Hyper Protect Virtual Servers Wildfire Workshop

Introduction to Hyper Protect Virtual Servers

Barry Silliman
Garrett Woodworth
Jin VanStee

Introduction to Hyper Protect Services

Hyper Protect Virtual Servers Hosting Appliance Setup Overview

Hardware Security Module Exploitation Lab Introduction (GREP11)

Hardware Security Module Exploitation Lab

Secure Build Lab Introduction

Secure Build Lab

What is Hyper Protect?

IBM Cloud Hyper Protect Offerings

Hyper Protect Virtual Servers on-premises

Demo

Key goals and challenges of cloud adoption

- **Modernize** workloads through **containers**
- **Integrate** on and off prem environments
- **Embrace** DevOps, microservice, etc.
- **Invest** in existing infrastructure

- **Cost** of setup and maintenance
- **Increased attack vector** surface and **risk of data breach**
- **Downtime** and other impacts to business or reputation
- Difficulty **maintaining compliance**

Cloud Adoption: Security concerns & threats

62%

Data Privacy and Confidentiality[1]

- **Unauthorized access**
- **Malicious insider threats**
- Malware
- Human Error
- A combination

70%

Enterprises experienced an insider threat in the past 12 months[2]

What has made it more difficult to prevent?

- Insiders already have access to the network and services
- Increased use of applications that can leak data
- Increased amount of data that leaves protected boundary

How can organizations adopt cloud while minimizing security risks?

Data Breaches – How can we Hyper Protect?

