PUBLIC SECTOR SYMPOSIUM

BRUSSELS | MARCH 28, 2023

BAT302

Cryptographic and confidential computing on AWS

Andy Bunn
Security Specialist SA Manager
AWS World Wide Public Sector

Dusko Karaklajic
Security Specialist SA
AWS World Wide Public Sector

Agenda

Introduction

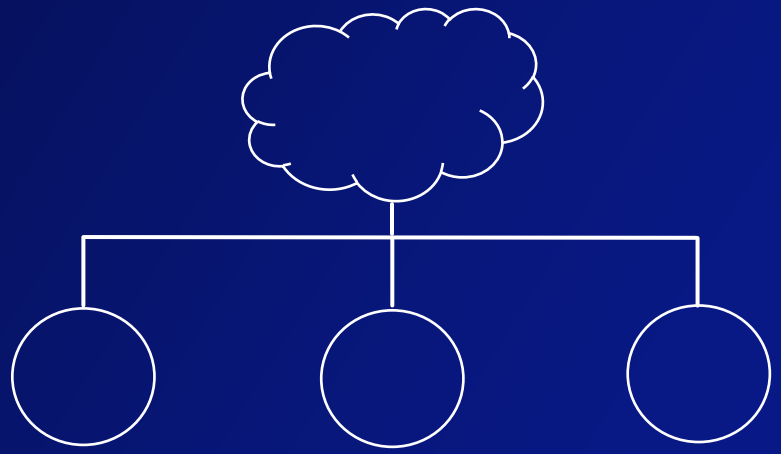
Cryptographic computing

Practical confidential computing on AWS

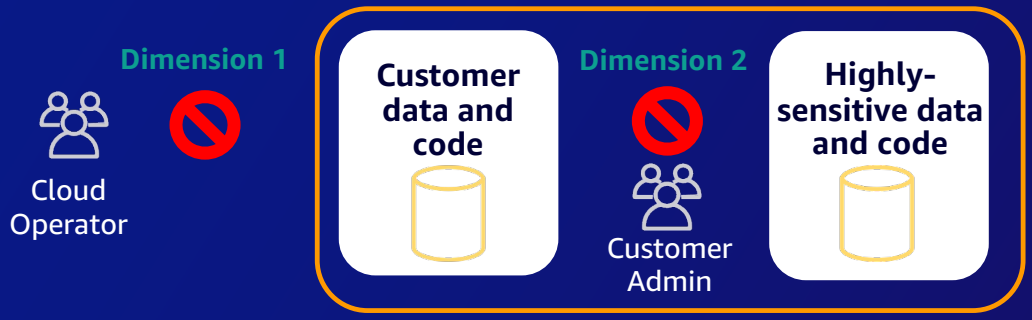
Use cases

Key takeaways

Why confidential computing?

