AWS re:Invent

SEC337

Toyota Motor North America: Securing the cloud with AWS KMS

Matthew Costello
Principal
Booz Allen Hamilton

Kell Rozman
Senior Manager, Security Software Engineering
Toyota Motor North America

Rajkumar Copparapu
Senior Product Manager
Amazon Web Services

AWS re:Invent

aws

Agenda

How Toyota and Booz Allen Hamilton used AWS KMS to secure their SOC in AWS

- The challenge
- Architecture/orchestration overview
- Data flow
- Use case
- Security details

The challenge

Imagine being tasked with **collecting**, **analyzing**, and **securing** data from **hundreds of sources** around the world, in **multiple** cloud and on-premises environments

Toyota Motor North America, along with **Booz Allen Hamilton**, has created a **secure, cloud-native solution** to analyze **billions** of messages per day using AWS Key Management Service (**AWS KMS**)

Provide	Provide a robust data pipeline to collect security event data from existing tools on premises, in the cloud, and from global affiliates
Secure	Build a highly secured environment with reliability metrics and instrumentation
Ensure	Ensure that all existing feeds to security operations continued to work through the migration
Migrate	Migrate existing analytic dashboards to AWS cloud native tools
Support	Continue to support ongoing security incident response as needed

Global security event collection

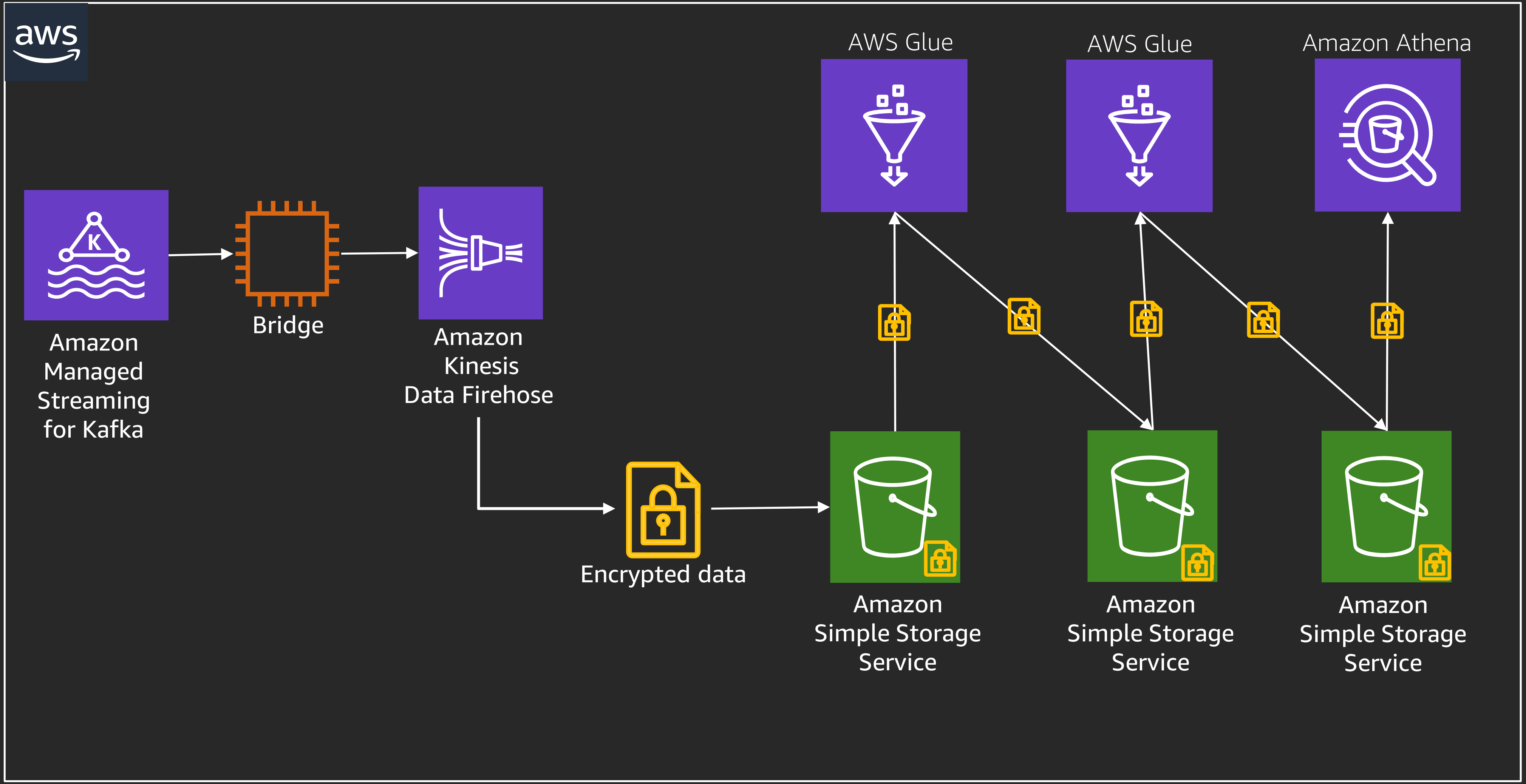
Global insights

Collection and aggregation of data sets produced in multiple geographical regions **enables** new advanced analytics, spanning multiple regions, including near real-time stream processing to deliver new global insights to security analysts

