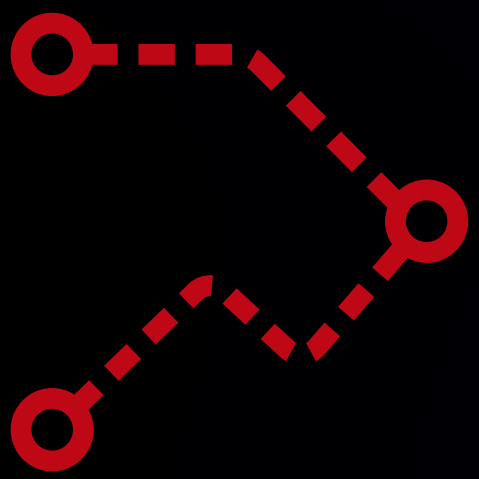
SEC301

Locks without keys: AWS and confidentiality

Colm MacCárthaigh
VP/Distinguished Engineer
Amazon Web Services

Disclaimers

- Compliance is a journey, and the AWS compliance team can help you with yours



- This talk includes several movie-plot threat models

Calling AWS support

- We love to help people
- AWS support can’t access your EC2 instances or your data
- `AWSSupportServiceRolePolicy`
- Customers have to explicitly grant any access

Customer data is “radioactive”

- We never want to see or touch it directly
- We build shielding so that we can’t see or touch it directly
- We give customers many of the same tools for their customer data

Shield material

AWS staff uses best practices

Physical security

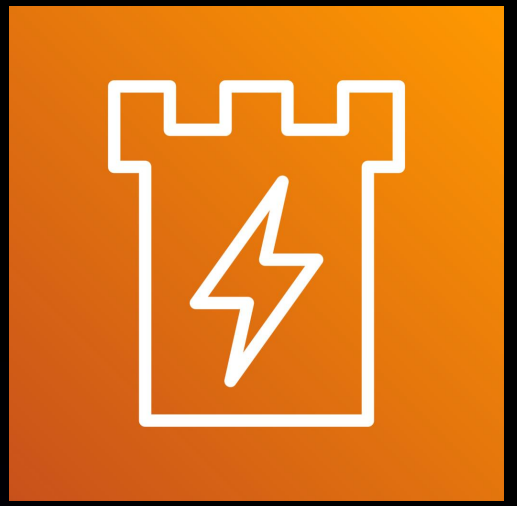
Monitoring and detective controls

Shield material

AWS Identity and Access Management

Cryptography

AWS Nitro



Principle of least privilege

- Don’t grant access unless it is needed
- Grant access only while it is needed
- Prove that it is needed

AWS Identity and Access Management (IAM)

- The IAM service and SigV4 protocols are widely used internally
- Access between services is mediated by principals, roles, policies, etc.

AWS Identity and Access Management (IAM)

- All access is reviewed by AWS Security and AWS IAM
- The IAM service is also ring-fenced internally

AWS Identity and Access Management (IAM)

- Transparency and consent are front and center
- Changes over time are not applied automatically and are published and tracked
- Customers can revoke access

AWS Identity and Access Management (IAM)

- Managed policies specify what kinds of permissions a service may have to your resources
- We use AWS IAM Access Analyzer to constantly baseline the permissions that we ourselves use

AWS IAM Access Analyzer

Access Analyzer

Monitor access to resources

How it works

1 Create an analyzer

You can set the scope for the analyzer to an organization or an AWS account. This is your zone of trust. The analyzer scans all of the supported resources within your zone of trust.

2 Review active findings

When Access Analyzer finds a policy that allows access to a resource from outside of your zone of trust, it generates an active finding. Findings include details about the access so that you can take action.

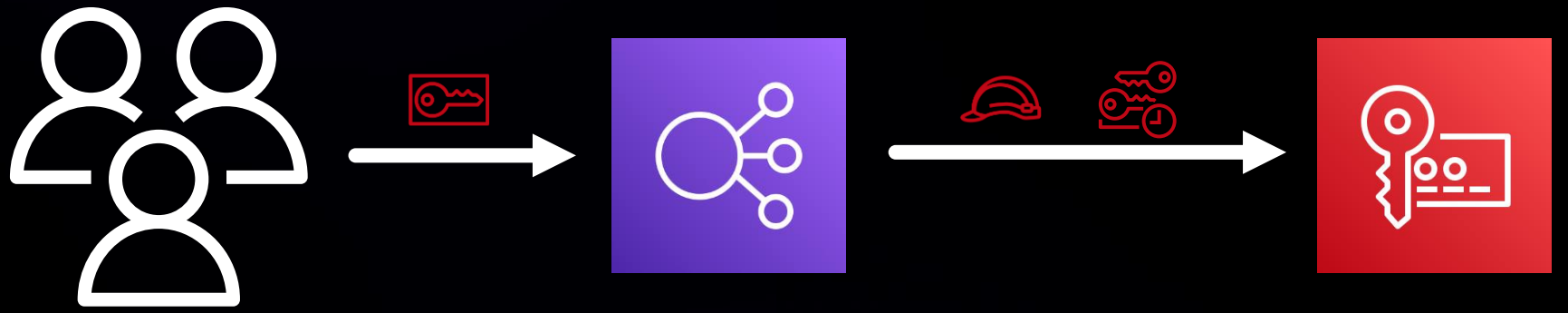
3 Take action

If the access is intended, you can archive the finding so that you can focus on reviewing active findings. If the access is not intended, you can resolve the finding by modifying the policy to remove access to the resource.

AWS Identity and Access Management (IAM)

- IAM also has support for time-limited “forward access sessions” based on a cryptographic chain of custody
- “On behalf of” access is granted to a service only if that service can prove it was recently called by the customer

IAM Forward Access Sessions



Customer signs request to S3 with their key

S3 signs request to KMS with a temporary key derived from the customer request

IAM Forward Access Sessions

- Server-side encryption with KMS keys
- Launching VPC PrivateLink endpoints
- Attaching VPC Transit Gateways

IAM Forward Access Sessions

- AWS CloudFormation
- AWS Cloud Control API
- EC2 access to EBS encryption key grants

IAM and SigV4

- Customer’s AWS secret keys are stored only in the central IAM system and are not on our AWS services
- Signing keys are per day, per service, per Region
- SigV4A uses public-private keys

Contingent authorization

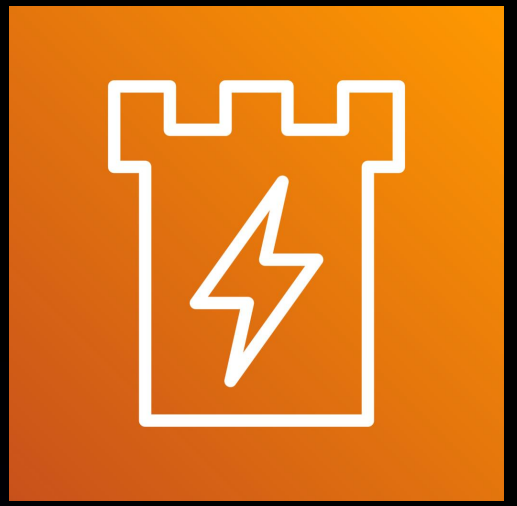
- Our philosophy: “hands off,” “no login,” and “no general purpose access” management of AWS systems
- What about unpredictable emergencies? Break-glass only access with contingent authorization and reporting

