Top 10 Azure Security Best Practices

Gregor Reimling

About "Gregor Reimling"

Azure Meetup
BONN
azurebonn

Focus
Azure Governance, Security and IaaS

Certifications
Cloud Architect & MVP for MS Azure

From
Cologne, Germany

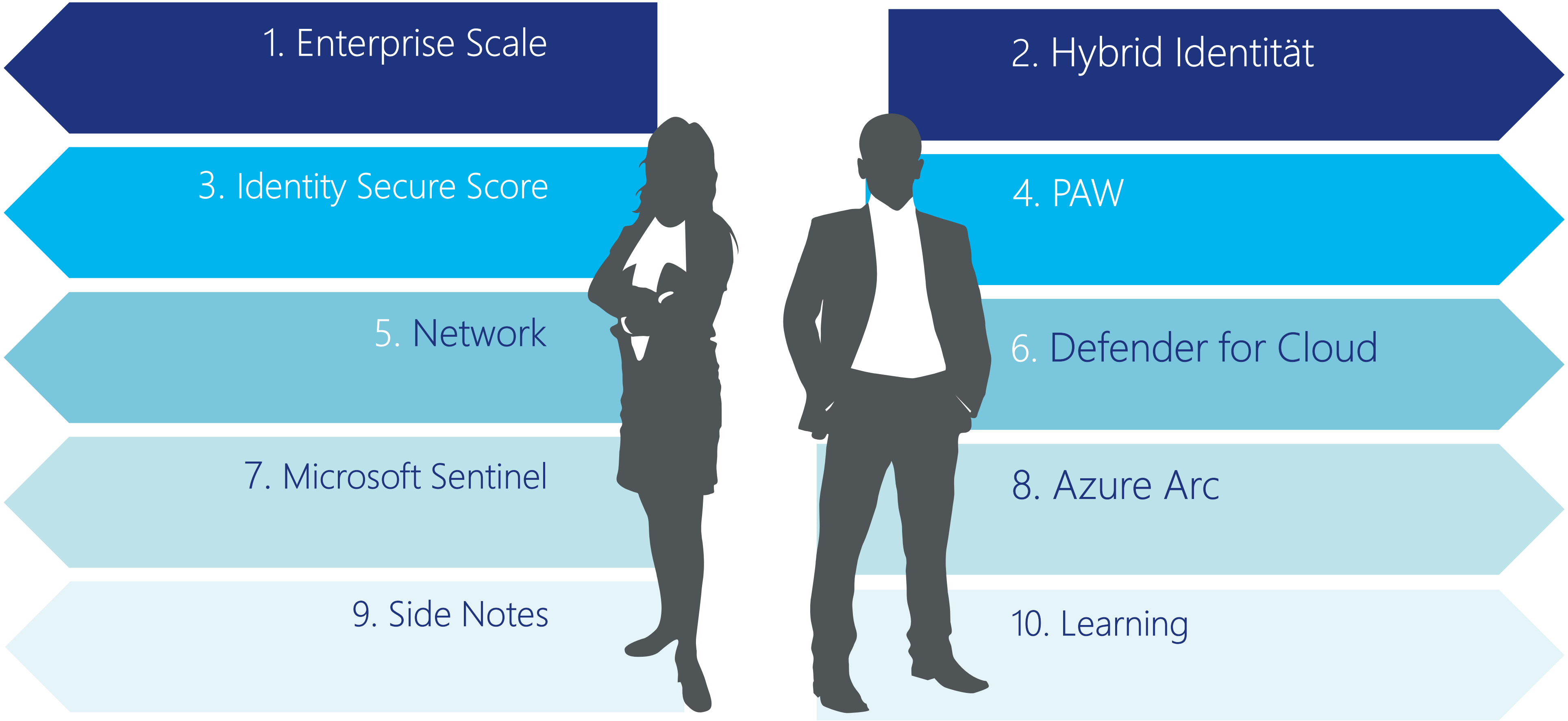
Hobbies
Family, Community,
Worldtraveler

My Blog
https://www.Reimling.eu

Cloud
Inspires
Podcast
Stories and people behind
Cloud Transformation
www.cloudinspires.me

Contact
@GregorReimling
@CloudInspires

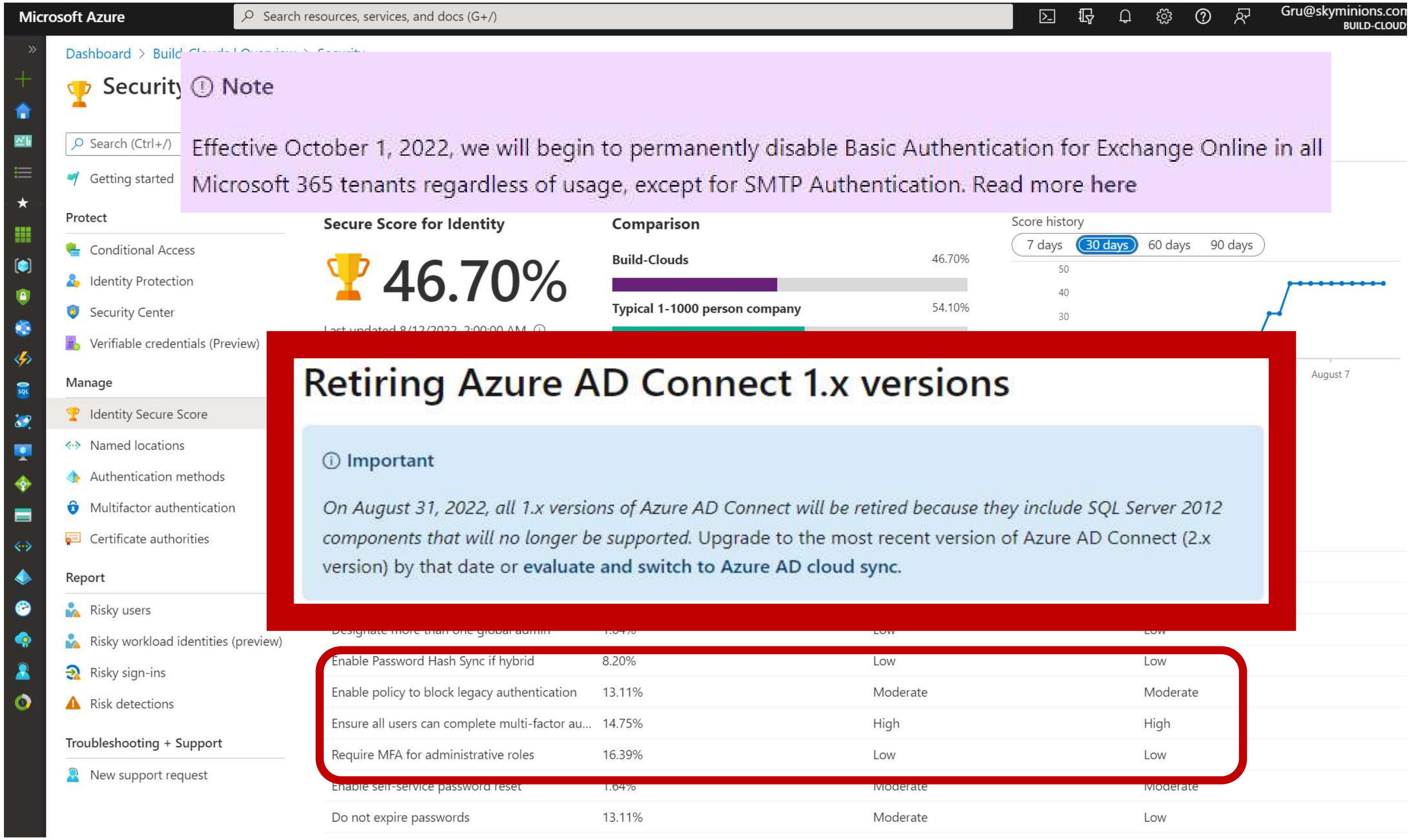
Introduction



1. Enterprise Scale
2. Hybrid Identität
3. Identity Secure Score
4. PAW
5. Network
6. Defender for Cloud
7. Microsoft Sentinel
8. Azure Arc
9. Side Notes
10. Learning

AZURE

Important Dates



ⓘ Note

Effective October 1, 2022, we will begin to permanently disable Basic Authentication for Exchange Online in all Microsoft 365 tenants regardless of usage, except for SMTP Authentication. Read more here

Secure Score for Identity

46.70%

Last updated 8/12/2022, 2:00:00 AM

Retiring Azure AD Connect 1.x versions

ⓘ Important

On August 31, 2022, all 1.x versions of Azure AD Connect will be retired because they include SQL Server 2012 components that will no longer be supported. Upgrade to the most recent version of Azure AD Connect (2.x version) by that date or **evaluate and switch to Azure AD cloud sync.**

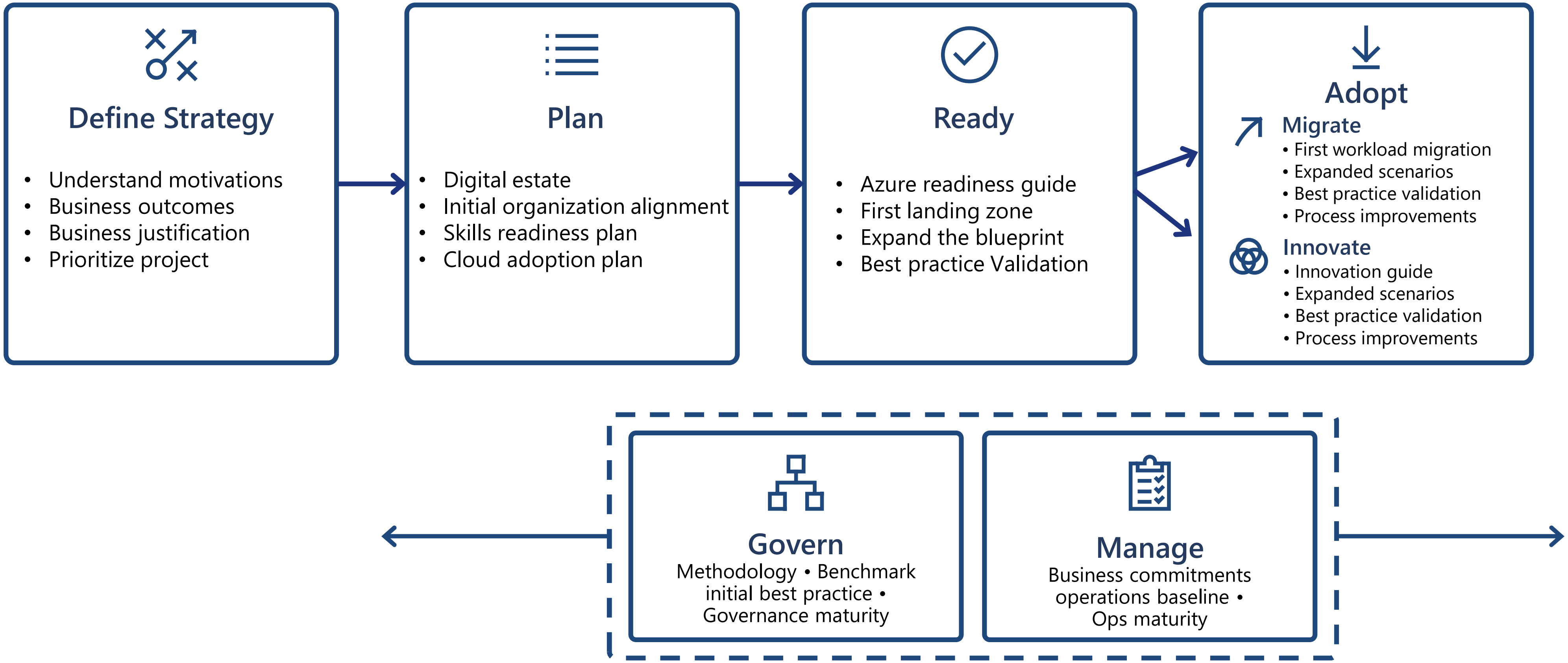
Designate more than one global admin	1.64%	Low	Low
Enable Password Hash Sync if hybrid	8.20%	Low	Low
Enable policy to block legacy authentication	13.11%	Moderate	Moderate
Ensure all users can complete multi-factor au...	14.75%	High	High
Require MFA for administrative roles	16.39%	Low	Low
Enable self-service password reset	1.64%	Moderate	Moderate
Do not expire passwords	13.11%	Moderate	Low

