
How infra admins can move from scheduled tasks to cloud and event based activities

Mika Vilpo

IT Geek Building Clouds

@Elisa Oyj

Like to talk about identity, automation and serverless

25+ years in IT and 15+ years in cloud

Spending free time as Red Cross volunteer in disaster management, first aid and search & rescue

mika.vilpo@elisa.fi

@mikavilpo

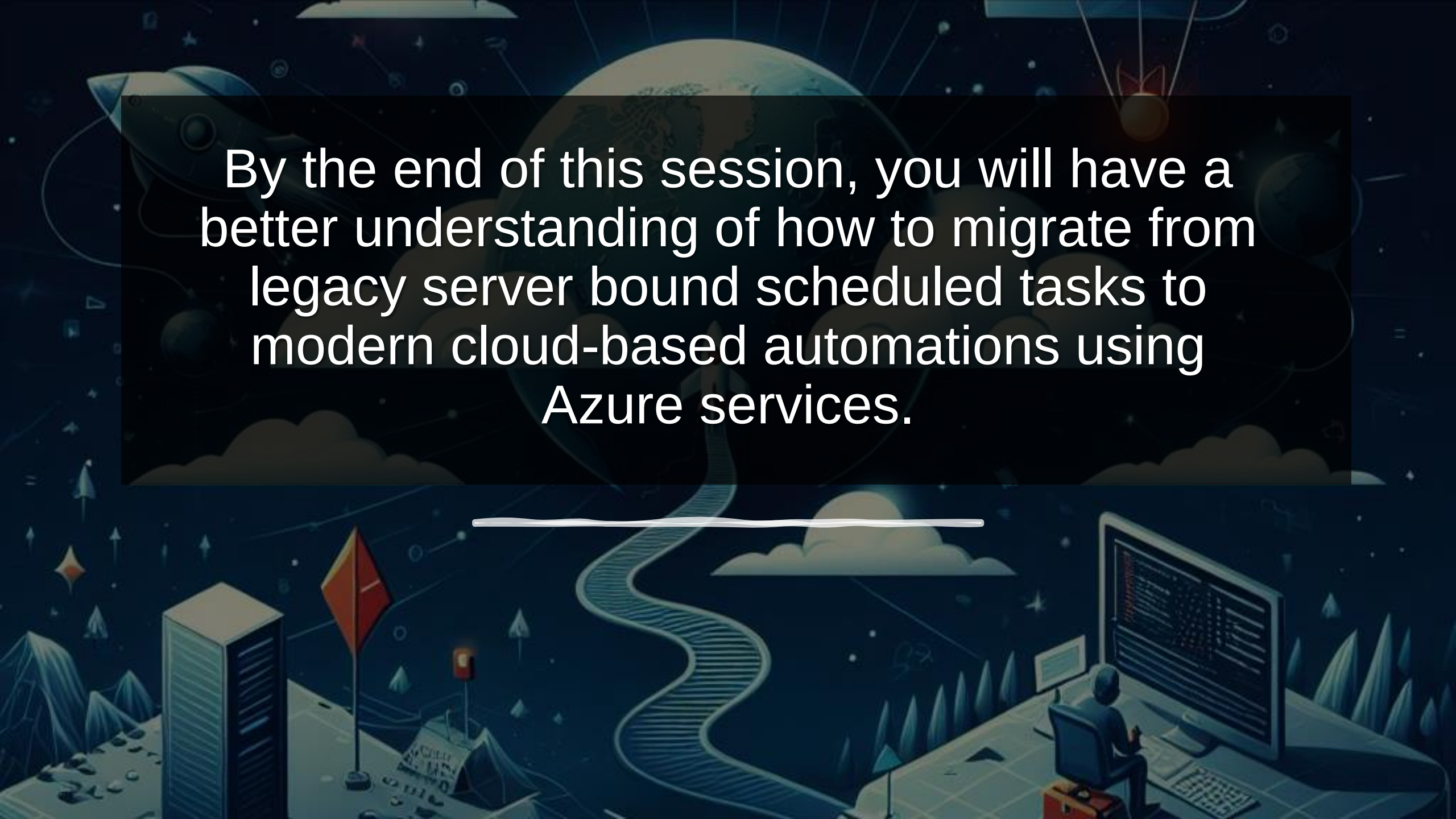
Microsoft Certified: Azure Solutions Architect Expert

Microsoft Certified: Cybersecurity Architect Expert

Microsoft Certified: DevOps Engineer Expert

Microsoft 365 Certified: Enterprise Administrator Expert

Microsoft Certified Trainer: MCT 2022 - 2023


By the end of this session, you will have a better understanding of how to migrate from legacy server bound scheduled tasks to modern cloud-based automations using Azure services.

