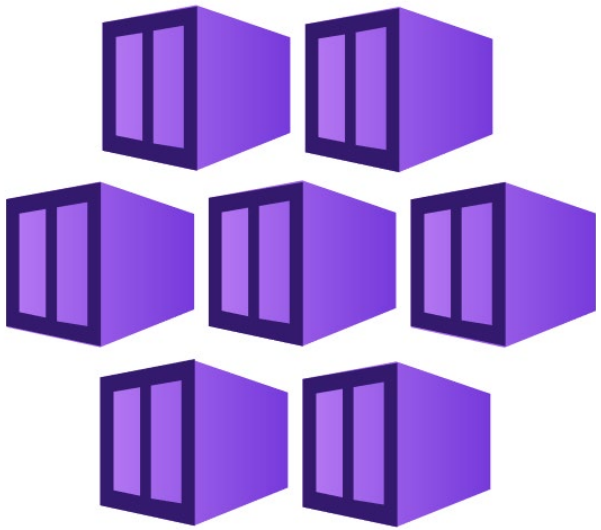


AKS Office Hours

Topic: AKS On-Premises

June 2nd, 2022 @11am CST

Microsoft Azure

AKS Public Office Hours

Alice Gibbons
Dave Strebel
Ray Kao

Cloud Native/Digital App
Innovation Global Black Belt Team

CLOUD NATIVE GBB

Who are we?

Azure ❤

TM

Why AKS Office Hours?

- https://github.com/Azure/aks-gbb-officehours

- Provide AKS customers with updates pertaining to AKS and the Cloud Native Ecosystem
- Host a short talk and/or demo on Cloud Native technologies related to Kubernetes and AKS
- Collect feedback from customers on issues, blockers, use cases, and questions related to AKS

What to expect

- Call agenda
- 5-10 minutes: Welcome, followed by AKS and ecosystem updates
- 20-30 minutes: AKS-OnPrem Deep Dive with Sarah Cooley 
- 10-20 minutes: “Ask us anything” and customer feedback discussion

Keep in mind

- We want two-way interaction, but please stay on mute when you are not speaking
- This call and how it is conducted will evolve based on feedback and growth
- Recordings and content will be available post-call, barring any technical difficulties (See our office hours github link for details -> https://github.com/Azure/aks-gbb-officehours)

Microsoft Azure

AKS Updates

- github.com/azure/aks/projects/1
- github.com/azure/aks/releases

CLOUD NATIVE GBB

AKS Updates

https://github.com/Azure/AKS/releases/tag/2022-05-22

Announcements

- From Kubernetes 1.23, containerd will be the default container runtime for Windows node pools. Docker support will be deprecated in Kubernetes 1.24. You are advised to test your workloads before Docker deprecation happens by following the documentation here.
- Starting with 1.24 the default format of clusterUser credential for AAD enabled clusters will be 'exec', which requires kubelogin binary in the execution PATH. If you are using Azure CLI, it will prompt users to download kubelogin. There will be no behavior change for non-AAD clusters, or AAD clusters whose version is older than 1.24. Existing downloaded kubeconfig will still work. We provide an optional query parameter 'format' when getting clusterUser credential to overwrite the default behavior change, you can explicitly specify format to 'azure' to get old format kubeconfig.
- Konnectivity rollout will continue in May 2022 and is expected to complete by end of May.
- Update your AKS labels to the recommended substitutions before deprecation after the Kubernetes v1.24 release. See more information on label deprecations and how to update your labels in the Use labels in an AKS cluster documentation.

Release Notes

- https://github.com/Azure/AKS/releases/tag/2022-05-22
- Preview features
  - ARM64 agent pools is now in public preview.
  - Azure Disk CSI driver v2 is now in private preview.
  - Draft extension for Azure Kubernetes Service (AKS) is now in public preview.
  - KEDA add-on is now in public preview.
  - Web application routing add-on is now in public preview.
  - Windows Server 2022 host support is now in public preview.
- Bug fixes
  - BYOCNI nodes will no longer be provisioned with additional secondary IPs
  - Calls to admission webhooks in Konnectivity clusters will properly use the Konnectivity tunnel to reach the webhook URL
- Component Updates
  - Azure Disk CSI driver has been updated to v1.18.0
  - AKS Ubuntu 18.04 image updated to AKSUbuntu-1804-2022.05.10.
  - AKS Windows 2019 image has been updated to 17763.2928.220511.
  - AKS Windows 2022 image has been added with version 20348.707.220511.
  - Cloud controller manager has been updated to versions v1.23.12/v1.1.15/v1.0.19 (see the version matrix to see which CCM version maps to which AKS version)
  - CoreDNS has been updated to v1.8.7 for AKS clusters >=1.20.0. Clusters before 1.20.0 remain on 1.6.6.
  - external-dns has been updated to v0.10.2

