[MVP Session] Ochrona serwerów w środowisku Multicloud

Konrad Sagała

Cloud Security Architect

TROCHĘ O SOBIE

- Cloud Security Architect – Azure/M365
- Microsoft Certified Trainer since 2007
- Microsoft MVP since 2007 – M365
- Twitter - @sagus
- LinkedIn - @konradsagala
- Github - https://github.com/ksagala
- Blog – https://pepugmaster.blogspot.com
- Hobby – Podróże, Śpiew, Taniec

Microsoft MCT

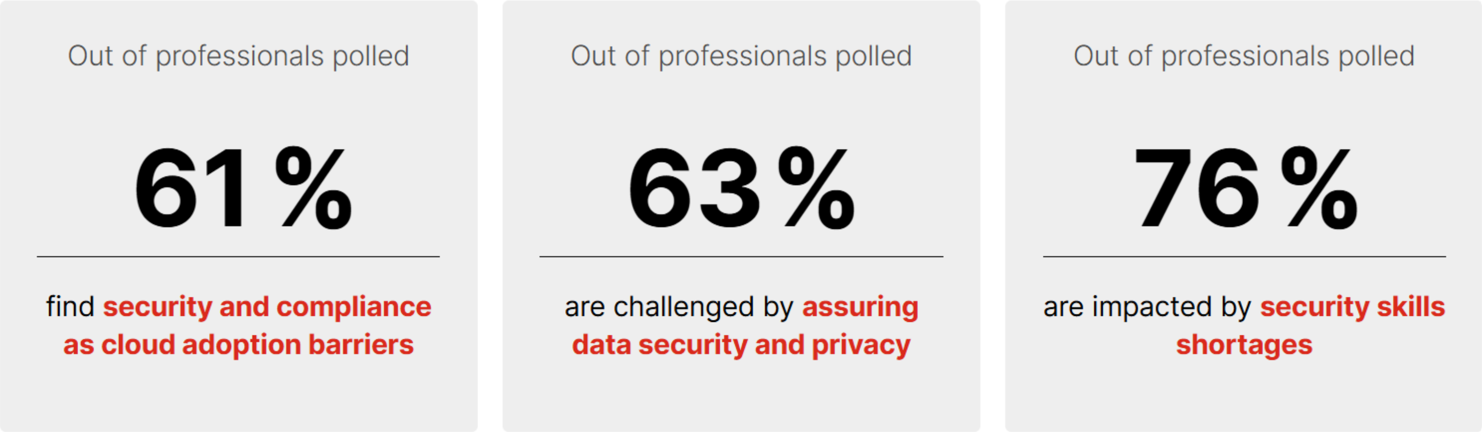
Microsoft Most Valuable Professional MVP

Agenda

- Multi-cloud security
- Azure Arc
- Azure Update Manager
- Defender for Cloud and AWS and GCP
- CSPM capabilities for AWS and GCP
- CWP(P) capabilities for AWS and GCP

Multicloud security challenges

- Data management and compliance
- Identity and access management
- Threat detection and management
- Complexity reduction in managing multi-cloud environment



Out of professionals polled

61 %

find **security and compliance as cloud adoption barriers**

Out of professionals polled

63 %

are challenged by **assuring data security and privacy**

Out of professionals polled

76 %

are impacted by **security skills shortages**

https://www.fortinet.com/resources/reports/cloud-security

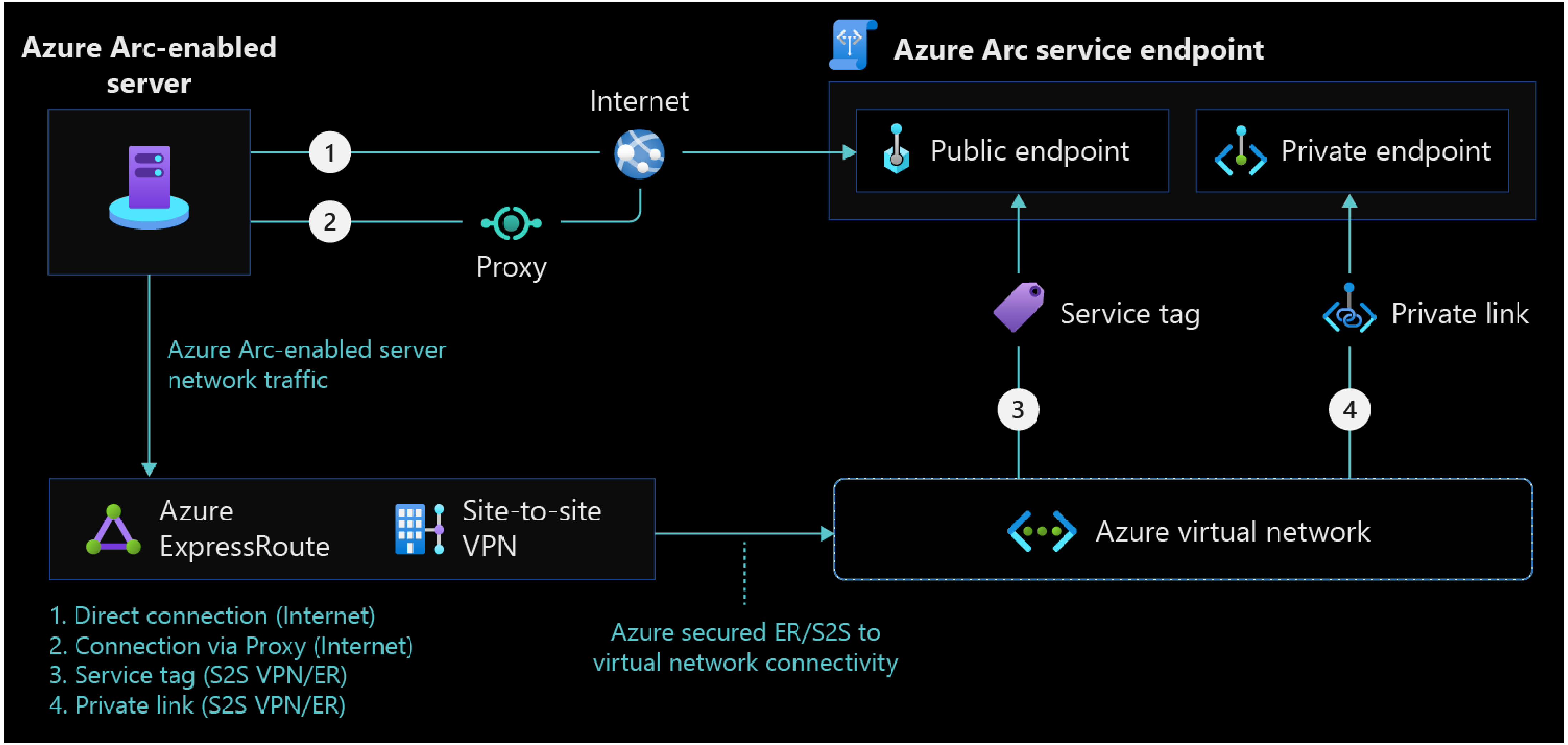
Azure Arc

Azure Arc is a bridge that extends the Azure platform to help you build applications and services with the flexibility to run across datacenters, at the edge, and in multicloud environments.