suprema BIOMETRICS & SECURITY

28 million
Fingerprints, facial data

CapitalOne

106 million
Credit scores, addresses, names

Marriott starwood Hotels and Resorts

383 million
Credit card numbers

100 million
Log in credentials

moviepass™

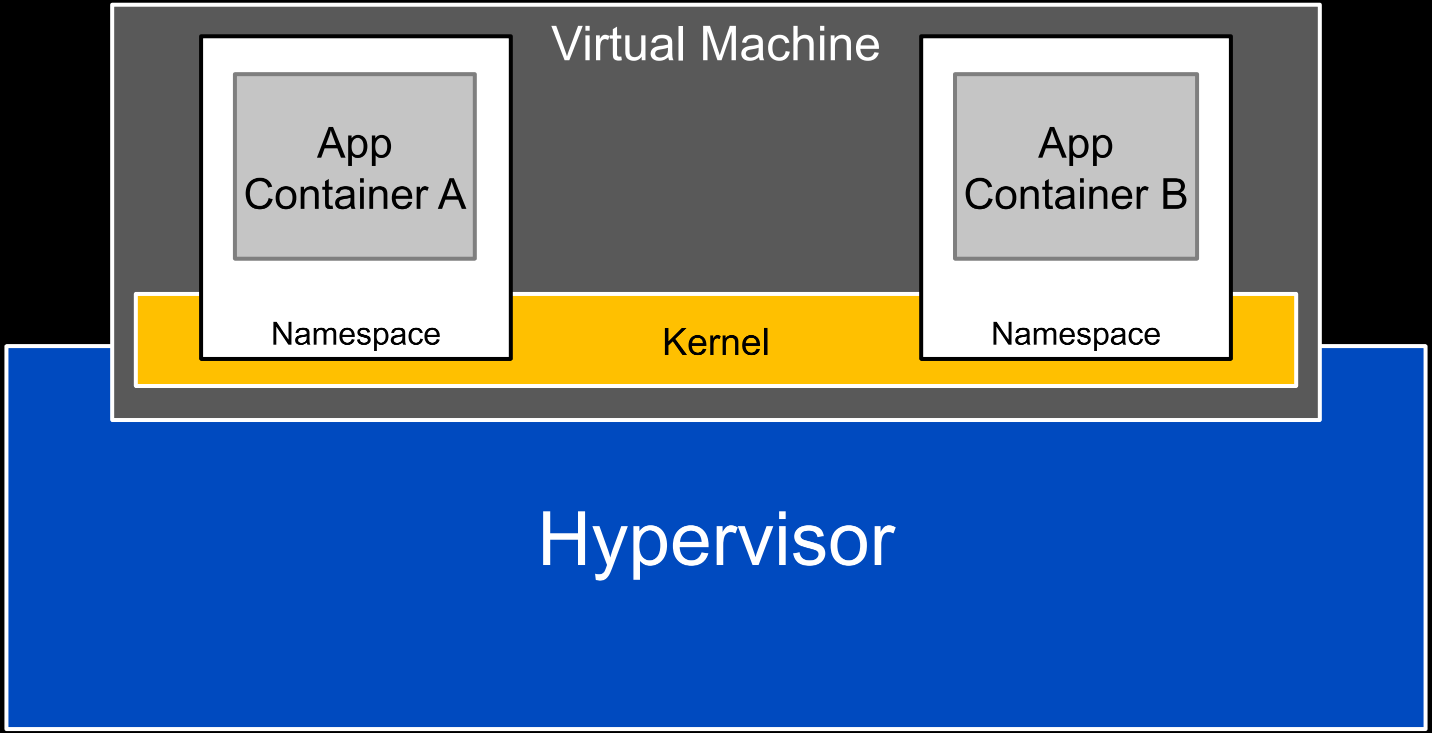
160 million
Credit card numbers

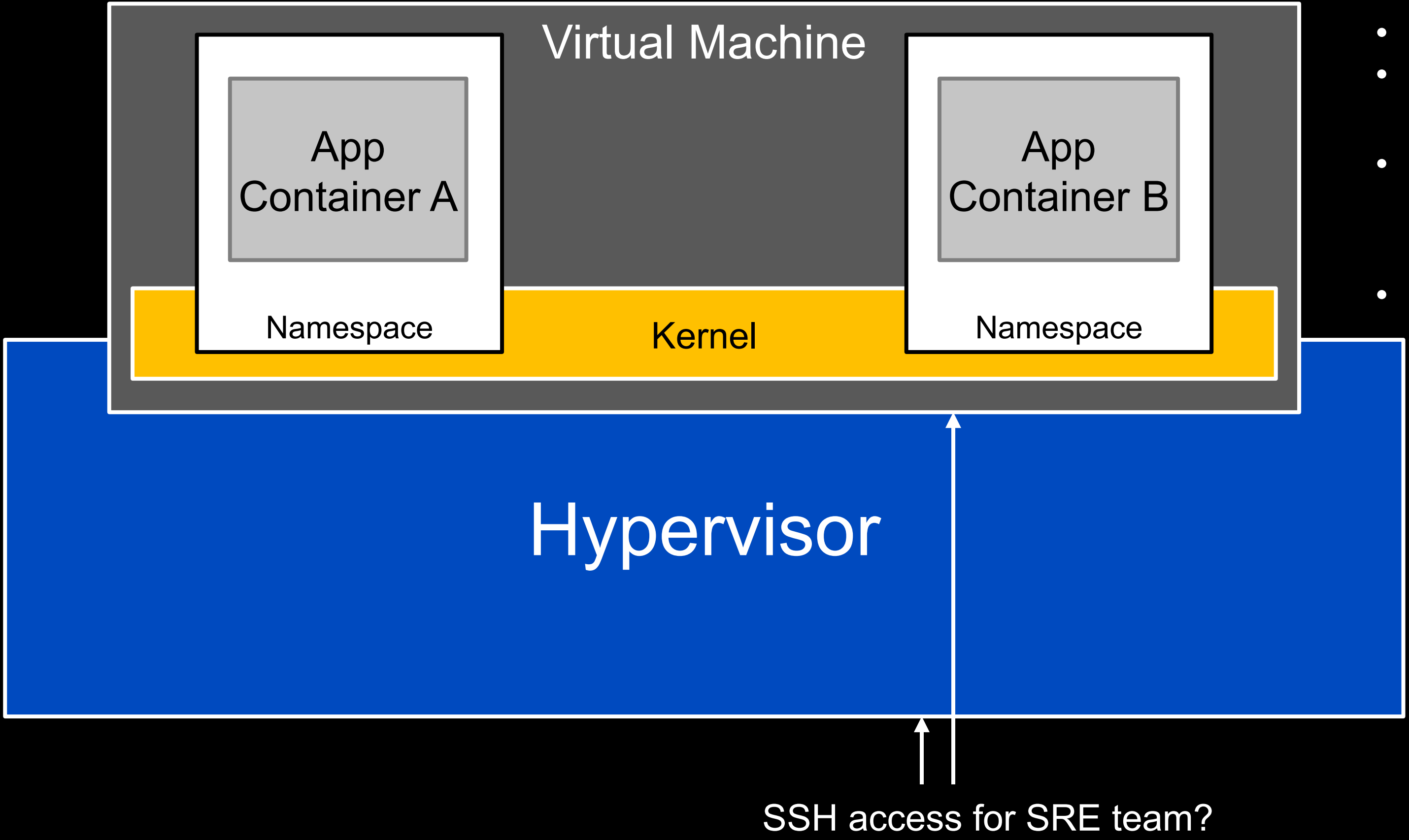
Most data breaches caused by unencrypted sensitive data or insider attack - IBM Hyper Protect Services mitigates this risk

✓ All data-at-rest and data-in-flight is encrypted

✓ Reduced attack surface for insider and privileged attacks

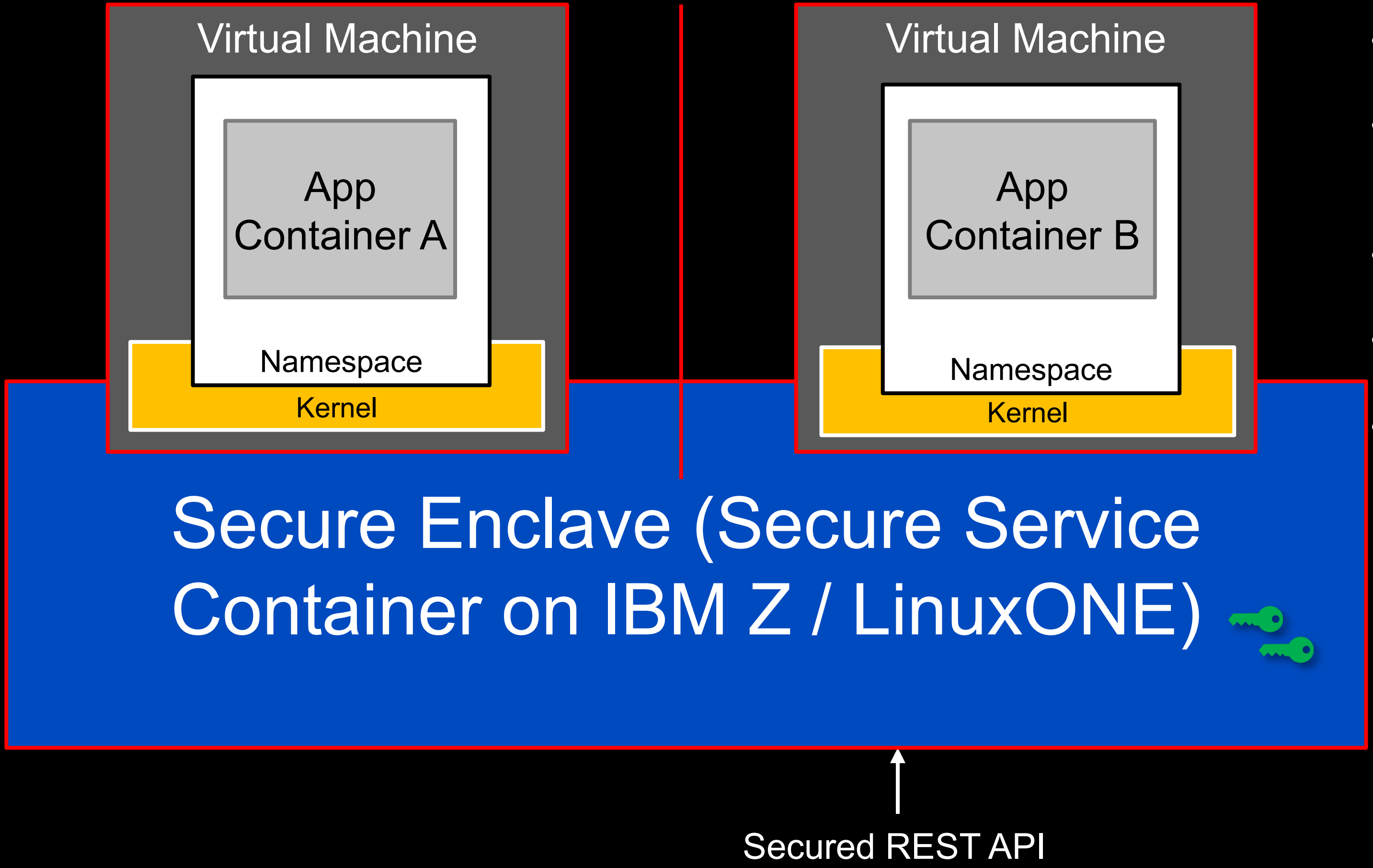
Hyper Protect Foundations


Virtual Machine
App
Container A
Namespace
App
Container B
Namespace
Kernel
Hypervisor



SSH access for SRE team?

