



Build AI enabled devices in semi-connected scenarios

Marco Dal Pino

Technical Consultant



Platinum Sponsor



Gold Sponsor



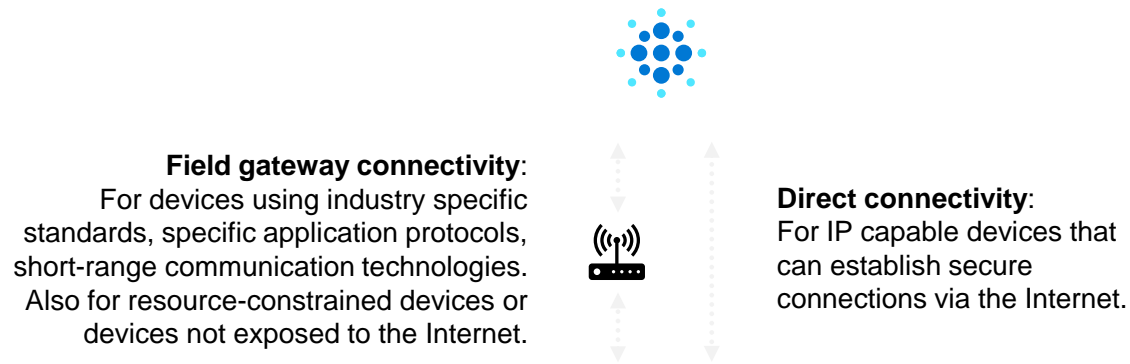
Technical Sponsor





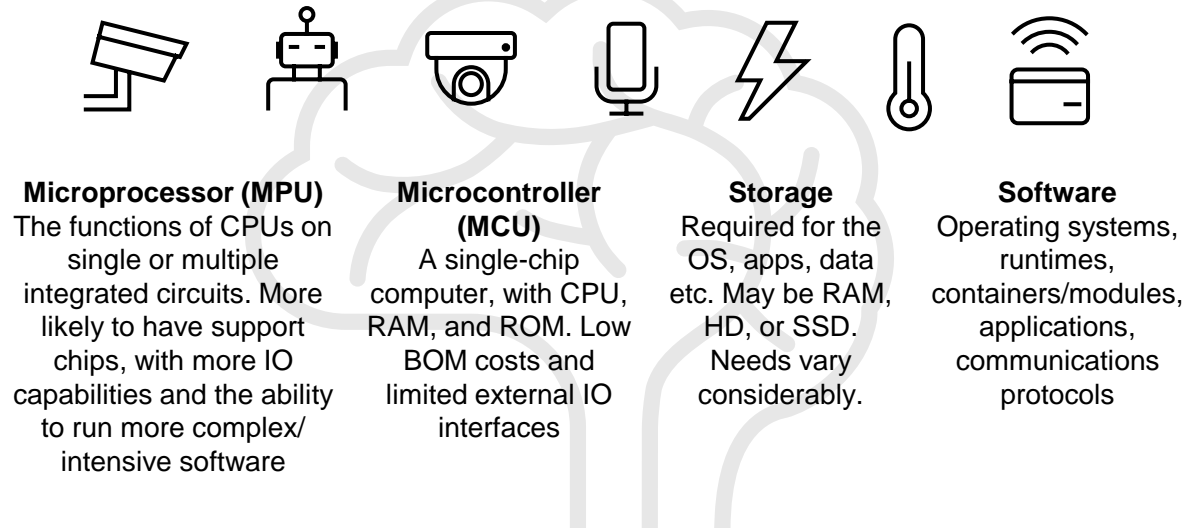
- Azure RTOS
- Azure Sphere
- Azure IoT Edge
- Windows for IoT
- IoT Gateways

Intelligent IoT devices need software and connectivity



Anatomy of an IoT device

(Typically embedded systems or intelligent devices)



Many variables in choosing edge technologies

Compute power required perform the device tasks

- **Power requirements** (battery or powered, consumption, heat dissipation etc.)
- **Storage** amount required based on promised functionality
- **Serviceability and support** (management and updates, component customization, etc.)
- **User interface** and input requirements (GUI, touch, pen, keypad etc.)
- **Determinism of response** (e.g. predictable or guaranteed latency requirements)
- **Development** environment, tools, expertise
- **Cost** of components and overall device price point
- **Security** requirements
- **Connectivity** (IO, USB, Wi-Fi, HDMI, Ethernet, I2C Modbus etc.)
- **Connection** continuity and dependability, bandwidth, latency
- **Communication protocols:** HTTPS, AMQP, MQTT, UDP, BLE, BACnet, Modbus, OPC-UA etc.

Summary comparison of Microsoft edge offerings

	Azure RTOS	Azure Sphere	Azure IoT Edge	Windows for IOT
Product/Components	Real-time OS, middleware & Windows tools	Silicon chips, OS & cloud security services	A fully managed runtime services with cloud connectivity and device lifecycle	Full featured OS offering
Headline	Small memory footprint for resource constrained devices. Hard real time processing (Sub-microsecond interrupt response). Inexpensive. Deployed to billions of devices.	Fairly small memory footprint. Meets the 7 properties of highly secured devices and supports a secured root of trust. Ongoing servicing for updates to keep devices secure.	Deploy your cloud workloads—artificial intelligence, Azure and third-party services, or your own business logic—to run on edge devices via standard containers.	Windows for specific-use (dedicated), embedded devices where a full feature set or GUI is required for complex scenarios. More than 1B Windows 10 devices deployed.
Primary Target Audience	Semiconductor companies of 32-bit parts as well as original equipment manufacturers (OEMs) and SOC suppliers	Greenfield manufacturers (or OEMs) who build new MCU-class connected devices Organizations who want to securely connect existing (brownfield) equipment	Intelligent edge devices needing to run containers locally and eventually coordinate through Azure IoT Hub.	OEMs/ODMs building specific/dedicated use devices with long lifecycles
Typical use case	Low cost, resource-constrained devices requiring reliably fast performance	Highly-secured, Internet-connected microcontroller (MCU) devices	Low latency required to determine alerts/actions on-premises OR enabling intelligence at the edge when devices may be disconnected.	Connected or unconnected devices which may have a rich GUI experience and require a higher level of processing power
Licensing	Production license included with Azure RTOS enabled MCUs; or available separately from MS	NTE \$8.61/unit; one-time purchase includes all components (MCU, OS, and Security Service)	Azure IoT Edge Runtime is free IoT Hub and Modules may have cost implications	Windows 10 IoT Core – Royalty Free Windows 10 IoT Core Services – \$0.30/mo. / device Windows 10 IoT Enterprise – Based on silicon
Requires Cloud connection?	No	Yes	Yes (not constant)	No
Azure Connectivity*	Azure RTOS ships with an Azure Security Center for IoT security module that covers threats and vulnerabilities on real-time operating system devices.	Azure Sphere only natively connects to AS3 security service (no different to Windows getting an update).	Cloud interface through IoT Hub	Windows 10 IoT includes an IoT Device Agent, etc.
Availability	Made available through pre-licensed partners, availability depends on the partner's device distribution model. Also available through MS licensing GA (May 2020)	GA (Feb 2020)	GA	GA

*Applications may also connect to Azure. For example, an application running on Azure Sphere can make it's own connection to it's own Azure IoT Hub.

