TechU

IBM Cloud Hyper Protect Services Use Cases

Dr Chris Poole
Developer Advocate, IBM

2020 IBM Systems TechU
14 May 2020

IBM

Why Cloud?

Business
No longer always a differentiator to own your own hardware

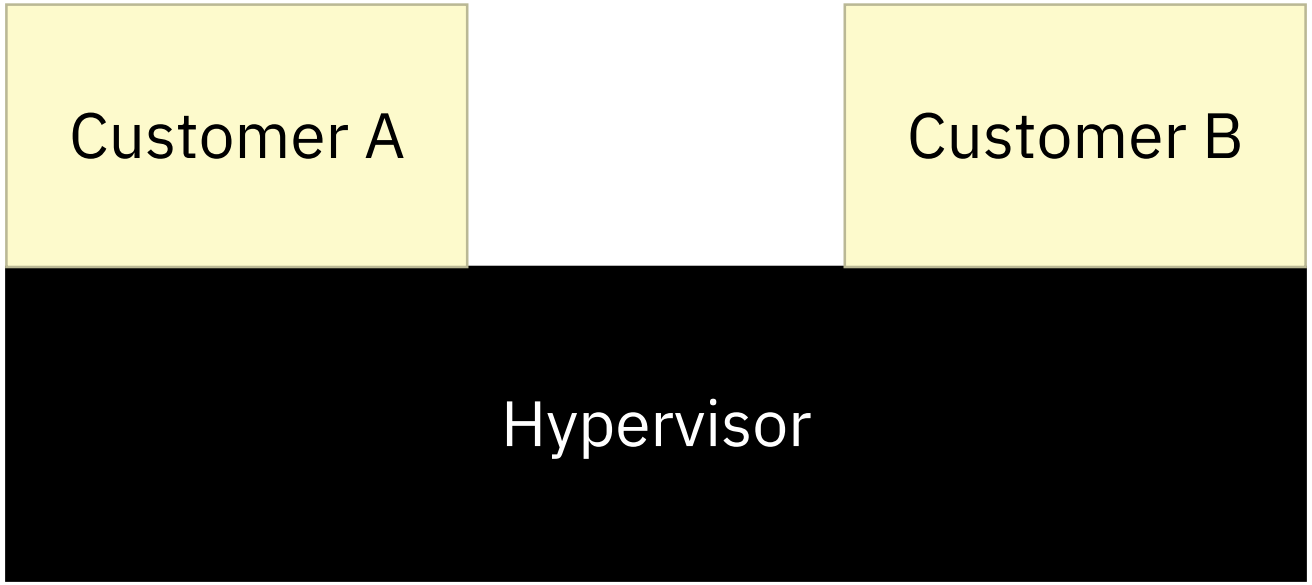
Development
Goal of “here’s my app: make it run!”

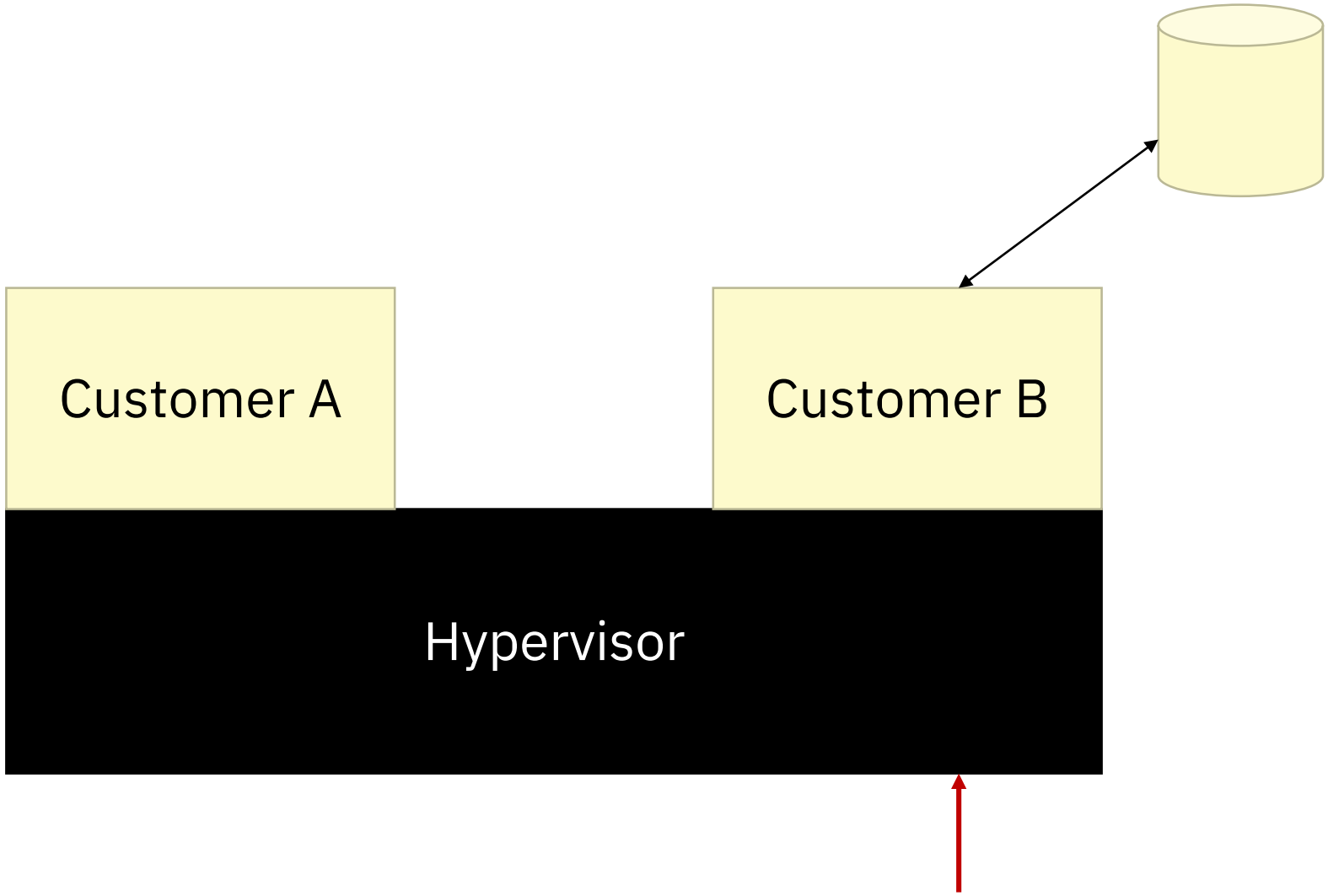
trust

transitive verb
\ ˈtrəst \
1a: to rely on the truthfulness or accuracy of
b: to place confidence in
c: to hope or expect confidently soon
2a: to commit or place in one's care or keeping
b: to permit to stay or go or to do something without fear or misgiving