- Storage encrypted?
- Application images correct and verifiable?
- Can SRE team / System admins access your customers' data?
- How thick are the walls between tenants and between hypervisors?



- Encryption keys never leave the box
- Use only signed and trusted application and firmware images
- Remove all access methods
- Add defined, restrictive secured REST API
- Maximize wall thickness

IBM Cloud Hyper Protect offerings

IBM Cloud Hyper Protect Services

Industry-leading security for Cloud data, digital assets and workloads

Hyper Protect Crypto Services

GA

Keep your own keys for cloud data encryption protected by a dedicated, fully managed cloud Hardware Security Module (HSM)*

Promo Codes offered for up to 30 days

- * Built on industry's only FIPS 140-2 Level 4 certified HSM

Hyper Protect DBaaS

GA

Complete data Confidentiality for your sensitive data

Get started with free version on the IBM Cloud [PostgreSQL](#) [MongoDB](#) EE

Hyper Protect Virtual Server

GA

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

Get started with free version for 30 days

(Ubuntu, BYOL**)

** Support for RHEL in plan

Only you have access to your data, encryption keys and workloads

Even the IBM cloud admin has no access!

[Demos and Code Patterns](#)

Built On IBM LinuxONE

LinuxONE secure enclaves

Secure Service Container

Technical vs. Operational Assurance

Technical Assurance

"IBM cannot access your data"

Based on:

- **Technical proof**
- **Data Encryption**
- **Runtime Isolation**

...and we prove that it is technically impossible...

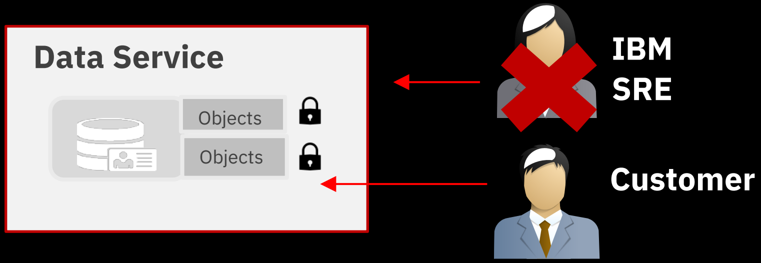
Operational Assurance

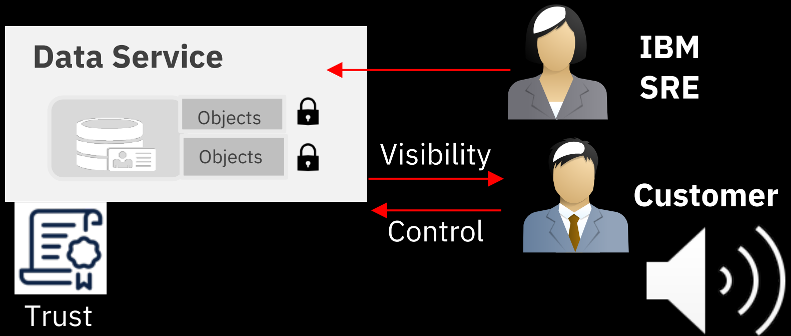
"IBM will not access your data"

Based on:

- **Trust** (external certifications)
- **Visibility** (audit log via ActivityTracker)
- **Control** (cryptographic erase via BYOK)

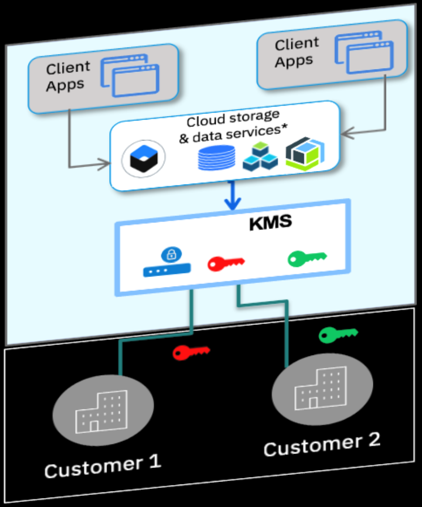
...and if we would, you would find out and could pull the plug...





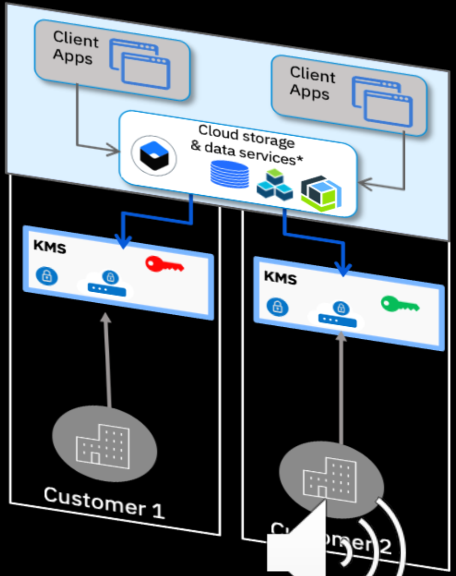
Keep Your Own Keys (KYOK) provides technical assurance that IBM *cannot* access the keys, with industry's highest level of security

Industry's Bring Your Own Keys (BYOK)



Industry BYOK	Cloud key management capabilities	IBM's KYOK
✓	Customer key lifecycle management	✓
✓	As a service. Integrated with Cloud services	✓
✓	Client can bring their keys from onprem HSM	✓
✓	Operational assurance - provider will not access keys	✓
	Technical assurance - IBM can not access the keys	✓
	Single tenant, dedicated KMS	✓
	Client has exclusive control of HSM's master key	✓
	Highest level security – FIPS 140-2 Level 4 HSM	✓
	Client manages master key, with smart card	✓
	Client can perform key exchange ceremony	✓

IBM's Keep Your Own Keys (KYOK)

