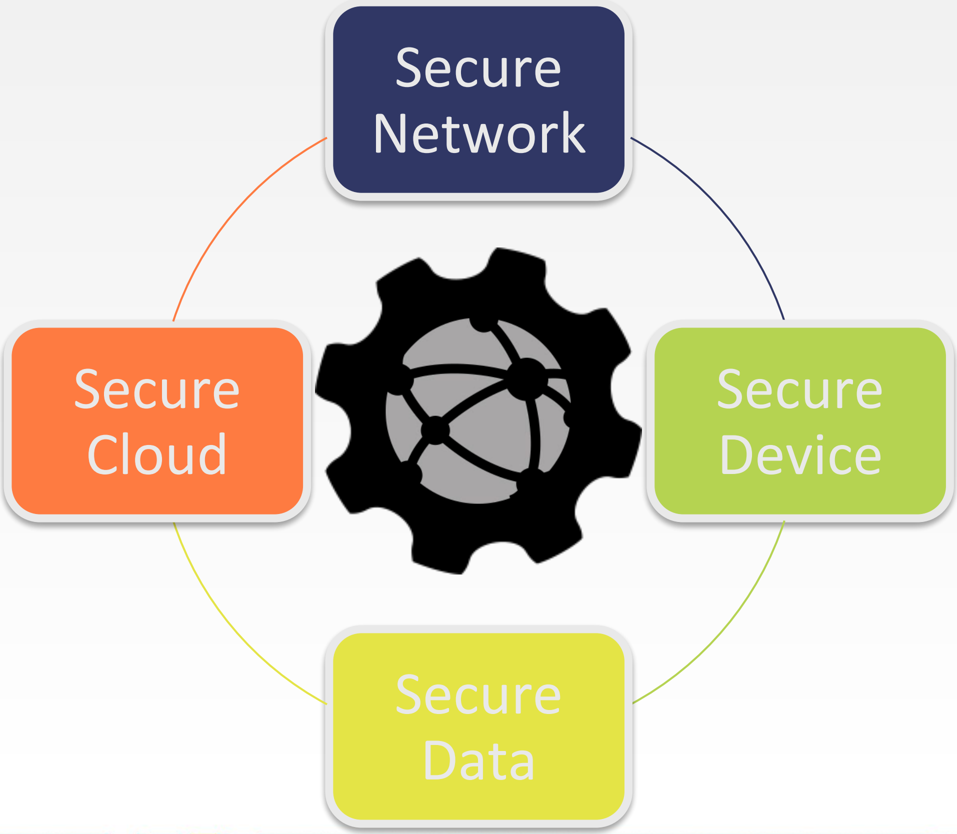
Unmonitored network

(OT network remains unprotected)

Lack of endpoint visibility & security

(Agents cannot be deployed)

How can we change?



