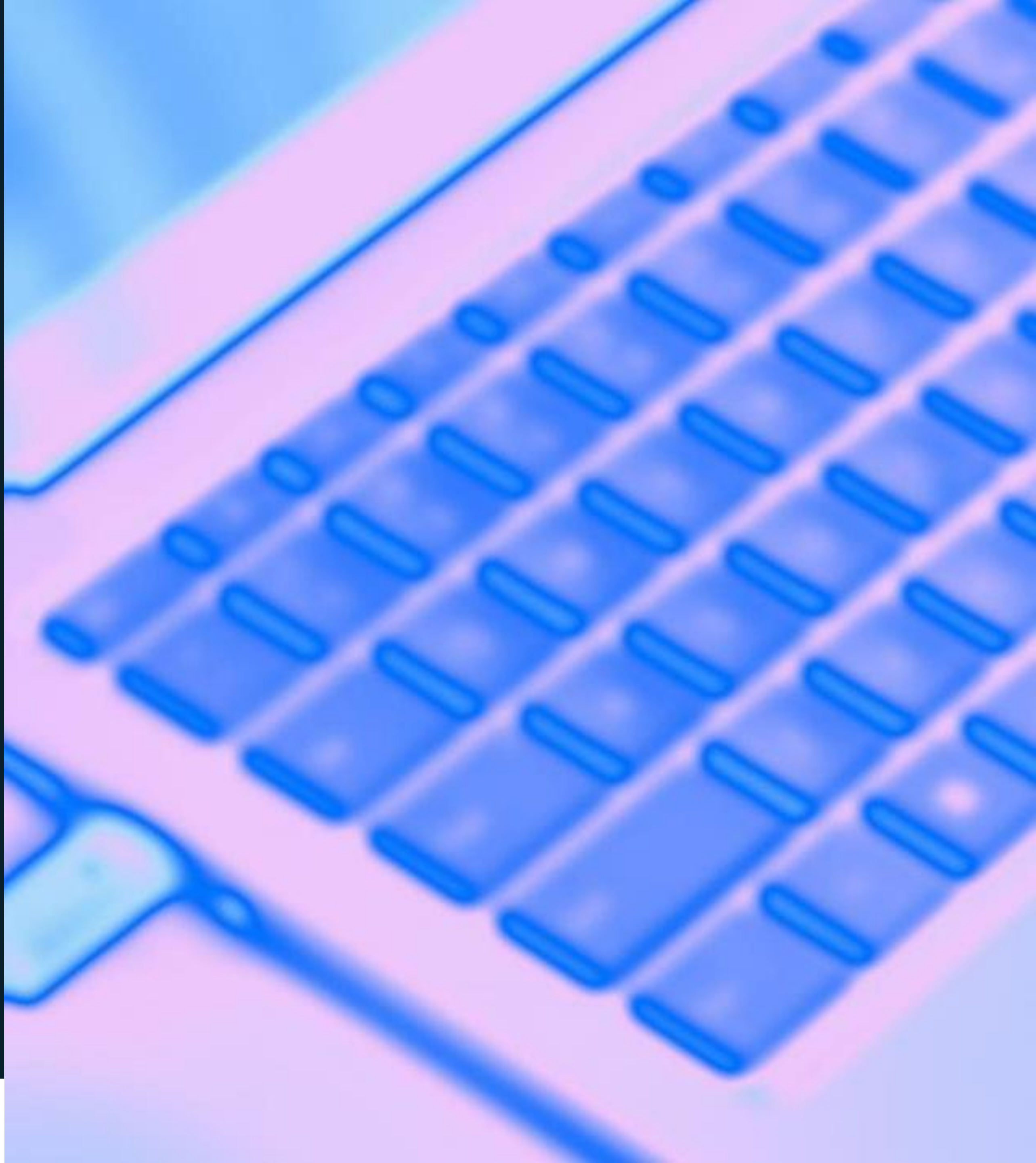
Microsoft Security

Microsoft Defender for Cloud

Alena Šeflová – Cloud Solution Architect
Microsoft



ALSO ARROW TD SYNNEX GOPAS Microsoft system4u

Představení

Alena Šeflová

Cloud Solution Architect for Security

Consultant for Microsoft 365 and Enterprise Mobility & Security, 15+ years in IT

Alena (Poulová) Šeflová | LinkedIn

