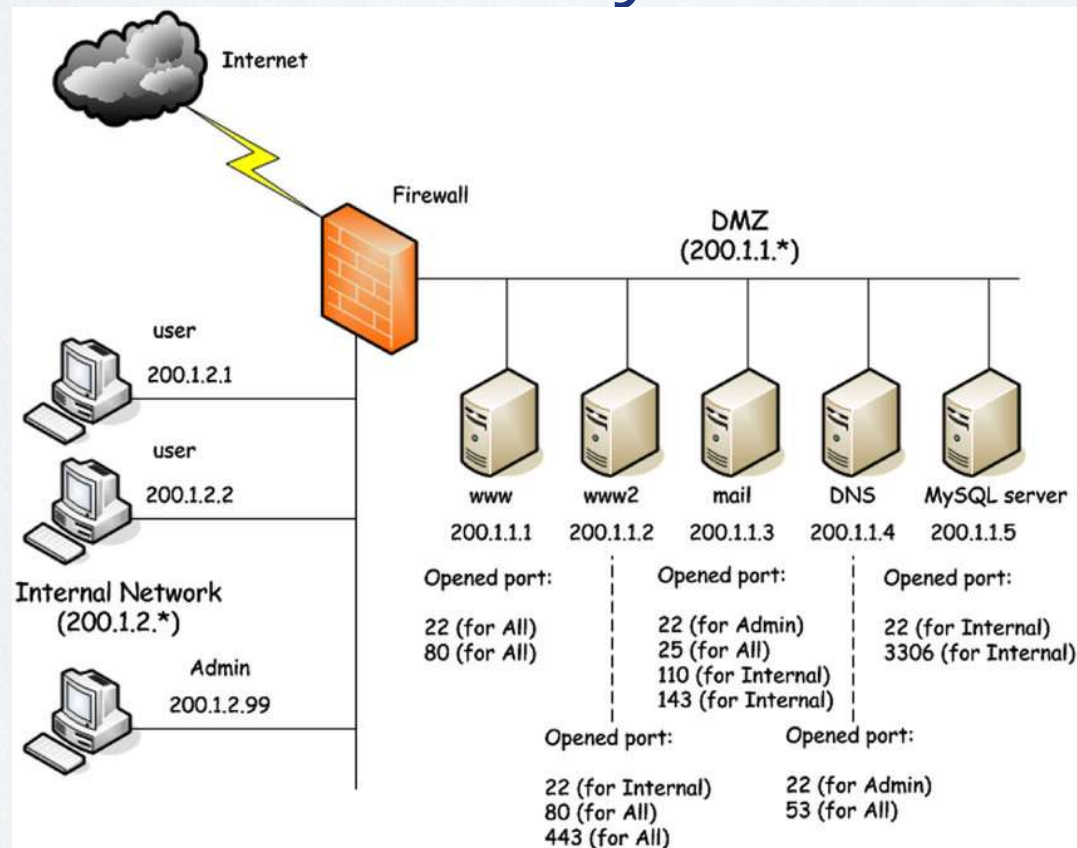


# Top 10 Azure Security Best Practices

Gregor Reimling



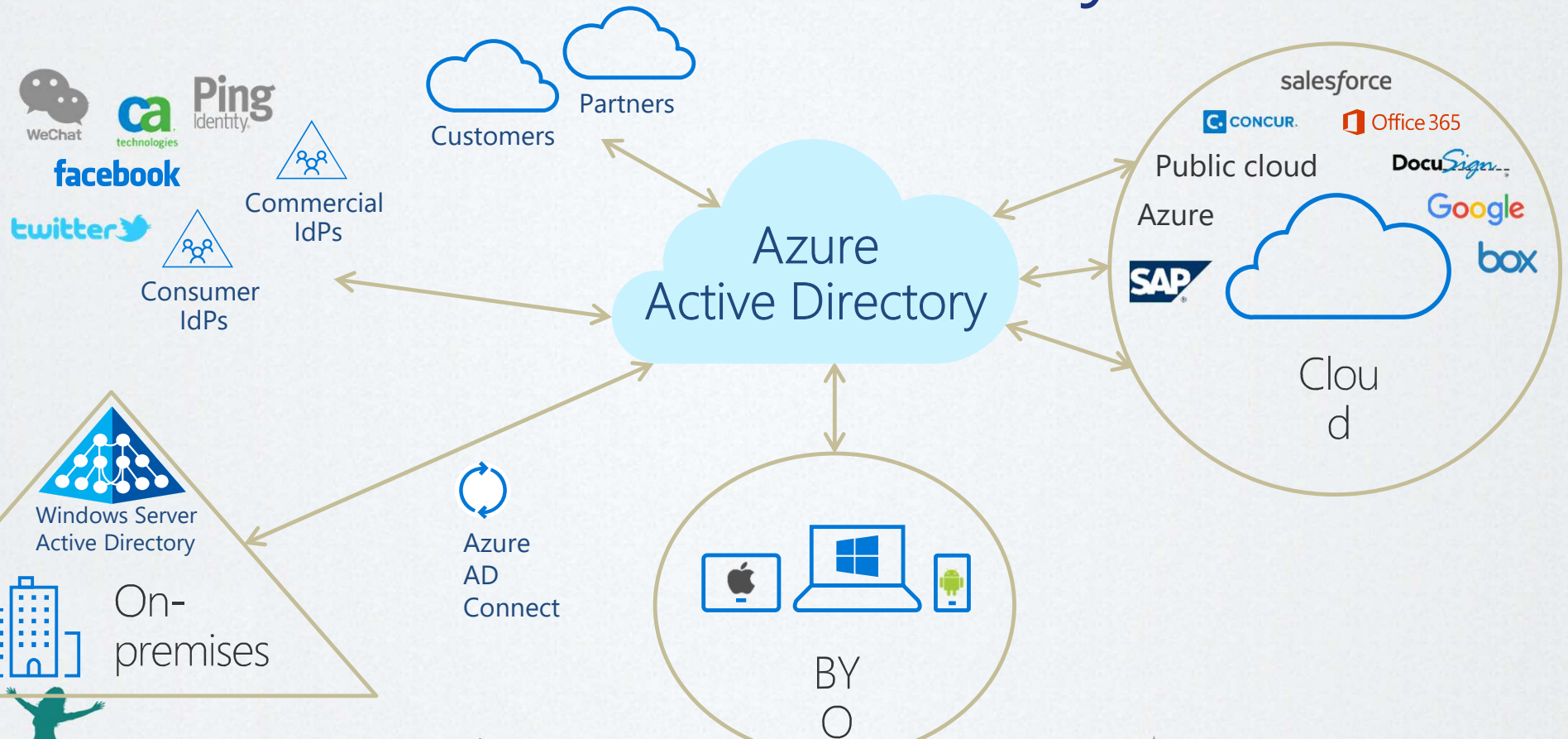
# Yesterday or Today?



A medium size network with a DMZ. | Download Scientific Diagram (researchgate.net)

AZURE

# Definitive Today ☺



Delta-N  
Connecting the Cloud

cegeka

NRGW

LIQUIT

INSPARK

Microsoft





AZURE

# About "Gregor Reimling"



## Focus

Azure Governance, Security and IaaS

## From

Cologne, Germany

## My Blog

<https://www.Reimling.eu>



## Certifications

Cybersecurity Architect, MVP for MS Azure

## Hobbies

Family, Community, Worldtraveler

## Contact



@GregorReimling  
@CloudInspires



[www.cloudinspires.me](http://www.cloudinspires.me)