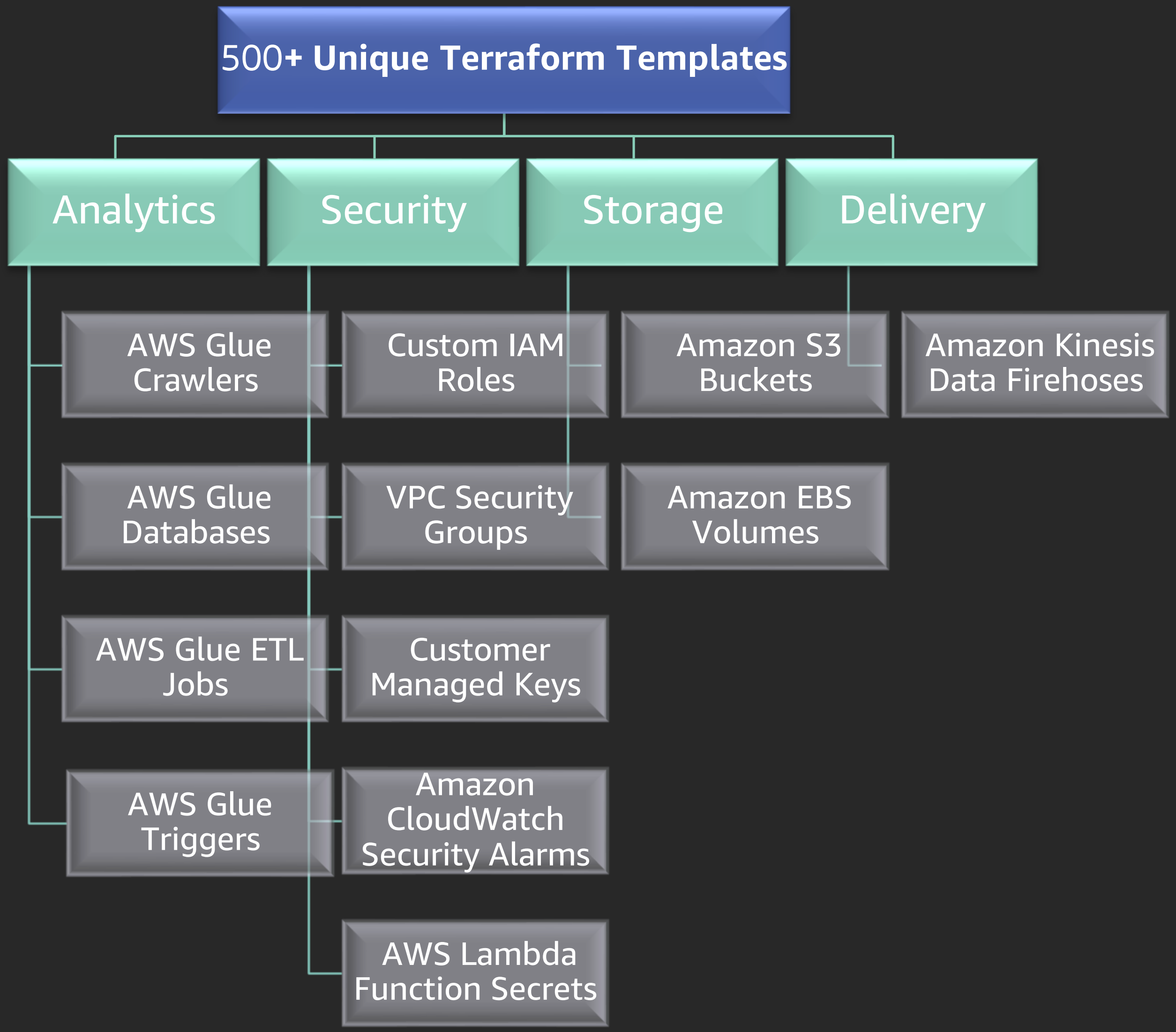
Architecture overview

Highlights

- 230+ data alarms configured
- 4+ TB data volume daily
- 2.7+ billion records per day
- 178+ TB written in storage
- 7+ affiliates actively monitored
- 8 Additional affiliates planned
- 60+ actively monitored data sources
- 210+ additional monitored data sources planned


aws
Amazon Managed Streaming for Kafka
Bridge
Amazon Kinesis Data Firehose
Encrypted data
AWS Glue
AWS Glue
Amazon Athena
Amazon Simple Storage Service
Amazon Simple Storage Service
Amazon Simple Storage Service

