

The background features a dark blue gradient with large, overlapping, curved shapes in shades of orange, pink, and purple on the right side, creating a modern, abstract design.

AWS re:Invent

NOV. 27 – DEC. 1, 2023 | LAS VEGAS, NV

Protect sensitive data in use with AWS confidential computing

J.D. Bean

Principal Security Architect, EC2
AWS

Arvind Raghu

Principal Specialist, EC2
AWS

Aleks Rudzitis

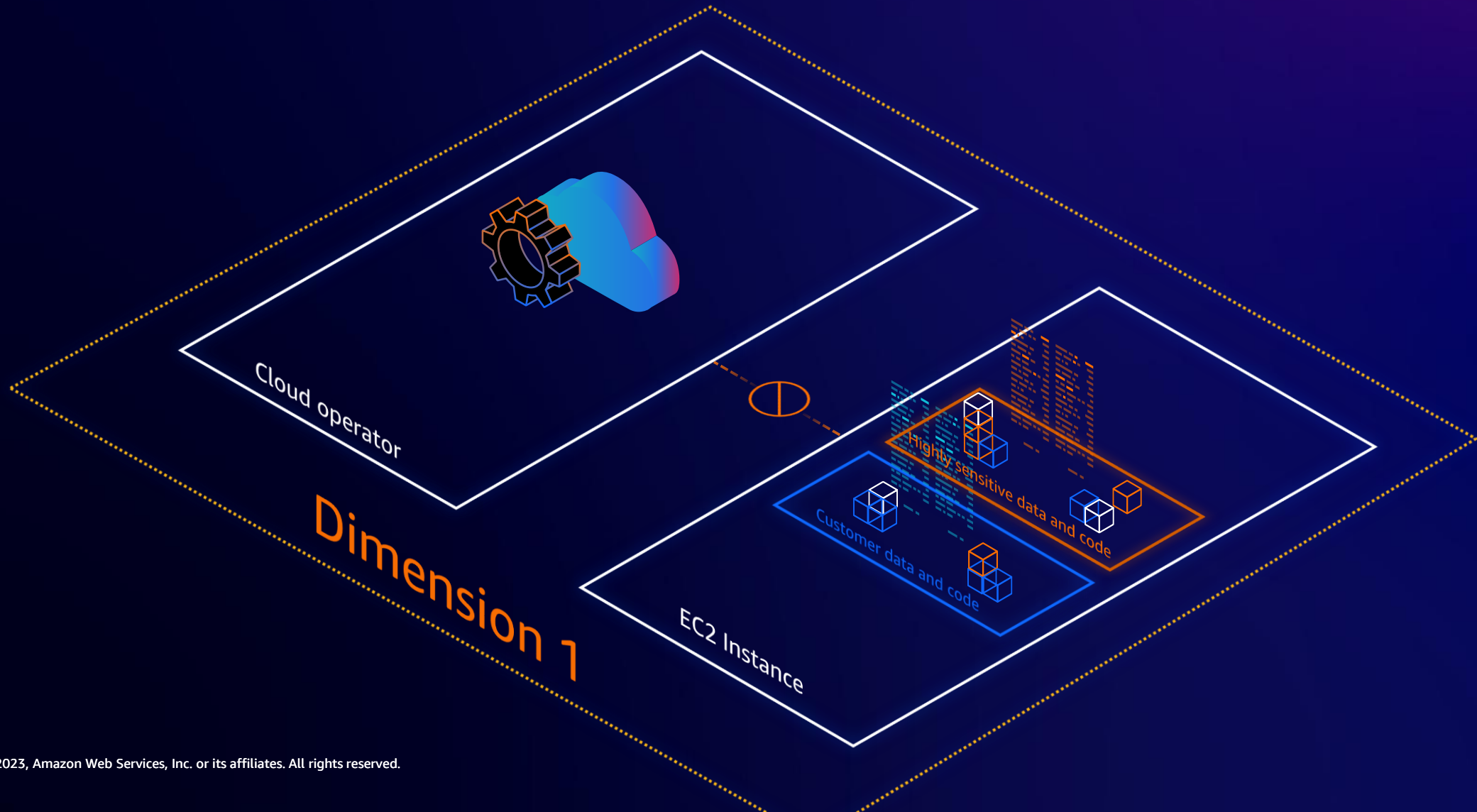
Staff Software Engineer
Stripe

Agenda

- 01 Confidential computing on AWS
- 02 Intro to Nitro System – no operator access
- 03 Nitro Enclaves – Deep dive, key features, benefits
- 04 Stripe – Customer solution leveraging Nitro Enclaves
- 05 Popular use cases
- 06 Resources

