AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

IOT310

Implementing a Zero Trust security model with AWS IoT

Ryan Dsouza
Principal IoT Solutions Architect
AWS

Eknath Venkataramani
IoT Security Engineer
AWS

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

- What is Zero Trust
- NIST 800-207 Zero Trust tenets, NCSC Zero Trust design principles, and AWS IoT alignment
- Workshop labs
- AWS IoT security best practices
- Wrap up

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

NIST.SP.800-207 “Zero Trust Architecture”



- “Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources.”
- “Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned).”

Rose, Borchert, Mitchell, and Connelly, “Zero Trust Architecture,” https://doi.org/10.6028/NIST.SP.800-207

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

National Cyber Security Centre (NCSC) “Zero trust architecture design principles”



- “Zero trust (ZT) is an architectural approach where inherent trust in the network is removed, the network is assumed hostile and each request is verified based on an access policy.”

UK National Cyber Security Center, “Zero trust architecture design principles,” https://www.ncsc.gov.uk/collection/zero-trust-architecture/introduction-to-zero-trust

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS perspective on Zero Trust



- "Zero Trust is a conceptual model and an associated set of mechanisms that focus on providing security controls around digital assets *that do not solely or fundamentally depend on traditional network controls or network perimeters*."

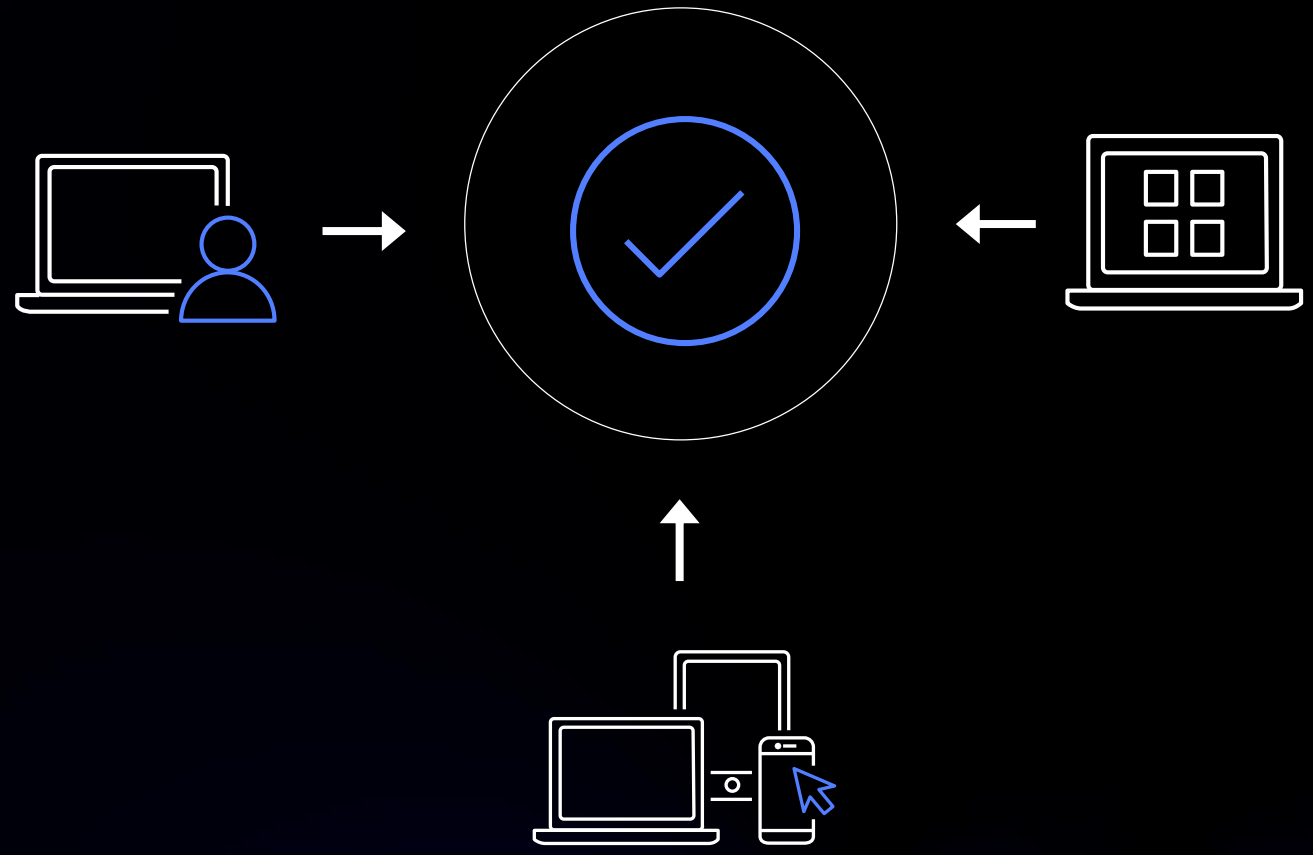
Ryland and Van Deman, "Zero Trust architectures: An AWS perspective,"
https://aws.amazon.com/blogs/security/zero-trust-architectures-an-aws-perspective/