AZURE

1. Enterprise Scale

AZURE

MS Cloud Adoption Framework



Define Strategy

- Understand motivations
- Business outcomes
- Business justification
- Prioritize project

Plan

- Digital estate
- Initial organization alignment
- Skills readiness plan
- Cloud adoption plan

Ready

- Azure readiness guide
- First landing zone
- Expand the blueprint
- Best practice Validation

Adopt

Migrate

- First workload migration
- Expanded scenarios
- Best practice validation
- Process improvements

Innovate

- Innovation guide
- Expanded scenarios
- Best practice validation
- Process improvements

Govern

Methodology • Benchmark
initial best practice •
Governance maturity

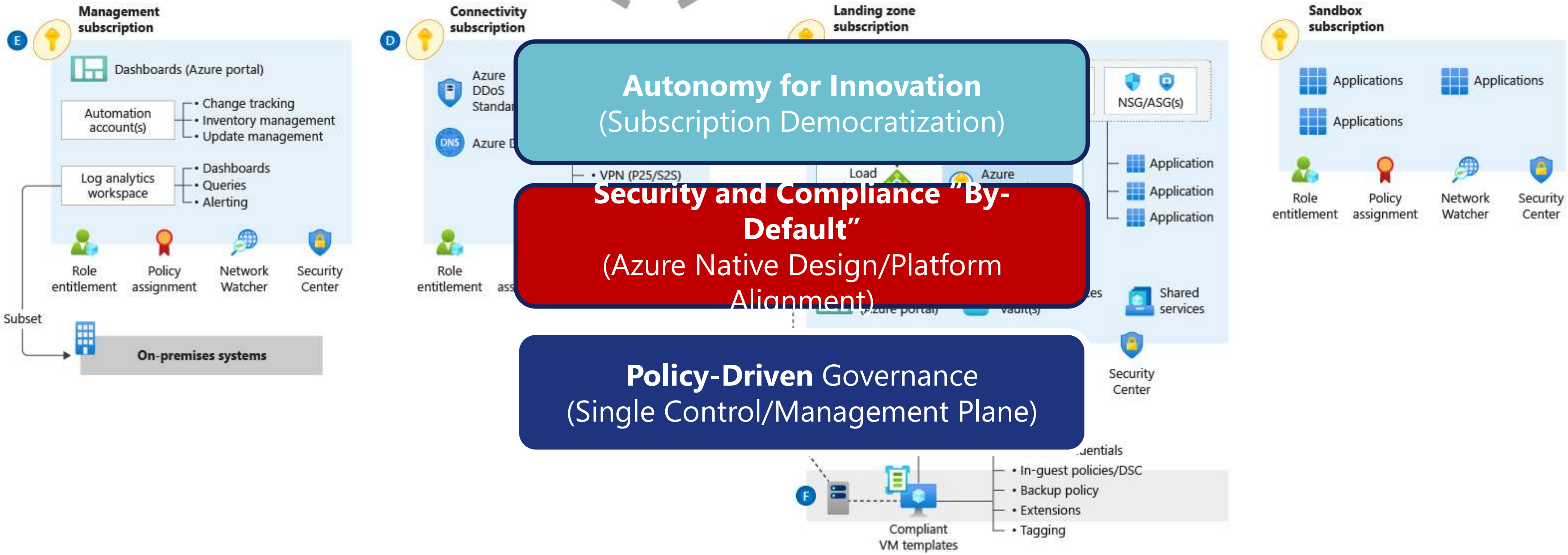
Manage

Business commitments
operations baseline •
Ops maturity

Enterprise-Scale - Design Principles

Tenant Root Group

Build Clouds



Autonomy for Innovation
(Subscription Democratization)

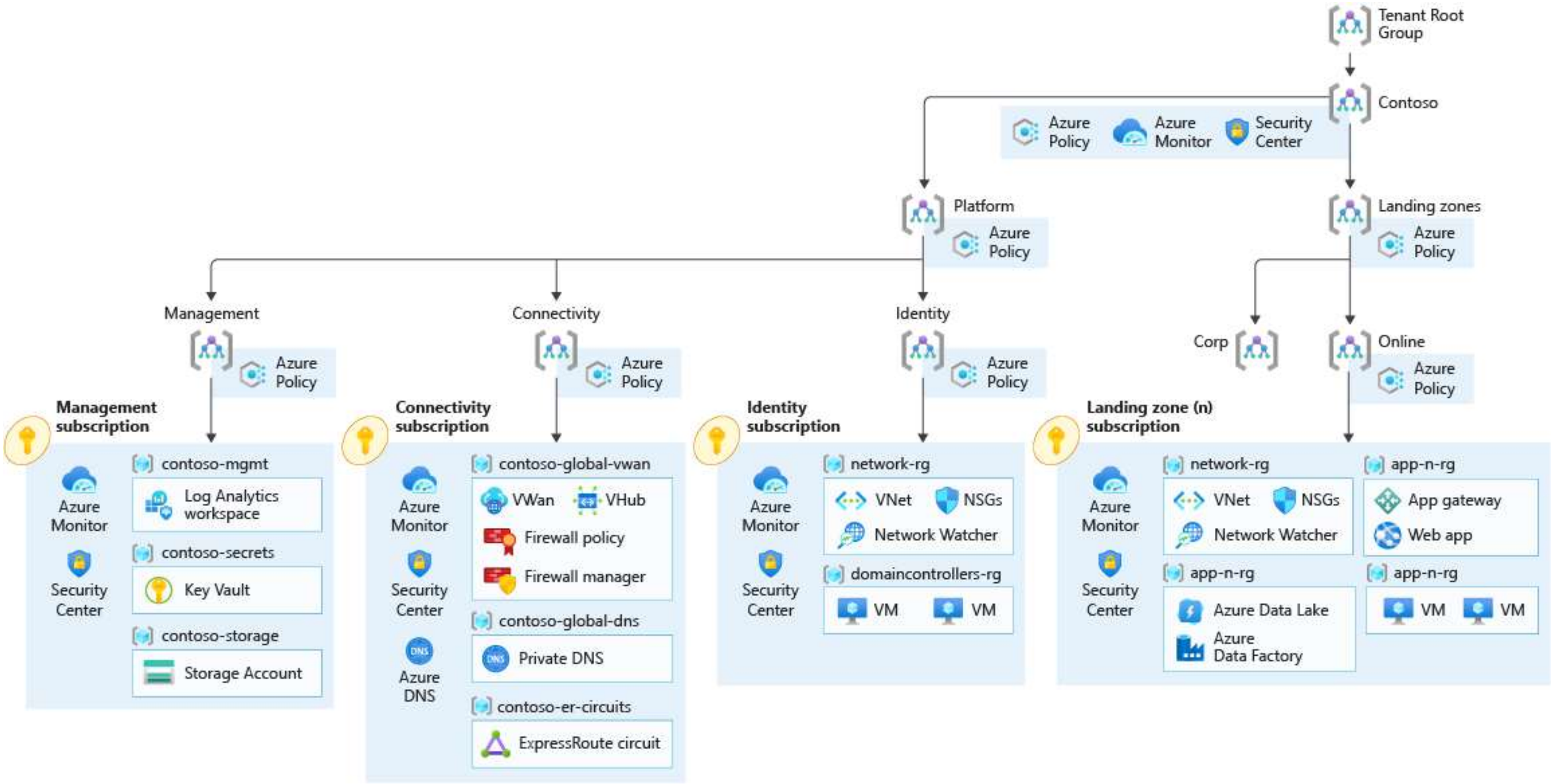
Security and Compliance "By-Default"
(Azure Native Design/Platform Alignment)

Policy-Driven Governance
(Single Control/Management Plane)

AZURE

GitHub Enterprise Scale Templates

Deploy Enterprise-Scale with Azure VWAN



GitHub - Azure/Enterprise-Scale: The Azure Landing Zones (Enterprise-Scale) architecture provides prescriptive guidance coupled with Azure best practices, and it follows design principles across the critical design areas for organizations to define their Azure architecture

Azure Tenant Design approach

Tenant Root Group

Build Clouds

BC- Platform

BC- Connectivity

Sub Connectivity

Sub vWAN

BC- Identity

Sub Identity

Sub Connectivity

BC- Landing Zones

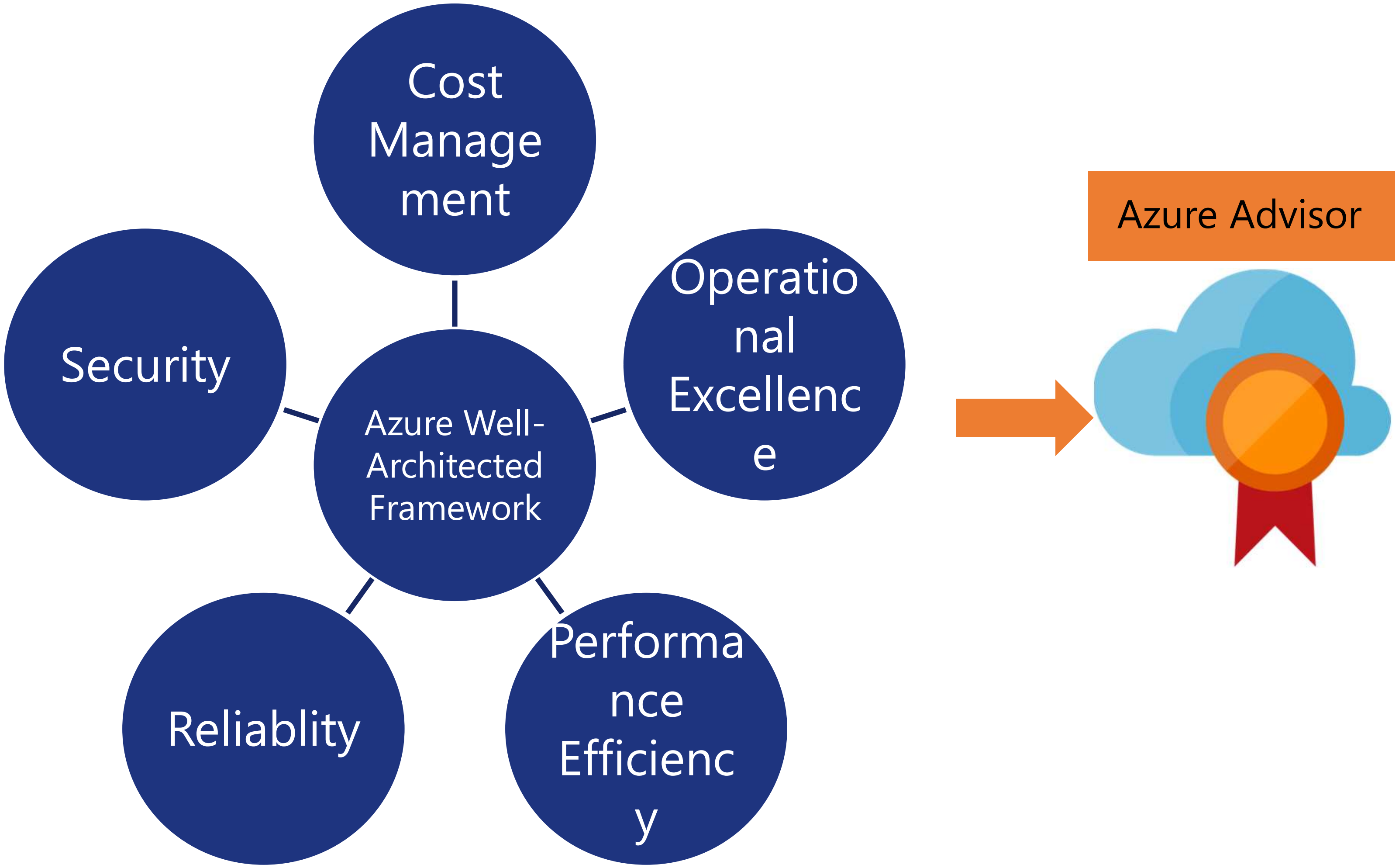
Sub Infrastructure

Sub AVD

Sub AVD

Well-architected Framework

"The Azure Well-Architected Framework is a set of guiding tenets that can be used to improve the quality of a workload."