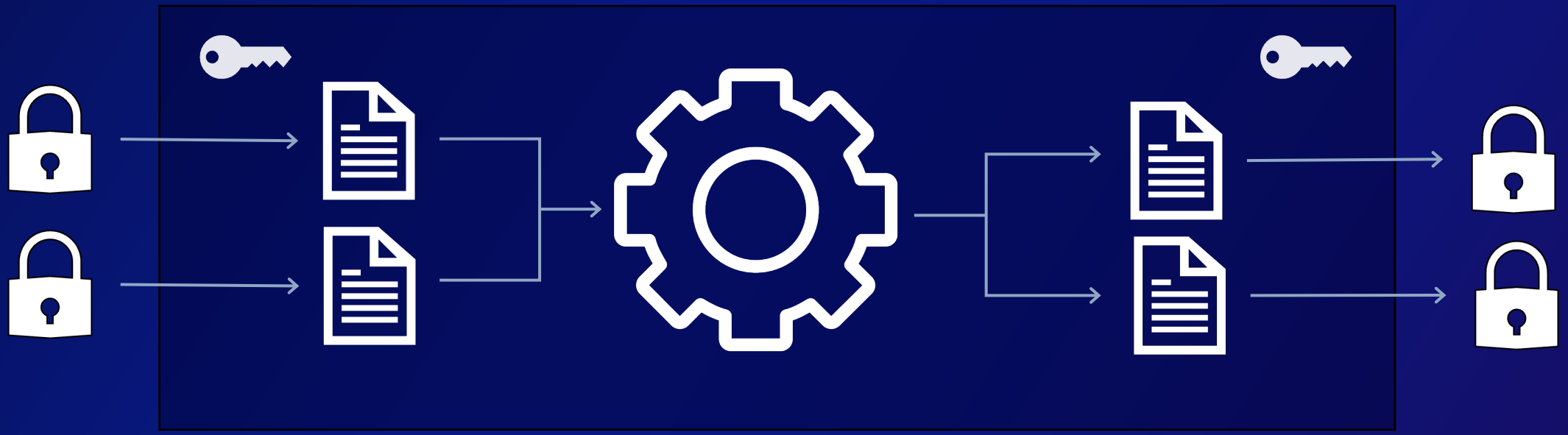


Collaborate

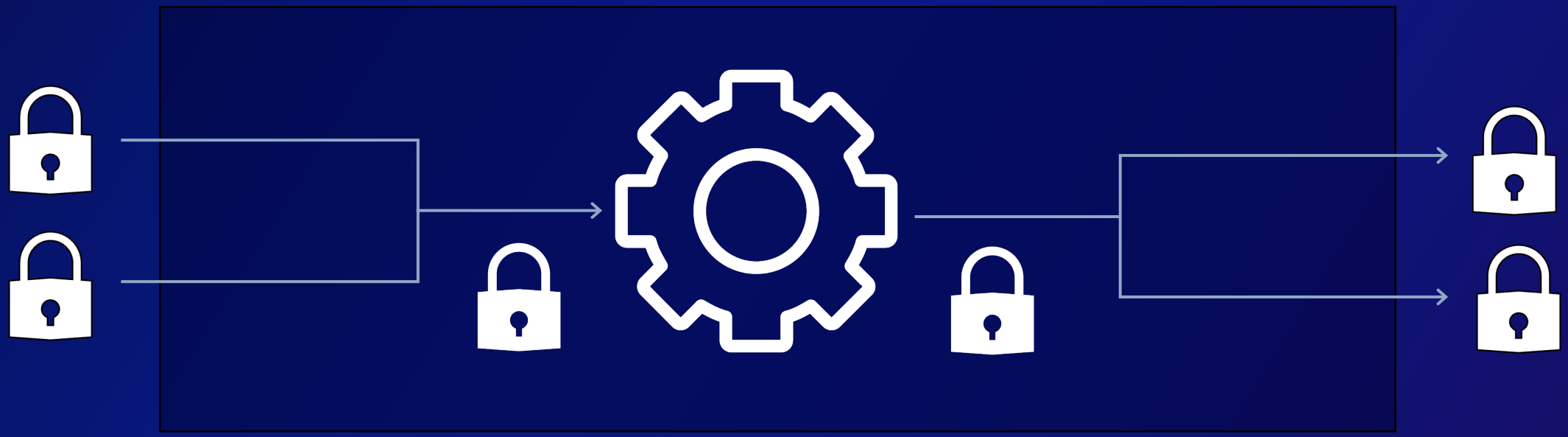


Securely

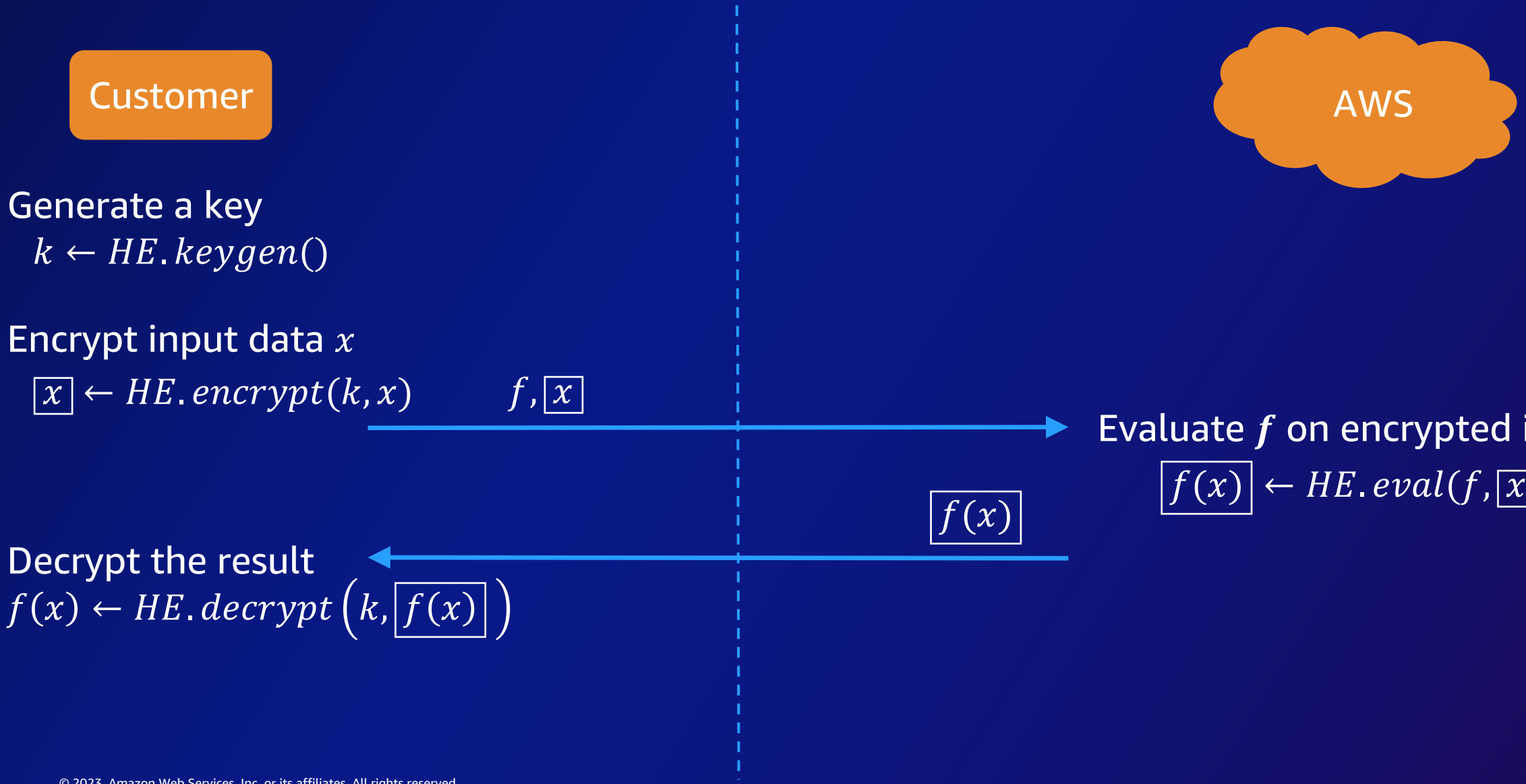
Traditional computing



Cryptographic computing

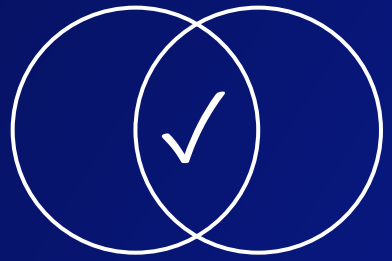


Vision: fully homomorphic encryption

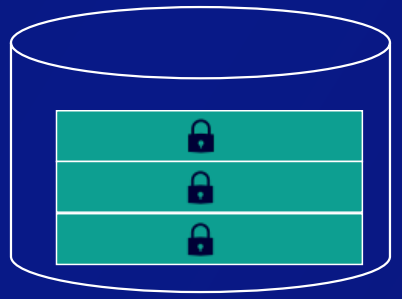


Practical use of cryptographic computing

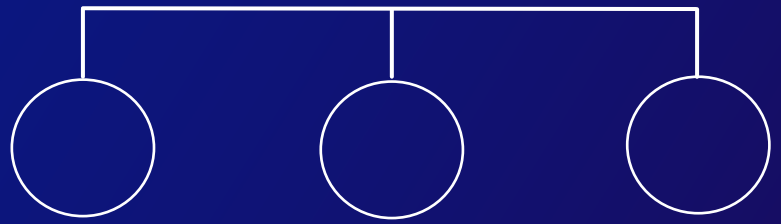
Private set intersection



Searchable encryption



Privacy-preserving federated learning



AWS Clean Rooms (Preview)

Create clean rooms in minutes. Collaborate with your partners without sharing raw data.

