aws health

EMEA HCLS WORKSHOPS

Security, Encryption, and Data Protection

Summer series of free half-day technical workshops

Alexander Barge

Senior Solutions Architect
AWS

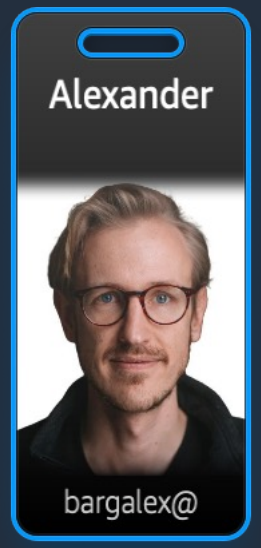
Agenda

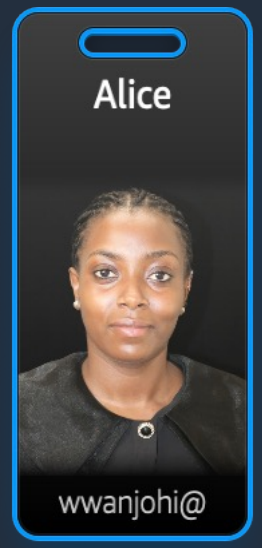
- Security, Identity & Compliance at AWS
- Data Protection Overview
- AWS Key Management & CloudHSM
- LAB – Encryption on AWS
- AWS Secrets Manager
- LAB – Managing Secrets
- Nitro System & Zero Trust

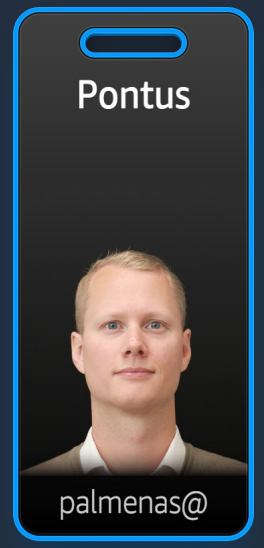
Workshop materials and instructions

- https://catalog.us-east-1.prod.workshops.aws/workshops/aad9ff1e-b607-45bc-893f-121ea5224f24/en-US
- https://catalog.us-east-1.prod.workshops.aws/workshops/8e3a5338-cfc0-4d53-9b97-e8f96c59950a/en-US

Your team for today



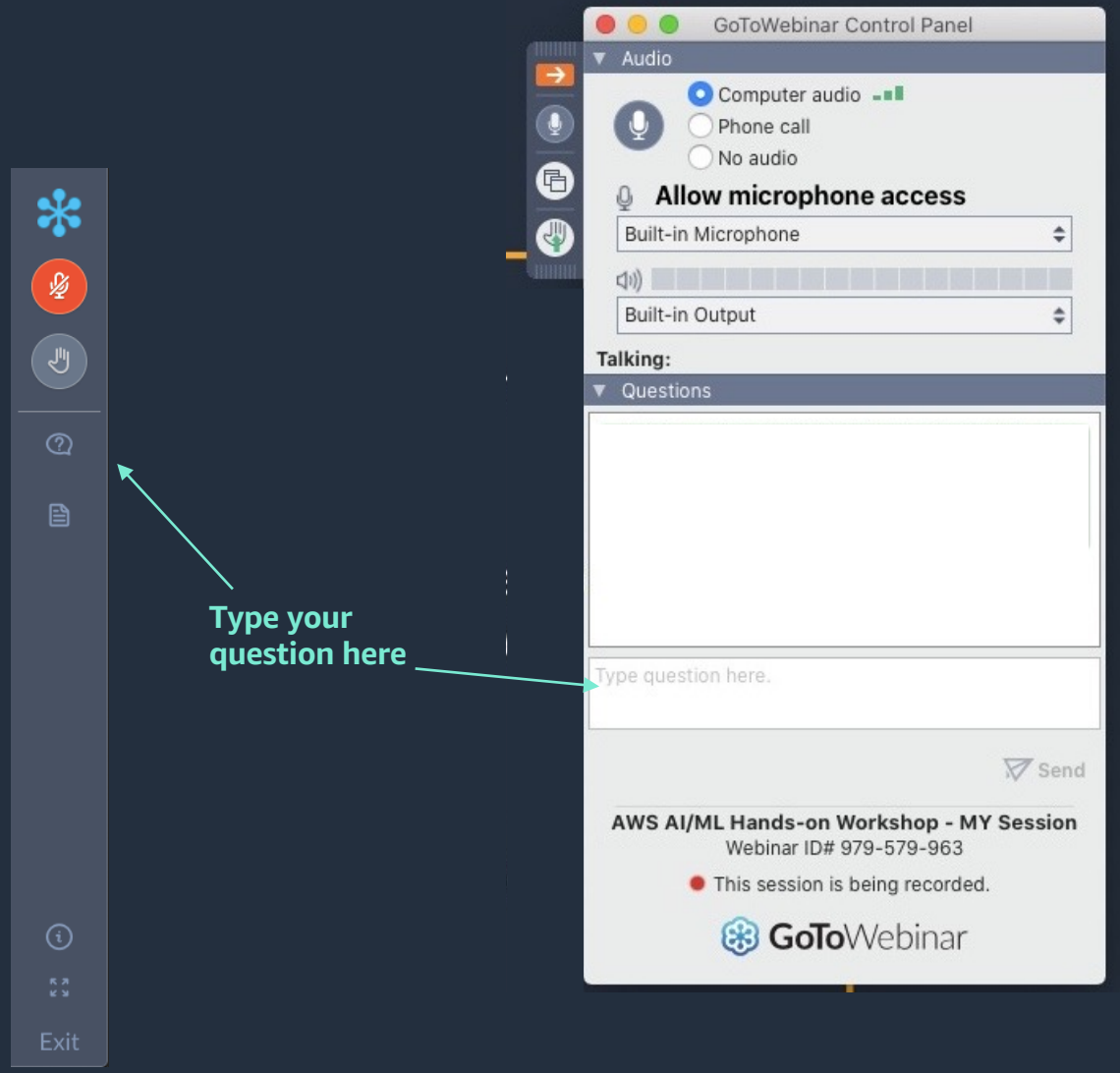




Questions & Answers

If you have any questions or encounter issues during the workshop, our support team is online.

You can submit your query in the GoToWebinar Questions function. To submit questions, select
“Send”



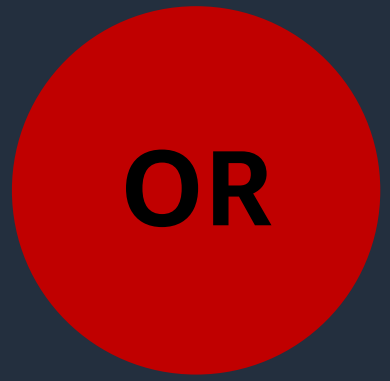
Security, Identity & Compliance at AWS

Why is on-premises security traditionally challenging?

Lack of visibility

Low degree of automation

Before…

Move fast 

Stay secure

Now…

Move fast  Stay secure

The most-sensitive workloads run on AWS

"We prioritize data privacy and security in our platforms as well as ensuring we observe customer preferences. AWS was chosen because it's great in rich web application services."

— Christopher Bird, global platform CTO of messaging, HSBC's Wealth & Personal Banking

"The maturity of AWS infrastructure and the level of security audits that AWS performs on its data centers and services gave us peace of mind. We knew that the privacy and security of patient and customer data would be the top priority."

— Mark Maalouf, Vice President, Global Digital Health, Teva

"Our security program on AWS is far more mature and streamlined than our legacy on premises infrastructure. Using AWS Security Hub in conjunction with our in house tools, we have come a long way in managing security risks since we migrated to AWS."

— Aarushi Goel, Application Security Manager, GoDaddy

Infrastructure & services to elevate your security

Inherit global security and compliance controls

Scale with superior visibility and control

Highest standards for privacy and data security

Automate & reduce risk with deeply integrated services

Largest ecosystem of security partners and solutions

Inherit global security and compliance controls

CSA cloud security alliance SM

CyberGRX exchange member THIRD-PARTY CYBER RISK MANAGEMENT

ISO 9001 International Organization for Standardization

ISO 22301 International Organization for Standardization

ISO 27001 International Organization for Standardization

ISO 27017 International Organization for Standardization

ISO 27701 International Organization for Standardization

ISO 27018 International Organization for Standardization

PCI Security Standards Council PARTICIPATING ORGANIZATION™

AICPA SOC — SOC 1

AICPA SOC — SOC 2

AICPA SOC — SOC 3

CCCS
PIPEDA

CJIS

FedRAMP

FERPA

FIPS 140-2 CRYPTOGRAPHY

FISMA FEDERAL INFORMATION SECURITY MANAGEMENT ACT

GxP

HIPAA

ITAR International Traffic in Arms Regulations Compliant

MPAA

SEC Rule
17a-4(f)

VPAT
Section 508

FINTECH

FISC

irap

정보보호 관리체계 인증 ISMS Information Security Management System

iDA SINGAPORE

FFIEC Federal Financial Institutions Examination Council

C5

CISPE data protection CODE OF CONDUCT

CYBER ESSENTIALS PLUS

CERTIFICACIÓN DE CONFORMIDAD CON EL ens Esquema Nacional de Seguridad Categoría ALTA RD 3/2010