With Microsoft Defender for Servers Plan 2, Azure Policy guest configuration and Azure Update Manager are included at no additional cost. With Microsoft Defender for Cloud Plan 1, these two additional services are not included and can be purchased separately.

Services	Price
Inventory. Tag your resources, organize them into resource groups, subscriptions, and management groups, and query at scale with Azure Resource Graph to unify your environments.	FREE
Manage. Administrate your servers anywhere using SSH Arc, Run Command, and Custom Script Extension.	FREE
VM Self-service. Perform lifecycle management such as (create, resize, update and delete) and powercycle operations such as (start, stop, and restart on VMware vCenter and System Center Virtual Machine Manager Virtual Machines.	FREE

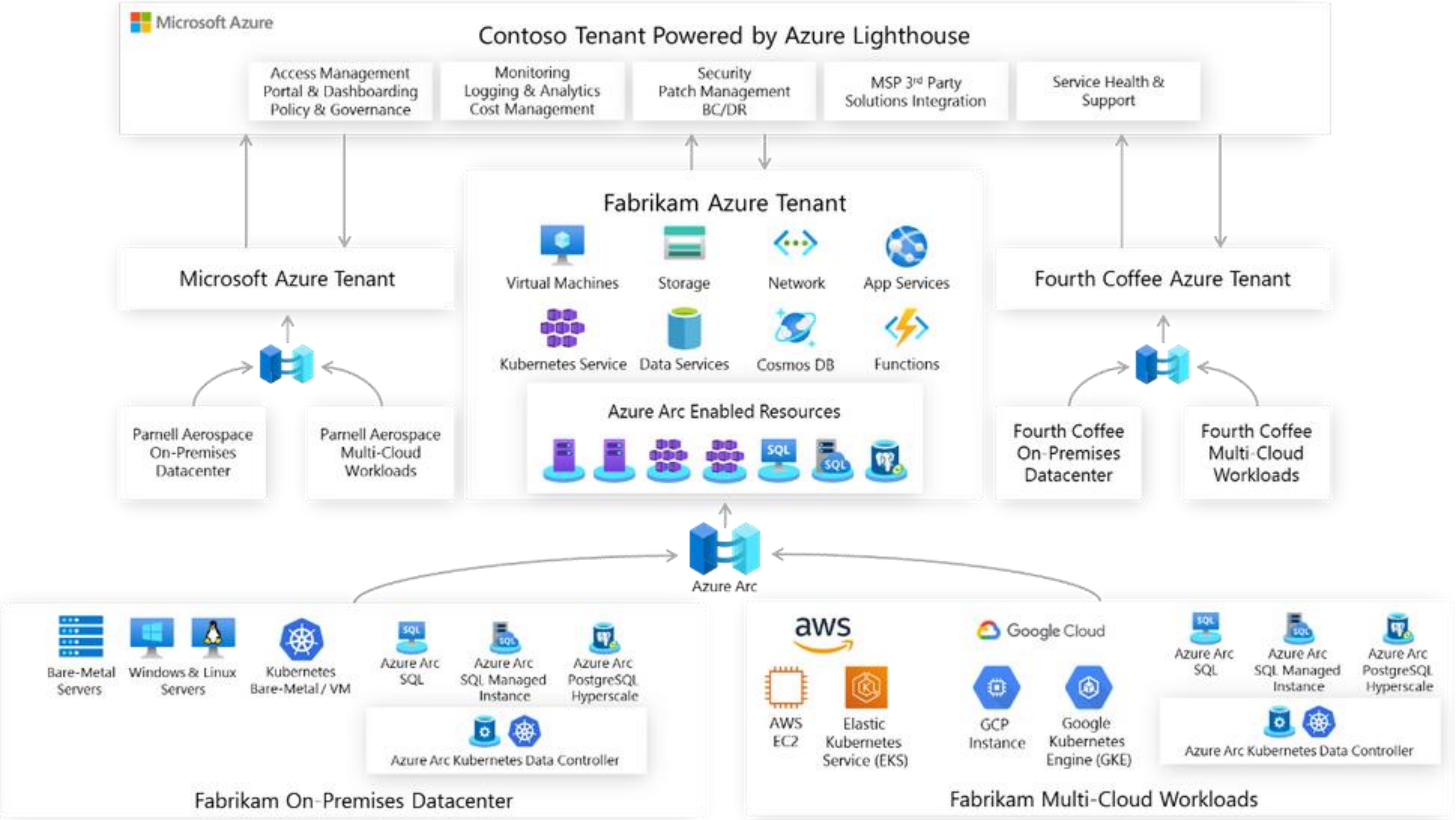
Azure Arc – server connectivity



1. Direct connection (Internet)
2. Connection via Proxy (Internet)
3. Service tag (S2S VPN/ER)
4. Private link (S2S VPN/ER)

