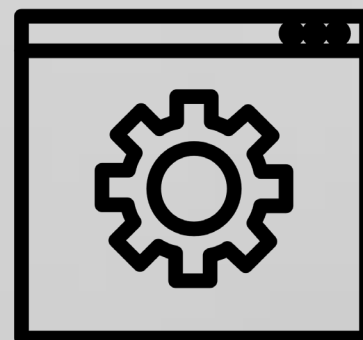
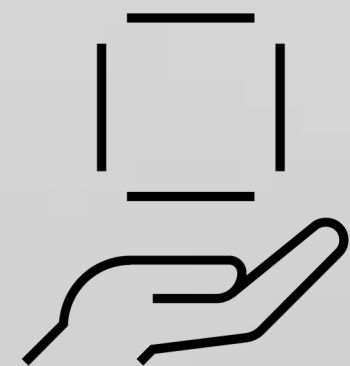


Confidential Computing for today's Security needs

Achieving total data privacy assurance
with Secure Execution for Linux
on IBM® LinuxONE and Linux on
zSystems



Stefan Liesche
IBM Distinguished Engineer
IBM Hybrid Cloud and Hyper Protect Services
zSystems



IBM® LinuxONE Rockhopper 4 and Linux on z16 A02/AGZ

Helping you turn your sustainability strategy into action

Build privacy and protection with a cyber-resilient system

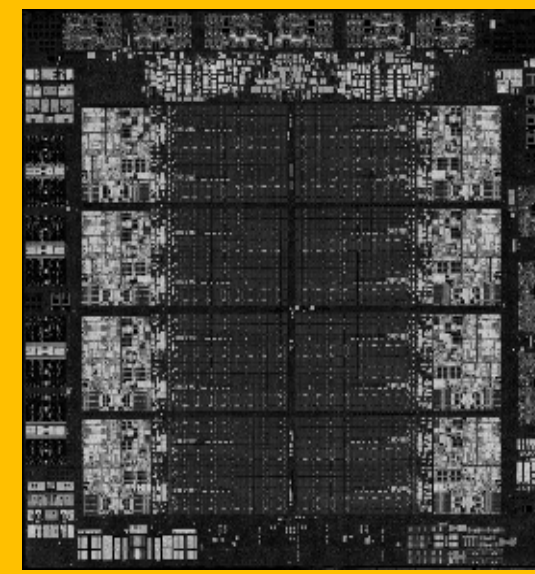
- **Quantum-safe** to protect data, workloads and infrastructure now and in the future
- **Confidential computing** to protect data in-use
- **Pervasive encryption** to protect data at-rest and in-flight
- **Simplified compliance** to improve audit readiness



IBM® LinuxONE Rockhopper 4 systems, with GDPS, IBM DS8000 series with HyperSwap and running a Red Hat OpenShift Container Platform environment, are designed to deliver **99.99999%** availability

One system, 1-68 cores, up to 16TB,
Factory frame or Rack mounted

DISCLAIMER: IBM internal data based on measurements and projections was used in calculating the expected value. Necessary components include IBM LinuxONE Emperor 4; IBM z/VM V7.2 systems collected in a Single System Image, each running RHOC 4.10 or above; IBM Operations Manager; GDPS 4.5 for management of data recovery and virtual machine recovery across metro distance systems and storage, including Metro Multi-site workload and GDPS Global; and IBM DS8000 series storage with IBM HyperSwap. A MongoDB v4.2 workload was used. Necessary resiliency technology must be enabled, including z/VM Single System Image clustering, GDPS xDR Proxy for z/VM, and Red Hat OpenShift Data Foundation (ODF) 4.10 for management of local storage devices. Application-induced outages are not included in the above measurements. Other configurations (hardware or software) may provide different availability characteristics.



LinuxONE and Linux on zSystems

In multi-workload environments data can be visible to administrators and vulnerable to attack

- ⚠ Malicious insiders
- ⚠ Compromised credentials
- ⚠ Privilege Escalation

Hardware-based security for confidential computing

Technically enforced isolation of workloads at massive scale with secure execution

Delivers data integrity by protecting data at rest, in flight and in use

Administrators can still perform their role but do not have data access

Mitigating the impacts of cyber attacks

\$4.35M

the average cost of a data breach according to an IBM report in July 2022

83%

of organizations studied have had more than one security breach

81%

of executives consider security a brand attribute that differentiates their organization

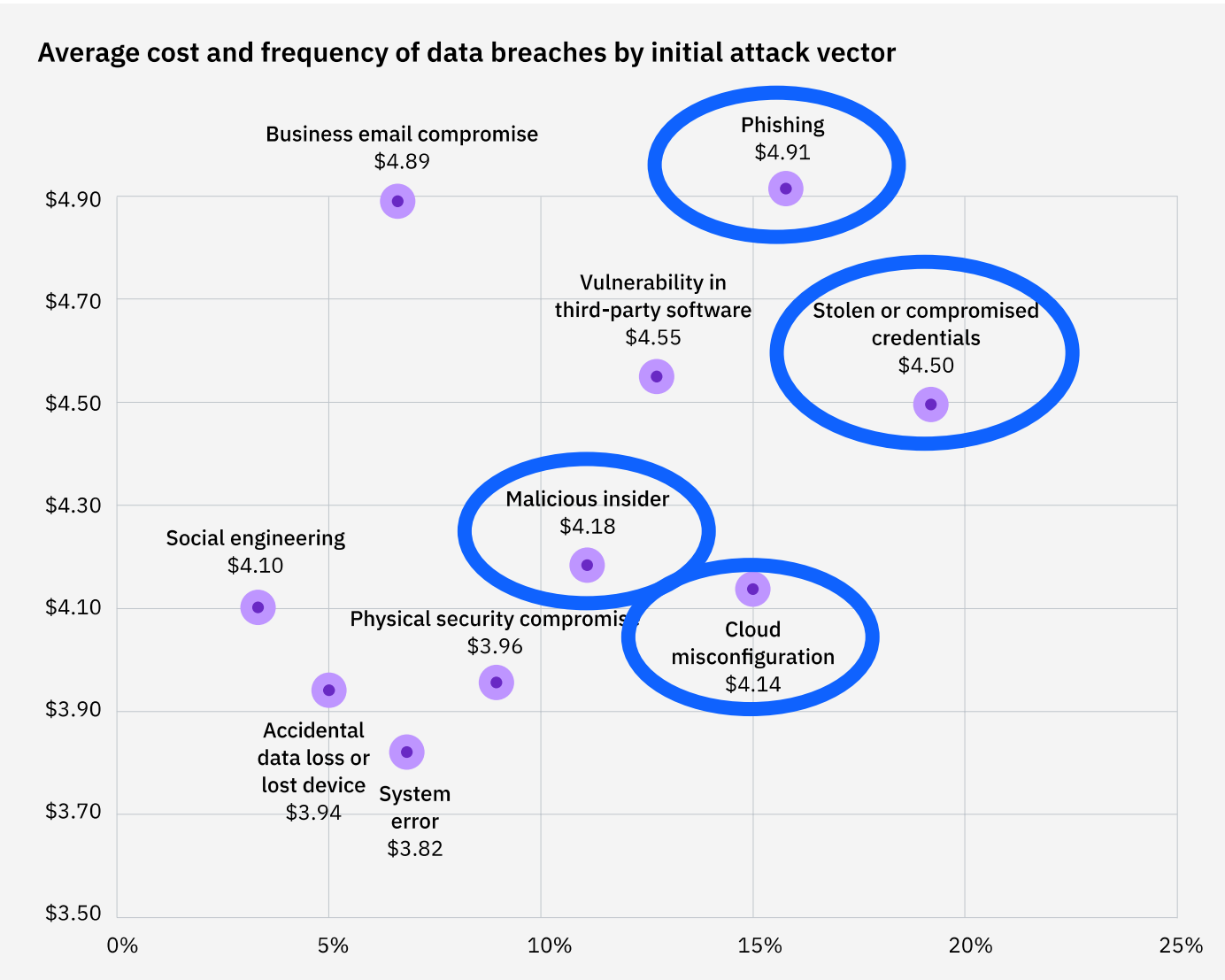


Figure 11: Measured in USD millions

Average time to identify and contain a data breach by initial attack vector

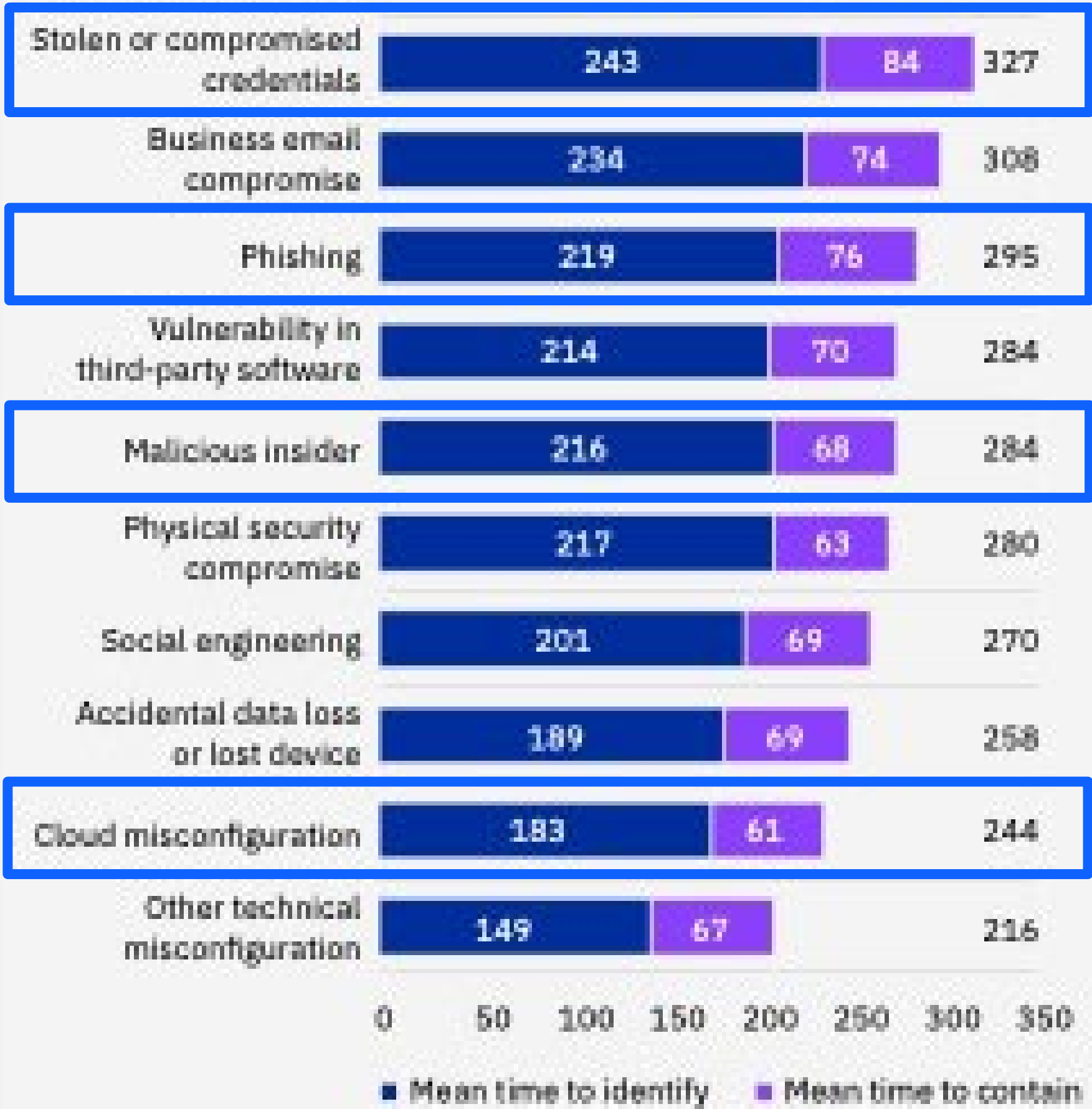
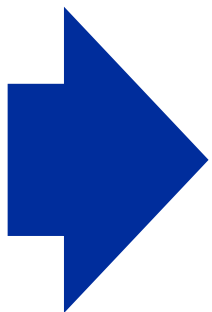


Figure 12: Measured in days

Data in the Hybrid Cloud – Market Trends

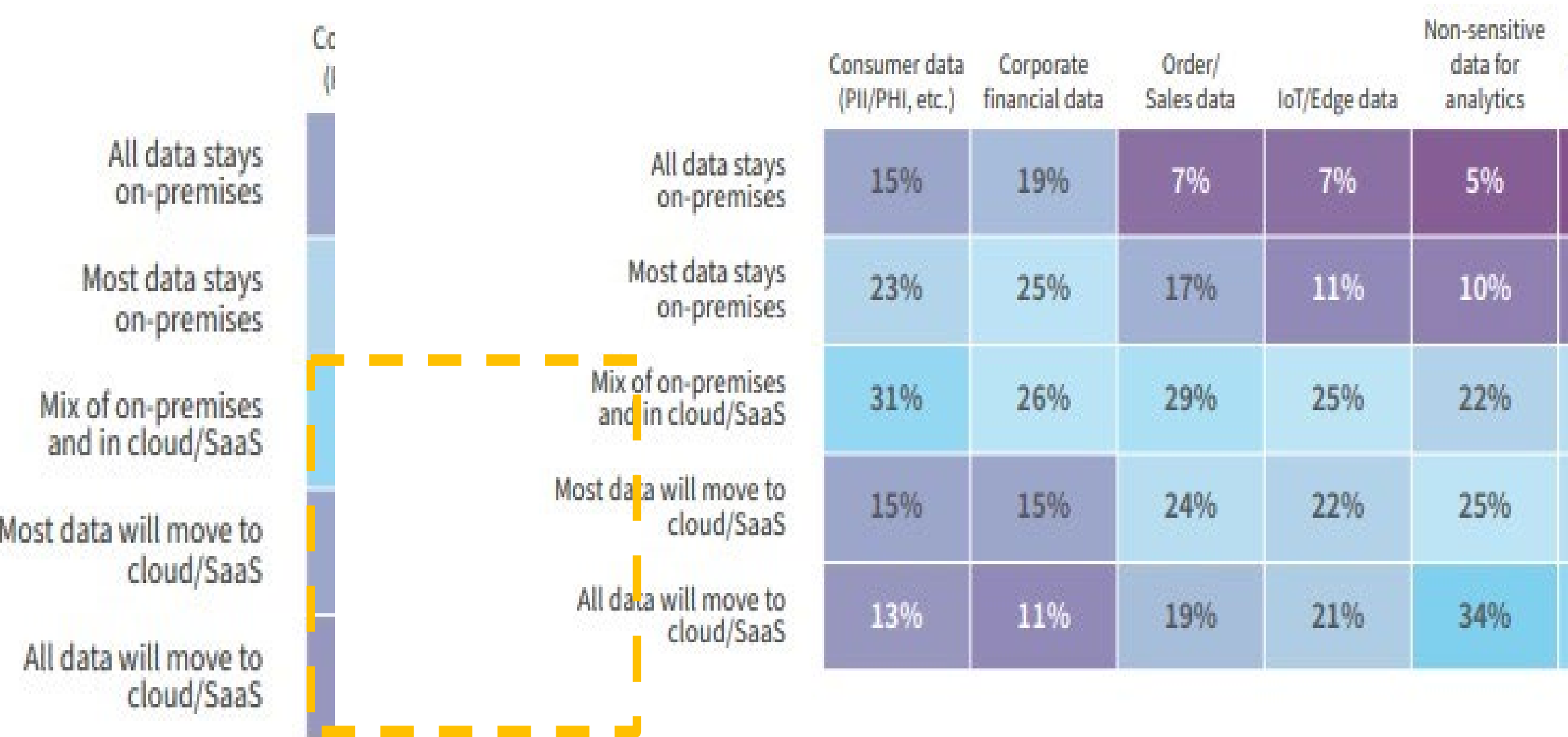
Security of processing through Encryption of personal and sensitive data

Sensitive	Confidential	Internal	Public
<ul style="list-style-type: none">SSNDriver's licenseFinancial transactionsDigital Assets	<ul style="list-style-type: none">Employee pay stubsCustomer PIICredit card information	<ul style="list-style-type: none">Internal emailsProject documentsOrganizational charts policy guides	<ul style="list-style-type: none">Press releases,Published annual reportsSocial media feeds



As countries and supranational unions tighten the requirements and regulation for data privacy and sovereignty

According to Flexera, More than half the enterprises they polled are planning to move sensitive data to the cloud



N=753
Source: Flexera 2022 State of the Cloud Report

GDPR Chapter 4 - Art. 32

Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- the pseudonymisation and encryption of personal data;
 - the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- [...]

Source: https://www.dsgvo-portal.de/gdpr_article_32.php

The New Swiss Federal Act on Data Protection – the nFADP – introduces changes that better align with the [GDPR](#). Switzerland is implementing new legislation to better protect its citizens' data. Swiss companies will have to comply with this legislation from September 1, 2023.



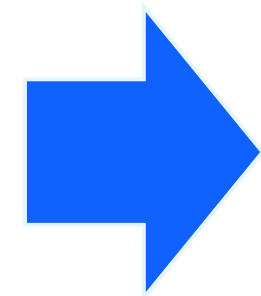
“One of the ways organizations can achieve privacy by design is through pseudonymization. This process involves adding encryption or replacing personal data with artificial identifiers to limit access to only authorized users.”

