Red Hat Summit

Connect

Confidential Computing

Trust me when I tell you not to trust anyone

Marcos Entenza

Marcos Entenza

Product Manager
Hybrid Platforms - OpenShift Core

What we'll cover

- Common security challenges
- What is Zero Trust? What is Confidential Computing? How are they related?
- What use cases will be addressed with Red Hat products?
- What is Attestation?
- Let's see a demo
- What's our roadmap

Key Challenges

Protecting Sensitive Data in Memory

There are many options to protect data at rest and data in motion, but what about data in use? When applications process data, it resides in memory (RAM).

Regulatory & Compliance Requirements

Industries such as finance and healthcare require strict guarantees that sensitive workloads remain confidential, even from cloud providers.

Insider Threats & Malicious Actors

Cloud providers, administrators, or attackers with root access can potentially view or manipulate data.

Lack of Trust in Cloud & Third Parties

Organizations hesitate to migrate sensitive workloads to the cloud due to concerns about unauthorized access by cloud operators or legal access requests.

Multi-Tenant & Shared Infrastructure Risks

Public cloud environments expose workloads to potential cross-tenant attacks if an adversary gains access to the underlying system.

Zero Trust and Confidential Computing

A Move Towards Zero Trust

Traditional Security Models

Assumed Trust

Perimeter based security model which assumed trust. Higher level of trust once inside the perimeter

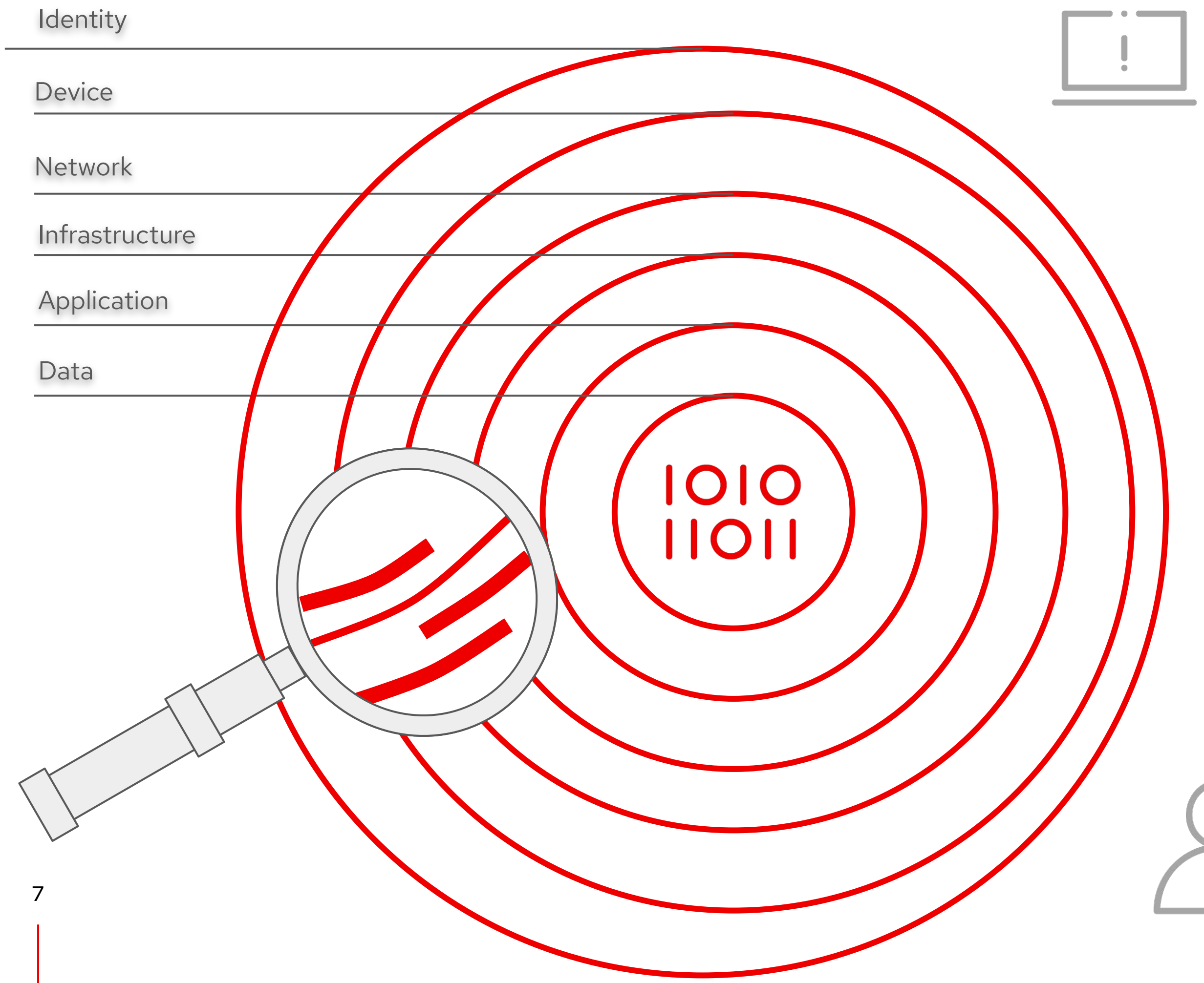
Zero Trust Security Model

Deny all, Verify all

No implicit trust. Authentication and authorization required between all parties. Identity, Integrity, Isolation

Zero Trust and Confidential Computing

Confidential computing supports a zero trust architecture



Zero Trust is about tightly managing access

- Who is on each side of the gate
- What is allowed through the gate
- How Is the gate itself protected

Confidential computing enables isolation and more ....