Templated orchestration



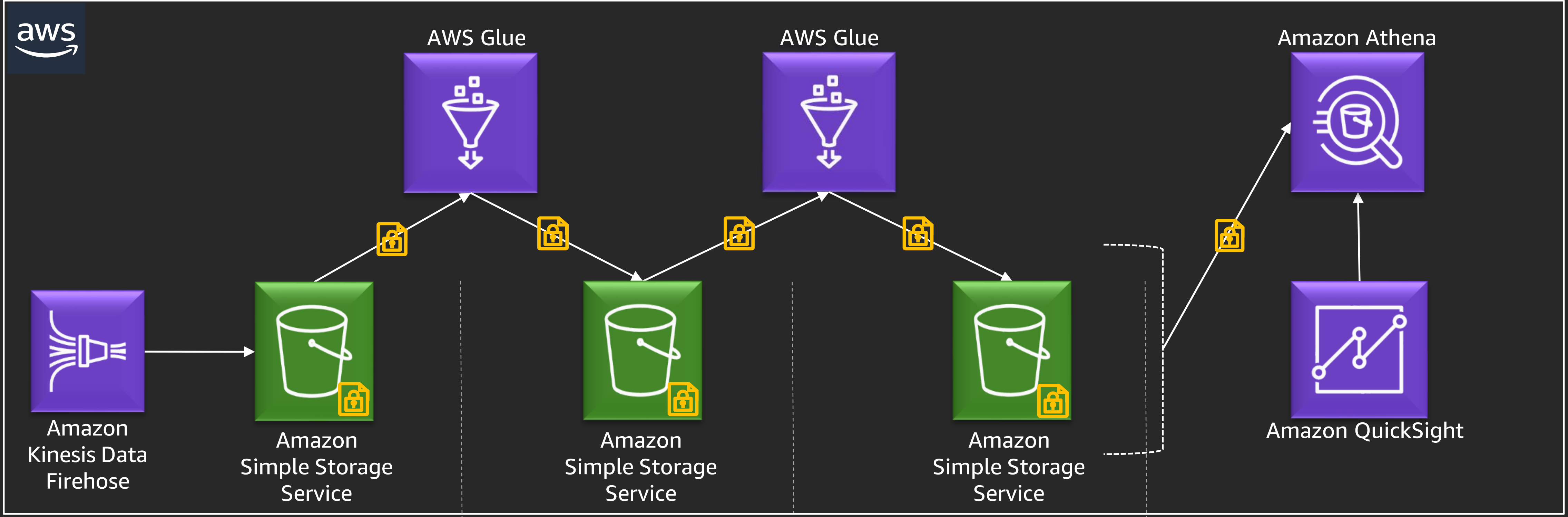
500+ **Unique Terraform Templates**

- Analytics
  - AWS Glue Crawlers
  - AWS Glue Databases
  - AWS Glue ETL Jobs
  - AWS Glue Triggers
- Security
  - Custom IAM Roles
  - VPC Security Groups
  - Customer Managed Keys
  - Amazon CloudWatch Security Alarms
  - AWS Lambda Function Secrets
- Storage
  - Amazon S3 Buckets
  - Amazon EBS Volumes
- Delivery
  - Amazon Kinesis Data Firehoses

Key features

- Provides a consistent and expected output
- Version control allows for better governance
- Greater efficiency when deploying similar services
- Easier to understand when creating layered security model
- Teardown and build up efficiency
- Provides easier disaster recovery in a different region
- CLI quicker than using GUI

Secure data enrichment flow


aws
AWS Glue
AWS Glue
Amazon Athena
Amazon Kinesis Data Firehose
Amazon Simple Storage Service
Amazon Simple Storage Service
Amazon Simple Storage Service
Amazon QuickSight

Landing zone layer

- Raw data lands in S3 buckets
- AWS Glue ETL Job loads raw data to Parsed layer

Parsed layer

- Parsed data lands in S3
- ETL Job transforms data based on Analytics Use Case

Transform layer

- Transformed data lands in S3

Insight!