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Context of using Zero Trust

- A zero trust architecture (ZTA) uses zero trust principles to plan industrial and enterprise infrastructure and workflows
- It’s an area of increasing government scrutiny
- It can address the modern challenges we face today such as expansion of the attack surface, hybrid environments, increasing threats, and remote workers
- Start with a zero trust architecture for IoT/IIoT use cases



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

NIST SP 800-207: Tenets of Zero Trust and AWS alignment

1. “All data sources and computing services are considered resources.” (e.g., devices, SaaS, systems, services) – AWS services also operate on “resources” and have since the start of AWS
2. “All communication is secured regardless of network location.” – All communication between devices and between devices & cloud services is secured independent of network location by individually authenticating and authorizing every AWS API call over TLS
3. “Access to individual enterprise resources is granted on a per-session basis.” – AWS IoT services and AWS API calls grant access to resources on a per-session basis
4. “Access to resources is determined by dynamic policy.” – AWS IoT supports dynamic policies using anomaly detection and static thing groups

Source: Rose, Borchert, Mitchell, and Connelly, “Zero Trust Architecture,” https://doi.org/10.6028/NIST.SP.800-207

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

NIST SP 800-207: Tenets of Zero Trust and AWS alignment

5. “The enterprise monitors and measures the integrity and security posture of all owned and associated assets.” – AWS IoT Device Defender can continuously audit and monitor your fleet of IoT devices, and you can use other AWS services for continuous audit & monitoring, which can be used to evaluate the security posture of an asset when evaluating a resource request

6. “All resource authentication and authorization are dynamic and strictly enforced before access is allowed.” – AWS IoT performs authentication and authorization before access is allowed, and the same is true with every AWS API call

7. “The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.” – You can get insights from data collected on AWS (audit, logging, telemetry data, analytics) and use AWS IoT services (Jobs & Tunneling) and other AWS services to make continuous improvements to an enterprise’s security posture, which can include fine-tuning permissions

Source: Rose, Borchert, Mitchell, and Connelly, “Zero Trust Architecture,” https://doi.org/10.6028/NIST.SP.800-207

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

NCSC ZT architecture design principles

1. “Know your architecture, including users, devices, services and data”
2. “Know your user, service and device identities”
3. “Assess user behavior, service and device health”
4. “Use policies to authorise requests”
5. “Authenticate and authorise everywhere”
6. “Focus your monitoring on users, devices and services”
7. “Don’t trust any network, including your own”
8. “Choose services which have been designed for zero trust”