Shield material

AWS Identity and Access Management

Cryptography

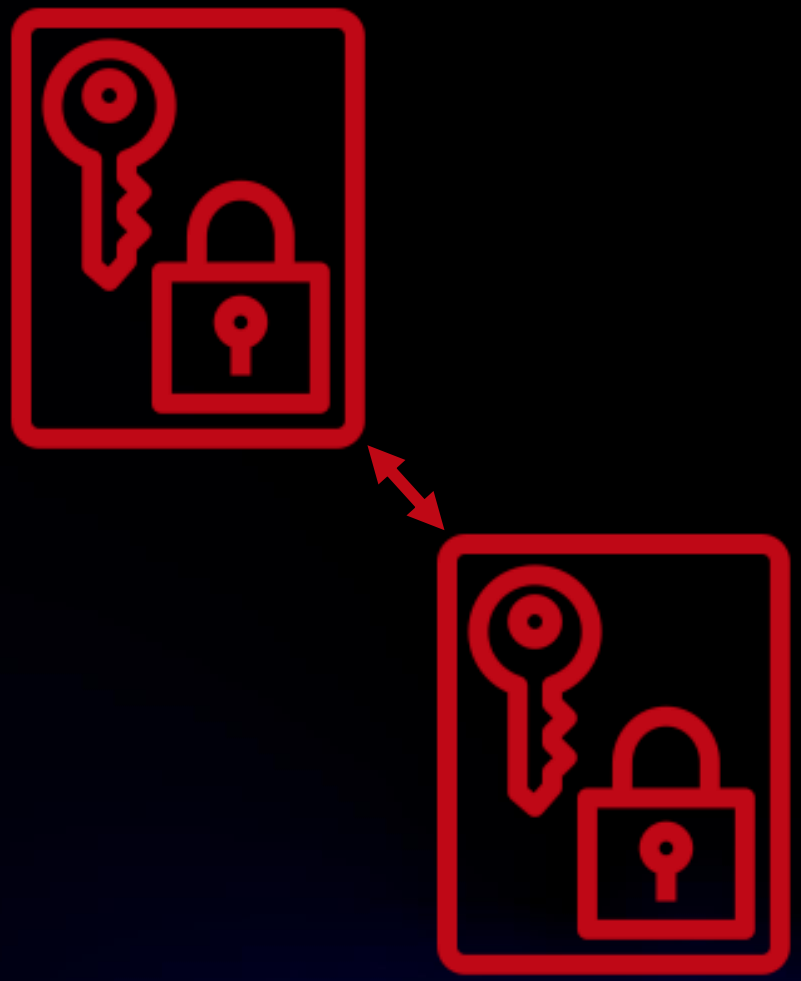
AWS Nitro



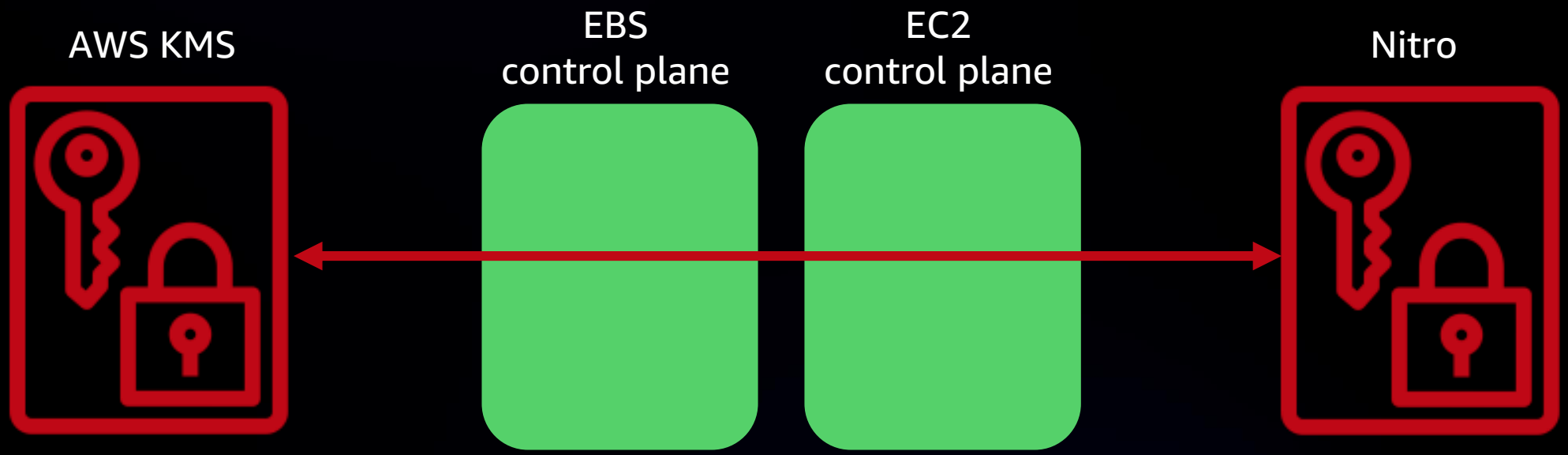
Using cryptography to minimize surface area

End-to-end encryption

- End-to-end encryption is used to secure data from the systems it needs to transit
- Example: envelope encrypting EBS keys within the EC2 system

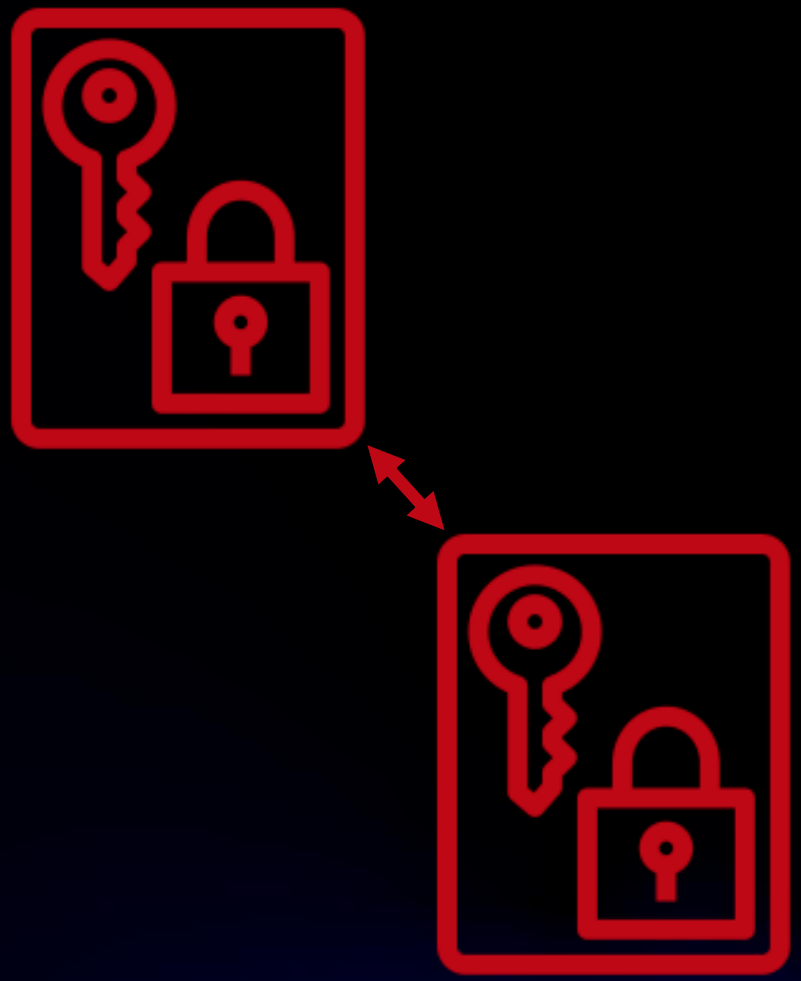


End-to-end encryption

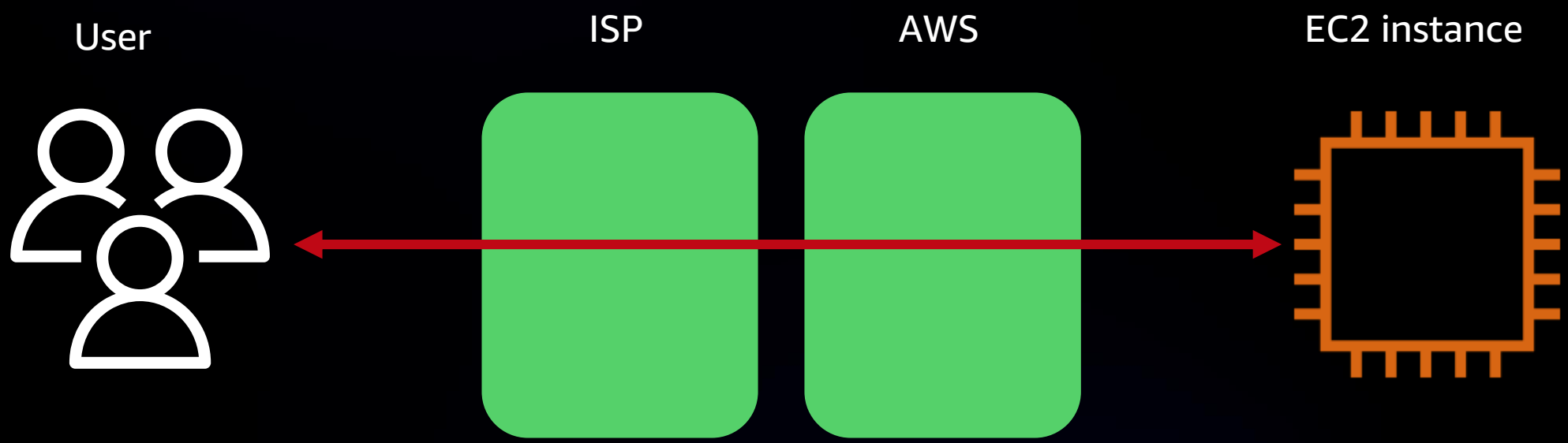


End-to-end encryption

- EC2 SSH keys use end-to-end encryption
- We have no copy of a customer's SSH private key
- Security is end-to-end between the SSH client and the EC2 instance

