Gregor Reimling

Top 10 Azure Security Best Practices

About “Gregor Reimling”

Azure Meetup
BONN

azurebonn

Focus

Azure Governance, Security and IaaS

Certifications

Cloud Architect & MVP for MS Azure

Cologne, Germany

Family, Community, Worldtraveler

https://www.Reimling.eu

Cloud Inspires Podcast

Stories and people behind Cloud Transformation

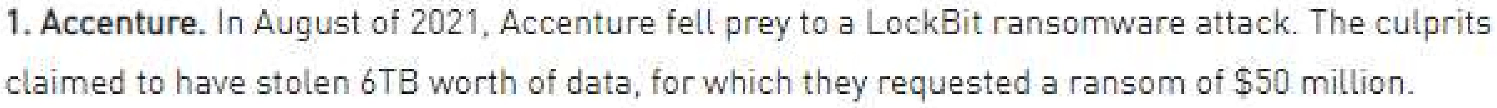
cloudinspires

@GregorReimling

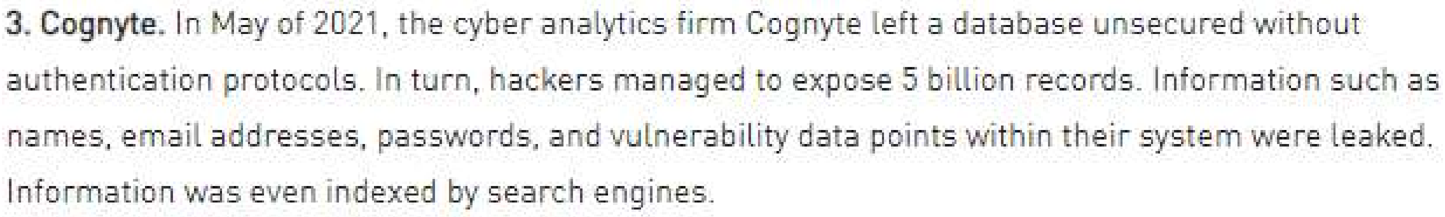
@CloudInspires

81% of companies had a cloud security incident in the last year

81% of companies had a cloud security incident in the last year (cloudcomputing-news.net)



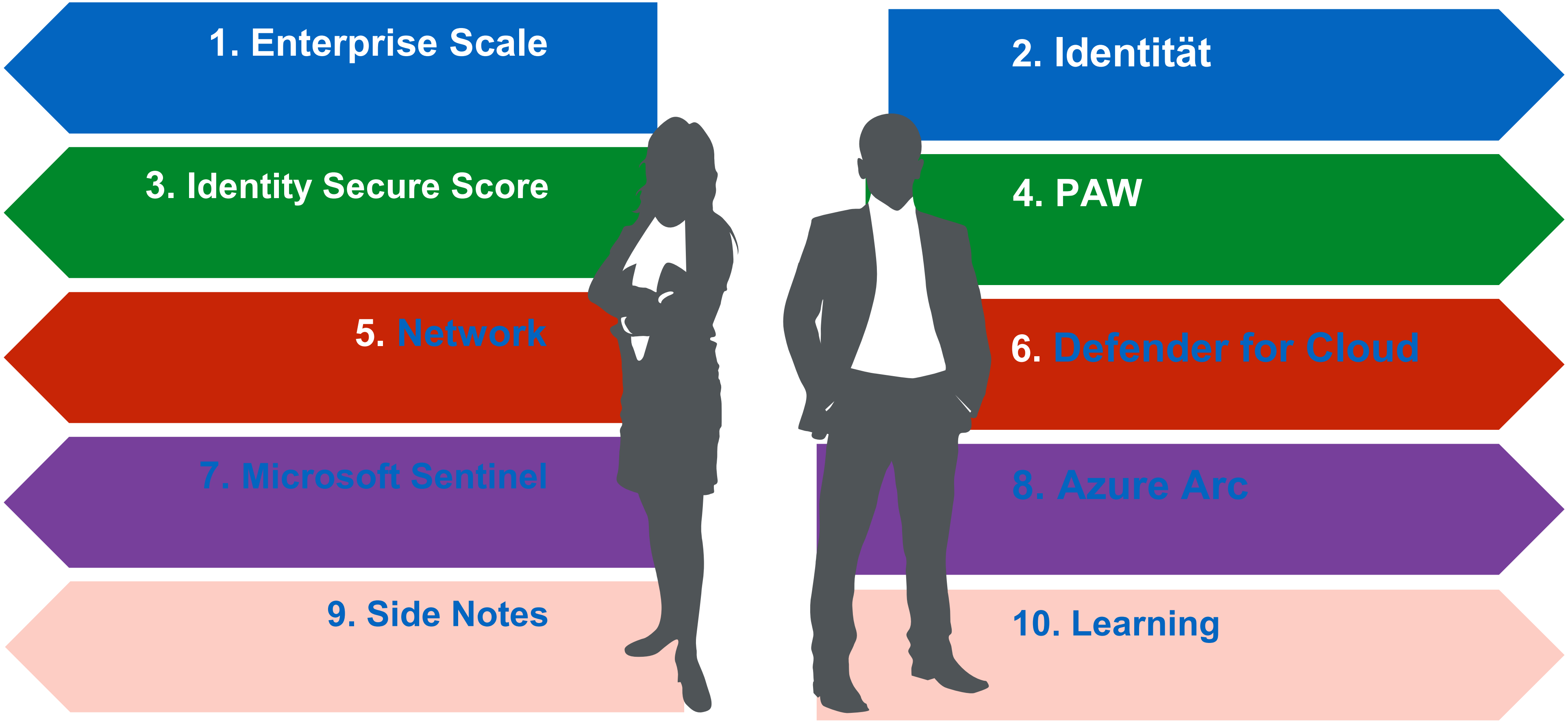
1. Accenture. In August of 2021, Accenture fell prey to a LockBit ransomware attack. The culprits claimed to have stolen 6TB worth of data, for which they requested a ransom of $50 million.



3. Cognyte. In May of 2021, the cyber analytics firm Cognyte left a database unsecured without authentication protocols. In turn, hackers managed to expose 5 billion records. Information such as names, email addresses, passwords, and vulnerability data points within their system were leaked. Information was even indexed by search engines.

Top 5 cloud security breaches (and lessons) 2021 and 2022 (cybertalk.org)