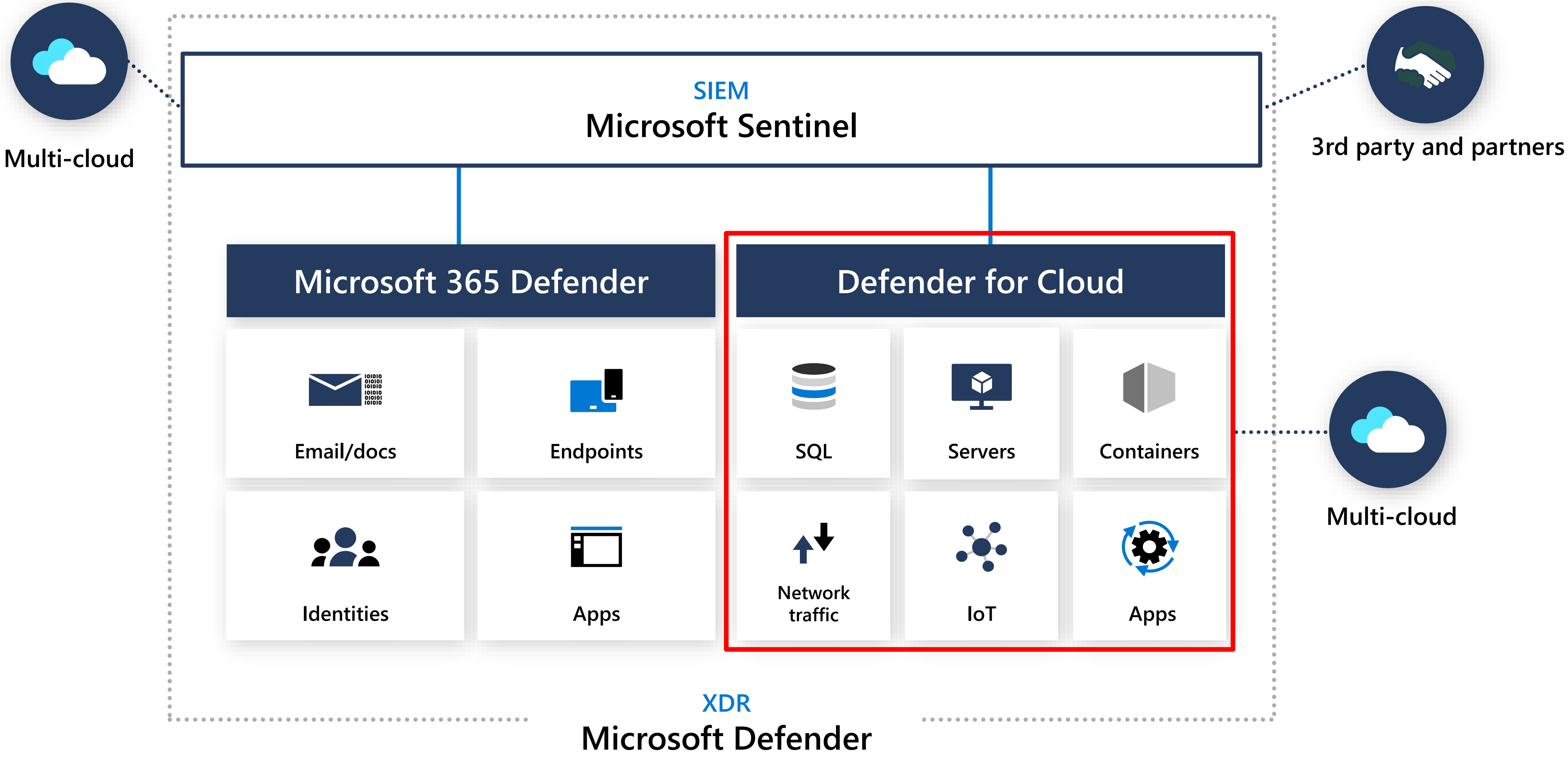
Agenda

Co všechno je Defender (for Cloud)

Workloads

Demo

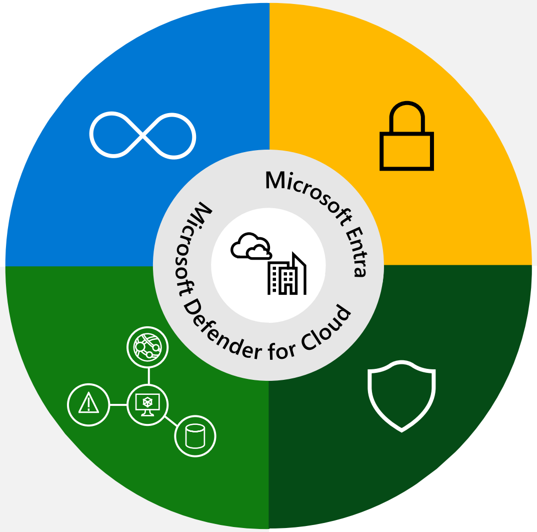
Integrated threat protection for your enterprise



Microsoft’s cloud-native application protection platform (CNAPP)

DevSecOps

Unify your DevOps security management across multi-pipelines.



Cloud infrastructure entitlement management