Create your own clean room, add participants, and start collaborating in a few clicks.

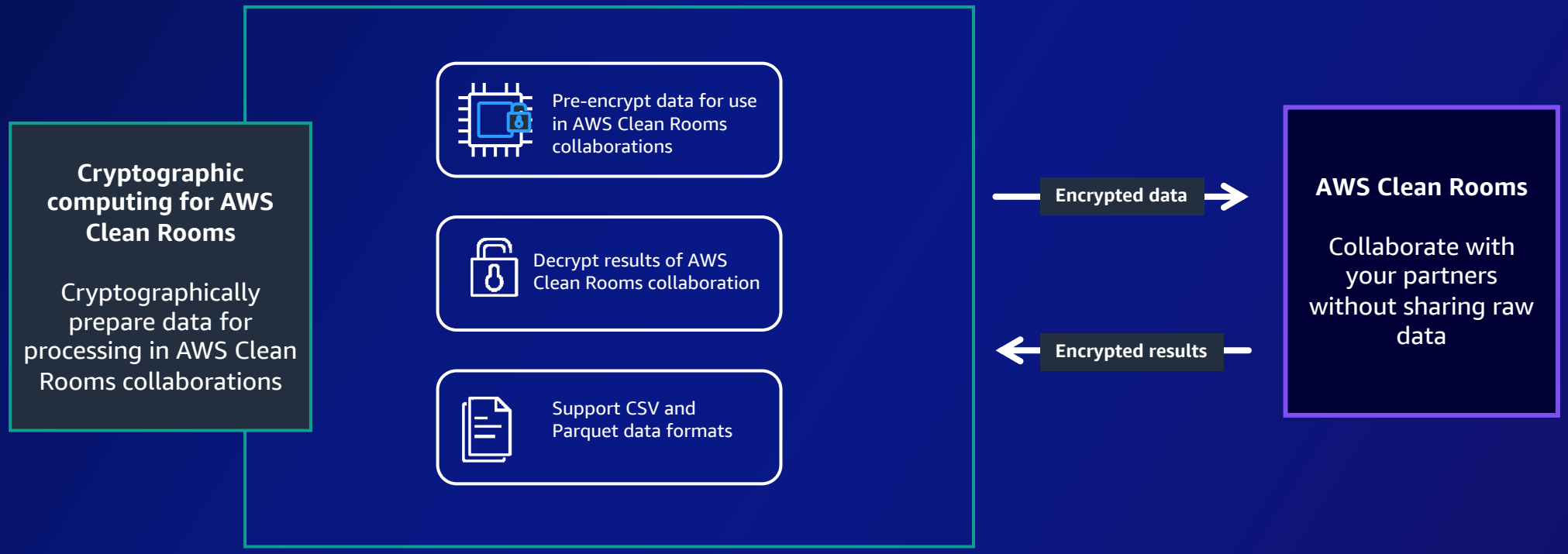
Collaborate with hundreds of thousands of companies on AWS without sharing or revealing underlying data

Protect underlying data with a broad set of privacy-enhancing controls for clean rooms

Use built-in, flexible analysis rules to tailor queries to your specific business needs

LEARN MORE	https://aws.amazon.com/clean-rooms

How it works: cryptographic computing in AWS Clean Rooms



Where to go for more...