- Amazon QuickSight visualizes data from the Transform layer

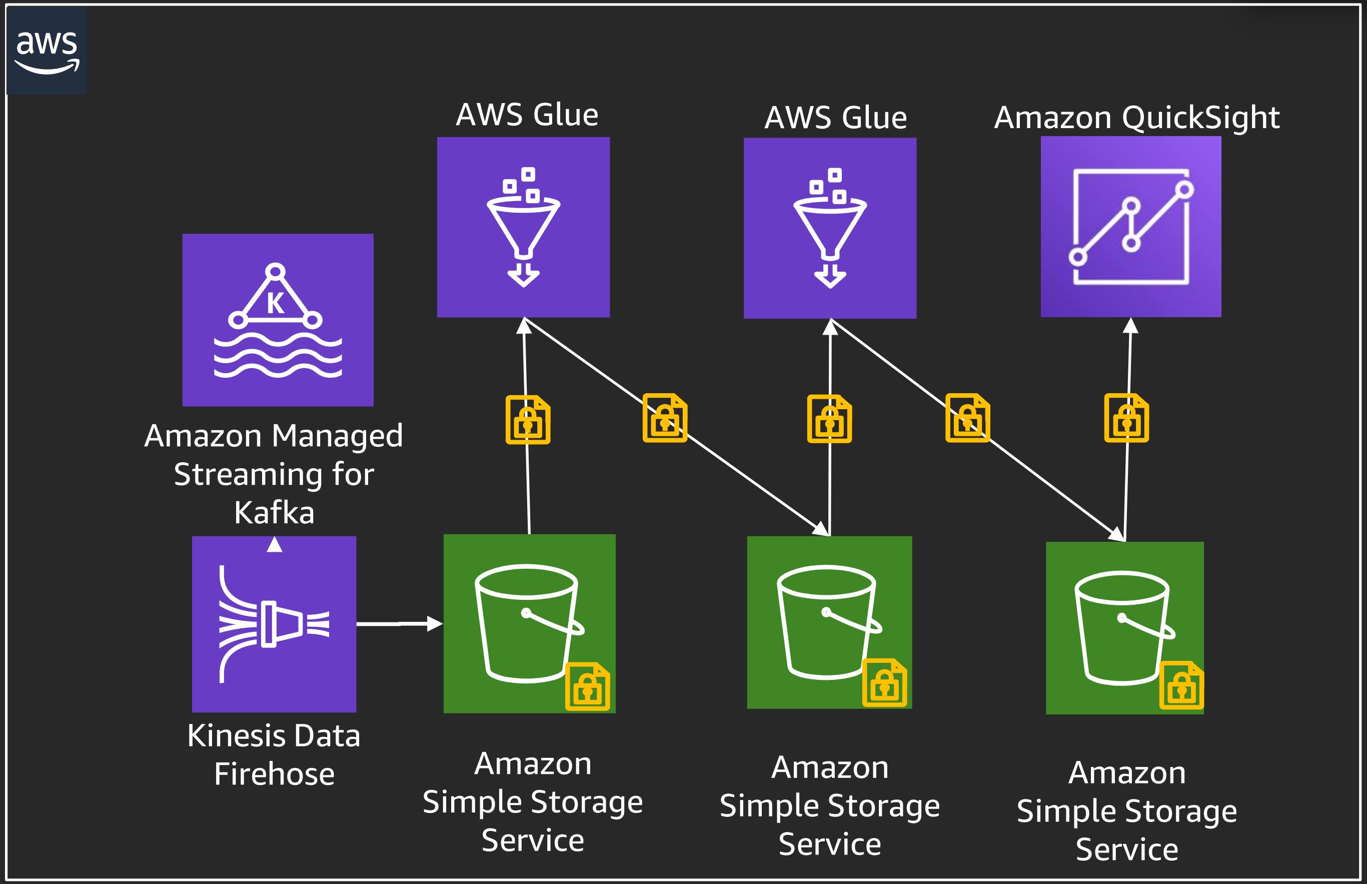
Endpoint health use case

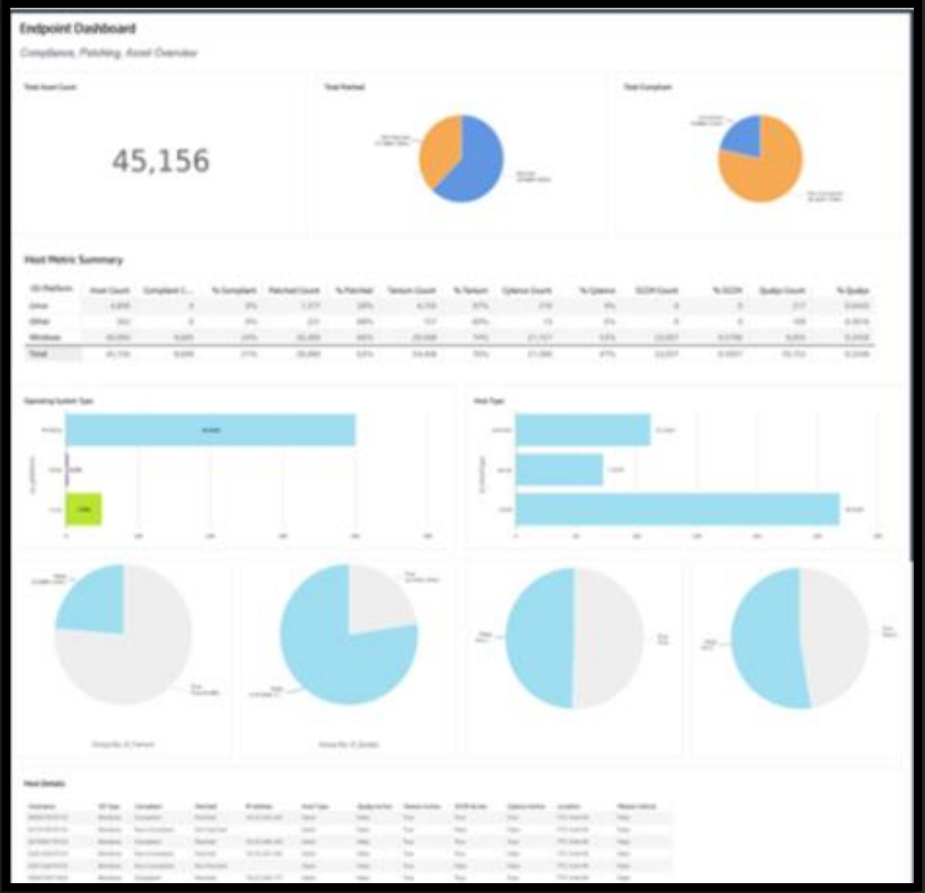
Inputs

- Endpoint Logs
- Vulnerability Scanners
- CMBD Logs
- Malware Scanners
- DHCP Logs