cegeka

NRW



LIQUIT



INSPARK



Microsoft



AZURE

# Introduction

1. Important Dates

2. Identity Secure Score

3. Use WHfB and TAP

4. Azure AD Cloud Sync

5. PAW

6. Enterprise Scale

7. Network

8. Defender for Cloud

9. Update Management

10. Learning





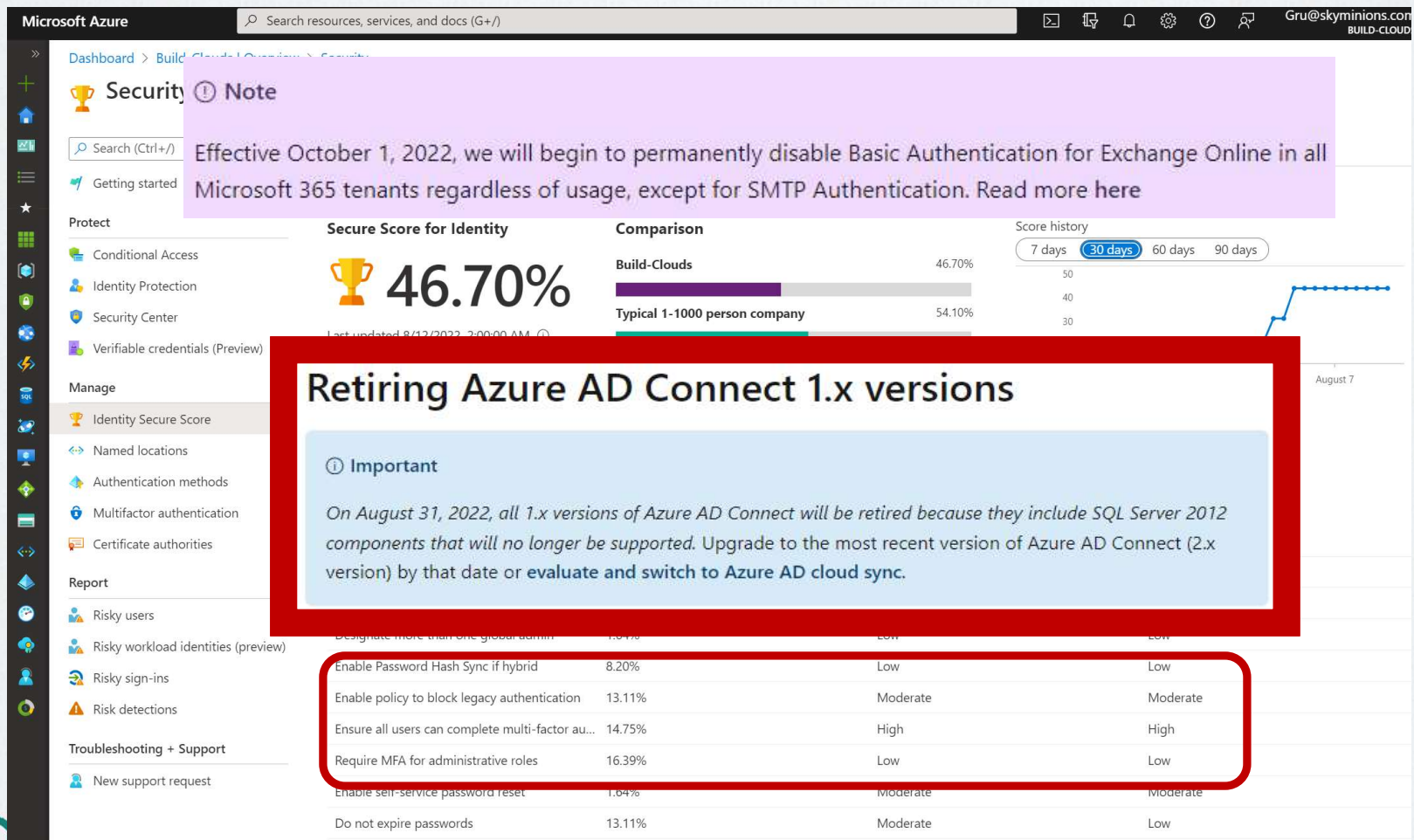
AZURE

# 1. Important Dates





# Identity Secure Score





AZURE

## 2. Identity Secure Score

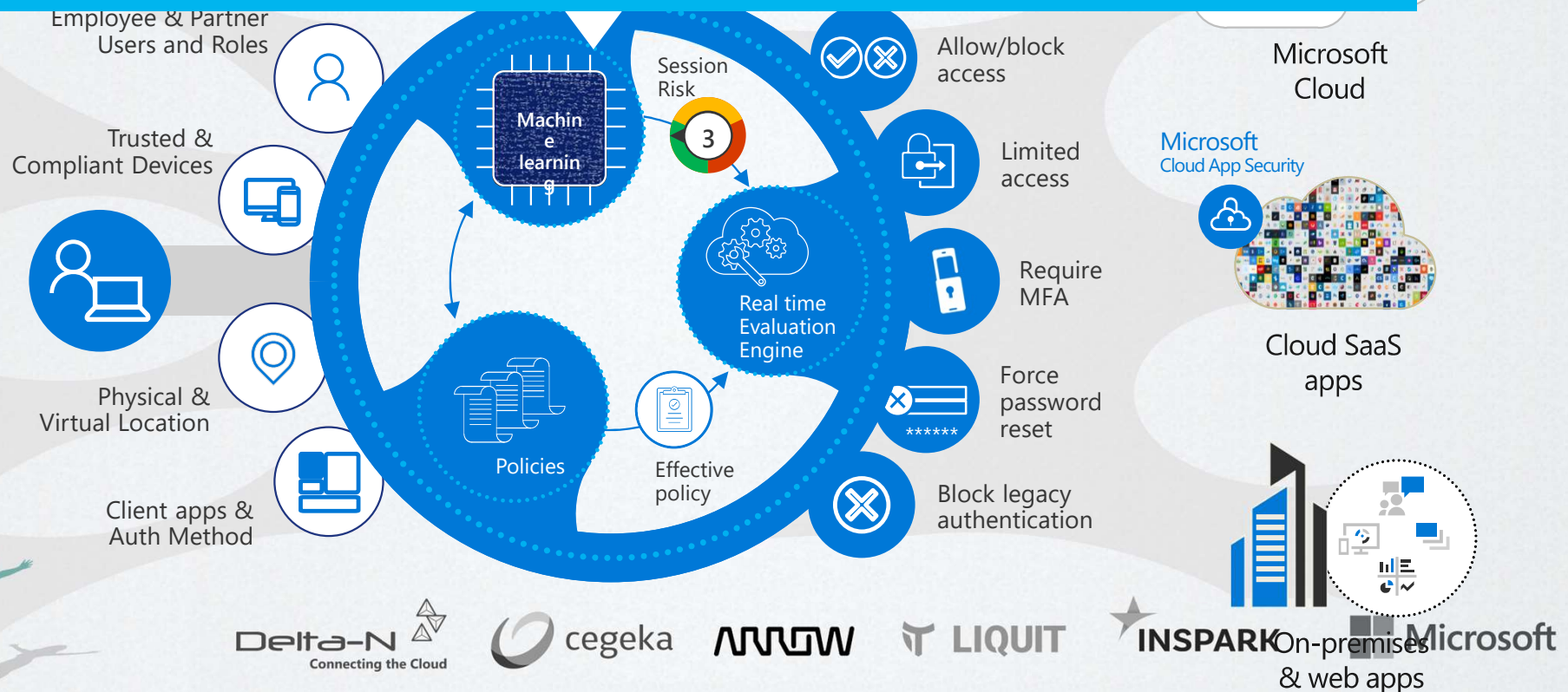




AZURE

# 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






AZURE

Show following settings

- Identity Secure Score
- Conditional Access Template



Delta-N   
Connecting the Cloud

 cegeka

 NRGW

 LIQUIT

 INSPARK

 Microsoft



AZURE

### 3. WHfB and TAP







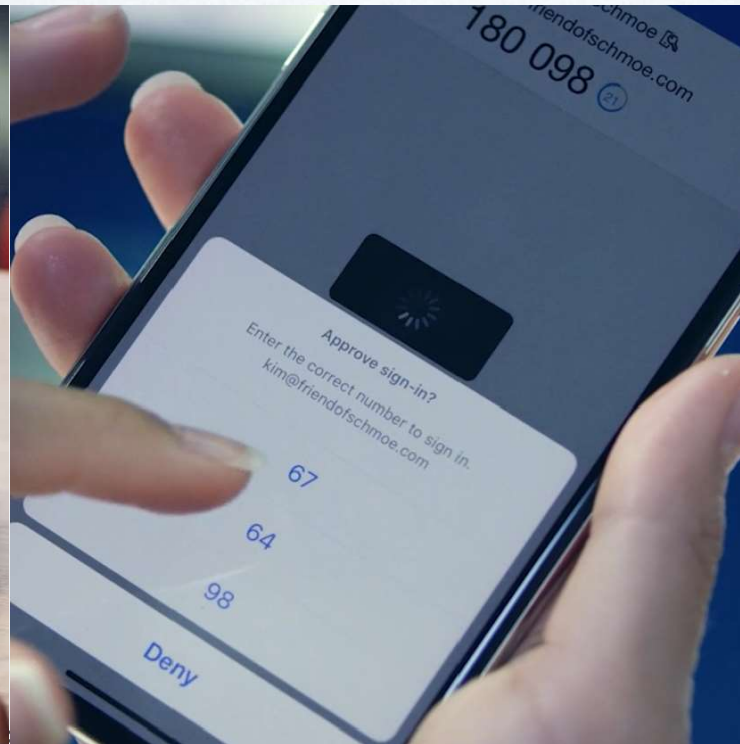
AZURE

# Windows Hello for Business

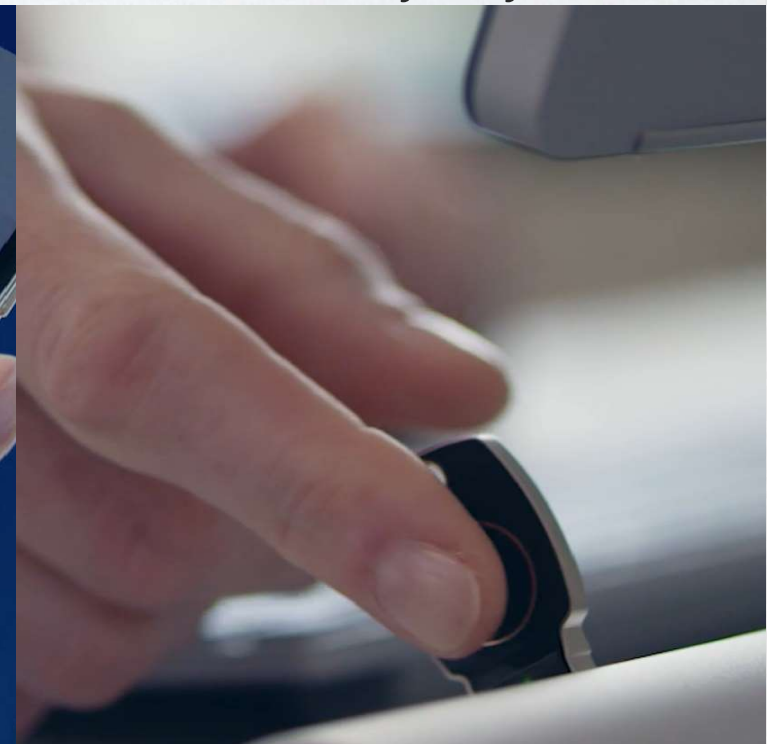
Windows Hello  
for Business



Microsoft  
Authenticator



FIDO2  
Security Keys



Connecting the Cloud

Azure Active Directory passwordless sign-in - Microsoft Entra | Microsoft Docs



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

Temporary Access Pass is a time-limited pass strong credentials and allow onboarding of new users. The Temporary Access Pass authentication method is available for users in the tenant between the duration of the passes in the tenant between 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



← 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.

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

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



Delta-N  
Connecting the Cloud

cegeka

NRGW

LIQUIT

INSPARK

Microsoft

<https://aka.ms/mysecurityinfo>





AZURE

# Checklist for WHfB

## WHfB

- ✓ Windows 10 (1703) or Windows 11
- ✓ MFA must be enabled for the Users
- ✓ Working DNS for internal and external Names
- ✓ Device must be Hybrid Azure AD joined or Full Azure AD joined

## TAP

- ✓ Can be activated under Authentication methods via Azure AD
- ✓ Classic Rollout possible – first for a selected group of users and then for all
- ✓ User in this group will be redirected directly to <https://aka.ms/mysecurityinfo> and must be configure MFA (Authenticator App, FIDO2, etc.)







AZURE

## 4. Azure AD Cloud Sync



AZURE

# Identity Secure Score

Enable PHS  
and forgot  
ADFS

## 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:

Microsoft Azure

Search resources, services, and docs (G+)