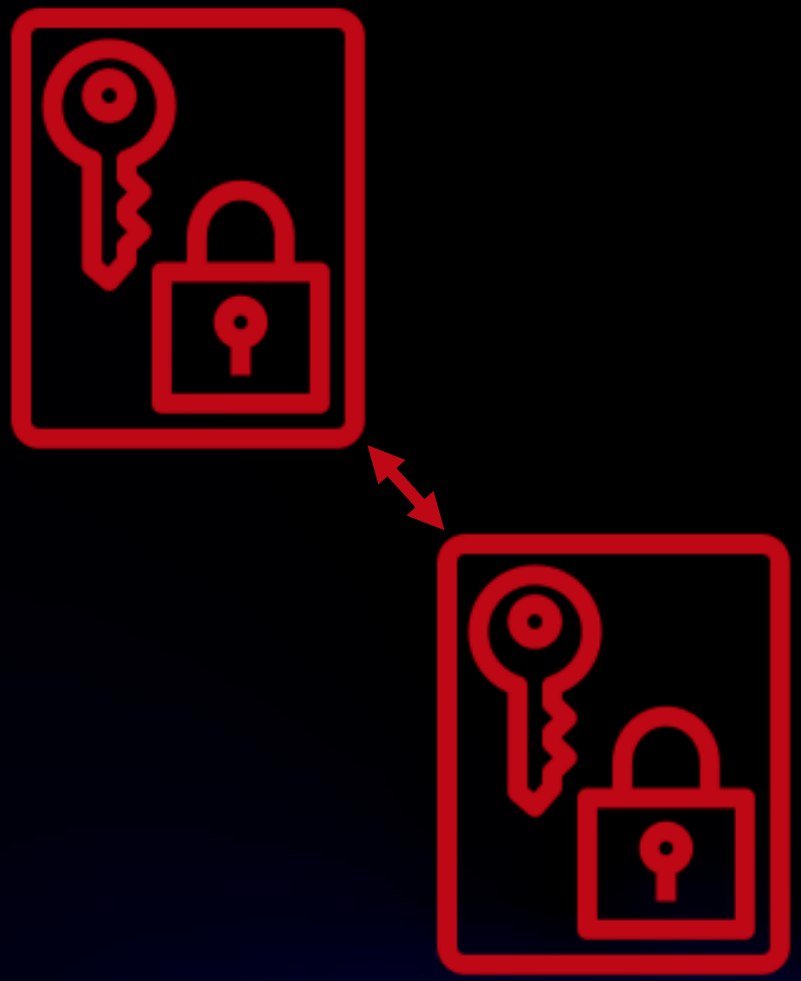


End-to-end encryption



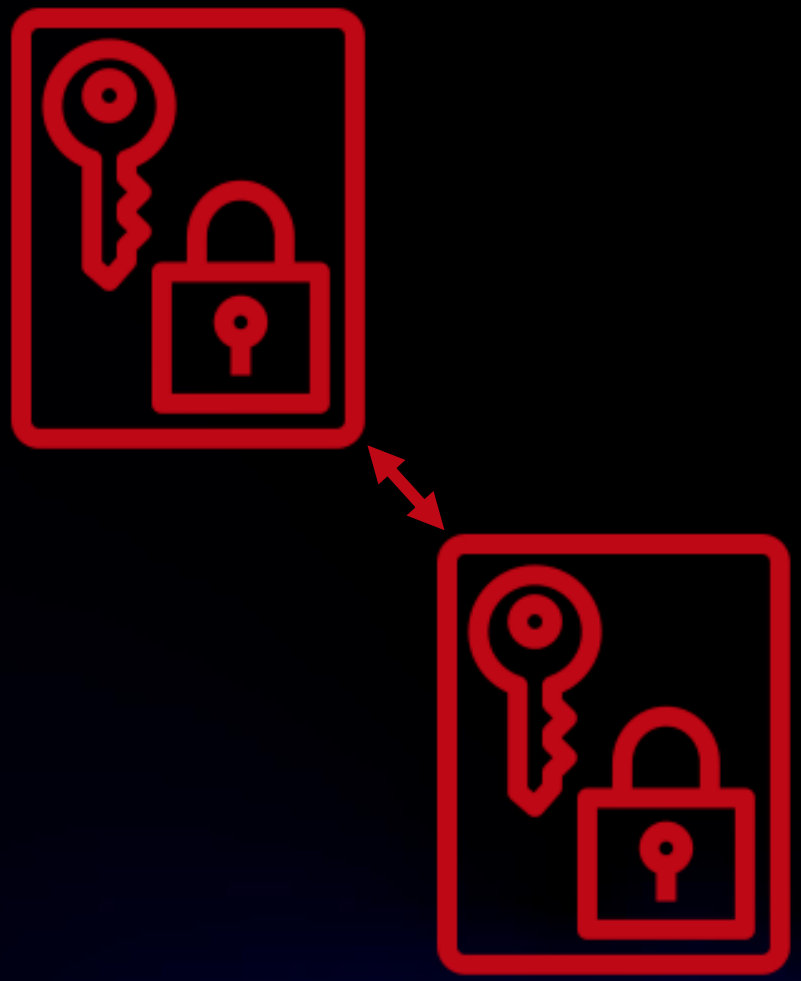
Client-side encryption

- General-purpose AWS Encryption SDK
- Service-specific Encryption SDKs available for Amazon S3 and Amazon DynamoDB
- AWS Nitro Enclaves encryption



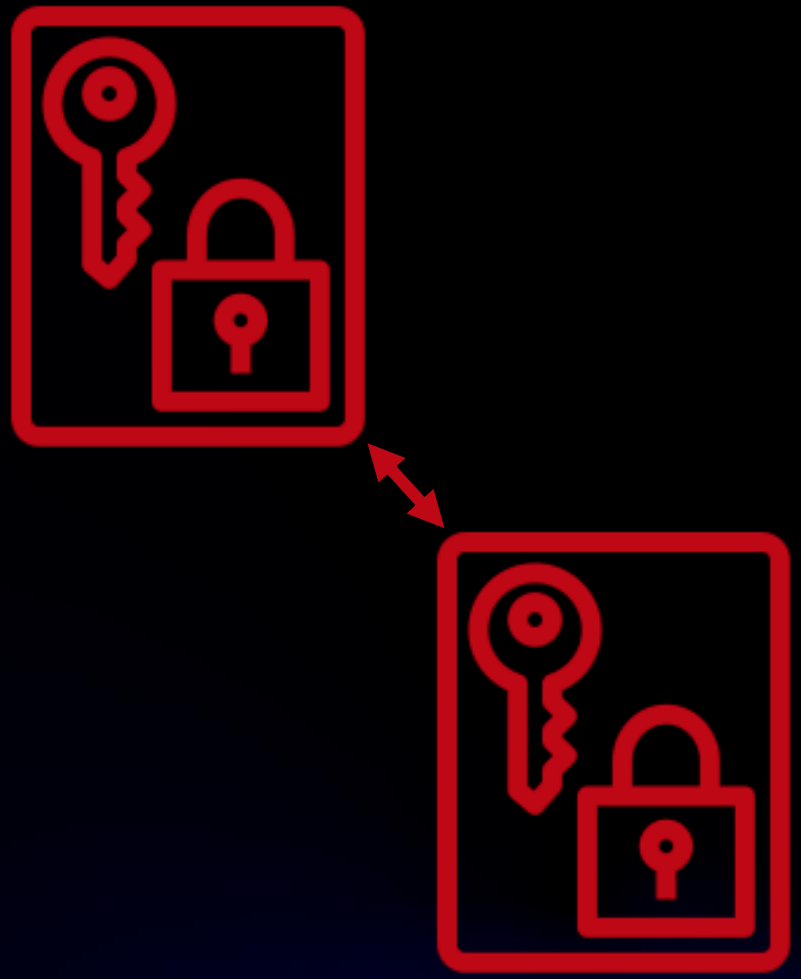
AWS Key Management Service (AWS KMS)

- Traditional downside of client-side encryption is key management
- AWS KMS is a multi-party system that is backed by tamper-evident hardware security modules
- AWS KMS system of grants enables rapid revocation



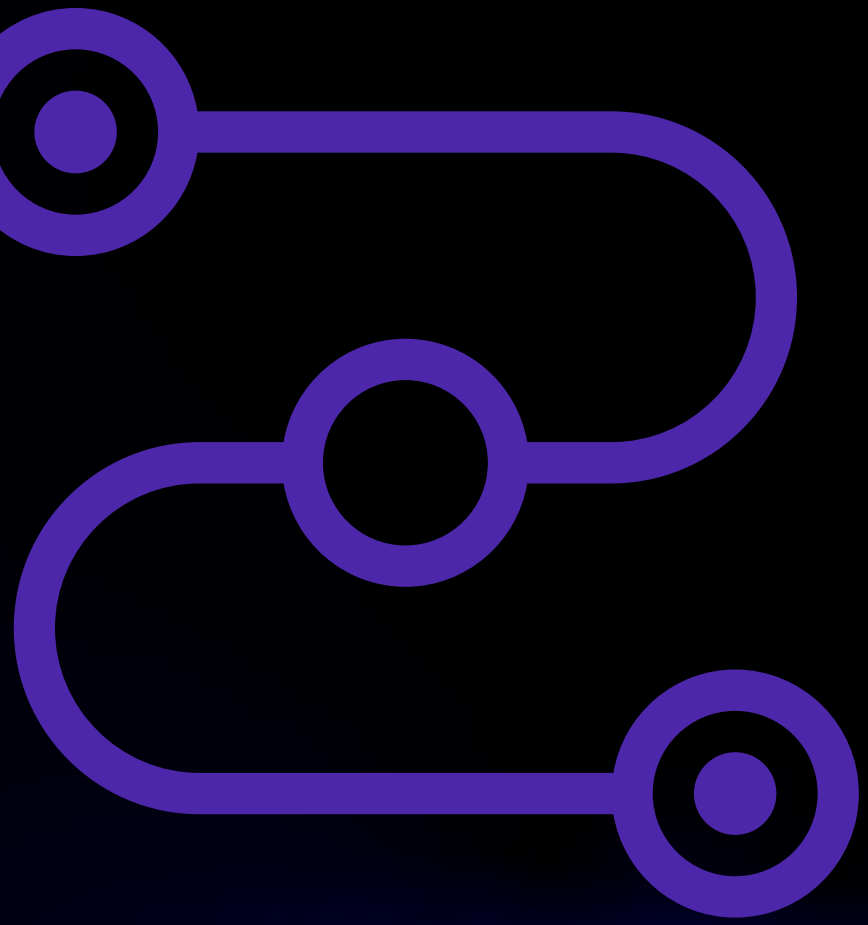
Client-side key retention

- Amazon S3 supports server-side encryption with customer-supplied keys
- AWS exposure to the key is temporary
- Enables crypto-shredding and other cases



Defense-in-depth encryption

- All network traffic on links out of AWS physical control is encrypted using AES256 or optical-layer encryption
- This includes all traffic between AWS data centers, buildings, and Regions
- This encryption is always on



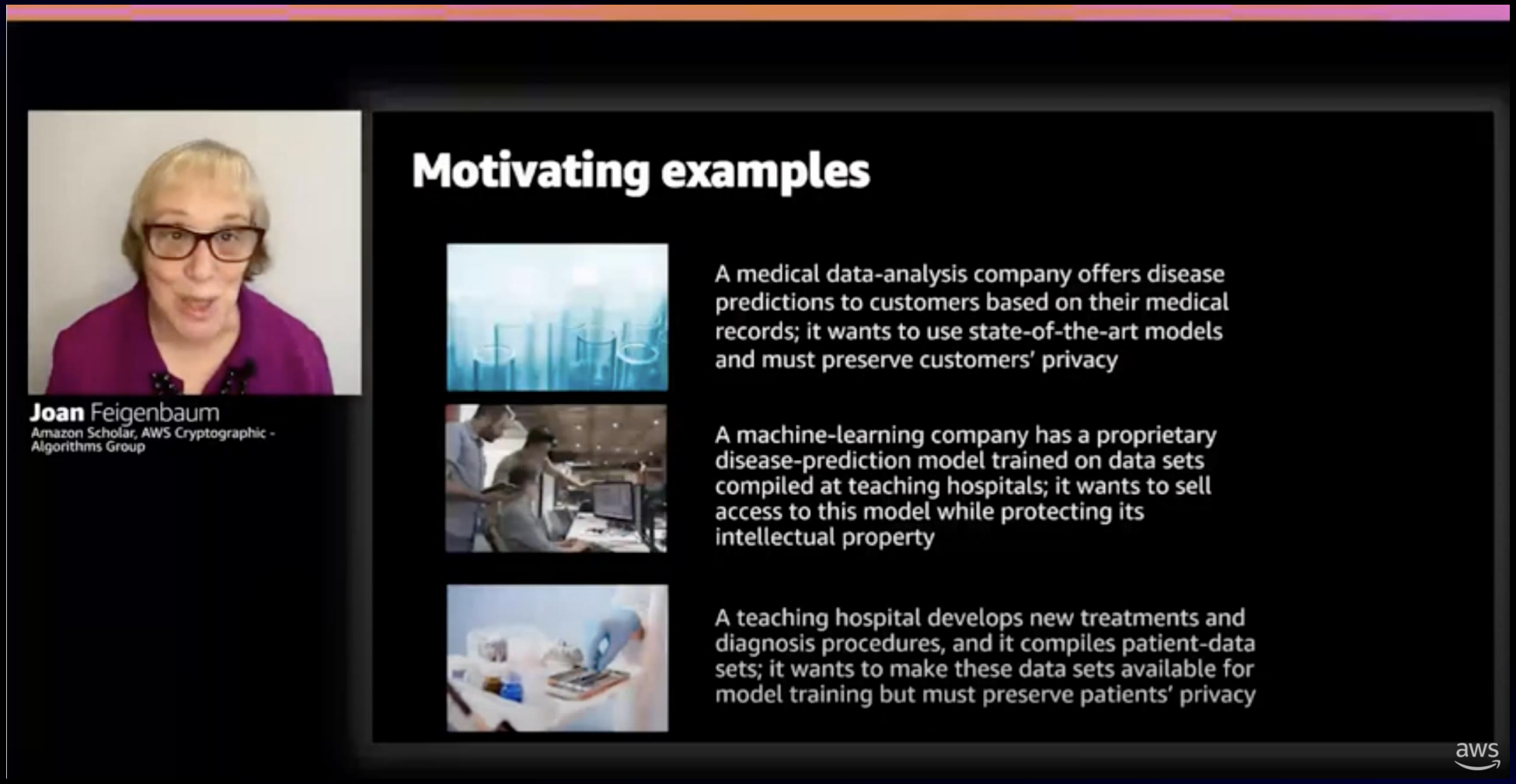
VPC encryption

VPC encryption provides always-on encryption between supported EC2 instance types

Works across VPC peering and between different AWS customers

VPC encrypted traffic is anonymized and privacy preserving

Privacy-preserving encryption



What about compute?