Enforce principle of least privilege across multicloud with CIEM.

Cloud security posture management

Visibility and contextual insights to identify and help remediate your most critical risk.

Cloud workload protection

Help detect and respond to modern threats across your cloud workloads in runtime.

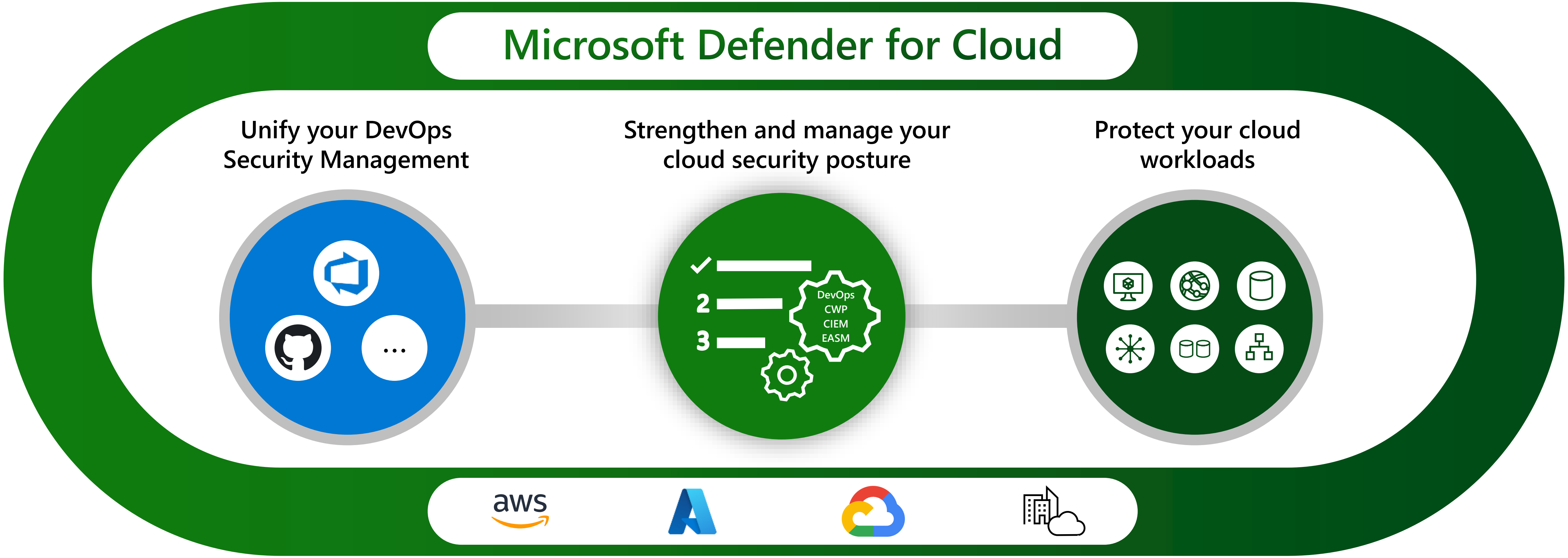
Integrated to protect across your cloud infrastructure

