
AWS
re:Invent

IOT305

Elevating your IoT security with AWS's multi-layered security approach

Ryan Dsouza

Sr. IoT Solution Architect

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

IoT use cases & security challenges

AWS multi-layered security approach, principles, and services

Consumer IoT use case

Industrial IoT use case

Demo

Conclusion



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What are customers doing with AWS IoT?



Predictive maintenance



Wellness & health solutions



Remote patient monitoring



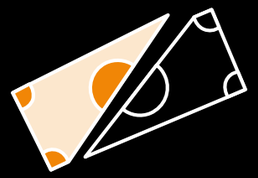
Connected buildings and city systems



Maintaining device fleets



Monitoring energy efficiency

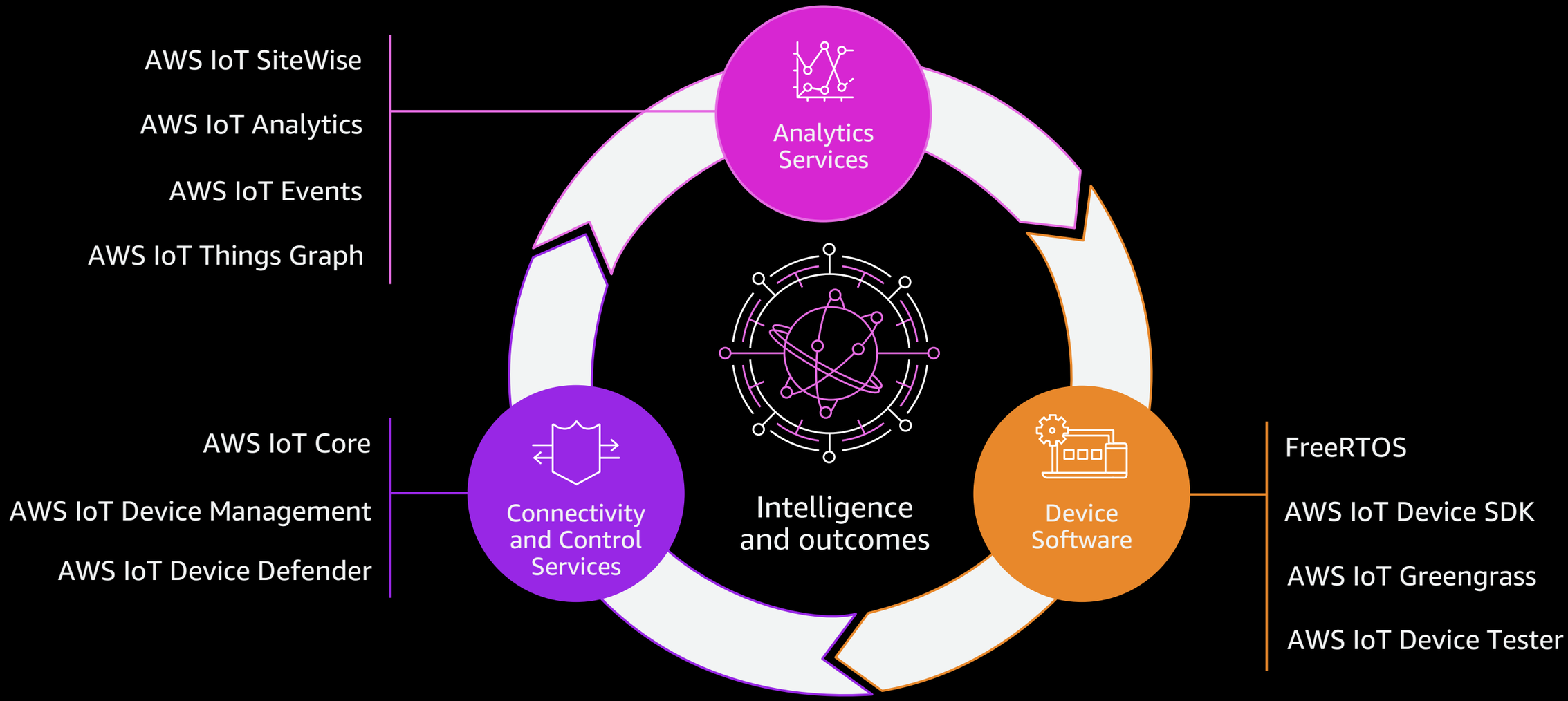


IoT payment and connected commerce

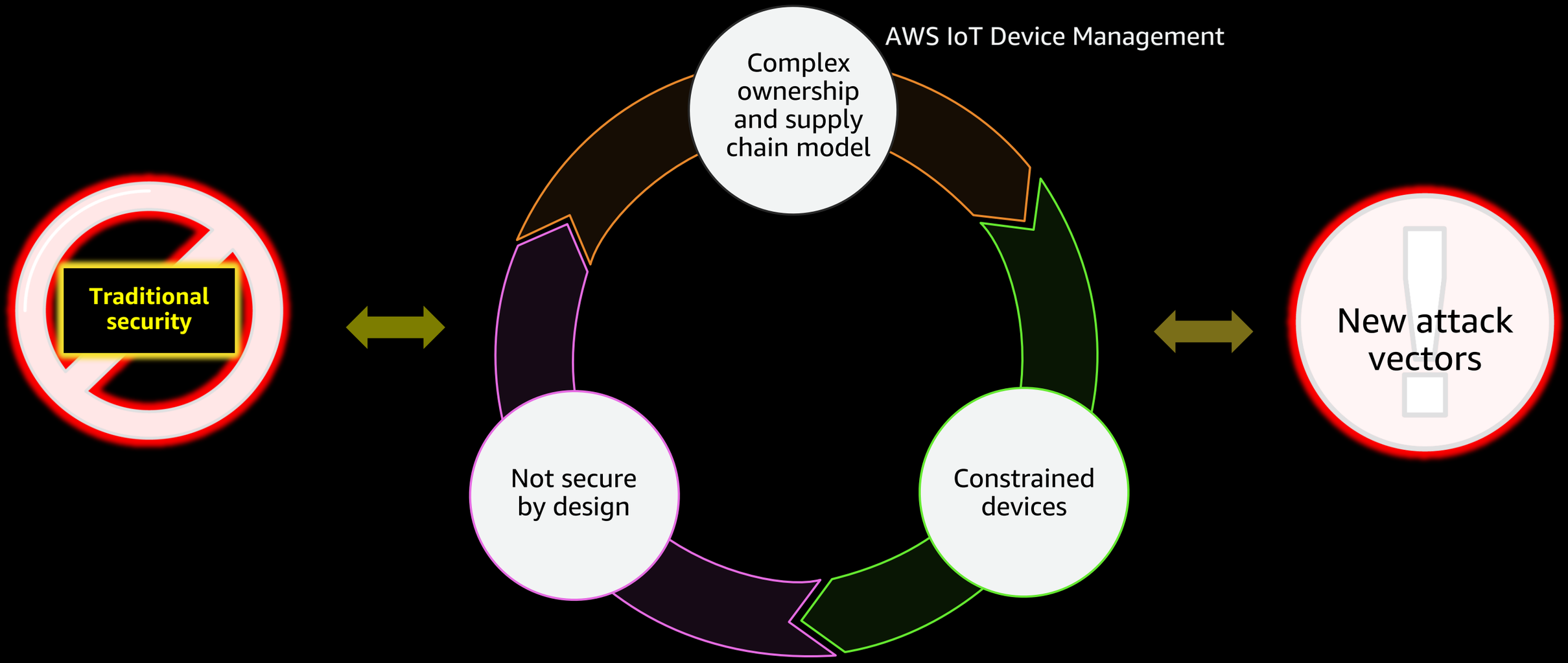


Optimizing manufacturing operations

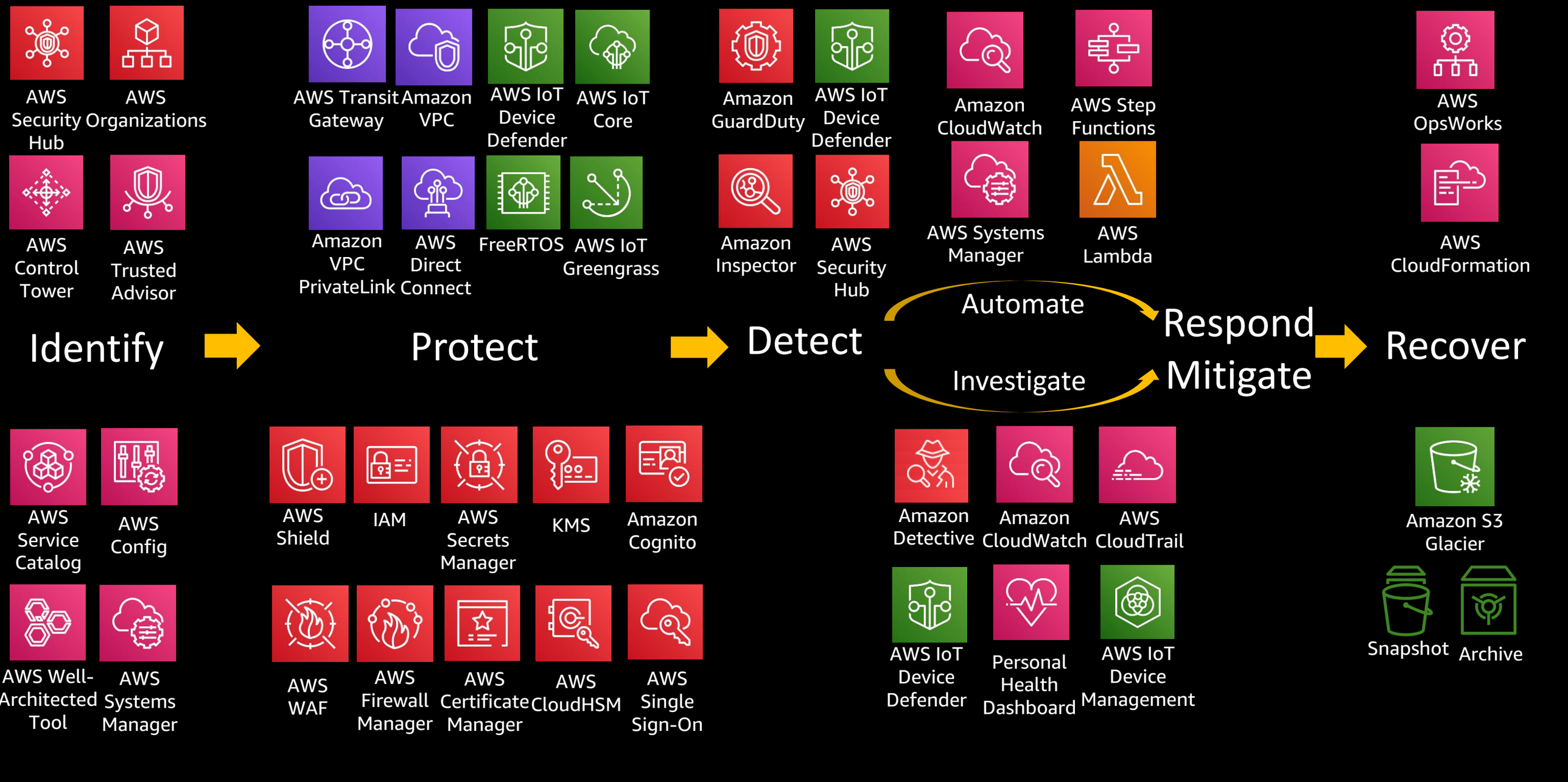
AWS IoT services



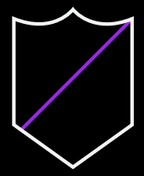
Challenges with IoT security



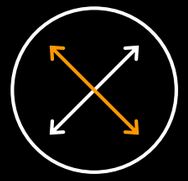
AWS Foundational and Multi Layered Security Services