Homomorphic encryption

Cryptographic Computing

Enabling computation on cryptographically protected data

AWS Cryptography tools and services utilize a wide range of encryption and storage technologies that can help customers protect their data at rest and in transit. In some instances, customers also require protection of their data even while it is in use. To address this need, AWS is developing new techniques for cryptographic computing, an emerging technology that allows computations to be performed on encrypted data, so that sensitive data is never exposed. It is the foundation used to help protect the privacy and intellectual property of data owners, data users, and other parties involved in machine learning activities.

Our team of experts is innovating in Privacy Preserving Machine Learning with techniques such as Homomorphic Encryption and Secure Multi-Party Computation to help AWS and its customers meet their security and compliance goals, while allowing them to take advantage of the flexibility, scalability, performance and ease of use that AWS offers.

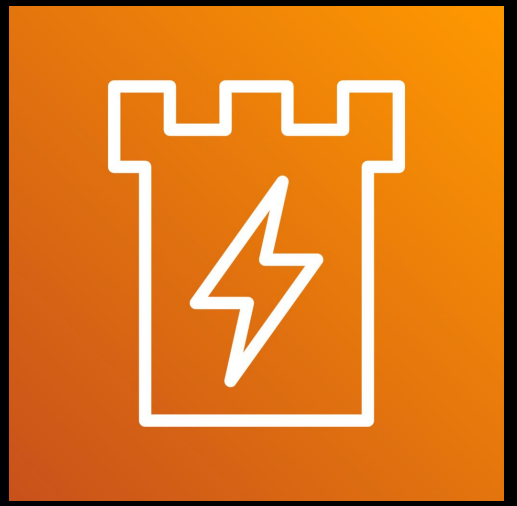
Privacy-Preserving Machine Learning

Shield material

AWS Identity and Access Management

Cryptography

AWS Nitro

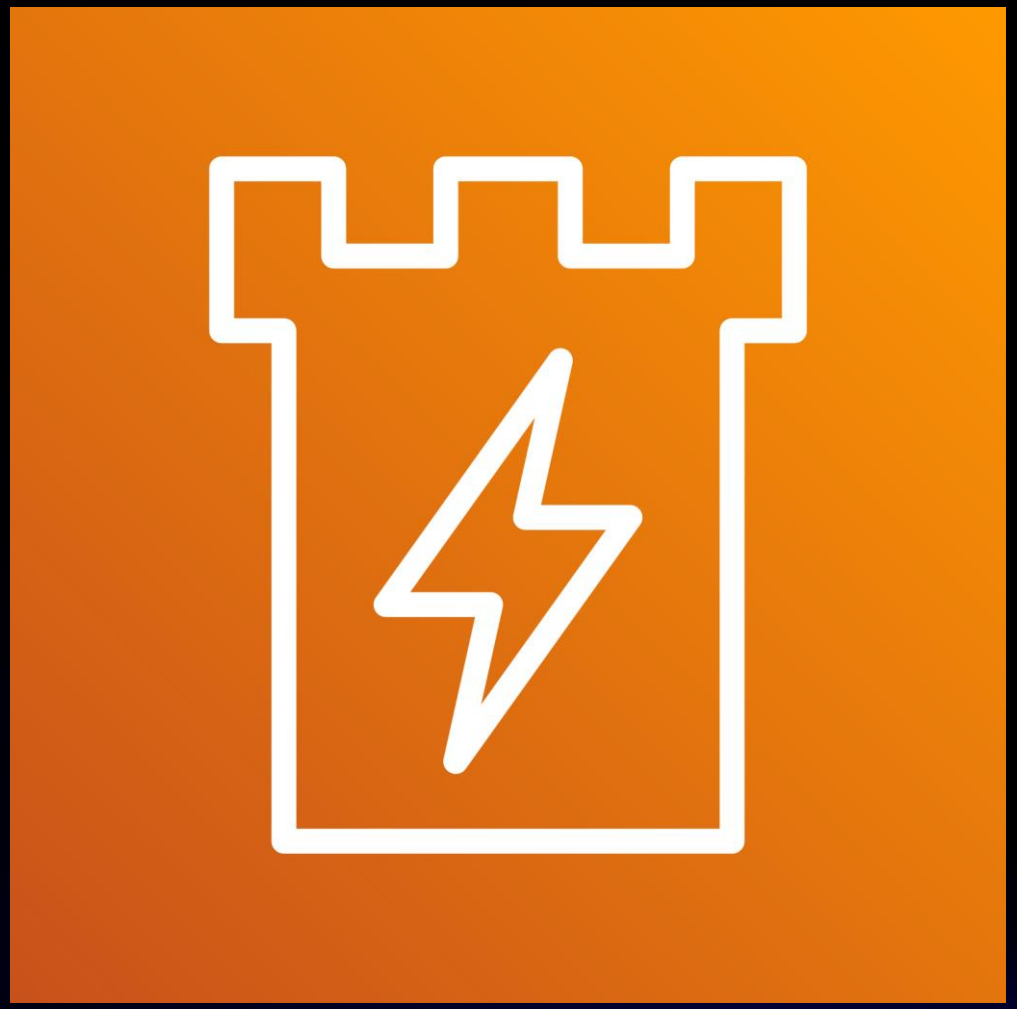


AWS Nitro System

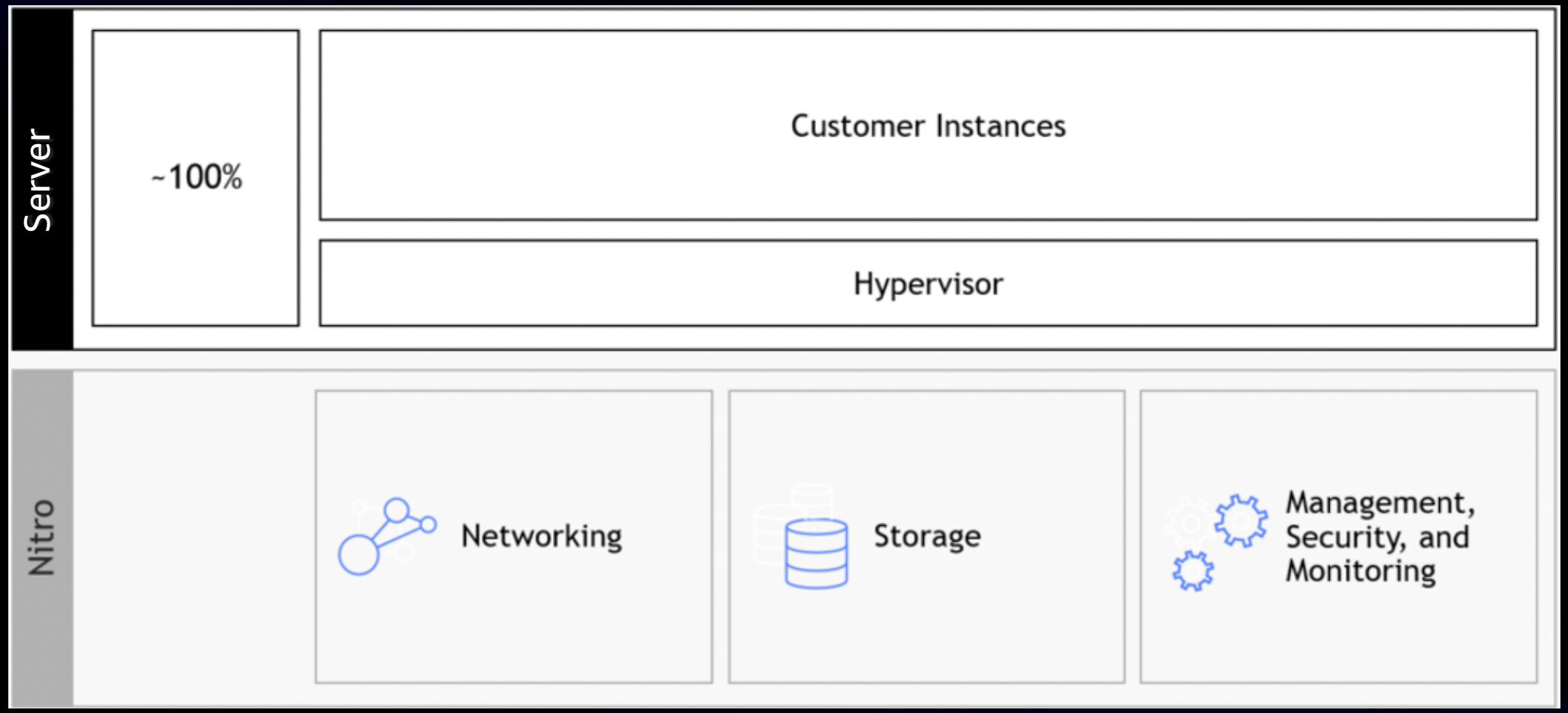
Designed from day one to provide strong isolation between AWS and the customer

