APPS & SOLUTIONS

OC3

OPEN CONFIDENTIAL COMPUTING CONFERENCE | MARCH 13 | ONLINE

Louisa Muschal & Andrea Corbelli

Navigating Compliance: Leveraging Confidential Compute for DORA-Driven Regulatory Adherence

Encryption is vital to cloud data security and digital trust

$4.35M

Global average cost of a data breach [1]

67%

67% of Organizations Already Store Sensitive Data in Public Cloud Environments[2]

Encryption

One of the largest cost mitigators

reduces breach costs by an average of $252,000[1]

Confidential Compute

in use by 27% of respondents, and 55% have plans to deploy it to lock down data and workloads[2]

[1] 2022 Ponemon Institute Cost of a Data Breach Report

[2] 2022 Cloud Security Alliance

Privacy

California

Personal Information Protection and Electronic Documents Act - Canada

Regulatory Compliance

Often mandates encryption of data at rest and in transit or strongly encourages **technical measures** to protect data

But who has access to your data and keys?

Example Regulation: Financial Services – Resilience

The European Commission initiated DORA to harmonize ICT regulation in the financial services sector in the European Union (EU), imposing common requirements in all EU member states in the following areas:

1. Information Communication Technologies (ICT) Risk Management & Governance,
2. Incident Reporting and management
3. Operational resilience testing
4. Management of ICT third-party risk

Information Sharing is encouraged but not mandatory

When: Enforceable Jan 17th,2025

Why: Support the Potential of digital finance in terms of innovation and competition while mitigating the risk arising from it.

Digital Operational Resilience Act (DORA)
Data Encryption and Protection

RTS Article 6 Encryption and cryptographic controls

2. (a) [...] rules for the encryption of data at rest, in transit and, where relevant, in use, taking into account the results of the approved data classification [...] If encryption of **data in use** is not possible, financial entities shall process data in use in a **separated and protected environment** [...]

b. [...] encryption of internal network connections and traffic with external parties [...]

Article 7 Cryptographic key management

1. [...] cryptographic key management policy [...] requirements for managing cryptographic keys through their whole lifecycle, including generating, storing, backing up, archiving, retrieving, transmission, retiring, revoking and destroying keys [...]

- Data encryption is required throughout the data lifecycle (at rest, in transit & in use).
- All networked traffic, internal and external is to be encrypted.
- Lifecycle management is required for cryptographic keys.

Protecting data is top of mind while adopting Hybrid Cloud

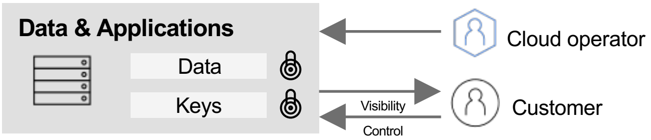
Public	Internal	Confidential	Sensitive
• Press releases, • Published annual reports • Social media feeds • Information on public record • Product/Pricing catalog	• Internal emails • Project documents • Training materials • 5 Organizational charts policy guides	• Employee pay stubs • Customer information • Personal contact information • Customer preferences • Credit card • Non-public contracts • NDA agreements offering roadmaps	• Government identification numbers • SSN • Driver's license • Financial transactions • Digital Assets • Information that could pose an identity threat

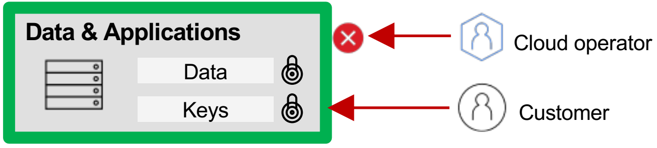
Operational assurance

"Cloud provider *will not* access your data & keys"

Technical assurance

"Cloud provider *cannot* access your data & keys"



