Security in Azure Arc:

Simplify operations, management and security across distributed environments

Presented by:
Molina Sharma
Partner Solution Architect
LinkedIn Profile

Microsoft Azure

Agenda

1. Why Hybrid & Azure Arc Overview
2. Enhance your practice cover key Security Use Cases
3. Securing Azure Arc-enabled servers with Microsoft Defender for Cloud
4. Gain security insights from your Arc-enabled servers using Microsoft Sentinel
5. New Extended Security Updates enabled by Azure Arc
6. Best Practices for Hybrid Cloud Adoption
7. Next Steps and Q&A

Hybrid & Multi-Cloud Trends

Microsoft Azure

Cloud migration continues to be top of mind

82% of breaches involve human error[4]

Manage cyber risk and evolving compliance

45% of all IT spend will be on cloud by 2026[1]

Fully-managed services

90% of new apps will embed AI by 2025[2]

AI

#1 organizational initiative[5]

Offset costs, outmaneuver recessions

But…

100+ vendors and tools for an organisation[6]

Control cloud sprawl and tool proliferation

Innovate for the future

95% of new initiatives will be cloud-native by 2025[3]

Cloud-native

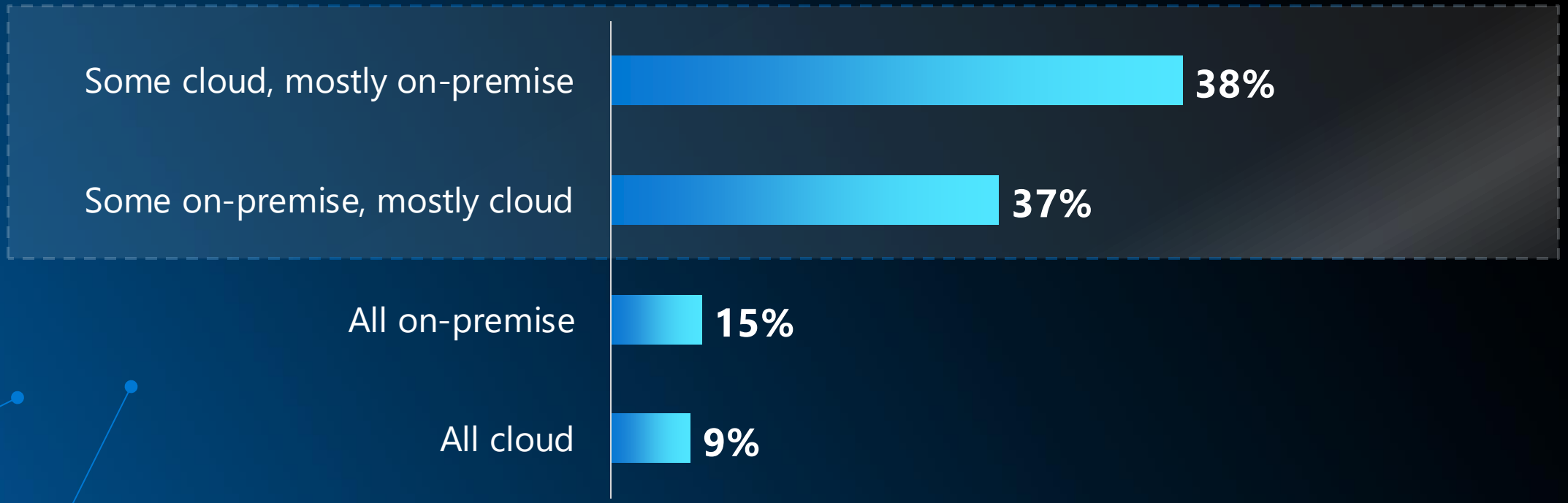
Microsoft Azure

1. Gartner Says Four Trends Are Shaping the Future of Public Cloud – Gartner, August 2021
2. IDC FutureScape Outlines the Impact "Digital Supremacy" Will Have on Enterprise Transformation and the IT Industry | Business Wire – IDC, October 2019
3. Gartner Identifies the Top Strategic Technology Trends for 2022 – Gartner, October 2021
4. 2023 Data Breach Investigations Report (DBIR) – Verizon, 2023
5. Flexera 2023 State of the Cloud Report
6. Going lean: How vendor consolidation creates big gains, MIT Technology Review, June 2020

Migration to Azure is the path to innovation

Microsoft Azure

Most enterprises are using a hybrid cloud approach



Foundry Cloud Computing Study, 2022 (EMEA)

Azure Arc Overview

> > > >

Microsoft Azure

Azure Arc

Public cloud

Azure

Use Azure services in public cloud with support for hybrid, edge, and multi-cloud resources enabled by Azure Arc

Azure Arc

Azure Arc-enabled infrastructure

Connect and operate hybrid resources as native Azure resources

Azure Arc-enabled services

Deploy and run Azure services outside of Azure while still operating it from Azure

Multi-cloud

Datacenter

Edge

Microsoft Azure

Unified operations and management across hybrid and multi-cloud

Secure, develop, and operate infrastructure, apps, and Azure services anywhere

Simplify operations and management

Leverage cloud-based threat detection

Integrated Role Based Access Control

Observability across the stack

Automated recovery from failures

Deliver cloud agility anywhere

Run Azure services on-premises

Low-latency for distributed compute

New and existing infra

Build cloud-native K8s apps

Ops-as-code

Transform operations with cloud and AI

Connect data from physical operations to the cloud to harness AI and insights

Automate site workflows across locations

Build reliable edge solutions with intermittent connectivity

Azure Arc

Amazon Web Services

Google Cloud Platform

Windows & SQL

3P Platforms

Azure Stack HCI

IoT Devices

Microsoft Azure

Azure Arc-enabled servers

Bring Azure capabilities to your on-premises and multicloud servers with Azure Arc

Reach

Windows and Linux

VM and bare metal

At scale searchable inventory

Configure

Consistent VM extensions

Centralized agent management - Monitoring, Security, Update Management

Govern

Built-in Azure policies

Compliance across environments

Audit and enforce OS settings

Secure

Azure Active Directory Managed Identity

Server security baselines

Role-Based Access control

Any infrastructure, familiar tools

Microsoft Azure

Azure hybrid data manageability for SQL Server

Manage, govern, and protect your SQL Server from Azure

Manage all your SQL estate using Azure

Single view of all SQL Servers deployed on-premises, in Azure and other cloud

Fully automated technical assessment for SQL Server – no additional

Control and govern your entire data estate

Central insights and governance across all SQL Servers with Microsoft Purview

Purview access policies readily available for SQL Servers on-premises

Protect all your data using Azure security

Protect your on-premises data using **Microsoft Defender** for Cloud

Secure identities with **Single Sign-On** and **Azure Active Directory**

Easy connection enabled by Azure Arc for existing SQL Servers without migration

*SQL Server 2022 required for Azure Active Directory. All other features supported on SQL Server 2012, 2014, 2016, 2017, and 2019.

Microsoft Azure

Azure hybrid data manageability for SQL Server

SQL Server on Arc-enabled servers

(powered by Azure Arc server agent)

Organize, inventory

Microsoft Defender for advanced security

Free SQL Assessment service

No migration needed

Azure Arc-enabled SQL Managed Instance

(powered by Azure Arc data controller)