Azure RTOS – Product description

Comprehensive suite of multithreading facilities, middleware, and Windows tools for developing embedded IoT applications on small, resource-constrained devices with hard real-time requirements. Features Azure RTOS ThreadX, a small, fast, reliable real-time operating system that is already powering more than 6.2 billion devices worldwide. The Azure RTOS ThreadX kernel and set of libraries are delivered as source code that is compiled and linked with an OEM application and board support package (BSP) from the OEM or silicon partner to create the binary image for a device.

- **Azure RTOS ThreadX** – high performance real-time operating system (RTOS) kernel
- **Azure RTOS NetX Duo** – TCP/IP IPv4/IPv6 embedded network stack that supports TLS/DTLS security protocols
- **Azure RTOS FileX** – embedded FAT file system that offers optional fault tolerance and flash memory wear leveling for always-on devices

Azure RTOS USBX – a USB host and device embedded stack

Azure RTOS GUIX – a small-footprint, low-overhead runtime engine and development tool featuring automatic code generation for embedded systems capable of graphic display

Azure RTOS GUIX Studio – complete design environment to create and maintain Windows-based GUIs

Azure RTOS TraceX – graphical view of real-time system events to help analyze unexpected behaviors and resolve problems

Memory footprint:
2 KB (ThreadX OS Kernel)

Architecture support:
All 32-bit CPU architectures, including various ARM cores, MIPS, PowerPC, and RISC-V. Also supports 64-bit ARM cortex A53, and SMP ARM

Positioning



Small memory footprint for resource constrained devices. Hard real-time processing. Easy to use. Inexpensive. For connecting deeply embedded sensors, devices, and gateways from the edge to the Internet. Enables fast to market and access to the power of Azure.

- Features preemptive, deterministic, and time-bound capabilities and predictable response times
- Supports the most popular embedded development tools

Example use cases

- Smart phones (esp. Wi-Fi chips)
- Consumer Electronics (e.g. cameras, fitness trackers)
- Office/Business Automation
- Retail Automation
- Industrial Automation & Energy/Power
- Low capacity sensors like lightbulbs, temperature gauges, traffic sensors, and more
- Anti-lock brakes, ADAS, Vehicle-to-everything (V2X) and more automotive features
- Safety-critical applications requiring guaranteed maximum response time (in milliseconds)

Other things to know

- Azure RTOS partners provide integrated solutions for prototyping and developing enterprise-ready solutions.



- Azure RTOS ThreadX was launched in 1997 and was part of the X-Ware IoT platform developed by Express Logic which Microsoft acquired in April 2019. It is deployed to billions of devices.

Azure RTOS (cont'd)



Microsoft Security

When we rebranded the product to Azure, we changed the code, albeit in minor ways. As a result, the code must be re-reviewed and re-certified by governing authorities. We are working to get off-the-shelf safety re-certifications for core products (ThreadX, FileX, GUIX, NetX Duo, USBX) from TUV and UL).

In addition, NetX Secure TLS and NetX MQTT will be re-certified under EAL4+ and the NetX software crypto library will be re-certified to FIPS 140-2.

Azure RTOS ThreadX is currently MISRA compliant (with MISRA C:2004 and MISRA C:2012). MISRA C is a widely recognized standard for embedded C programming in most safety-related industries.



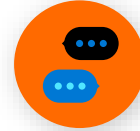
Licensing

Available to freely to test and explore the source code (available on GitHub)

Production license included at no cost if deployed to any of the supported pre-licensed devices from listed Semiconductor partners (initially STMicroelectronics, Renesas, NXP, Microchip, and Qualcomm). A list of pre-licensed devices will be available on GitHub.

Simple annual licensing for all other devices. \$29,000 annual fee (direct from Microsoft) for up to 1M devices. (Contact Microsoft of deploying more than 1M devices.)

Optional add-on industrial certification package (formal reports with test results from TUV, UL and others certifying that the code behind specific Azure RTOS components has met rigorous safety and security standards) available in fall 2020 for \$30,000 annual fee.



FAQs

Can Azure RTOS and Azure Sphere be used together?

Yes. Azure Sphere chips include real-time processing cores that are protected by the Azure Sphere OS, however, does not provide the real-time operating system (RTOS). But Azure RTOS can be used with Azure Sphere to allow embedded developers to take advantage of these real-time processing cores enabling a highly secure device with real-time processing capabilities.

Can Azure RTOS broadly available?

Azure RTOS is currently in "public preview" which is really about showing off the integration work done by industry leading partners in their embedded development kits which feature Azure RTOS ThreadX. These partners together represent the vast majority of the market for 32-bit MCUs.

Azure Sphere – Product description

Azure Sphere is a comprehensive IoT device security solution that is purpose-built to allow any developer to create a connected device that is highly secured by default. It is an integrated solution that includes Azure Sphere-certified hardware, the Azure Sphere operating system, and Azure Sphere Security Service with ongoing OS and security updates. Azure Sphere is a certified MCU device that works seamlessly with OS and cloud security components to provide active security by default.

- **Azure Sphere certified chips (from hardware partners)** – physical MCUs and SOCs with built-in Microsoft security technology. Supports a secured hardware root of trust for connected, intelligence edge devices
- **Azure Sphere OS** – OS offers defense in depth, i.e., multiple layers of security combining security innovations pioneered in Windows, threat monitoring, and a custom Linux kernel to create a highly-secured software environment and a trustworthy platform for new IoT experiences

Azure Sphere Security Service – a SaaS cloud service that brokers trust for device-to-cloud communication, detects threats, and continually renews device security

Azure Sphere SDK – provides integrated development tooling for programming and debugging Azure Sphere solutions in Visual Studio and Visual Studio Code

Memory footprint: 4 MB

Azure Sphere certified chips are available today from MediaTek. Development kits and modules are available from ecosystem partners Avnet, AI-Link, Seeed Studio, USI, and qiao. NXP and Qualcomm chips coming soon.

Positioning



An integrated hardware, software, and cloud services solution for securely connecting existing equipment and to create new IoT devices with built-in device to cloud security.

- Provides a complete solution to enable any developer—by default—to build highly-secured connected devices.
- Suitable to secure even devices that connect directly to the internet due to its defense-in-depth approach across hardware, software/OS, and security service

Example use cases

- Food services
- Refrigeration
- Industrial/Manufacturing/Infrastructure
- Logistics/Transportation
- HVAC controls
- Medical devices
- Drones
- Home appliances
- Escalators/elevators
- Badge scanners

Other things to know

Azure Sphere guardian modules.

Azure Sphere guardian modules (developed by partners) are secure data connectors built on Azure Sphere that can help securely connect legacy “brownfield” devices (and existing architectures) to the cloud.

- Guardian module functions:
- Processes data
 - Authenticates cloud endpoints
 - Validates messages between cloud and device

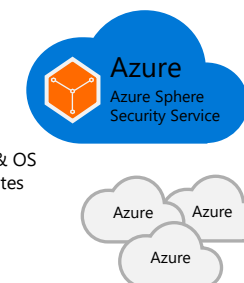


Device



Guardian module

Apps & OS updates
App data & telemetry



Azure Sphere (cont'd)



Microsoft Security

OEMs using Azure Sphere are building on top of a platform that, by default, provides all 7 properties of highly secured devices.