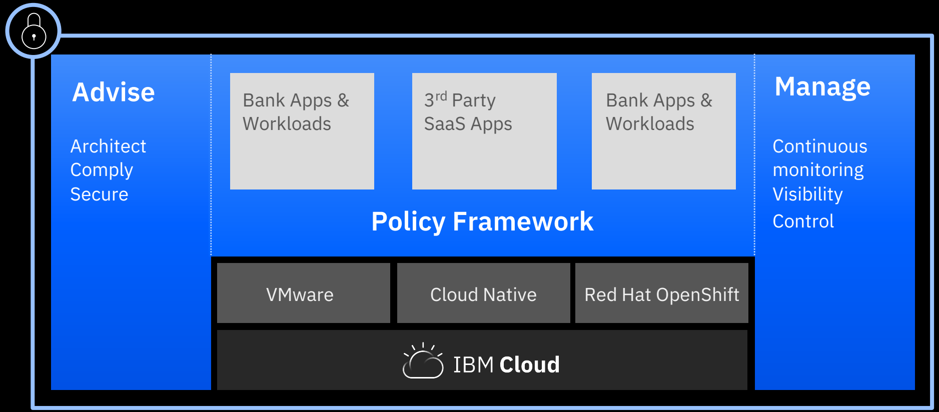


Hyper Protect Crypto Services

World's first Financial Services-ready public cloud

IBM has designed the **world's first financial services-ready public cloud** to address FSS institutions' requirements for regulatory compliance, security and resiliency. IBM will welcome financial services institutions, and their suppliers, to join the financial services-ready public cloud. As its first collaborator, Bank of America will use the platform built on IBM's public cloud to host key apps and workloads.

- Rich catalog of trusted ISV and SaaS solutions
- Robust Financial Services Policy Framework
- Extensive infrastructure services – VMware, cloud-native, Red Hat OpenShift as-a-service
- Secure and enterprise grade, built on IBM's public cloud
- Promontory risk analysis and security regulation consulting and expertise on-demand.



Financial Services-ready Public Cloud

IBM Cloud today offers unique technologies for trusted computing:

- Monitoring and security to the microchip level
- Highest level of encryption certification
- Robust isolation options and data protection
- Data immutability with Hyper Protect Services
- Risk analysis, security consulting, and IBM Promontory industry expertise.

Customer Value: Securing Sensitive Data & IP in the Public Cloud

Benefits

- Industry-leading security for Cloud data and digital assets
- Respond to market changes with enhanced agility – wherever you are in your cloud journey
- Reduced data compromise risk due to in-built protection against privileged access threats
- Regulatory compliance through data encryption and controls on privileged access

Enabling large enterprises and innovative new use cases

VICOM Infinity

VIVA

Cloud-Based Voice Assistant for Securing Enterprise Data

SOLITAIRE INTERGLOBAL

Media Streaming while securing Intellectual Property

Onchain Custodian

IDSR

New Frontiers: Crypto Currency Trading and Digital Asset Custody Service

Geens

Enabling members to store their private digital information securely and share only with stakeholders that they choose

On-premises Hyper Protect Offerings

IBM Hyper Protect virtual servers

A secure virtualization platform that protects your critical Linux® applications during build, deployment, and management lifecycle phases on IBM Z® and LinuxONE

Build applications with integrity

Leverage the secure image build process to sign images, validate code, and integrate into your CI/CD pipeline

Deploy workloads with trust

Validate the provenance of your applications before deployment

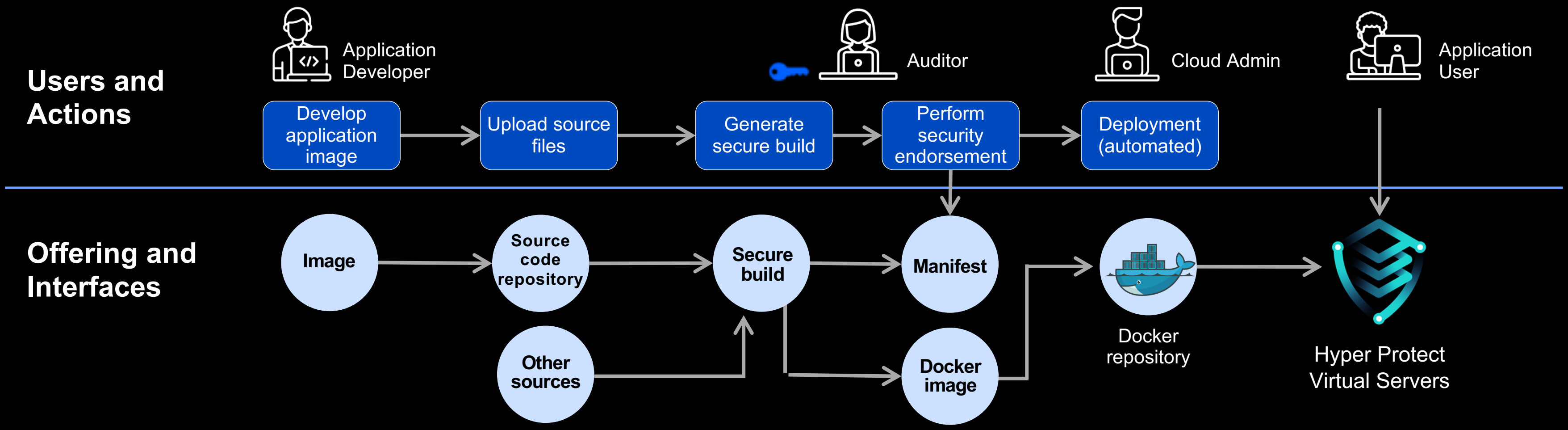
Manage applications with simplicity

Manage your infrastructure without visibility to sensitive code or data – RESTful API deployment

Encrypt & Sign critical solution components

Give your images access to the industry leading FIPS 140-2 level 4 Hardware Security Module for signing and encryption needs

Trusted CI/CD stages: Bring your own image, sign, register, approve and deploy



Users and Actions

Application Developer

Auditor

Cloud Admin

Application User

Develop application image

Upload source files

Generate secure build

Perform security endorsement

Deployment (automated)

