
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

SEC331

Security at the industrial edge

Ryan Dsouza
Principal Solutions Architect
AWS

Emir Ayar
Edge Prototyping Tech Lead
AWS

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

- Introduction to the industrial edge
- Security challenges in Industrial IoT
- Golden rules to secure OT/IIoT solutions
- Industrial edge security demo
- Chalk talk Q&A
- Wrap up

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

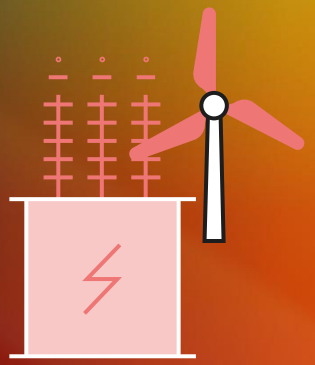
Industrial edge is used across industries



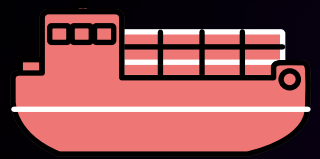
Discrete & process manufacturing



Buildings & cities



Power & utilities, renewables



Transportation & logistics



Mining



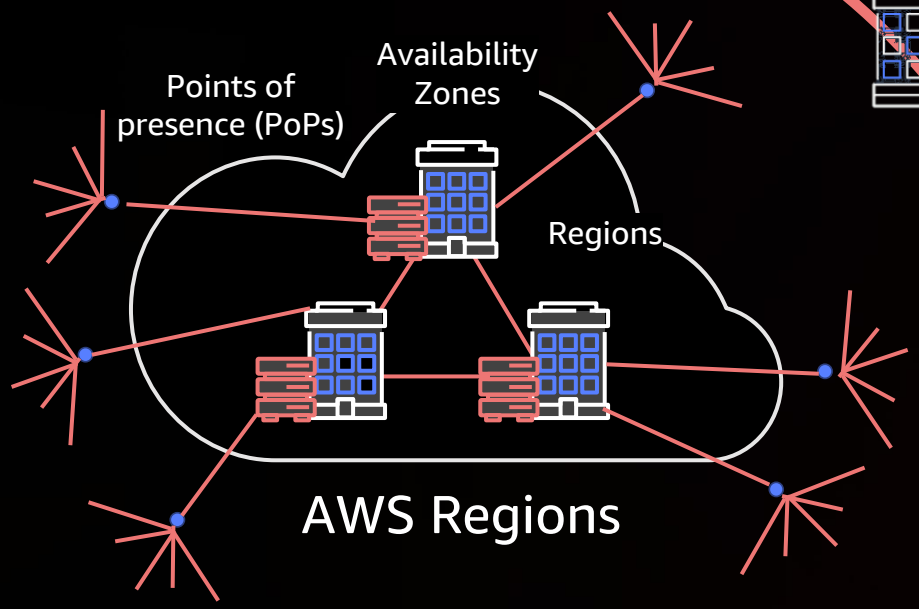
Energy (oil & gas)

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Cloud-to-edge continuum

For many use cases



For low latency, local data processing, and data residency

On premises
AWS Outposts

Metro centers
AWS Local Zones

5G networks
AWS Wavelength

IoT/robotics/ML
AWS IoT Greengrass
AWS IoT SiteWise Edge
FreeRTOS
AWS RoboMaker
Amazon Monitron
AWS Panorama