<https://www.kmu.admin.ch/kmu/en/home/facts-and-trends/digitization/data-protection/new-federal-act-on-data-protection-nfadb.html>

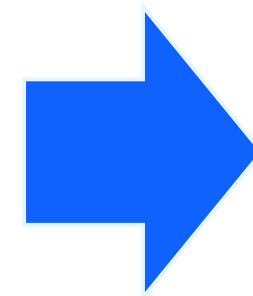
Looking for the right infrastructure “recipe”

As enterprises continue to adopt a hybrid cloud infrastructure, security remains one of their top challenges.

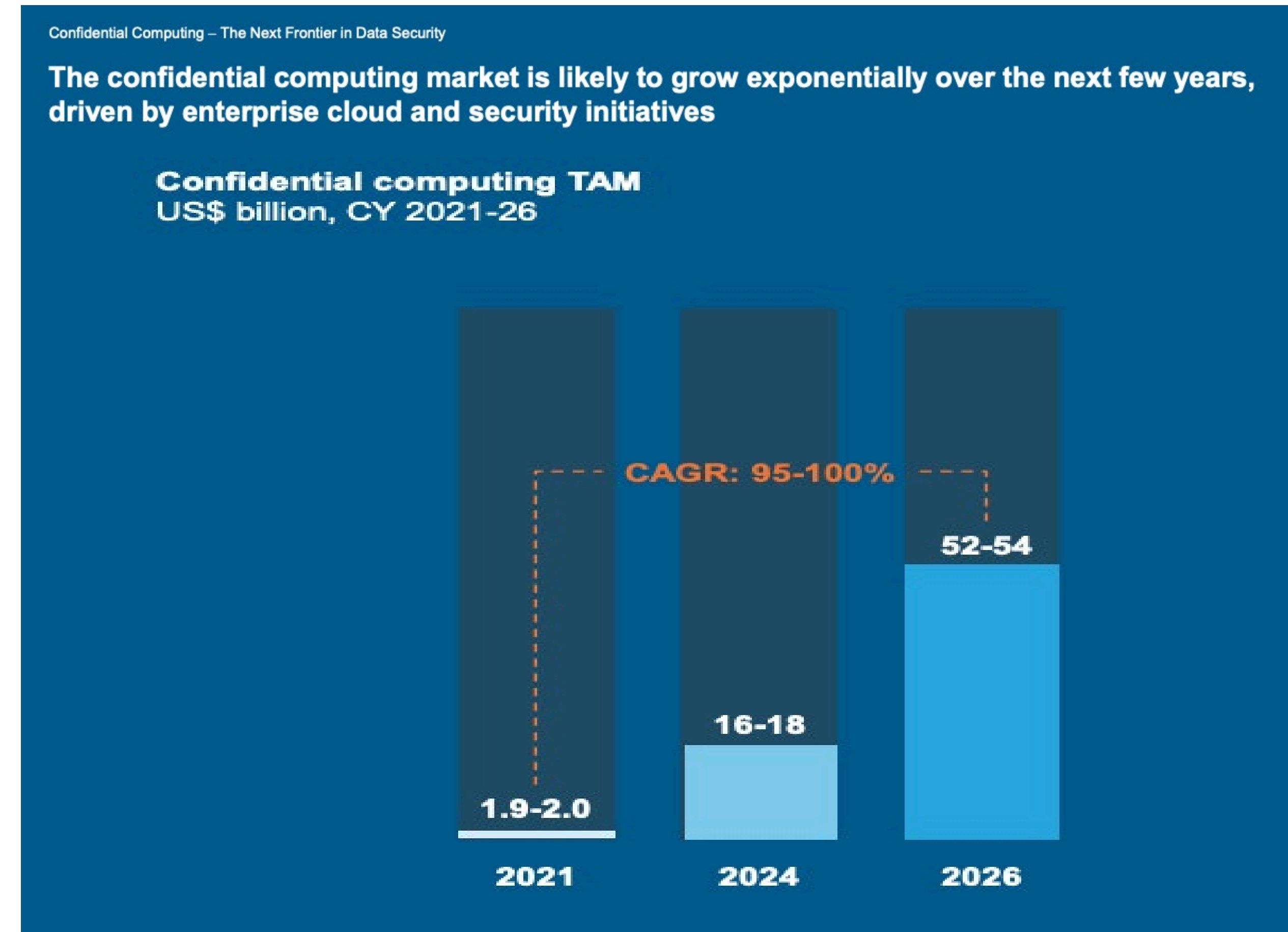
Data privacy and data sovereignty are top of mind when clients look to adopt hybrid cloud



Determining the appropriate **security strategy** is critical

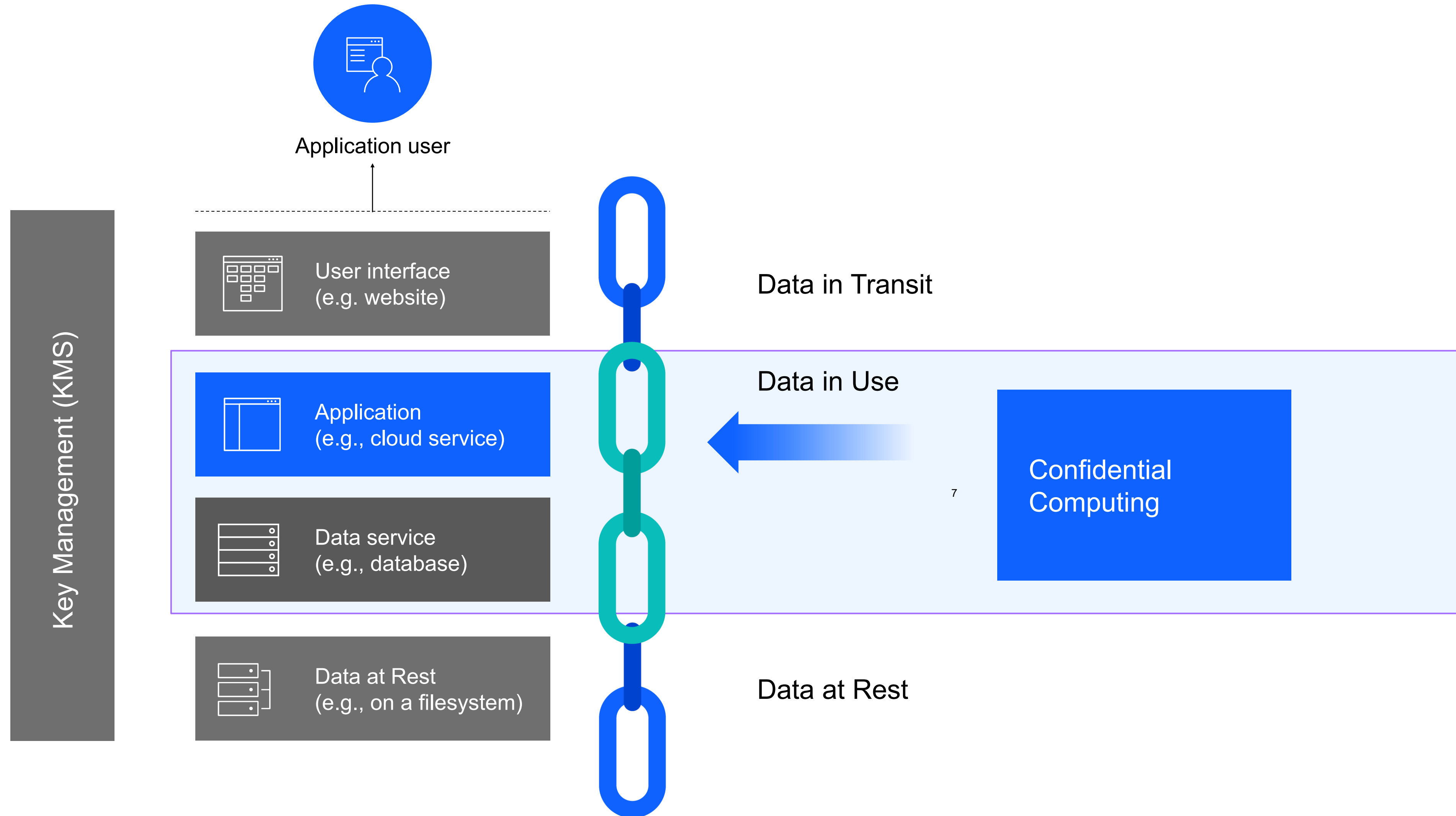


Confidential Computing technologies on-prem and in the cloud can help!

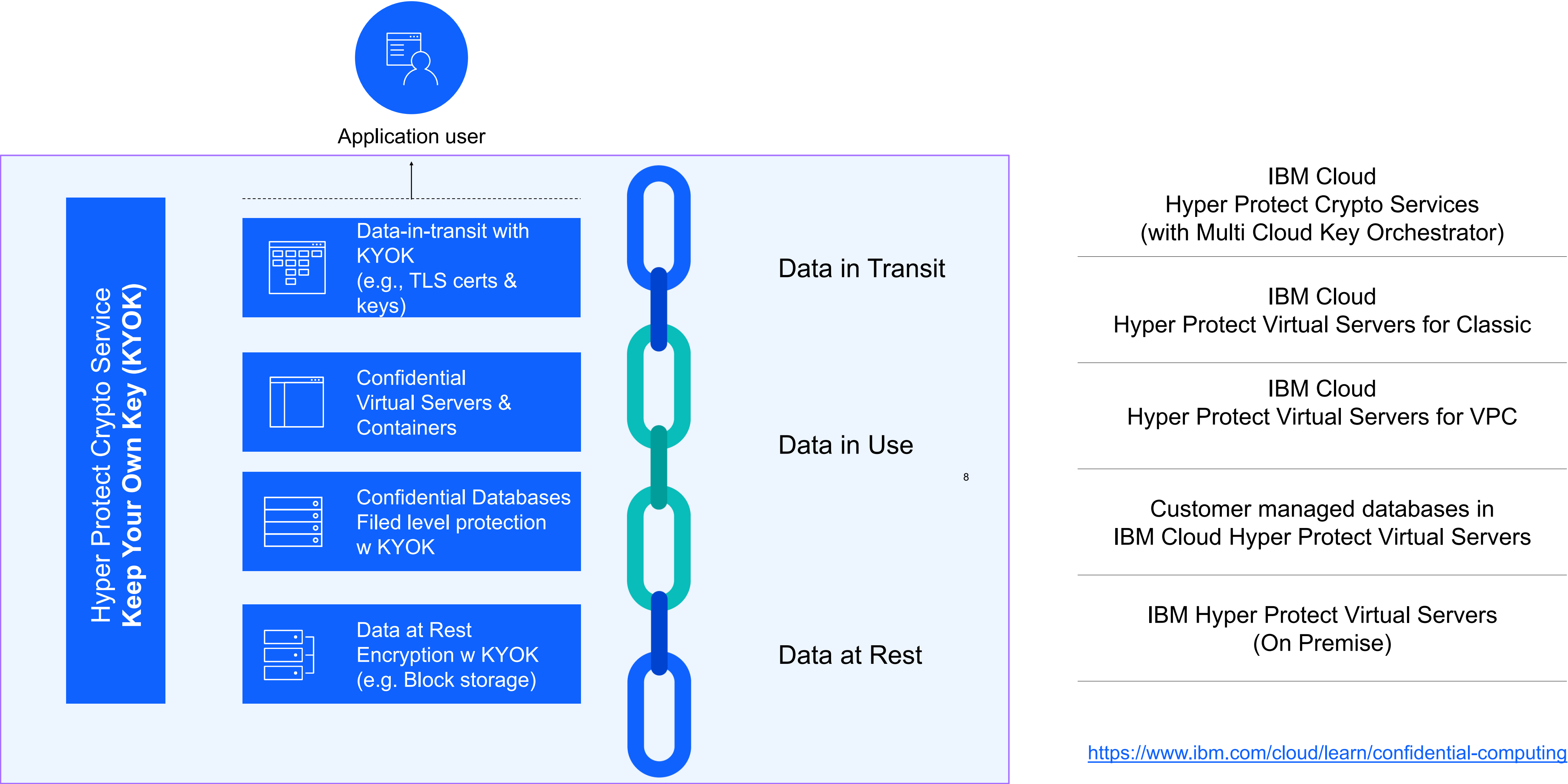


Confidential Computing Consortium [Research Study](#)

Confidential Computing is about 'Data in Use'



Confidential computing enables total privacy assurance



Confidential Computing

IBM Cloud Hyper Protect Services

powered by Secure Execution for Linux

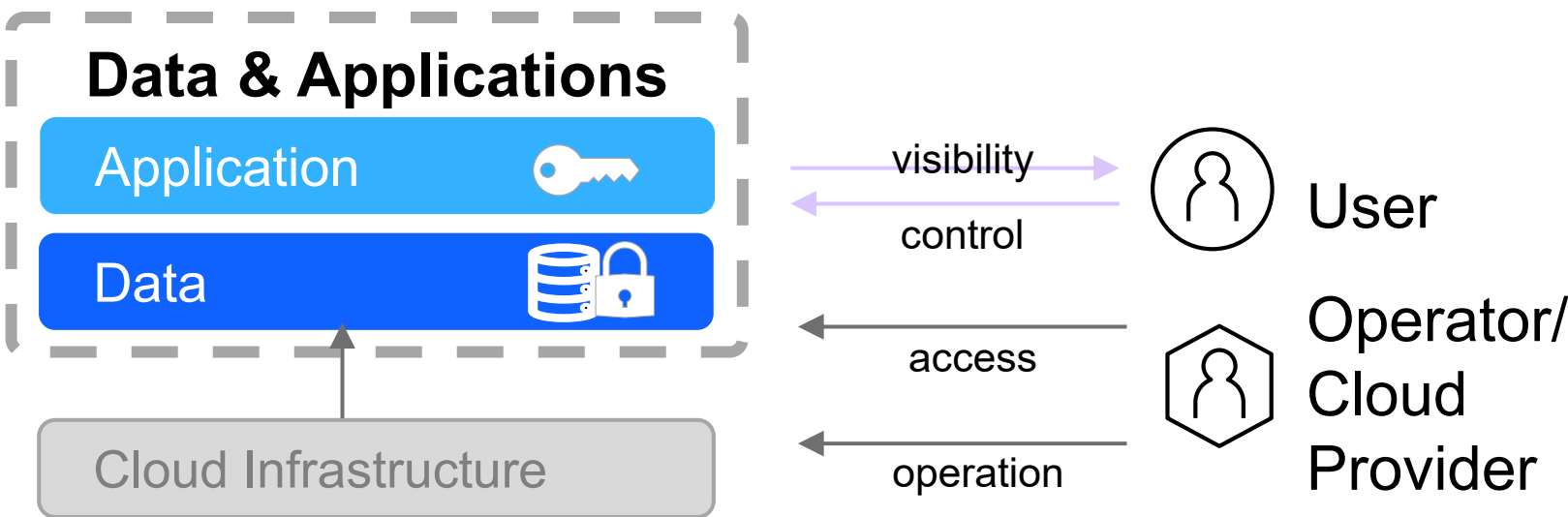
Operational assurance

“Administrators and Operators *will not* access your data & keys”

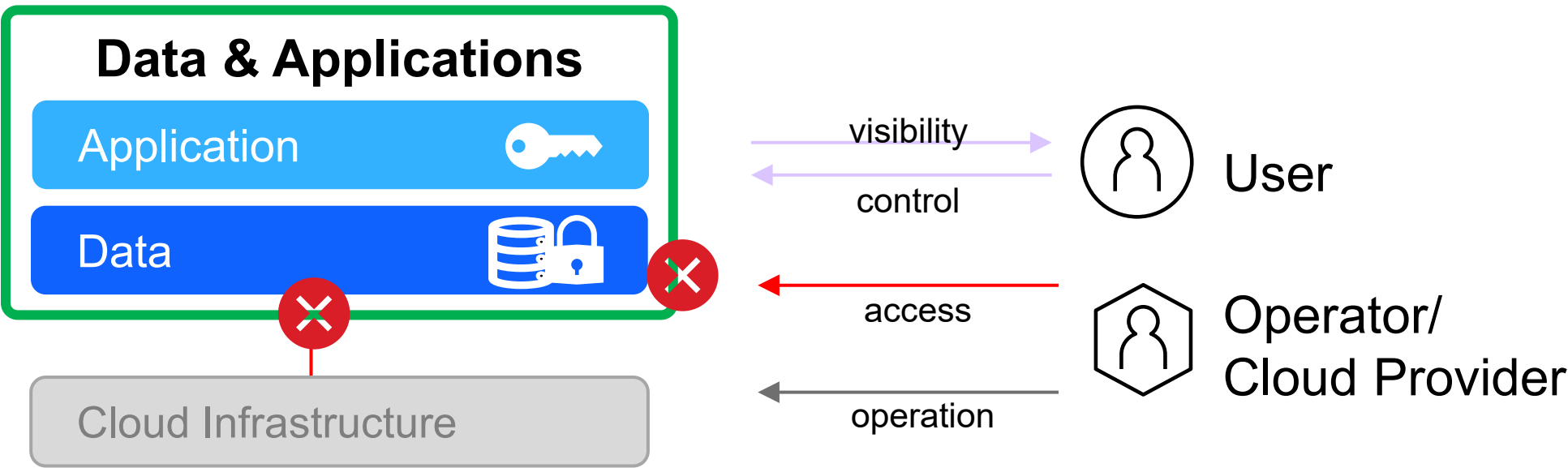
Technical assurance

“Administrators and Operators *cannot* access your data & keys”