Introduction

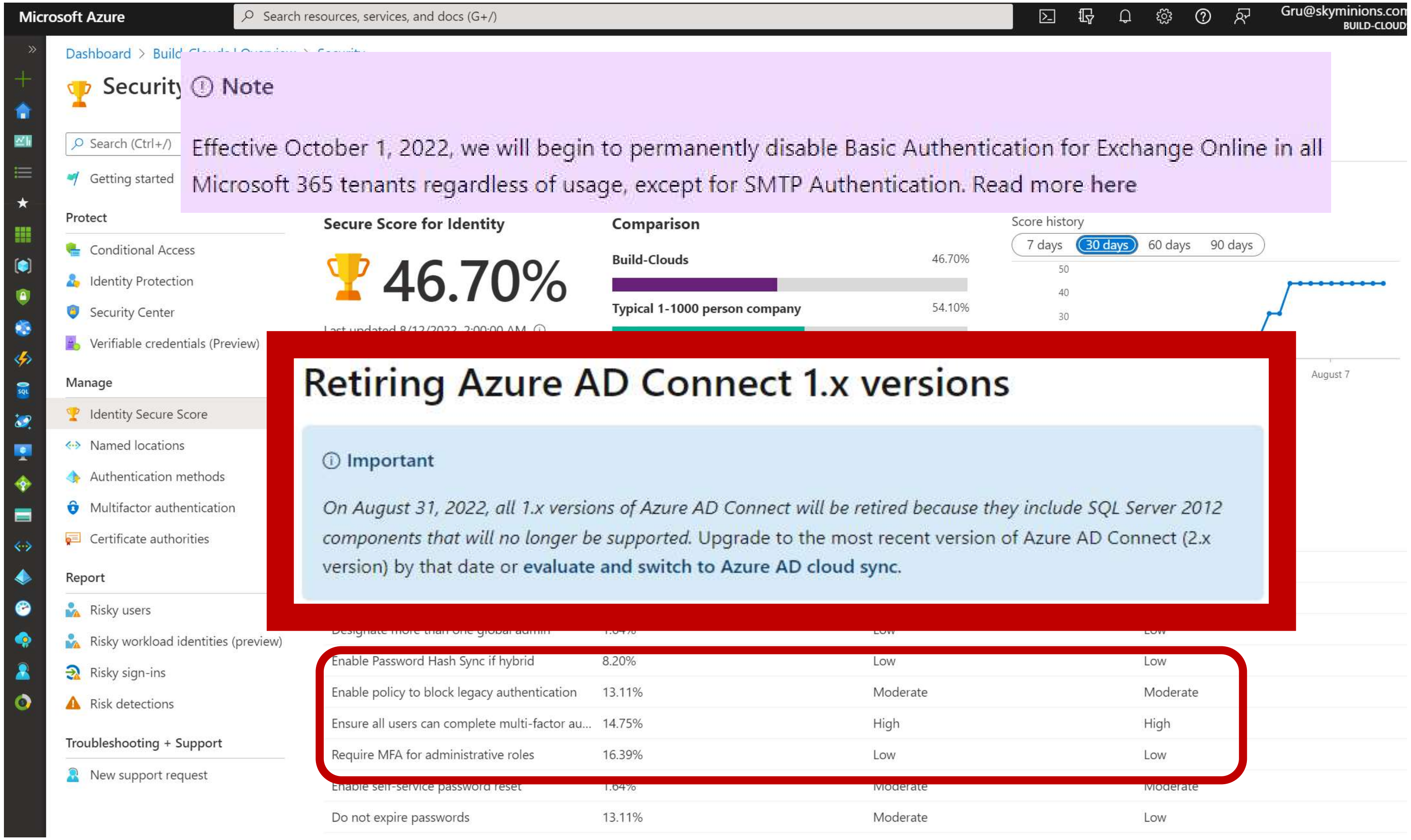


1. Enterprise Scale
2. Identität
3. Identity Secure Score
4. PAW
5. Network
6. Defender for Cloud
7. Microsoft Sentinel
8. Azure Arc
9. Side Notes
10. Learning

@GregorReimling

#ITTage

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

Retiring Azure AD Connect 1.x versions

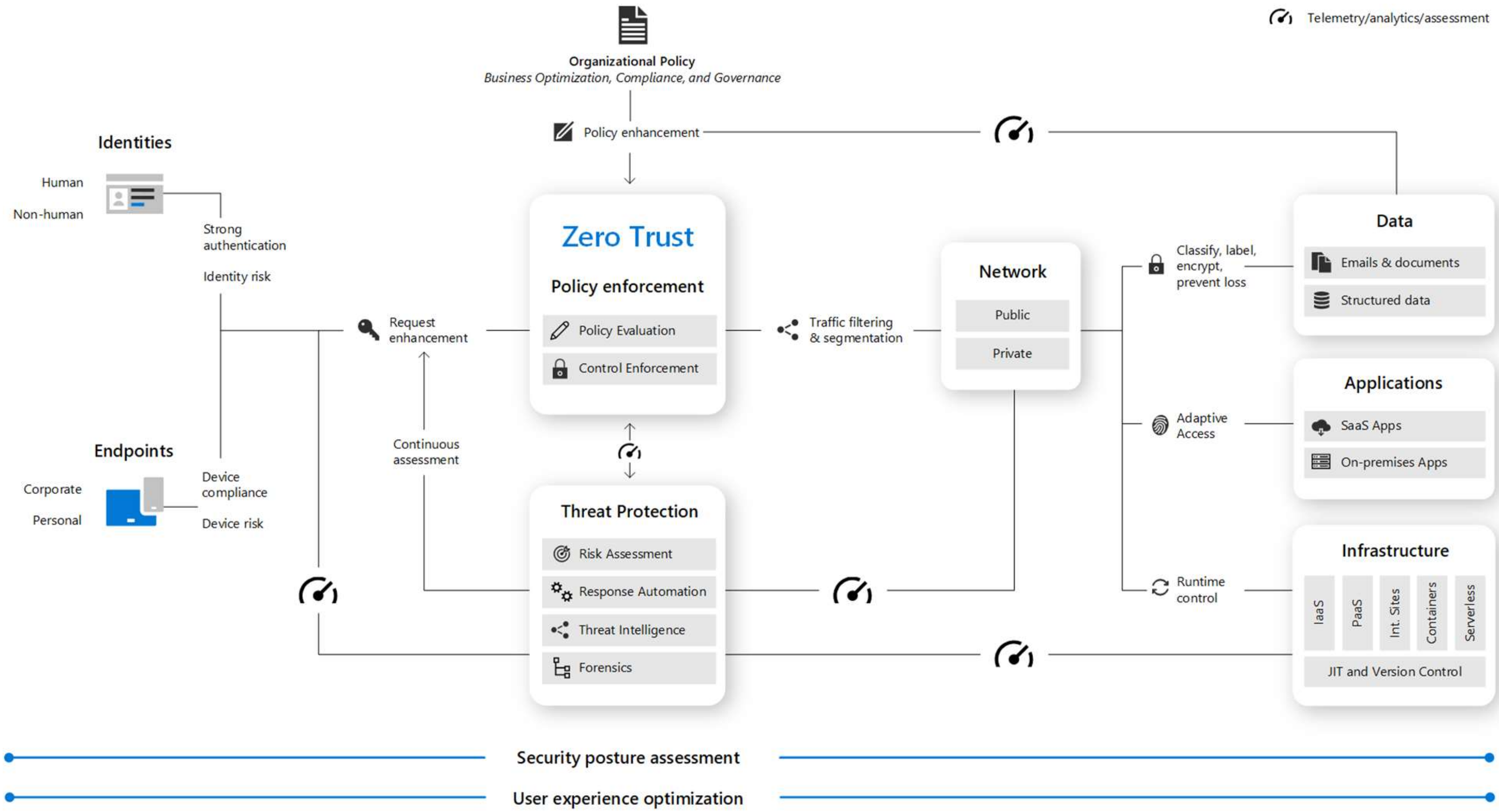
ⓘ **Important**

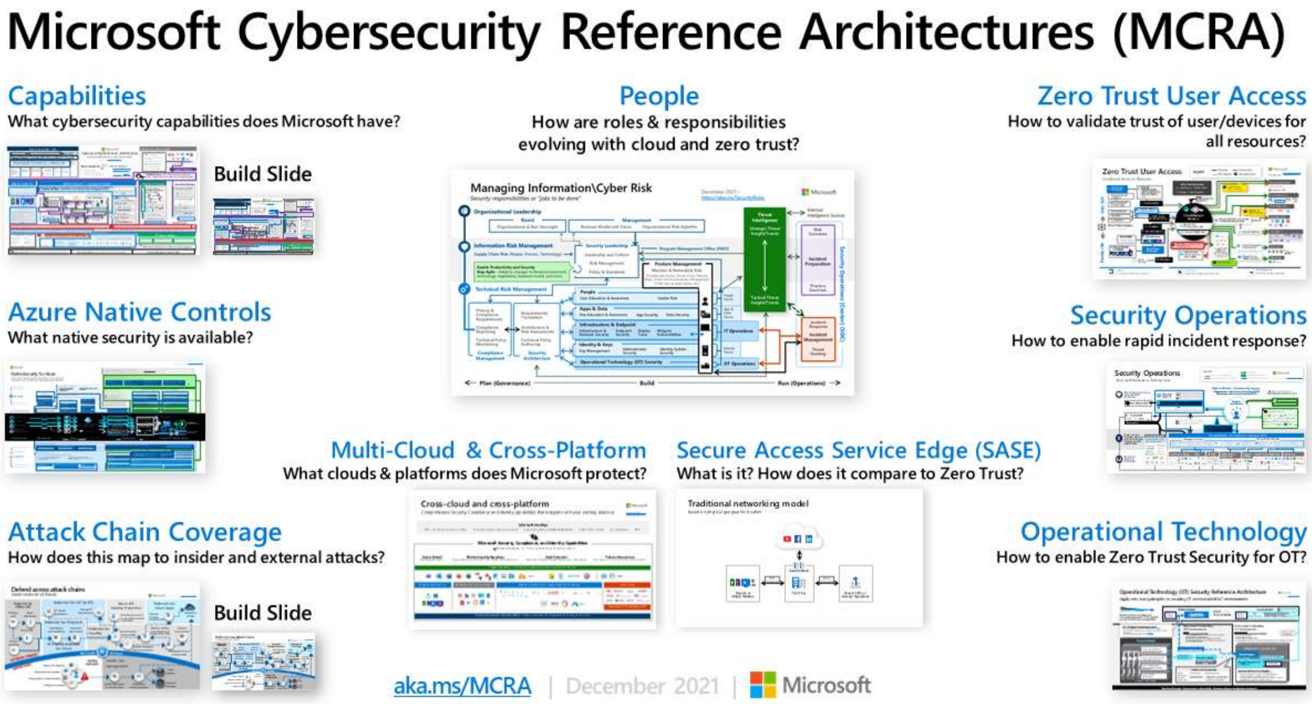
On August 31, 2022, all 1.x versions of Azure AD Connect will be retired because they include SQL Server 2012 components that will no longer be supported. Upgrade to the most recent version of Azure AD Connect (2.x version) by that date or **evaluate and switch to Azure AD cloud sync.**

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

Zero Trust

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?