Offering and Interfaces

Image

Source code repository

Other sources

Secure build

Manifest

Docker image

Docker repository

Hyper Protect Virtual Servers

Workload Lifecycle Phases

- Code Development
- Workload Build
- Pre-Production
- Production

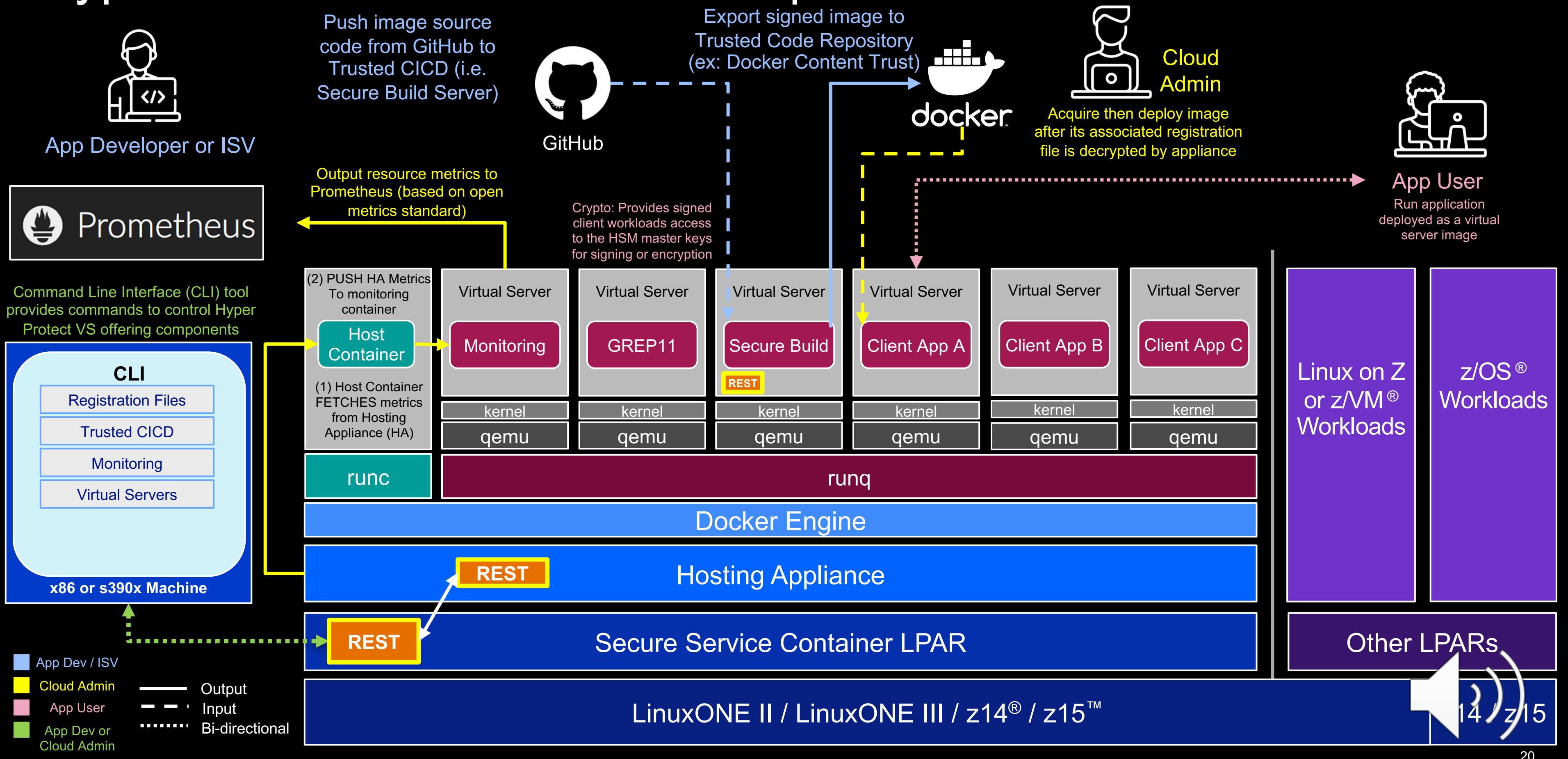
Threat Vectors pose Potential Risks

- Alter workload
- Alter build environment
- Modify workload deployment conditions
- Secrets visible to admin

How Hyper Protect Virtual Servers COMBATS risks:

- Sign application via secure build flow
- Encrypt and register application configuration info
- Validate image provenance via workload **manifest**
- Decrypt application registration file – only possible vi[illegible]cure Service Container (confidential computing environmen[illegible]
- Manage infrastructure via only RESTful interfaces

Hyper Protect virtual servers on-premises – Architecture



App Developer or ISV

Push image source code from GitHub to Trusted CICD (i.e. Secure Build Server)

GitHub

Export signed image to Trusted Code Repository (ex: Docker Content Trust)

docker

Cloud Admin

Acquire then deploy image after its associated registration file is decrypted by appliance

App User

Run application deployed as a virtual server image

Prometheus

Output resource metrics to Prometheus (based on open metrics standard)

Crypto: Provides signed client workloads access to the HSM master keys for signing or encryption

Command Line Interface (CLI) tool provides commands to control Hyper Protect VS offering components

CLI

Registration Files

Trusted CICD

Monitoring

Virtual Servers

x86 or s390x Machine

(2) PUSH HA Metrics To monitoring container

Host Container

(1) Host Container FETCHES metrics from Hosting Appliance (HA)

Virtual Server	Virtual Server	Virtual Server	Virtual Server	Virtual Server	Virtual Server
Monitoring	GREP11	Secure Build REST	Client App A	Client App B	Client App C
kernel	kernel	kernel	kernel	kernel	kernel
qemu	qemu	qemu	qemu	qemu	qemu

runc

runq

Docker Engine

REST

Hosting Appliance

REST

Secure Service Container LPAR

Linux on Z or z/VM® Workloads

z/OS® Workloads

Other LPARs

LinuxONE II / LinuxONE III / z14® / z15™

z14 / z15

🟦	App Dev / ISV
🟨	Cloud Admin
🟪	App User
🟩	App Dev or Cloud Admin

———	Output
— —	Input
·······	Bi-directional

Where it matters

A Secure Infrastructure Foundation

IBM Hyper Protect Virtual Servers serves as both a solution for clients to securely build Docker based applications on IBM Z and LinuxONE and a foundational component of IBM solutions

Hyper Protect Digital Assets Platform

Enables custodians, exchanges, & Distributed Ledger Technology (DLT) ecosystem partners to protect tokenized assets and validate participants for transactions

Data Privacy Passports

Provides a secure host environment to deploy the Passport Controller used for policy enforcement and data transformation in Data Privacy Passports

