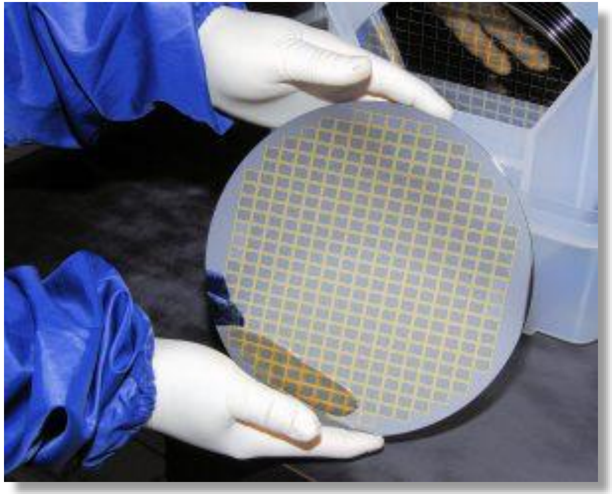
Cybersecurity at the Intersection of IoT, Industrial Controls, and Smart Cities

Del Rodillas

Director, Industrial and IoT Cybersecurity Product Solutions

A Little About Myself

- 20+ years in High Tech Industry
  - Engineering, Business Operations, Product Management & Marketing
- First job as a Manufacturing Yield Engineer
  - MS Electrical Engineering (Santa Clara Univ.)
  - Semiconductor industry
- 6+ years at Palo Alto Networks
  - Industrial and IoT cybersecurity
  - Marketing and business strategy
  - GICSP certified (Industrial Cybersecurity)
  - Masters Business Administration (Wharton)



MIX Smart City Conference CIO Survey Results

Q1	How important is IoT Security to you?							
Answer options	▲	"Very High - Top 3 initiative."	♦	"High, but not top of mind."	●	"On the list, we'll get to it eventually."	■	"Not on my radar."

Q2	"My responsibility includes securing Industrial Control Systems"							
Answer options	▲	"Agree."	♦	"Disagree."	●	"Not sure."		

MIX Smart City Conference CIO Survey Results

Q3	"I have a smart city initiative involving IoT."							
Answer options	▲	"Agree"	♦	"Disagree"				

Q4	Where are you in terms of your IoT/ICS security journey?							
Answer options	▲	"Implemented and feeling secure."	♦	"Implemented some, but more to do."	●	"Nothing in place yet. Just planning."	■	"I am not responsible for IoT/ICS cybersecurity."

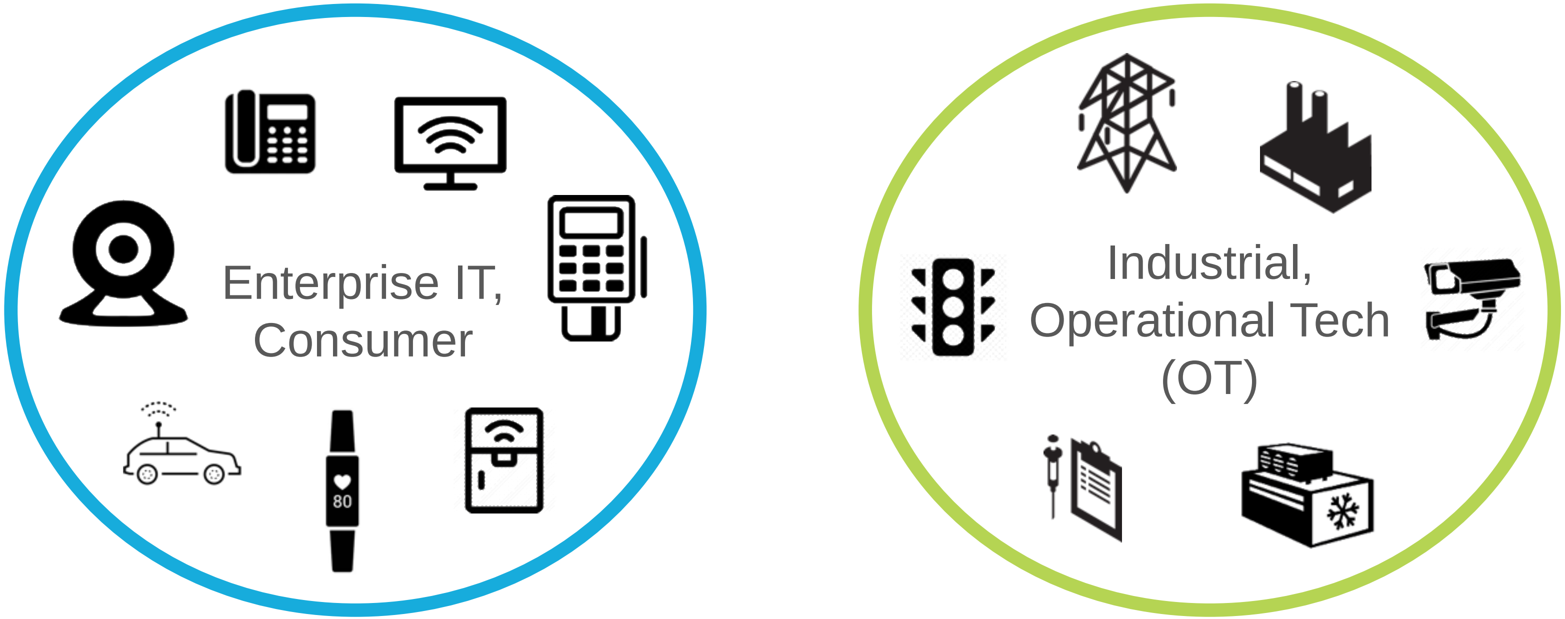
MIX Smart City Conference CIO Survey Results

Q5	Where is the best place to secure IoT?							
Answer options	▲	"The IoT device itself."	♦	"The enterprise network."	●	"The ISP / carrier network."	■	"The analytics core in the cloud."