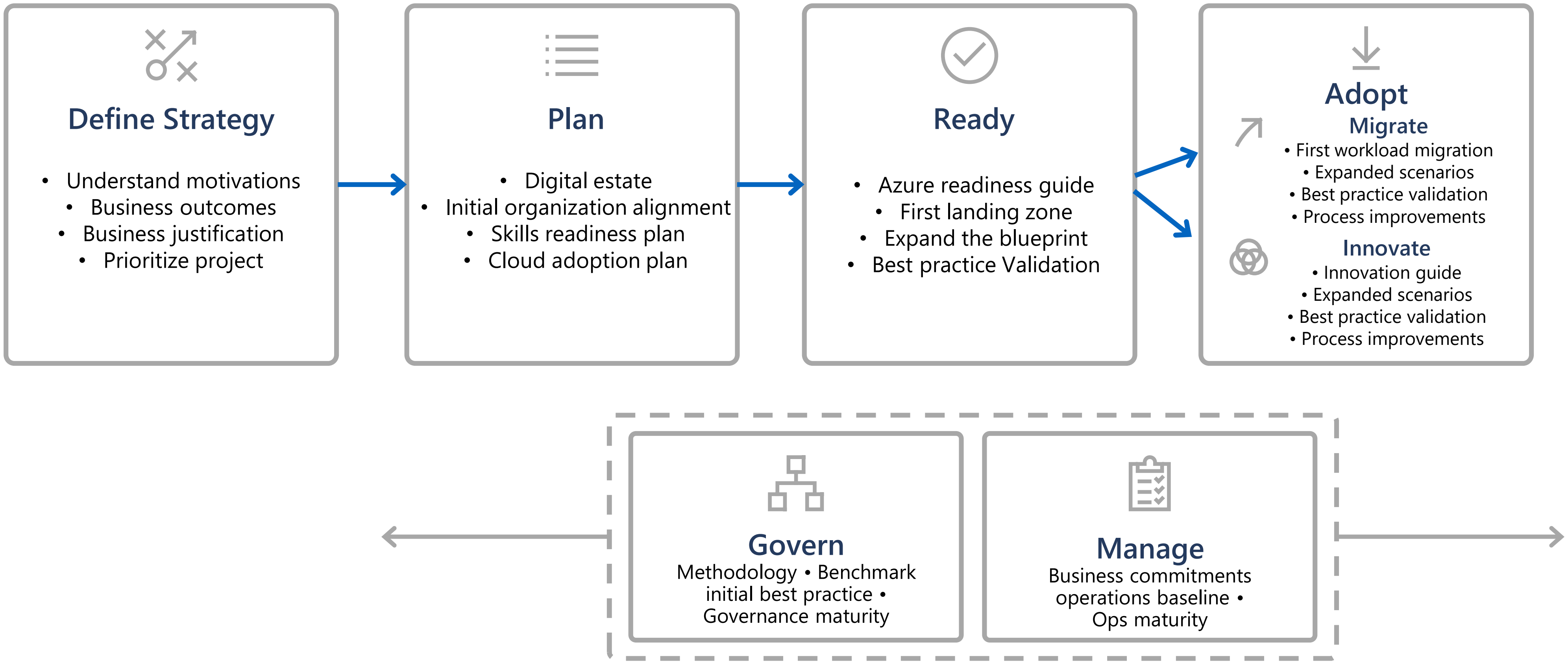
Attack Chain Coverage
How does this map to insider and external attacks?

Build Slide

Operational Technology
How to enable Zero Trust Security for OT?

aka.ms/MCRA | December 2021 | Microsoft

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

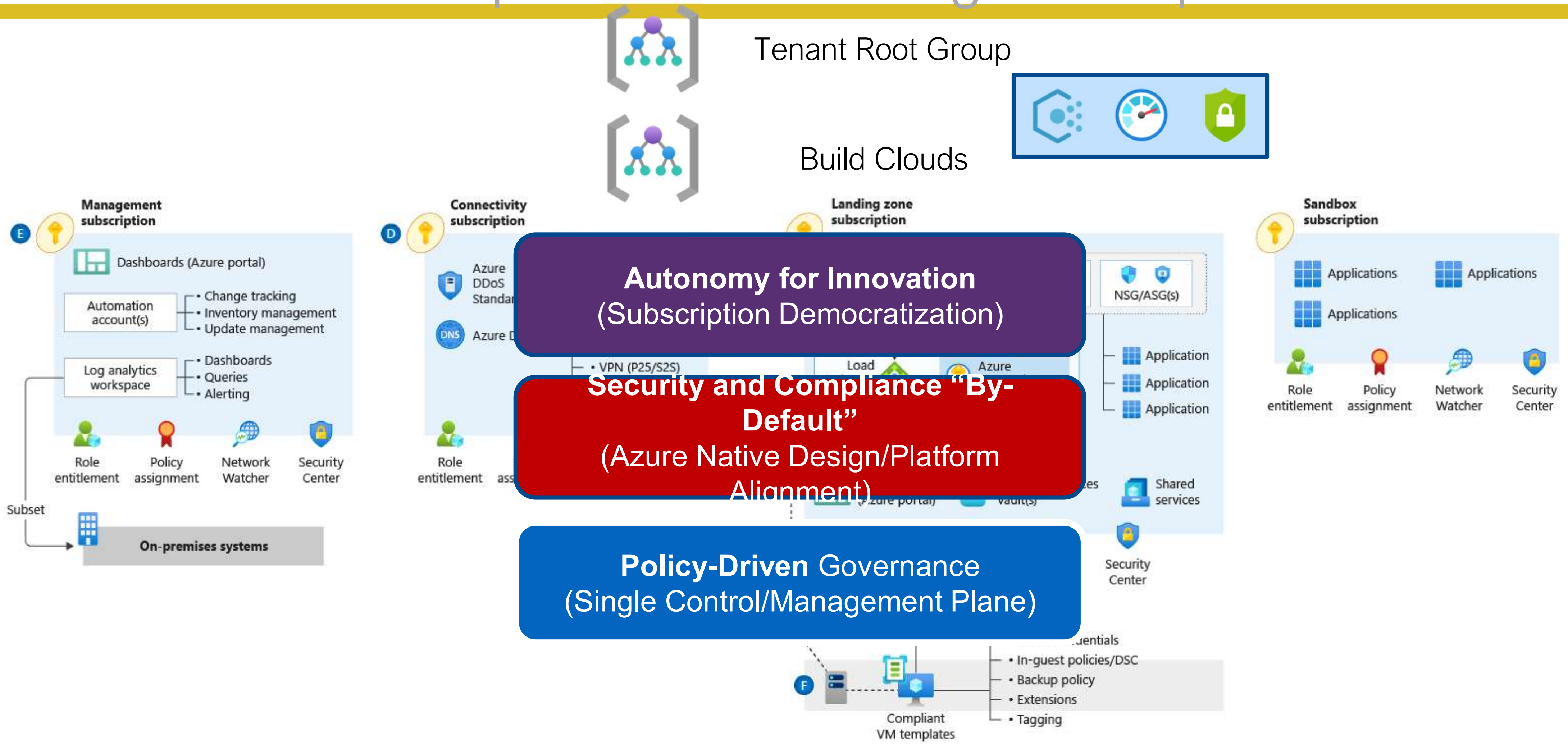
Methodology • Benchmark
initial best practice •
Governance maturity