Secure Network

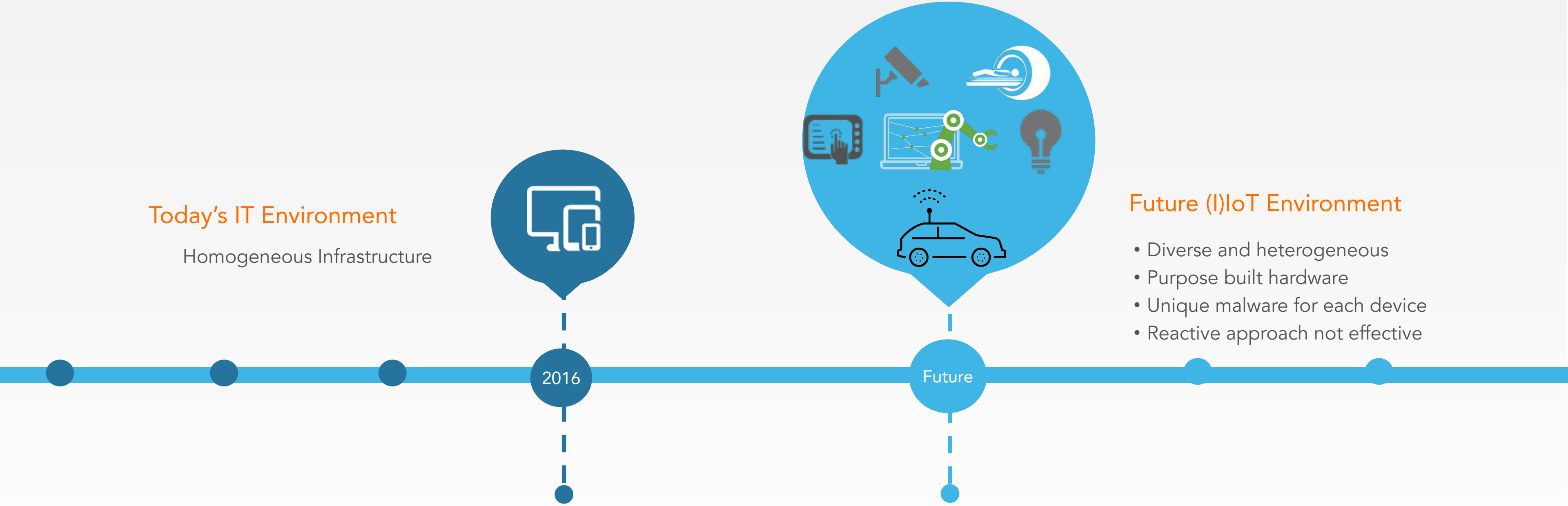
Secure Cloud

Secure Device

Secure Data

Our Unique Approach

IoT Security Need a New Solution



Today’s IT Environment

Homogeneous Infrastructure

Future (I)IoT Environment

- Diverse and heterogeneous
- Purpose built hardware
- Unique malware for each device
- Reactive approach not effective

Malware Behavior < The common thread > IoT Personality

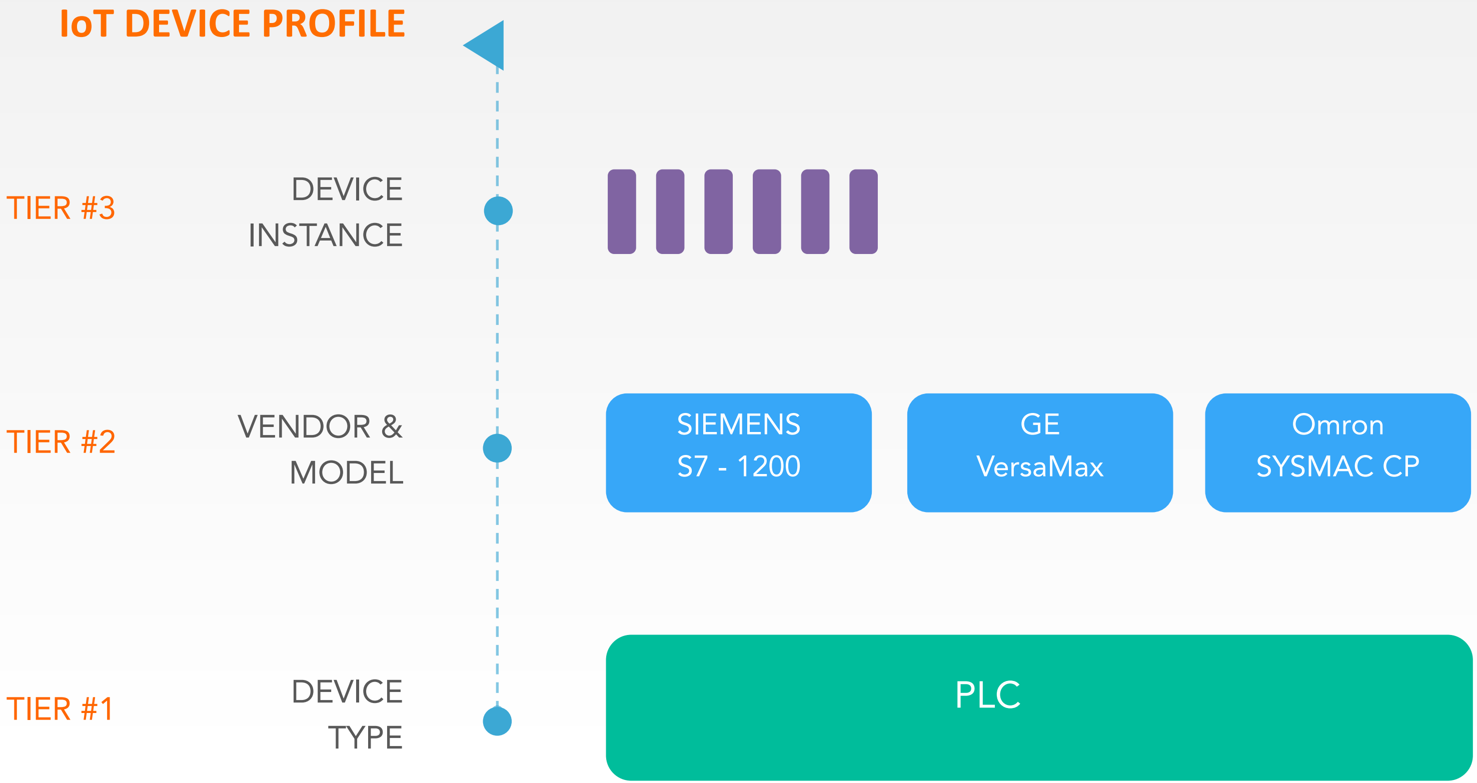
Malware portable across homogeneous platforms