Azure SQL Managed Instance

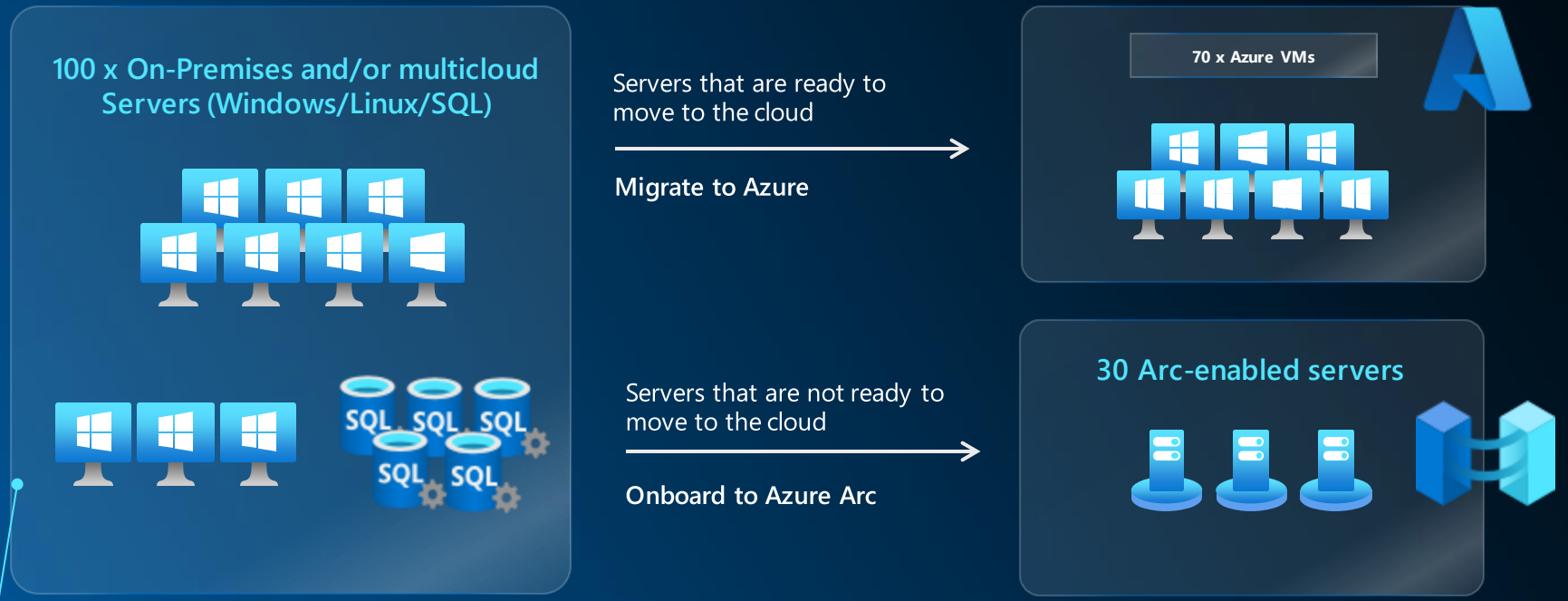
on any infrastructure

PaaS-like, evergreen SQL Server

Cloud billing model for on-premises

Migrate and Modernize to Azure on your own terms

Azure Arc helps you consistently secure and govern infrastructure across hybrid environments as you migrate and modernize



Turn on Azure security, monitoring and governance services for all servers **no matter where you are in the migration journey**

- Microsoft Defender for Cloud
- Microsoft Sentinel
- Azure Policy
- Azure Monitor

Microsoft Azure

Arc-enabled SQL Server with cloud data manageability

Manage, govern, and secure your SQL Server from Azure

Manage all your SQL estate via Azure Arc

- **Single view** of all SQL Servers deployed on-premises, in Azure and other cloud
- **Fully automated technical assessment** for SQL Server – no additional cost

Control and govern your entire data estate

- **Central insights and governance** across all SQL Servers with Microsoft Purview
- Purview access policies readily available for SQL Servers on-premises

Secure all your data using Azure security

- Protect your on-premises data using **Microsoft Defender** for Cloud
- Secure identities with **Single Sign-On** and **Azure Active Directory***

Easy connection enabled by Azure Arc for existing SQL Servers without migration

**SQL Server 2022 required for Azure Active Directory. All other features supported on SQL Server 2012, 2014, 2016, 2017, 2019, 2022, under L+SA or PAYG*

Securing Azure Arc-enabled servers with Microsoft Defender for Cloud

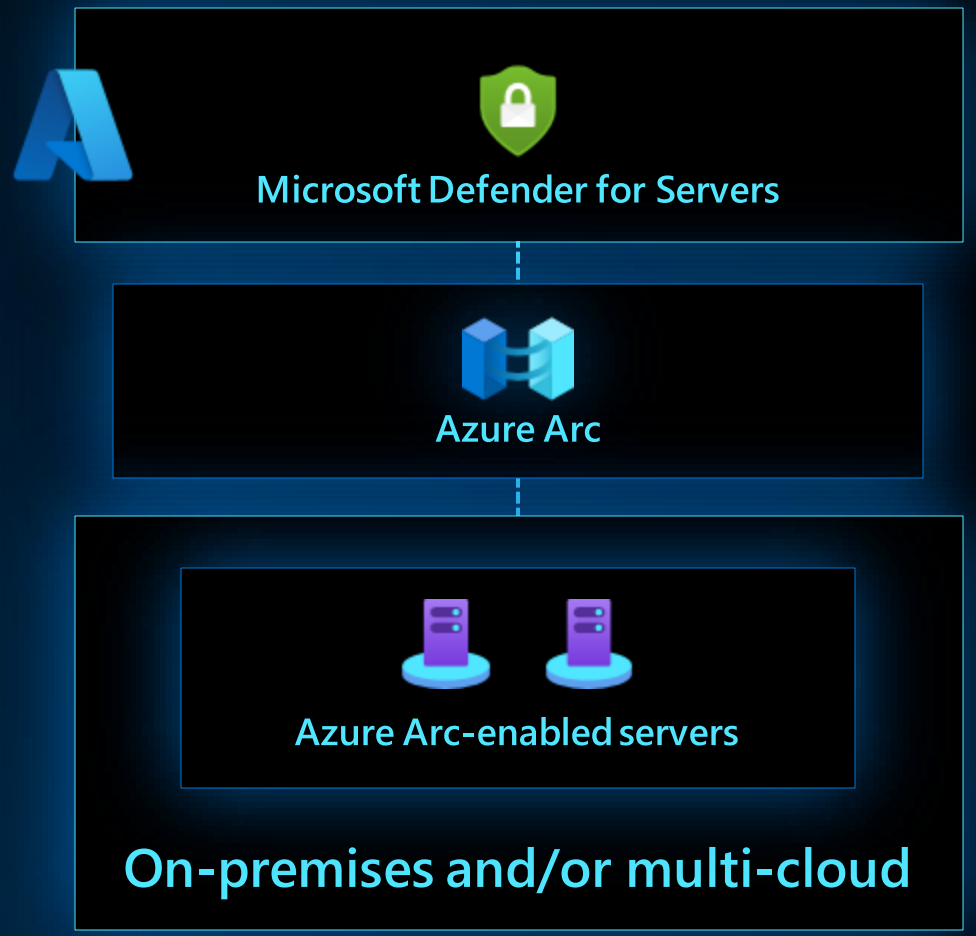
Microsoft Defender for Cloud

Assess, secure, and defend your hybrid and multicloud workloads

- **Continuously assess.** Understand your current security posture, identify and track vulnerabilities. Get a bird's eye-view of your security posture with Secure Score
- **Secure**. Harden connected resources and services by following customized and prioritized recommendations with Azure Security Benchmark
- **Defend**. Detect and resolve threats to those resources and services. With prioritized **security alerts**, focus on what matters the most and surface to the right audience