Revisiting the definition of IoT

“Any networked device that performs a single function, delivers a single application, or performs a single service.”

IoT in Consumer, Enterprise, and Industrial/OT



Enterprise IT, Consumer

Industrial, Operational Tech (OT)

Industrial Control Systems and IoT

mesaaz
Smart City

Phase I Master Plan

- AMI – Advanced Metering Infrastructure
- Downtown digital kiosks
- Building & Facilities Automation
- FirstNet

A Smart City is one in which the latest technologies and data-driven insights are leveraged to improve the quality of life, civic engagement, economic development, service delivery, and community vibrancy for its citizens, businesses and visitors.

“You can’t have a successful Smart City initiative without IoT”

- Lester Godsey, CISO, City of MESA

IoT/IIoT Initiatives at a State Government

Non Line-of-sight UAV

Weather Analytics & Management

Acoustic fiber in Roadways

Pipeline monitoring

Precision Agriculture

Medical Devices

"In 3 years we went from being afraid of technology taking away jobs to technology enabling the creation of wealth". This entails proper cybersecurity strategy.

- CTO of State Government

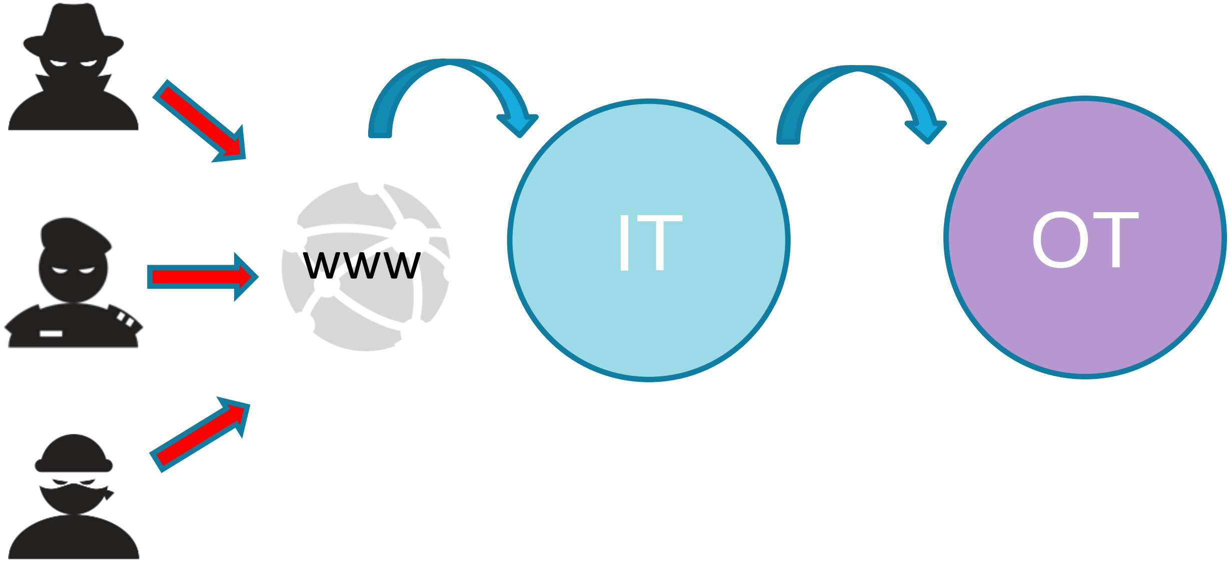
How should cybersecurity be managed in converged IT-OT-Cloud?

Cyberattacks Involving Pivot from IT-OT with Cyberphysical Impact

German Steel Mill
(2015)

Crash Override,
Ukraine Grid Attacks
(2015, 2016)

Petya
Ransomware
Attacks (2017)