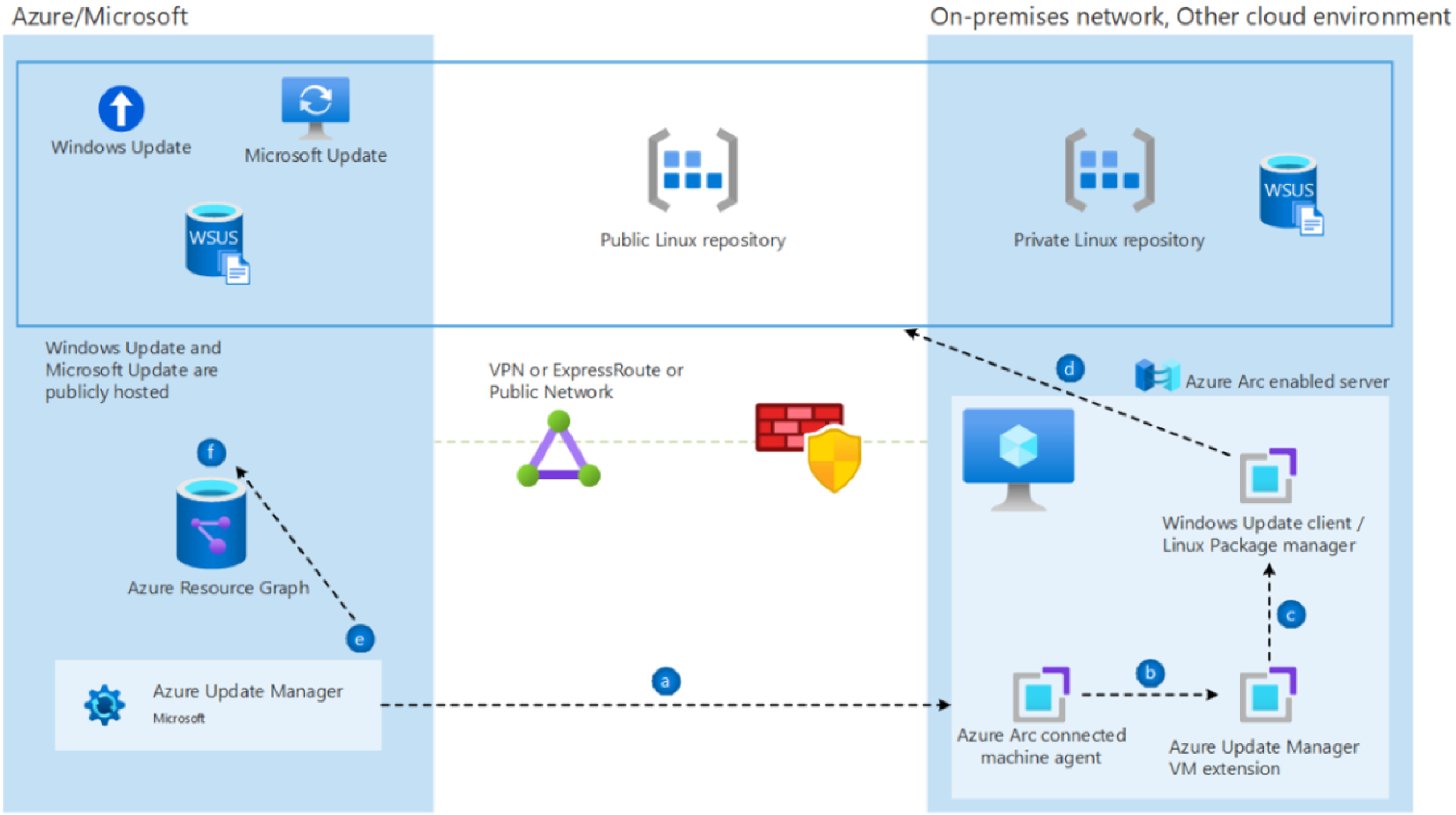
Azure secured ER/S2S to virtual network connectivity

Azure Arc – multitenancy and multicloud



https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/scenarios/hybrid/arc-enabled-servers/eslz-cost-governance

Azure Update Manager


Azure/Microsoft
On-premises network, Other cloud environment
Windows Update
Microsoft Update
WSUS
Public Linux repository
Private Linux repository
WSUS
Windows Update and Microsoft Update are publicly hosted
VPN or ExpressRoute or Public Network
d
Azure Arc enabled server
f
Azure Resource Graph
Windows Update client / Linux Package manager
c
e
Azure Update Manager
Microsoft
a
b
Azure Arc connected machine agent
Azure Update Manager VM extension

a Azure Update Manager operation

b For any 1st time-initiated Azure Update Manager operation, VM Guest Agent installs Azure Update Manager VM Extension

c Azure Update Manager VM Extension makes API calls to/from Windows Update client or Linux Package manager to check for update(s), download update(s), or deploy update(s)

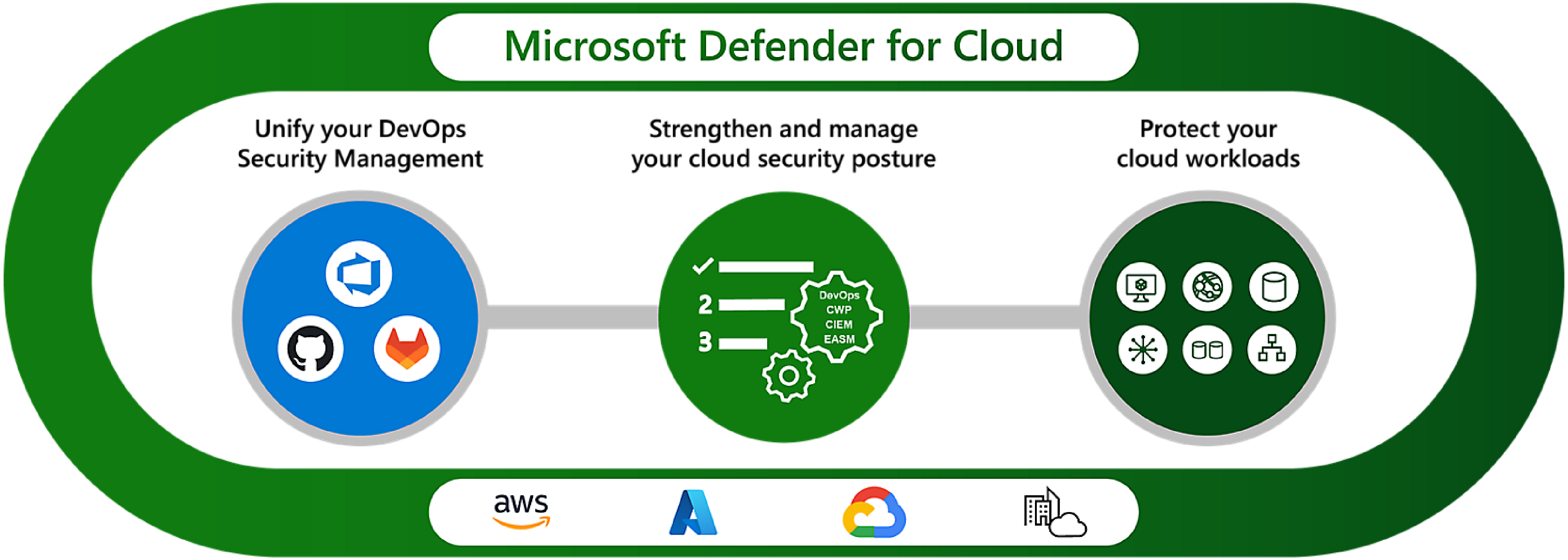
d Searches, downloads, and installs updates from Windows Update, Microsoft Update, WSUS or a public/private Linux repository. Azure Update Manager honors VM setting, which specifies the updates repository that VM points to, and deploys updates accordingly

e Assessment and deployment compliance data is received by Azure Update Manager

f Assessment and deployment compliance data is stored in Azure Resource Graph

https://learn.microsoft.com/en-us/azure/update-manager/workflow-update-manager?tabs=azure-vms%2Cupdate-win