Confidential computing

PROTECTING CUSTOMER CODE AND SENSITIVE DATA IN USE



Confidential computing

PROTECTING CUSTOMER CODE AND SENSITIVE DATA IN USE



Processing highly sensitive data on Amazon Elastic Compute Cloud (Amazon EC2)



Personally
identifiable
information



Encryption
keys



Healthcare



Financial



Intellectual
property (IP)

Confidential computing capabilities

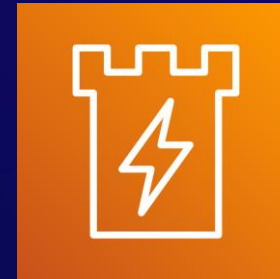
AWS Nitro System



Foundation of virtualization in modern Amazon EC2 instances

DIMENSION 1

AWS Nitro Enclaves



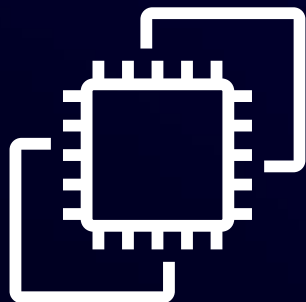
Additional Isolation with hardened, highly isolated compute environment

DIMENSION 2

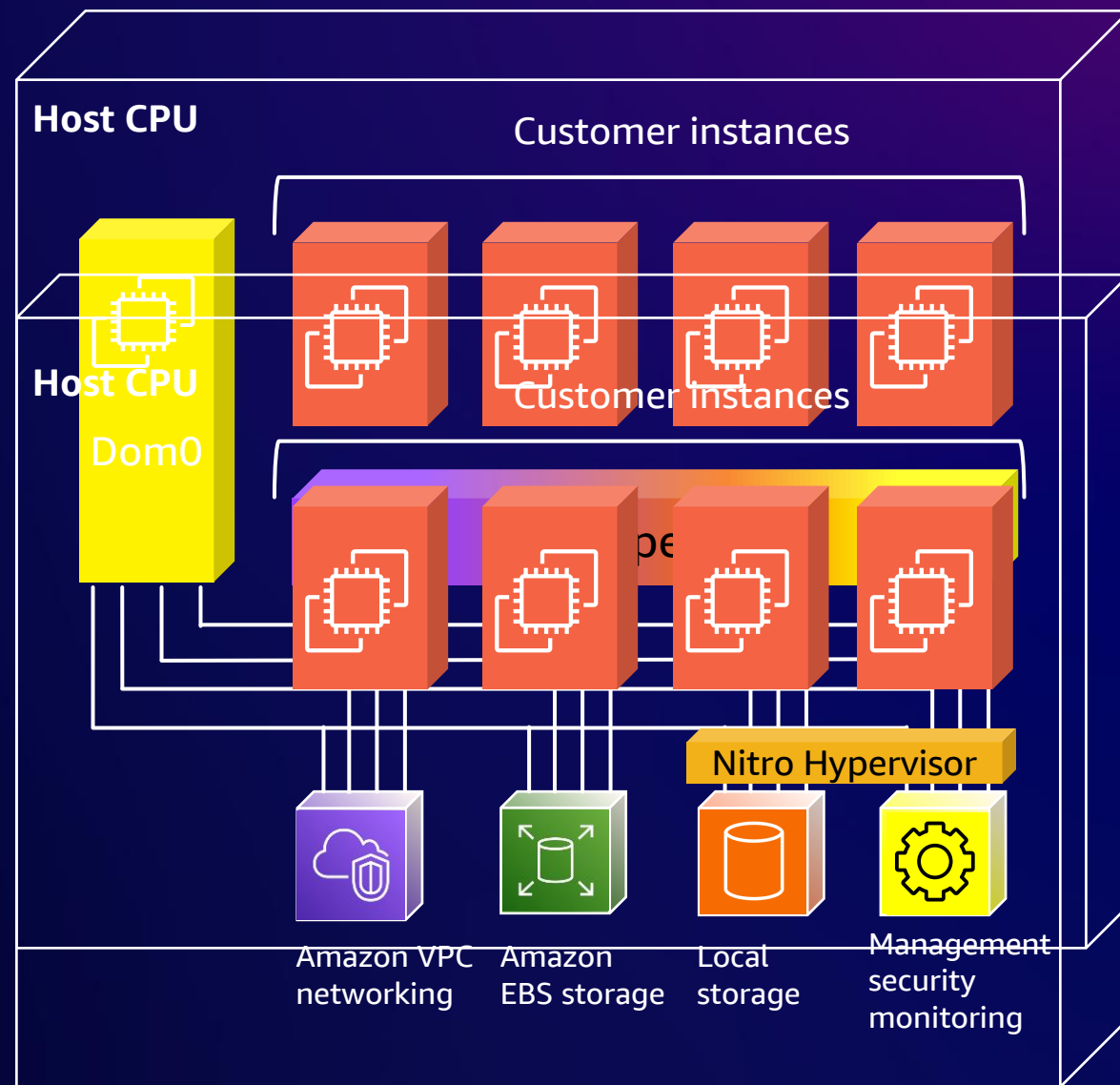
Introduction to AWS Nitro System



AWS Nitro System

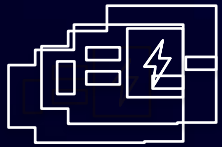


AWS Nitro System



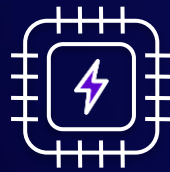
Key components

Nitro Cards



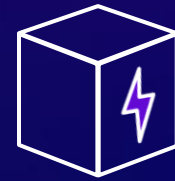
- Local NVMe storage
