Microsoft

SAP on Azure Enablement

Wednesday, Oct 14, 2020

Anil Malekani
Nicolas Yuen
APAC, Singapore

Module Two – Week Two

Day 1 – Monday, Oct 18th, 2020

IMPT NOTICE:

- If you choose to participate in this session using Microsoft Teams, your name, email address, phone number, and/or title may be viewable by other session participants.
- **Please note that the training will not and cannot be recorded in alignment with Microsoft's policies**

SAP on Azure Partner Enablement

Module Two – Week Two

Day 1 - Azure Security & Best Practices for SAP

Anil Malekani
CISSP, CCSP
Cyber Security Solutions

Nicolas Yuen
Cloud Solution Architect

Ravi Gangampalli
Cloud Solution Architect–
SAP on Azure

Check-in

We are happy to host you ☺

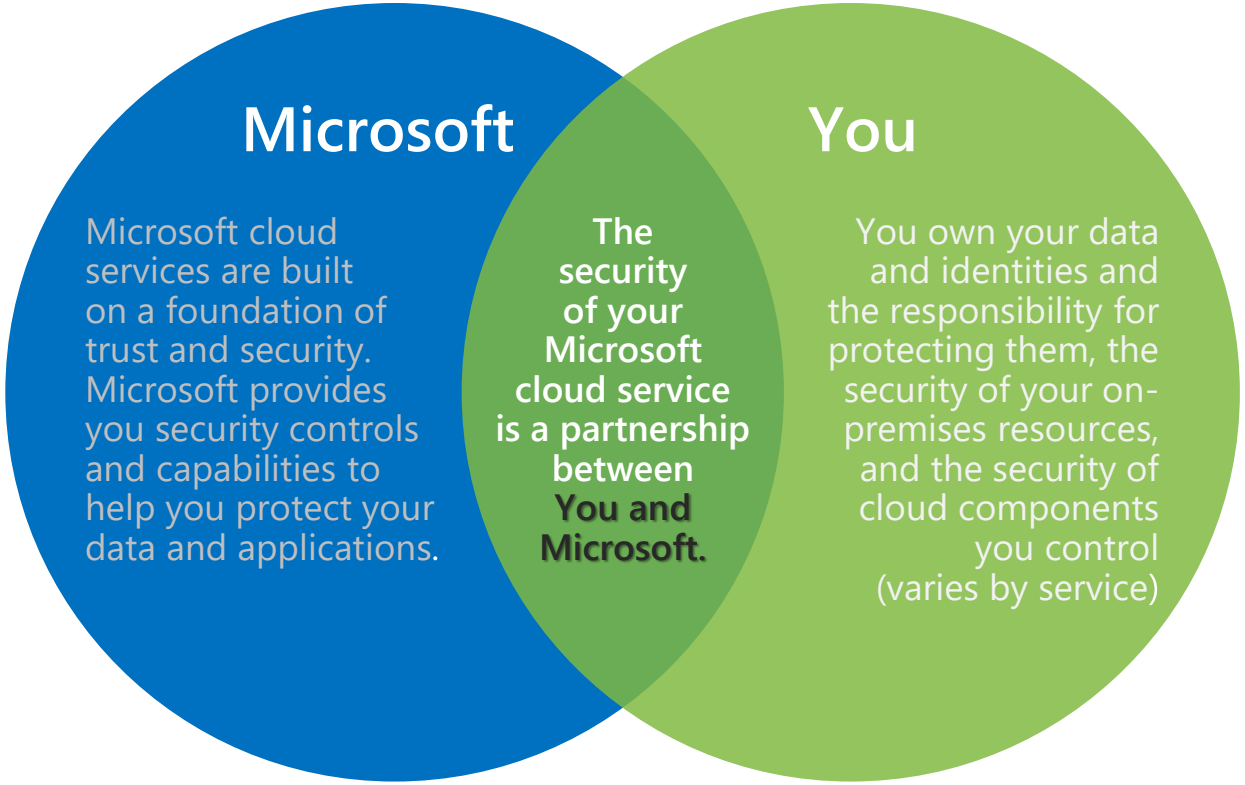
https://aka.ms/apac-enablement-check-in

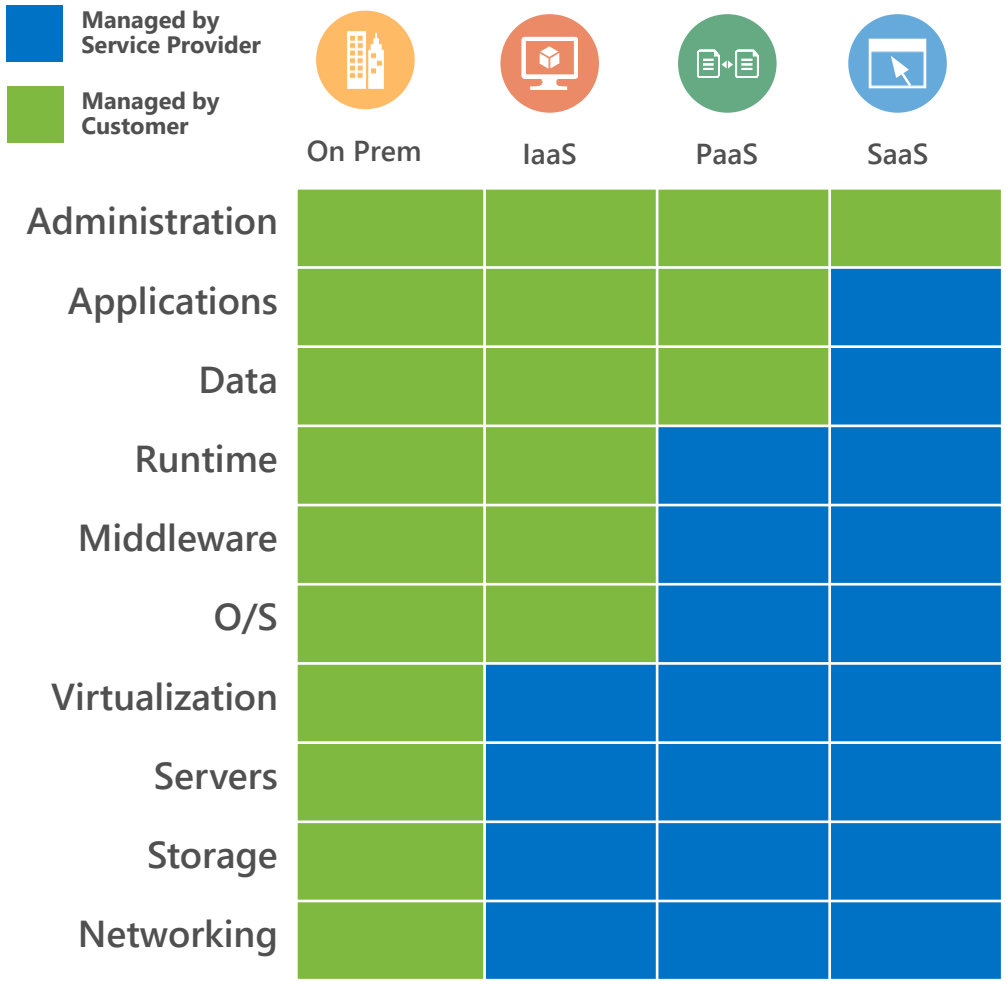
https://aka.ms/apac-sap-enablement

Agenda

1. Security Model
2. Azure Security Services
3. Azure Defender
4. Security Management
5. Running a secured Global SAP instance on Azure

Cloud Services Security is a Shared Responsibility





Technical Details on Azure internal architecture

Most current information in documentation

https://docs.microsoft.com/en-us/azure/security/azure-security-infrastructure

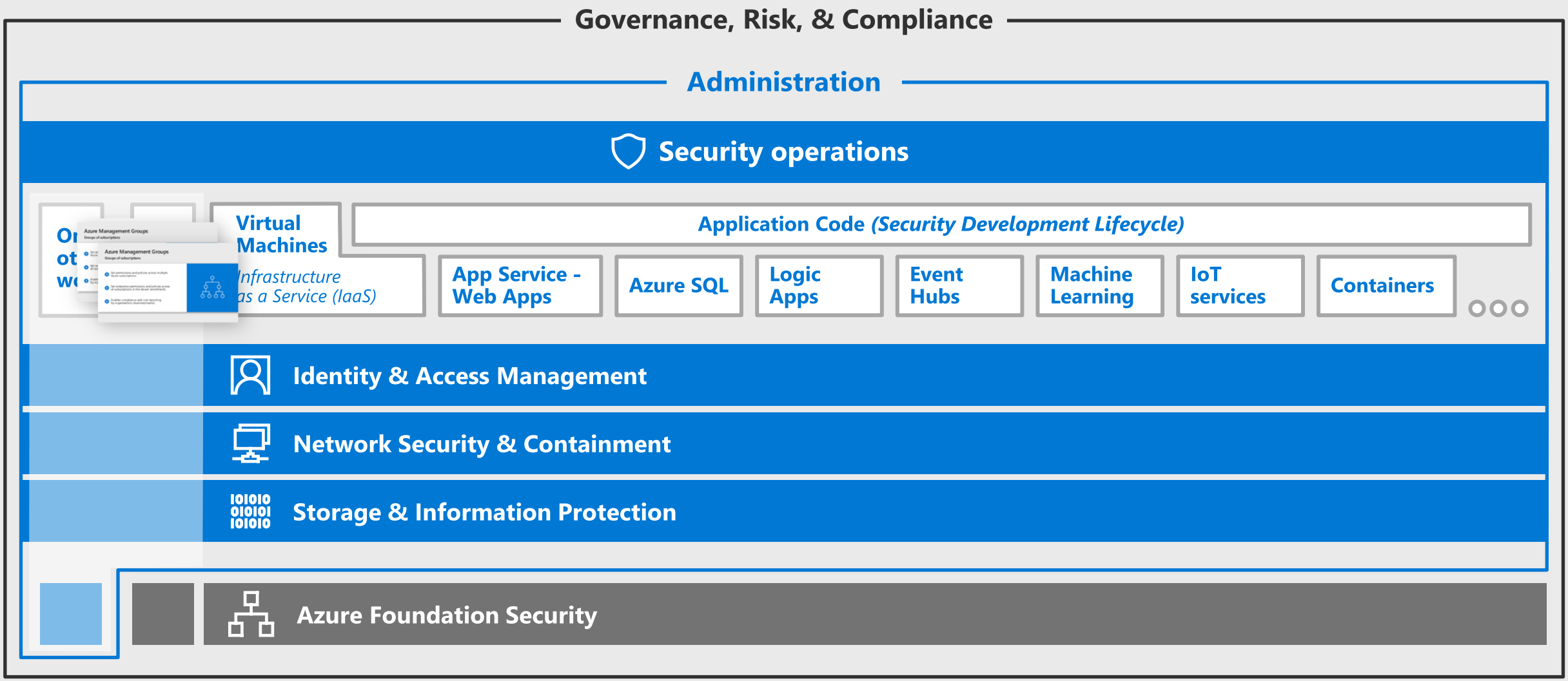
3rd party validated information in Service Trust Portal (STP) -