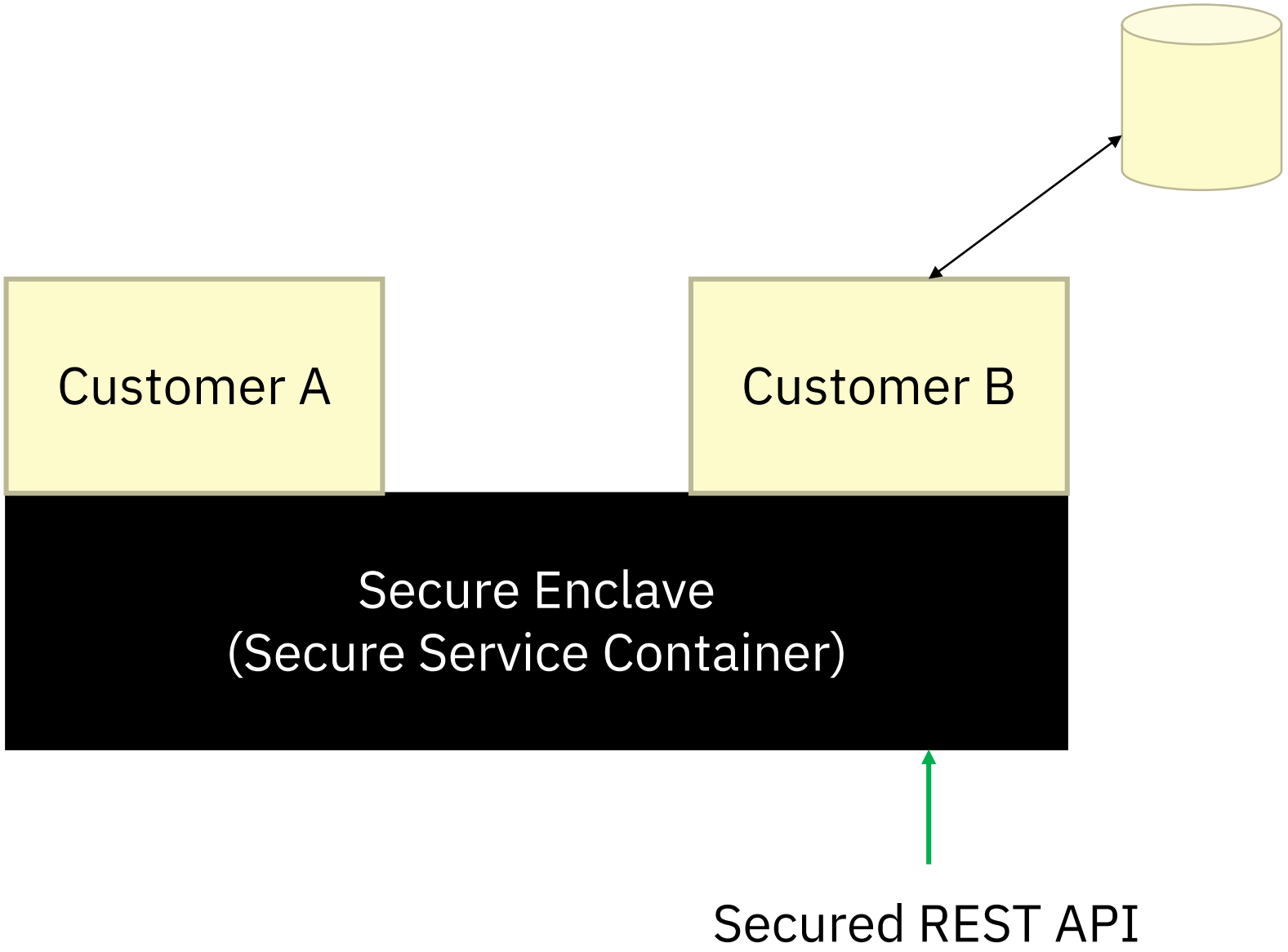
merriam-webster.com/dictionary/trust

In whom or what do you trust? What is most important to you?





- Storage encrypted?
- Application images correct, verified?
- Can SRE team access your customers' data?
- How thick are the walls?



- Encryption keys never leave the box
- Use Docker Content Trust
- Remove all access methods
- Add defined, restrictive, secured REST API
- Increase wall thickness

Cryptography necessitates secure key storage

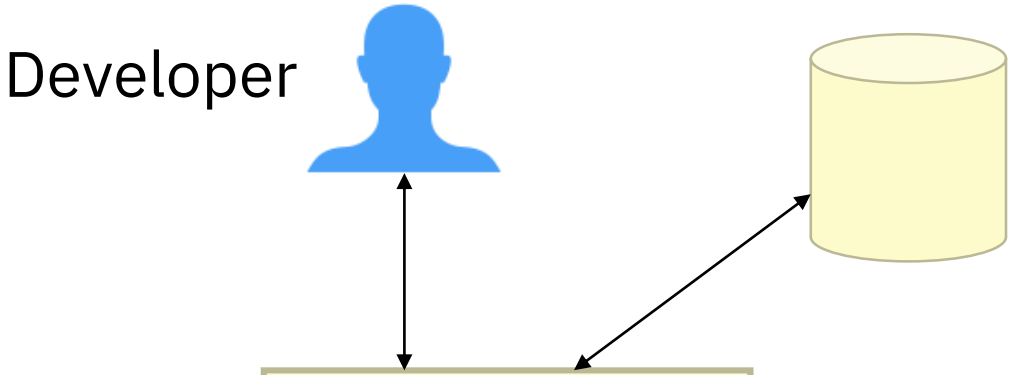
Hardware Security Module

Purpose-built hardware device to securely store keys

FIPS 140-2

1. No specific physical security mechanisms are required
2. Requires features that show evidence of tampering, including tamper-evident coatings or seals
3. Attempts to prevent the intruder from gaining access, zero plaintext, etc.
4. Provide a complete envelope of protection around the cryptographic module including environmental protection

