Microsoft

# The role of confidential computing in a zero-trust architecture

Andy Kennedy

Sr. Cloud Solution Architect
Microsoft UK

in https://www.linkedin.com/in/packetdiscards/

packetdiscards

# Data protection

EXISTING ENCRYPTION

## Data at rest

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

## Data in transit

Encrypt data that is flowing between untrusted public or private networks

# Data protection life cycle

## Existing encryption

### Data at rest

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

### Data in transit

Encrypt data that is flowing between untrusted public or private networks

## Confidential computing

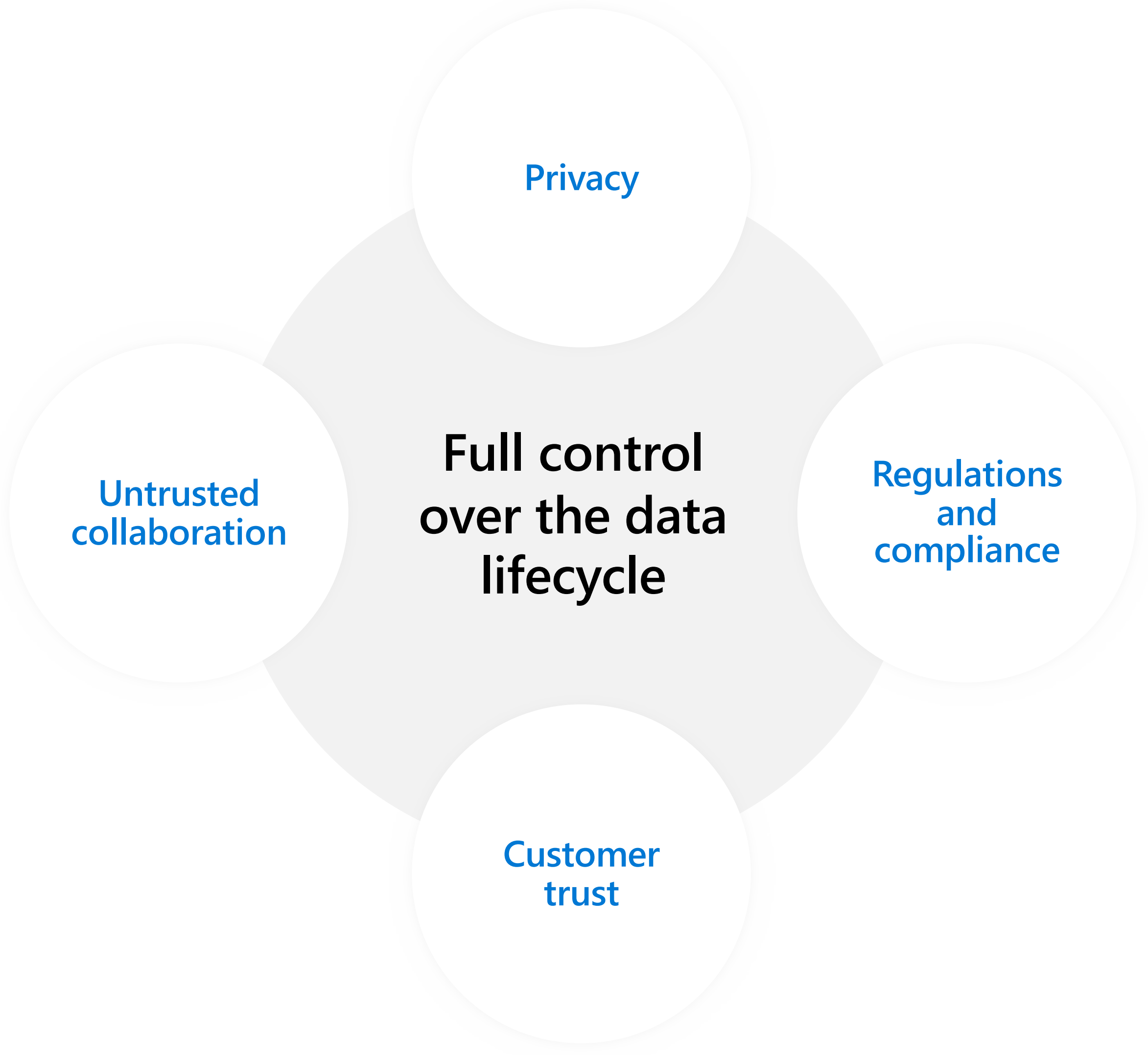
### Data in use

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

CONFIDENTIAL COMPUTING CONSORTIUM

