Zero Trust Security with IoT

Syed Rehan
Sr. Global IoT Developer Evangelist
AWS

Agenda

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

What is Zero Trust

NIST.SP.800-207

"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

What is Zero Trust

National Cyber Security Centre - UK (NCSC)

"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

Protection principles for Zero Trust

Paranoia – Internal and external threats always exist

Assume hostility – Always assume every device is hostile

Gate keeper – Always authenticate and authorize

Trust issues – Trusted devices are never trusted

Guard – Update and change policies dynamically

AWS IoT security best practices

Decouple ingestion from processing

Design for offline behaviour

Design lean data at the edge and enrich in the cloud

Handle personalization

Ensure devices regularly send status checks

AWS IoT security best practices

Manage device security lifecycle holistically

Ensure least privilege permissions

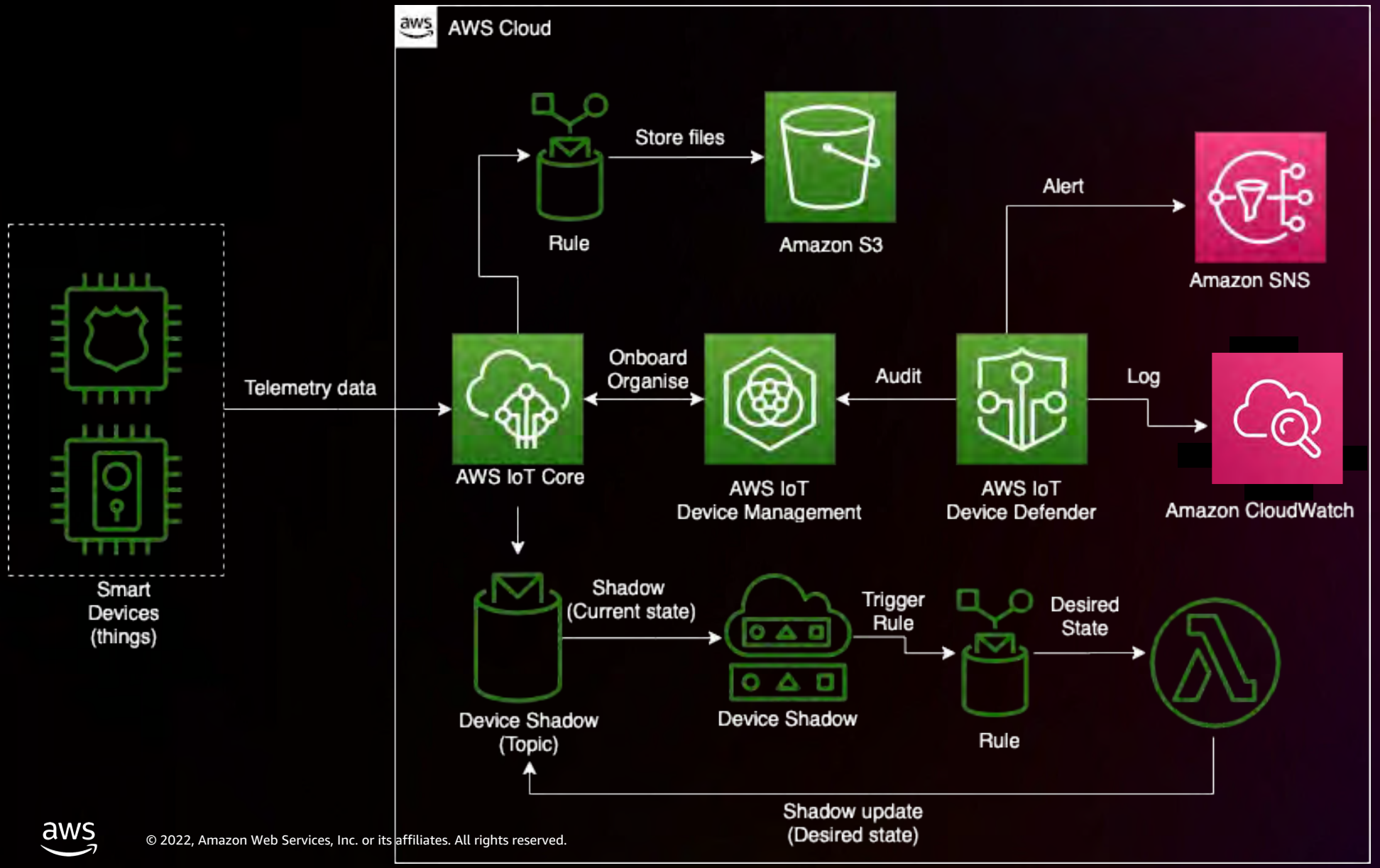
Secure device credentials at rest

Implement device identity lifecycle management

Utilise Machine Learning (ML) where you can

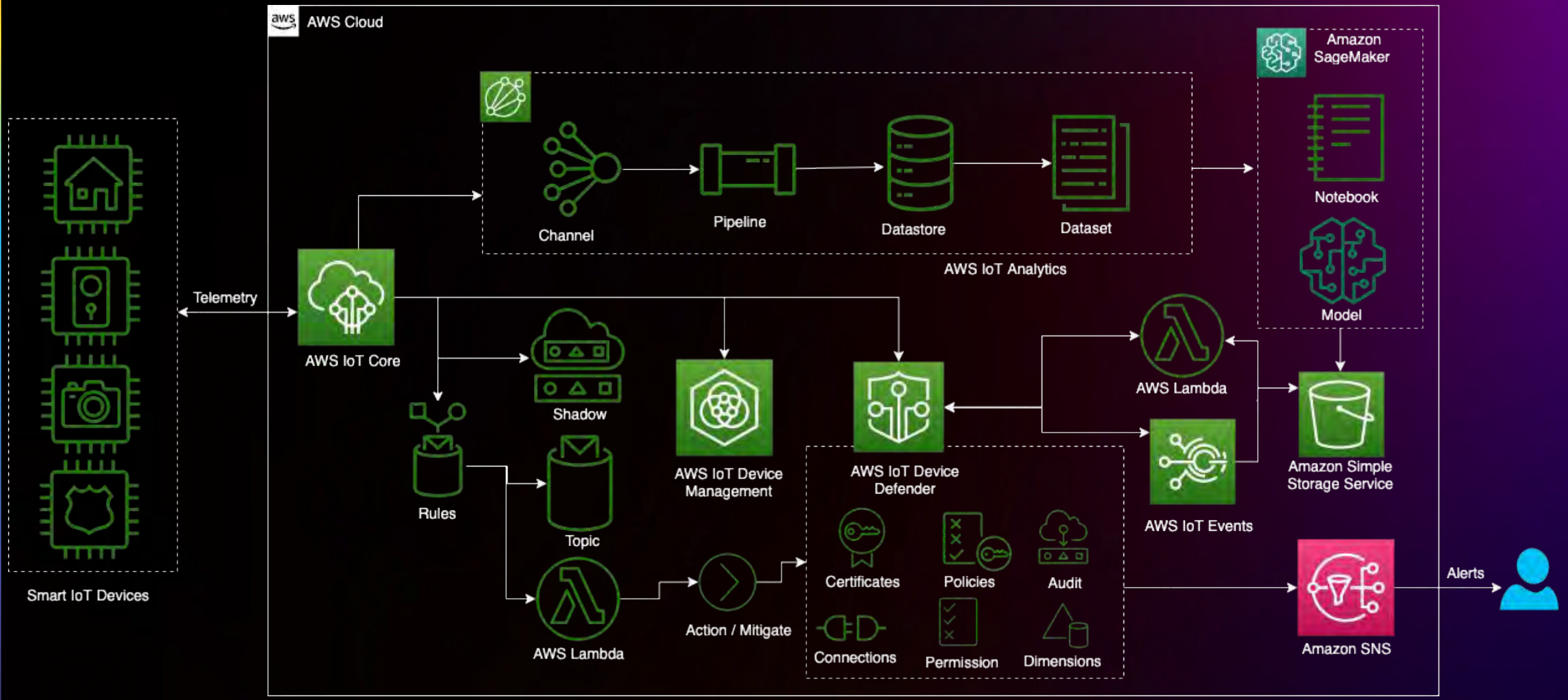
Take a holistic view of data security

Telemetry before machine learning

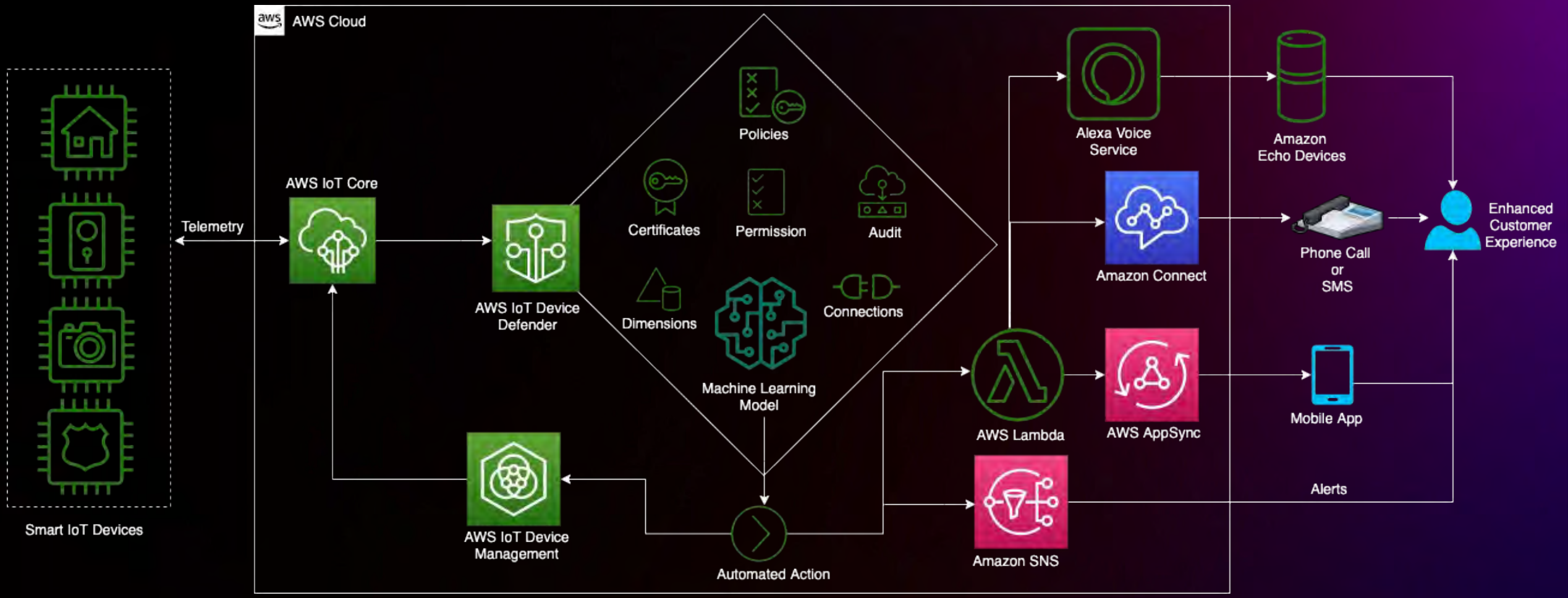


- Secure using AWS IoT Device Defender
- Store historic data in files for future usage
- Analyze states using Lambda