Lab setup

- Azure
  - Couple tenants, VMs hosted everywhere
- Onprem DC @Turku, Finland
  - No inbound connectivity at firewall
- No VPN etc. between

- Laptop and W365 connected only to internet

What we are currently running on our on-premises servers as scheduled jobs?

- Disk management
  - Log rotation
  - Temp-folder cleanup
- Software management
- Clean Inactive computer accounts

- IAM tasks
  - User account mover / cleaner
  - Expiring account notifier
  - Group management tasks
    - Remove disabled users from groups etc.

What to do with scheduled tasks?

Easy

- **Migrate** to Azure Automation
  - Centralized view of automation
  - Alerting based on logs

Harder

- **Refactor**
  - Use Azure Functions, Logic App or Azure Automation based on the need

Scheduling is slow and old - or is it?

Getting feasible **events** from legacy servers can be hard if previously only event has been **time**

Time is a event

Where do I get events?

Azure Monitor

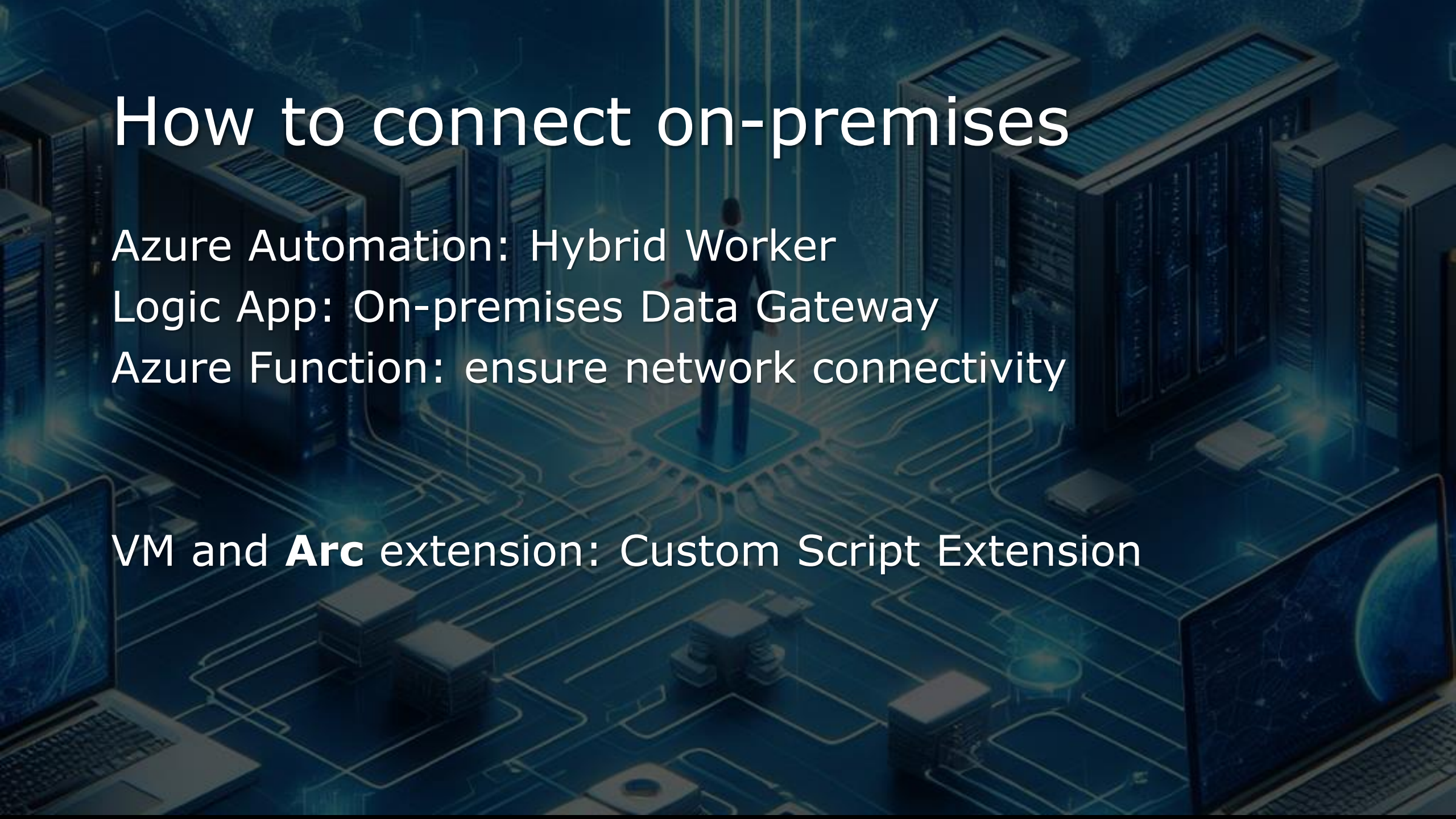
- Convert ‘legacy events’ from logs to events