G-Cloud

TISAX ENX ASSOCIATION

Scale with superior visibility and control

Control where your data is stored and who can access it

Fine-grain identity and access controls so users and groups have the right access to resources

Reduce risk via security automation and continuous monitoring

Integrate AWS services with your solutions to support existing workflows, streamline ops, and simplify compliance reporting

Highest standards for privacy and data security

Meet data residency requirements
Choose an AWS Region, and AWS will not replicate it elsewhere unless you choose to do so

Encryption at scale with keys managed by AWS Key Management Service or manage your own encryption keys with AWS CloudHSM using FIPS 140-2 Level 3 validated HSMs

Comply with local data privacy laws by controlling who can access content, its lifecycle, and its disposal

Access services and tools that enable you to **build compliant infrastructure** on top of AWS

Automate and reduce risk with integrated services

Comprehensive set of APIs
and security tools

Continuous monitoring
and protection

Threat remediation
and response

Operational efficiencies to
focus on critical issues

Securely deploy business
critical applications

AWS security, identity, and compliance solutions

Identity and access management

AWS Identity and Access Management (IAM)

AWS IAM Identity Center

AWS Organizations

AWS Directory Service

Amazon Cognito

AWS Resource Access Manager

Amazon Verified Permissions

Detective controls

AWS Security Hub

Amazon GuardDuty

Amazon Security Lake

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

Amazon VPC

AWS PrivateLink

AWS Systems Manager

AWS Verified Access

Data protection

Amazon Macie

AWS Key Management Service (KMS)

AWS CloudHSM

AWS Certificate Manager

AWS Private CA

AWS Secrets Manager

AWS VPN

Server-Side Encryption

Incident response

Amazon Detective

Amazon EventBridge

AWS Backup

AWS Security Hub

AWS Elastic Disaster Recovery

Compliance

AWS Artifact

AWS Audit Manager

Large community of security partners & solutions

Network and infrastructure security

ALERT LOGIC Security. Compliance. Cloud.
APPGATE
ARMOR
Barracuda
Check Point SOFTWARE TECHNOLOGIES LTD.
cisco
ExtraHop
FORTINET
Guardicore
paloalto NETWORKS
PROTECTWISE
SKinfosec co.,ltd.
SOPHOS
zscaler

Host and endpoint security

CROWDSTRIKE
Symantec
TREND MICRO
SentinelOne

Identity and access control

okta
onelogin
Ping Identity
SAVIYNT

Application security

Barracuda
Checkmarx
f5

Vulnerability and configuration analysis

bridgecrew
ExtraHop
Qualys.
RAPID7
tenable
threat stack

Data protection and encryption

CYBERARK
DataSunrise Data & Database Security
gemalto security to be free
HashiCorp
PRIVITAR
THALES
COHESITY

Logging, monitoring, SIEM, threat detection, and analytics

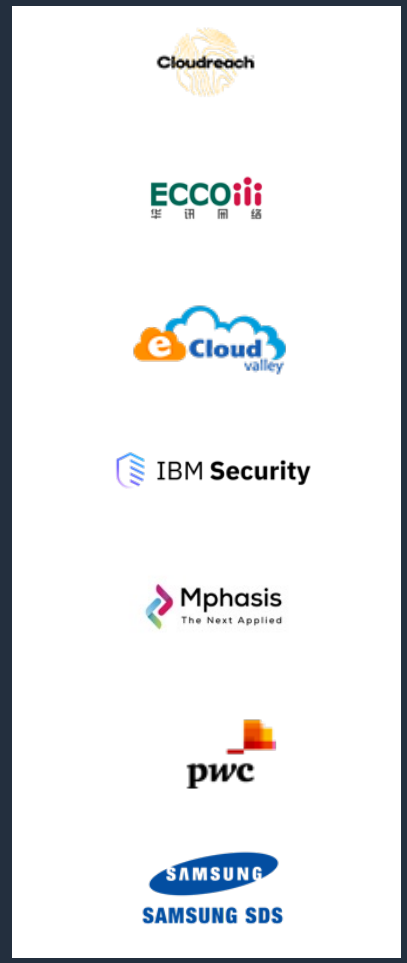
ALIEN VAULT
LACEWORK
McAfee Together is power.
SECURONIX Security Analytics. Delivered.
splunk>
sumo logic

Consulting and technology competency partners

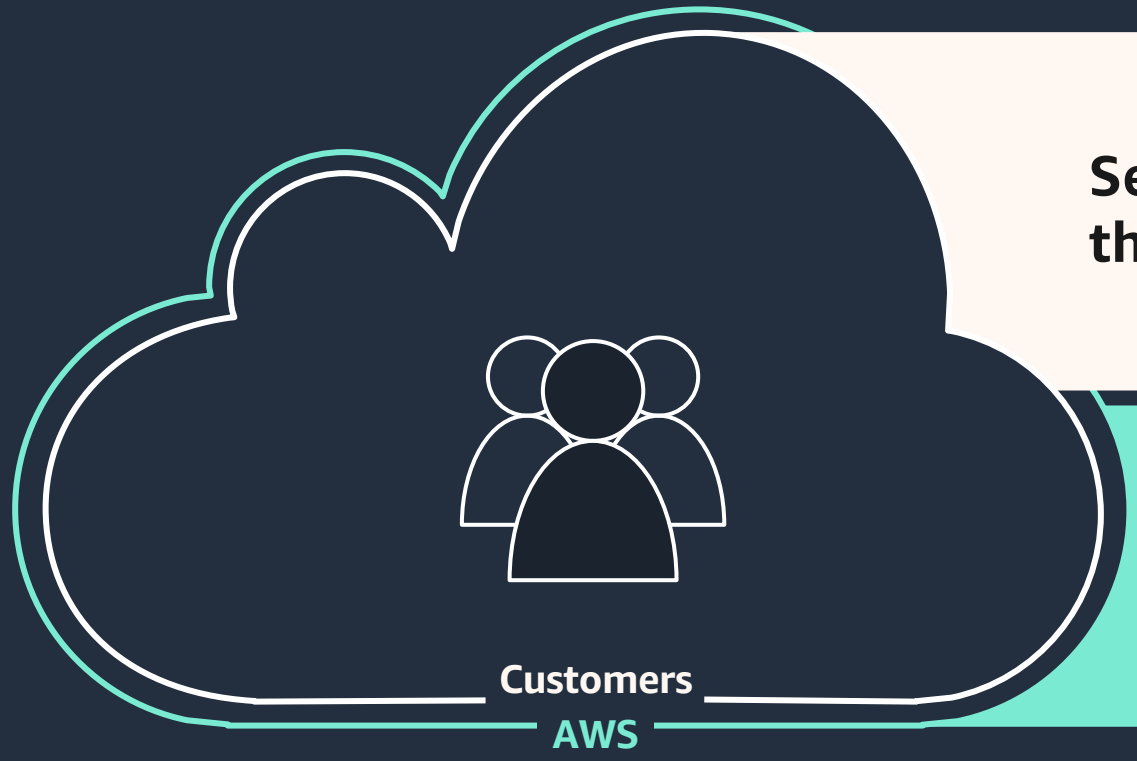
Security engineering

Governance, risk, and compliance

Security operations and automation



Shared responsibility model



Security IN the Cloud

Customer responsibility is determined by the AWS Cloud services a customer selects.

Security OF the Cloud

AWS is responsible for protecting the infrastructure that runs all the services offered in the AWS Cloud.

Identity and access management

Define, enforce, and audit user permissions across AWS services, actions, and resources

AWS Identity and Access Management (IAM)

Securely manage access to AWS services and resources

AWS IAM Identity Center

Centrally manage SSO access to multiple AWS accounts and business apps

AWS Directory Service

Managed Microsoft Active Directory in AWS

Amazon Cognito

Add user sign-up, sign-in, and access control to your web and mobile apps

AWS Organizations

Policy-based management for multiple AWS accounts

AWS Resource Access Manager

Simple, secure service for sharing AWS resources

Amazon Verified Permissions

Fine-grained permissions and authorization for your applications

aws health

Detective controls

Gain the visibility you need to spot issues before they impact your business, improve your security posture, and reduce the risk profile of your environment

AWS Security Hub
Automate AWS security checks and centralize security alerts.

Amazon GuardDuty
Protect your AWS accounts with intelligent threat detection.

Amazon Inspector
Automated and continual vulnerability management at scale.

Amazon CloudWatch
Observe and monitor resources and applications on AWS, on premises, and on other clouds.

AWS Config
Assess, audit, and evaluate configurations of your resources.

AWS CloudTrail
Track user activity and API.

VPC Flow Logs
Capture info about IP traffic going to and from network interfaces in your VPC.

Amazon Security Lake
Automatically centralize your security data in a few steps.

aws health

Infrastructure protection

Reduce surface area to manage and increase privacy for and control of your overall infrastructure on AWS

AWS Firewall Manager

Centrally configure and manage firewall rules across your accounts.

AWS Network Firewall

Deploy network firewall security across your VPCs.

AWS Shield

Maximize application availability and responsiveness with managed DDoS protection.

AWS WAF

Protects your web applications from common exploits.

Amazon Virtual Private Cloud

Define and launch AWS resources in a logically isolated virtual network.

