



Hyper Protect Offerings for IBM Cloud and on-prem environments

JC Yao

jcy@us.ibm.com

Program Director, zCAT, Hyper Protect Services, z Hybrid Cloud

Mitigating the impacts of cyber attacks

\$4.35M

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

83%

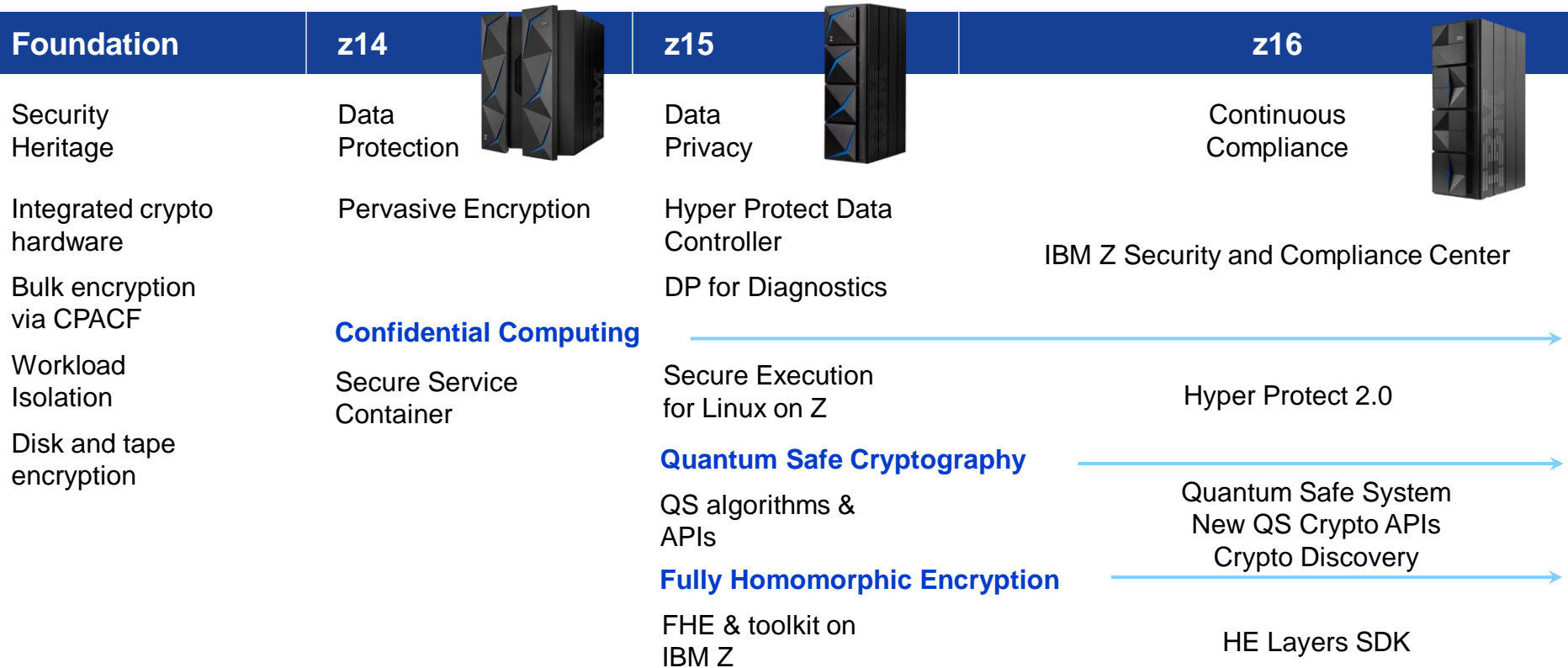
of organizations studied have had more than one security breach

81%

of executives consider security a brand attribute that differentiates their organization

Source: [IBM: Cost of a Data Breach Report 2022](#)

IBM Z and LinuxONE security leadership



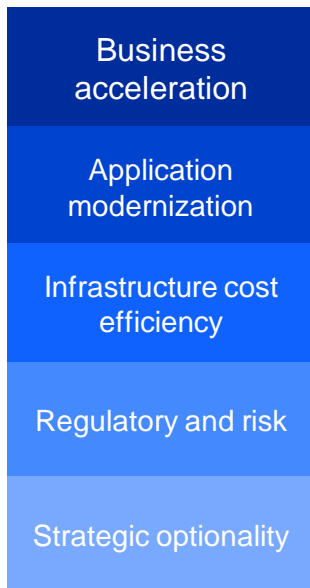
Hybrid unlocks the full value of your IT infrastructure