Azure Resource Changes

- Available at Event Grid topics

Microsoft Graph API Change Notification

- Can be subscribed to Service Bus, Event Hub or Event Grid



How to connect on-premises

Azure Automation: Hybrid Worker
Logic App: On-premises Data Gateway
Azure Function: ensure network connectivity

VM and **Arc** extension: Custom Script Extension

What does Azure Arc do?

- Extends the Azure platform to enable consistent management and governance of resources across datacenters, edge, and multicloud environments.
- Enables running Azure workloads on any Kubernetes cluster and deploying Azure data service on any infrastructure

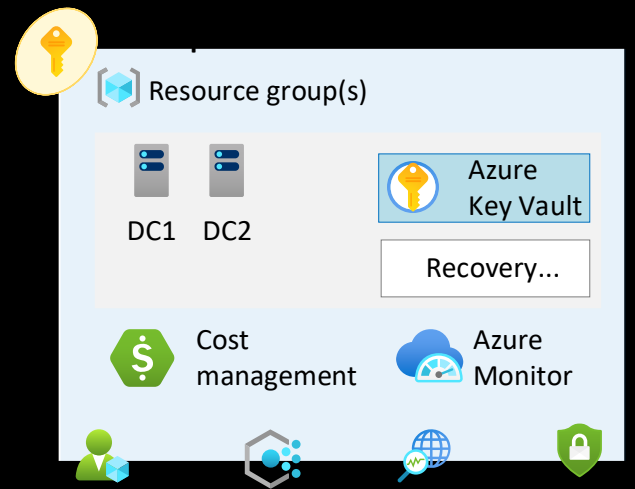
Where to Arc

Own Subscriptions vs. Existing Subscriptions

→ Own Management Group hierarchy

→ Own Policies?