AWS PrivateLink

Establish connectivity between VPCs and AWS services without exposing data to the internet.

AWS Systems Manager

Gain operational insights into AWS and on-premises resources.

AWS Verified Access

Provide secure access to corporate applications without a VPN.

aws health

Data protection

A suite of services designed to automate and simplify many data protection and security tasks ranging from key management and storage to credential management.

Amazon Macie
Discover and protect your sensitive data at scale.

AWS Key Management Service (AWS KMS)
Create and control keys used to encrypt or digitally sign your data.

AWS CloudHSM
Manage single-tenant hardware security modules (HSMs) on AWS.

AWS Certificate Manager
Provision and manage SSL/TLS certificates with AWS services and connected resources.

AWS Secrets Manager
Centrally manage the lifecycle of secrets.

AWS VPN
Connect your on-premises networks and remote workers to the cloud.

Server-Side Encryption
Flexible data encryption options using AWS service managed keys, AWS managed keys via AWS KMS, or customer managed keys.

AWS Private CA
Create private certificates to identify resources and protect data.

aws health

Incident response

During an incident, containing the event and returning to a known good state are important elements of a response plan. AWS provides the following tools to automate aspects of this best practice.

Amazon Detective

Analysis and visualization of security data to get to the root cause of potential security issues quickly

Amazon EventBridge

Serverless event bus that makes it easier to build event-driven applications to scale your programmed, automated response to incidents

AWS Backup

Centrally manage and automate backups across AWS services to simplify data protection at scale

AWS Security Hub

Out-of-the-box integrations with ticketing, chat, SIEM, SOAR, threat investigation, incident management, and GRC tools to support your security operations workflows

AWS Elastic Disaster Recovery

Fast, automated, cost-effective disaster recovery

Compliance

AWS supports security standards and compliance certifications to help you satisfy compliance requirements for virtually every regulatory agency around the globe.

AWS Artifact

No-cost, self-service portal for on-demand access to AWS compliance reports

AWS Audit Manager

Continuously audit your AWS usage to simplify how you assess risk and compliance

aws health

aws health

EMEA HCLS WORKSHOPS

Data Protection Overview

Summer series of free half-day technical workshops

Alexander Barge

Senior Solutions Architect
AWS

Agenda

1. How AWS customers view data protection
2. Overview of AWS data protection services portfolio
3. Security assurance and putting it all together
4. Getting Started

How AWS customers view data protection & privacy

Organizations face unique data protection and data sovereignty risks and challenges

In their shift to the cloud, companies across all industries and sectors are confronting a range of familiar and emerging data privacy issues

Evolving regulatory requirements

Requirements that vary significantly across regions

Highly dynamic security & privacy threat landscape

Stringent reporting and documentation requirements

Limited cloud knowledge & specialists

Drivers of data protection technology

How do I keep my data confidential?

How do I know my data and resources are trustworthy?

How do I control and manage sensitive data?

How do I prove security and compliance to auditors?

Top 4 customer needs from data protection services

Data at rest

Storage encryption

Easily encrypt the data where it resides

Data in transit

Network encryption

Encrypt the data as it moves between networks – enforce data sovereignty

Application Credentials

Managed secrets

Encrypted secrets without the management overhead

Lifecycle Management

Automation

Make security easy and reduce human error

Customers don’t want to day-to-day management for cryptography or preventative controls

Overview of AWS data protection services portfolio

Data protection drives better business outcomes

Protect intellectual property and trade secrets

Protect customer information and build a trusted brand

Automate tasks to save time and reduce risk

Scale with visibility and control as your business grows

Ease of use - integration with hundreds of AWS services

Inherit global security and compliance controls

aws health

Data Protection on AWS

A suite of services designed to automate and simplify many security tasks ranging from key management and storage to credential management

Amazon Macie
Discover and protect your sensitive data at scale

AWS Key Management Service (AWS KMS)
Create and control keys used to encrypt or digitally sign your data

AWS CloudHSM
Manage single-tenant hardware security modules (HSMs) on AWS

AWS Certificate Manager
Provision and manage SSL/TLS certificates

AWS Private Certificate Authority
Create private certificates to identify resources and protect data

AWS Secrets Manager
Centrally manage the lifecycle of secrets

aws health

Data protection

A suite of services designed to automate and simplify many data protection and security tasks ranging from key management and storage to credential management.

Amazon Macie
Discover and protect your sensitive data at scale.

AWS Key Management Service (AWS KMS)
Create and control keys used to encrypt or digitally sign your data.

AWS CloudHSM
Manage single-tenant hardware security modules (HSMs) on AWS.

AWS Certificate Manager
Provision and manage SSL/TLS certificates with AWS services and connected resources.

AWS Secrets Manager
Centrally manage the lifecycle of secrets.

AWS VPN
Connect your on-premises networks and remote workers to the cloud.

Server-Side Encryption
Flexible data encryption options using AWS service managed keys, AWS managed keys via AWS KMS, or customer managed keys.

AWS Private CA
Create private certificates to identify resources and protect data.

aws health

How does AWS help customers with data protection?

"How do we move our data to AWS securely?"

Client-side encryption to encrypt inbound data

AWS Certificate Manager for SSL/TLS certificates

"How do we keep data on AWS confidential?"

Server-side encryption to encrypt data at-rest

AWS KMS and CloudHSM for enterprise key management and FIPS 140 validated HSMs

"How do we securely share data and resources within the cloud?"

AWS Identity and Access Management – Cross-Account Access

"How do we manage authentication and authorization?"

AWS IAM and Secrets Manager for identity and credentials management

"How do I prove security and compliance to auditors?"

AWS Management & Governance integrations

"How do we optimize cost and performance?"

"How do we architect for availability?"

"How do we scale?"

- Well-Architected Guidance
- Available in all Regions
- Our services are used by all other AWS services
- Cryptographic SDKs for application encryption
- Multi-Region Keys for Disaster Recovery

aws health

Security assurance and provable data protection

Notify me if my desired encryption settings are modified

AWS Config

Utilize AWS Config Managed Rules to monitor encryption configuration changes in your AWS environment

Examples:

- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- cloud-trail-encryption-enabled

Monitor usage of ACM certificates and KMS keys

AWS CloudTrail

Use AWS CloudTrail to create detailed logs of API calls to the KMS and ACM services for audit purposes

A KMS API action was called:

- by who (user, account, IP)
- when (timestamp)
- where, why (KMS key, AWS resource)

Audit important lifecycle events for certificates and KMS keys

Amazon CloudWatch

Use Amazon CloudWatch Metrics and Events to monitor important events and API calls in your AWS accounts
Examples:

- Metrics: time until key/certificate expiration
- Events: key rotation, key deletion, imported key expiration, certificate renewal

AWS Data Privacy & Security Differentiation

Storage: Customers choose the AWS Region(s) in which their content is stored and the type of storage to comply with data sovereignty regulations.

Security: Customers choose how their content is secured. AWS uses FIPS 140 validated HSMs for storing cryptographic key material and NIST standardized cryptographic primitives, algorithms and schemes.

Access: AWS prohibits, and our systems are designed to prevent, remote access by AWS personnel to customer data for any purpose, including service maintenance, unless access is requested by the customer, is required to prevent fraud and abuse, or to comply with law.

Disclosure of Customer Content: We will not disclose customer content unless we're required to do so to comply with the law or a binding order of a government body.

Security Assurance: AWS security protections and control processes are independently validated by multiple third-party independent assessments. 2,500 security controls audited each year.