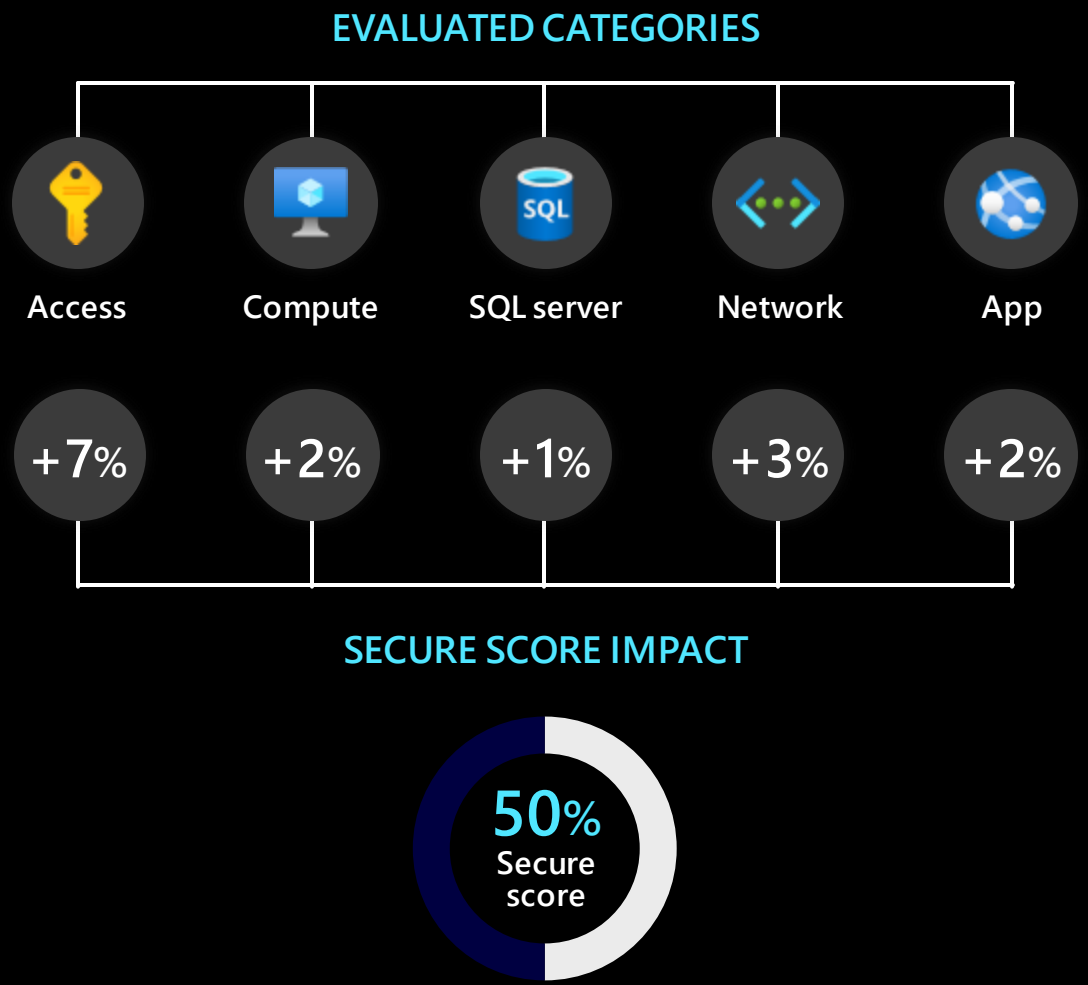
Deploy Defender for Servers anywhere

- Easily deploy as extensions in Azure without re-installing agents
- Vulnerability assessment built-in with flexibility to use tools like Qualys offering integrated vulnerability scanning for your connected machines
- Use Just-in-Time VM access to control access to commonly attacked management ports
- Block malware with adaptive application controls
- Set guardrails with Azure Policy integration, server owners can view and remediate to meet their compliance



Continuous assessment and Security posture management

- Gain insights into the security state of your cloud workloads across Azure, AWS, and GCP
- Address security vulnerabilities with prioritized recommendations
- Improve your secure score and overall security posture in minutes
- Speed up regulatory compliance
- Granular control of secure score



Secure with tailored recommendations

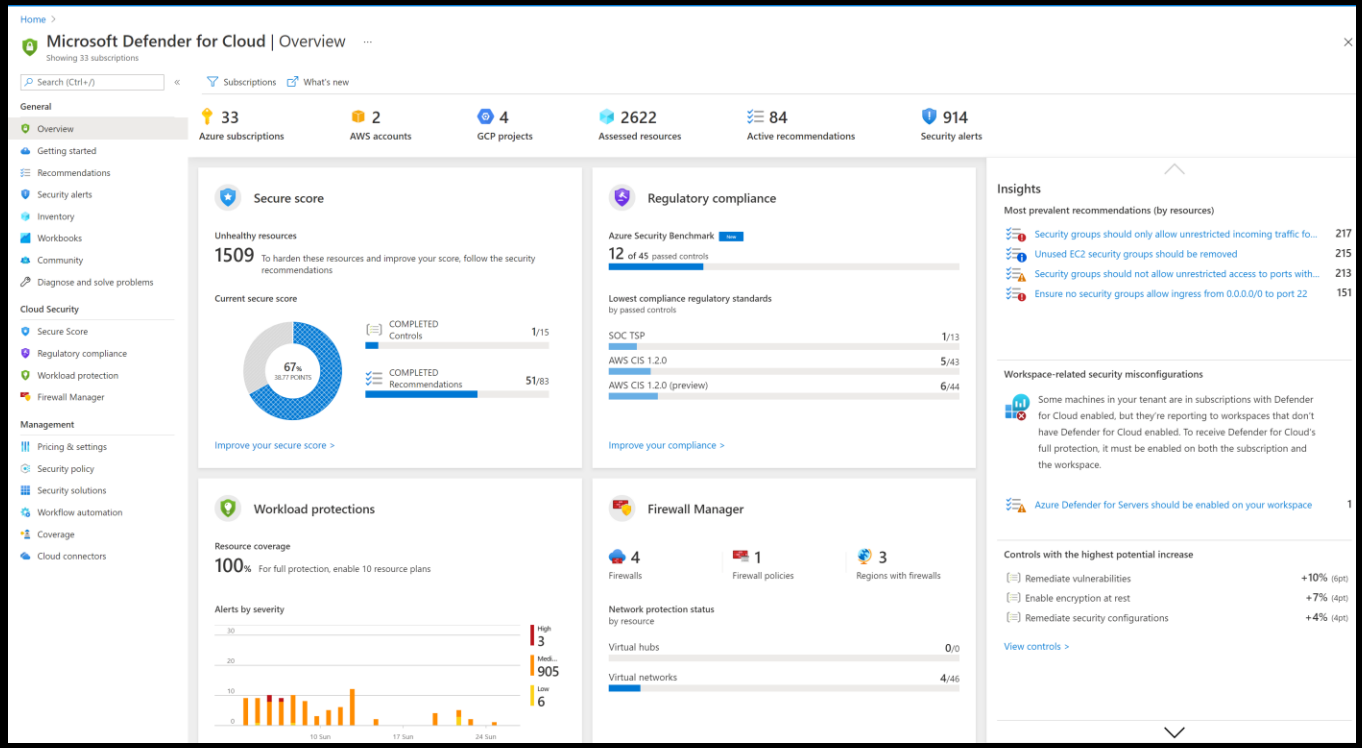
Unified resource view

- All your cloud resources in one place: Azure, AWS, on-premises, and other clouds
- Focused views for security posture, compliance, and workload protection

Clear & simple view

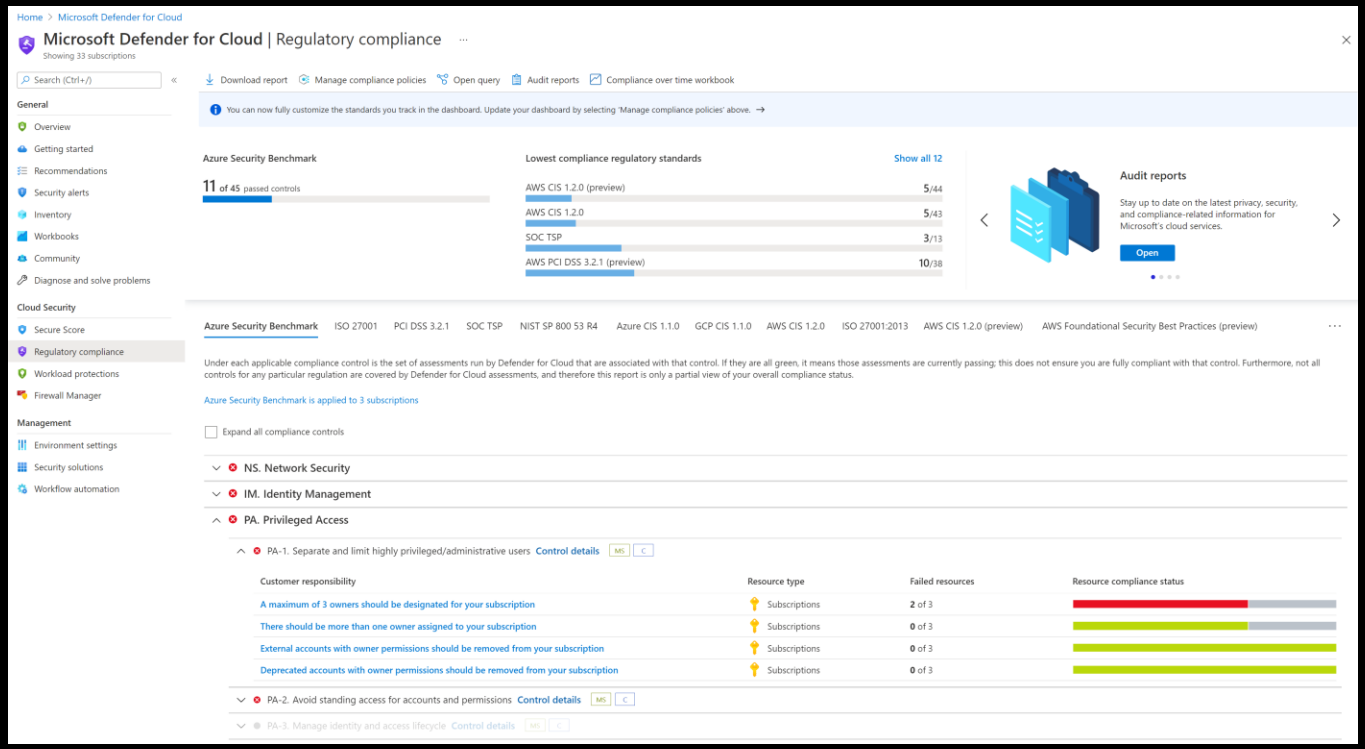
- Identify all your security related stats at a glance