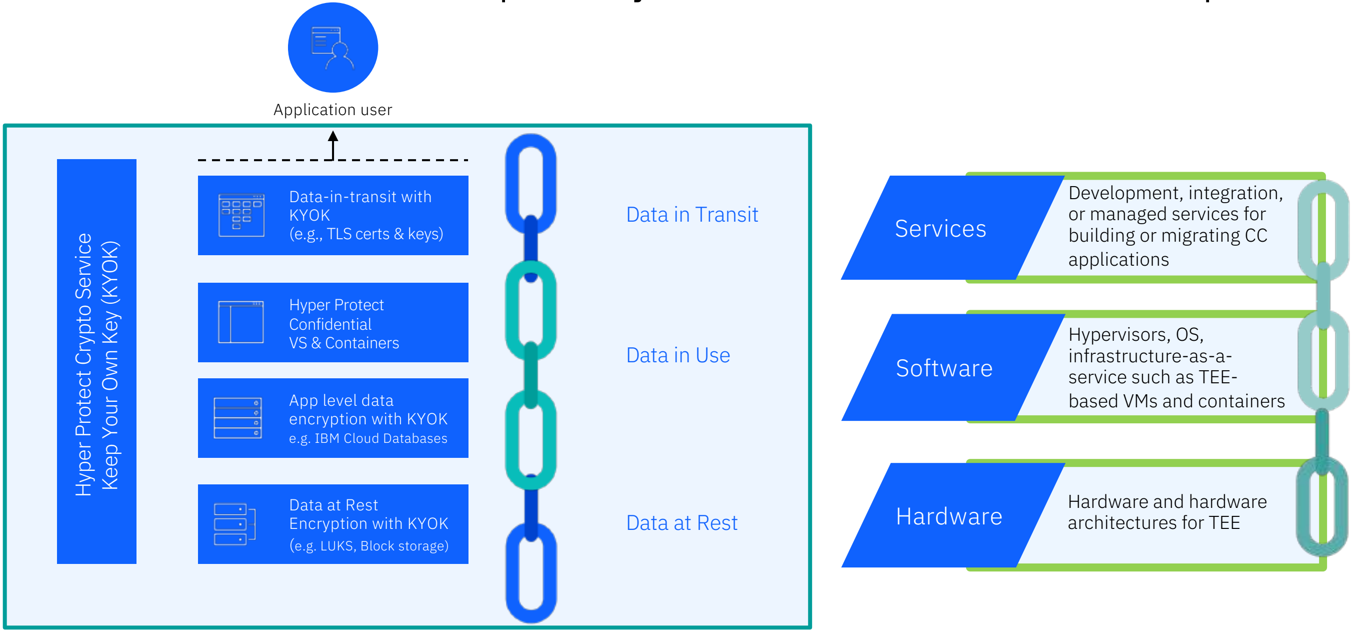


IBM Hyper Protect (IBM Secure Execution)

Operational Assurance
… someone will not

Technical Assurance
… someone can not

Protecting all states within the data Lifecyle leveraging technical assurance enables total privacy assurance for Cloud Adoption



Application user

Hyper Protect Crypto Service
Keep Your Own Key (KYOK)

Data-in-transit with KYOK
(e.g., TLS certs & keys)

Hyper Protect Confidential VS & Containers

App level data encryption with KYOK
e.g. IBM Cloud Databases

Data at Rest Encryption with KYOK
(e.g. LUKS, Block storage)

Data in Transit

Data in Use

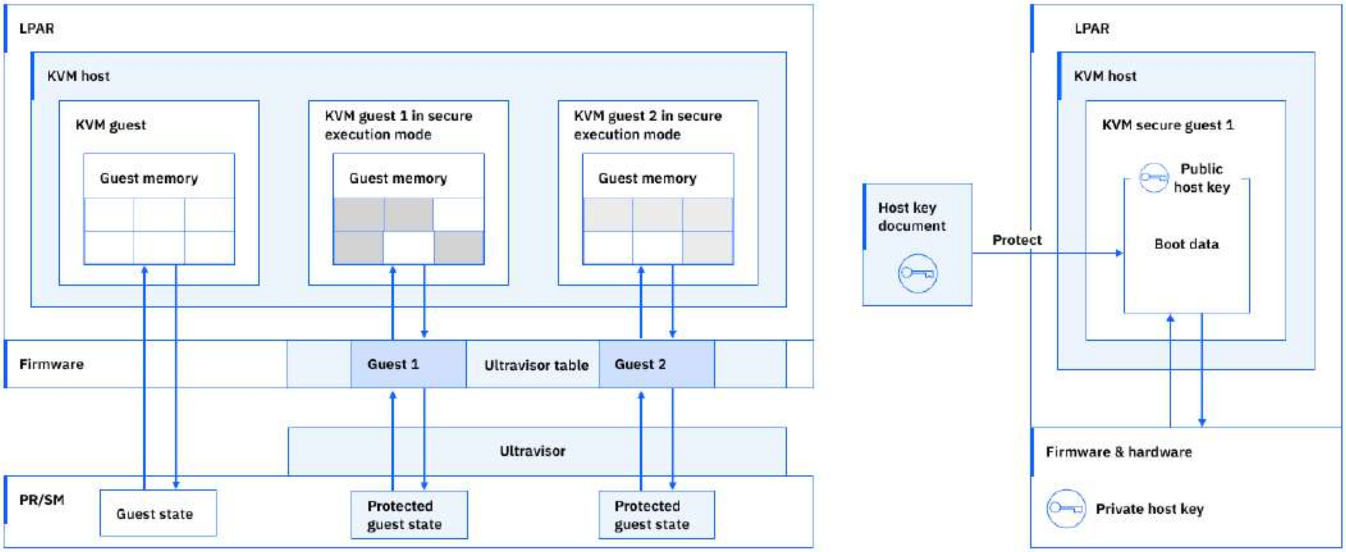
Data at Rest

Services: Development, integration, or managed services for building or migrating CC applications