Microsoft Azure

AKS On-Prem Deep Dive with Sarah Cooley

CLOUD NATIVE GBB

Agenda

- AKS on prem value prop
- What's next? – it's good

For IT Administrators,

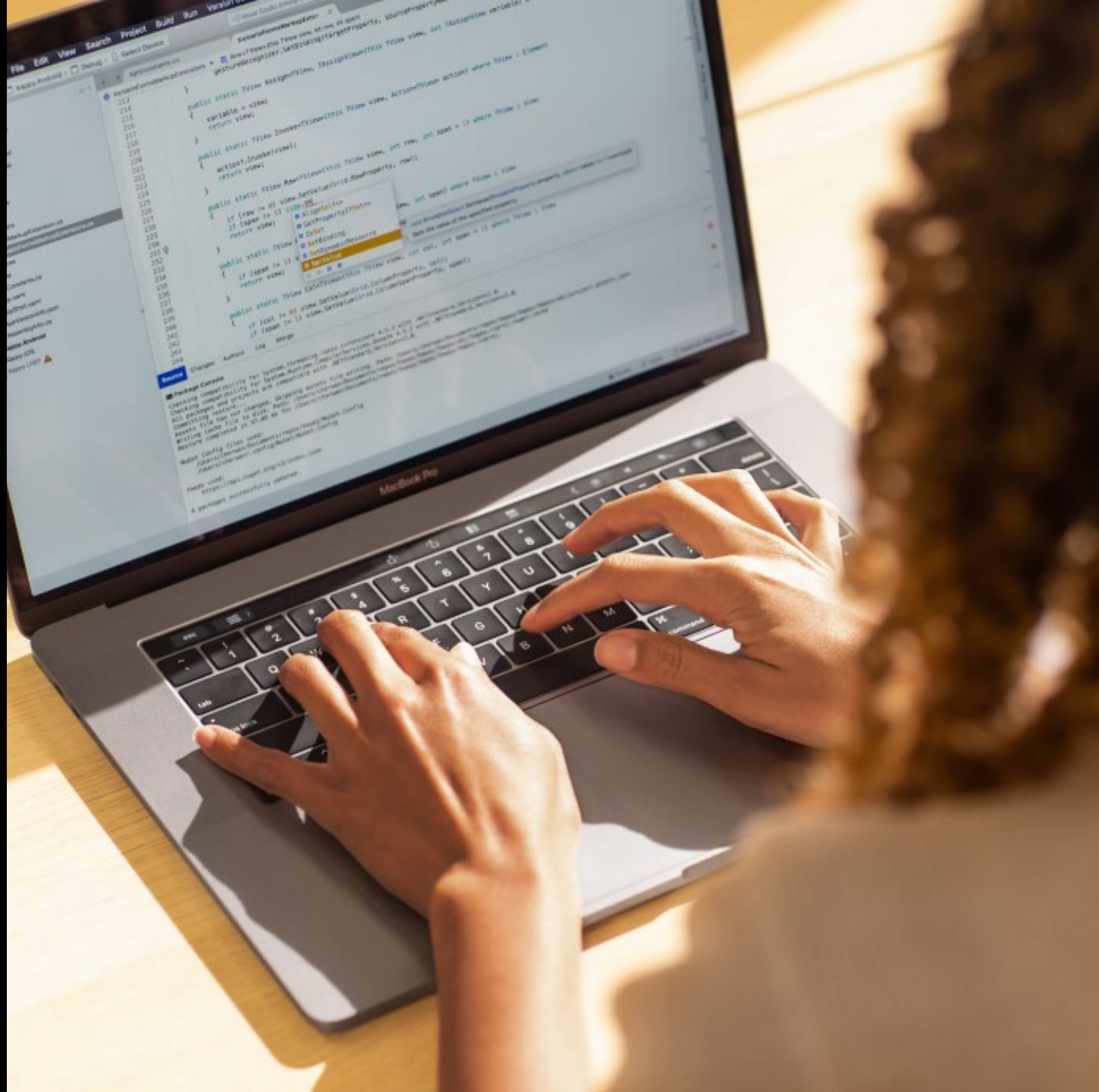
AKS provides a simple & secure Kubernetes experience on-premises with end-to-end support.

For developers,

AKS provides a consistent developer experience with familiar tooling from Azure cloud to edge