A hybrid strategy unleashes the full potential for customers

2.5x

more value with a hybrid strategy than on-prem or aaS strategy alone

Value Source



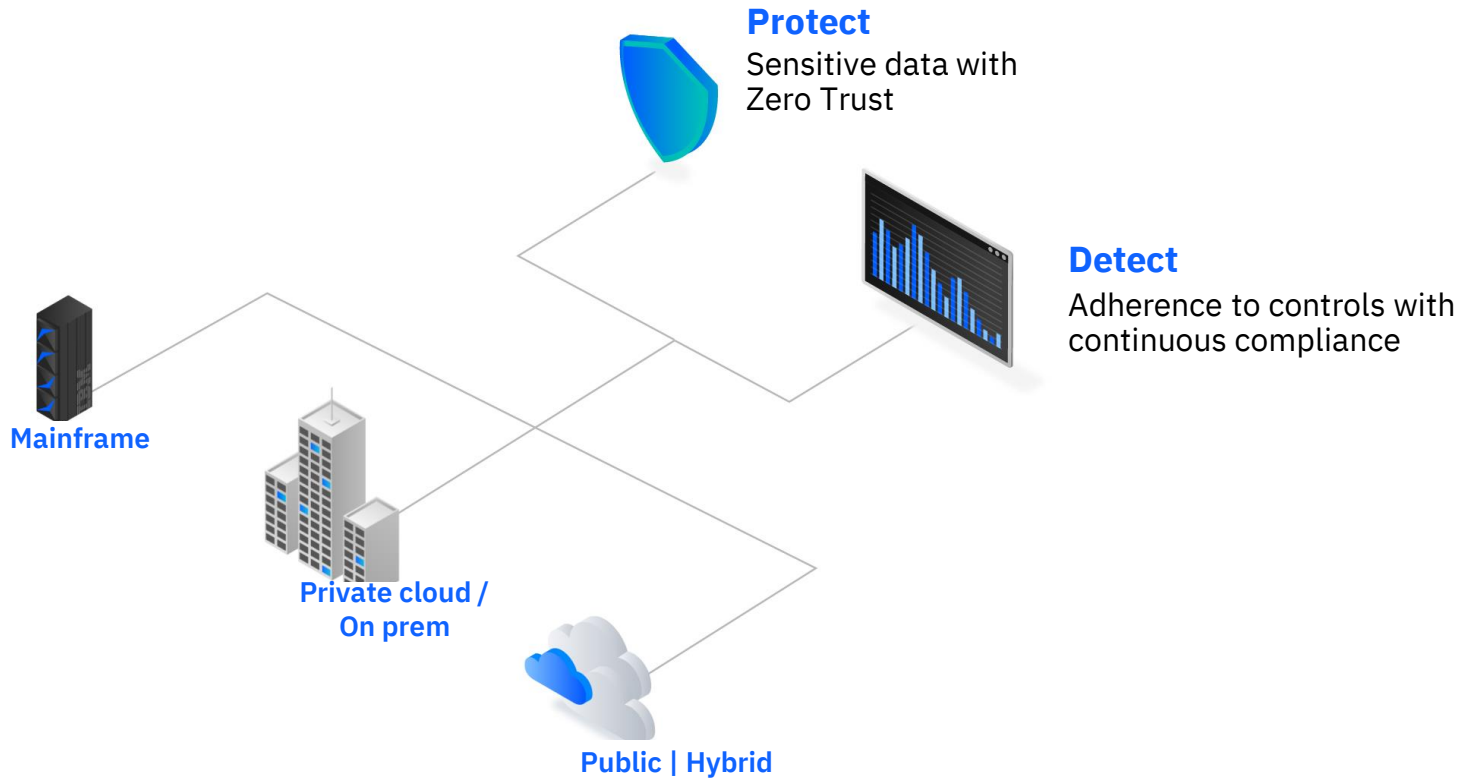
Primary

- Get 2.5x more benefit
- Speed up app release from months to weeks
- Cut infrastructure costs by 4x with less maintenance
- Reduce compliance spend by 25%
- Realize a more agile and flexible architecture