More than DDoS, e.g. Mirai

Casino Gets Hacked Through Its Internet-Connected Fish Tank Thermometer

RENAULT

NISSAN

Transportation

Germany's Deutsche Bahn national railway operator

NHS England

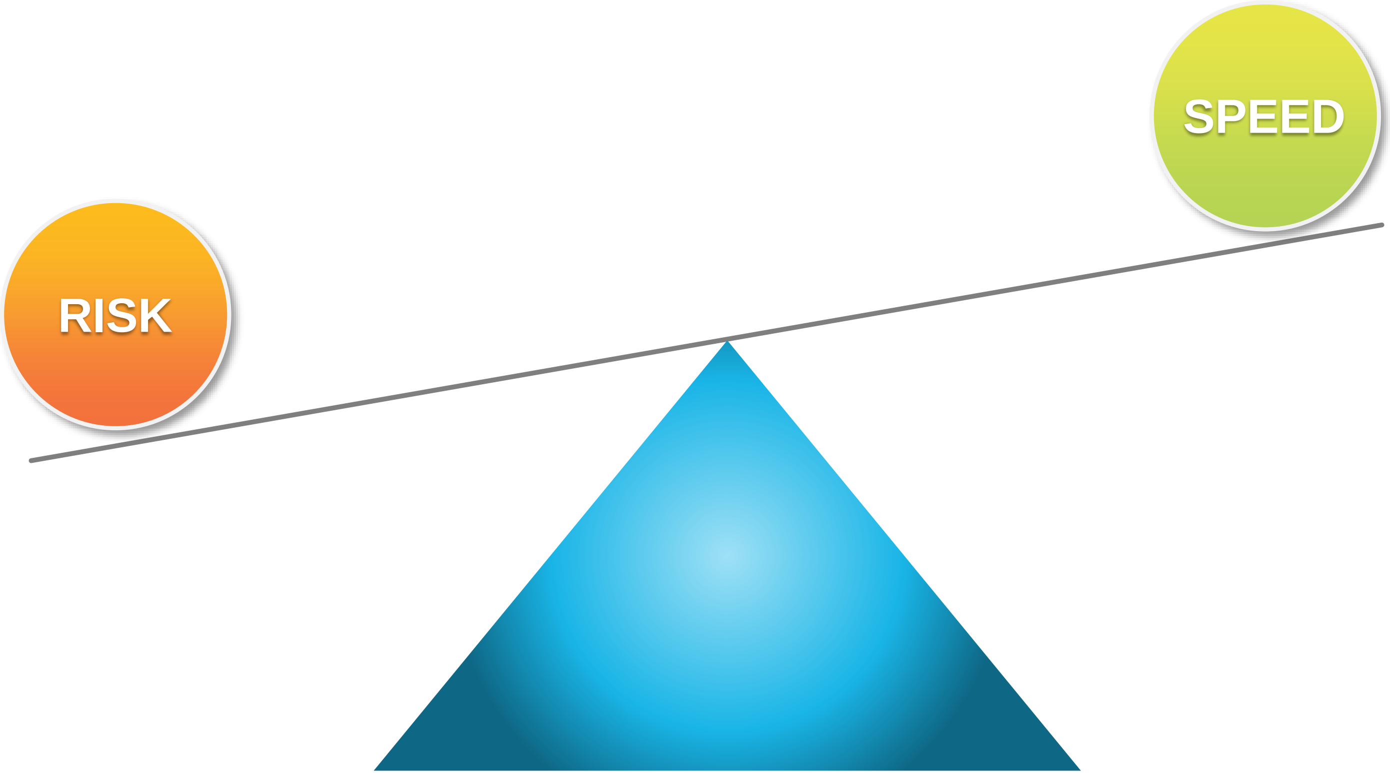
Medical Equipment

MRI machines from a major US device maker were affected

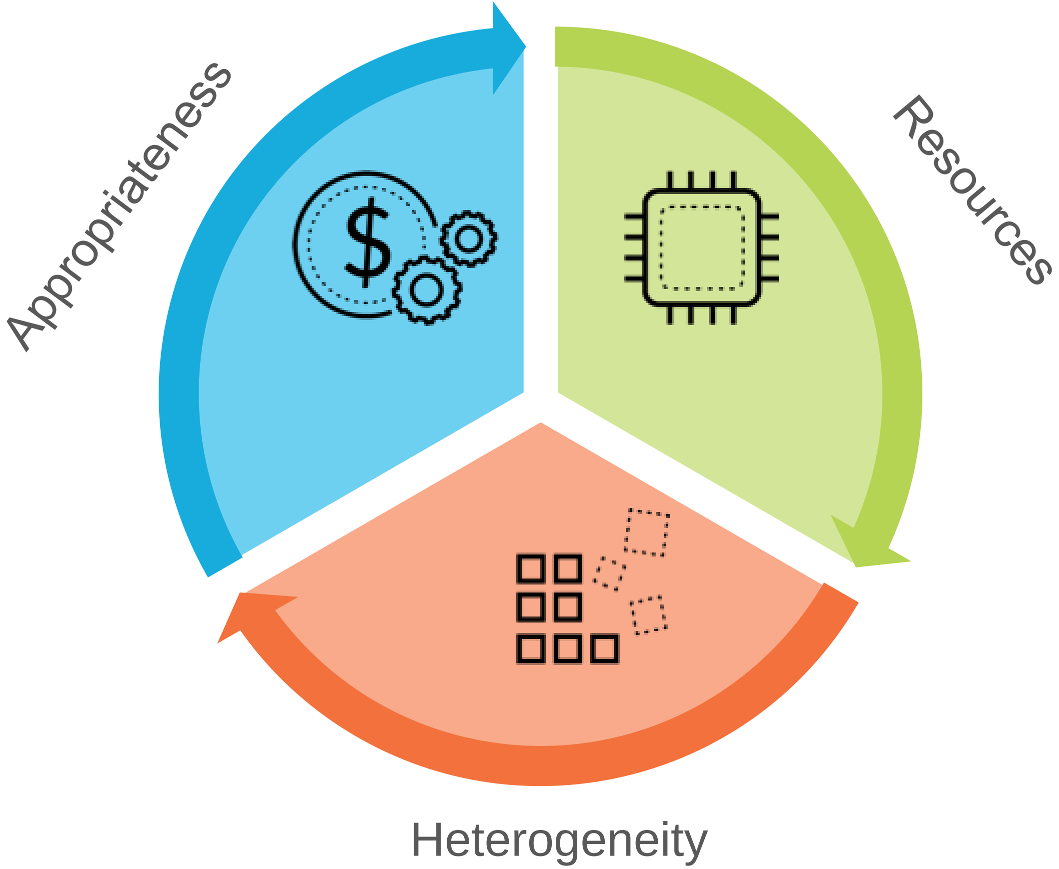
Q-Park

Payment systems were affected

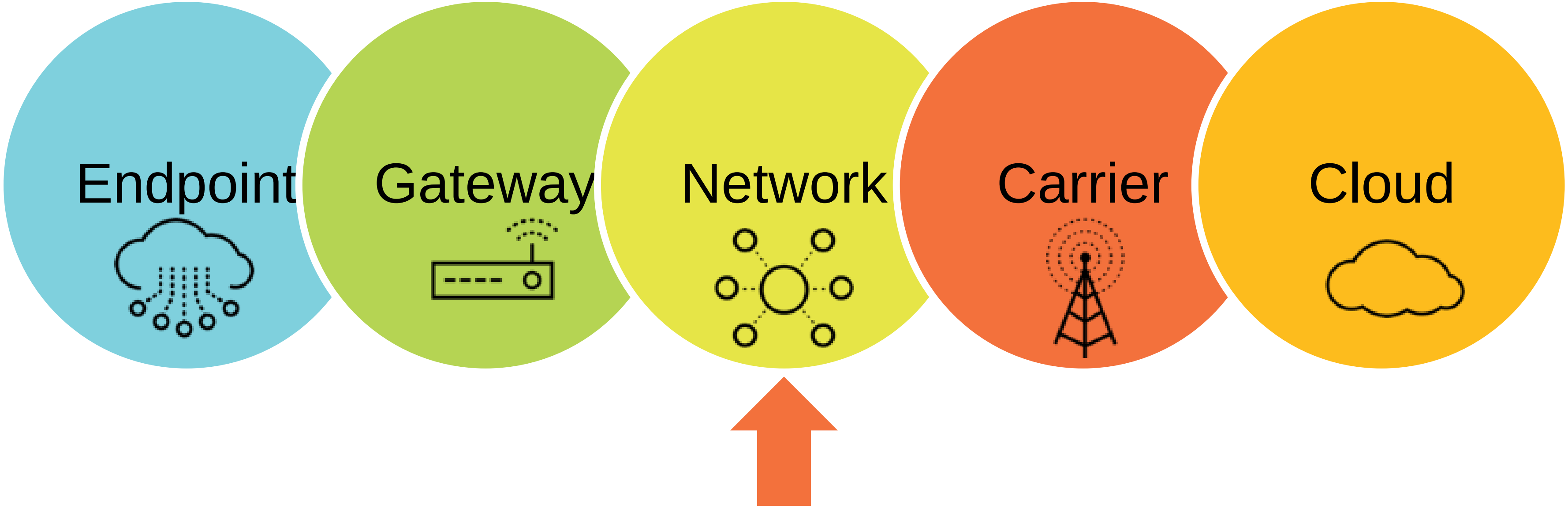
THE CHALLENGE FOR IT LEADERS



The challenges with IoT device security



Network Security – Biggest bang for the buck