Outputs

- A reliable and automated list of active on-premises and cloud assets
- A powerful and insightful vulnerability management tool with details around patching & compliance

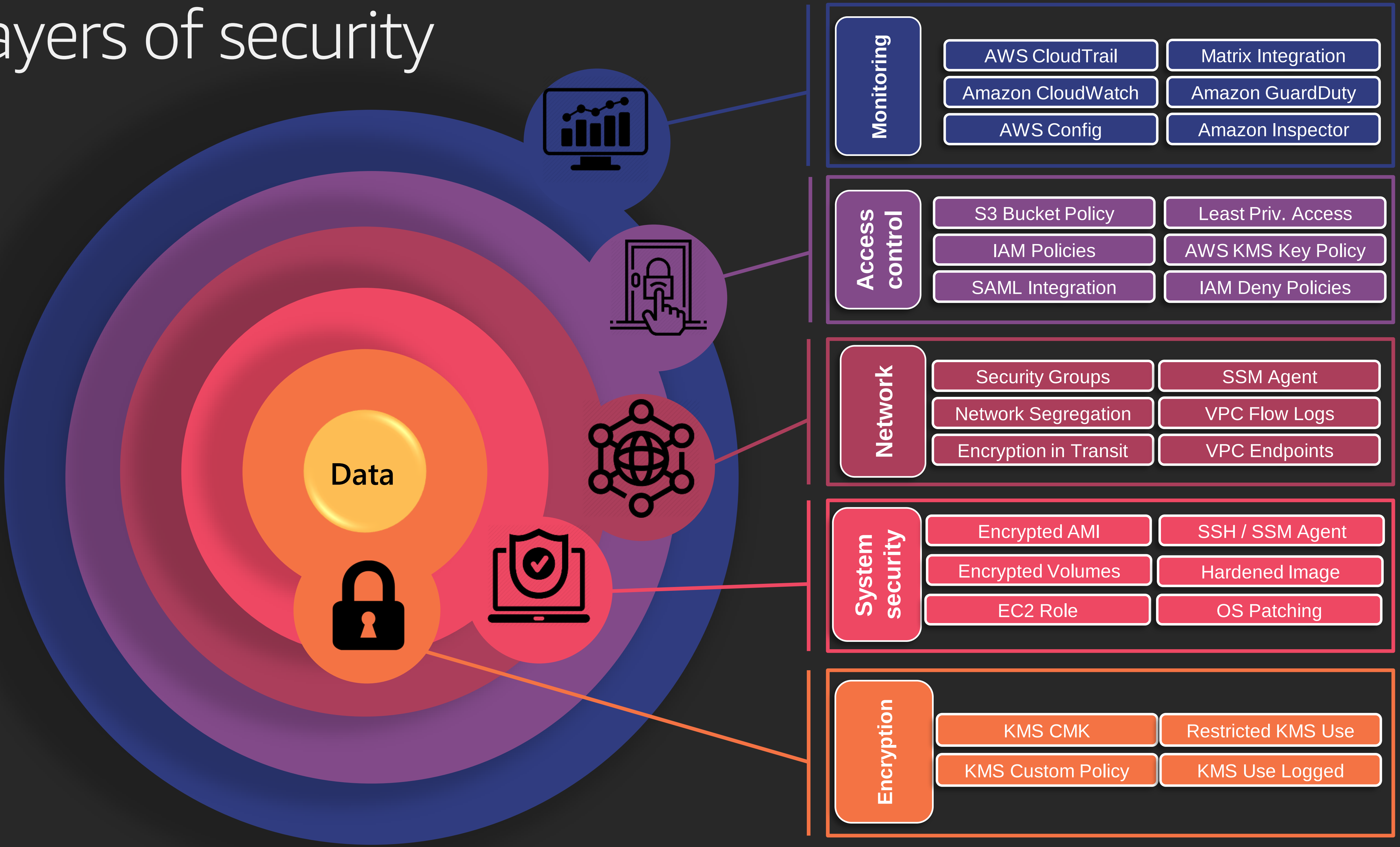

aws
AWS Glue
AWS Glue
Amazon QuickSight
Amazon Managed Streaming for Kafka
Kinesis Data Firehose
Amazon Simple Storage Service
Amazon Simple Storage Service
Amazon Simple Storage Service


Endpoint Dashboard

Compliance, Patching, Asset Overview

45,156

Layers of security



Monitoring

- AWS CloudTrail
- Matrix Integration
- Amazon CloudWatch
- Amazon GuardDuty
- AWS Config
- Amazon Inspector

Access control

- S3 Bucket Policy
- Least Priv. Access
- IAM Policies
- AWS KMS Key Policy
- SAML Integration
- IAM Deny Policies

Network

- Security Groups
- SSM Agent
- Network Segregation
- VPC Flow Logs
- Encryption in Transit
- VPC Endpoints