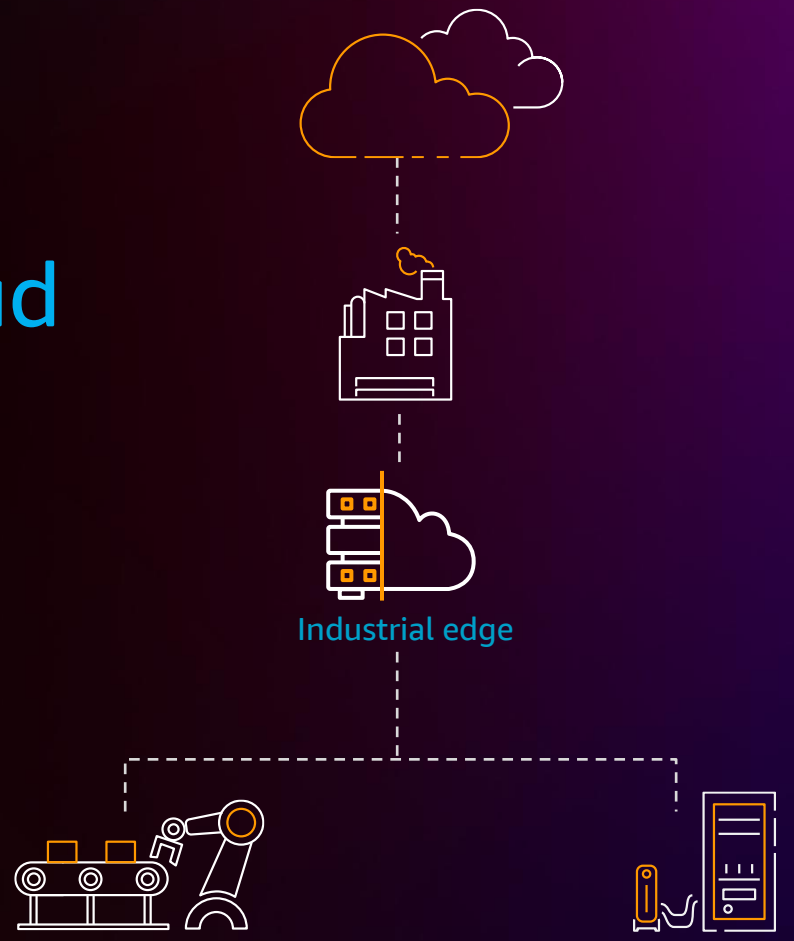
Rugged/austere edge
AWS Snowball
AWS Snowcone

Cloud continuum

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

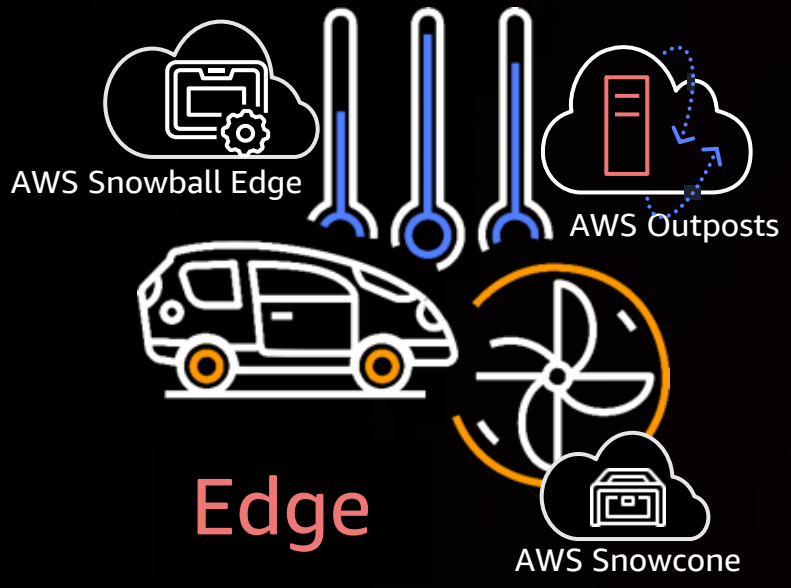
What is the industrial edge?

A compute and storage platform within the four walls of a factory or industrial facility which extends cloud services to these environments



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Running workloads at the edge is challenging



Law of
physics

Law of
economics

Law of
the land



aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Industrial edge: Compute & storage

SIEMENS

BECKHOFF

ONLOGIC

ADLINK TECHNOLOGY INC.