- Elastic block storage
- Networking, monitoring, and security

Nitro Security Chip



- Integrated into motherboard
- Protects hardware resources

Nitro Hypervisor



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

No AWS operator access to the Nitro System

- There is no operator access mechanism in the Nitro System design
- No SSH or general purpose access of any kind
- All Nitro operations are performed via secure, authenticated, authorized, logged & audited administrative APIs
- No APIs provide access to customer data



Additional assurance for the Nitro System



[Whitepaper](#)

Security Design of the
AWS Nitro System



[3rd party validation – Nitro Security](#)

NCC Group report - “no gaps in the
Nitro System that would
compromise these security claims”



[AWS Service Terms](#)

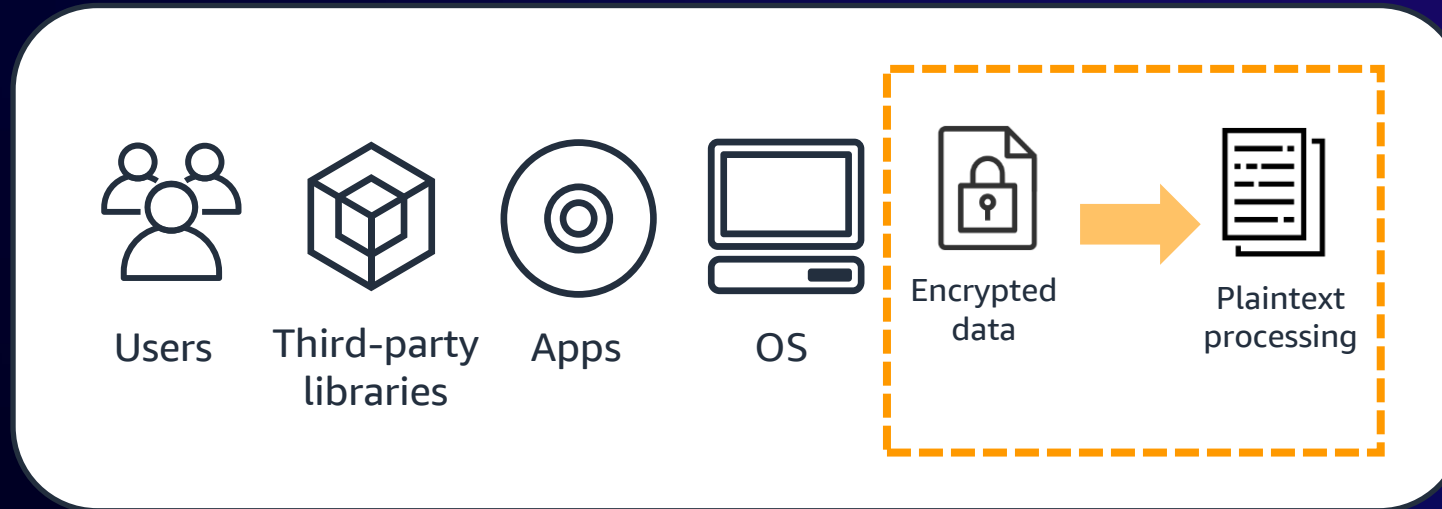
Updated Service terms, to
reflect “no operator access”

AWS Nitro Enclaves

Key features and benefits



What is AWS Nitro Enclaves?