# What is Confidential Computing?

***The protection of data in-use*** by performing computation in a hardware-based Trusted Execution Environment (TEE).



Full control over the data lifecycle

Privacy

Untrusted collaboration

Regulations and compliance

Customer trust

# Hardware root of trust

intel

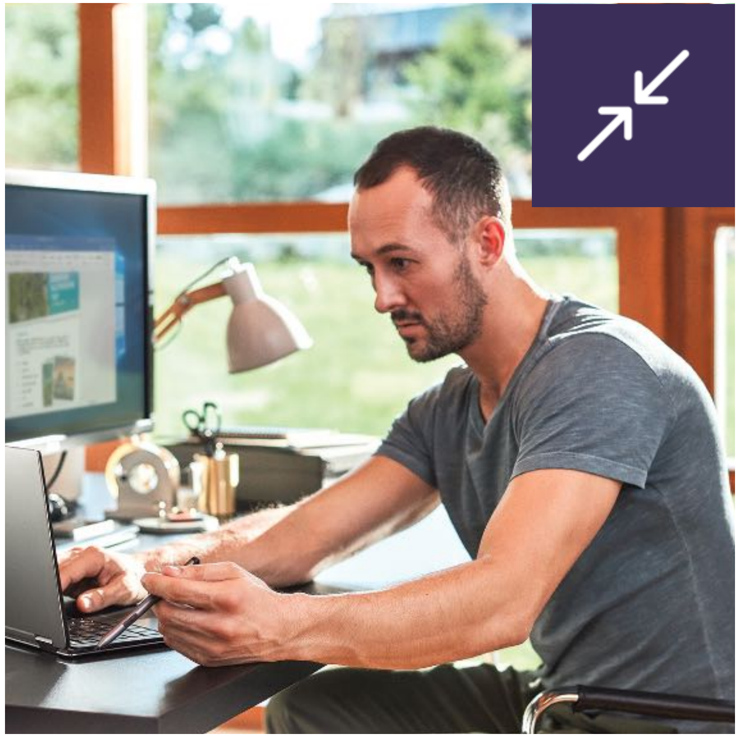
Intel-based DCsv3 confidential VMs
- Intel SGX hardware-protected application enclaves.
- Total Memory Encryption-Multi-Key (TME-MK) so that each VM can be secured with a unique hardware key.

AMD

AMD-based DCasv5/ECasv5 confidential VMs
- Secure Encrypted Virtualization-Secure Nested Paging (SEV-SNP) to provide hardware-isolated virtual machines

Nov 2021: Key foundations for protecting your data with Azure confidential computing

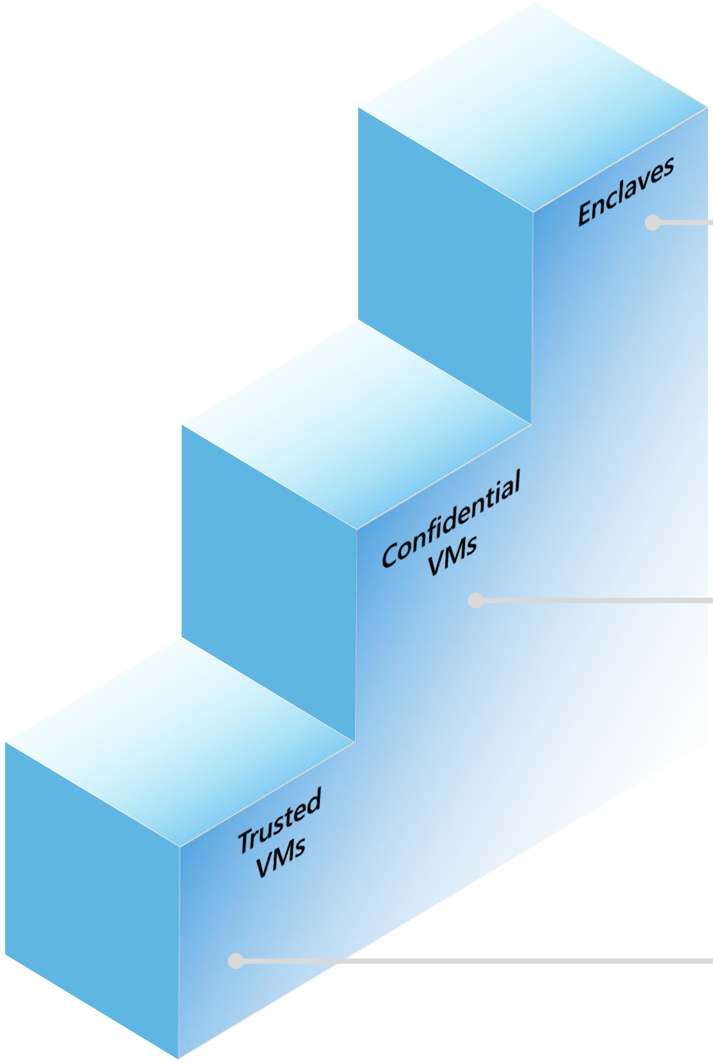
# Principles of a Zero Trust Architecture