- Data in-use isolation and confidentiality
- Application isolation and confidentiality
- Human and machine identity
- Device / Infrastructure integrity
- Network and application integrity

Confidential Computing

Existing Encryption

Data At Rest

Data Encryption and System Attestation

- Protect Data on Disk using LUKS and Network Bound Disk Encryption (NBDE)
- Attest system state on boot, ensuring that system packages have not been compromised with IMA and Keylime
- Attest container workloads with Key Brokering Service (KBS)
- Ensure data remains unreachable in case of unauthorized access to the disk

Data In Motion

Encrypt Traffic Leveraging Strong, Future Proof Cryptography

- Protect data moving through the environment using strong, smart and validated cryptography
- Centralized management and establishment of secured connections native part of workflow for Red Hat Platform
- Automation provided allows consistent deployment and security configuration

New

Data In Use

Confidential Computing Use Trusted Execution Environment Capabilities

- Protect data and workloads in use with Trusted Execution Environments as Confidential Computing is enabled on the major hardware platforms for AMD, Intel and NVIDIA
- Leverage these Trusted Execution Environments on prem or in the major cloud platforms
- Increases the security level of organizations that manage sensitive and regulated data

What's required to secure data in use?

New

Data In Use

Confidential Computing Use Trusted Execution Environment Capabilities

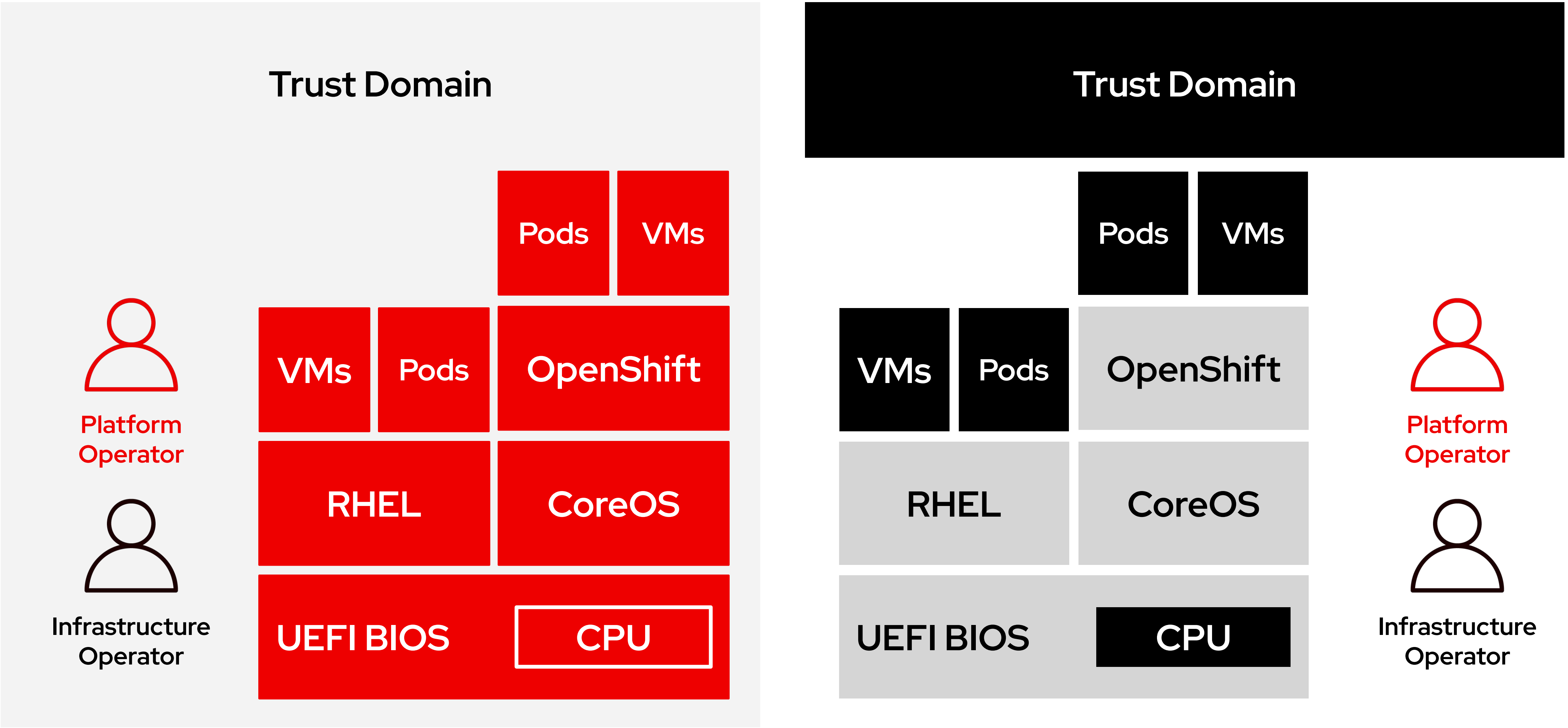
- Protect data and workloads in use with Trusted Execution Environments as Confidential Computing is enabled on the major hardware platforms for AMD, Intel and NVIDIA
- Leverage these Trusted Execution Environments on prem or in the major cloud platforms

Hypervisor / Host System Accessed by Provider Administrator

Memory used for the application / VM

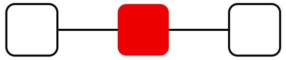
Hidden from the Operating System and Kernel inside a Trusted Execution Environment. Access only through special API.

Who & What to trust?



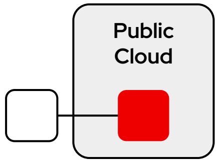
Categorization of Use Cases

What are customers asking for?