Software: Hypervisors, OS, infrastructure-as-a-service such as TEE-based VMs and containers

Hardware: Hardware and hardware architectures for TEE

Roof of trust lies in hardware: IBM Secure Execution for Linux



https://www.ibm.com/docs/en/linux-on-systems?topic=virtualization-introducing-secure-execution-linux

Protect data-in-use

IBMs & Red Hats approach towards orchestrating Confidential Containers with Zero Trust

Existing Approach

The protection barrier is only up to the virtual machine.
Kubernetes Admin has access to data

Current state of Protection in Market Approach

- ○ K8s cluster need to be user-provisioned
- ○ K8s nodes in enclave
- ✓ protect against Pod breakout
- ✓ protect against Cloud Infrastructure

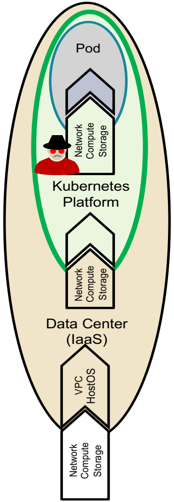
X NOT protected from K8S admin.

X NOT suitable for provider managed setups.
Kubernetes platform provider can gain Kubernetes Admin role and access to data.

X Worker node needs to be trusted!

OPENSHIFT

Available with OpenShift 4.12+ on s390x



Eliminating Attack Vectors with

The protection barrier is at the Pod Enclave, fully protecting the workload against malicious actors including the Kubernetes Admin

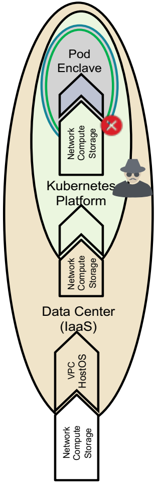
➔ K8s with IBM Hyper Protect
K8S clusters are provider managed
K8s pods/container in enclaves

- ✓ protect against Pod breakout
- ✓ protect against Cloud Infrastructure
- ✓ isolated from K8s admin
- ✓ Policy enforcement & Zero Knowledge proof through encrypted contract concept

Worker Node does not need to be trusted!

OPENSHIFT

Available soon with IBM Secure Execution for Linux on s390x



Operational assurance
"Kubernetes Admin **will not** access your data & keys"

Technical assurance
"Cloud provider & Kubernetes admin **cannot** access your data & keys"

UseCase: Banking Example

Example

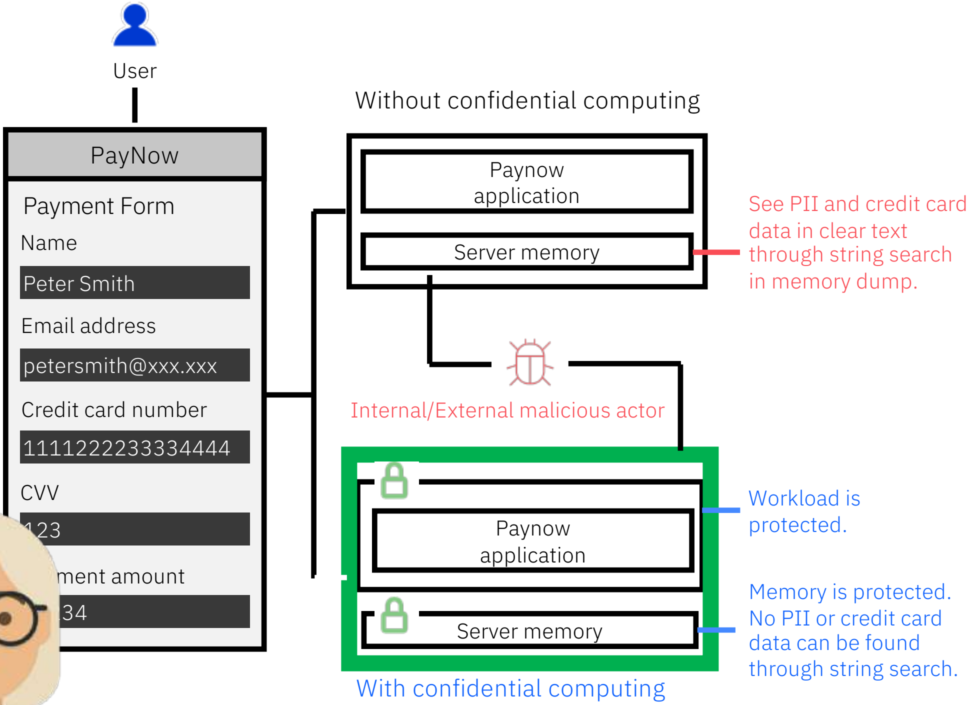
Confidential Compute made easy: One Application, no code change:

Without confidential computing:

- Root user can “dump” contents of the server memory and steal data.

With confidential computing:

- Even a root user cannot access th memory.
- Data in use is protected by Secure Execution and Hyper Protect Platform.

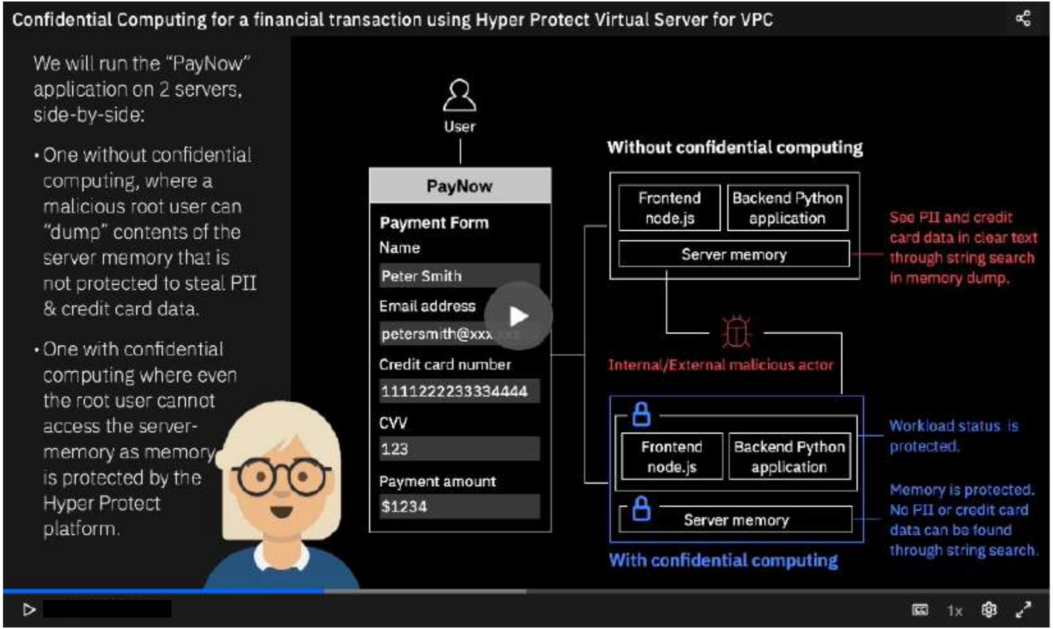


See PII and credit card data in clear text through string search in memory dump.

Workload is protected.

Memory is protected. No PII or credit card data can be found through string search.

See it in Action!



Confidential Computing for a financial transaction using Hyper Protect Virtual Server for VPC

We will run the "PayNow" application on 2 servers, side-by-side:

- One without confidential computing, where a malicious root user can "dump" contents of the server memory that is not protected to steal PII & credit card data.
- One with confidential computing where even the root user cannot access the server-memory as memory is protected by the Hyper Protect platform.

PayNow

Payment Form

Name: Peter Smith

Email address: petersmith@xxx

Credit card number: 1111222233334444

CVV: 123

Payment amount: $1234

See PII and credit card data in clear text through string search in memory dump.

Workload status is protected.

Memory is protected. No PII or credit card data can be found through string search.

