

# Security in Azure Arc:

Simplify operations, management  
and security across distributed  
environments

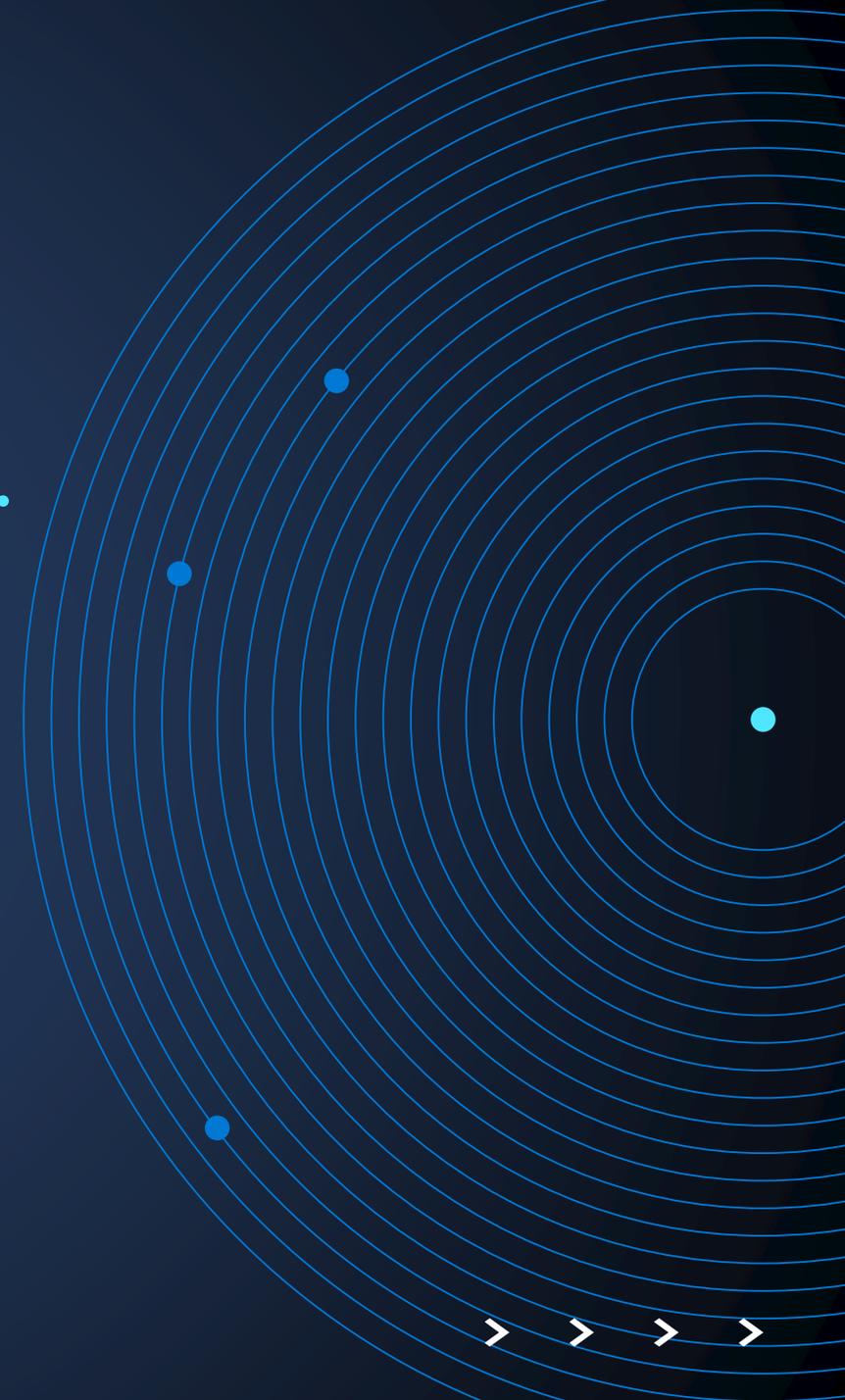
> > > >

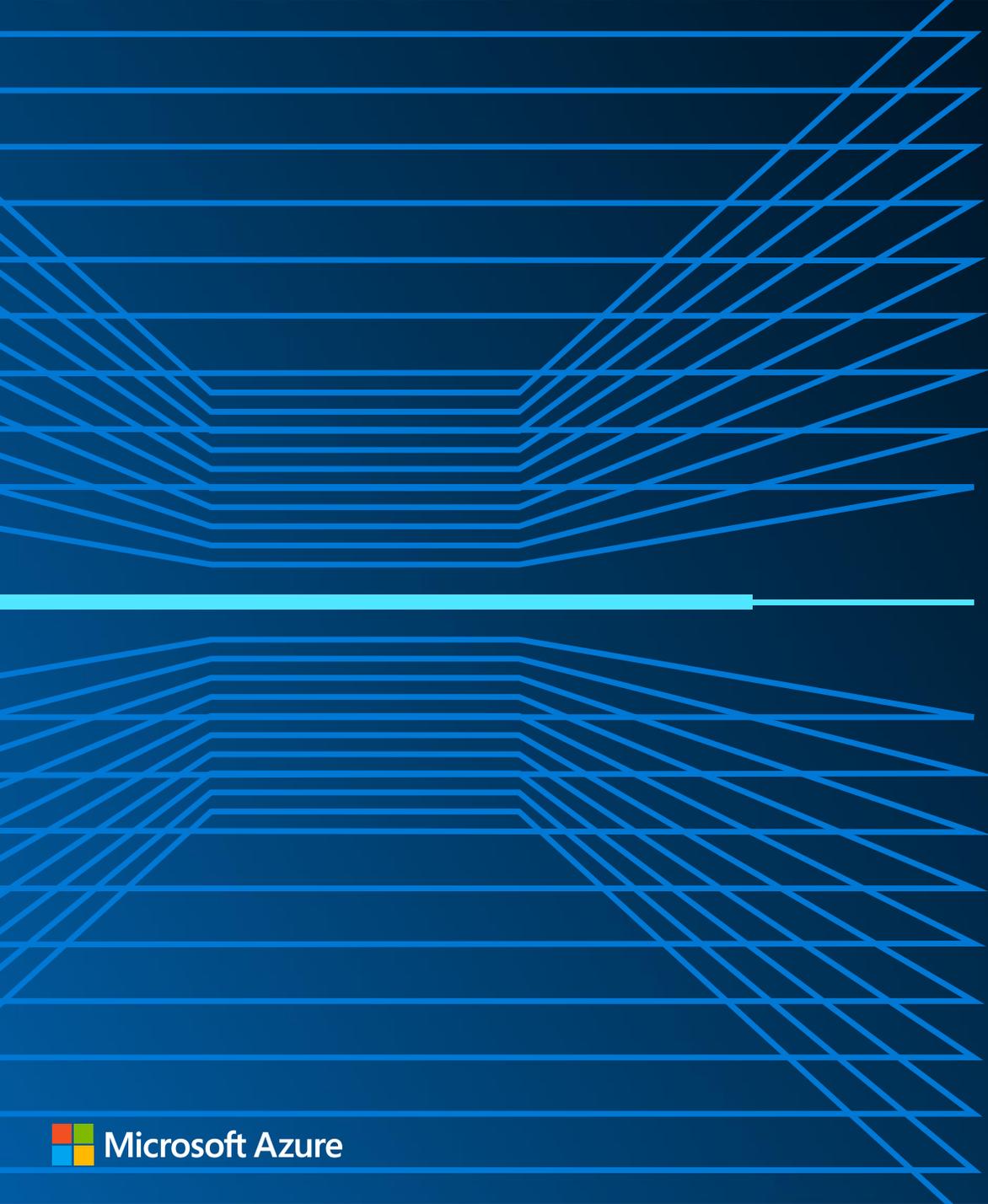


Presented by:  
Molina Sharma  
Partner Solution Architect  
[LinkedIn Profile](#)

# 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



The background of the slide features a complex pattern of blue lines. On the left side, there are several horizontal lines that transition into a series of lines that fan out and curve towards the right, creating a sense of depth and movement. A single, thicker horizontal line is positioned across the middle of the page, intersecting the fanning lines.