https://docs.microsoft.com/en-us/azure/architecture/framework/

Demo

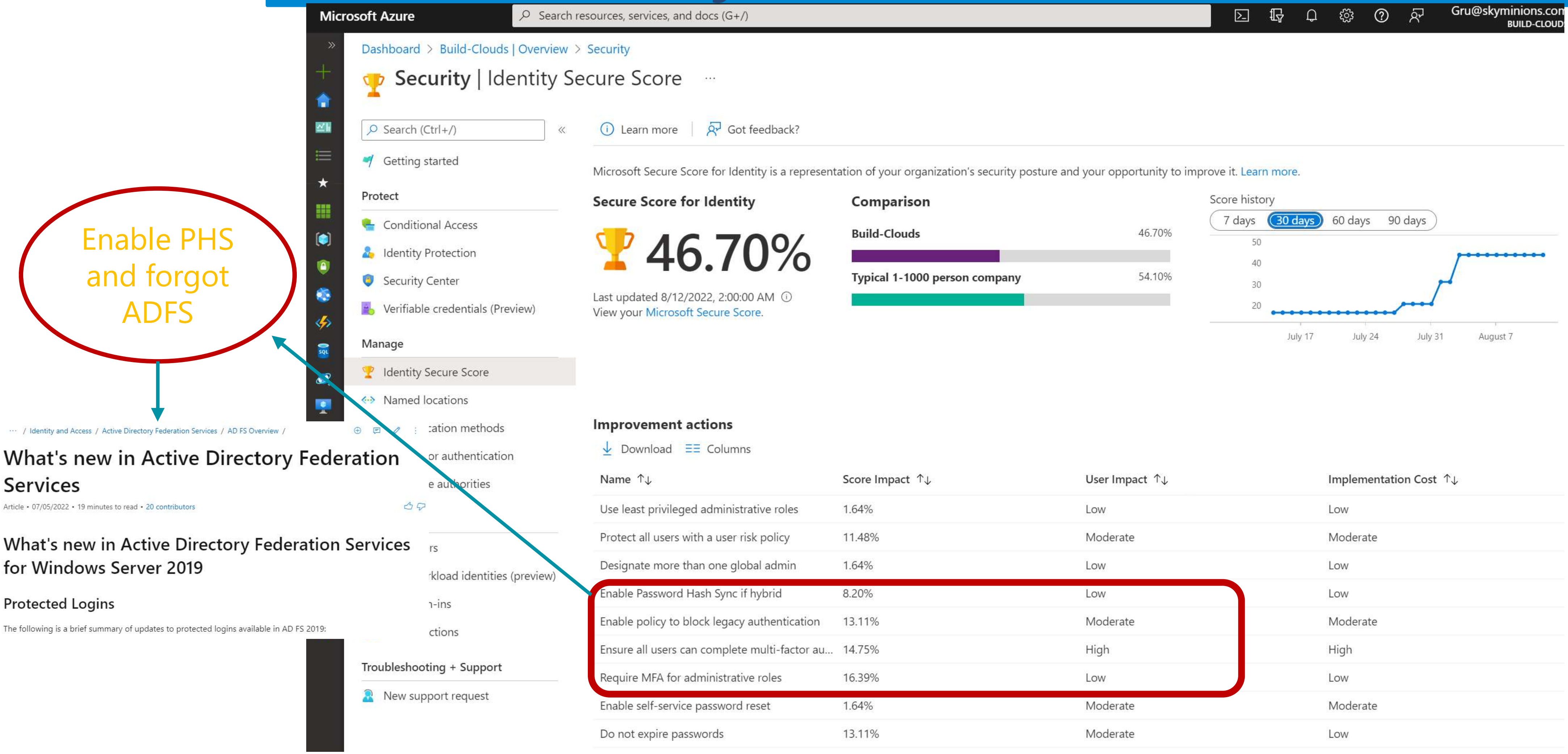
Dive into the Azure Portal

- Enterprise Scale
- Azure Advisor

2. Hybrid Identity

AZURE

Identity Secure Score



Enable PHS and forgot ADFS

Microsoft Azure

Search resources, services, and docs (G+/)

Gru@skyminions.com
BUILD-CLOUD

Dashboard > Build-Clouds | Overview > Security

Security | Identity Secure Score

Search (Ctrl+/)

Getting started

Protect

Conditional Access

Identity Protection

Security Center

Verifiable credentials (Preview)

Manage

Identity Secure Score

Named locations

:ation methods

or authentication

e authorities

rs

:kload identities (preview)

ı-ins

ctions

Troubleshooting + Support

New support request

Learn more | Got feedback?

Microsoft Secure Score for Identity is a representation of your organization's security posture and your opportunity to improve it. Learn more.

Secure Score for Identity

46.70%

Last updated 8/12/2022, 2:00:00 AM

View your Microsoft Secure Score.

Comparison

Build-Clouds	46.70%
Typical 1-1000 person company	54.10%

Score history

Improvement actions

Download | Columns

Name	Score Impact	User Impact	Implementation Cost
Use least privileged administrative roles	1.64%	Low	Low
Protect all users with a user risk policy	11.48%	Moderate	Moderate
Designate more than one global admin	1.64%	Low	Low
Enable Password Hash Sync if hybrid	8.20%	Low	Low
Enable policy to block legacy authentication	13.11%	Moderate	Moderate
Ensure all users can complete multi-factor au...	14.75%	High	High
Require MFA for administrative roles	16.39%	Low	Low
Enable self-service password reset	1.64%	Moderate	Moderate
Do not expire passwords	13.11%	Moderate	Low

… / Identity and Access / Active Directory Federation Services / AD FS Overview /

What's new in Active Directory Federation Services

Article • 07/05/2022 • 19 minutes to read • 20 contributors

What's new in Active Directory Federation Services for Windows Server 2019

Protected Logins

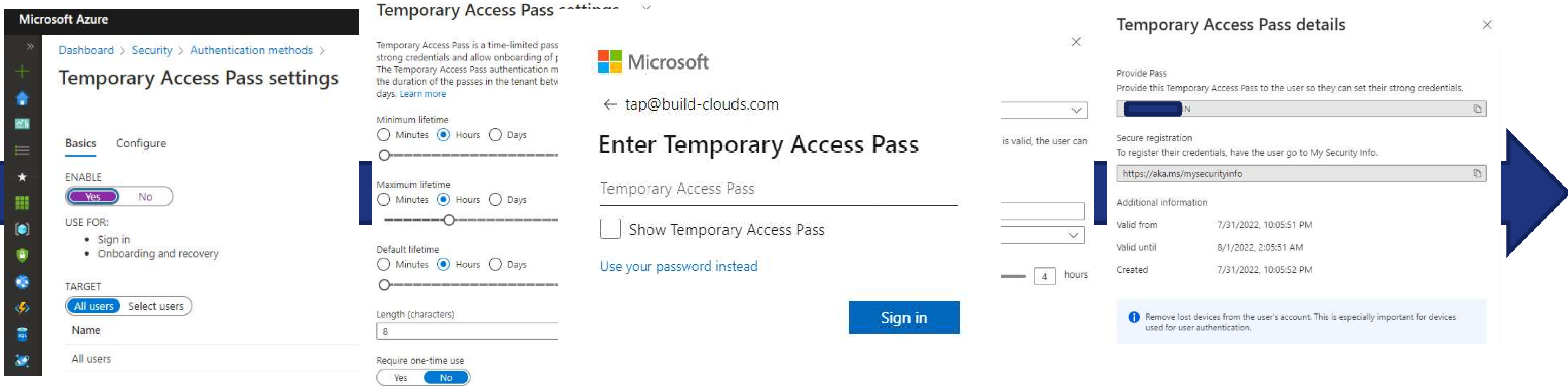
The following is a brief summary of updates to protected logins available in AD FS 2019:

Azure AD Cloud ~~Connect~~ Sync

	Connect Sync	Cloud Sync
Connect to multiple disconnected on-premises AD forests	No	Yes
Lightweight agent installation model	No	Yes
Multiple active agents for high availability	No	Yes
Connect to LDAP directories	Yes	No
Support for device objects	Yes	No
Support for device writeback	Yes	No
Support for group writeback	Yes	No
Support for Pass-Through Authentication	Yes	No

AZURE

Temporary Access Pass



Microsoft Azure

Dashboard > Security > Authentication methods >

Temporary Access Pass settings

Basics Configure

ENABLE

[✓ Yes] No

USE FOR:

- Sign in
- Onboarding and recovery

TARGET

[✓ All users] Select users

Name
All users

Temporary Access Pass settings

Temporary Access Pass is a time-limited pass
strong credentials and allow onboarding of p
The Temporary Access Pass authentication m
the duration of the passes in the tenant betw
days. Learn more

Minimum lifetime

○ Minutes ● Hours ○ Days

Maximum lifetime

○ Minutes ● Hours ○ Days

Default lifetime

○ Minutes ● Hours ○ Days

Length (characters)

8

Require one-time use

Yes [✓ No]

is valid, the user can

4 hours

Microsoft

← tap@build-clouds.com

Enter Temporary Access Pass

Temporary Access Pass

□ Show Temporary Access Pass

Use your password instead

Sign in

Temporary Access Pass details

Provide Pass

Provide this Temporary Access Pass to the user so they can set their strong credentials.

[redacted]

Secure registration

To register their credentials, have the user go to My Security Info.

https://aka.ms/mysecurityinfo

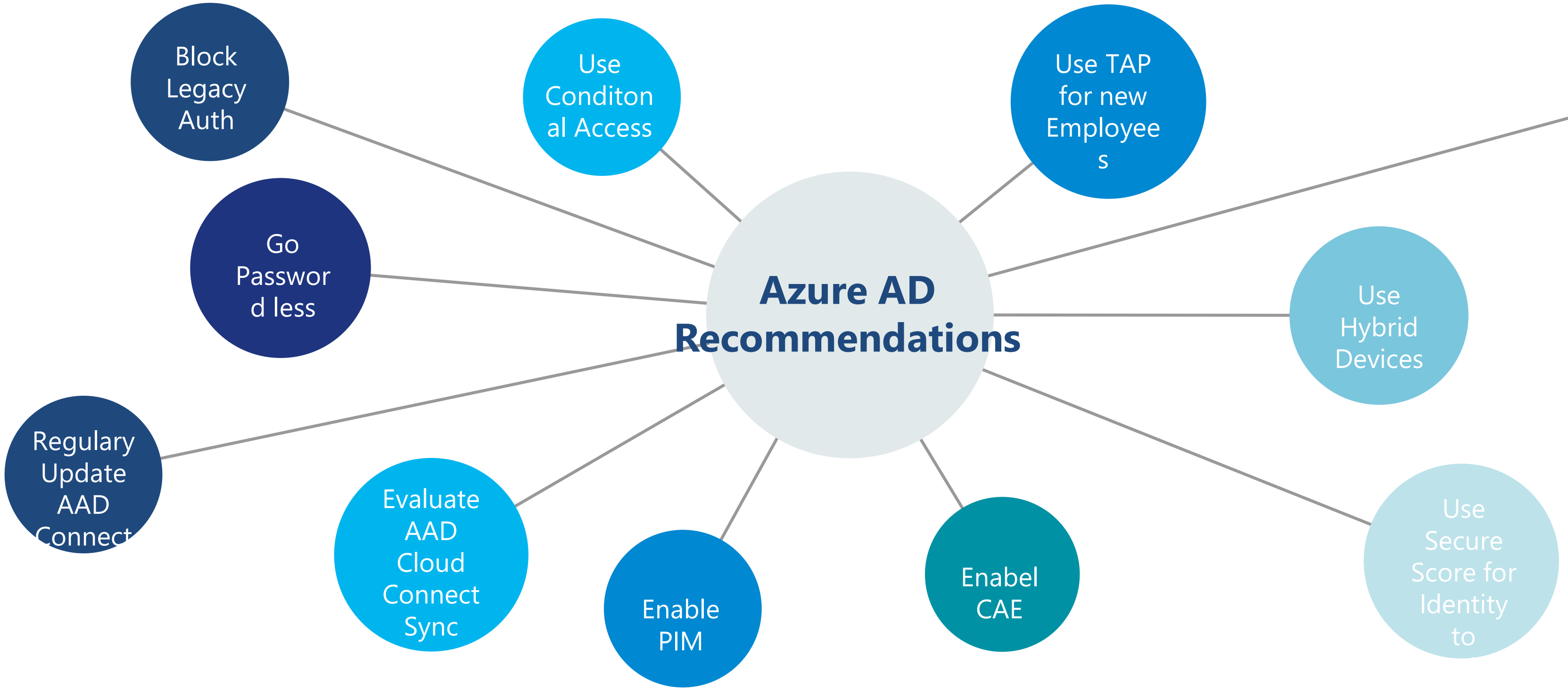
Additional information

Valid from	7/31/2022, 10:05:51 PM
Valid until	8/1/2022, 2:05:51 AM
Created	7/31/2022, 10:05:52 PM