Use least privilege access

Verify explicitly

Assume breach



Generally available

## Hardware enclaves with Intel SGX

*"I just trust my app code and the chip."*

Public preview

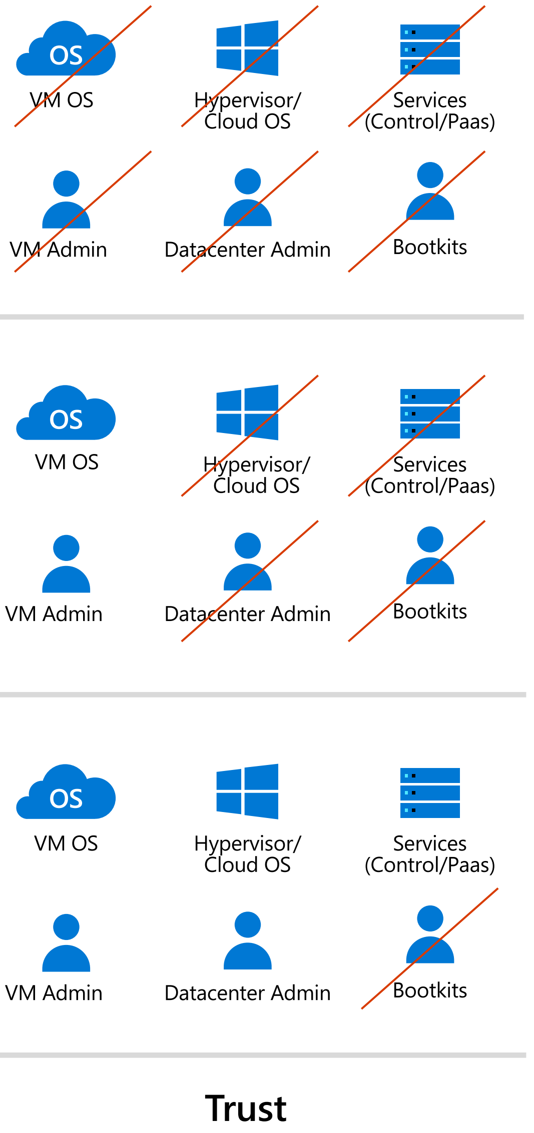
## Hardware confidential VMs with AMD Sev-SNP

*"Microsoft cannot touch my stuff in my VM."*

Public preview

## Trusted launch VMs

*"Only known, trusted code is running on my VM."*



# Confidential Computing Spectrum

**Added data security** | **Regulations & compliance** | **Untrusted collaboration** | **Auditable services**

← Ease of use ——— Security Control →

### “Easy button”

Existing apps, sometimes no app source

“I want CC, please turn it on in the cloud”

Minimal effort across the board (people, infra)

HW isolation; Don’t trust CSP. Guest OS and guest admin is trusted

### “Balanced”

Existing apps, open to minor changes

“I will do some work for CC”

HW Isolation; Don’t trust CSP, or Guest admin. Additional code is trusted

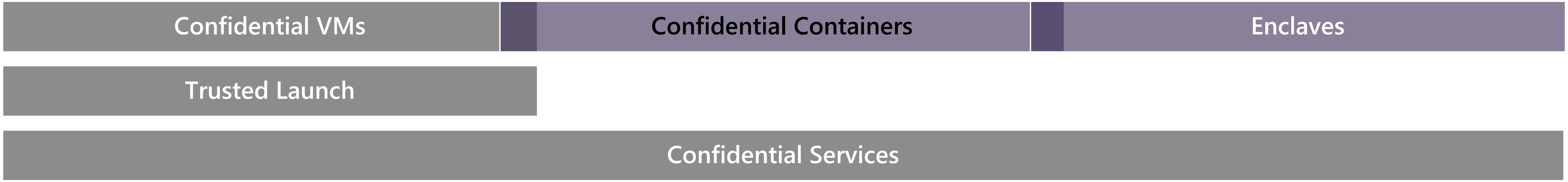
### “Most control”

Line of code control

Custom apps

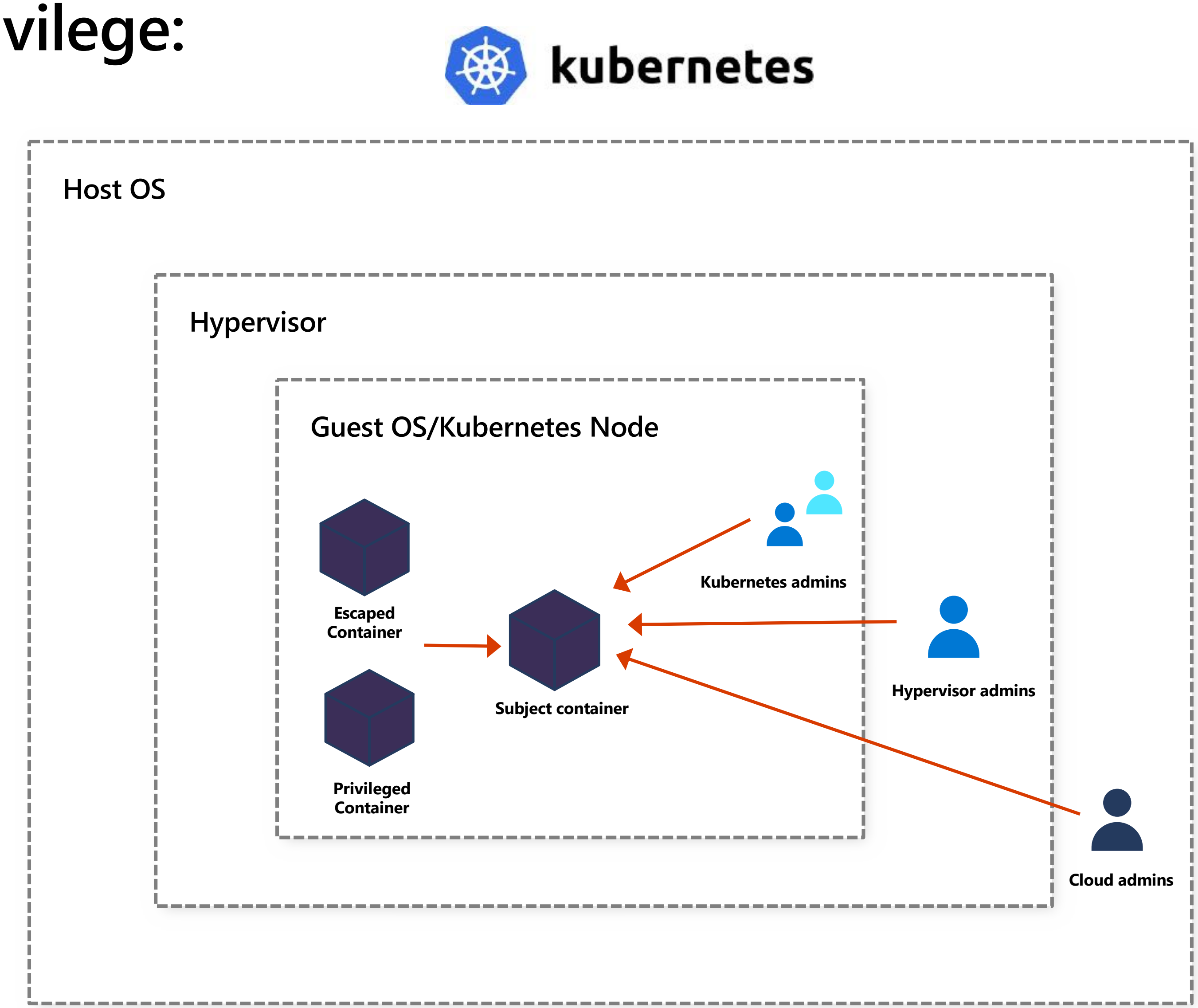
“I want control”