Endpoint

Gateway

Network

Carrier

Cloud

Secure the Network with a

Zero-Trust Mindset and Approach

TRUST is a dangerous

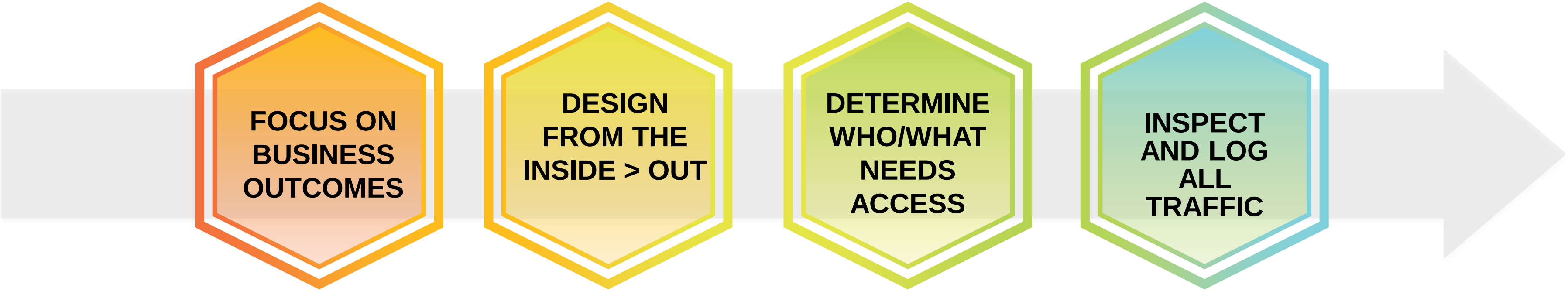
VULNERABILITY

that is EXPLOITED

by

MALICIOUS actors

ZERO TRUST DESIGN CONCEPTS



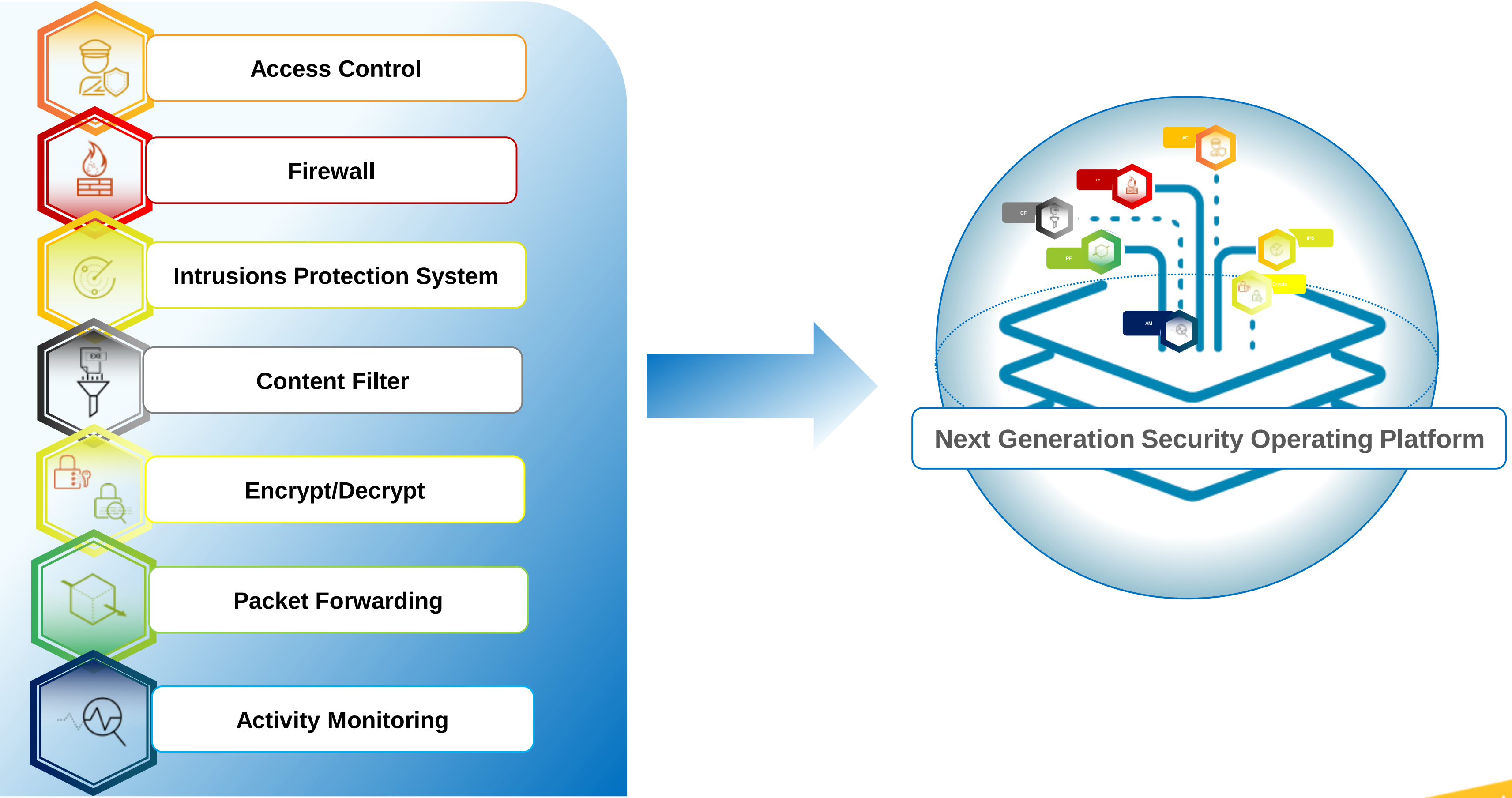
FOCUS ON BUSINESS OUTCOMES

DESIGN FROM THE INSIDE > OUT

DETERMINE WHO/WHAT NEEDS ACCESS

INSPECT AND LOG ALL TRAFFIC

Segmentation Gateway, Micro-Perimeters



Access Control

Firewall

Intrusions Protection System

Content Filter

Encrypt/Decrypt

Packet Forwarding