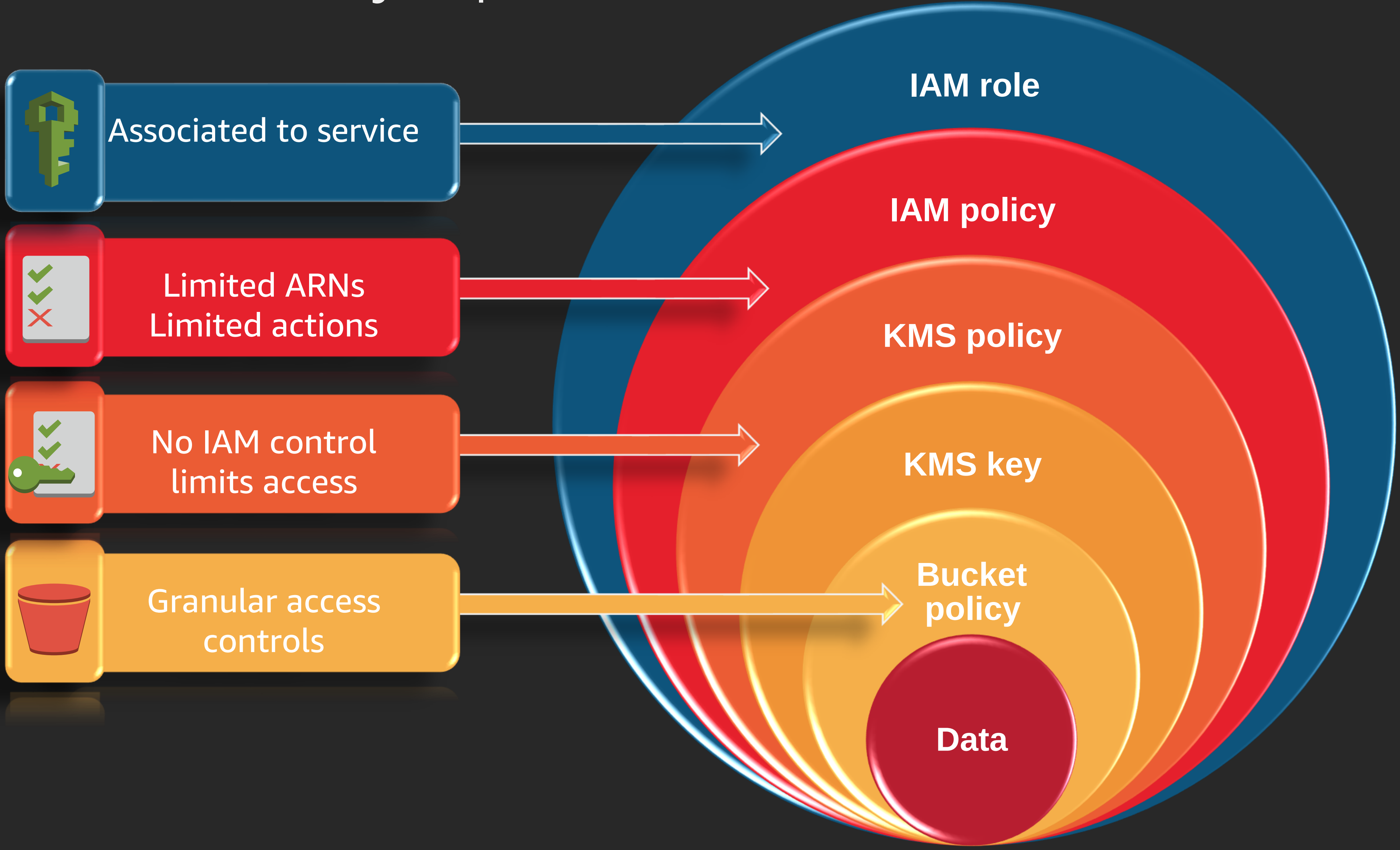
System security

- Encrypted AMI
- SSH / SSM Agent
- Encrypted Volumes
- Hardened Image
- EC2 Role
- OS Patching