Emphasis on visibility & clear KPIs



Compliance assessment and governance

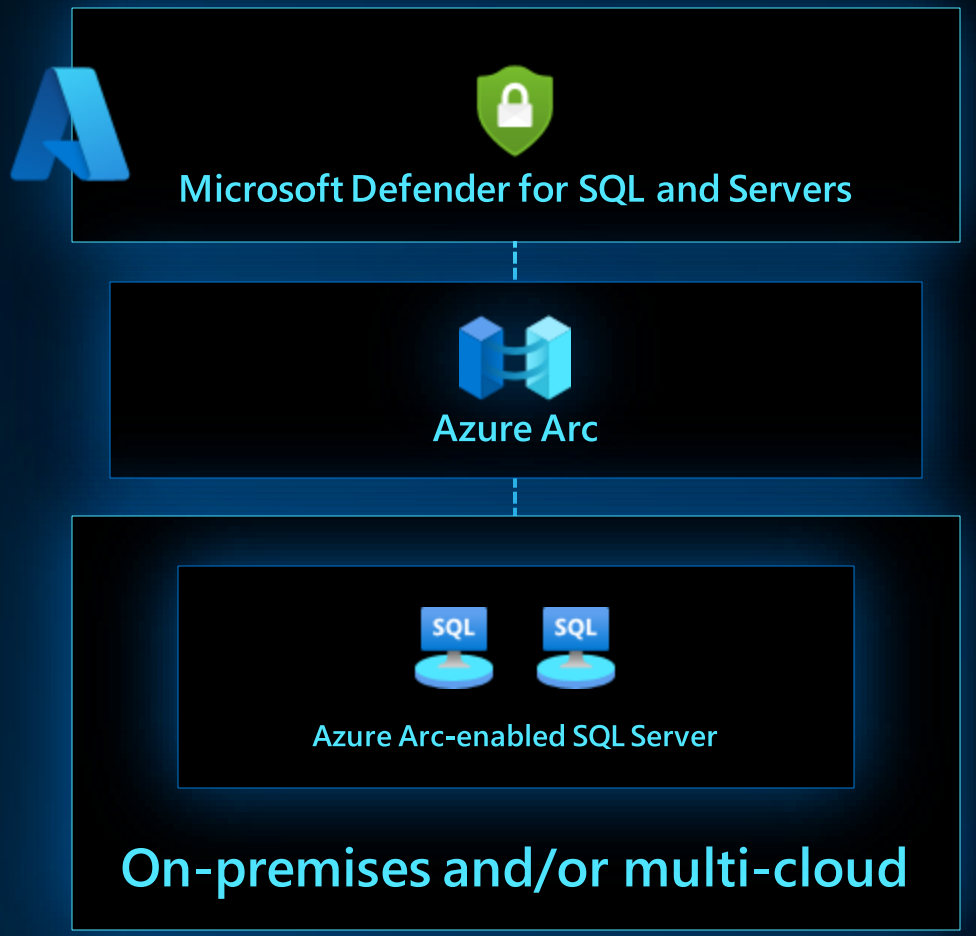
- Demonstrate compliance status, based on continuous assessments of your Azure and AWS resources
- Azure Security Benchmark monitoring enabled by default
- Mapped to the MITRE ATT&CK® framework
- Support for common industry and regulatory standards, as well as custom requirements
- Overview and reports of your compliance status



Microsoft Defender for Cloud – database protection

Comprehensive database protection with Microsoft Defender for Cloud

- Continuously assess, secures, and hardens your hybrid and multi-cloud SQL server estate against vulnerabilities and threats
- Deploy **Defender for SQL** and **Defender for Servers** at scale to protect your Arc-enabled SQL Server estate
  - ✓ Vulnerability assessment scanning
  - ✓ Built-in Recommendations
  - ✓ Advanced threat protection
- Remediate potential vulnerabilities with point and click fixes or detailed guidance
- Incident management and threat intelligence through integration with Microsoft Sentinel/external SIEM

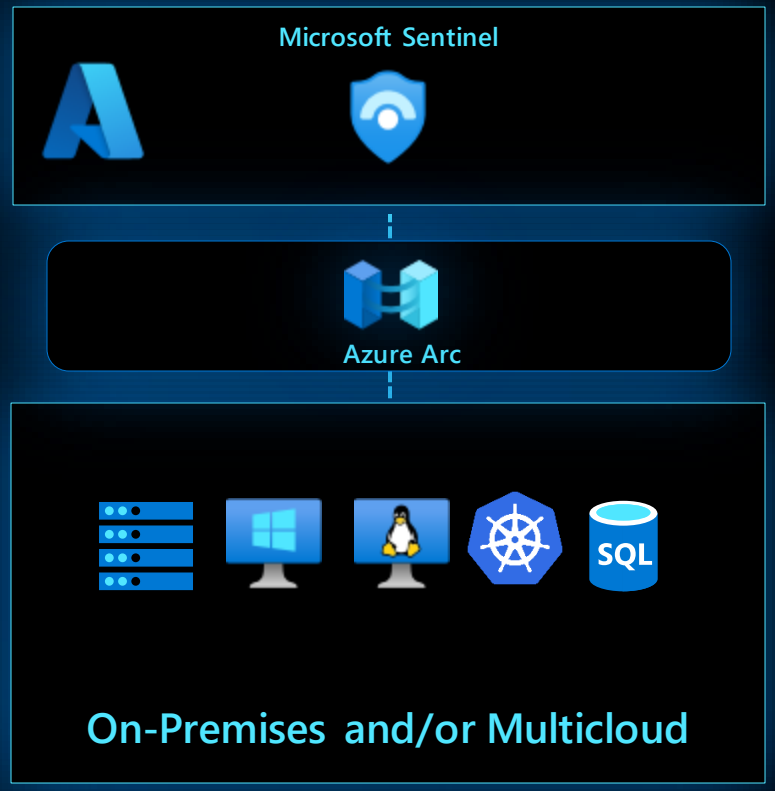


Gain security insights from your Arc-enabled servers using Microsoft Sentinel

Microsoft Sentinel

Intelligent, scalable, and cloud native SIEM and SOAR solution.

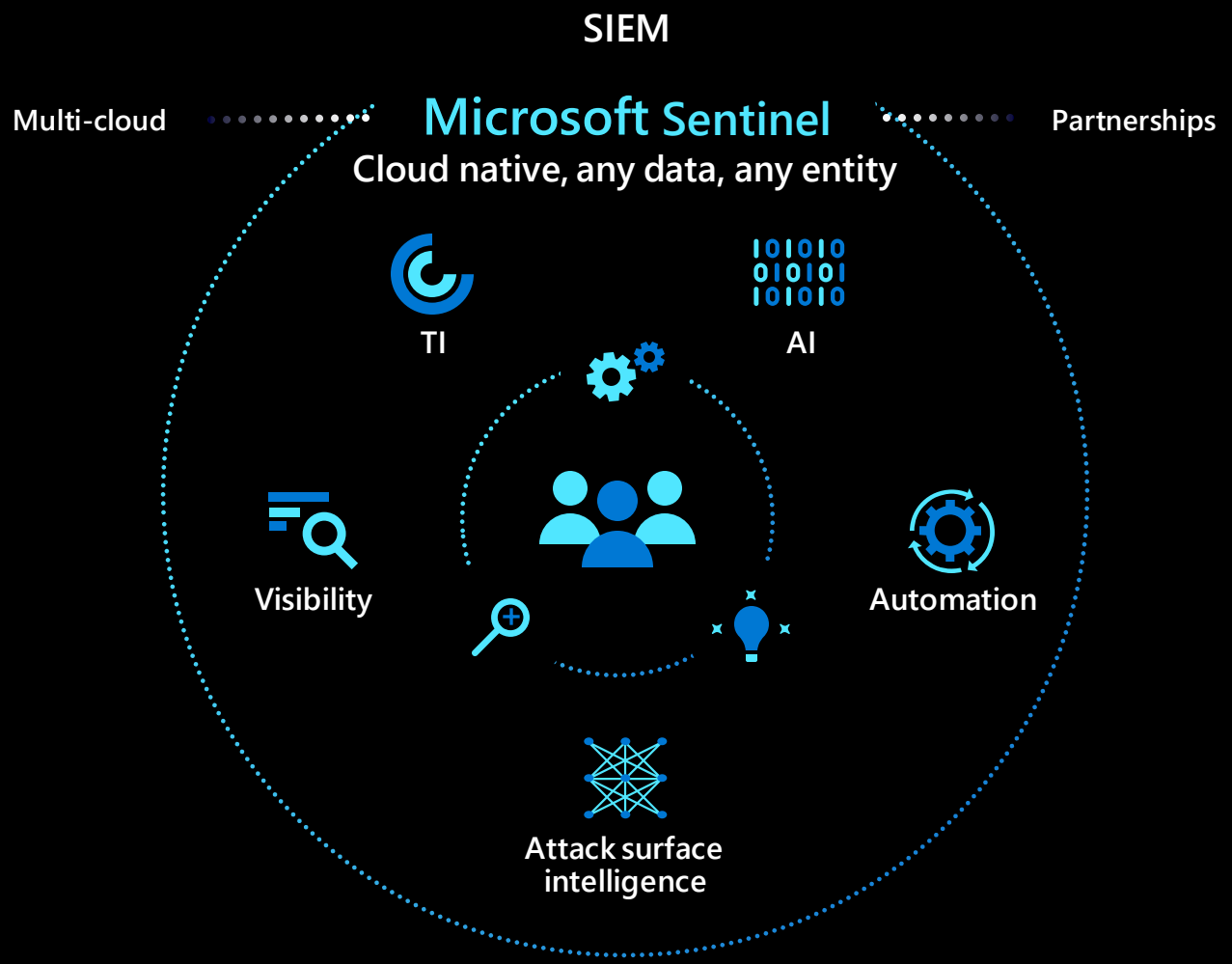
- **Collect** data at cloud scale—across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds
- **Detect** previously uncovered threats and minimize false positives using analytics and threat intelligence from Microsoft
- **Investigate** threats with AI and hunt suspicious activities at scale, tapping into decades of cybersecurity work at Microsoft
- **Respond** to incidents rapidly with built-in orchestration and automation of common tasks