Cryptographic Computing

Enabling computation on cryptographically protected data

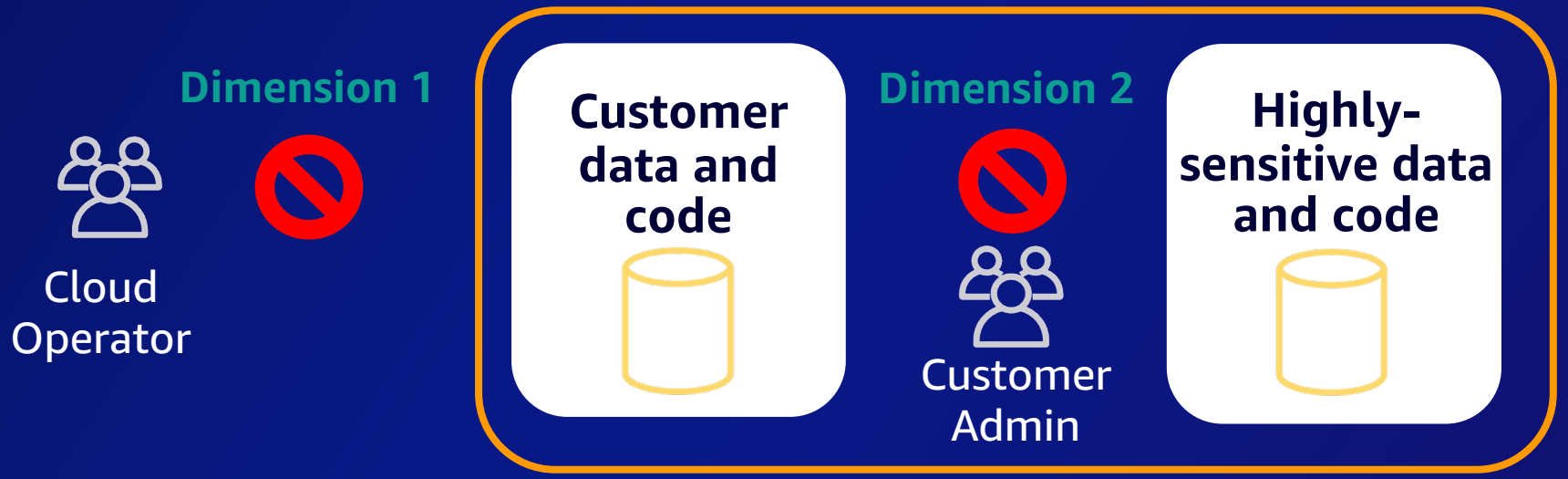
AWS Cryptography tools and services utilize a wide range of encryption and storage technologies that can help customers protect their data at rest and in transit. In some instances, customers also require protection of their data even while it is in use. To address this need, AWS is developing new techniques 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.

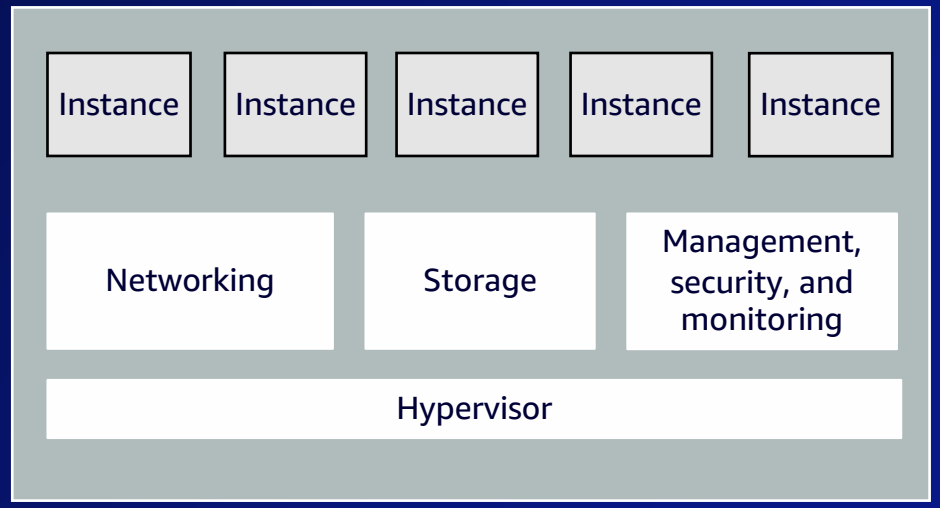
Privacy-Preserving Machine Learning

Practical confidential computing AWS Nitro System

What are we trying to protect?