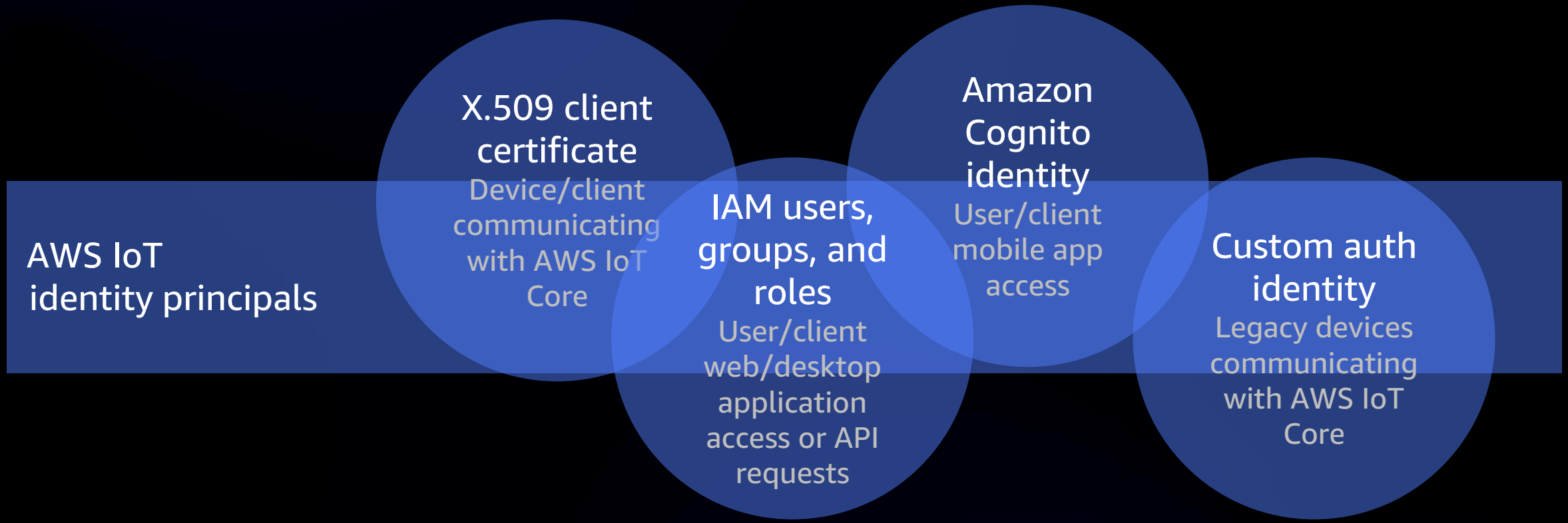
Source: UK National Cyber Security Center, “Zero trust architecture design principles,” https://www.ncsc.gov.uk/collection/zero-trust-architecture/introduction-to-zero-trust

AWS and AWS IoT support these architecture design principles by default while focusing on customer use cases, business value, and desired business outcomes

aws

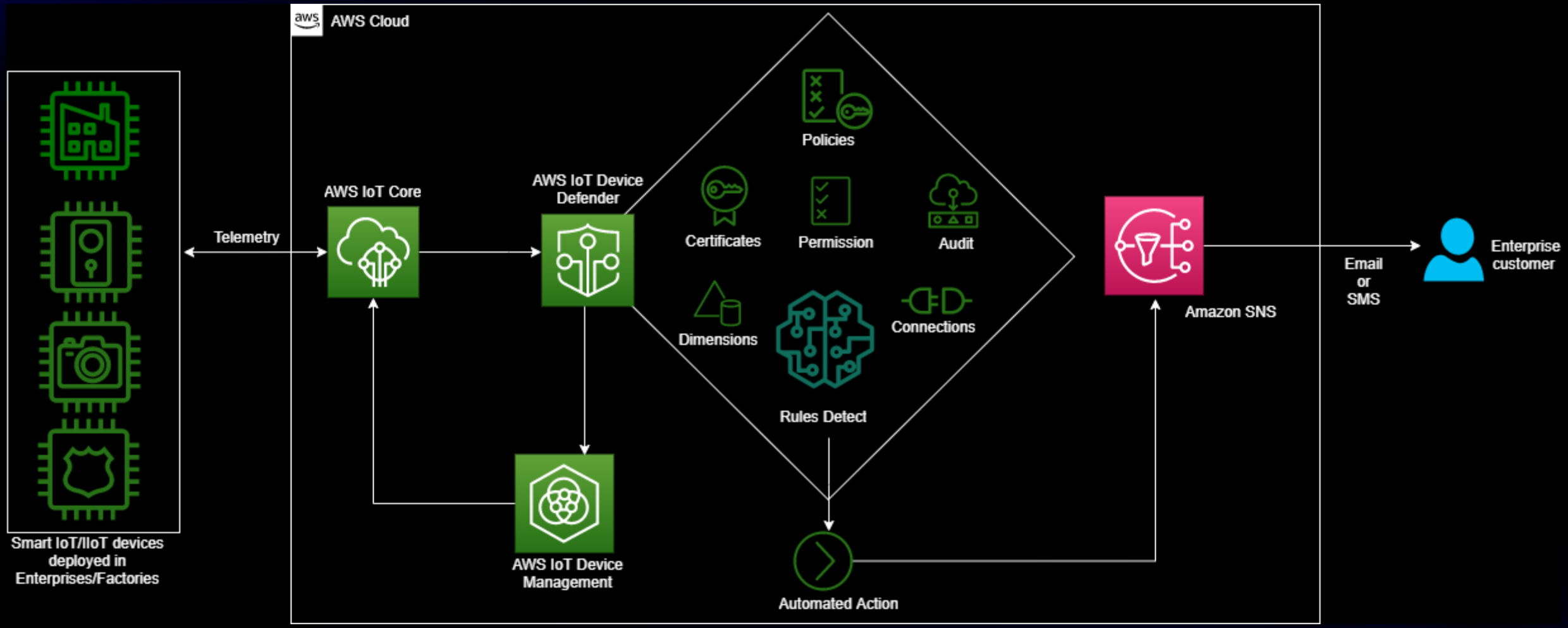
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS IoT supports Zero Trust by default