IoT security principles



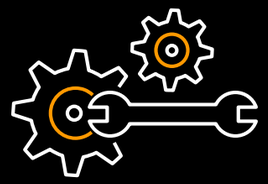
Unique Identity
and
Secure network
communication



Authorization
and
Least privilege



Patching
Remote access
Onboarding



Encryption of
Data in Transit
Data at Rest



Auditing
and
Monitoring



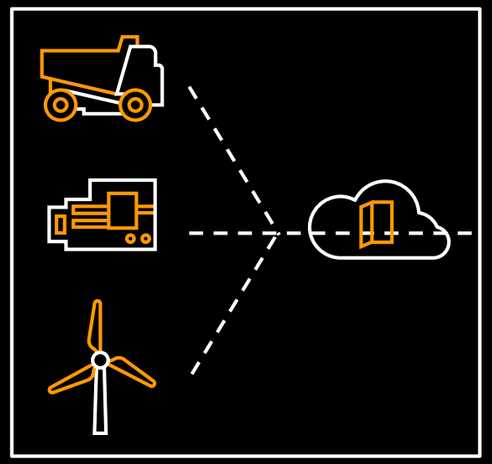
Alert, Remediation
and
Recovery

Multi layered security approach

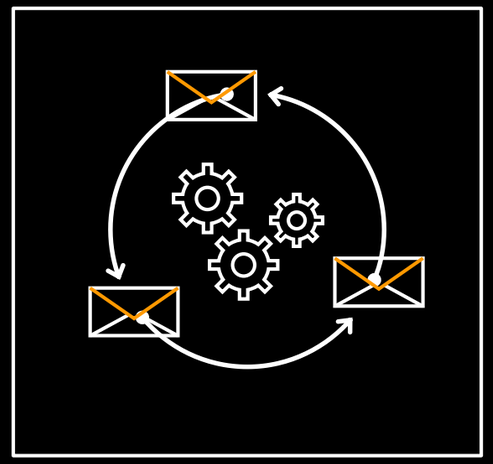
AWS IoT Core

Protect

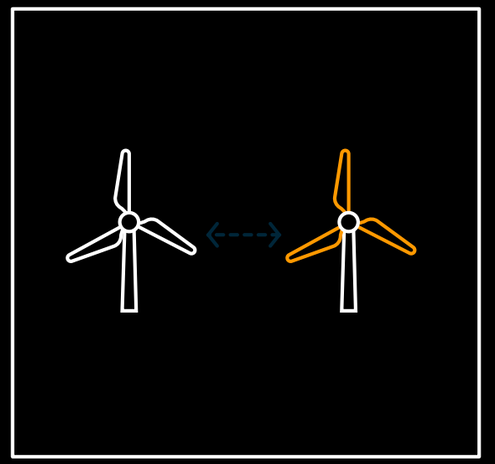
AWS IoT Core is a managed service that lets connected devices easily and securely interact with cloud applications and other devices.



To securely connect devices to the AWS cloud and other devices at scale



To route, process, and act upon data from connected devices



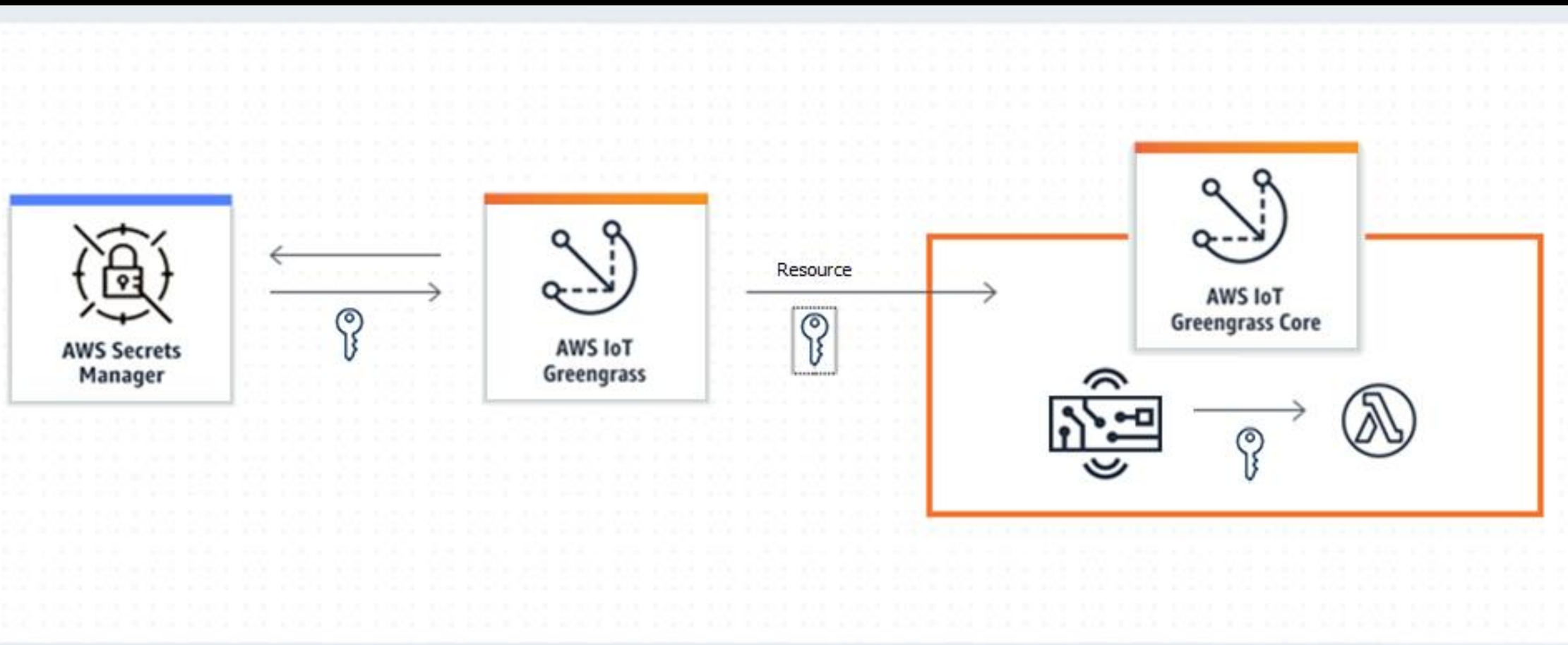
To enable applications to interact with devices even when they are offline