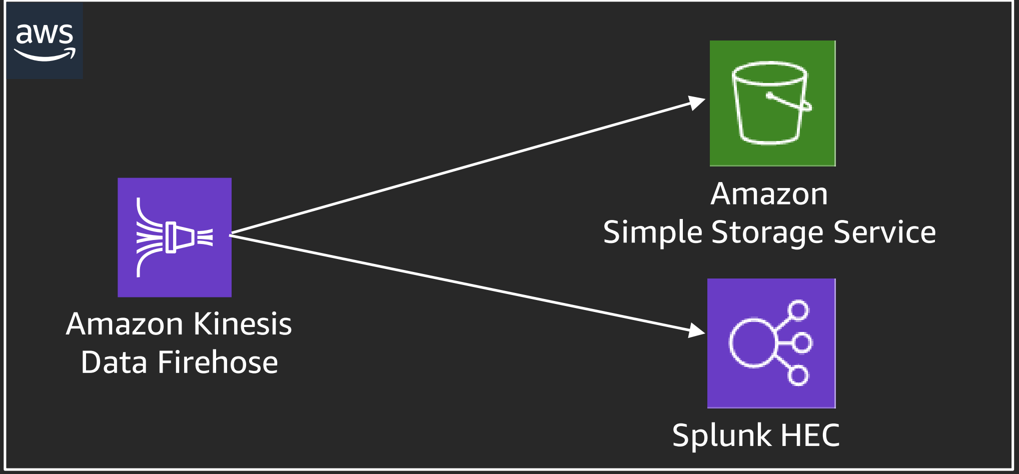
Encryption

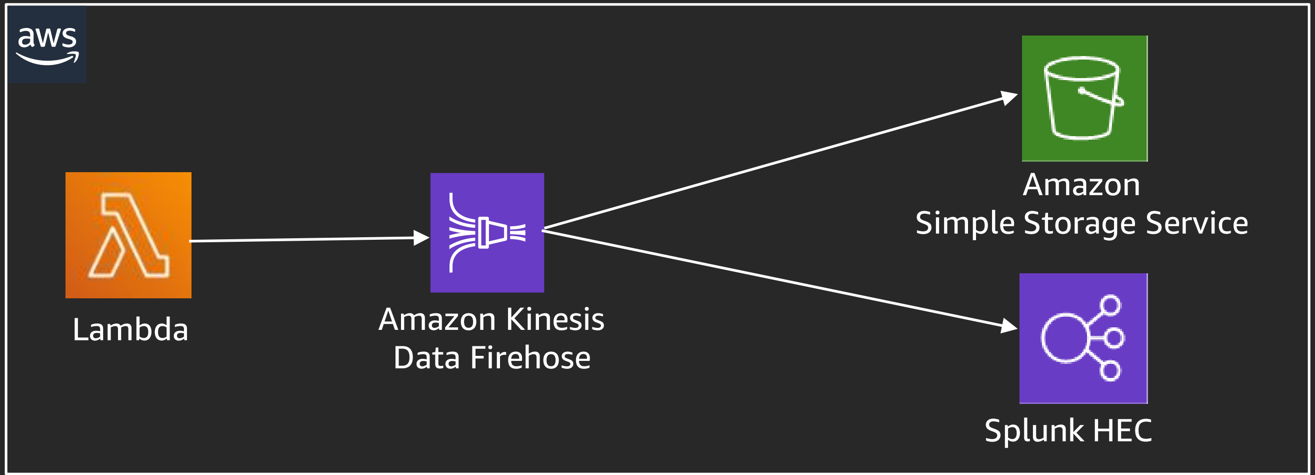
- KMS CMK
- Restricted KMS Use
- KMS Custom Policy
- KMS Use Logged

Layers of security – policies & roles



Ingestion methods





Agents

- Kinesis agents send data directly to Kinesis Data Firehose, where it is forwarded to S3 and Splunk

Syslog

- Native syslog clients send directly to Kinesis Data Firehose or one of many syslog aggregation clusters

Kafka bridge

- A custom, scalable, Kafka bridge in AWS replicates data from on-premises Kafka clusters and cloud providers

Lambda

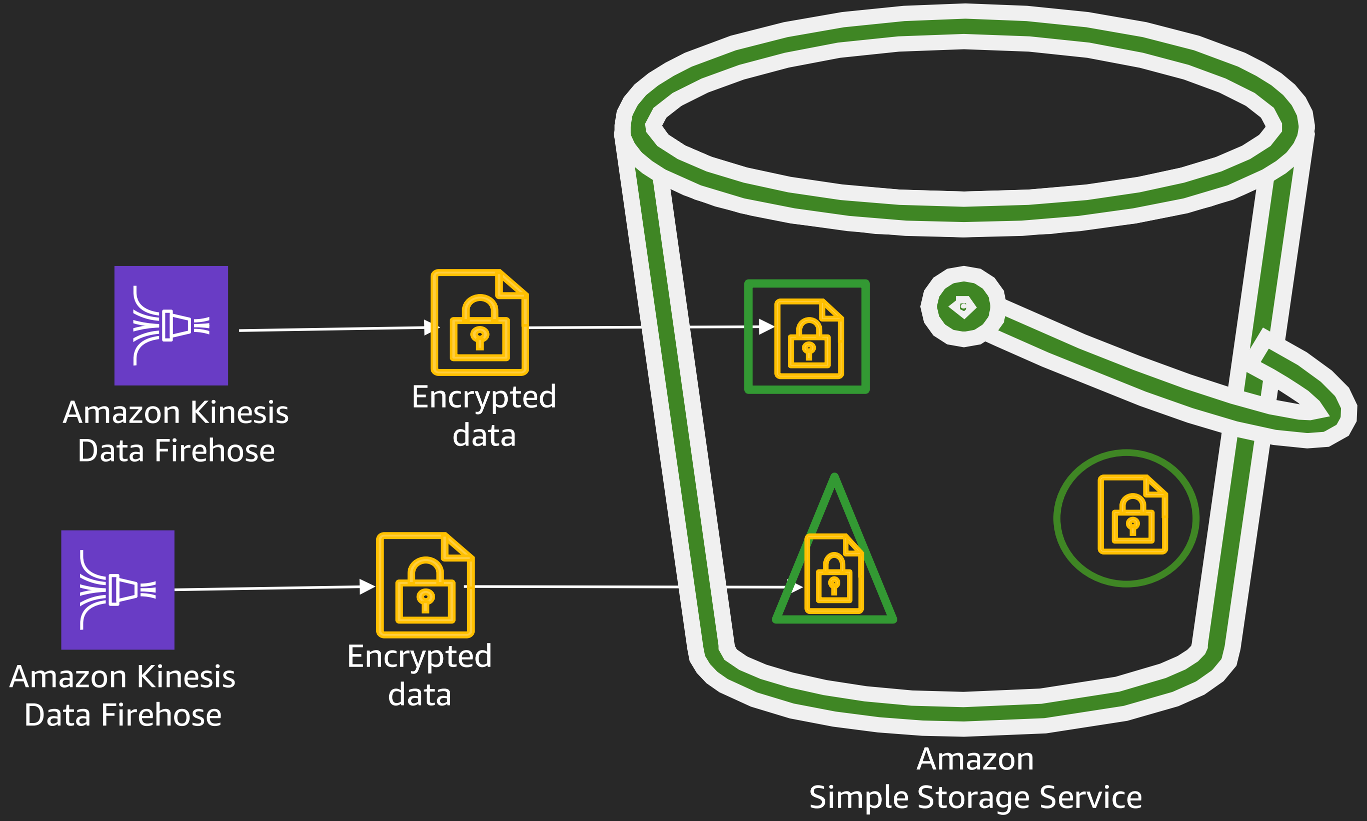
- Lambda functions, managed by Amazon CloudWatch Events and AWS Step Functions, periodically poll third-party APIs for data