Hybrid cloud model

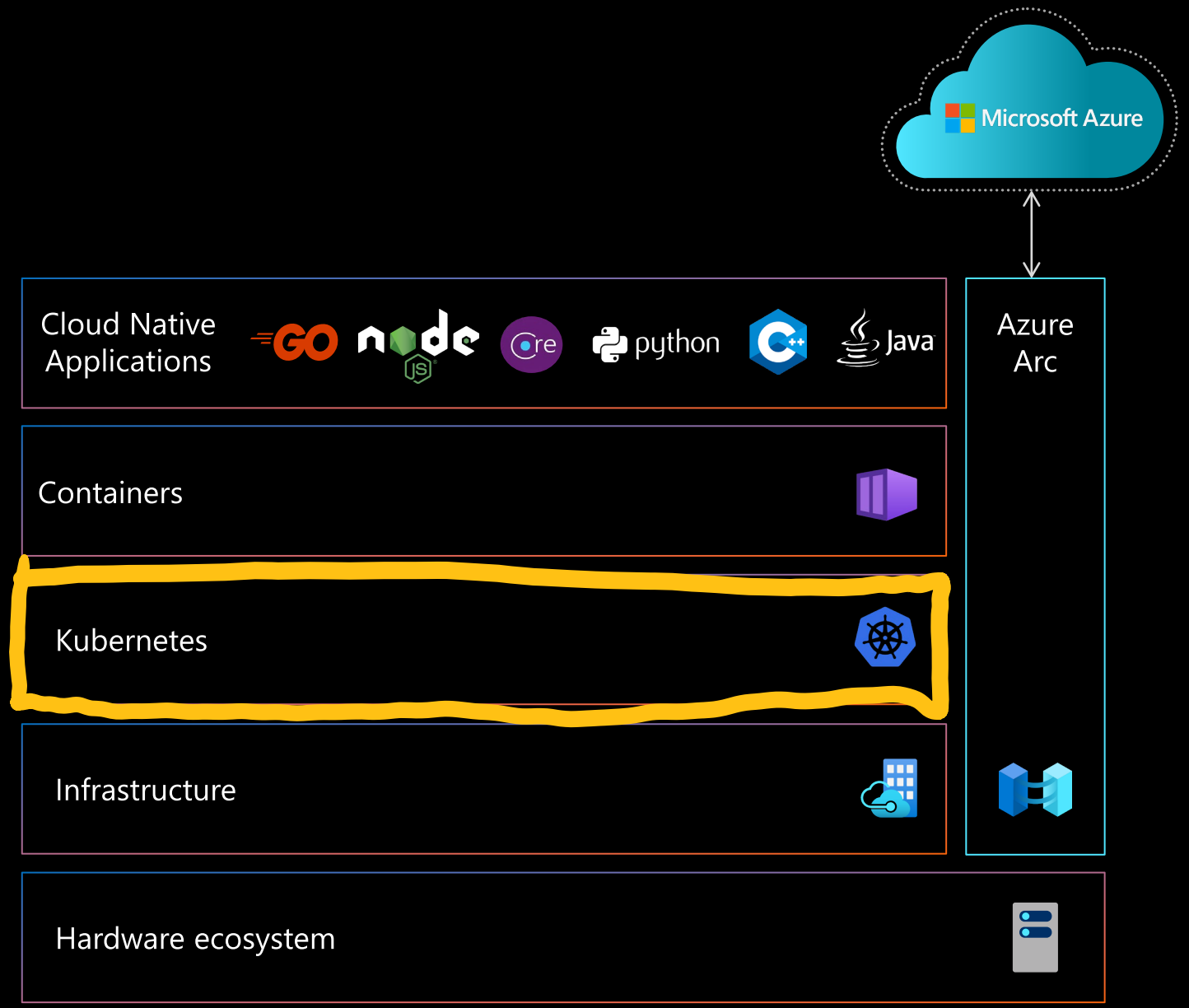
Focused on Kubernetes…



DIY Kubernetes

DIY Kubernetes is complicated…

- Many configurations for IT to choose:
  - Container runtime
  - Networking Interface (CNI)
  - Secret storage (CSI)
  - Cluster API
  - Web UI/Dashboard
  - Load balancer
  - Monitoring, Logging
  - Backup
  - Container registry
- Many components to add for multi-node physical clusters:
  - High availability
  - SDN/network load balancing
- Process for updating components can be challenging



Full Microsoft Stack

Single provider support end to end.

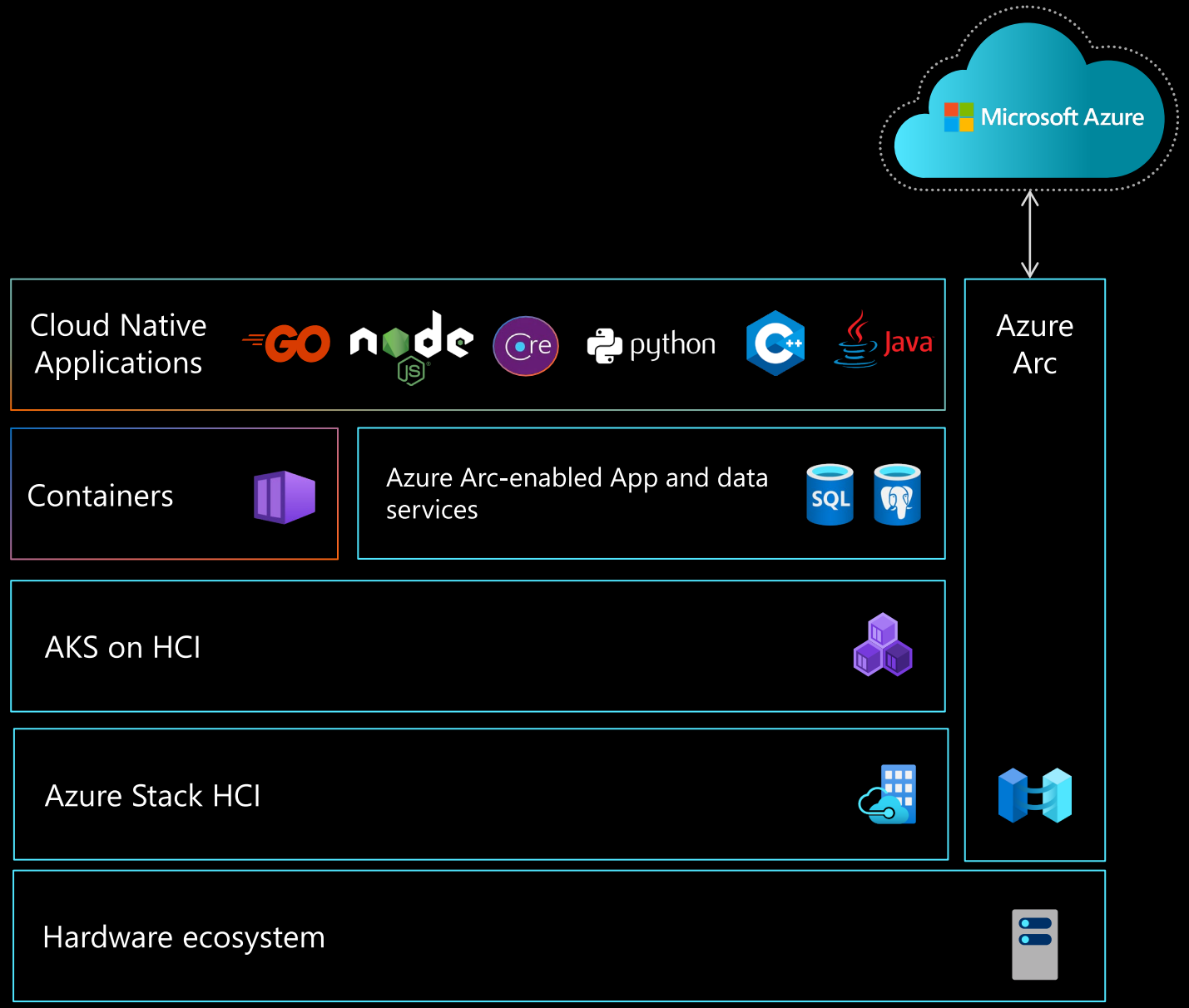
Best in class support for Windows Containers.