To fully integrate with other AWS services to reason on top of the data
(Analytics, Databases, AI, etc.)

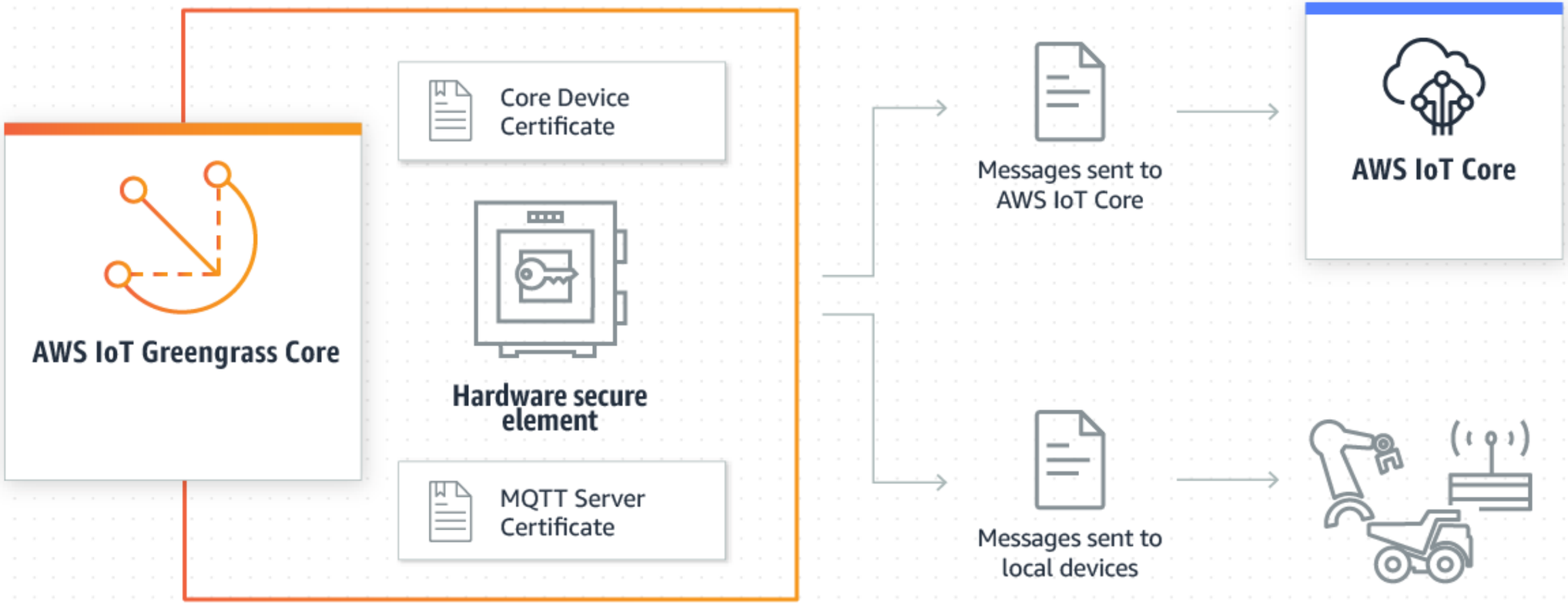
AWS IoT Greengrass Secrets Manager

Protect



AWS IoT Greengrass hardware security

Protect



Secure Tunneling

Securely access devices behind restricted firewalls

Protect and Respond

Securely open and close tunnel using API or the console

Access individual device using remote shell or remote desktop operations

Manage device authorization for each tunnel session using IAM permissions and configurable timeouts up to 12 hours