HW Isolation, Don’t trust CSP, VM admin, VM OS

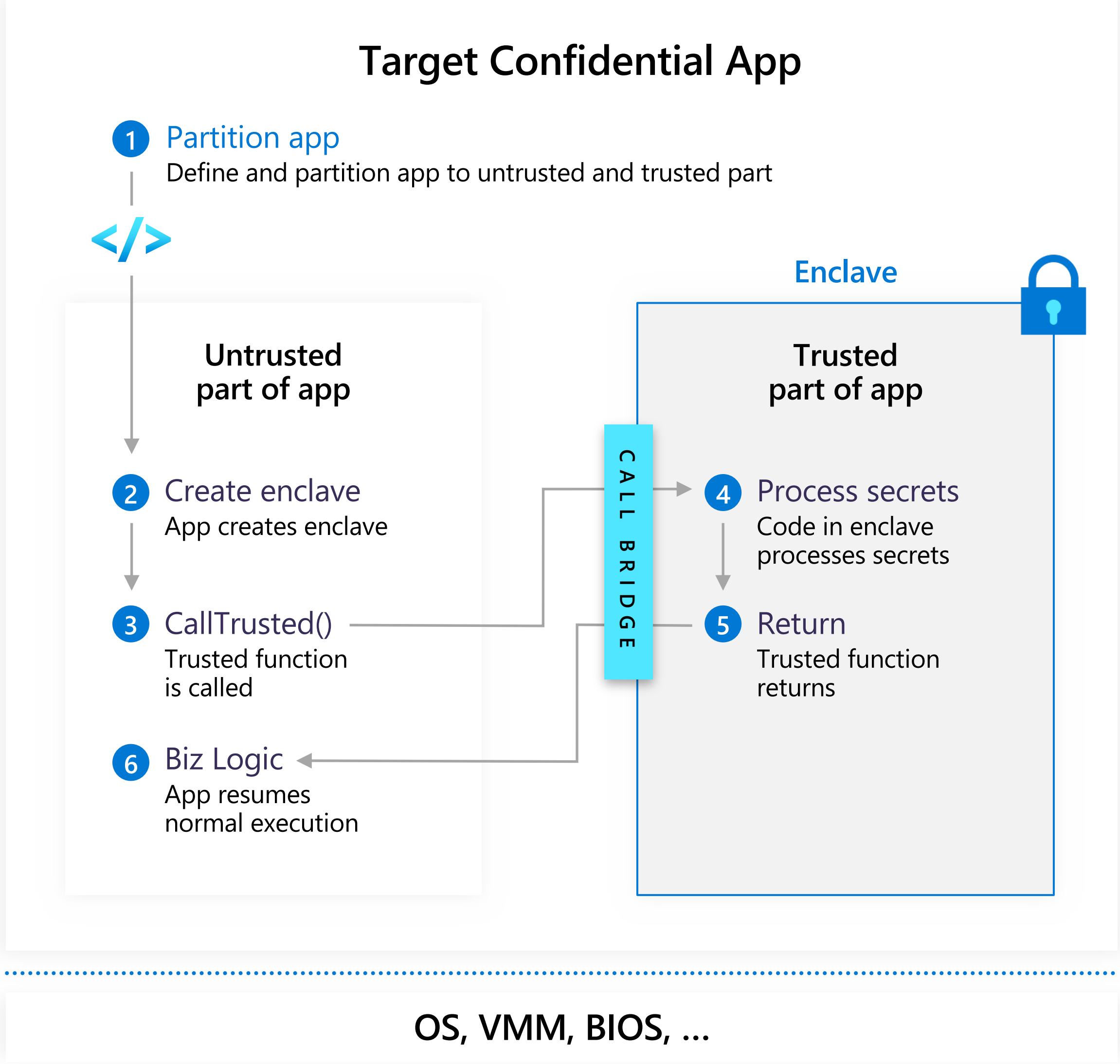


# Principle of least privilege:

## Possible in-memory attack surface area



# Principle of least privilege:



Target Confidential App

1 Partition app
Define and partition app to untrusted and trusted part

Untrusted part of app

2 Create enclave
App creates enclave

3 CallTrusted()
Trusted function is called

6 Biz Logic
App resumes normal execution

CALL BRIDGE

Enclave

Trusted part of app

4 Process secrets
Code in enclave processes secrets

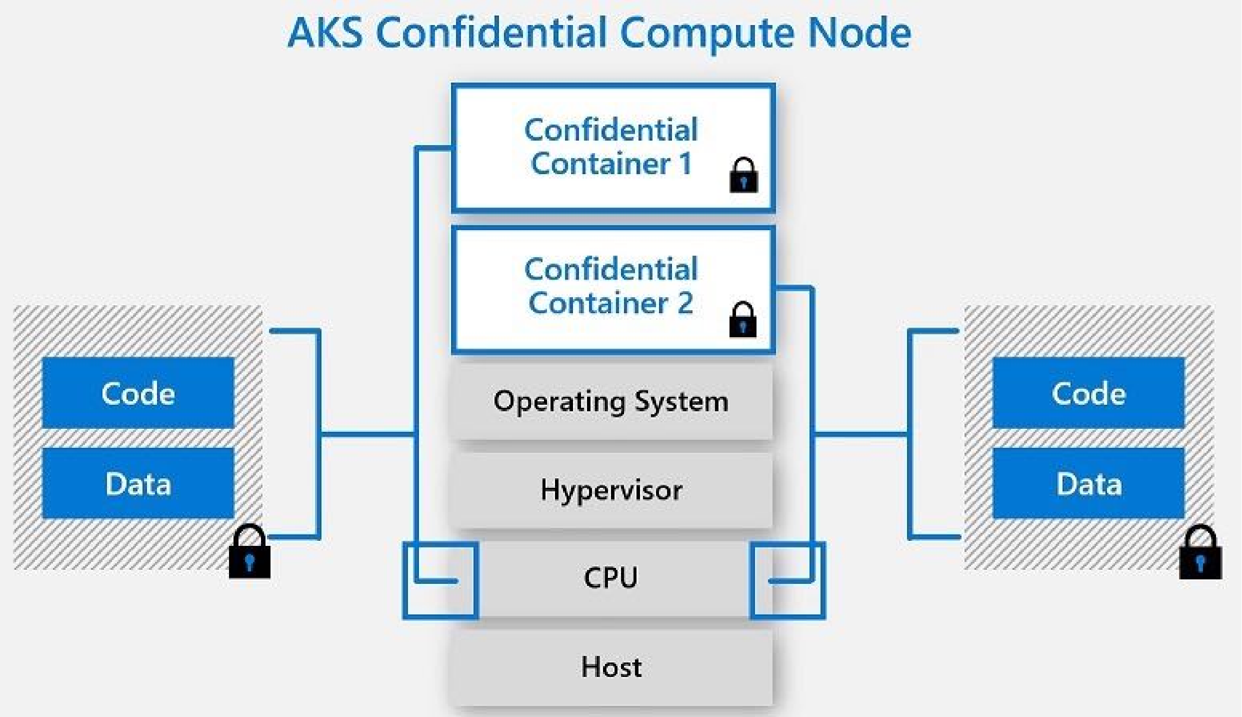
