Confidential Compute and Confidential Containers on AKS

Data Sovereignty with Azure

Thomas Van Laere

- Microsoft Azure Consultant
- ThomasVanLaere.com

Contents

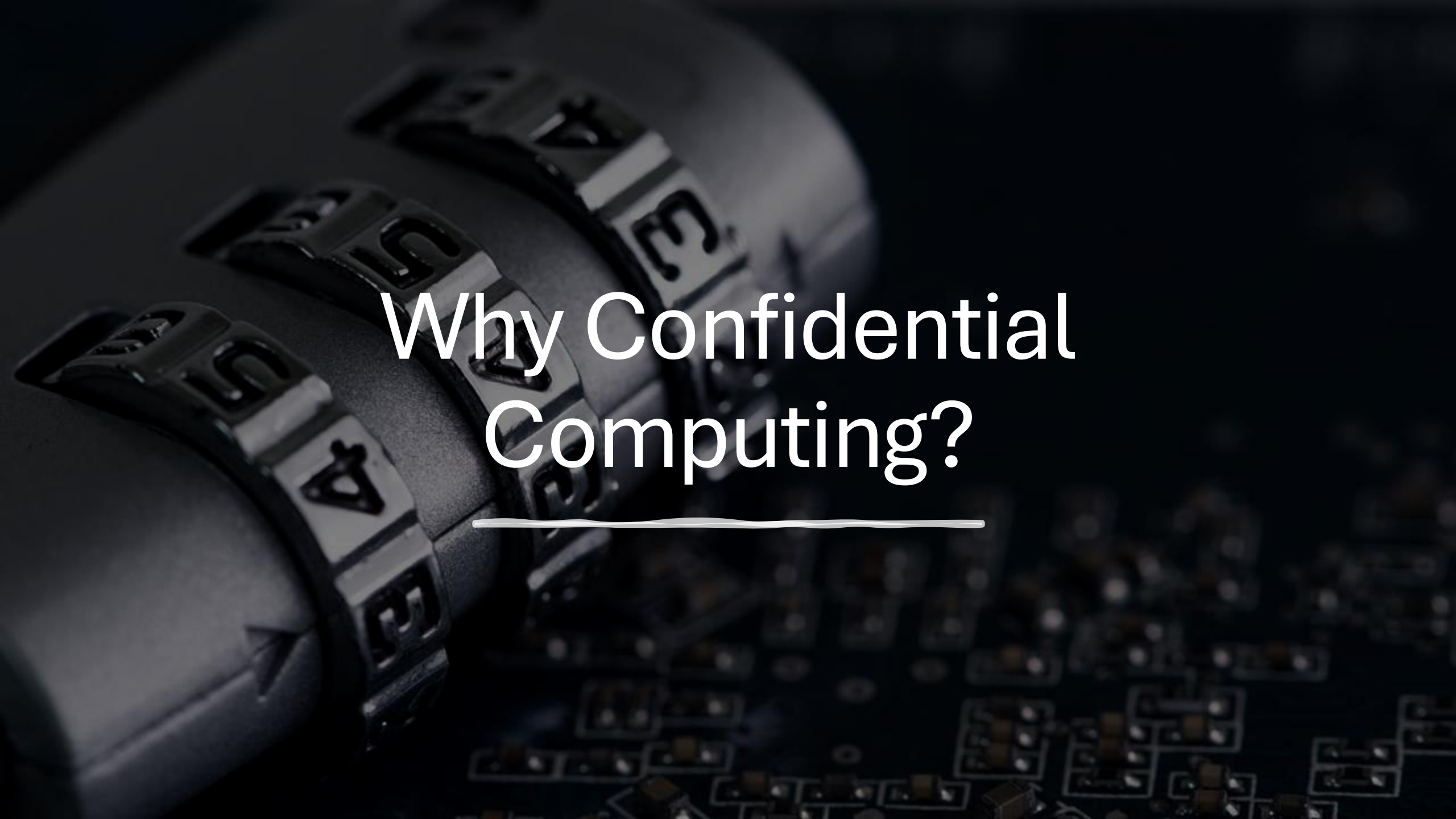
Why Confidential Computing?

What does it protect against?

How does it do it?

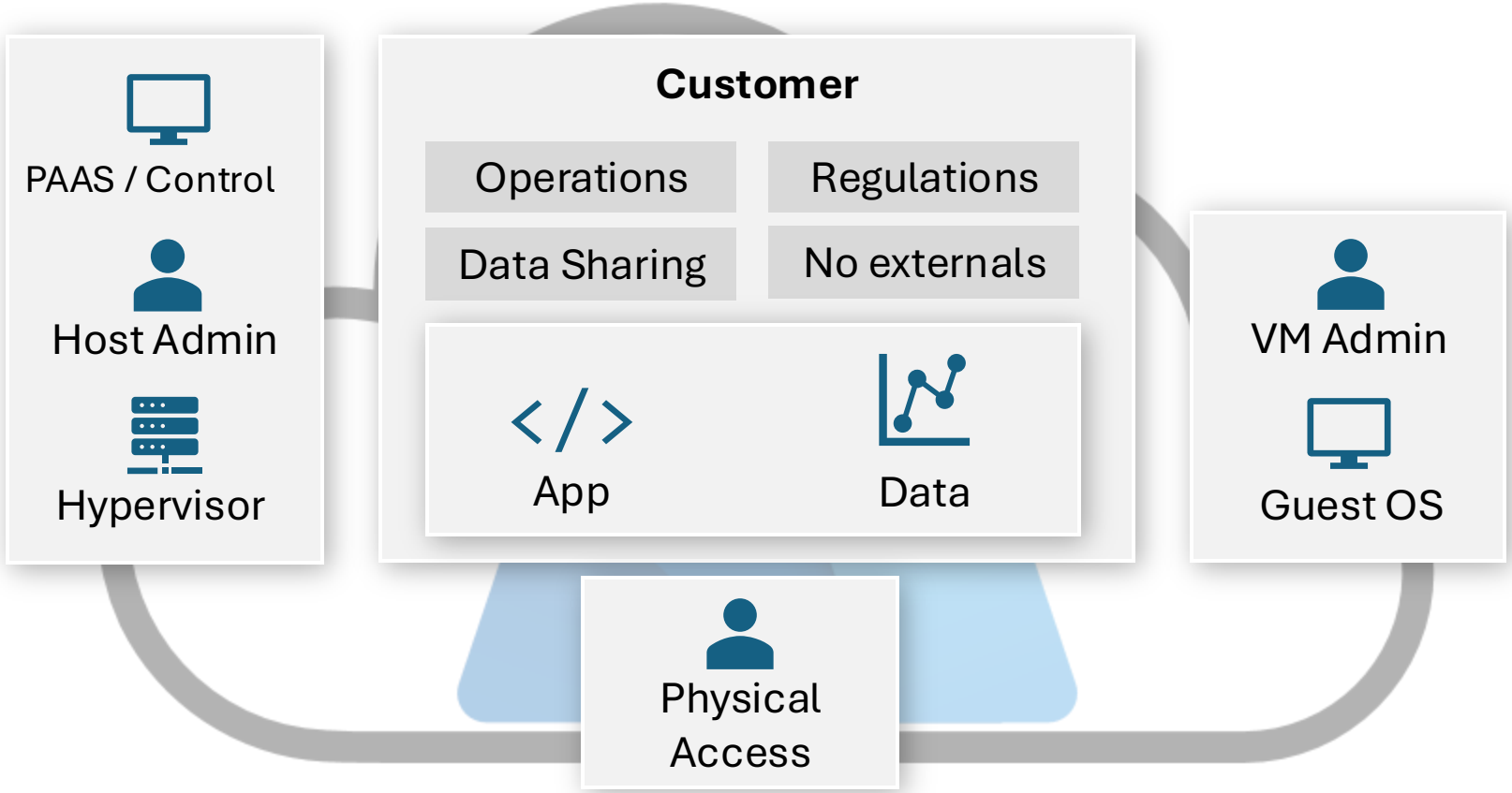
What are my options in Azure Kubernetes Service?

Confidential Containers!



Why Confidential Computing?

Trusting Azure today means..



… Even more challenges to overcome

Projects blocked

Due to data privacy and compliancy concerns

Cloud migration stalled

Due to data control and sovereignty concerns

Security worries

Due to sophisticated persistent threats to data and intellectual property

Confidential Computing can help solve these challenges!

Common Protection Measures

Data at rest

Data in transit

Data in use

More Protection Mechanisms!

Existing Encryption

Confidential Computing

Data at rest

Ecrypted inactive data when stored in blob storage, database, etc..

Data in transit

Encrypt data flows between untrusted public or private networks.

Data in use

Protect data that is in use, while in RAM, and during computation

Protect against

Insider threats

Priviledged admins abusing rights

Hackers

Exploits in the Hypervisor/OS

Third parties

Access without customer consent

The protection of data in use by performing computing in a hardware-based, attested, Trusted Execution Environment.

Verifiable assurance for data and/or code integrity and confidentiality.

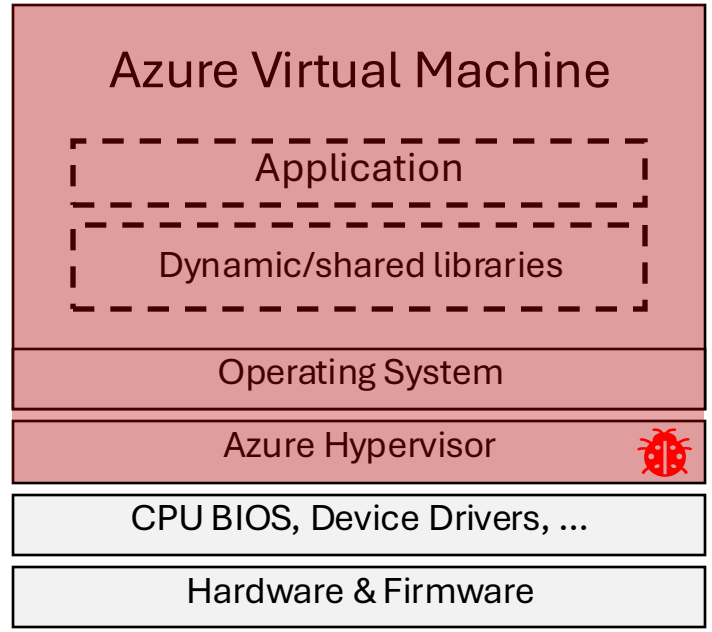
Trusted Computing Base

The totality of elements in a computing environment that must be trusted not to violate the confidentiality of computation.

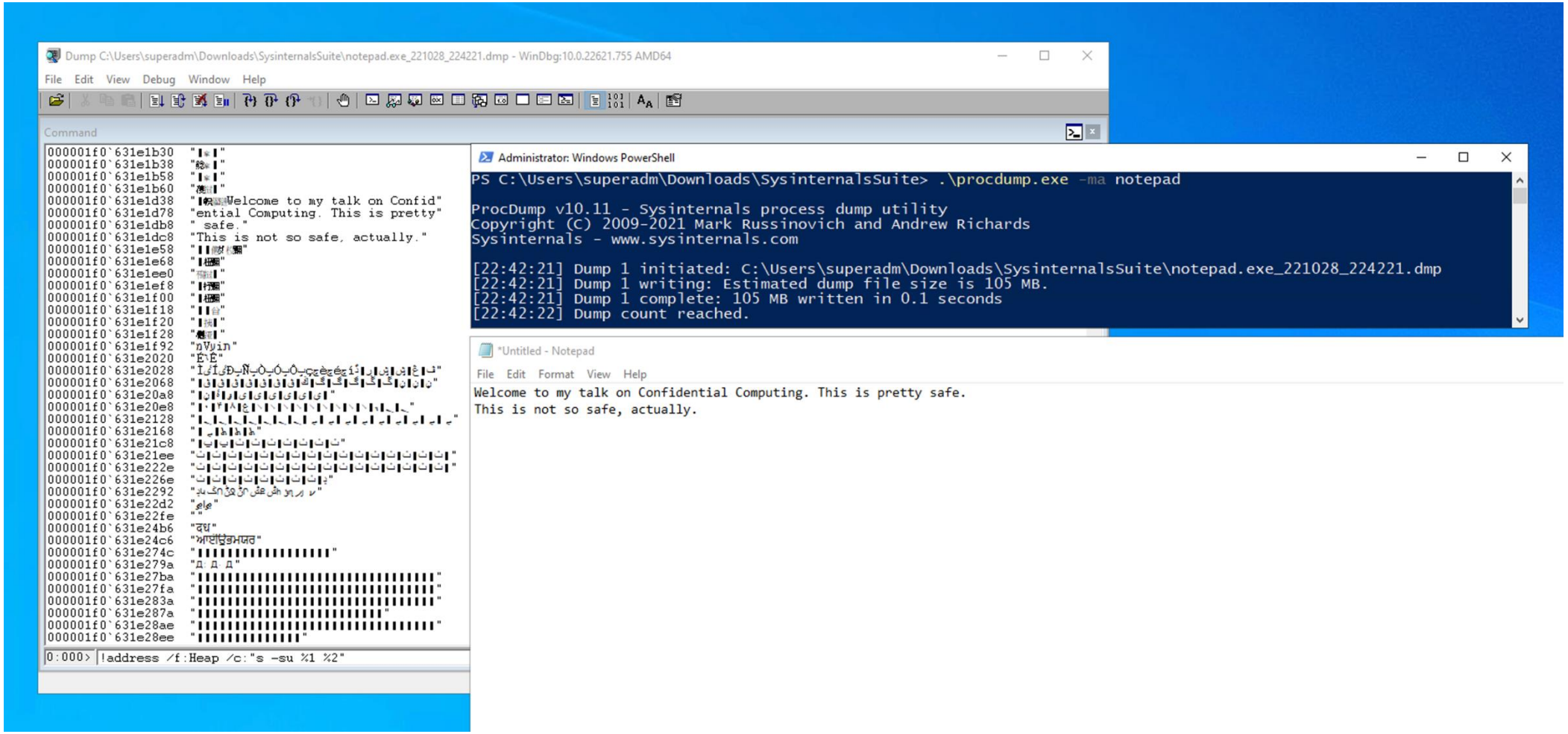
The TCB can include software, hardware, and human administrators, among other things.