Hyper Protect Crypto Services



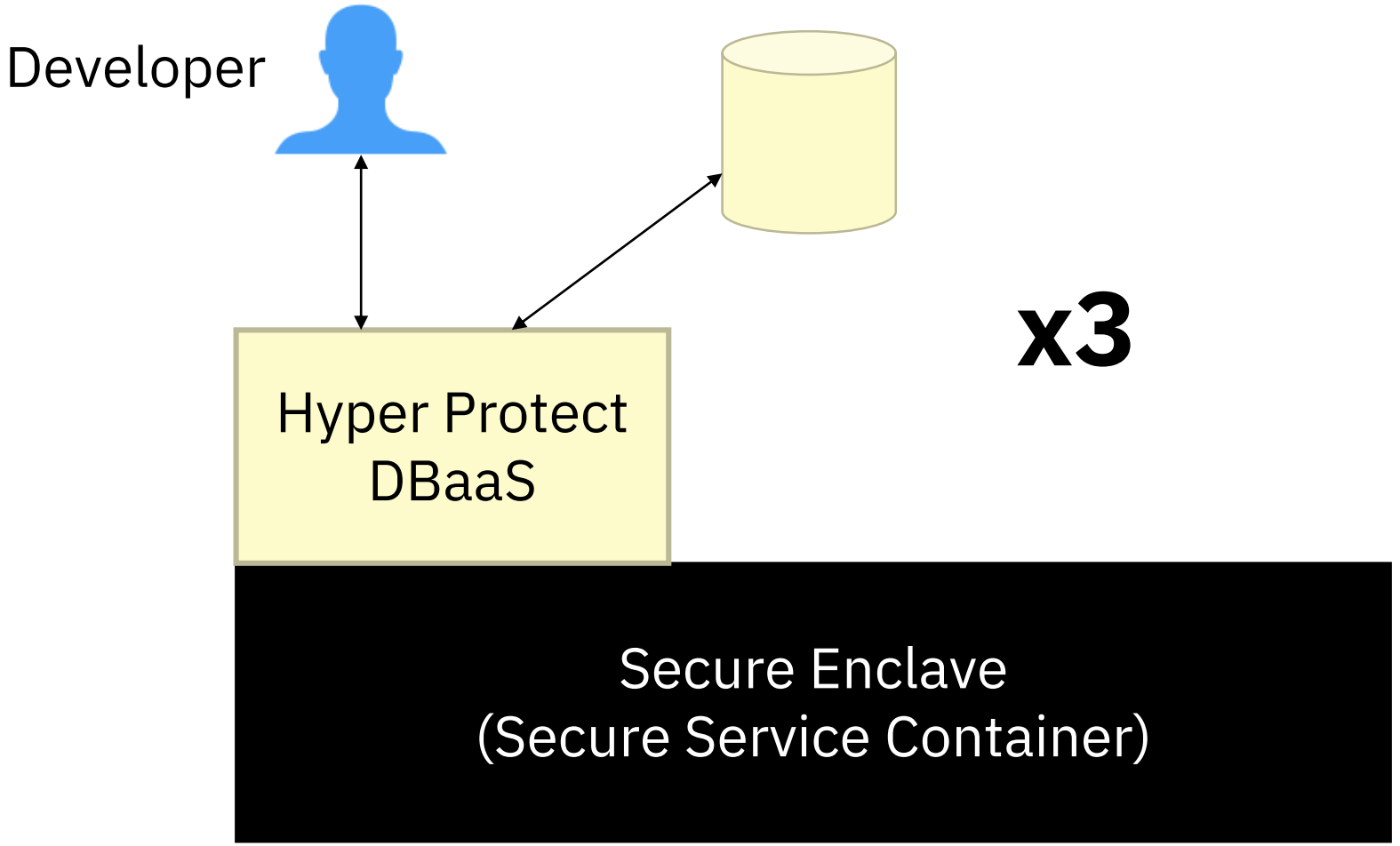
Hyper Protect Crypto Services

Hardware Security Module

Secure Enclave (Secure Service Container)

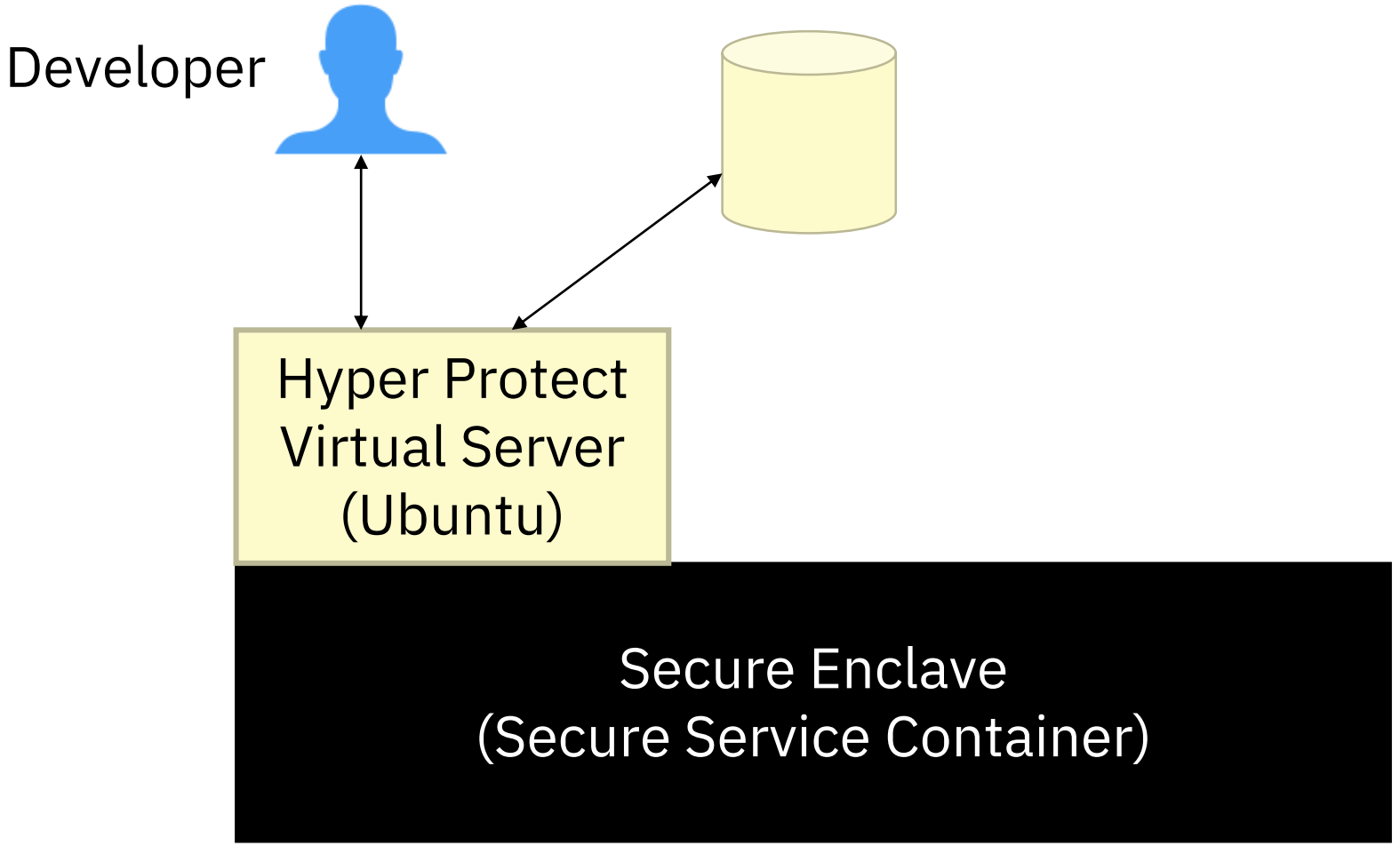
- Delivered unprimed: Keep Your Own Key
- Master Key defined using Trusted Key Entry
- REST API
- Low level EP11 API

Hyper Protect Database as a Service



- Primary + 2 secondaries
- Fully managed
- Encryption key never leaves the enclave
- Encrypted logs & storage
- MongoDB EE
- PostgreSQL