Malware Signatures, Attack Behaviors, Payload Analysis

Similar device behaviors across various deployments

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

Device and Context



IoT DEVICE PROFILE

TIER #3 DEVICE INSTANCE

TIER #2 VENDOR & MODEL

SIEMENS S7 - 1200

GE VersaMax

Omron SYSMAC CP

TIER #1 DEVICE TYPE

PLC

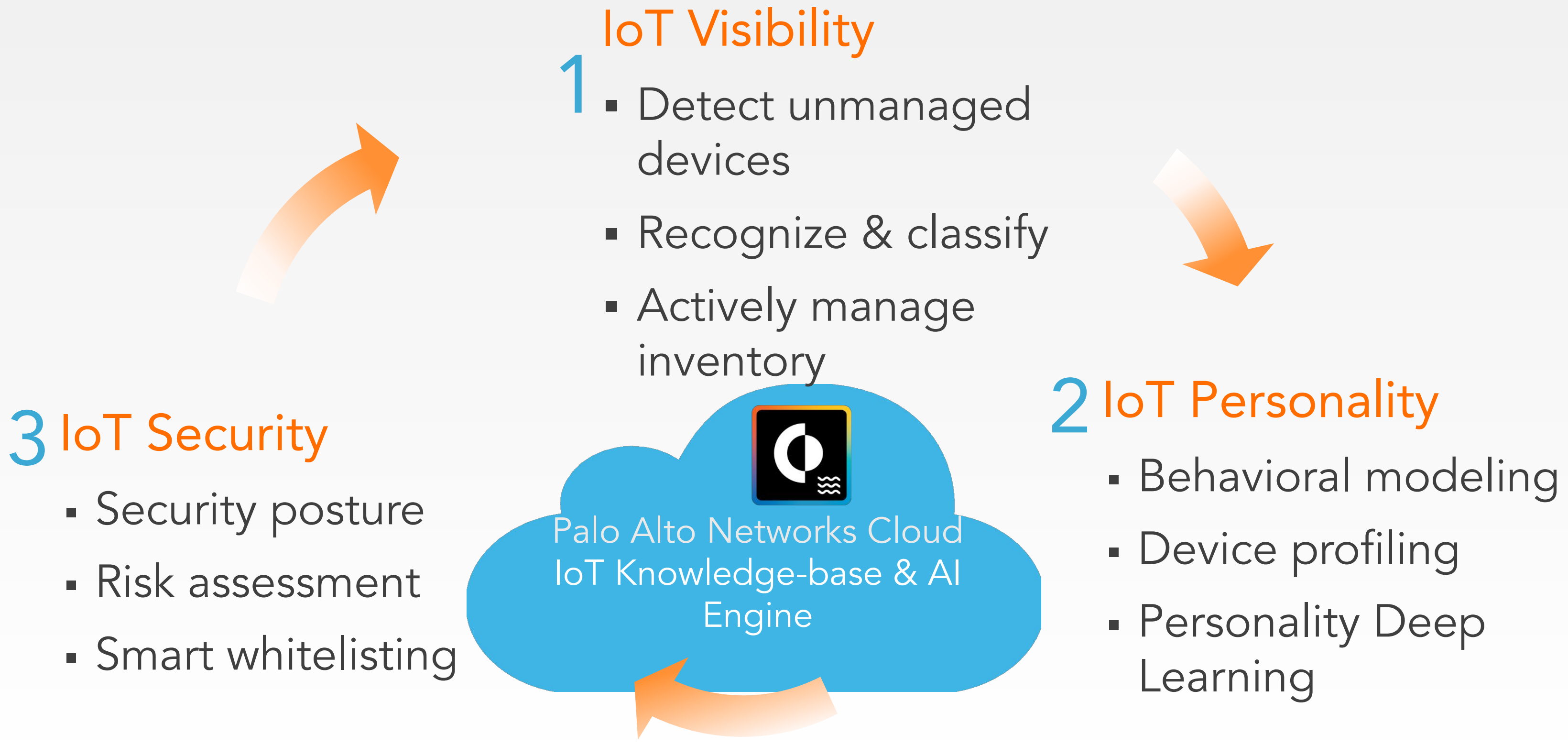
Deep Learning –

IoT Device Recognition,