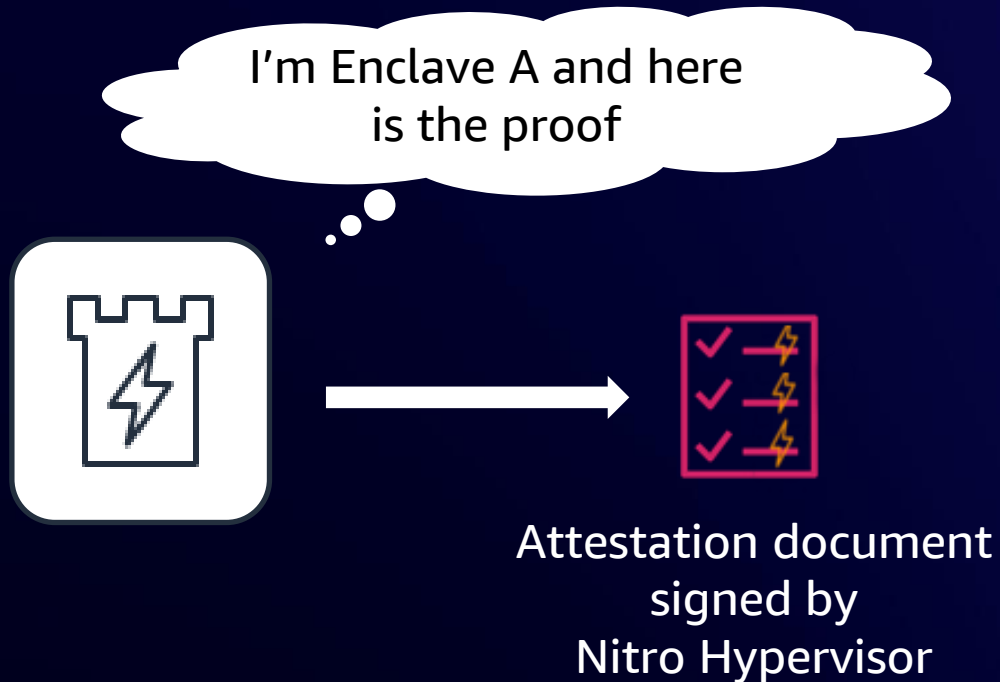
Amazon EC2 instance

What is AWS Nitro Enclaves?



Nitro Enclaves provides additional isolation for data in use

Nitro Enclaves provide proof of identity



Attestation document - hashes

Enclave Image

Application in the enclave

Parent Instance ID

AWS Identity and Access Management

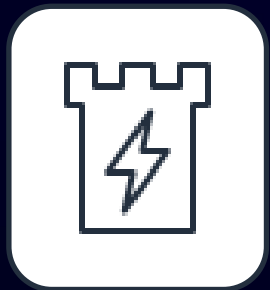
Role of parent instance

User defined info
e.g. Nonce

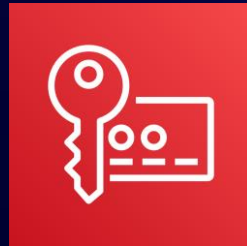
First-class integration with AWS KMS



Signed attestation
document



Nitro enclaves



AWS KMS

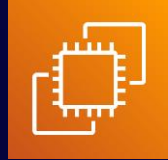
- The **enclave** can prove its identity to **AWS KMS** with attestation document
- AWS KMS validates document against the AWS KMS key policy
- Enclave can perform cryptographic operations with AWS KMS keys

AWS Nitro Enclaves features and benefits



Additional isolation and security

- No storage, access, and networking
- Secure local channel with parent EC2



Flexible

- Processor-agnostic technology
- Combinations of CPU and memory



Cryptographic attestation

- Proves its identity and authorizes code
- Creates its own key pair and integrated with AWS KMS

No additional cost

Where is it used?



Decrypt



Sign



Tokenize



Mask



Infer



Customers from different segments

stripe

okta

 theTradeDesk®

 Itaú

 ACINQ

 Footprint

 evervault

anJuna

 crypto.com

 DASHLANE

 M10

 Oblivious

 Cape Privacy

stripe

What does Stripe do?

**PAYMENT PROCESSING
SOFTWARE AND API**

**ENABLES MILLIONS OF
CUSTOMERS**

Accept Payments

Send Payouts

Automate
Financial Processes

Provide Banking
as a Service

Securing sensitive information



Credit Card
Data



Bank Account
Numbers



Transaction
Information



Personally Identifiable
Information

HOW DO WE PROTECT THE DATA?