Additional

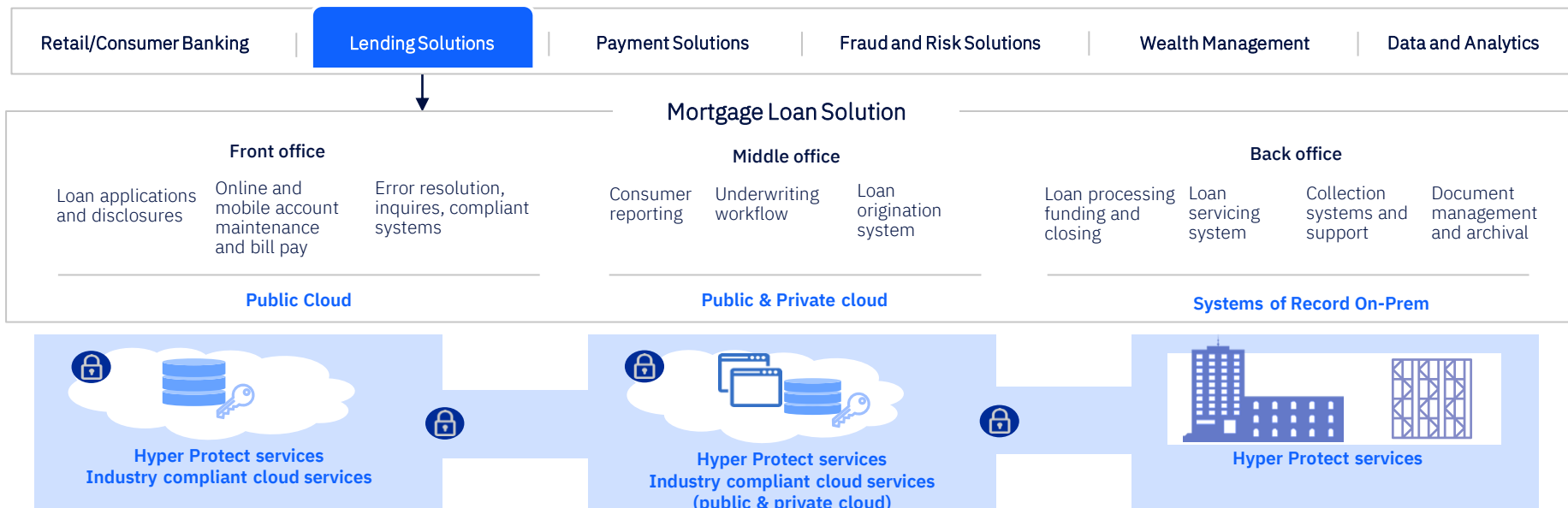
- New insights & better client experience
- Faster time to market
- Innovate in securely and consistently
- Modernize 66% more applications
- Consistent skills and agile devops
- Automation and less rework
- 95% incident reduction / higher resiliency
- Greater utilization
- 10% infrastructure cost savings
- Single pane of control
- Consistent security & compliance policies
- Automation across stack
- Avoid vendor lock in
- Match workloads to right cloud model
- Optimize cost by moving workloads

Keep Control of your Data and reduce risk across a Hybrid Cloud



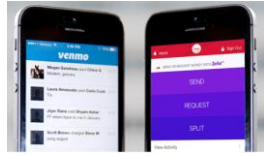
Data security/privacy and regulatory compliance require additional focus as workloads are deployed to public cloud

Hyper Protect Hybrid Cloud – With Built-in Data Security and Privacy
Industry-compliant cloud services that incorporate regulatory requirements



Middle office applications can be deployed across hybrid – either in private or public cloud

Example Solution View – Lending Solutions across Enterprise



**Mortgage
Payment app**
on Public Cloud

Public Cloud



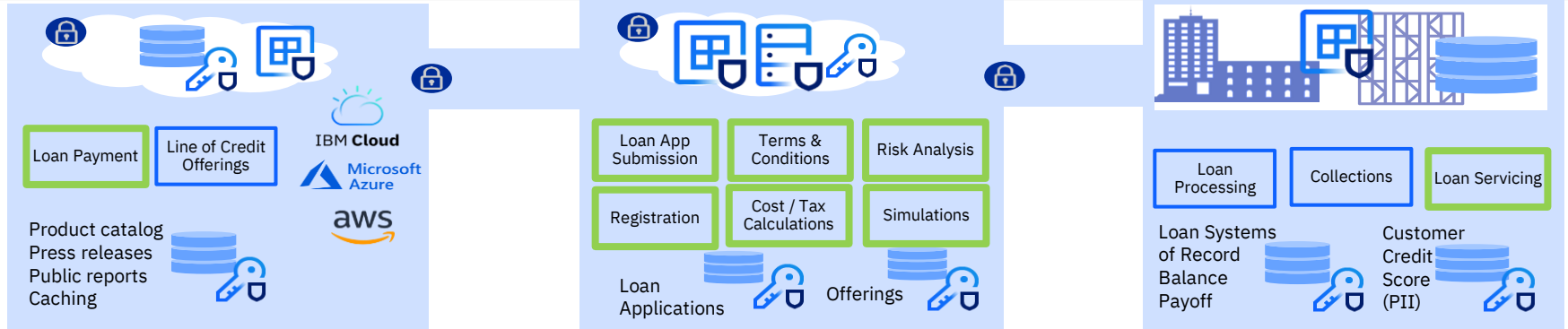
Loan Origination app
on OpenShift
Private/Public Cloud