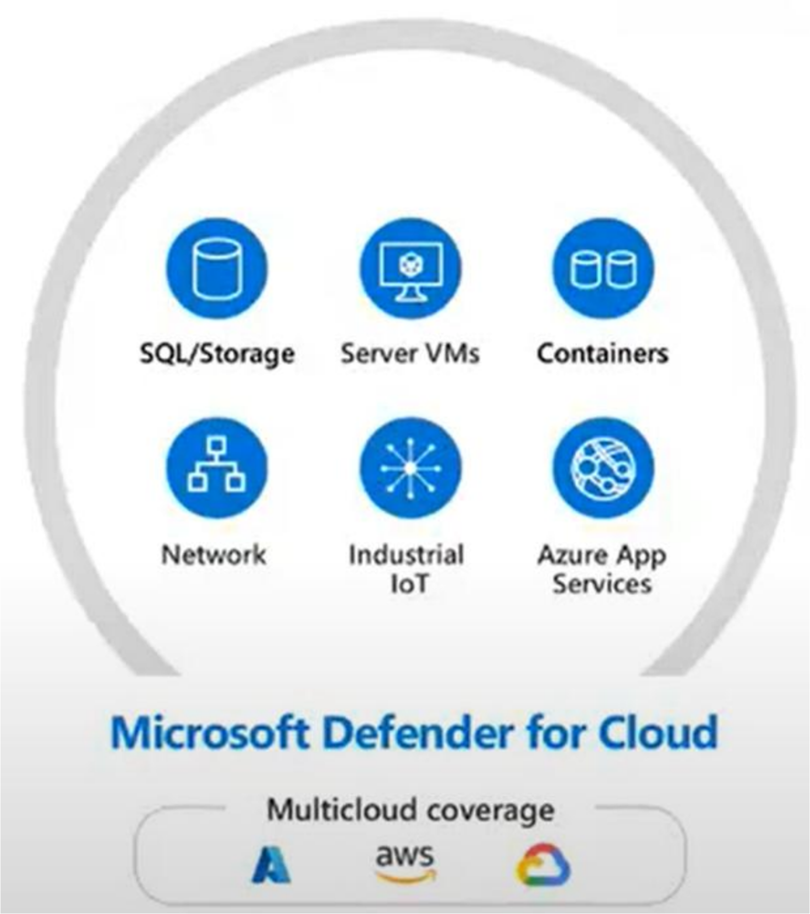
Microsoft Defender for Cloud



Microsoft Defender for Cloud
Unify your DevOps Security Management
Strengthen and manage your cloud security posture
Protect your cloud workloads
1
2
3
DevOps
CWP
CIEM
EASM
aws

Microsoft Defender for Cloud

Secure your critical workloads running in AWS, Azure and Google Cloud

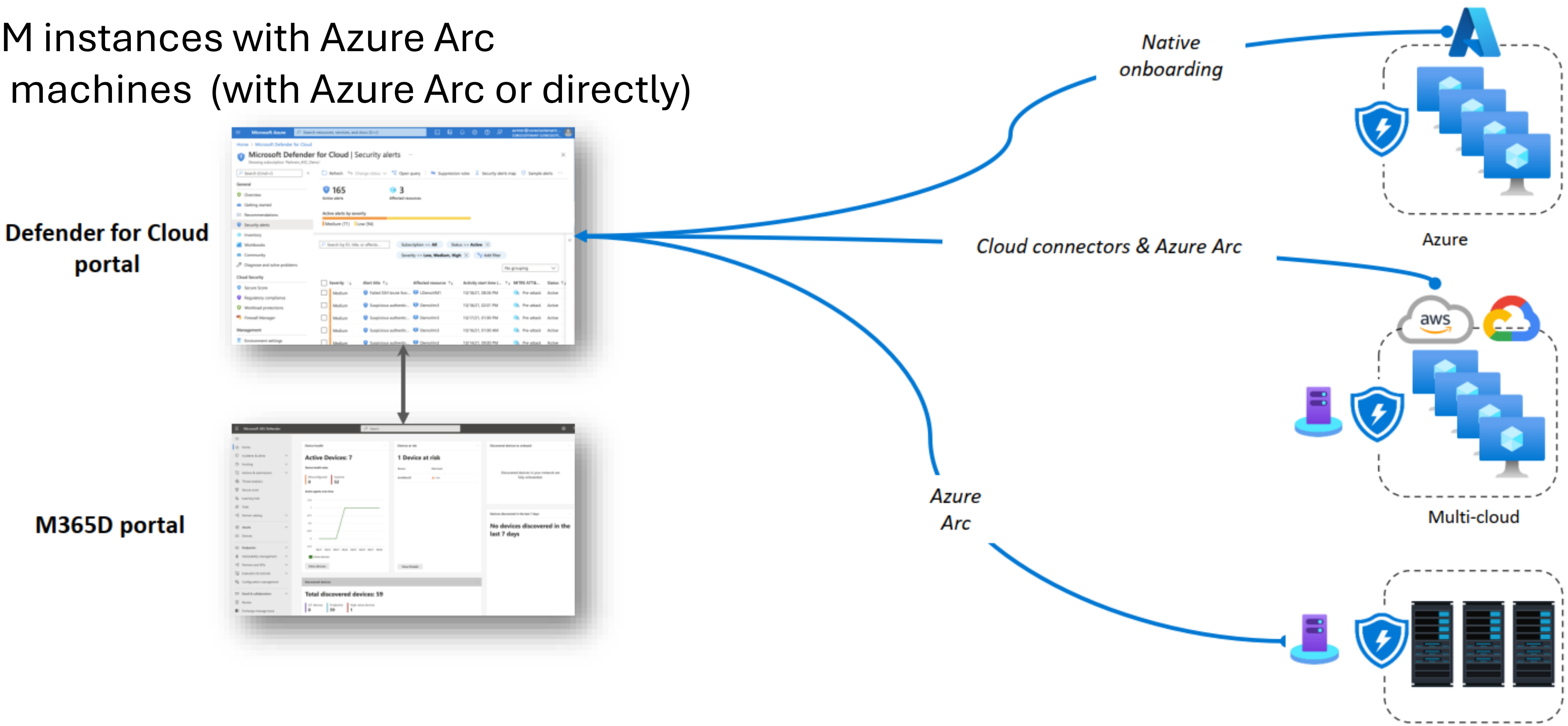


- ➢ Easy onboarding of AWS accounts and native support for Azure
- ➢ Assess and implement best practices for compliance and security in the cloud
- ➢ Get a bird’s-eye view of your security posture and vulnerabilities across clouds with secure score
- ➢ Protect Amazon EKS and GKE clusters
- ➢ Protect GCP VM instances and AWS EC2 workloads