Gain insights across your entire enterprise

First cloud-native SIEM on a major cloud platform, with over 9,000 customers

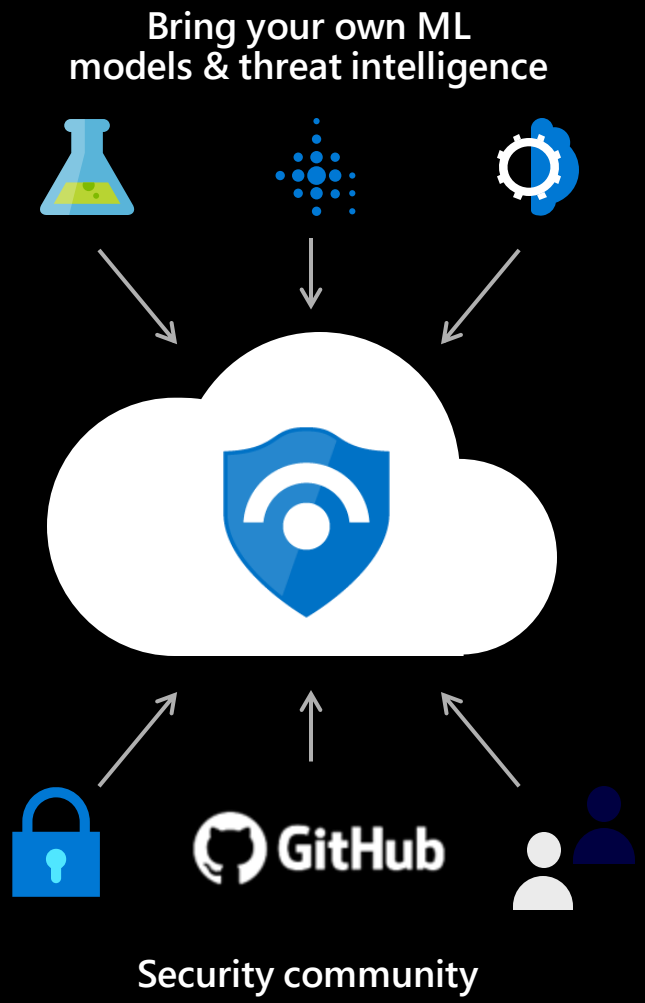
- Collect security data at cloud scale and integrate with your existing tools
- Leverage AI to detect emergent threats, reducing false positives by 79% over three years[1]
- Respond rapidly with built-in orchestration and automation



1: Commissioned study-The Total Economic Impact™ of Microsoft Azure Sentinel, conducted by Forrester Consulting, 2020

Optimize for your needs

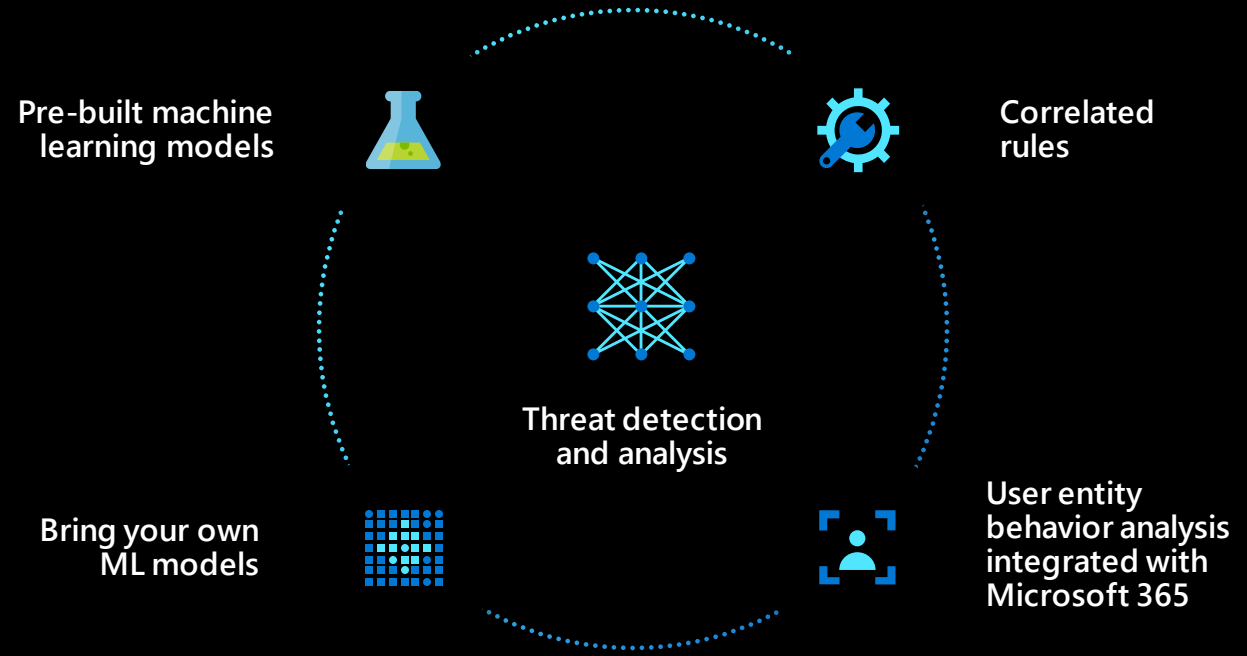
- **Bring your own insights,** machine learning models, and threat intelligence
- Tap into our **security community** to build on detections, threat intelligence, and response automation



Detect threats and analyze security data quickly with AI

- ML models based on **decades of Microsoft security experience and learnings**
- Millions of signals filtered to few **correlated and prioritized incidents**
- Insights based on vast **Microsoft threat intelligence** and your own TI

Reduce alert fatigue by up to 90%



Enhance your practice cover key Security Use Cases

Key Security use cases	Solution capabilities	Value to the customer
Security posture management and threat protection	**Microsoft Defender for Clou**d protects non-Azure workloads against evolving threats. You will be able to understand vulnerabilities with insights from industry-leading security research and secure your critical workloads against threats. Use many options to automate and streamline your security administration from a single place. **Secure Score** helps you understand and improve your current security posture.	• Understand your current security posture across hybrid and multicloud environments. • Security recommendations aligned to key industry and regulatory standards • Prioritized hardening tasks to improve overall security posture across hybrid and multicloud resources. • Reduce security management overheads across multiple clouds/platforms.
Comprehensive security visibility across the enterprise for detection, proactive hunting and threat response.	**Microsoft Sentinel** on Arc-enabled servers and Kubernetes delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for attack detection, threat visibility, proactive hunting, and threat response.	• Collect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds. • Detect previously undetected threats and investigate them with AI built-in and hunt for suspicious activities at scale. • Respond to incidents rapidly with built-in orchestration and automation of common tasks.
Enforcing security compliance across multiple clouds and on-premises	**Regulatory Compliance** in Azure Policy provides security governance across hybrid and multicloud resources, with several built-in security controls.	• Simplified governance at scale for all resources – Automated guardrails and checks to ensure that all resources stay secured and compliant.
Identity and access control across hybrid and multicloud	Use managed identities with Azure Arc-enabled servers with Azure AD (Active Directory) and manage access controls with Azure role-based access control (RBAC)	• With Azure AD and RBAC, customers can simplify identity and access management with cloud-based controls. • They can decide who should manage Arc-enabled servers, remove any local access if needed, and provide access to the system in the Azure Portal.
Increased costs with : • Multiple security tools for on-premises and multiple public clouds. • Training internal employees to use disparate tools. • Maintenance.	Azure Arc enables a single pane of glass for security management across the customer's environment. With Arc, customers can extend Azure security tools and services they are familiar with, to on-premises and multicloud environments.	• Consistent way to monitor and protect resources across the entire IT landscape. • Reduced costs with standardization on a simple interface and set of tools. Employees can get skilled with cloud native practices and use them anywhere. • Less management overhead with adoption of cloud native security services.