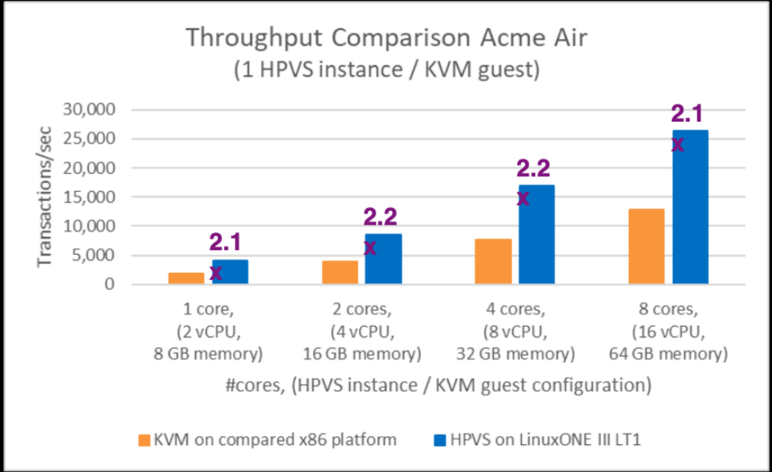
Reduce Regulatory Compliance Scope

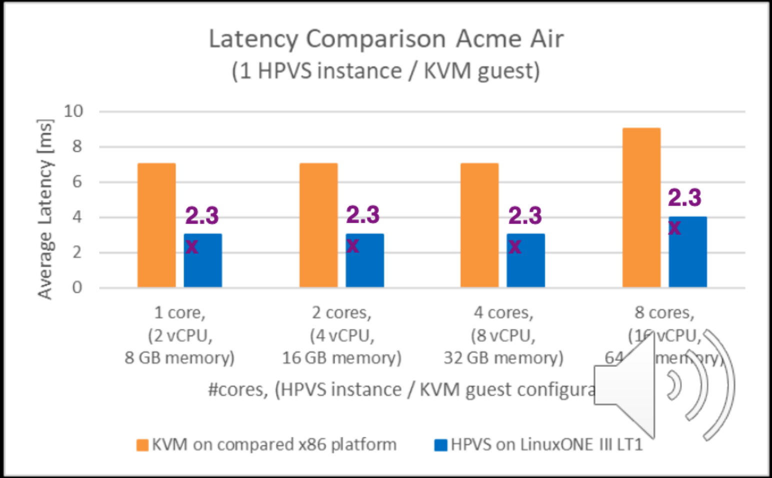
Host sensitive workloads that require a high degree of isolation and data protection to meet security & compliance needs for your organization, industry, or geography

IBM Hyper Protect Virtual Servers

Acme Air Performance on Hyper Protect Virtual Servers on LinuxONE III LT1 vs. under KVM on x86 Skylake

Run the Acme Air benchmark with up to 2.2x more throughput per core and up to 2.3x lower latency on IBM Hyper Protect Virtual Servers 1.2.0 on LinuxONE III LT1 versus on compared x86 platform under KVM with encryption enabled





DISCLAIMER: Performance results based on IBM internal tests running the Acme Air microservice benchmark (https://github.com/blueperf/acmeair-mainservice-java) on Hyper Protect Virtual Servers (HPVS) 1.2.0 on LinuxONE III LT1 versus on compared x86 platform using KVM. One Acme Air instance was running in one HPVS instance on LinuxONE III LT1 and in one KVM guest on x86. Acme Air was driven remotely from JMeter 5.2.1. TLS v1.2 was used to encrypt the communication. Per core the HPVS instance and KVM guest had 2 vCPUs and 8 GB memory configured and 16 driver threads were used. Results may vary. LinuxONE III LT1 configuration: LPAR with 1 - 8 dedicated cores, 128 GB memory, running HPVS 1.2.0. x86 configuration: 1 - 8 Skylake Intel® Xeon® Gold CPU @ 2.60GHz with Hyperthreading turned on, 128 GB memory, running KVM on Ubuntu 18.04. Database volume encrypted via dm-crypt using aes-xts-plain64 with 4k sector size.

What is **your** most valuable data?

What is **your** most valuable data?

Admins don‘t know

What is **your** most valuable data?

Admins don‘t **even *need* to** know

What is **your** most valuable data?

Admins don‘t even *need* to know

But it‘s **protected**

- **Cloud Provider** ✅
- **Hypervisor/System Admin** ✅
- **And even from you***! ✅

* Configurable and flexible based on client needs

Additional Information

Learn More

- Content Solution Page
- Knowledge Center – Technical Docs
- IBM Z Community - Validated Open Source on Z / LinuxONE
- IBM Hyper Protect Services Redbook

Start a Conversation

Contact Offering Manager:
for Additional Help

Diana Henderson,
dmhender@us.ibm.com

See the Value

- Offering Announcement
- Hyper Protect Virtual Servers Webpage
- Secure Service Container Video
- IBM Systems Magazine Article

Digital Assets

Digital Asset Custody Services (DACS

- IBM Blog
- Coindesk Article
- Blockonomi Article
- Crowdfund Insider Article

Phoenix Systems:

- IBM Video
- IBM Case Study

Offer Trial or POC

Contact Offering Manager:

Diana Henderson *dmhender@us.ibm.com*

Hyper Protect Accelerator Program

Blog Entry

IBM Hyper Protect Virtual Servers workshop

http://ibm.biz/hyperprotect-vs

Wallet Hacking Demo

What are Digital Assets?