Dashboard > Build-Clouds | Overview > Security

### Security | Identity Secure Score

Search (Ctrl+/) 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

7 days 30 days 60 days 90 days

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

DELTA  
Connecting the Cloud

tegeka

AVCWW

LIQUID

INSPIRE

MICROSOFT



AZURE

# 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

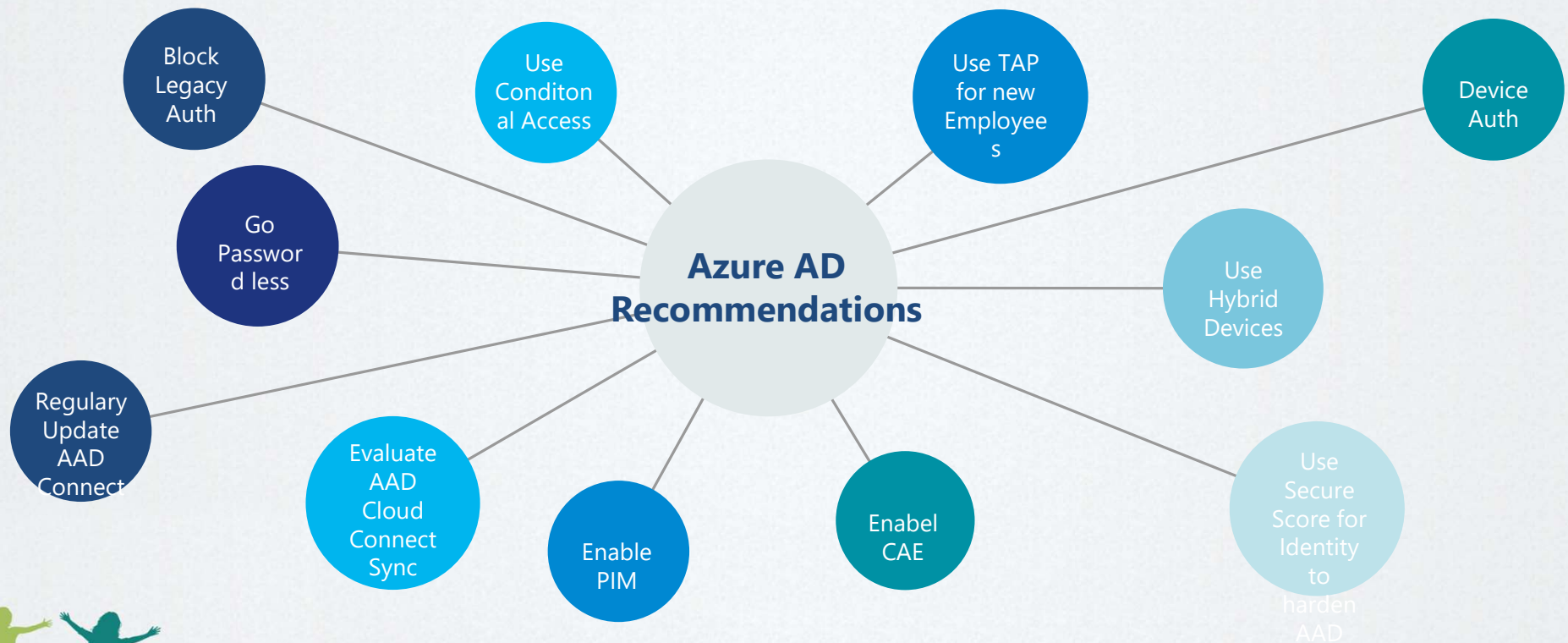






AZURE

# Azure AD Recommendations



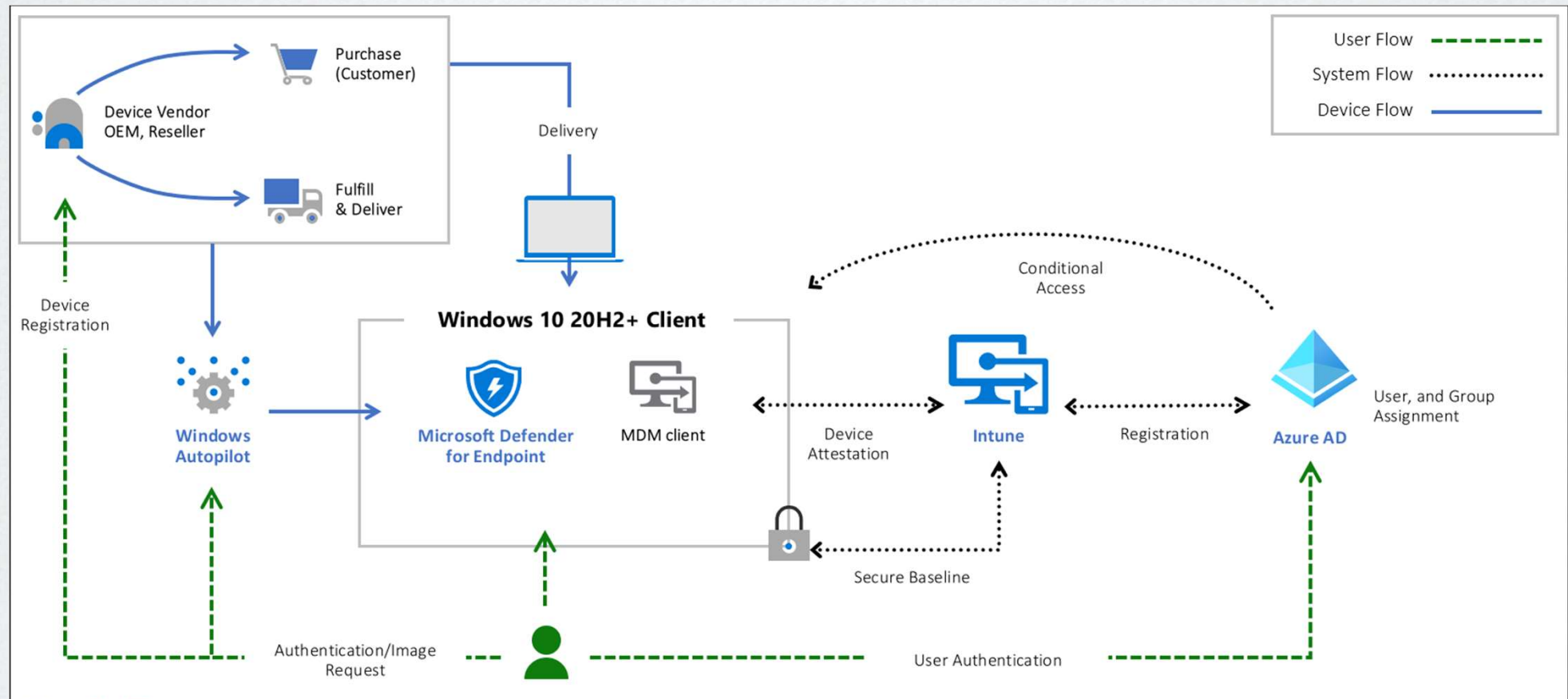


AZURE

## 4. PAW



# Privileged Access Devices



Why are privileged access devices important | Microsoft Learn





AZURE

# PAW with AVD

- ✓ All users needs MFA
- ✓ All Devices must be compliant
- ✓ Minimum of Windows 10 1809 or Windows 11 for Personal
- ✓ Minimum of Windows 10 1903 or Windows 11 for Pooled Desktops
- ✓ Session Hosts in Azure AD DS ≠ Management via Intune
- ✓ Using Windows 10, 2004, 20H2, or 21H1 builds -> install July 2021 Windows Update or a later



Delta-N   
Connecting the Cloud

 cegeka

 NRGW

 LIQUIT

 INSPARK

 Microsoft



AZURE

# Privileged Admin Workstation

- ✓ Use dedicated VMs for manage Azure/Microsoft 365 environments
- ✓ Use this VMs only for Administration tasks
- ✓ Do not enable Internet- / Social media access on this VMs
- ✓ Enforce Device compliance via Conditional Access for this VMs