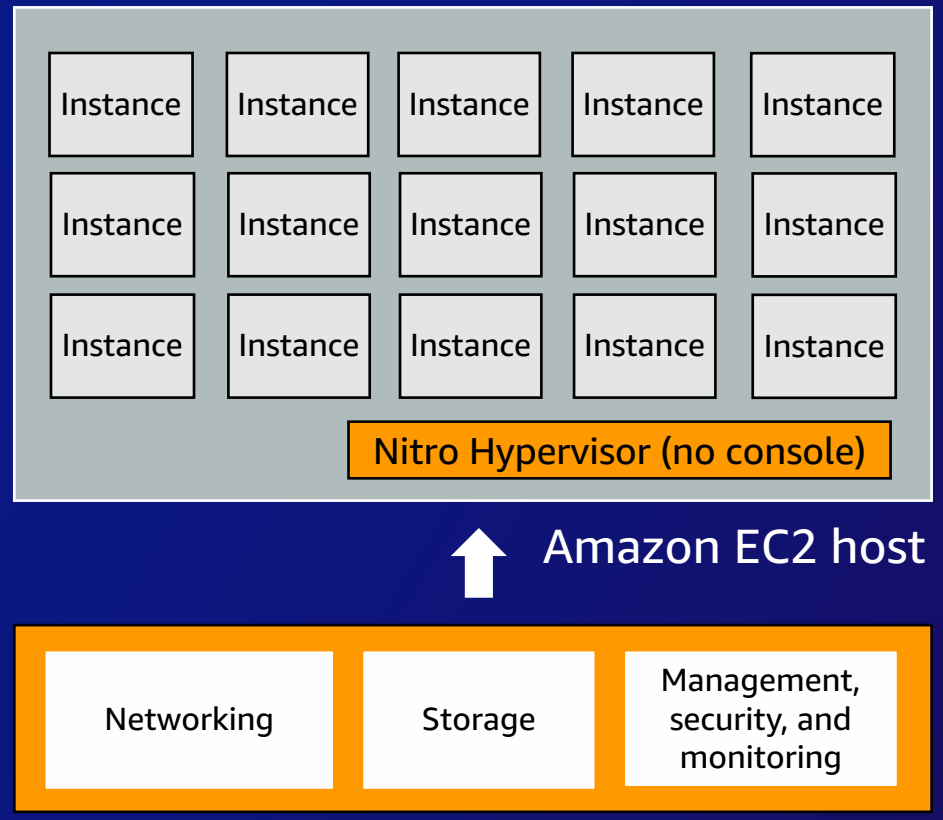


AWS Nitro System: reinventing virtualization for the cloud



Host

Classical virtualization



Amazon EC2 host

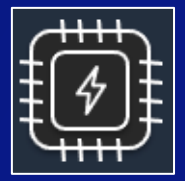
AWS Nitro System

AWS Nitro System: components

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

AWS Nitro System: confidential computing

The Security Overview of the AWS Nitro System whitepaper

- Detailed review of the security design the three primary components of the AWS Nitro System:
  - Nitro Cards
  - Nitro Security Chip
  - Nitro Hypervisor

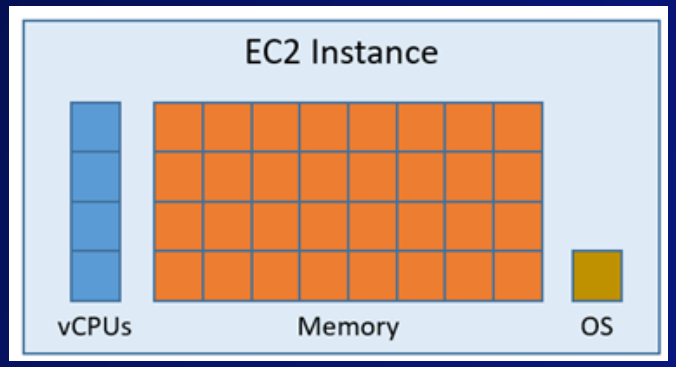
- Deep dive on the AWS Nitro System integrity protections, tenant isolation model, and no operator access design

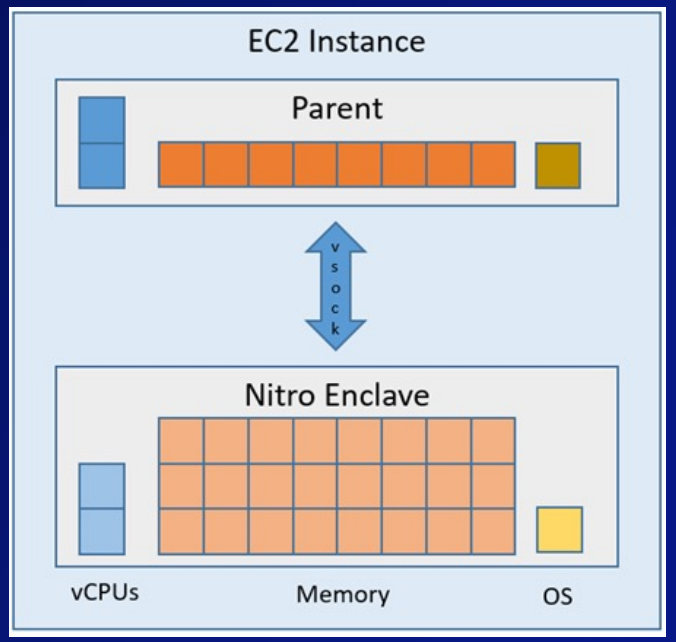
https://a.co/hYWhsH9

Confidential computing from the cloud perspective: Nitro

AWS Nitro Enclave

What is a Nitro enclave?