https://servicetrust.microsoft.com/ - *Requires NDA*

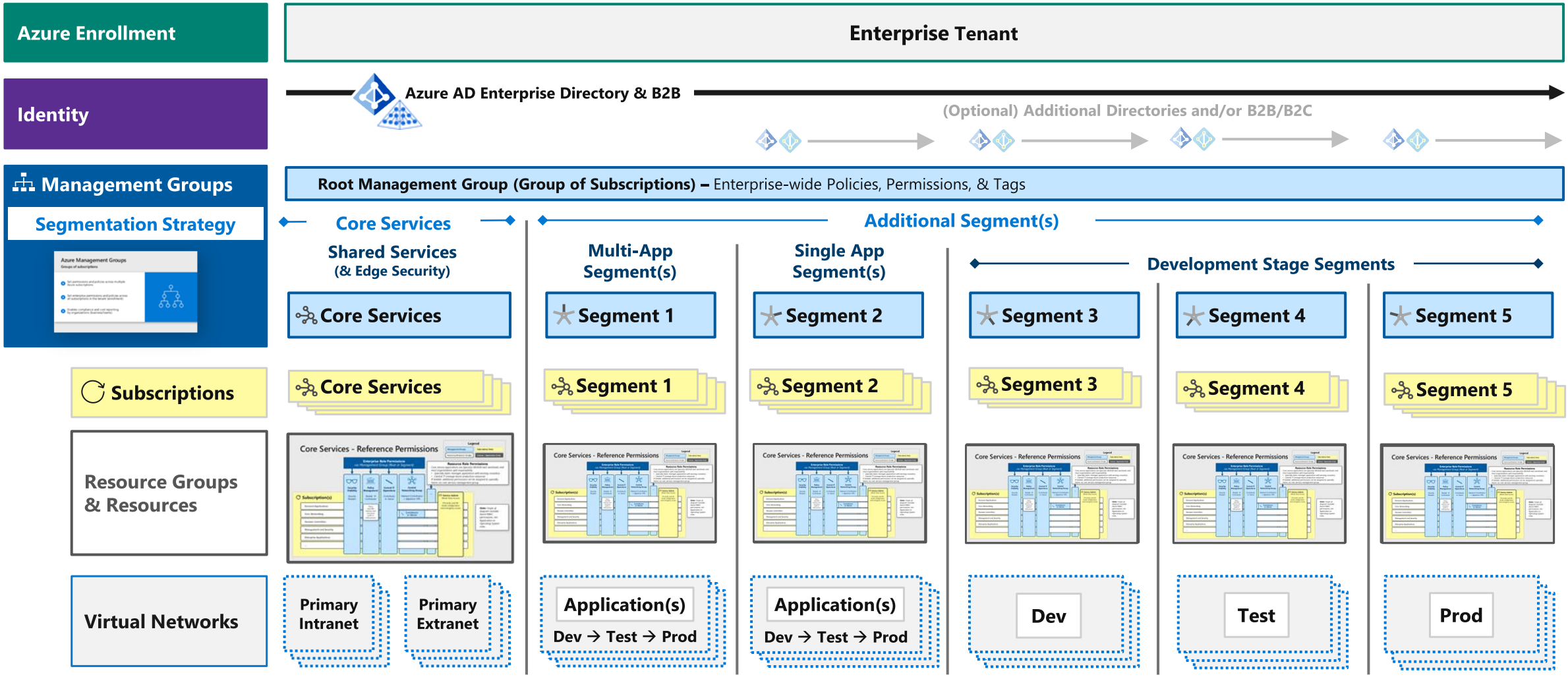
Most frequently requested information is:

- Azure & Azure Government SOC 2 Type 2 Report (in STP)
- Azure - FedRAMP Moderate System Security Plan (in STP)
- Cloud Security Alliance (CSA) STAR Self-Assessment https://www.microsoft.com/en-us/trustcenter/compliance/csa-self-assessment
- CIS Benchmark - https://azure.microsoft.com/en-us/resources/cis-microsoft-azure-foundations-security-benchmark/

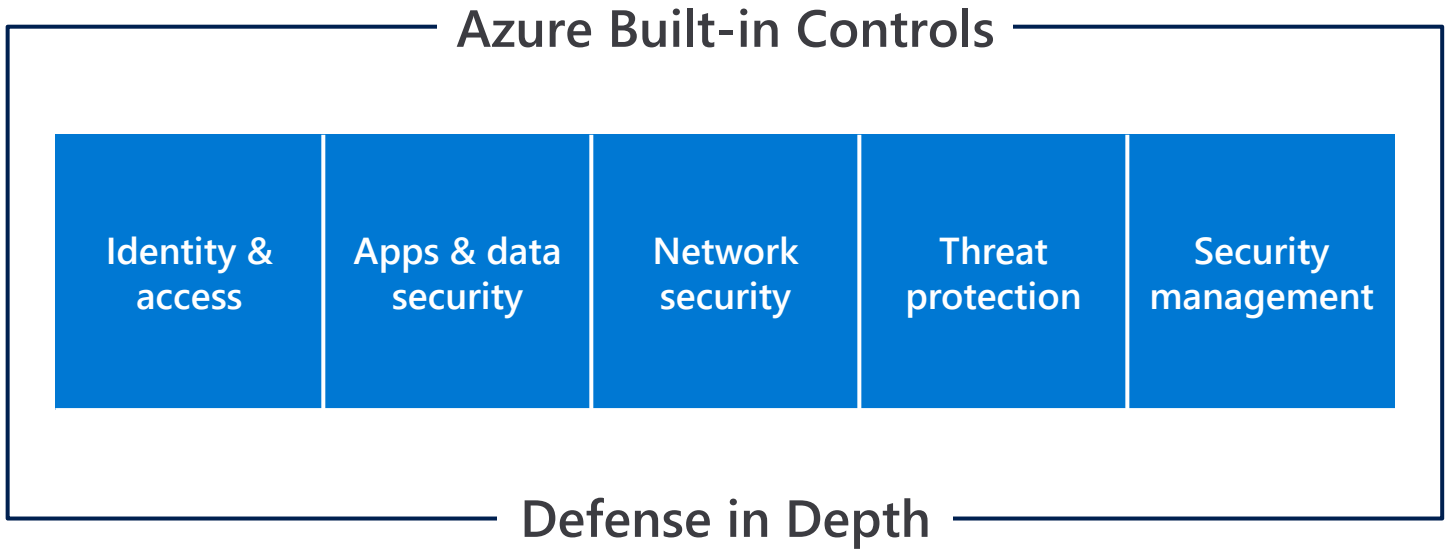
Azure Security Reference Model



Reference Design - Azure Administration Model



Technology


Azure Built-in Controls
Identity & access
Apps & data security
Network security
Threat protection
Security management
Defense in Depth

Agenda

1. Security Model
2. Azure Security Services
3. Azure Defender
4. Security Management
5. Running a secured Global SAP instance on Azure

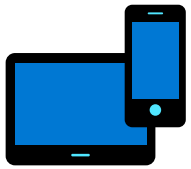
Security Services

Identity and access management

Identity and access management

Secure identities to reach zero trust

Secure authentication, Conditional Access, MFA, SSO



Role based access control, Privileged Identity Management

Identity protection, User Lifecycle Management

Best practices - Identity & Access Management

Centralize Identity management. Designate a single Azure AD directory as the authoritative source.

Enforce SSO and Multi Factor Authentication.

Leverage Azure RBAC with Privileged Identity Management.

Actively monitor for suspicious activities using AAD anomaly reports.

Use Azure AD for storage authentication.

Security Services

Apps and data security

Control data through its lifecycle

Standard Data Protection		Protect data in use

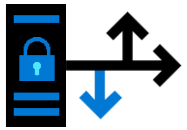
At rest

Encrypt data when stored in blob storage, database, etc.

Examples:

Azure Storage Service Encryption

SQL Server Transparent Database Encryption (TDE)



In transit

Encrypt data that is flowing between untrusted public or private networks

Examples:

HTTPS

TLS

In use

Protect/Encrypt data that is in use during computation

Examples:

Trusted Execution Environments such as Intel SGX and VBS

Homomorphic encryption

Azure Data Encryption

Layers (and why each is important)

Encrypt Documents and unstructured data

- Regulatory requirements
- Data Leakage (malicious or inadvertent)

Application Layer Encryption

- Meet regulatory requirements
- Mitigate against attacks on cloud provider/infrastructure

Azure Service Encryption

- Same as application layer
- Near zero management effort (for Microsoft managed key)

Virtual Machine / Operating Systems

- Mitigate against loss/leakage of VM Disks from storage account

Storage System

- Mitigate against attacks on cloud provider/infrastructure
- On by default and unable to disable

Encryption Technologies

- Azure Information Protection (AIP) or 3rd party solutions

- **BYO Encryption** - .NET Libraries, client-side encryption, etc.

- **SQL** Transparent Data Encryption, Always Encrypted>
- **HDInsight** Encryption
- **Azure Backup** Encrypted at Rest**,** Encrypted VM support

- **Azure Disk Encryption** - *<BitLocker [Windows], DM-Crypt [Linux]>*
- **Partner Volume Encryption** – <CloudLink® SecureVM, Vormetric, etc.>
- **BYO Encryption** – <Customer provided>

- **Azure Storage Service Encryption (server side encryption)** *<AES-256, Block, Append, and page Blobs>*

Azure Storage

Azure Cloud Storage:

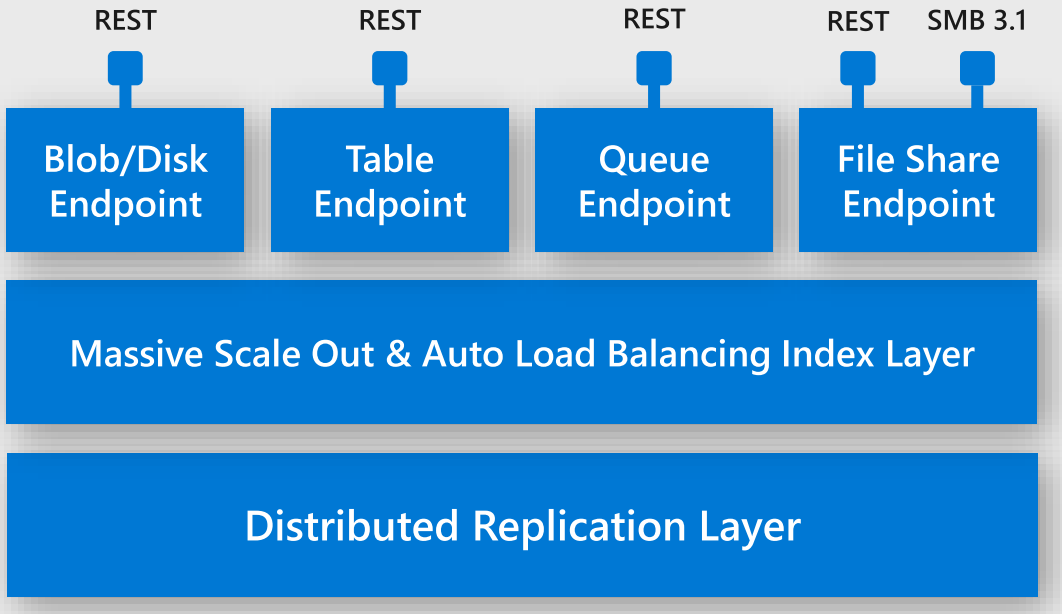
- Object based, durable, massively scalable storage
- Designed from ground up by Microsoft
- Presents as Blobs, Disks, Tables, Queues and Files
- Accessed via REST APIs, Client Libraries and Tools

Access Control

- Azure Active Directory (Azure AD)
- Symmetric Shared Key Authentication
- Shared Access Signature (SAS)

Notable Security Attributes

- All data is encrypted by the service
- No read without write (mitigate cross-tenant data leaks)
- Maintains 3 Synchronous copies of data
- Virtual storage, not dedicated disks
- Detailed activity logging availability (Opt in)
- Data will remain only in the region you choose



More Information

Storage System Design and Architecture:

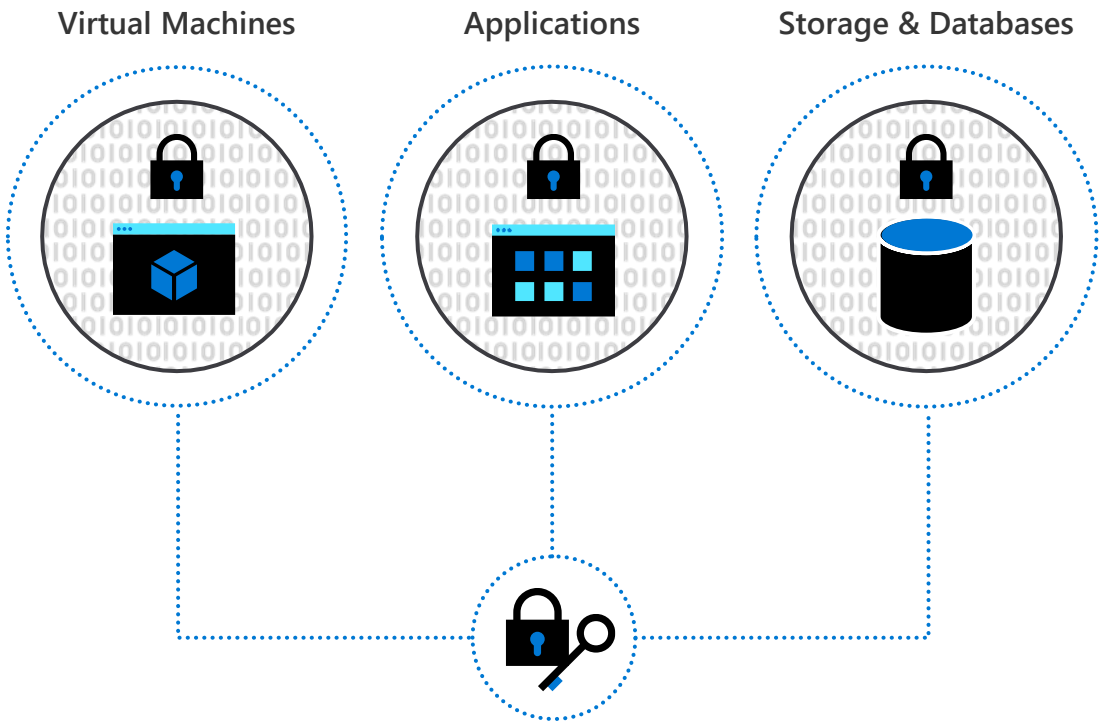
Azure Storage Managed Disks

Safeguard cryptographic keys and other secrets used by cloud apps and services

Encrypt keys and small secrets using keys in Hardware Security Modules (HSMs)