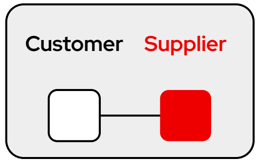
Partner Interaction

2 protected datasets interacting in confidential container in the same cluster



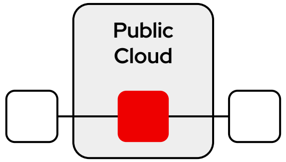
Secure Cloudburst

Using the public cloud to for peak workload or shared resources



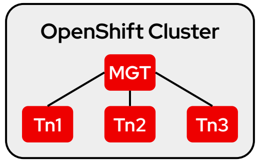
IP Protection/Integrity

Protection of supplier data and business logic in customer environments



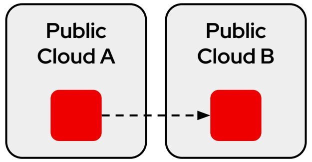
Edge Use Case

Protecting Edge device data in the public cloud for aggregation



Single Tenant Isolation

Isolating OpenShift Clusters



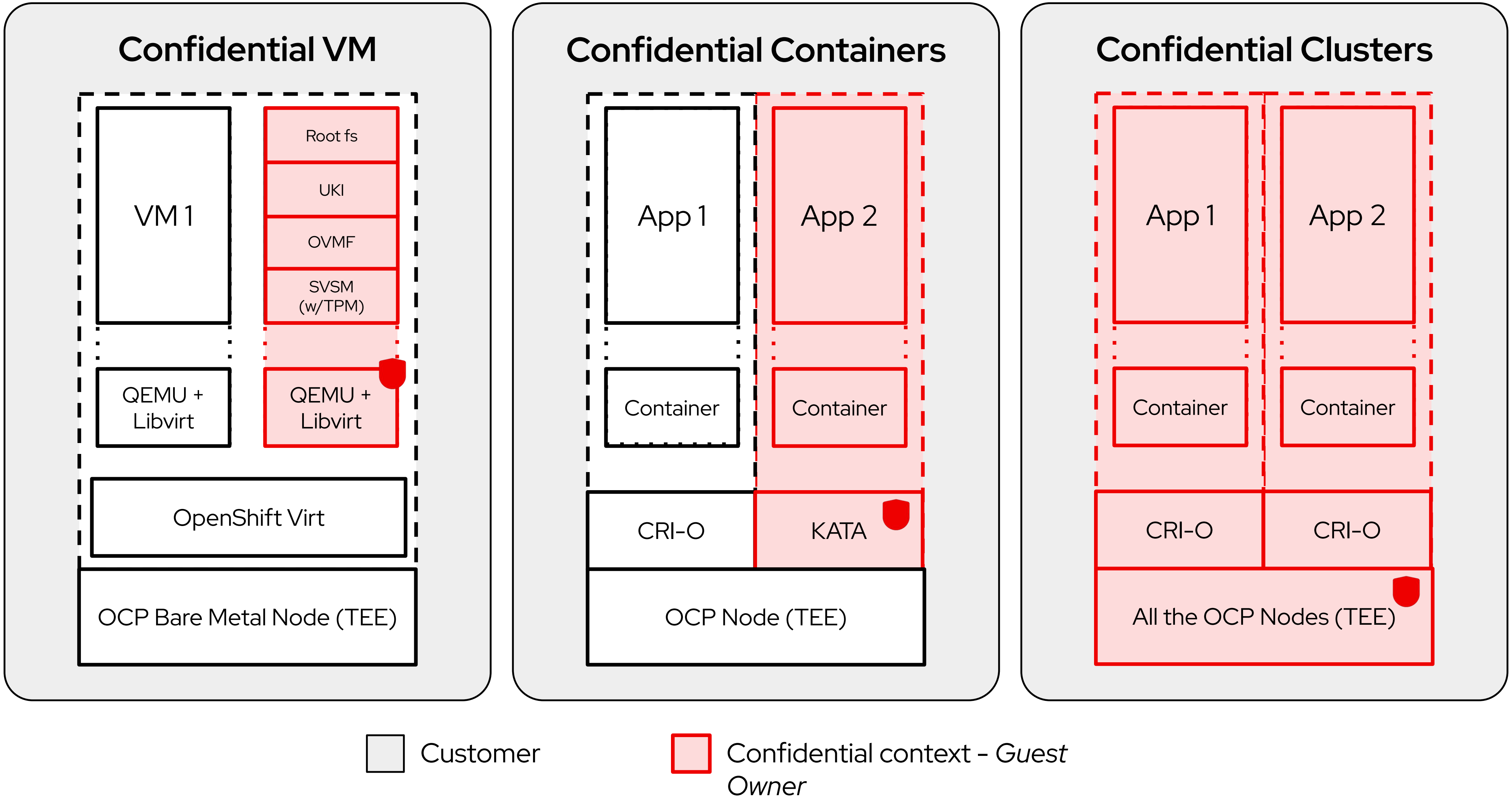
Digital Sovereignty

Encapsulating and moving workload from one provider to the next

How does Red Hat help?

Red Hat Investments in Confidential Computing

What does Red Hat do?



Red Hat Confidential Computing solutions

- **RHEL Confidential VM (guest)** – RHEL as a confidential guest on public cloud/hypervisor.
- **OpenShift Confidential Containers** – OpenShift sandboxed containers where the Kata pod is a confidential VM (an implementation detail hidden from the end user, who would choose the Confidential Containers runtime of OSC)
- **OpenShift Virtualization Confidential VMs** – OpenShift Virtualization with Confidential Computing enabled, i.e. its VMs can be Confidential VMs
- **OpenShift Confidential Clusters** – an OpenShift Cluster where the nodes are installed in Confidential VMs, e.g. OpenShift cluster installed on Azure CVM nodes

Scope of RHEL Confidential VMs (guest)