Private & Public Cloud



**Loan Processing
System**
On-Prem

Systems of Record On-Prem



Total Data Privacy – End2End Data Protection – Data Centric Zero Trust

Protected Applications (Workload)

- Hyper Protect Virtual Server
 - IBM public Cloud
 - Private Cloud (LinuxONE)
 - Systems of Record (LoZ)

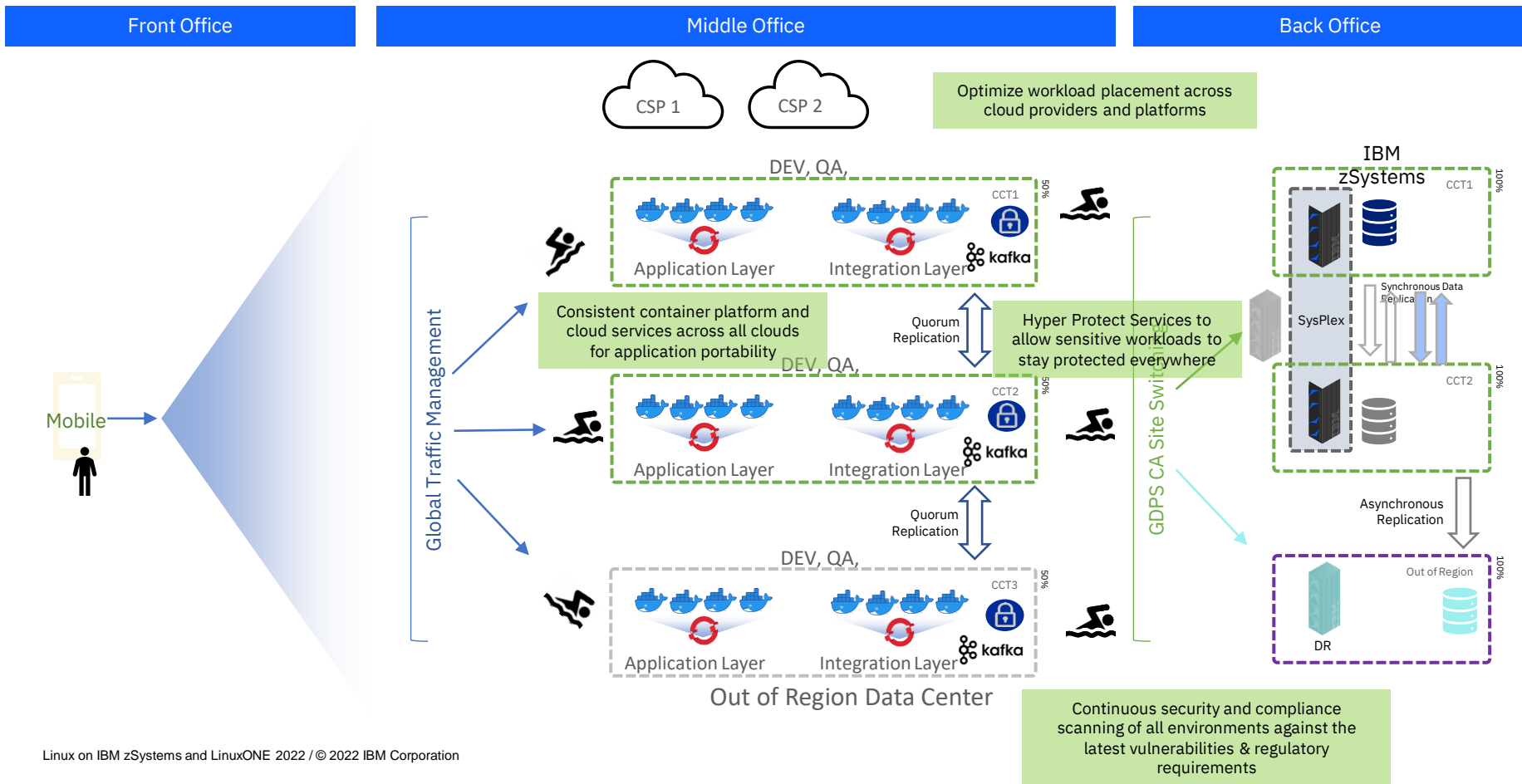
Protected Data at Rest

- Hyper Protect DataBases
 - IBM public Cloud
 - Mongo, PostgreSQL
- Baffle.IO
 - Field Level Protection

End-End Key Management for Hybrid Cloud

- Hyper Protect Crypto Services
 - IBM public Cloud
 - Keep Your Own Key
- Multi Cloud Key Orchestrator
 - IBM Cloud, Azure, AWS

The right deployment architecture helps mitigate these risks

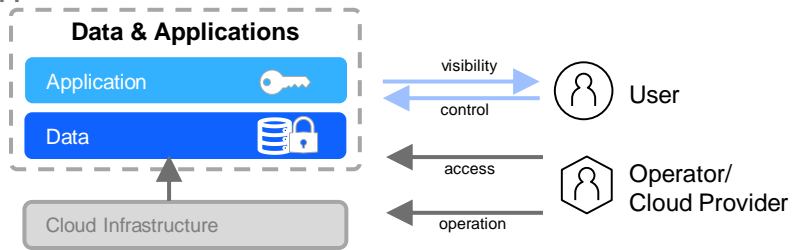


Regulated clients require technical assurance. Operational assurance is not sufficient.