# Hybrid & Multi-Cloud Trends

> > > >

82%

of breaches involve human error<sup>4</sup>



Manage cyber risk and evolving compliance

45%

of all IT spend will be on cloud by 2026<sup>1</sup>

Fully-managed services

90%

of new apps will embed AI by 2025<sup>2</sup>

AI

# Cloud migration continues to be top of mind

## But...

#1

organizational initiative<sup>5</sup>



Offset costs, outmaneuver recessions

100+

vendors and tools for an organisation<sup>6</sup>



Control cloud sprawl and tool proliferation



Innovate for the future

95%

of new initiatives will be cloud-native by 2025<sup>3</sup>

Cloud-native

Migration to Azure  
is the path to innovation



Maximize  
ROI



Unmatched performance  
and resilience



Comprehensive code  
to cloud security



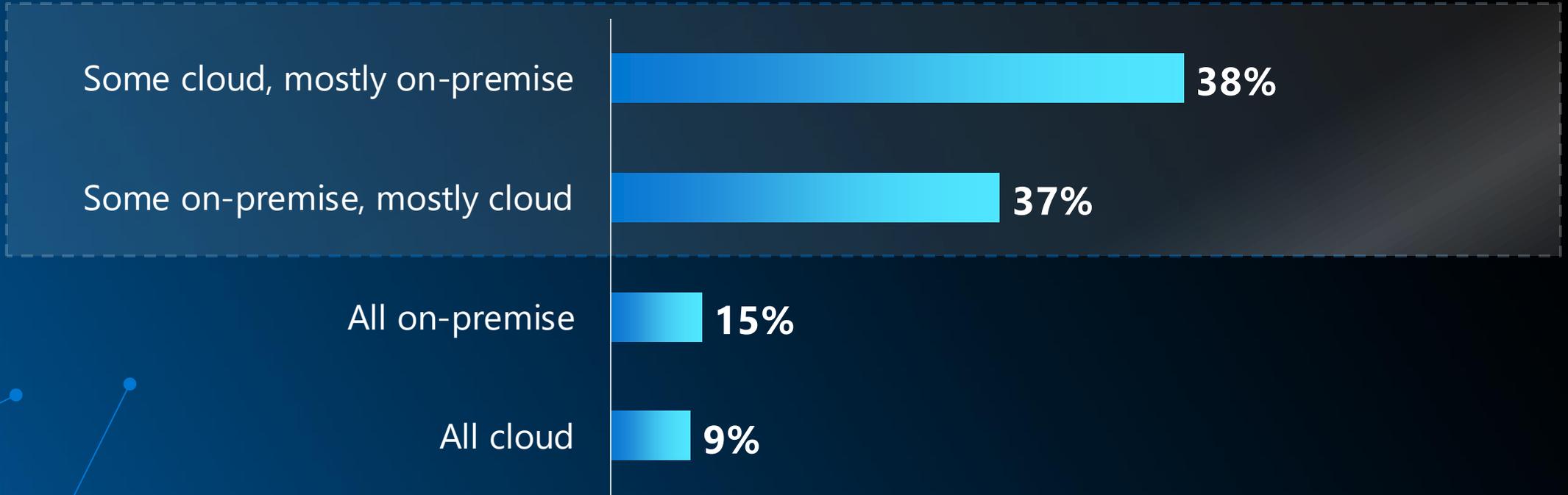
Be  
AI ready

Cloud-native  
workloads

AI

Fully-managed  
services

# Most enterprises are using a hybrid cloud approach



Foundry Cloud Computing Study, 2022 (EMEA)