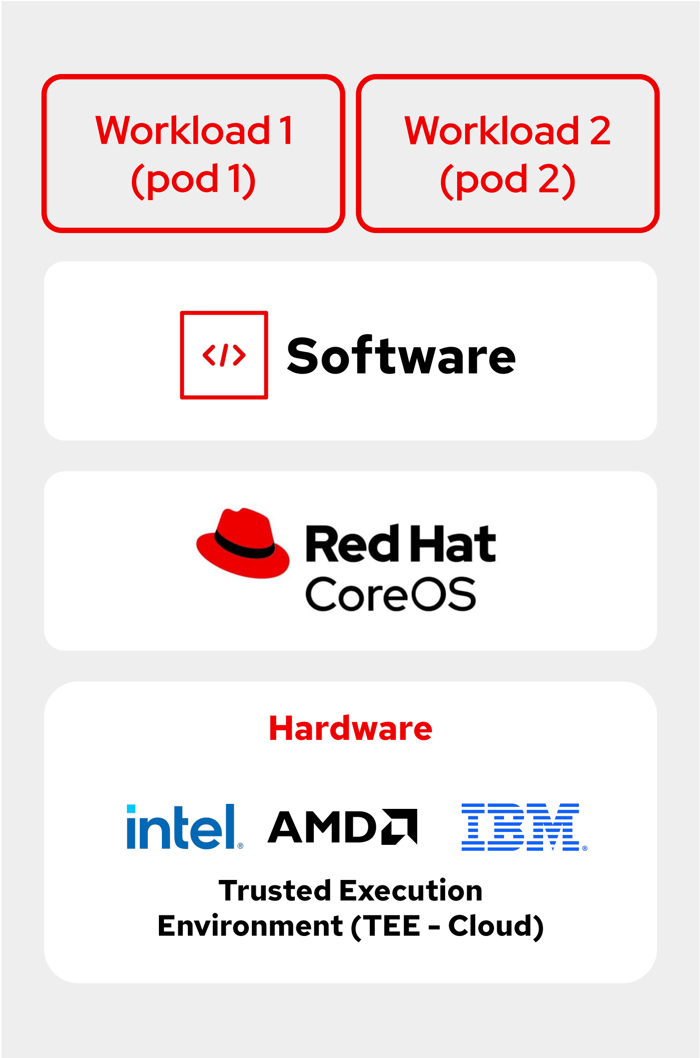
- RHEL Confidential Virtual Machines on Public Cloud
  - RHEL on Azure [GA with RHEL 9.6/10.0] - Including attestation
  - RHEL on Google Cloud Platform (GCP) [GA]
  - RHEL on AWS (SEV-SNP only) [GA]
- RHEL Confidential Virtual Machines on Hypervisors
  - OpenShift Virtualization
- Unified Kernel Images (UKIs)
  - Red Hat signed UKIs for RHEL, being consumed by RHEL CVM on any footprint

Scope of Confidential Containers

- OpenShift sandboxed containers (OSC), built on Kata Containers, provide the additional capability to run confidential containers (CoCo).
- Confidential Containers (CoCo) run containers in Trusted Execution Environments (TEEs)
- Isolate and protect workloads inside a shared OpenShift cluster
- The CoCo feature was promoted to GA with OSC 1.10 release (July 2025) for Azure
    - Tech Preview for Azure Red Hat OpenShift (ARO) for both Intel TDX and AMD SEV-SNP.
    - Tech preview on IBM Z and LinuxONE using Secure Execution for Linux (IBM SEL)
    - Dev Preview on Bare Metal for AMD SEV-SNP

What is Attestation?

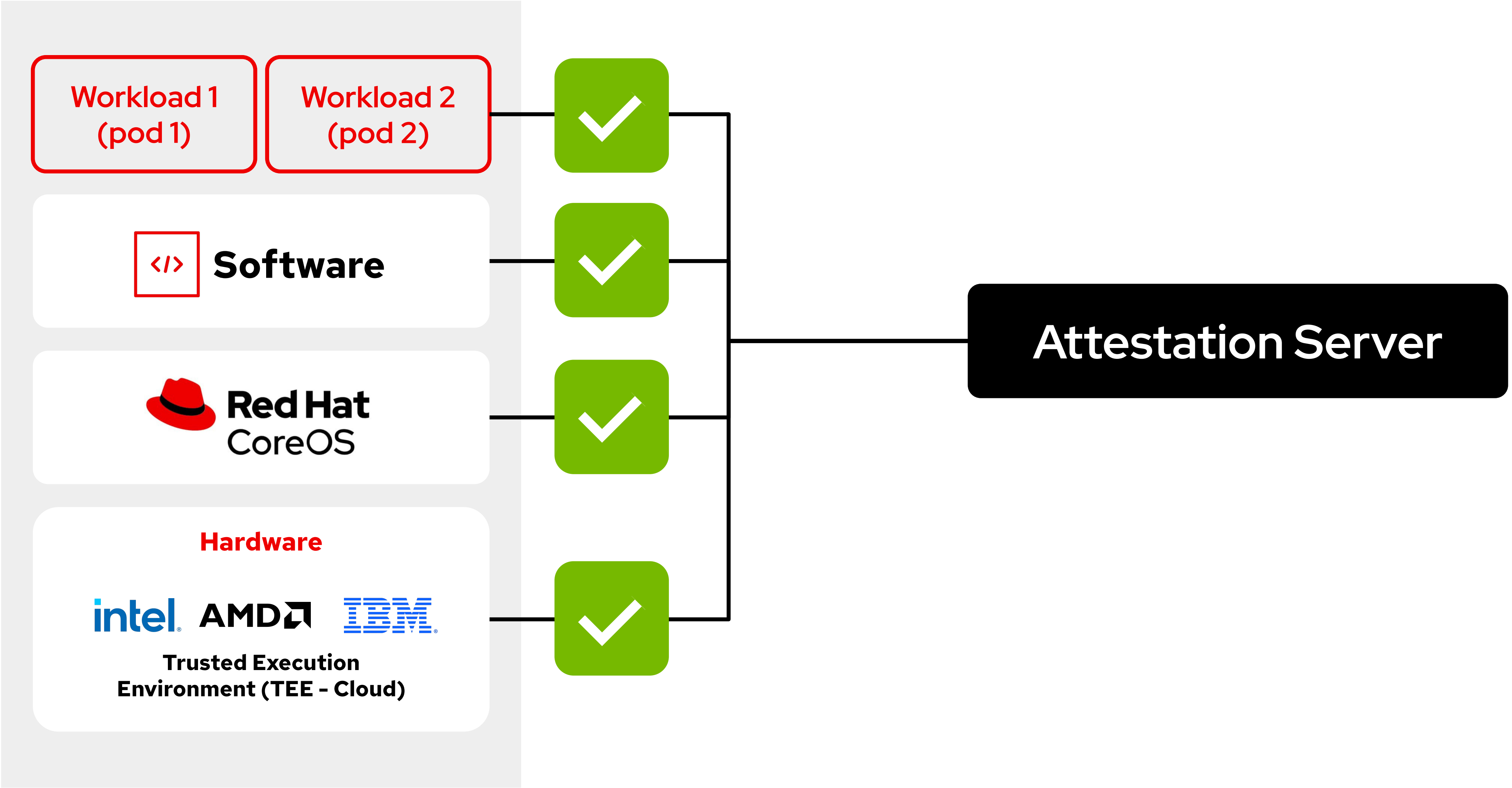
What about the Software Stack?