Activity Monitoring

Next Generation Security Operating Platform

A ZERO TRUST STRATEGY REDUCES ATTACK OPPORTUNITIES

PROBLEM

FREE ACCESS INCREASES RISK

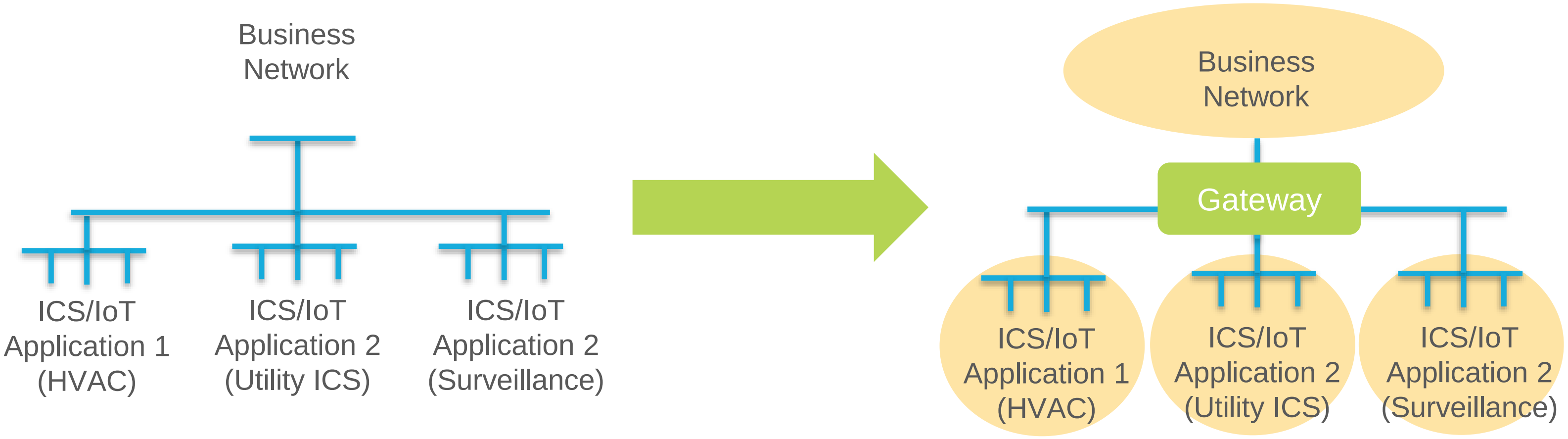
ACTION

LIMIT ACCESS TO SENSITIVE DATA

BENEFIT

REDUCE INCIDENT VOLUME

Network Segmentation is fundamental


Business Network
ICS/IoT Application 1 (HVAC)
ICS/IoT Application 2 (Utility ICS)
ICS/IoT Application 2 (Surveillance)
Business Network
Gateway
ICS/IoT Application 1 (HVAC)
ICS/IoT Application 2 (Utility ICS)
ICS/IoT Application 2 (Surveillance)