Remove lost devices from the user's account. This is especially important for devices used for user authentication.

https://aka.ms/mysecurityinfo

Azure AD Recommendations



Azure AD Recommendations

Block Legacy Auth

Use Conditon al Access

Use TAP for new Employee s

Device Auth

Go Passwor d less

Use Hybrid Devices

Regulary Update AAD Connect

Evaluate AAD Cloud Connect Sync

Enable PIM

Enabel CAE

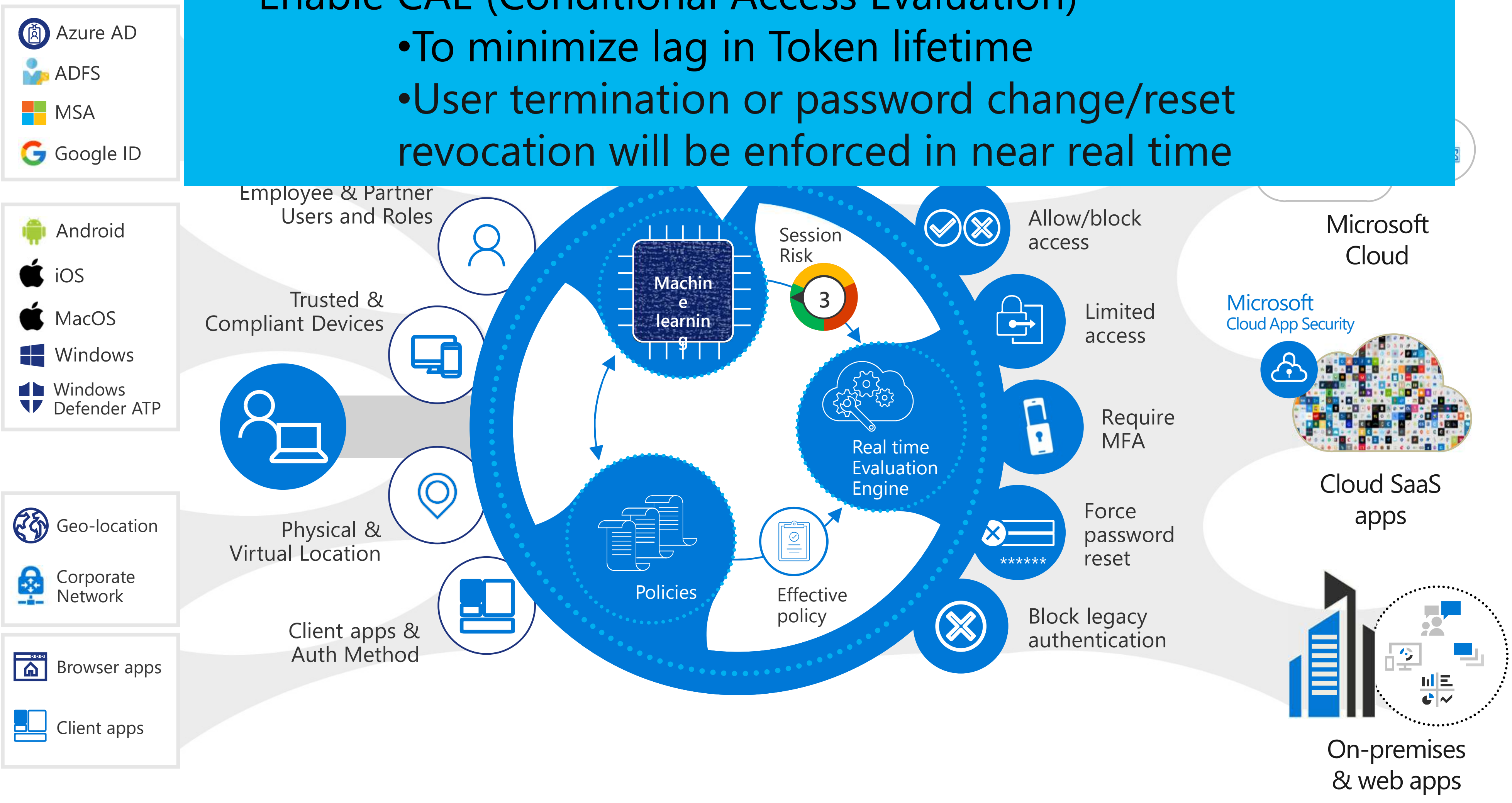
Use Secure Score for Identity to

3. Identity Secure Score

AZURE

Identity Protection with Conditional Access

- Enable CAE (Conditional Access Evaluation)
  - •To minimize lag in Token lifetime
  - •User termination or password change/reset revocation will be enforced in near real time