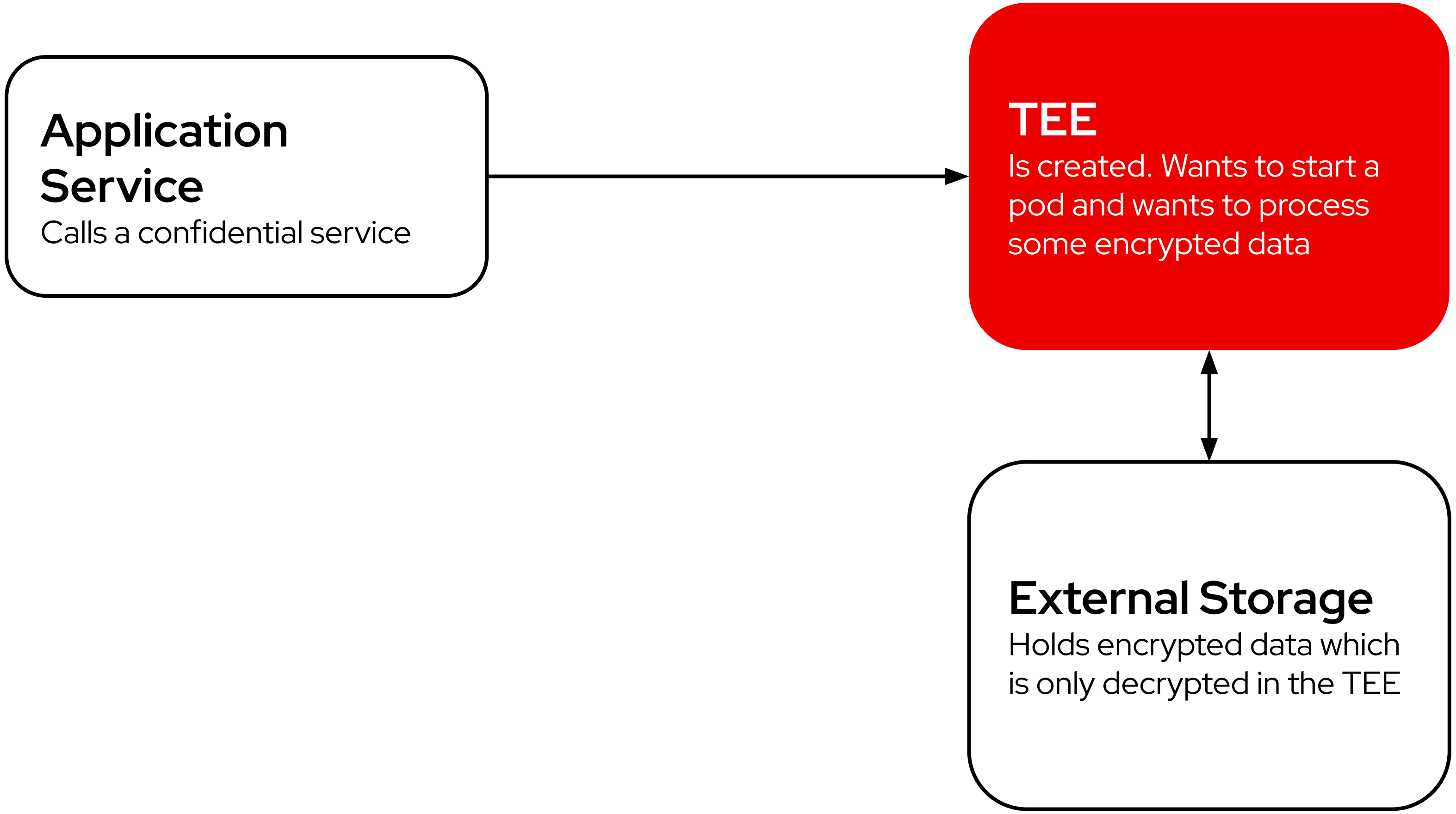
- Software cannot be trusted in its own
- Need a way to check has not been altered
- Need a way to build trust from the TEE
- Need to ensure the hardware was unaltered