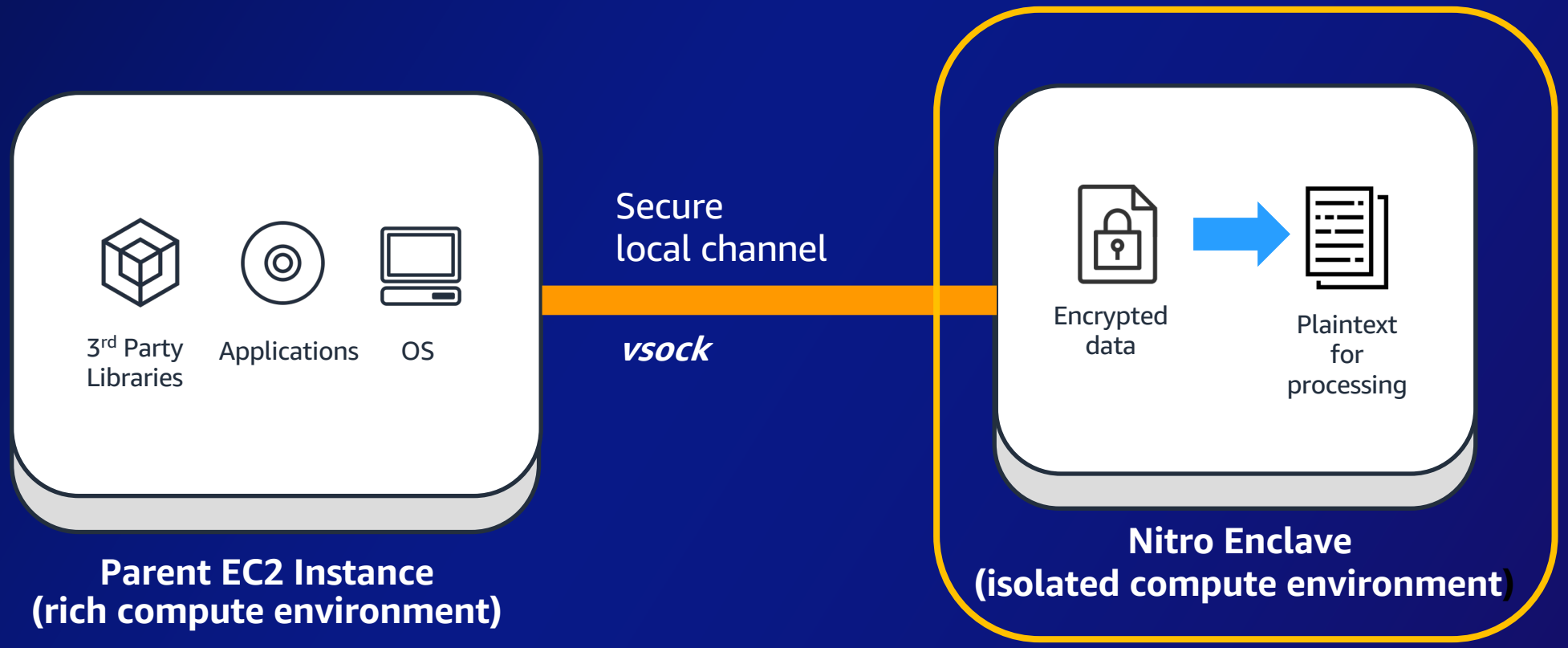




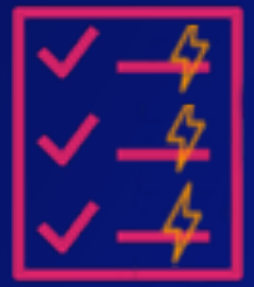
- Highly isolated
- No durable storage
- No network access
- No interactive access

https://aws.amazon.com/blogs/aws/aws-nitro-enclaves-isolated-ec2-environments-to-process-confidential-data/

Isolated compute environment



Enclaves can produce attestation documents that are signed by the Nitro Hypervisor



Signed Attestation Document

Signed Attestation Document contains:

- Enclave Public Key
- Hash of the Enclave Image
- Platform Configuration Registers (PCR)
  - Example : kernel, bootstrap process, application, instance ID, IAM roles
- Other user-defined information
  - Nonce

Example – with Encrypted S3 data and AWS KMS

Data Owner

Set up – client-side encryption with S3

1. Create a new symmetric customer managed KMS Key
2. Generate a data key from the customer managed KMS Key
3. Use the data key to encrypt the highly sensitive data

4. Upload the encrypted data and encrypted data key to S3 bucket

Example – with Encrypted S3 data and AWS KMS

Data Owner

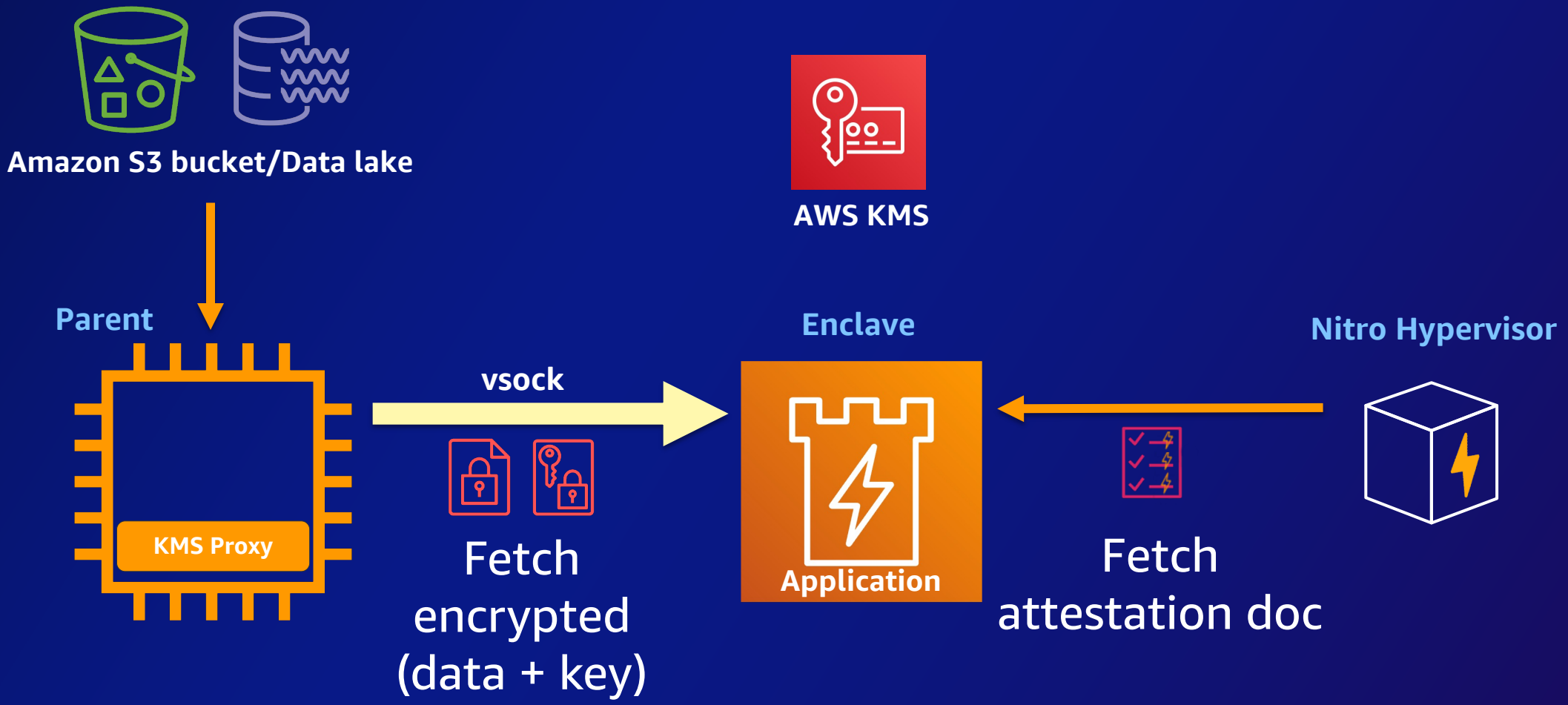
Developer

Set up – enclave image hash and KMS key policy

1. Inspect the code/application from the developer
2. Use the Nitro CLI to convert it to an Enclave Image File
3. Note down the measurements (e.g. PCR 0,1,2)
4. Add that as a condition key to the KMS key policy