Set yourself up for Zero-trust

- ❑ Visibility and enforcement (granular)
- ❑ Segment IT from OT
- ❑ Create IoT application clusters

IT Applications vs. ICS/IoT Applications

Modbus

DNP3

Profinet IO

OPC

MQTT

CIP EtherNet/IP

OSIsoft PI

Schneider Oasys

Synchrophasor

GE EGD

IP-based protocols which could be secured by Next-generation Firewalls

SCADA remediation effort	IoT Initiative
Establish a DMZ between ICS and city network	
Upgrade legacy systems that have know vulnerabilities and/or losing vendor support	
Develop cybersecurity policy and procedures for SCADA	
Create zones within the ICS to provide barriers to contain malware and limit breaches	
Generate an ICS strategic plan and perform a risk assessment	

Device awareness leads to more granular and secure zero-trust policies

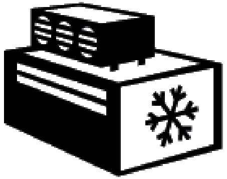
?

Device

Known IP

Unknown Device

Vs.



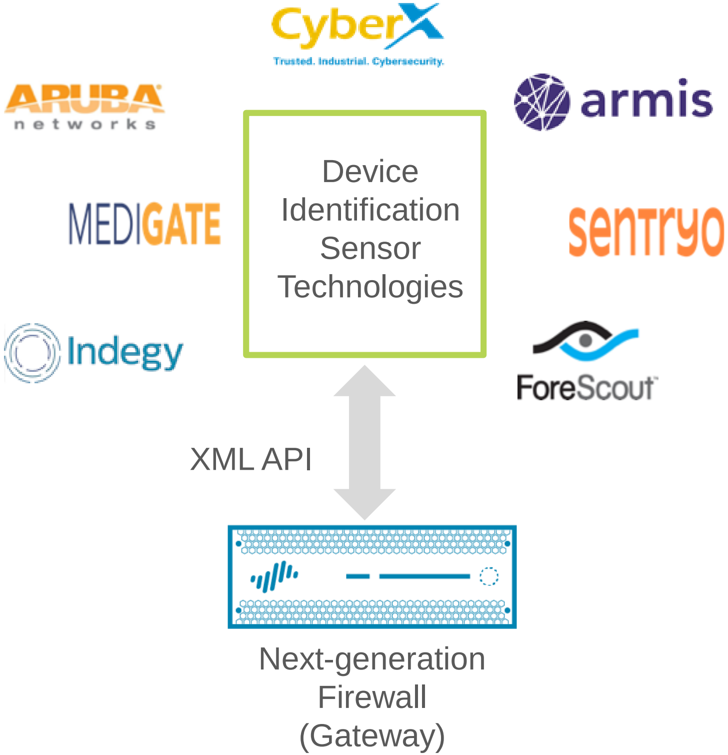
Known IP

Known Device

- **Type: Chiller**
- **Vendor: Berg**
- **Protocol: Modbus, SSH, and HTTPS**
- **Vulnerabilities**

Action	Device	From Zone	To Zone	Application
Allow	Chiller	HVAC	Operator	Modbus, SSH, HTTPS

Automated IoT Policy Creation and Threat Response



Device Identification Sensor Technologies

XML API

Next-generation Firewall (Gateway)

- API Integration: Sensor ⬄ NGFW
- Automated Policy Creation & Threat Response
  - Assign polices to IoT devices
  - Quarantine or limit network access of IoT devices or communication between IoT devices
- Value
  - Better situational awareness
  - Automatically reduce attack surface
  - Real-time threat prevention
  - Reduced operational burden

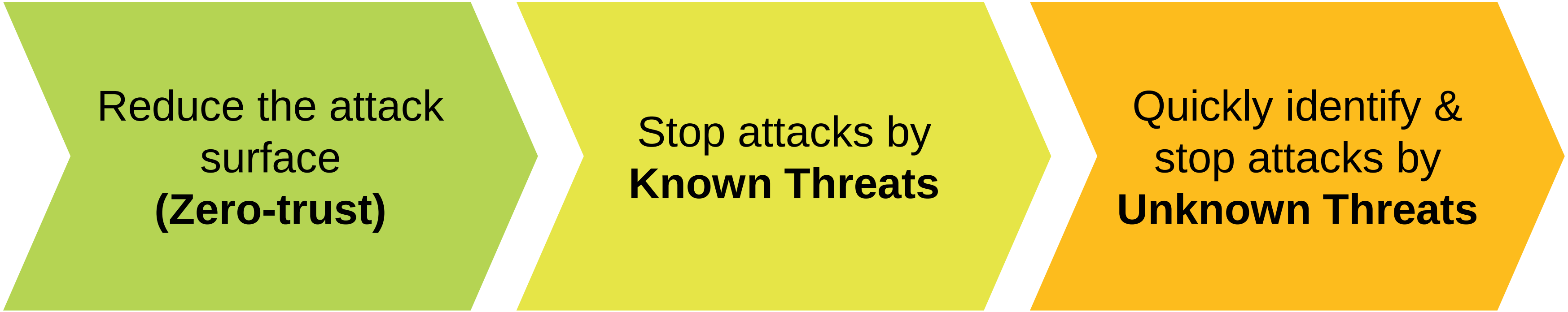
Section Key Take-aways

- IT-OT integration is a runaway train that cannot be stopped – Plan for it
- Zero-trust mindset reduces your attack surfaces – Apply it to IoT
- Risk-based approach can help determine your segmentation strategy