➔ **Attestation**

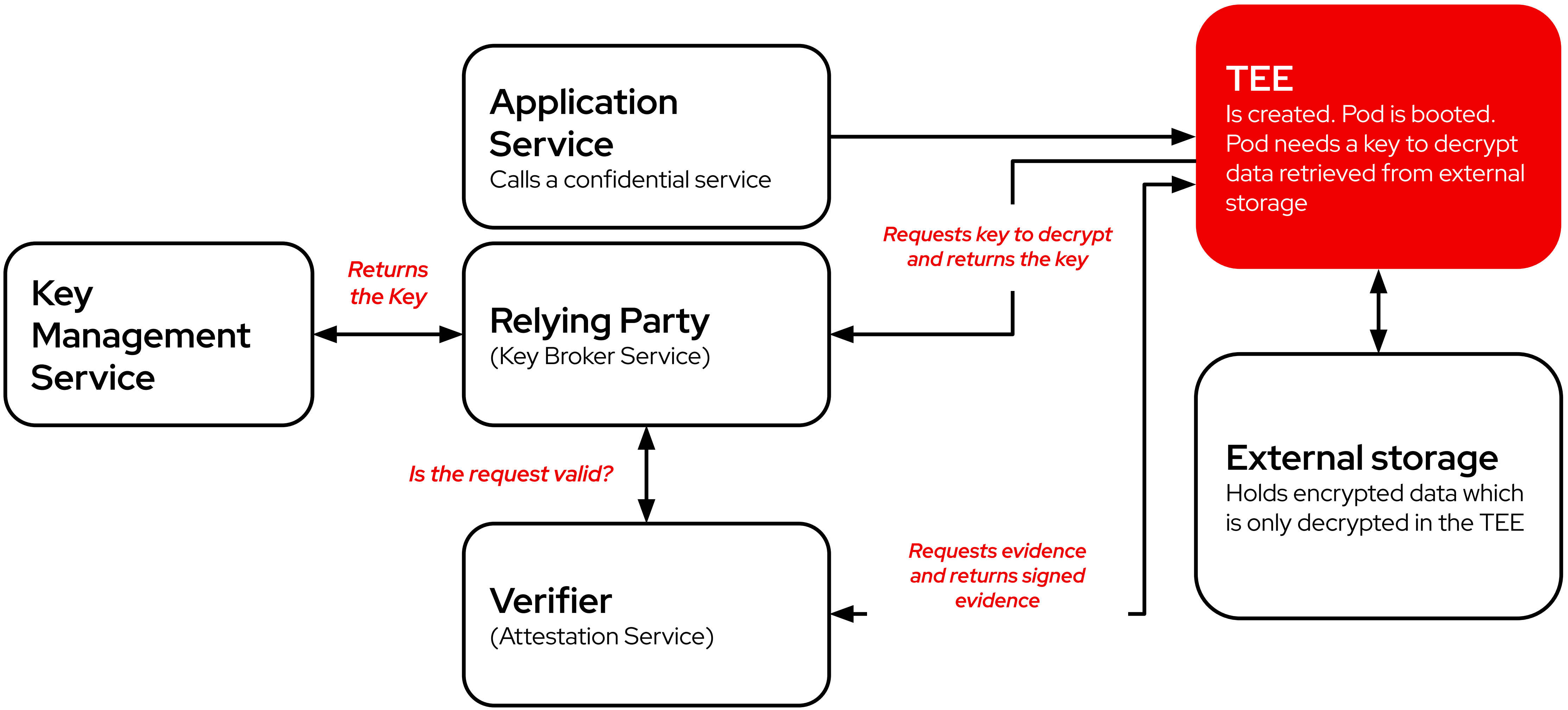
What about the Software Stack?