Third-party validation

aws health

EMEA HCLS WORKSHOPS

AWS Key Management Service and CloudHSM

Alice Wanjohi

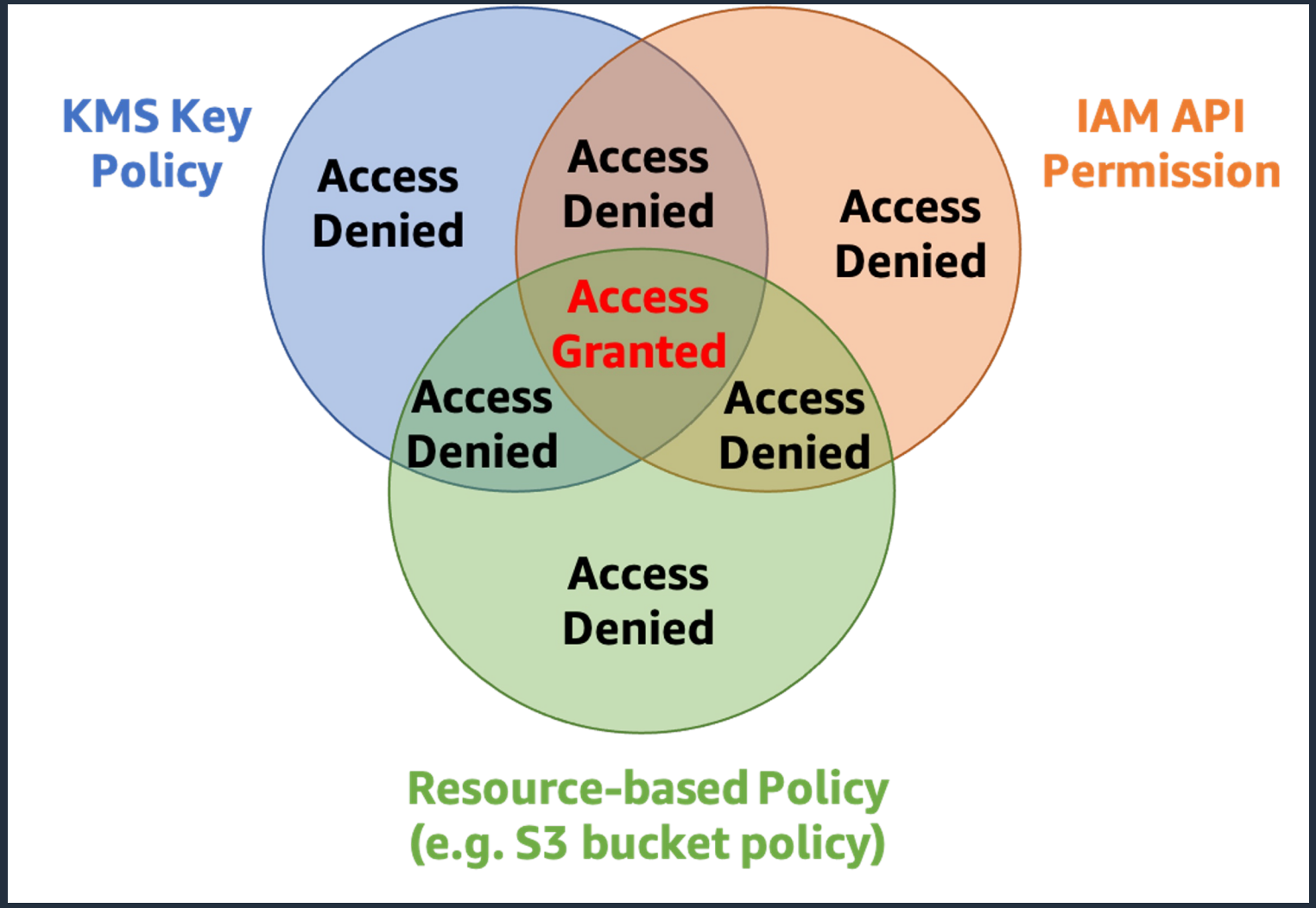
Associate Solutions Architect
AWS

Agenda

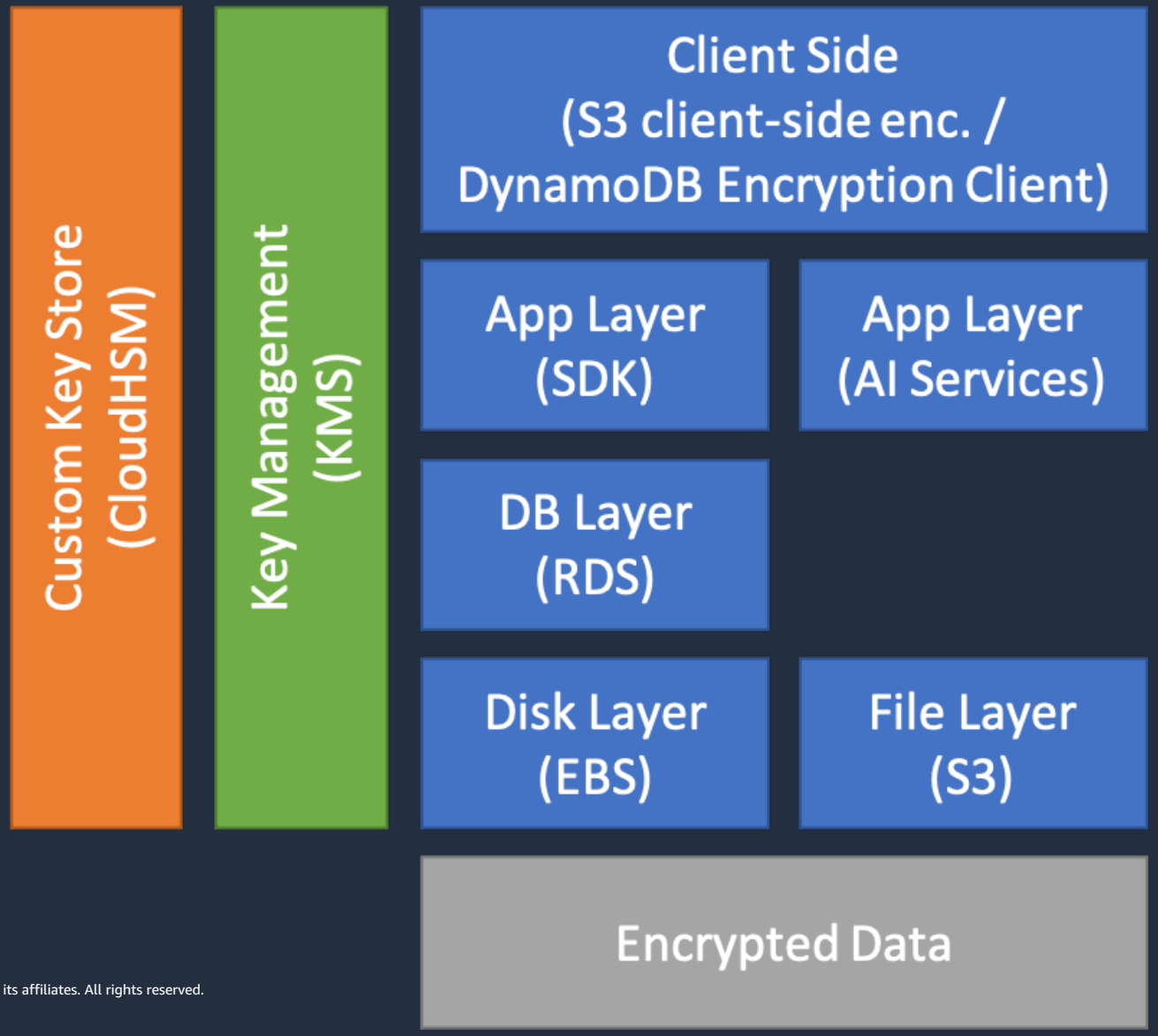
1. Why Encrypt?
2. Levels of encryption
3. AWS KMS
4. AWS CloudHSM
5. Get started with AWS Encryption Workshop

aws health

Why Encrypt?



Levels of Data Encryption



aws health

EMEA HCLS WORKSHOPS

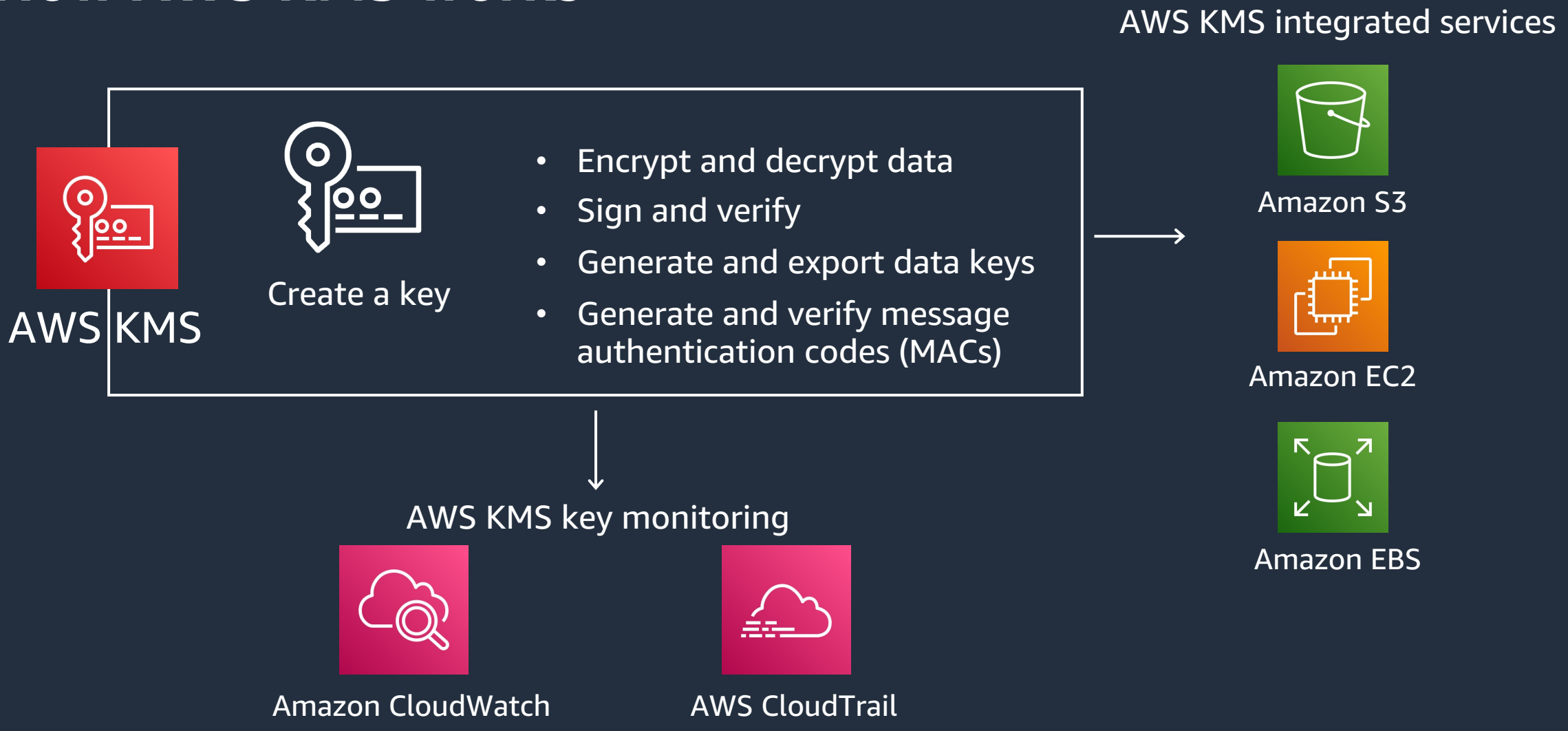
AWS Key Management Service

Create and control keys used to encrypt or digitally sign your data

What is AWS KMS?