Manage

Business commitments
operations baseline •
Ops maturity

https://azure.microsoft.com/en-us/cloud-adoption-framework/

Enterprise-Scale - Design Principles



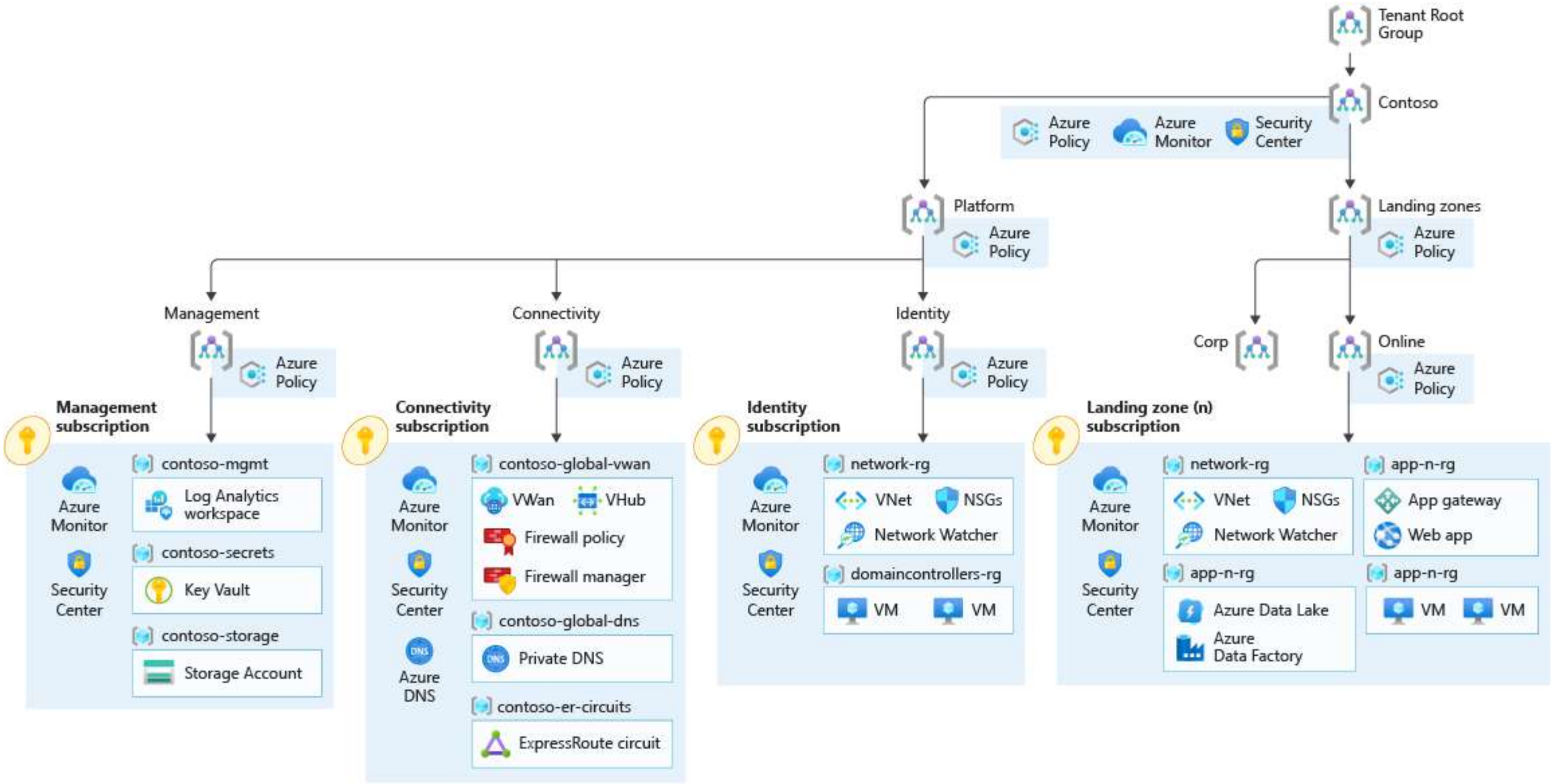
Autonomy for Innovation
(Subscription Democratization)

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

Policy-Driven Governance
(Single Control/Management Plane)