Azure Sphere's integrated hardware, software, and cloud services work seamlessly together and deliver active security by default.

Every Azure Sphere device comes with over 10 years of security and OS updates. Microsoft builds, manages and deploys these updates directly to the devices.

Security updates and improvements are delivered automatically to each Azure Sphere device from the Azure Sphere Security Service continuously. OEMs can use the same Azure Sphere Security Service to remotely update their applications.

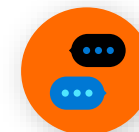


Licensing/Pricing

The Azure Sphere includes three components, always sold together as one solution: Azure Sphere certified MCU, Azure Sphere OS, Azure Sphere Security Service

Customers purchase the solution (chips) from a distributor. Each chip comes bundled with the Azure Sphere license that covers the Azure Sphere OS—including more than 10 years of ongoing security and OS improvements—and a subscription to the Azure Sphere Security Service for as long as the device is connected. (Separate subscriptions are required for other cloud services.)

Prices will be variable by each partner developed Azure Sphere MCU depending on the capabilities and manufacturer requirements. For the first Azure Sphere MCU, the MediaTek MT3620 AN, the price will be less than \$8.65 (including all three components) and varies based on volume.



FAQs

Does a company have to be an Azure customer to use Azure Sphere?

No. The Azure Sphere Security Service is engineered to let device manufacturers integrate with the tools and services they already use. While the Azure Sphere Security Service runs in Azure, customers have the choice to connect to any proprietary or public cloud for app data.

Is a Visual Studio License required?

Customers have a choice of which development tools they use, however leveraging Visual Studio and Azure IoT services, allows organizations to develop applications for Azure Sphere more efficiently. Proper licensing of Visual Studio is required to use the Visual Studio Tools for Azure Sphere.



Azure IoT Edge for Linux
on Windows

EFLOW

Azure IoT Edge For Linux On Windows brings the best of both worlds



Windows IoT

- Robust user experience
- Extensive application ecosystem
- Trusted Enterprise-grade security
- Established IT Admin infrastructure
- World-class long-term servicing
- Flexible hardware options



Linux

- Containerized Microservices
- Native Docker packaging
- Broad Edge module adoption
- Enable AI/ML scenarios
- Enable IIoT workloads

Azure EFLOW



Lower Cost

One device can do it all

- Simple to deploy, manage, and update with existing tooling
- Leverage existing app and infrastructure investments
- Minimal impact to IT Administration



New Capabilities

- Easily connect to Azure
- Broadest of AI/ML modules
- Existing IIoT module support
- Even more 3rd party modules

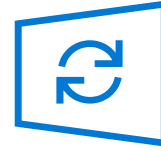
Enabling Linux-base cloud native workloads on Windows edge device



Microsoft Supported
Linux VM



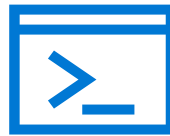
IoT Edge Linux
Module ready



Always up
to date



Windows
Administration

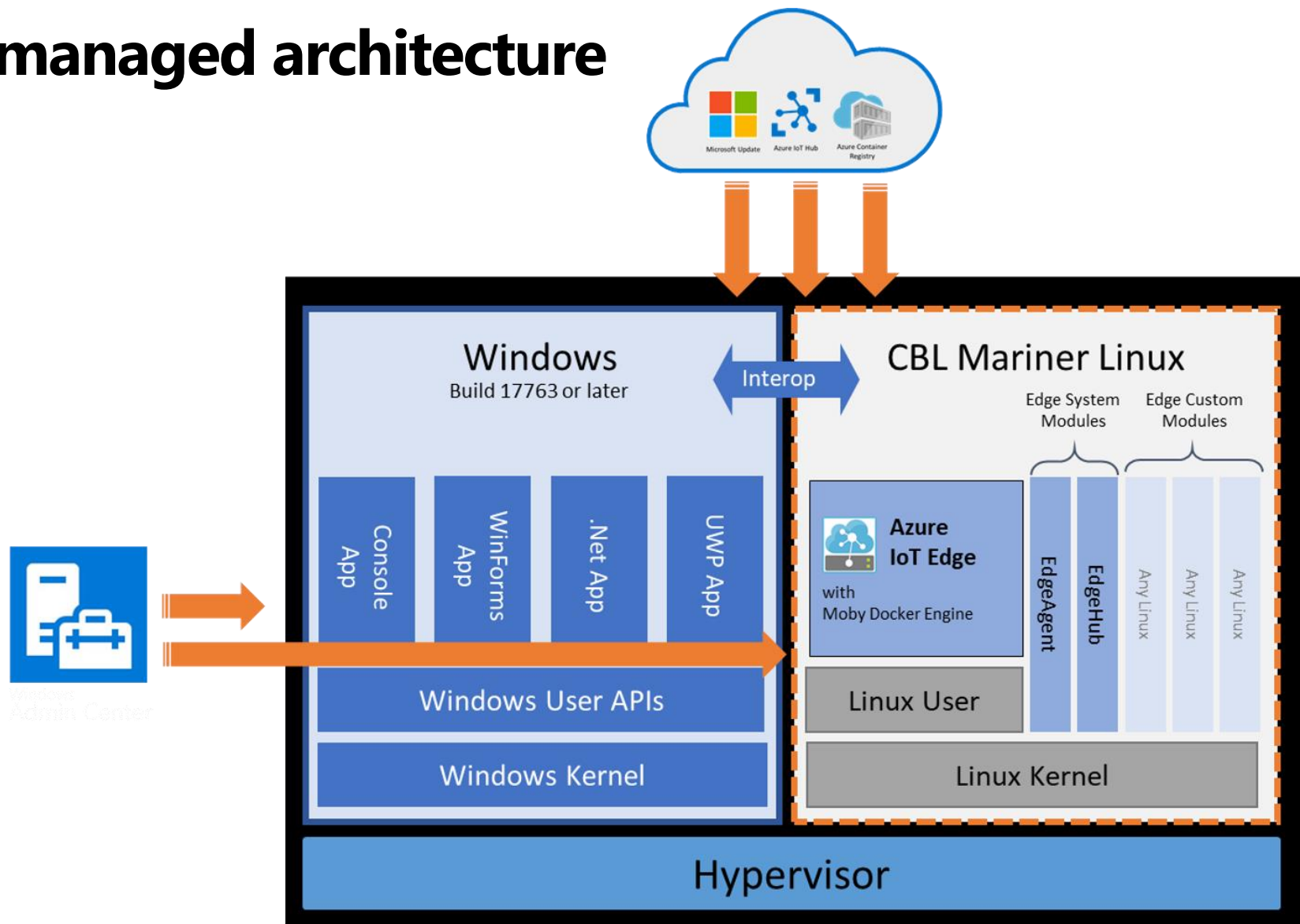


Flexible
Scripting



App to Module
Interoperability

Microsoft managed architecture



Multiple reasons to choose EFLOW

If your organization...

is a Microsoft shop and does not want to introduce a different OS

does not have Linux knowledge in house or on location

is sometimes deploying solutions in remote, less accessible locations

has network latency, outages and/or delays that prohibits running workload in the cloud

is using Linux today but would prefer Windows to perform the same function

wants to keep the cost of hardware assets in check

has both Windows and Linux devices and wants to reduce overhead

is developing IoT Edge solutions and selling those in the IoT Edge marketplace

EFLOW provides...