# Azure Arc Overview

> > > >

# 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

# 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

vmware



3P Platforms



NUTANIX



Azure Stack HCI



IoT Devices

# 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



# 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.

# 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

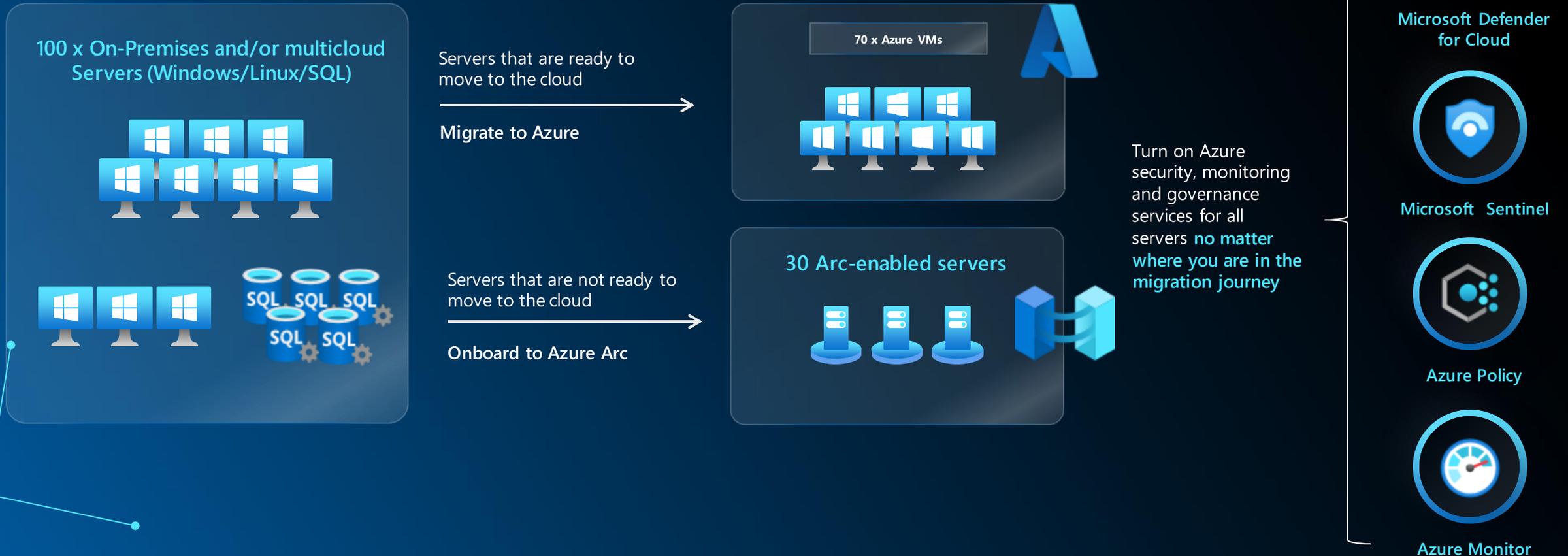
on any infrastructure

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



# 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



# Securing Azure Arc-enabled servers with Microsoft Defender for Cloud

# Microsoft Defender for Cloud

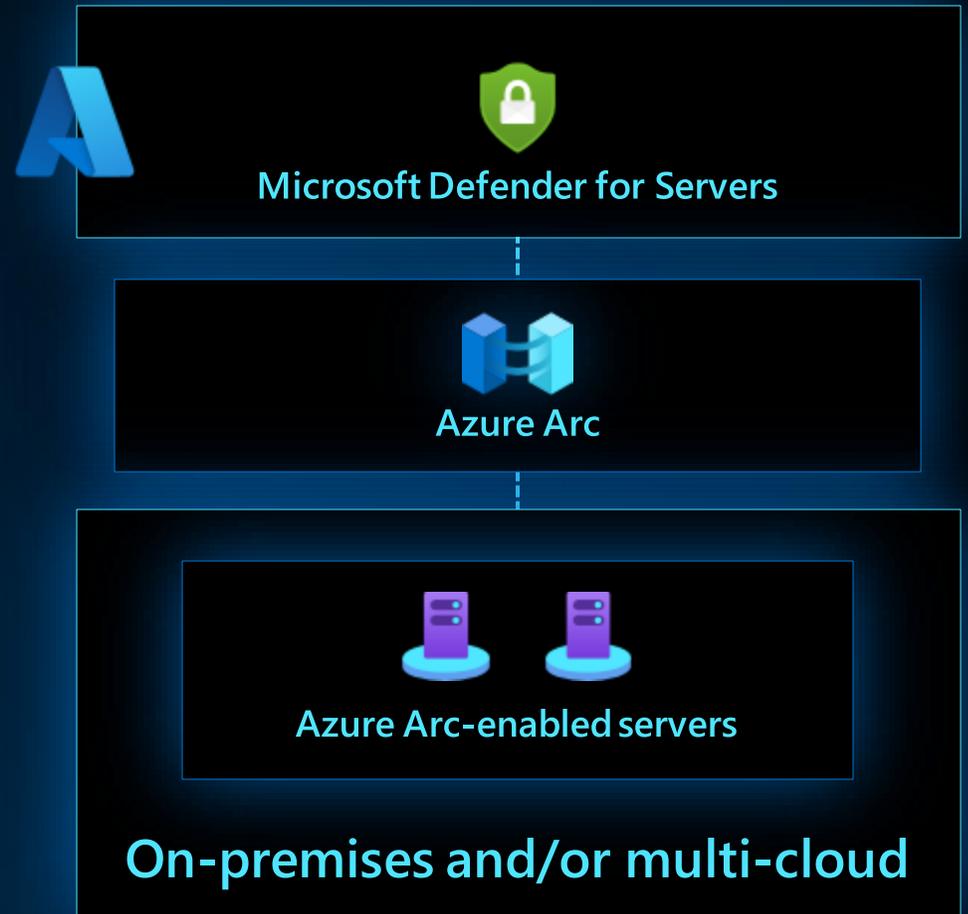
Assess, secure, and defend your hybrid and multicloud workloads

- **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



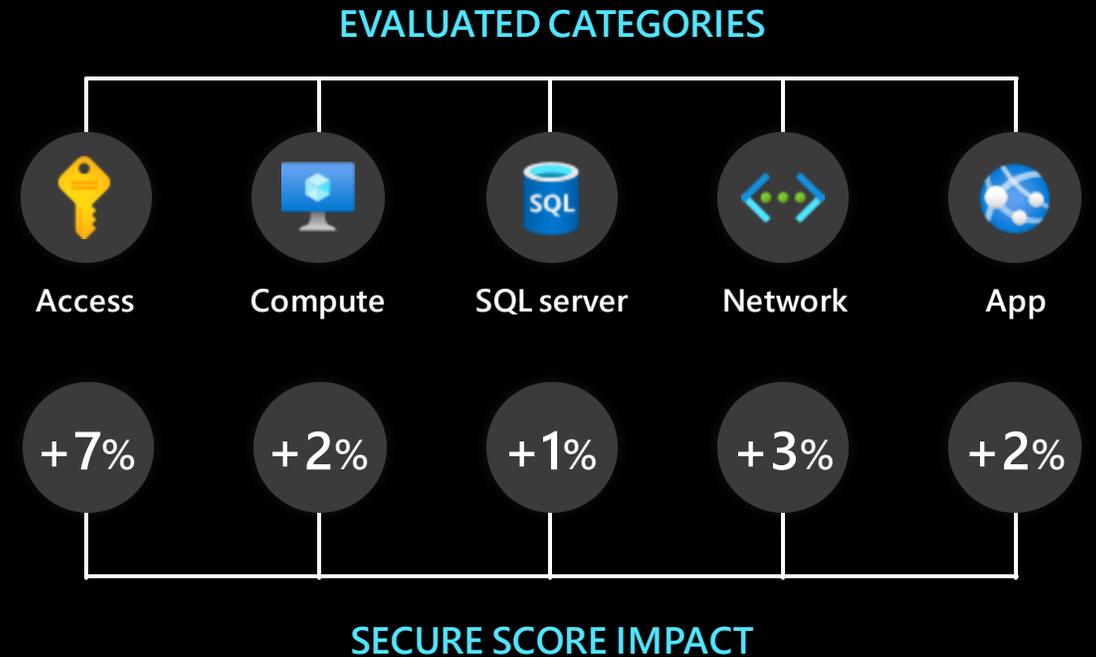
# Deploy Defender for Servers anywhere

- 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

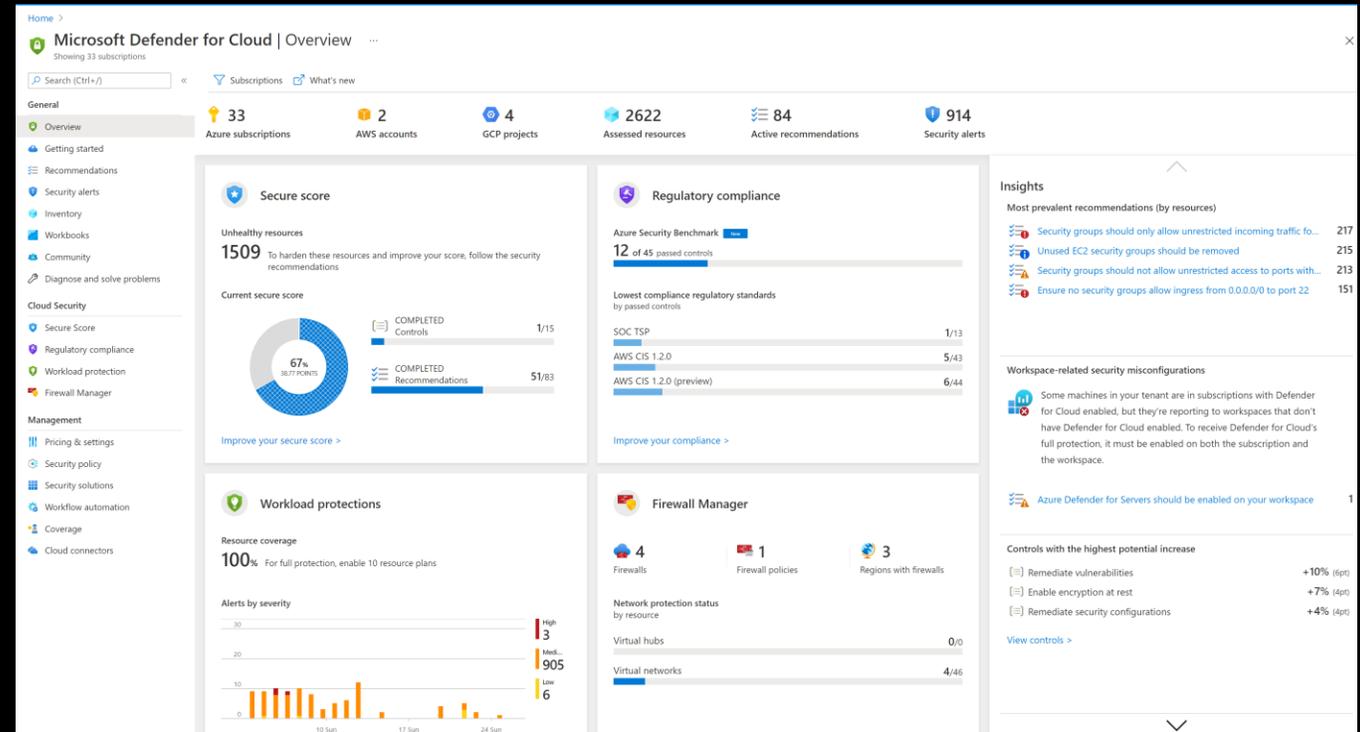
## Unified resource view

- 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 | Regulatory compliance

Showing 33 subscriptions

Search (Ctrl+F) | Download report | Manage compliance policies | Open query | Audit reports | Compliance over time workbook

You can now fully customize the standards you track in the dashboard. Update your dashboard by selecting 'Manage compliance policies' above. →

### Azure Security Benchmark

11 of 45 passed controls

#### Lowest compliance regulatory standards

Standard	Score
AWS CIS 1.2.0 (preview)	5/44
AWS CIS 1.2.0	5/43
SOC TSP	3/13
AWS PCI DSS 3.2.1 (preview)	10/38

Show all 12

### Audit reports

Stay up to date on the latest privacy, security, and compliance-related information for Microsoft's cloud services.