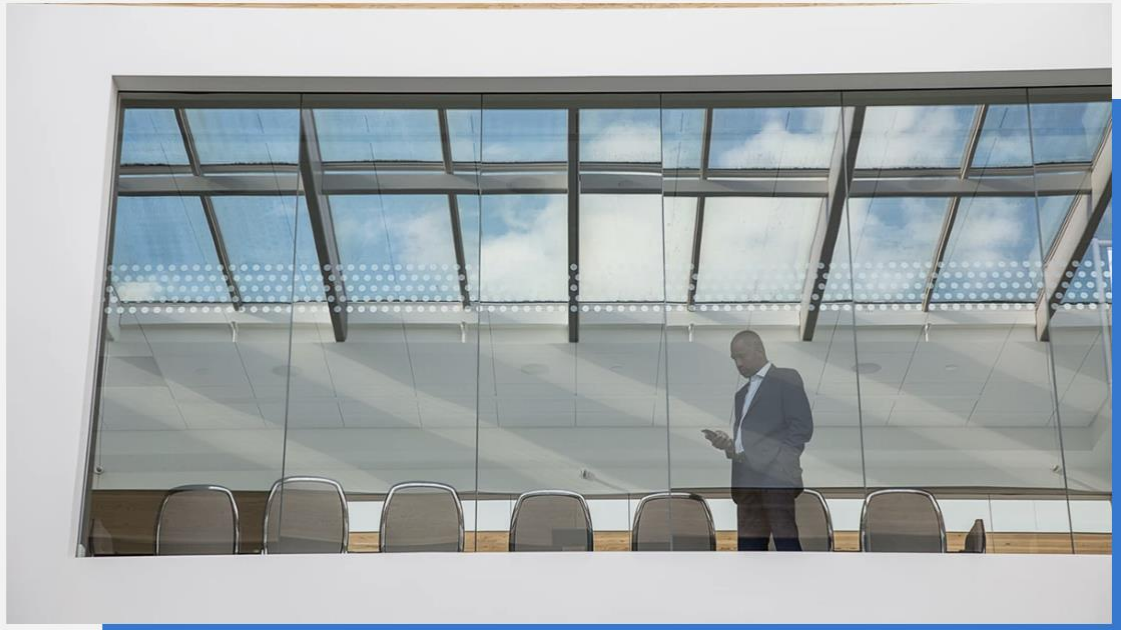
By removing elements from the TCB, the components that can be compromised are reduced, decreasing the attack surface.

Confidential Computing decreases the size of the trusted computing base (TCB).



Do I need it?


Dump C:\Users\superadm\Downloads\SysinternalsSuite\notepad.exe_221028_224221.dmp - WinDbg:10.0.22621.755 AMD64
File Edit View Debug Window Help
Command
000001f0`631e1d38 "Welcome to my talk on Confid"
000001f0`631e1d78 "ential Computing. This is pretty"
000001f0`631e1db8 " safe."
000001f0`631e1dc8 "This is not so safe, actually."
0:000> !address /f:Heap /c:"s -su %1 %2"
Administrator: Windows PowerShell
PS C:\Users\superadm\Downloads\SysinternalsSuite> .\procdump.exe -ma notepad
ProcDump v10.11 - Sysinternals process dump utility
Copyright (C) 2009-2021 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com
[22:42:21] Dump 1 initiated: C:\Users\superadm\Downloads\SysinternalsSuite\notepad.exe_221028_224221.dmp
[22:42:21] Dump 1 writing: Estimated dump file size is 105 MB.
[22:42:21] Dump 1 complete: 105 MB written in 0.1 seconds
[22:42:22] Dump count reached.
*Untitled - Notepad
File Edit Format View Help
Welcome to my talk on Confidential Computing. This is pretty safe.
This is not so safe, actually.



Research Threat intelligence

Attacker techniques, tools, and infrastructure

10 min read

Analysis of Storm-0558 techniques for unauthorized email access

By Microsoft Threat Intelligence

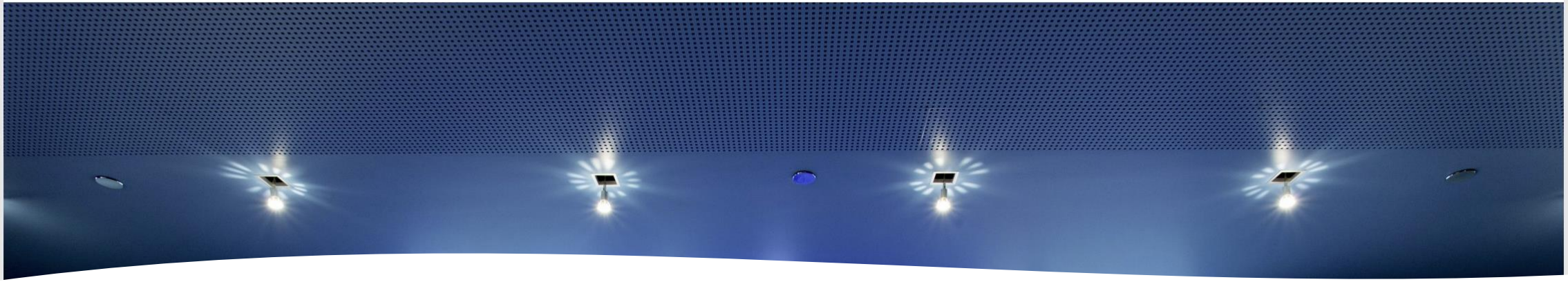
What are the odds?

- MSA signing private key stolen
  - Retrieved from a consumer signing system's crash dump in April 2021.
- Vector
  - exploited a bug in the Azure AD v2 authentication. Due to validation error, the MSA signing private key was used to generate access tokens for OWA and Outlook.com.
- Impact
  - *"**Access to user email** from approximately **25 organizations**, including **government** agencies and related **consumer** accounts in the public cloud."*

Source: https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access

A new world of security: Microsoft's Secure Future Initiative

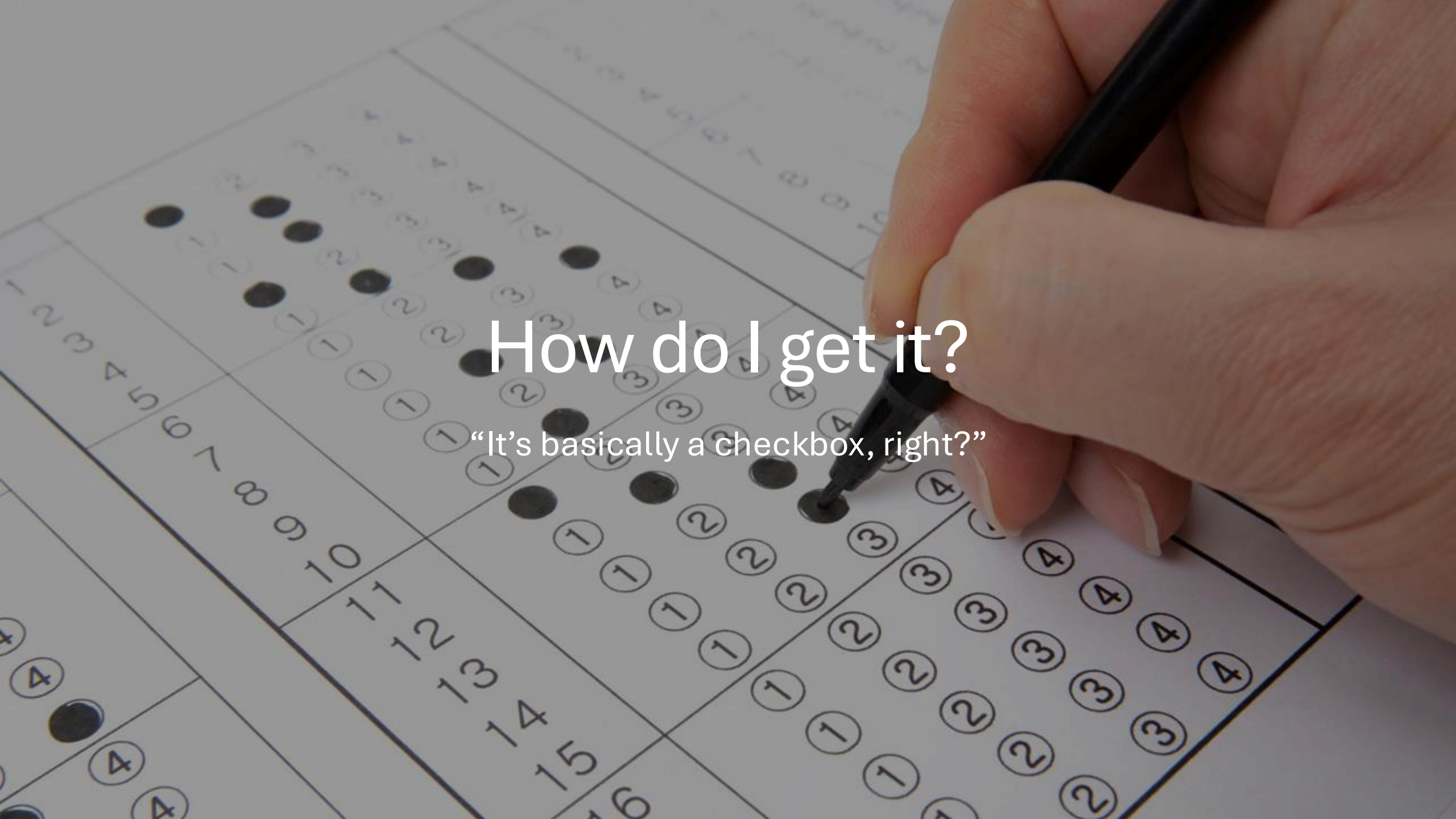
Nov 2, 2023 | Brad Smith - Vice Chair & President



*"As part of this initiative, we will migrate to a **new** and fully automated **consumer and enterprise key management system** with an architecture designed to ensure that keys remain inaccessible even when underlying processes may be compromised.*

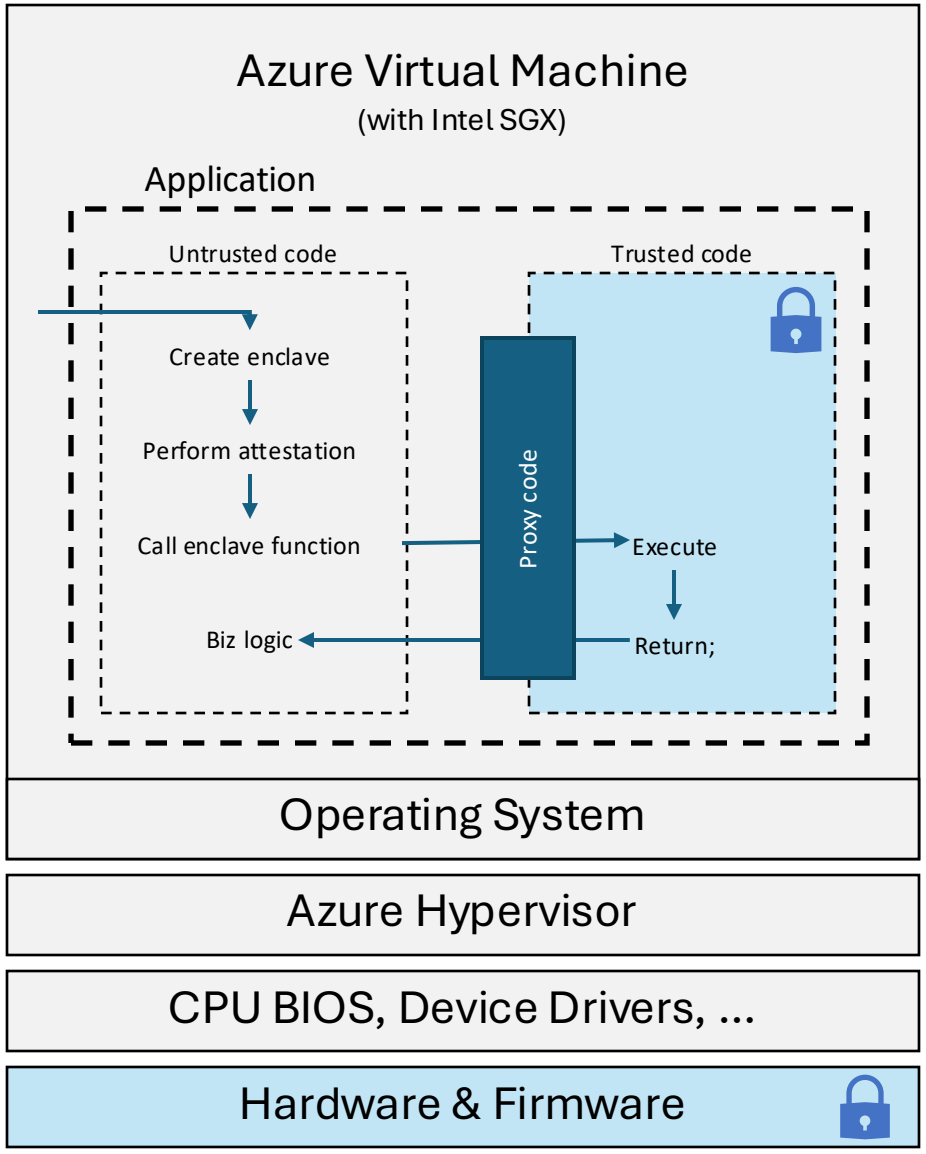
*This will **build upon** our confidential computing architecture and the use of hardware security modules (HSMs) that store and protect keys in hardware and that **encrypts data** at rest, in transit, and **during computation**."*

Source: https://blogs.microsoft.com/on-the-issues/2023/11/02/secure-future-initiative-sfi-cybersecurity-cyberattacks



How do I get it?

“It’s basically a checkbox, right?”