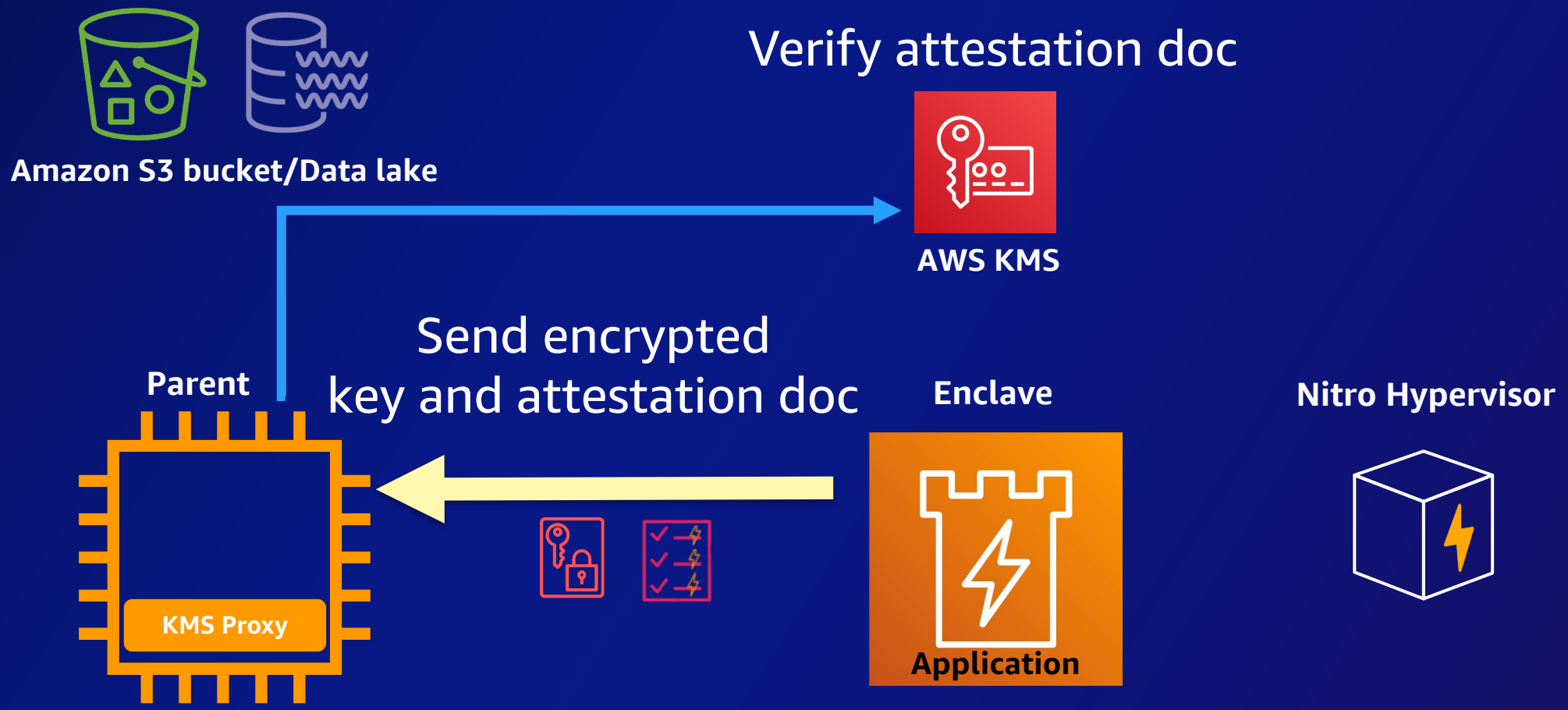
Encrypted Amazon S3 data and AWS KMS

Step 1 – Fetch (Data, Key, and Doc)