Delta-N  
Connecting the Cloud

cegeka

NRGW

LIQUIT

INSPARK

Microsoft

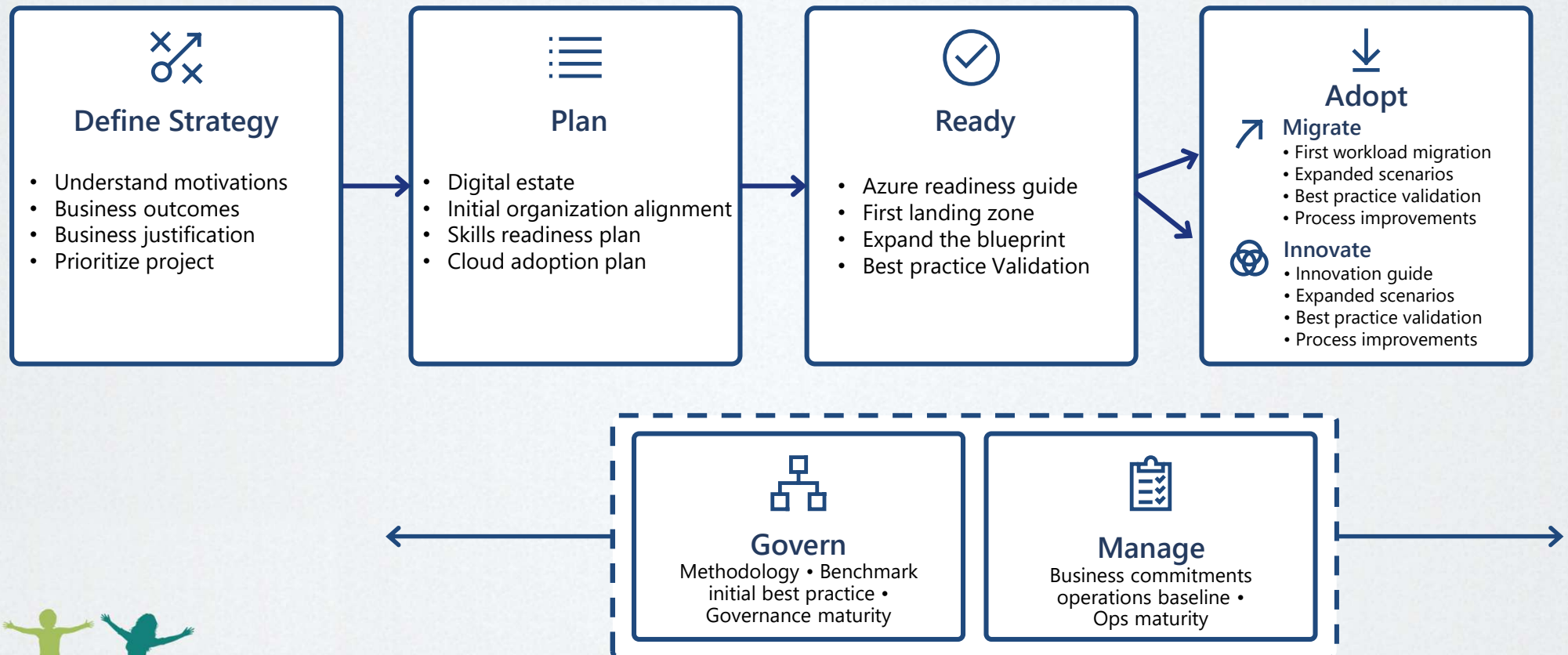
AZURE

## 4. Enterprise Scale



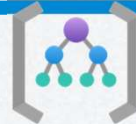


# MS Cloud Adoption Framework

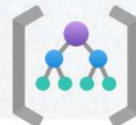


AZURE

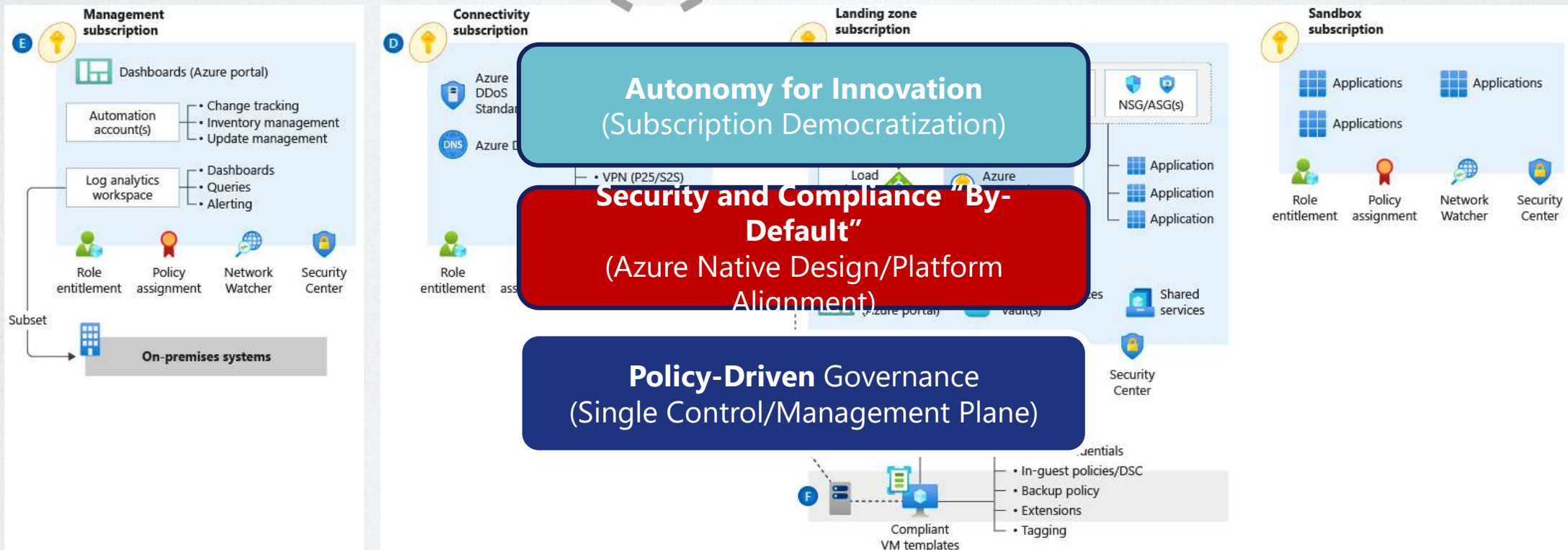
# Enterprise-Scale - Design Principles



Tenant Root Group



Build Clouds



Delta-N  
Connecting the Cloud

cegeka

NRW

LIQUIT

INSPARK

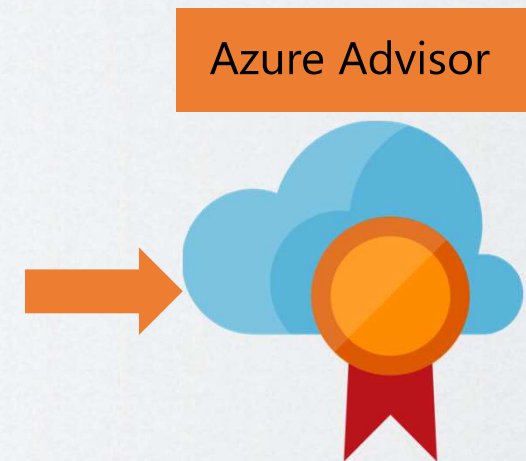
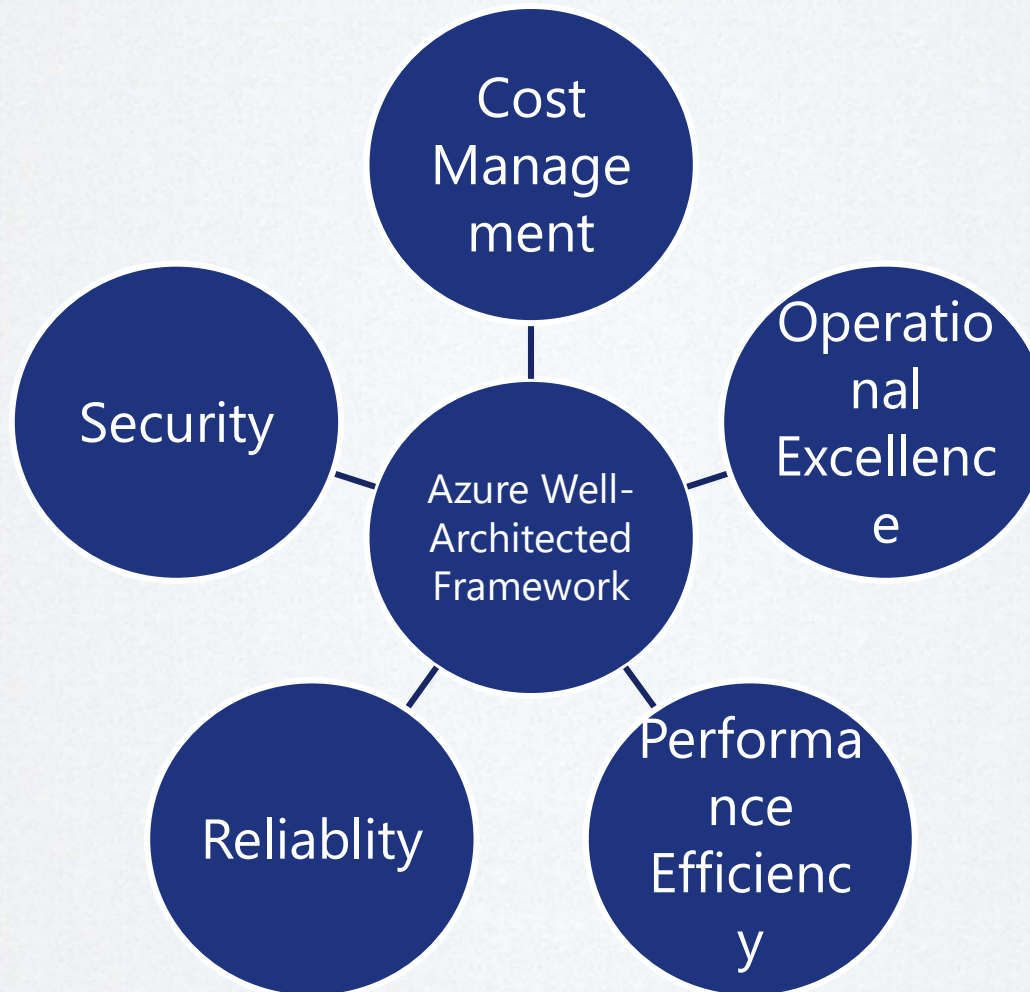
Microsoft



AZURE

# 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."



Delta-N  
Connecting the Cloud

cegeka

ANW

LIQUIT

INSPARK

Microsoft

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





AZURE

# Manage Subscription Policies

## Subscriptions | Manage policies ...

 Feedback

Configure policy settings for Azure subscription operations.

### Subscription leaving AAD directory:

This policy controls if users can change the AAD directory of Azure subscriptions from this directory to a different one. [Learn more](#)

☒ Allow everyone (default)