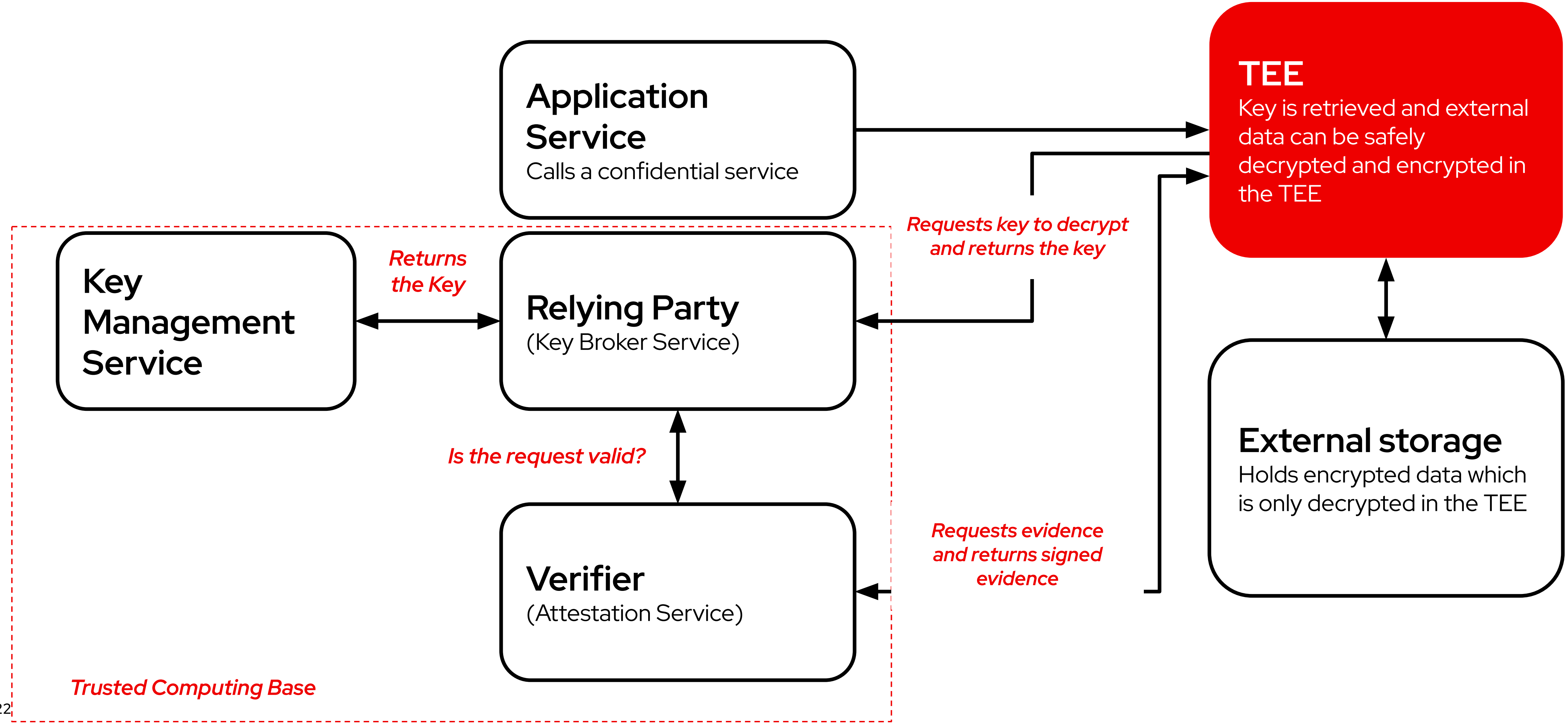
Flow of the Attestation



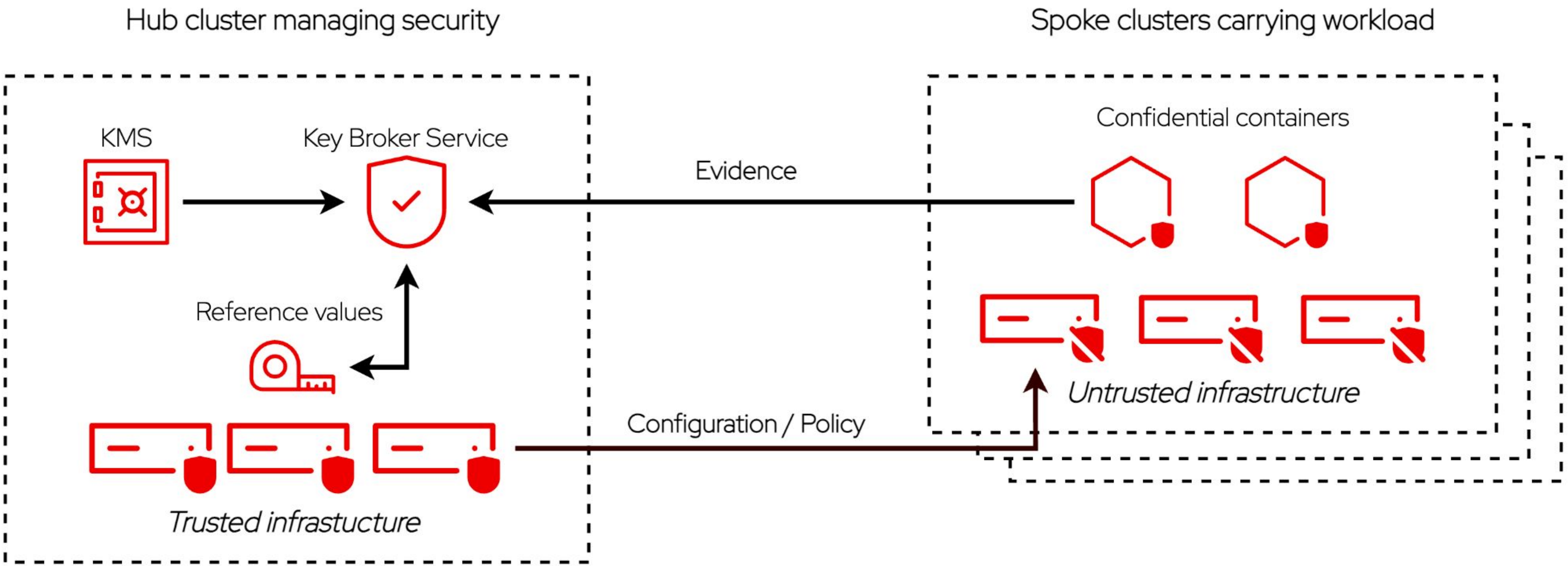
Flow of the Attestation



Flow of the Attestation



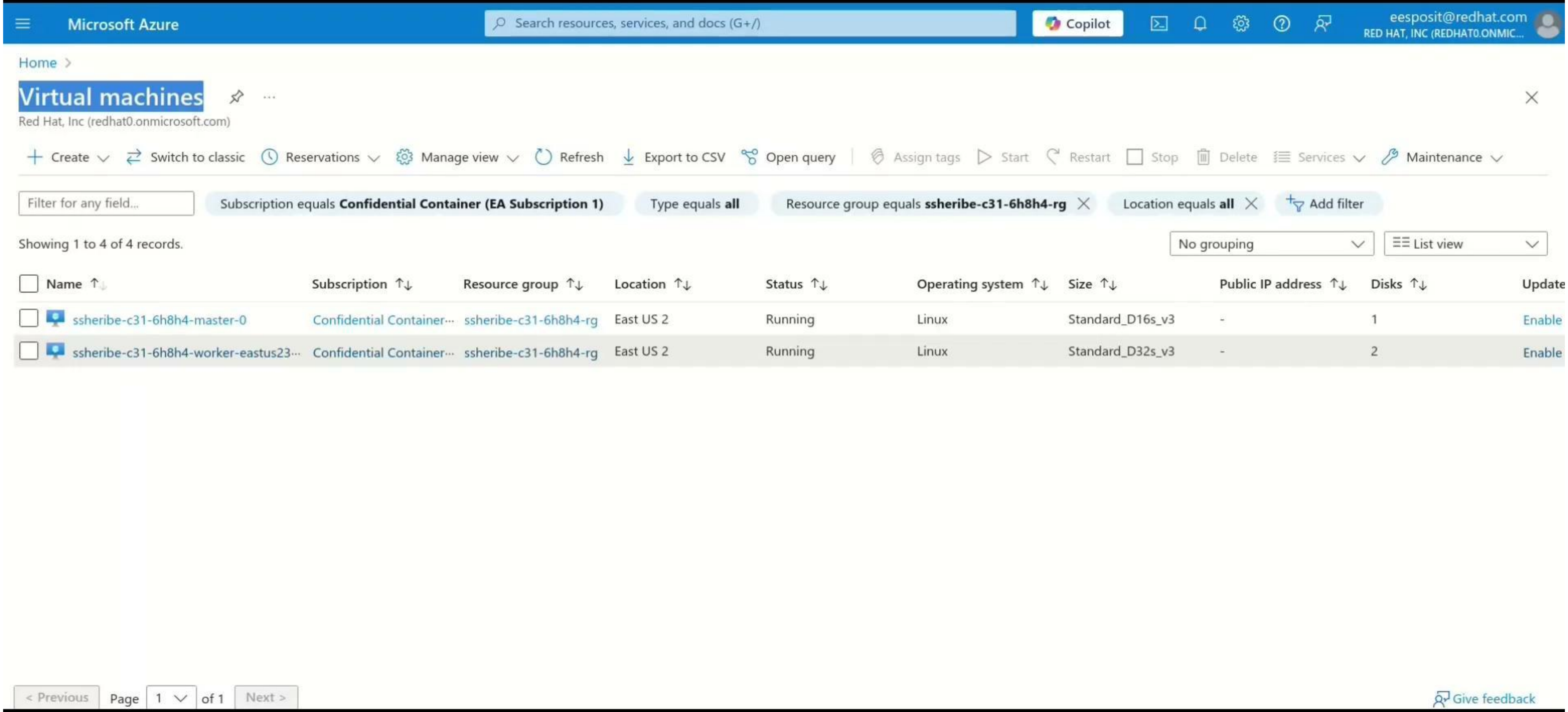
Remote attestation requires a hub & spoke model



Let’s see a Demo

Secure AI Inferencing - A short Demo

- This demo will show AI inferencing workload running in a **Confidential Container**, using **NVidia NIM**, inside an **OpenShift AI cluster**. The workload will consume a **Confidential GPU**.


