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

IOT301

Protect your IoT devices from DDoS events and enforce with Zero Trust

Syed Rehan

Sr. Global IoT Technologist and Evangelist
Amazon Web Services

Victor Lesau

Sr. Product Manager Technical
Amazon Web Services

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

Agenda

DDoS and protection principles

Zero Trust and protection principles

NIST and NCSC Zero Trust design principles

AWS IoT security best practices

Demo: Enforcing and securing devices using AWS IoT + Zero Trust

Discussion

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

DDoS

DoS (Denial of Service) – denied access to resources

DDoS (Distributed Denial of service) – attack arriving from multiple sources

Why?

Cheap and easy to run

Effective against strong targets

Used often

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

Protection principles for DDoS

Understand a shared responsibility model

Understand your services

Set up defenses upstream

Build and scale using cloud-native services

Have a response plan (continue to operate)

Monitor and test regularly using cloud-centered services

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

What is Zero Trust?

NIST.SP.800-207



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

What is Zero Trust?



National Cyber Security Centre, UK (NCSC)

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

Protection principles for Zero Trust

Awareness – Internal and external threats always exist

Caution – Assume every device has potential to be hostile

Gatekeeping – Always authenticate and authorize

Trust issues – Even trusted devices can be compromised

Guard – Update and change policies dynamically

aws

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

AWS IoT security best practices

Decouple ingestion from processing

Design for offline behavior

Design lean data at the edge and enrich in the cloud

Handle personalization

Ensure devices regularly send status checks

Utilise machine learning (ML) capabilities to automate

aws

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

AWS IoT security best practices

Manage device security lifecycle holistically

Ensure least privilege permissions

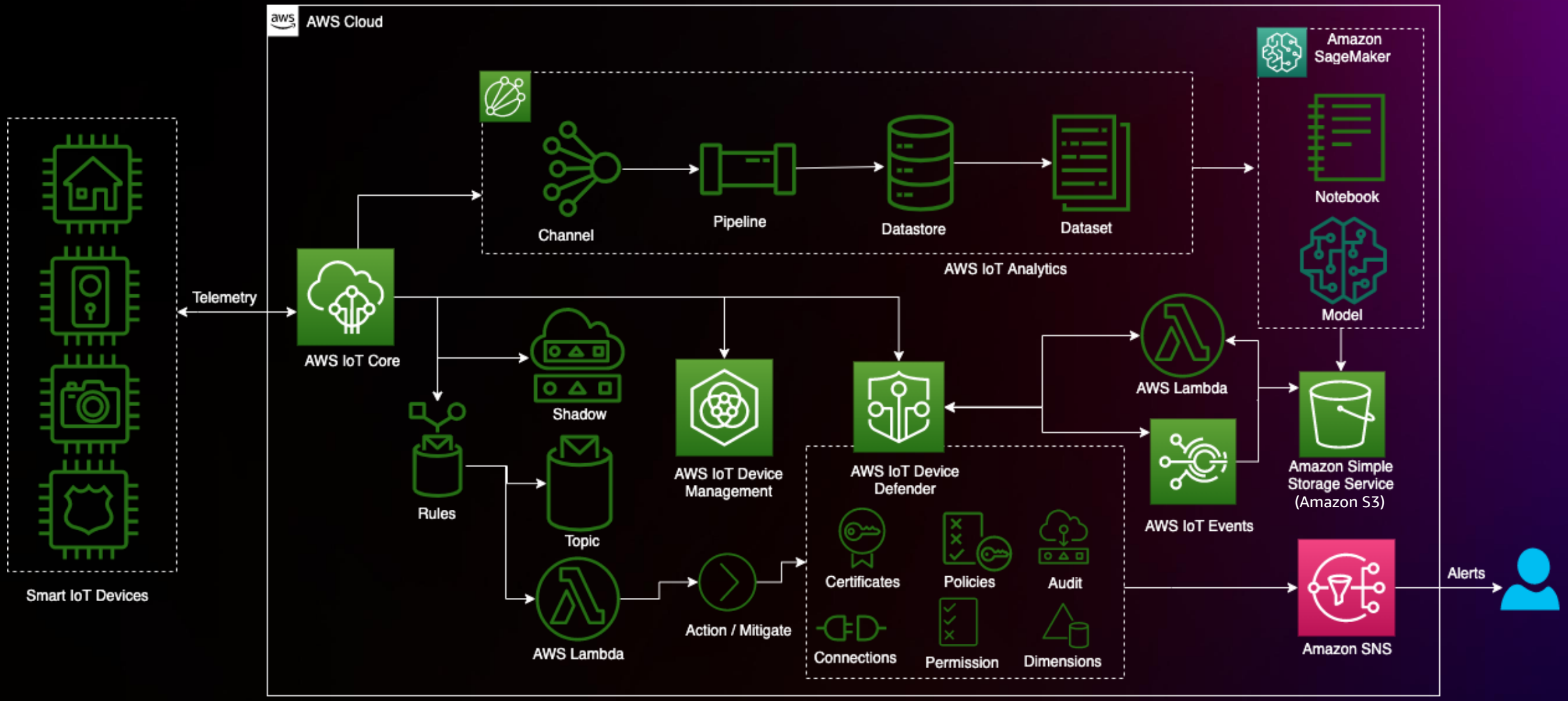
Secure device credentials at rest

Implement device identity lifecycle management

Take a holistic view of data security

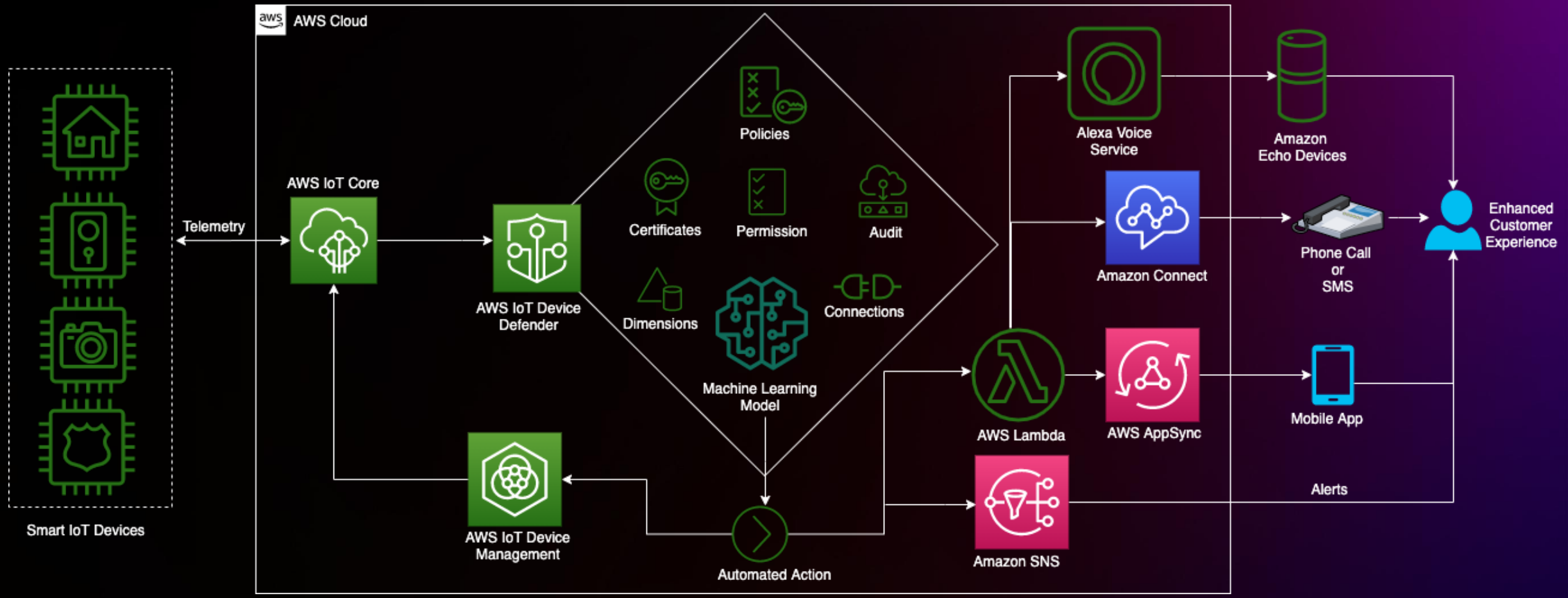
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Defending devices with Amazon ML