Questions to Ask Your Self & Organization

- ❑ How segmented is our IT and OT?
  - ❑ Are my IoT/ICS application clusters separated?
- ❑ Do we have policies defined for our IoTs? For admins/vendors interacting with IoTs?
- ❑ Are our policies granular or coarse grained?
- ❑ Do we know what IoTs are in our network?
- ❑ Can I detect IoT misbehavior? What is IoT ”proper” behavior?
- ❑ Are we able to quarantine or limit IoT device access to the network in the event of an attack?

When ”bad” things get in ...



Reduce the attack surface **(Zero-trust)**

Stop attacks by **Known Threats**

Quickly identify & stop attacks by **Unknown Threats**

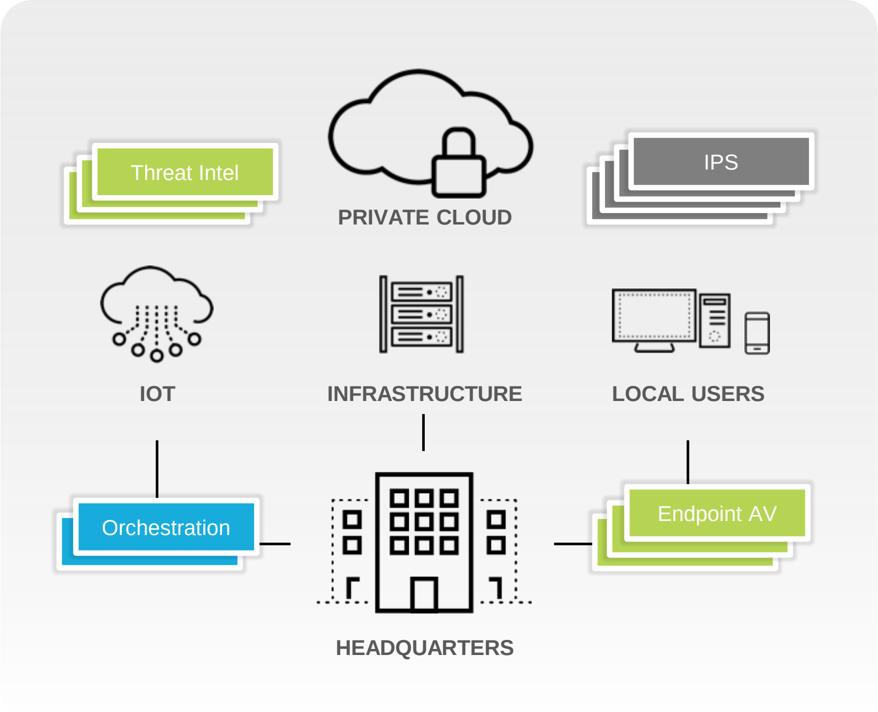
- IPS / IDS
- URL Filtering
- Endpoint protection

- Sandbox
- Behavioral Analytics
- Advanced Endpoint protection

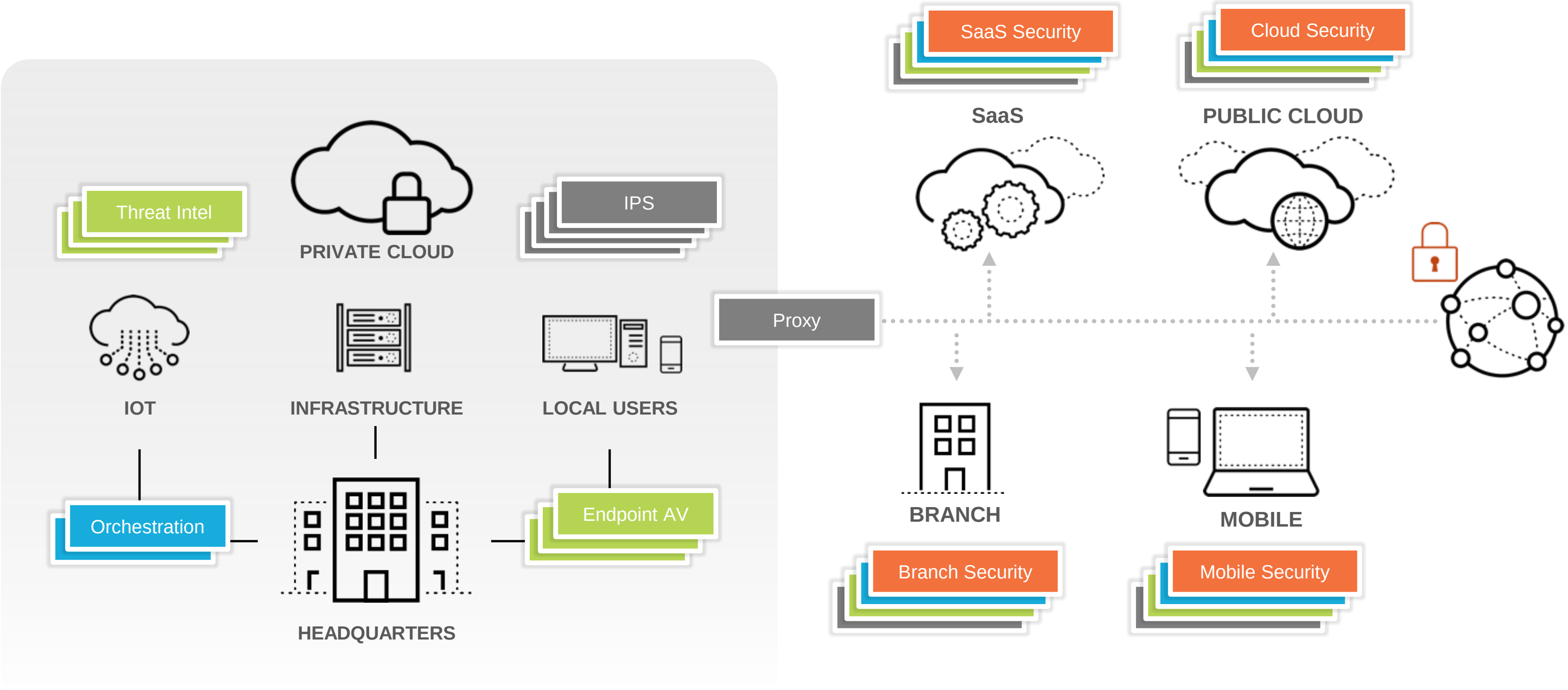
Automation?