- AWS KMS lets you create, manage, and control cryptographic keys across your applications
- AWS KMS is incorporated in over 100 AWS services to encrypt sensitive data and create digital signatures

How AWS KMS works



Benefits

Centrally manage keys and define policies across integrated services and applications from a single point

Encrypt data within your applications with the AWS Encryption SDK data encryption library

Perform **signing operations** using asymmetric key pairs to validate digital signatures

Securely generate Hash-based Message Authentication Codes (HMACs) that provide message **integrity** and **authenticity**

Why **AWS KMS**?

AWS KMS is a highly available, cost-effective service that manages encryption keys on AWS

Use cases

Protect your data at rest

Encrypt and decrypt data

Sign and verify digital signatures

Validate JSON web tokens using HMAC

aws health

EMEA HCLS WORKSHOPS

AWS CloudHSM

Manage your security in the cloud

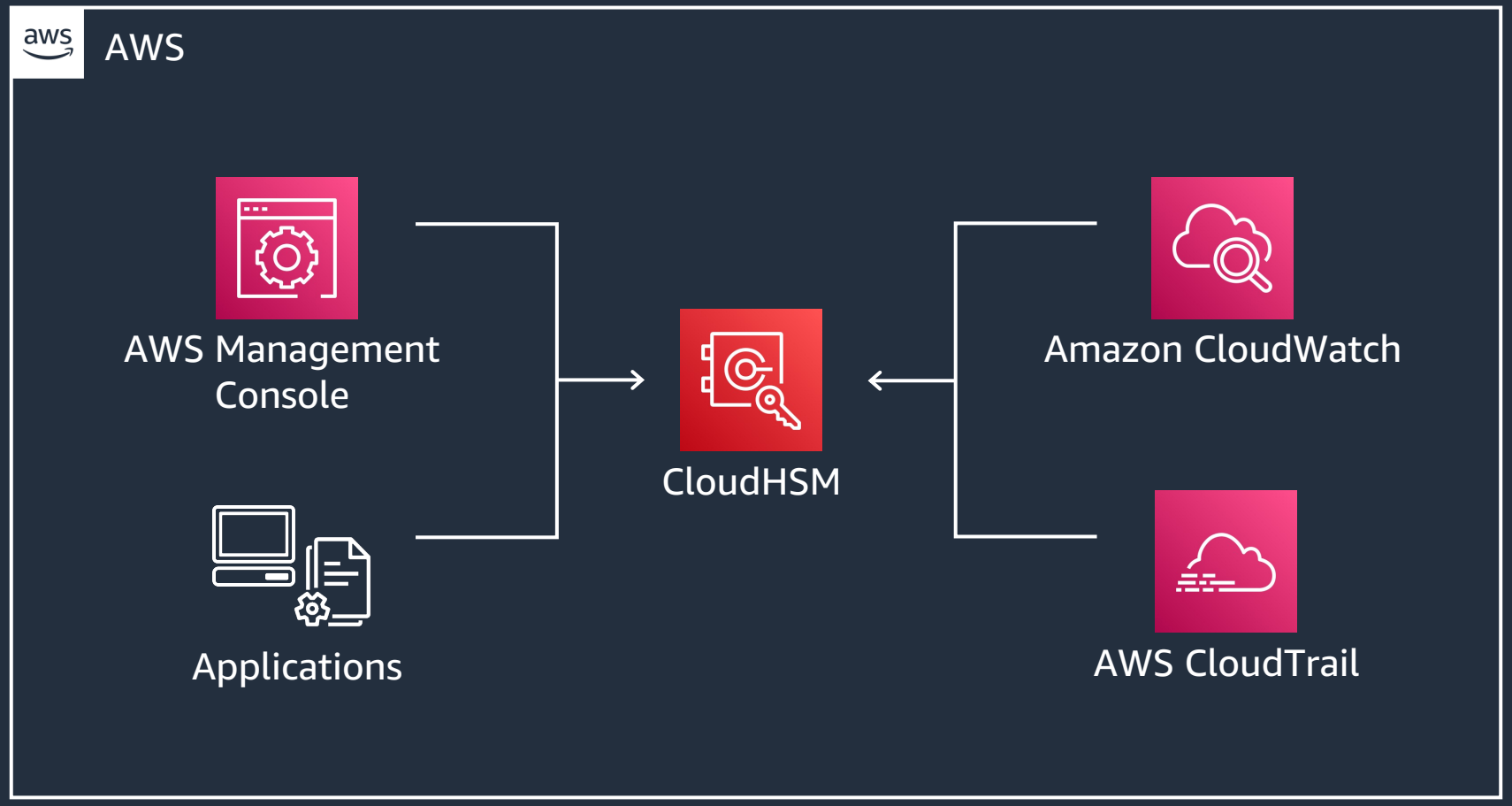
What is CloudHSM?

CloudHSM

CloudHSM allows you to manage single-tenant hardware security modules (HSMs) on AWS

It helps you meet corporate, contractual, and regulatory compliance requirements for data security

How CloudHSM works



Benefits

Deploy workloads with **high reliability** and **low latency**, and help meet **regulatory compliance**

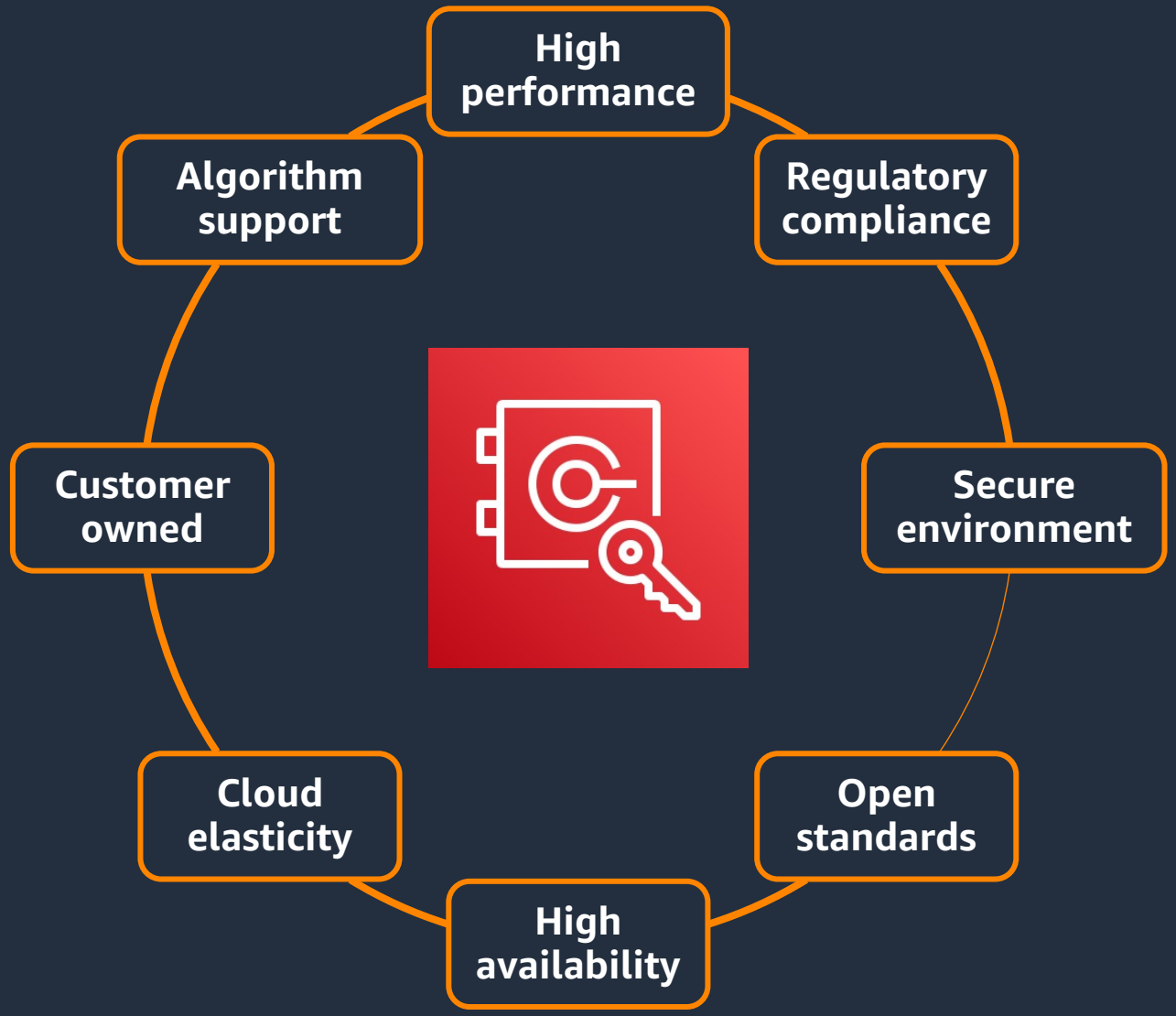
Generate and use cryptographic keys on dedicated FIPS 140-2 L3 single-tenant HSM instances

Pay by the hour, and back up and shut down HSMs when they're not needed

Manage HSM capacity and **control your costs** by adding and removing HSMs from your cluster

Why CloudHSM?