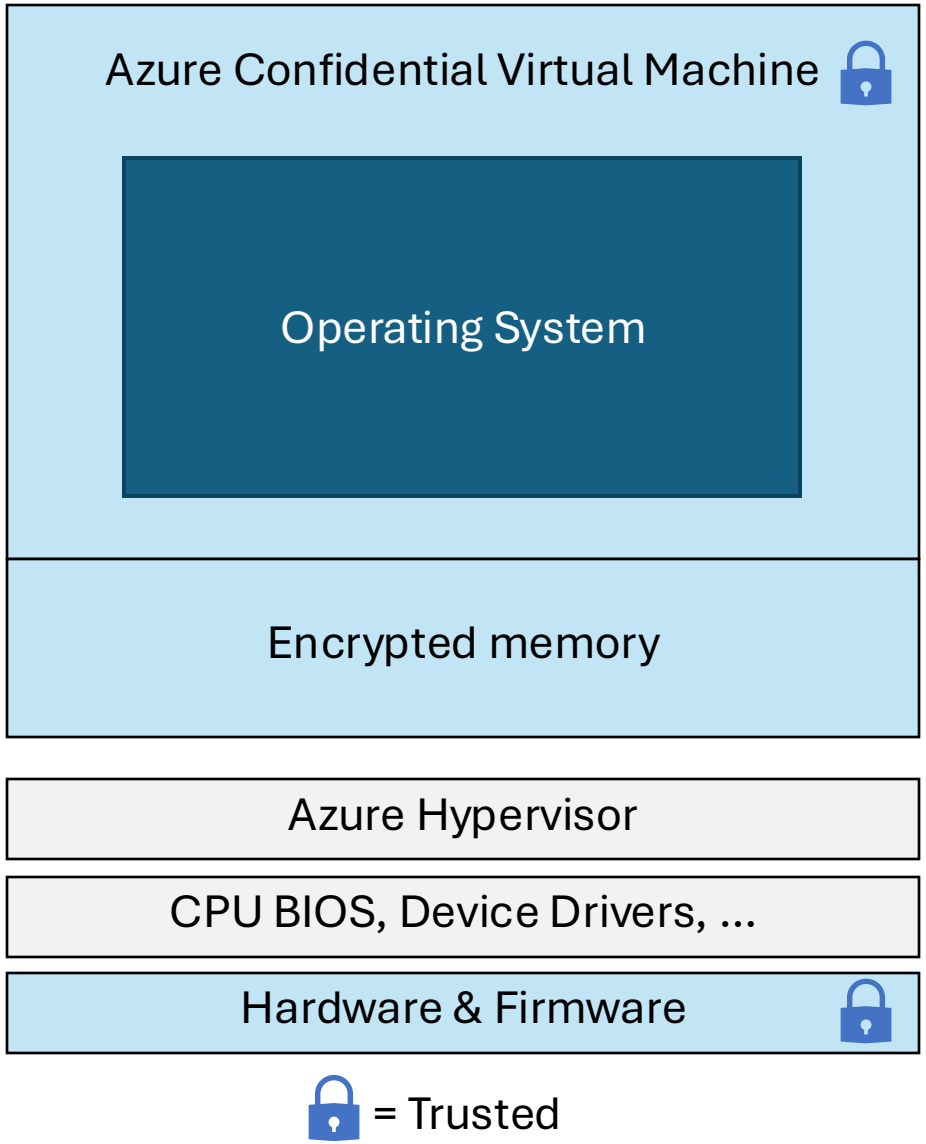


VMs with App Enclaves (Intel SGX)

* DCsv2 (General purpose)
* DCsv3 and DCdsv3 (General purpose)

Confidential Virtual Machines

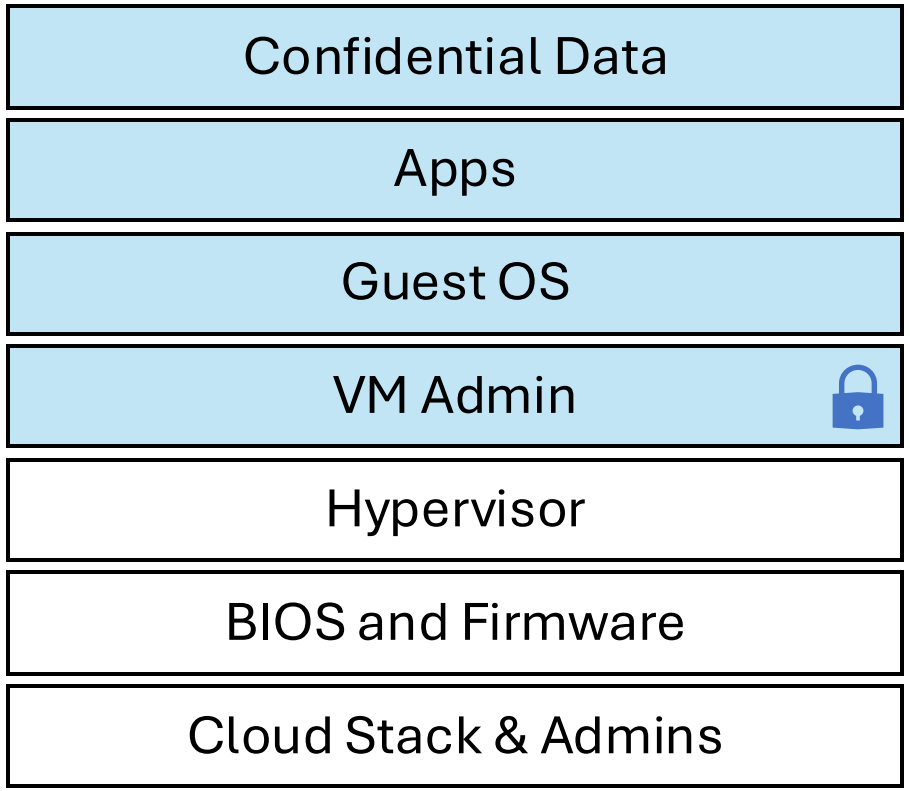
ADM SEV-SNP Intel TDX



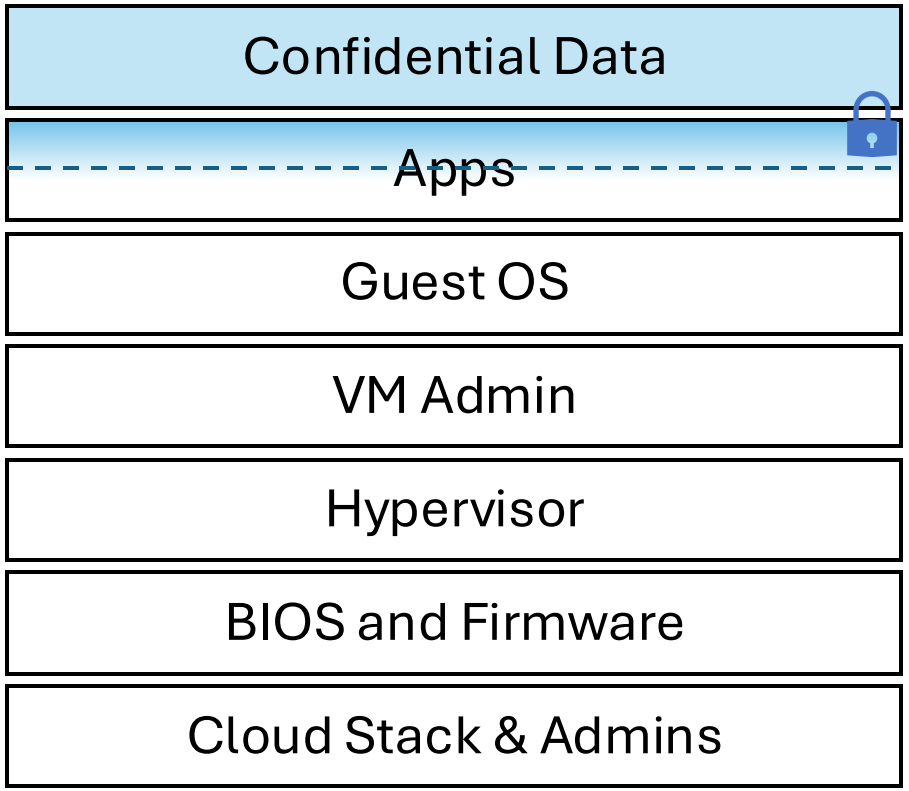
* DCasv5 and DCadsv5 (General purpose)
* ECasv5 and ECadsv5 (Memory optimized)
* DCesv5 and DCedsv5 (General purpose)
* ECesv5 and ECedsv5 (Memory optimized)

Trust boundaries

VM Isolation



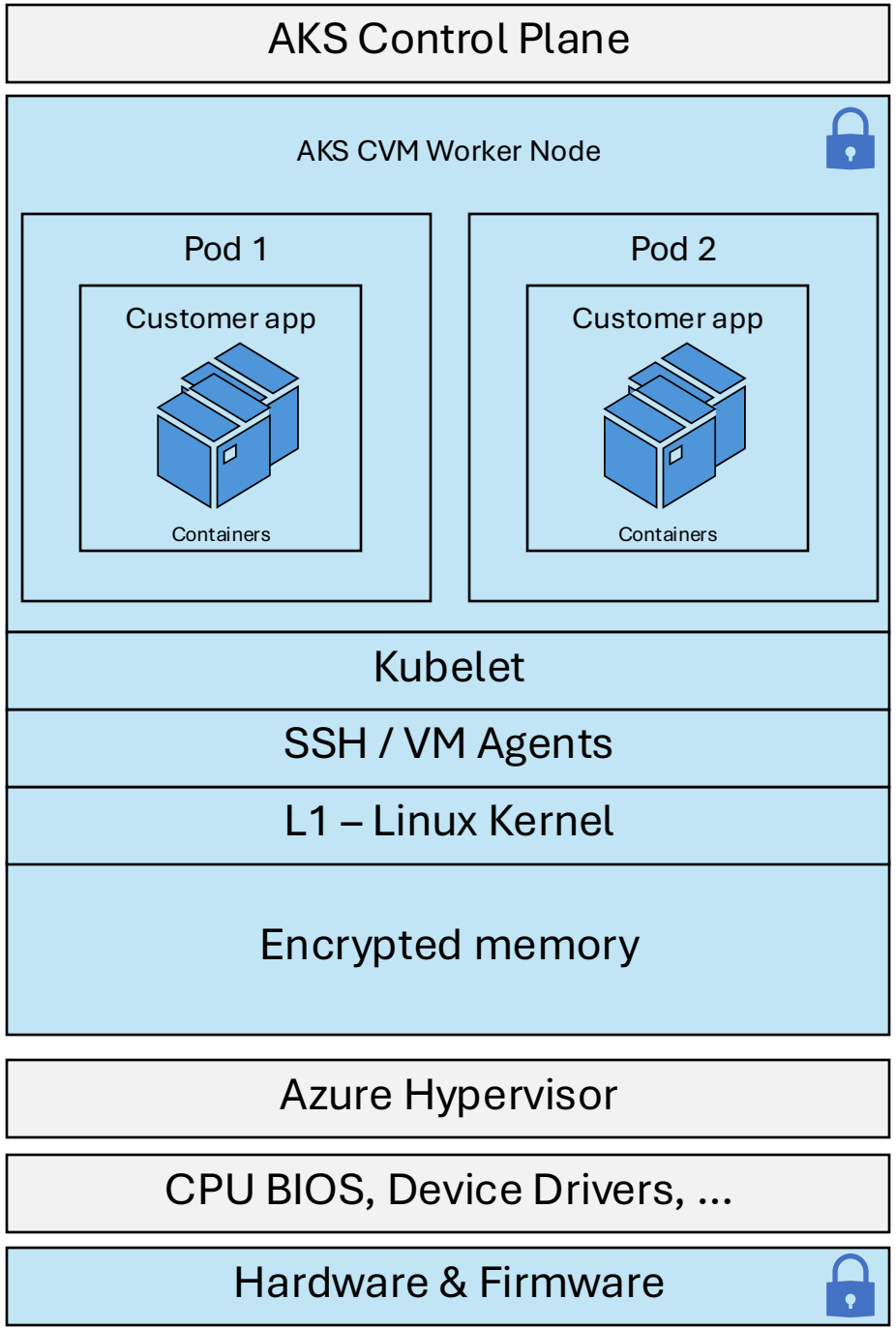
App Isolation

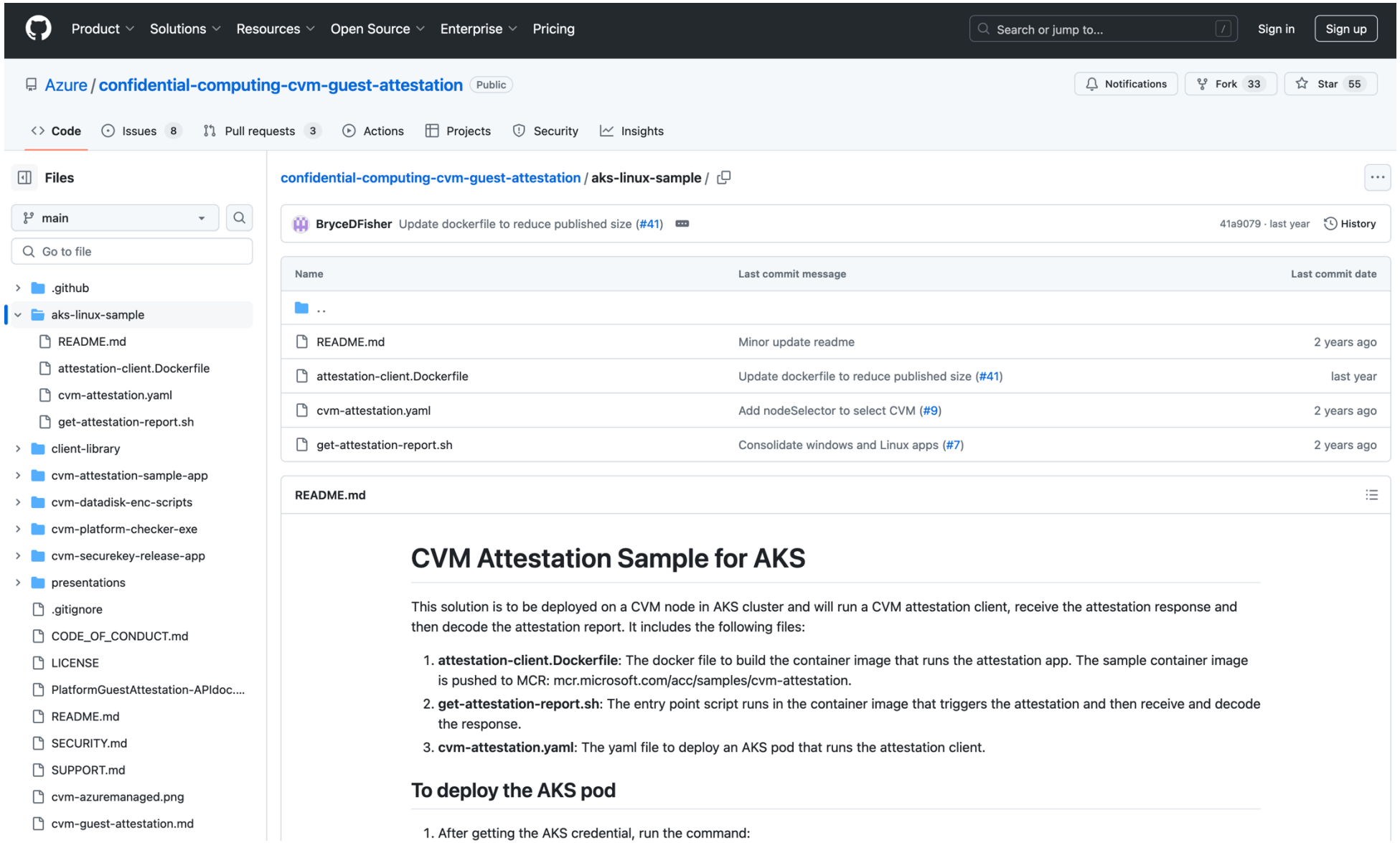


Source: https://learn.microsoft.com/en-us/azure/confidential-computing/confidential-computing-deployment-models

Confidential VM Node Pools on AKS

- Data-in-use with full memory encryption
- All pods on the CVM are in the same trust boundary
- No code changes required for apps
- Easy way to lift-and-shift - simply adjust the YAML





Source: https://github.com/Azure/confidential-computing-cvm-guest-attestation

Woah, hold up a minute!