Open

### Compliance Standards

Azure Security Benchmark | ISO 27001 | PCI DSS 3.2.1 | SOC TSP | NIST SP 800 53 R4 | Azure CIS 1.1.0 | GCP CIS 1.1.0 | AWS CIS 1.2.0 | ISO 27001:2013 | AWS CIS 1.2.0 (preview) | AWS Foundational Security Best Practices (preview)

Under each applicable compliance control is the set of assessments run by Defender for Cloud that are associated with that control. If they are all green, it means those assessments are currently passing; this does not ensure you are fully compliant with that control. Furthermore, not all controls for any particular regulation are covered by Defender for Cloud assessments, and therefore this report is only a partial view of your overall compliance status.

Azure Security Benchmark is applied to 3 subscriptions

Expand all compliance controls

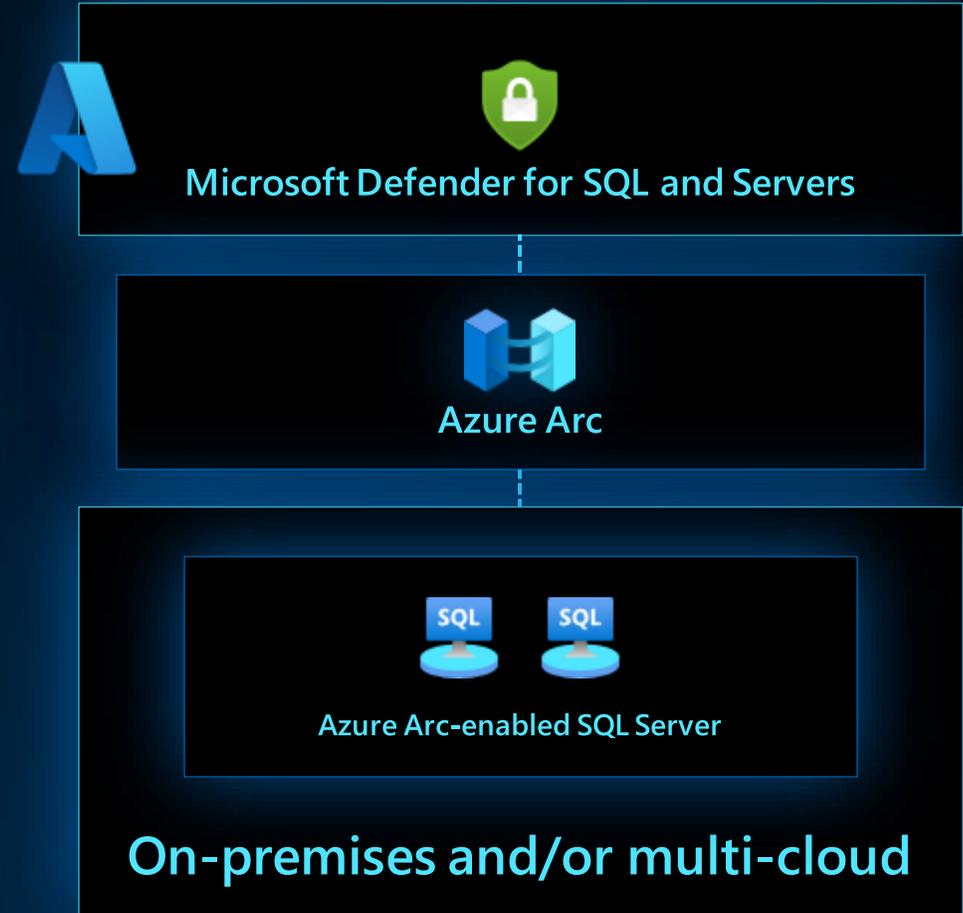
- NS. Network Security
- IM. Identity Management
- PA. Privileged Access
  - PA-1. Separate and limit highly privileged/administrative users [Control details](#) [MS](#) [C](#)

Customer responsibility	Resource type	Failed resources	Resource compliance status
A maximum of 3 owners should be designated for your subscription	Subscriptions	2 of 3	<div style="width: 66%; background-color: red;"></div>
There should be more than one owner assigned to your subscription	Subscriptions	0 of 3	<div style="width: 100%; background-color: green;"></div>
External accounts with owner permissions should be removed from your subscription	Subscriptions	0 of 3	<div style="width: 100%; background-color: yellow;"></div>
Deprecated accounts with owner permissions should be removed from your subscription	Subscriptions	0 of 3	<div style="width: 100%; background-color: yellow;"></div>
  - PA-2. Avoid standing access for accounts and permissions [Control details](#) [MS](#) [C](#)
  - PA-3. Manage identity and access lifecycle [Control details](#) [MS](#) [C](#)

# 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.

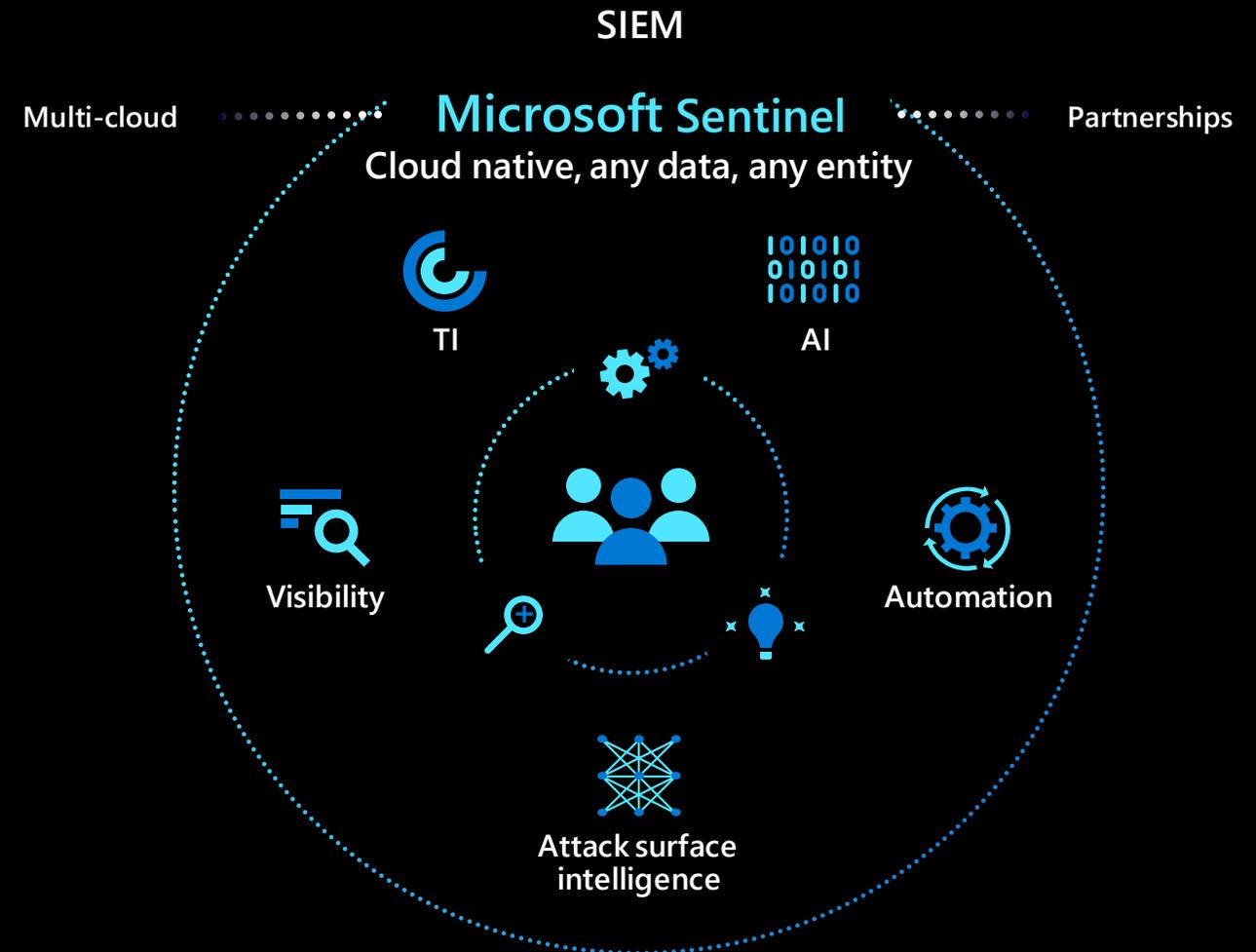
- **Collect** data at cloud scale—across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds
- **Detect** previously uncovered threats and minimize false positives using analytics and threat intelligence from Microsoft
- **Investigate** threats with AI and hunt 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