Application Execution Environment

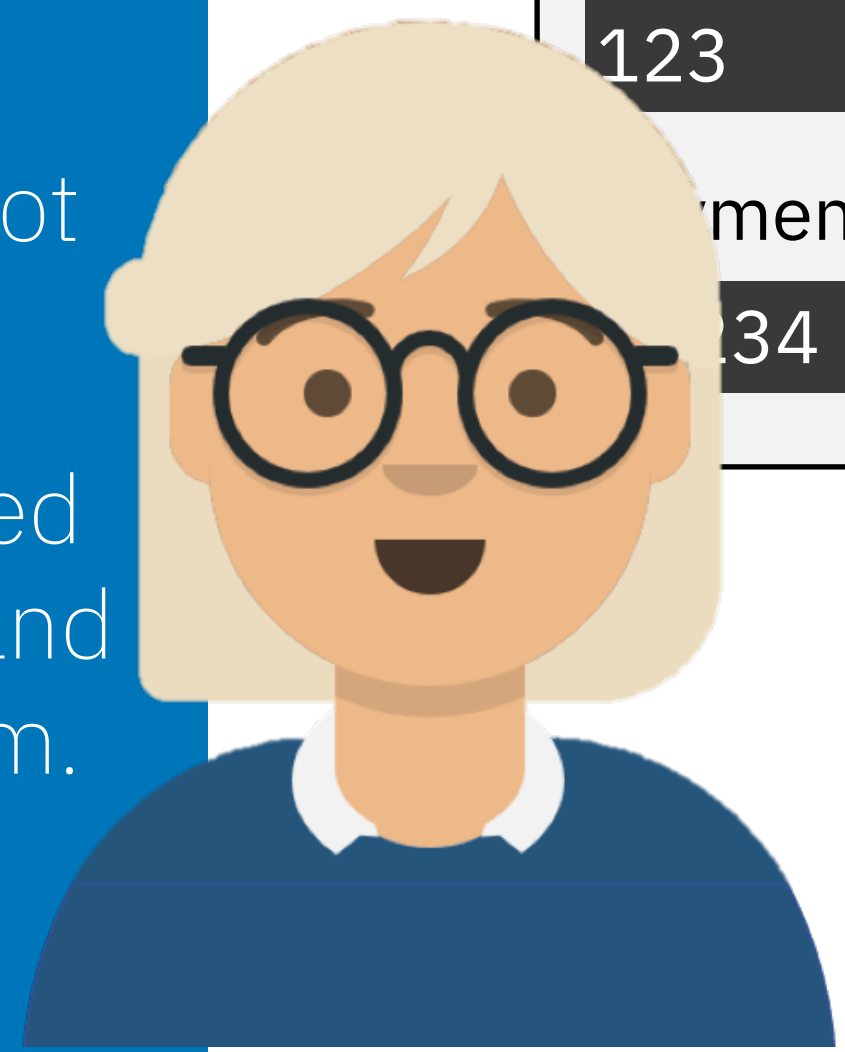


Confidential Computing (Secure Execution)



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 the memory.
 - Data in use is protected by secure execution and Hyper Protect Platform.



User

PayNow

Payment Form

Name

Peter Smith

Email address

petersmith@xxx.xxx

Credit card number

1111222233334444

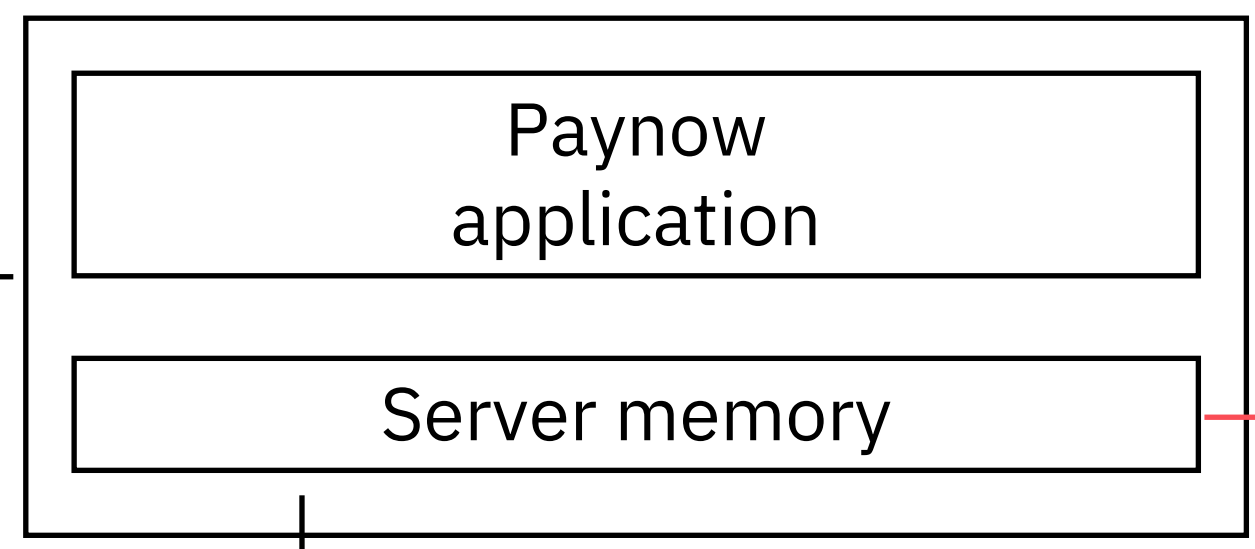
CVV

123

Payment amount

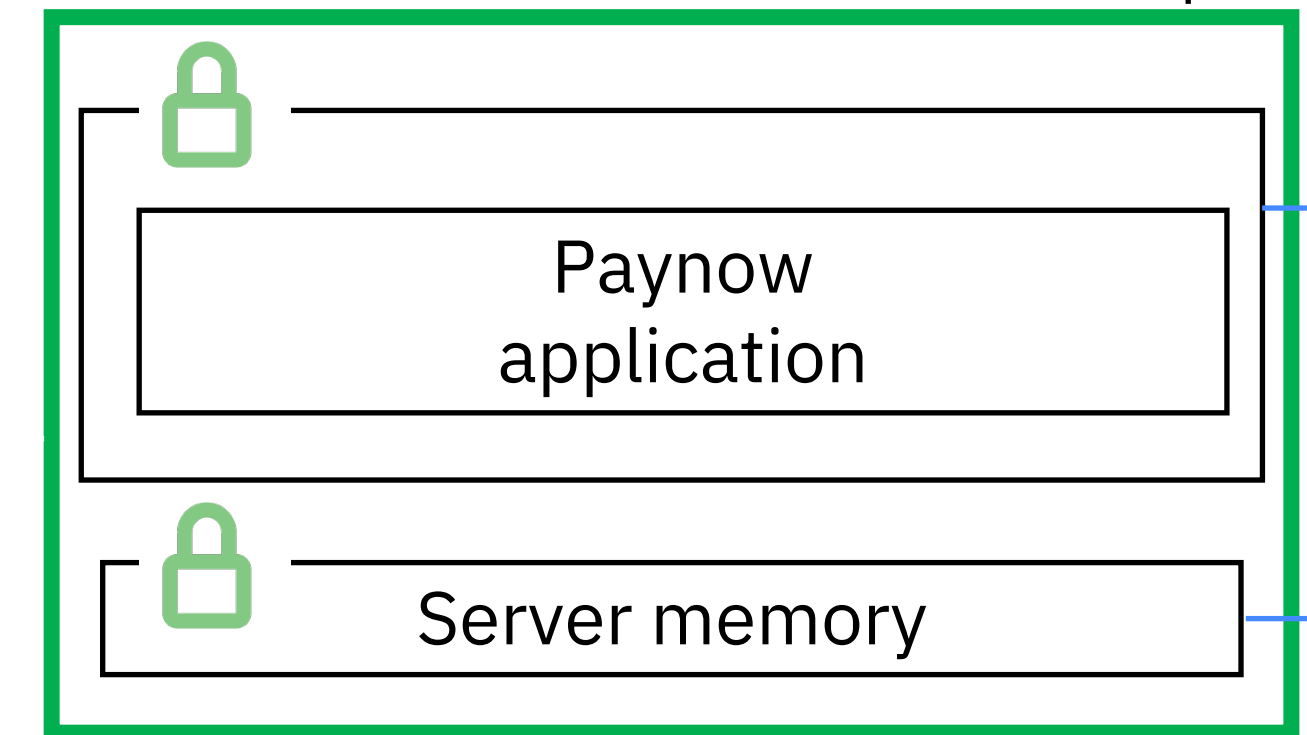
34

Without confidential computing



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

Internal/External malicious actor



With confidential computing

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

Go deeper and experience *the live running demo*, ask your questions and see it right here today!!!

What about other PETs?

Privacy-enhancing technologies (PET)

are technologies that embody fundamental data protection principles by minimizing personal data use, maximizing data security, and empowering individuals. ... PETs use techniques to minimize possession of personal data without losing the functionality of an information system.*

Wikipedia:

*https://en.wikipedia.org/wiki/Privacy-enhancing_technologies

	Virtualization	Fully Homomorphic Encryption (FHE)	Multi Party Computation (MPC)	Confidential Computing
Hardware agnostic feature (CPU)	✓	✓	✓	✗
General Use (any Computation)	✓	✗	✗	✓
Comparable Performance	✓	✗	implementation	✓
Data Confidentiality	✗	✓	✓	✓
Workload Confidentiality	✗	✗	✗	✓
Verifiable (Attestation)	✗	✗	✗	✓
Data Integrity	✗	✗	✗	implementation
Workload Integrity	✗	✗	✗	optional

**inspired by Mike Bursell, CEO & co-founder, Profian, “Confidential Computing and Privacy-Enhancing Technologies - the Landscape”

Top Use Case Examples for Confidential Computing

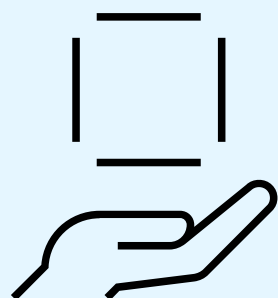


Hyper Protect Services maintain the confidentiality and integrity of your data, digital assets or intellectual property



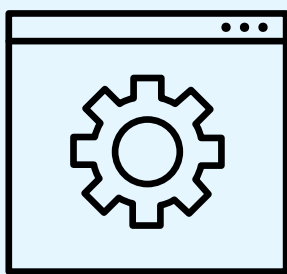
Secure Containerized Workloads

containerising applications within a Hyper Protect Confidential Computing environment ensures that your applications are always protected.



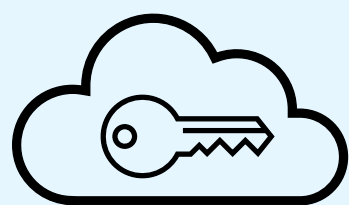
Digital Assets

the trusted platform for digital custody solutions, for storing and transferring high value digital assets in highly secure wallets, reliable at scale.



Secure Multi Party Collaboration (SMPC)

enabling distributed SMPC, where participants are ensured their data and insights are protect even when being calculated outside their direct control.



Exclusive Control of Data and Keys (KYOK)

Mitigate risk of data loss and meet regulatory requirements



Quantum-Safe Cryptography

technology for a new cryptographic era supporting NIST selected IBM co-developed quantum-safe algorithms

Top Use Case Examples for Confidential Computing

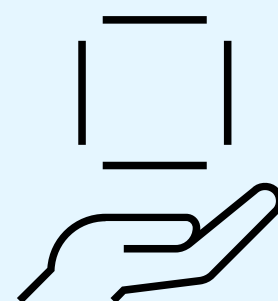


Hyper Protect Services maintain the confidentiality and integrity of your data, digital assets or intellectual property



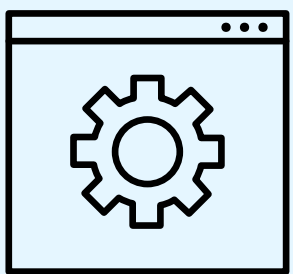
Secure Containerized Workloads

containerising applications within a Hyper Protect Confidential Computing environment ensures that your applications are always protected.



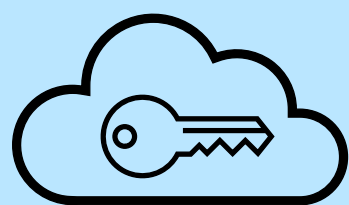
Digital Assets

the trusted platform for digital custody solutions, for storing and transferring high value digital assets in highly secure wallets, reliable at scale.



Secure Multi Party Collaboration (SMPC)

enabling distributed SMPC, where participants are ensured their data and insights are protect even when being calculated outside their direct control.



Exclusive Control of Data and Keys (KYOK)

Mitigate risk of data loss and meet regulatory requirements



Quantum-Safe Cryptography

technology for a new cryptographic era supporting NIST selected IBM co-developed quantum-safe algorithms

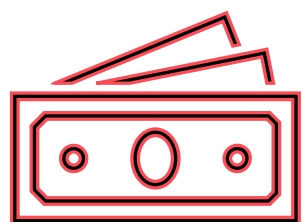
IBM Cloud Hyper Protect Crypto Services

De-Risk with the highest possible level of Security

Client Pain Points

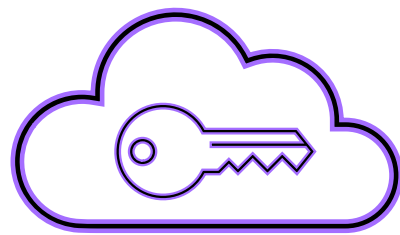


- **Data Security & Compliance** requirements for sensitive data



- **Lack of skill & high costs** to manage HSMs and maintain security posture

Outcomes with HPCS



- **Industry-leading data protection** through **exclusive encryption key control**, even IBM Cloud admins have no access

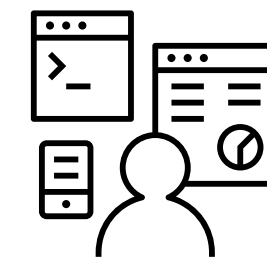


- **Reduced operational complexity** from IBM Cloud managed HSM
- As a Service solution with **consumption-based costs**

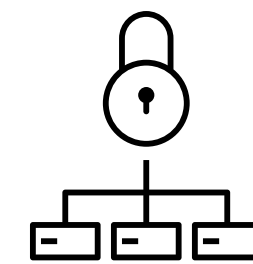
Customer Value	Exclusive encryption key control	Managed HSM	Simplified Key Lifecycle Management	Datacenter Availability
Benefits	<ul style="list-style-type: none">• Even IBM Cloud admins do not have access• Built on industry-leading security: FIPS 140-2 Level 4 certified HSM, customer control of HSM	<ul style="list-style-type: none">• IBM provisions, monitors and manages HA and Backup* <p>* Master key is not backed up</p>	<ul style="list-style-type: none">• Create, import, rotate, delete, audit keys• Support for industry standards like PKCS #11• Integration with IBM Cloud Services for access management (IAM), logging and monitoring,	<ul style="list-style-type: none">• NA: Dallas, Washington D.C, Toronto• Germany: Frankfurt• UK: London• Brazil: Sao Paulo• Australia: Sydney• Japan: Tokyo

Application development with IBM Cloud Hyper Protect Crypto Services and GREP11 onPrem

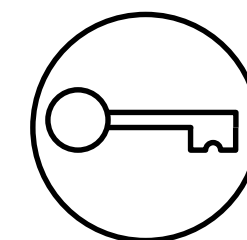
Developers can use both **quantum-safe** and **classical cryptography** to build new applications or modernize existing ones in the cloud and on-premises.



Leverage the stateless **Enterprise PKCS#11 provider** to code your applications for quantum-safe digital signature generation.