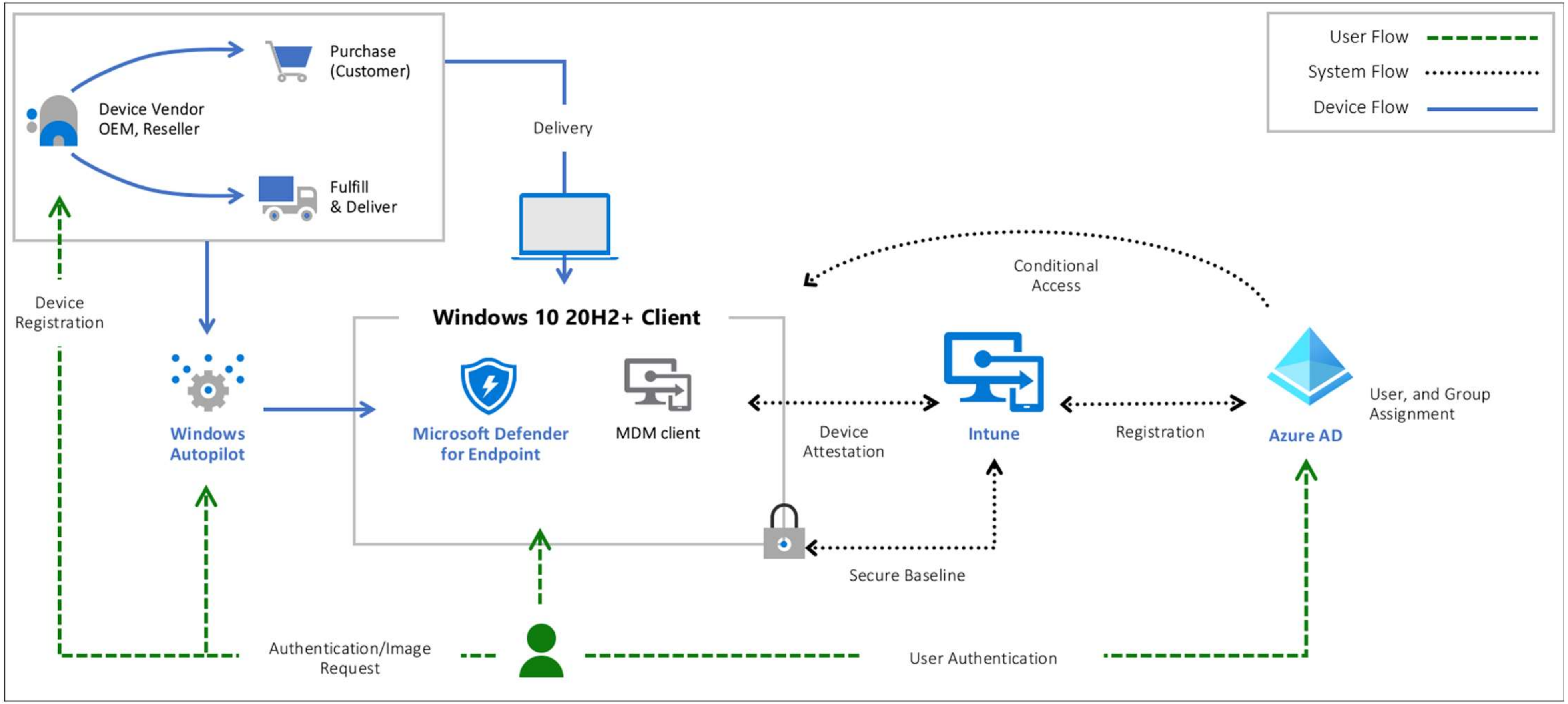
Show following settings

- Identity Secure Score

4. PAW

AZURE

Privileged Access Devices



Why are privileged access devices important | Microsoft Learn

AZURE

Privileged Admin Workstation

✓ Use dedicated VMs for manage Azure/Microsoft 365 environments

✓ Use this VMs only for Adminstration tasks

✓ Do not enable Internet- / Social media access on this VMs

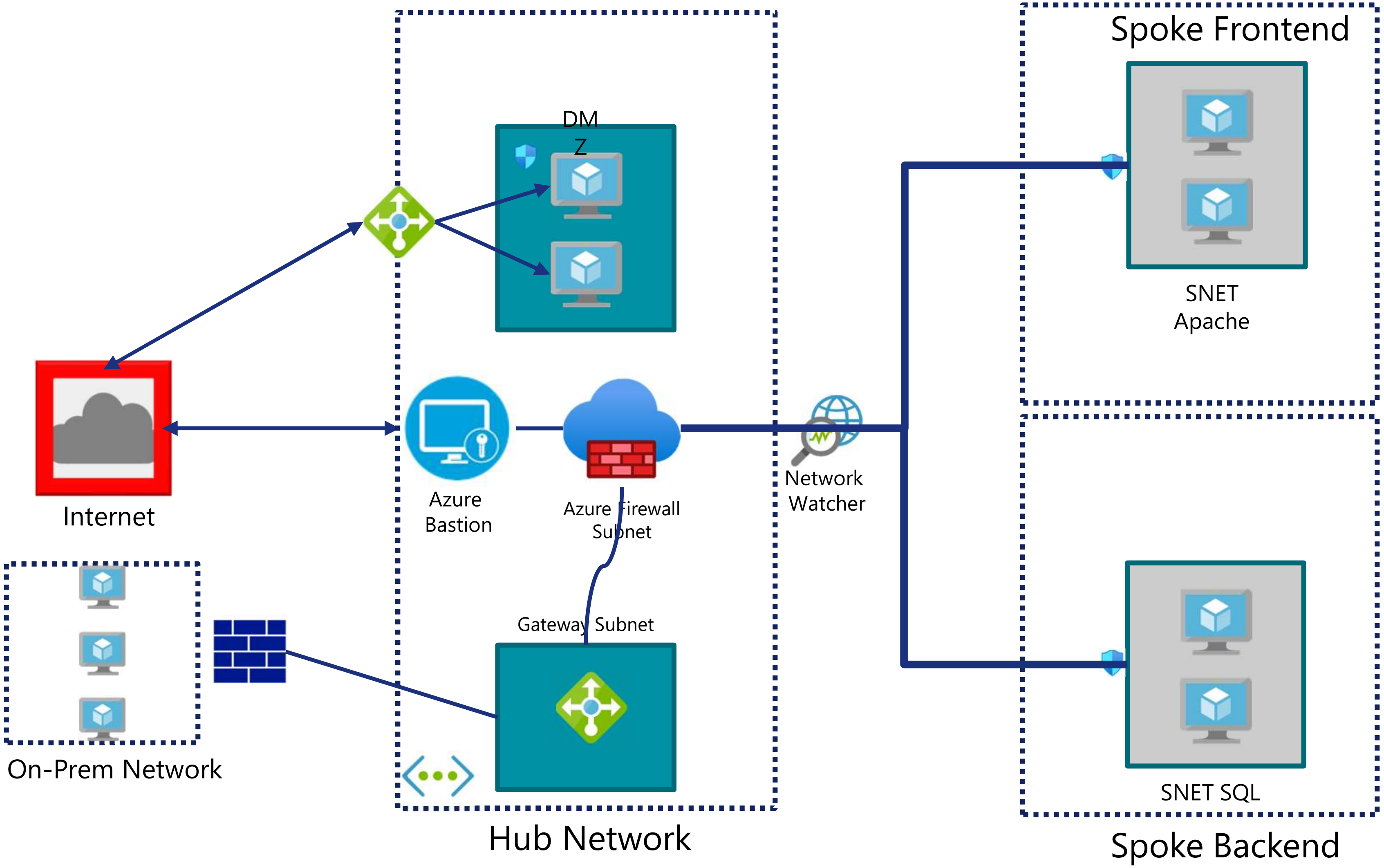
✓ Enforce Device compliance via Conditional Access for this VMs

✓ Use AVD as PAW solution

5. Network

AZURE

Network Protection



Azure IaaS Recommendations

- Segmentation of Virtual Networks
- Define Subnets and use NSG at Subnet Level
- Use a NVA or Azure Firewall at the Hub Network
- Define UDR to Route traffic over the Hub Network and Firewall
- Use Azure Web Application Firewall for Internetapplications
- Use DDoS Protection for Web Applications
- Use Azure Bastion for VM Management

Azure Firewall Editions

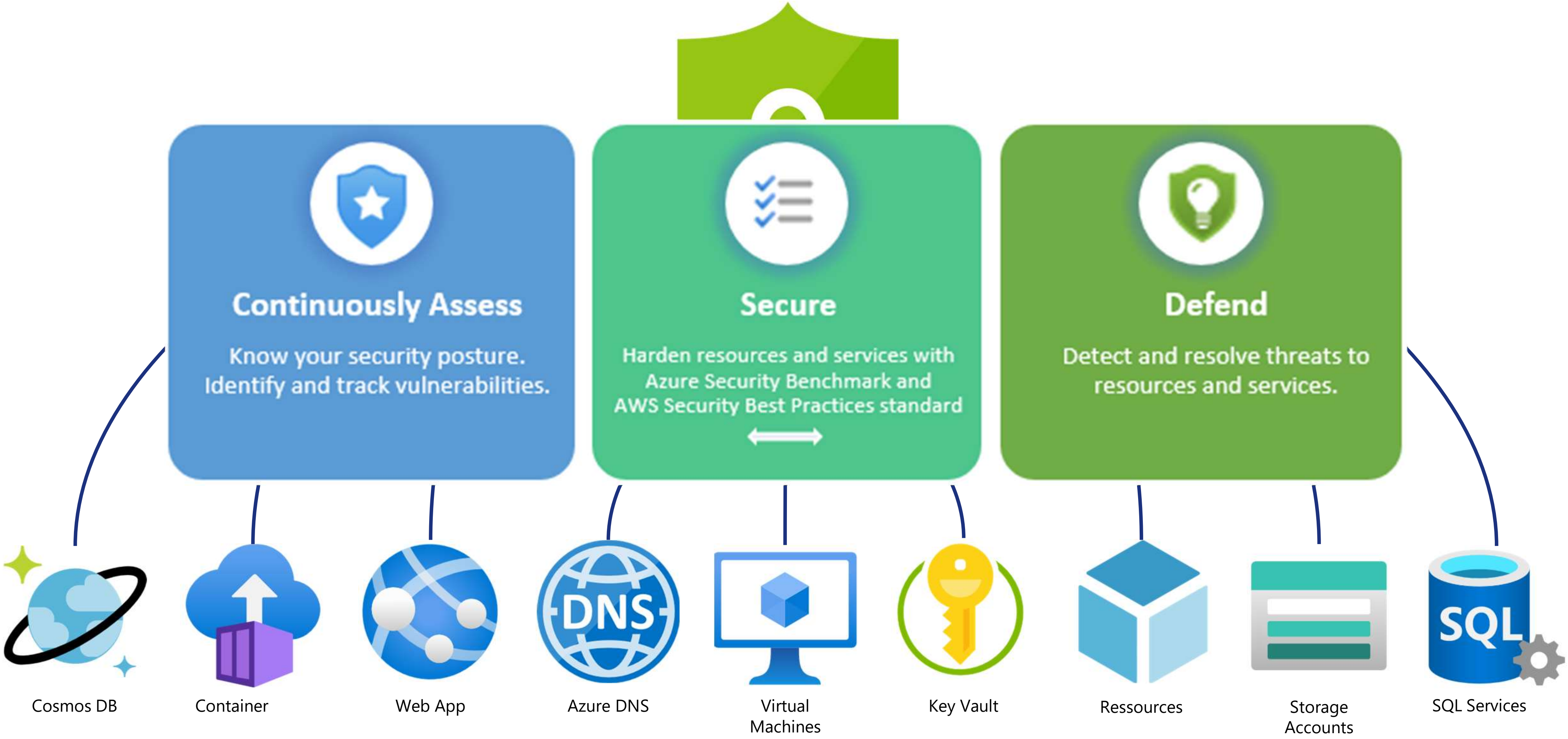
New in Public Preview (MS Ignite 2022)

Azure Firewall Basic	Azure Firewall Standard	Azure Firewall Premium
2 VMs fixed under the hood	Built-in high availability	**All from Standard +**
Availability Zones	Availability Zones	TLS Inspection
App FQDN Filtering Rules?	Application FQDN Filtering Rules	IDPS
Fixed Scale	Unrestricted Cloud Scalability	URL Filtering
Threat Intelligence (Alert Mode only)	Threat Intelligence	Web categories
FQDN in Network rules	FQDN in Network rules	FQDN in Network rules
250-500MBps	30GBps	30GBps
Around XXX€	901,24€ per month	1.262,29€ per month

6. MS Defender for Cloud

AZURE

Microsoft Defender for Cloud



Continuously Assess

Know your security posture. Identify and track vulnerabilities.

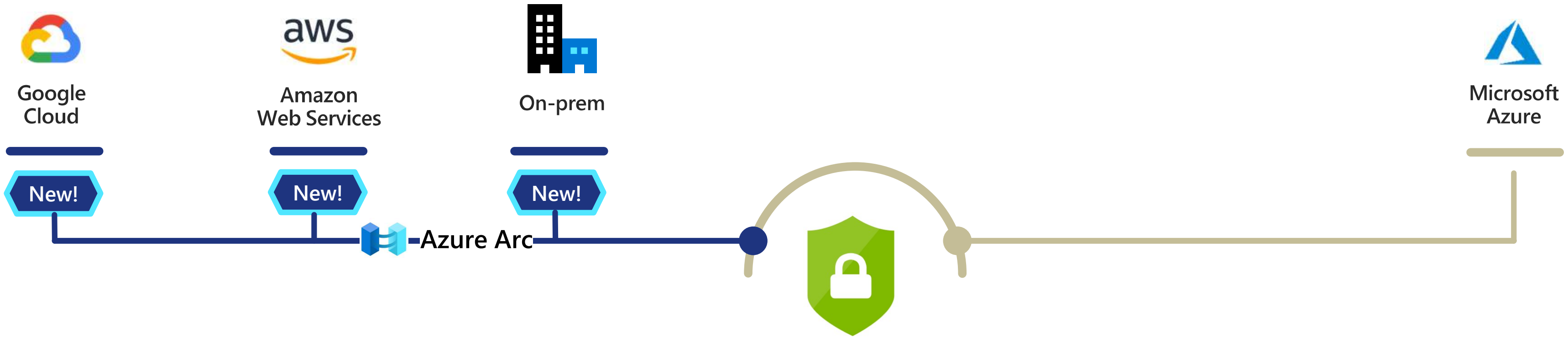
Secure

Harden resources and services with Azure Security Benchmark and AWS Security Best Practices standard

Defend

Detect and resolve threats to resources and services.

MS Defender for Cloud



Security posture & compliance	Secure score	Asset management	Policy
Server protection (Microsoft Defender for Cloud for VMs)	Threat detection	VA (power by Qualys)	Application control
Automation & management at scale	Automation	SIEM integration	Export

AZURE

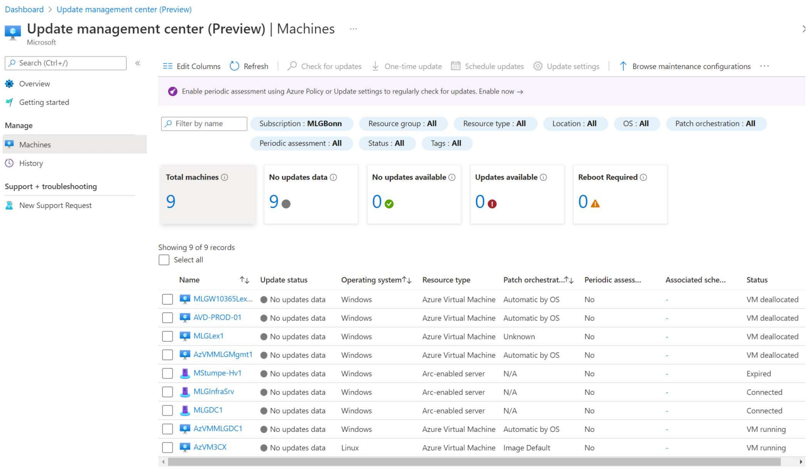
Defender for Servers Plans

	Plan 1	Plan 2
Unified View	Yes	Yes
Automatic MDE provisioning	Yes	Yes
MS Threat and Vulnerability management	Yes	Yes
Security Policy and Regulatory Compliance	No	Yes
Integrated Vulnerability by Qualys	No	Yes
Log Analytics 500MB free data ingestion per day	No	Yes
Threat detection	No	Yes
Adaptive application control	No	Yes
File integrity monitoring	No	Yes
Just-in-Time VM access	No	Yes
Adaptive Network hardening	No	Yes
Docker host hardening	No	Yes
Fileless attack detection	No	Yes
Price	**5$ per Server**	**15$ per Server**

Demo

Dive into the Azure Portal

- Microsoft Defender for Cloud



Update management center (Preview) | Machines

Microsoft

Enable periodic assessment using Azure Policy or Update settings to regularly check for updates. Enable now →

Filter by name · Subscription : **MLGBonn** · Resource group : **All** · Resource type : **All** · Location : **All** · OS : **All** · Patch orchestration : **All** · Periodic assessment : **All** · Status : **All** · Tags : **All**

Total machines	No updates data	No updates available	Updates available	Reboot Required
9	9 ●	0 ✓	0 !	0 ⚠