Are these Microsoft-managed control-plane nodes able to control our confidential worker nodes?

Almost good enough

- We’re only getting **limited security benefits**
- This setup provides runtime encryption for our nodes
- Direct memory access is prevented
- For this approach this might just actually mean that we’d have to trust the control plane.

Can we do better?

- We can self-host!
- Or we use..

CLOUD NATIVE COMPUTING FOUNDATION

About Projects Training Community Blog & News Join

PROJECTS

Confidential Containers

Confidential Containers is an open source community working to enable cloud native confidential computing by leveraging Trusted Execution Environments to protect containers and data.

Confidential Containers was accepted to CNCF on March 8, 2022 at the **Sandbox** maturity level.

VISIT PROJECT WEBSITE

Source: https://www.cncf.io/projects/confidential-containers

OpenInfra FOUNDATION

PROJECTS MEMBERSHIP EVENTS ABOUT NEWS LOGIN JOIN

Projects

ALL PROJECTS HOSTING SERVICES FUNDING CONTACT US

Projects & Communities at OpenInfra Foundation

Projects that call OpenInfra Foundation their home each value open collaboration and exemplify the Four Opens (source, design, development, community). All of our projects have a strategic focus, vision & scope that furthers the OpenInfra Foundation mission of supporting the development and adoption of production infrastructure with open source components.

KATA CONTAINERS

katacontainers.io →

Secure, lightweight CRI compatible virtualized containers.

Kata Containers is an open source project delivering increased container security and workload isolation through an implementation of lightweight virtual machines.

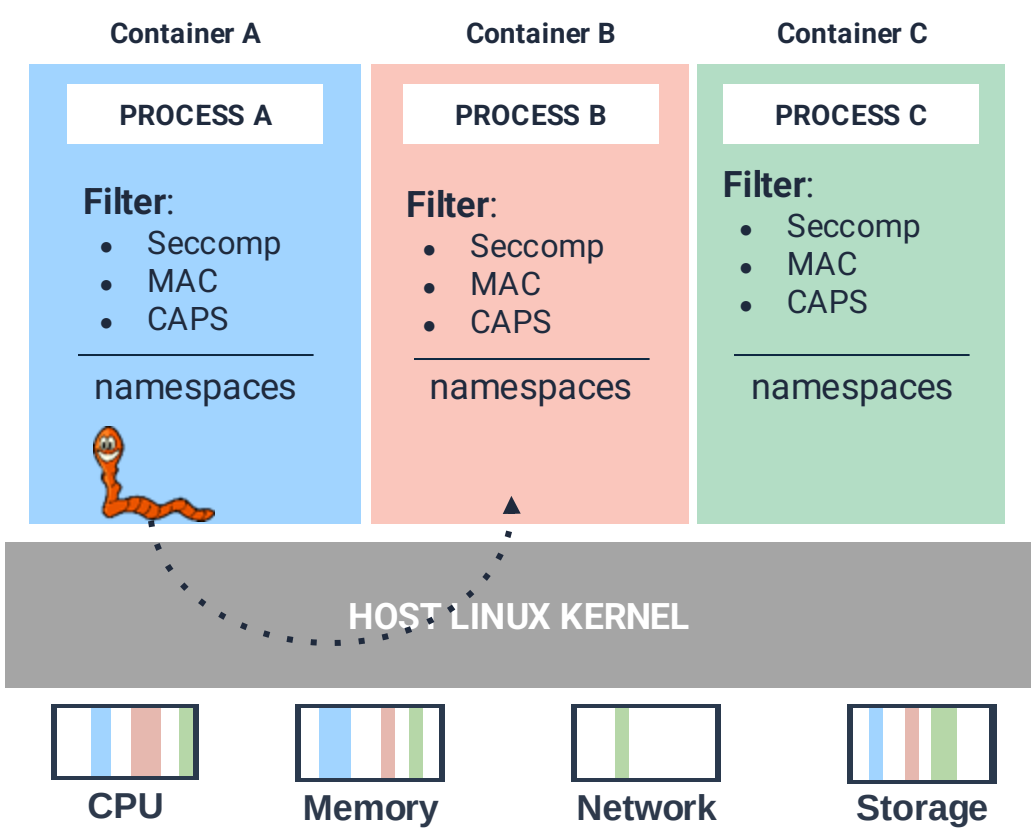
Mailing Lists	Documentation
Releases	Blog
Code	User Survey

Source: https://katacontainers.io

Kata Containers

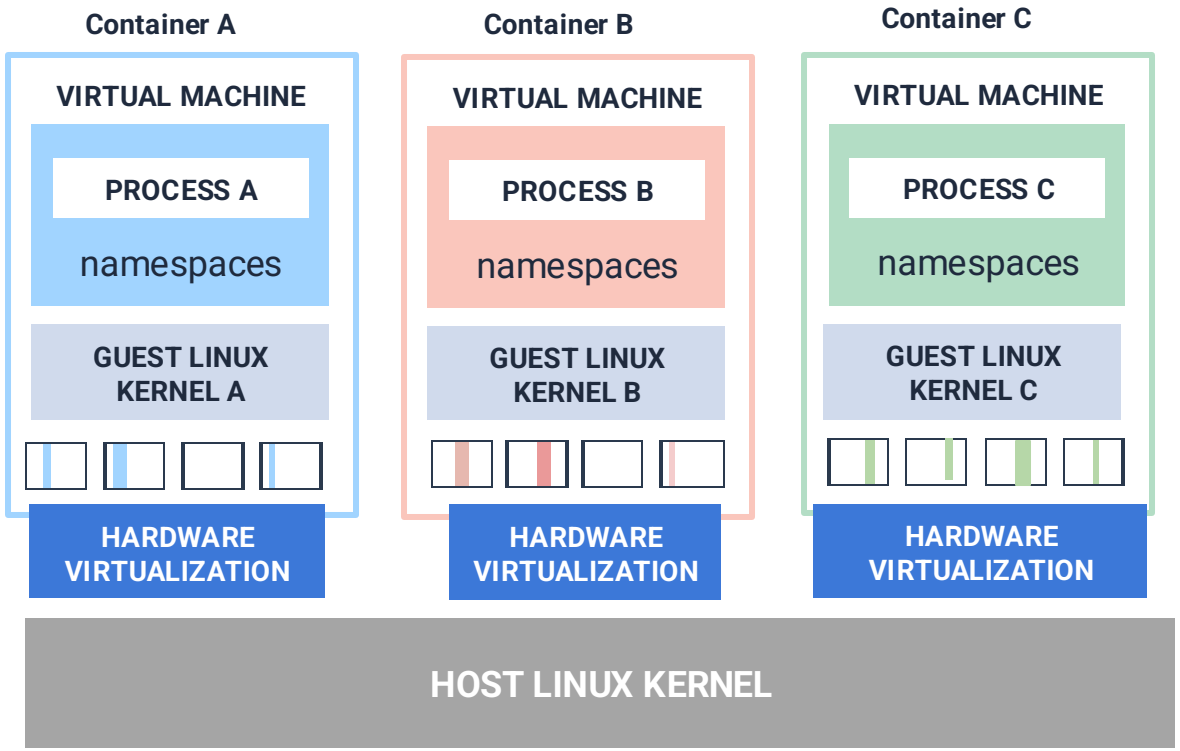
Traditional Containers

Isolation by namespaces, cgroups with shared kernel

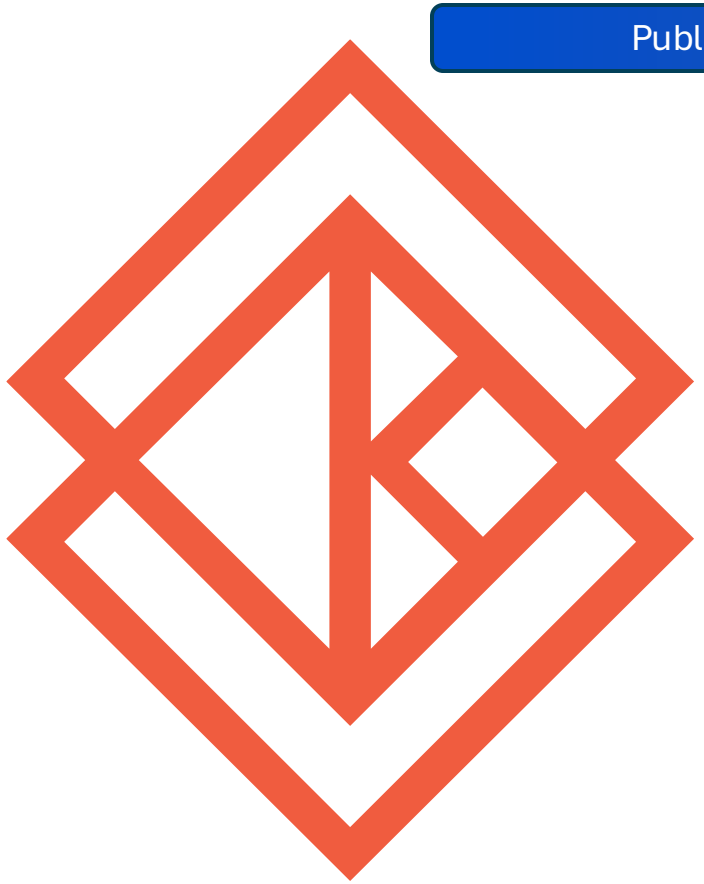


Kata Containers

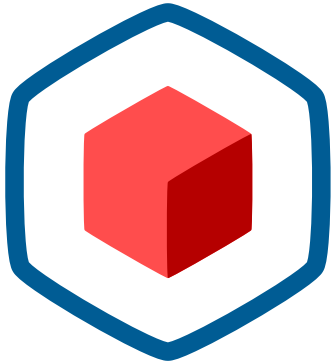
Each container or pod is more isolated in its own lightweight VM