Built on **FIPS 140-2 Level 4 certified HSM** hardware, your keys are protected on IBM Cloud with the highest security level for cloud-based HSMs



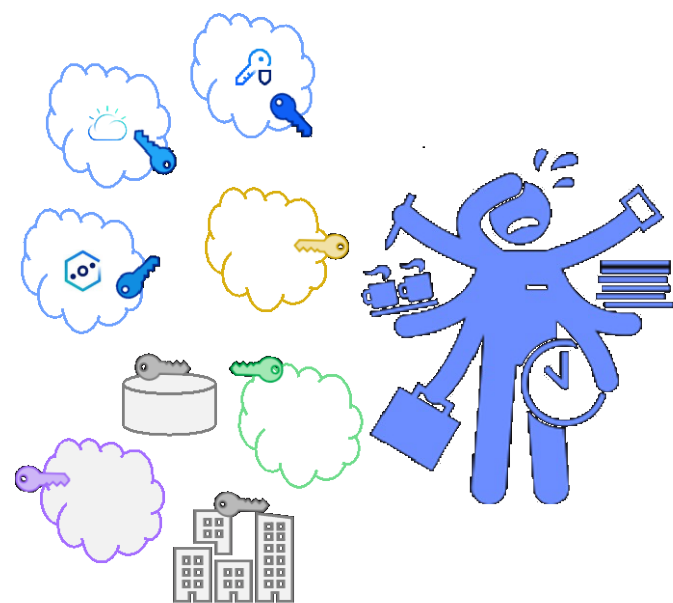
Own the root trust for all your key hierarchy with your own master key established through IBM's unique '**Keep Your Own Key**' (KYOK) technology

Unified Key Orchestrator in Hyper Protect Crypto Services

Simplify key management in a hybrid, multi-cloud setup

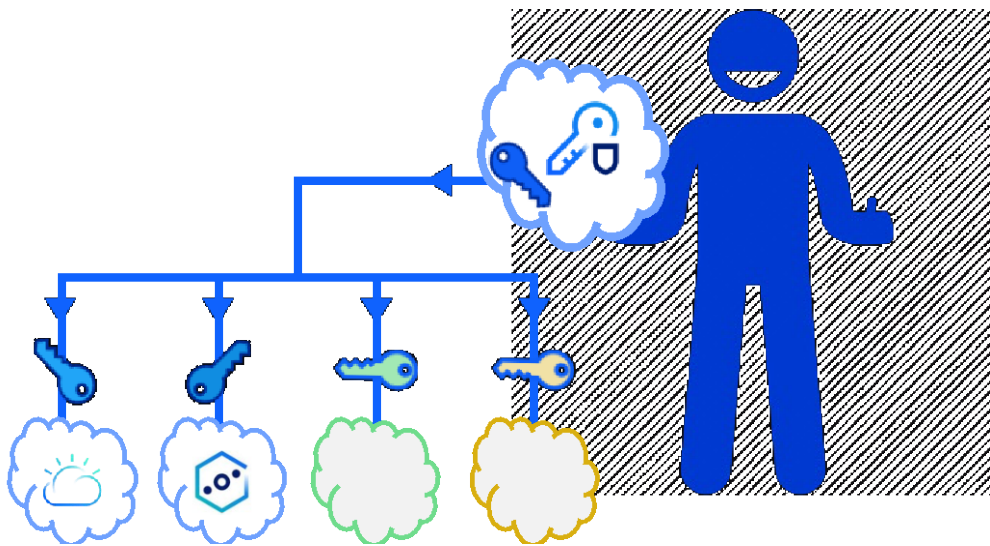
Customer Challenge

IT estate across multiple public clouds, private cloud and/or on-premise introduces **significant complexity and risk** in maintaining multiple key management tools, logins, and security postures



Outcome with UKO

Simplify to one control point in IBM Cloud with Unified Key Orchestrator



Customer Value	Multi-cloud key management as a service	Orchestrate keys across multi-cloud	Centrally backup all enterprise keys	Automate enterprise key operations
Benefits	Manage keys in IBM Key Protect, Azure Key Vault, Amazon KMS, GCP (New!)	Single point of control from IBM Cloud	Redistribute keys to quickly recover from fatal cloud errors	Simplify operations and free up time to focus on other tasks



Landesbank Baden-Württemberg



German federal Bank is enhancing control & security to reduce risk while enhancing operational ease with managing Key through Unified Key Orchestrator for Azure & O365

Business Problem:

Client project for implementation & roll-out of Office 365 was stopped due to the fact, that the Data Privacy Officer needed an adequate level of Data Protection through customer managed keys in Azure. But hosting an own HSM + Key Management System was too complex and costly – an easier but secure solution was needed.

Solution:

Hyper Protect Crypto Service with Unified Key Orchestrator: A single tenant cloud HSM with FIPS 140-2 Level 4 Certification combined with a single pane of glass Key management UI for multicloud

Business Value:

Unified Key Orchestrator with HPCS enables the client to use a cloud HSM with the highest level of security as well as the ease of use of a cloud native solution. This saves costs, eases operational burdens & enabled the cloud adoption, driving innovation.

Solution Components:

IBM Hyper Protect Crypto Service with Unified Key Orchestrator



[IBM Cloud Press Release](#)

Top Use Case Examples for Confidential Computing

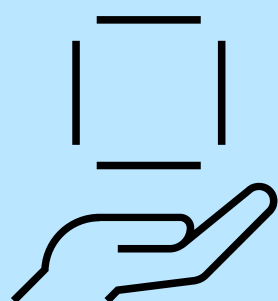


Hyper Protect Services maintain the confidentiality and integrity of your data, digital assets or intellectual property



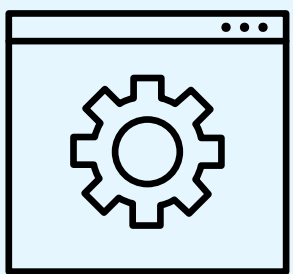
Secure Containerized Workloads

containerising applications within a Hyper Protect Confidential Computing environment ensures that your applications are always protected.



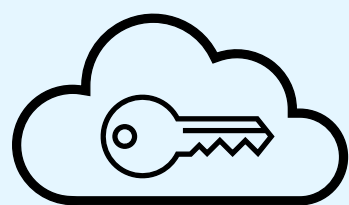
Digital Assets

the trusted platform for digital custody solutions, for storing and transferring high value digital assets in highly secure wallets, reliable at scale.



Secure Multi Party Collaboration (SMPC)

enabling distributed SMPC, where participants are ensured their data and insights are protect even when being calculated outside their direct control.



Exclusive Control of Data and Keys (KYOK)

Mitigate risk of data loss and meet regulatory requirements



Quantum-Safe Cryptography

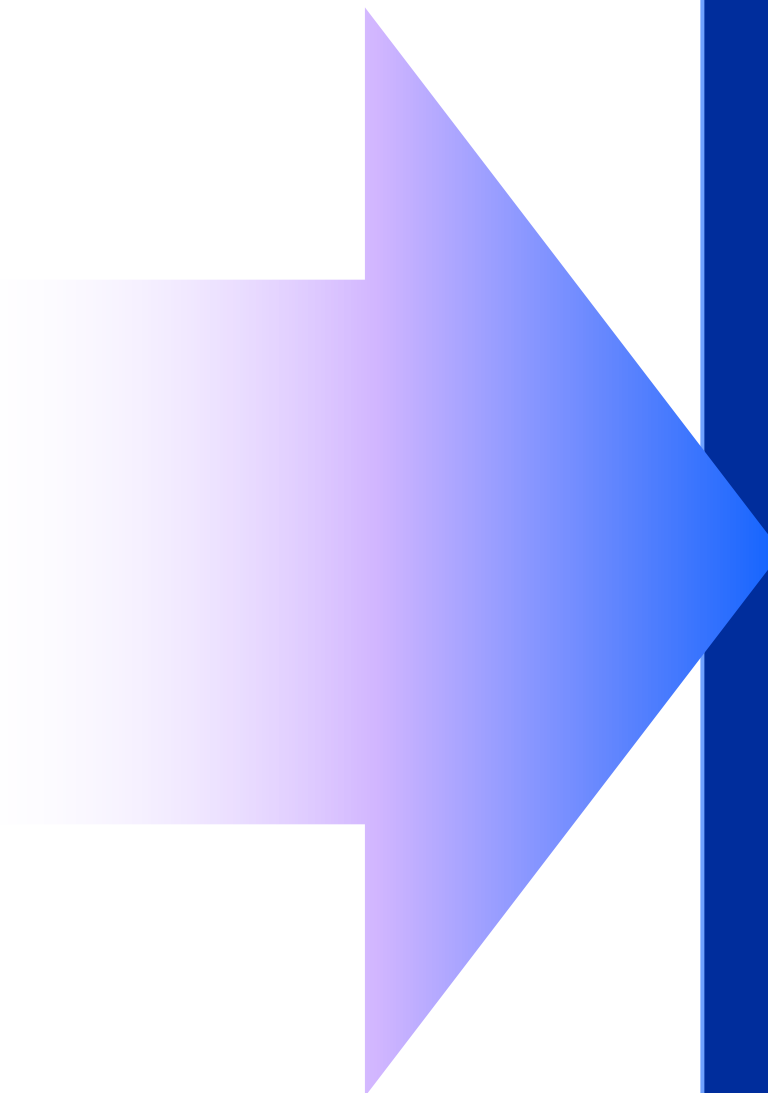
technology for a new cryptographic era supporting NIST selected IBM co-developed quantum-safe algorithms

What are digital assets?

Digital assets are a basket of different asset classes enabled by a common technology, cryptographically secured on a distributed ledger technology (DLT).

Examples:

- Cryptocurrencies
 - decentralized
 - CBDC
- Stablecoins
- Tokenized assets
- Non fungible tokens (NFTs)
- ...

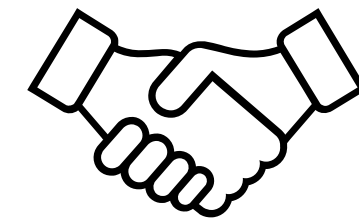


Why banks need digital asset custody

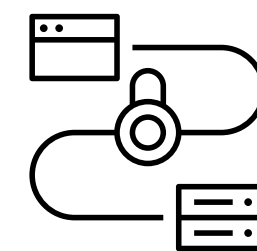
- Financial institutions (FI) are focused on finding yield generation with digital assets
- The storage and transfer of digital assets are operationalized by cryptographic key management
- All stakeholders in the digital assets industry, regardless of whether or not they are aware of it, are exposed to some degree of risk when it comes to managing private keys used to sign transactions. If you control the private keys, you control the assets
- A FI's first priority is to deploy digital asset custody for private keys necessary to offer lending, staking, token issuance, and liquidity provision to their customer
- FIs are relying upon digital asset custody technology platforms (custody tech) to compete
- Custody tech ISVs value hardware protections for key material and air-gapped isolation for their applications over software only key management
- IBM Hyper Protect provides the highest commercially available FIPS 140-2 Level 4 hardware security modules to protect keys in a massively scalable way
- IBM Hyper Protect and IBM® LinuxONE, zSystems Secure Execution for Linux workload isolation protects custody tech applications from administrator access and internal and external threats
- IBM Hyper Protect is an ideal target technology for custody tech ISVs, like Metaco, to deploy both cloud and on-premise custody solutions to help FIs compete

IBM Digital Assets Infrastructure

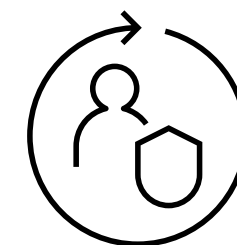
Orchestrate **IBM Hyper Protect Services** to provide competitive differentiation in trust for regulated industries and clients.



Co-create with selected digital custody providers to deliver end-to-end-to-end solutions that help clients de-risk their digital asset initiatives



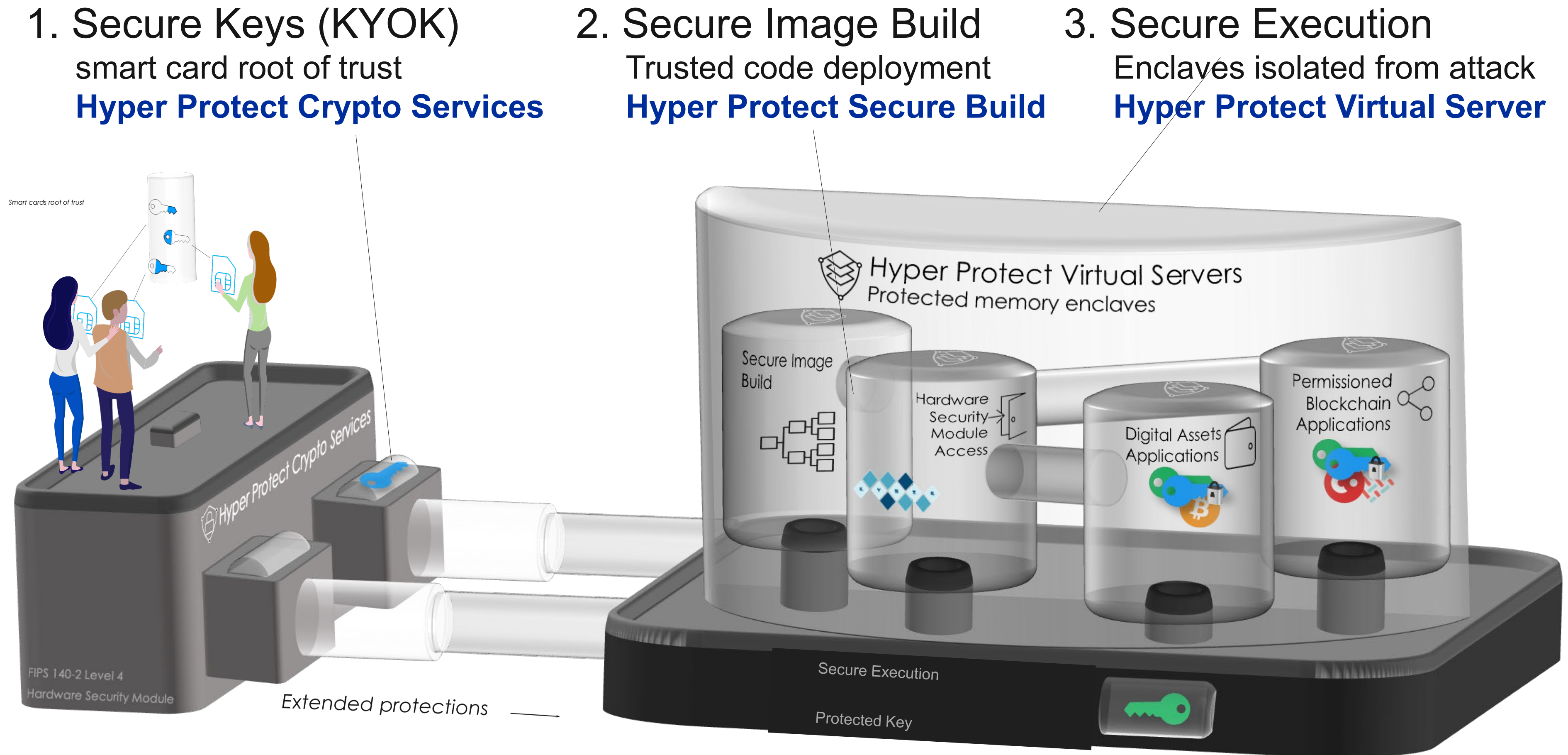
Leverage the differentiated features of IBM's confidential computing technology including trusted local keys, protected memory, and our innovative HSM



Extend zero trust principles to remove human attack vectors from code build and deployment, transaction approvals, cold storage solutions, and platform administration

IBM Digital Assets Infrastructure

Use IBM Hyper Protect Services to create new business services which safely **extend HSM constrained applications into protected memory enclaves** to promote growth and flexibility while reducing administrative complexity.



Digital Assets Infrastructure – ISVs on Hyper Protect



One of the world's leading digital asset service providers leverages IBM Hyper Protect Services, powered by IBM® LinuxONE, to sell an embedded digital asset management solution with IBM



Top Use Case Examples for Confidential Computing

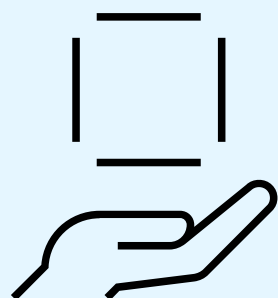


Hyper Protect Services
maintain the confidentiality and integrity of your data, digital assets or intellectual property



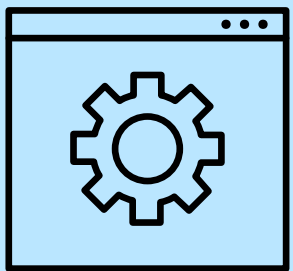
Secure Containerized Workloads

containerising applications within a Hyper Protect Confidential Computing environment ensures that your applications are always protected.



Digital Assets

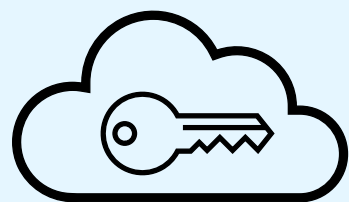
the trusted platform for digital custody solutions, for storing and transferring high value digital assets in highly secure wallets, reliable at scale.



Secure Multi Party Collaboration (SMPC)

enabling distributed SMPC, where participants are ensured their data and insights are protect even when being calculated outside their direct control.