Operational assurance

“Cloud provider **will not** access your data”

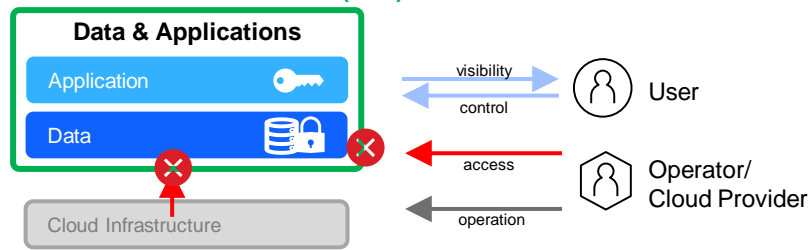
Application Execution Environment



Technical assurance

“Cloud provider **cannot** access your data”

Trusted Execution Environment (TEE)



Go beyond confidential computing for the highest level of privacy assurance. Protect data in use with complete authority, with an integrated developer experience.

These capabilities are where we can differentiate vs AWS, Azure, and GCP!

IBM zSystems in IBM Public Cloud

One System that does it all:

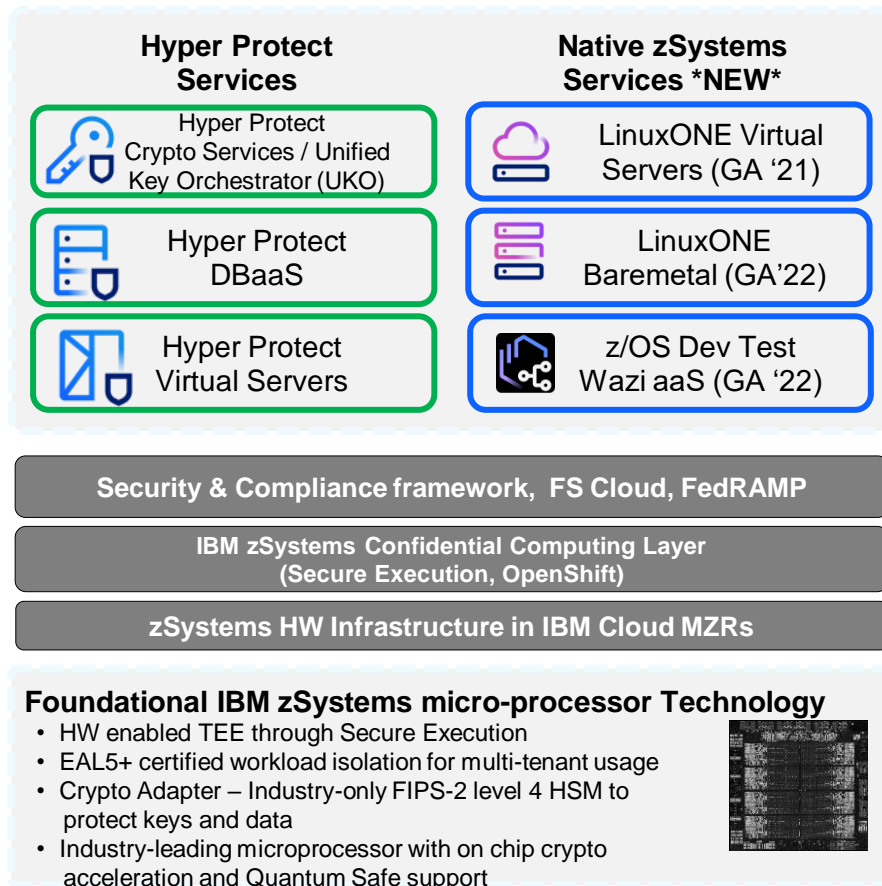
A technology stack constructed to combine virtual cloud flexibility of IBM Cloud with the enterprise strength of IBM zSystems. One system, many options.