Automatically receive access token for each device via MQTT message



Software updates

Organize and trigger actions on groups of devices

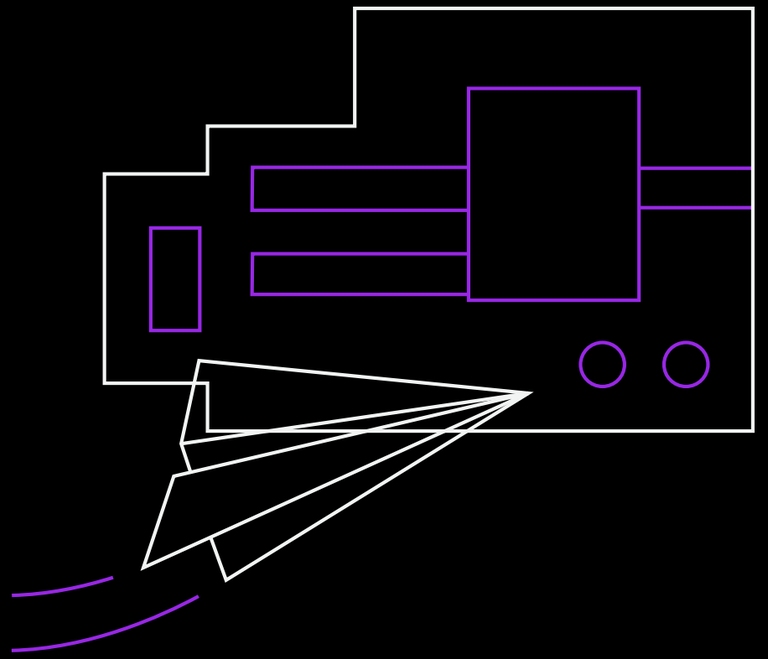
Protect and Respond

Receive status updates for individual devices to monitor your updates as they execute

Target groups of devices to update in bulk, or pinpoint single devices to update

Control your deployment velocity and set failure criteria to reduce the blast radius of any update

Digitally sign your jobs before they are sent to your devices to protect your devices from being compromised



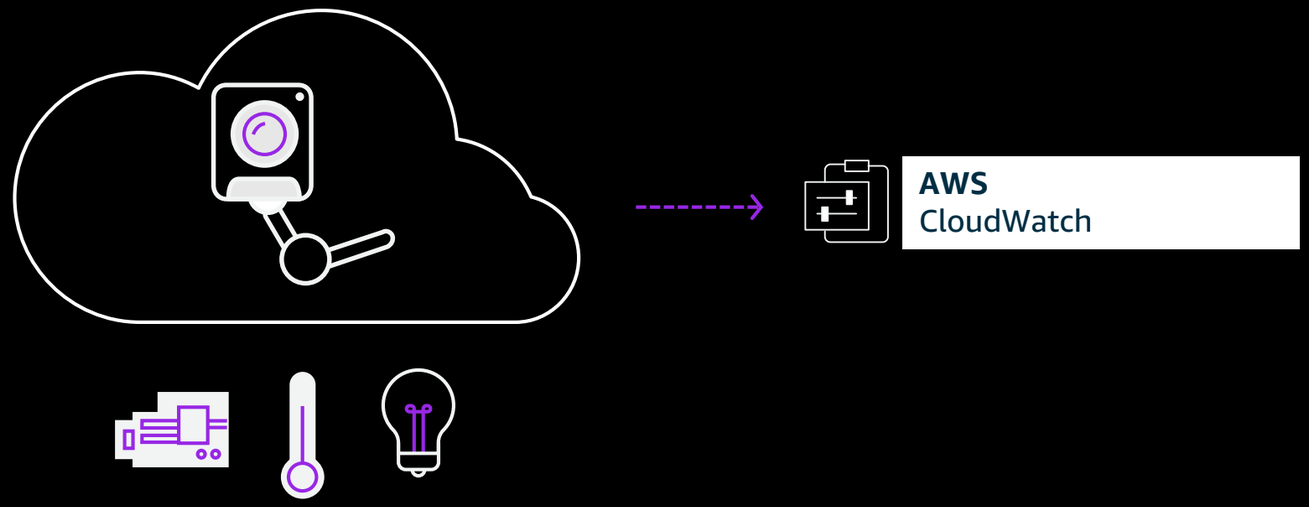
Fine-grained device logging and monitoring

Collect device logs to identify and remediate problems

Configure the logging level on a per device basis or on a group of devices

To troubleshoot an issue, you can selectively increase diagnostic levels across a subset of devices that are malfunctioning