LARGE INDUSTRY ORGANIZATION



Exclusive Control of Data and Keys (KYOK)

Mitigate risk of data loss and meet regulatory requirements



Quantum-Safe Cryptography

technology for a new cryptographic era supporting NIST selected IBM co-developed quantum-safe algorithms

Secure Multi-Party Collaboration (SMPC)

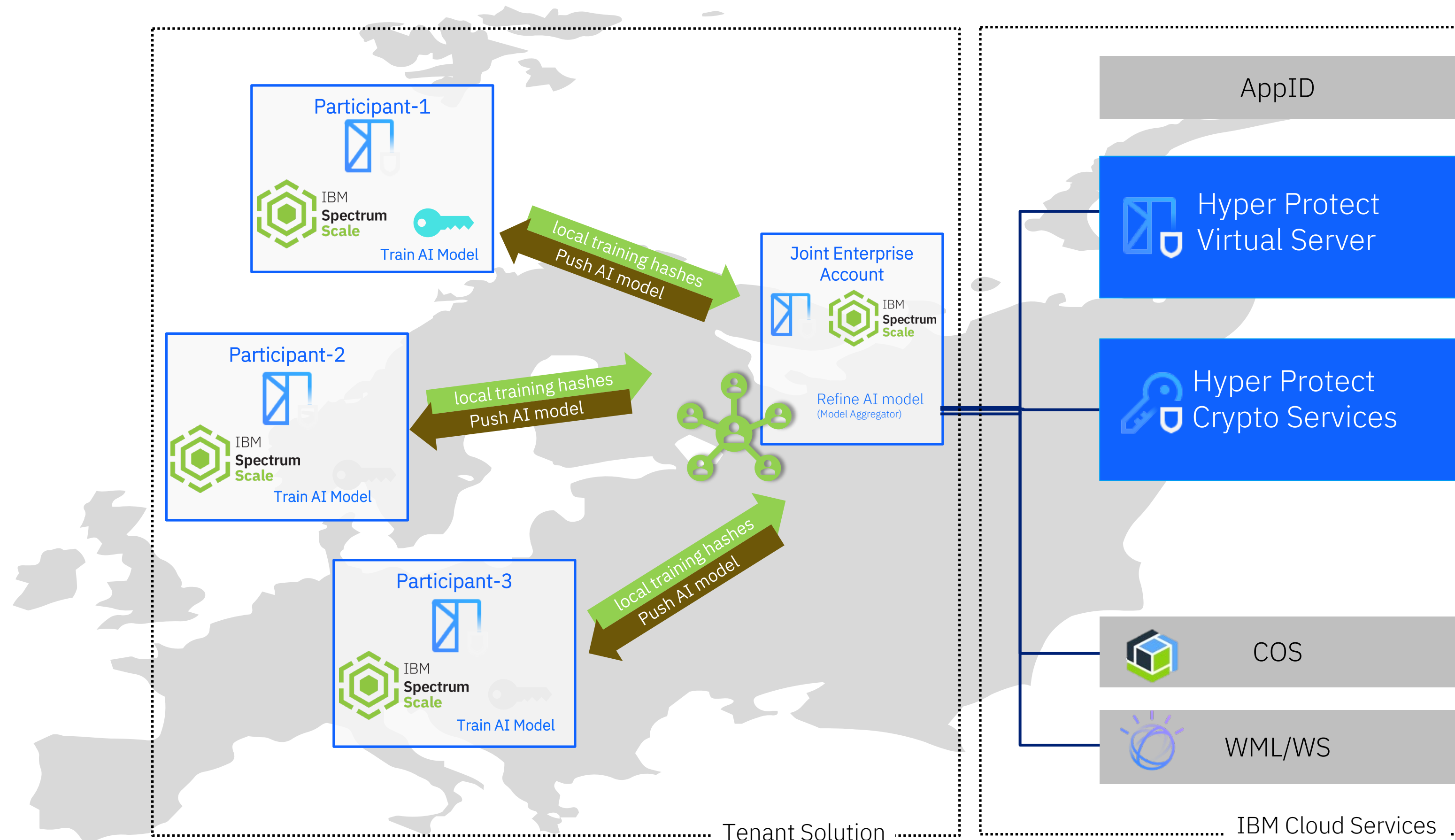
Challenges	Solution	Benefits
<ul style="list-style-type: none">• Clients demand Federated Machine Learning capabilities which is training AI models without exposing the data and conform to various data privacy and confidentiality regulations.• Collaborate to refine an AI model but keep data strictly private and within premise.• Refine a Central AI model using Decentralized data• Homomorphic encryption can be resource intensive and expensive when dealing with user contracts containing private data	<ul style="list-style-type: none">• Critical components protected by <i>Secure Execution</i> technology. <i>Technical Assurance</i> prevents privileged user access• Secure <i>Trusted Execution Environments</i> leveraged• Reduce risk of malicious code insertion using an encrypted <i>Multi-Party contract</i> which allows persona separation, attestation and third-party certification• Secure MPC allows multiple parties each to encrypt their private data sections and combine into a single unified contract which can be decrypted only in a Trusted Execution environment like HPVS	<ul style="list-style-type: none">• Multiple parties collaborate, train AI models on their private (on-prem) data without exposing them.• Each party's private training datasets are completely protected (within HPVS Secure enclaves on-prem) against which AI models are run.• Each party's training hashes are aggregated to refine the centralized/ shared AI models.• Private data is neither exposed nor derived• No single party can ever have access to all the data

AI and analytics on sensitive data – with secure multi-party analytics patterns

Secure MPC with Confidential Computing enabled AI collaboration with total data privacy.

Gain better and deeper insights together while keeping all data private.

Federated machine learning in the distributed multi-party setup with total data privacy using confidential computing. A hub for collaboration, capability sharing, data source collections and observation management.



Technology

- Confidential Servers and Containers as core enabling technology for Confidential Computing
- Use Keep Your Own Key with per-party keys (IBM Cloud Hyper Protect Crypto Services)
- Build AI/models and apps on top of confidential computing platform

Top Use Case Examples for Confidential Computing



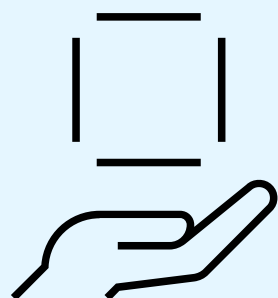
Hyper Protect Services
maintain the confidentiality and integrity of your data, digital assets or intellectual property

PHOENIX SYSTEMS



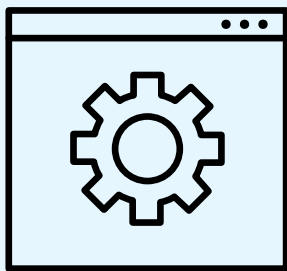
Secure Containerized Workloads

containerising applications within a Hyper Protect Confidential Computing environment ensures that your applications are always protected.



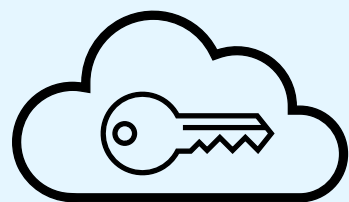
Digital Assets

the trusted platform for digital custody solutions, for storing and transferring high value digital assets in highly secure wallets, reliable at scale.



Secure Multi Party Collaboration (SMPC)

enabling distributed SMPC, where participants are ensured their data and insights are protect even when being calculated outside their direct control.



Exclusive Control of Data and Keys (KYOK)

Mitigate risk of data loss and meet regulatory requirements

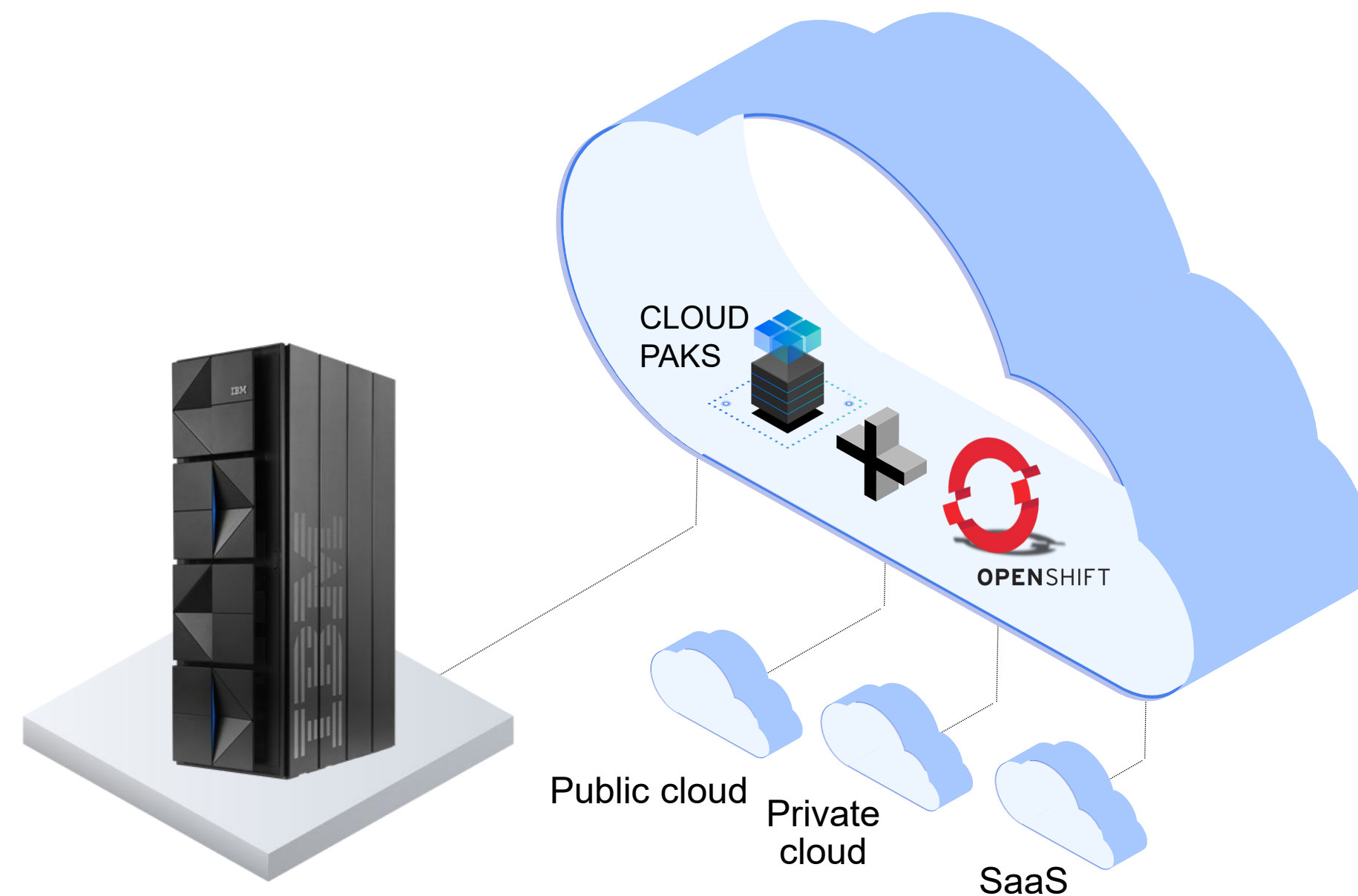


Quantum-Safe Cryptography

technology for a new cryptographic era supporting NIST selected IBM co-developed quantum-safe algorithms

The best of the mainframe and the innovation of Cloud

IBM zSystems integrated in a Hybrid Cloud Platform



Enterprise standardization

Platform integration

With IBM zSystems in the Hybrid Cloud:

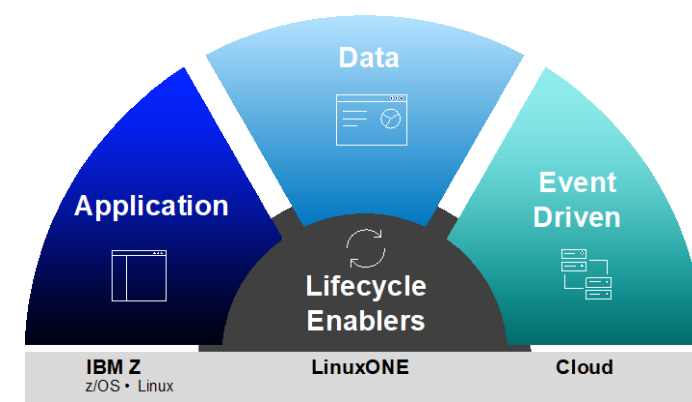
Reduce the talent gap with common tools and operating models across platforms

Accelerate time to market for cloud native services with a consistent DevOps experience

Easily access IBM zSystems data without moving off-platform

Optimize costs with a cloud consumption model that extends to IBM zSystems

Application Modernization



Digital use cases drive data and functionality needs that are hosted on IBM zSystems

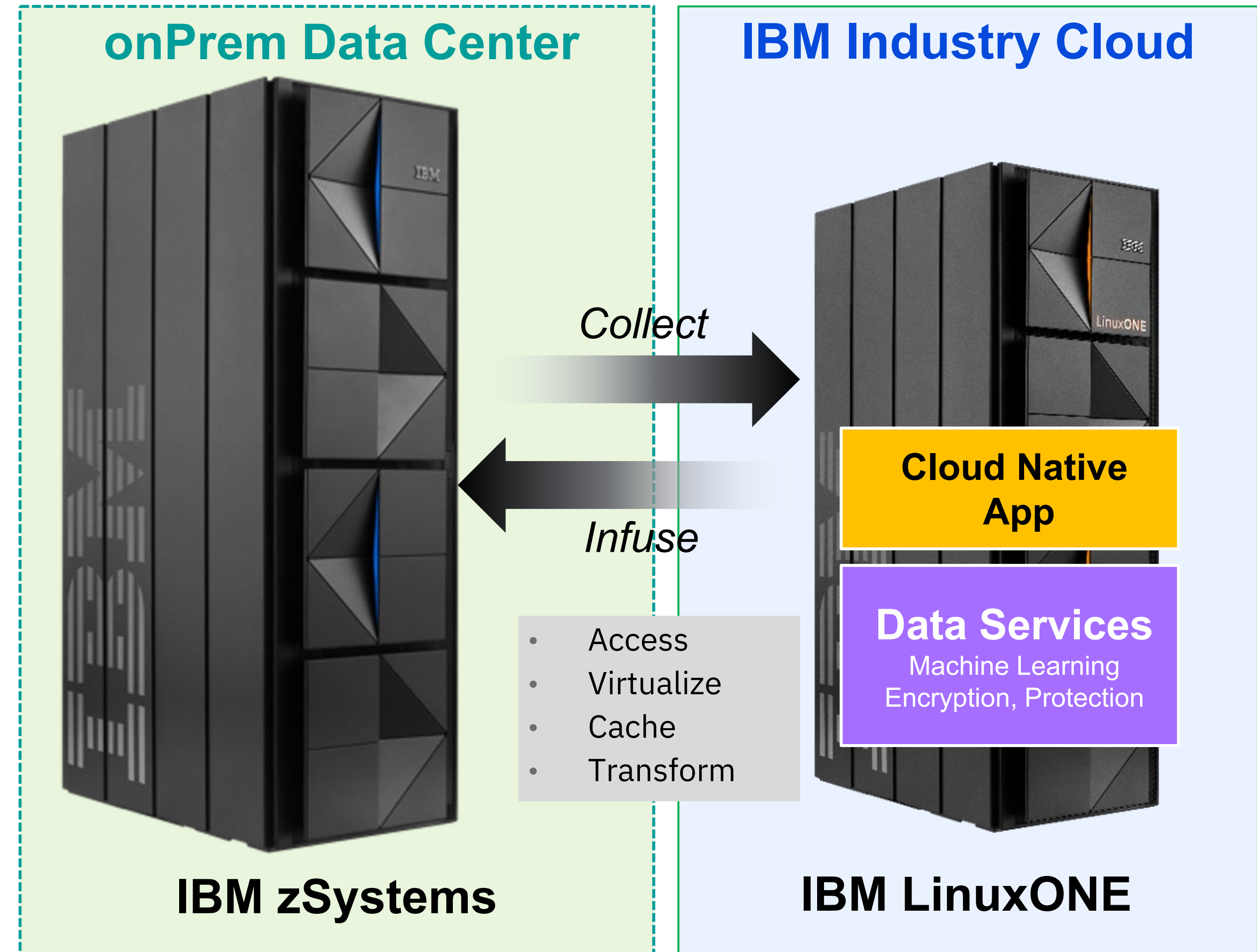
Hyper Protect Services On-Prem and in IBM Cloud

Confidential computing keeps your data protected

- Improve compliance and risk management for your workloads.
- Leverage private or public cloud based managed services while keeping data private with confidential computing.

Containers simplify and standardize management

- Start from a large repository of existing containers, runtimes and modules provided by them.
- Hyper Protect Virtual Server is based on Confidential Computing to ensure data is kept secure and protected.



Don't let data security and data privacy block your application modernization journey.



Swiss based IT service provider with strong focus on Confidential Computing and Data Sovereignty leverages IBM Hyper Protect Services, powered by IBM® LinuxONE, to operate virtual datacenters

Business Problem:

Offer customers simplicity without worrying about the infrastructure underneath as they bring their data to the home of sensitive workloads.

Solution:

Bring your own Code or your ISV solution to a datacenter based on Confidential Computing allowing them to separate their business from their physical infrastructure.

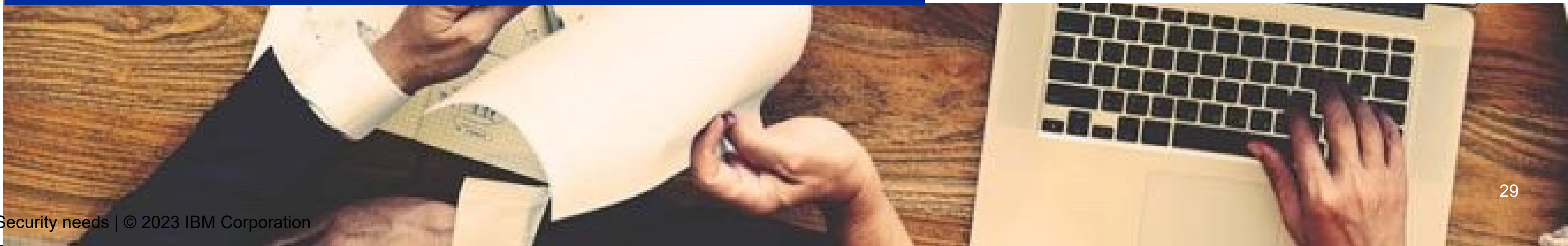
Business Value:

Phoenix Systems can now grow faster than their competition of cloud companies in Europe as they provide data sovereignty aware containerized environments.