Hyper Protect Services enables Confidential Computing and enable IBM Cloud's regulated industry cloud.



Native zSystems services form the portfolio to serve zSystems clients in the public cloud and enable Hybrid Cloud use cases.



IBM Cloud Hyper Protect Crypto Services feature: Unified Key Orchestrator



Easy management of encryption keys
across multicloud deployments with
Unified Key Orchestrator

Hyper Protect Crypto Services

+ **Unified Key Orchestrator (UKO)**

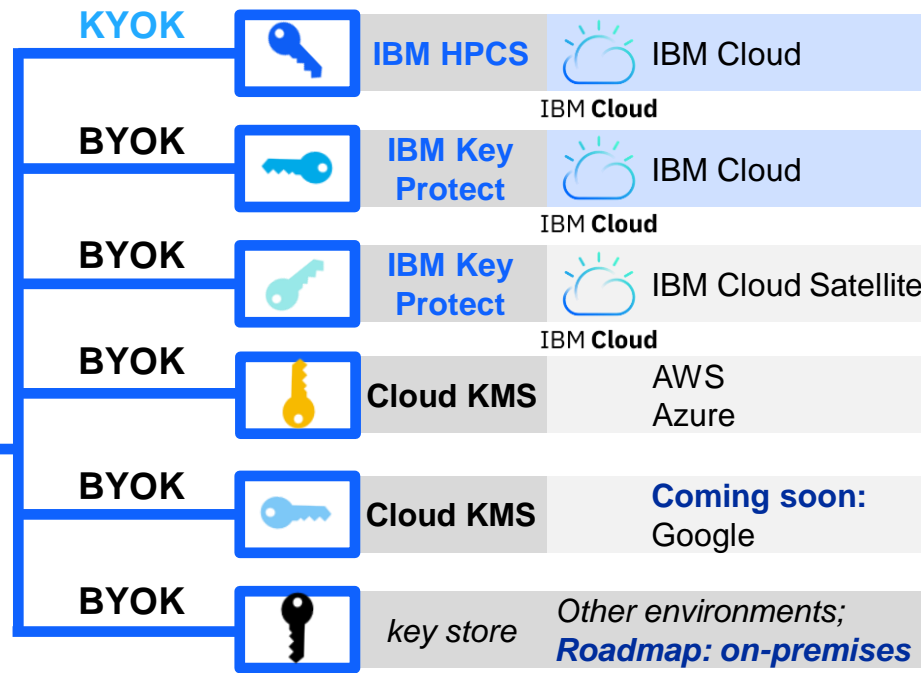
EP11 HSM with Master Key



IBM Cloud

IBM Z as a Service

** Built on FIPS140-2 Level 4 Certified Hardware – Level 4 is the highest achievable level*



LinuxONE IaaS enables Hybrid Cloud for Linux on Z!

