



Dublin Cloud Day

DUBLIN | MARCH 28TH

DCD-T4

Protect your most valuable assets with AWS native and partner- provided data protection services

Patrick Palmer (he/him)

Sr. Security Specialist SA



Your best assets; data



It's all about Data



Controlling this requires tools



Encryption is powerful



Don't go alone

Modern Companies are **Data
Companies**, building in the **Cloud**.



Data **is** your business



How can I keep my data confidential?

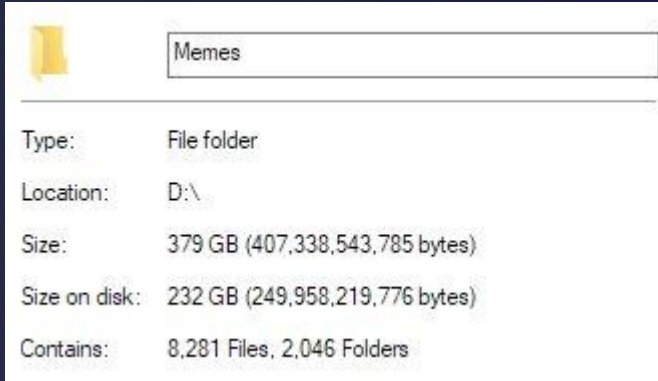


How do I know my data and resources are trustworthy?



How do I keep control of my personal data?

Data Classification



Memes

Type: File folder

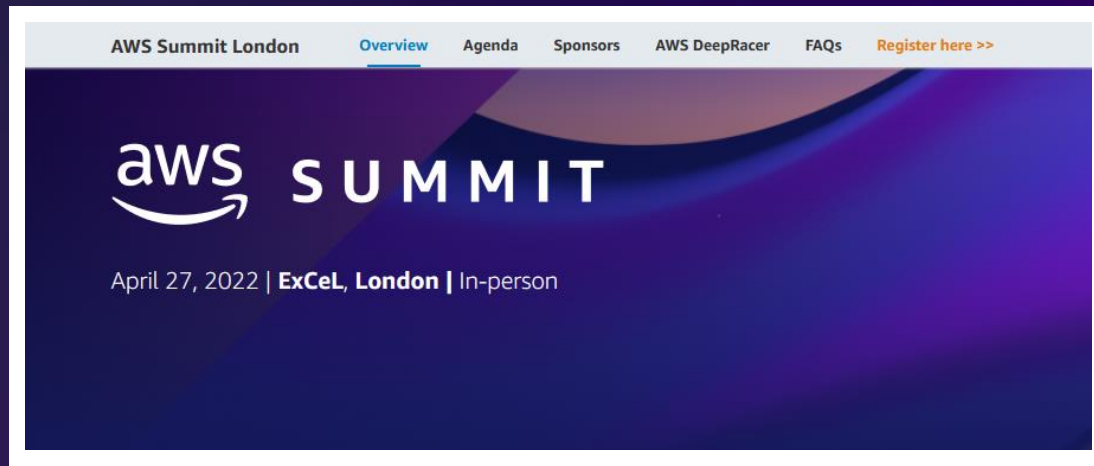
Location: D:\

Size: 379 GB (407,338,543,785 bytes)

Size on disk: 232 GB (249,958,219,776 bytes)

Contains: 8,281 Files, 2,046 Folders

A	B	C	D
Customers	Name	Age	Credit Card
1	Aaron	=RANDBETWEEN(21,88)	4166825422144165
2	Bridget		25 4164605682089867
3	Charlie		65 4187200840659923
4	Deirdre		76 4185536372365987



AWS Summit London

[Overview](#) [Agenda](#) [Sponsors](#) [AWS DeepRacer](#) [FAQs](#) [Register here >>](#)

aws SUMMIT

April 27, 2022 | ExCeL, London | In-person

Data Classification

Data Classification: Secure Cloud Adoption
AWS Whitepaper

Abstract

- Data Classification Overview
- Existing Data Classification Models
 - U.S. National Classification Scheme
 - U.S. Information Categorization Scheme
 - United Kingdom (UK) Government**
 - Customer Considerations for Implementing Data Classification Schemes

United Kingdom (UK) Government

[PDF](#) | [RSS](#)

In 2014, the UK simplified its data classification scheme by reducing the levels from six to three. They are:

1. Official — Routine business operations and services, some of which could have damaging consequences if lost, stolen, or published in the media, but none of which is subject to a heightened threat profile.
1. Secret — Very sensitive information that justifies heightened protective measures to defend against determined and highly capable threat actors (e.g., compromise could significantly damage military capabilities, international relations, or the investigation of serious organized crime).
2. Top secret — Most sensitive information requiring the highest levels of protection from the most serious threats (e.g., compromise could cause widespread loss of life or could threaten the security or economic well-being of the country).