Encrypted Amazon S3 data and AWS KMS

Step 2 – Send and Verify



Encrypted Amazon S3 data and AWS KMS

Step 3 – Receive

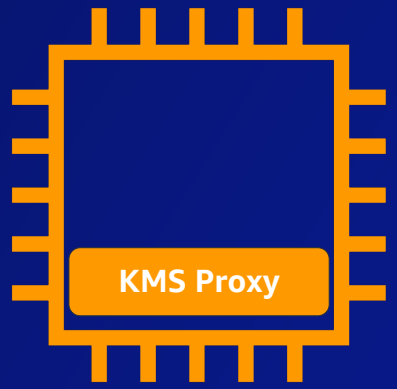
S3 bucket/Data lake

Re-encrypt the data key

AWS KMS

Receive data key to enclave

Parent



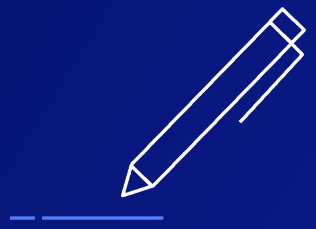
Enclave

Nitro Hypervisor

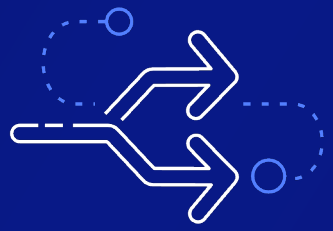
Use cases

Sensitive data processing

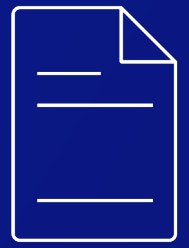
Decrypt



Sign



Tokenize

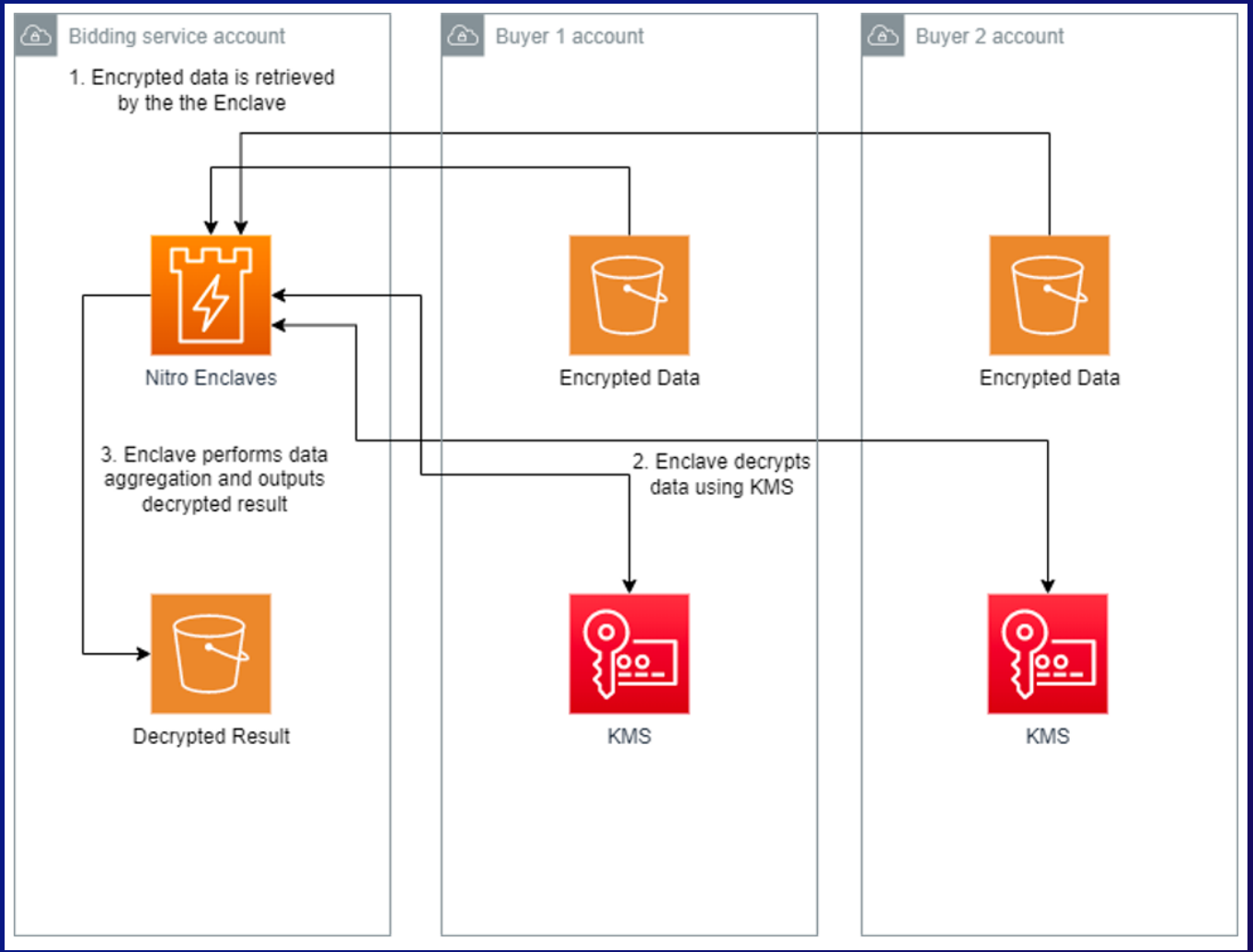


Mask

Infer

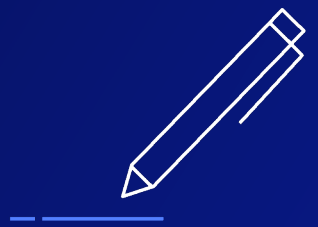
Multi-party computation

Two or more parties process sensitive data without giving access to each other

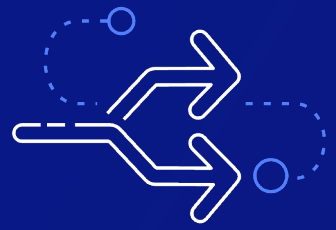


Other use cases

Multi-signing protocols



Tokenization apps



IP Protection

Key takeaways

- General purpose fully homomorphic encryption is not practical (yet); emerging solutions for specific use cases (AWS Clean Rooms)
- Isolated environments with hardware root of trust provide practical solutions
- Cloud admin and internal admin access dimensions need to be considered in the context of cloud
- Memory encryption does not solve it; still encrypt everything to achieve defence-in-depth.

Thank you!

Please complete the session survey in the mobile app

Andy Bunn
bunnand@amazon.co.uk

Dusko Karaklajic
dkkarakl@amazon.com