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Enterprise IoT workshop use case



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Workshop modules

1. Device provisioning and unique identity
2. Auditing against IoT security best practices
3. Anomaly detection using rules detect
4. Incident response and mitigation
5. Continual updates (advanced module)

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Workshop summary

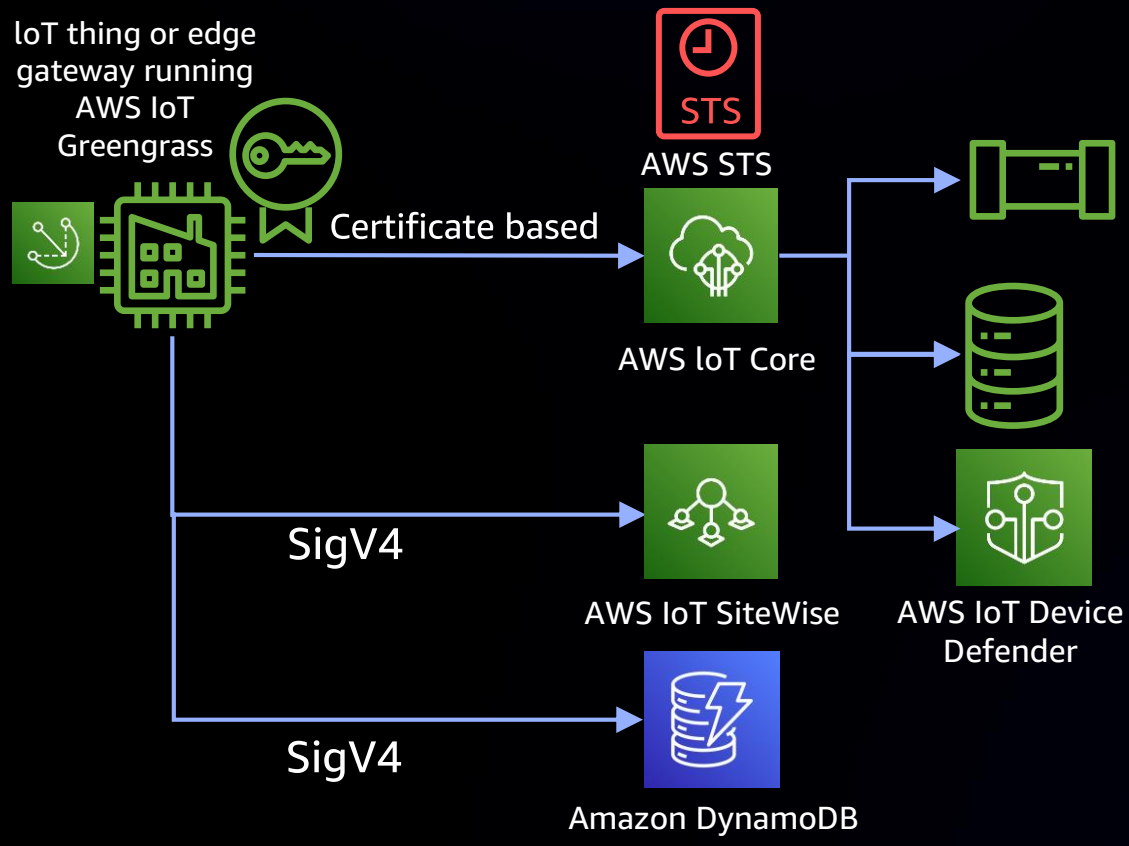
Zero Trust capabilities	AWS IoT services & features
Unique identity	AWS IoT identities
Least privilege access	AWS IoT policies
Device registration, inventory, lifecycle management	AWS IoT Device Management
Secure connection & data in transit	AWS IoT Core
Auditing (against IoT security best practices)	AWS IoT Device Defender audit
Device health monitoring and behavior analytics	AWS IoT Device Defender Detect
Security monitoring and incident response	AWS IoT Device Defender
Continuous updates to keep devices healthy	AWS IoT jobs