IBM provides the technical assurance no one, not even the admin can access any assets, intellectual property or sensitive client information.

Solution Components:

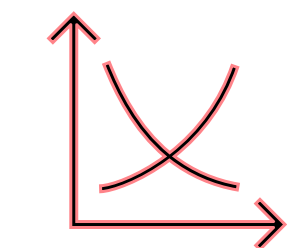

IBM Hyper Protect Virtual Server
IBM Crypto Express adapter





IBM Cloud Hyper Protect Virtual Servers

Speed up time to market, enable digital transformation with reduced risk

Client Pain Points

- 
 - **Authorization of access to data is abused-** malicious or accidental
- 
 - **Loss of control over sensitive data** through cyber-attack or mishap can result in irreversible loss.

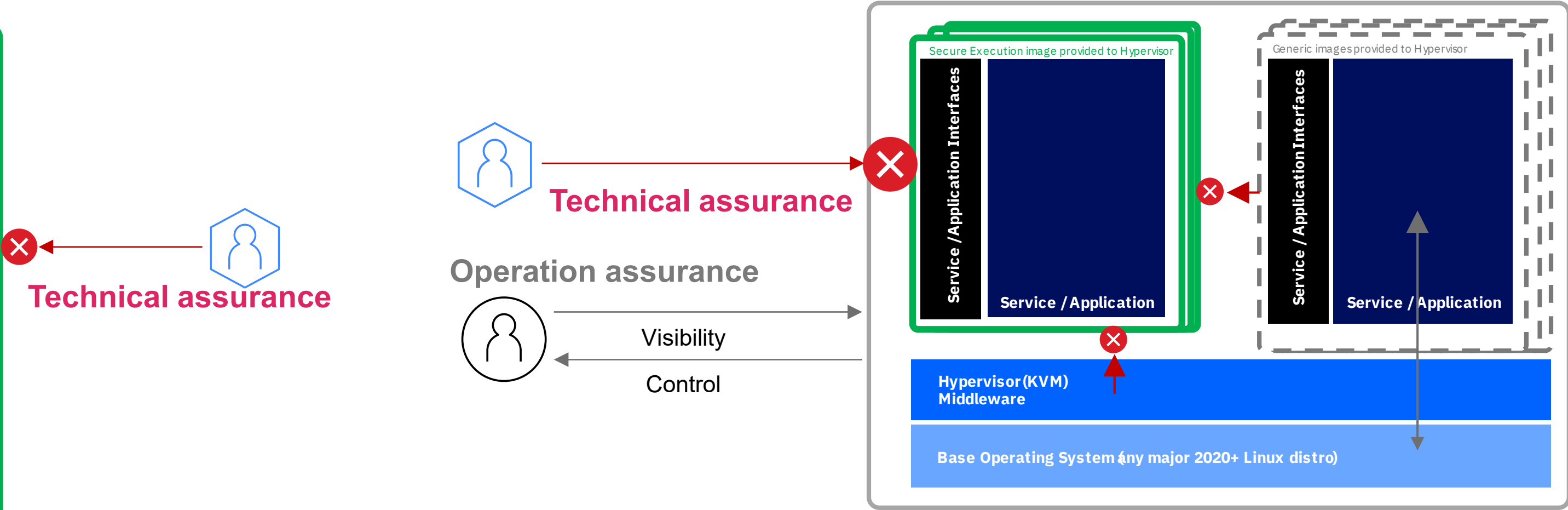
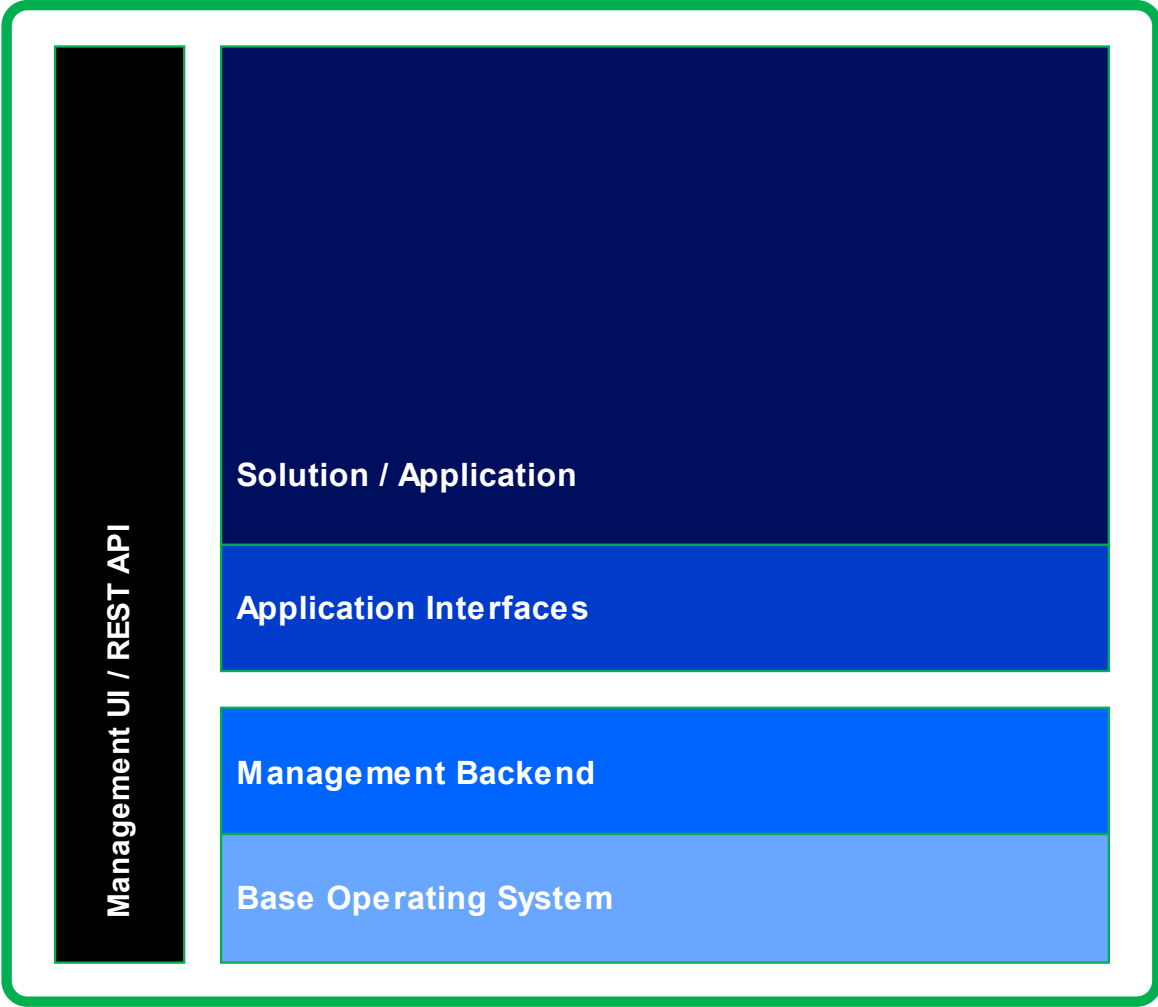
Outcomes with HPVS in IBM Cloud & on-prem

- 
 - **Secure execution** - Technical assurance that unauthorized users including IBM Cloud admins do not have access to the application
 - **Zero Trust principles** based on an encrypted contract concept. Multiple personas can collaborate without data compromise, deployment can be validated by auditor persona
- 
 - **Malware protection:** Utilize Secure Build to ensure that only authorized code can run
 - **Flexible deployments:** Choose from a variety of profile sizes and grow as needed within Cloud or size per IFL on-prem

Customer Value	Support for data sovereignty requirements	Containerized applications with built-in protections	Hybrid Cloud based advantages	Deployment Options
Benefits	<ul style="list-style-type: none"> • Data privacy enhancing technology • Isolation down to the runtime level to protect against internal and external threats 	<ul style="list-style-type: none"> • Use standard Open Container Initiative (OCI) images to start building • No vendor lock-in / CNCF 	<ul style="list-style-type: none"> • Scalability and savings of public cloud • Security advantages of private cloud • Consistent Environment within a hybrid Cloud architecture 	<ul style="list-style-type: none"> • In IBM Cloud DC's: London, Toronto, Sao Paulo, Washington D.C, Tokyo, Madrid (coming soon) • On-premises, running on LinuxONE or IBM zSystems

Confidential Computing Progression (SSC to Secure Execution)

Protection Boundary Granularity



Secure Execution
“Selective KVMs/Services run in individual enclaves”

Secure Service Container
“The LPAR is the enclave”



z14
LinuxONE II

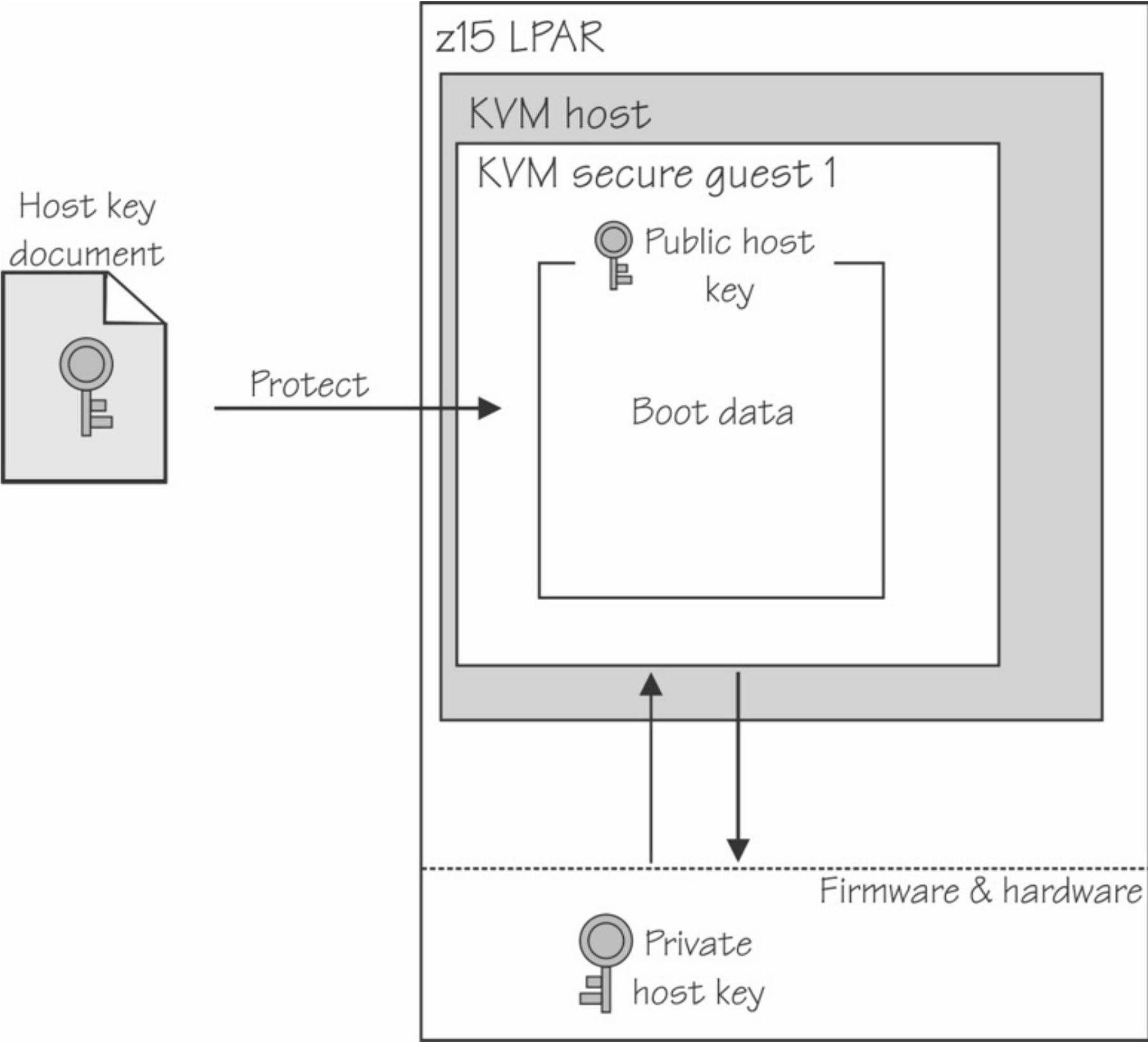
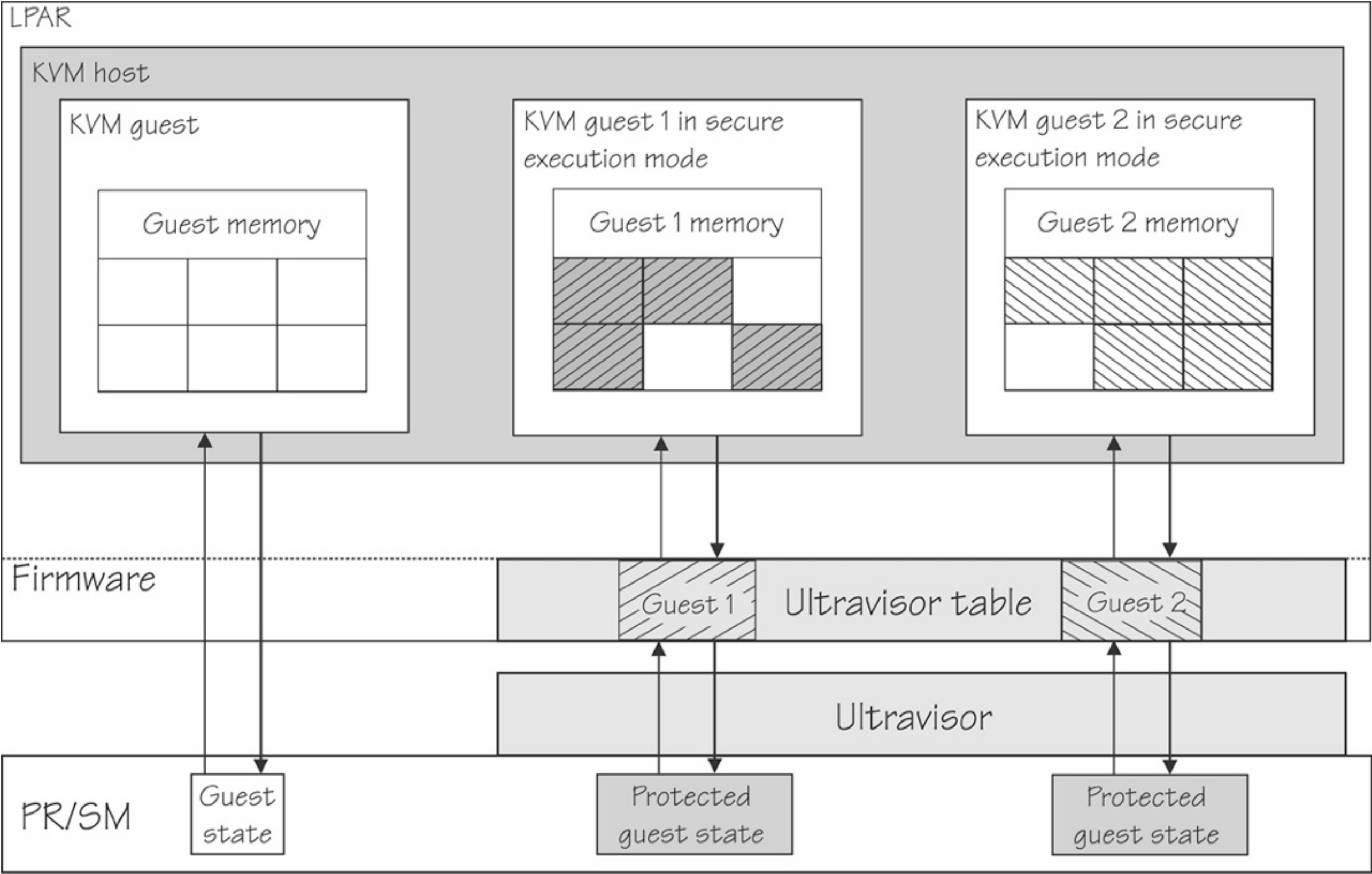


z15
LinuxONE III



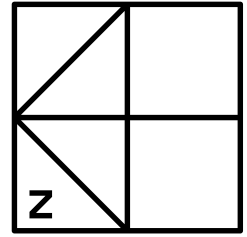
z16
LinuxONE 4

Secure Execution for Linux



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

Secure Execution Enhancements for Confidential Computing (IBM z16 and IBM® LinuxONE 4)



Physical Memory Encryption

Encryption of data in memory and on memory buses

Encryption of Secure Execution, Hyper Protect keys

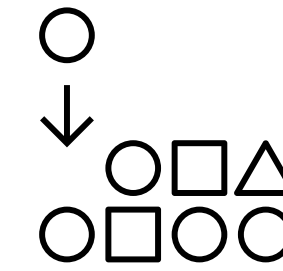
Full System-memory encryption protects data in any memory module within the z16/LinuxONE 4 system. Besides the already present protection of memory the additional encryption of any system memory prevents the whole stack from firmware to operating system and middle-ware to any workload runtime being disclosed by malicious access to modules