Tier 0 assets require special attention




Demo of Azure Arc,
WAC and magical SSH

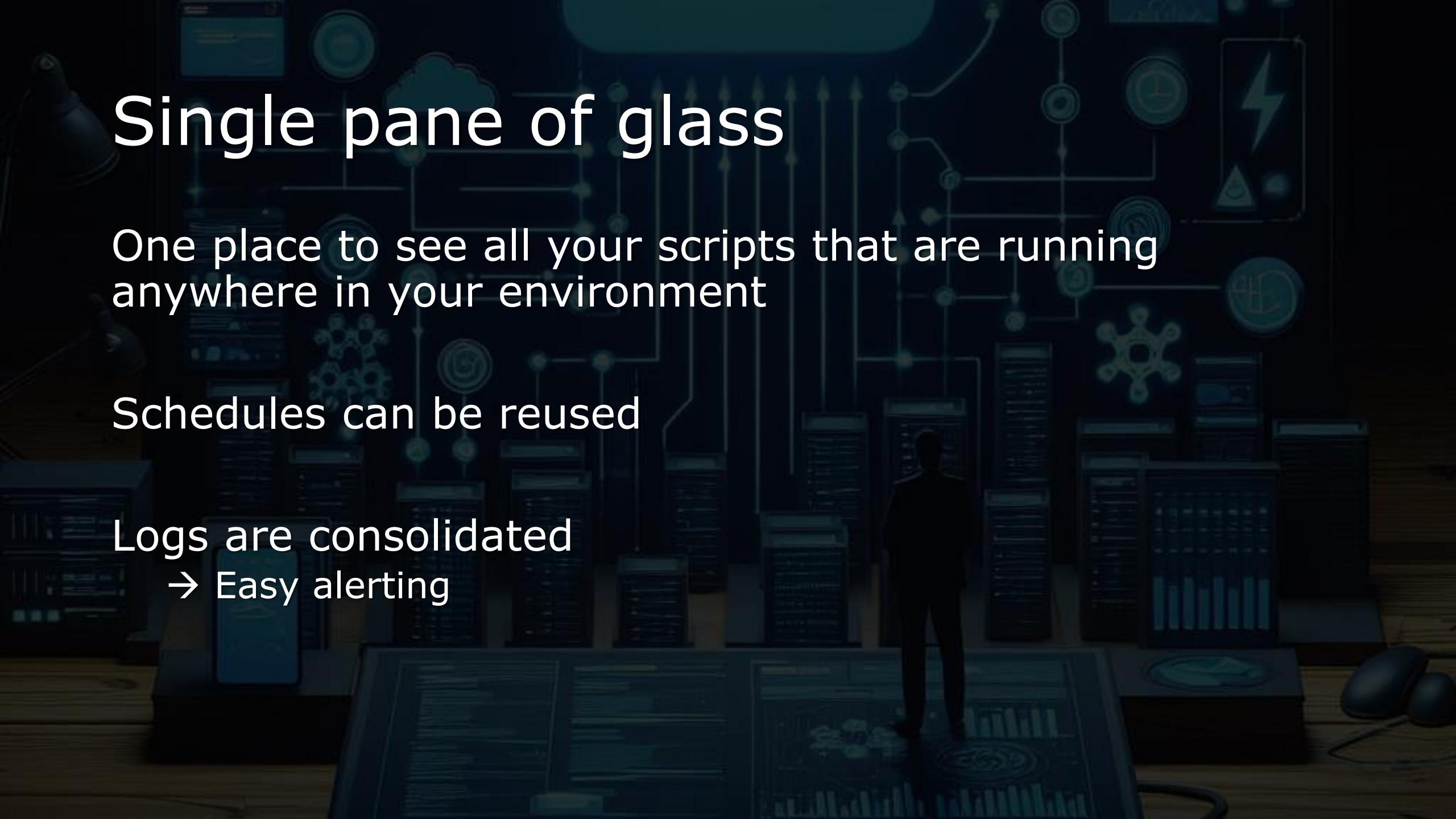
Azure Automation Account

Cloud based automation engine

- **PowerShell 5.1 & 7.1**, Python
- **Code** and Graphical

- Automations can be run on ”cloud” or ”server”