Familiar Windows management tools for deploying Linux workloads






Deployment of cloud-native workloads to the edge

Ability to use existing Linux modules but manage & secure your devices with Windows

Linux IoT Edge modules run on Windows devices

Linux + Windows capabilities and interoperability on a single machine

Run EFLOW on your existing edge devices

	Supported OS	Windows Pro / Enterprise 2109 (build 17763) or later Windows Server 2019 (build 17763) or later
	Free Storage	10GB Minimum*
	Memory	Physical: 4GB Minimum* - Free: 1GB Minimum*
	Virtualization	Physical: 4GB Minimum* - Free: 1GB Minimum*
	Licensing	Free with supported OS versions – Azure subscription required

Resource	Link
Documentation	https://aka.ms/AzEFLOW-Docs
Wiki	https://aka.ms/AzEFLOW-Wiki
Release Notes	https://aka.ms/AzEFLOW-Releases
Sample Code	https://aka.ms/AzEFLOW-Samples
GitHub	https://aka.ms/AzEFLOW-Github

* Memory and Storage requirements depend on the size of the VM selected at deployment

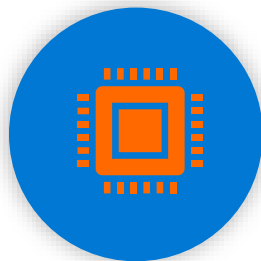
Hardware access



TPM 2.0

Trusted Environment for
DPS Provisioning

Learn More:
aka.ms/AzEFLOW-TPM



GPU

HW Accelerated
Inferencing

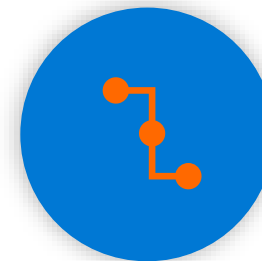
Learn More:
aka.ms/AzEFLOW-GPU



Camera

AI / ML with USB
attached Camera

Learn More:
aka.ms/AzEFLOW-USB-Camera-To-RTSP



Serial

Data ingestion from serial
attached devices

Learn More:
aka.ms/AzEFLOW-Serial-Passthrough

IT Admin Target Audience

Company Attributes

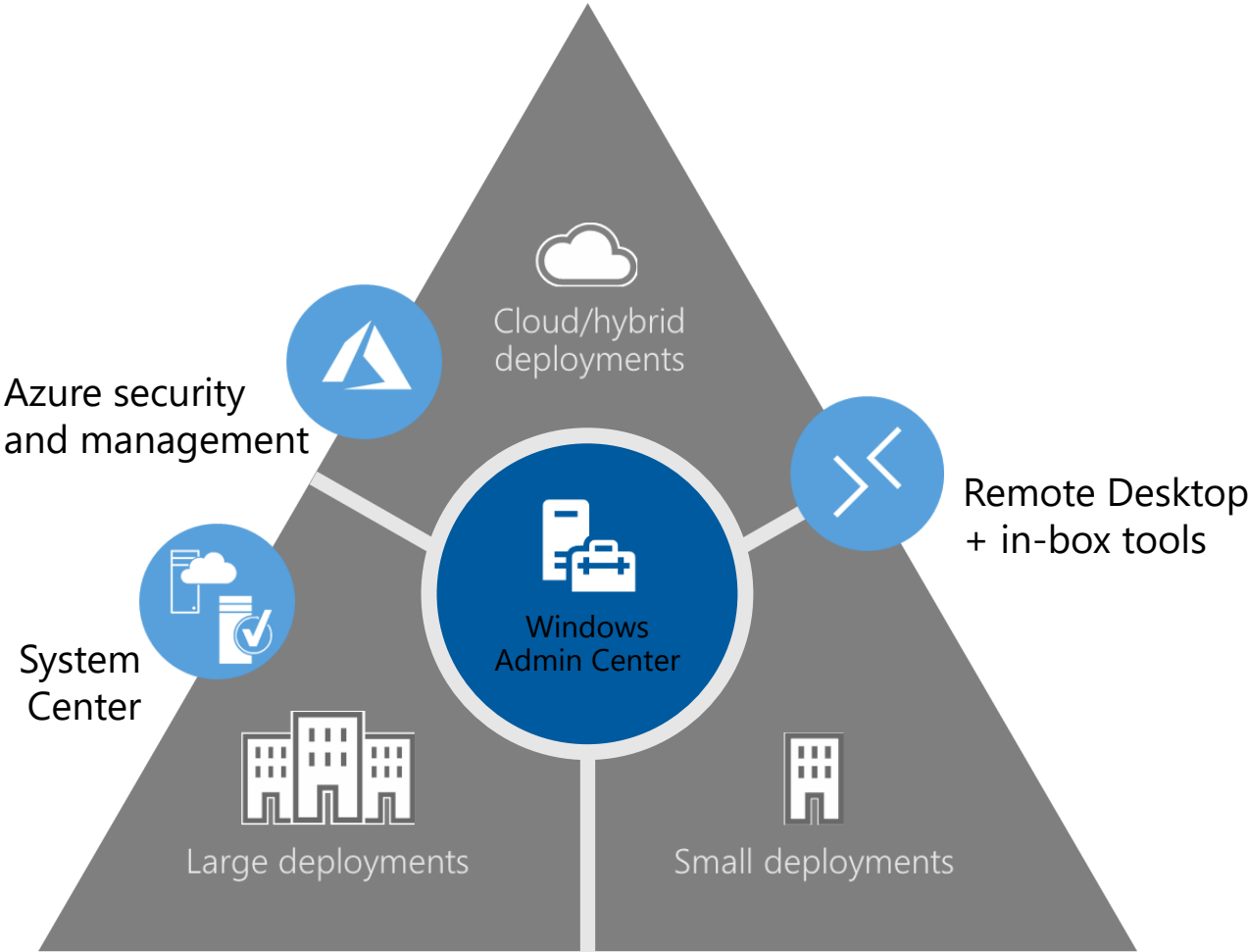
Primary Operating System

Management Control Pane

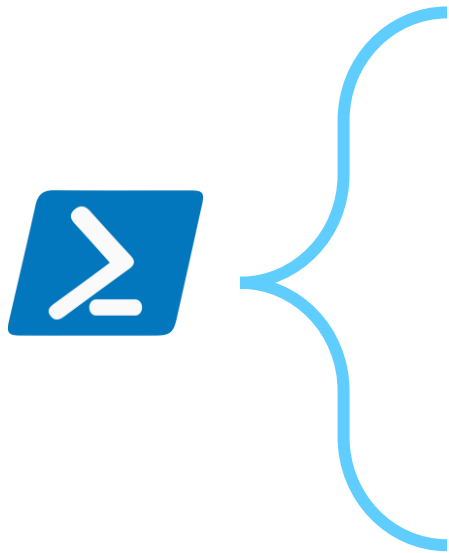
Existing Software Investments

IT Staff Knowledge

OS



Package installation and configurations using PowerShell



- PowerShell 5.1
- PowerShell 6
- PowerShell 7 (soon)
- PowerShell SDK (soon)