Use AWS CloudWatch to configure alarms and search for your logs



AWS IoT Device Defender

Protect
Detect
Mitigate

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

Alerts

Know when & what to investigate

Mitigate

Remediate potential issues

Best IoT Security solution 2019 IoT World Awards

AWS IoT Device Defender ML Detect

Detect and Mitigate



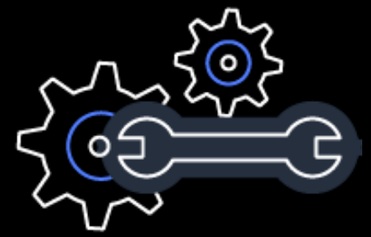
Enables onboarding
Detect quickly



No prior device behavior knowledge required



Adjusts to device data continuously

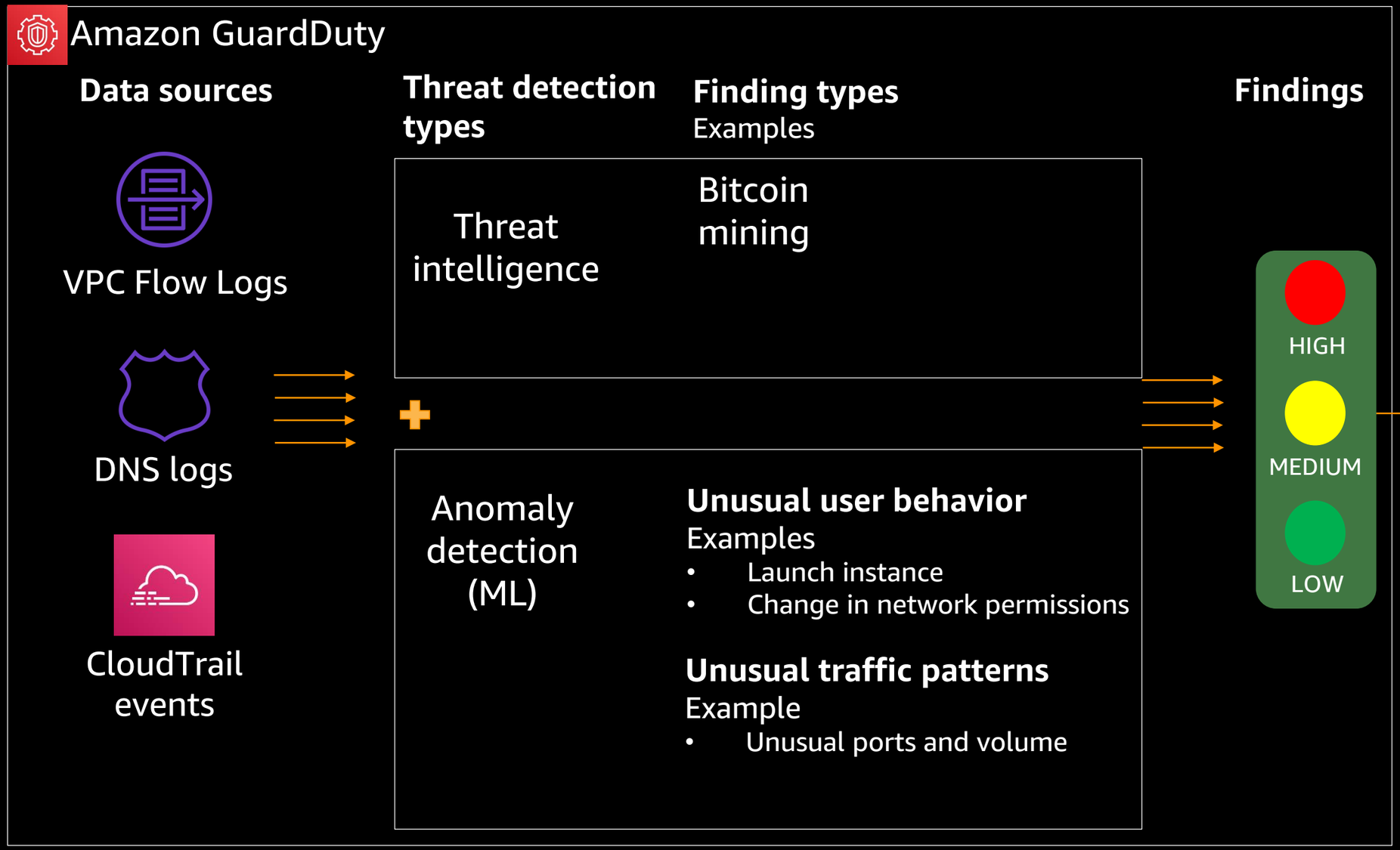


Provides predefined mitigation actions

Launched in public preview

Amazon GuardDuty

Detect and Respond



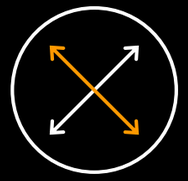
Key elements of AWS IoT security

AWS multi layered security approach and services



Unique Identity
and
Secure network
Communication

AWS IoT
IAM
MQTT & HTTPS



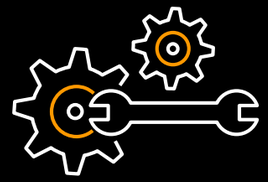
Authorization
and
Access control

IoT Policies
IAM Policies



Patching
Remote access
Onboarding

IoT Device
Management
Systems
manager



Encryption
Transit
Rest

TLS 1.2
KMS



Auditing
and
Monitoring

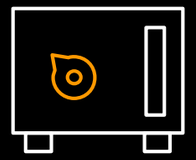
CloudWatch
CloudTrail
Device Defender
GuardDuty



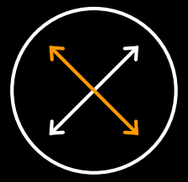
Alert
and
Mitigate

IoT Device
Management
Device Defender
SNS

Elevate your security with the AWS Cloud



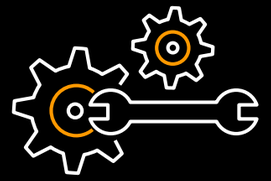
Inherit global security and compliance controls