- Built-in secret and variable handling and sharing between runbooks



Single pane of glass

One place to see all your scripts that are running anywhere in your environment

Schedules can be reused

Logs are consolidated

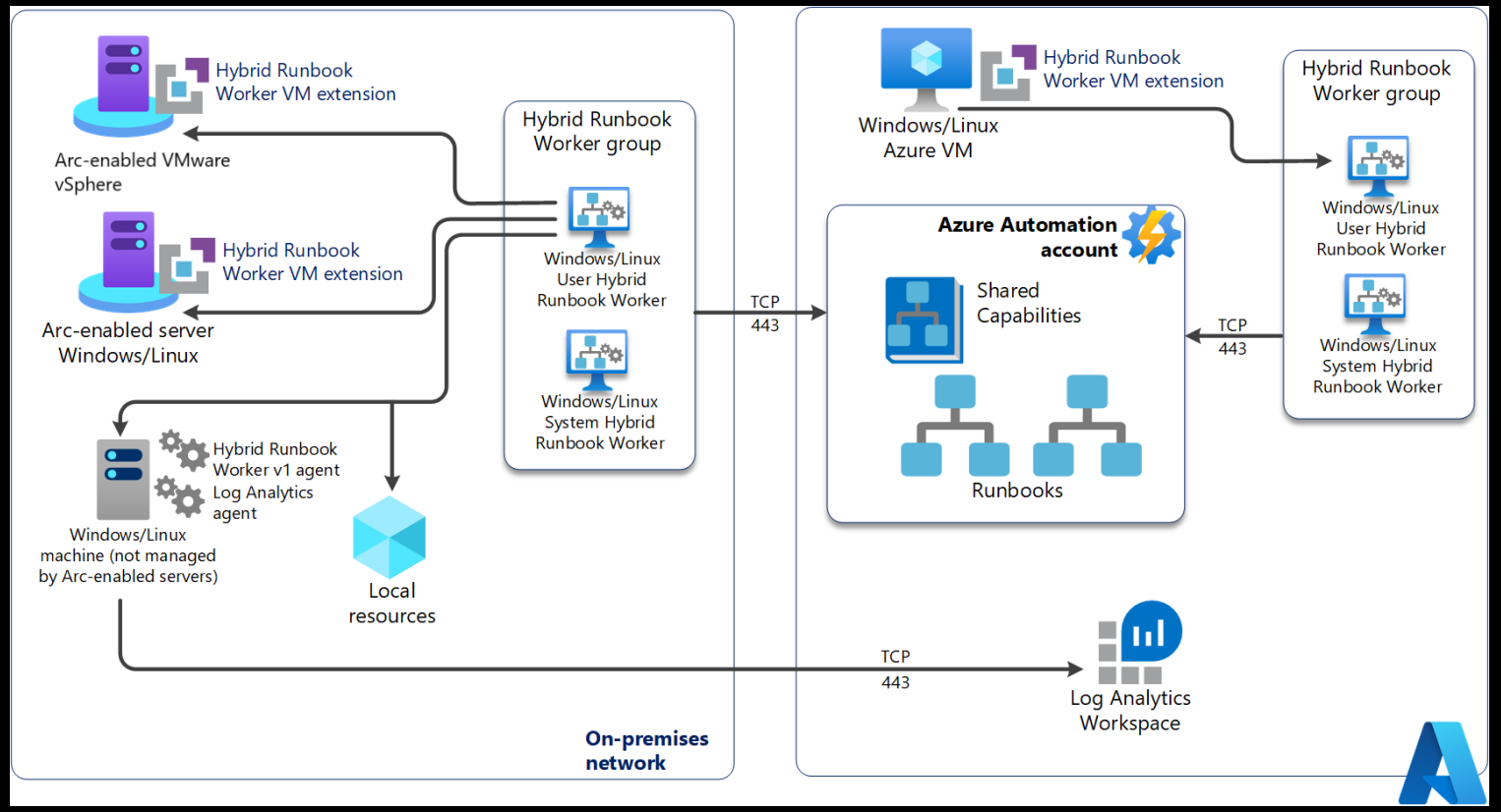
→ Easy alerting

No more Hybrid Worker Agents

Old way deprecating

Use Azure VM or Arc extension (v2)