According to a cabinet office core briefing, the UK government categorizes information into three levels of sensitivity: Official, Secret, and Top Secret. For more information, see [/government/uploads/system/uploads/attachment_data/file/2514](#)

OFFICIAL

SECRET

TOP SECRET

Data Classification; et al



Identity & access management

AWS Identity & Access Management (IAM)
AWS Single Sign-On
AWS Organizations
AWS Directory Service
Amazon Cognito
AWS Resource Access Manager



Detection

AWS Security Hub
Amazon GuardDuty
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 – Web application firewall
Amazon Virtual Private Cloud (VPC)
AWS PrivateLink
AWS Systems Manager



Data protection

Amazon Macie
AWS Key Management Service (KMS)
AWS CloudHSM
AWS Certificate Manager
AWS Secrets Manager
AWS VPN
Server-Side Encryption



Incident response

Amazon Detective
CloudEndure DR
AWS Config Rules
AWS Lambda



Compliance

AWS Artifact
AWS Audit Manager

[PARTNERS.AMAZONAWS.COM](https://partners.amazonaws.com)

AWS Security Competency Partners

Helping customers elevate and enhance their security in the cloud

[Contact an AWS Partner specialist](#)



AWS has data protection resources to help organizations at any stage of their cloud journey



Use data protection services to achieve granular control over access and policy enforcement



Reduce operational risk through automation and increased visibility



Engage with the AWS network of security and consulting partners

Data Protection on AWS, building in the Cloud.



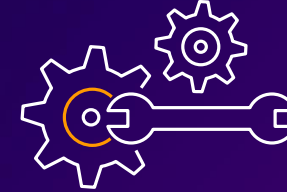
Why use Data Protection on AWS?



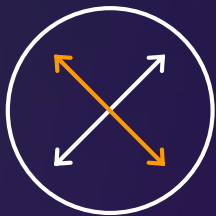
Protect intellectual property and trade secrets



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

Maintain control over your data on AWS



Manage privacy controls for your data



Control how your data is used



Manage who has access to your data



Control how your data is encrypted

Maintain control over your data on AWS



Manage privacy controls for your data



Control how your data is used



Manage who has access to your data



Control how your data is encrypted



Data Encryption on AWS

- Customers use separate KMS Keys to partition access to data
- KMS Key policy defines access
- KMS Key authorization ought to separate key administrators from encryption key users
- Improves the intentionality and discretion of data access



Data Encryption on AWS

- Customers use separate KMS Keys to partition access to data
- KMS Key policy defines access
- KMS Key authorization ought to separate key administrators from encryption key users
- Improves the intentionality and discretion of data access



Encrypt like everyone is watching

```
[cloudshell-user@ip-10-0-165-97 ~]$ aws kms encrypt --key-id alias/Imported --plaintext `echo example | base64`  
{  
  "CiphertextBlob": "AQICAHijVd51m4UcTYBveJf8V+kSxRdK1F7cDpChgPBygyJknQHLu2pK8FTUHAuaMDU0a461AAAAZjBkBgkqhkiG9w0BBwz  
mQ=="
```

My Debit Card Information:

AQECAHgu+VBKMC+fPRAogv0PheI5oiwP1aJ
avfVkBOveVD364QAAAGlwYAYJKoZIHvcNAQ
cGoFMwUQIBADBMBgkqhkiG9w0BBwEwHgY
JYIZIAWUDBAEuMBEEDBaHQ9C4ByGQ1sgk
WwIBEIAfWm6mJcXoyRFf9+aiJL4puswwyEh
DySIIfB8ctOM5Zw==



Encrypt like everyone is watching

```
[cloudshell-user@ip-10-0-165-97 ~]$ aws kms encrypt --key-id alias/Imported --plaintext `echo example | base64`  
{  
  "CiphertextBlob": "AQICAHijVd51m4UcTYBveJf8V+kSxRdK1F7cDpChgPBygyJknQHLu2pK8FTUHAuaMDU0a461AAAAZjBkBgkqhkiG9w0BBwz  
mQ=="
```

My Debit Card Information:

AQECAHgu+VBKMC+fPRAogv0PheI5oiwP1aJ
avfVkBOveVD364QAAAGlwYAYJKoZIHvcNAQ
cGoFMwUQIBADBMBgkqhkiG9w0BBwEwHgY
JYIZIAWUDBAEuMBEEDBaHQ9C4ByGQ1sgk
WwIBEIAfWm6mJcXoyRFf9+aiJL4puswwyEh
DySIIfB8ctOM5Zw==



Building like it's 1022





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 AWS WAF rules across accounts and applications



AWS Network Firewall

Deploy network security across your Amazon VPCs with just a few clicks



AWS Shield

Managed DDoS protection service that safeguards web applications running on AWS



AWS WAF—Web Application Firewall

Protects your web applications from common web exploits ensuring availability and security



Amazon Virtual Private Cloud

Provision a logically isolated section of AWS where you can launch AWS resources in a virtual network that you define



AWS PrivateLink

Access services hosted on AWS easily and securely by keeping your network traffic within the AWS network

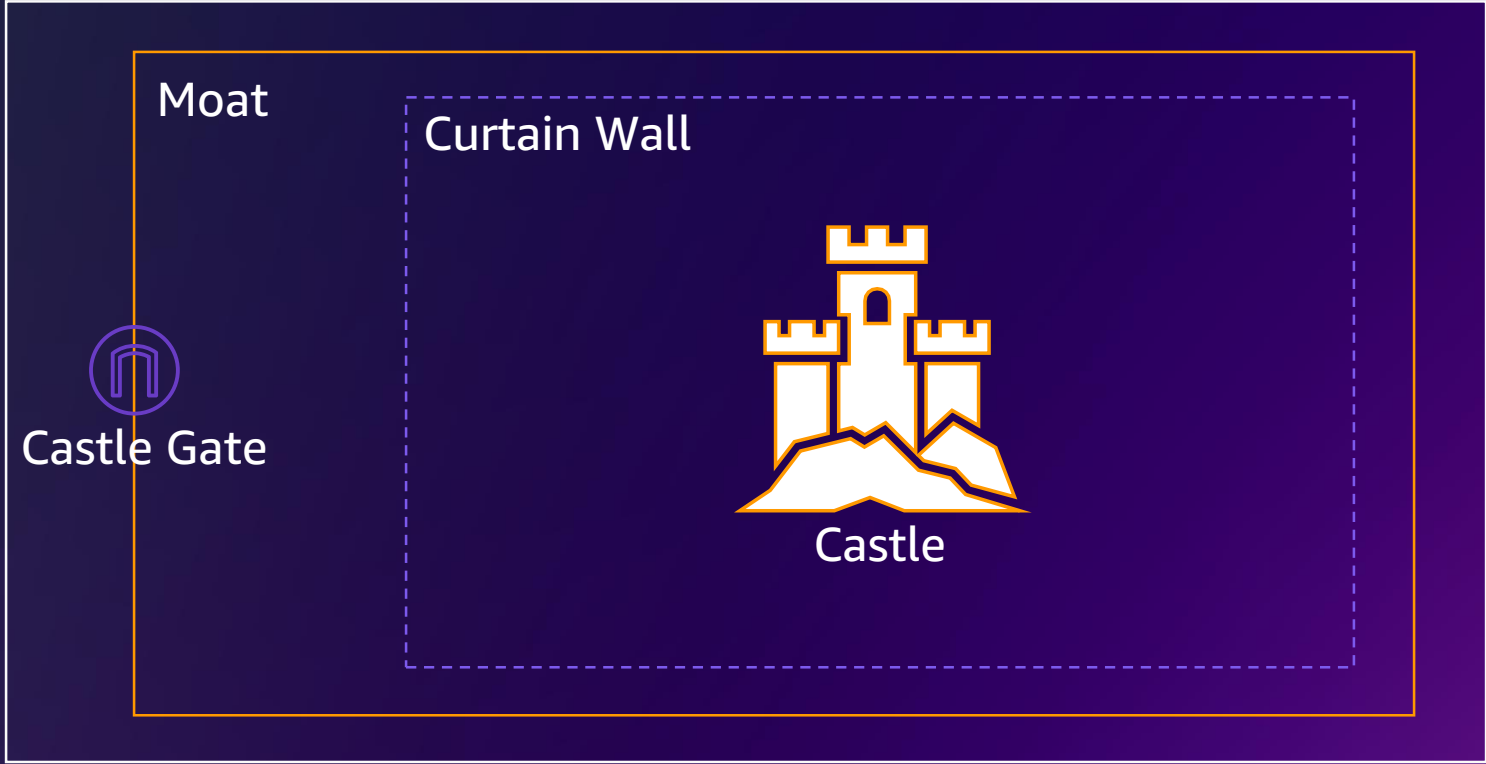


AWS Systems Manager

Easily configure and manage Amazon EC2 and on-premises systems to apply OS patches, create secure system images, and configure secure OSs