Classification and profiling.

- Device Context not just IP address
- Beyond OS Recognition
- Tighter control than IT Policies
- Security from Day-1

Device Security via Machine Learning



1 IoT Visibility

- Detect unmanaged devices
- Recognize & classify
- Actively manage inventory

2 IoT Personality

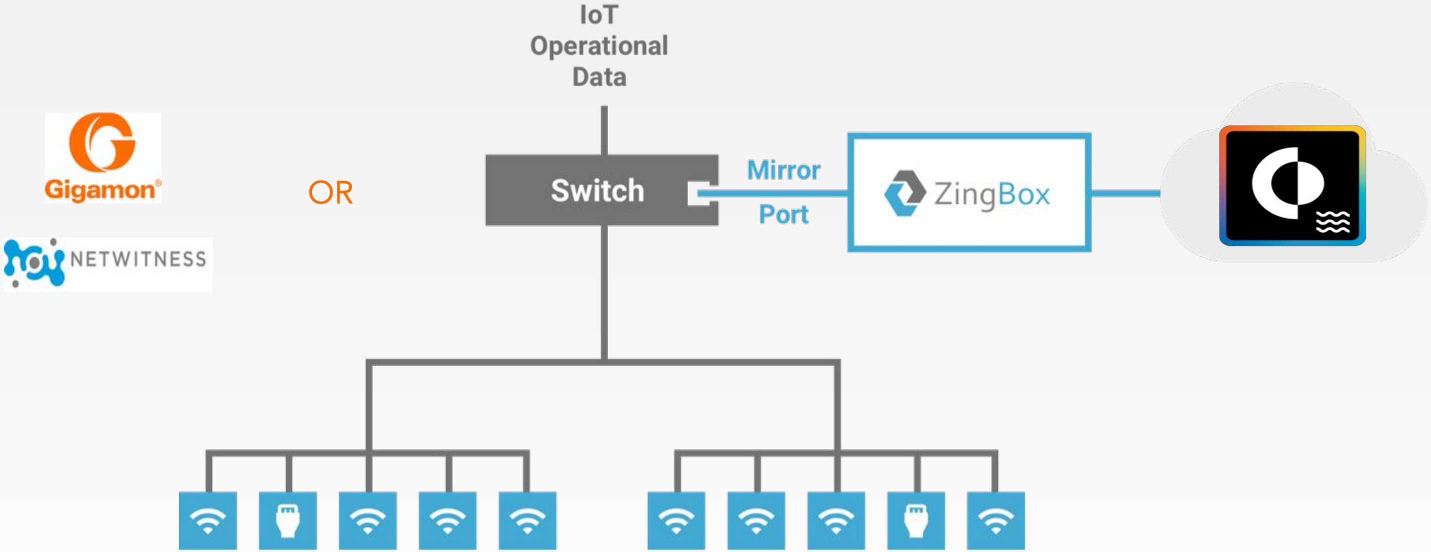
- Behavioral modeling
- Device profiling
- Personality Deep Learning