☐ Permit no one



### Subscription entering AAD directory:

This policy controls if users can bring Azure subscriptions from a different AAD directory into this directory. [Learn more](#)

☒ Allow everyone (default)

☐ Permit no one



### Exempted Users

These are special users who can bypass the policy definitions and will always be able to take subscriptions out of this AAD directory or bring subscriptions into this one.

Search user name or email:

Search by name or email address

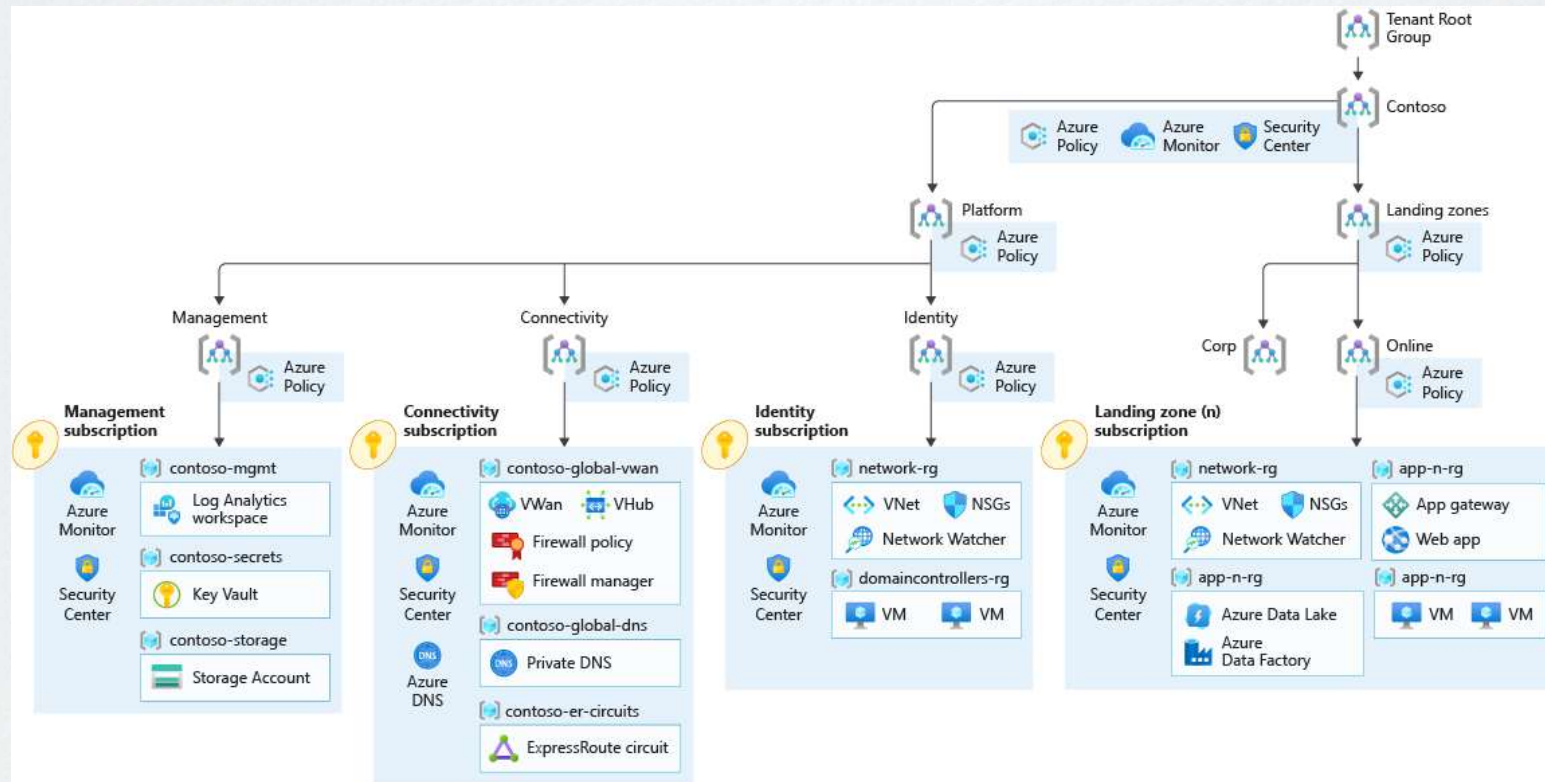


Can be configured in the Overall subscription blade



# 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

# Managed Identities

	System-assigned	User-assigned
Creation	Is part of an Azure resource	Is a stand-alone Azure resource
Life-cycle	Shared life-cycle with the created Azure resource. Delete Azure resource delete also this MI	Must be managed by Azure admin
Sharing across Azure resources	Can not be shared	Can be shared
Common use cases	Workload that contains single Azure resources (like a single VM)	Workloads that run on multiple resources