Function

Deploy-Eflow

Provision-EflowVm

Start-EflowVm / Stop-EflowVm

Connect-EflowVm

Get-EflowVm

Set-EflowVm

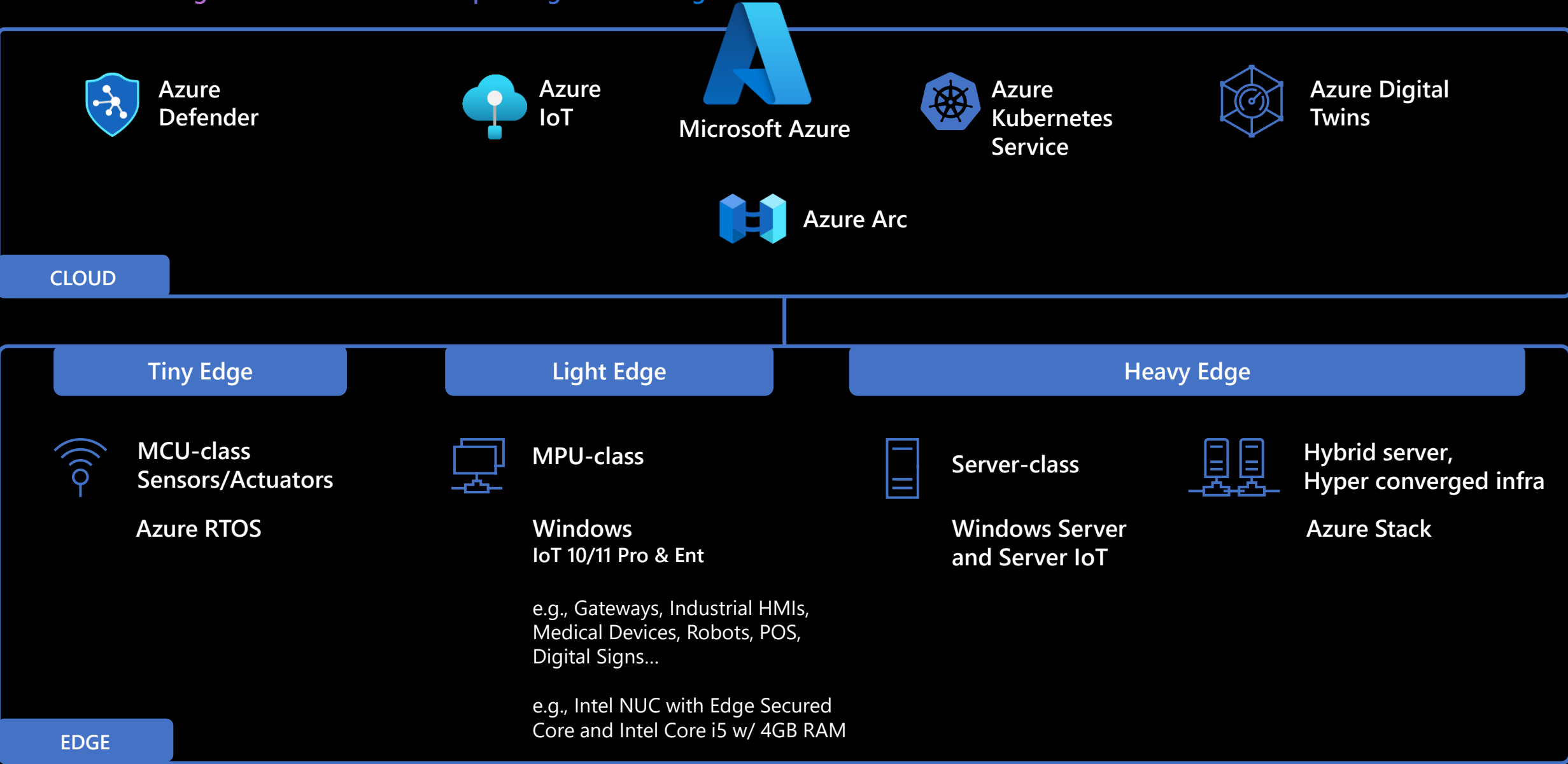
Invoke-EflowVmCommand

Copy-EflowVmFile

Learn more: <https://aka.ms/AzEFLOW-PowerShell>

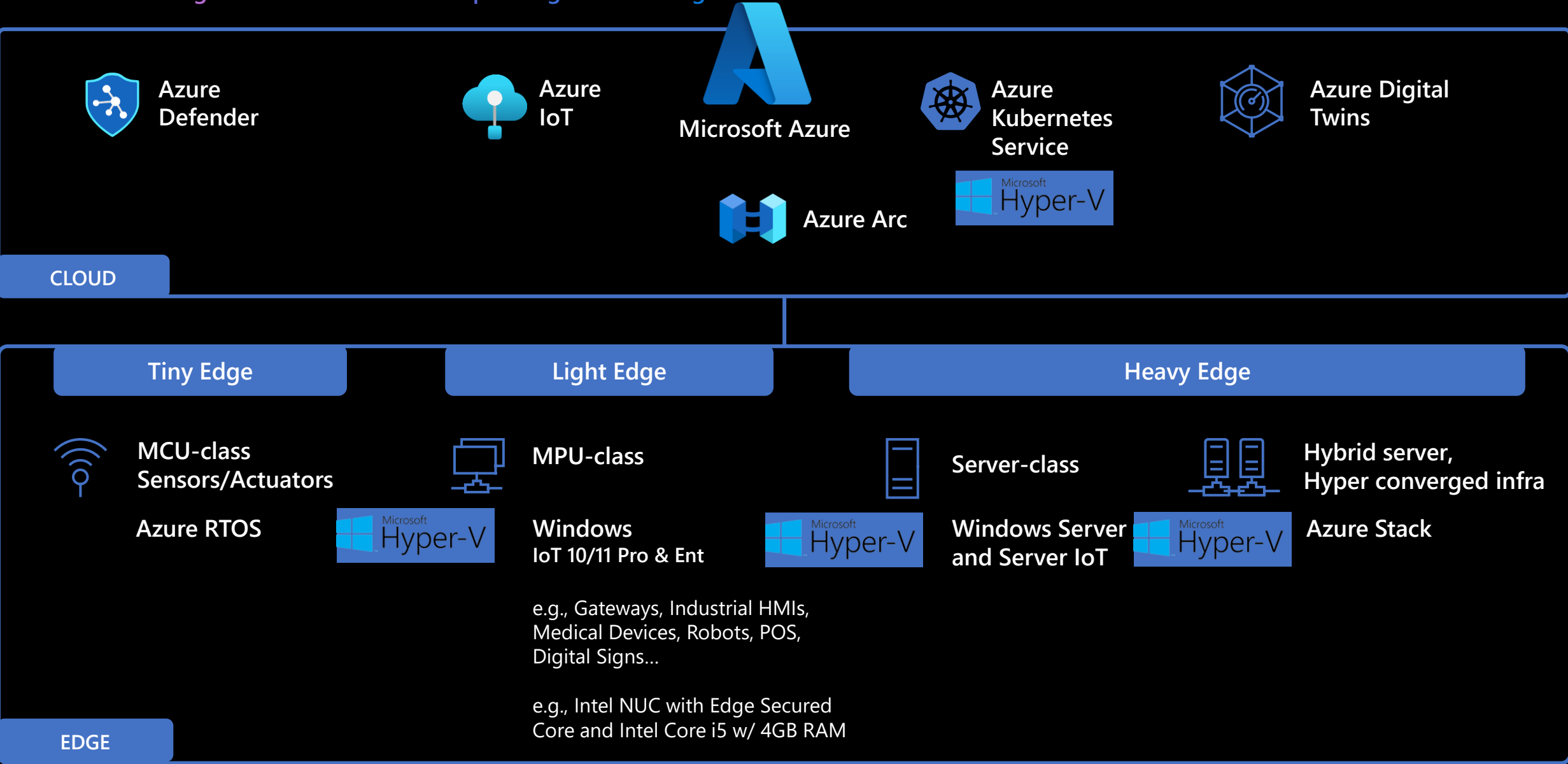
Azure Kubernetes Service (AKS)