5 Return
Trusted function returns

OS, VMM, BIOS, …

# Principle of least privilege:
# Azure Kubernetes Service (AKS) Confidential Nodes

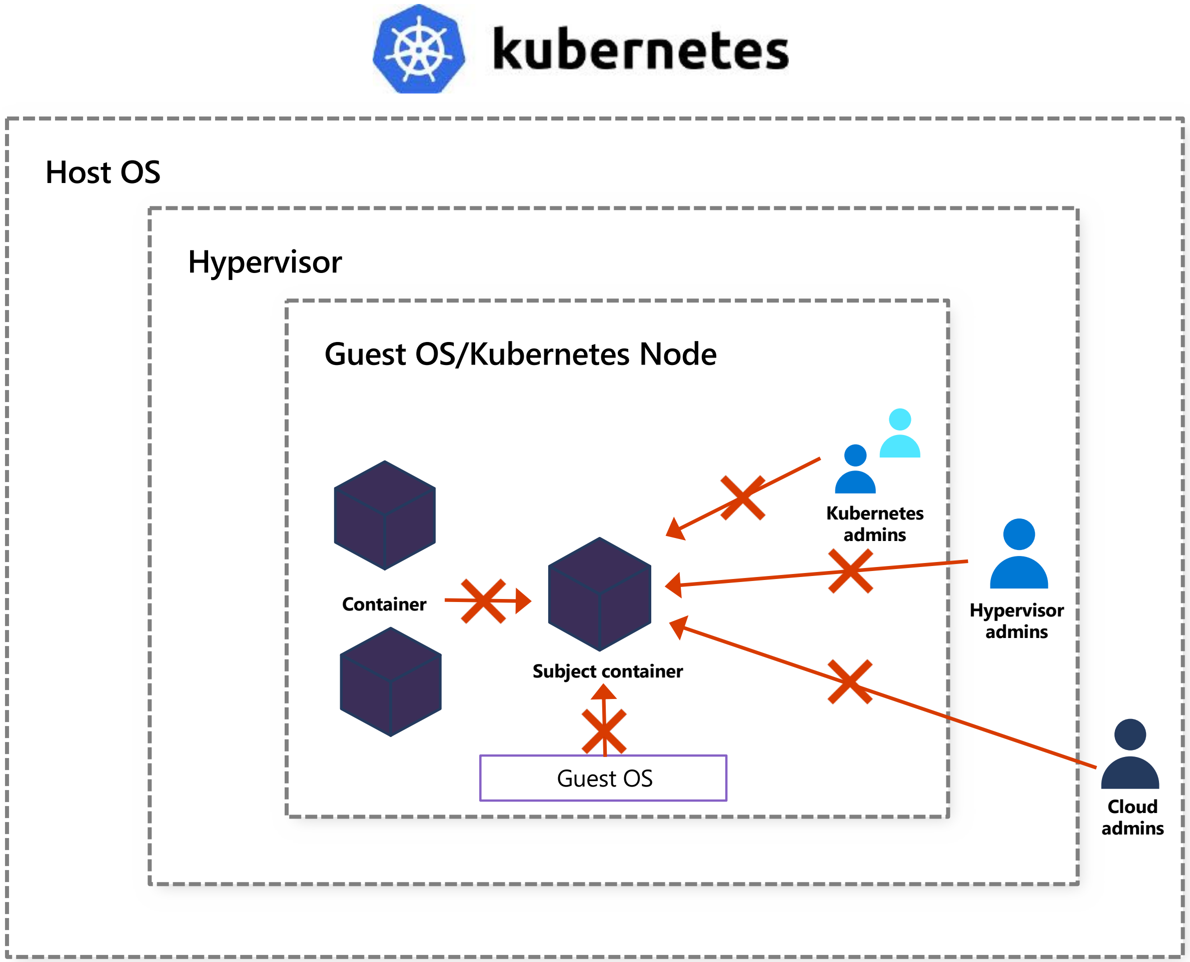
```
az aks create -g $RESGRPNAME \
       --name akcc-aks-cluster \
       --generate-ssh-keys \
       --enable-addons confcom
```

```
az aks nodepool add --cluster-name \
akcc-aks-cluster \
       --name confcompool1 \
       --resource-group $RESGRPNAME \
       --node-vm-size Standard_DC2s_v2 \
       --node-count 1
```



# Principle of least privilege:

With confidential computing