Simplify and automate tasks for SSL/TLS certificates, enroll and automatically renew certificates

Rapidly scale to meet the cryptographic needs of your cloud applications and match peak demand



Key, Secrets & Certificate Management- Azure Key Vault

Azure Storage Firewalls

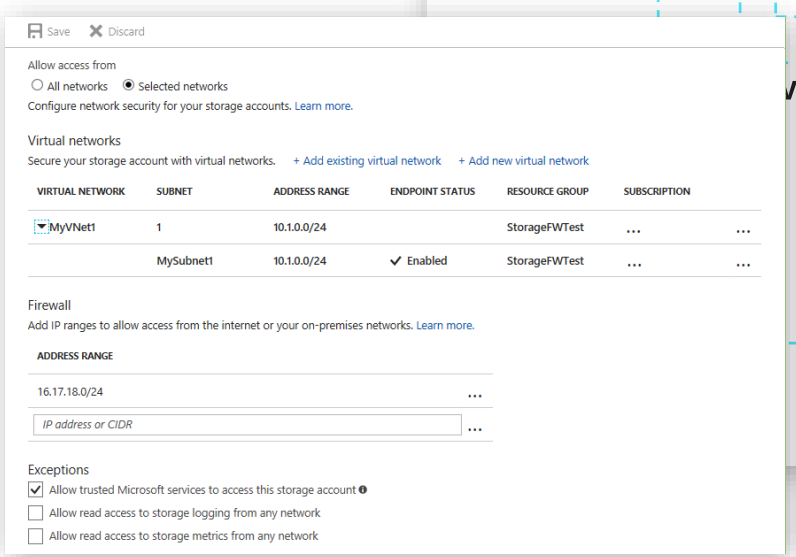
Configured on each Storage Account
(prompt during creation)

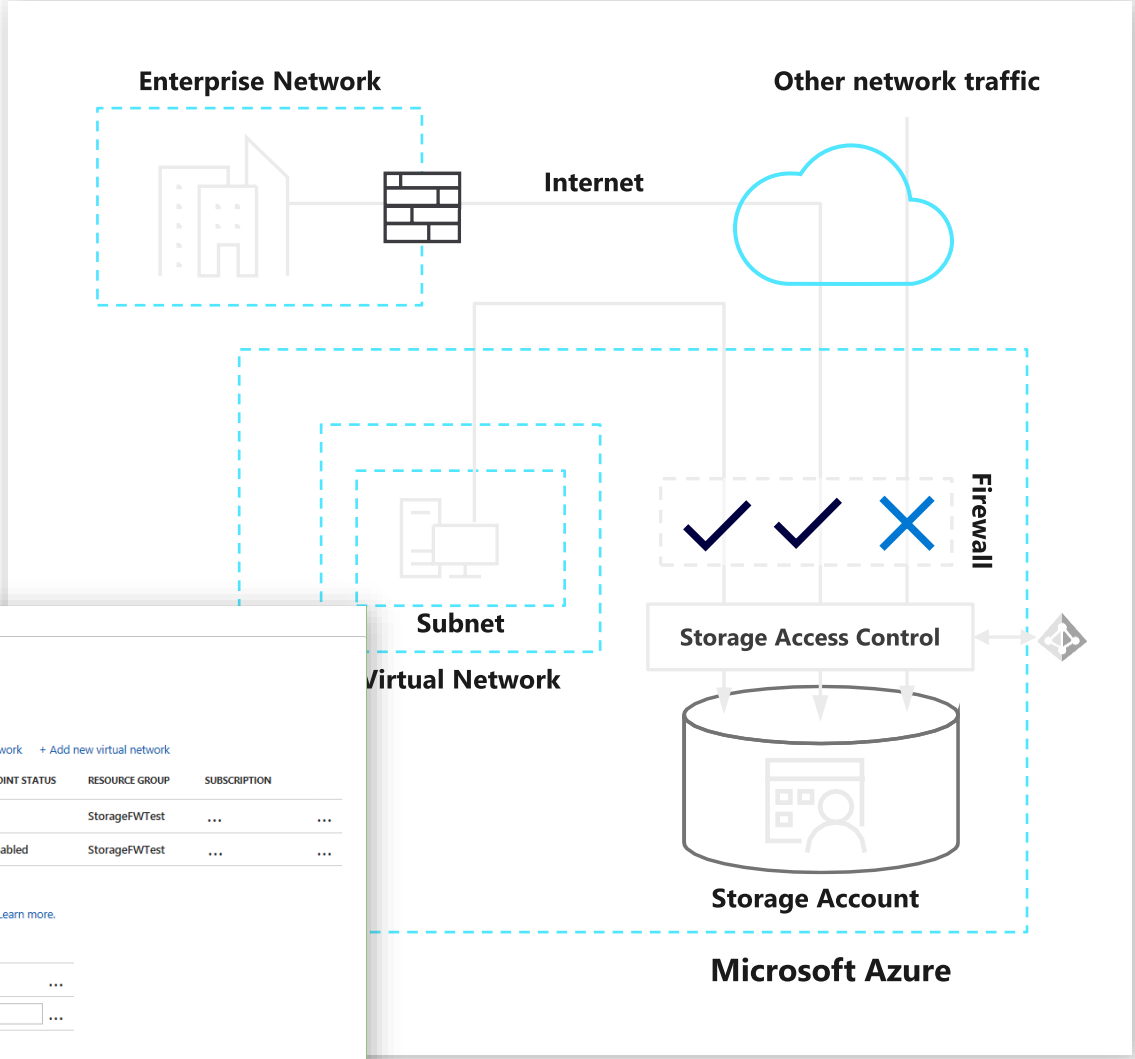
- Controls network access using ACLs
- Enforced on all network protocols
- If not configured, all networks can access

Authentication is still required
to access storage (Azure AD, SAS tokens, etc.)

Access by Azure Services
must be configured to allow connection (checkbox)

- VM Access to VM Disks not affected by storage firewall
- https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security

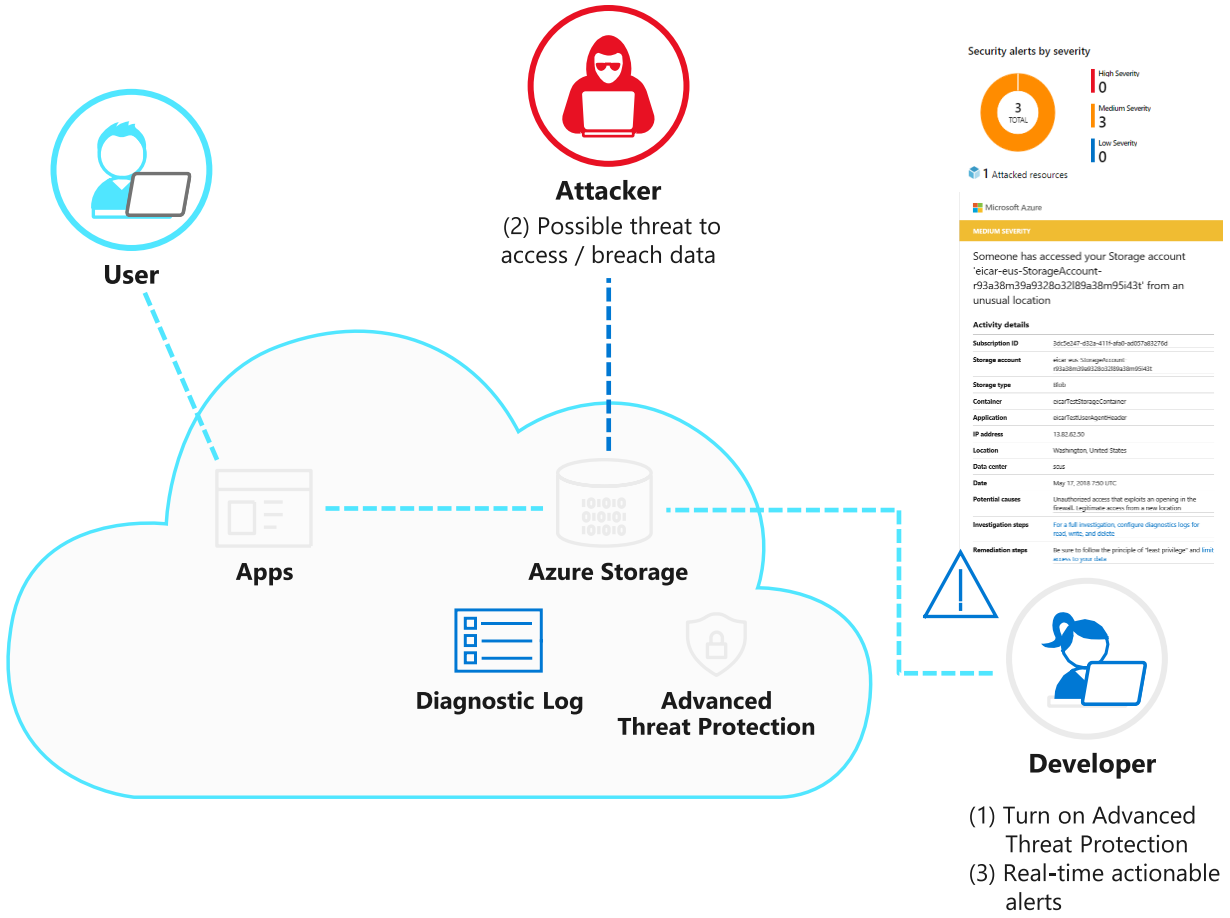




Azure Defender for Azure Storage

- Alerts on **anomalous access** & potential **data exfiltration**
- Investigation & remediation guidance
- Alerts in Azure Security Center

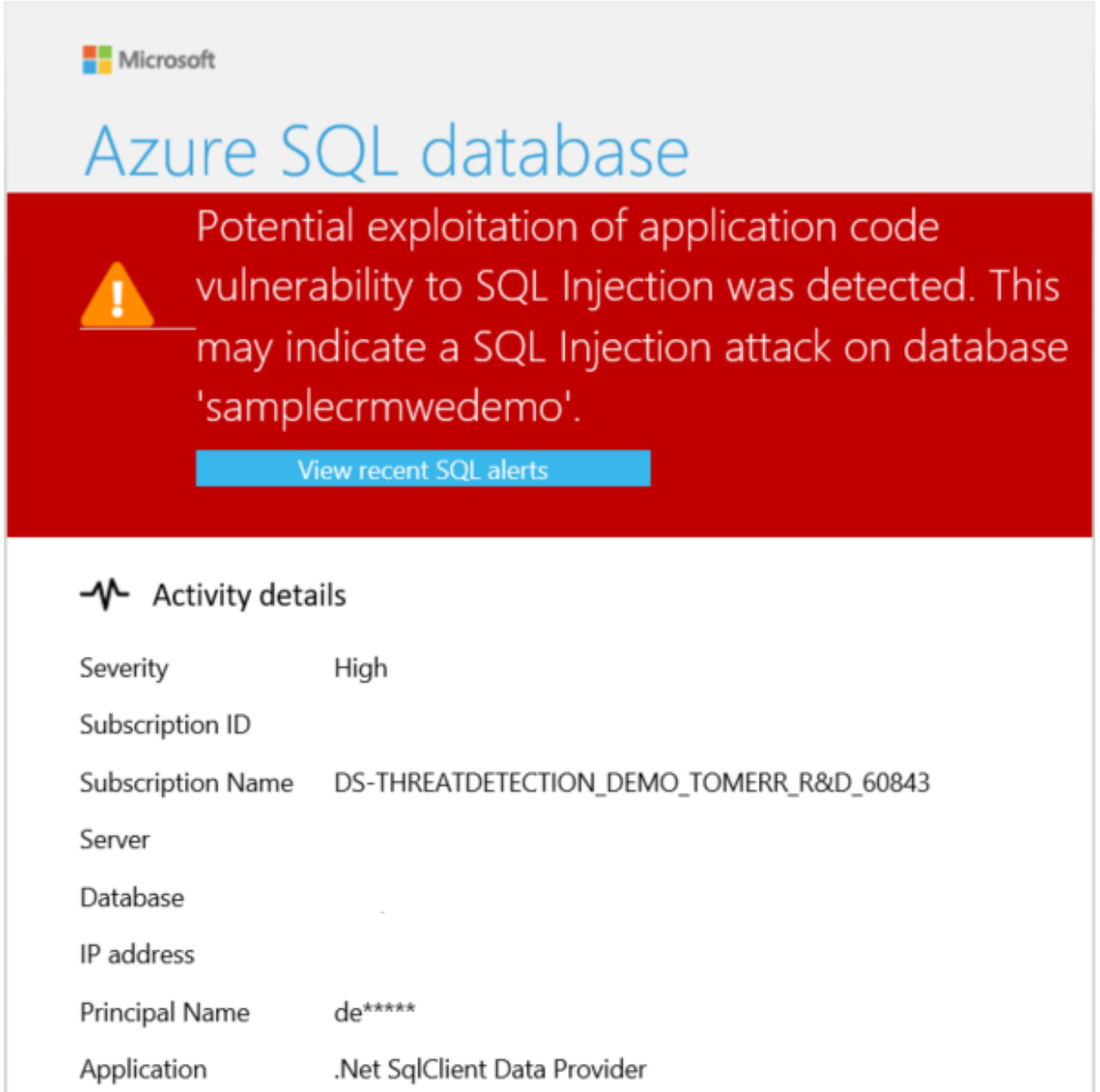
https://docs.microsoft.com/en-us/azure/storage/common/storage-advanced-threat-protection