AZURE


# Demo

Dive into the Azure Portal

- Enterprise Scale
- Azure Advisor



Delta-N   
Connecting the Cloud

 cegeka

 NRGW

 LIQUIT

 INSPIRE

 Microsoft



AZURE

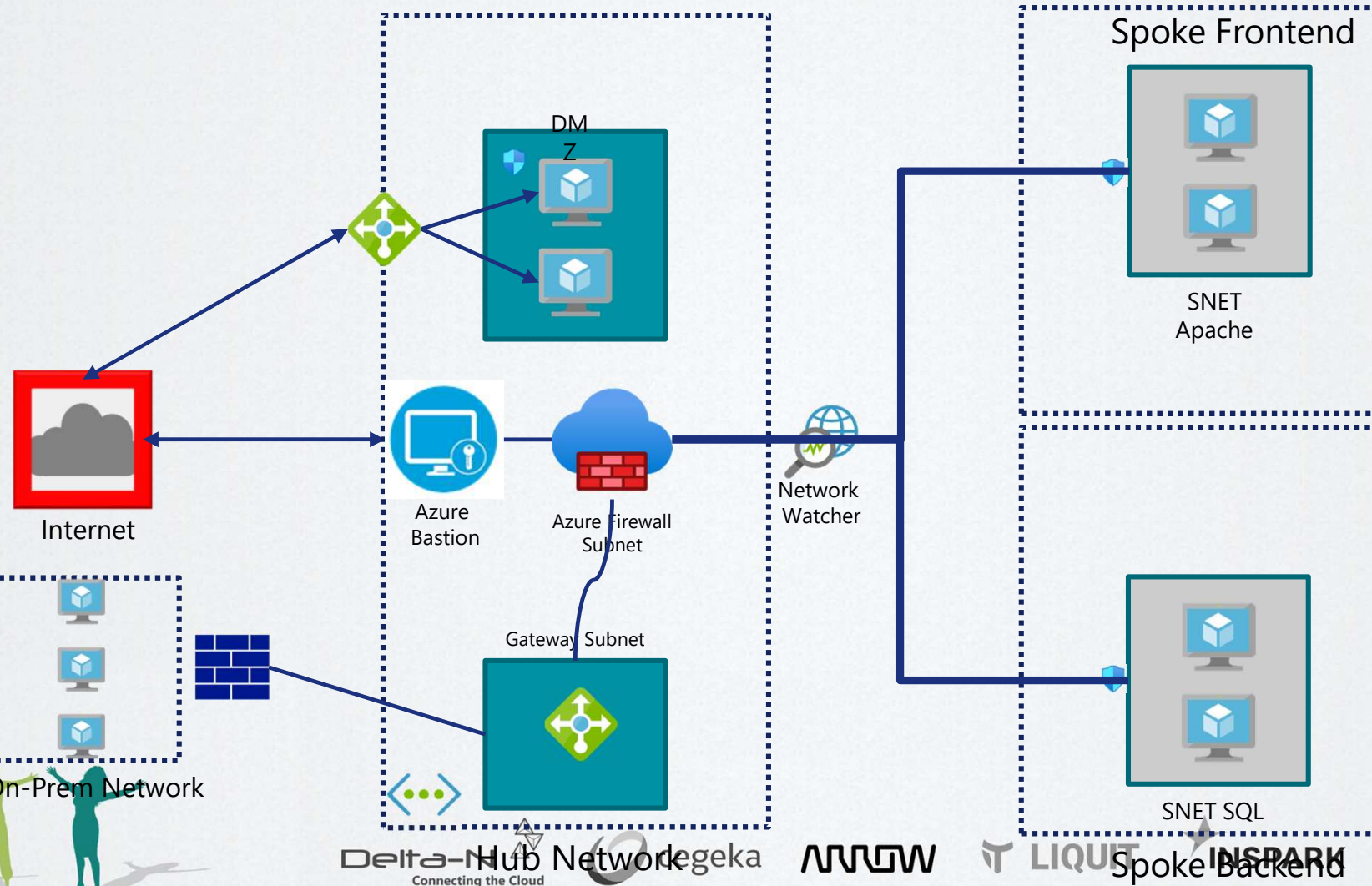
# 7. Network





AZURE

# Network Protection



Delta-Hub Network  
Connecting the Cloud

WGW

LIQUET

INSPIRE  
Spoke Backend

Microsoft





AZURE

# 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 Internet applications



Use DDoS Protection for Web Applications



Use Azure Bastion for VM Management

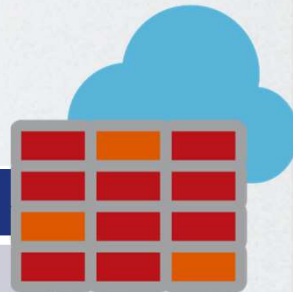




AZURE

# Azure Firewall Editions

New in Private Preview



## Azure Firewall Basic

2 VMs fixed under the hood

Availability Zones

App FQDN Filtering Rules?

Fixed Scale

Threat Intelligence  
(Alert Mode only)

FQDN in Network rules

250-500MBps

Around XXX€

## Azure Firewall Standard

Built-in high availability

Availability Zones

Application FQDN Filtering  
Rules

Unrestricted Cloud Scalability

Threat Intelligence

FQDN in Network rules

30GBps

901,24€ per month

## Azure Firewall Premium

**All from Standard +**

TLS Inspection

IDPS

URL Filtering

Web categories

FQDN in Network rules

30GBps

1.262,29€ per month





AZURE



## 8. MS Defender for Cloud



Delta-N  
Connecting the Cloud

cegeka

NRGW

LIQUIT

INSPARK

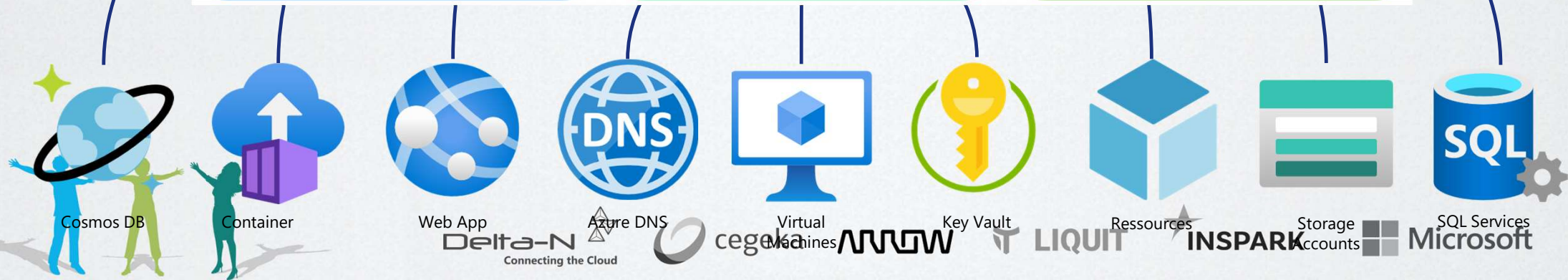
Microsoft





AZURE

# Microsoft Defender for Cloud





AZURE

# 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

Delta-N  
Connecting the Cloud

cegeka

NRGW

LIQUIT

INSPARK

Microsoft

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
<b>Price</b>	<b>5\$ per Server</b>	<b>15\$ per Server</b>