GitHub Enterprise Scale Templates

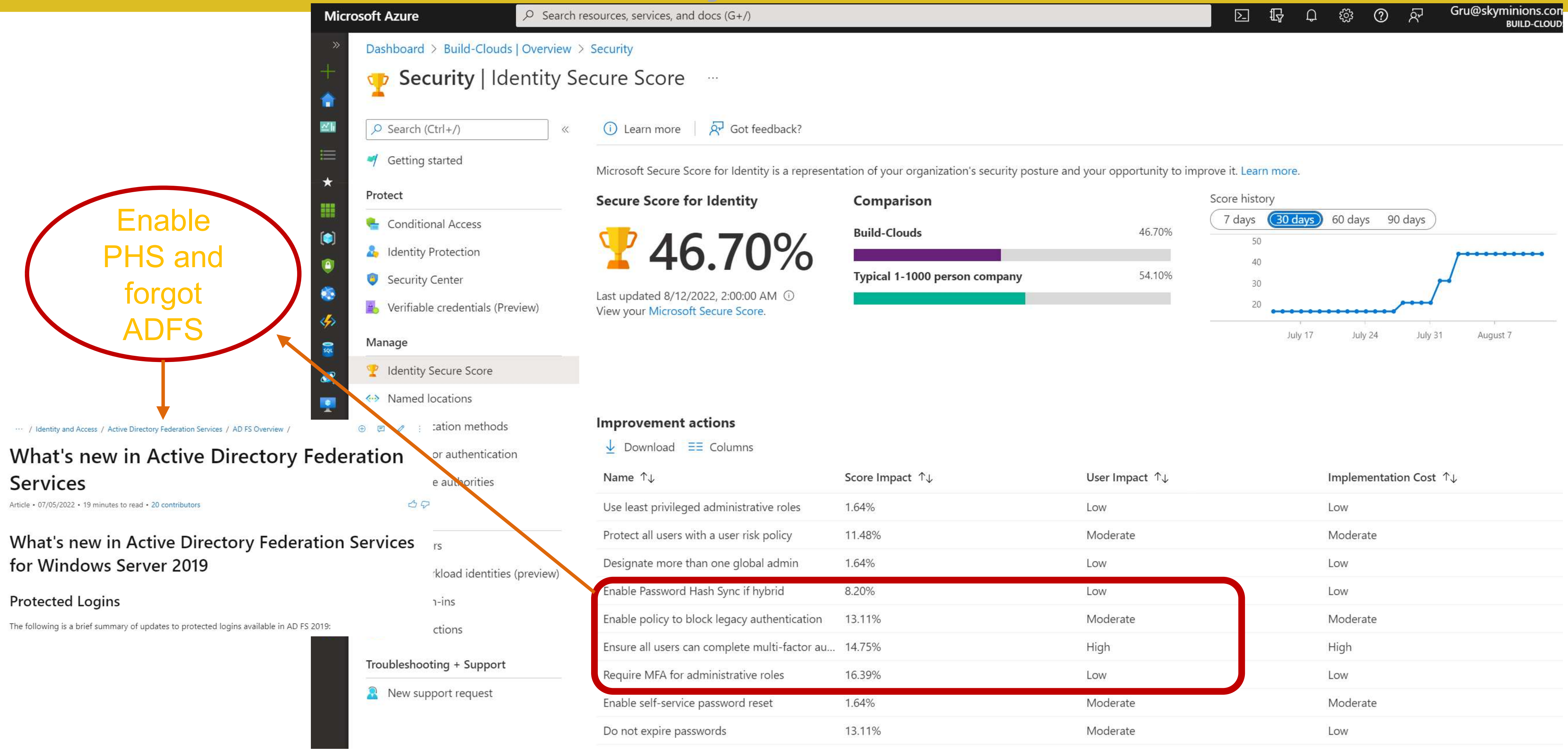
Deploy Enterprise-Scale with Azure VWAN



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

2. (Hybrid) Identity

Identity Secure Score



Security | Identity Secure Score

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%

Improvement actions

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

Enable PHS and forgot ADFS

··· / 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

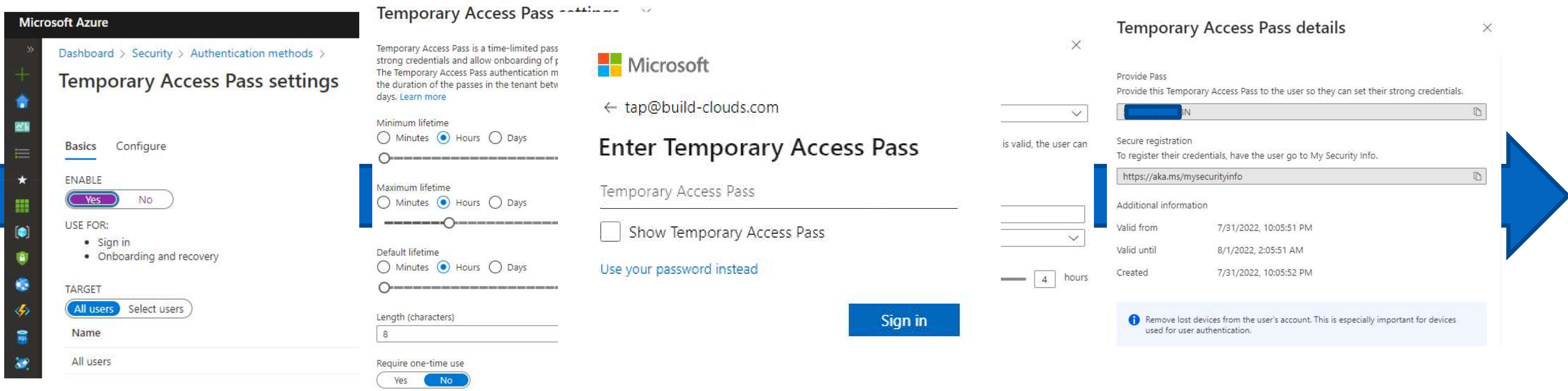
Protected Logins

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

@GregorReimling

#ITTage

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

Microsoft

← tap@build-clouds.com

Enter Temporary Access Pass

Temporary Access Pass

□ Show Temporary Access Pass

Use your password instead

Sign in

is valid, the user can

4 hours

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

@GregorReimling

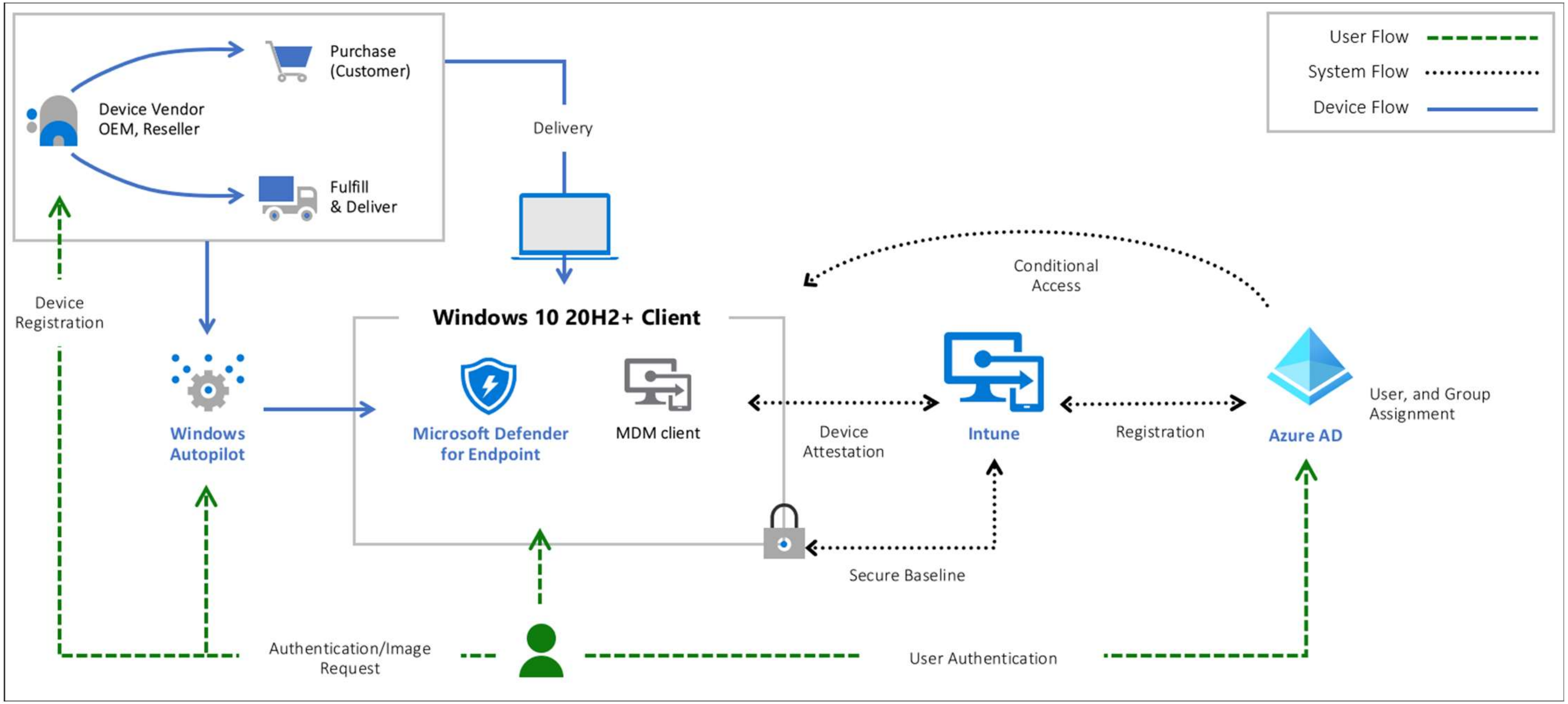
#ITTage

Identity Empfehlungen

- ✓ Einrichtung von Conditional Access
- ✓ Multifaktor Authentifizierung ist Pflicht
- ✓ Priviliged Identity Management aktivieren (P2)
- ✓ Mobile Worker mit Sign-In Risk Richtlinien zusätzlich absichern (P2)
- ✓ Temporary Access Pass für On-boarding neuer Mitarbeiter einrichten
- ✓ Geräterichtlinien ausrollen
- ✓ Administrative Tätigkeiten mit separatem Account und Geräteprüfung