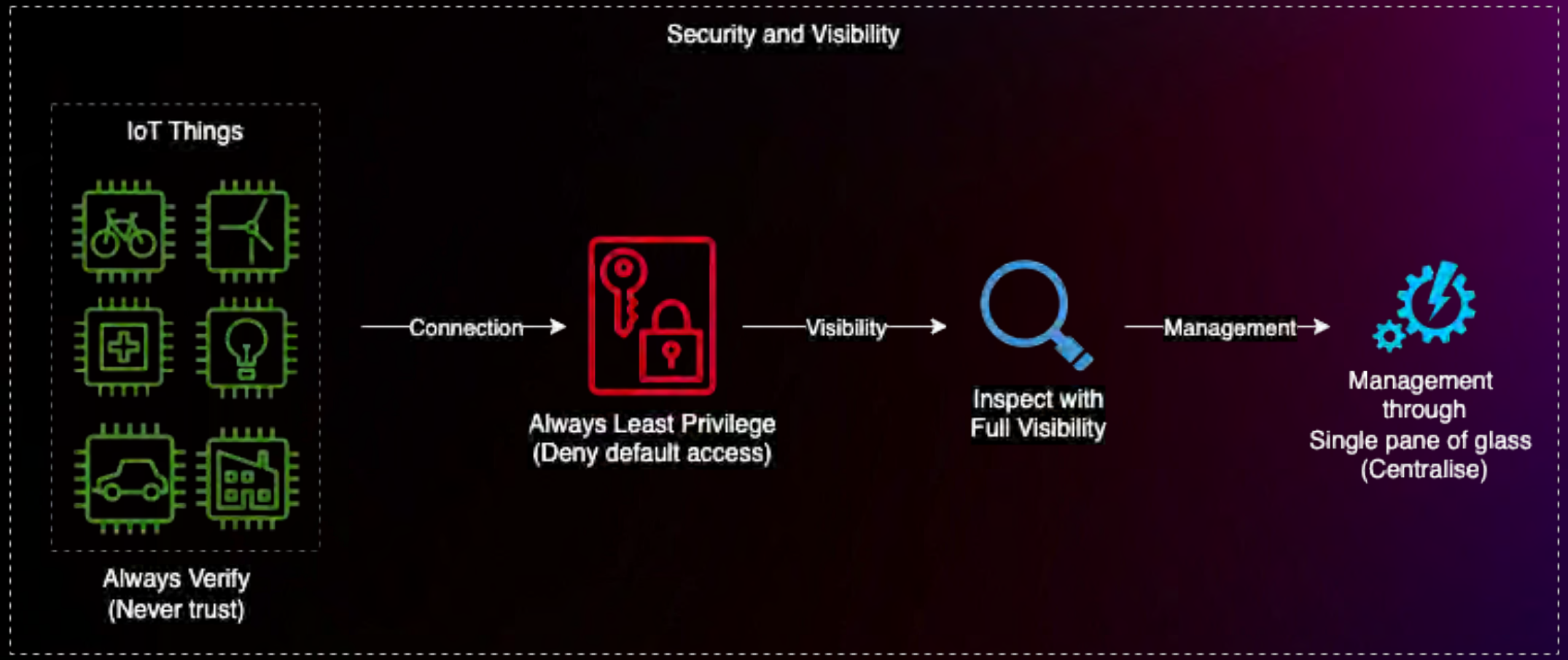
Defending devices with Amazon ML



Automate and eliminate risks



Demo architecture & steps for Zero Trust



Demo using AWS Services

Further Learnings

Workshops:

- http://getstartedwithawsiot.com
- http://awsiotzerotrustworkshop.com
- http://greengrassworkshop.com

Github (AWS IoT open source projects):

- https://github.com/awslabs/aws-iot-device-client
- https://github.com/aws-greengrass

YouTube – Subscribe for videos

Dev.to – Follow for posts

Thank you!

Syed Rehan

Sr. Global IoT Developer Evangelist

AWS

@iamsyed

@SyedCloud