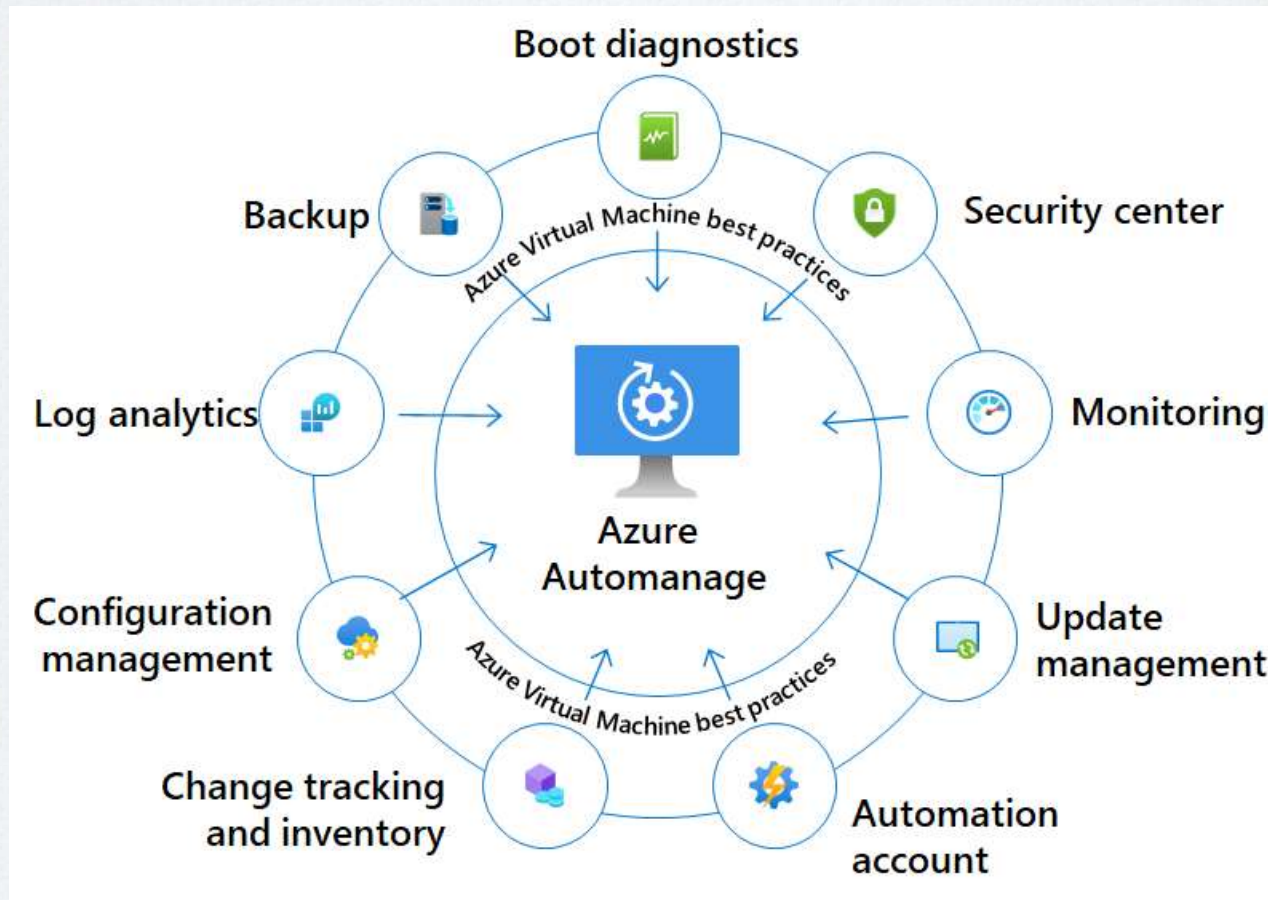






AZURE

# Azure Automanage



**Delta-N**  
Connecting the Cloud

**cegeka**

**NRGW**

**LIQUIT**

**INSPARK**

**Microsoft**



AZURE

# Azure Arc

- Integrate resources outside of Azure into the Azure control plane
- Enable MS Defender for Cloud for all servers (including Azure Arc machines)





AZURE


# Demo

Dive into the Azure Portal

- Microsoft Defender for Cloud
- Threat Protection
- Alerting and Protection



Delta-N   
Connecting the Cloud

 cegeka

 NRGW

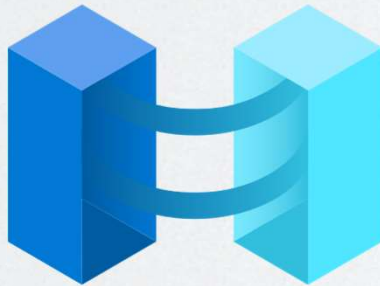
 LIQUIT

 INSPARK

 Microsoft



AZURE



Dashboard > Update management center (Preview) | Machines

Search (Ctrl+F)

Overview  
Getting started

Manage  
Machines  
History  
Support + troubleshooting  
New Support Request

Filter by name  
Subscription: MLGBorn Resource group: All Resource type: All Location: All OS: All Patch orchestration: All

Periodic assessment: All Status: All Tags: All

Total machines: 9  
No updates data: 9  
No updates available: 0  
Updates available: 0  
Reboot Required: 0

Showing 9 of 9 records  
Select all

Name	Update status	Operating system	Resource type	Patch orchestrat...	Periodic assess...	Associated sche...	Status
MLGW106SLex...	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
AVVMMLGMynt1	No updates data	Windows	Azure Virtual Machine	Automatic by OS	No	-	VM deallocated
MLSumpe-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
AVVMMLGDC1	No updates data	Windows	Azure Virtual Machine	Automatic by OS	No	-	VM running
AVVM3CX	No updates data	Linux	Azure Virtual Machine	Image Default	No	-	VM running



## 9. Arc & Update Management



Delta-N  
Connecting the Cloud

cegeka

NRGW

LIQUIT

INSPARK

Microsoft



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



Delta-N  
Connecting the Cloud

cegeka

NRGW

LIQUIT

INSPARK

Microsoft



AZURE

# Azure Policy In-Guest







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





AZURE


# Demo

Dive into the Azure Portal

- Update Management Center



Delta-N   
Connecting the Cloud

 cegeka

 NRGW

 LIQUIT

 INSPARK

 Microsoft

# Learning

Popular learning paths and modules

<p>LEARNING PATH</p> <p>Microsoft Azure Fundamentals: Describe cloud concepts</p> <p>🕒 52 min</p> <p>Azure • Administrator • Beginner</p> <p>🔒 Save</p>	<p>LEARNING PATH</p> <p>Microsoft Azure Data Fundamentals: Explore core data concepts</p> <p>🕒 45 min</p> <p>Azure • Data Analyst • Beginner</p> <p>🔒 Save</p>	<p>MODULE</p> <p>Discuss Azure fundamental concepts</p> <p>🕒 24 min ⭐⭐⭐⭐ 4.8 (123,249)</p> <p>Azure • Administrator • Beginner</p> <p>🔒 Save</p>
<p>MODULE</p> <p>Explore fundamentals of data visualization</p> <p>🕒 38 min ⭐⭐⭐⭐ 4.7 (4,086)</p> <p>Azure • Administrator • Beginner</p> <p>🔒 Save</p>	<p>MODULE</p> <p>Introduction to Azure fundamentals</p> <p>🕒 43 min ⭐⭐⭐⭐ 4.8 (202,694)</p> <p>Azure • Administrator • Beginner</p> <p>🔒 Save</p>	<p>MODULE</p> <p>Describe core Azure architectural components</p> <p>🕒 27 min ⭐⭐⭐⭐ 4.8 (88,090)</p> <p>Azure • Administrator • Beginner</p> <p>🔒 Save</p>
<p>LEARNING PATH</p> <p>Microsoft Azure Data Fundamentals: Explore relational data in Azure</p> <p>🕒 1 hr 13 min</p> <p>Azure • Data Analyst • Beginner</p> <p>🔒 Save</p>	<p>MODULE</p> <p>Introduction to Microsoft Power Platform</p> <p>🕒 36 min ⭐⭐⭐⭐ 4.7 (37,807)</p> <p>Microsoft Power Platform • Business Analyst • Beginner</p> <p>🔒 Save</p>	<p>LEARNING PATH</p> <p>Microsoft Azure Data Fundamentals: Explore non-relational data in Azure</p> <p>🕒 1 hr 9 min</p> <p>Azure • Data Analyst • Beginner</p> <p>🔒 Save</p>