Secure and easy to update.

Application and data platforms for developer consistency

We still have flexibility and can leverage the OSS ecosystem

Azure Arc integrated OSS components



Full Microsoft Stack

Single provider support end to end.

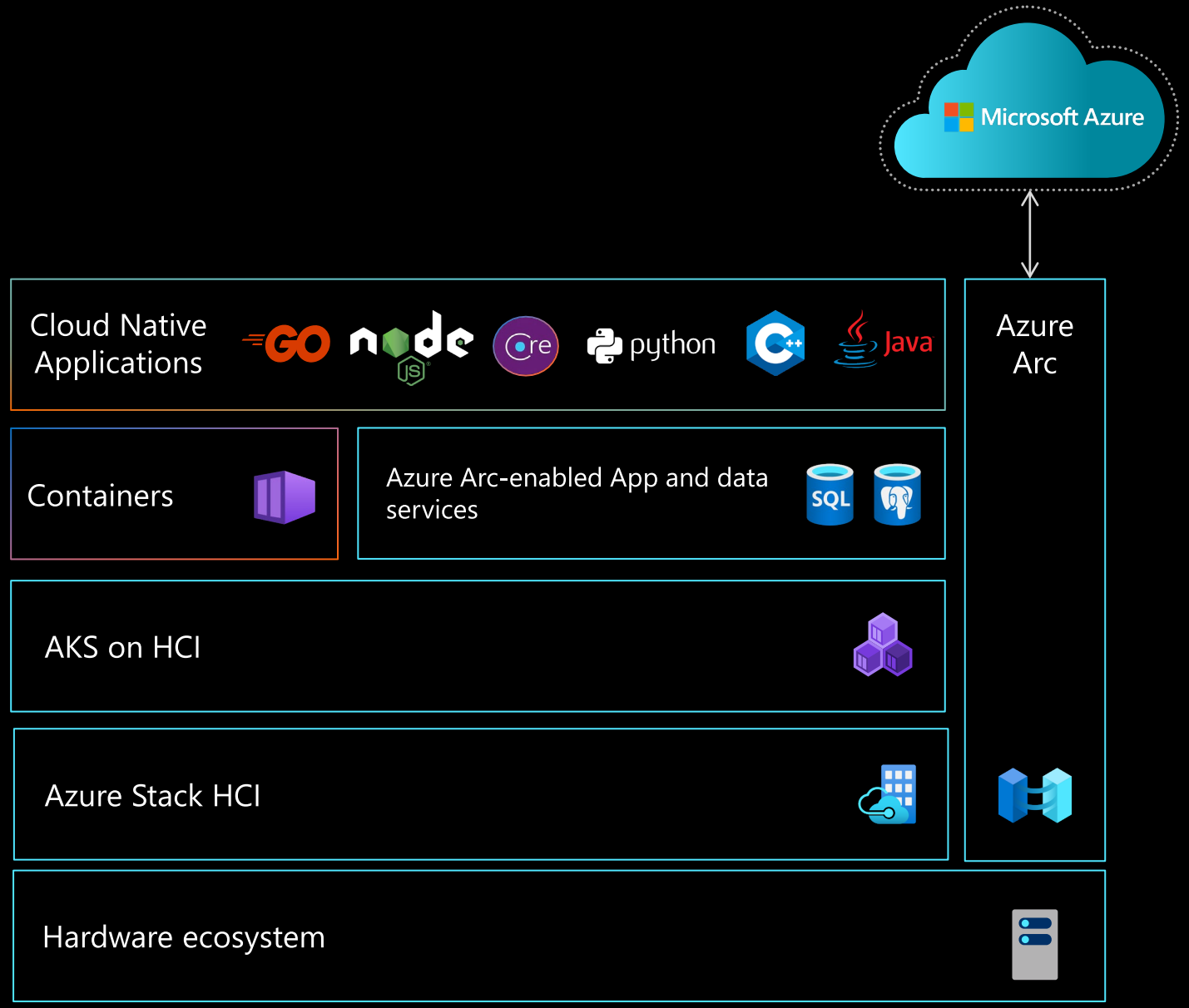
Best in class support for Windows Containers.

Secure and easy to update.

Application and data platforms for developer consistency

We still have flexibility and can leverage the OSS ecosystem

Azure Arc integrated OSS components



Full Microsoft Stack

Single provider support end to end.