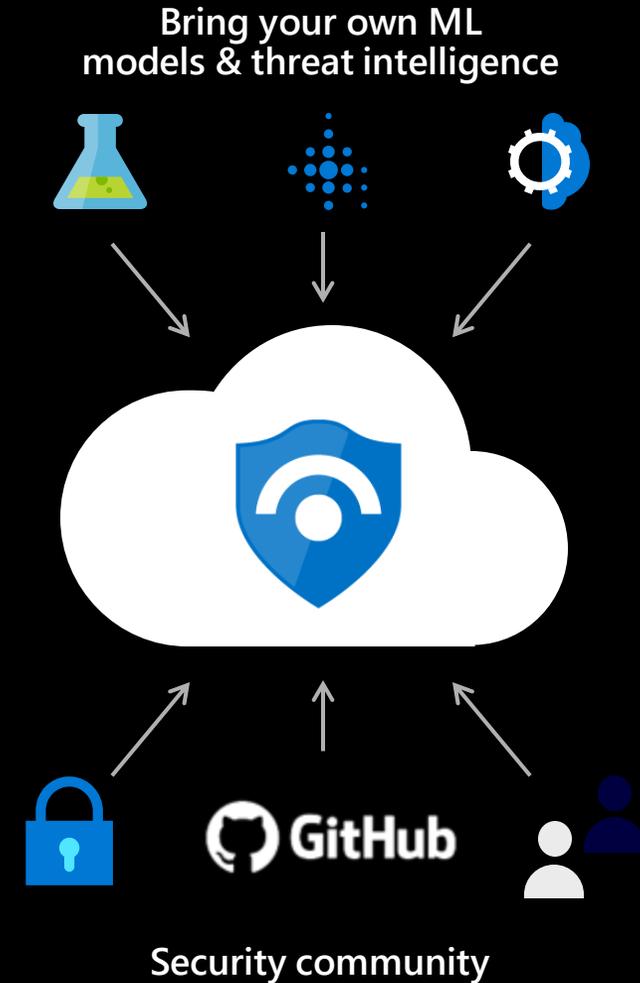
- Collect security data at cloud scale and integrate with your existing tools
- Leverage AI to detect emergent threats, reducing false positives by 79% over three years<sup>1</sup>
- Respond rapidly with built-in orchestration and automation



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

# Optimize for your needs

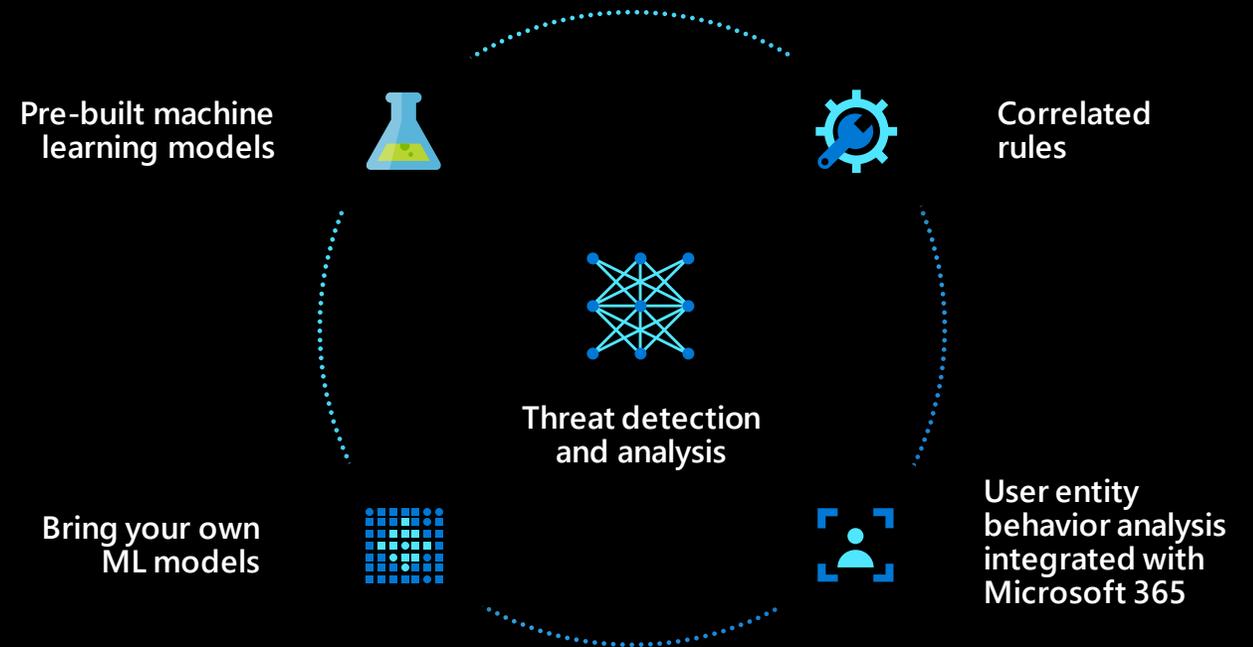
- **Bring your own insights**, machine learning models, and threat intelligence
- Tap into our **security community** to build on detections, threat intelligence, and response automation