3 IoT Security

- Security posture
- Risk assessment
- Smart whitelisting

Palo Alto Networks Cloud IoT Knowledge-base & AI Engine

Non- Disruptive Deployment



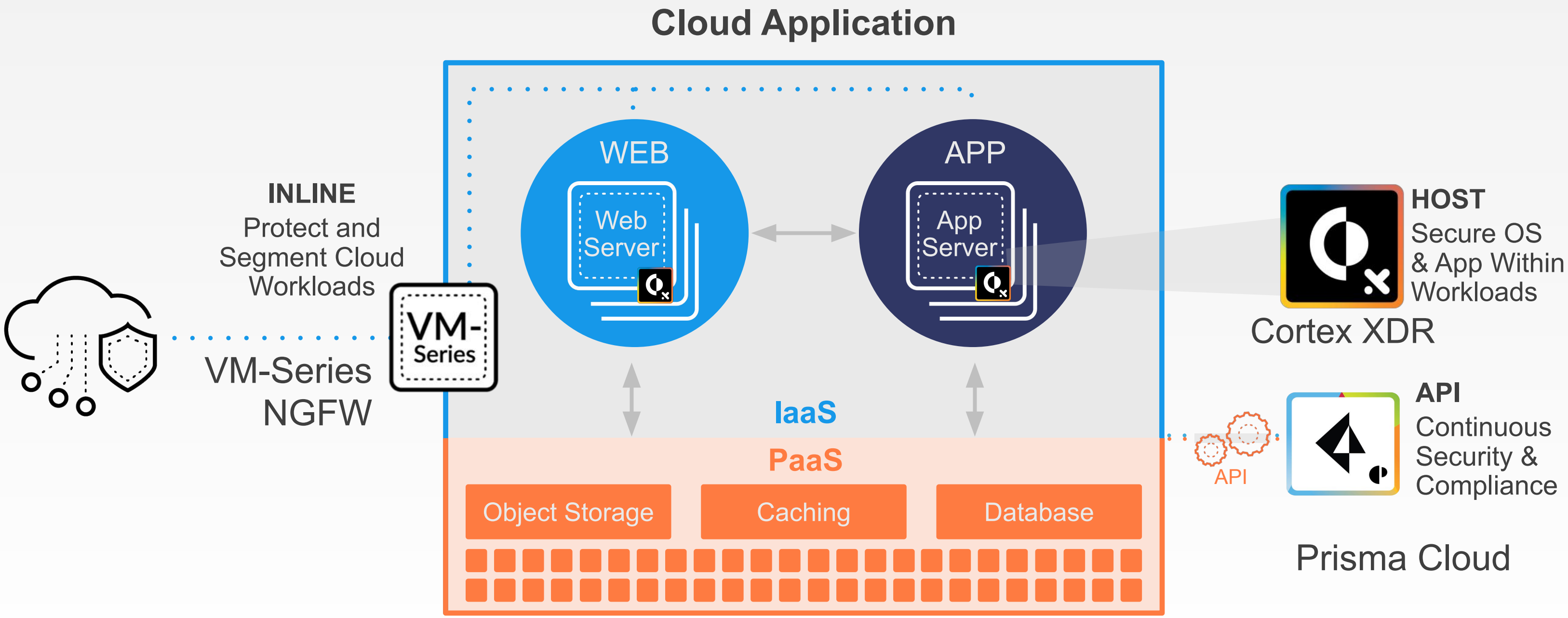
Quick Setup

15 minute deployment.
Integrates with existing security infrastructure.

Non-disruptive

Passive, out-of-band deployment ensures operational continuity.