New Options for Extended Security Updates

Microsoft Azure

Lifecycle management timelines

July 9, 2022

SQL Server 2008, 2008 R2 Extended Security Updates end

July 12, 2022

SQL Server 2012 End of Support

July 12, 2023

Extended Security Updates for SQL Server 2012 enabled by Azure Arc available for Year 2

SQL Server 2008 and 2008 R2 Extended Security Updates on Azure come to an end

October 10, 2023

Windows Server 2012 and 2012 R2 End of Support

July 9, 2024

SQL Server 2014 End of Support

Asses your options for EOS workloads

Modernize on Azure

Modernize with Azure App Service and Azure SQL Managed Instance to avoid end of support and always stay up-to-date

Upgrade your OS version while migrating with Azure Migrate

Offload cloud management to focus on delivering innovative apps and customer experiences

Migrate for free to ESUs[1]

Get 3 additional years of Extended Security Updates at no cost

Save even more when combined with Azure Hybrid Benefit

Cost efficient consumption models with Reserved Instances and Azure Savings Plan

New: Deploy ESUs enabled by Azure Arc[2]

Flexible, monthly billing model centralized in Azure

Purchase Extended Security Updates enabled by Azure Arc for seamless and automated patching

Extend Azure operations and management to hybrid and multicloud environments

Enhance protection with cloud-native security solutions with Microsoft Defender for Cloud

[1]Includes Azure VMs, Dedicated Host, Azure VMware Solution, Nutanix Cloud Clusters on Azure, and Azure Stack (HCI/Hub/Edge)
[2]Server or operating system license eligibility requirements apply.

Microsoft Azure

Technical benefits of Azure Arc Enabled ESUs

Flexible billing and savings

Monthly billing model centralized in Azure to run end-of-support operating systems

Visibility and reliability

Ensure consistent Windows Server 2012/R2 and SQL Server 2012 performance with high availability and visibility over your entire data and server estate. Keyless delivery.

Security and compliance

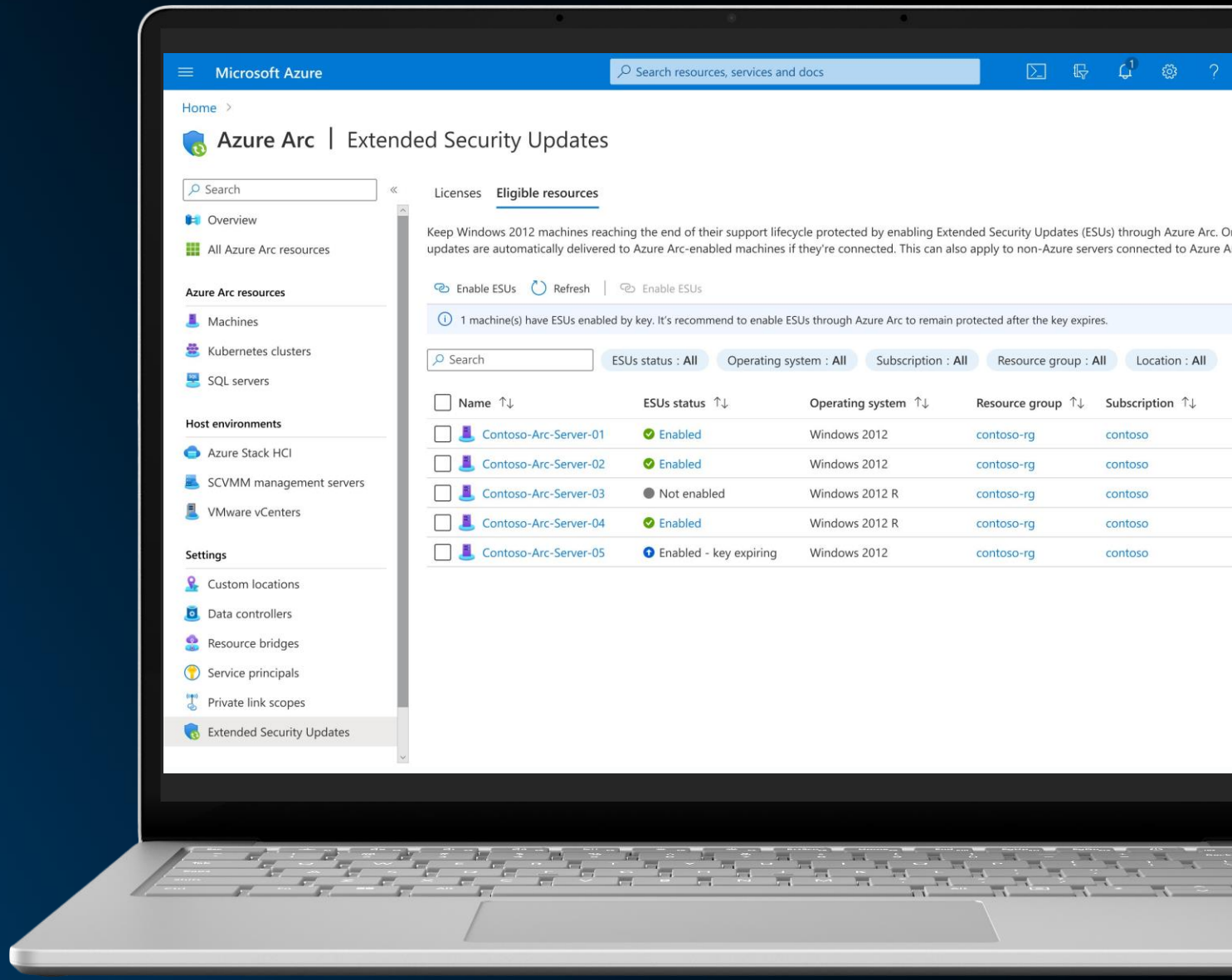
Seamlessly extend Azure security and governance to your environment and stay compliant with supported software