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

Dedicated CPU, memory, and hardware security chip



AWS Nitro System

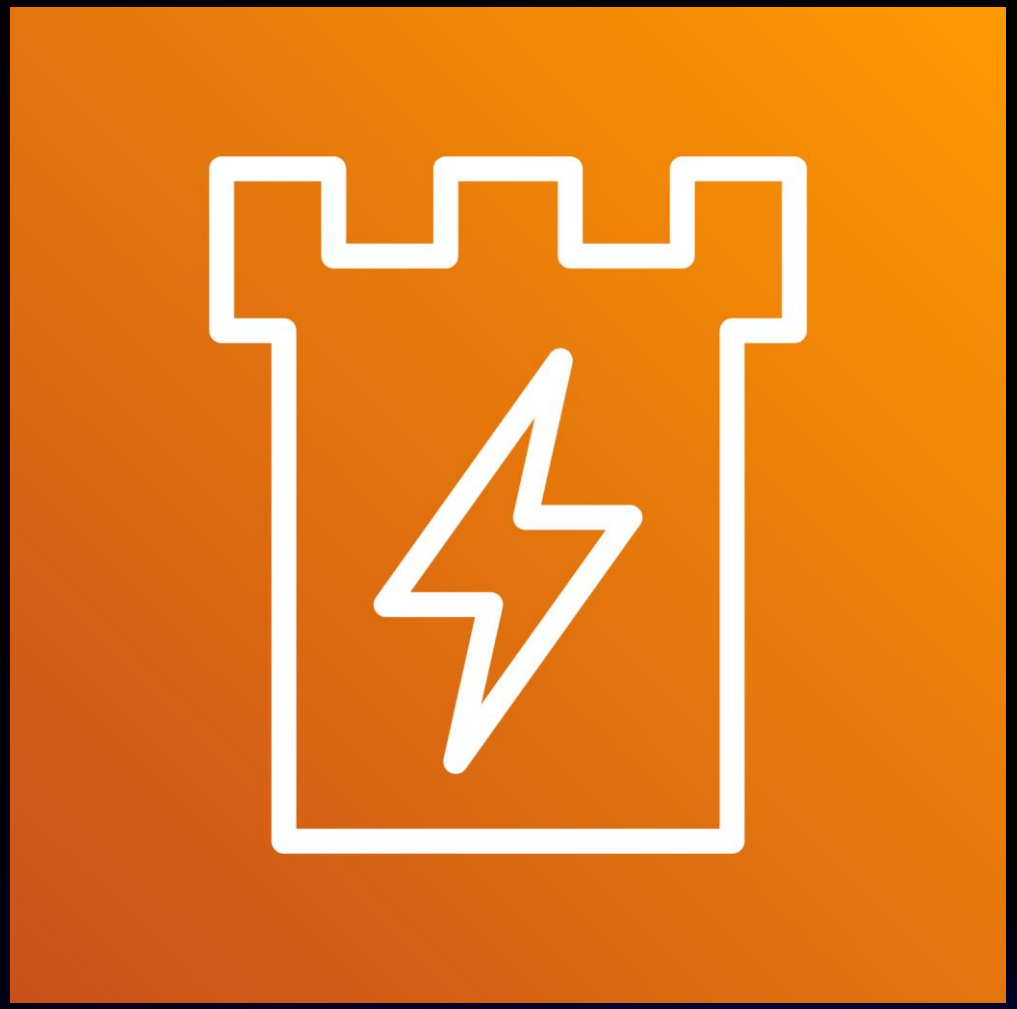


AWS Nitro System

There is no operational access to the AWS Nitro System

No SSH, no general-purpose access of any kind

All Nitro operations are done via secure, authenticated APIs and microservices



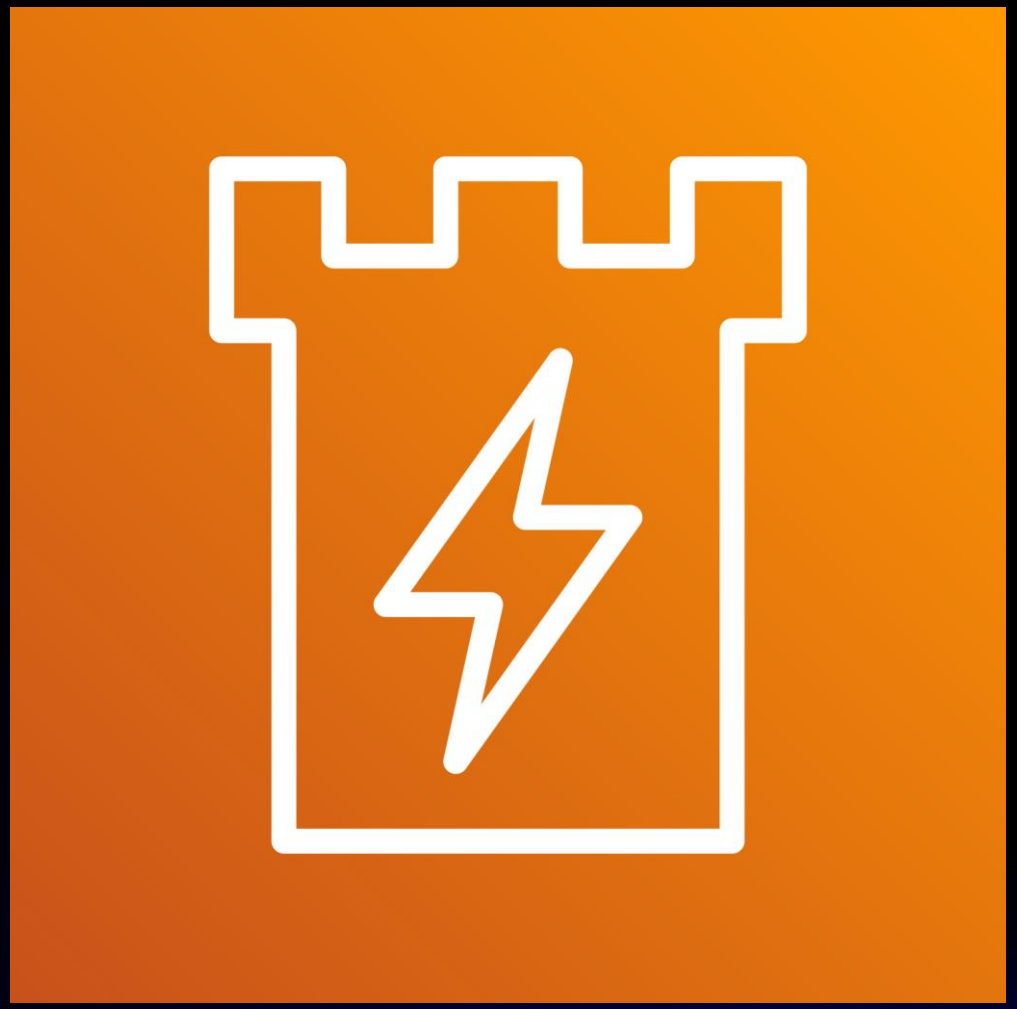
AWS Nitro System

Every build is signed and every operation is pre-vetted for safety

Nitro Systems run in an isolated network

Debugging features can’t disclose customer data