Adapted from: https://katacontainers.io/learn



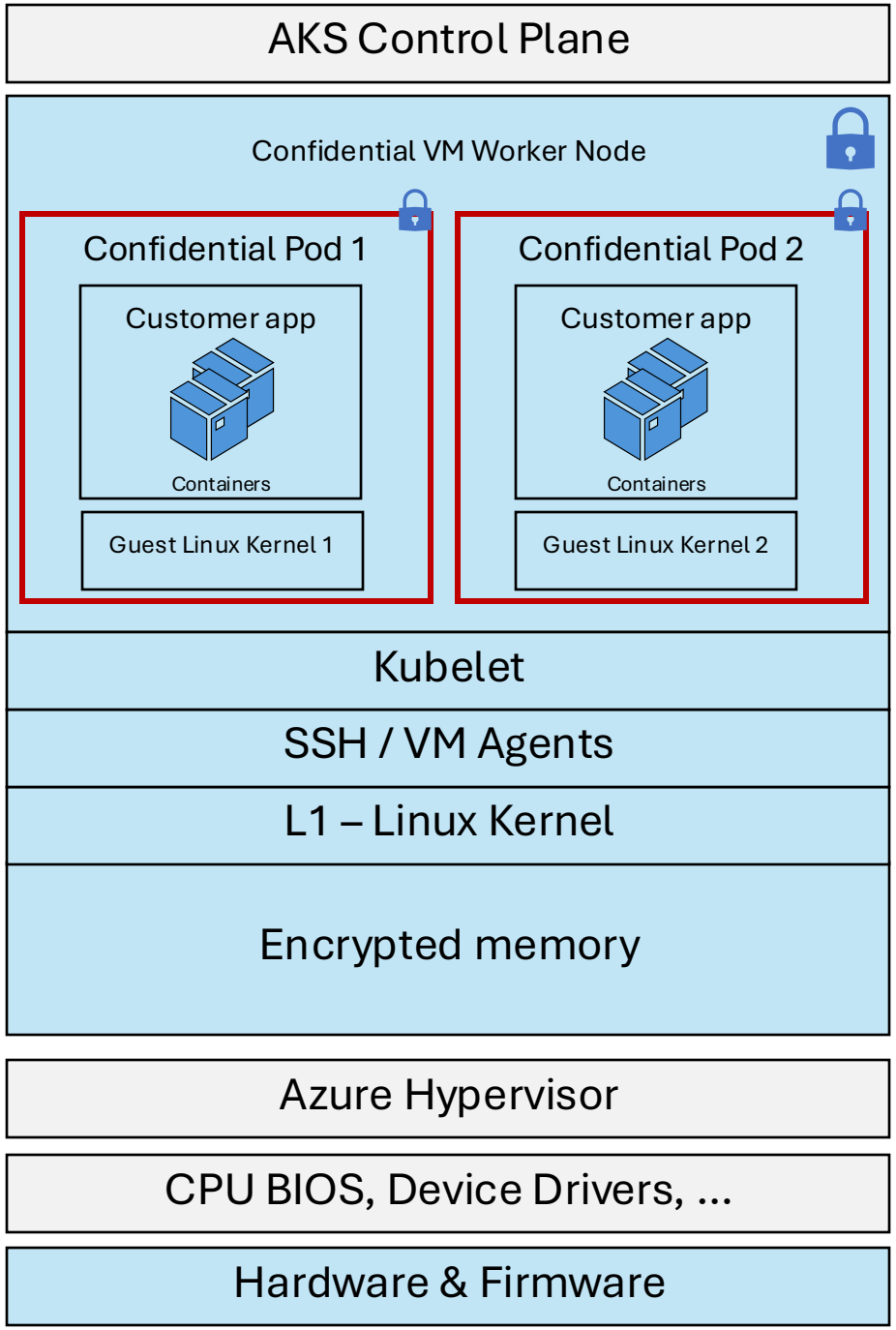
Public Preview



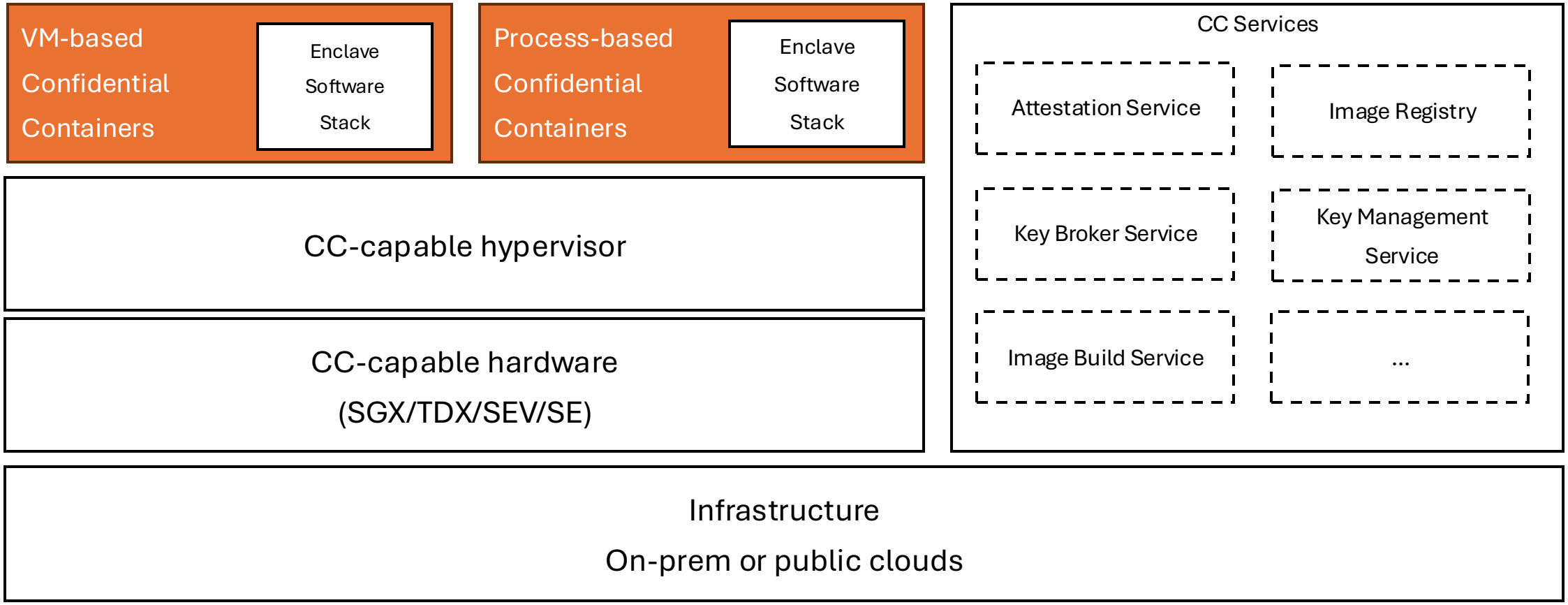
CONFIDENTIAL CONTAINERS

Confidential Containers on Azure Linux

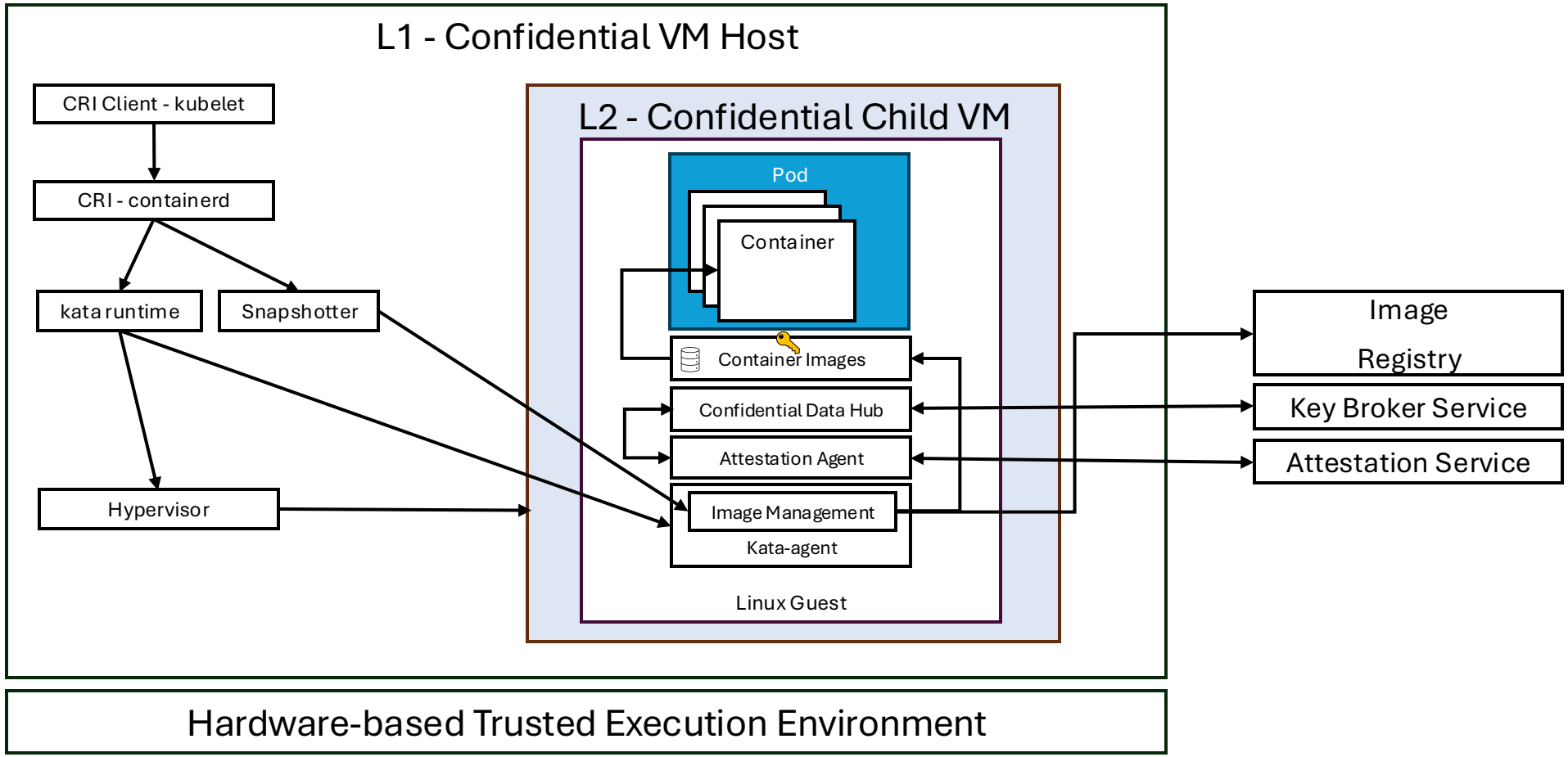
- Pod sandboxing feature for increased isolation
- Kata Containers and Cloud Hypervisor VMM
- Zero-trust security and operator access lockdown
- Code integrity with shared OS protection
- Run unmodified standard containers



CoCo Buiding Blocks



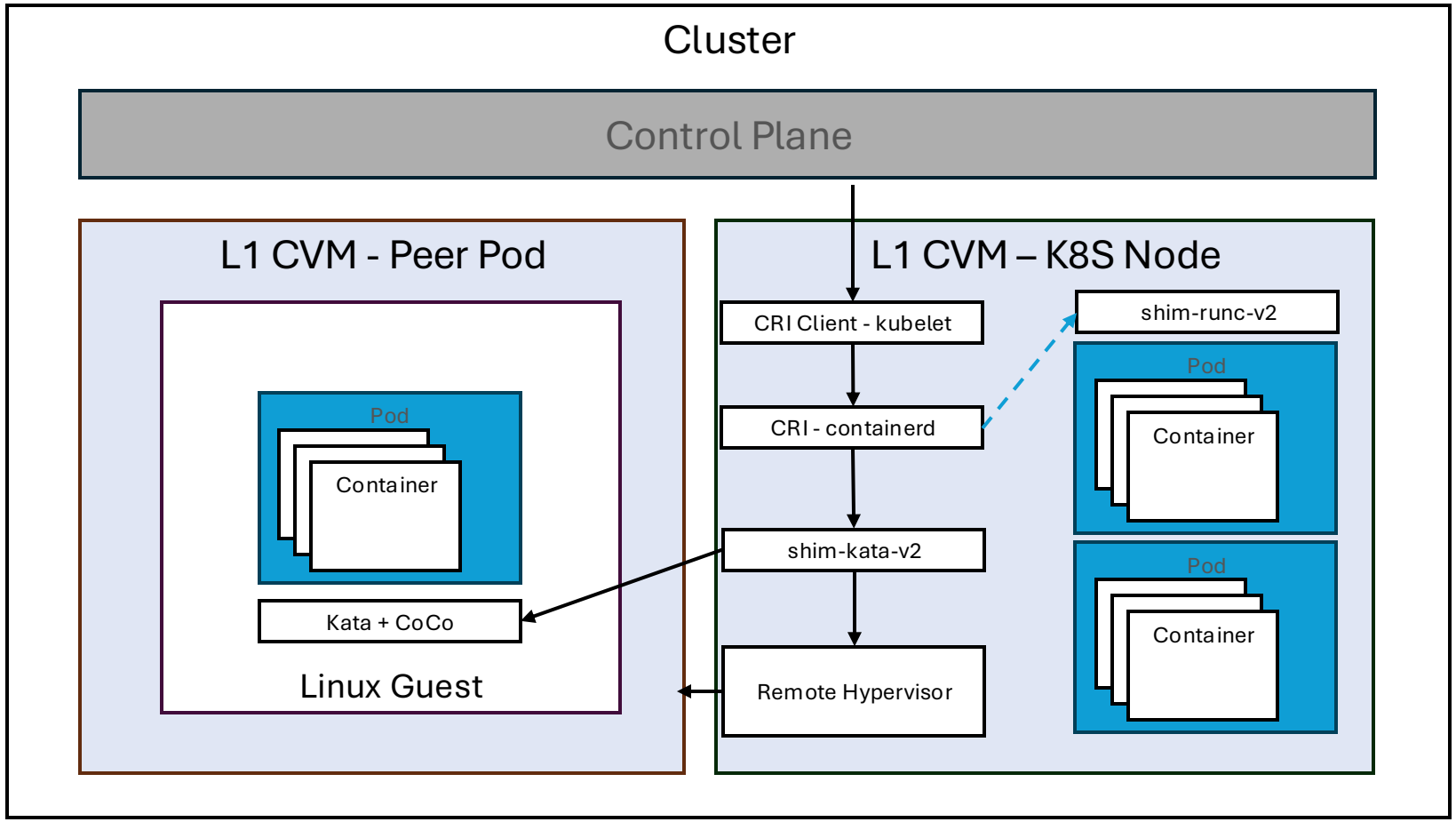
VM based CoCo



Hold up another minute!

Come on, nested virtualization, really?

Peer-Pods / Cloud API Adaptor



More info: https://confidentialcontainers.org/docs/cloud-api-adaptor/azure

CoCo - Trust boundaries

*"In **a typical Kubernetes context**, the **infrastructure provider** (such as a public cloud provider) is **a trusted actor** of a Kubernetes deployment."*

*"In a confidential computing context, that assumption no longer applies, and the infrastructure provider is a potential threat agent. Confidential Computing in general, and **Confidential Containers** in particular, try to **protect Kubernetes workload owners** from the infrastructure provider. **Any software component that belongs to the infrastructure (e.g., the Kubernetes control plane) is untrusted**."*

	Without CC	CC with CVMs	CC with CVMs & CoCo
Infrastructure Operator	✅	❌	❌
Hardware	✅	✅	✅
BIOS, Device Drivers	✅	❌	❌
Azure Hypervisor	✅	❌	❌
Host OS	✅	❌	❌
VM Guest admins	✅	✅	❌
K8S Control Plane	✅	✅	❌
Guest OS	✅	✅	❌
Guest Shared libraries	✅	✅	❌
Guest Kubernetes components	✅	✅	❌
Guest Application	✅	✅	❌
Utility VM (firmware, kernel, ..)			✅
Confidential Containers Stack			✅
CoCo Pod w/ Containers			✅

Adapted from: https://www.redhat.com/en/blog/understanding-confidential-containers-attestation-flow

Confidential Containers Runtime Operator

Confidential Containers Runtime Operator

An operator to deploy and configure confidential containers runtime on Kubernetes cluster

Install

Custom Resource Definitions

Cc Runtime

CcRuntime is the Schema for the ccruntimes API

View YAML Example

CHANNEL
alpha

VERSION
0.9.0 (Current)

MIN K8S VERSION
1.24.0

CAPABILITY LEVEL
- Basic Install
- Seamless Upgrades
- Full Lifecycle

Source: https://operatorhub.io/operator/cc-operator

AKS feature flag

Azure CLI

```
az feature register --namespace "Microsoft.ContainerService” \
                    --name "KataCcIsolationPreview”

az aks nodepool add  --resource-group "myResourceGroup”  \
                    --name "nodepool2" \
                    --cluster-name "myAKSCluster" \
                    --node-count 2 \
                    --os-sku AzureLinux  \
                    --node-vm-size Standard_DC4as_cc_v5 \
                    --workload-runtime KataCcIsolation
```

Source: https://learn.microsoft.com/en-us/azure/aks/deploy-confidential-containers-default-policy

DCas_cc_v5 and DCads_cc_v5-series (Preview)

Article • 08/22/2024 • 3 contributors

Feedback

In this article

Applies to: ✓ Linux VMs in Azure Kubernetes Service

> **Note**
>
> Preview Terms - These VM sizes are subject to the Supplemental Terms of Use for Microsoft Azure Previews.

> **Note**
>
> Confidential child capable VMs are currently enabled only through Azure Kubernetes Service (AKS) when you choose these VMs as your agent node sizes. If you wish to enable it outside AKS, please contact azconfidentialpm@microsoft.com.

Confidential child capable VMs allow you to borrow resources from the parent VM you deploy, to create AMD SEV-SNP protected child VMs. The parent VM has almost complete feature parity with any other general purpose Azure VM (for example, D-series VMs). This parent-child deployment model can help you achieve higher levels of isolation from the Azure host and parent VM. These confidential child capable VMs are built on the same hardware that powers our Azure confidential VMs. Azure confidential VMs are now generally available.