User
Without confidential computing
Frontend node.js
Backend Python application
Server memory
Internal/External malicious actor
Frontend node.js
Backend Python application
Server memory
With confidential computing
1x

[redacted]

https://mediacenter.ibm.com/media/Confidential+Computing+for+a+financial+transaction+using+Hyper+Protect+Virtual+Server+for+VPC/1_vv3j2oo6

UseCase: Digital Assets

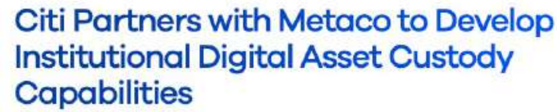
Institutional Digital Asset Custody, Trading and DeFi

One of the world's leading digital asset service providers leverages Confidential Compute (through IBM Hyper Protect Services, powered by LinuxONE) to create an embedded digital asset management solution in order to:

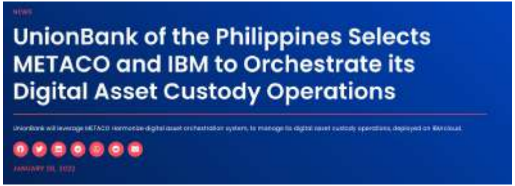
- Launch large-scale digital asset capabilities based on mission-critical custody infrastructure.
- Common components for hybrid deployments based on zSystems and IBM Cloud
- Leverage Confidential Computing for key vault and notary to ensure protection

IBM's Confidential Compute Services were able to achieve:

- Highly Secure Hosting Environment to protect your private keys, applications and data based on Technical Assurance
- Security-first solution design leveraging Privacy Protection Technologies like Confidential Computing and Zero Trust
- Cloud consumption model: pay for what you use & scale fast along with growing business
- Hardware Security Module as a Service with Keep-Your-Own-Key



Citi Partners with Metaco to Develop Institutional Digital Asset Custody Capabilities

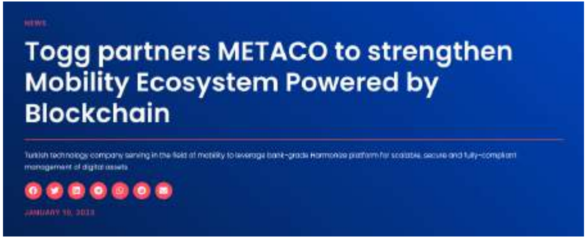


NEWS

UnionBank of the Philippines Selects METACO and IBM to Orchestrate its Digital Asset Custody Operations

UnionBank will leverage METACO Harmonize digital asset orchestration system, to manage its digital asset custody operations, deployed on IBM cloud.

JANUARY 18, 2022



NEWS

Togg partners METACO to strengthen Mobility Ecosystem Powered by Blockchain

Turkish technology company serving in the field of mobility to leverage bank-grade Harmonize platform for scalable, secure and fully-compliant management of digital assets

JANUARY 10, 2023

UseCase: Printing & Output Management

Secure Hybrid Cloud Printing to ensure Financial Services Business Continuity

"It's impressive what level of security we can achieve with a cloud solution by using IBM Hyper Protect Services. We can deliver our cloud service to our customers safe in the knowledge that their data is fully protected throughout the entire application lifecycle."
- Thomas Tikwinski, CTO

100%
Zero Trust Principles
Delivers complete protection and data security throughout the entire application lifecycle with confidential computing features.

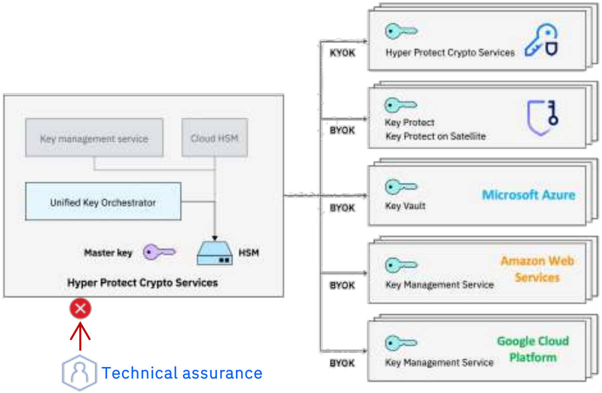
Data-in-use
Protection ensures, neither the Cloud Provider nor the Service Provider has the ability to see or modify confidential data to be printed – allowing Confidential Output Management aaS & preparing for DORA

SEALSYSTEMS
ENTERPRISE OUTPUT SOLUTIONS

UseCase: Secure & Sovereign Cloud Key Management

Building a Key Management Solution for the Banking & Public Sector by leveraging Confidential Compute

Confidential Compute allows the IBM Hyper Protect Team to build a secure Key Management Solution as a Service ("Unified Key Orchestrator") for compliance



Keep control over your Keys by leveraging the highest level of Security - not even IBM Admins could access client keys

Allows to stay worry free with an all-in aaS Key Management Solution

Creating a central backup to redistribute & rotate keys to quickly recover from loss & minimize security threats – without being able to access Key's but leveraging HA & DR of the hybrid Cloud

Contact us!

andrea.corbelli@it.ibm.com
louisa.muschal@ibm.com