Industrial PC

vSphere
VMWare



AWS Snowcone



AWS Snowball Edge

AWS OUTPOSTS FAMILY

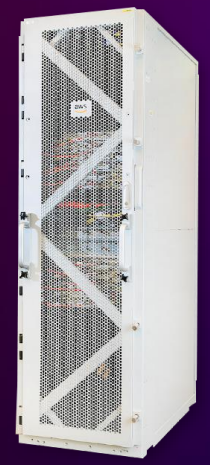
1U SINGLE SERVER



2U SINGLE SERVER



42U FULL RACK



Line side ⟷ Data center

Amazon CloudWatch

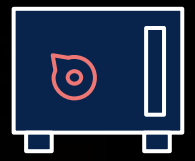
AWS Systems Manager

IAM

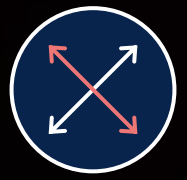
AWS CloudTrail

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

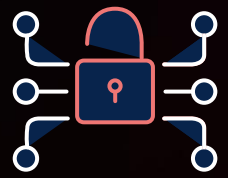
Some security challenges in OT & IIoT



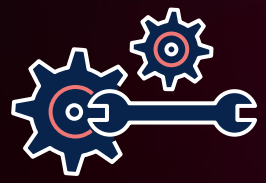
General lack of cyber risk mitigation



Inflexible change control procedures



Inconsistent endpoint visibility



Security update challenges



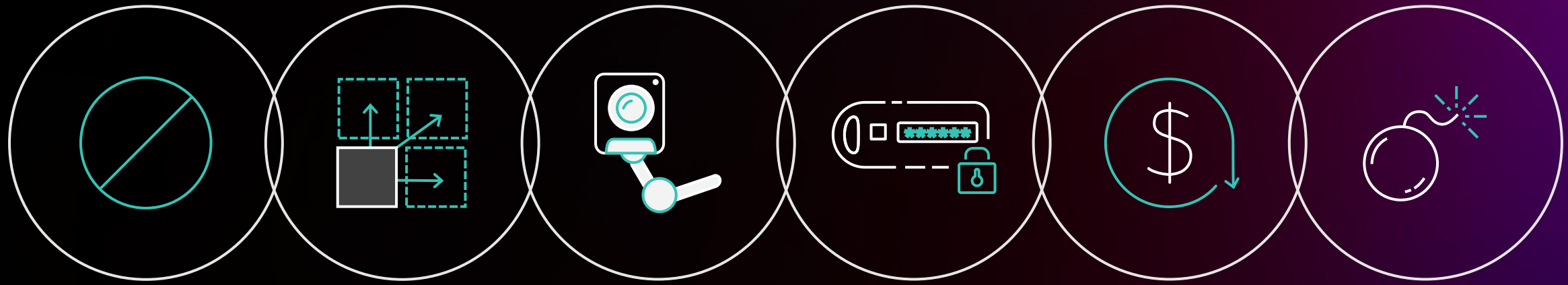
Insecure legacy industrial protocols

Safety and reliability

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Edge security use cases



Denial of service

Devices are engaged in DoS attacks against an external host

Lateral threat escalation

Unauthorized user gains initial access and moves through the network with increased privileges

Surveillance

Malicious code is used to surveil user activities and to obtain credentials for reconnaissance