We’ve been extending this model to other systems

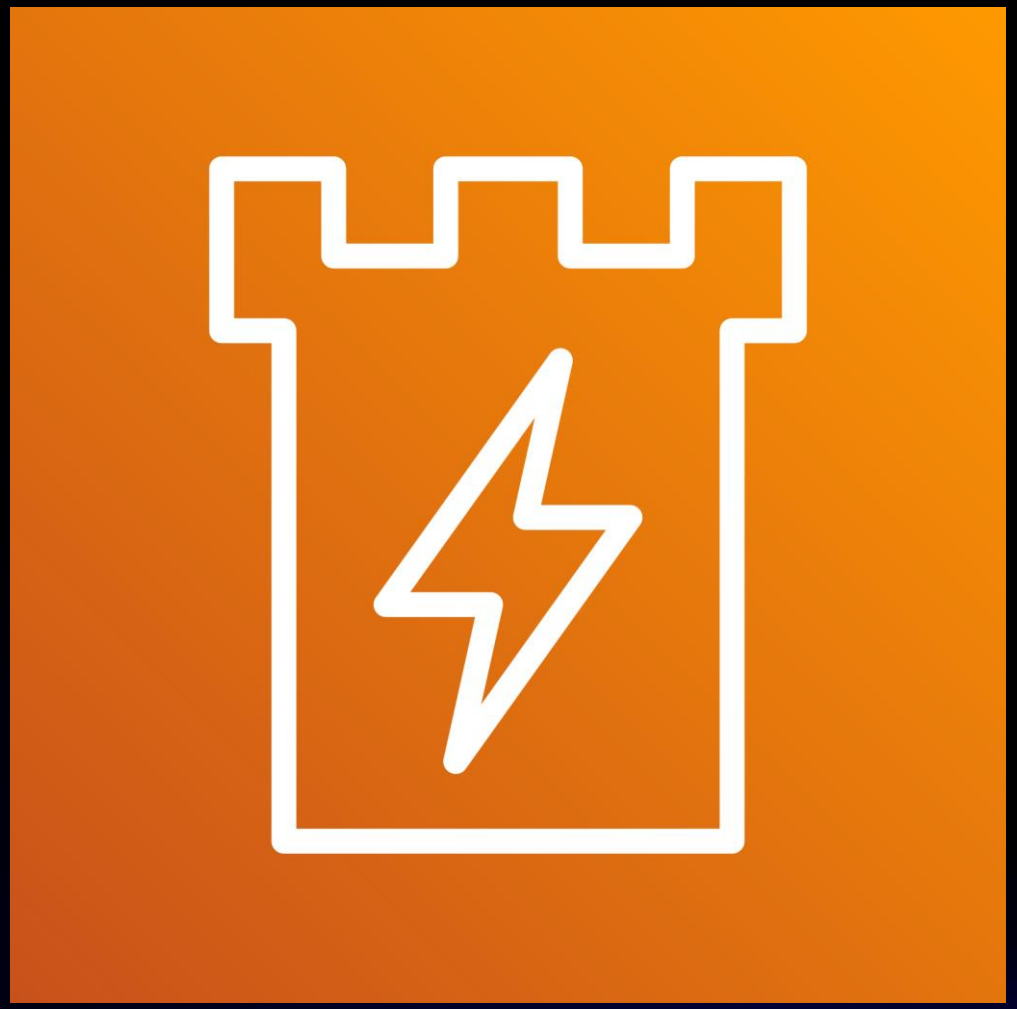


AWS Nitro System

With metal instances, customers get the dedicated hardware

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

Instances don’t share CPU cores or L1/L2 cache lines

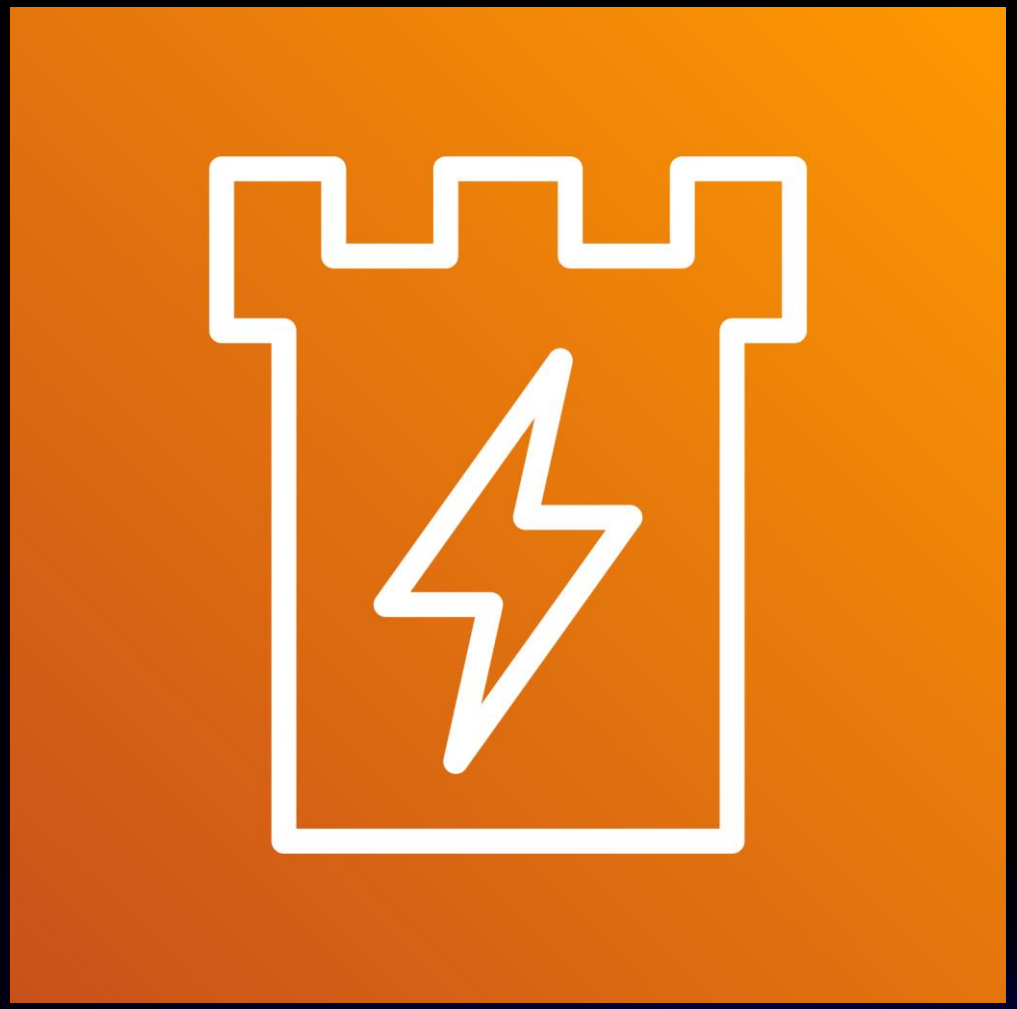


AWS Nitro System

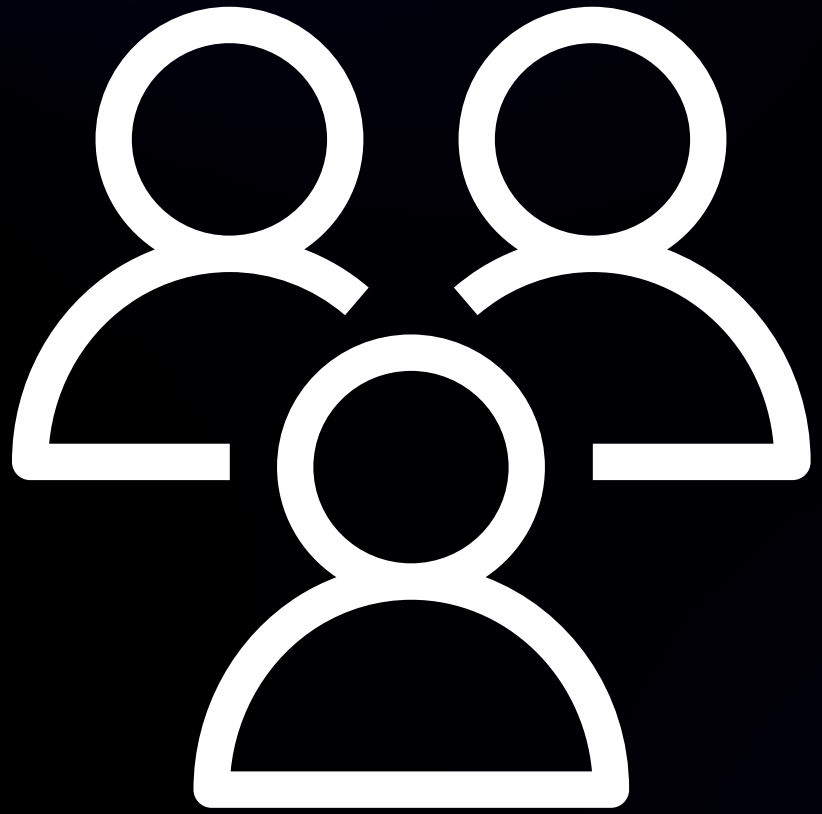
Nitro provides confidential computing based on hard isolation that complements encryption

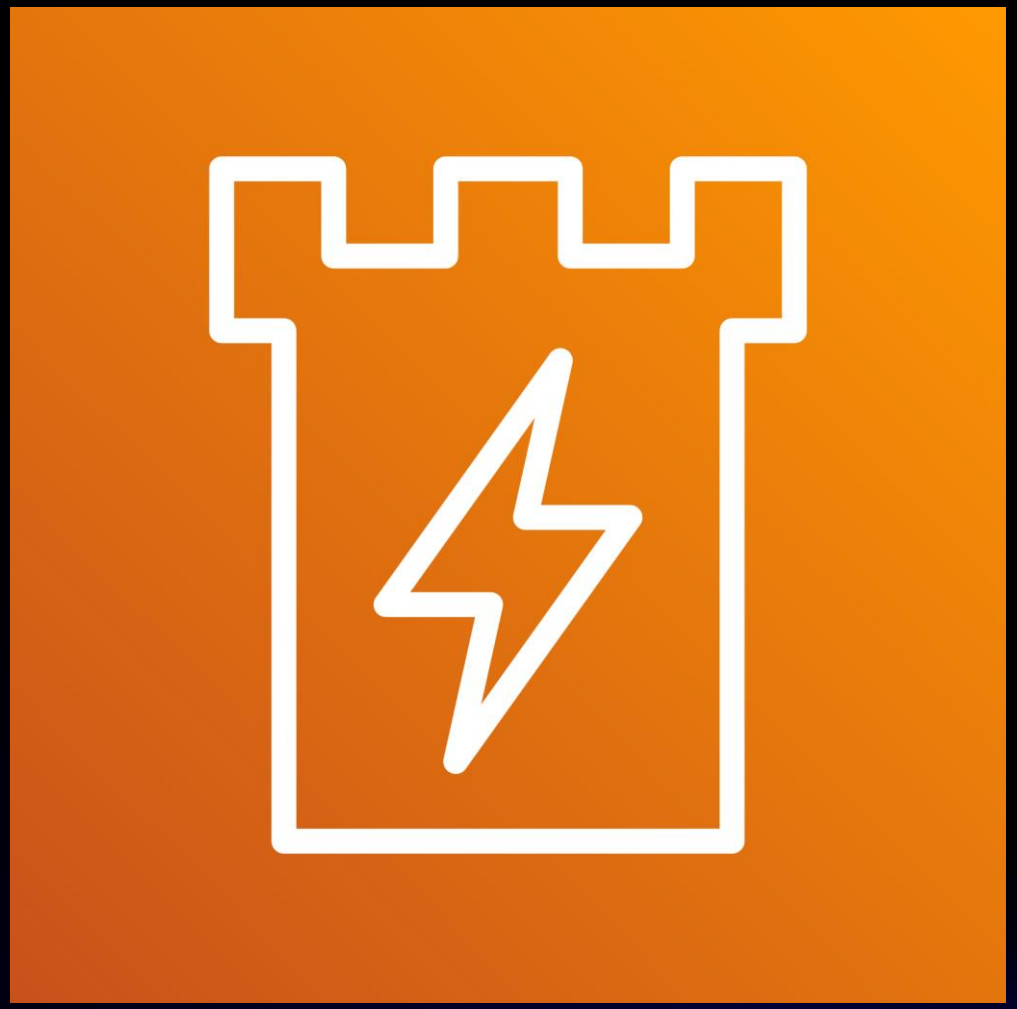
AWS Graviton2 includes memory encryption