Scale with superior visibility and control



Highest standards for privacy and data security



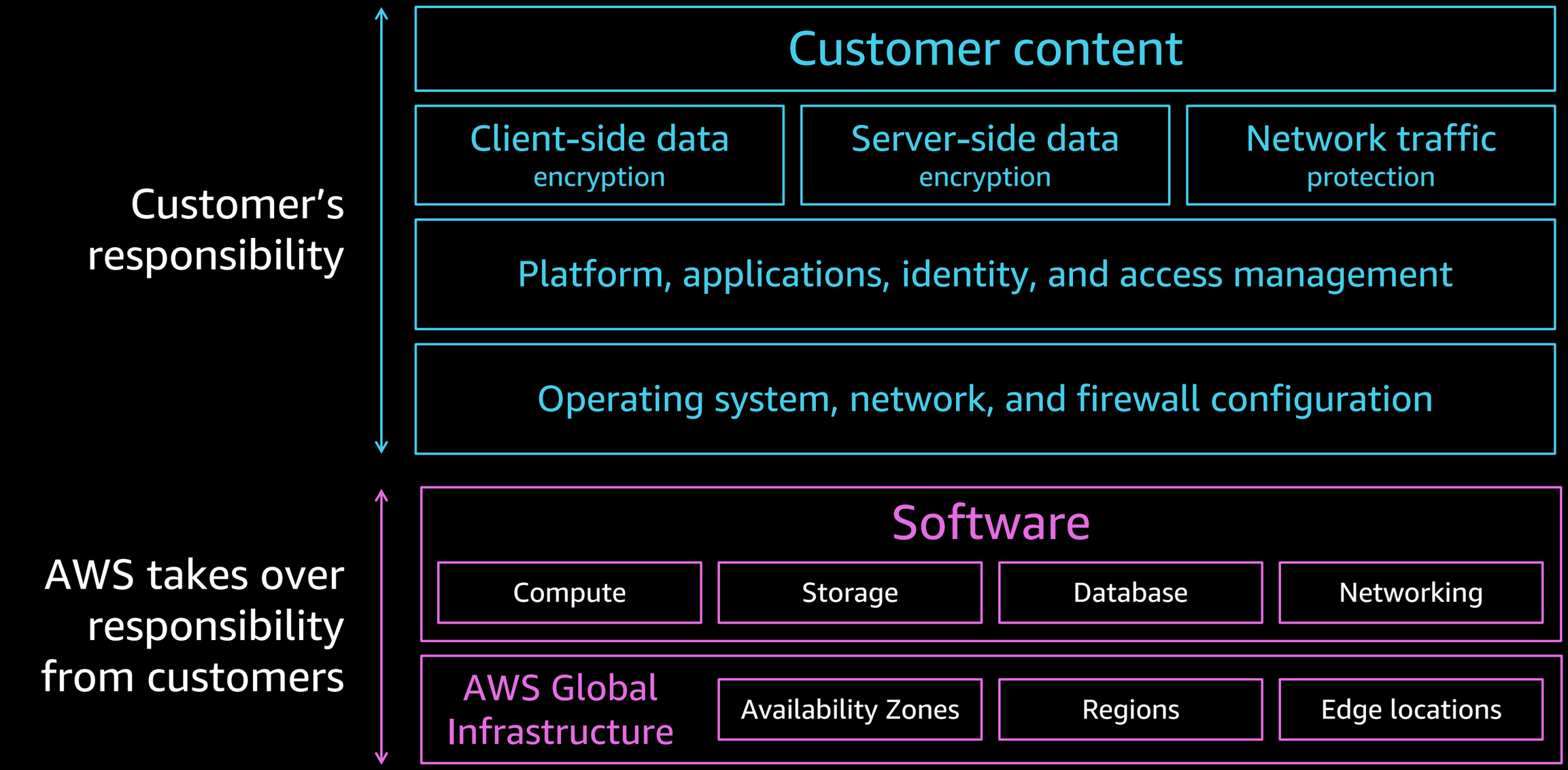
Automate with comprehensive, integrated security services



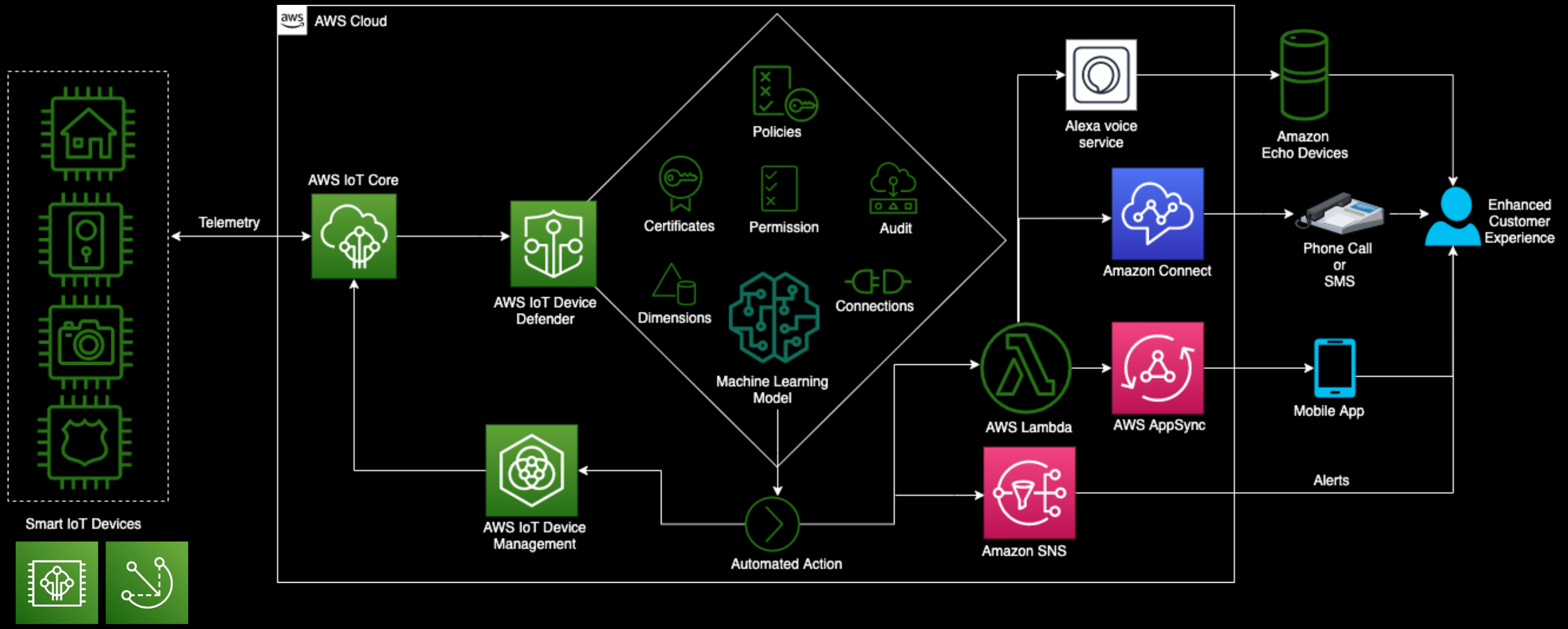
Largest network of security partners and solutions