This series supports Standard SSD, Standard HDD, and Premium SSD disk types. Billing for disk storage and VMs is separate. To estimate your costs, use the Pricing Calculator. For more information on disk types, see What disk types are available in Azure?

Additional resources

Training

Module
Optimize performance and costs by using Azure Disk Storage - Training

Azure Disk Storage offers a range of disk types and capabilities that you can use to optimize application performance and costs in specific...

Certification
Microsoft Certified: Azure Virtual Desktop Specialty - Certifications

Plan, deliver, manage, and monitor virtual desktop experiences and remote apps on Microsoft Azure for any device.

Documentation

Azure DCasv5 and DCadsv5-series confidential virtual machines - Azure Virtual Machines

Specifications for Azure Confidential Computing's DCasv5 and DCadsv5-series confidential virtual machines.

Azure DCesv5 and DCedsv5-series confidential virtual machines - Azure Virtual Machines

Specifications for Azure Confidential Computing's DCesv5 and DCedsv5-series confidential virtual machines.

DCsv3 and DCdsv3-series - Azure Virtual Machines

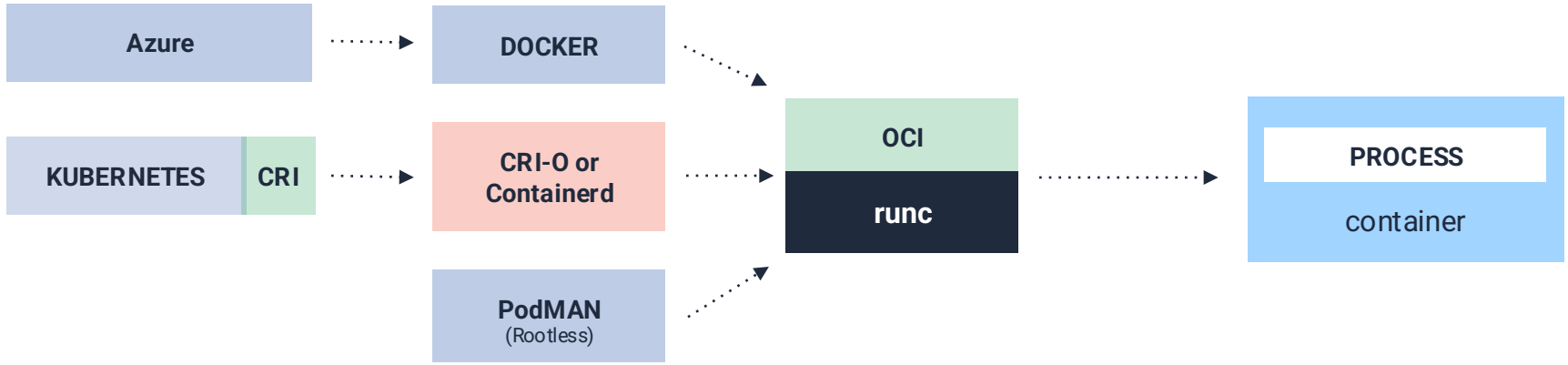
Specifications for the DCsv3 and DCdsv3-series Azure Virtual Machines.

Show 5 more

Source: https://learn.microsoft.com/en-us/azure/virtual-machines/dcasccv5-dcadsccv5-series

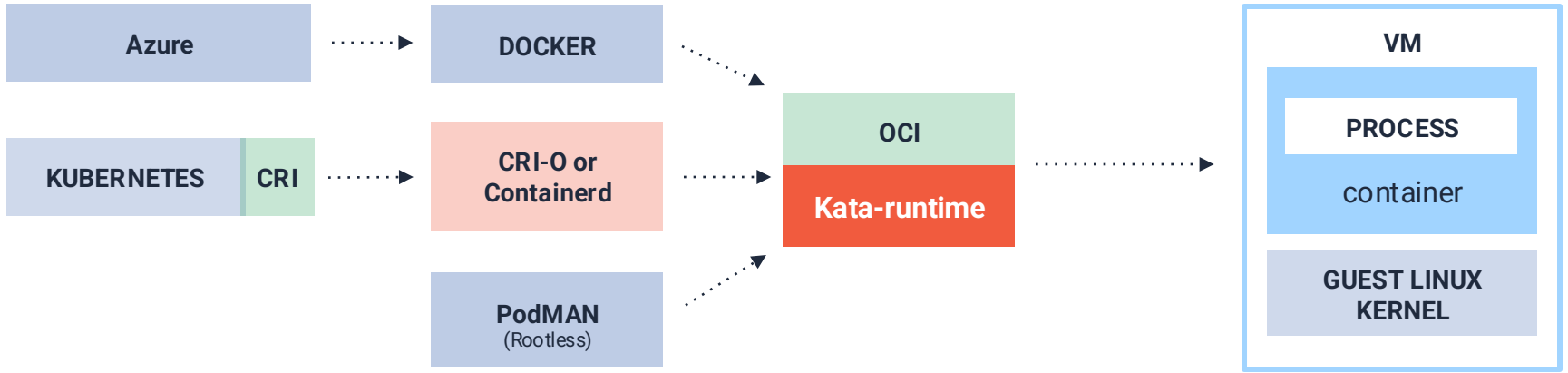
Seamless integration

Standard container initiation



Kata Containers initiation

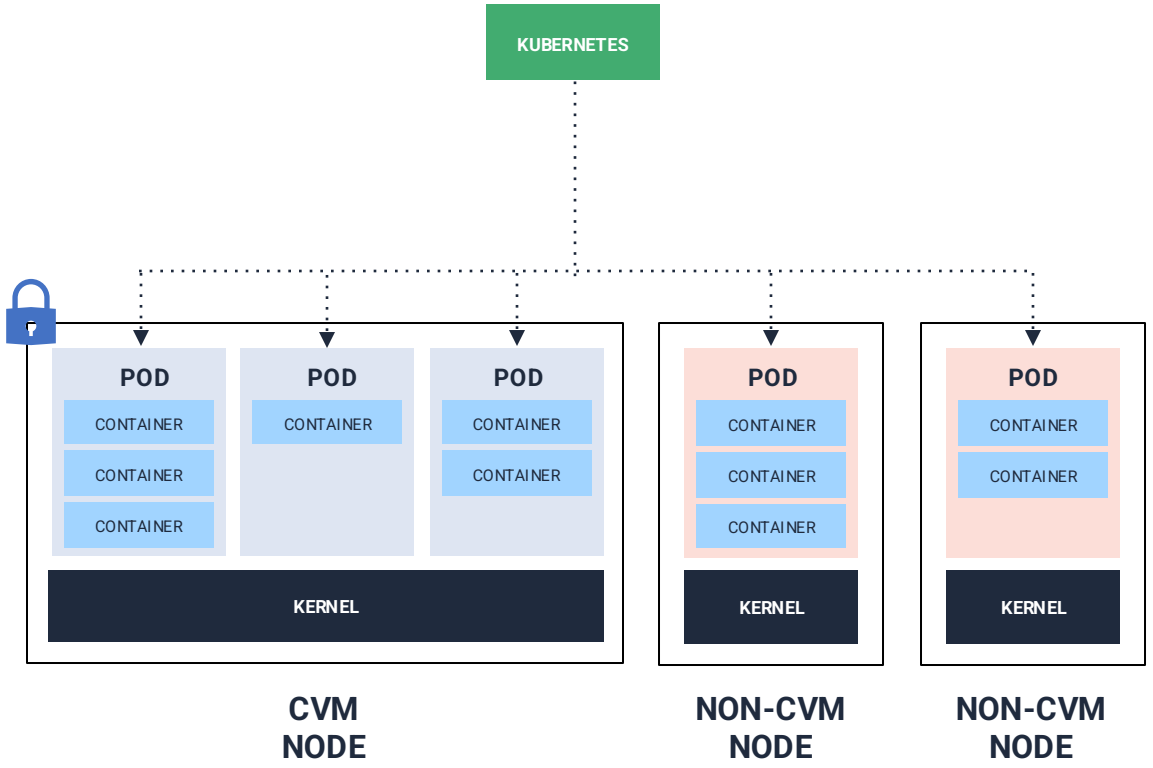
Looks and acts like a container using K8s, Docker or PodMAN



Adapted from: https://katacontainers.io/learn

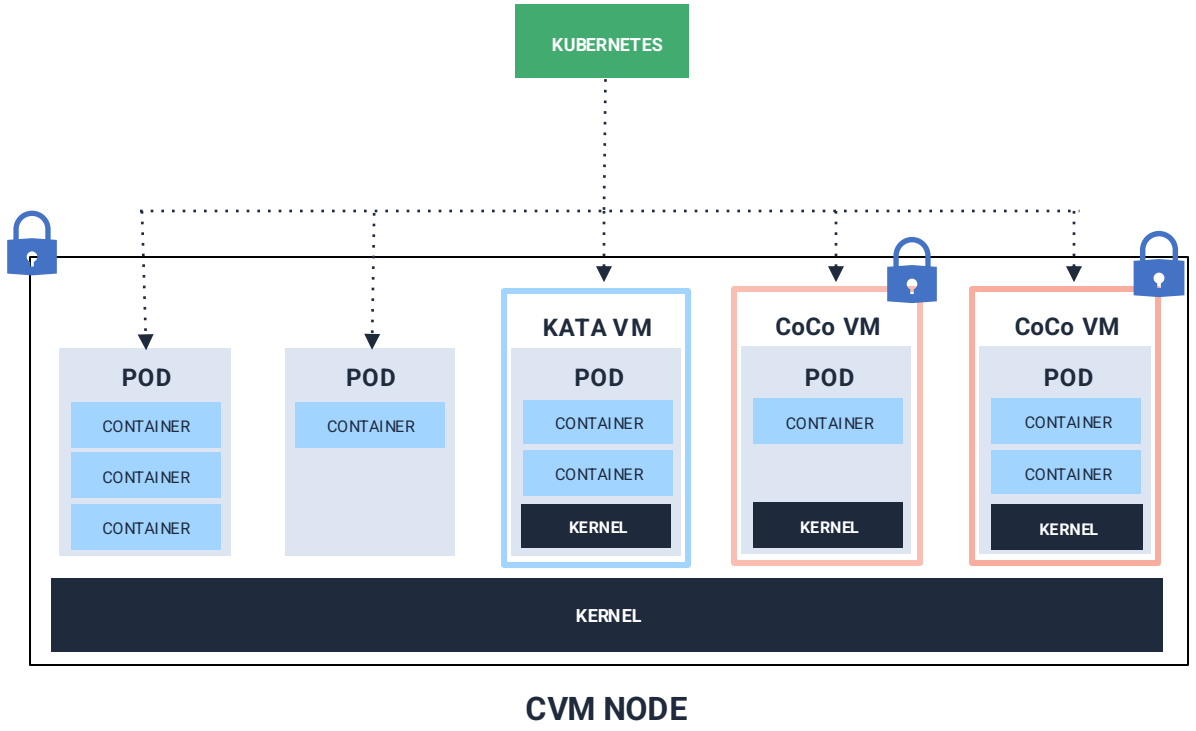
Confidential Containers on AKS

Standard containers



Isolate sensitive workloads by node

Confidential Containers with Kata Containers

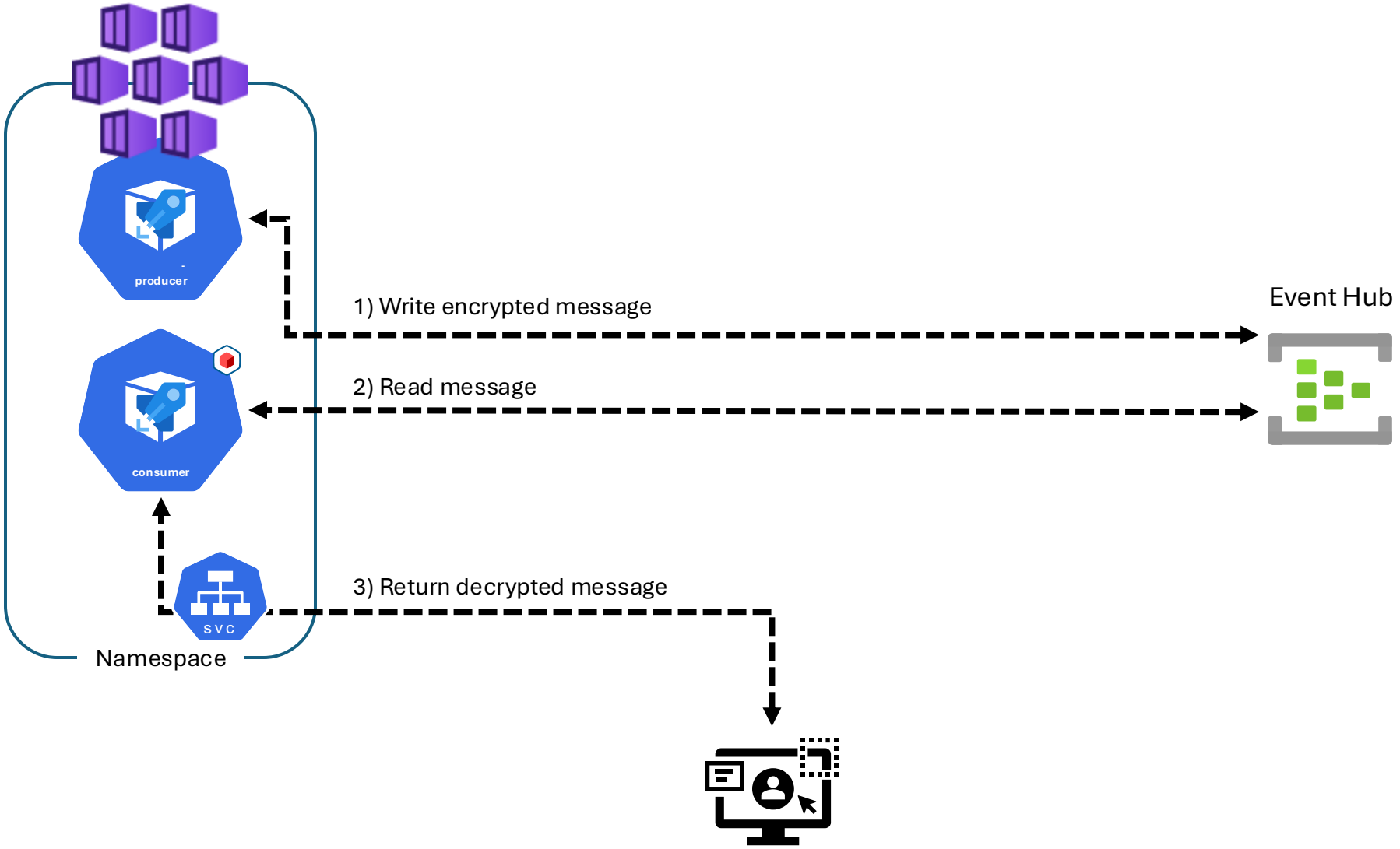


Pod isolation and **protection from unauthorized access and achieve code integrity for sensitive workloads** within a node