Credentials - for authentication

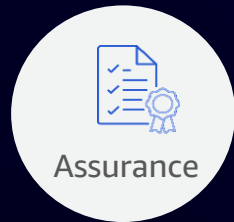


Keys – for secure data exchange

Ideal Solution



RESTRICT ACCESS TO ENCRYPTION KEYS



**USAGE OF KEYS MODERATED BY SOFTWARE
WITH AUDIT TRAIL**



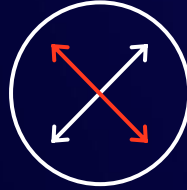
**TRUSTED SOFTWARE - REVIEWED,
RELEASED, AND IN USE**

Nitro Enclaves - addressing the requirements



PROTECT KEYS & CREDENTIALS

- No external communication
- No interactive access by default



SCALABILITY, COST, AVAILABILITY

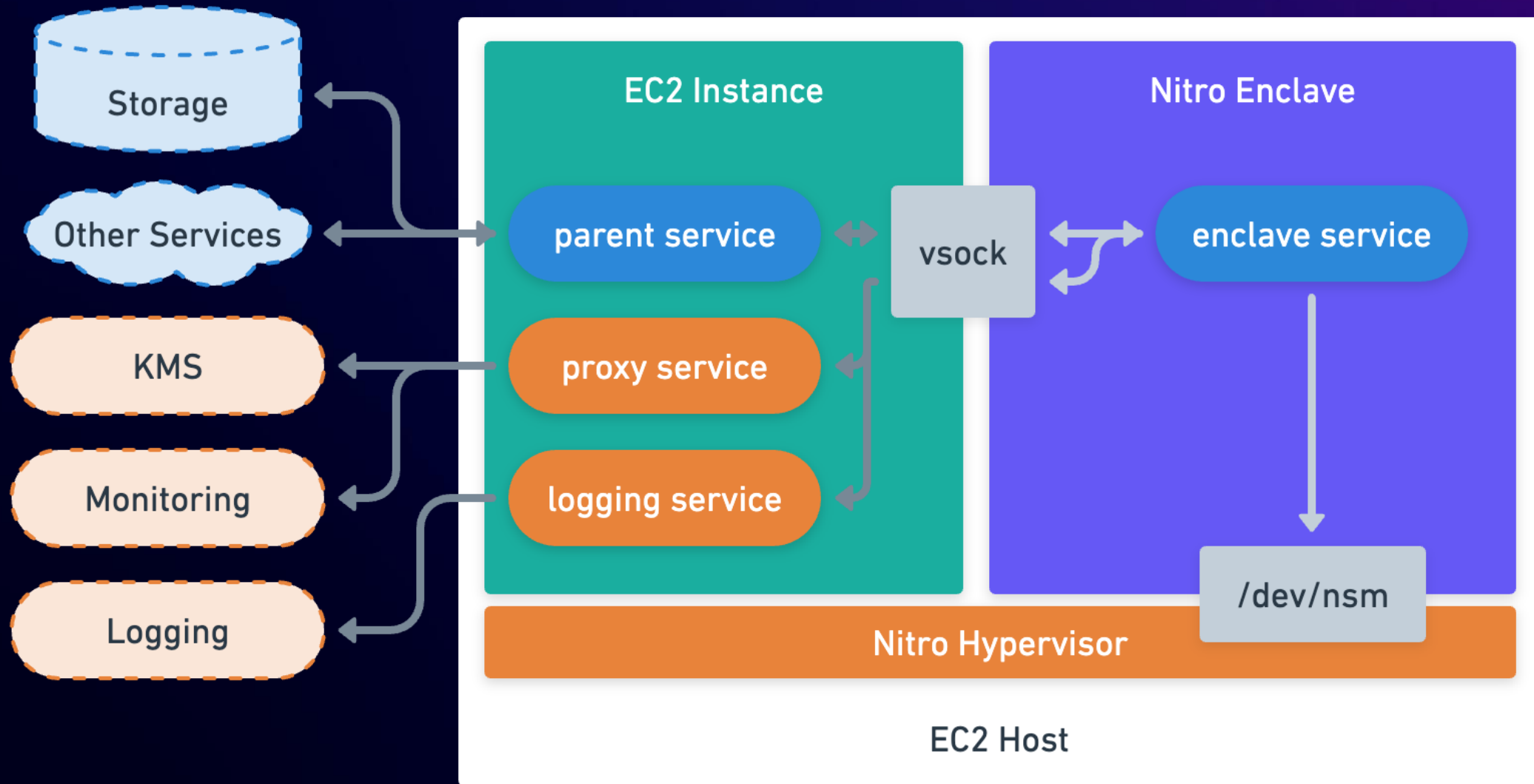
- Easy to provision, upgrade, and non-proprietary
- Low net cost