# Detect threats and analyze security data quickly with AI

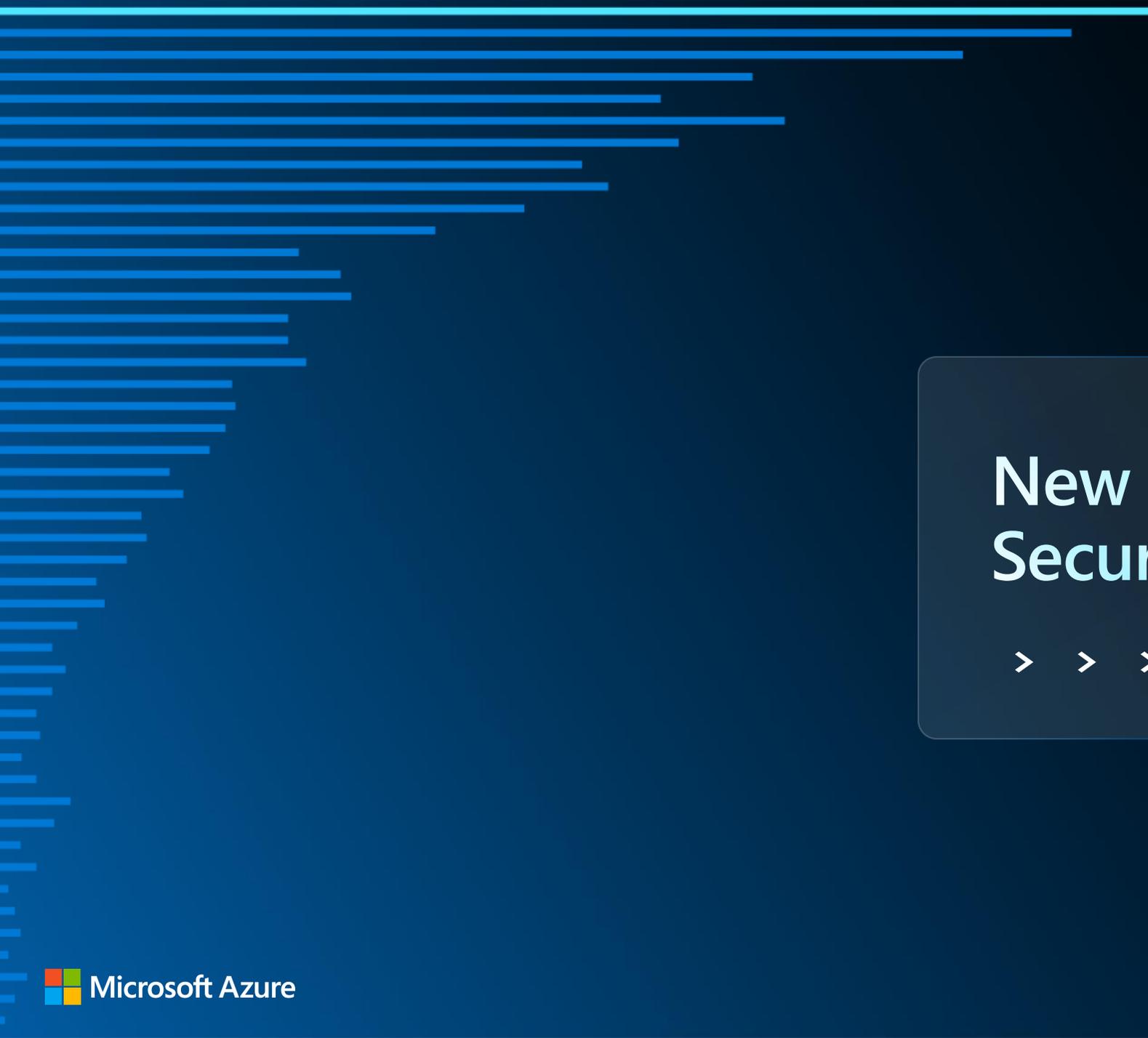
- ML models based on **decades of Microsoft security experience and learnings**
- Millions of signals filtered to few **correlated and prioritized incidents**
- Insights based on vast **Microsoft threat intelligence** and your own TI

**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
<b>Security posture management and threat protection</b>	<p><b>Microsoft Defender for Cloud</b> 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.</p> <p><b>Secure Score</b> helps you understand and improve your current security posture.</p>	<ul style="list-style-type: none"> <li>• Understand your current security posture across hybrid and multicloud environments.</li> <li>• Security recommendations aligned to key industry and regulatory standards</li> <li>• Prioritized hardening tasks to improve overall security posture across hybrid and multicloud resources.</li> <li>• Reduce security management overheads across multiple clouds/platforms.</li> </ul>
<b>Comprehensive security visibility across the enterprise for detection, proactive hunting and threat response.</b>	<b>Microsoft Sentinel</b> 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.	<ul style="list-style-type: none"> <li>• Collect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.</li> <li>• Detect previously undetected threats and investigate them with AI built-in and hunt for suspicious activities at scale.</li> <li>• Respond to incidents rapidly with built-in orchestration and automation of common tasks.</li> </ul>
<b>Enforcing security compliance across multiple clouds and on-premises</b>	<b>Regulatory Compliance</b> in Azure Policy provides security governance across hybrid and multicloud resources, with several built-in security controls.	<ul style="list-style-type: none"> <li>• Simplified governance at scale for all resources – Automated guardrails and checks to ensure that all resources stay secured and compliant.</li> </ul>
<b>Identity and access control across hybrid and multicloud</b>	Use managed identities with Azure Arc-enabled servers with Azure AD (Active Directory) and manage access controls with Azure role-based access control (RBAC)	<ul style="list-style-type: none"> <li>• With Azure AD and RBAC, customers can simplify identity and access management with cloud-based controls.</li> <li>• 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.</li> </ul>
<p>Increased costs with :</p> <ul style="list-style-type: none"> <li>• Multiple security tools for on-premises and multiple public clouds.</li> <li>• Training internal employees to use disparate tools.</li> <li>• Maintenance.</li> </ul>	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.	<ul style="list-style-type: none"> <li>• Consistent way to monitor and protect resources across the entire IT landscape.</li> <li>• Reduced costs with standardization on a simple interface and set of tools. Employees can get skilled with cloud native practices and use them anywhere.</li> <li>• Less management overhead with adoption of cloud native security services.</li> </ul>



# New Options for Extended Security Updates

> > > >

# 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<sup>1</sup>

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<sup>2</sup>

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

<sup>1</sup>Includes Azure VMs, Dedicated Host, Azure VMware Solution, Nutanix Cloud Clusters on Azure, and Azure Stack (HCI/Hub/Edge)

<sup>2</sup>Server or operating system license eligibility requirements apply.