AWS multi layered security approach and services

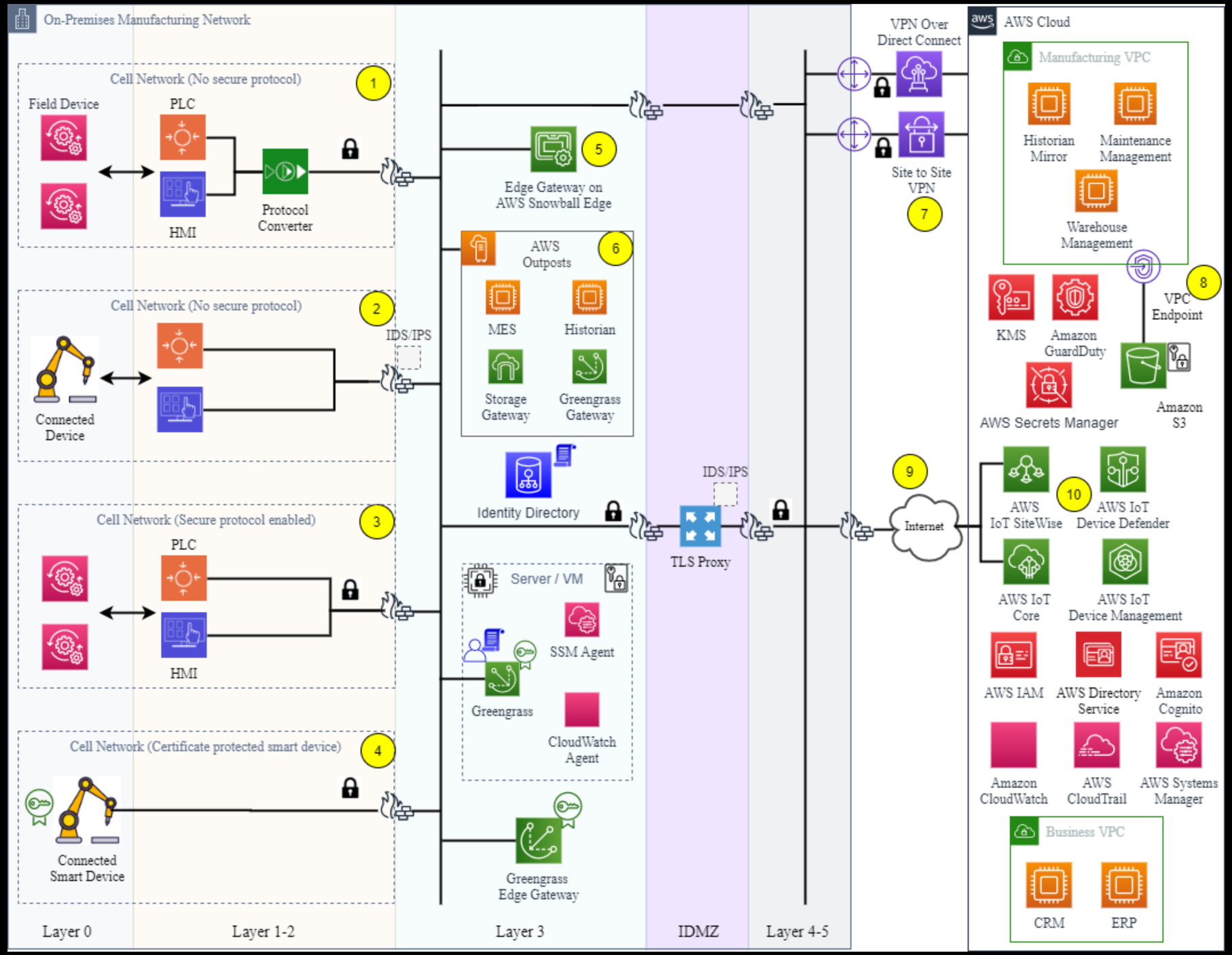
Shared responsibility between AWS and the customer



Consumer IoT use case – Smart Home



Industrial IoT use case – Smart Factory



Demo



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Summary

- AWS provides a multi layered security approach and services
- AWS combines cloud services and edge software to deliver an end-to-end security solution with a suite of services
- AWS IoT Device Defender ML Detect feature makes it easier for customers to detect devices anomalies
- AWS provides a wide variety of best practices documents including Well-Architected Framework, IoT Lens, and security best practices guides
- AWS provides you with the easiest, quickest, and most cost-effective path towards comprehensive, continuous, and scalable IoT security

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, and IoT security best practices guide



Validate expertise with the AWS Certified Security – Specialty exam

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

See more customer stories



Learn how Volkswagen Group is building the Industrial Cloud with AWS



Learn how iRobot easily handled a 20x traffic spike with AWS IoT



Learn how Bayer Crop Science drives innovation in precision agriculture using AWS IoT



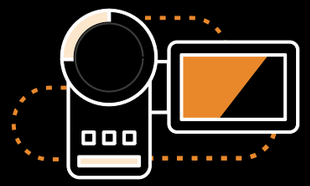
Learn how Woodside Energy uses AWS to power IoT and big data operations

See customer stories at:

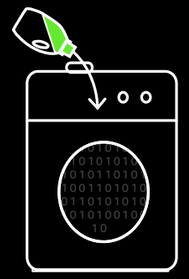
aws.amazon.com/iot

Get started with AWS IoT Solutions

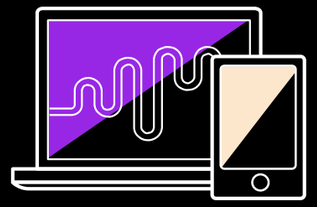
AWS IoT Connected Camera Solution



AWS IoT Smart Product Solution



IoT Device Simulator Solution



Connected Factory solution



Explore AWS IoT solutions at:

aws.amazon.com/iot/solutions

Thank you!

Ryan Dsouza

Sr. IoT Solution Architect

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Please complete the session survey

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.