Combined with the rest of the AWS platform to secure your IoT/IIoT systems and applications

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS IoT Zero Trust foundations from Day 1

Required authentication and encryption at all points



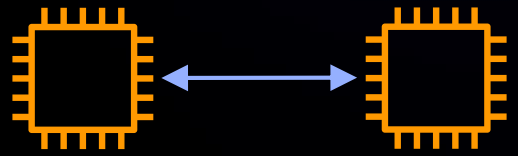
1. All data sources and computing services are considered resources
2. All communication is secured
3. Access to individual enterprise resources is granted on a per-session basis
4. Access to resources is determined by dynamic policy
5. The enterprise monitors and measures the integrity and security posture
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed
7. Collect information and use it to improve the enterprise security posture

aws

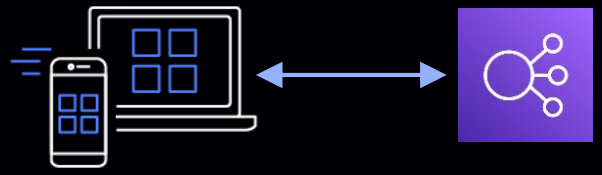
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Zero Trust guiding principles

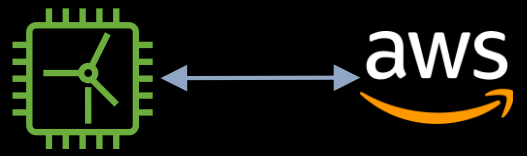
1. Focus on use cases, organization objectives, and business outcomes



Machine-to-machine



Human-to-application



Digital transformation

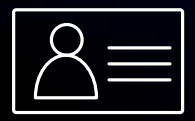
2. Where possible, use identity and network capabilities together

3. Apply Zero Trust to your systems and data in accordance with their value, not a one-size-fits-all scenario

aws

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS security, identity, and compliance solutions



Identity & access management

- AWS Identity and Access Management (IAM)
- AWS Single Sign-On
- AWS Organizations
- AWS Directory Service
- Amazon Cognito
- AWS Resource Access Manager (AWS RAM)



Detection

- AWS Security Hub
- Amazon GuardDuty
- Amazon Inspector
- Amazon CloudWatch
- AWS Config
- AWS CloudTrail
- VPC Flow Logs
- AWS IoT Device Defender



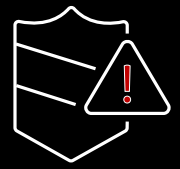
Infrastructure protection

- AWS Firewall Manager
- AWS Network Firewall
- AWS Shield
- AWS WAF – web application firewall
- Amazon Virtual Private Cloud (Amazon VPC)
- AWS PrivateLink
- AWS Systems Manager



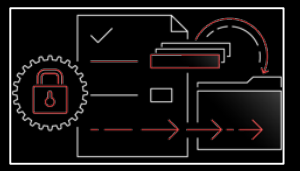
Data protection

- Amazon Macie
- AWS Key Management Service (AWS KMS)
- AWS CloudHSM
- AWS Certificate Manager (ACM)
- AWS Secrets Manager
- AWS VPN
- Server-side encryption



Incident response

- Amazon Detective
- CloudEndure Disaster Recovery
- AWS Config rules
- AWS Lambda



Compliance

- AWS Artifact
- AWS Audit Manager

© 2021, 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, and IoT security best practices guide, OT Security whitepaper, Security Golden Rules



Validate expertise with the AWS Certified Security – Specialty exam

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

aws

Thank you!

Ryan Dsouza
rydsouza@amazon.com

Eknath Venkataramani
eknatv@amazon.com

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.