4. PAW

Privileged Access Devices



Why are privileged access devices important | Microsoft Learn

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

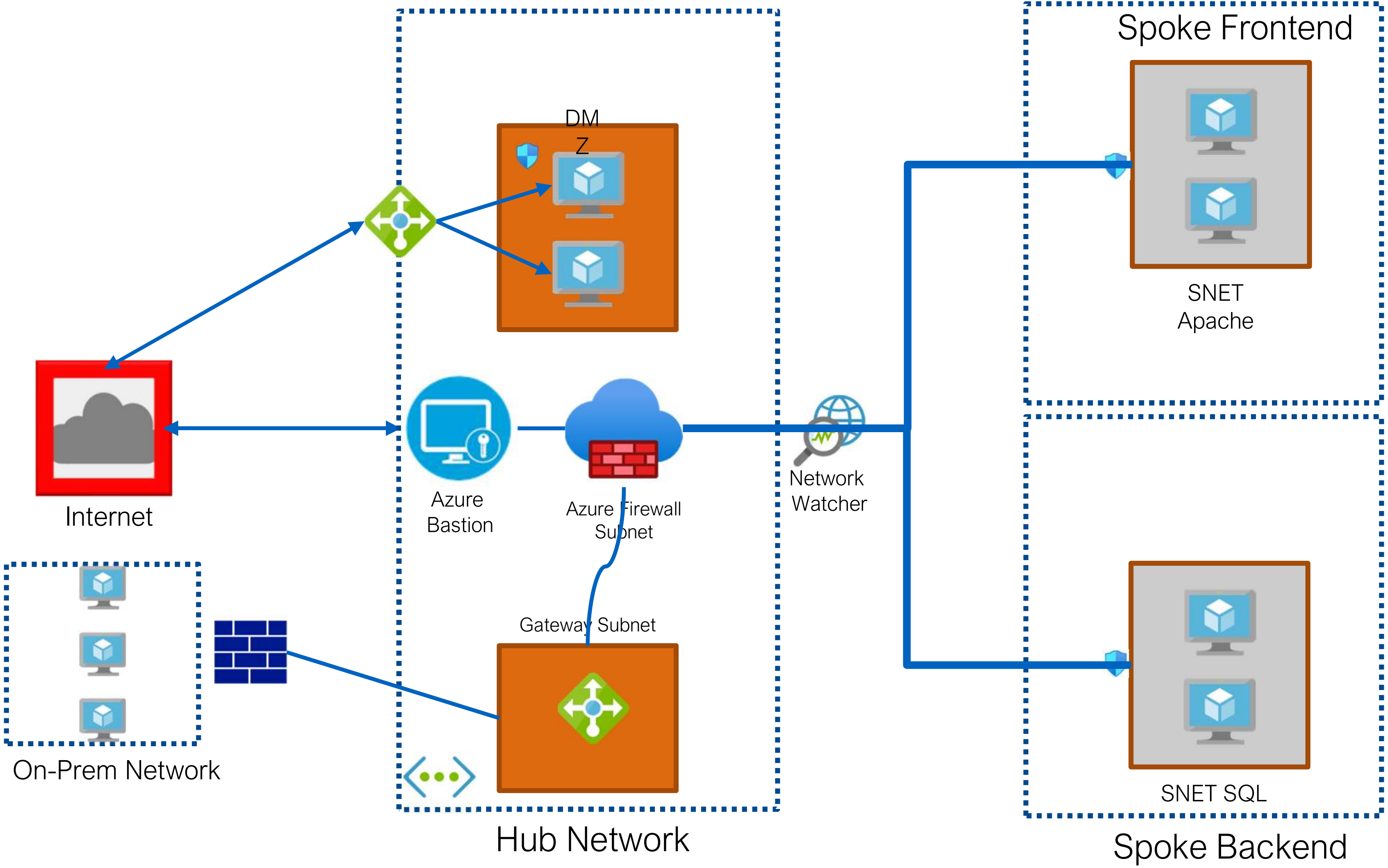
Use AVD as PAW solution

5. Network

@GregorReimling

#ITTage

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

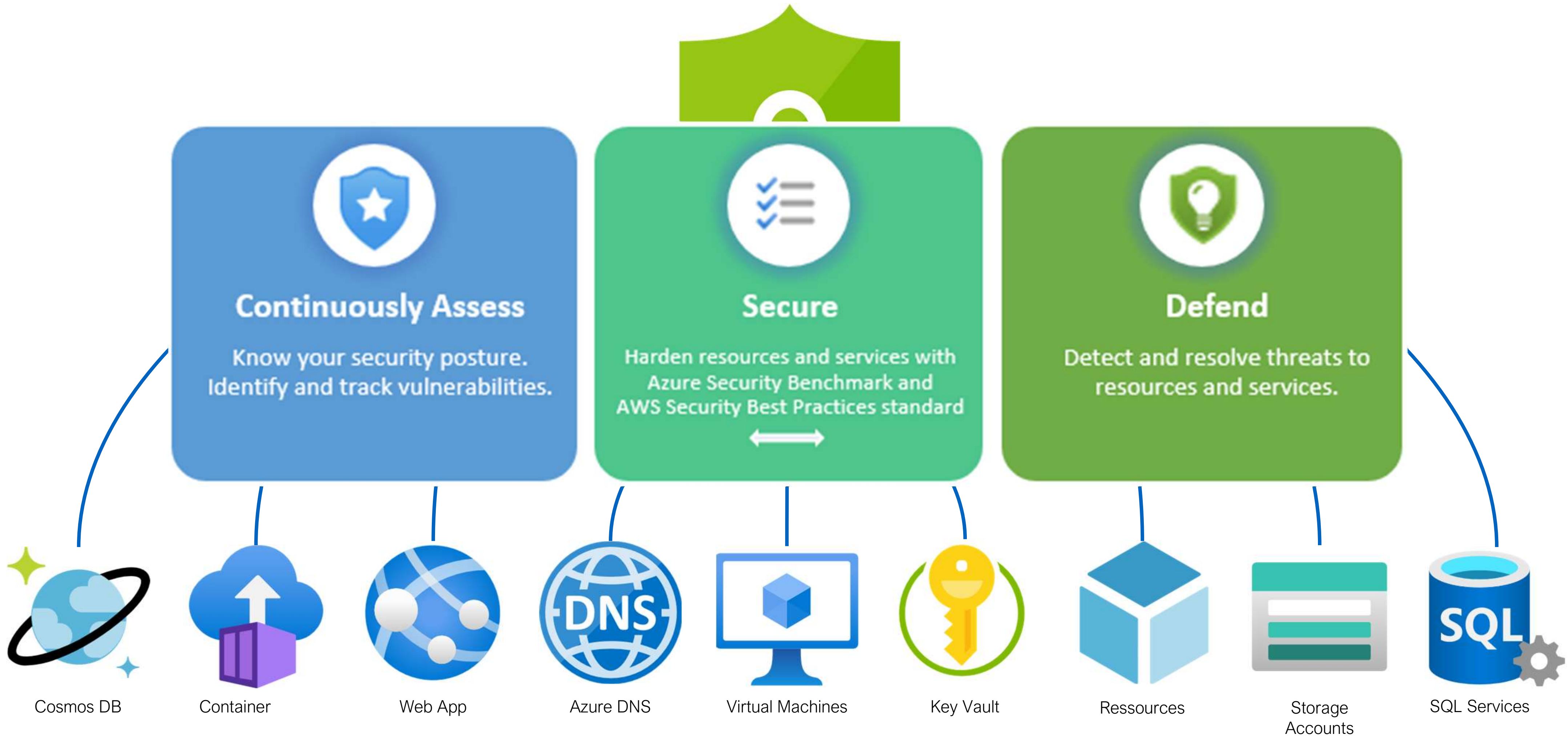
Azure Firewall Editions

New since 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 300€	901,24€ per month	1.262,29€ per month

6. MS Defender for Cloud

Microsoft Defender for Cloud



Continuously Assess

Know your security posture.
Identify and track vulnerabilities.