Intel SGX Enclave container protection

# Verify Explicitly
# Attestation use cases

## Customer requirements

Is the enclave genuine?

Is the enclave conforming to the latest security standards?

Is the code running in the enclave signed?

A need for “Enclave attestation”?

## Challenges

How to support for multiple enclave technologies?

Can customers define what is trusted?

Can common validation logic be used for multiple relying parties?

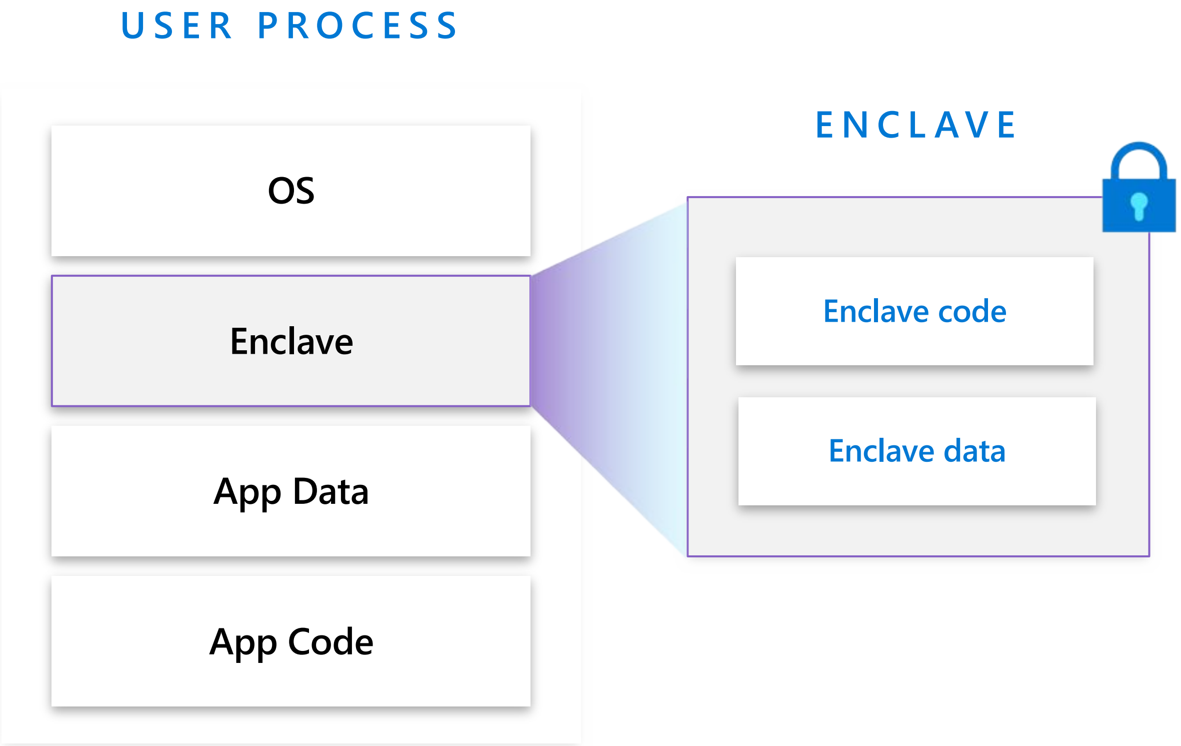
How can keys be securely transmitted to enclaves?