Microsoft Defender for Cloud

Microsoft Sentinel

Azure Policy

Azure Monitor



Enroll and purchase ESUs directly in the Azure Portal

Microsoft Azure

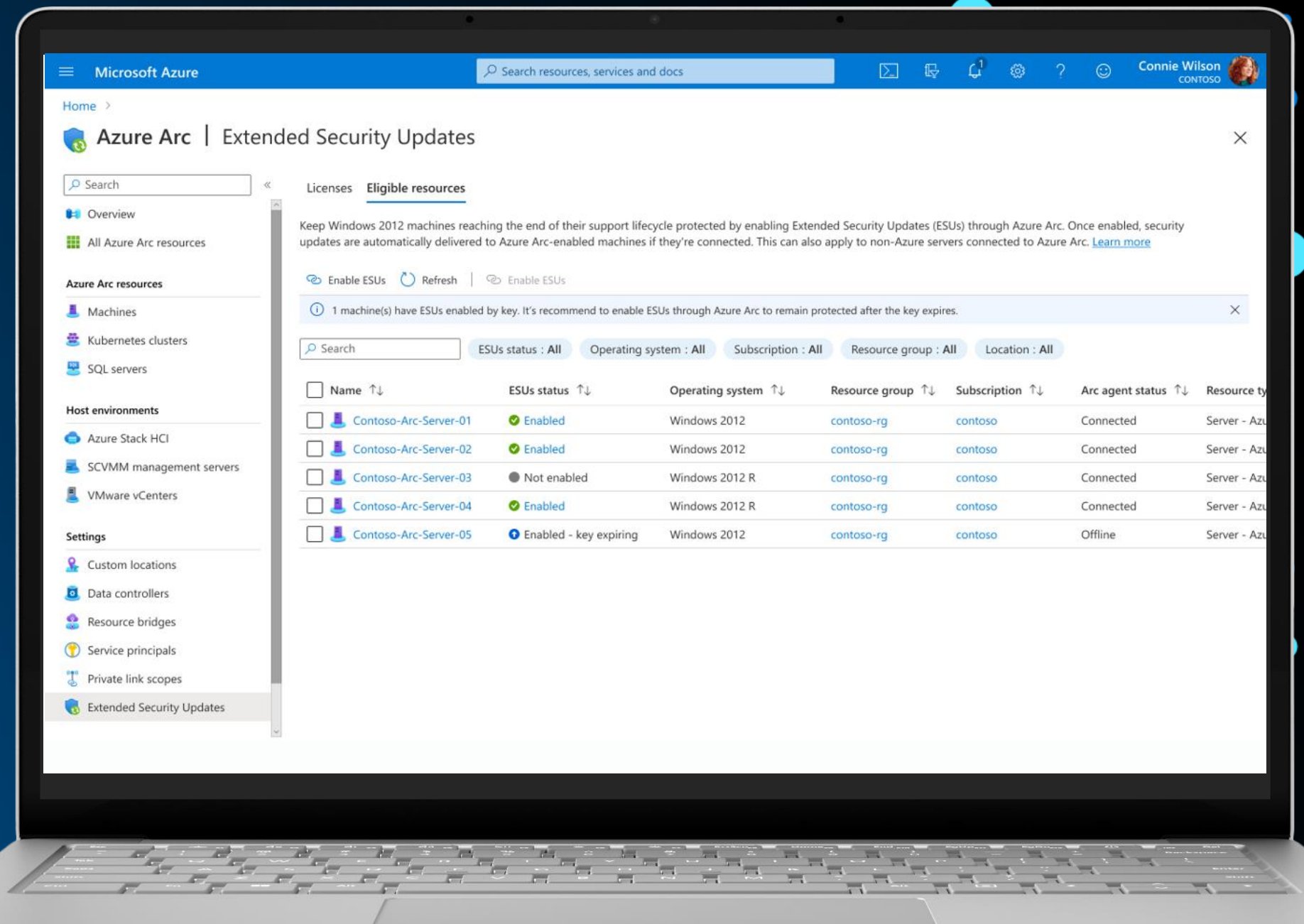
Demo

Extended Security Updates Enabled by Azure Arc

> > > >

Microsoft Azure

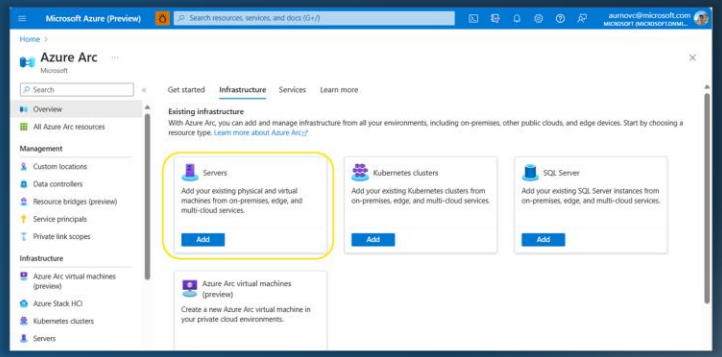
Azure Arc Extended Security Updates Demo



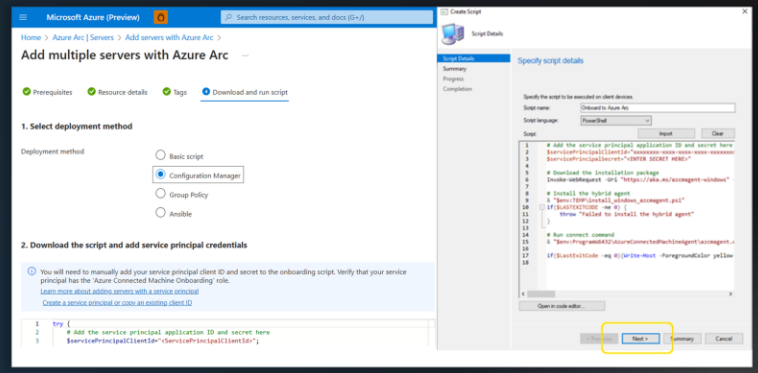
Microsoft Azure

Get ESU for Windows Server through Azure portal here.

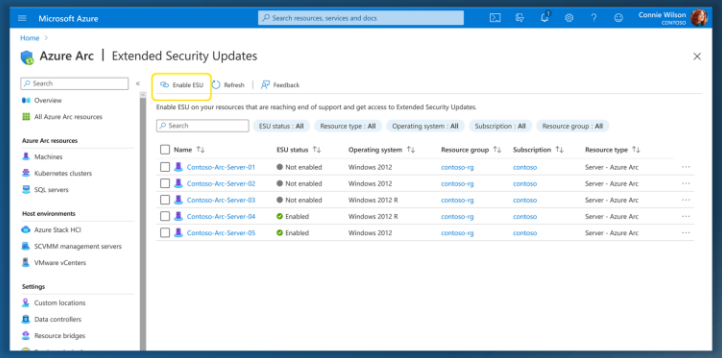
Step 1: Go to the Azure Arc blade in the Azure Portal and begin onboarding servers to Azure Arc by clicking 'Servers'.



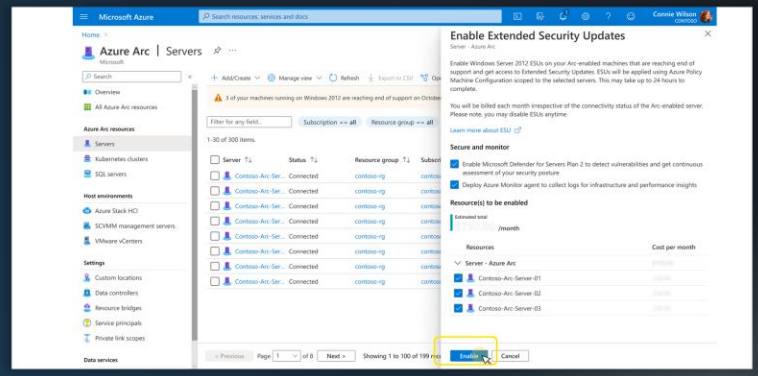
Step 2: Onboard servers Azure Arc by downloading the Azure Connected Machine Agent and install the agent using SCCM, PowerShell or your tool of choice



Step 3: View Windows Server inventory for servers both enabled and not enabled with ESUs via 'ESU Status'.



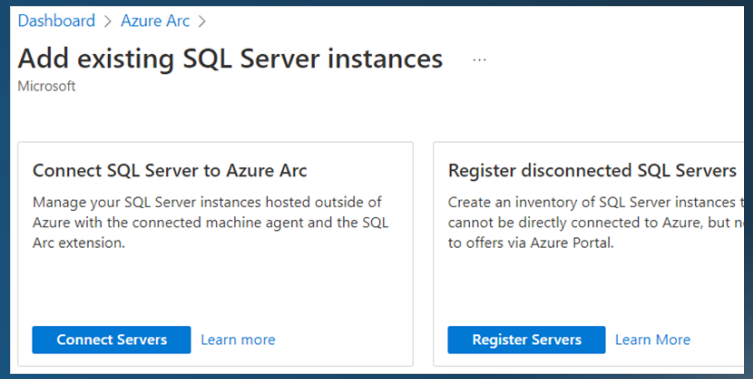
Step 4: Activate ESUs through the Azure portal through the assignment of an Azure Policy. Additionally, add Microsoft Defender for Cloud and Azure Monitor.



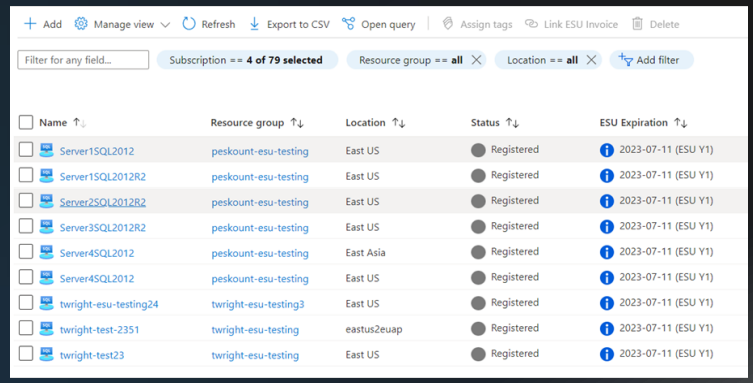
Microsoft Azure

Get ESU for SQL Server through Azure portal here.