Hyper Protect Virtual Servers

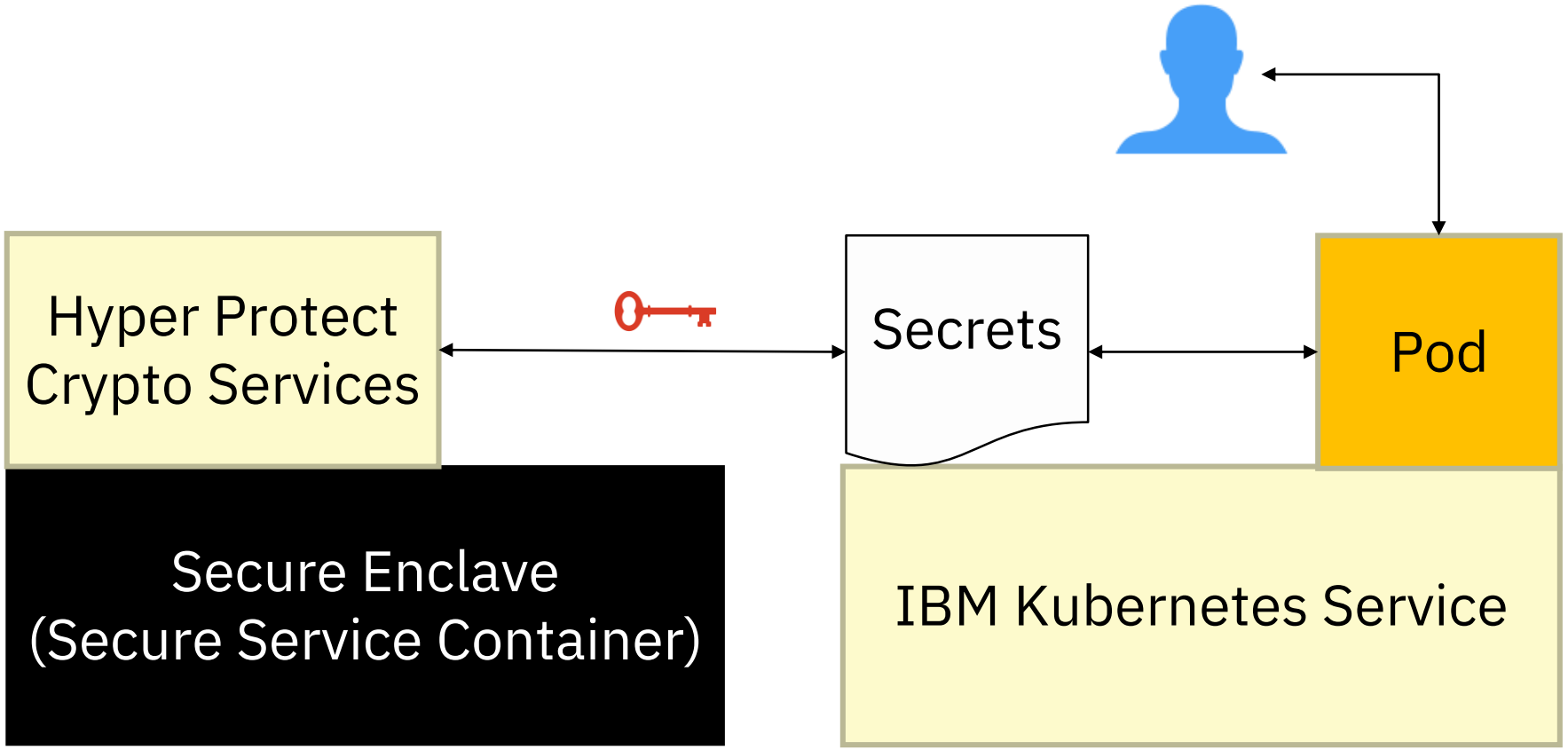


- Access only via SSH with key
- Key inserted into server image, not accessible to SREs
- Ports closed by default

Use Cases

Hyper Protect Crypto Services +

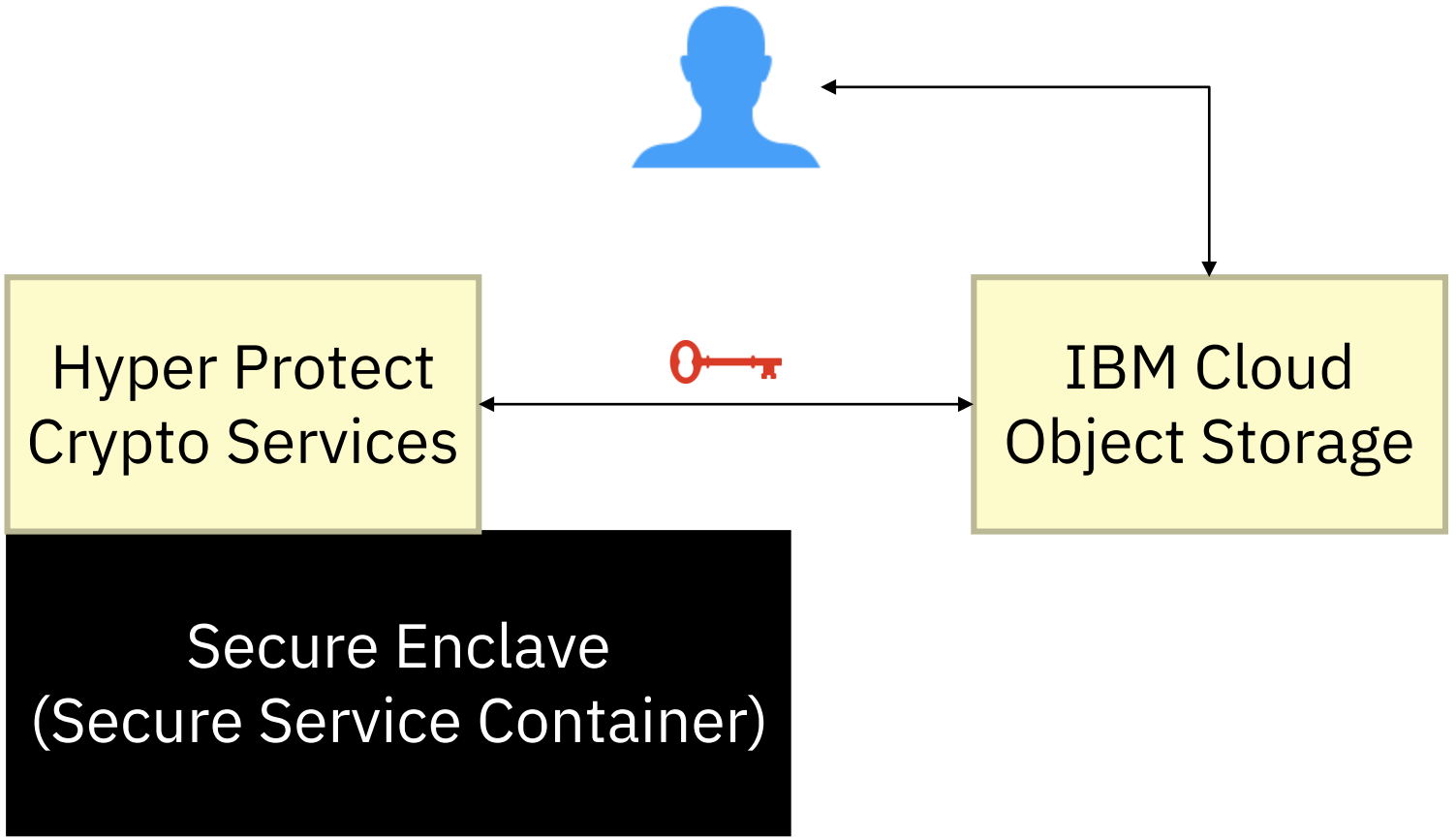
- **IBM Kubernetes Service Secrets**
- **Cloud Object Storage**
- **DBaaS KYOK**



- Kubernetes can provide secrets to pods: OAuth tokens, passwords, etc.
- Pods can read secrets when stood up
- Transparent encryption of secrets