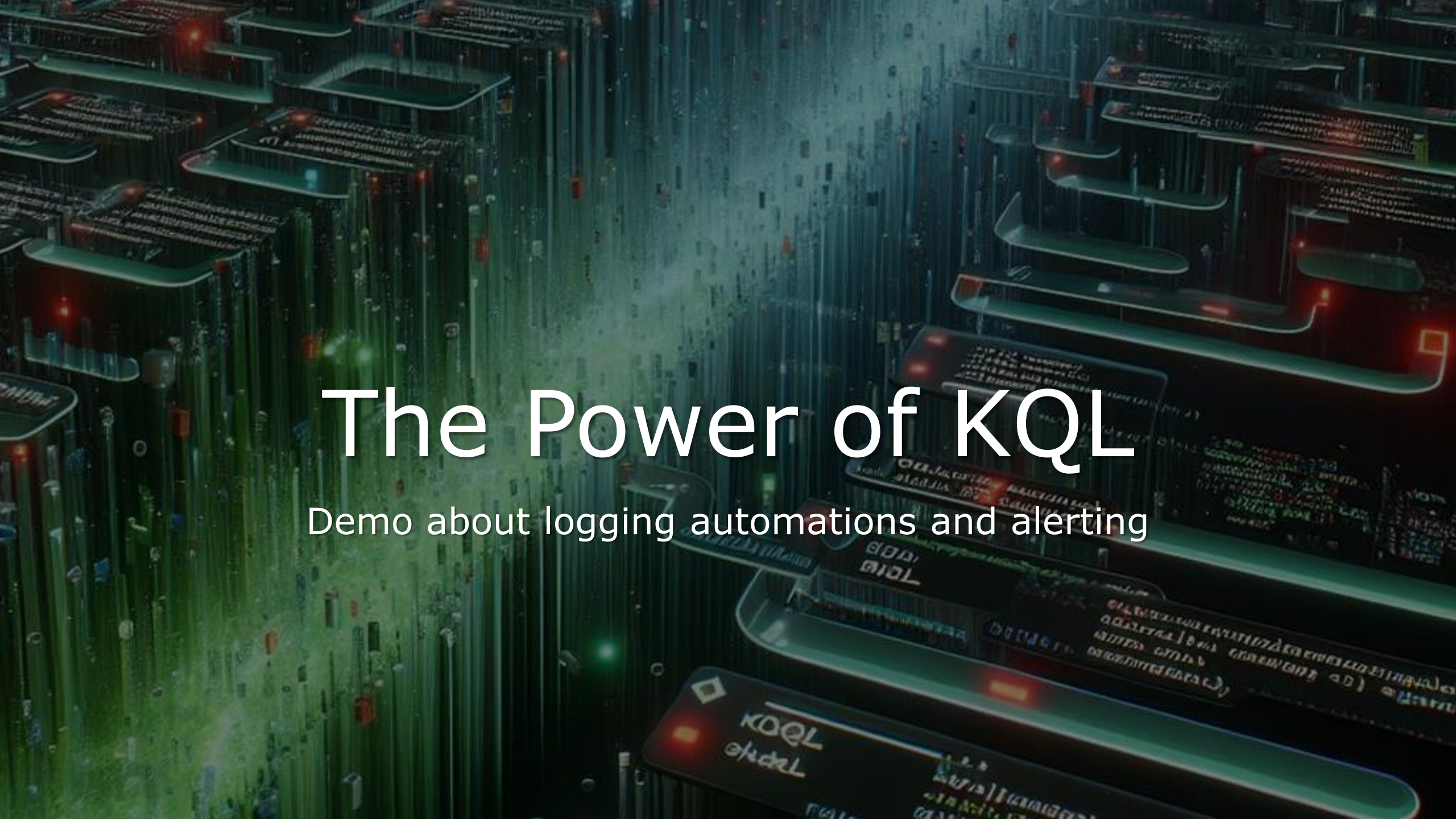
Can be still run on Local System or Custom Credential



No more Run As Accounts

- Run As accounts deprecated 2023-09-30
- Use System Managed Identities while doing Hybrid worker stuff towards Azure (or other Microsoft APIs)
  - the system-assigned managed identity for the Automation account
  - the virtual machine (VM) managed identity for an Azure VM running as a hybrid runbook worker
    - When you enable the Automation account's managed identity, it takes precedence, and you cannot override
- User-assigned identities are supported for cloud jobs only

Use separate automation accounts, if machine bound Managed Identities and Automation Account’s Managed Identity are needed



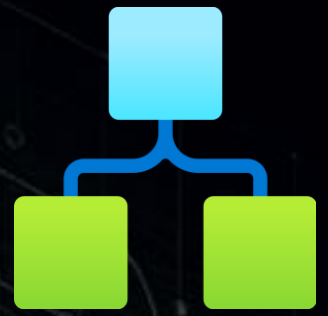
The Power of KQL

Demo about logging automations and alerting

Refactoring automation to more cloud native

Tools available

Logic App



- Process orchestrator – step motor
- Can be integrated with Azure Functions and Azure Automation account (and many more)
- Direct on-prem connectivity using on-prem data gateway

Azure Functions

- Serverless platform for running code – e.g. PowerShell
- Consumption based or provisioned capacity
- Connectivity to onprem by
  - Integrating App Service plan to vNet
  - Establishing connectivity to onPrem

Can be run on Azure Stack HCI – onPrem

Custom Script Extension

- Ability to run code from blob on machine
- Can be installed on Azure VM or Arc machine
- Very easy and powerful tool for mass automation

Lessons learnt from the field

Secure access to resources

Azure Owner permissions == ‘standing next to the server’

Use Just In Time, Just Enough Administration approach

Do we still need local admins, or could we only use Local System + Azure Audit logs?