Showing 9 of 9 records

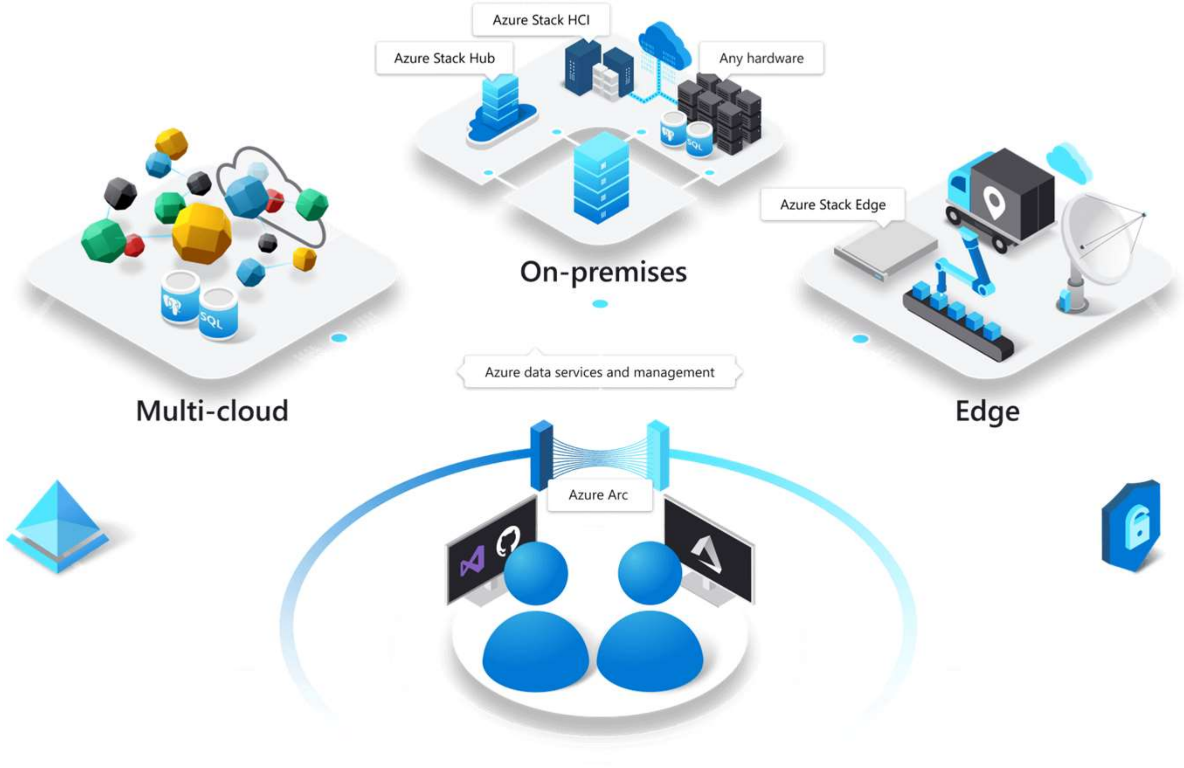
□ Select all

	Name ↑↓	Update status	Operating system↑↓	Resource type	Patch orchestrat...↑↓	Periodic assess...	Associated sche...	Status
□	MLGW10365Lex...	● No updates data	Windows	Azure Virtual Machine	Automatic by OS	No	-	VM deallocated
□	AVD-PROD-01	● No updates data	Windows	Azure Virtual Machine	Automatic by OS	No	-	VM deallocated
□	MLGLex1	● No updates data	Windows	Azure Virtual Machine	Unknown	No	-	VM deallocated
□	AzVMMLGMgmt1	● No updates data	Windows	Azure Virtual Machine	Automatic by OS	No	-	VM deallocated
□	MStumpe-Hv1	● No updates data	Windows	Arc-enabled server	N/A	No	-	Expired
□	MLGInfraSrv	● No updates data	Windows	Arc-enabled server	N/A	No	-	Connected
□	MLGDC1	● No updates data	Windows	Arc-enabled server	N/A	No	-	Connected
□	AzVMMLGDC1	● No updates data	Windows	Azure Virtual Machine	Automatic by OS	No	-	VM running
□	AzVM3CX	● No updates data	Linux	Azure Virtual Machine	Image Default	No	-	VM running

7. Microsoft Sentinel

8. Azure Arc

Azure Arc


Azure Stack HCI
Azure Stack Hub
Any hardware
On-premises
Multi-cloud
Azure Stack Edge
Edge
Azure data services and management
Azure Arc

AZURE

Azure Arc: *at a high level*

Bring Azure services and management to any infrastructure, anywhere

Run Azure data services anywhere

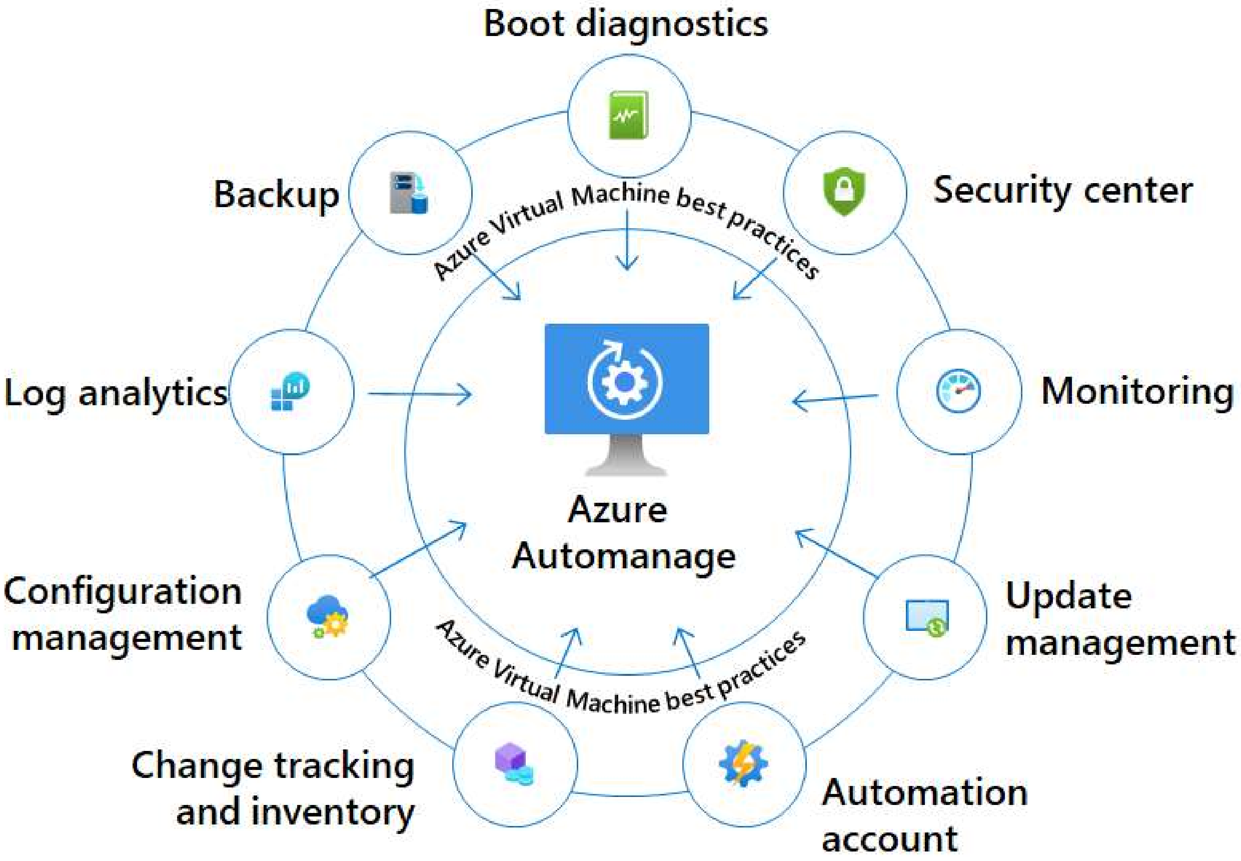
Extend Azure management across your environments

Adopt cloud practices on-premises

Implement Azure security anywhere

Azure Arc is a set of technologies that extends Azure management and enables Azure services to run across on-premises, multi-cloud, and edge

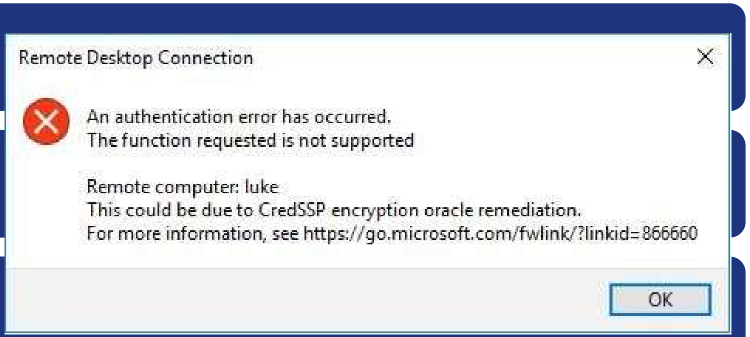
Azure Automanage



AZURE

Update Management Center (preview)

- New solution for centrally Update Management accross different environments
- No dependencys to Log Analytics Agent
- Fully support for Azure Arc managed VMs
- Support Windows and Linux Vms
- Support automatic VM guest patching
- Support Hot patching
- Is in preview wait for production until release going to GA

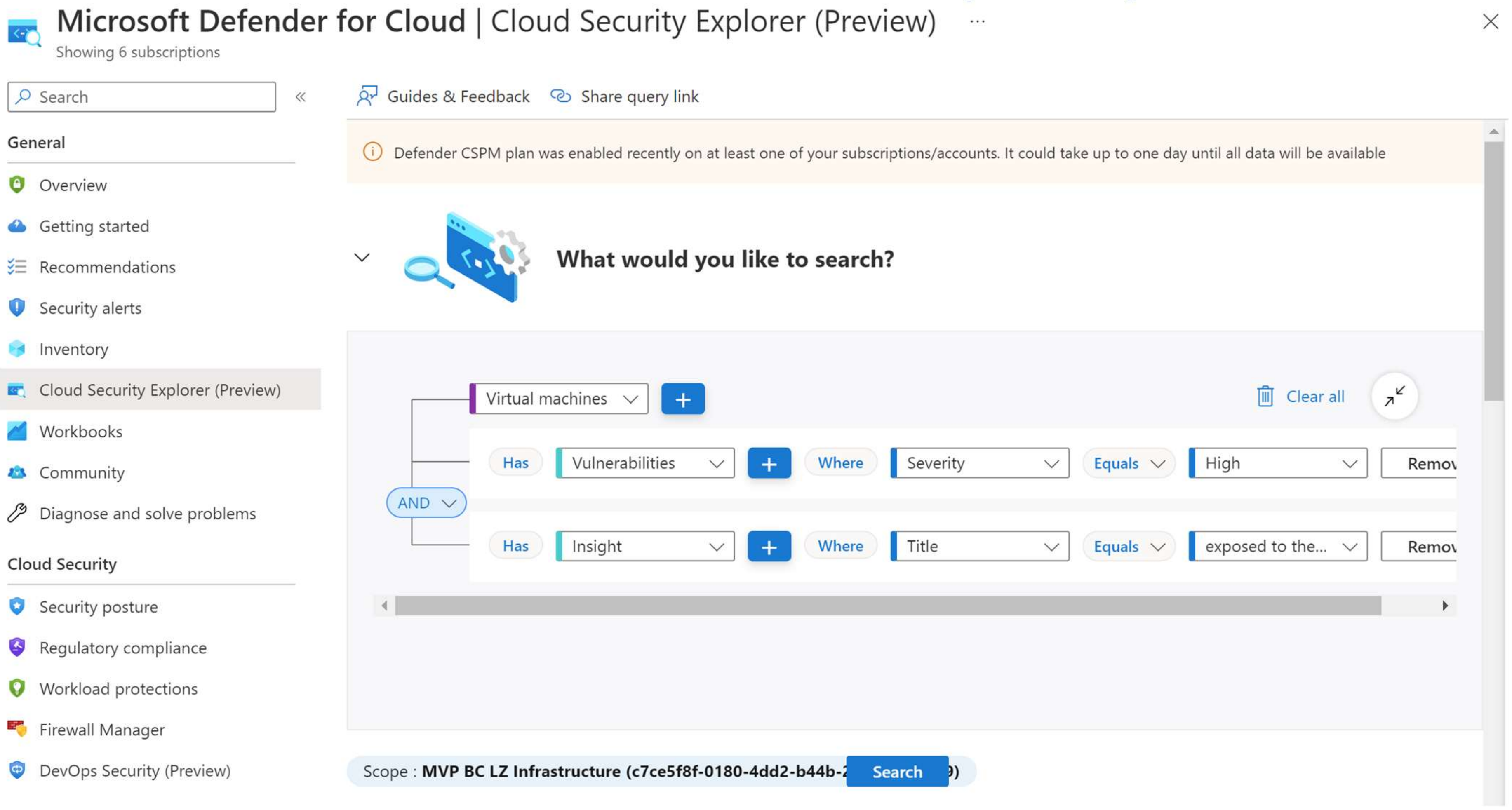


An authentication error has occurred.
The function requested is not supported

Remote computer: luke
This could be due to CredSSP encryption oracle remediation.
For more information, see https://go.microsoft.com/fwlink/?linkid=866660

AZURE

Cloud Security Explorer



Microsoft Defender for Cloud | Cloud Security Explorer (Preview)

Showing 6 subscriptions

Defender CSPM plan was enabled recently on at least one of your subscriptions/accounts. It could take up to one day until all data will be available

What would you like to search?