Hyper Protect Crypto Services +

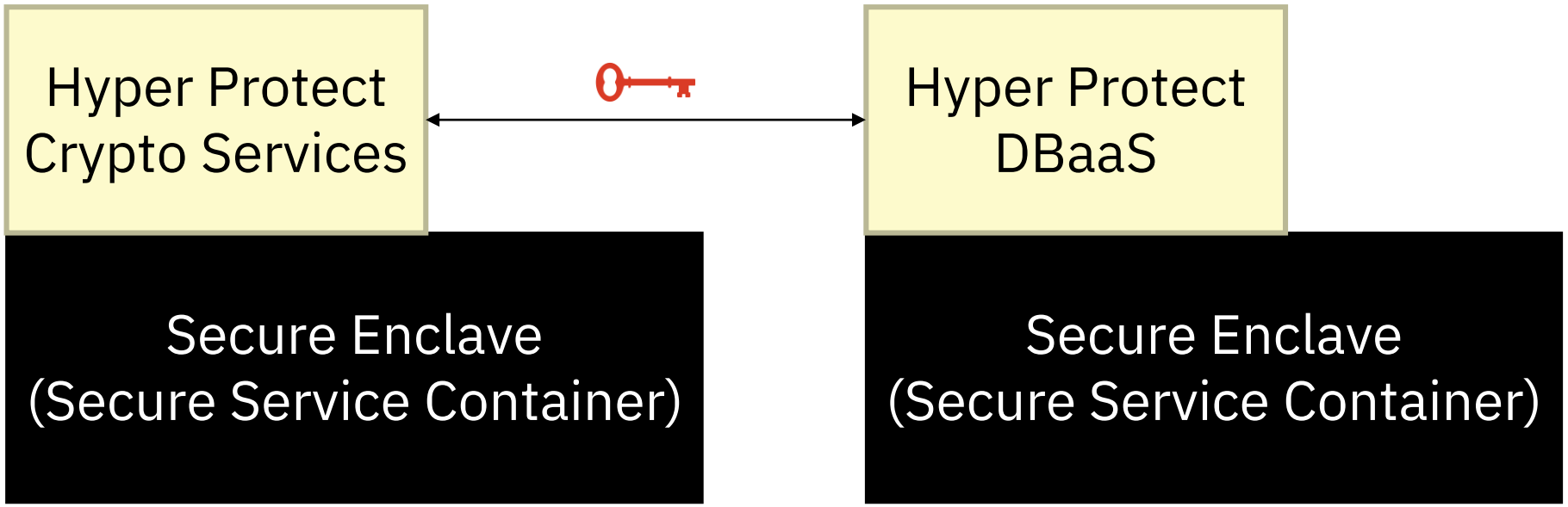
- **IBM Kubernetes Service Secrets**
- **Cloud Object Storage**
- **DBaaS KYOK**



- Connect the services to encrypt objects put into a bucket
- Backup and recovery
- Data archiving
- Binary blob storage