Advanced Threat Protection for Azure SQL Database

- Alerts on **anomalous database activities** & **unusual access** or **exploit of database**
- Alerts in Azure Security Center
- For a full investigation experience, it is recommended to enable [SQL Database Auditing]

https://docs.microsoft.com/en-us/azure/sql-database/sql-database-threat-detection-overview



Best practices – Apps and Data security

Leverage Key Vault to store cryptographic keys and secrets. Control access through RBAC

Manage Azure Key Vault access at Management plane and Data plane

Encrypt data and rest and data in transit. Use client-side encryption for high value data

Leverage Advance Data Security (ADS) for Azure SQL

Leverage Azure Security Center to identify assets that do not have encryption at rest enabled

Security Services:

Network security

Network protection services enabling zero trust

DDoS protection

DDOS protection tuned to your application traffic patterns

Web Application Firewall

Centralized inbound web application protection from common exploits and vulnerabilities

Azure Firewall

Centralized outbound and inbound (non-HTTP/S) network and application (L3-L7) filtering

Network Security Groups

Distributed inbound & outbound network (L3-L4) traffic filtering on VM, Container or subnet

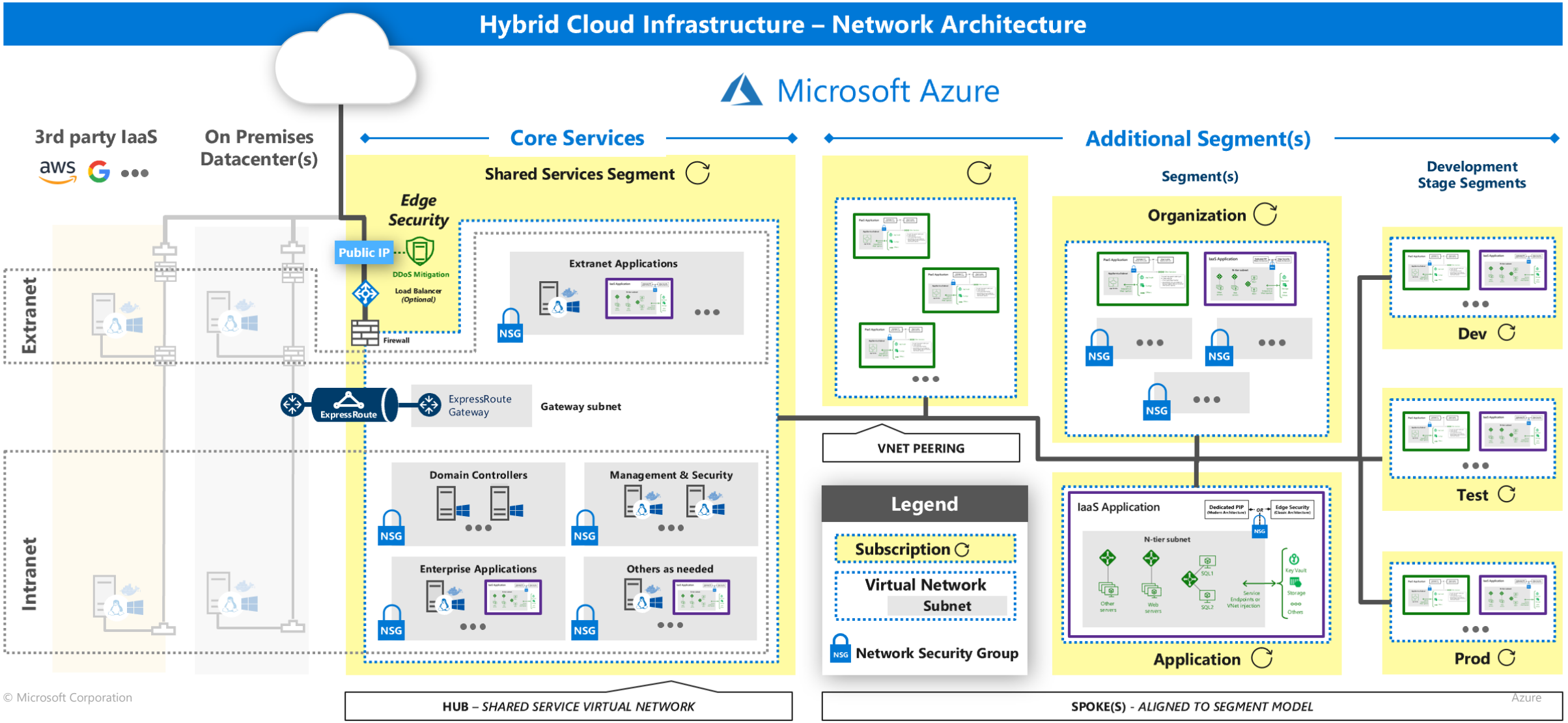
Service Endpoints

Restrict access to Azure service resources (PaaS) to only your Virtual Network

Application protection

Micro segmentation

Reference Enterprise Design - Azure Network Security



Best practices – Network Security

Adopt a Zero Trust approach

Control routing behavior and avoid implications of default routes

Disable RDP/SSH Access to virtual machines over internet

Choose whether to use Native Azure Controls or 3rd party Network Virtual Appliances (NVAs) for internet edge security (North-South)

Simplify NSG rule management by defining application security groups (ASGs)

Agenda

1. Security Model
2. Azure Security Services
3. Azure Defender
4. Security Management
5. Running a secured Global SAP instance on Azure

Azure Security Center

Strengthen multi cloud security posture

Secure Score | Policies and compliance | Improved automation

Leveraging Azure Arc

Protect your hybrid cloud with Azure Defender

For servers | For cloud native workloads | For databases and storage

For Azure service layers | For IoT devices

Streamline security management

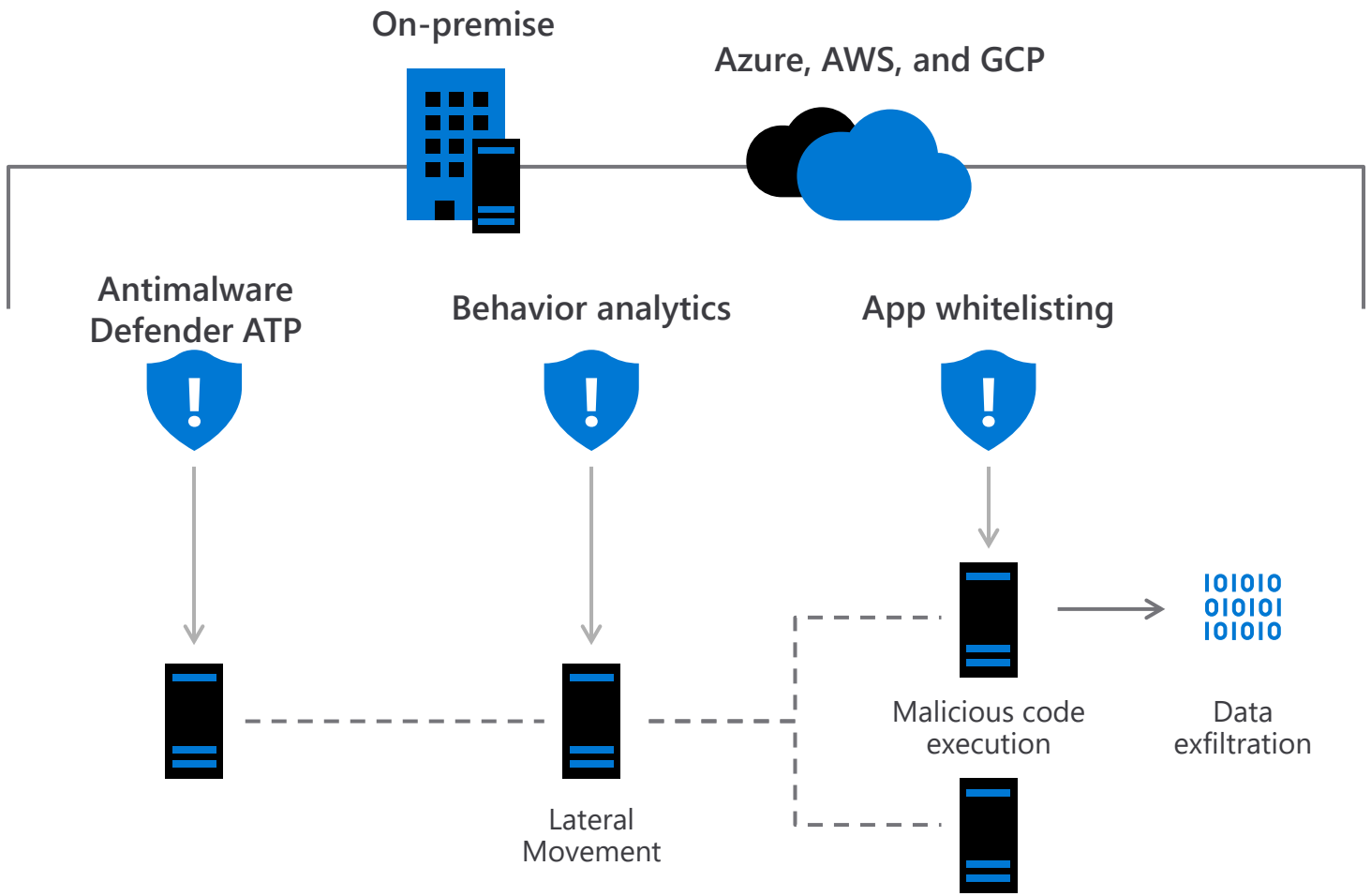
Protect Linux and Windows servers from threats

Reduce open network ports

- Use Just-in-Time VM to control access to commonly attacked management ports
- Limit open ports with adaptive network hardening

Block malware with adaptive application controls

Protect Windows servers and clients with the integration of Microsoft Defender ATP and Linux servers