Attestation of Trusted Execution Environment

Attestation for Secure Execution

Attestation provides cryptographic assurance to the customer that a given workload is executed in a Secure Execution enclave. It is an explicit ask by customers and compliance that an enclave is in the position to provide proof for computing confidentially

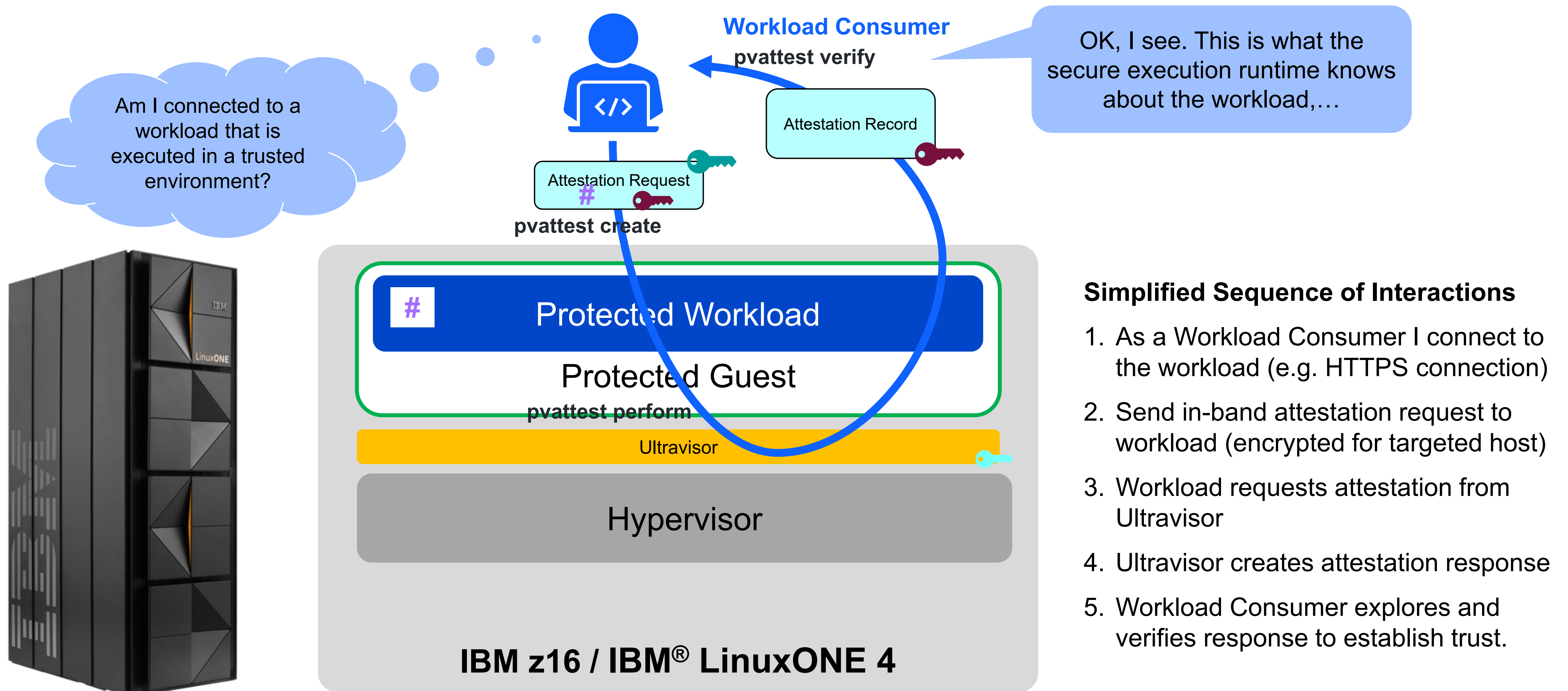


Automation and Ease of Use (audit, dump, manage)

Encrypted customer readable dump

Clients can obtain an encrypted debug/dump data from a Secure Execution enclave without compromising security/assurance claims

Secure Execution for Linux Attestation on z16 and IBM® LinuxONE 4



Hyper Protect Virtual Server for VPC & Hyper Protect Virtual Server v2.1



zSystems
IBM® LinuxONE

IBM Cloud
VSI for VPC

Take advantage of Secure Execution to provide greater authority and isolation down to the instance level for containerized images

Building containerized applications

- Highly performant and scalable
- Use standard Open Container Initiative (OCI) images to start building
- No vendor lock-in / CNCF Confidential Containers

Based on Secure Execution for Linux

- Provides a Trusted Execution Environment (TEE) that protects data in use
- Isolation down to the runtime level to protect against internal and external threats
- Sovereign control / data privacy enhancing tech

Capture new business opportunities with Virtual Private Cloud and Private Cloud capabilities

- Scalability and savings of public cloud
- Security advantages of private cloud

Hyper Protected Container Runtime

Hyper Protect Virtual Servers

takes advantage of the IBM Secure Execution for Linux technology to provide a memory protection for each individual instance. With the added protections:

- ✓ Isolation for KVM guests from hypervisor
- ✓ Isolation between KVM guests
- ✓ Technical assurance that only the KVM guest workload (OCI containers) can access guest memory and data in the environment
- ✓ Seamless at rest data protection using filesystem encryption based on multi party runtime contract
- ✓ Hardware root of trust and runtime protection keys never leave the secure execution environment and are protected from hypervisor, guest and workload

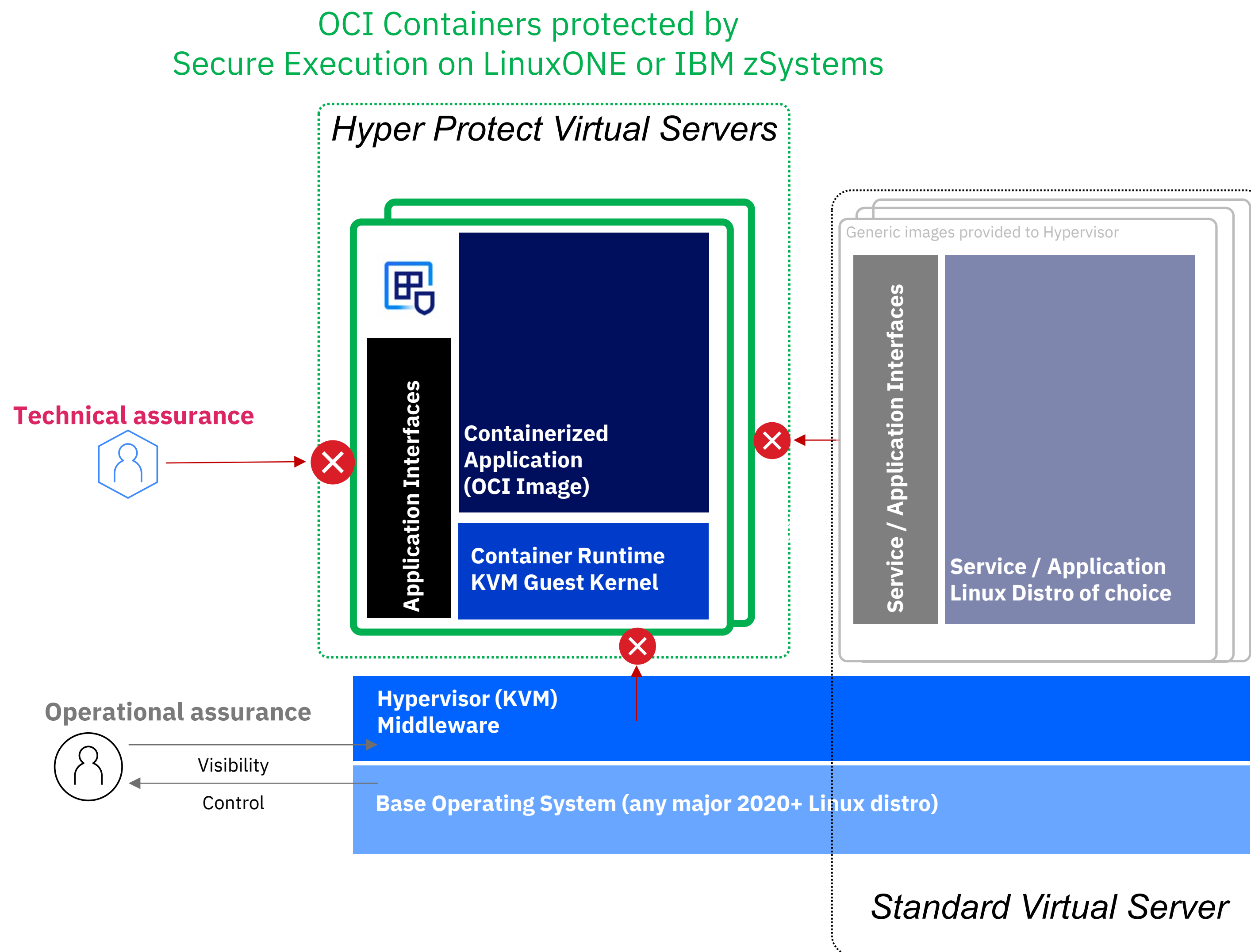


Illustration of Trusted Execution Environment with Secure Execution provided by Hyper Protect Virtual Server (on-prem and IBM Cloud)

Hyper Protect Virtual Servers

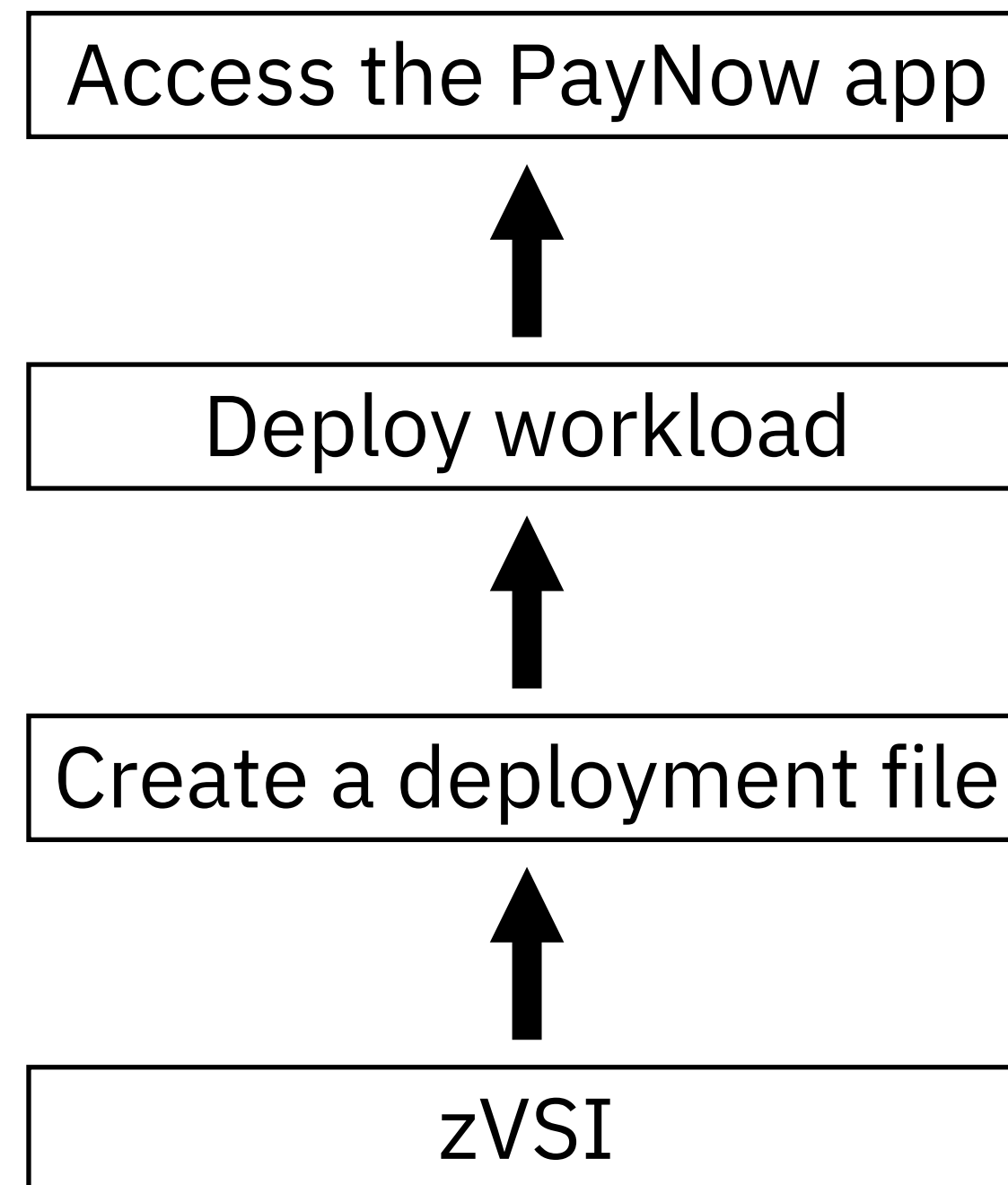
provides the runtime for your container workloads protected with secure execution for Linux. In the cloud and on-premises

On IBM LinuxONE and Linux on zSystems

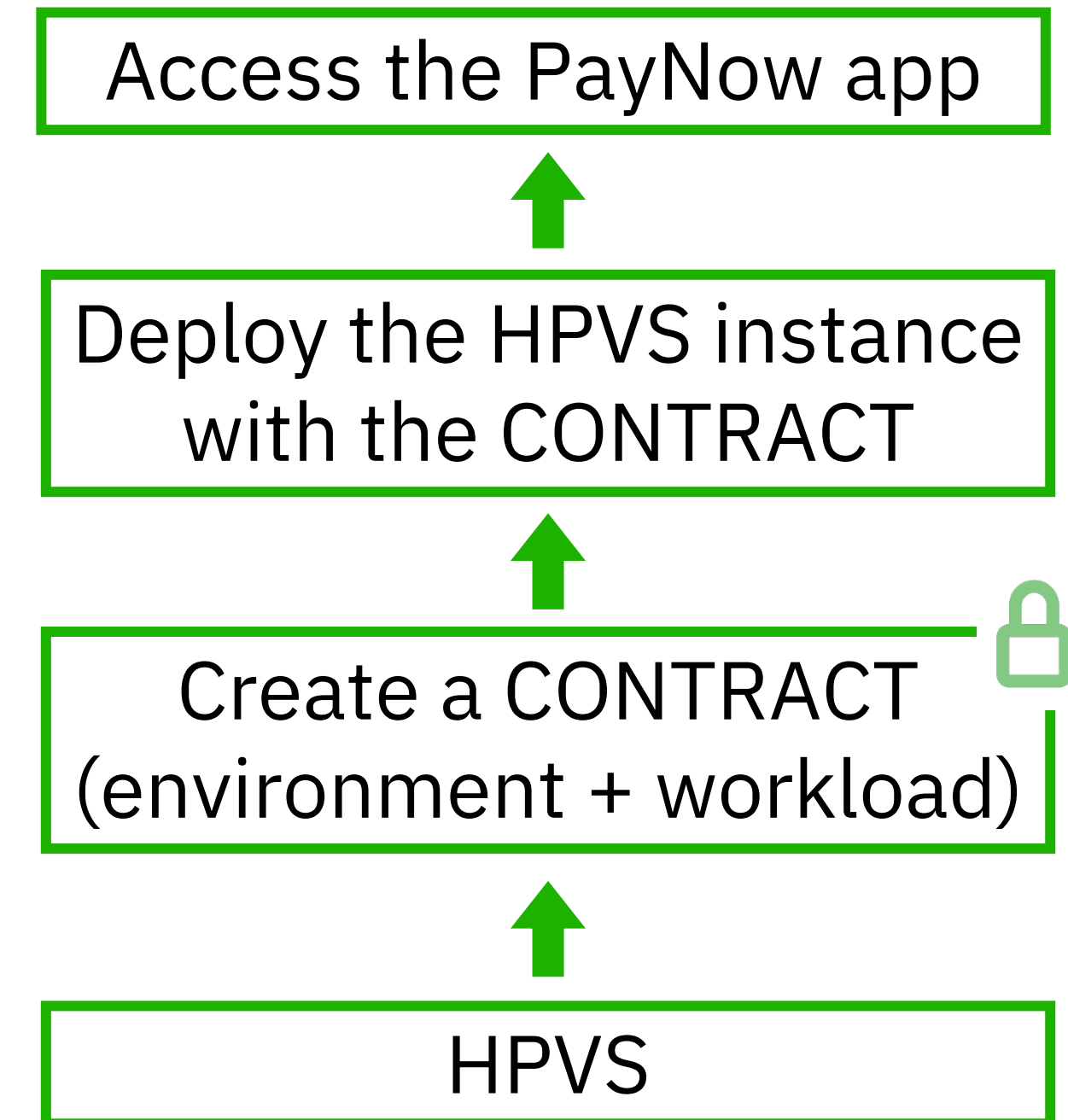


Creating servers for the demo environment

Without confidential computing



With confidential computing



IBM LinuxONE or Linux on zSystems

The IBM Hyper Protect Platform Generation 2

A technical overview



by Stefan Amann, Timo Kußmaul, Carsten Leue, Stefan Liesche,
Anbazhagan Mani, Asha Shekarappa, Divya Knoor, Nicolas Mäding, James
Magowan, Peter Morjan and Stefan Schmitt

Table of Contents

1. MOTIVATION	3
2. INTRODUCTION	4
3. UNDERLAYING TECHNOLOGY – SECURE EXECUTION FOR LINUX	5
4. HYPER PROTECT PLATFORM	7
4.1. ARCHITECTURAL CONCEPTS	8
4.1.1. Personas	8
4.1.2. Contract	9
4.1.3. Data Volume Encryption	11
4.1.4. 3 rd party Attestation of boot	12
4.2. HYPER PROTECT CONTAINER RUNTIME	14
4.2.1. Bootloader	14
4.2.2. Hyper Protect Layer Services	16
4.2.3. Data Volume Encryption Services	17
4.2.4. Workload Deployment and Considerations	19
5. CONSIDERATION OF TRUST	21
5.1. Leveraging Secure Execution for the Hyper Protect Platform	21
5.2. Hyper Protect Build Environment	21
5.3. Contract	24
5.4. Secure Build for Hyper Protect Container Runtime	26
6. LEVERAGE THE SECURE PLATFORM	27
6.1. IBM HYPER PROTECT VIRTUAL SERVERS FOR ZSYSTEMS AND IBM® LINUXONE	27
6.2. IBM CLOUD VIRTUAL PRIVATE CLOUD (VPC)	27
7. USE CASES OF THE HYPER PROTECT PLATFORM	29
7.1. DIGITAL ASSETS	29
7.2. MULTI-PARTY COMPUTE	30
7.3. DATA PROTECTION	31
7.4. KUBERNETES AND CONFIDENTIAL CONTAINERS	32
8. SUMMARY	34



<https://www.ibm.com/downloads/cas/GPVMWPM3>

Containers and Kubernetes?