A Microsoft managed Kubernetes solution spanning Azure to Edge



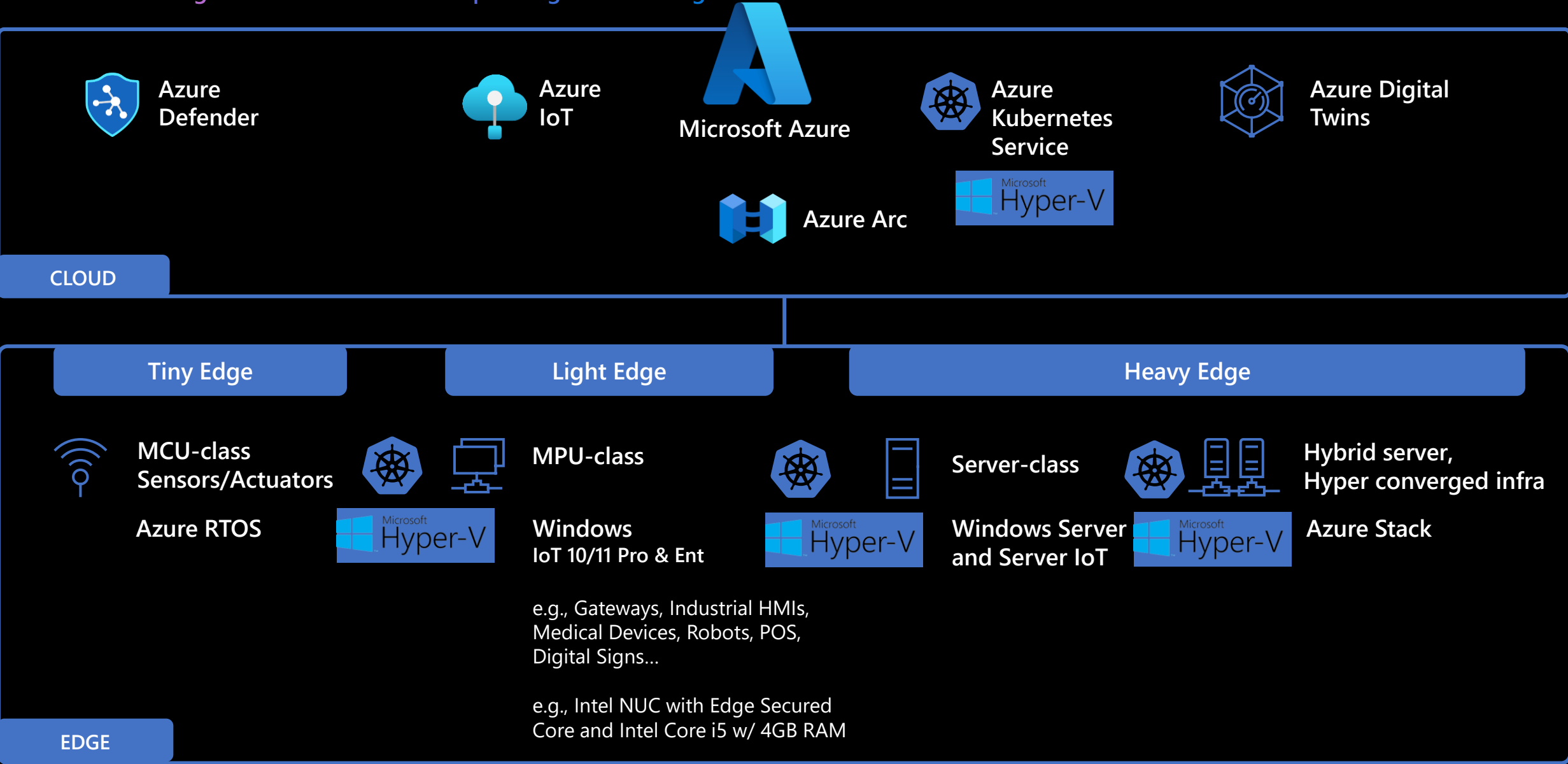
Azure Kubernetes Service (AKS)