Customers use HSMs on AWS because they need **low-latency access** to a **secure root of trust** that is under **their control**



Options to meet your requirements

CloudHSM and AWS Key Management Service (AWS KMS) both offer a high level of security and compliance for your cryptographic keys

AWS KMS is a highly managed, cost-effective service that manages encryption keys on AWS

CloudHSM gives you the option of single-tenant access and control over your HSMs, suitable for legacy workload requirements

Create a **custom key store**, a secure location for storing cryptographic keys, using an AWS KMS resource associated with a CloudHSM cluster that you own and manage

Use cases

- Encrypt data at rest
- Offload SSL processing for web servers
- Protect private keys for an issuing certificate authority (CA)
- Protect private keys for native database encryption solutions

Get started

AWS security workshops

Engage in hands-on workshops to build, deploy, and manage security services on AWS

AWS Security Immersion Day

Participate in a guided day of security and data protection with AWS solutions architects

AWS Management Console

Start generating and using your own encryption keys on AWS

AWS Encryption Workshop

- 1 hour long. End time: 3.30pm
- Remember to check the region of services and resource creation
- What to cover()
  - Introduction – setting up environment
  - Key Management: KMS
  - Encrypt and decrypt data on at least one service
- Event engine:
  - https://dashboard.eventengine.run/
  - Event Hash: 58d6-1b2bed1384-f2

https://catalog.us-east-1.prod.workshops.aws/workshops/aad9ff1e-b607-45bc-893f-121ea5224f24/

aws health

EMEA HEALTHCARE & LIFE SCIENCES WORKSHOPS

AWS Secrets Manager

Centrally manage the lifecycle of secrets

Désirée Brunner (she/her)

Solutions Architect
Amazon Web Services

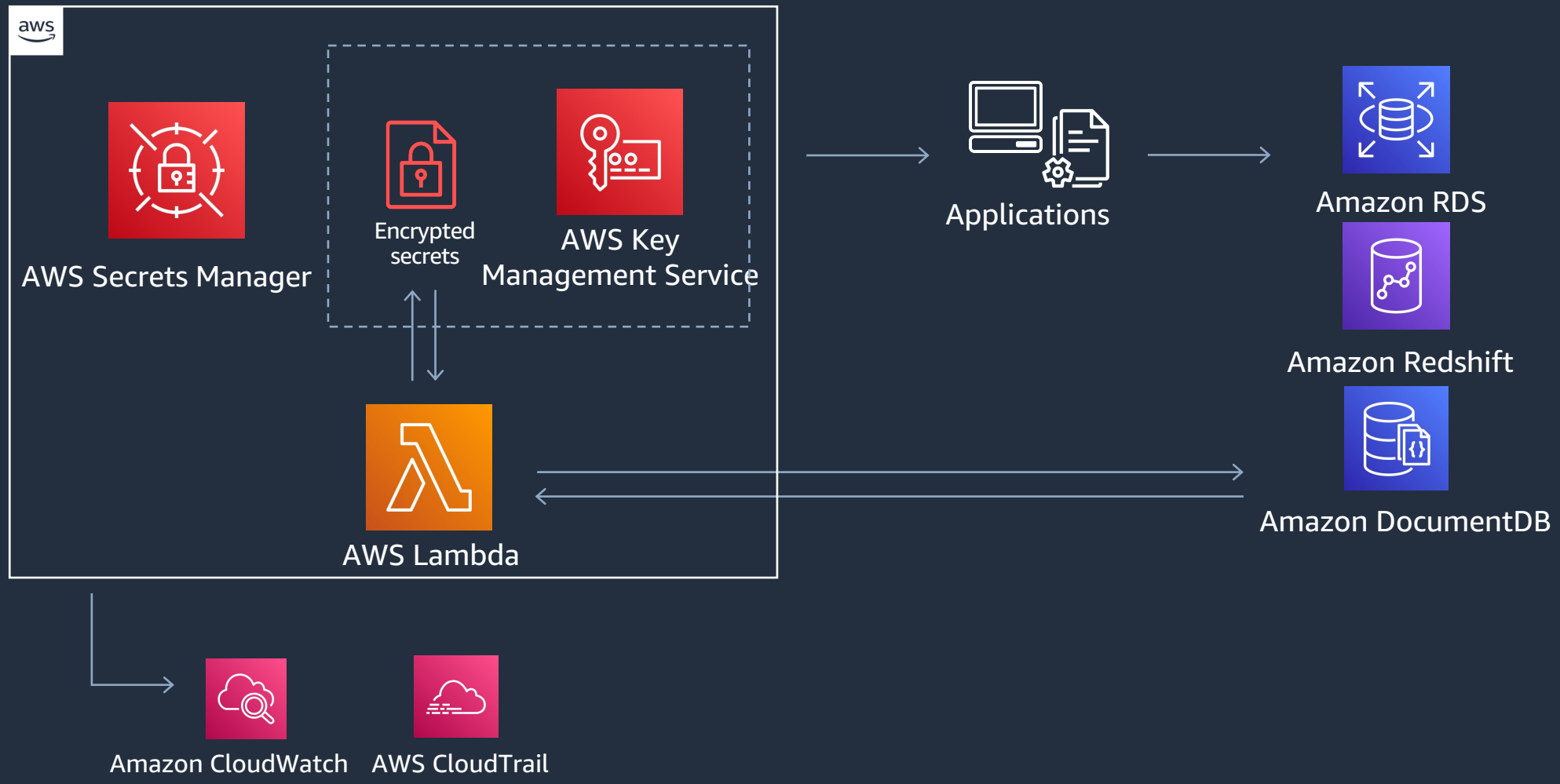
Agenda

- What is AWS Secrets Manager?
- Service benefits and features
- Get started / Lab

What is AWS Secrets Manager?

AWS Secrets Manager helps you manage, retrieve, and rotate database credentials, API keys, and other secrets throughout their lifecycle

How AWS Secrets Manager works



Benefits

Securely **encrypt** and centrally **audit** secrets such as database credentials and API keys

Manage access with **fine-grained** AWS Identity and Access Management (IAM) controls and resource-based policies

Automatically rotate secrets to meet your security and compliance requirements

Replicate secrets to support multi-Region applications and disaster recovery scenarios

Get started

AWS security workshops

Engage in hands-on workshops to build, deploy, and manage security services on AWS

AWS Security Immersion Day

Participate in a guided day of security and data protection with AWS solutions architects

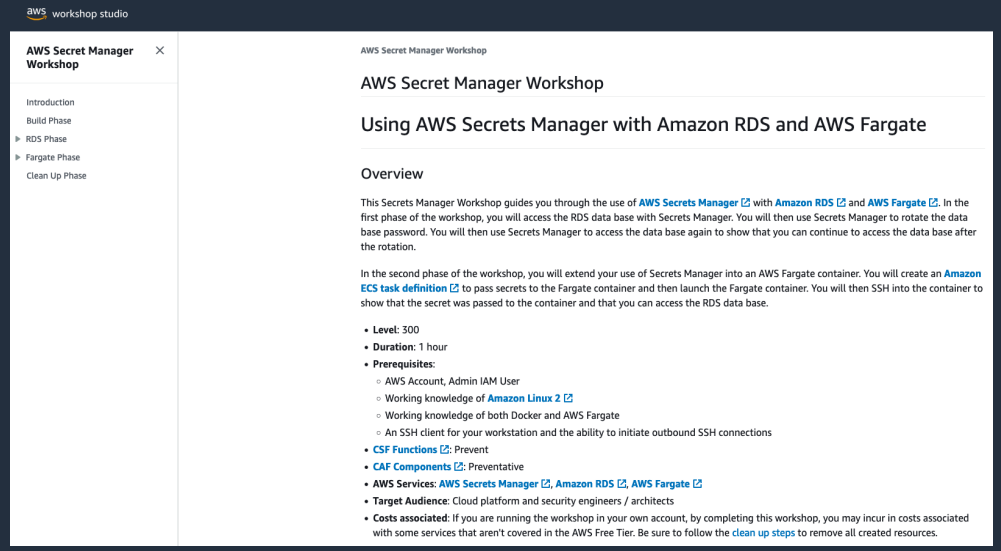
AWS Management Console

Start encrypting secrets at rest in tandem with AWS KMS

Get started

https://dashboard.eventengine.run/

Event Hash:
58d6-1b2bed1384-f2



https://catalog.us-east-1.prod.workshops.aws/workshops/8e3a5338-cfc0-4d53-9b97-e8f96c59950a/en-US/