Launch and run your application as normal, no modifications needed



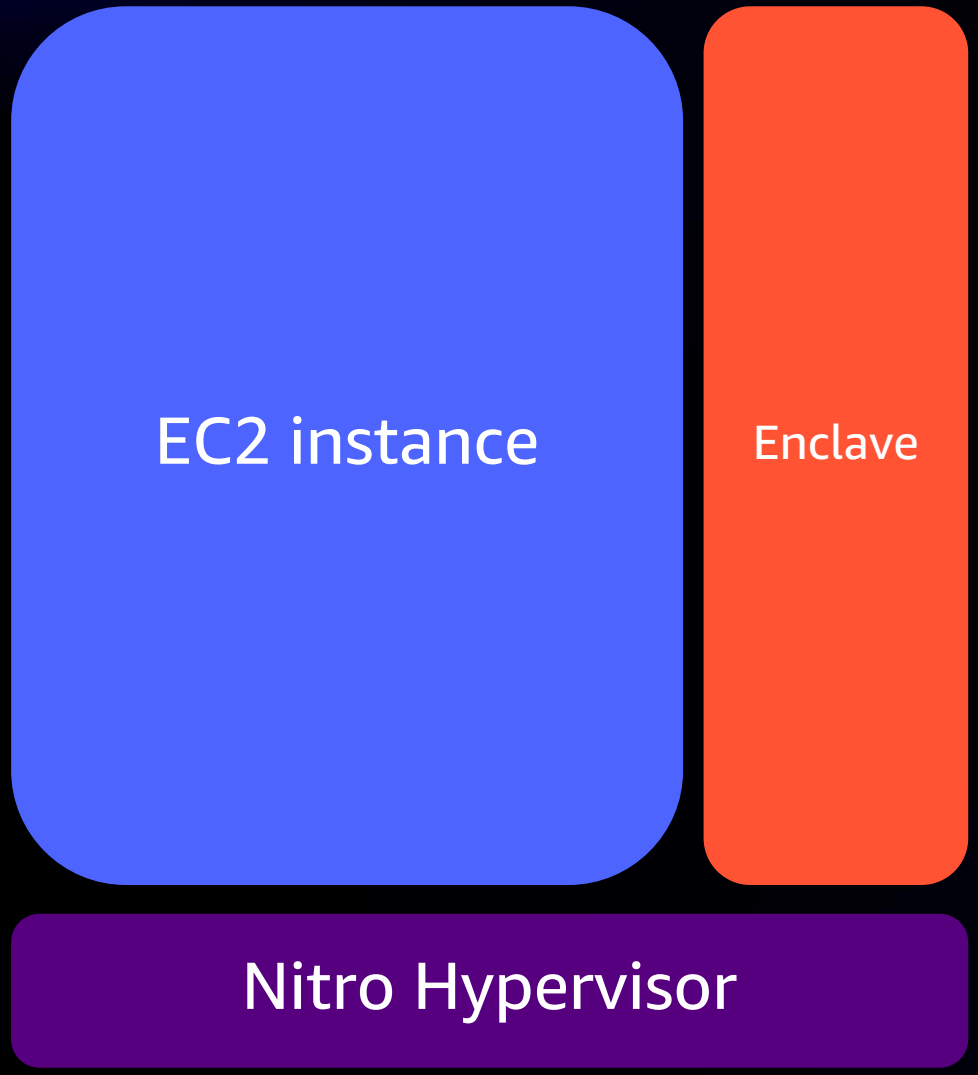
AWS Nitro Enclaves



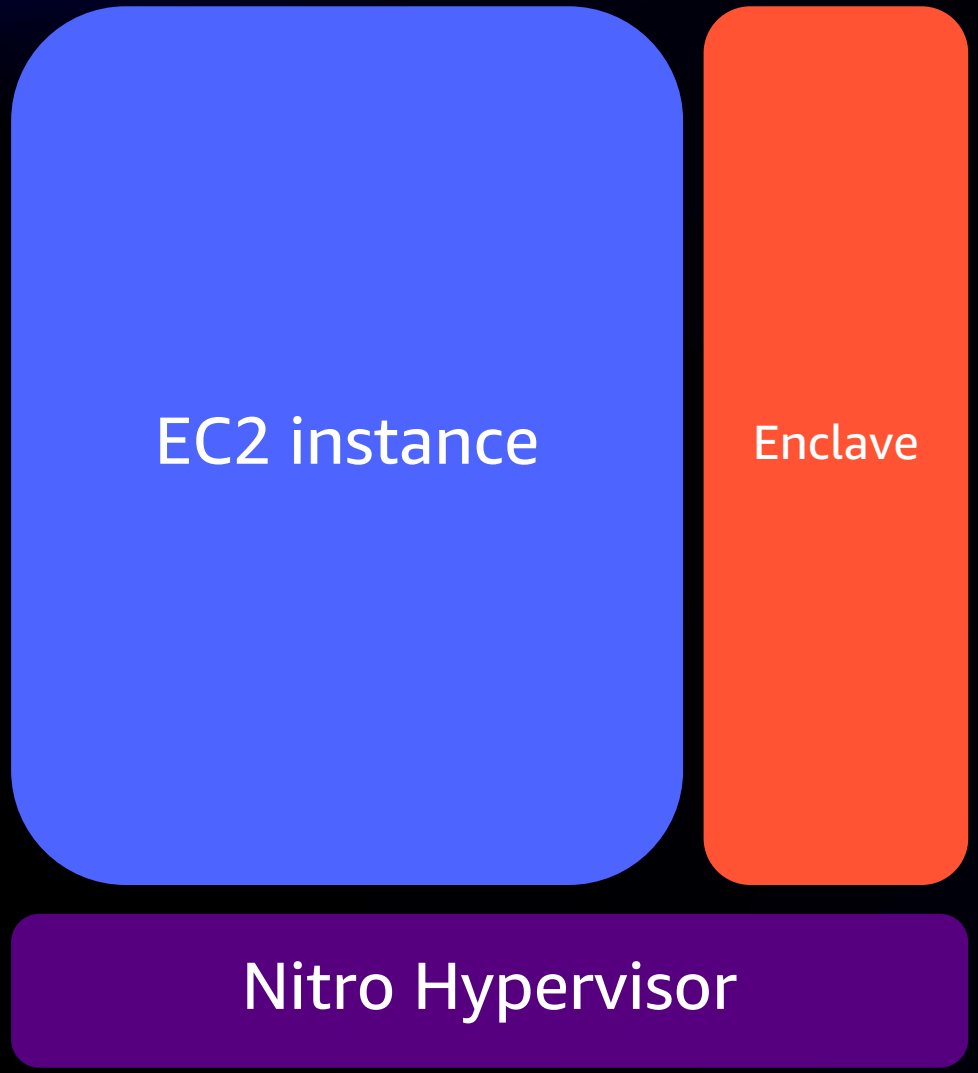


AWS Nitro Enclaves

AWS Nitro Enclaves

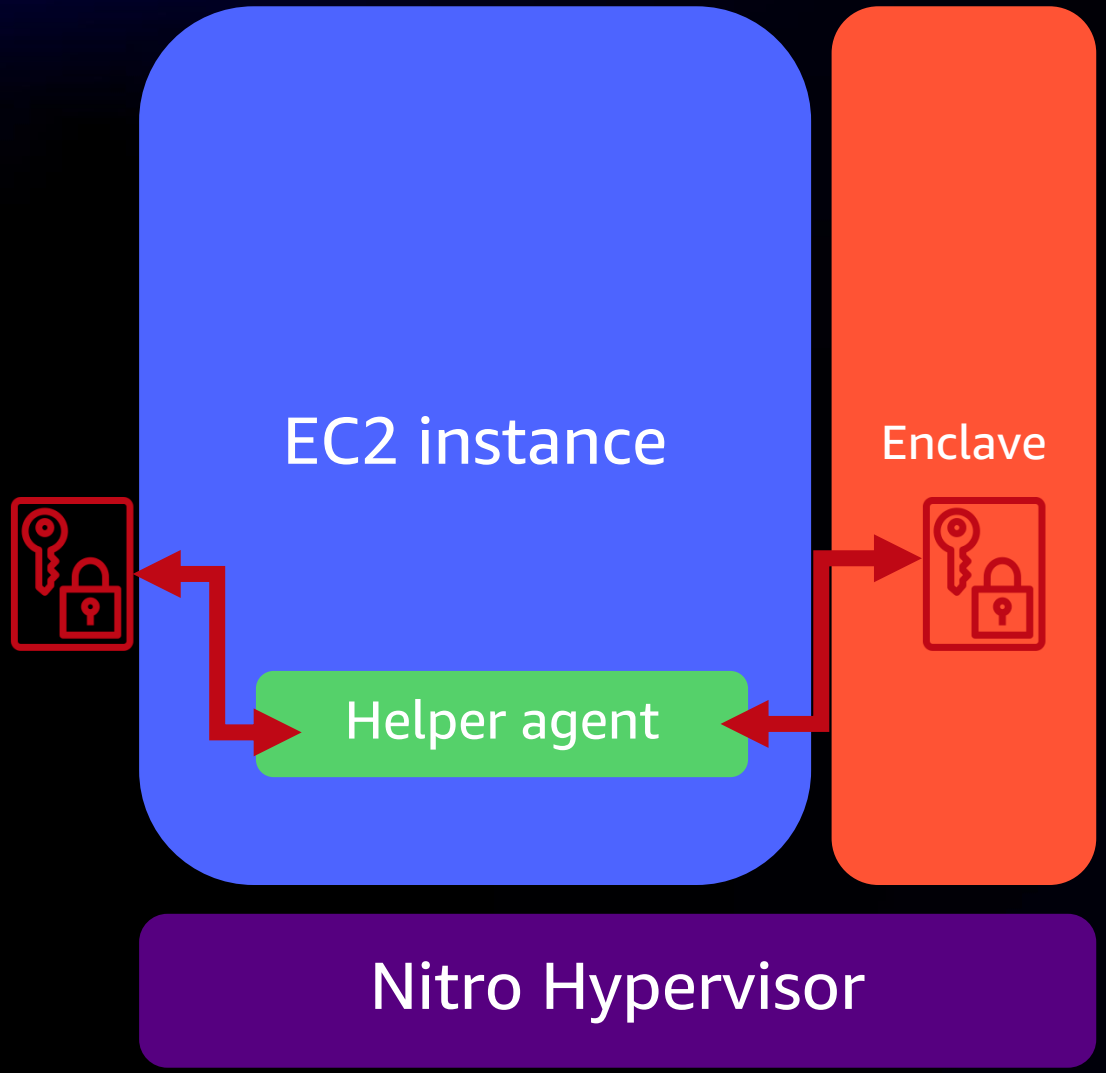


AWS Nitro Enclaves



- Nitro Enclaves are highly isolated
- No durable storage
- No network access
- No interactive access
- No metadata service, DNS, NTP