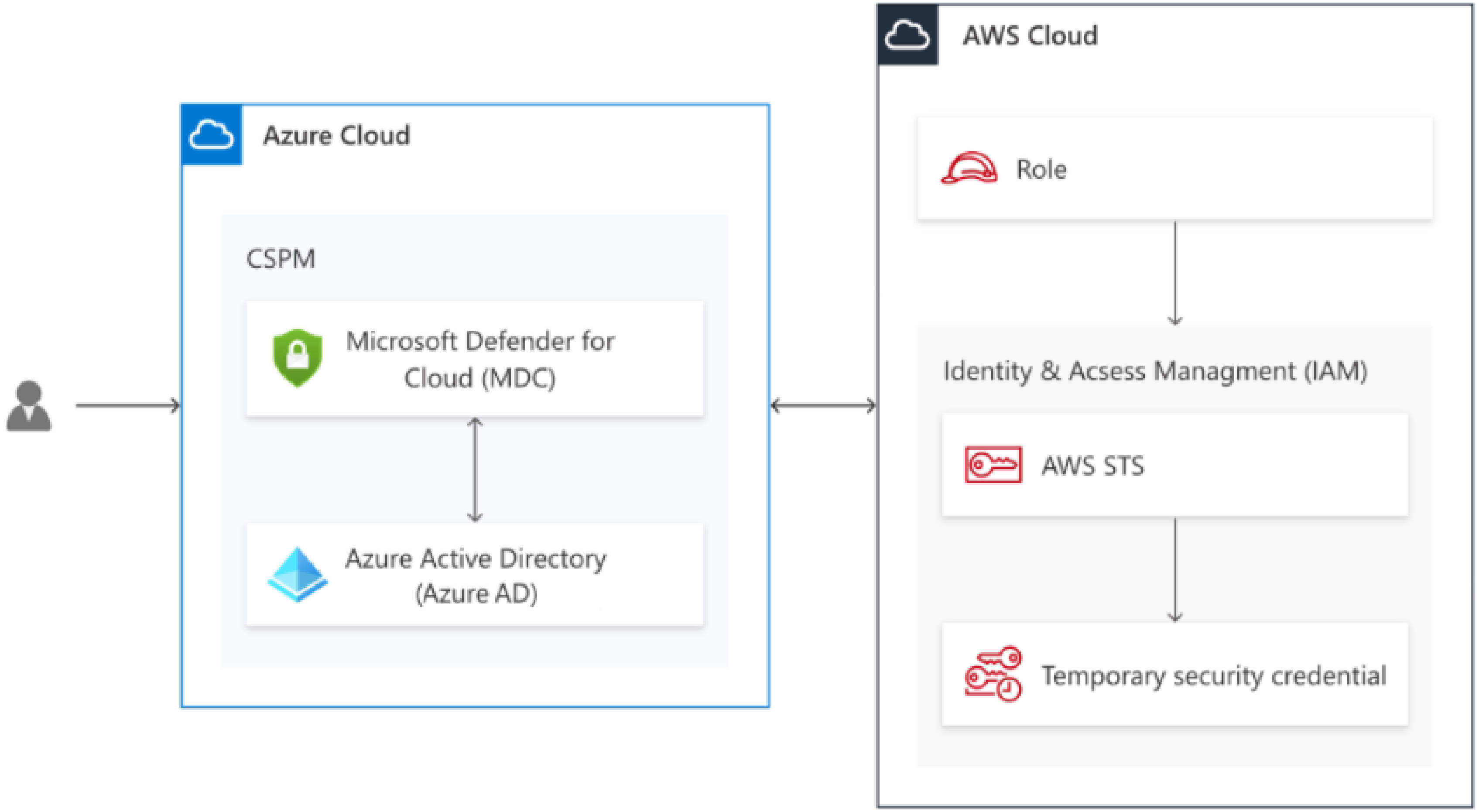
Defender for Servers in multicloud

All servers are secured the same way:

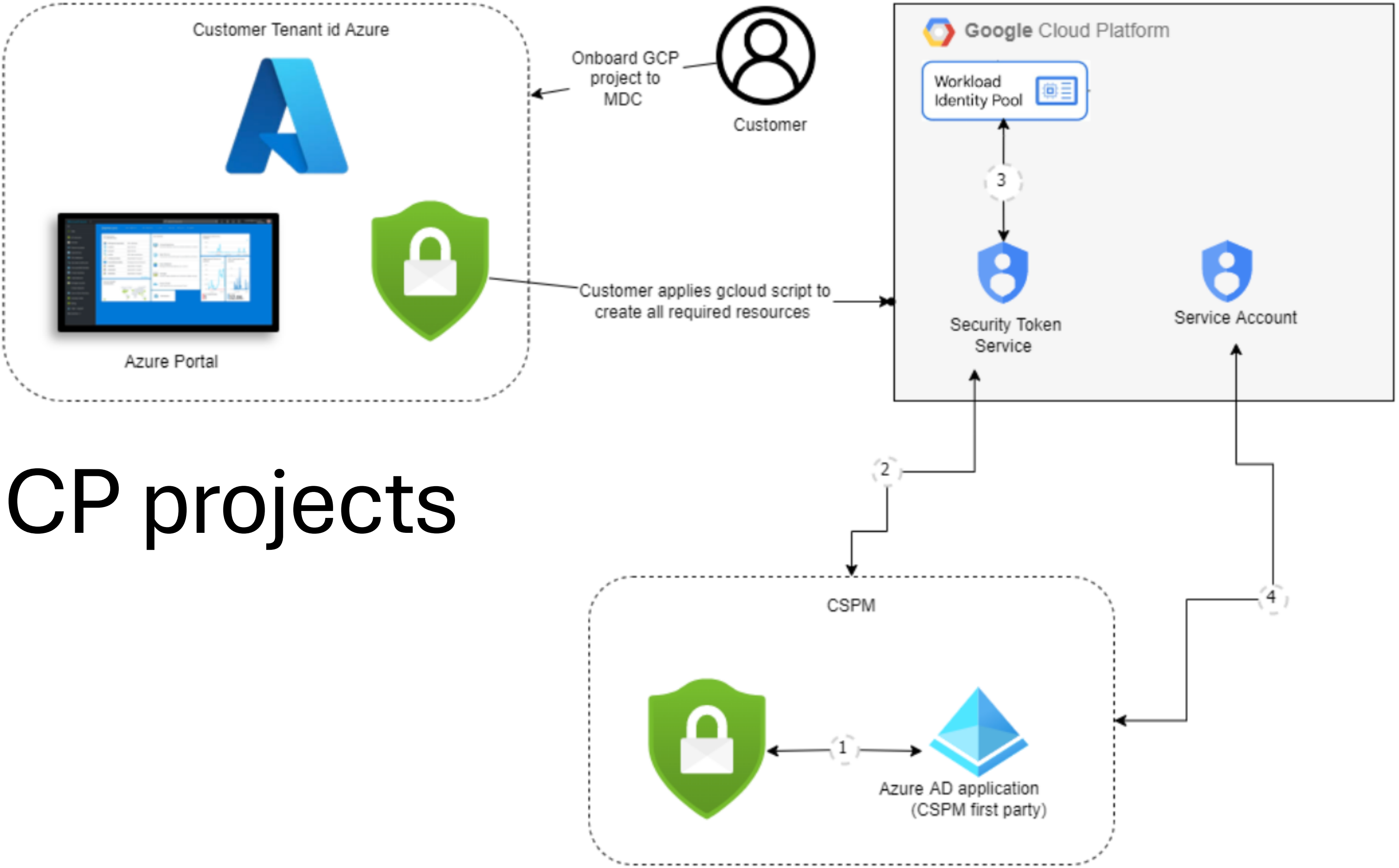
- Windows and Linux EC2 instances on AWS with Azure Arc
- Google VM instances with Azure Arc
- On-prem machines (with Azure Arc or directly)