Sabotage attacks

Malware-infected devices cause damage or disruption

Cryptocurrency mining

Devices are infected by cryptomining code and used in mining cryptocurrency

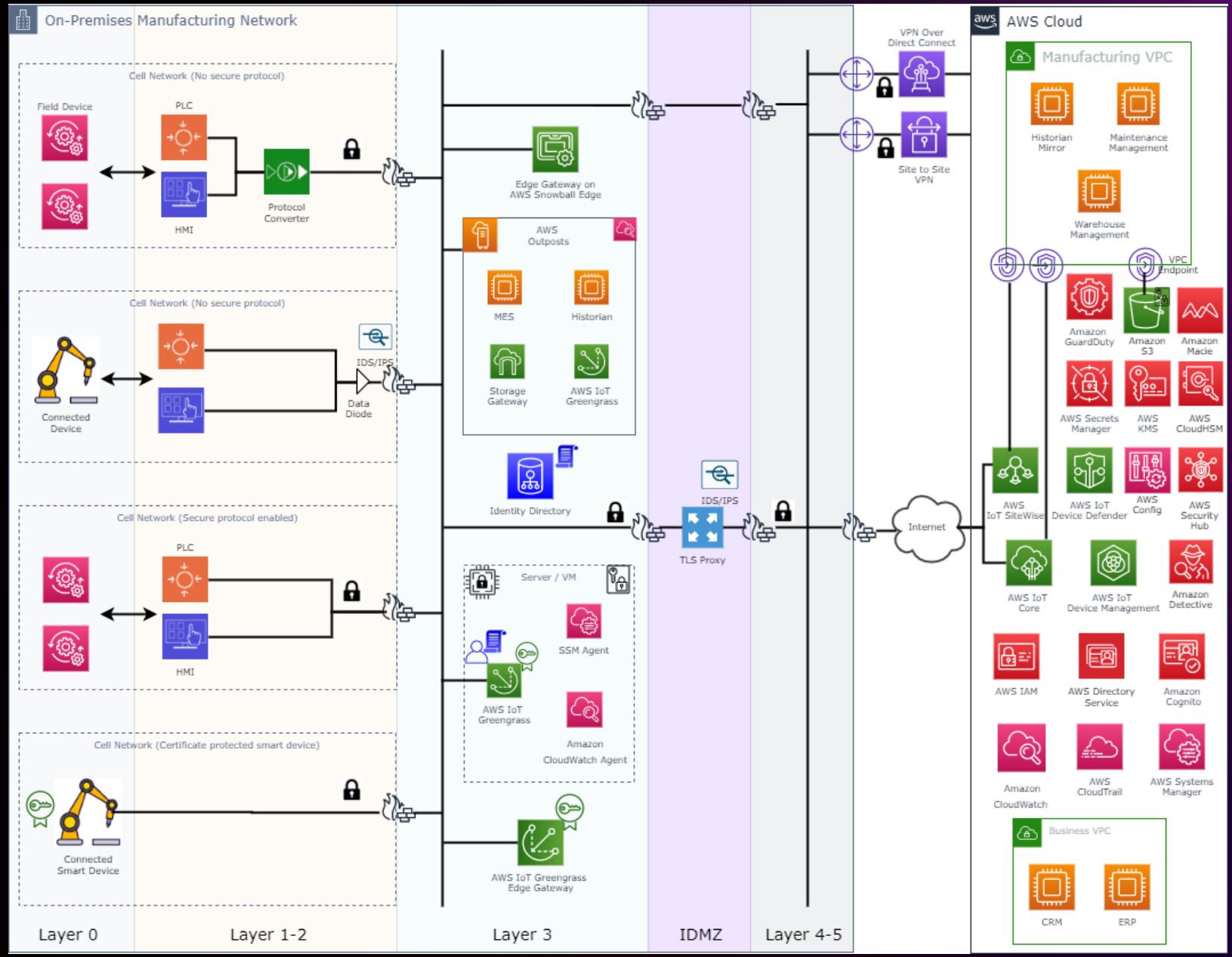
Ransomware & data exfiltration

Users lose access to their data on a device due to encryption employed by ransomware or data is exfiltrated

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

IIoT security architecture



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Golden rules for IIoT security

1. **Cybersecurity risk assessment and network segmentation**
   Conduct a cybersecurity risk assessment – prioritize and group assets into security zones and tighten the trust boundary using micro-network segmentation, firewalls, and unidirectional gateways; isolate or disconnect insecure assets from the network
2. **Asset inventory and network architecture**
   Maintain an asset inventory of all connected assets – categorize them by safety, criticality, patchability, suitability for air-gapped environments, etc.; create a network architecture showing interconnection between assets and their relationships
3. **Identity and access management**
   Provision modern IIoT devices and systems with unique identities and credentials; apply authentication and access-control mechanisms
4. **Patch management**
   Prioritize and implement OT- and IIoT-specific patch management and software- and firmware-update mechanisms; check software integrity to ensure safety and availability of production systems
5. **Encrypt data at rest**
   Secure manufacturing data at the edge and in the cloud by encrypting data at rest; create mechanisms for secure data sharing, governance, and sovereignty

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Golden rules for IIoT security

6. **Encrypt data in transit**
   Whenever possible, use cryptographic network protocols for data, monitoring, administration, provisioning, and deployments; convert insecure protocols into standardized secure protocols as close to the source as possible
7. **Harden and securely manage connected resources and establish secure network connections**
   Harden internet connected resources; establish secure connections to cloud services and secure remote access to on-premises resources
8. **Auditing and monitoring**
   Deploy security auditing and monitoring mechanisms across OT and IIoT and centrally manage security alerts across OT, IIoT, and cloud
9. **Incident response**
   Create incident response playbooks and build automation as your security response matures to contain events and return to a known good state
10. **Business continuity and disaster recovery**
    Create a business continuity and recovery plan including a plan for backups and cybersecurity testing

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Key elements of AWS IIoT security