A Microsoft managed Kubernetes solution spanning Azure to Edge



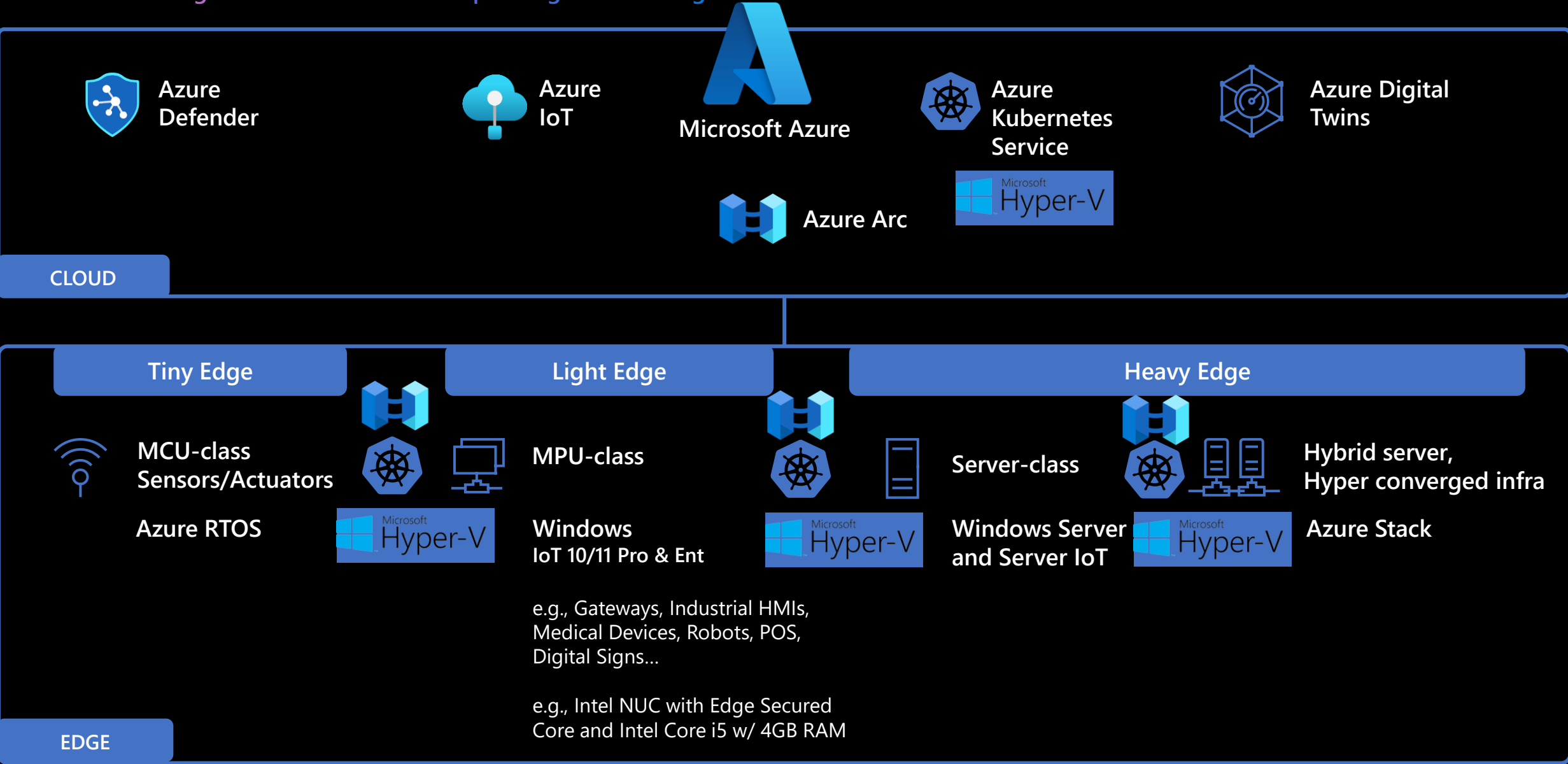
Azure Kubernetes Service (AKS)

A Microsoft managed Kubernetes solution spanning Azure to Edge



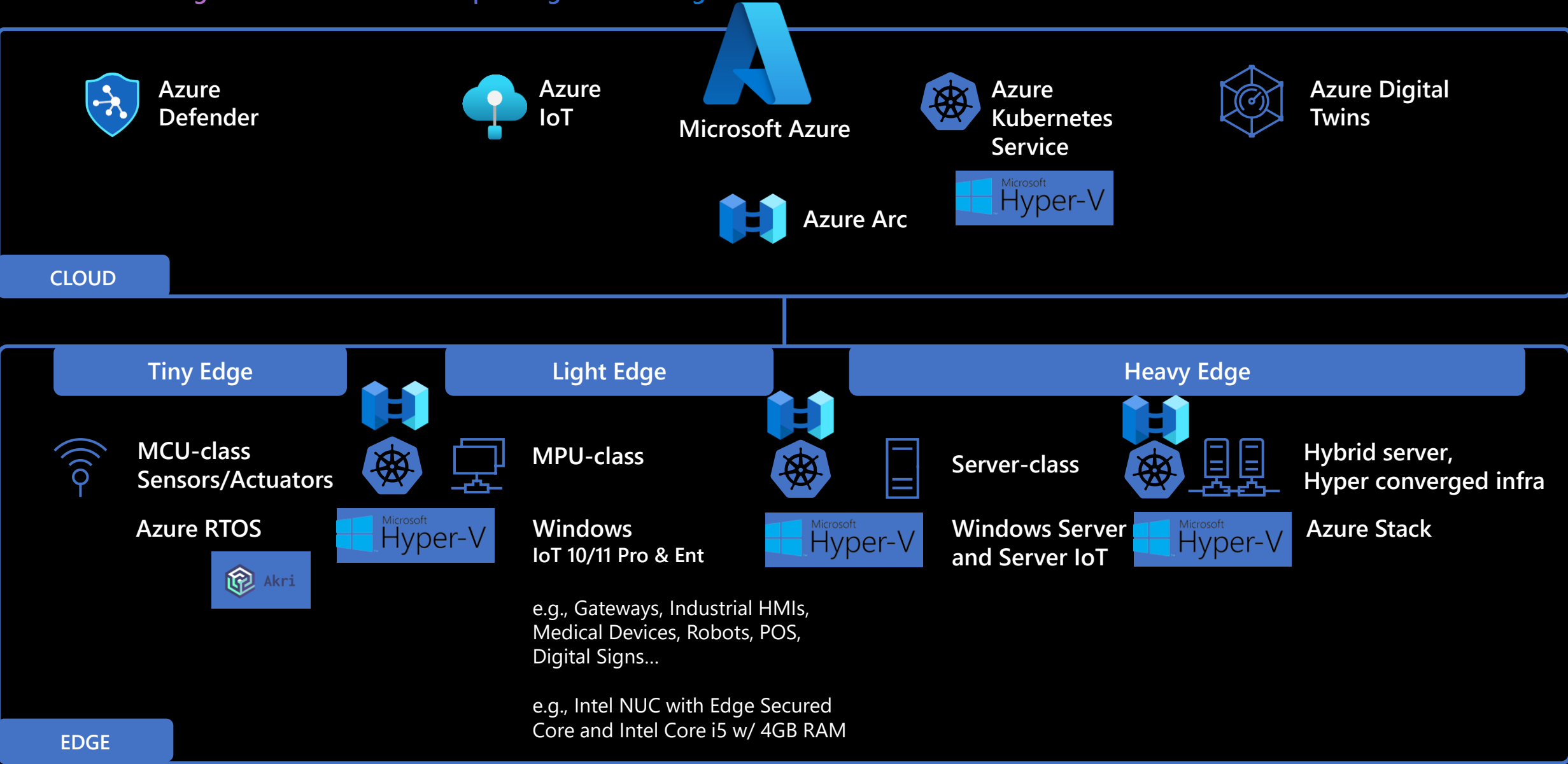
Azure Kubernetes Service (AKS)

A Microsoft managed Kubernetes solution spanning Azure to Edge



Azure Kubernetes Service (AKS)

A Microsoft managed Kubernetes solution spanning Azure to Edge



Interoperability with Windows Apps



Windows



Hardware

Azure to Edge



Azure Resource Manager

Build and manage cloud deployments directly from the Azure portal



Deploy Cluster extensions



Azure Monitor

Monitor servers in Azure, machines on-premises or at other cloud providers.



Azure Policy

Enforce organizational standards and assess compliance at-scale.



Azure App Service

Quickly build, deploy, and scale web apps and APIs on Kubernetes or Azure.