Hundreds of validated combinations for hardware -> OS -> infra -> cloud

Application and data platforms for developer consistency

We still have flexibility and can leverage the OSS ecosystem

Azure Arc integrated OSS components

Microsoft Enhanced Stack with AKS on Prem

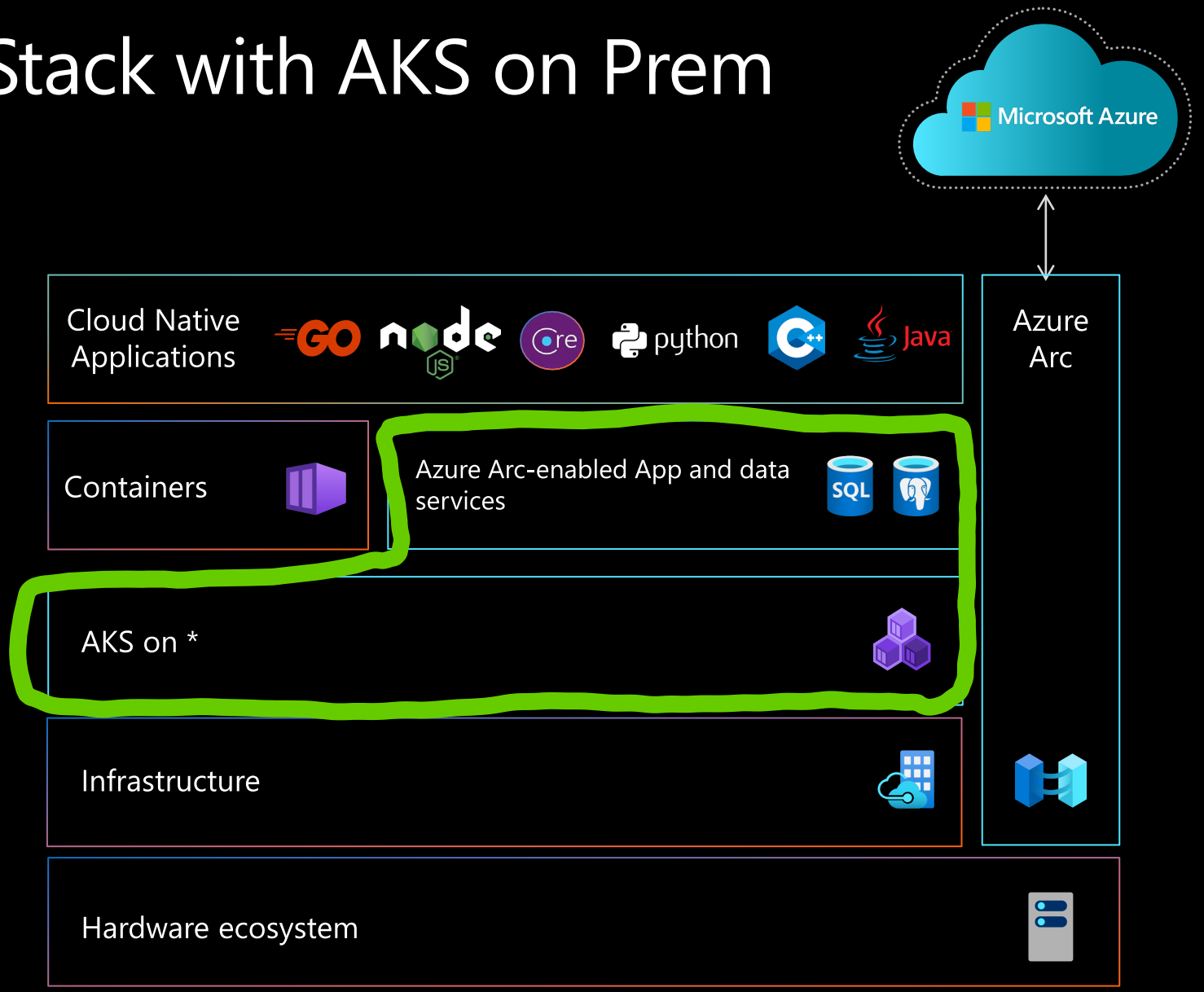
Smart defaults for Kubernetes infra that work well with AKS and Arc:

- Kubernetes version matching with AKS
- Container runtime – containerd
- Secure Windows and Linux base images
- CNI – Calico
- Load balancer – HA Proxy
- Identity management – AD/k8s
- Secret storage – CSI + AKV
- Monitoring – Prometheus, Grafana, Azure

AKS on prem service handles update for management cluster, control plane, and easy controls for target clusters.

Regular validation with Azure Arc + Arc extensions.

Continued ability to leverage the OSS ecosystem.



Microsoft Enhanced Stack with AKS on Prem

Smart defaults for Kubernetes infra that work well with AKS and Arc:

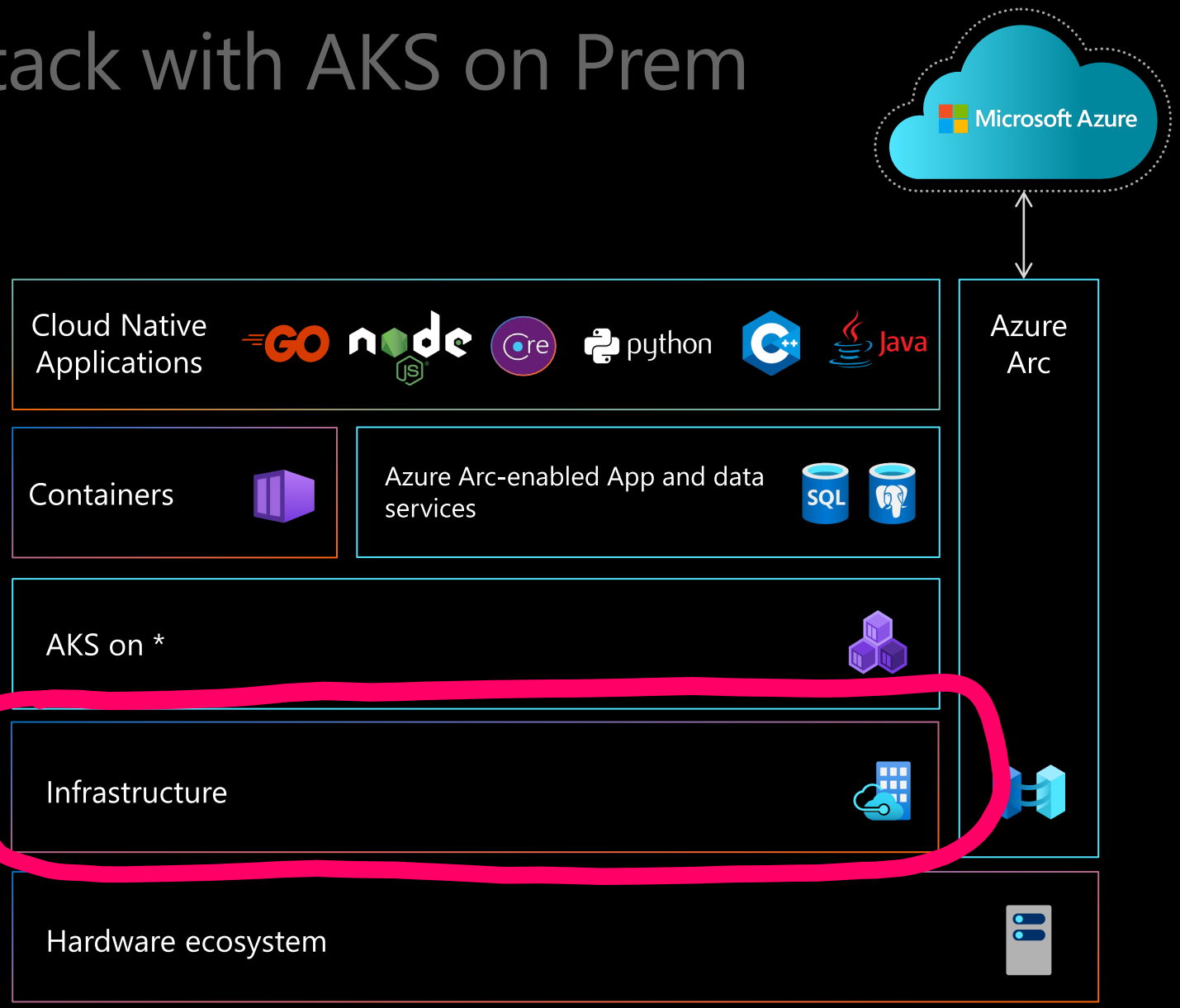
- Container runtime – containerd
- Secure Windows and Linux base images
- CNI – Calico
- Load balancer – HA Proxy
- Identity management – AD/k8s
- Secret storage – CSI

AKS on prem service handles update for management and control plane.

Regular validation with Azure Arc + Arc extensions.

Continued ability to leverage from the OSS ecosystem.

Let's talk Infra...