Defender for Cloud portal
Microsoft Defender for Cloud | Security alerts
165
3
M365D portal
Active Devices: 7
1 Device at risk
No devices discovered in the last 7 days
Total discovered devices: 59
Native onboarding
Azure
Cloud connectors & Azure Arc
aws
Multi-cloud
Azure Arc

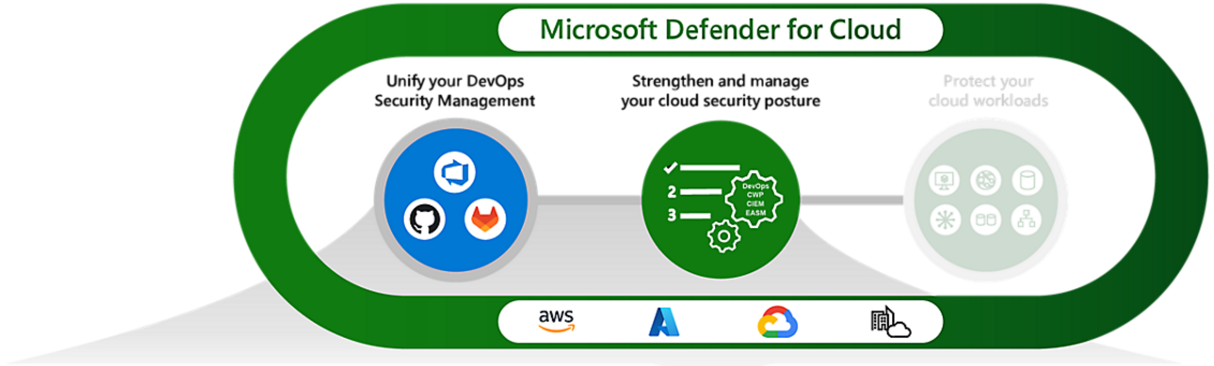
Connecting AWS accounts


Azure Cloud
CSPM
Microsoft Defender for Cloud (MDC)
Azure Active Directory (Azure AD)
AWS Cloud
Role
Identity & Acsess Managment (IAM)
AWS STS
Temporary security credential

Connecting GCP projects



Defender for Cloud - CSPM


Microsoft Defender for Cloud

Unify your DevOps Security Management

Strengthen and manage your cloud security posture

Protect your cloud workloads

Foundational CSPM (free)

Asset inventory and secure score analysis
Frictionless onboarding | +450 built-in assessments | Custom capabilities | Policy management

Infrastructure as code security
ARM | Bicep | Terraform | CloudFormation | Many more

Application posture visibility
Code | Dependencies | Secrets | Container images | Infrastructure-as-Code security insights

Advanced remediation and automation
Quick-fix remediation | Automated remediation using LogicApps | Enforcement policies | Out-of-the-box and custom automations triggered by security events

Data export and out-of-the-box reporting
Built in Azure Workbooks | At-scale data streaming and export | Integration with SIEM/SOAR solutions

Defender CSPM

Agentless vulnerability scanning
Visibility on software and CVEs | Disc snapshots | Insecure secrets and keys

Data-aware security posture
Multicloud data estate discovery | Identify data flows and resources containing sensitive and shadow data | Uncover potential sensitive data exposure and data breaches

Governance management
Assign owners automatically | Drive accountability in the organization | Grace period | Reduce time to remediate

Integrated data and insights
DevOps Platforms | Defender External Attack Surface Management | Entra Permissions Management

Contextual cloud security and risk prioritization
Attack path analysis | Intelligent cloud security graph | Custom path queries on cloud security explorer | Risk -based prioritization

Regulatory compliance and industry benchmarks
Over 50 standards | Multicloud Microsoft security benchmark | Compliance dashboard and reporting | Integration with Microsoft Purview compliance manager

CSPM – security recommendations

- API based
- More than 160 out of the box recommendations for AWS
- More than 130 out of the box recommendations for GCP
- More than 30 resource types
- Regulatory compliance standards – CIS, PCI DSS, Best Practices