Protect your workloads from threats

Use industry's most extensive threat intelligence to gain deep insights

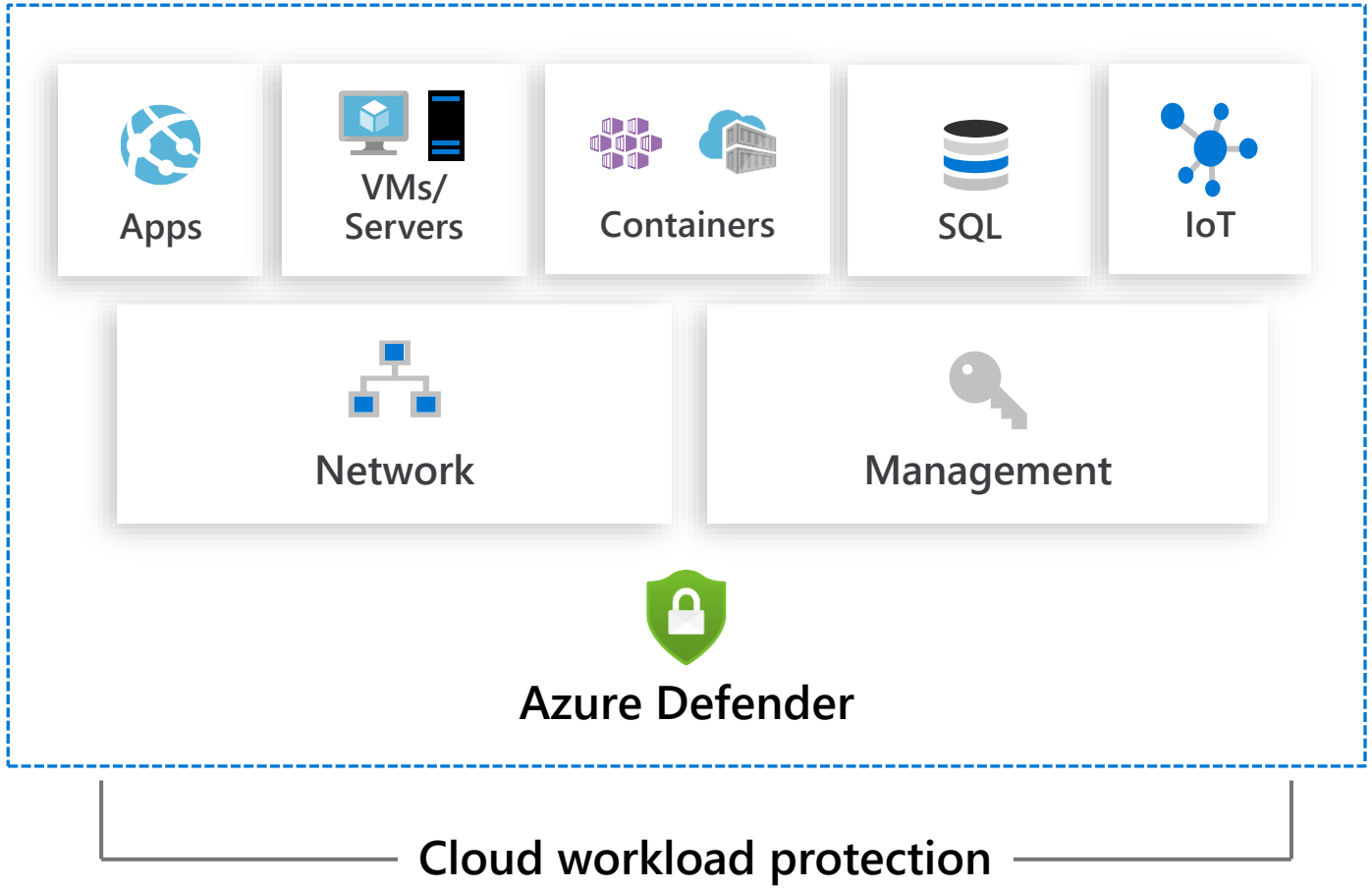
Detect & block advanced malware and threats for Linux and Windows Servers on any cloud

Protect cloud-native services from threats

Protect data services against malicious attacks

Protect your Azure IoT solutions with near real time monitoring

Service layer detections: Azure network layer and Azure management layer (ARM)



Threat Detection - How Azure Defender detects threats?

Integrated Threat Intelligence

Threat Intel from Microsoft Cloud Services, DCU, MSRC and third parties

Behavioral Analytics

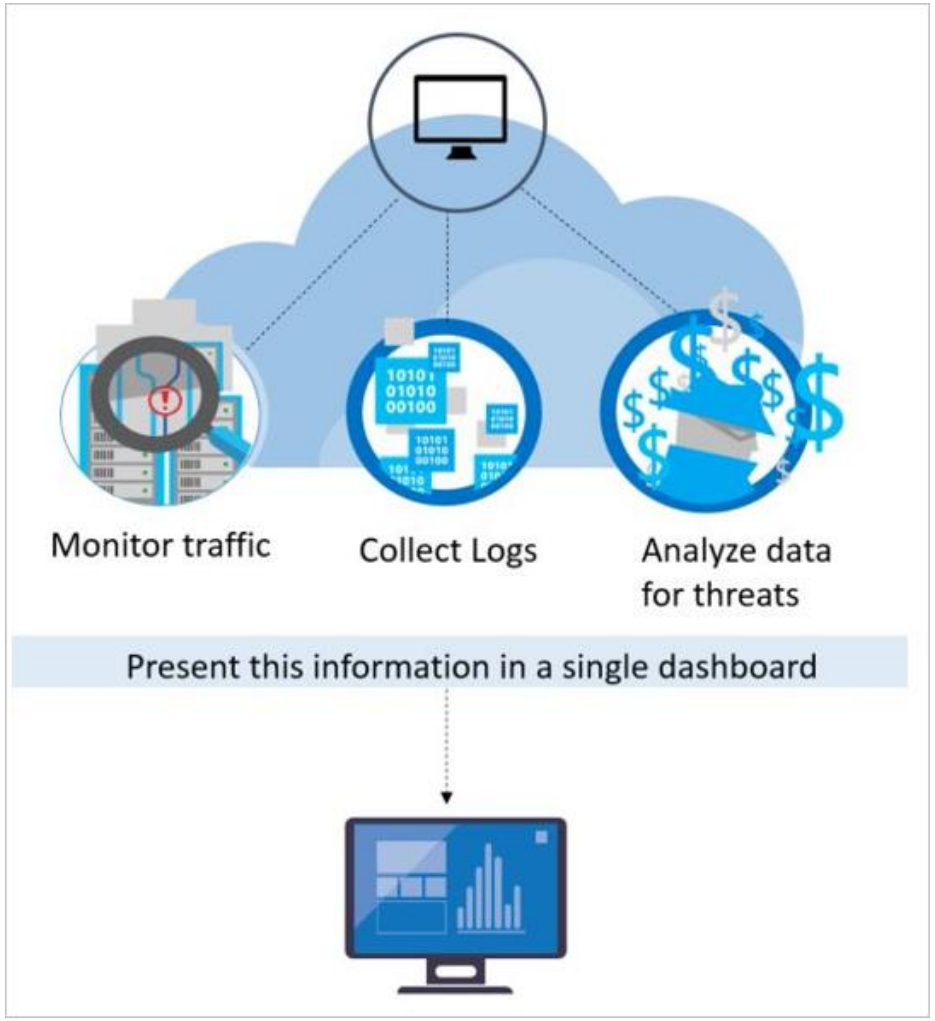
Behavioral analytics achieved by comparing data to collection of known patterns, determined through complex ML.

Anomaly Detection

Personalized and focuses detection on baselines that are specific to your deployments

https://docs.microsoft.com/en-us/azure/security-center/security-center-alerts-overview

Azure Defender



Agenda

1. Security Model
2. Azure Security Services
3. Azure Defender
4. Security Management
5. Running a secured Global SAP instance on Azure

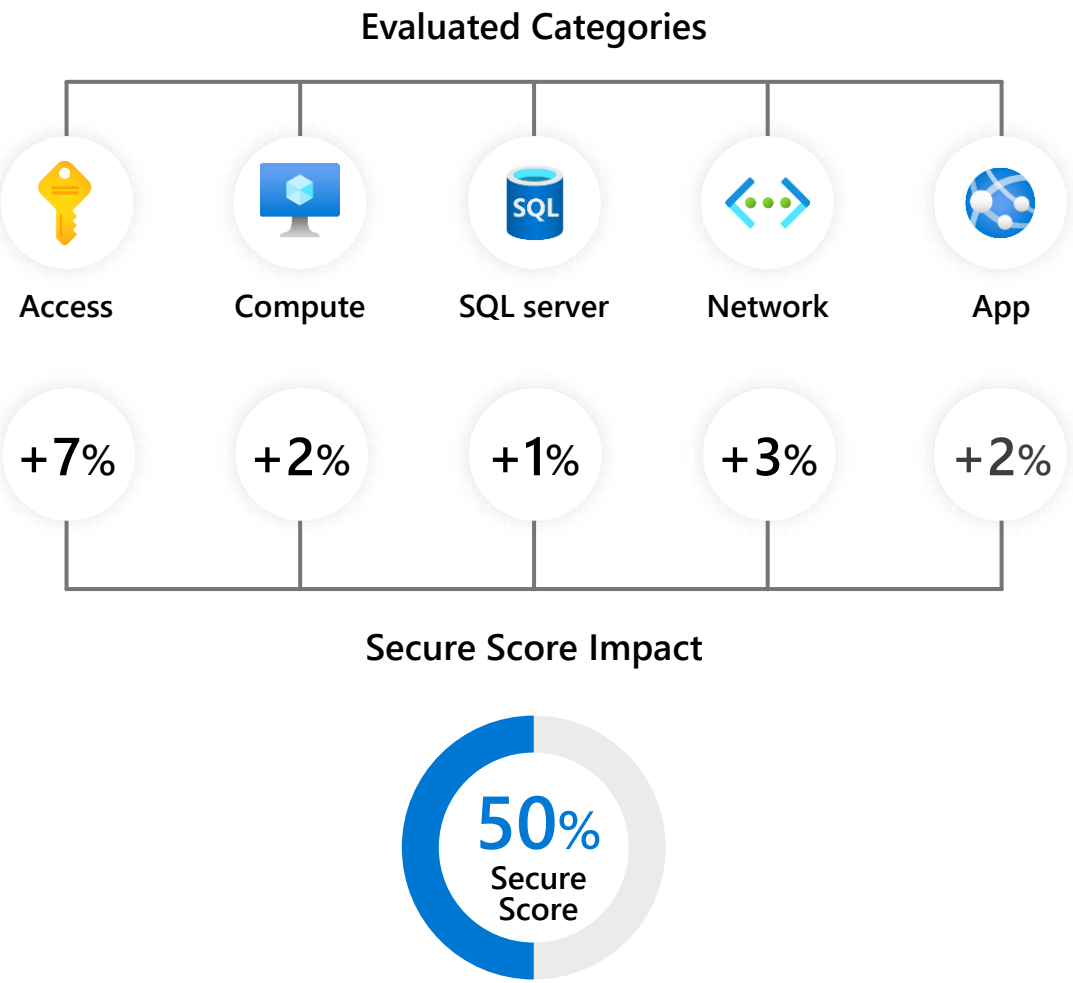
Security posture management with Secure Score

Gain instant insight into the security state of your cloud workloads

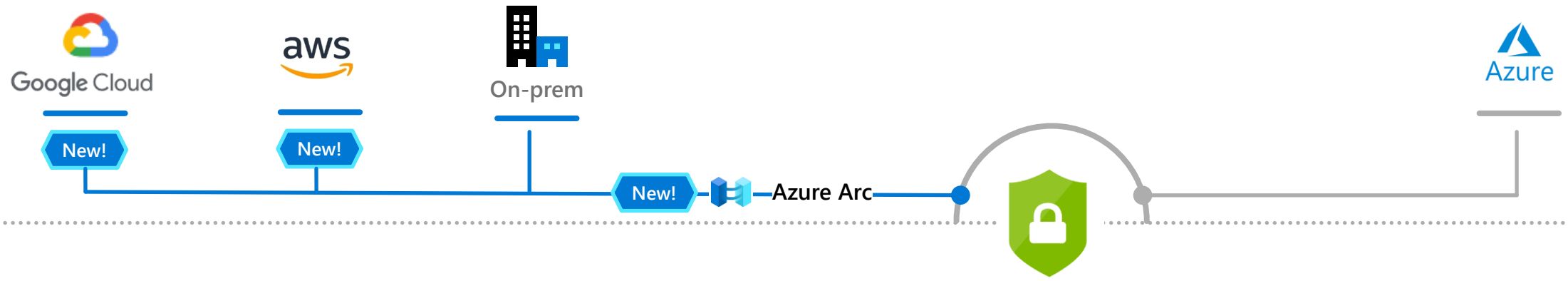
Address security vulnerabilities with prioritized recommendations