Deploy your own workloads

PR Pipeline

App repository

GitOps

Manage your desired state Kubernetes cluster configurations with Git



CI Pipeline



CD Pipeline

GitOps repository



Microsoft Artifact Registry

Build, store, and manage container artifacts for your deployments

OS and VM Updates

Windows Update

Get the latest fixes, updates and security improvements



Azure Arc



Deploy AKS lite on a device like an application



Connected via
Azure Arc-enabled Kubernetes

Connected via
Azure Arc-enabled servers

Cluster extensions



User workloads



Flux



Containerized workloads

AKS lite Kubernetes Platform



K8s/K3s

Linux VM



Windows VM (optional)



Windows Host OS (with Hyper-V)



Hardware

Pull cluster desired state

From Azure
to edge
and back

AKS lite hybrid option (preview)



Deploy your Linux and/or Windows containerized workloads

AKS hybrid options on Windows



Azure Arc control plane to manage your cluster in Azure



Standard kubectl to manage your cluster using PowerShell



CNCF-conformant Kubernetes platform

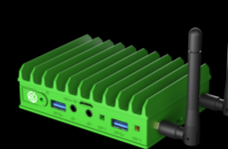


PowerShell cmdlets and agents to enable provisioning and control of VMs and infra

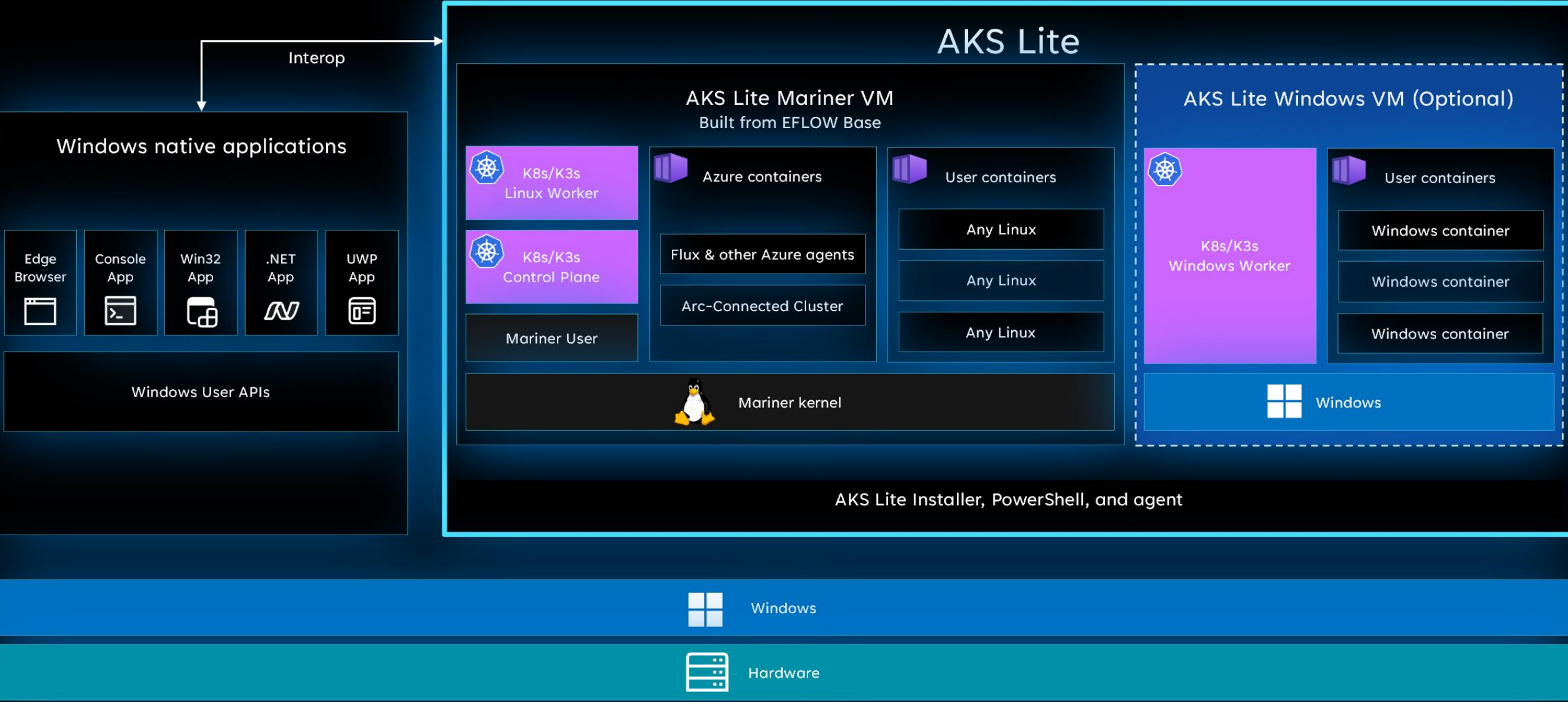


Windows 10/11 (IoT Enterprise / Enterprise / Pro /) and Windows Server

Edge computing devices (with 8GB+ RAM)



Azure Kubernetes Service (AKS) Lite architecture



Enabling solutions with Edge Modules from Microsoft



Azure Video Analyzer

Generate real-time business insights from video streams, processing data near the source and applying AI of your choice.

Learn more: <https://aka.ms/LVA>



Cognitive Services

Embed the ability to see, hear, speak, search, understand, and accelerate decision-making

Learn more: <https://aka.ms/Cognitive>



Anomaly Detector

Monitor and detect abnormalities in your time series data without having to know machine learning.

Learn More:
<https://aka.ms/AnomalyDetector>



Blob Storage

Enables Edge modules that use Azure Storage SDK to alternatively store the data locally on a local blob store.

Learn more: <https://aka.ms/SQLEdge>



SQL Edge

Manage data at the edge with data streaming, time series data analysis, and machine learning-based data inferencing.

Learn more: <https://aka.ms/SQLEdge>



Industrial IoT

OPC Publisher connects to existing OPC UA servers and publishes data from these servers in OPC UA "Pub/Sub" format

Learn more: <https://aka.ms/OPCPublisher>

Modbus enables acquisition of data through Modbus TCP or RTU protocols

Learn more: <https://aka.ms/Modbus>



Any questions for me?



Resources

Blogs & Videos

General Availability

Blog: aka.ms/AzEFLOW-blog

IoT Show: aka.ms/AzEFLOW-show

EFLOW and WSL in Edge Dev

Blog: aka.ms/AzEFLOW-wslblog

IoT Show: aka.ms/AzEFLOW-wslshow

Product

Overview: aka.ms/AzEFLOW-docs

QuickStart: aka.ms/AzEFLOW-quickstart

Install: aka.ms/AzEFLOW-install

PowerShell: aka.ms/AzEFLOW-powershell

Modules: aka.ms/AzEFLOW-modules

GitHub

Home: aka.ms/AzEFLOW-github

Wiki: aka.ms/AzEFLOW-wiki

Issues: aka.ms/AzEFLOW-issues

Samples: aka.ms/AzEFLOW-samples

Releases: aka.ms/AzEFLOW-releases

Marco Dal Pino

Technical Consulting
Microsoft

- 30+ years in IT (Developer, Architect, Consultant, PM, Trainer)
- Speaker, Community addicted
- IoT Influencer



<https://www.linkedin.com/in/marcodalpino>



<https://about.me/marcodalpino>



<https://twitter.com/marcodalpino>



info@contoso.blog



<https://www.twitch.tv/dpcons>





Platinum Sponsor



Gold Sponsor



Technical Sponsor