Resource Graph

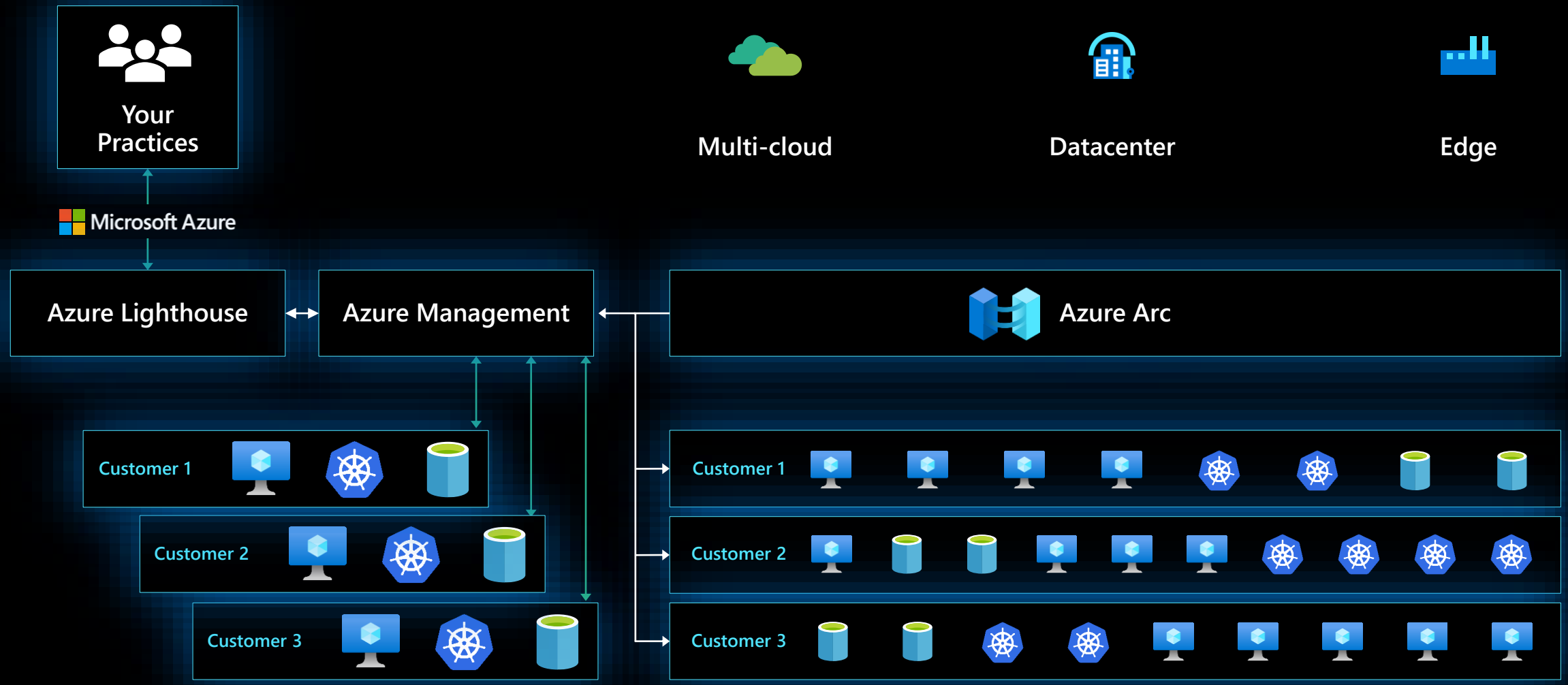
Ability to use KQL for querying resources

→ Faster than enumerating all servers with Get-VM

Can be queried from Azure Monitor to enrich alert data (tags, state etc.) → More meaningful events!