Building like it's 1022

AWS WAF





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 AWS WAF rules across accounts and applications



AWS Network Firewall

Deploy network security across your Amazon VPCs with just a few clicks



AWS Shield

Managed DDoS protection service that safeguards web applications running on AWS



AWS WAF—Web Application Firewall

Protects your web applications from common web exploits ensuring availability and security



Amazon Virtual Private Cloud

Provision a logically isolated section of AWS where you can launch AWS resources in a virtual network that you define



AWS PrivateLink

Access services hosted on AWS easily and securely by keeping your network traffic within the AWS network

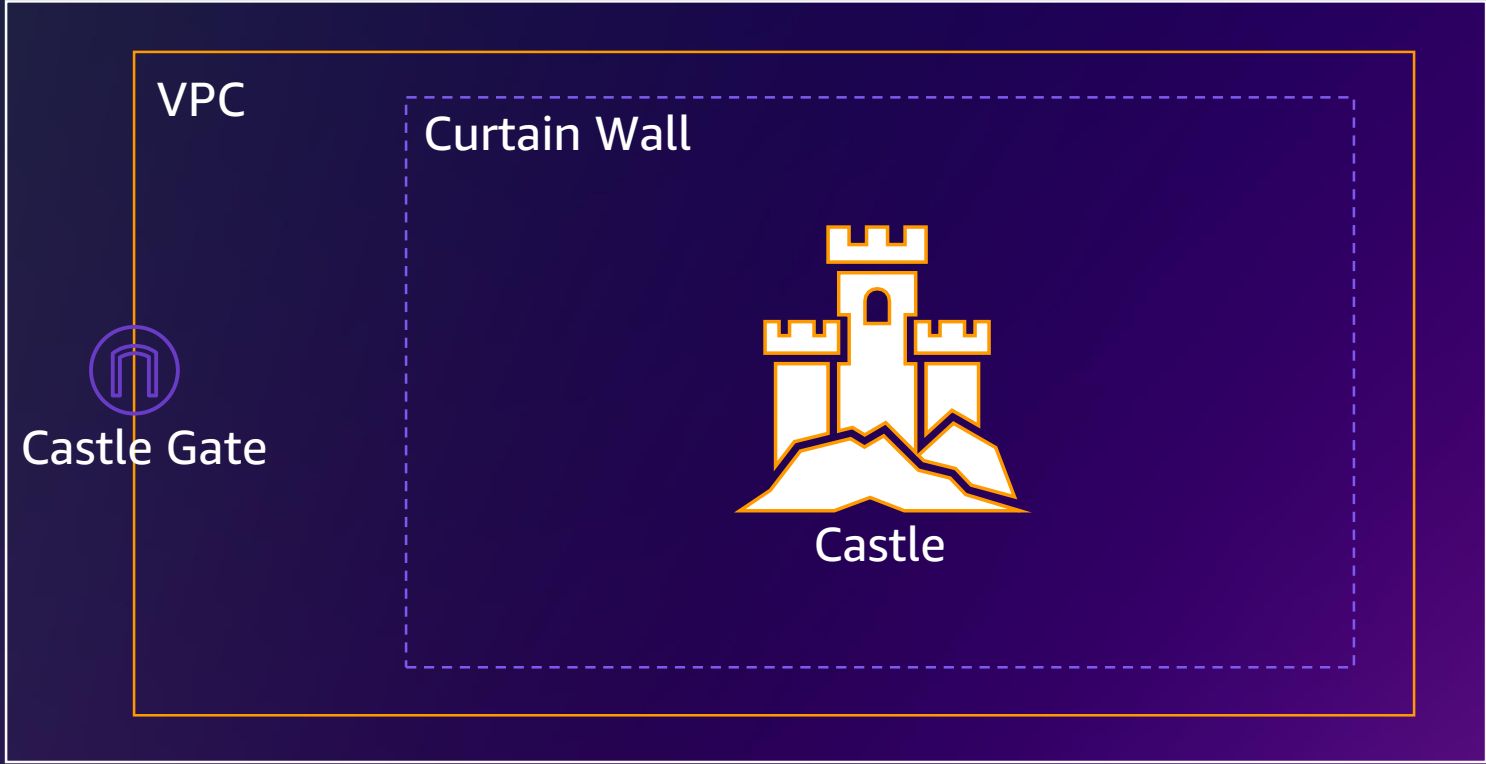


AWS Systems Manager

Easily configure and manage Amazon EC2 and on-premises systems to apply OS patches, create secure system images, and configure secure OSs