Annual CNCF report 2021

Kubernetes is mainstream today and adoption of cloud-managed and serverless accelerates in the market.

96%

Kubernetes adoption

Kubernetes has crossed the adoption chasm to become a mainstream global technology, as organizations are either using or evaluating Kubernetes

90%

Cloud-managed Services

With its mainstream status solidified, Kubernetes is starting to go "under the hood", as K8s Users leverage services towards serverless concepts

79%

Certified K8s Hosted Platforms

As Trusted Computing Platform and Privacy Enhancing Technologies get adopted use of certified K8S Hosted Platforms become mainstream and expected by users and decision maker.

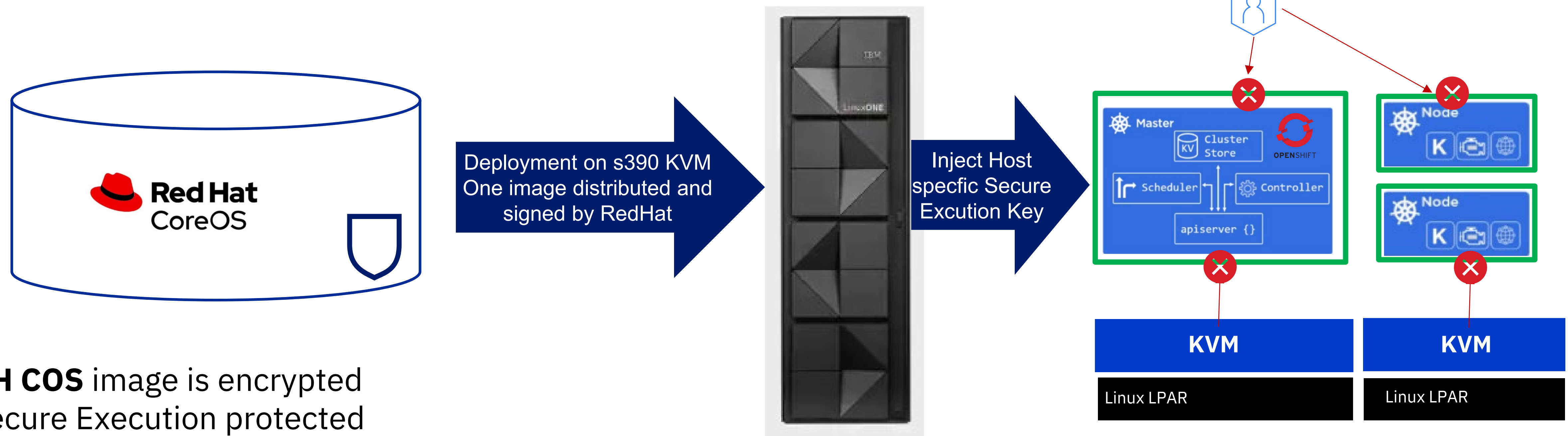
CNCF Annual report: https://www.cncf.io/wp-content/uploads/2022/02/CNCF-AR_FINAL-edits-15.2.21.pdf

RedHat Core OS for x390x – 4.12 Tech Preview



Provide RHCOS image, which is Secure Execution protected **and** the resulting deployment leverages Secure Execution

RH COS image is encrypted
Secure Execution protected
Leveraging.  Hyper Protect Key and BuildVM



Secure Execution for Linux protection boundary
for Openshift Master and worker nodes
For a given customer owned host or datacenter

Confidential Computing for Kubernetes

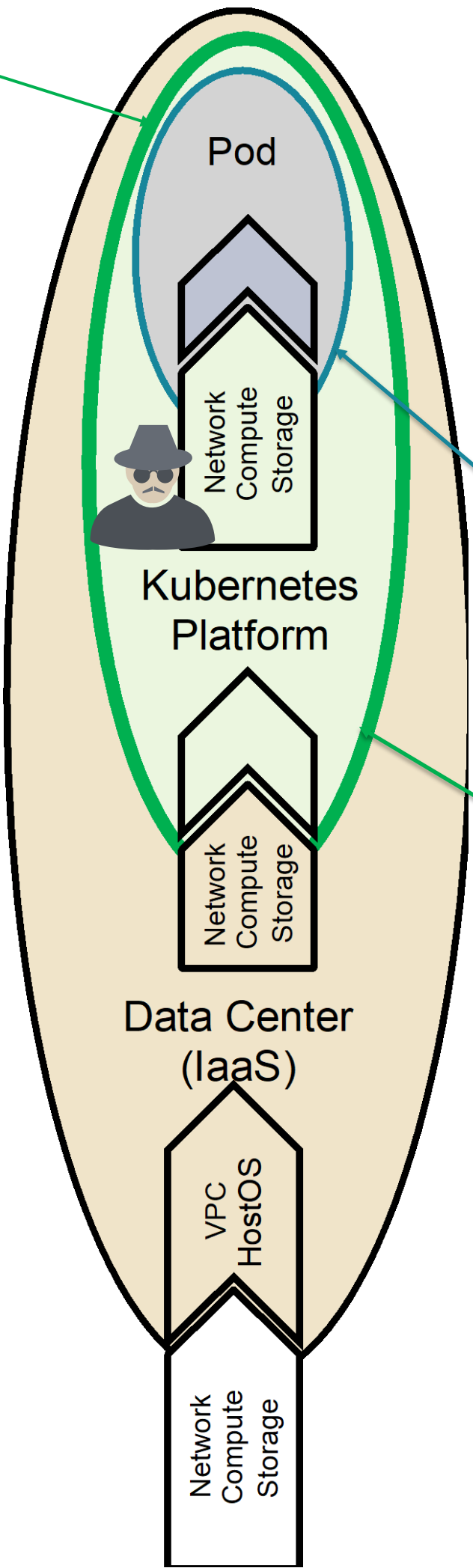
SOON

protected virtual machine

as-is:
K8s cluster are user-provisioned
or can be provider managed
K8s nodes in enclaves
(protect against Pod breakout)
(protect against Cloud)

NOT protected from K8S admin,
self managed or provider managed.
Worker node needs to be trusted!

NEW
OpenShift 4.12 Tech Preview



Kubernetes/OpenShift with Hyper Protect

→ to-be:
K8S clusters are managed/provided
K8s pods/container in enclaves
(protect against Pod breakout)
(protect against Cloud)
AND K8s admin

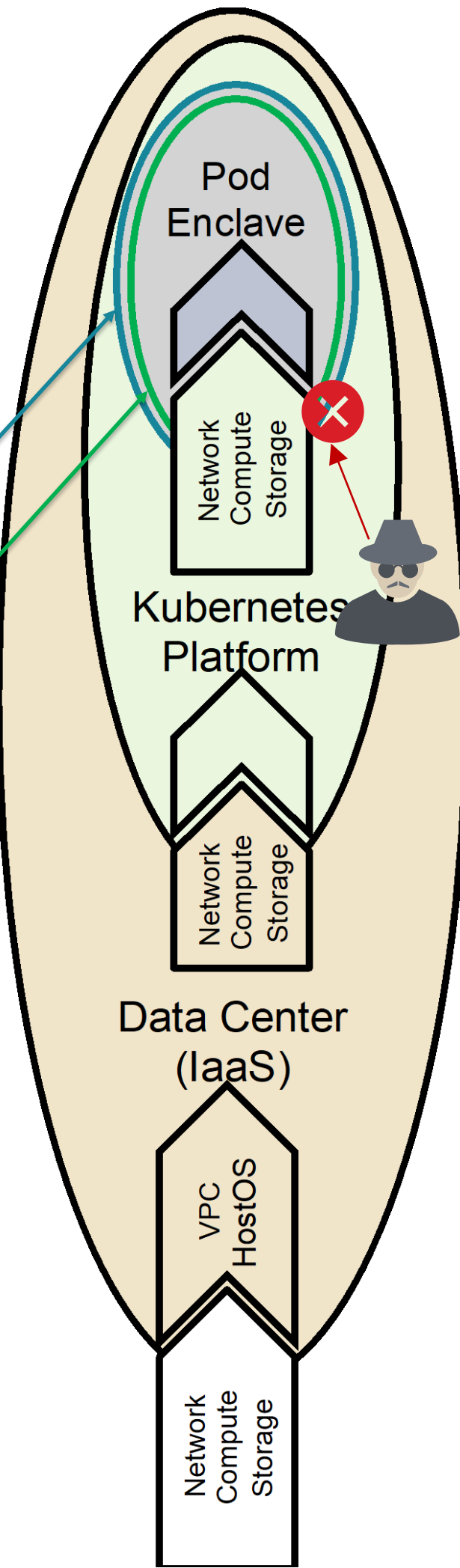
Kata intend

Protect Platform
against malicious workload

Enclave

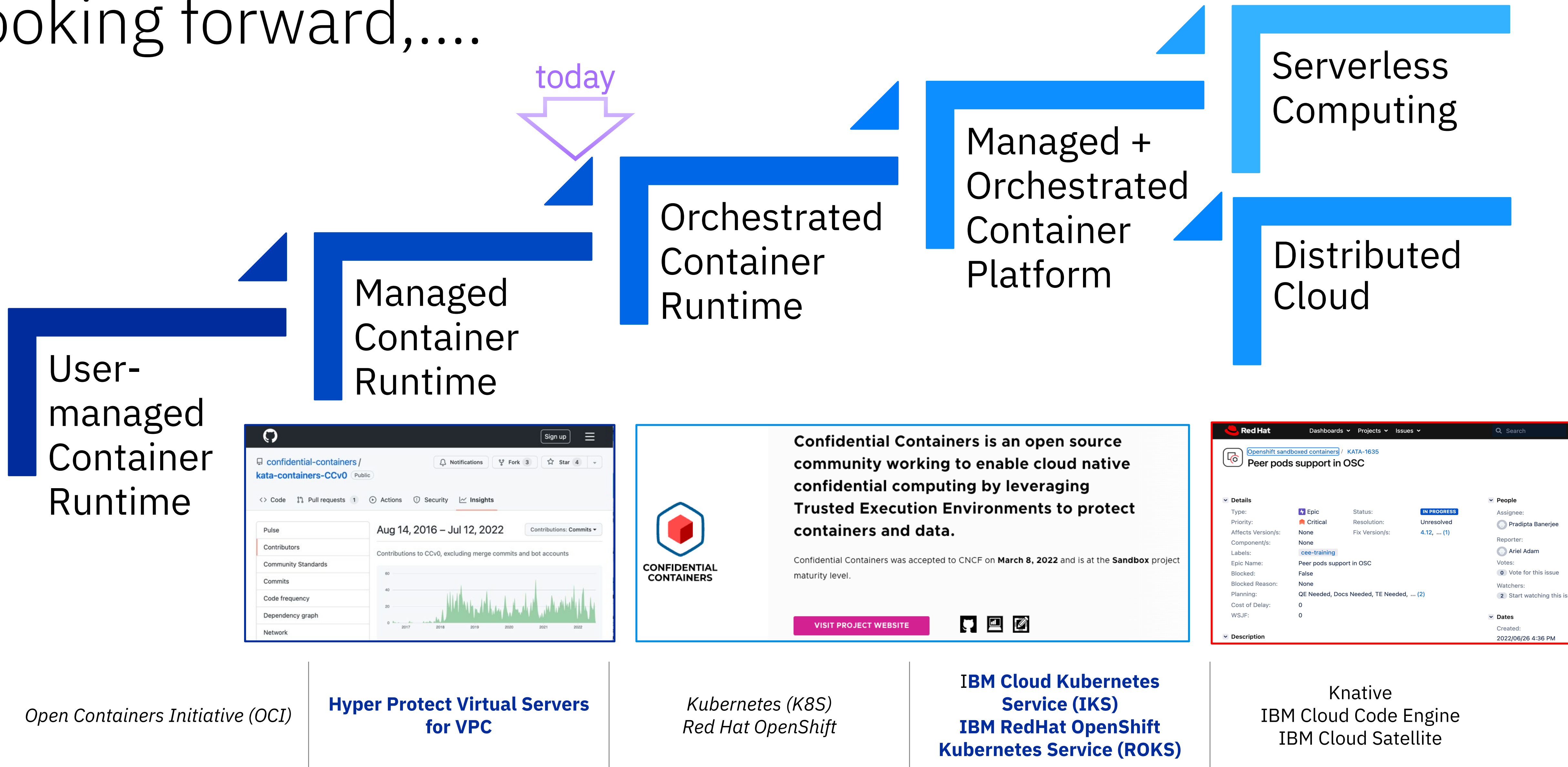
Protect Workload
against malicious platform
aka. Confidential Computing

Kata+CC



Confidential Computing for Containers

Looking forward,....



IBM Hyper Protect Services in the IBM Hybrid Cloud

leverage confidential computing everywhere – based on Secure Execution for Linux on zSystems.

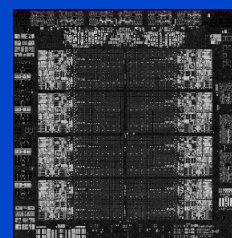


Hyper Protect Services

Enables Confidential Computing to underpin IBM Cloud’s regulated industry strategy
Key aspect for Data Sovereignty



Hyper Protect Virtual Servers 2.1



zSystems, IBM® LinuxONE On-prem

Hyper Protect Services



Hyper Protect Crypto Services
with Unified Key Orchestrator



Hyper Protect Virtual Servers for VPC

Native zSystems Services



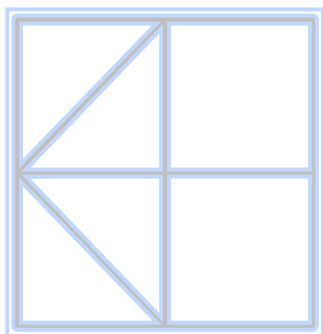
Wazi aaS – z/OS Dev & Test



IBM® LinuxONE Bare Metal Servers



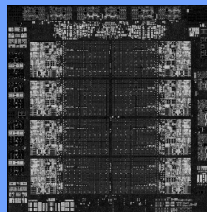
IBM® LinuxONE Virtual Servers



Native zSystems

Serve zSystems and IBM® LinuxONE clients in the public cloud and enable Hybrid Cloud use cases

IBM® LinuxONE in IBM Cloud



IBM LinuxONE Portfolio in IBM Hybrid Cloud

leverage Privacy-enhancing technology and data protection everywhere - build upon Zero-Trust

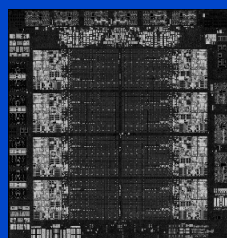


Hyper Protect Services

Enables Confidential Computing to underpin IBM Cloud’s regulated industry strategy
Key aspect for Data Sovereignty



Hyper Protect Virtual Servers 2.1



zSystems,
IBM® LinuxONE
On-prem

Hyper Protect Services



Hyper Protect Crypto Services
with Unified Key Orchestrator

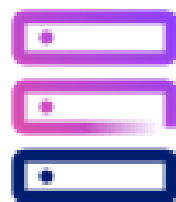


Hyper Protect Virtual Servers for VPC

Native zSystems Services



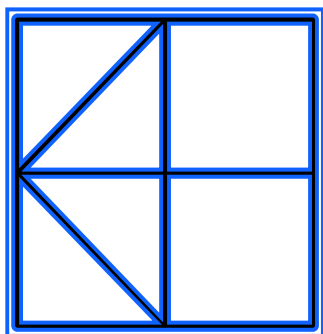
Wazi aaS – z/OS Dev & Test



IBM® LinuxONE Bare Metal Servers



IBM® LinuxONE Virtual Servers



Native zSystems

Serve zSystems and IBM® LinuxONE clients in the public cloud and enable Hybrid Cloud use cases