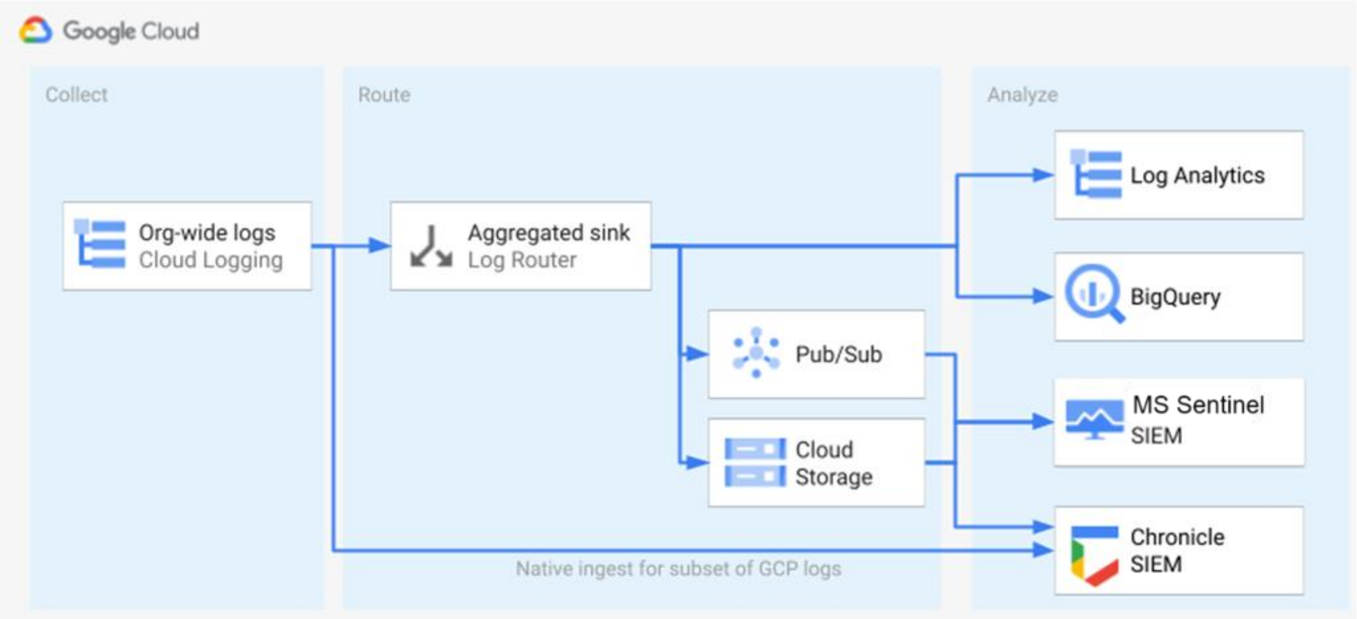
Compliance management

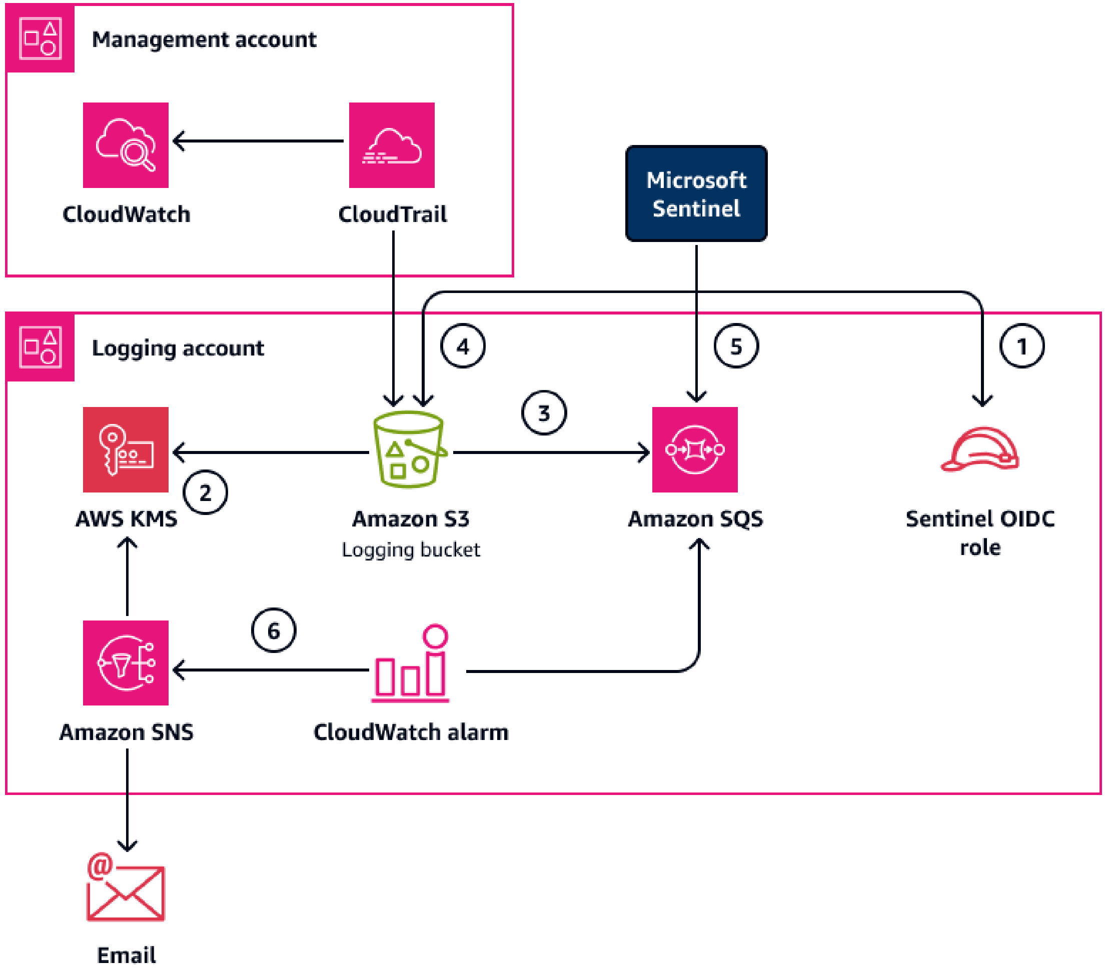
- Show compliance status, based on continuous assessments of Azure, AWS and GCP resources
- Monitor AWS and GCP resources
- Microsoft Cloud Security Benchmark monitoring enabled by default
- Mapped to the MITRE ATT&CK framework
- Support for common regulatory and compliance standards
- Reports of compliance status
- Custom recommendations possible

Microsoft Sentinel in multicloud

Connectors for AWS and GCP:

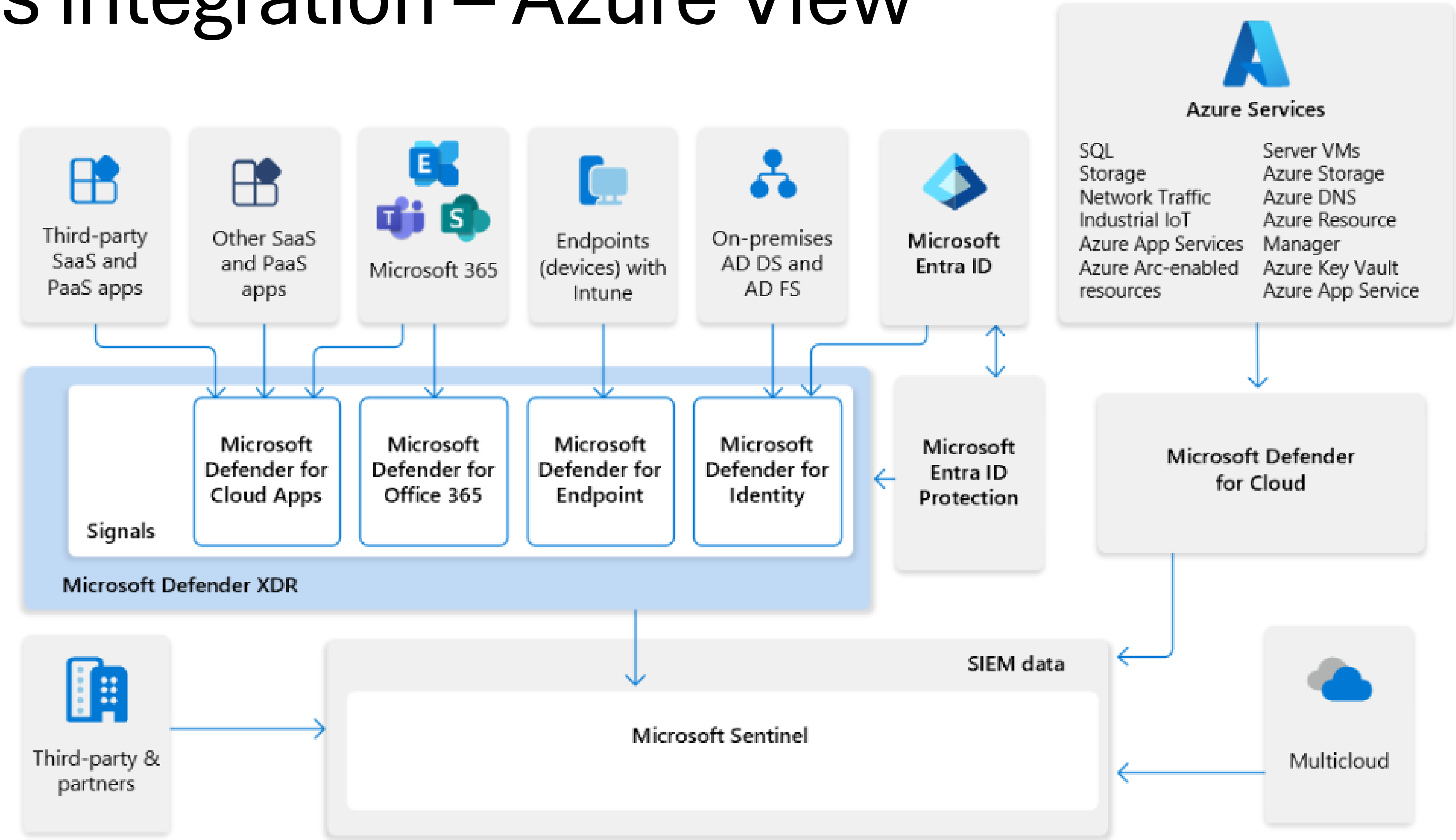
- Terraform (or Cloud Formation) code to configure integration with specific cloud