Building like it's 1022

AWS WAF





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 Single Sign-On (SSO)

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

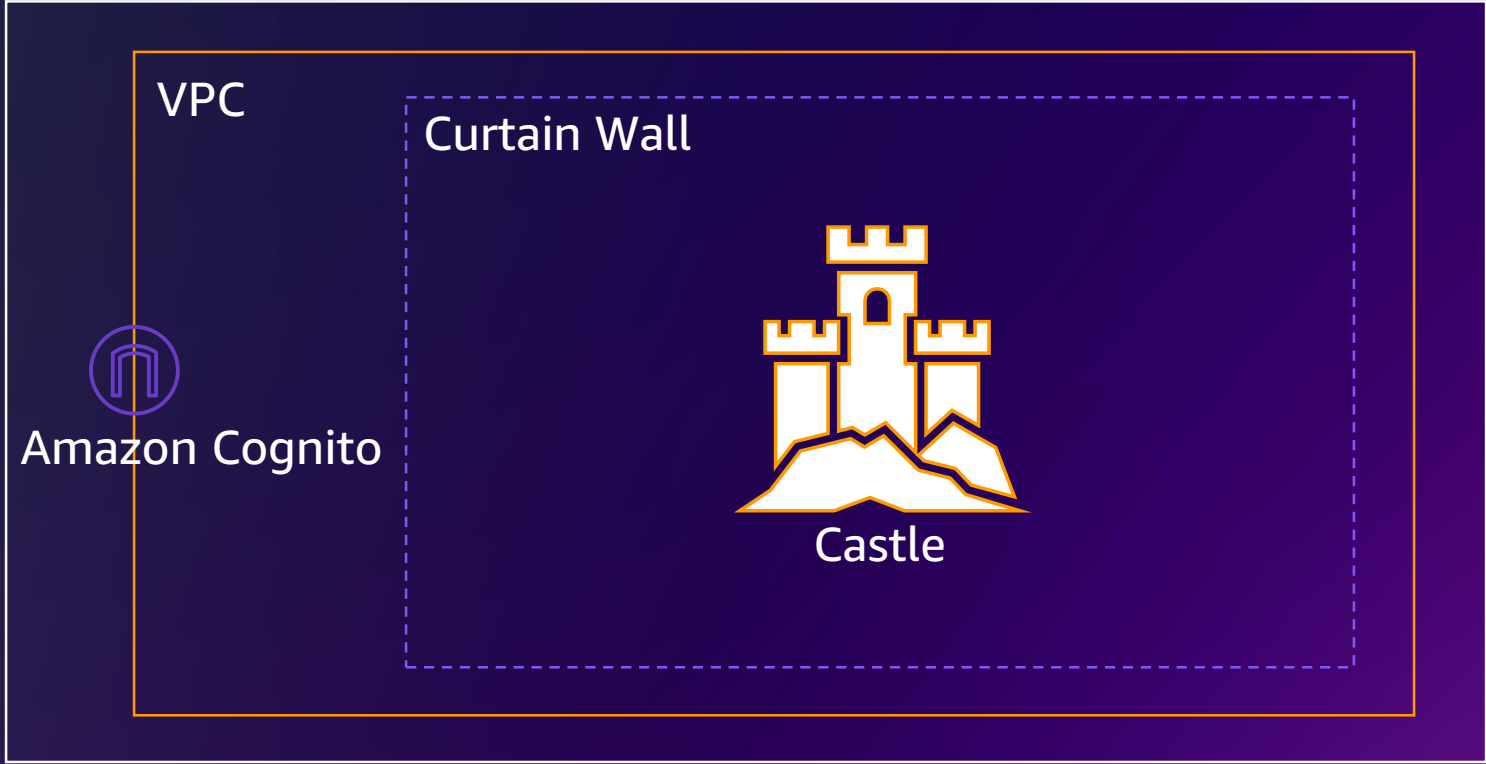


AWS Resource Access Manager

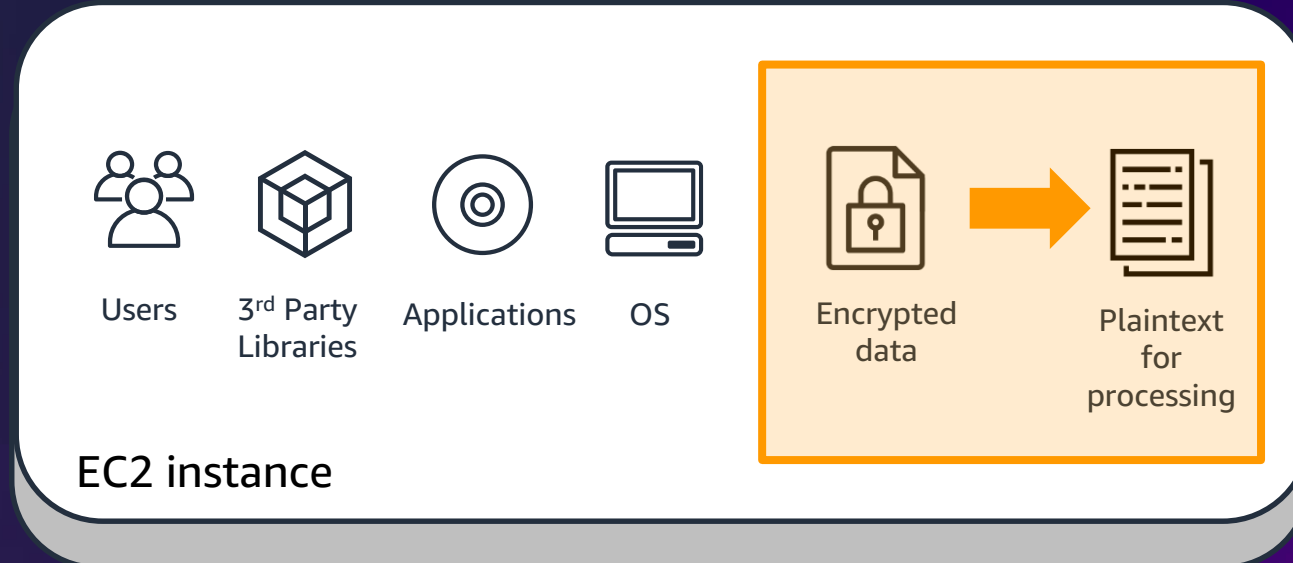
Simple, secure service for sharing AWS resources

Building like it's 1022

AWS WAF



AWS Nitro System



...by creating an **isolated environment** to process sensitive data without providing access to **their own system administrators, developers, and applications.**

AWS Nitro System

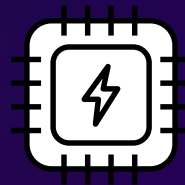
- Built with security in mind from the ground up – from the silicon chips to the software running in the servers

Nitro Card



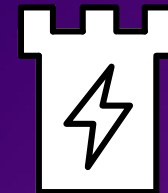
Local NVMe storage
Elastic Block Storage
Networking, monitoring, and security

Nitro Security Chip



Integrated into motherboard
Protects hardware resources

Nitro Enclave



Isolated compute environment to
protect and securely process
sensitive data

AWS Nitro System

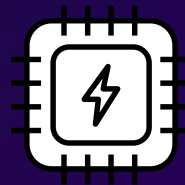
- Built with security in mind from the ground up – from the silicon chips to the software running in the servers

Nitro Card



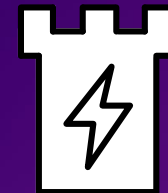
Local NVMe storage
Elastic Block Storage
Networking, monitoring, and security