New



LinuxONE Virtual Servers

The industry's only LinuxONE Virtual Servers with greater performance and a seamless hybrid cloud experience in IBM Cloud VPC



LinuxONE Bare Metal

LinuxONE managed single-tenant LPAR in IBM Cloud VPC for high performant workloads

GA 2Q22



Hyper Protect Virtual Servers

Complete authority over your LinuxONE Virtual Servers for workloads with sensitive data or business IP

Basic LinuxONE Compute options

Confidential Computing LinuxONE Compute

These new capabilities bring the game-changing benefits of public cloud to IBM Z and LinuxONE

- Empower our clients to capture the benefits of Hybrid Cloud for their LinuxONE / Linux on Z investment
 - On-demand infrastructure in minutes
 - Cost effective LinuxONE compute by only provisioning resources needed for the job
 - Option to configure with best in class Confidential Computing Capabilities
- All founded with the security and performance of IBM LinuxONE



Hyper Protect Crypto Services

Keep your own keys for data encryption and orchestrate keys across public and private clouds

Hyper Protect Services offers end to end protection



Hyper Protect Crypto Services

WITH UNIFIED KEY ORCHESTRATOR

Keep your own keys for data encryption protected by a dedicated cloud HSM*

* Industry's only FIPS 140-2 Level 4-certified HSM



Hyper Protect DBaaS

Complete data confidentiality for your sensitive data

(PostgreSQL, MongoDB EE)



Hyper Protect Virtual Servers

Create Linux VMs with own public ssh key to maintain exclusive access to code and data

(Ubuntu, BYOI)

Transition to

Hyper Protect Virtual Servers for VPC

Complete data privacy and protection over your containerized workloads with sensitive data or business IP.

Isolation from the OS and Hypervisor vulnerabilities via Secure Execution Technology

Isolation between instances

Technical assurance that even IBM cannot access the environment

Only you have access to your data, encryption keys and workloads. Even the IBM cloud admin has no access!

[Demos and Code Patterns](#)



Hyper Protect Virtual Servers OnPrem Roadmap



HPVS v2.1

Hyper Protect Virtual Servers v2.1

- **Hyper Protect Container Runtime**
 - Flexible Deployment as KVM rather than LPAR
 - Leverage existing Hypervisor, Middleware and Management
 - Harden Hyper Protect Layer with Container Runtime
 - Encrypted Multi-Party Contract
 - Integrated Data-at-rest volume encryption
- **Crypto Express Network API for Secure Execution Enclaves**
 - Digital Asset requirement for z15 customer base

HPVS v1.2.7

- PSIRT/HA4.4 update
- RedHat Simple Signing for ICR
- ISV secrets
- SUSE registry support
- ILMT support

- Secure Build support for HPCR
- Multi-OCI support within enclave
- Data-at-rest encryption BYOK with CEX Adapter

More to come...