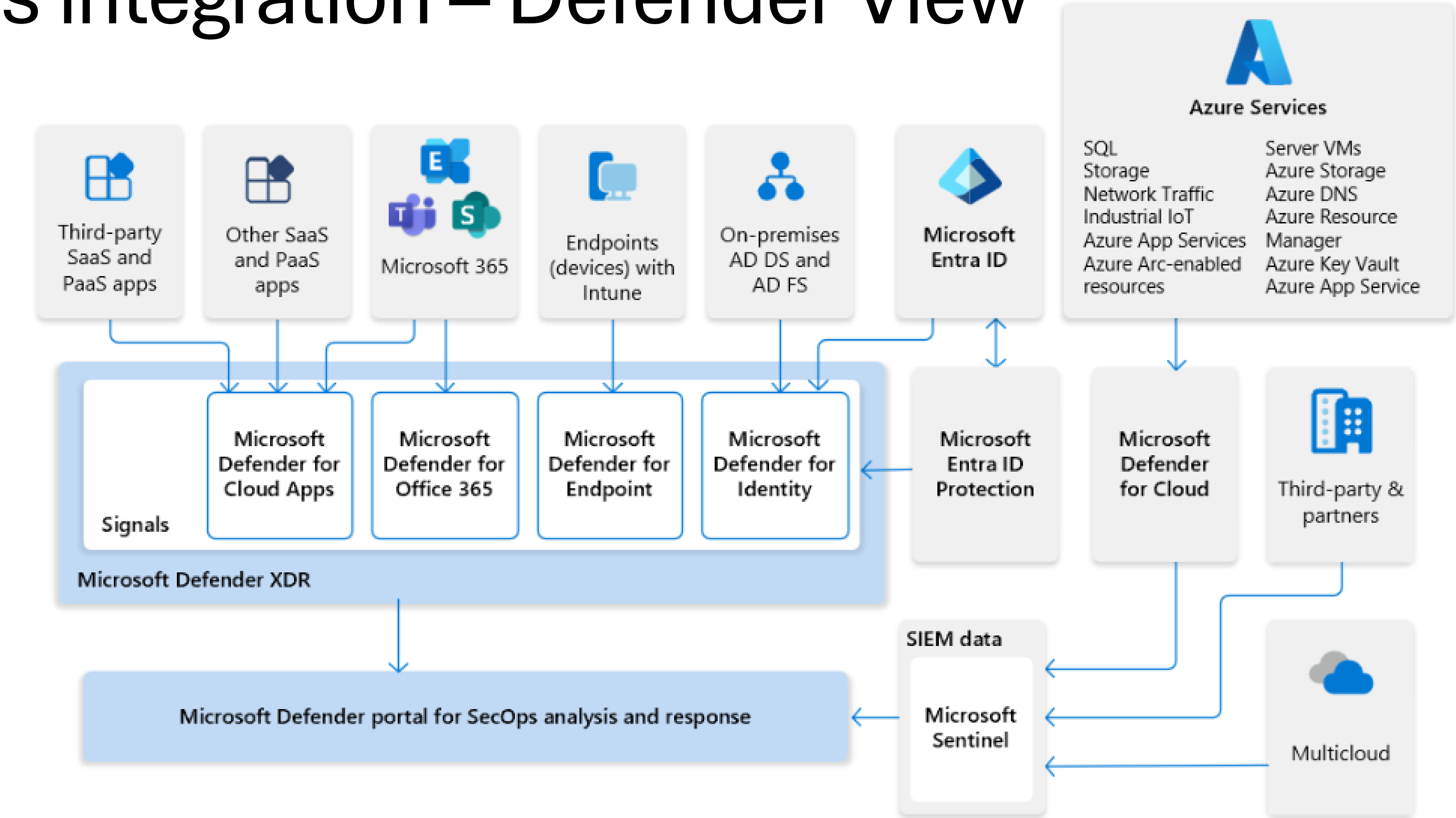
https://learn.microsoft.com/en-us/azure/sentinel/connect-aws
https://learn.microsoft.com/en-us/azure/sentinel/connect-google-cloud-platform

Tools integration – Azure View


Azure Services
SQL
Storage
Network Traffic
Industrial IoT
Azure App Services
Azure Arc-enabled resources
Server VMs
Azure Storage
Azure DNS
Azure Resource Manager
Azure Key Vault
Azure App Service
Third-party SaaS and PaaS apps
Other SaaS and PaaS apps
Microsoft 365
Endpoints (devices) with Intune
On-premises AD DS and AD FS
Microsoft Entra ID
Signals
Microsoft Defender for Cloud Apps
Microsoft Defender for Office 365
Microsoft Defender for Endpoint
Microsoft Defender for Identity
Microsoft Defender XDR
Microsoft Entra ID Protection
Microsoft Defender for Cloud
SIEM data
Microsoft Sentinel
Third-party & partners
Multicloud

https://learn.microsoft.com/en-us/azure/sentinel/microsoft-365-defender-sentinel-integration?tabs=azure-portal

Tools integration – Defender View


Azure Services
SQL
Storage
Network Traffic
Industrial IoT
Azure App Services
Azure Arc-enabled resources
Server VMs
Azure Storage
Azure DNS
Azure Resource Manager
Azure Key Vault
Azure App Service
Third-party SaaS and PaaS apps
Other SaaS and PaaS apps
Microsoft 365
Endpoints (devices) with Intune
On-premises AD DS and AD FS
Microsoft Entra ID
Signals
Microsoft Defender for Cloud Apps
Microsoft Defender for Office 365
Microsoft Defender for Endpoint
Microsoft Defender for Identity
Microsoft Defender XDR
Microsoft Entra ID Protection
Microsoft Defender for Cloud
Third-party & partners
SIEM data
Microsoft Sentinel
Multicloud
Microsoft Defender portal for SecOps analysis and response

https://learn.microsoft.com/en-us/azure/sentinel/microsoft-365-defender-sentinel-integration?tabs=defender-portal

Feedback

Zeskanuj kod i zostaw swoją opinię

//MSTS/ MS TECH SUMMIT

[MVP Session] Ochrona serwerów w środowisku Multicloud

Konrad Sagała

https://mstechsummit.pl/user.html#!/lecture/MSTS25-78a9/rate