Nitro Security Chip



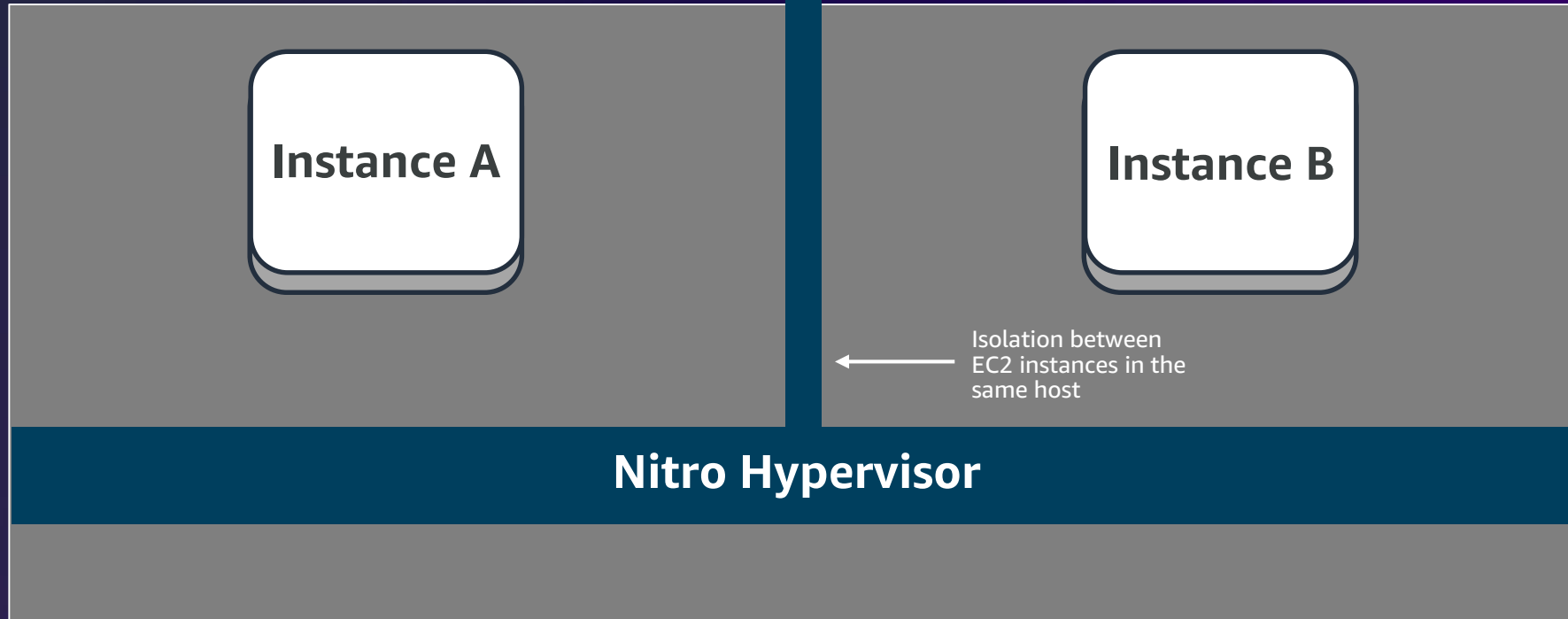
Integrated into motherboard
Protects hardware resources

Nitro Enclave



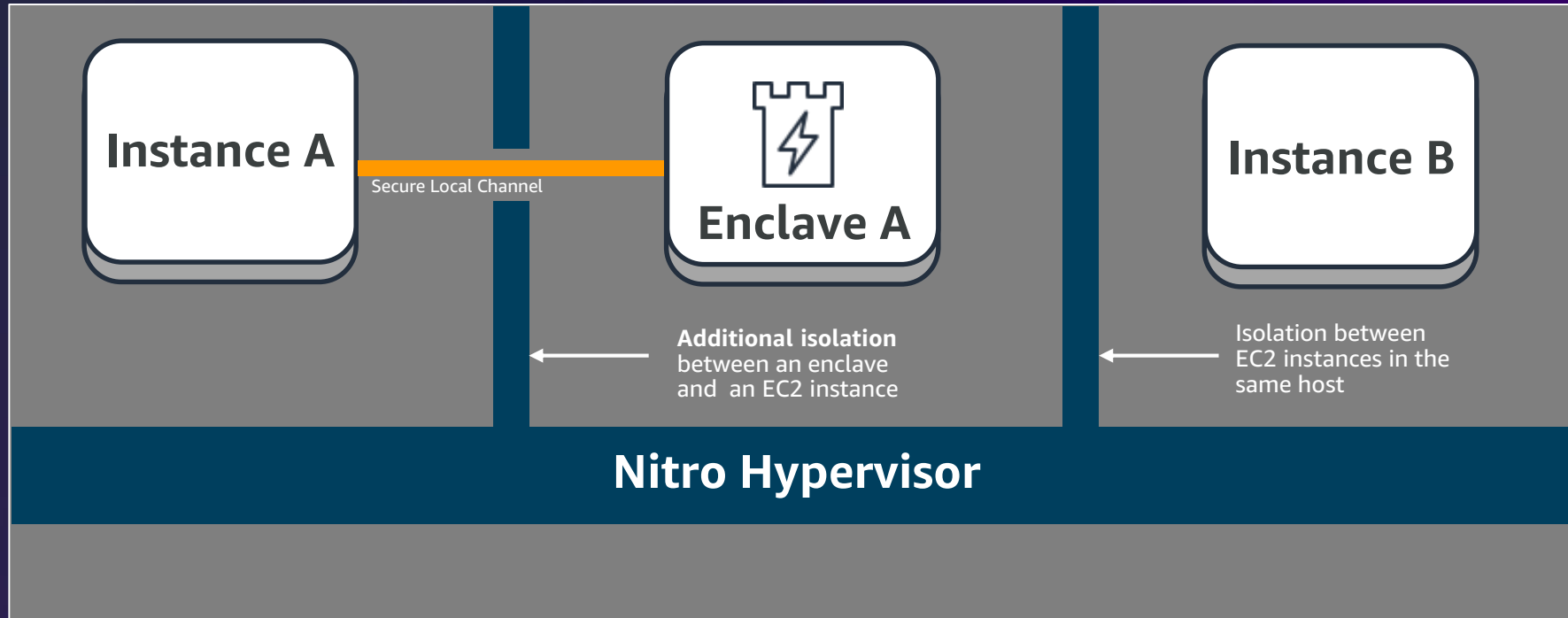
Isolated compute environment to
protect and securely process
sensitive data