Securing the data pipeline

- Unique AWS KMS key per Kinesis data firehose

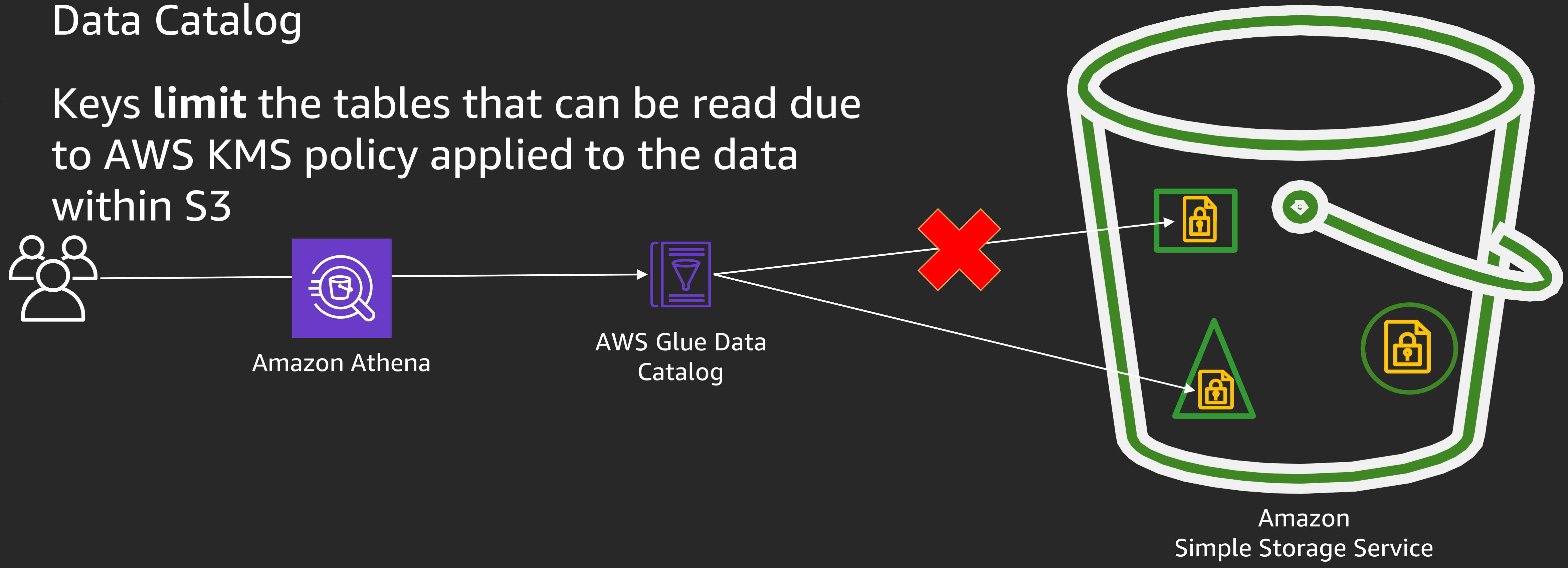
- Different data exists in a single bucket but has different AWS KMS keys

- This allows for granular access to data within a shared bucket


Amazon Kinesis Data Firehose
Encrypted data
Amazon Kinesis Data Firehose
Encrypted data
Amazon Simple Storage Service

Securing Amazon Athena

- AWS KMS keys permit a role to access a Data Catalog
- Keys **limit** the tables that can be read due to AWS KMS policy applied to the data within S3



Learn security with AWS Training and Certification

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 Introduction to Amazon GuardDuty and Deep Dive on Container Security

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

Validate expertise with the **AWS Certified Security - Specialty** exam

Visit aws.amazon.com/training/paths-specialty/

aws training and certification

Thank you!

Kell Rozman
kell.rozman@toyota.com
Matt Costello
costello_matthew@bah.com

Please complete the session survey in the mobile app.