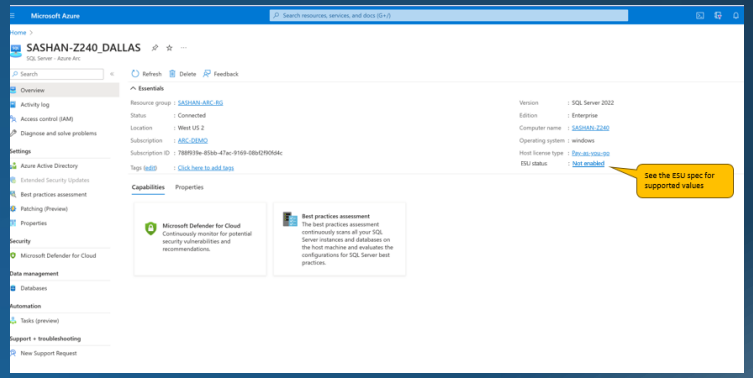
Step 1: Connect and register customer options.



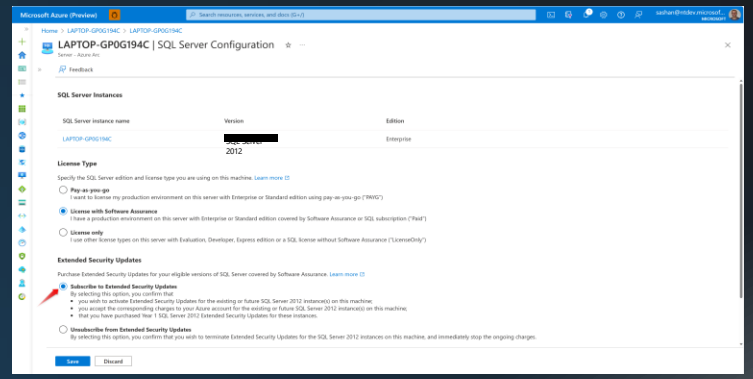
Step 2: View SQL inventory for both connected and registered SQL instances



Step 3: Drill into ESU options



Step 4: Subscribe to Extended Security Updates



Microsoft Azure

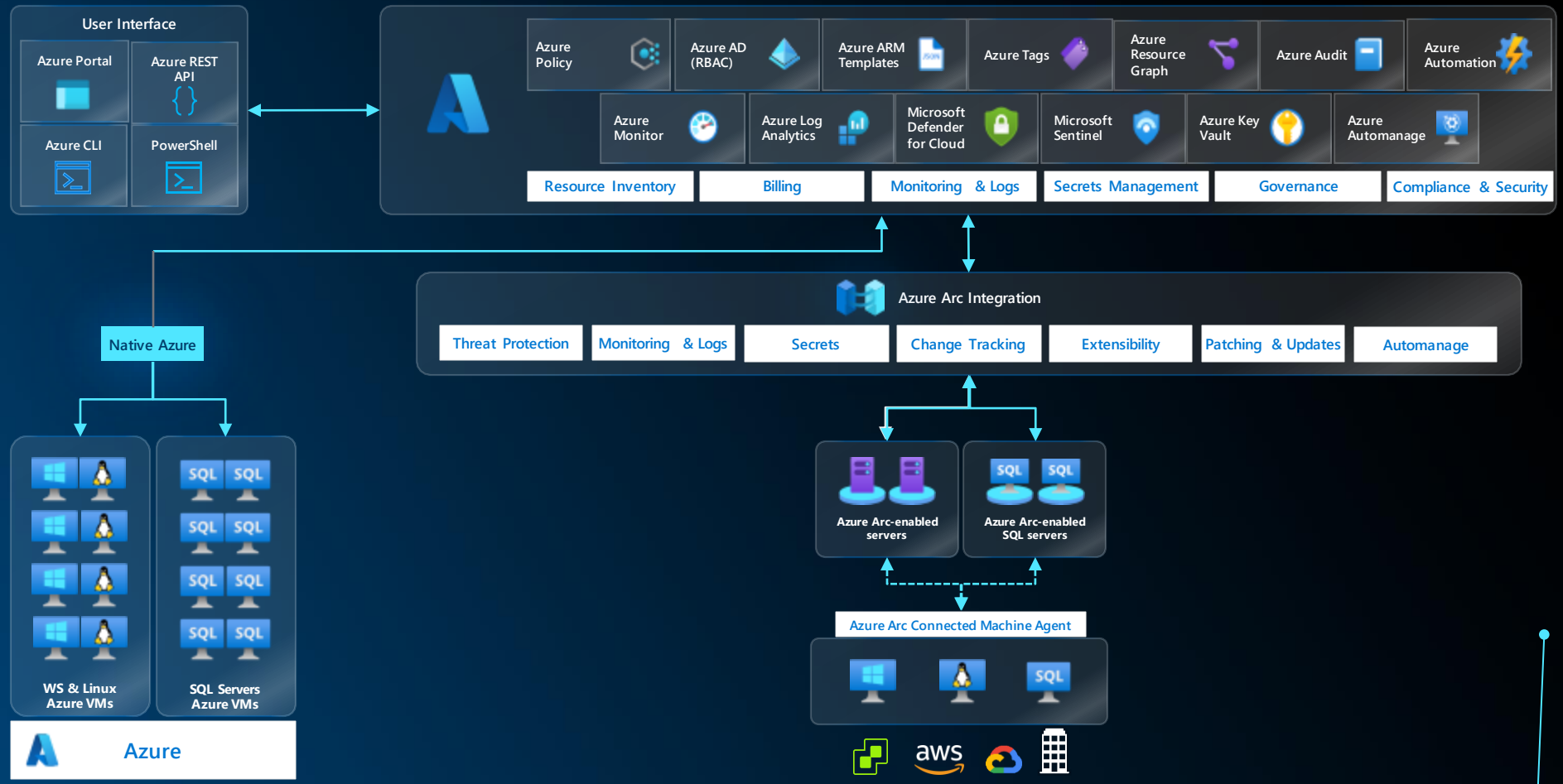
Best Practices for Hybrid Cloud Application

> > > >

Microsoft Azure

Azure Arc-enabled servers & Azure Arc-enabled SQL server

On-premises and multi-cloud integration



Microsoft Azure

Complete guidance for hybrid and multicloud approach

Build skills across your team with **Microsoft Learn**

Accelerate deployment with **Reference Architectures**

Optimise workloads with **Azure Well-Architected**

Apply **best practices** to rapidly onboard

Review **technical documentation** on featured products

https://aka.ms/ArcLZAcceleratorReady

Start with the cloud adoption framework to guide your cloud journey and build on it using the hybrid adoption scenario guidance

Microsoft Azure

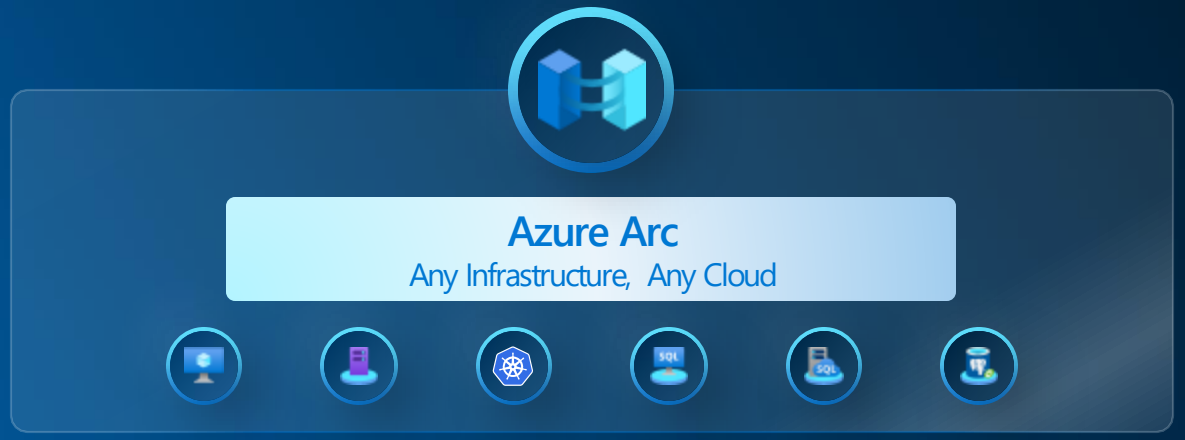
Next steps

Onboard your non-Azure resources to Azure Arc. Use the Azure Arc Jumpstart to get going with ease.

Secure and protect your Arc-enabled resources by enabling Microsoft Defender for Cloud and Microsoft Sentinel.

Get best practices and guidance with the landing zone accelerator for Azure Arc

Learn More



Azure Arc Jumpstart:
https://aka.ms/AzureArcJumpstart

Technical documentation:
https://aka.ms/AzureArcDocs

Azure Arc Learning Path:
https://aka.ms/AzureArcLearn

Azure Arc Learning Companion:
https://aka.ms/pathways

Azure Arc ESU Docs:
https://aka.ms/arcesudocs

Azure Arc Total Economic Impact Report:

https://aka.ms/arcforresterstudy

Thank you!

Q&A

Microsoft Azure