Virtual machines

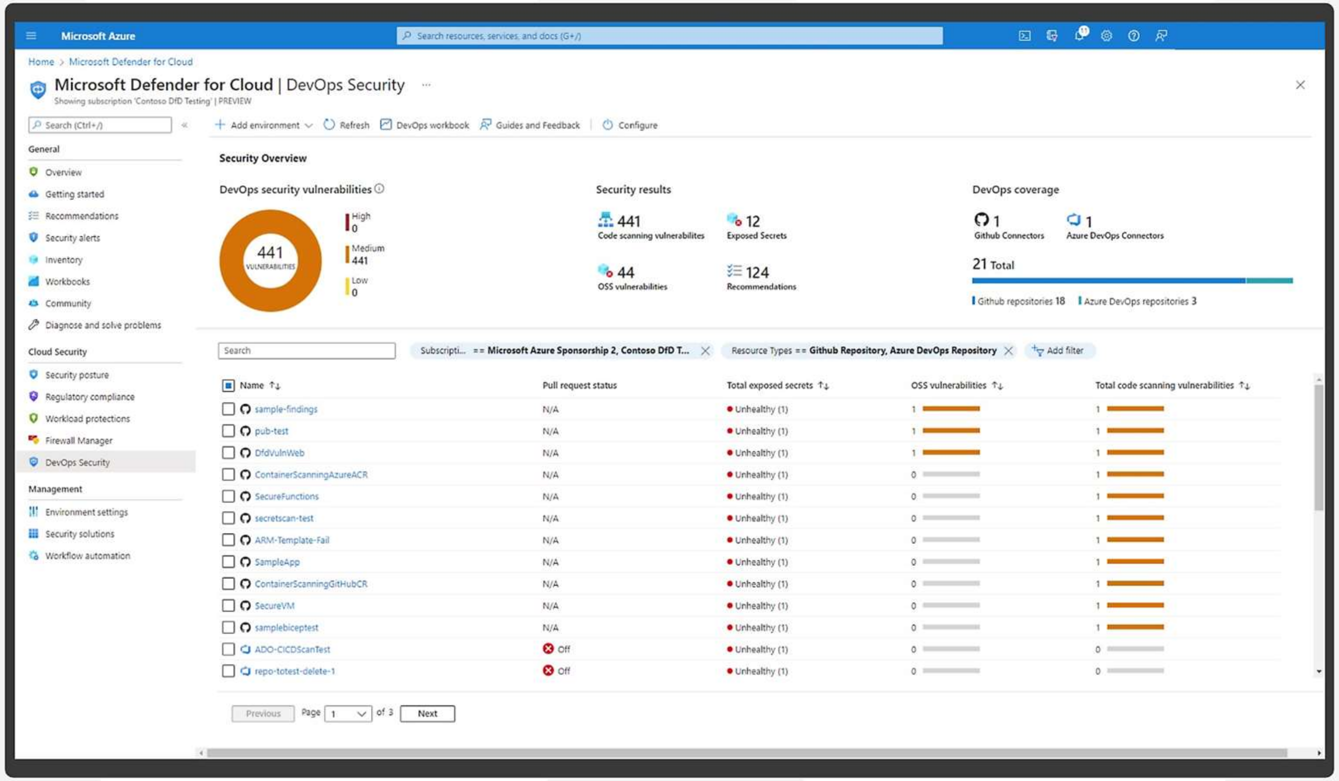
AND

Has Vulnerabilities Where Severity Equals High Remov

Has Insight Where Title Equals exposed to the... Remov

Scope : **MVP BC LZ Infrastructure (c7ce5f8f-0180-4dd2-b44b-2 9)**

Defender for DevOps



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Microsoft Defender for Cloud

Microsoft Defender for Cloud | DevOps Security

Showing subscription 'Contoso DfD Testing' | PREVIEW

Security Overview

DevOps security vulnerabilities

441 VULNERABILITIES

High	0
Medium	441
Low	0

Security results

Code scanning vulnerabilites	441
Exposed Secrets	12
OSS vulnerabilities	44
Recommendations	124

DevOps coverage

Github Connectors	1
Azure DevOps Connectors	1

21 Total

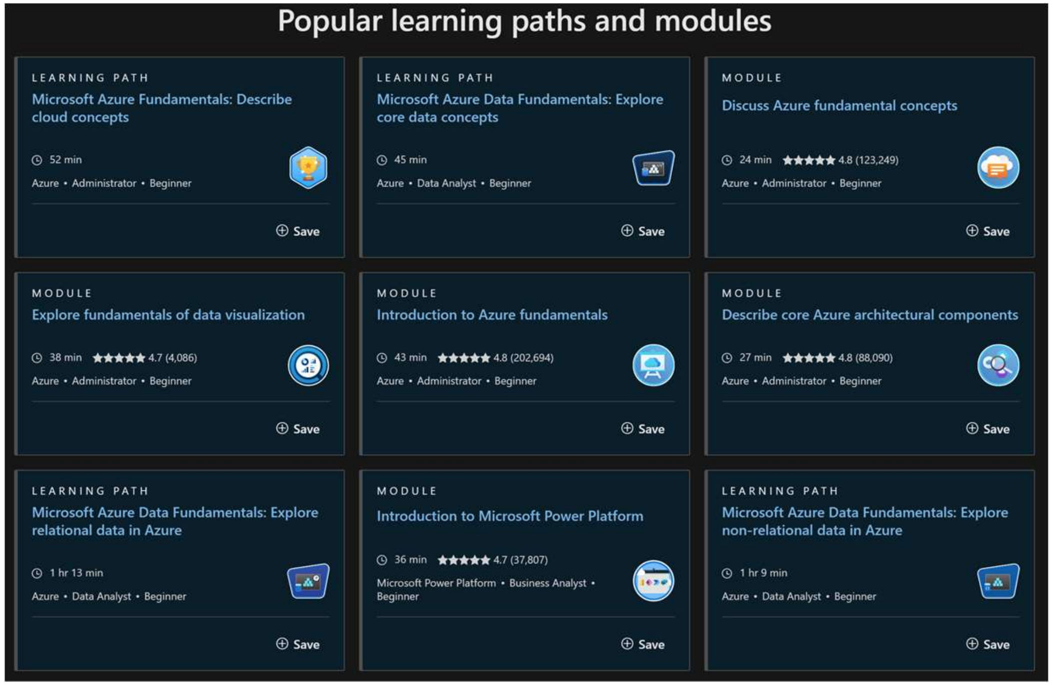
Github repositories 18 · Azure DevOps repositories 3

Search
Subscripti... == Microsoft Azure Sponsorship 2, Contoso DfD T...
Resource Types == Github Repository, Azure DevOps Repository
Add filter

Name	Pull request status	Total exposed secrets	OSS vulnerabilities	Total code scanning vulnerabilities
sample-findings	N/A	● Unhealthy (1)	1	1
pub-test	N/A	● Unhealthy (1)	1	1
DfdVulnWeb	N/A	● Unhealthy (1)	1	1
ContainerScanningAzureACR	N/A	● Unhealthy (1)	0	1
SecureFunctions	N/A	● Unhealthy (1)	0	1
secretscan-test	N/A	● Unhealthy (1)	0	1
ARM-Template-Fail	N/A	● Unhealthy (1)	0	1
SampleApp	N/A	● Unhealthy (1)	0	1
ContainerScanningGitHubCR	N/A	● Unhealthy (1)	0	1
SecureVM	N/A	● Unhealthy (1)	0	1
samplebiceptest	N/A	● Unhealthy (1)	0	1
ADO-CICDScanTest	☒ Off	● Unhealthy (1)	0	0
repo-totest-delete-1	☒ Off	● Unhealthy (1)	0	0

[Join Our Security Community - Microsoft Community Hub]

Learning



Popular learning paths and modules

LEARNING PATH
Microsoft Azure Fundamentals: Describe cloud concepts
52 min
Azure • Administrator • Beginner
Save

LEARNING PATH
Microsoft Azure Data Fundamentals: Explore core data concepts
45 min
Azure • Data Analyst • Beginner
Save

MODULE
Discuss Azure fundamental concepts
24 min ★★★★★ 4.8 (123,249)
Azure • Administrator • Beginner
Save

MODULE
Explore fundamentals of data visualization
38 min ★★★★★ 4.7 (4,086)
Azure • Administrator • Beginner
Save

MODULE
Introduction to Azure fundamentals
43 min ★★★★★ 4.8 (202,694)
Azure • Administrator • Beginner
Save

MODULE
Describe core Azure architectural components
27 min ★★★★★ 4.8 (88,090)
Azure • Administrator • Beginner
Save

LEARNING PATH
Microsoft Azure Data Fundamentals: Explore relational data in Azure
1 hr 13 min
Azure • Data Analyst • Beginner
Save

MODULE
Introduction to Microsoft Power Platform
36 min ★★★★★ 4.7 (37,807)
Microsoft Power Platform • Business Analyst • Beginner
Save