Improve your Secure Score and overall security posture in minutes

Speed up regulatory compliance

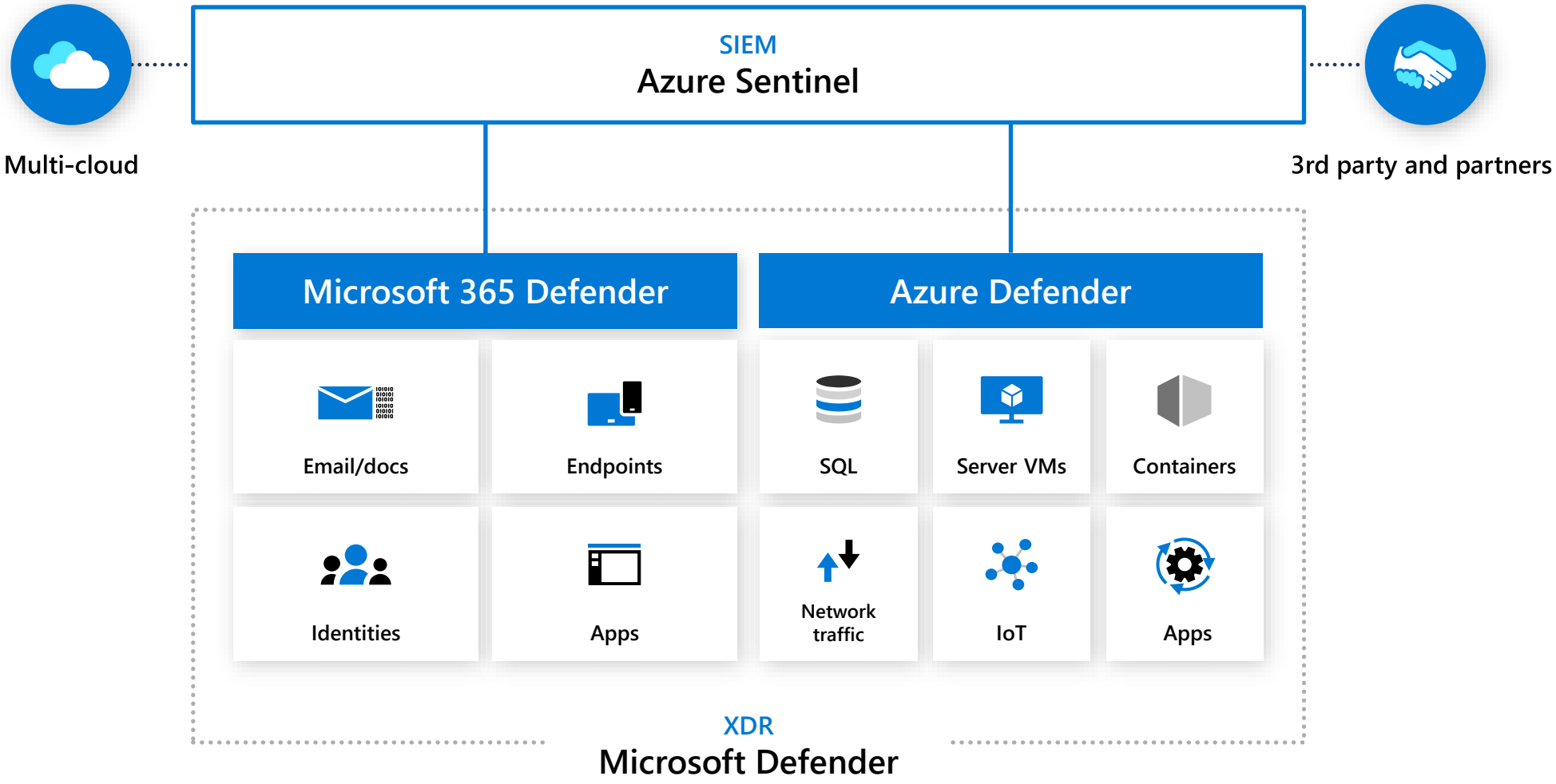


Protect hybrid workloads



Server hygiene	Secure score	Policy	VA (powered by Qualys)
Advanced protection	Application control	JIT VM Access	File Integrity Monitoring
Detection & response	Threat detection (powered by MDATP)	SIEM integration	Export & Automation

Integrated threat protection for your enterprise



Azure security

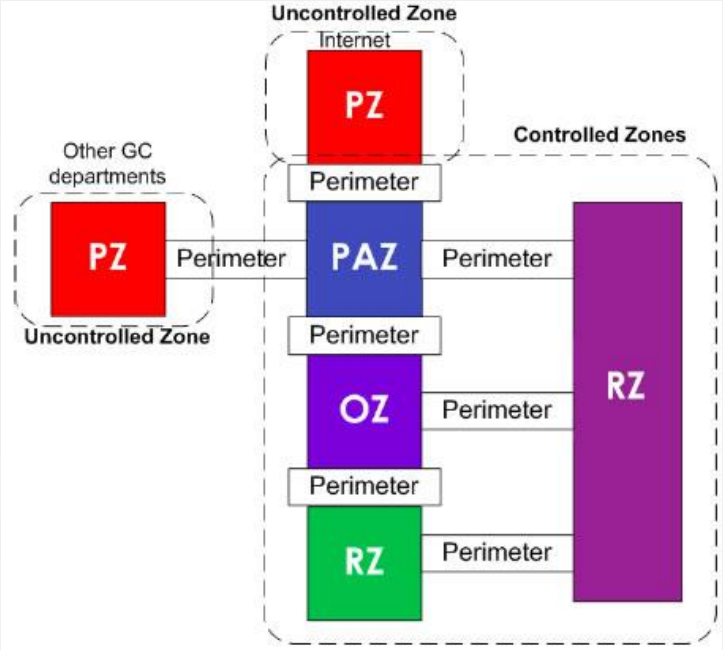
Defense in Depth

Identity & access	Apps & data security	Network security	Threat protection	Security management
Role based access	Encryption	DDoS Protection	Antimalware	Log Management
Multi-Factor Authentication	Confidential Computing	NG Firewall	AI Based Detection and Response	Security Posture Assessment
Central Identity Management	Key Management	Web App Firewall	Cloud Workload Protection	Policy and governance
Identity Protection	Certificate Management	Private Connections	SQL Threat Protection	Regulatory Compliance
Privileged Identity Management	Information Protection	Network Segmentation	IoT Security	SIEM

Microsoft + Partners

Security baseline for SAP

Scope Security Requirements



- Determine the corporate IDS/IPS posture for public cloud.
- Review NVA architecture and limits from a UDR and BGP routing perspective
- Determine if horizontal scale can be achieved by a system agent rather than traffic pattern matching
- What is the zoning model? https://www.cse-cst.gc.ca/en/node/266/html/27445
- Review AAD and Subscription security boundary constructs
- Match security posture to network posture

Scope Security Requirements

- Review data security requirements as it pertains to AAA/RBAC as well as EFS or encryption requirements.
- Ensure backup solution matches the posture
- Ensure backup retention has suitable compensation and controls for audit compliance
- Review logging requirements for accessibility and security

High Risk (Confidential)	Moderate Risk (Restricted)	Low Risk (Public)
• Protected health information • Personally identifiable information • Financial data • Employment records • Research data involving human subjects • User account or system passwords providing access to above elements	• Student records, except where covered under high risk • Unpublished research data • De-identified health-related research data • WCM operational data • WCM intellectual property • Donors or potential donors • Information security data • Other internal WCM data, limited by intention or discretion of author or owner	• WCM public websites • Public Directory data • Publicly available research data sets • Published research • Press releases • Job postings

Security Baseline for SAP on Azure

- Assessment of security posture and compliance requirement
- Mapping to Azure native security services and features
- Enablement of Cloud-based Threat Detection, Investigation and Response

Role-based Access Control

Threat Detection

Identify and Access Management

Encryption at Rest

Encryption in Transit

Network Segmentation

Compliance Monitoring

SAP on Azure – Native Security Controls

Identity and Access Management

Network Security

Data security

Security posture management
(CSPM)

Threat protection
(CWPP)

Security Operations

SAP on Azure – Native Security Controls

Identity and Access Management

- Build zero trust approach to security for both SAP admins and end users using Azure AD SSO, Conditional Access and MFA.
- Leverage existing Azure AD based credentials, MFA and RBAC controls for SAP.
- Use Azure AD privileged identity management for time bound and approval-based access to resources on Azure.
- Resource locking to prevent accidental/unintentional deletion or modification of SAP on Azure environment.

SAP on Azure – Native Security Controls

Network Security

- Secure hybrid connectivity - Azure ExpressRoute already in place and provides secure private connection.
- Network segmentation – Azure Network Security groups and Application Security Groups for micro segmentation on Azure
- Public endpoints – DDoS protection, App Gateway, Azure Front Door, WAF and Azure Firewall or NVAs
- Leverage Azure Bastion to access your environment
- Enable Just In Time access with Azure Defender

SAP on Azure – Native Security Controls

Data security

- Encryption at rest and encryption in transit controls.
- Azure key vault to store encryption keys, SSL/TLS certificates and other secrets.
- Azure Disk Encryption for SAP Application and Database servers.
- Transparent data encryption for SAP DBMS servers to encrypt data, logs and backups
- Leverage Managed Identities to access Azure services

SAP on Azure – Native Security Controls

Security posture management (CSPM)

- Track Security score, compliances and benchmarks like CIS 1.1.0, PCI DSS, SOC TSP. Define custom security baselines
- Hardening of the server OS. Vulnerability assessment for application and database servers and container images
- Updates management with Azure automation. Guest OS configurations check and DSC.
- AI/ML assisted application whitelisting recommendations and audit of unapproved executions
- Audit file and registry changes with investigation and dashboarding capabilities

SAP on Azure – Native Security Controls

Threat protection (CWPP)

- Detection of advance persistent threats using Threat Intel, AI/ML and UEBA for Azure Storage, Networking, DB services, Azure Key Vault, Containers and VMs.
- EDR and EPP for servers VMs using best in class Microsoft Defender ATP solution. Integrated natively with ASC Std, Sentinel.
- Just in time VM access and Adaptive network hardening using AI/ML assisted learning of network traffic and NSG rules

SAP on Azure – Native Security Controls

Security Operations

- Azure offers two options. Either leverage Azure Sentinel or integrate with existing third party SIEM
- Azure Sentinel comes with out of box use cases for SAP on Azure. No need to take logs, alerts out of Azure environment. Avoid egress, latency and parsing dependencies on external SIEM.
- Collect, corelate and analyze logs within Azure environment.

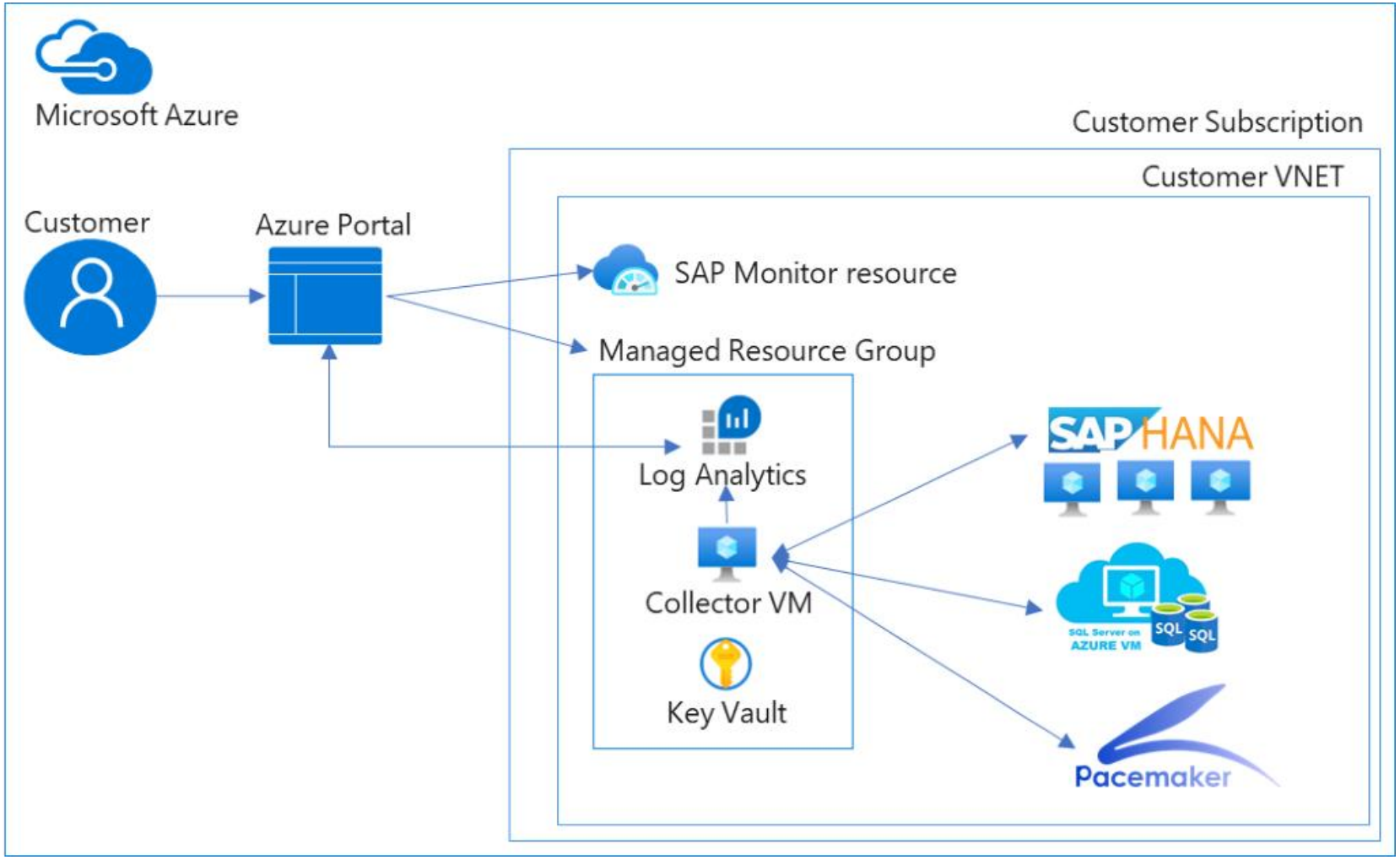
Azure Monitor for SAP- Architecture Diagram

What data does Azure Monitor for SAP solutions collect?