Connected asset inventory	Identity and access control	Patching and software updates	Secure edge gateway	Secure cloud connections and secure remote access	Data security	Auditing and monitoring	Alert and mitigate	Backup and recovery
#2	#3	#4	#7	#7	#5 & #6	#8	#8 & #9	#10
AWS IoT Device Management	AWS IoT	AWS IoT jobs	AWS IoT Greengrass	Direct Connect	TLS 1.2	CloudWatch	AWS IoT Device Management	AWS Backup
AWS Systems Manager	AWS IAM	AWS Systems Manager	Secure elements	Secure VPN	AWS KMS	CloudTrail	AWS IoT Device Defender	AWS IoT Greengrass
	Amazon Cognito		Secrets Manager	IoT tunneling	AWS IoT SDK	AWS IoT Device Defender	Amazon SNS	Storage gateway
				AWS Systems Manager		GuardDuty	AWS Systems Manager	
				VPC endpoints		Security Hub		

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Audit and monitor IoT devices with AWS IoT Device Defender

AWS IoT Device Defender is a fully managed IoT security service that enables customers to secure their fleet of connected devices on an ongoing basis



Audit

Validate IoT configuration is secure

Detect

Detect anomalies in device behavior

Alert

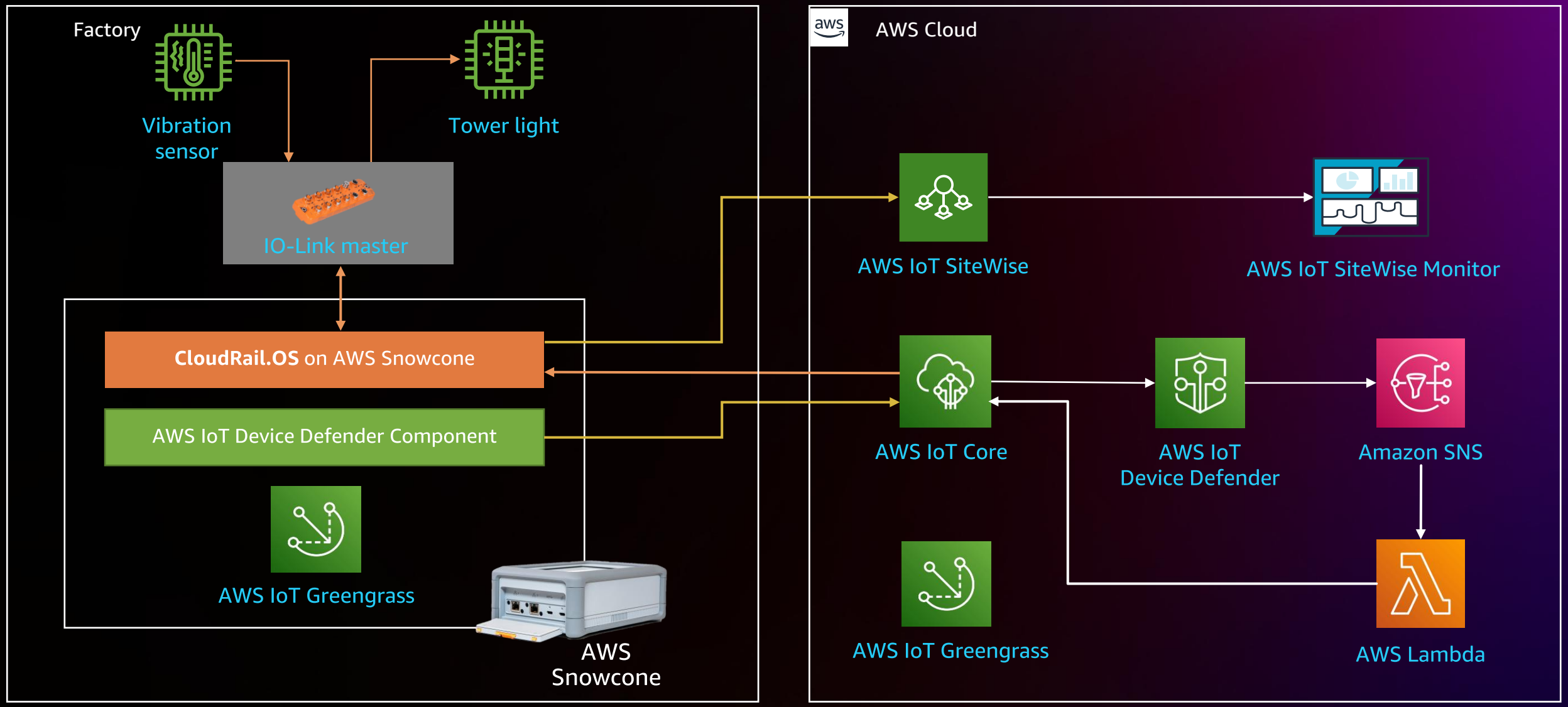
Know when and what to investigate

Mitigate

Remediate potential issues

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Edge security demo architecture