Azure Lighthouse and Azure Arc

Azure Arc extends Azure management, services, and Azure Lighthouse anywhere



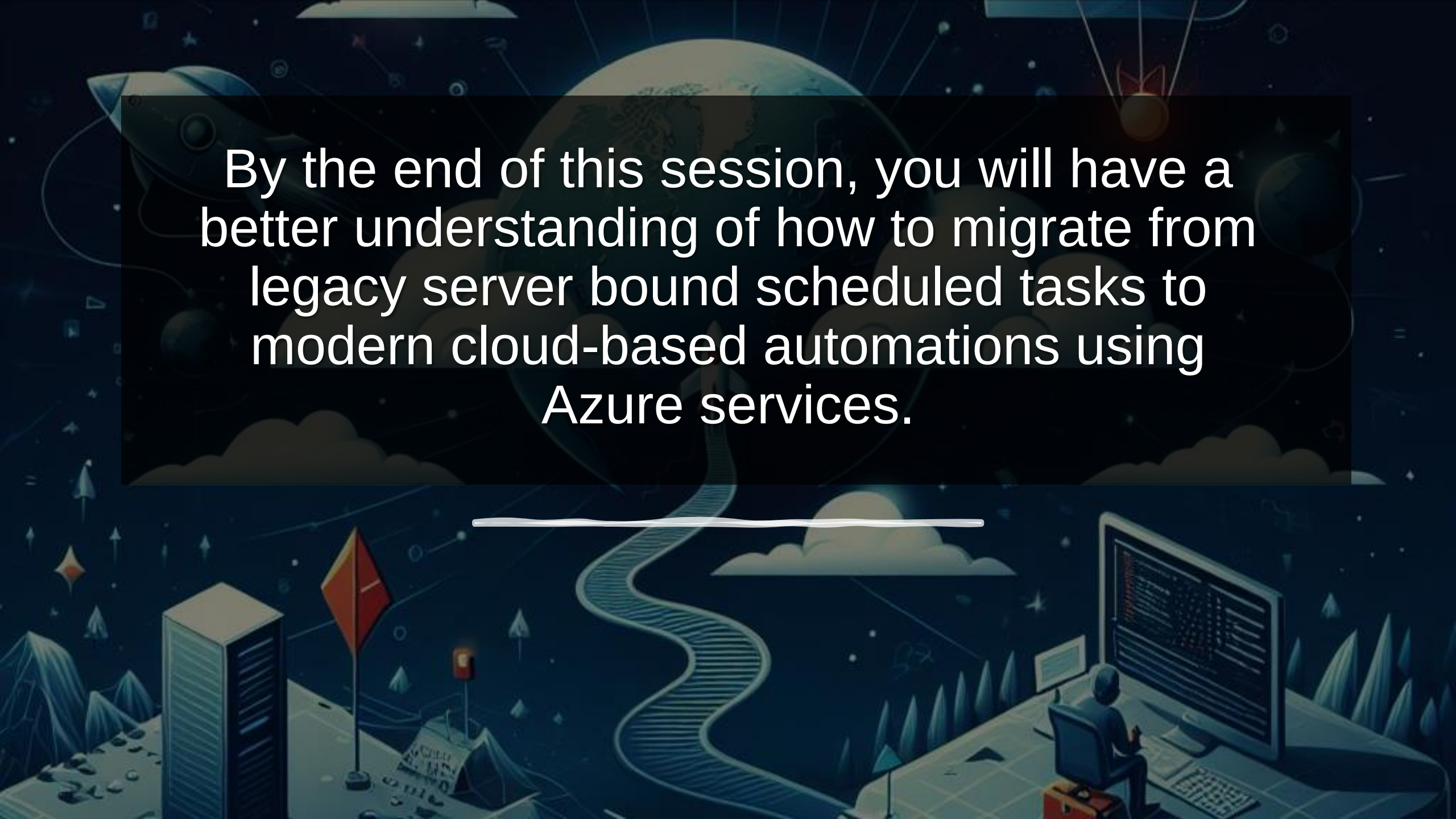
Manage multiple customers using Lighthouse, Resource Graph and Custom Script Extension

What to take home?

Arc enable everything and remember security

Azure Automate is the best way to consolidate your scripts and their logging

Use logic app to orchestrate complex automations


By the end of this session, you will have a better understanding of how to migrate from legacy server bound scheduled tasks to modern cloud-based automations using Azure services.


Q & A

Thank you!

Use event application for checking agenda and sharing photos!

https://bit.ly/cloudbrew-app

Please rate this session in the app!