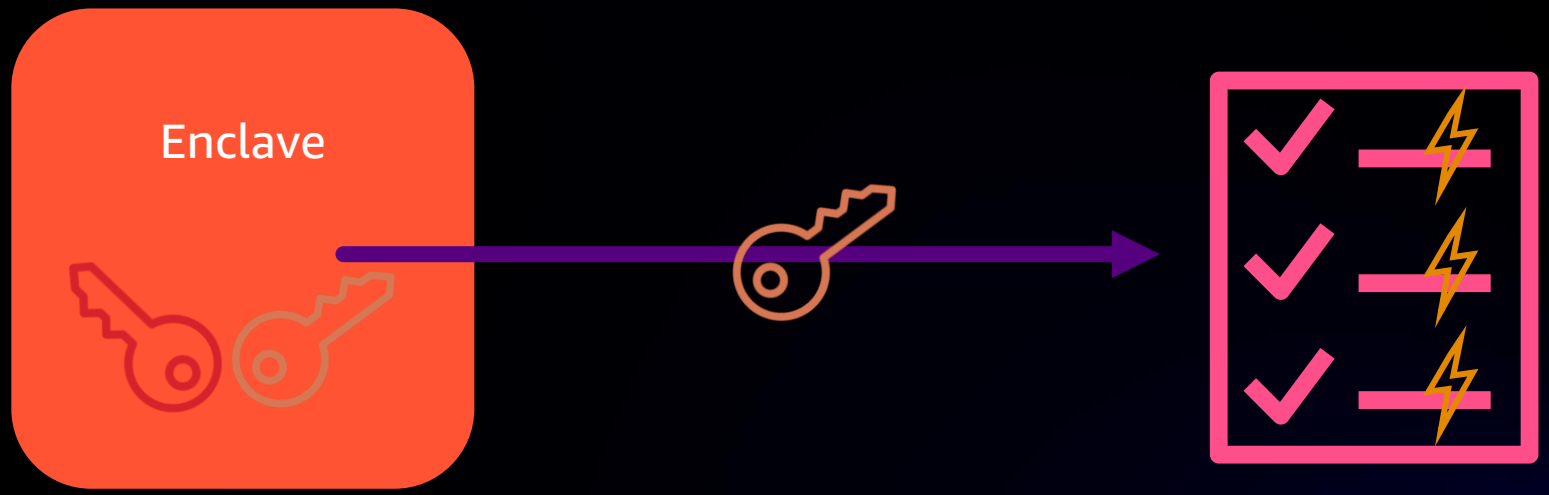
AWS Nitro Enclaves



- Helper agent forwards end-to-end encrypted communications between the enclave and select services
- Communications can be SSL/TLS or message-level encryption
- The agent has no visibility of the plaintext

AWS Nitro Enclaves attestation

- Enclave generates a local public-private key pair
- Enclave supplies the public key, and an optional nonce, to the Nitro attestation service

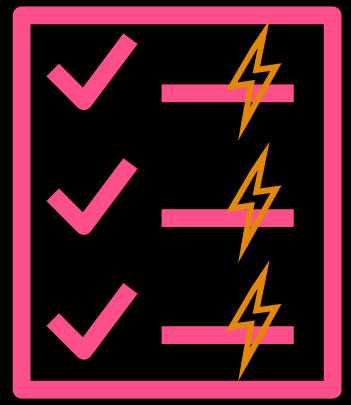


AWS Nitro Enclaves attestation

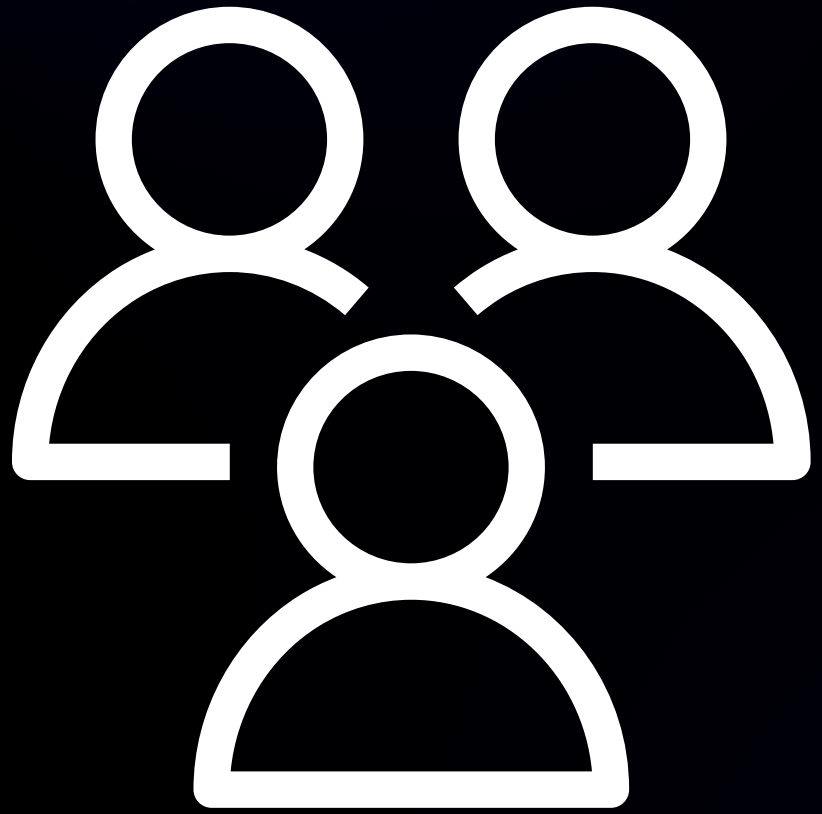
- Nitro attestation service produces an attestation document that covers:

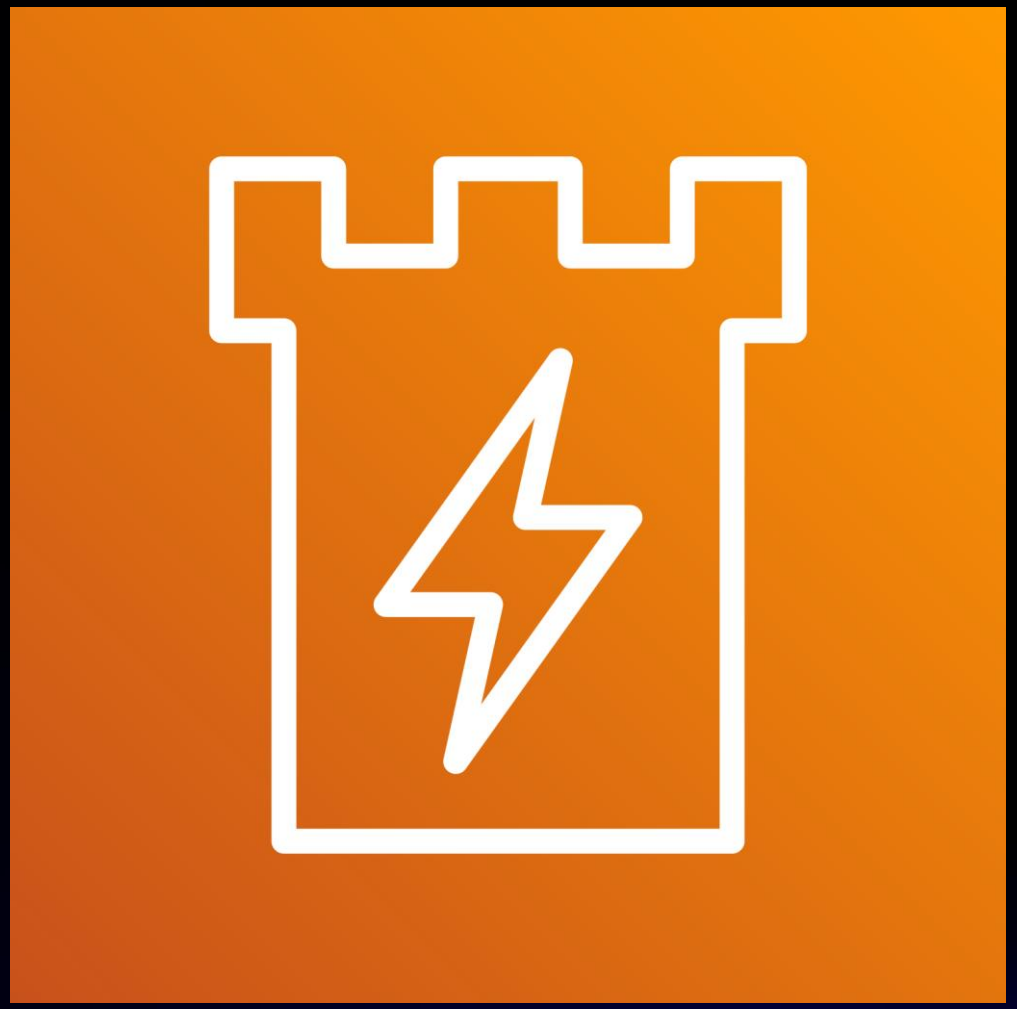
  Nonce, public key, enclave image checksum, kernel checksum, application checksum, enclave signing key, attached instance, instance role, launch time, current time

- Attestation document is signed by the AWS Nitro Attestation PKI



AWS Nitro Enclaves



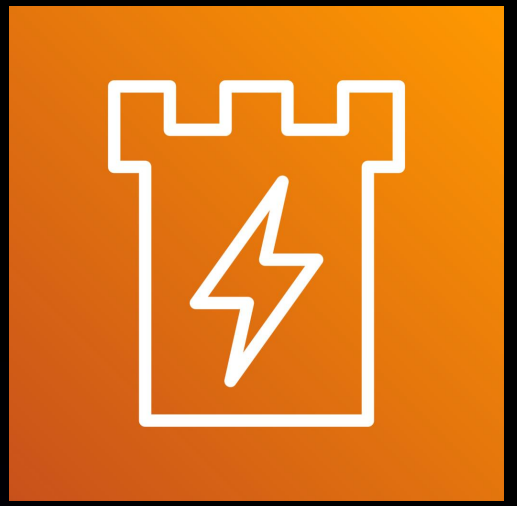


Shield material

AWS Identity and Access Management

Cryptography

AWS Nitro



Key takeaways

Key takeaways

- IAM provides strong permissions boundaries that are enforced even within and between AWS services
- The principle of least privilege can be very powerful
- Encryption can be a primary and a secondary security control

Key takeaways

- AWS can’t take away the keys
- AWS staff and operators have no access to systems such as Nitro and AWS KMS
- Customers can do the same for their own workloads with AWS Nitro Enclaves

Thank you!

Colm MacCárthaigh

@colmmacc