AWS Secrets Manager Workshop

- ~ 40 min
- AWS CloudFormation initial stack creation takes ca. 10min
- Important to check the region of services and resource creation
- Fargate use case:
  - Run on Bastion Host
    sed s/amazonlinux/amazonlinux:2/1 Dockerfile
  - Add to the Bastion Host IAM Role
    arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerRegistryFullAccess
  - AWS ECS – Task definitions, Run task is under “Deploy” not Actions
  - To run a task and be able to connect, use the same VPC Network created in the demo and use the Bastion Host Security Group

aws health

EMEA HEALTHCARE & LIFE SCIENCES WORKSHOPS

Zero Trust and **confidential computing**

An AWS Perspective

Pontus Palmenäs (he/him)

Solutions Architect, HCLS
Amazon Web Services

Your presenter today

Pontus Palmenäs

palmenas@amazon.com

Agenda

- Zero Trust Fundamentals
- Supporting services and Partner solutions
- Confidential compute with AWS Nitro System

Zero Trust Fundamentals

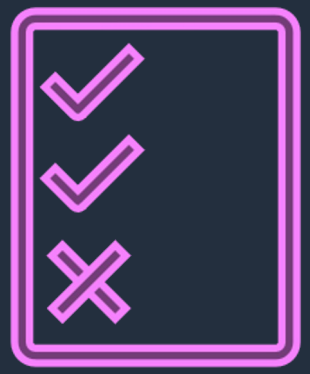
Zero Trust is a **conceptual model** and an associated set of **mechanisms** that focuses on providing security controls around digital assets *that do not solely or fundamentally depend on traditional network controls or network perimeters*

Who can access what

Who

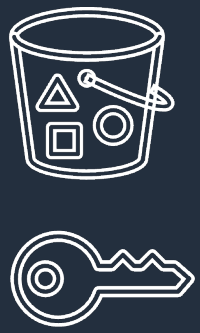
Developers and applications

Can access



Permissions

What



Resources

Zero Trust Decision Points

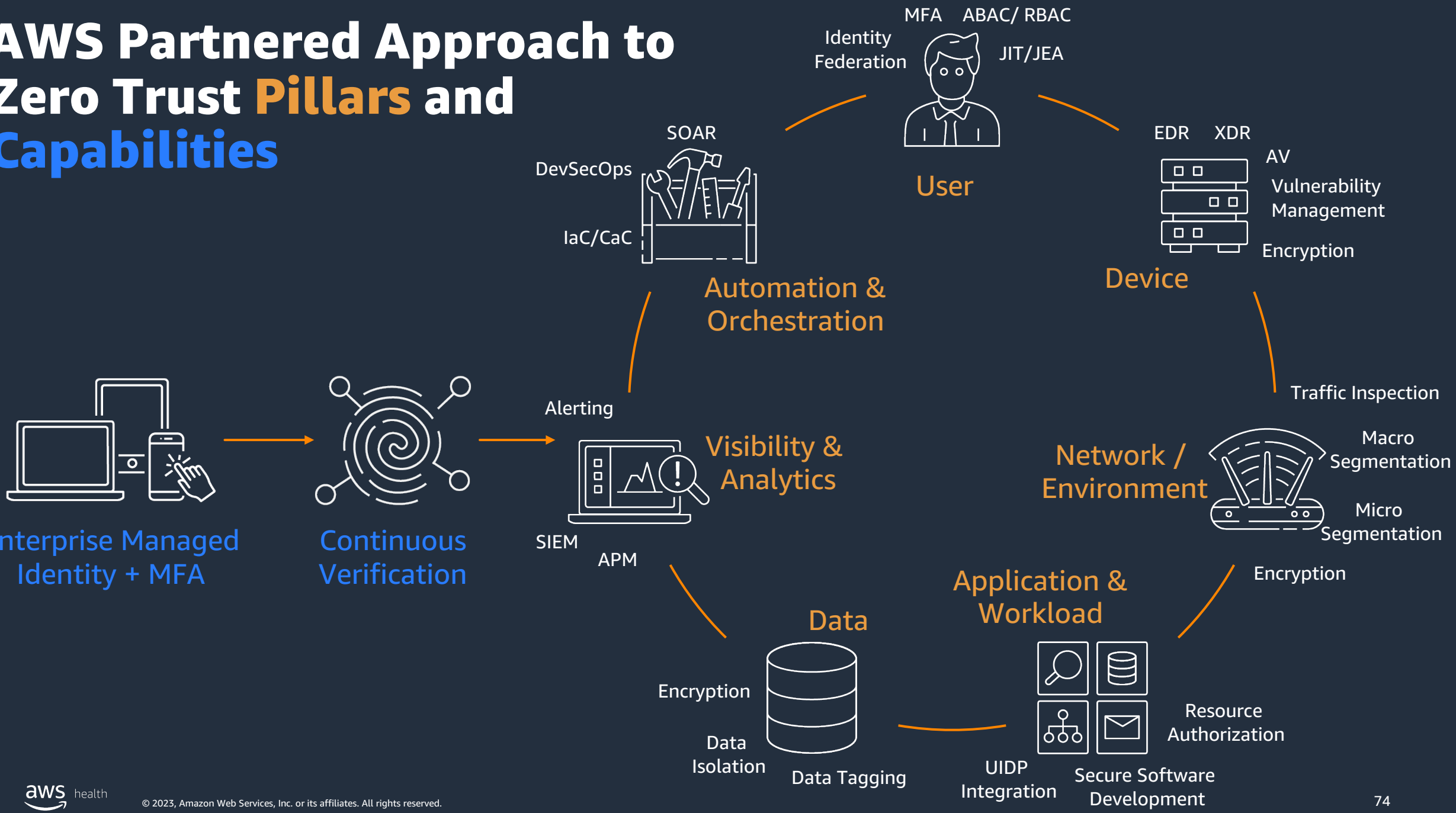
- Who (role)
- What (application, resource)
- Where (physical or network location)
- When (time of day)
- Why (intent, classification)
- How (posture, risk score)

AWS Zero Trust Principles

1. Verify and authenticate
2. Least privilege access
3. Micro-segmentation
4. Continuous monitoring and analytics
5. Automation and orchestration

AWS Prescriptive Guidance
“Embracing Zero Trust”

AWS Partnered Approach to Zero Trust Pillars and Capabilities



AWS Supporting Services

Multi-Factor Authentication and Least-Privilege Access

AWS Identity and Access Management

MFA Support

Identity Federation

AWS Identity and Access Management

Enterprise IDP (IDaaS, etc.)

Encryption

AWS Key Management Service (KMS)

AWS Certificate Manager (ACM)

Macro-Segmentation

Amazon VPC

AWS WAF

AWS Transit Gateway

Fine-Grained User and Device Access

Session Manager

Amazon WorkSpaces

Amazon AppStream 2.0

AWS Verified Access

Vulnerability Management

Amazon Inspector

User and Application Inventory

AWS Systems Manager

AWS Directory Service

Amazon Cognito

Automated Vulnerability and Patch Management

AWS Systems Manager

Patch Manager

Micro-Segmentation

AWS Network Firewall

AWS PrivateLink

Amazon VPC Lattice

Security and Audit Logging

Amazon OpenSearch Service

AWS CloudTrail

Amazon VPC Flow Logs

Amazon CloudWatch

Amazon Security Lake

Critical Process Automation

AWS OpsWorks

AWS CloudFormation

AWS Command Line Interface (AWS CLI)

AWS CodePipeline

AWS Tools and SDKs

AWS Zero Trust Partners

DoD Data Centric Security Protections

Network-centric

- Login/password access
- User-based Access (file permissions)
- Device-based Access
- Role-Based Access Control (RBAC)
- Encryption at Rest