Microsoft Purview
(Data Security)

Microsoft Defender External Attack
Surface Management (EASM)

Azure Network
Security

Microsoft Sentinel
(SIEM)



Microsoft Defender for Cloud

Unify your DevOps Security Management

Strengthen and manage your cloud security posture

Protect your cloud workloads

Microsoft Defender CSPM

Contextual and prioritized security posture management across the entire cloud application lifecycle

Pinpoint and remediate risks

Identify and remediate critical risks and potential attack paths across your cloud environments and developer pipelines

Unify security standards and cloud policies

Streamline multicloud compliance and security best practices with built-in security standards and custom recommendations

Fortify sensitive data across clouds

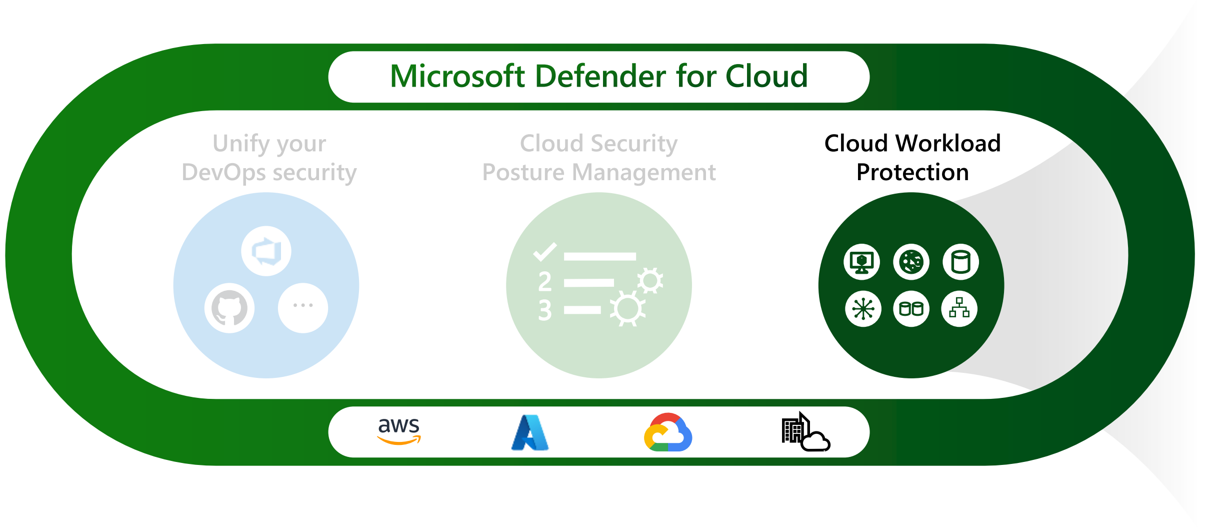
Maintain ongoing visibility into your cloud data estate and proactively harden at-risk resources containing sensitive data