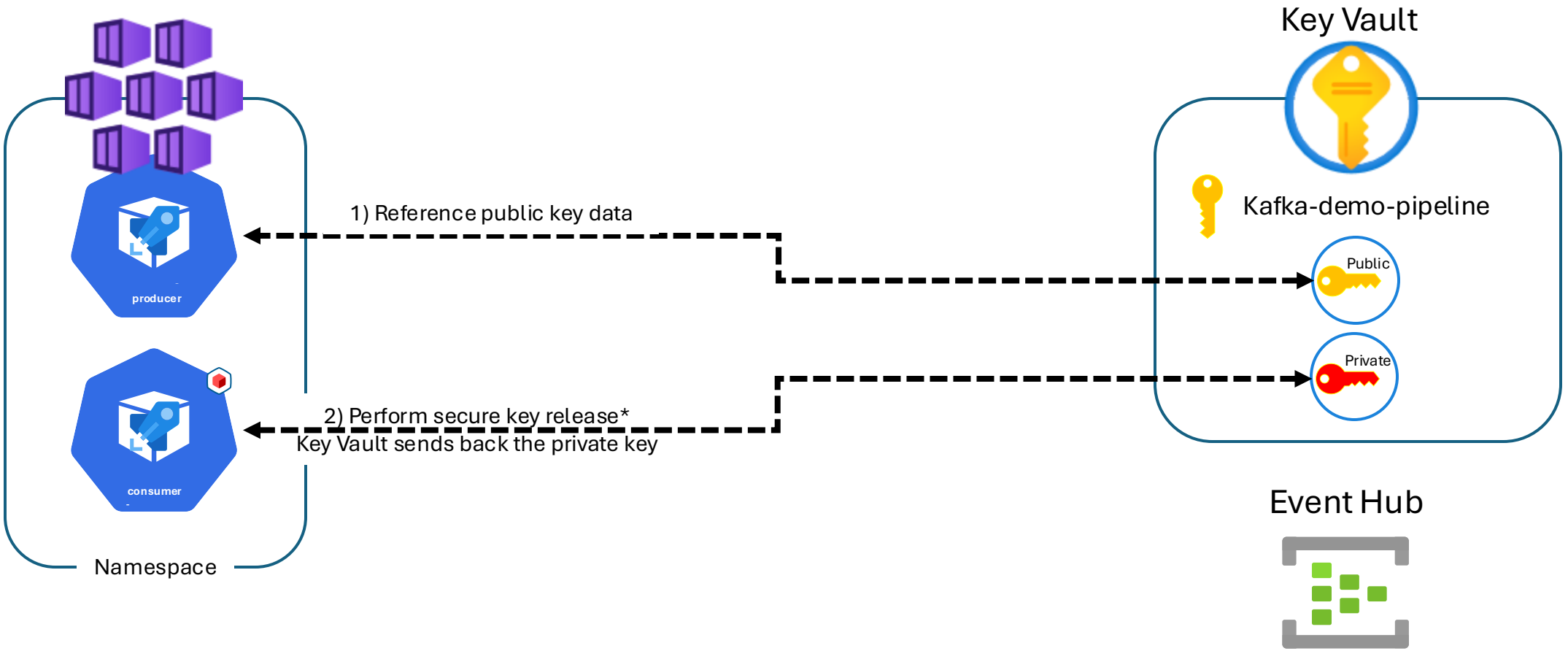
Adapted from: https://katacontainers.io/learn


Demo time

Demo – What are we doing?

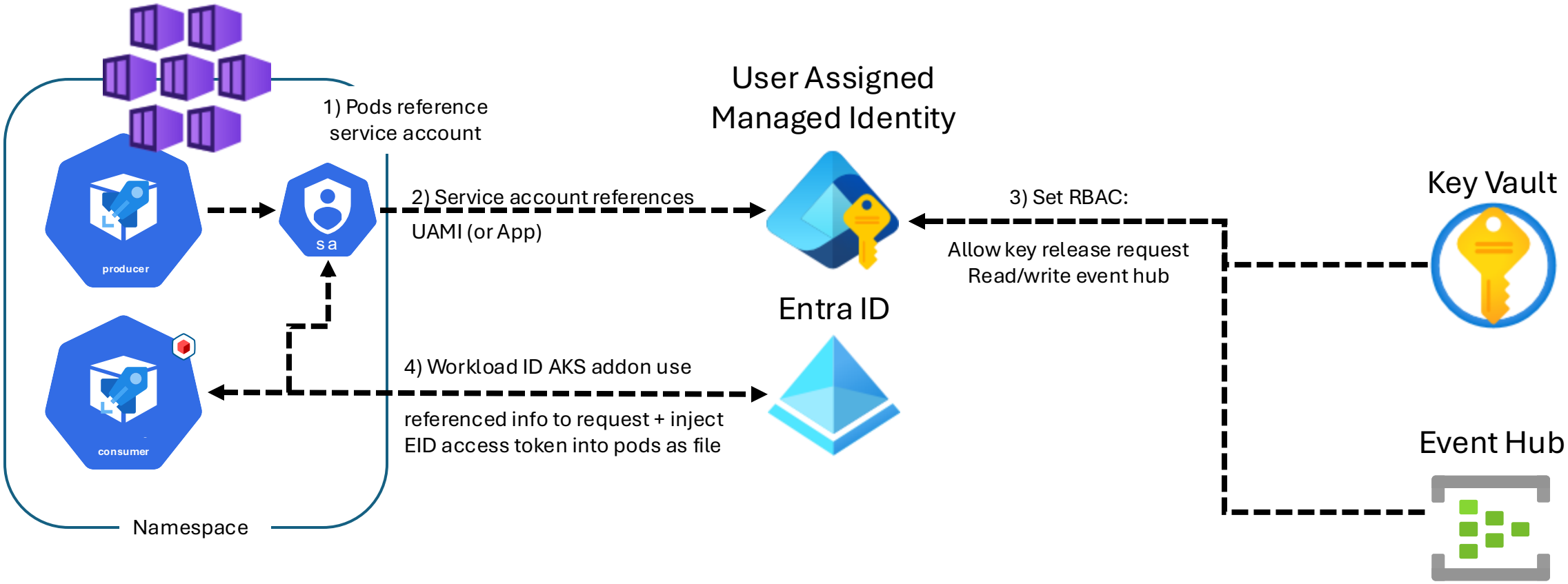


Demo – Secure Key Release

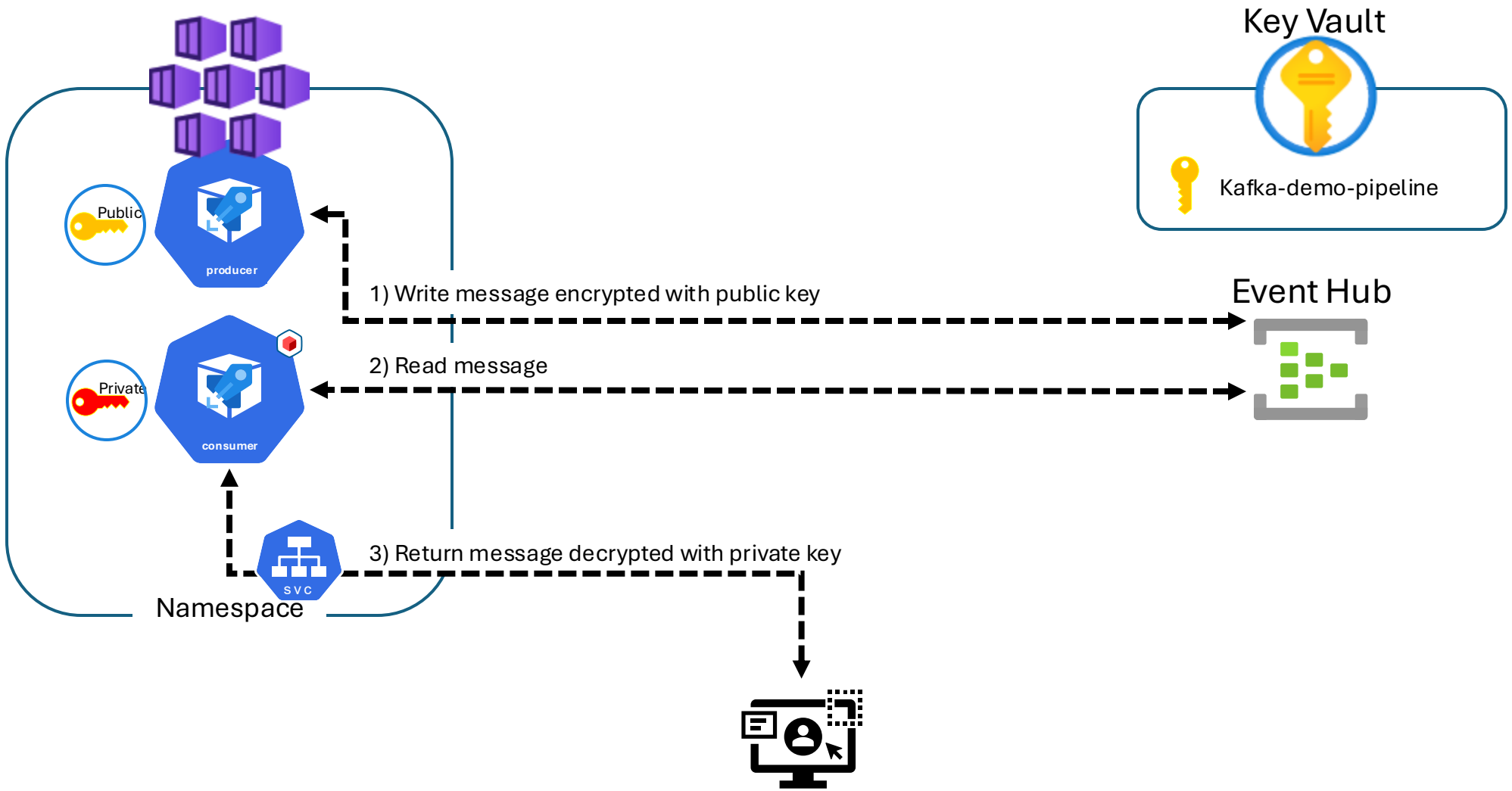


** "Secure key release enables the release of an HSM protected key from AKV to an attested Trusted Execution Environment"*