Critical Cloud Protections



Cloud Application

INLINE
Protect and
Segment Cloud
Workloads

VM-Series
NGFW

WEB

Web Server

APP

App Server

IaaS

PaaS

Object Storage

Caching

Database

HOST
Secure OS
& App Within
Workloads

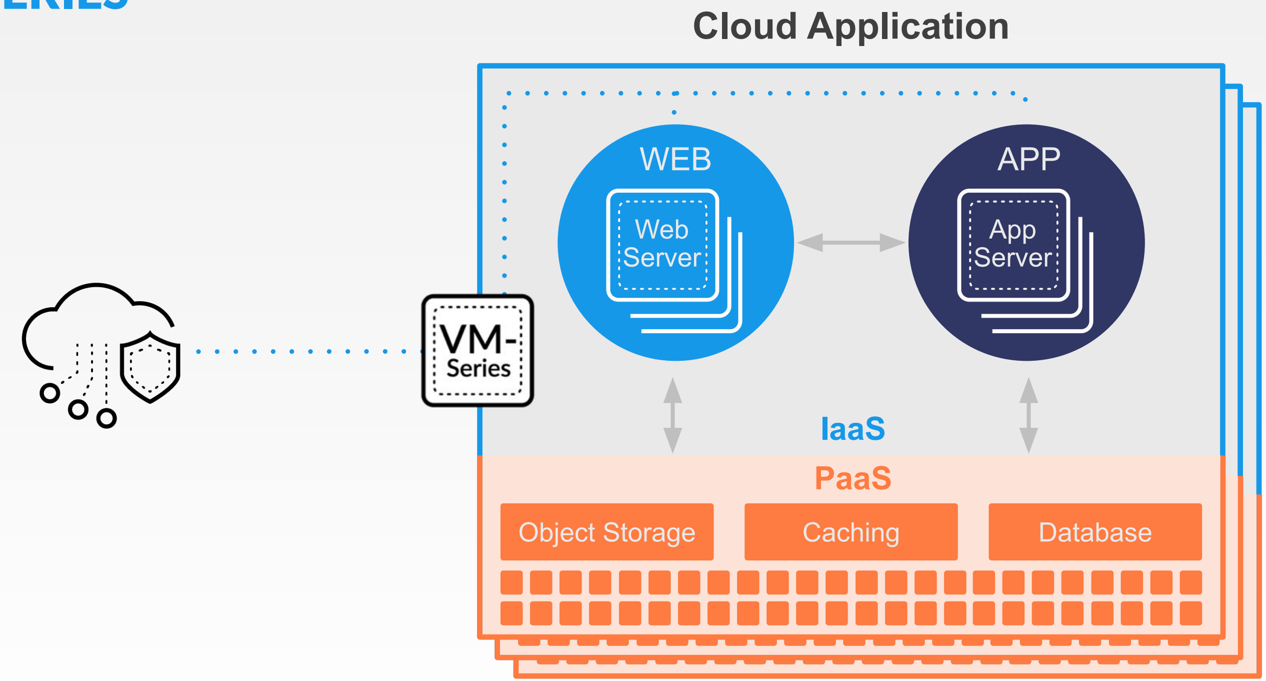
Cortex XDR

API
Continuous
Security &
Compliance

Prisma Cloud

PROTECT AND SEGMENT CLOUD WORKLOADS

VM-SERIES



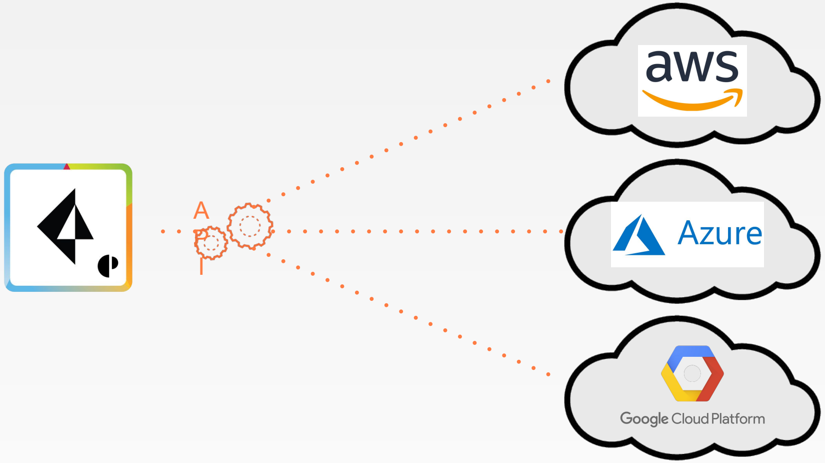
Prevent outbound and inbound attacks

Application visibility and workload segmentation

Auto-scale based on triggers

Continuous monitoring and compliance

Prisma Cloud



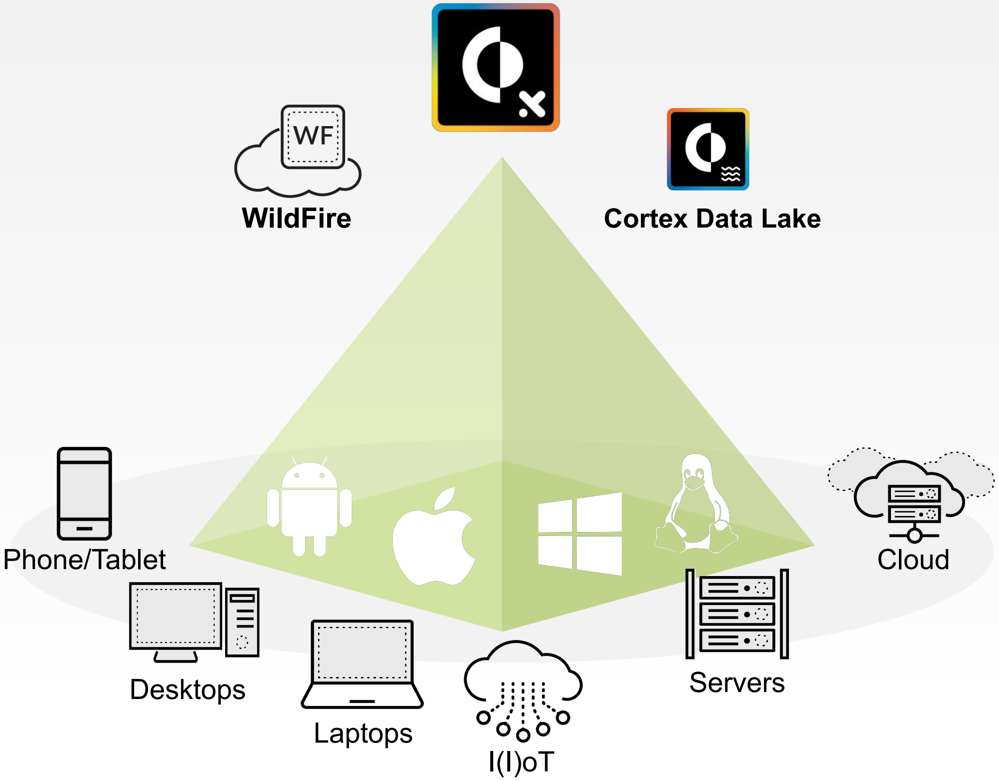
- Is MFA Enabled?
- Is any sensitive data exposed?
- What services are running?
- Who has access to this resource?

Discover and Monitor Resources

Compliance Reporting

Secure Storage Services

Prevent Advanced Endpoint Attacks With Cortex XDR



Stop malware, ransomware with machine learning and behavioral threat protection

Block exploits and fileless attacks by technique

Included with Cortex XDR to coordinate enforcement and accelerate response

22 | © 2018, Palo Alto Networks. All Rights Reserved.

Production Process and Business Continuity

Simplify Management

VISIBILITY

- Single pane-of-glass for all IIoT/OT assets
- Device discovery, identification, classification & behavioral insights
- Automate acquisition integration process

Reduce Risk

SECURITY

- Production safety insurance
- Lower Brand/Reputation Risks
- Behavior based security risk assessment and threat prevention
- AI assisted forensic analysis