Deeper into the **Enclave**



EC2 host

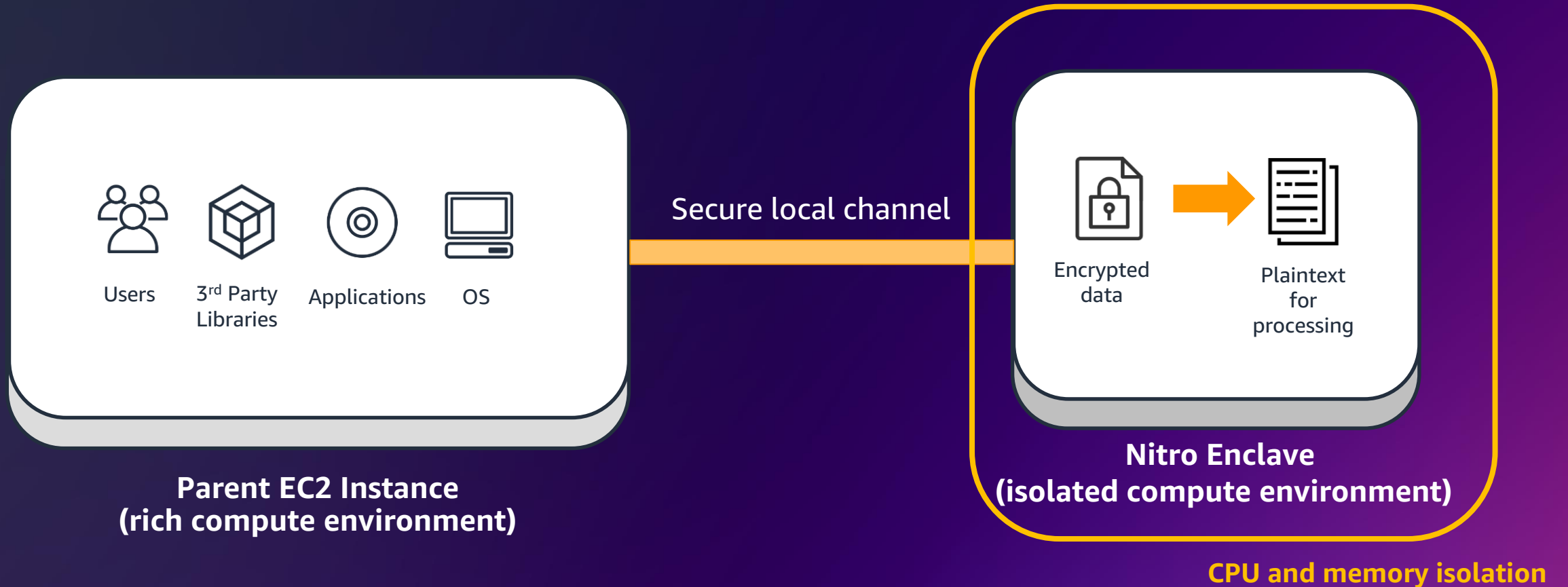
Deeper into the **Enclave**



EC2 host

Deeper into the **Enclave**

Ability to create **isolated compute environments** from EC2 instances to process highly sensitive data



Building like it's 1022

AWS WAF



Your best assets; data



It's all about Data



Controlling this requires tools



Encryption is powerful



Don't go alone

Thank you!

Patrick Palmer

[LinkedIn: patrick-palmer-aws](#)



















“

”



Thank you!

Speaker Name

 example@amazon.com

 @example

 Example Last Name





Please complete
the session survey