Demo – Azure RBAC + Workload ID

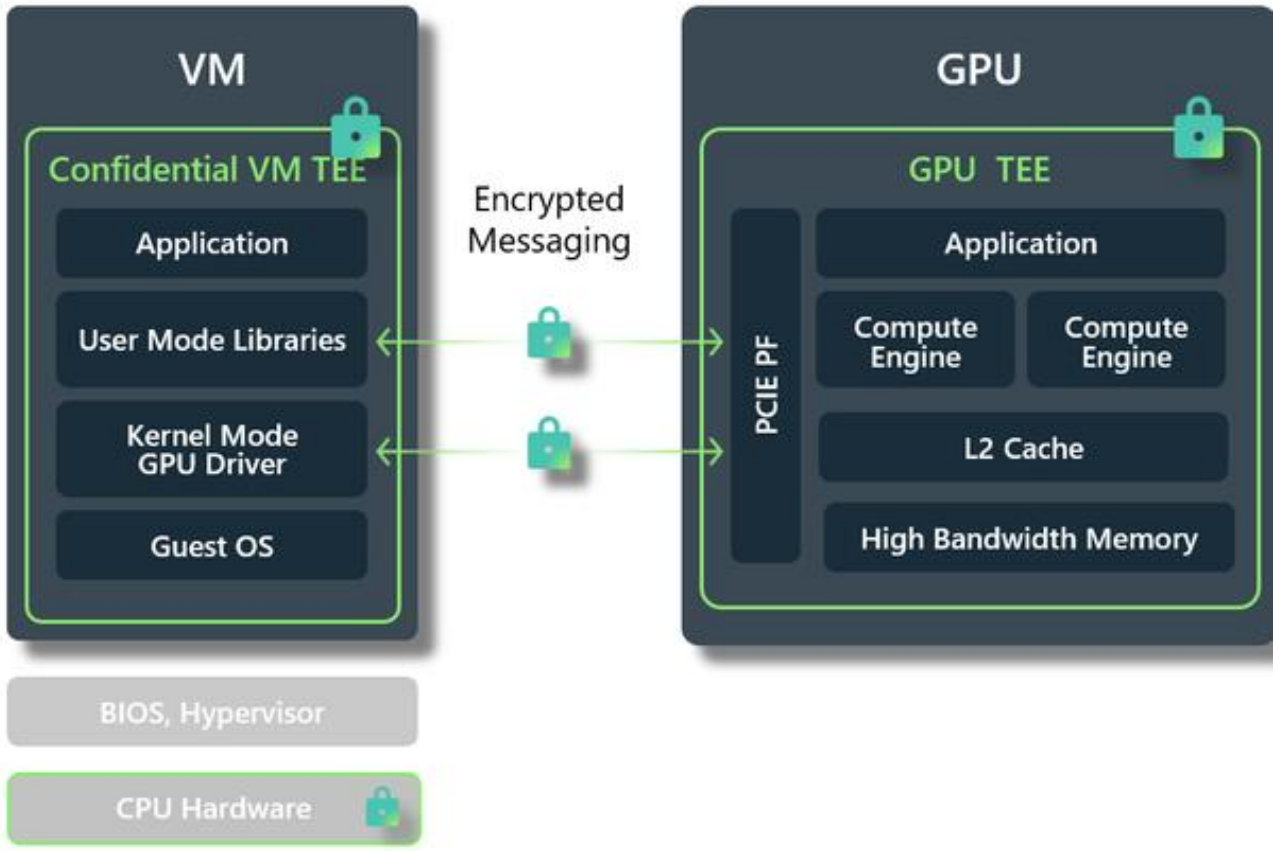


Demo – Processing messages



CVMs with NVIDIA H100 Tensor Core GPUs

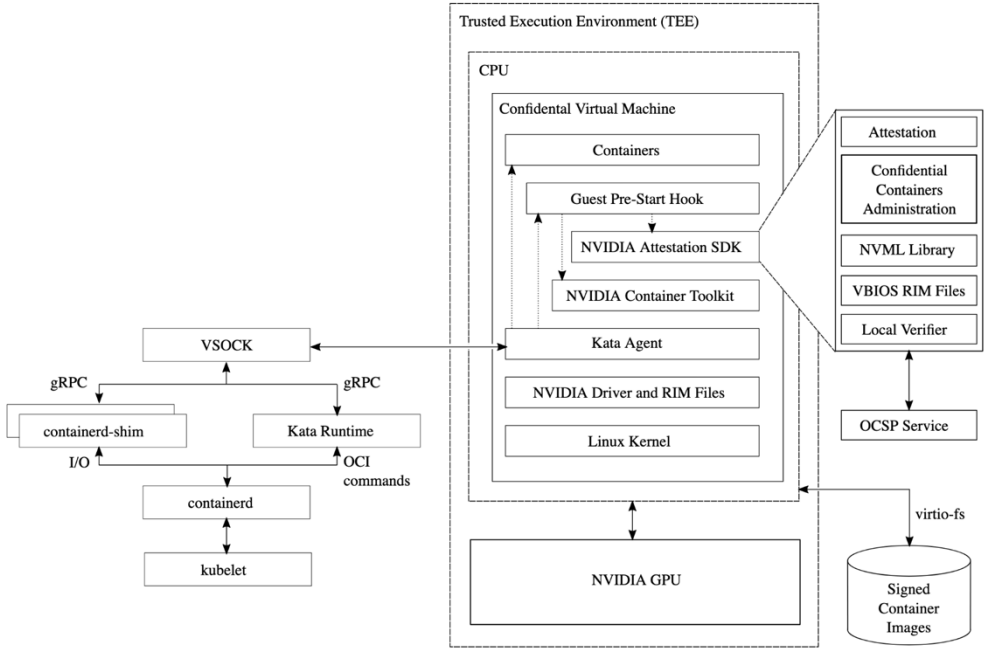
- *Next-generation CPUs:* AMD 4th Gen EPYC processors with SEV-SNP technology to meet CPU performance for AI training/inference.
- *AI state-of-the-art GPUs:* NVIDIA H100 Tensor Core GPUs with 94GB of High Bandwidth Memory 3 (HBM3).
- *Trusted Execution Environment (TEE)* that spans confidential VM on the CPU and attached GPU, enabling secure offload of data, models and computation to the GPU.
- *VM memory encryption* using hardware-generated encryption keys.
- *Encrypted communication* over PCIe between confidential VM and GPU.
- *Attestation:* Ability for CPU and GPU to generate remotely verifiable attestation reports capturing CPU and GPU security critical hardware and firmware configuration.



Source: https://techcommunity.microsoft.com/t5/azure-confidential-computing/announcing-azure-confidential-vms-with-nvidia-h100-tensor-core/ba-p/3975389

NVIDIA GPU Operator with CoCo

About Support for Confidential Containers



High-Level Logical Diagram of Software Components and Communication Paths

Requirements

Refer to the *Confidential Computing Deployment Guide* at the https://docs.nvidia.com/confidential-computing website for information about supported NVIDIA GPUs, such as the NVIDIA Hopper H100.

The following topics in the deployment guide apply to a cloud-native environment:

- Hardware selection and initial hardware configuration, such as BIOS settings.
- Host operating system selection, initial configuration, and validation.

Source: https://docs.nvidia.com/datacenter/cloud-native/gpu-operator/latest/gpu-operator-confidential-containers.html

CoCo and CPU-only AI inferencing

microsoft / confidential-ai Public

Notifications | Fork 12 | Star 37

Code | Issues 3 | Pull requests 1 | Actions | Projects | Security | Insights

Files

main

Go to file

- .devcontainer
- inference
  - ci
  - client
  - deployment
  - docs
    - images
    - arch.md
  - external
  - maa
  - models
  - policy
  - server
  - .gitignore
  - README.md
  - env.sh
- vendor
- .gitmodules
- CODE_OF_CONDUCT.md
- LICENSE
- README.md
- SECURITY.md
- SUPPORT.md

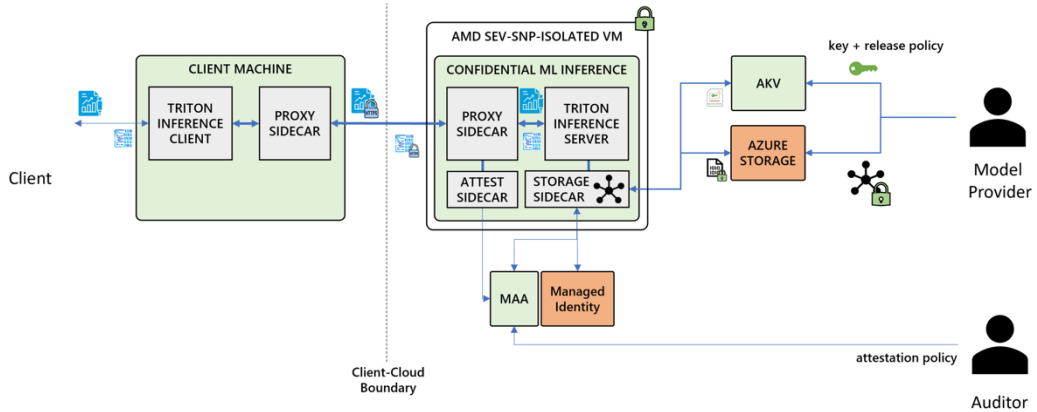
confidential-ai / inference / docs / arch.md

kapilvgit Initial commit — 4e65936 · last year — History

Preview | Code | Blame | 72 lines (42 loc) · 12.7 KB — Raw

Architecture

Overview



The figure above illustrates the architecure of the proposed confidential ML inference service.

Preperation. The model provider signs and encrypts the model in a clean room (on their premises). Signing is done using private/public cryptography (e.g., elliptic-curve) and encryption is done using an AES variant. The provider then uploads the encrypted model and the encryption key to Azure Storage and Azure Key Vault, referred to as AKV. The model provider also provisions a user-assigned managed identity, which is assigned the required Azure Resource Control roles for the Azure Storage and AKV resources.

Source: https://github.com/microsoft/confidential-ai

New scenarios


Internal Tools


SaaS offerings


ISV Partners


Finance


Governments


Healthcare

Dev tools


VS Studio/Code


WinDbg


CCF SDK


OpenEnclave SDK


Mystikos


Containerization

Confidential Enabled Azure PAAS


Azure SQL


Azure Machine Learning


Azure Key Vault


Azure Confidential Ledger


Azure Attestation


Azure Kubernetes Service


Azure IoT


Azure Databricks


Azure Data Explorer


Azure Data Share

Cloud and Edge


Azure VMs w/ App Enclaves


Azure Confidential VMs


Azure Trusted Launch


Azure IoT Edge Devices


Confidential Containers on ACI


Azure Virtual Desktop with CVMs


Azure Managed CCF**

New Hardware


Intel


AMD


ARM


NVIDIA**

Standardization


Confidential Computing Consortium


Microsoft Research

Public preview
****Limited preview***

Confidential Computing at Microsoft

Key Takeaways

Overcome cloud adoption challenges

CoCo standardizes Confidential Computing at the pod level

CoCo simplifies Confidential Computing in Kubernetes

CoCo runs on the Kata Containers project

Kata Containers pods use nested virtualization or peer-pods

CoCo on any cloud using Confidential Computing hardware

Confidential Computing workloads must use attestation

Want to learn more about Azure Confidential Computing?

Take a look at these blog posts over at

https://thomasvanlaere.com

VERIFYING MICROSOFT AZURE ATTESTATION TOKENS

AZURE CONFIDENTIAL COMPUTING: SECURE KEY RELEASE

AZURE CONFIDENTIAL COMPUTING: IAAS

AZURE CONFIDENTIAL COMPUTING: CONFIDENTIAL VMS

AZURE CONFIDENTIAL COMPUTING (SGX/OPENENCLAVE)

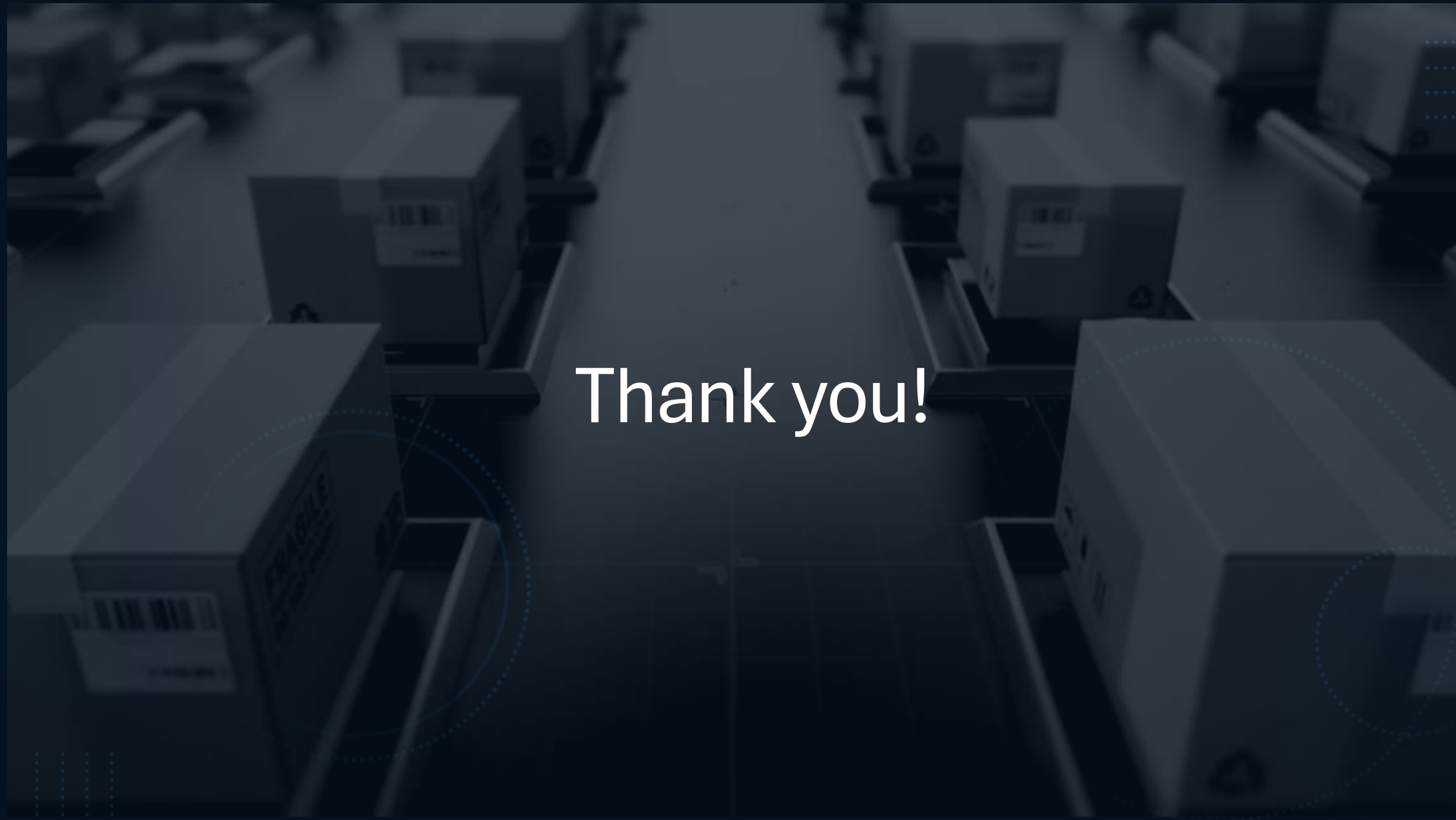
AZURE RBAC FOR SECURE KEY RELEASE

SECURE KEY RELEASE - PART 2

CONFIDENTIAL TEMP DISK ENCRYPTION

COCO - CONFIDENTIAL CONTAINERS

MICROSOFT AZURE ATTESTATION


Thank you!

References

- Confidential Containers Explained - James Magowan (IBM), Samuel Ortiz (Apple) – June 2022
  - https://www.youtube.com/watch?v=rdC2ETvzun0
- Confidential Containers: Verifiably secure computation in the cloud - Sean T. Allen (Microsoft) – July 18, 2022
  - https://www.microsoft.com/en-us/research/blog/confidential-containers-verifiably-secure-computation-in-the-cloud/
- Understanding the Confidential Containers Attestation Flow - Pradipta Banerjee (Red Hat), Samuel Ortiz (Rivos) - December 22, 2022
  - https://www.redhat.com/en/blog/understanding-confidential-containers-attestation-flow
- Confidential Containers Architecture - Confidential Containers team – April 1, 2023
  - https://github.com/confidential-containers/confidential-containers/blob/7a7808d4893affe5dc58fdcd7282f690356249be/architecture.md
- Experience with “Hard Multi-Tenancy” in Kubernetes Using Kata Containers - Shuo Chen (Databricks) - May 1, 2023
  - https://www.youtube.com/watch?v=hVUqqEGO2-Q
- Confidential Containers on Azure with OpenShift: A technical deep dive - Magnus Kulke, Pradipta Banerjee, Suraj Deshmukh, Jens Freimann – May 22, 2023
  - https://www.redhat.com/en/blog/confidential-containers-azure-openshift-technical-deep-dive
- Confidential Kubernetes: Use Confidential Virtual Machines and Enclaves to improve your cluster security - Fabian Kammel (Edgeless Systems), Mikko Ylinen (Intel), Tobin Feldman-Fitzthum (IBM) - July 6, 2023
  - https://kubernetes.io/blog/2023/07/06/confidential-kubernetes/
- Confidential Containers: Why, How, and Where Are We? - Magnus Kulke (Microsoft) - Oct 2023
  - https://www.youtube.com/watch?v=6fbzHTJk6BE
- Azure confidential computing and Intel: Technology for the AI Era | BRKFP308H - Vikas Bhatia (Microsoft), Anil Rao (Intel) – November 16, 2023
  - https://www.youtube.com/watch?v=bGLklrV-nD8
- Kata Containers: Security and Containers Without Compromise - Ildiko Vancsa (Open Infrastructure Foundation) – May 1, 2024
  - https://www.youtube.com/watch?v=1-0JT7xFd-E
- Deep Dive: Secure Orchestration of Confidential Containers on Azure Kubernetes Service – Manual Hueber (Microsoft) - May 17, 2024
  - https://techcommunity.microsoft.com/t5/linux-and-open-source-blog/deep-dive-secure-orchestration-of-confidential-containers-on/ba-p/4137179