CRYPTOGRAPHIC ATTESTATION

- Ensure only authorized code is running
- Integration with AWS KMS

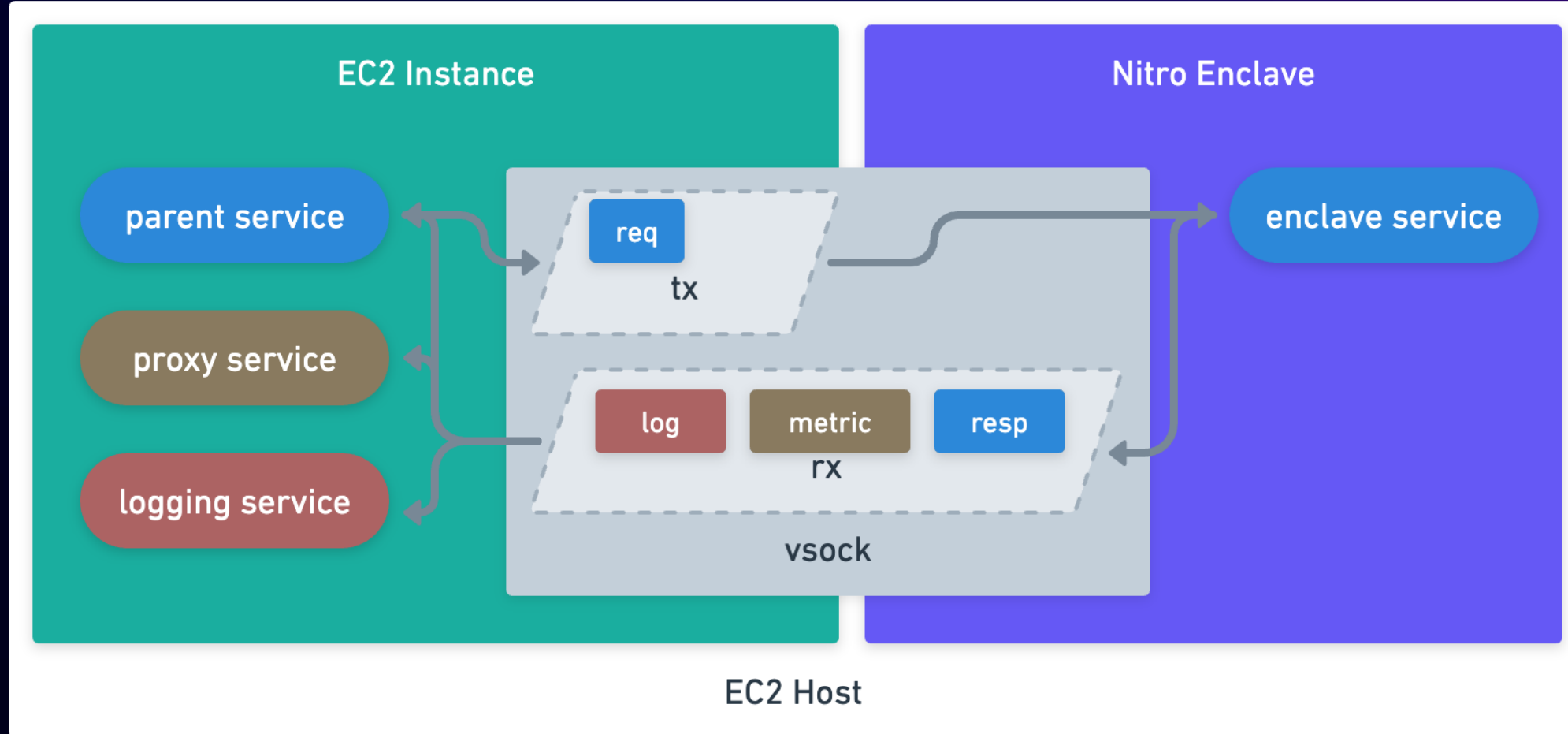
Enclave based service



Integration process

- Building an internal Go SDK
- Creating our own Go-based TCP/UDP proxy
- Logging proxy
- TLS communication with parent EC2 instance

Performance limitations



Outcome of the implementation

REDUCED

HUMAN TOIL

COMPLEXITY

LATENCY

RECOVERY TIME

Popular use cases

Protecting IP – ML model licensing

GOAL: PROTECT AND MAKE IP CONSUMABLE

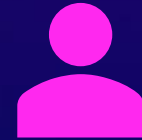


ML model provider



Encrypted IP

- Model provider has trained ML model – “secret sauce” to protect
- Data owner wants to license the trained ML model for inferencing
- Both benefit from collaborating, but code and data should not be visible