AKS *(is available)* on

Azure Stack HCI

Windows Server

Azure Stack Edge preview

Azure Stack Hub preview

Windows IoT preview

AKS *(is available)* on

Azure Stack HCI

Windows Server

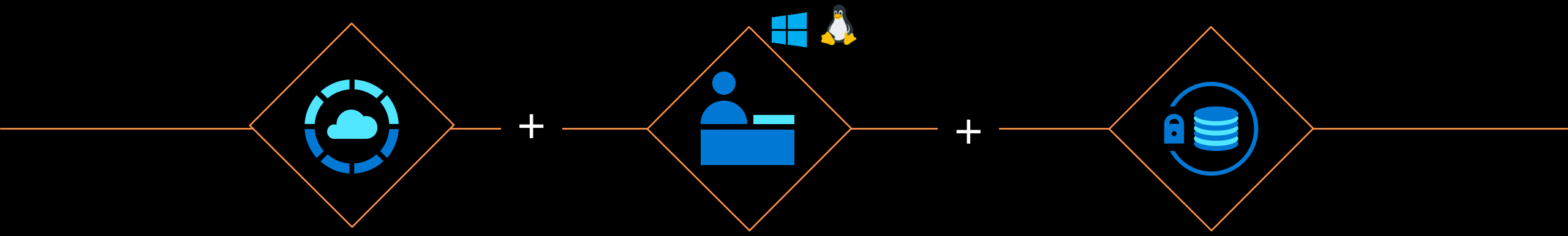
+ Single Node

Azure Stack Edge preview

Azure Stack Hub preview

Windows IoT preview

AKS on Azure Stack HCI and Windows Server



Azure hybrid by design

AKS-consistent Kubernetes cluster management

Easy AKS deployment on Azure Stack HCI or Windows Server

Built-in Azure Arc capability

Best platform for .NET apps on-premises

Support for both Linux and Windows applications

Differentiated container solution for Windows

Local administration with Windows Admin Center and PowerShell

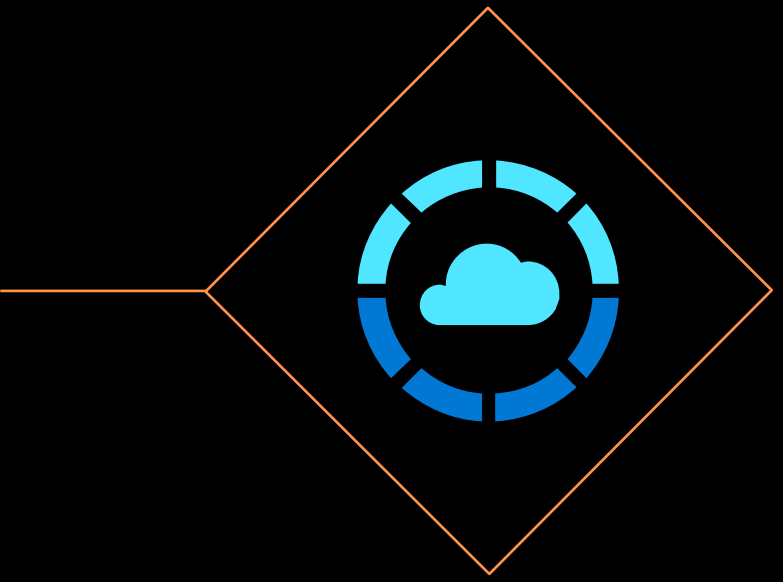
Built-in security

Secure and trusted platform

Single and consistent identity

Always up-to-date like Azure

Azure hybrid by design



AKS-consistent Kubernetes cluster management

- Centrally managed from Azure Portal
- Fleet management for Kubernetes platform and containers

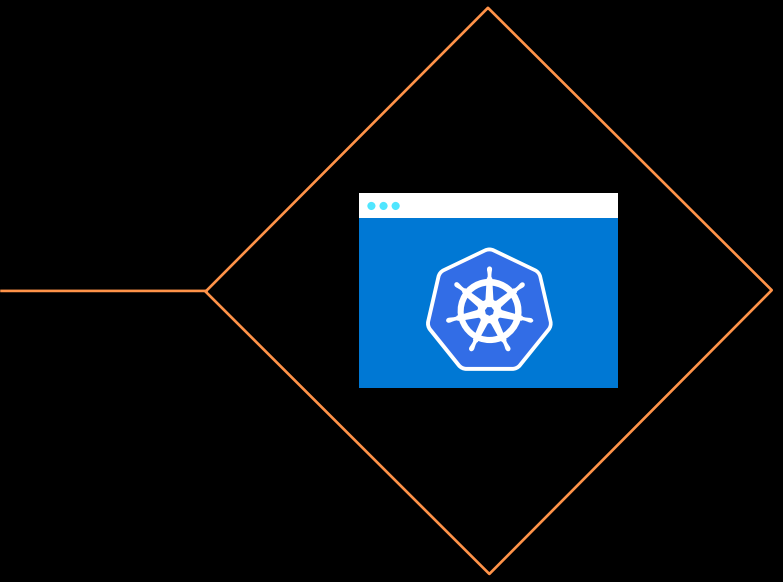
Easy AKS deployment on Azure Stack HCI or Windows Server

- “Single”-step installation and update of a fully-conformant Kubernetes cluster
- Built-in logging, monitoring, load-balancing, and certificate management

Built-in Azure Arc capability

- Easily bring Azure services on-premises with Azure Arc
- Consistent identity and security

Best platform for .NET apps on-premises



Built-in support for both Linux and Windows

- All-inclusive and fully-supported infra-ready to run Windows and Linux containers out-of-the-box
- Single vendor support leading to faster turnaround on support and fixes

Differentiated container solution for Windows

- Domain credentials in containers with gMSA v2
- AD and Azure AD integration

Local administration with Windows Admin Center

- Windows Admin Center and PowerShell for the Windows experts
- Integrated Windows app migration tooling

Built-in security

Secure and trusted platform

- Secure endpoints and Kubernetes clusters with Azure Active Directory, Azure Security Center, and Azure Sentinel
- Runtime protection to defend the K8s platform from attacks and vulnerabilities

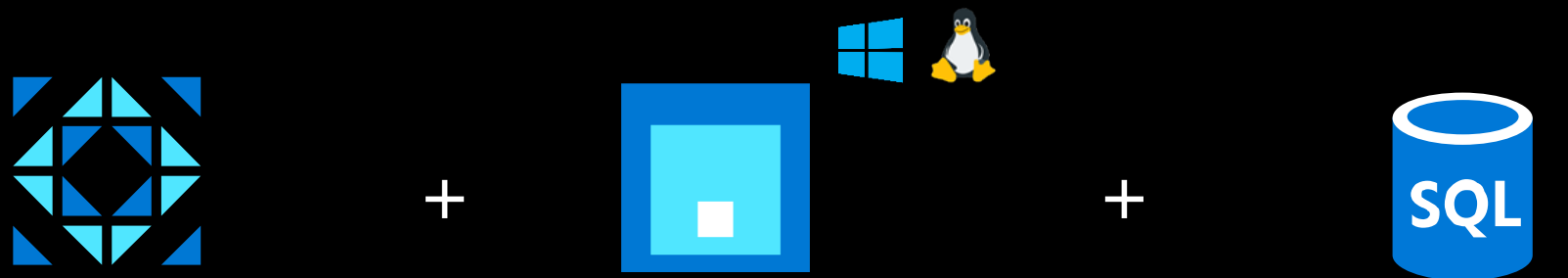
Single and consistent identity

- Security updates for all components, including OSS
- Certificate Authority for secure intra-cluster communication