Threat intelligence?

DISCONNECTED TOOLS DON'T PROVIDE EFFECTIVE SECURITY



TOTALLY INEFFECTIVE FOR CLOUD, IoT AND MOBILE WORKFORCE



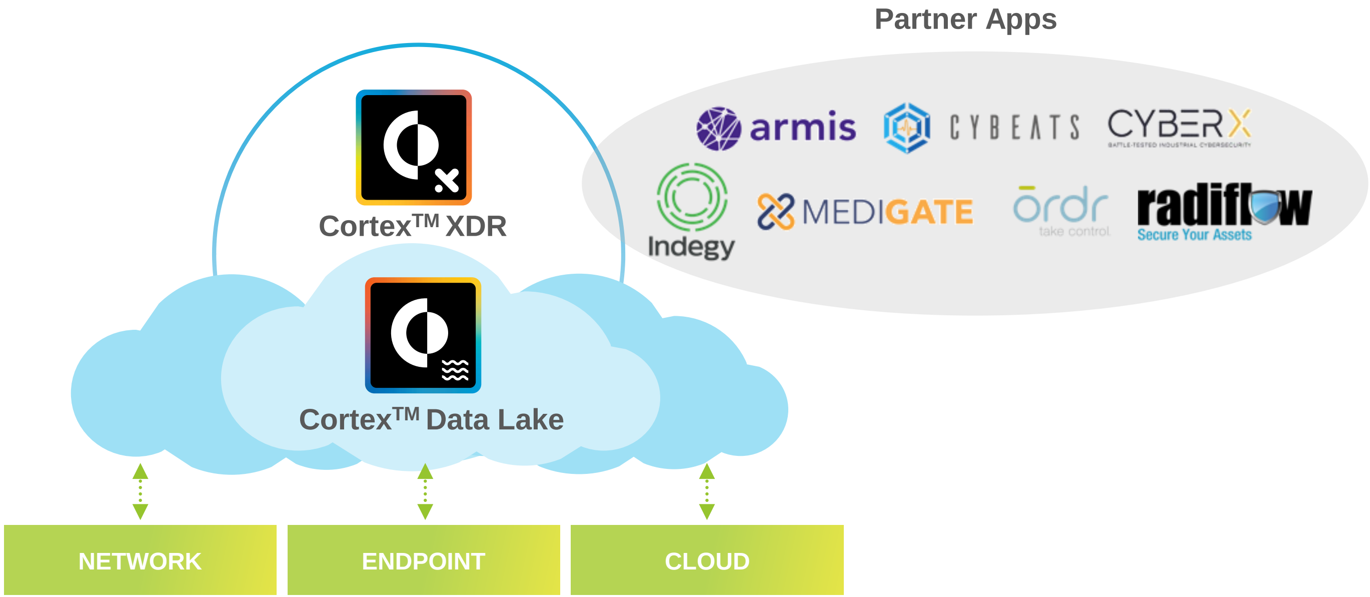
SECURITY MUST TRANSFORM

ANALYTICS

AUTOMATION

CLOUD-DELIVERED

Securing the Future with Cortex and Cortex XDR



Partner Apps

Cortex^{TM} XDR

Cortex^{TM} Data Lake

NETWORK

ENDPOINT

CLOUD

Automatically detect attacks using rich data & cloud-based behavioral analytics

Accelerate investigations by stitching data together to reveal root cause

Tightly integrate with enforcement points to stop threats & adapt defenses

Section Key Take-aways

- Hardening systems cannot fully prevent successful attacks
- Must implement technologies that stop both known and unknown threats at the network, endpoint and the cloud
- Threat intelligence should aggregate multiple sources and make them accessible to the network, endpoint, and cloud
- An approach based on combining disjoint point products is not the answer
  - Cybersecurity ineffectiveness and operational burden are exacerbated
- A prevention-focused platform which provides automation is required

Questions to Ask Your Self & Organization

- ❑ Do we have disjointed point products for IPS, URL Filtering and Sandboxing protecting our devices and networks across the IoT value chain?
- ❑ Have we starting evaluating behavioral analytics technologies?
- ❑ How are we addressing these capabilities to secure our IoT infrastructure in AWS/Azure/GCP?
- ❑ Is there an opportunity to reduce the number of products/vendors for the above functions?