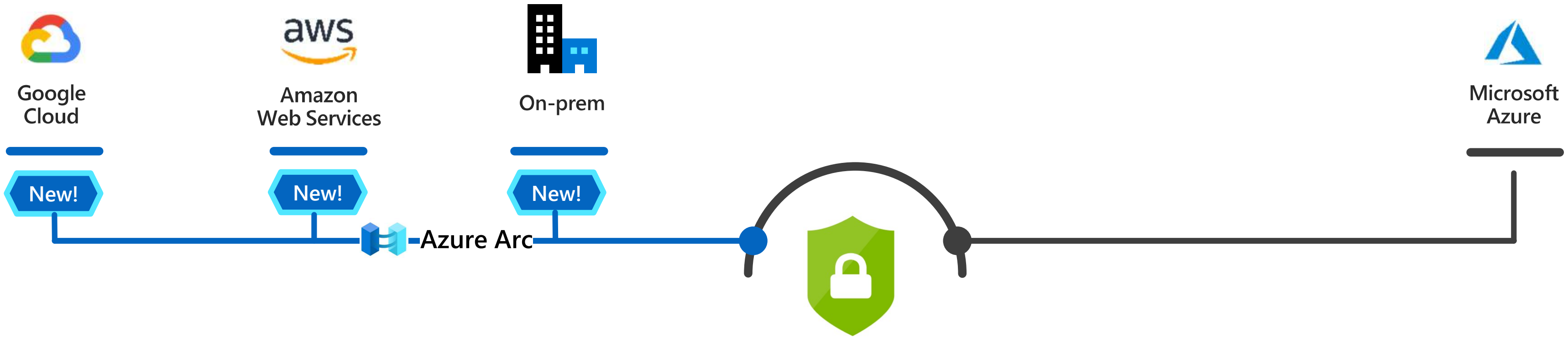
Secure

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

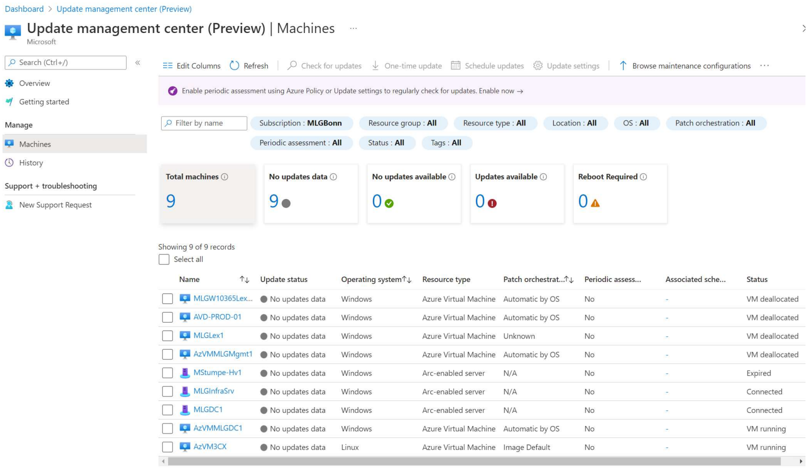
Defender for Servers Plans

	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 →

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

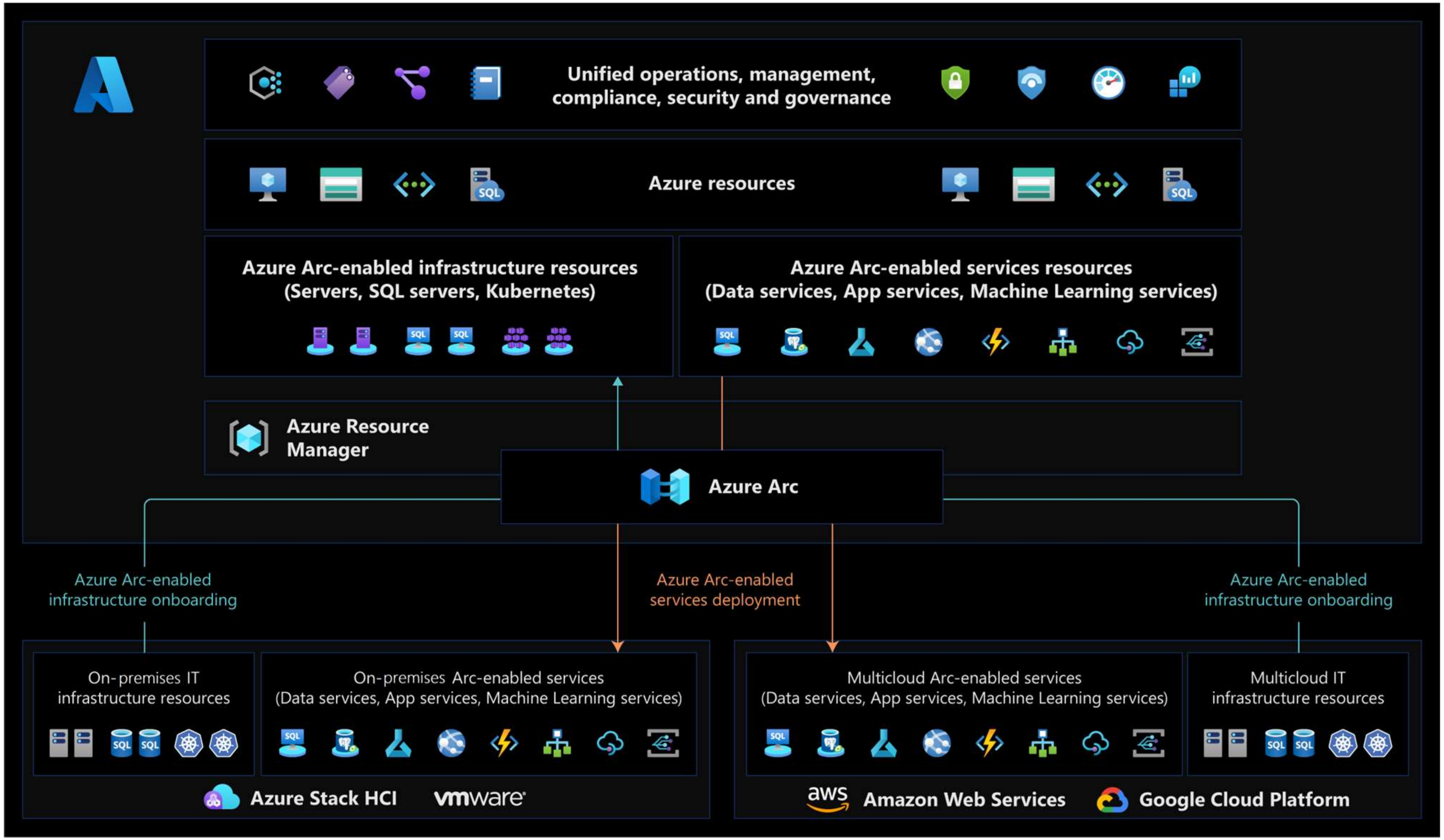
7. Microsoft Sentinel

8. Azure Arc

@GregorReimling

#ITTage

Azure Arc


Unified operations, management, compliance, security and governance
Azure resources
SQL
Azure Arc-enabled infrastructure resources (Servers, SQL servers, Kubernetes)
Azure Arc-enabled services resources (Data services, App services, Machine Learning services)
Azure Resource Manager
Azure Arc
Azure Arc-enabled infrastructure onboarding
Azure Arc-enabled services deployment
Azure Arc-enabled infrastructure onboarding
On-premises IT infrastructure resources
On-premises Arc-enabled services (Data services, App services, Machine Learning services)
Multicloud Arc-enabled services (Data services, App services, Machine Learning services)
Multicloud IT infrastructure resources
Azure Stack HCI
vmware
aws Amazon Web Services
Google Cloud Platform

Azure Arc: *at a high level*

Bring Azure services and management to any infrastructure, anywhere

Run Azure data services anywhere

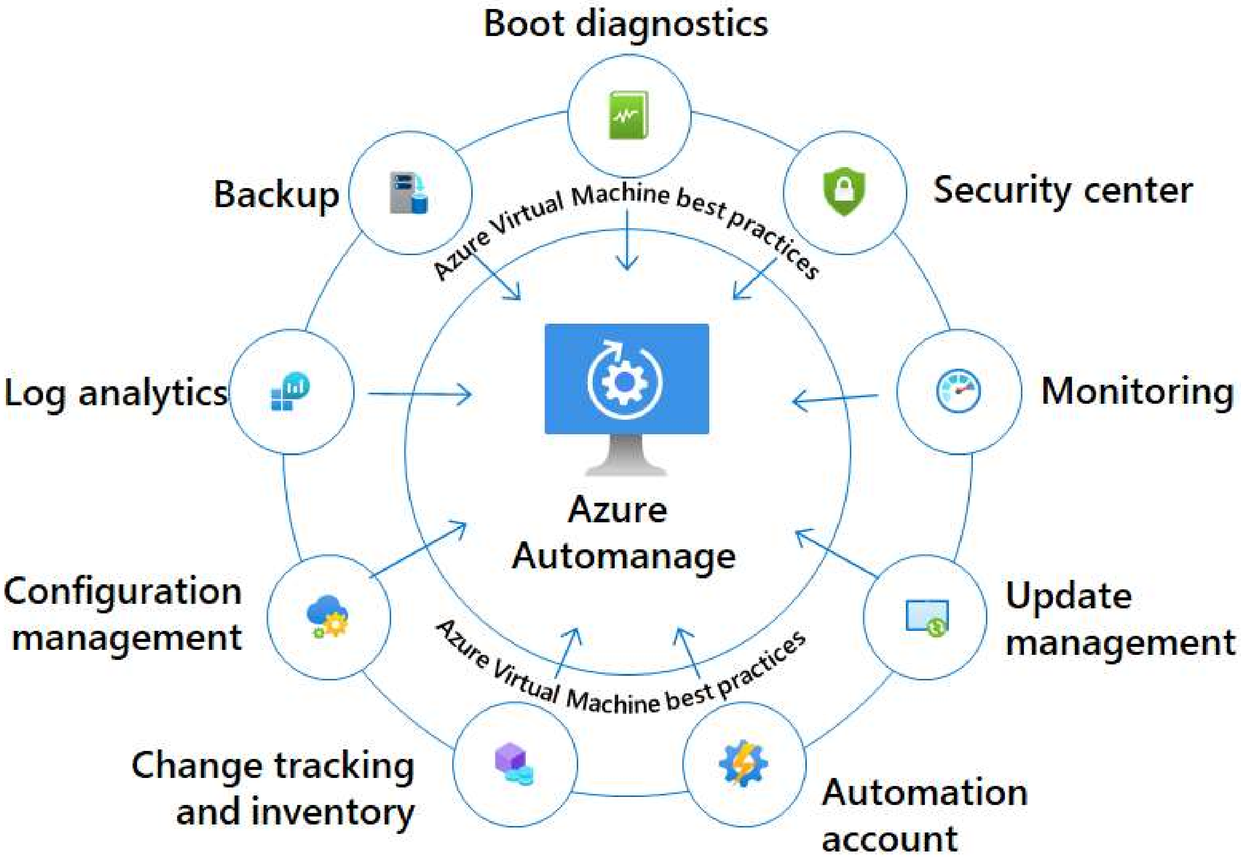
Extend Azure management across your environments