Always up-to-date like Azure

- Regular and consistent feature and security updates
  Unified Azure billing
- Leverage existing Azure support plan

Run Kubernetes on Azure Stack HCI or Windows Server and easily connect to Azure services



AKS applications on Azure Stack HCI or Windows Server

Develop in AKS but
deploy unmodified to the edge

Modernize Windows and Linux apps

.Net framework and
core apps being containerized

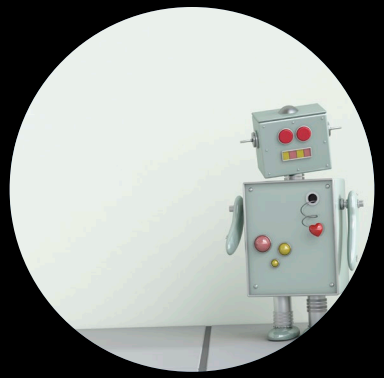
Data Services on Azure Stack HCI

Run Azure Arc for Data
Services on a resilient platform

What's next?

More Arc alignment

More reference architectures and prescriptive guidance



Focus on low-cost hardware

Integrate with existing on prem infrastructure

Continue shipping high quality monthly updates ☺

Call to Action

Get Started:

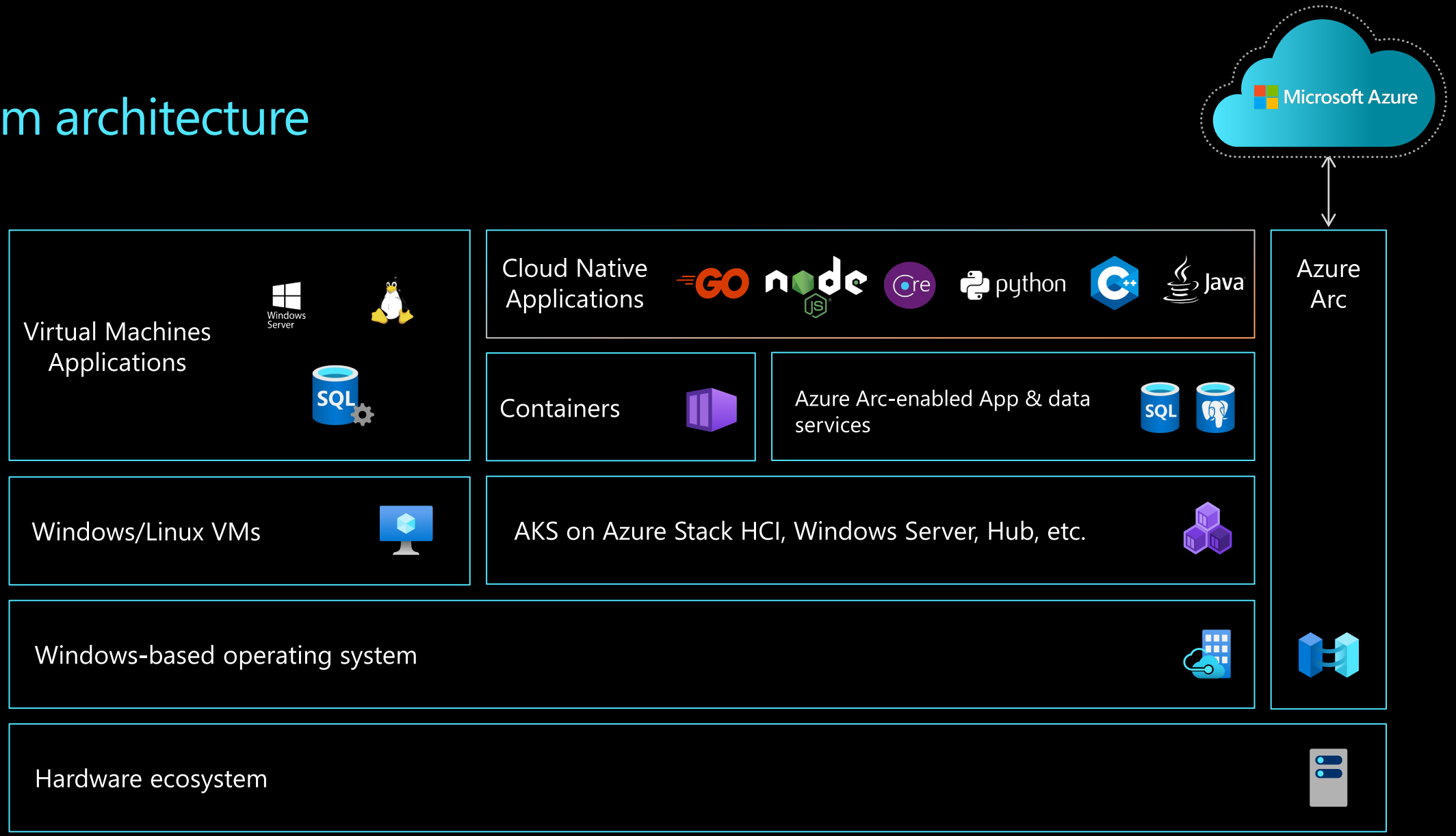
AKS on prem GitHub project + eval guide

AKS on prem documentation

https://aka.ms/ArcAksHciPriPreview

Thank You!

Platform architecture



Demo: Azure Policy with AKS

Abhilasha Agarwala

https://youtu.be/XZ_zk2yUcTI

Demo: Servicing

https://youtu.be/XaAAUjz_j2Y