Prevent future risks by fixing in code

Prevent reoccurring risks by tracing issues and enable developer collaboration to fix issues in infrastructure as code (IaC) templates

aws

Cloud workload protection



Microsoft Defender for Cloud

Unify your DevOps security

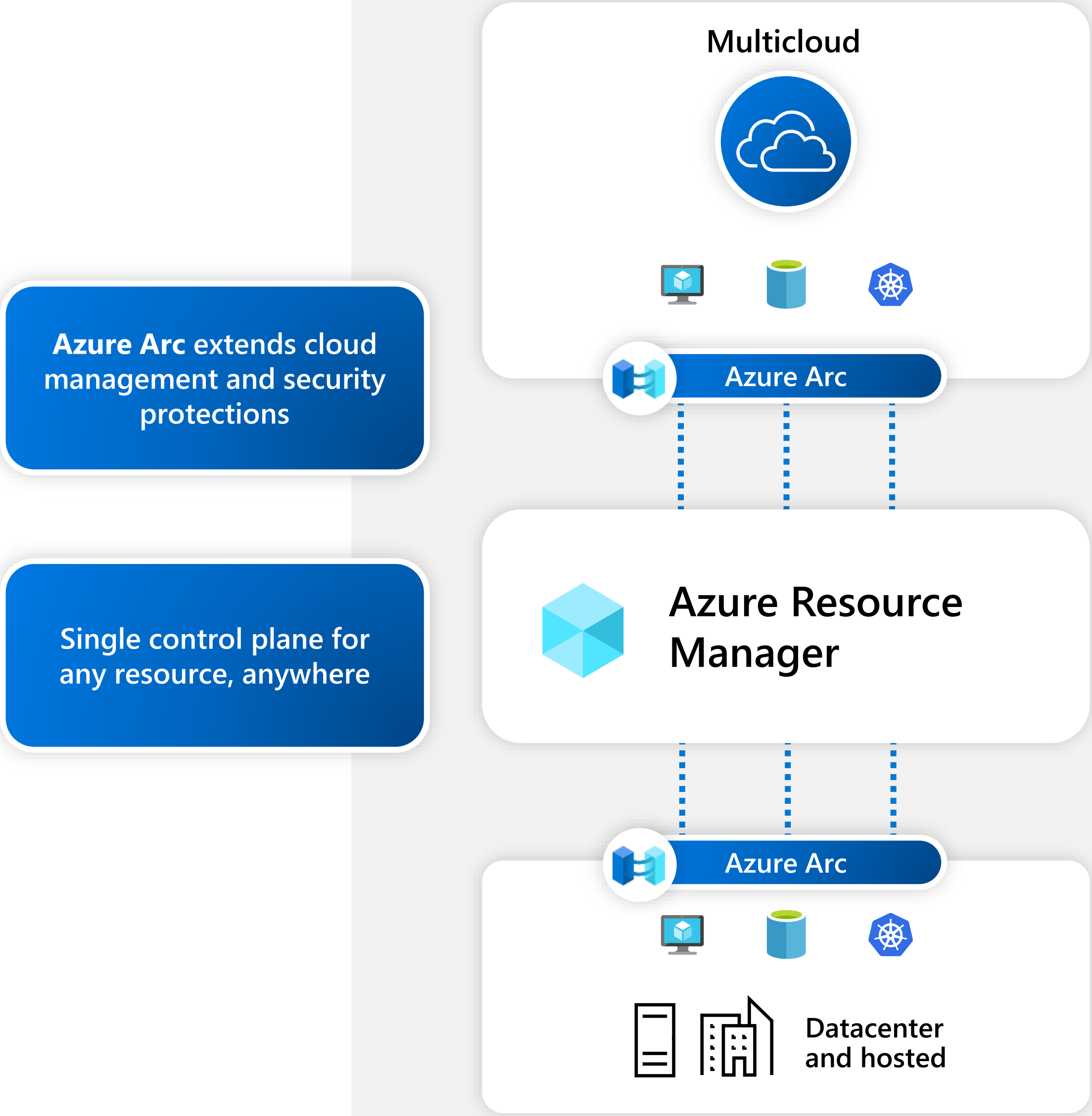
Cloud Security Posture Management

Cloud Workload Protection

Compute:	Any server	Azure VMSS	Azure K8s	App Services	Unmanaged K8s			
Service layer:	Azure DNS	Key Vault	Network Layer V1	Resource Management				
Databases and storage:	Blob storage	File storage	Maria DB	Cosmos DB	Azure SQL	MySQL	Postgres SQL	SQL on VM
AWS workloads:	Amazon EKS	Amazon EC2	SQL on VM	Unmanaged Kubernetes				
GCP workloads:	GKE clusters	Google Compute	SQL on VM	Unmanaged Kubernetes				
On-premises workloads:	Kubernetes	SQL on VM	Servers					

Use Azure Arc to connect workloads anywhere to Microsoft Defender for Cloud

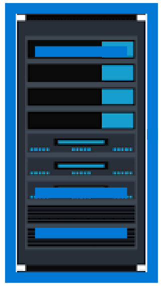
- Azure Arc is a bridge that extends the Azure platform so you can manage security for all your resources in a consistent way