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Snowcone for industrial edge workloads

AWS managed appliance with integration to multiple AWS services

Simplifies OT/IT integration and securely bridges OT and IT networks

OT/IT

TPM for hardware root of Trust

CloudRAIL.OS

Interoperability with thousands of industrial sensors & actuators (secondary sensing)



Amazon EC2 computing or AWS IoT Greengrass functions for local data processing & ML@edge

All data is encrypted using 256-bit AWS KMS keys

Secure erasure following NIST guidelines for media sanitation

Operates on unconditioned power and in non-datacenter environments (0° to 45°C)

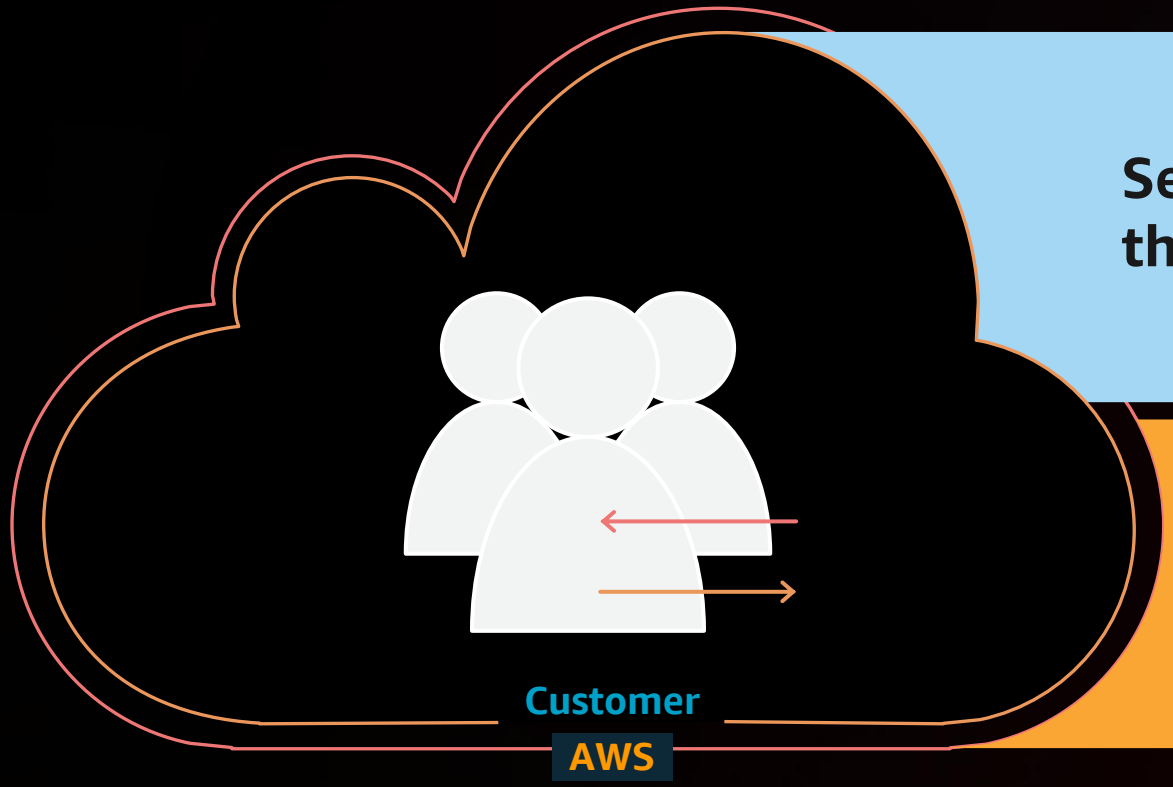
E Ink shipping label for tracking

Rugged, dust-tight, water- and wind-resistant, IP65, anti-tamper and tamper-evident enclosure handles vibration up to 50G RMS