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
eesposit@redhat.com
RED HAT, INC (REDHAT0.ONMIC...
Home >
Virtual machines
Red Hat, Inc (redhat0.onmicrosoft.com)
Create
Switch to classic
Reservations
Manage view
Refresh
Export to CSV
Open query
Assign tags
Start
Restart
Stop
Delete
Services
Maintenance
Filter for any field...
Subscription equals Confidential Container (EA Subscription 1)
Type equals all
Resource group equals ssheribe-c31-6h8h4-rg
Location equals all
Add filter
Showing 1 to 4 of 4 records.
No grouping
List view
Name
Subscription
Resource group
Location
Status
Operating system
Size
Public IP address
Disks
Update
ssheribe-c31-6h8h4-master-0
Confidential Container...
ssheribe-c31-6h8h4-rg
East US 2
Running
Linux
Standard_D16s_v3
-
1
Enable
ssheribe-c31-6h8h4-worker-eastus23...
Confidential Container...
ssheribe-c31-6h8h4-rg
East US 2
Running
Linux
Standard_D32s_v3
-
2
Enable
< Previous
Page
1
of 1
Next >
Give feedback

Roadmap

Confidential Computing Roadmap on RHEL

	H1 2025	H2 2025	H1 2026	H2 2026
RHEL CVM on Cloud	• **RHEL CVM is GA on AWS (SEV-SNP), GCP (SEV-SNP, TDX) without attestation** • **RHEL CVM is GA on Azure with Azure Attestation**	• PoCs for RHEL CVM on Cloud with Trustee attestation	• Tech Preview for RHEL CVM on Cloud with Trustee attestation	
Attestation	Trustee Boot Attestation “Crawl”	Keylime runtime Attestation “Crawl”	Trustee Boot Attestation “Walk”	

This roadmap is subject to change.

Confidential Containers Roadmap on OpenShift

	Q2 2025	Q3 2025	Q4 2025	H1 2026	H2 2026
Confidential Containers	• Conf Containers GA for IBM-Z via IBM Hyper Protect Services	• Conf Containers on Azure on Intel TDX and AMD SEV-SNP - GA	• Conf Containers on Bare Metal on Intel TDX and AMD SEV-SNP - TP • Conf Containers with Confidential GPUs on Azure - DP • Conf Containers with Confidential GPUs on Bare Metal - DP • Conf Containers on IBM-Z - GA • Conf Containers on ARO - GA	• Conf Containers with Confidential GPUs on Bare Metal - TP • Conf Containers with Confidential GPUs on Azure - TP/GA • Conf Containers on Bare Metal on Intel TDX and AMD SEV-SNP - GA	• Arm Support for confidential computing (planned) • Improved integration of CC features between RHEL, RHCOS and OCP • SVSM for RHCOS / OCP-Virt - Tech Preview
Attestation		• Red Hat Build of Trustee - GA • CPU, Kernel, boot, rootfs and bootstrap configuration attestation			

This roadmap is subject to change.

Confidential Cluster Roadmap on OpenShift

	Q2 2025	Q3 2025	Q4 2025	H1 2026	H2 2026
Confidential Clusters	• Conf Cluster on Azure on AMD SEV-SNP - GA without remote attestation • Conf Cluster on GCP on Intel TDX, AMD SEV-SNP - GA without remote attestation		• Conf Cluster on Azure on Intel TDX, AMD SEV-SNP - DP with remote attestation • Conf Cluster on GCP on Intel TDX, AMD SEV-SNP - DP with remote attestation • Conf Cluster with Confidential GPUs on Azure - DP	• Conf Cluster on Azure on Intel TDX, AMD SEV-SNP - TP with day 0 remote attestation • Conf Cluster on AWS on AMD SEV-SNP - GA without remote attestation • Conf Cluster on GCP on Intel TDX, AMD SEV-SNP - TP with day 0 remote attestation	• Conf Cluster on Azure on Intel TDX, AMD SEV-SNP - GA with day 0 remote attestation • Conf Cluster on GCP on Intel TDX, AMD SEV-SNP - GA with day 0 remote attestation • Conf Cluster with Confidential GPUs on Azure - GA
Attestation		• Red Hat Build of Trustee GA			

This roadmap is subject to change.

Confidential Virtual Machines Roadmap on OpenShift Virtualization

	H1 2025	H2 2025	H1 2026	H2 2026
Confidential VMs on OCP-V		• PoCs for RHEL CVM on OpenShift Virtualization with Trustee attestation • PoCs for Encrypted VMs on OpenShift Virtualization • Dev Preview for Encrypted VMs on OpenShift Virtualization • PoCs for firmware-based attestation with SVSM+VTPM with Keylime+Trustee		• Tech Preview for Encrypted VMs on OpenShift Virtualization • Dev Preview for attested VMs

Attestation

- In-guest Trustee Boot Attestation “Crawl” → In-guest Trustee Attestation “Walk”
- Firmware-based Keylime+Trustee Boot Attestation “Crawl”
- Keylime runtime Attestation “Crawl”

This roadmap is subject to change.

Key take-aways

- Confidential Computing helps to enable a zero trust architecture
- Red Had Confidential Computing solutions add another layer of protection to Red Hat's existing defense in depth capabilities
- Confidential Computing with attestation expands the options for using public cloud with confidence
- Confidential Computing is particularly important for protecting proprietary data in AI-enabled applications

Questions?

Red Hat Summit

Connect

Thank you

linkedin.com/company/red-hat

facebook.com/redhatinc

youtube.com/user/RedHatVideos

twitter.com/RedHat