How to reduce trust in cloud provider performing attestation?

# Verify Explicitly
# Attestation

## Attestation

- Process by which one enclave attests its Trusted Computing Base (TCB) to another entity outside of the platform
- Provider generates a cryptographic summary of build activities (code, data, stack, heap, location of pages, security flags)
- Verifier must:
    - Info should be fresh, and source validated
    - Securely obtain enclave's TCB
    - Securely obtain the expected enclave's TCB
    - Compare and verify the two values

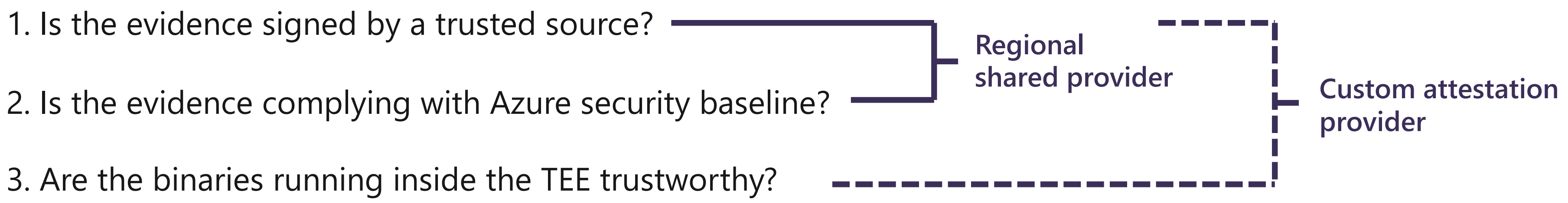


# Verify Explicitly
# Microsoft Azure Attestation

Azure Attestation is a customer-facing service and a framework for attesting Trusted Execution Environments (TEEs) like SGX enclaves, VBS enclaves, Trusted Launch and Confidential VMs. Attestation is a process of demonstrating that software binaries were properly instantiated on a trusted platform.

**Azure Attestation is now Generally Available**

**Validations performed in SGX attestation**



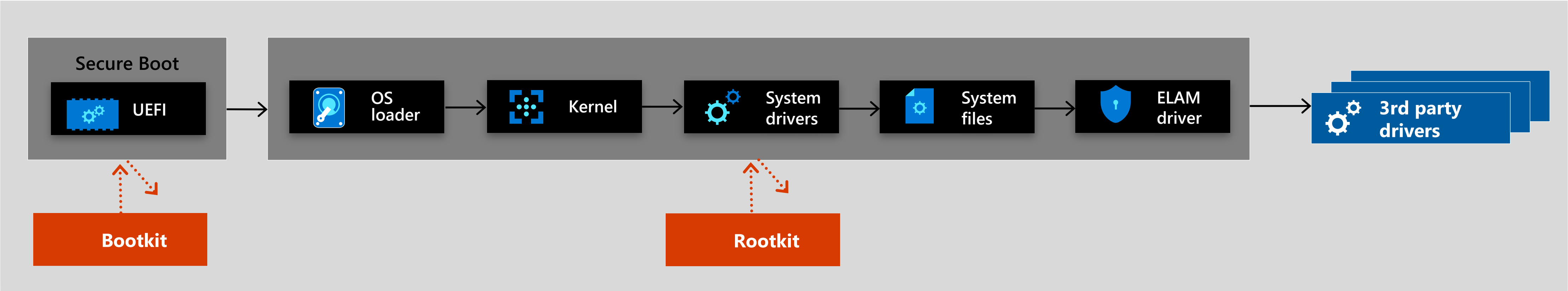
1. Is the evidence signed by a trusted source?
2. Is the evidence complying with Azure security baseline?
3. Are the binaries running inside the TEE trustworthy?

# Assume Breach
# Trusted Launch

Secure boot

Virtual Trusted Platform Module (vTPM)