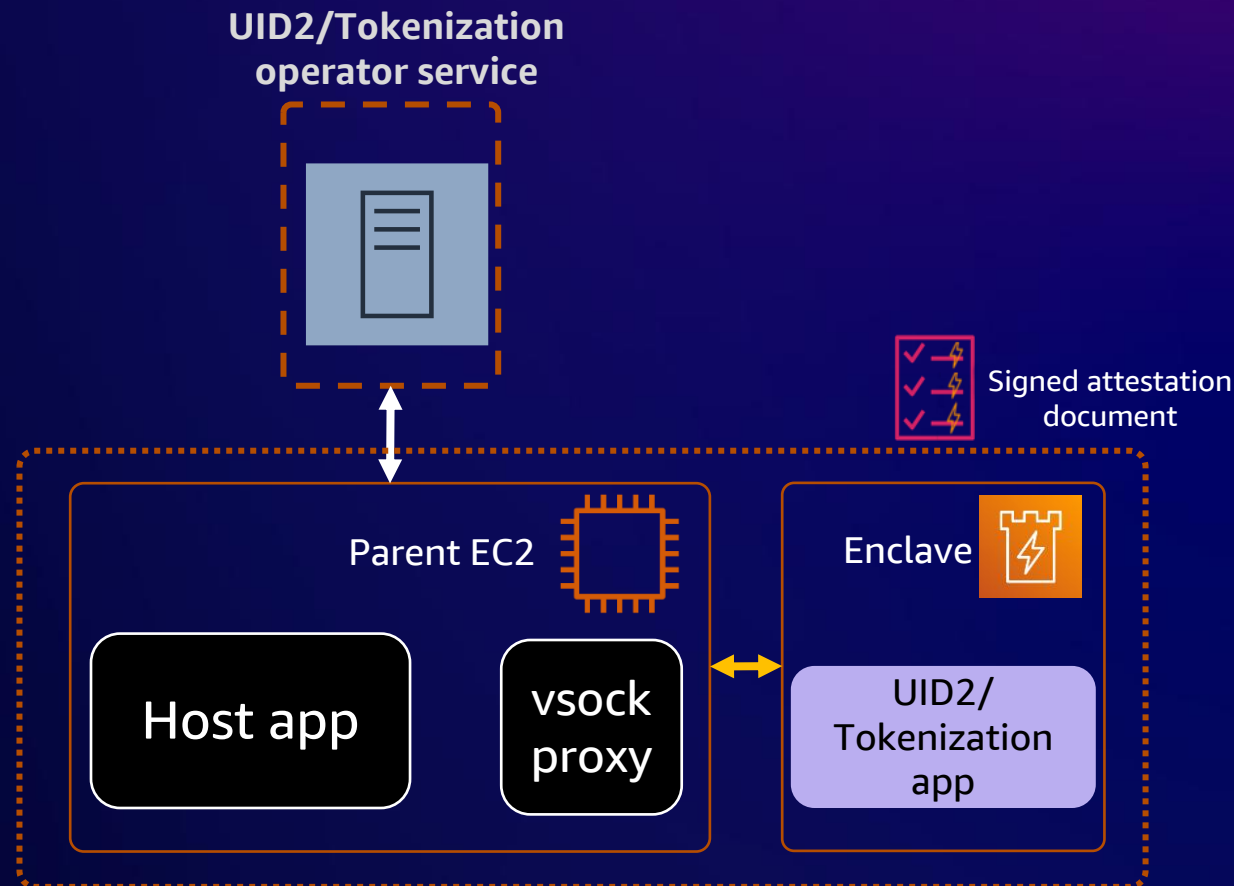
Data owner &
model consumer



Encrypted data

Tokenization for AdTech

- Cookies are going away – driven by emphasis on privacy
- Need for trusted environment to securely process PII data
- Use UID2 type identifiers to process and transform data in memory
- No persistent storage of encryption keys or UID2 type identifiers