# 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



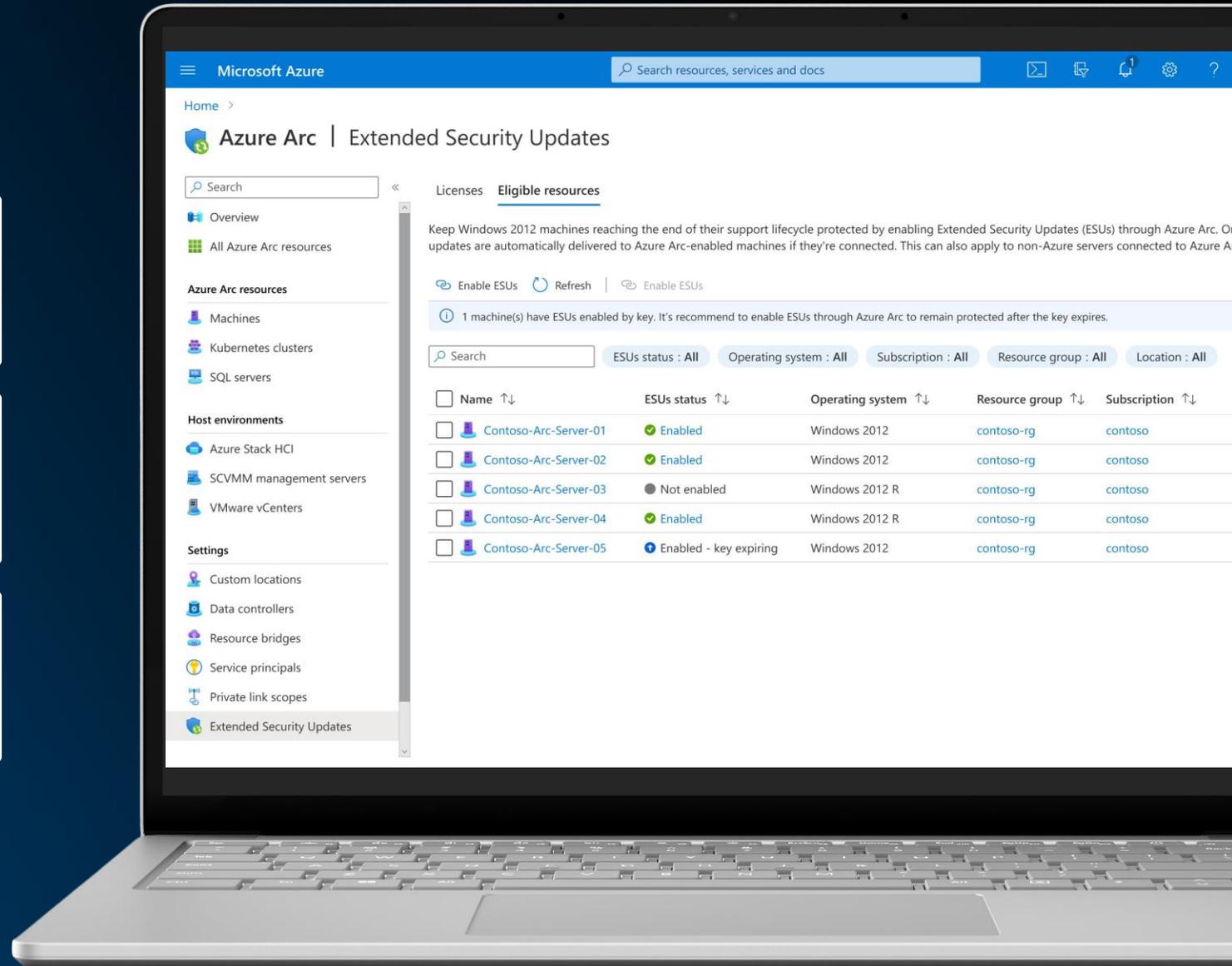
Microsoft Sentinel



Azure Policy



Azure Monitor



Enroll and purchase ESUs directly in the Azure Portal



# Demo

Extended Security Updates  
Enabled by Azure Arc



# Azure Arc Extended Security Updates Demo

Microsoft Azure

Search resources, services and docs

Home > Azure Arc | Extended Security Updates

Search

Overview  
All Azure Arc resources

Azure Arc resources

Machines  
Kubernetes clusters  
SQL servers

Host environments

Azure Stack HCI  
SCVMM management servers  
VMware vCenters

Settings

Custom locations  
Data controllers  
Resource bridges  
Service principals  
Private link scopes  
Extended Security Updates

Licenses Eligible resources

Keep Windows 2012 machines reaching the end of their support lifecycle protected by enabling Extended Security Updates (ESUs) through Azure Arc. Once enabled, security updates are automatically delivered to Azure Arc-enabled machines if they're connected. This can also apply to non-Azure servers connected to Azure Arc. [Learn more](#)

Enable ESUs Refresh Enable ESUs

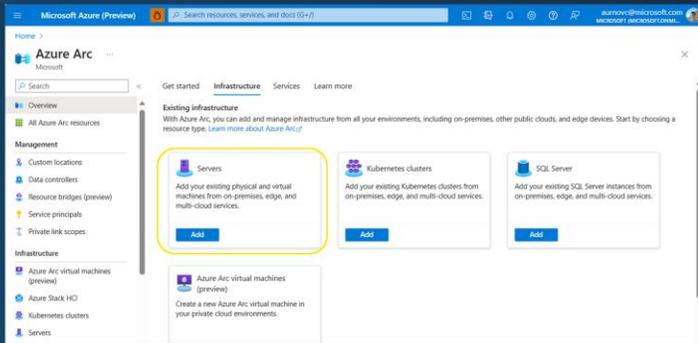
1 machine(s) have ESUs enabled by key. It's recommend to enable ESUs through Azure Arc to remain protected after the key expires.

Search ESUs status : All Operating system : All Subscription : All Resource group : All Location : All

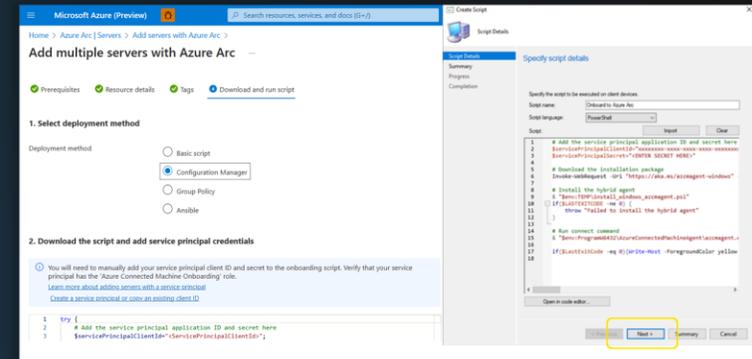
<input type="checkbox"/>	Name ↑↓	ESUs status ↑↓	Operating system ↑↓	Resource group ↑↓	Subscription ↑↓	Arc agent status ↑↓	Resource ty
<input type="checkbox"/>	Contoso-Arc-Server-01	Enabled	Windows 2012	contoso-rg	contoso	Connected	Server - Azu
<input type="checkbox"/>	Contoso-Arc-Server-02	Enabled	Windows 2012	contoso-rg	contoso	Connected	Server - Azu
<input type="checkbox"/>	Contoso-Arc-Server-03	Not enabled	Windows 2012 R	contoso-rg	contoso	Connected	Server - Azu
<input type="checkbox"/>	Contoso-Arc-Server-04	Enabled	Windows 2012 R	contoso-rg	contoso	Connected	Server - Azu
<input type="checkbox"/>	Contoso-Arc-Server-05	Enabled - key expiring	Windows 2012	contoso-rg	contoso	Offline	Server - Azu

# Get ESU for Windows Server through Azure portal [here](#).

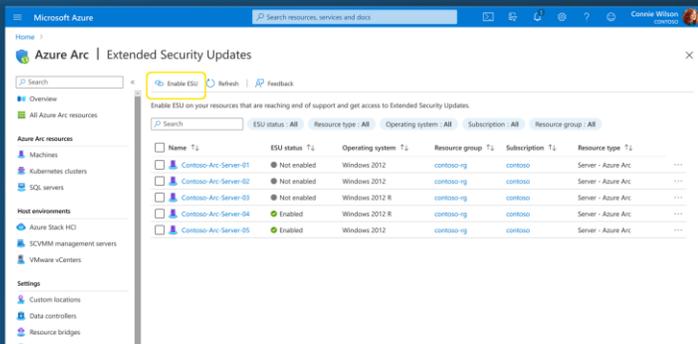
**Step 1:** Go to the Azure Arc blade in the Azure Portal and begin onboarding servers to Azure Arc by clicking 'Servers'.



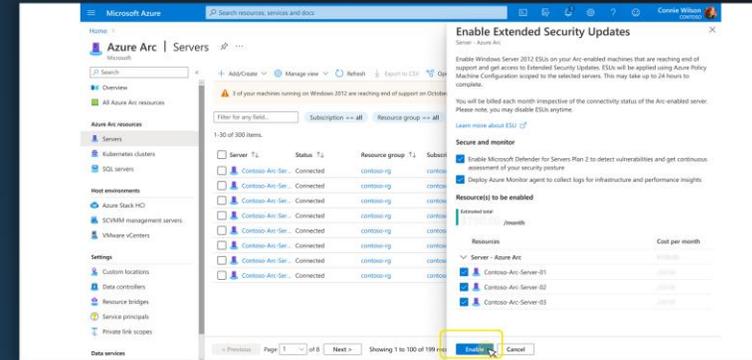
**Step 2:** Onboard servers Azure Arc by downloading the Azure Connected Machine Agent and install the agent using SCCM, PowerShell or your tool of choice



**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.



# Get ESU for SQL Server through Azure portal [here](#).

## Step 1: Connect and register customer options.

Dashboard > Azure Arc >

### Add existing SQL Server instances

Microsoft

#### Connect SQL Server to Azure Arc

Manage your SQL Server instances hosted outside of Azure with the connected machine agent and the SQL Arc extension.