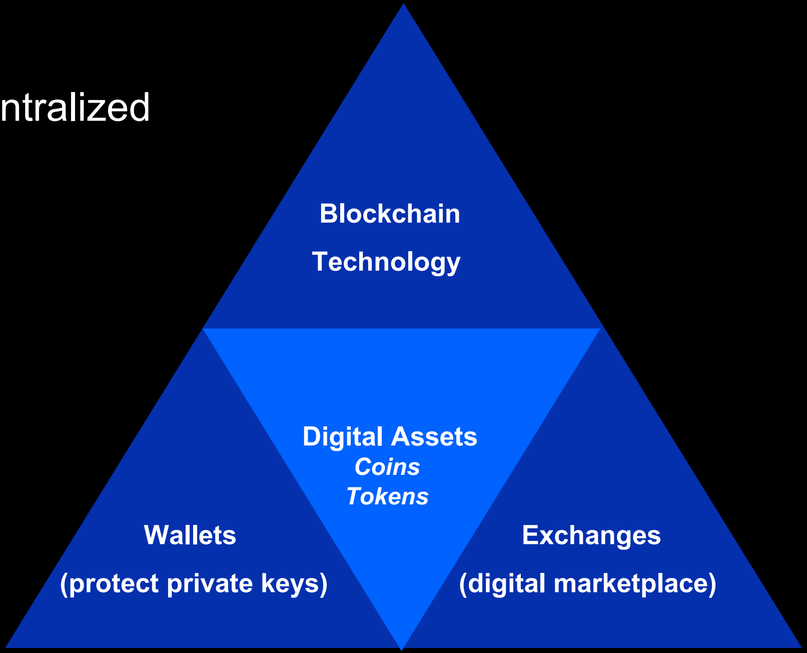
An emerging asset class for digital currency or tokens transacted on a blockchain with ownership rights established using cryptography

Coins

- Bitcoin - 1st cryptocurrency to utilize distributed and decentralized blockchain technology
- **Coins or Altcoins** (alternate coins)
  - Coins other than bitcoin (independent blockchain)
  - Unique blockchain and protocol e.g. Ethereum, Ripple

Tokens

- Digital asset e.g. commodities, loyalty points, gold
- Ledgered using blockchain
  - Ethereum blockchain, ERC-20 standard template
  - Smart Contract technology and DApps (distributed apps)



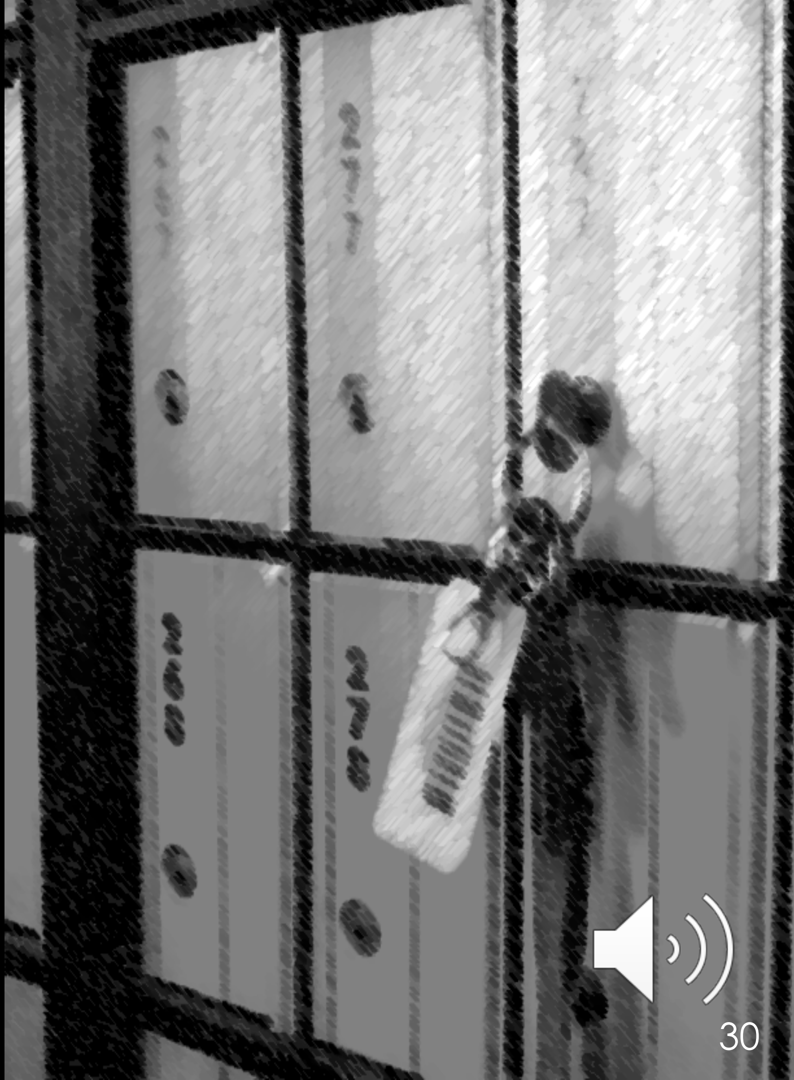
Digital assets are cryptographically secured with a public and private key pair

A public key is like a mailbox, everyone can see it and anyone can send digital assets to it.

The private key is like the key to that mailbox, the owner can open it and access what's inside.

"Wallets" store your private keys, public keys, and public addresses, and let you make transactions.

A "seed" phrase, "seed" recovery phrase or backup seed phrase is a list of words which can be used to recover the private key needed to access digital asset funds.