9/28/2022

10/14/2022

In development*

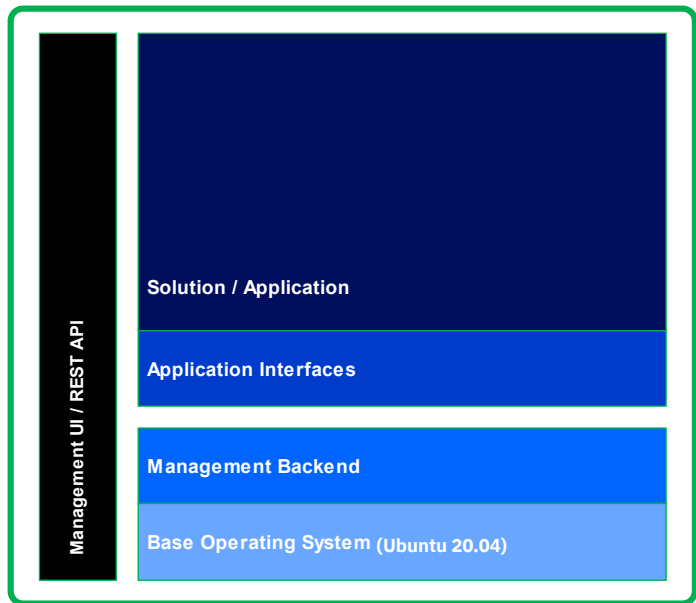
Future

* Future dates and availability are subject of change without notice

Confidential Computing Progression – Secure Execution for Linux

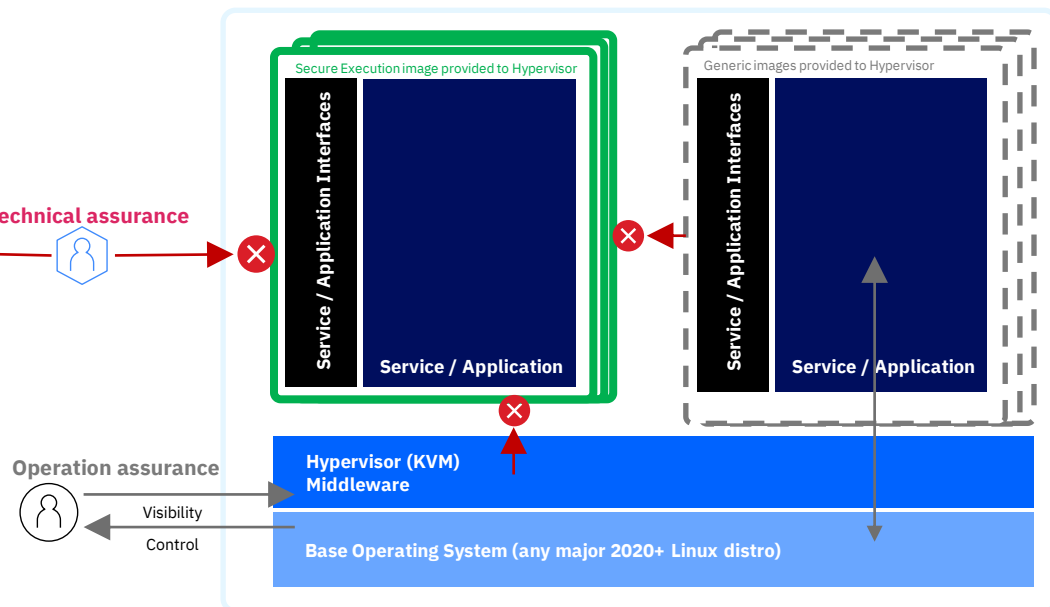
Secure Service Container

“The LPAR is the enclave”



Secure Execution

“Selective KVMs/Services run in individual enclaves”



Confidential Computing Platform Enhancements (IBM z16 and LinuxONE Emperor 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 Artemis system. Beside 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

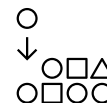
Attestation provides cryptographic assurance to the customer that a given workload is executed in a Secure Execution enclave. It is an explicit ask by customers and compliance that an enclave is in the position to provide proof for computing confidentially



Quantum-Safe Confidential Computing

Quantum-Safe Foundation for Secure Execution

Foundational support for Quantum-Safe Secure Execution enclaves.



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

Enabling a broad range of new and existing client scenarios across industries

Financial services and digital assets		Meeting the stringent security and compliance requirements around data and key protection
Banking and payments		Scalable privacy across mobile wallets to micro payments
Federated AI - Organized Crime Identification	 Industry Organization	A secure platform for collaboration between organizations using distributed AI to find patterns of Organized Crime.
Healthcare		Enabling user privacy and protecting PII—from Cloud to mobile
From enterprises to startups		Protecting data and privacy with exclusive control—across automobile, grid and retail

IBM leads the industry in Confidential Computing

	IBM Cloud	Azure	AWS	GCP
Confidential Infrastructure				
Confidential Databases		 <small>*Always Encrypt</small>		
Managed Crypto/Key services - KYOK				
Secure Build Server				
Confidential Containers				 <small>In Beta</small>

 Supported
 Alternative approach
 Not supported



"Outstanding for Confidential Computing: IBM Cloud" [June 2021]



"IBM Cloud platform strategy is focused on leveraging differentiated, confidential computing and policy based cloud security frameworks that enable enterprises to build cloud-native and hybrid architectures without compromising data security. This framework helps enterprises avoid accidental data, platform exposure due to misclassification and other security risks" [May 2021]

zCAT to support your confidential computing journey

Hyper Protect Client Acceleration Team

- Accelerate client adoption of HPS hybrid cloud solutions (cloud and on-prem) through evangelism, demos, POC, code patterns, solution consulting, deployment, scale
- Also provide feedback on engagement experience, identified gaps, and lessons learned back to product managers and development teams to improve HPS products and time-to-market
- Deliverable examples
 - [Hyper Protect Solution Patterns](#)
 - UKO demo videos
 - [AWS S3 demo](#)
 - AZURE demo (tba)
 - Tools
 - [Using IBM Cloud Code Engine for automation](#)
 - [UKO - AWS key End - End automation](#)
 - [Deploy MongoDB on HPVS for VPC \(Gen2\)](#)
 - [Integrating HPCS to Wazi custom image builder](#)
 - [More Terraform examples](#)

Contact us

- via email zCAT@ibm.com
- via Slack [#ask-hyper-protect](#)
- You can also contact JC Yao via jcy@us.ibm.com for urgent requests