[Connect Servers](#) [Learn more](#)

#### Register disconnected SQL Servers

Create an inventory of SQL Server instances that cannot be directly connected to Azure, but that are accessible via offers via Azure Portal.

[Register Servers](#) [Learn More](#)



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

Name	Resource group	Location	Status	ESU Expiration
Server1SQL2012	pekount-esu-testing	East US	Registered	2023-07-11 (ESU Y1)
Server1SQL2012R2	pekount-esu-testing	East US	Registered	2023-07-11 (ESU Y1)
Server2SQL2012R2	pekount-esu-testing	East US	Registered	2023-07-11 (ESU Y1)
Server3SQL2012R2	pekount-esu-testing	East US	Registered	2023-07-11 (ESU Y1)
Server4SQL2012	pekount-esu-testing	East Asia	Registered	2023-07-11 (ESU Y1)
Server4SQL2012	pekount-esu-testing	East US	Registered	2023-07-11 (ESU Y1)
twright-esu-testing24	twright-esu-testing3	East US	Registered	2023-07-11 (ESU Y1)
twright-test-2351	twright-esu-testing	eastus2euap	Registered	2023-07-11 (ESU Y1)
twright-test23	twright-esu-testing	East US	Registered	2023-07-11 (ESU Y1)



## Step 3: Drill into ESU options

Microsoft Azure

### SASHAN-Z240\_DALLAS

SQL Server - Azure Arc

Overview

Activity log

Access control (IAM)

Diagnose and solve problems

Settings

Azure Active Directory

Extended Security Updates

Best practice assessment

Properties

Microsoft Defender for Cloud

State management

Databases

Automation

Tasks (previous)

Support > Troubleshooting

New Support Request

Resource group: SASD001-ARC-03

Status: Connected

Location: West US 2

Subscription: SASD001-03-03

Subscription ID: 788919e4816b-47ac-9169-08b4c9094c

Tags: None

Version: SQL Server 2012

Edition: Enterprise

Computer name: SASD001-2012

Operating system: Windows

Host license type: SQL\_SERVER\_03

ESU status: Not enabled

See the ESU page for supported values.

## Step 4: Subscribe to Extended Security Updates

Microsoft Azure Portal

### LAPTOP-GP0G194C | SQL Server Configuration

SQL Server Instances

SQL Server instance name	Version	Edition
LAPTOP-GP0G194C	12.0.2600.5512	Enterprise

License Type

Specify the SQL Server edition and license type you are using on this machine. [Learn more](#)

Pay as you go

License with Software Assurance

License only

Extended Security Updates

Subscribe to Extended Security Updates

Do not subscribe to Extended Security Updates

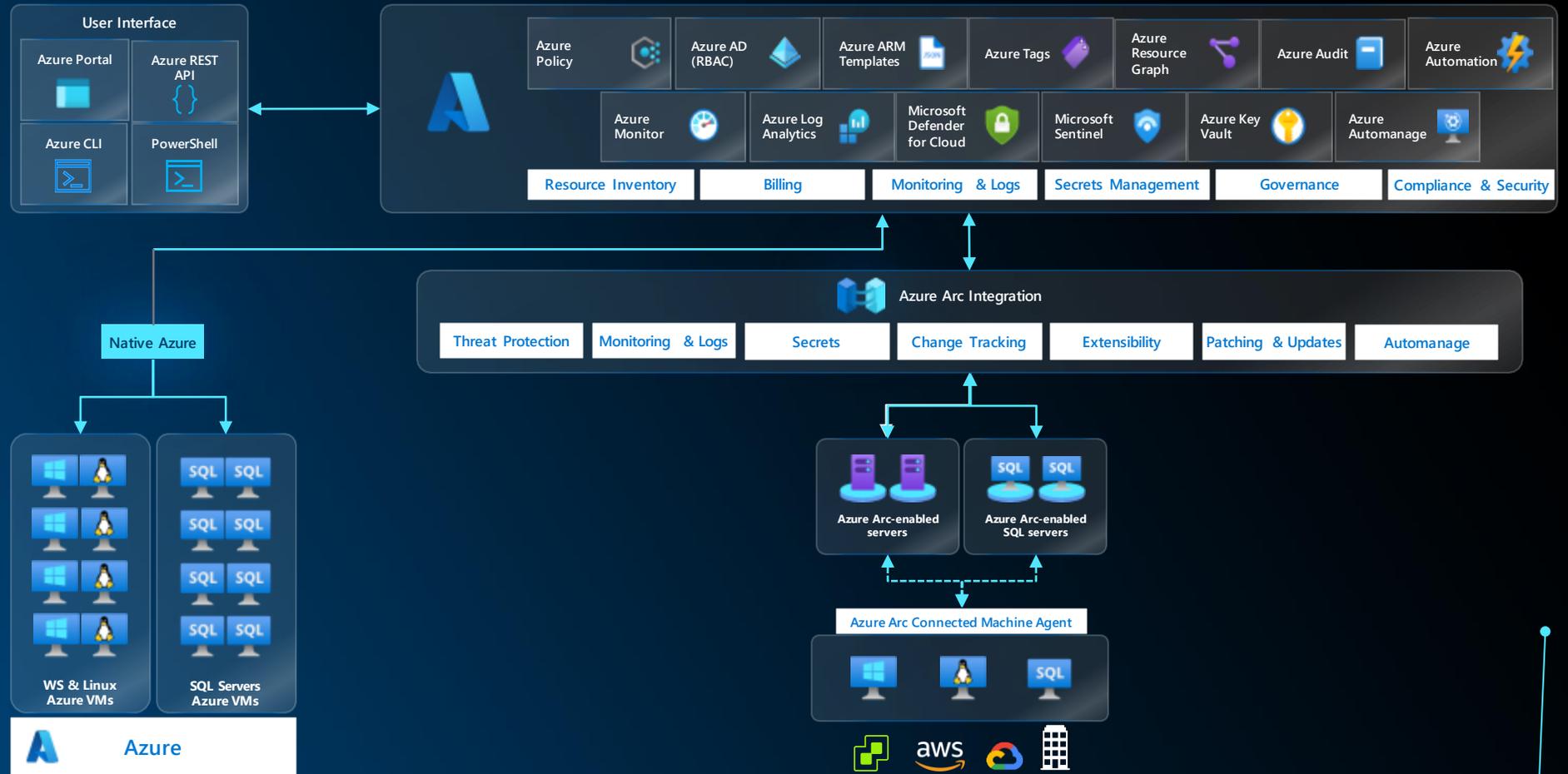
Unsubscribe from Extended Security Updates



# Best Practices for Hybrid Cloud Application

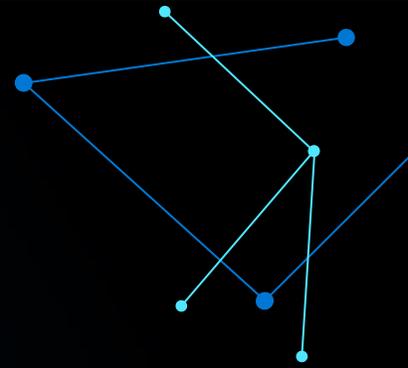
> > > >

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



On-premises and multi-cloud integration

# 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

# 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**  
Any Infrastructure, Any Cloud



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