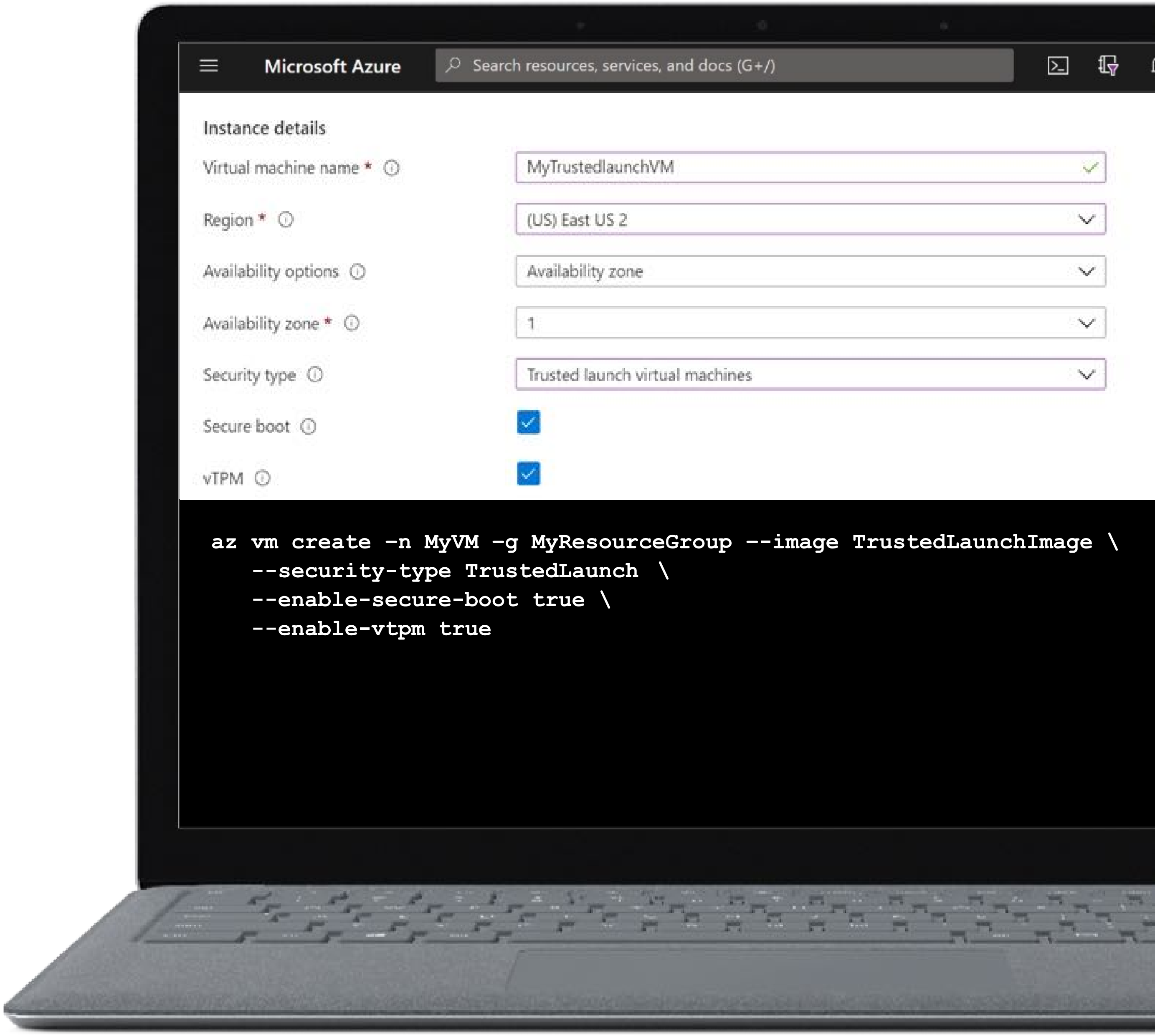
Integrity monitoring with Remote Attestation



# Assume Breach
# Trusted Launch

## GA ~ Now

- All major public regions
- On Gen2 VMs only
- Portal, ARM template, PowerShell, CLI, SDK
- Ubuntu, Redhat, SUSE, Windows Server, Windows 10, Windows 11



Instance details

| | |
|---|---|
| Virtual machine name * | MyTrustedlaunchVM |
| Region * | (US) East US 2 |
| Availability options | Availability zone |
| Availability zone * | 1 |
| Security type | Trusted launch virtual machines |
| Secure boot | ☑ |
| vTPM | ☑ |

```
az vm create -n MyVM -g MyResourceGroup --image TrustedLaunchImage \
   --security-type TrustedLaunch  \
   --enable-secure-boot true \
   --enable-vtpm true
```

# Confidential computing @ Azure

| | | | | | |
|---|---|---|---|---|---|
| Developer tools | ML (ONNX RT)<br>OSS | CCF SDK<br>OSS | Open enclave SDK<br>OSS | Mystikos LibOS<br>OSS | |
| Azure Confidential Services | SQL Azure<br>GA | Azure Key Vault M-HSM<br>GA | Microsoft Azure Attestation<br>GA | Azure Kubernetes Service (AKS)<br>GA: DC2 nodes | Azure Confidential Ledger<br>Preview |
| Virtual machines and edge | DCsv2 SGX VMs<br>GA | DCsv3/DCdsv3 SGX VMs<br>Preview | ECa/DCa SEV-SNP VMs<br>Preview | Trusted Launch VMs<br>GA | IoT Edge Device<br>GA |
| Innovative new hardware | intel<br>GA | AMD<br>Preview | TrustZone System Security by ARM<br>GA | | |
| Industry leadership and standardization | CONFIDENTIAL COMPUTING CONSORTIUM<br>Co-founded | Microsoft Research<br>Stewardship | | | |

Azure confidential computing offerings cover not just VMs, but also Azure PaaS/SaaS services.
Choose a 'most-secure' route with control over every line of code, or an 'easy button' route to lift-n-shift existing apps to be confidential.

Microsoft

Azure Confidential Computing