High-availability Pacemaker cluster telemetry:
•Node, resource, and SBD device status
•Pacemaker location constraints
•Quorum votes and ring status
•Others

SAP HANA telemetry:
•CPU, memory, disk, and network utilization
•HANA System Replication (HSR)
•HANA backup
•HANA host status
•Index server and Name server roles

Microsoft SQL server telemetry:
•CPU, memory, disk utilization
•Hostname, SQL Instance name, SAP System ID
•Batch Requests, Compilations, and page Life Expectancy over time
•Top 10 most expensive SQL statements over time
•Top 12 largest table in the SAP system
•Problems recorded in the SQL Server Error logs
•Blocking processes and SQL Wait Statistics over time



Azure Sentinel for SAP- Private Preview (NDA)

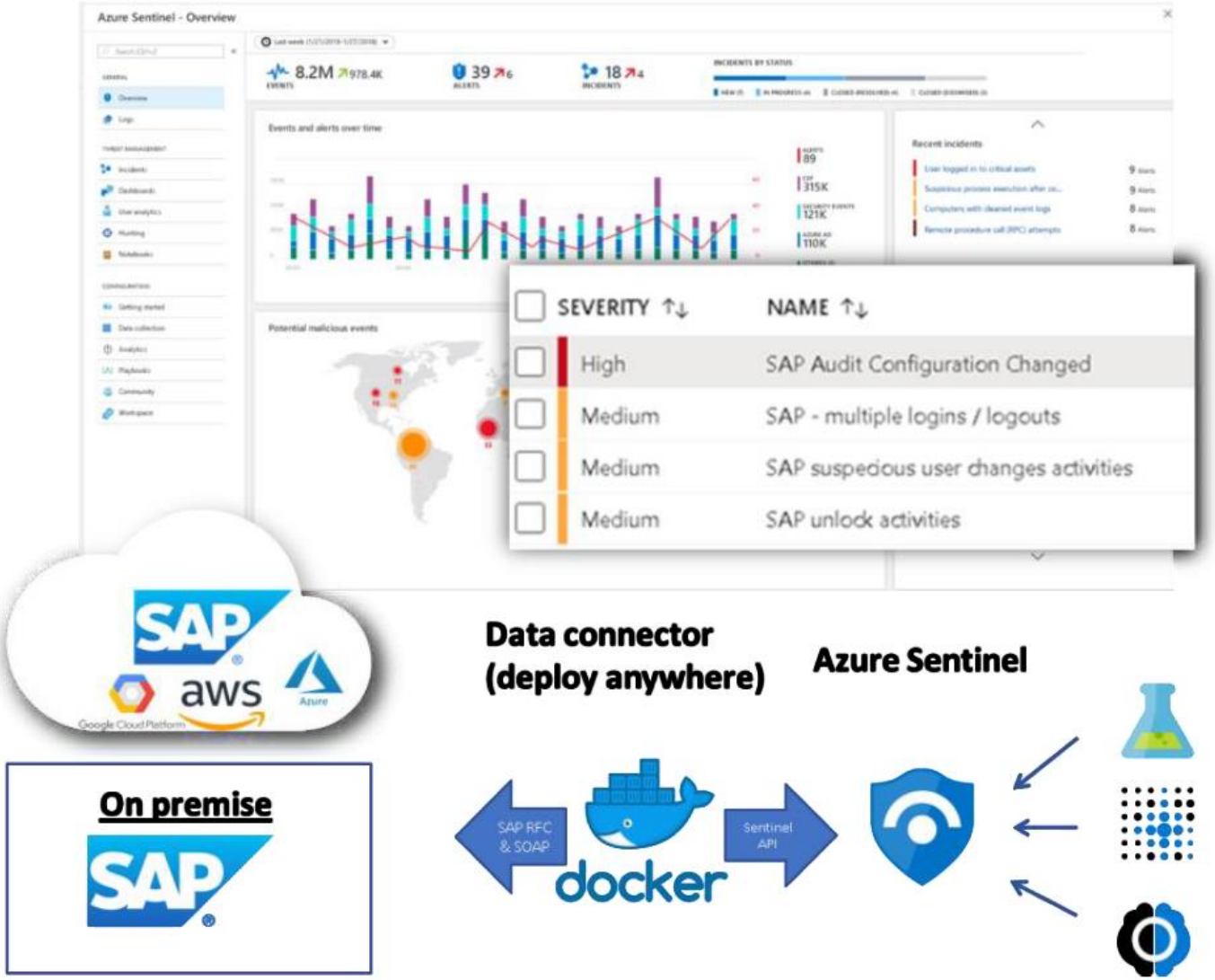
Collect data at cloud scale—across all users, devices, applications and infrastructure, both on-premises and in multiple clouds

Detect previously uncovered threats and minimize false positives using analytics and unparalleled threat intelligence from Microsoft

Investigate threats with AI and hunt suspicious activities at scale, tapping into decades of cybersecurity work at Microsoft

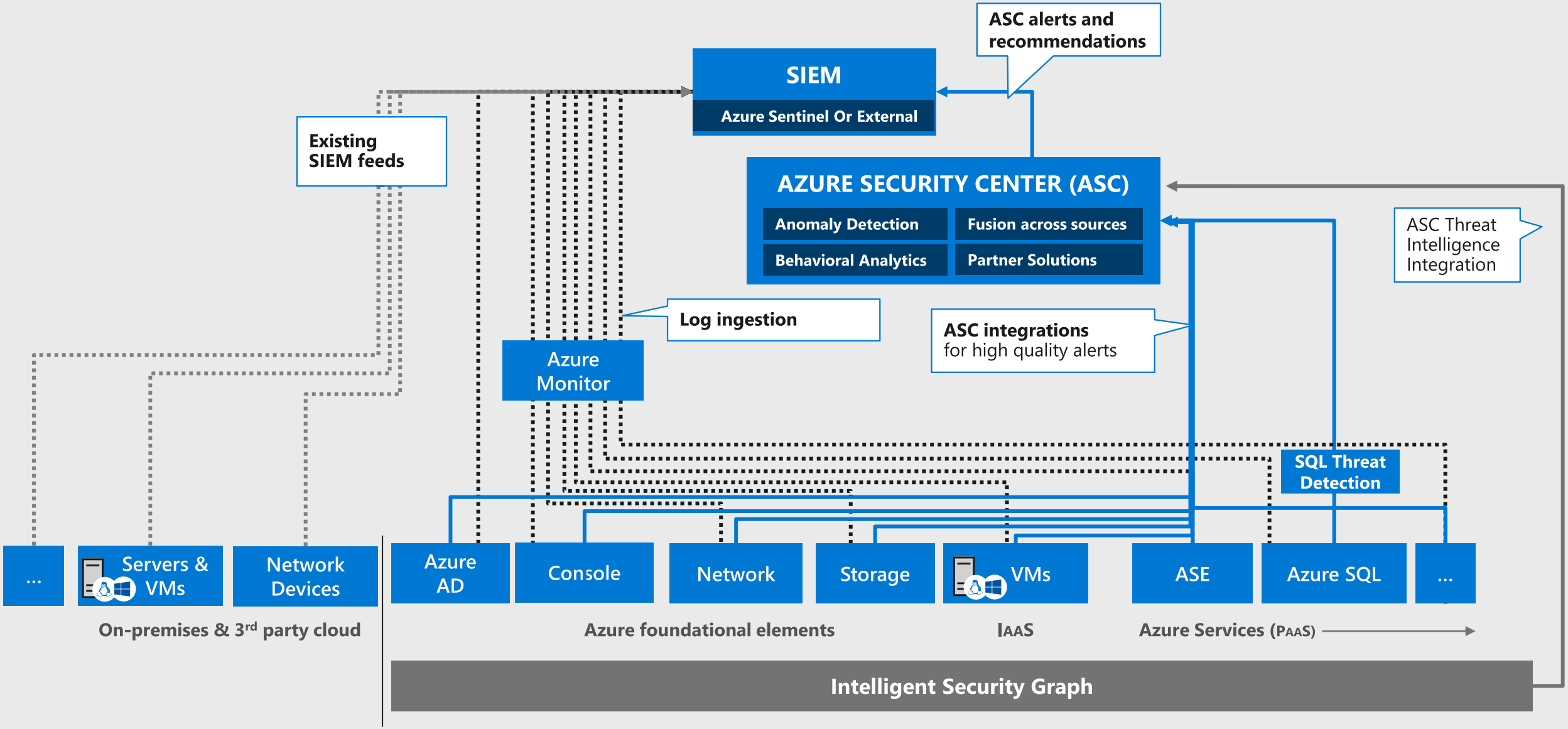
Respond to incidents rapidly with built-in orchestration and automation of common tasks

Cloud speed and scale
Invest in security, not infrastructure setup and maintenance with first cloud-native SIEM from a major cloud provider. Never again let a storage limit or a query limit prevent you from protecting your enterprise. Start using Azure Sentinel immediately, automatically scale to meet your organizational needs and only pay for the resources you need.



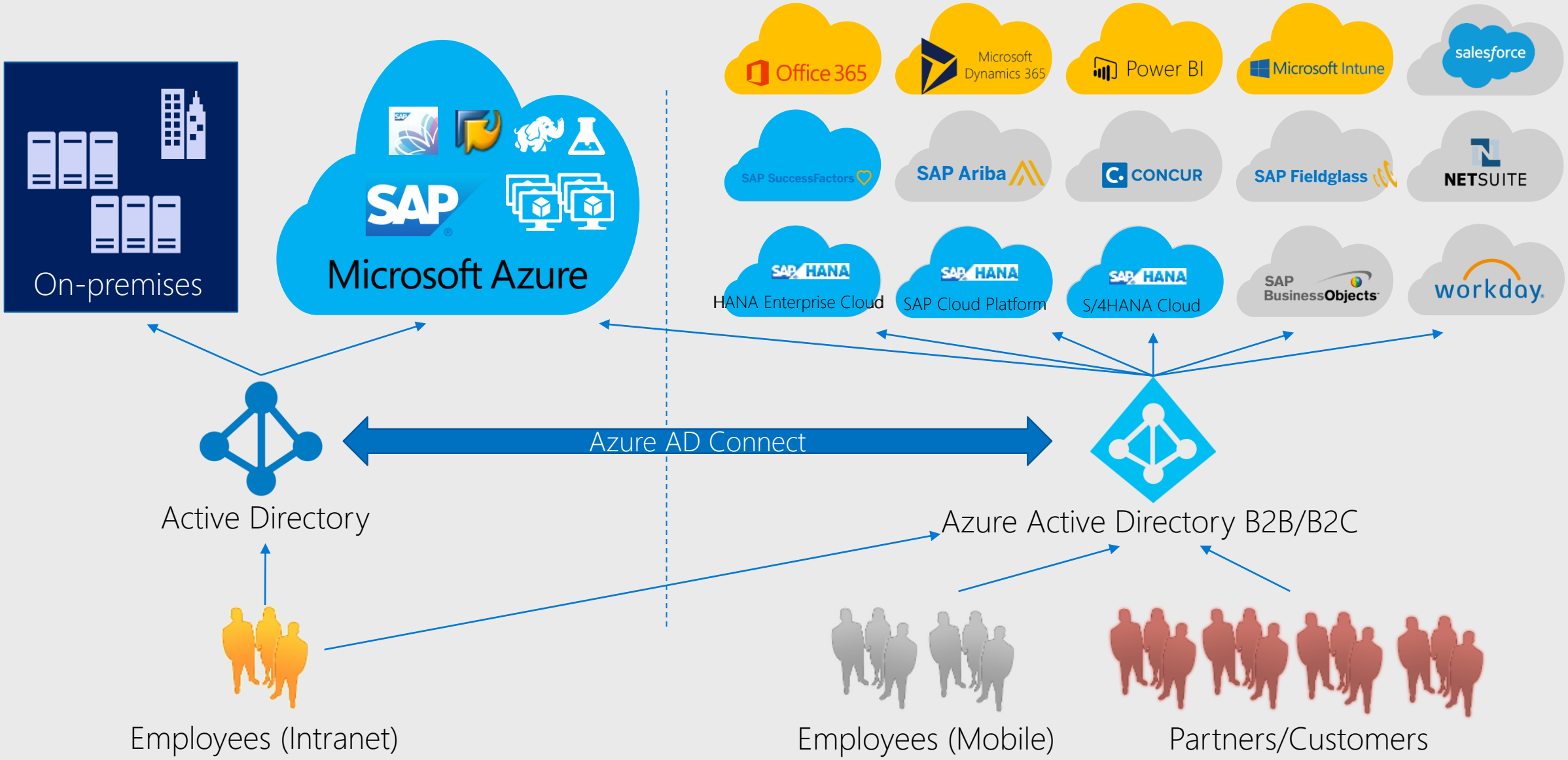
Log Ingestion	Workbooks	Alert Rules, Incidents	Automation, SOAR