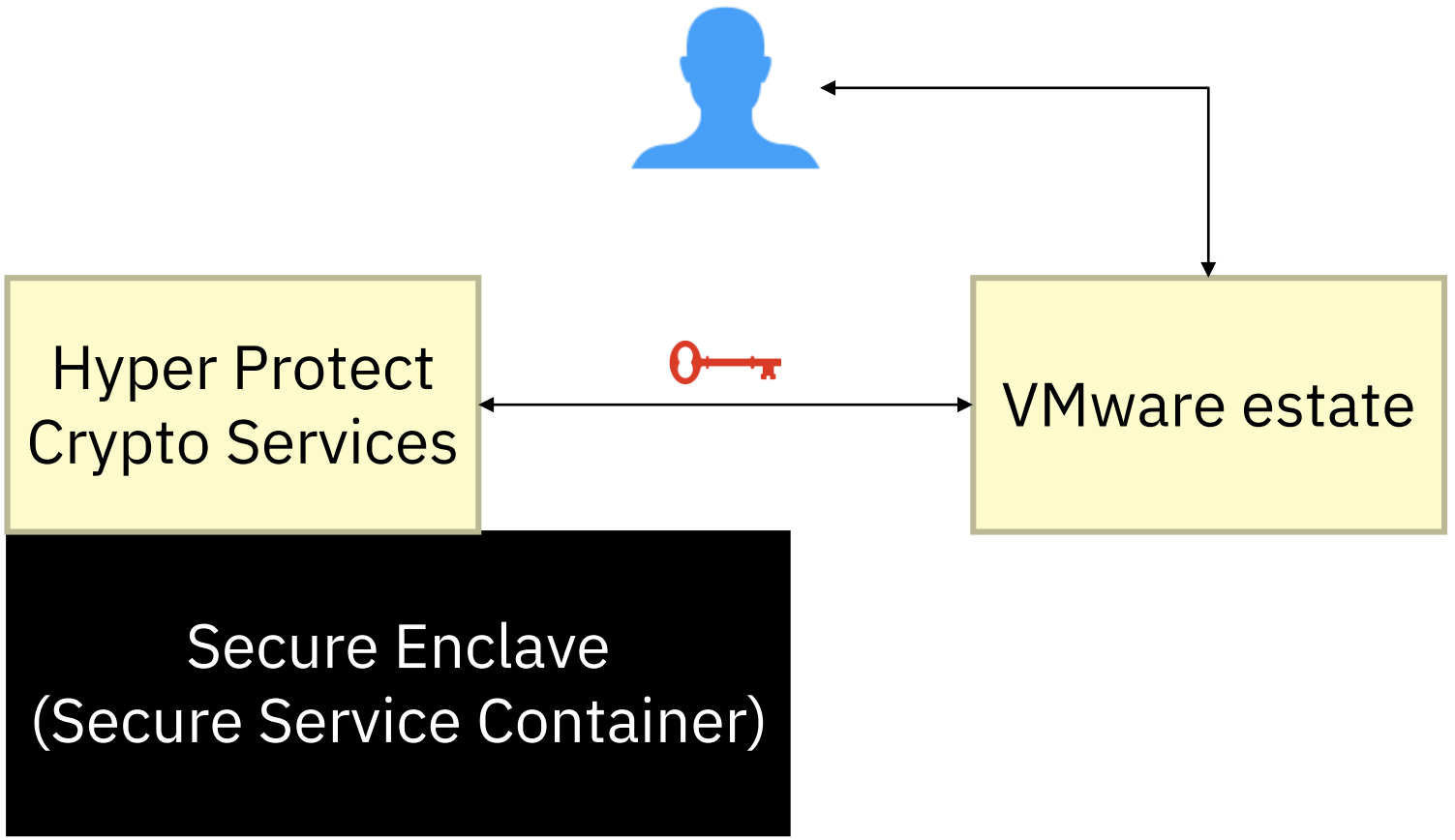
Hyper Protect Crypto Services +

- **IBM Kubernetes Service Secrets**
- **Cloud Object Storage**
- **DBaaS KYOK**



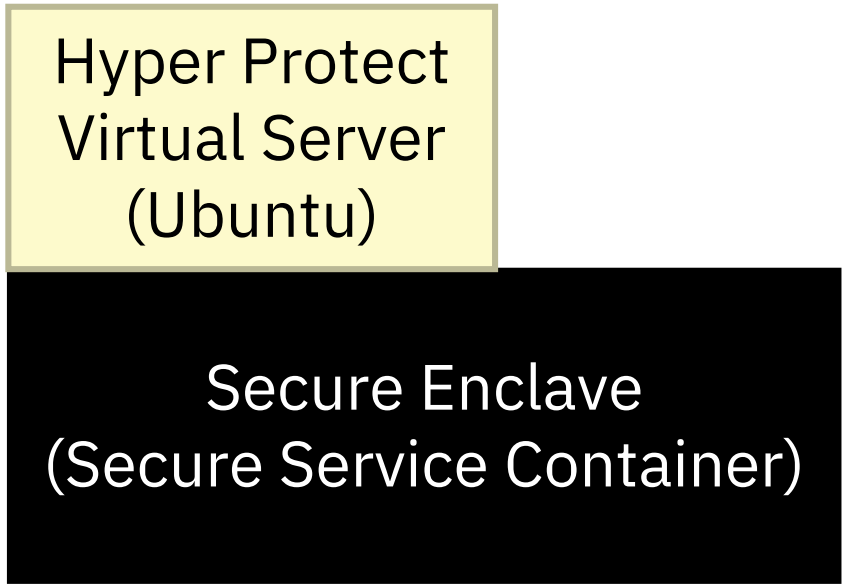
- KYOK: store the key in the HSM
- Use tamper-resistant hardware

Hyper Protect Crypto Services + VMware in IBM Cloud



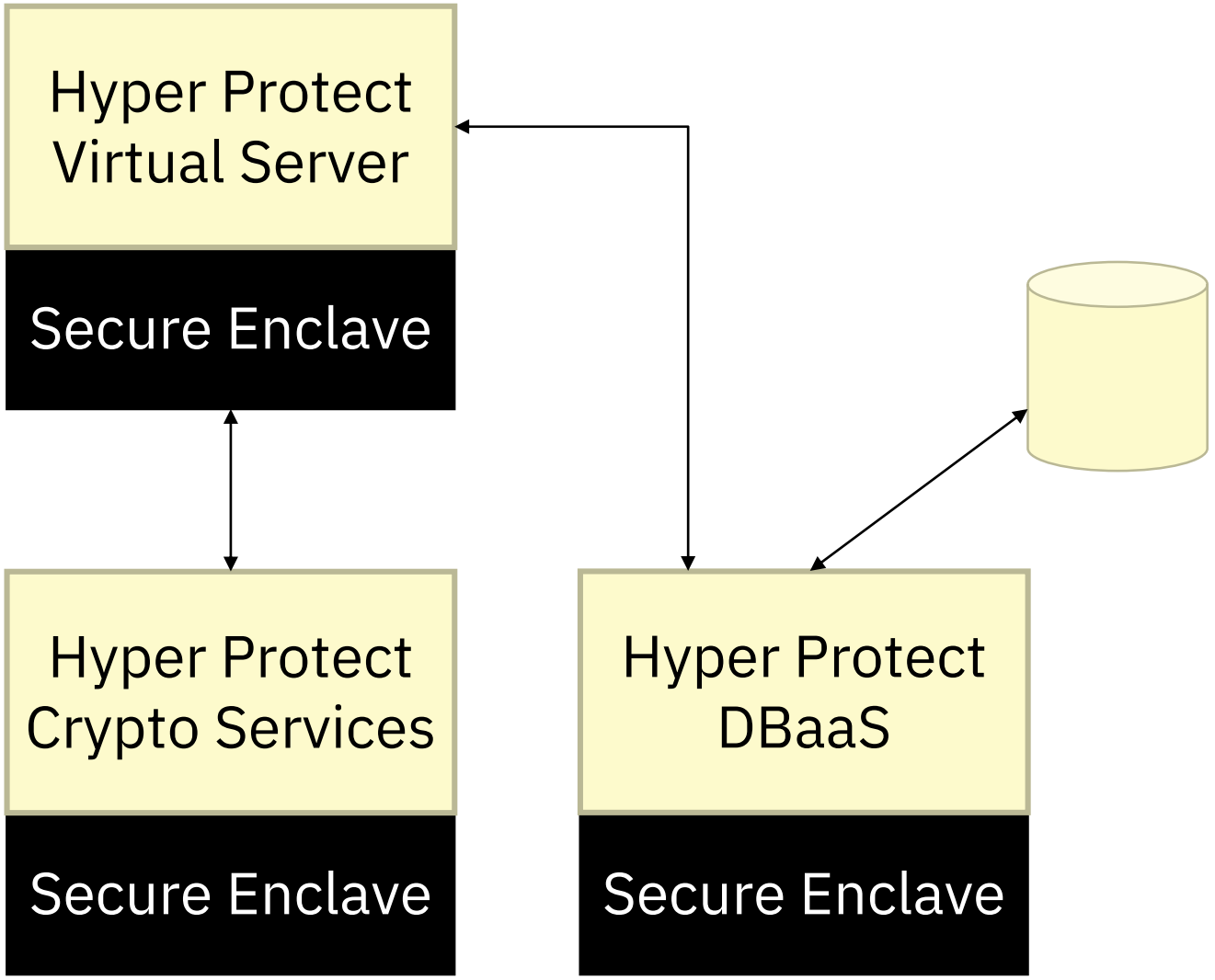
- Transparently encrypt VMware disks
- Store the key in HPCS

Hyper Protect Virtual Servers



- Secure CICD server: use it to build and/or run your applications
- Offsite build: docker doesn’t cross-compile
- Only production-ready cloud s390x Linux platform
- Quickly spin up dev/test systems with reduced overhead of cost and time

Digital Assets Platform



- End to end security for assets
- Secure key management
- Ideal solution for these platforms