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

AWS IoT ML capabilities



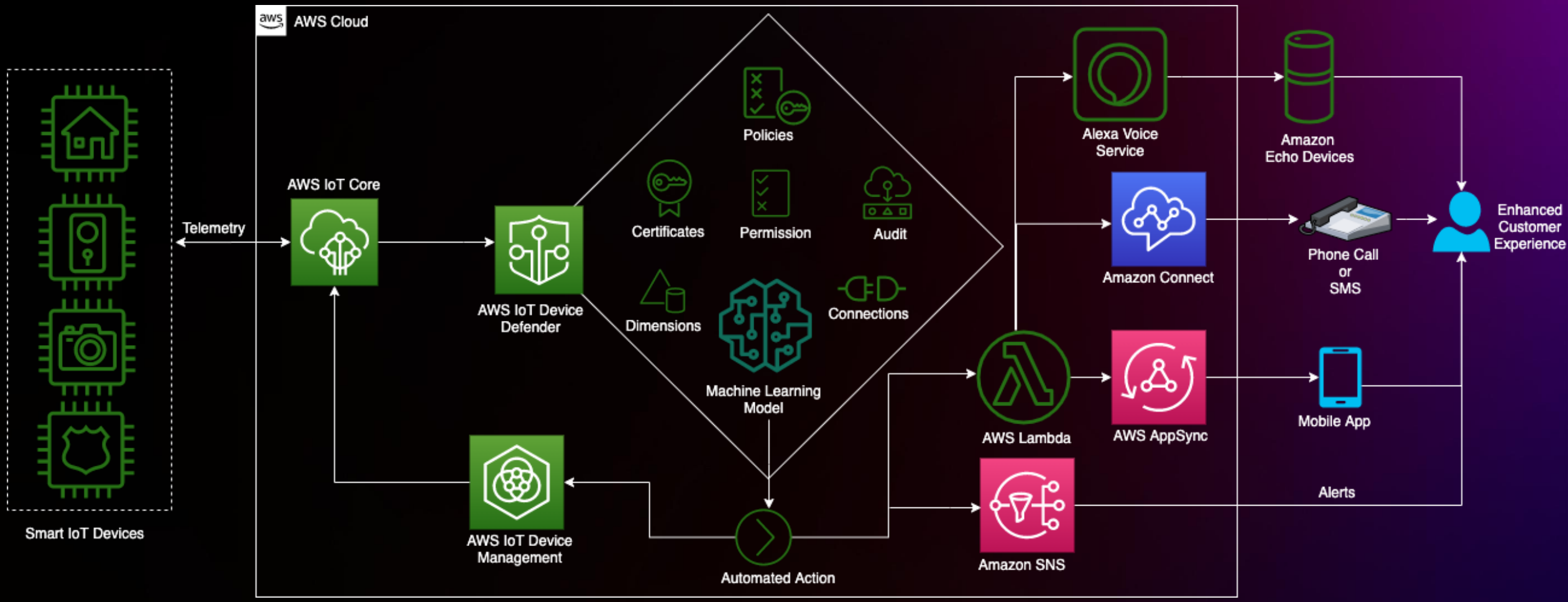
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

ERA Home Security Customer: Product Demo Connected Lock



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

ERA Home Security – Connected Lock



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

Demo architecture and steps for Zero Trust



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

Further learnings

Workshops



getstartedwithawsiot.com



awsiotzerotrustworkshop.com



greengrassworkshop.com

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

Thank you!

Syed Rehan

LinkedIn @iamsyed

Twitter @SyedCloud

Victor Lesau

LinkedIn @lesau

Twitter @VictorLesau



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

aws

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