- Enforce compliance and simplify audit reporting
- Asset organization and inventory with a unified view in the Azure Portal using Azure tags and resource groups
- Server owners can view and remediate to meet their compliance—RBAC in Azure
- Set guardrails with Azure Policy integration, server owners can view and remediate to meet their compliance



Azure Arc extends cloud management and security protections

Single control plane for any resource, anywhere

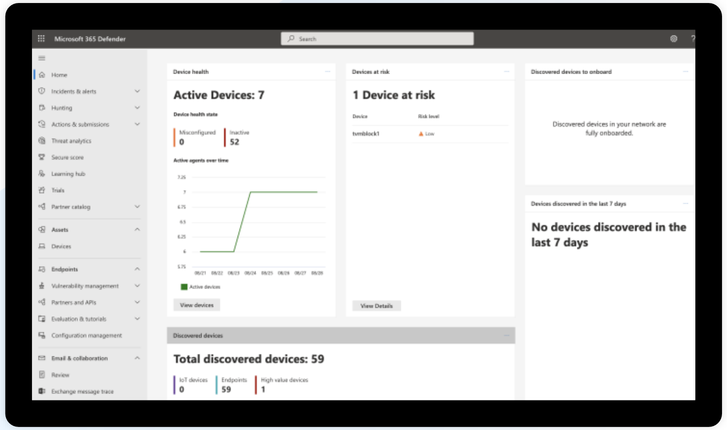
New – onboarding with MDE to Microsoft Defender for Servers P1 without Azure Arc for your on-premises servers



MDE agent

On-premises server

- Standard MDE deployment package for servers



Device health

Active Devices: 7

Device health state

Misconfigured 0 | Inactive 52

Active agents over time

Devices at risk

1 Device at risk

Device	Risk level
tvmblock1	Low

Discovered devices to onboard

Discovered devices in your network are fully onboarded.