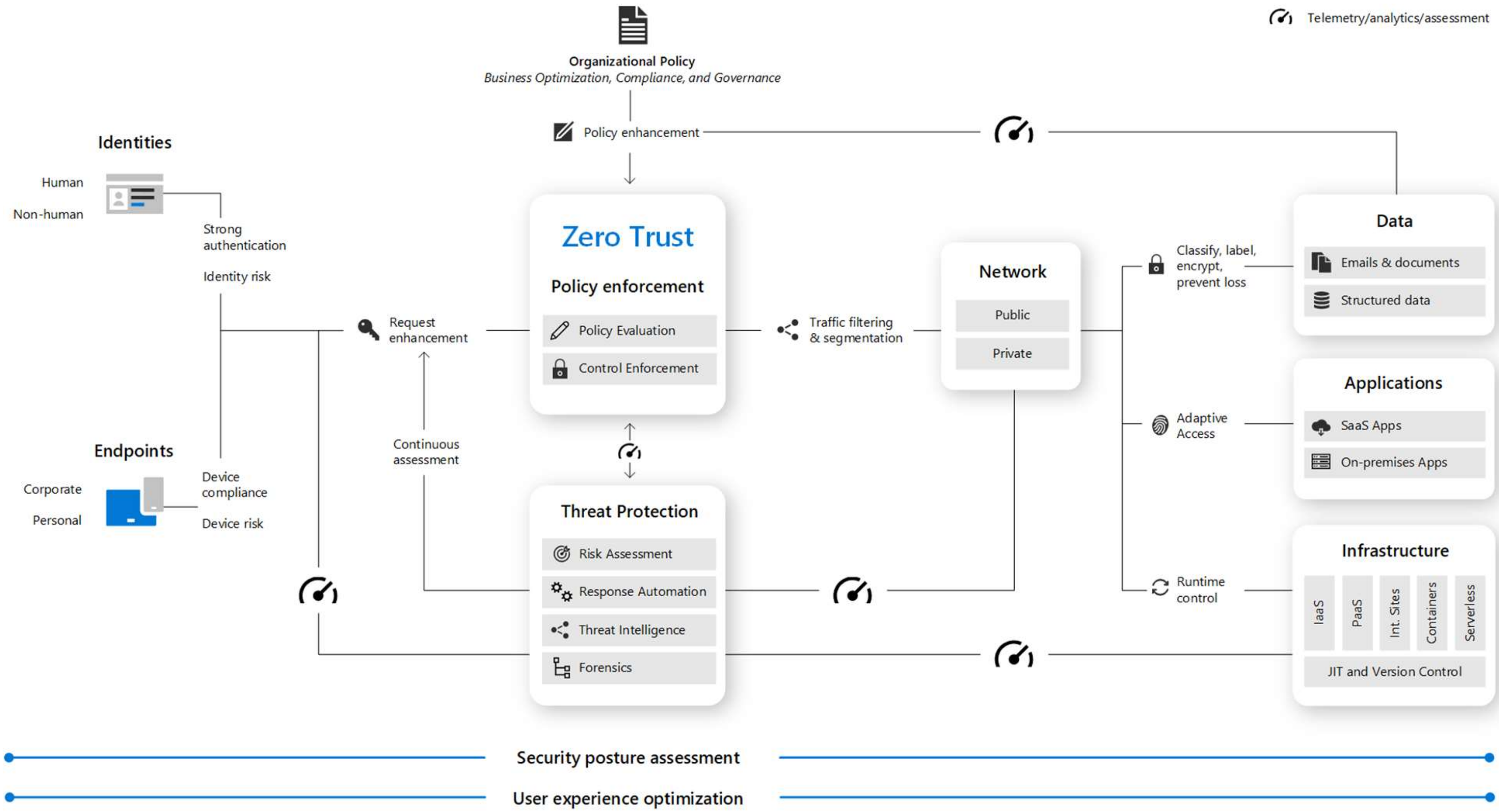
LEARNING PATH
Microsoft Azure Data Fundamentals: Explore non-relational data in Azure
1 hr 9 min
Azure • Data Analyst • Beginner
Save

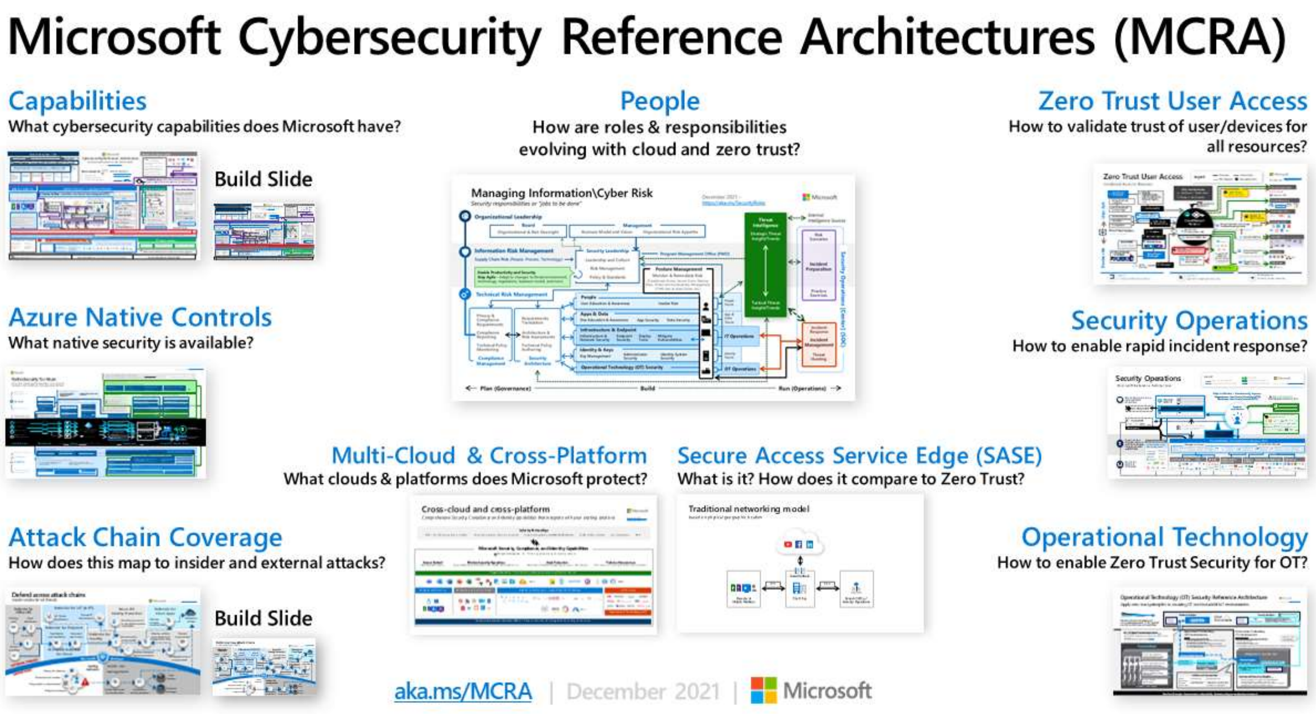
Training | Microsoft Learn

Join Our Security Community - Microsoft Tech Community

AZURE

Zero Trust architecture





Microsoft Cybersecurity Reference Architectures (MCRA)

Capabilities

What cybersecurity capabilities does Microsoft have?

Build Slide

People

How are roles & responsibilities evolving with cloud and zero trust?

Managing Information\Cyber Risk
Organizational Leadership
Information Risk Management
Technical Risk Management
Plan (Governance)
Build
Run (Operations)

Zero Trust User Access

How to validate trust of user/devices for all resources?

Azure Native Controls

What native security is available?

Security Operations

How to enable rapid incident response?

Multi-Cloud & Cross-Platform

What clouds & platforms does Microsoft protect?

Secure Access Service Edge (SASE)

What is it? How does it compare to Zero Trust?

Attack Chain Coverage

How does this map to insider and external attacks?

Build Slide

Operational Technology

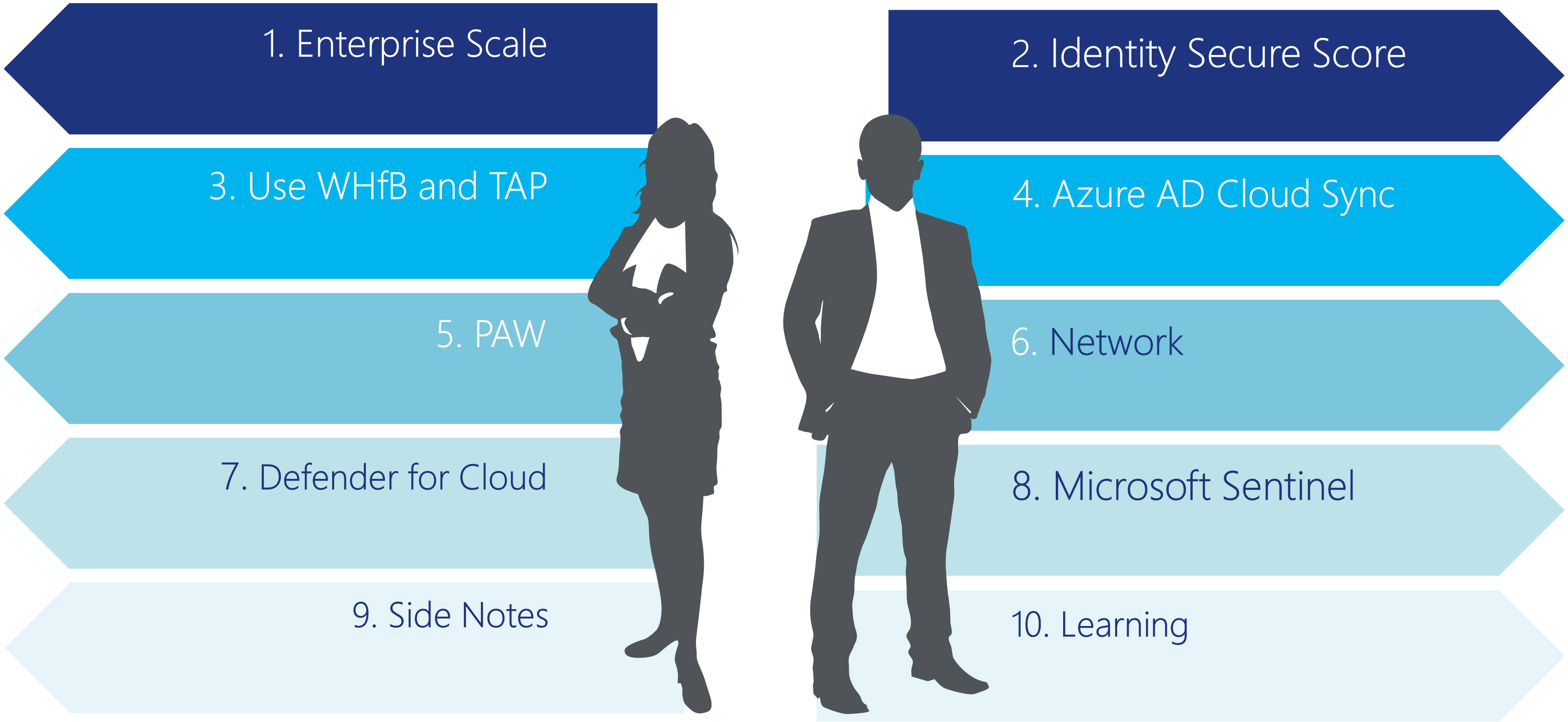
How to enable Zero Trust Security for OT?

aka.ms/MCRA | December 2021 | Microsoft

Top 5 Must have Settings

1. Enable Multifactor Authentication
2. Enable and Integrate Conditional Access
3. Use Azure Advisor recommendations
4. Cloud Security Posture Management is needed

Conclusion



1. Enterprise Scale
2. Identity Secure Score
3. Use WHfB and TAP
4. Azure AD Cloud Sync
5. PAW
6. Network
7. Defender for Cloud
8. Microsoft Sentinel
9. Side Notes
10. Learning

Links

- Reimling.eu – Microsoft will disable Basic auth – What this means and what you have to do
- Block legacy authentication - Azure Active Directory - Microsoft Entra | Microsoft Docs
- Deprecation of Basic authentication in Exchange Online | Microsoft Docs
- Common Conditional Access policies - Azure Active Directory - Microsoft Entra | Microsoft Learn
- Configure a TAP in Azure AD to register Passwordless authentication - Microsoft Entra | Microsoft Docs
- Azure AD Connect: Version release history - Microsoft Entra | Microsoft Docs
- Zero Trust security in Azure | Microsoft Docs
- Enterprise-Scale/README.md at main · Azure/Enterprise-Scale · GitHub
- Azure Active Directory passwordless sign-in - Microsoft Entra | Microsoft Docs
- Azure Arc | Microsoft Learn
- Update management center (preview) overview | Microsoft Docs
- Microsoft Cybersecurity Reference Architectures - Security documentation | Microsoft Learn
- Join Our Security Community - Microsoft Tech Community
- Managed identities for Azure resources - Microsoft Entra | Microsoft Learn
- Microsoft Certified: Azure Security Engineer Associate - Certifications | Microsoft Learn

About “Gregor Reimling”

Azure Meetup
BONN

www.azurebonn.de

Cloud
Inspires
Podcast
Stories and people behind
Cloud Transformation

www.cloudinspires.me

Thank You

Blog

- https://www.Reimling.eu

Contact

- @GregorReimling
- @CloudInspires