Security visibility on Azure



SSO Scenarios

Secure Enterprise Single Sign On including Partners On-premises & Cloud (IaaS & SaaS), SAP & Non-SAP

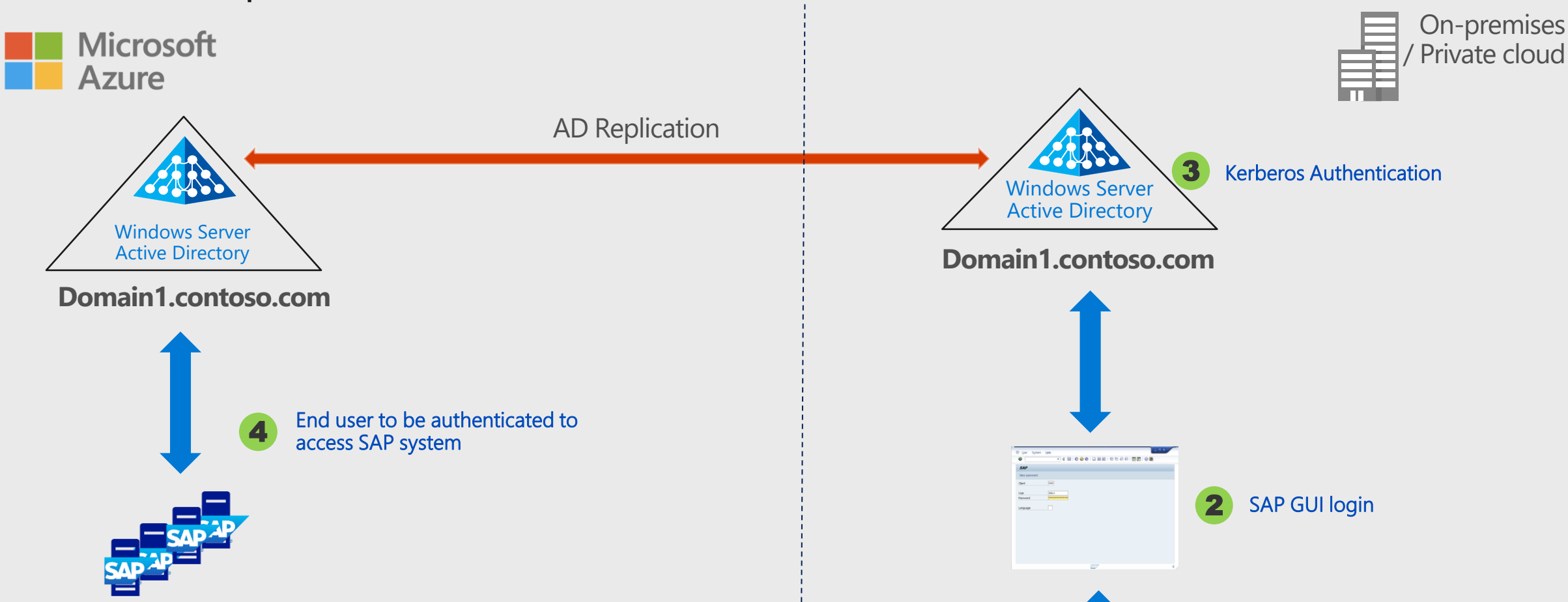


SAP Single sign-on – scenarios

Technology	On-Premise	Cloud
X.509 Certs	Support web and desktop apps	Require additional configuration
Kerberos/SPNEGO	Support web and desktop apps	AD/DS based additional configuration
SAML	Support browser Applications	Support browser applications

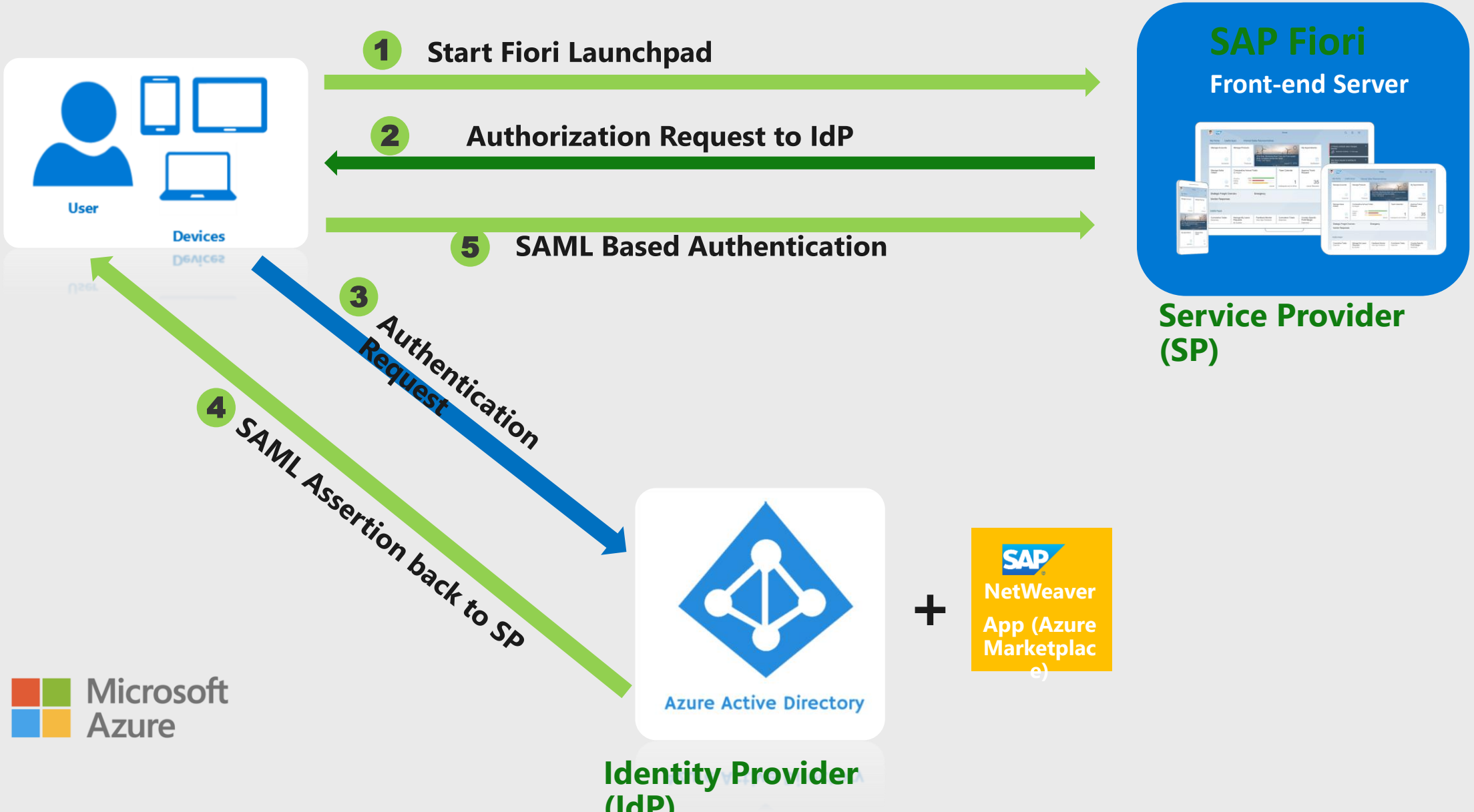
SSO - Hybrid Scenario (Kerberos/SPNEGO)

On Premise AD replicated to Azure

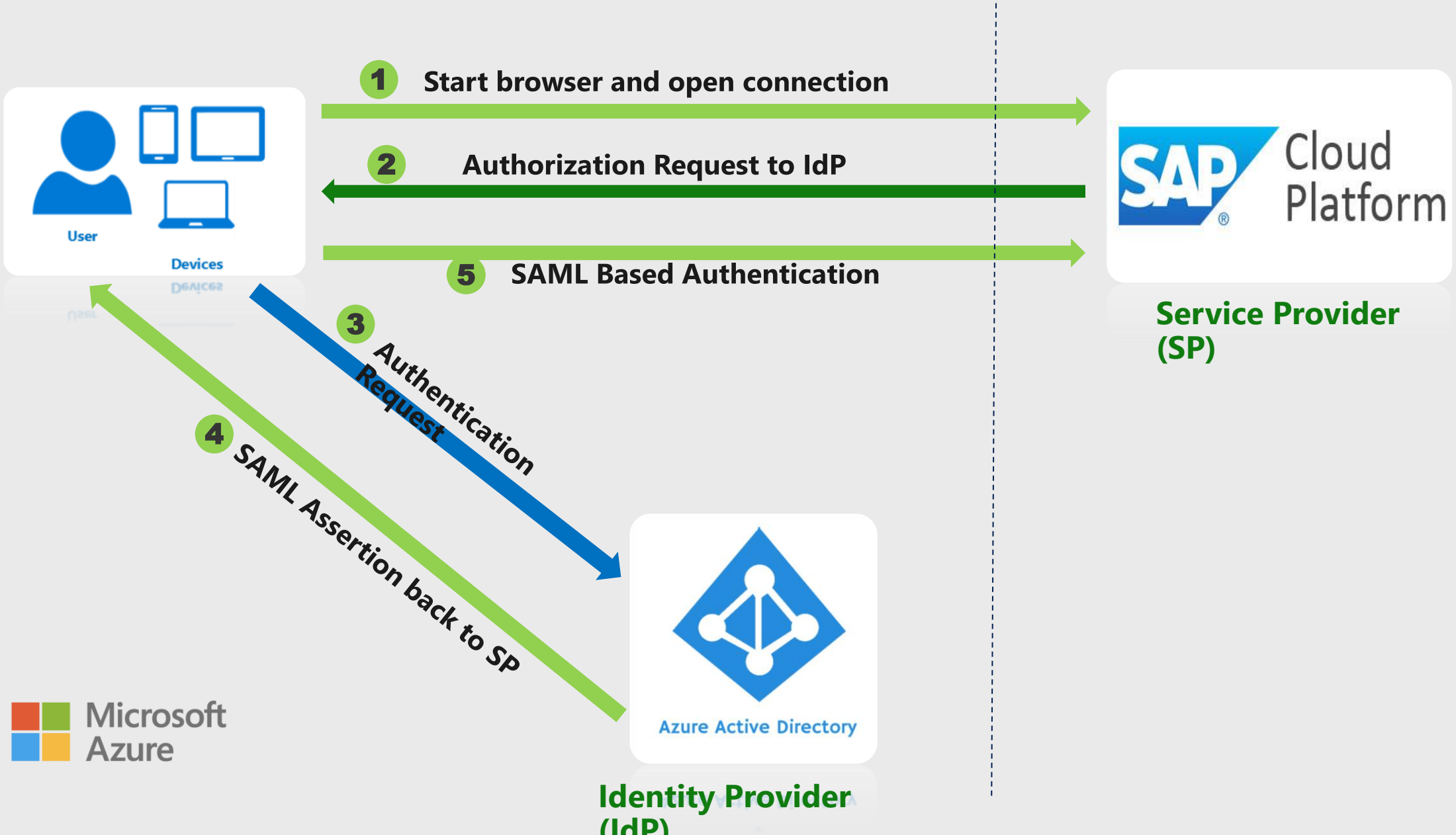


- On-prem AD/DNS extended into Azure. SAP systems located on-premises and Azure in same domain/AD
- ExpressRoute recommended for Production SAP - private dedicated connection which offers reliability (SLA), faster speed up to 100Gb/s(*), lower latency and higher security
- DR for On-premise AD in Azure

SSO(SAML) through SAP Fiori and Azure AD



SSO (SAML) to SAP C4C with Azure AD



SAP Single sign-on – References

- Azure Active Directory integration with SAP NetWeaver
- SAP Single Sign-On using Azure AD Domain Services
- Fiori Launchpad SAML Single Sign-On with Azure AD
- Azure Active Directory integration with SAP Cloud for Customer

Q&A

Reach out to the team

sap-on-azure-pe-apac@microsoft.com

Feedback

Your feedback is very important for us.

Your responses are Anonymous

https://aka.ms/SAPAPAC-POE-FEEDBACK

Microsoft

SAP on Azure Enablement

Next Session – Azure Governance

Tuesday, Oct 19, 2020, 10am SGT

Reach out to the team
sap-on-azure-pe-apac@microsoft.com

Microsoft Azure