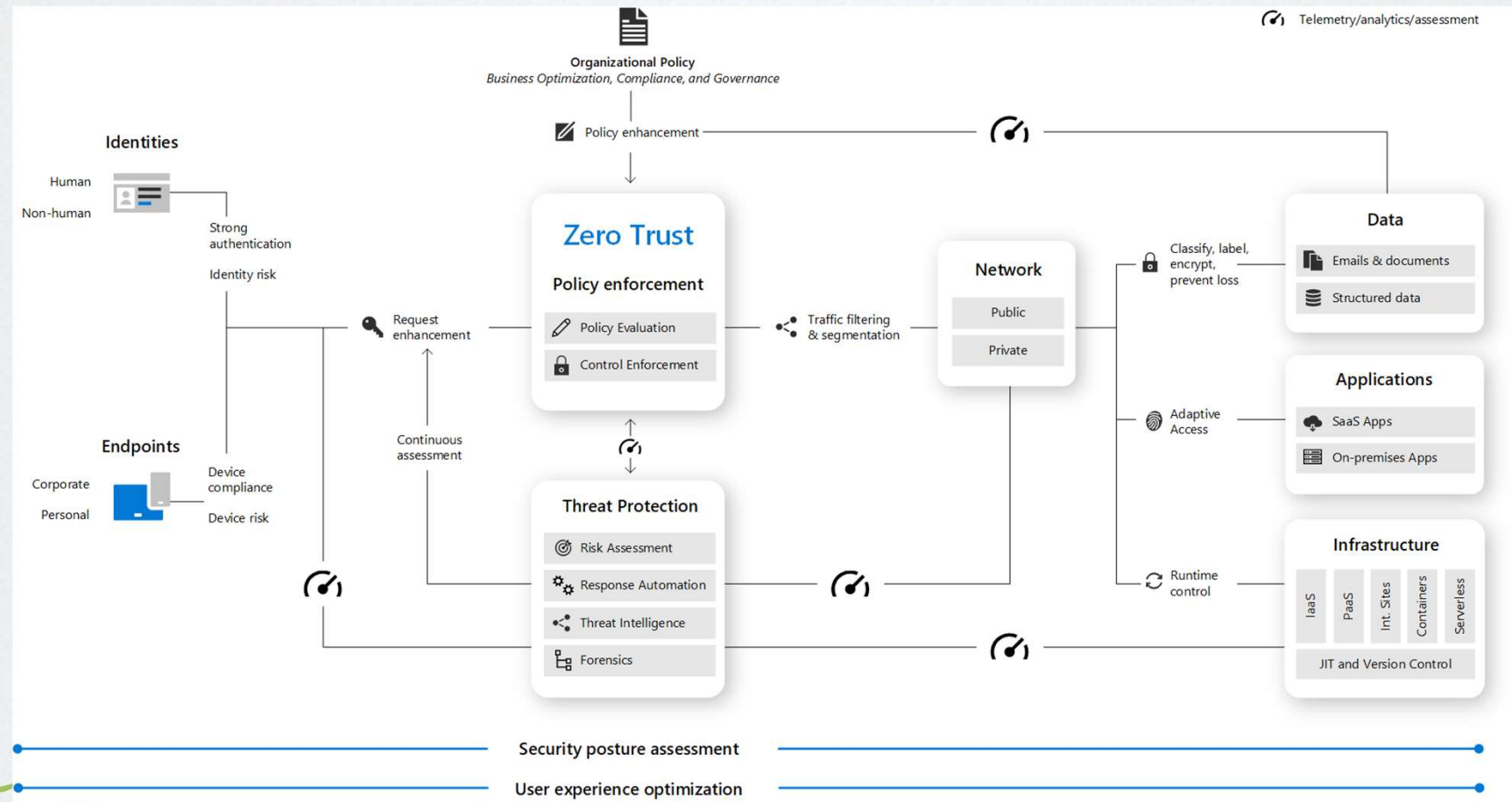
[Training | Microsoft Learn](#)

[Join Our Security Community - Microsoft Tech Community](#)





# Zero Trust architecture



# Microsoft Cybersecurity Reference Architectures (MCRA)

## Capabilities

What cybersecurity capabilities does Microsoft have?



## Azure Native Controls

What native security is available?



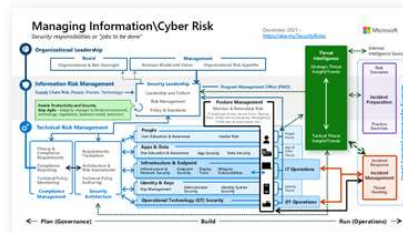
## Attack Chain Coverage

How does this map to insider and external attacks?



## People

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



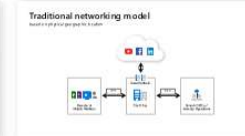
## Multi-Cloud & Cross-Platform

What clouds & platforms does Microsoft protect?



## Secure Access Service Edge (SASE)

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



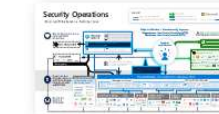
## Zero Trust User Access

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



## Security Operations

How to enable rapid incident response?



## Operational Technology

How to enable Zero Trust Security for OT?



[aka.ms/MCRA](https://aka.ms/MCRA) | December 2021 | Microsoft



AZURE

# Abstract

Use Identity Secure Score to harden your Credentials and your Tenant



Go with Enterprise Scale approach – use more than one subscription



Enable the benefits of Management Groups and Policy assignment



Hub and Spoke or virtual WAN is a requirement and not just a recommendation



Work with Azure Advisor



Harden your Azure Environment with Microsoft Defender for Cloud





AZURE

# Conclusion

1. Important Dates

2. Identity Secure Score

3. Use WHfB and TAP

4. Azure AD Cloud Sync

5. PAW

6. Enterprise Scale

7. Network

8. Defender for Cloud

9. Update Management

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](#)





SECURITY

# Thank you partners!

ULTIMATE



GOLD



Business  
Services



eG Innovations



COMMUNITY





SECURITY

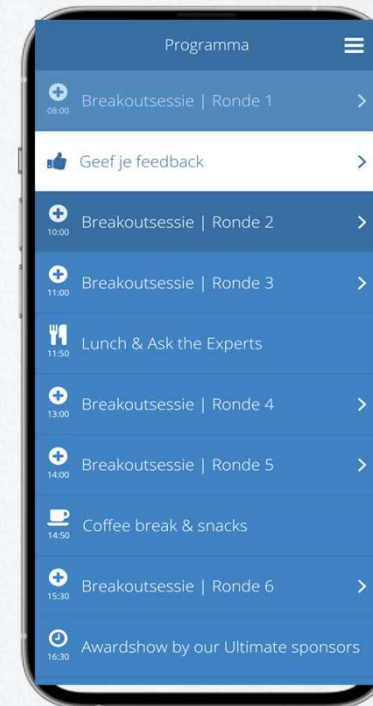
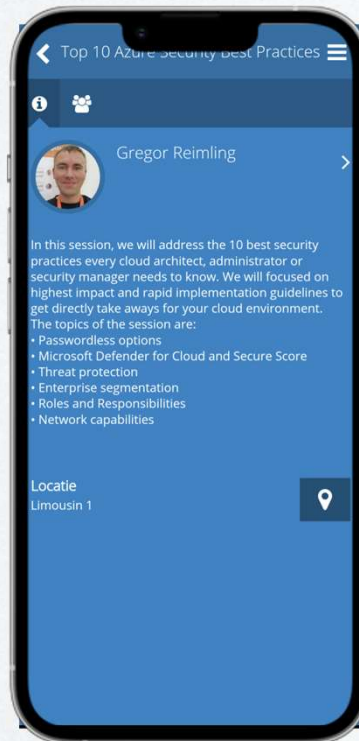
# Please rate my session in the Yellenge app



Event: **EXPERTS22**

Download on the  
**App Store**

ANDROID APP ON  
**Google play**



**Delta-N**  
Connecting the Cloud

 **cegeka**

**NRGW**

 **LIQUIT**

 **INSPARK**

 **Microsoft**

## About "Gregor Reimling"



Thank You



[www.cloudinspires.me](http://www.cloudinspires.me)

### Blog

- <https://www.Reimling.eu>



### Contact



- @GregorReimling
- @CloudInspires





AZURE



<https://forms.microsoft.com/r/Bwt6hjFEHs>

## Blog

- <https://www.Reimling.eu>



## About "Gregor Reimling"



## Thank You



[www.cloudinspires.me](http://www.cloudinspires.me)

## Contact



- @GregorReimling
- @CloudInspires







AZURE

## Turned-Off Basic Authentication – All Protocols

MC419351 · Published 24. Aug. 2022

 Archive  Share  Copy link  Mark as unread

### Service & monthly active users

 Exchange Online (11)  Microsoft 365 suite

### Tag

ADMIN IMPACT

USER IMPACT

### Message Summary

We are making some changes to improve the security of your tenant. [We announced](#) in 2019 we would be retiring Basic Authentication for legacy protocols and in early 2021 [we announced](#) we would begin to retire Basic Authentication for protocols not being used in tenants. You can always read the latest information about our plans to turn off Basic Authentication [here](#).

Today we turned off Basic Authentication for POP3, IMAP4, Remote PowerShell, Exchange Web Services, Offline Address Book, MAPI, RPC, SMTP AUTH and Exchange ActiveSync protocol in your tenant. Based on our telemetry, no-one is currently using Basic Authentication with those protocols in your tenant and so we expect there to be no impact to you.

We have previously communicated this change via Message Center: MC191153 on 9/20/19, MC204828 on 2/26/20, MC208814 on 4/6/2020, MC23771 on 2/4/2021, MC375736 on 5/4/2022 and most recently in the **Basic Authentication – All Protocols** Message Center post sent approximately 7 days ago.



INSPIRE





AZURE





AZURE







10<sup>TH</sup> ANNIVERSARY  
EDITION

**Experts**  **Live** Netherlands