Multi-party collaboration

TWO OR MORE PARTIES PROCESS SENSITIVE DATA WITHOUT GIVING ACCESS TO EACH OTHER



Party 1



Encrypted
dataset



Party 2



Encrypted
dataset

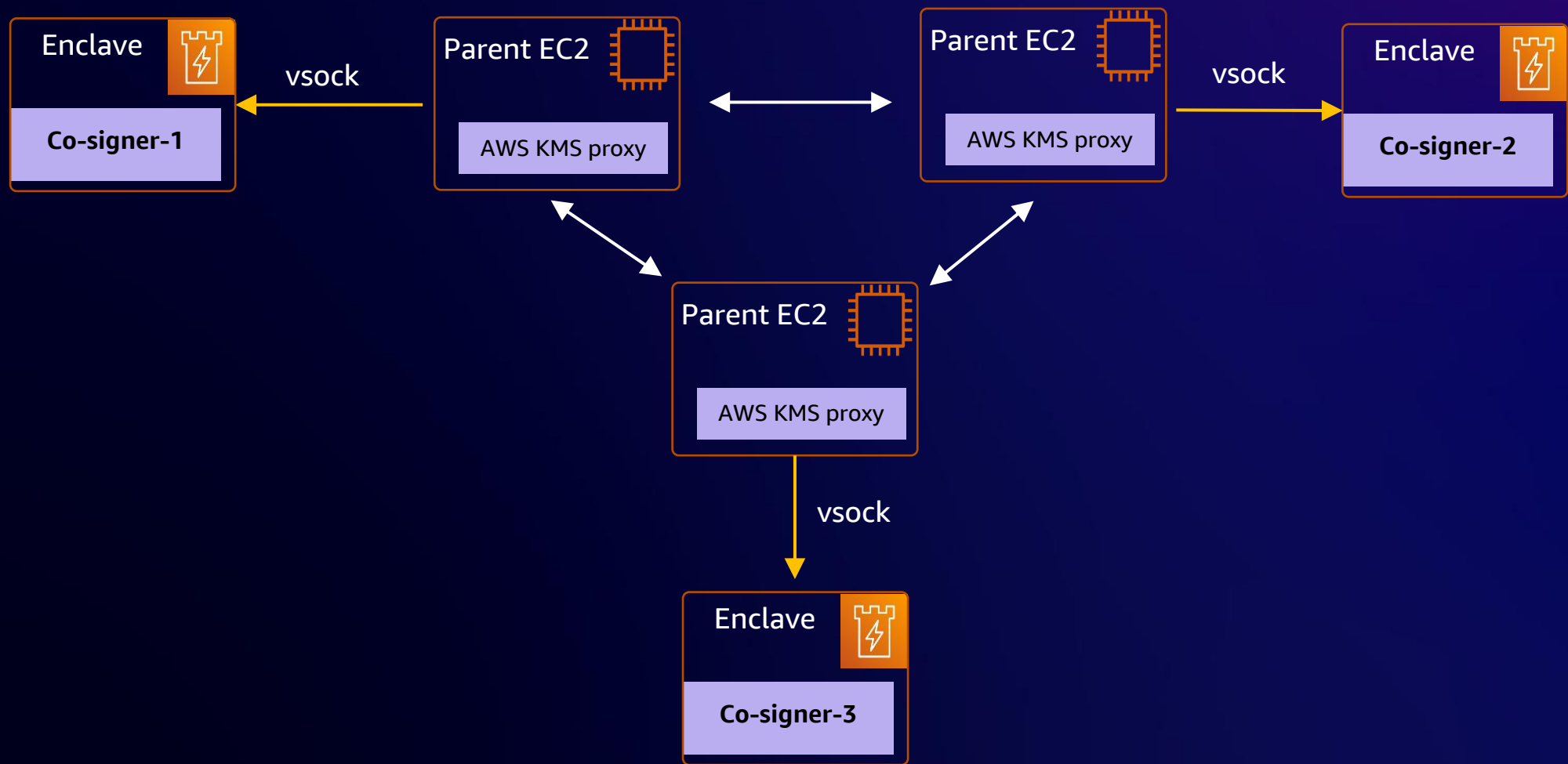


Nitro enclave

Emerging blockchain workloads

- Blockchain bridging – multiple chains
- Hot wallets for digital assets – exchanges and custodians
- Signature validator node – multiple key shards consensus

Emerging blockchain workloads



Resources to learn more



[AWS Nitro Enclaves](#)

Learn more about Nitro
Enclaves



[Nitro Enclaves Workshop](#)

Self-help self-paced workshop
to get hands on experience



[Confidential Compute Blog](#)

Learn about AWS' perspective
on Confidential computing

Continue your compute learning

Learn at your
own pace



Expand your
knowledge with
Learning Plans via
AWS Skill Builder

Increase your
knowledge



Use our **Ramp-Up Guides**
to build your Compute
knowledge



Earn your
Compute badge



Demonstrate your
knowledge by achieving
digital badges

Thank you!



Please complete the session survey in the mobile app