Devices discovered in the last 7 days

No devices discovered in the last 7 days

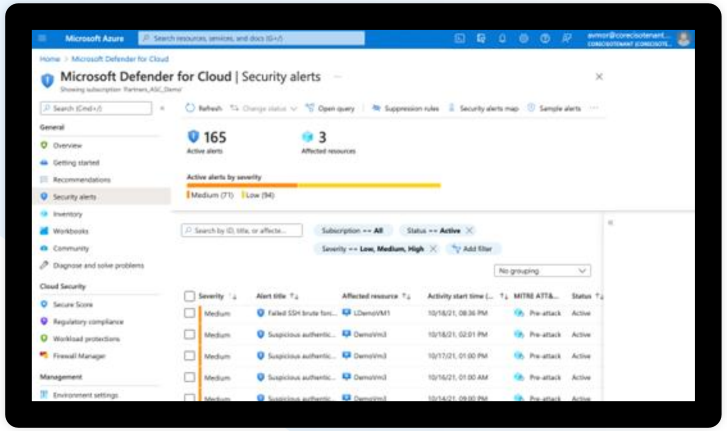
Discovered devices

Total discovered devices: 59

IoT devices 0 | Endpoints 59 | High value devices 1

Microsoft Defender XDR

- Full support for all protection and EDR management capabilities



Microsoft Defender for Cloud | Security alerts

Showing subscription 'Partners_ASC_Demo'

165 Active alerts

3 Affected resources

Active alerts by severity

Medium (71) Low (94)

Subscription == All | Status == Active | Severity == Low, Medium, High

Severity	Alert title	Affected resource	Activity start time (...	MITRE ATT&...	Status
Medium	Failed SSH brute forc...	LDemoVM1	10/18/21, 08:36 PM	Pre-attack	Active
Medium	Suspicious authentic...	DemoVm3	10/18/21, 02:01 PM	Pre-attack	Active
Medium	Suspicious authentic...	DemoVm3	10/17/21, 01:00 PM	Pre-attack	Active
Medium	Suspicious authentic...	DemoVm3	10/16/21, 01:00 AM	Pre-attack	Active
Medium	Suspicious authentic...	DemoVm3	10/14/21, 09:00 PM	Pre-attack	Active

Microsoft Defender for Cloud

- Direct onboarding to Microsoft Defender for Servers
- Consumption-based pricing model
- Same integration for alerts and MDVM data

Feature comparisons based on SKUs

Feature	Microsoft Defender for Servers Plan 1 ($5)	Microsoft Defender for Servers Plan 2 ($15)	Requires Azure Arc
Asset discovery	✓	✓	
Hardening recommendations	✓	✓	
Vulnerability assessment using Microsoft Defender Vulnerability Management	✓	✓	
Attack surface reduction	✓	✓	
Next generation antivirus protection	✓	✓	
Endpoint detection and response	✓	✓	
Automated self-healing	✓	✓	
Automatic discovery and agent onboarding for cloud-native compute (Azure, AWS, GCP)	✓	✓	
Network layer threat detection (threat intelligence and behavioral)		✓	
Microsoft Defender for DNS capabilities (malicious traffic detection)		✓	
Security explorer		✓	
Agentless scanning for cloud VMs		✓	
Agentless software inventory and vulnerability scanning		✓	
Agentless secret scanning		✓	
Agentless malware scanning		✓	
Agentless EPP coverage and configuration posture		✓	
Missing OS patches and update management		✓	✓
Windows and Linux hardening baselines		✓	✓
Regulatory compliance assessment		✓	
File integrity monitoring		✓	✓
Just-in-time VM access for management ports		✓	
Log Analytics log ingestion 500MB free benefit (per server per day)		✓	✓
Microsoft Defender Vulnerability Management Plan 2 capabilities: Security baselines, browser extensions and digital certificates assessments, firmware and hardware assessments, network share analysis, blocking vulnerable applications, authenticated scanning for Windows		✓	

Tři tipy a odkazy na závěr

1. **Microsoft Defender for Cloud – Docs**

What is Microsoft Defender for Cloud? - Microsoft Defender for Cloud | Microsoft Learn

2. **Microsoft Defender for Cloud Labs**

https://aka.ms/mdc-labs

3. **Microsoft Defender for Cloud Blog**

Microsoft Defender for Cloud Blog | Microsoft Community Hub

Microsoft Security

Microsoft Partner Security Day

Praha, 11. 2. 2025

ALSO ARROW TD SYNNEX GOPAS Microsoft system4u