Data-centric

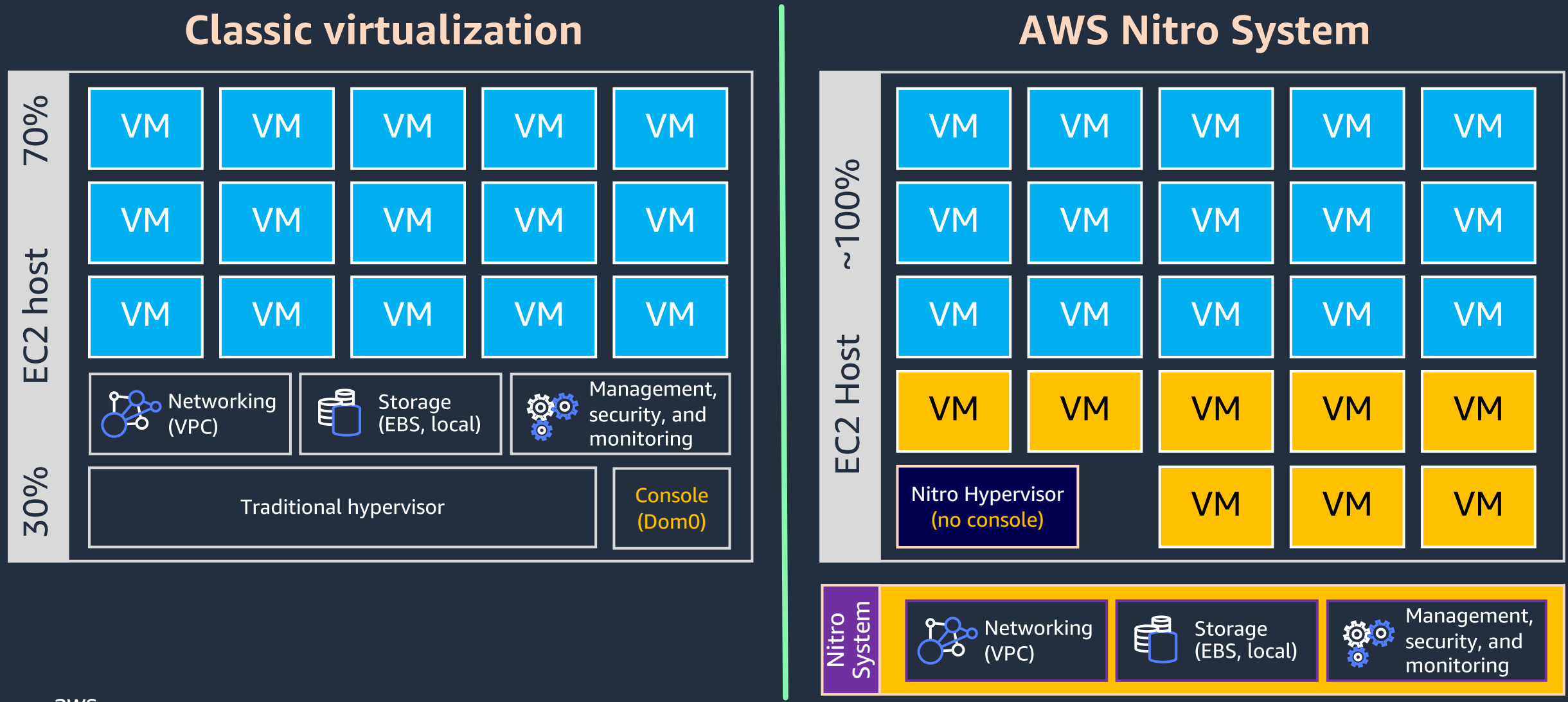
- Field & Record Level Encryption
- Universal Encryption in Transit
- Data Rights Management (DRM)
- Data Loss Prevention (DLP)
- Attribute-Based Access Control (ABAC)
- Data Tagging
- Dynamic Data Masking

AWS Nitro System

Today, over 60 million new instances are spun up every day on Amazon EC2*

** Including ECS, EKS, and AWS Batch on EC2*

Reinventing virtualization for the cloud

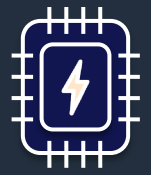


AWS Nitro System

Nitro Cards

VPC networking
Amazon EBS
Instance storage
Nitro SSDs
System controller

Nitro Security Chip



Integrated into motherboard
Traps I/O to nonvolatile storage
Hardware root of trust
Protects hardware resources

Nitro Hypervisor

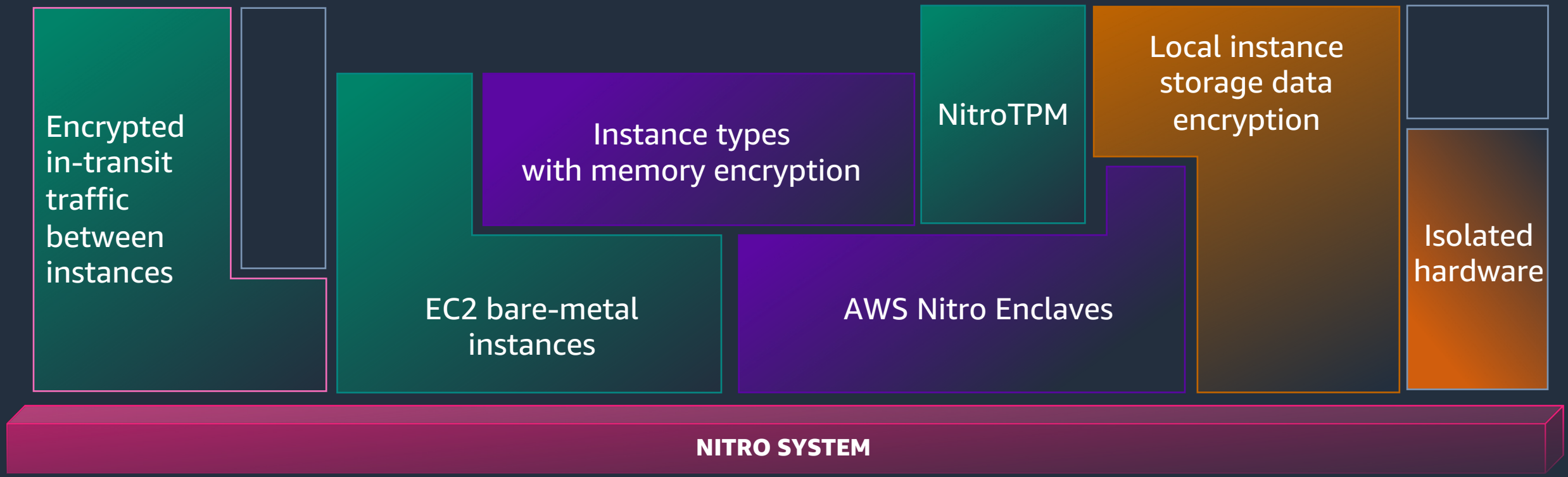
Lightweight hypervisor
Memory and CPU allocation
Bare-metal-like performance

NitroTPM

Trusted Platform Module 2.0
Instance health attestation
Cryptographic offload

Nitro System security

NITRO IS THE FOUNDATION FOR INNOVATIONS IN CONFIDENTIALITY AND PRIVACY



aws health

AWS Nitro System security

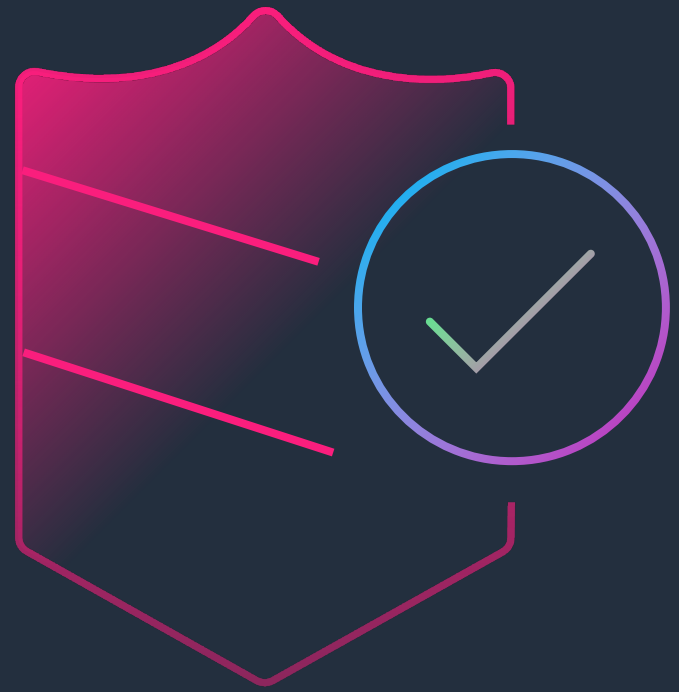
AWS Nitro Cards are physically separate from the hardware running customer instances

Dedicated CPU, memory, and hardware security chip

Virtual instances are fully isolated from one another and from the Nitro Hypervisor

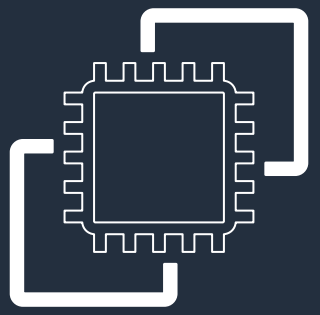
Instances don’t share CPU cores or L1/L2 caches

Memory encryption w/ Graviton 2/3/3E and Intel Ice Lake



aws health

Nitro security – Confidential compute



AWS Nitro System

No operator access whitepaper

All interactions with the AWS Nitro System are through narrow, authorized, and authenticated APIs

There is no mechanism for any system or person to log in to the underlying Amazon EC2 host **(no operational access)**

There is no interactive access (no SSH, no general-purpose access of any kind)

Debugging features can’t disclose customer data

Nitro Systems run in an isolated network

aws health

EMEA HEALTHCARE & LIFE SCIENCES WORKSHOPS

https://aws-experience.com/

- June 27th: AWS Cloud Fundamentals
- June 28th: Genomic Data Analysis with Amazon Omics
- July 4th: Machine Learning
- July 5th: AWS for Pharma Manufacturing
- July 6th: Security, Encryption & Data Protection Immersion Day
- July 11th: Sustainability
- July 13th: High-performance computing
- July 18th: Compliance in the Cloud

aws health

Please complete the workshop survey

https://www.aws-experience.com/emea/dach-cee/event-survey/cbfe7c90708b-a539-2b44-696f-add17524

aws health

Thank you!

Alexander Barge
bargalex@amazon.com

Alice Wanjohi
wwanjohi@amazon.ae

Désirée Brunner
desibru@amazon.de

Pontus Brunner
palmenas@amazon.com

Lorenzo Gatti
lgatti@amazon.ch