Adopt cloud practices on-premises

Implement Azure security anywhere

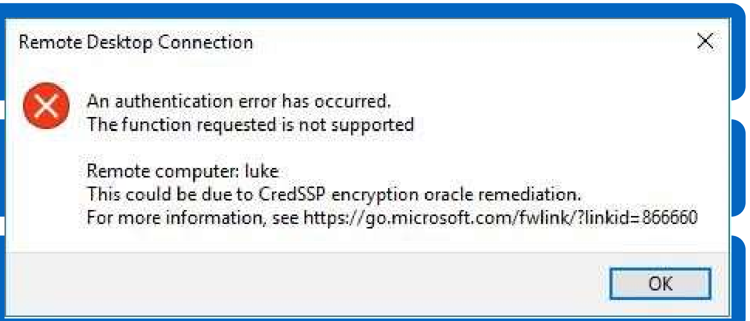
Azure Arc is a set of technologies that extends Azure management and enables Azure services to run across on-premises, multi-cloud, and edge

Azure Automanage



Update Management Center (preview)

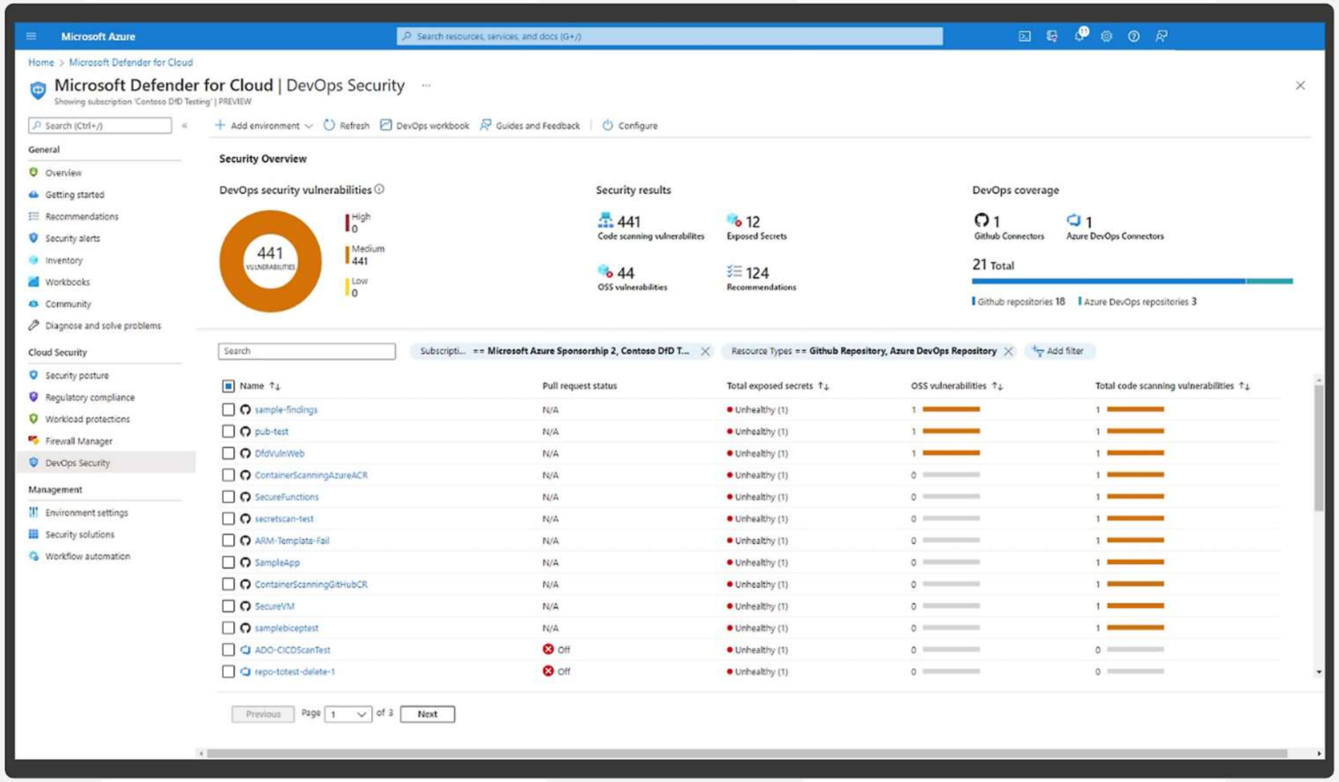
- New solution for centrally Update Management accross different environments
- No dependencys to Log Analytics Agent
- Fully support for Azure Arc managed VMs
- Support Windows and Linux Vms
- Support automatic VM guest patching
- Support Hot patching
- Is in preview wait for production until release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


Remote Desktop Connection

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

Defender for DevOps



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

441 Code scanning vulnerabilites

12 Exposed Secrets

44 OSS vulnerabilities

124 Recommendations

DevOps coverage

1 Github Connectors

1 Azure DevOps Connectors

21 Total

Github repositories 18

Azure DevOps repositories 3

Subscripti... == Microsoft Azure Sponsorship 2, Contoso DfD T...

Resource Types == Github Repository, Azure DevOps Repository

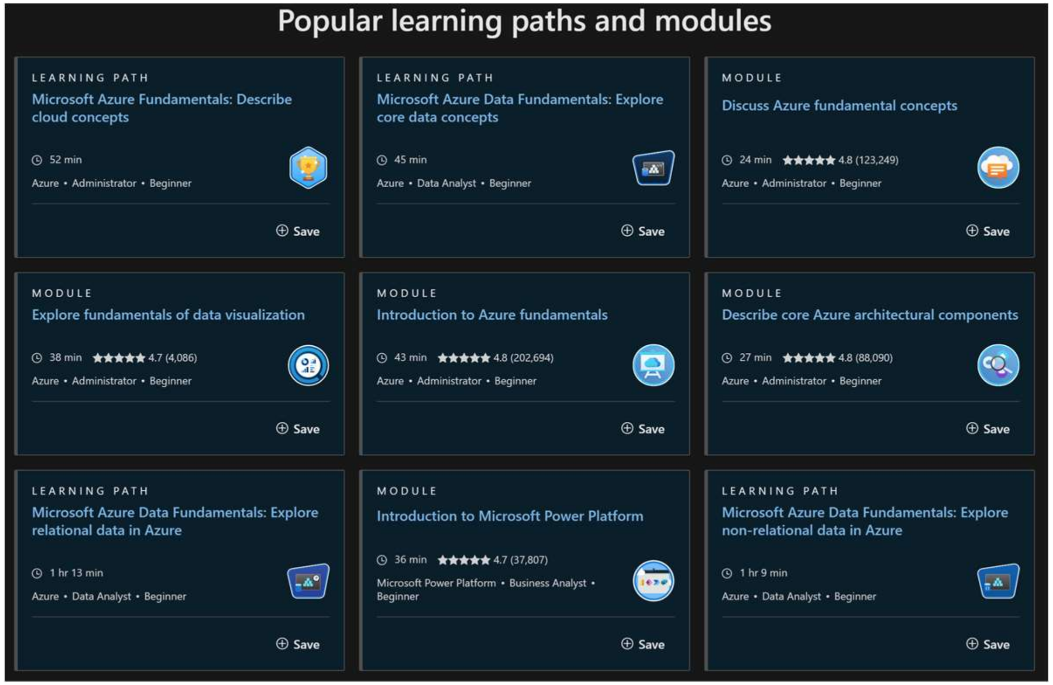
Name ↑↓	Pull request status	Total exposed secrets ↑↓	OSS vulnerabilities ↑↓	Total code scanning vulnerabilities ↑↓
□ sample-findings	N/A	● Unhealthy (1)	1	1
□ pub-test	N/A	● Unhealthy (1)	1	1
□ DfdVulnWeb	N/A	● Unhealthy (1)	1	1
□ ContainerScanningAzureACR	N/A	● Unhealthy (1)	0	1
□ SecureFunctions	N/A	● 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

Page 1 of 3

Join Our Security Community - Microsoft Community Hub

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

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
5. Enable Defender for Cloud for (Productive) workloads

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