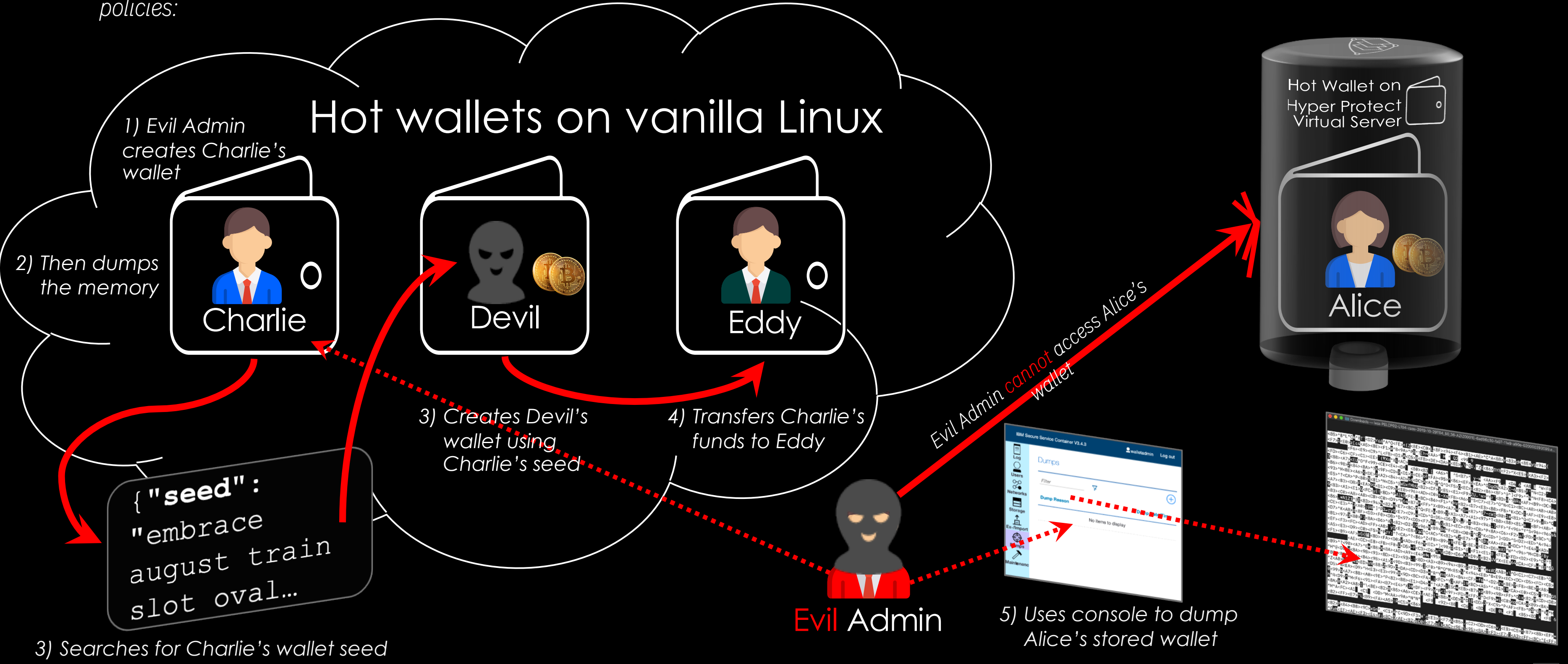


Operational Assurance

Asserted by contracts & policies: *“We won’t steal the private key”*

Technical Assurance

Prevented by technology: “We cannot steal the private key”



Hot wallets on vanilla Linux

1) Evil Admin creates Charlie’s wallet

2) Then dumps the memory

```
{"seed":
"embrace
august train
slot oval...
```

3) Searches for Charlie’s wallet seed

3) Creates Devil’s wallet using Charlie’s seed

4) Transfers Charlie’s funds to Eddy

Hot Wallet on Hyper Protect Virtual Server

Evil Admin cannot access Alice’s wallet

5) Uses console to dump Alice’s stored wallet

Volume dumps are encrypted (& no user data)

Thank you

Resource Requirements

Knowledge Center - Technical Documentation:
https://www.ibm.com/support/knowledgecenter/SSHPMH

Hardware Requirements

- **Linux Management Server**
  - IBM Z / LinuxONE (S390x architecture) or 64-bit x86
  - 1 IFL on Z / LinuxONE or 4 or more x86 Linux cores (2.4 GHz)
  - 16 GB RAM
  - 256 GB Disk Space

- **Secure Service Container Partition – Supported Servers**
  - IBM z15
  - IBM z14
  - IBM LinuxONE III
  - IBM LinuxONE Rockhopper II or IBM LinuxONE Emperor II
  - FC 0104 Container Hosting Foundation

- **Secure Service Container Partition –** Min. HW Requirements (for 1 Hyper Protect VS container + 1 Secure Build container)
  - 2 IFLs
  - 12 GB RAM
  - 190 GB Storage (50 GB Hosting Appliance, 100 GB for 1 Hyper Protect VS container, 40 GB for 1 Secure Build Container
  - *Note: the full resources required on the Secure Service Container partition are heavily dependent on the workload deployed*

- **Networking**
  - **1+ Open Systems Adapter (OSA)**
    - Network between Linux Management Server and Secure Service Container partition or between multiple Secure Service Container partitions
  - **2 Networks to create**
    - Hyper Protect VS containers (internal IP addresses)
    - External request handling to services inside workload deployed in Hyper Protect VS containers
  - **Network Interfaces**
    - Ethernet (Layer 2, Layer 3)
    - VLAN (Layer 2, Layer 3)
  - **Port Mapping**
    - 443: Hosting Appliance REST API
    - 443: Secure Build server or BYOI with Macvlan
    - Any non-rserved port: Secure Build Server
    - 8443: Monitoring infrastructure
    - 9876: GREP11 container
  - **Not Supported**
    - Hipersockets
    - SMC-D
    - SMC-R (RoCE)

- **Crypto Hardware** (optional - PKCS#11 over gRPC i.e. GREP11)
  - Trusted Key Entry (TKE) workstation
  - Crypto Express 7s
  - Crypto Express 6s

Resource Requirements Cont.

Software Requirements

- **Linux Management Server** (Linux 64-bit)
  - Ubuntu 18.04 LTS
  - Ubuntu 16.04 LTS

- **Secure Service Container Partition**
  - Ubuntu 18.04 LTS

- **Docker Versions**
  - V19.03.2 or above (s390x architecture)

- Note: Red Hat and SuSE operating systems are not supported in this initial release but will be evaluated for support in future releases.

Glossary

HPVS- Hyper Protect Virtual Servers	Secure containerized docker image instances able to interact with other cloud services
SBS - Secure Build Service	The process of building the application code from a Git-like source repository into a container image for s390x architecture, signing the image by using the authentication keys, and publishing the image to the remote repository for later integration
BYOI - Bring Your Own Image	part of IBM Hyper Protect Virtual Servers solution to support the development and deployment of your own container images on top of the Secure Service Container framework.
CLI - Command Line Interface	Command Line Interface to manage Hyper Protect Virtual Servers
OCP – Openshift Container Platform	Container Application platform based on based on kubernetes container Orchestrator for application development and deployment
SSC - Secure Service Container	A container framework based on the runq technology, that is supported by the IBM Z or LinuxONE servers.
HA - Hosting Appliance	A component within IBM Secure Service Container based appliances, providing the enablement for running Docker-based workloads.
RunQ	An open-sourced hypervisor-based Docker runtime environment, which is based on runc to run regular containerized images in a lightweight KVM or Qemu virtual machine.
Registry - Docker Registry	A Registry is a hosted service containing repositories of container images that responds to the Registry API. For example, Docker Hub.
Repository - Docker Repository	A repository is a set of containerized images. A repository can be shared by pushing it to a registry server. Different images in the repository can be labeled using tags. For example, hpvsop-base.
Repository Registration File	An encrypted registration file used to register the repository, for authentication or validation reasons, such that a Hosting Appliance will trust that the image, when pulled from the registry, is authentic.
OCI - Open Container Initiative	Open standard for OS level virtualization such as containers