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Shared responsibility model



Security IN the cloud

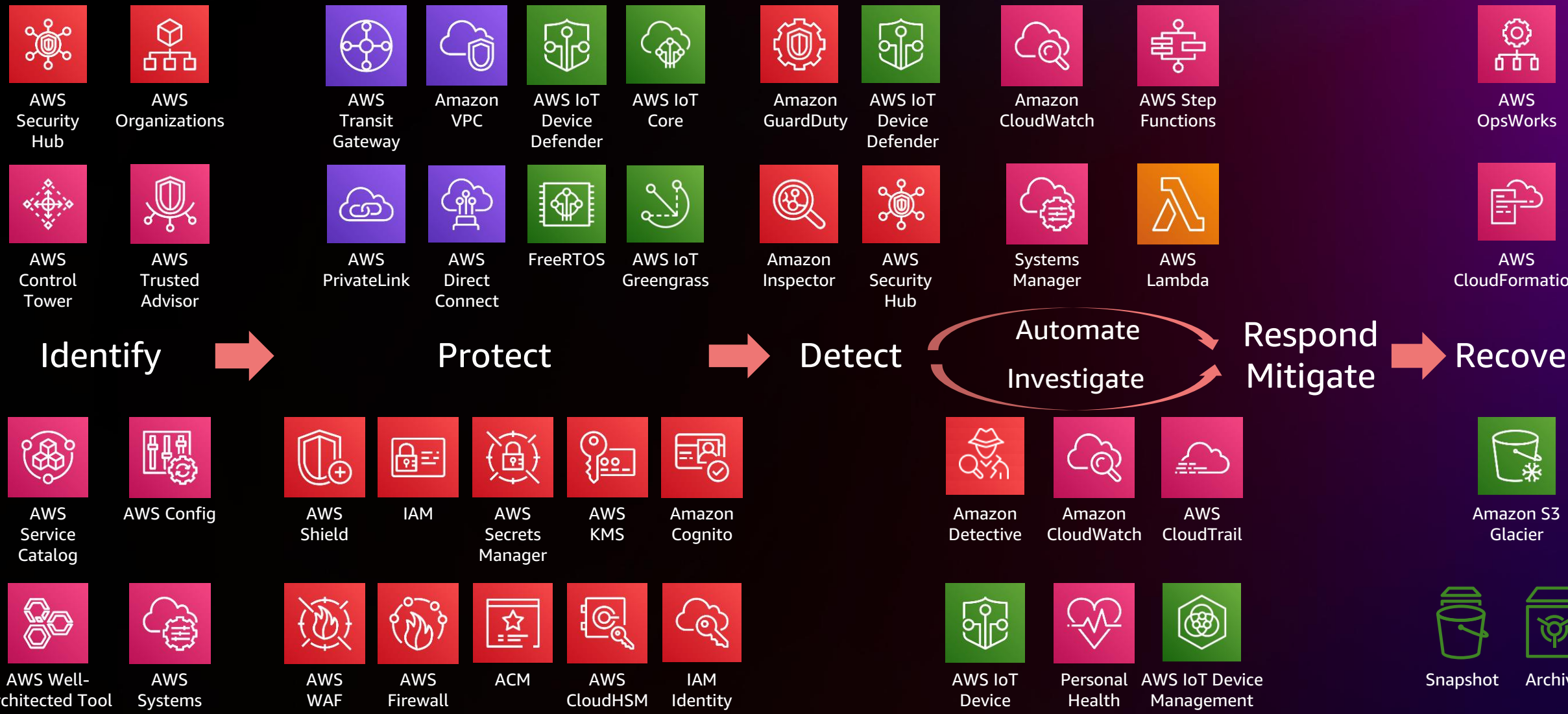
Customer responsibility will be determined by the AWS Cloud services that a customer selects

Security OF the cloud

AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS foundational and multi-layered security services



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Learn about security with AWS training and best practices

RESOURCES CREATED BY THE EXPERTS AT AWS TO HELP YOU BUILD AND VALIDATE CLOUD SECURITY SKILLS



30+ free digital courses cover topics related to cloud security, including Deep Dive into AWS IoT Security Primer, AWS IoT Authentication and Authorization, Introduction to Amazon GuardDuty, and Deep Dive on Container Security



Classroom offerings, such as Security Engineering on AWS, feature AWS expert instructors and hands-on activities



Well-Architected Framework, IoT Lens, IoT security best practices guide, OT Security whitepaper, Security Golden Rules, Security workshops



Validate expertise with the AWS Certified Security – Specialty exam

Visit the security learning path at https://aws.training/security

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Ryan Dsouza
rydsouza@amazon.com

Emir Ayar
emirayar@amazon.com



Please complete the session survey in the **mobile app**

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.