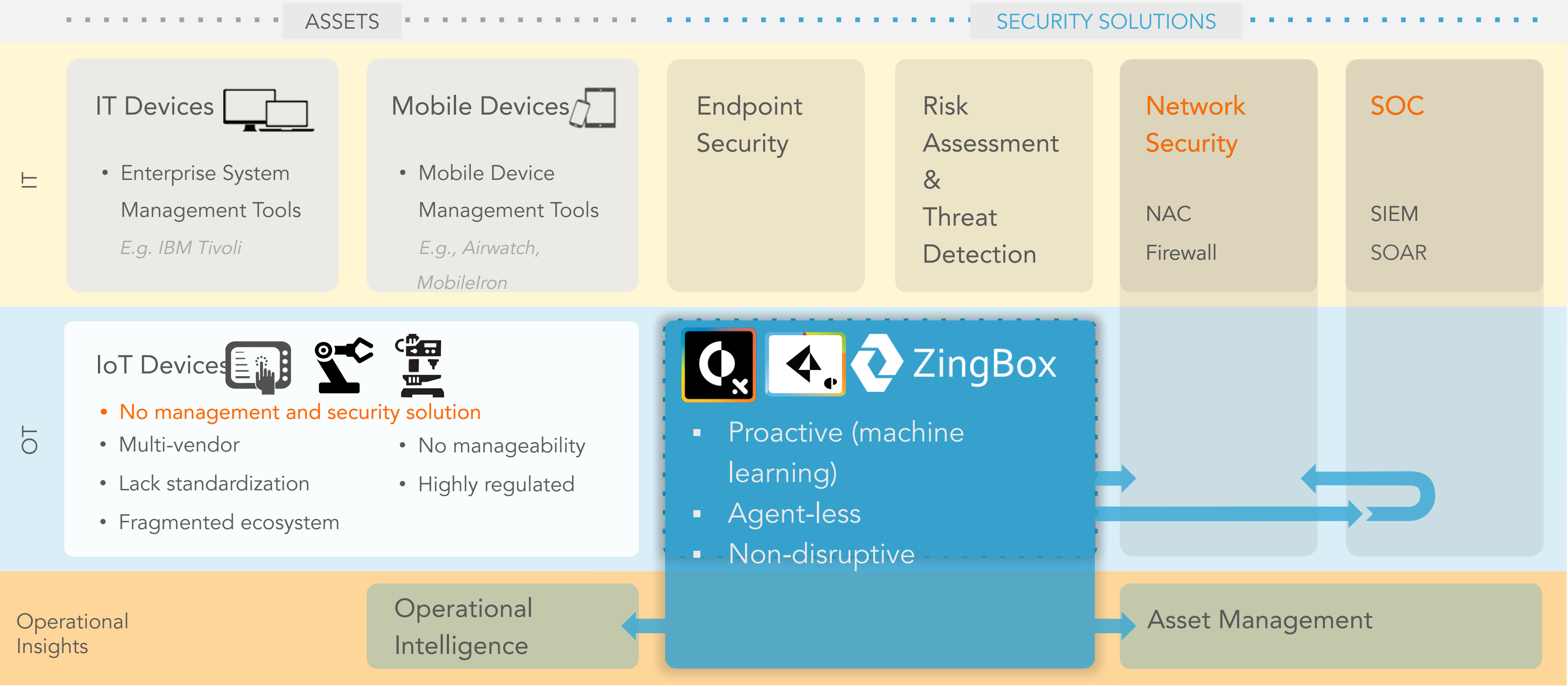
Increase ROI

OPERATIONAL INSIGHTS

- Increase Revenue by maximizing device utilization
- Minimize downtime
- Lower TCO
- Reduce maintenance costs
- Real-time OT analytics

23 | © 2019 Palo Alto Networks, Inc. All Rights Reserved.

I(I)oT Solution That Blends In



ASSETS

SECURITY SOLUTIONS

IT

IT Devices

- Enterprise System Management Tools

E.g. IBM Tivoli

Mobile Devices

- Mobile Device Management Tools

E.g., Airwatch, MobileIron

Endpoint Security

Risk Assessment & Threat Detection

Network Security

NAC

Firewall

SOC

SIEM

SOAR

OT

IoT Devices

- No management and security solution
- Multi-vendor
- Lack standardization
- Fragmented ecosystem
- No manageability
- Highly regulated

- Proactive (machine learning)
- Agent-less
- Non-disruptive

Operational Insights

Operational Intelligence

Asset Management

Thank You

paloaltonetworks.com

Email: ddebisarun@paloaltonetworks.com

Twitter: @PaloAltoNtwks