Hyper Protect Accelerator

42 Countries
15 Startups
FinTech
HealthTech

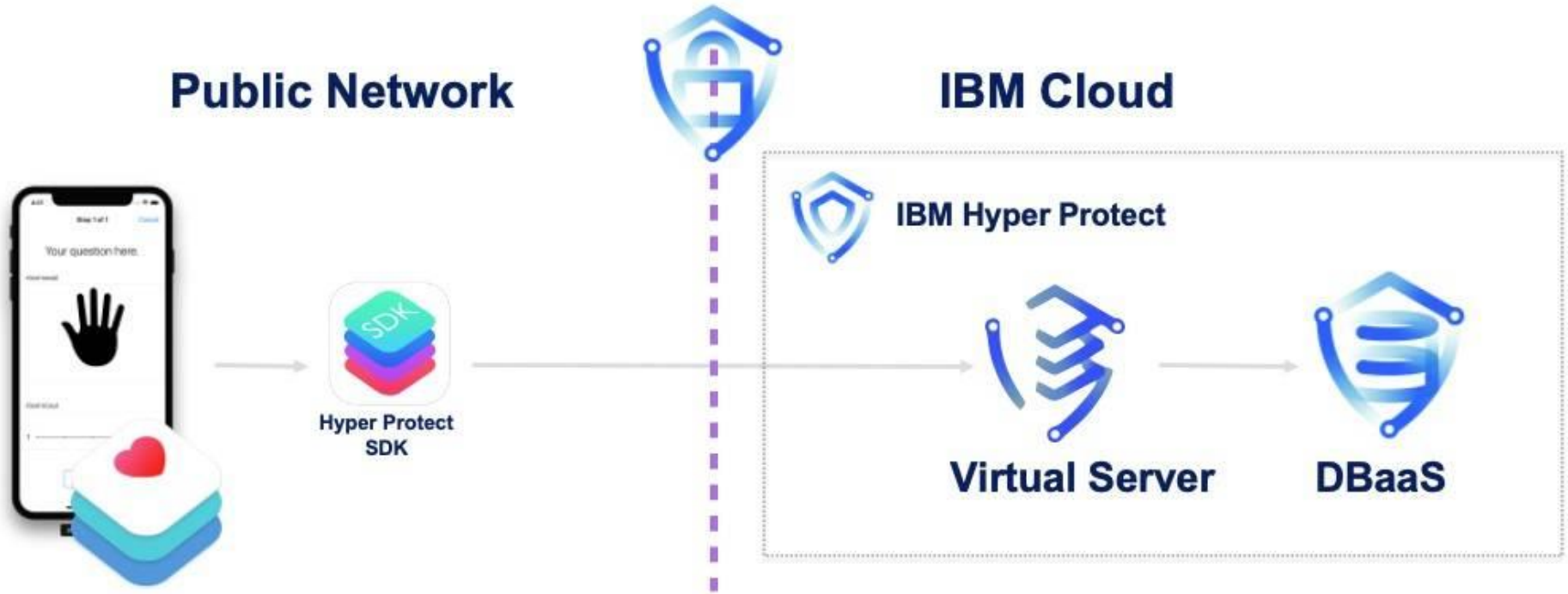
- Azaad Health
- BioTrillion
- bleu
- Ilara Health
- encore Pay
- Fostrum
- Galen Data
- Home Lending Pal
- MotionsCloud
- myAllergy
- Privakey
- PX Pulse
- Verge.Capital
- Wayapay
- Well Kept Beauty

- $10k/mo credits
- Business and technical advocates
- Mentoring

Submit your application by June 15, 2020

ibm.biz/hpa-apply

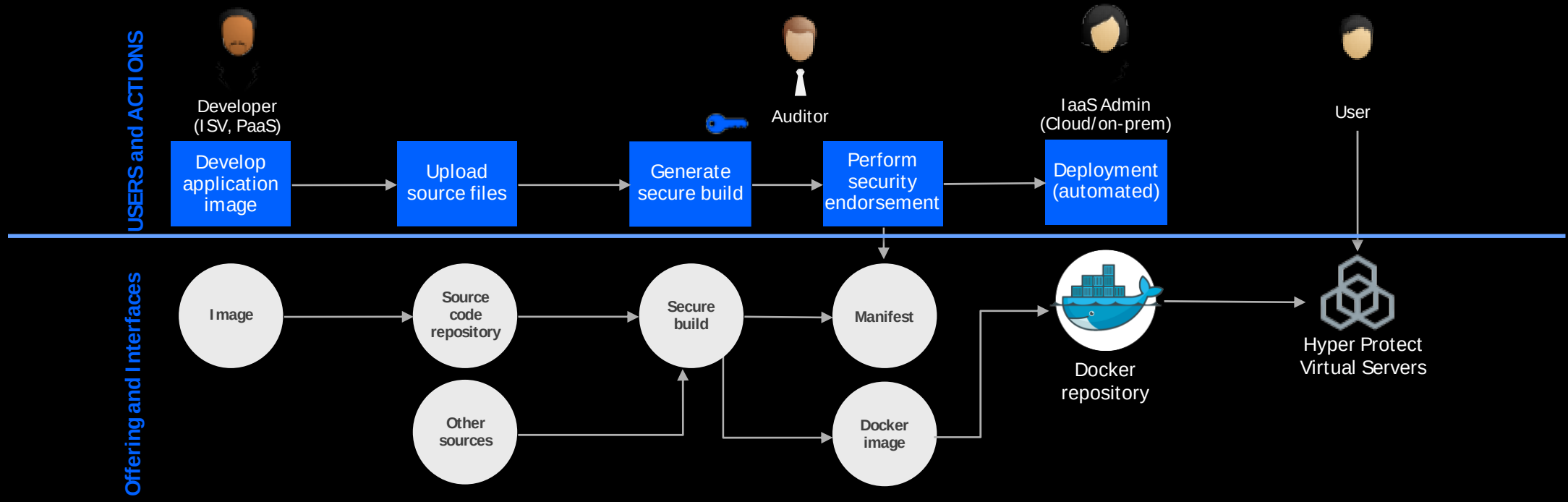
Hyper Protect iOS SDK for CareKit



github.com/carekit-apple/IBM-HyperProtectSDK
developer.apple.com/carekit

On-premises

Trusted CI/CD Stages: Bring your Own Image, Sign, Register, Approve and Deploy



Workload Lifecycle Phases

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

Threat Vectors pose Potential Risks

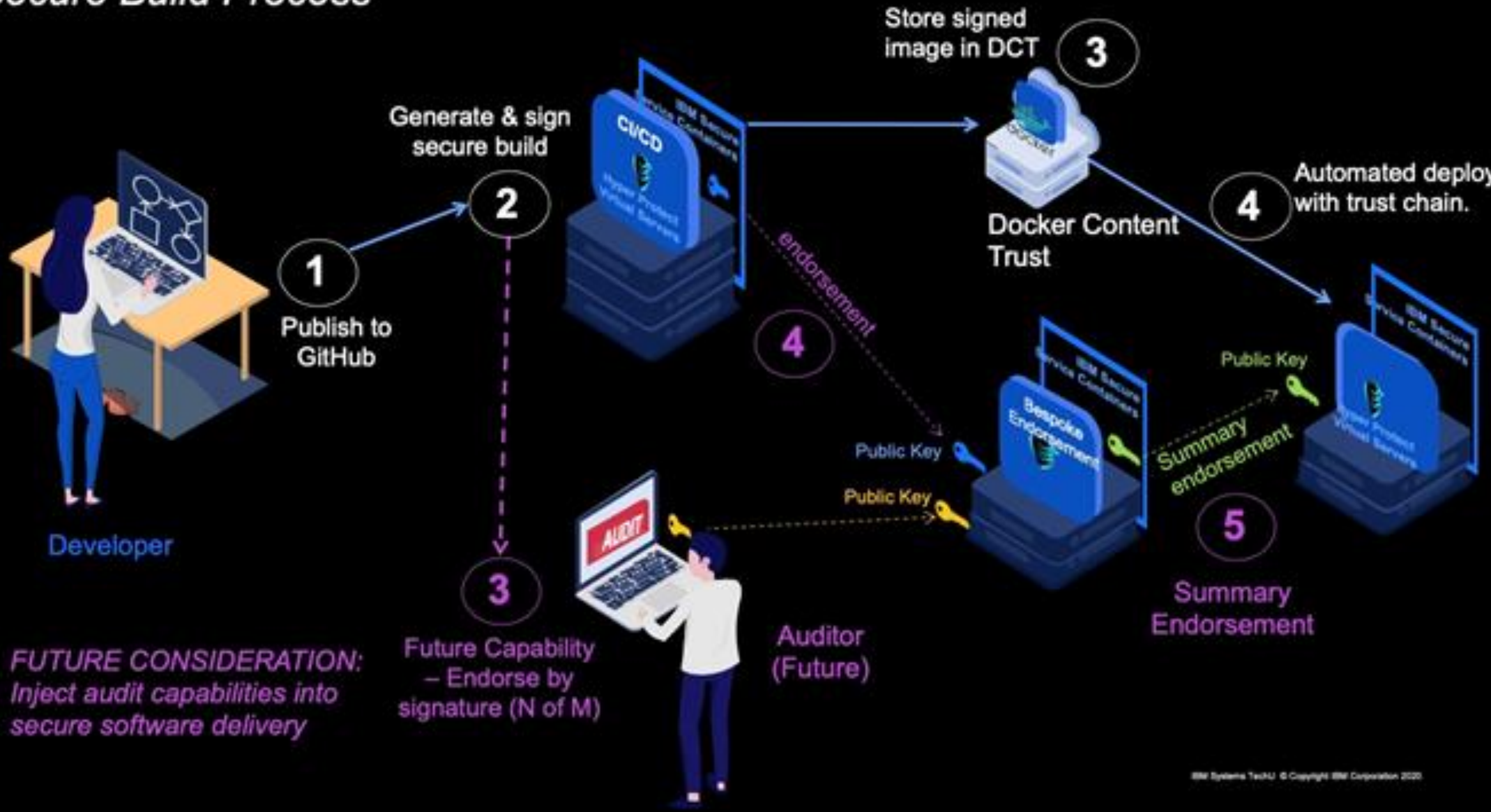
- Alter workload
- Alter build environment
- Modify workload deployment conditions
- Secrets visible to admin

How Hyper Protect Virtual Servers COMBATS risks:

- **Sign** application via secure build flow
- **Encrypt** and **register** application configuration info
- **Check image provenance** via workload **manifest**
- **Decrypt** application **registration file** – only possible via Secure Service Container (trusted execution environment)
- **Manage** infrastructure **via only RESTful interfaces**

Hyper Protect Virtual Servers – A Trusted CI/CD

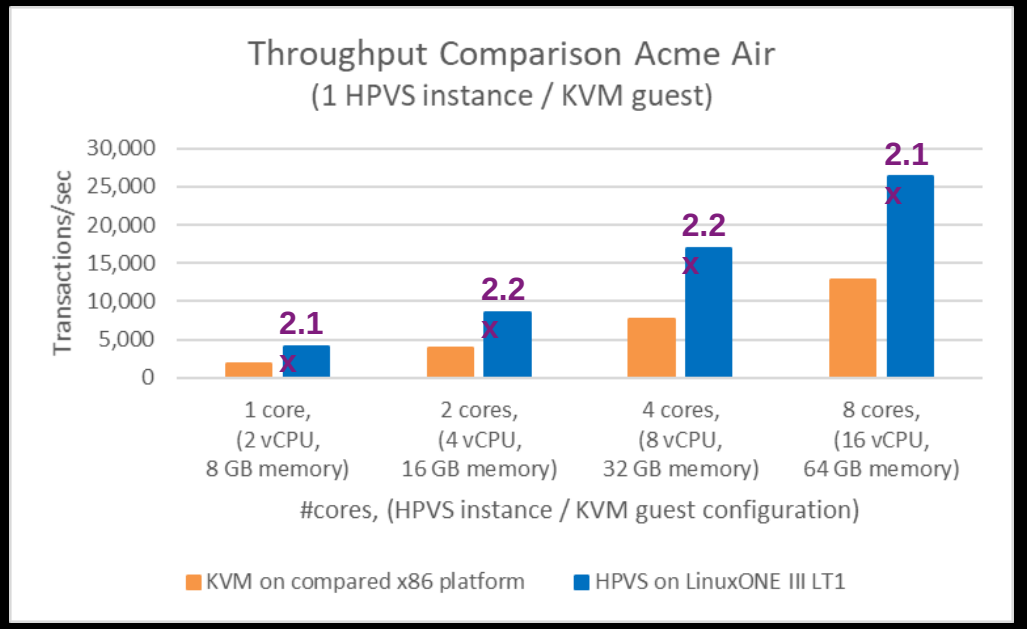
Secure Build Process

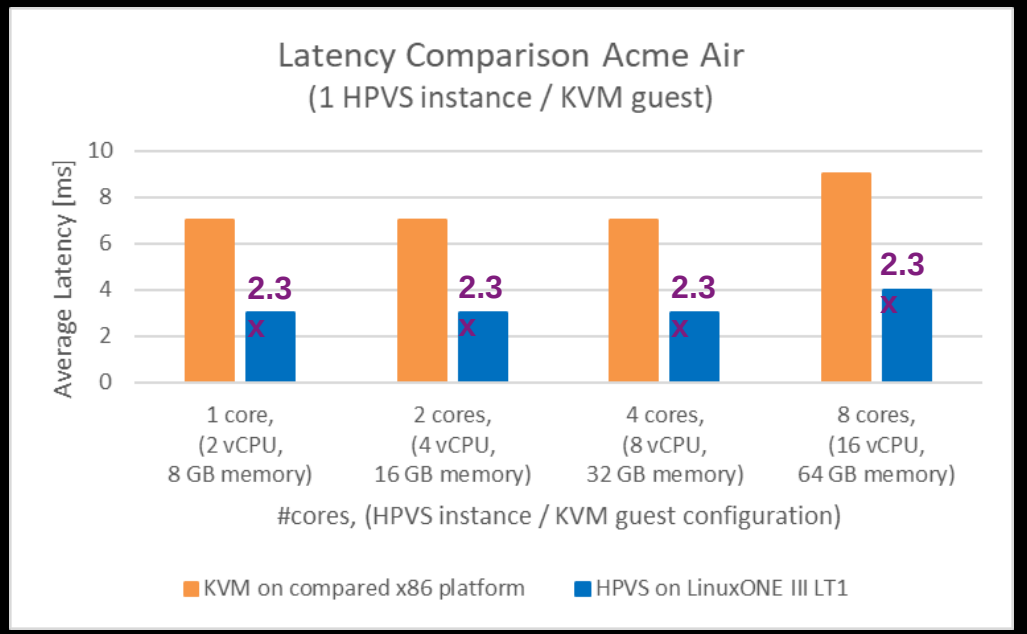


IBM Hyper Protect Virtual Servers

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.

Thank you!

Dr. Chris Poole **chrispoole@uk.ibm.com**

Developer Advocate, IBM **@chrispoole**

Where next?

ibm-hyper-protect.github.io

Notices and disclaimers

-
- **U.S. Government Users Restricted Rights — use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.**
- Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. **This document is distributed "as is" without any warranty, either express or implied. In no event, shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.** IBM products and services are warranted per the terms and conditions of the agreements under which they are provided.
- IBM products are manufactured from new parts or new and used parts.
  In some cases, a product may not be new and may have been previously installed. Regardless, our warranty terms apply."
- **Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.**
- Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those
- customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.
- References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.
- Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.
- It is the customer's responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer follows any law.

Notices and disclaimers continued

- Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products about this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM's products. **IBM expressly disclaims all warranties, expressed or implied, including but not limited to, the implied warranties of merchantability and fitness for a purpose.**
- The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.
- IBM, the IBM logo, ibm.com and [names of other referenced IBM products and services used in the presentation] are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at: www.ibm.com/legal/copytrade.shtml

