www.wpninjas.eu

Top 10 Azure Security Best Practices

By Gregor Reimling

Workplace Ninja Summit 2022

www.wpninjas.eu
#WPNinjaS

Platinum Sponsor

PATCH MY PC

Microsoft Security

Gold Sponsor

glueckkanja gab

LIQUIT

baseVISION
SECURE & MODERN WORKPLACE

Lenovo

RECAST SOFTWARE

Snapdragon

Silver and Special Sponsors

SD:>_
SwissDev Jobs

LUZERN
DIE STADT. DER SEE. DIE BERGE.

sepago®

EPIC FUSION

SCAPPMAN

AppManagEvent.com
2022
October 7
NETHERLANDS

dinext.

About “Gregor Reimling”

Azure Meetup
BONN
www.azurebonn.de

Focus

Azure Governance, Security and IaaS

Certifications

Cybersecurity Architect, MVP for MS Azure

From

Cologne, Germany

Hobbies

Family, Community, Worldtraveler

My Blog

https://www.Reimling.eu

Contact

@GregorReimling

@CloudInspires

www.cloudinspires.me

Agenda

Key takeaways:

- Overview of important Security settings
- Recommendation for higher security with simple steps
- Knowledge about the important settings

Harden Identities

Azure AD Recommendations

Harden Azure Tenant

CAF, Enterprise Scale and Advisor Recommendations

Harden Azure with Defender for Cloud

Defender for Cloud

Harden Azure with Policy

Recommendations for Minimum Azure Policy Settings

Harden Azure Network Layer

Recommendations for Azure Network and Firewall

Azure AD Hardening

Identity Attacks rising

300% increase in identity attacks over the past year.

Breach Replay

Password Spray

Phishing

562K high-risk enterprise sign-in attempts flagged in **January 2019**

158K compromised accounts detected in **January 2019**

4.8B attacker-driven sign-ins detected in **January 2019**

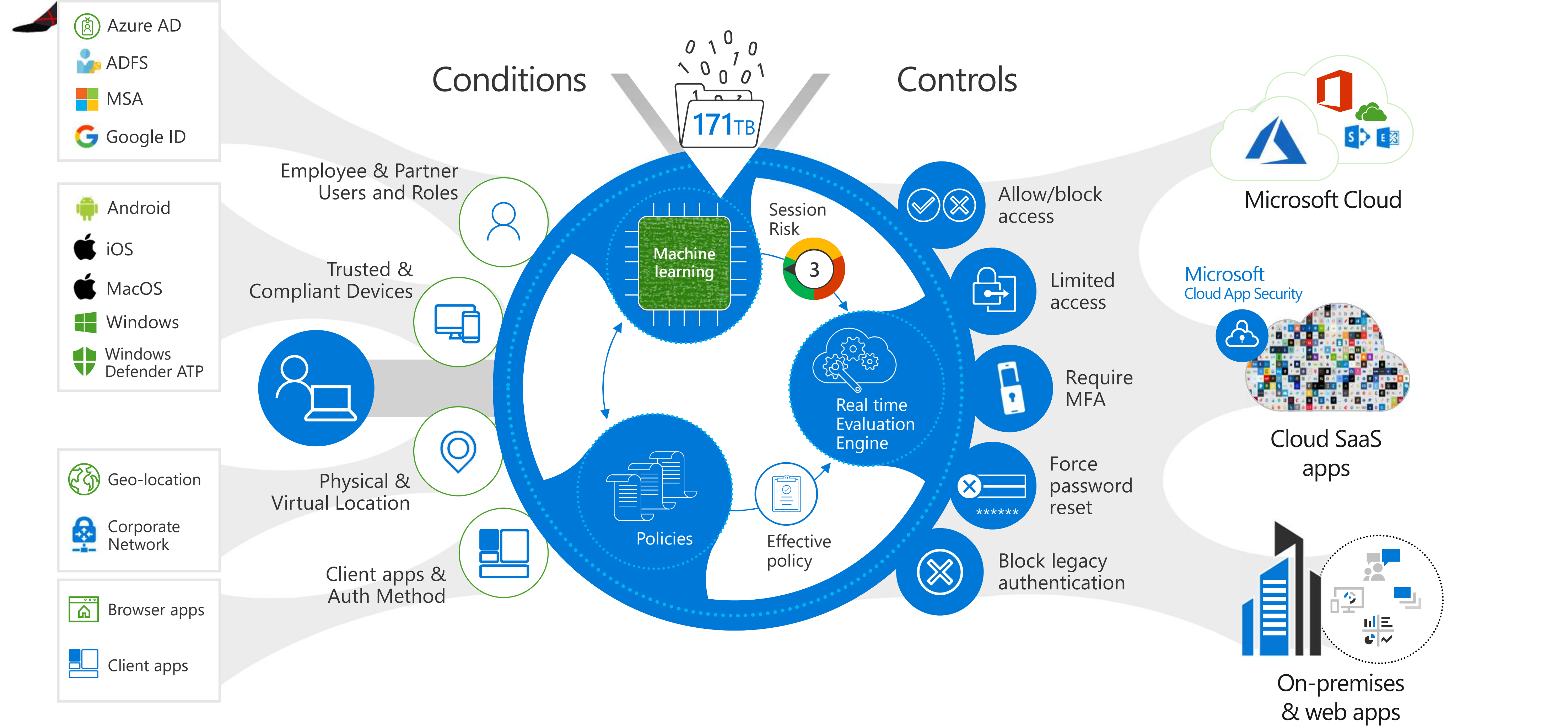
81% verizon

Verizon 2017 Data Breach Investigation Report

of hacking breaches leverage stolen or weak passwords

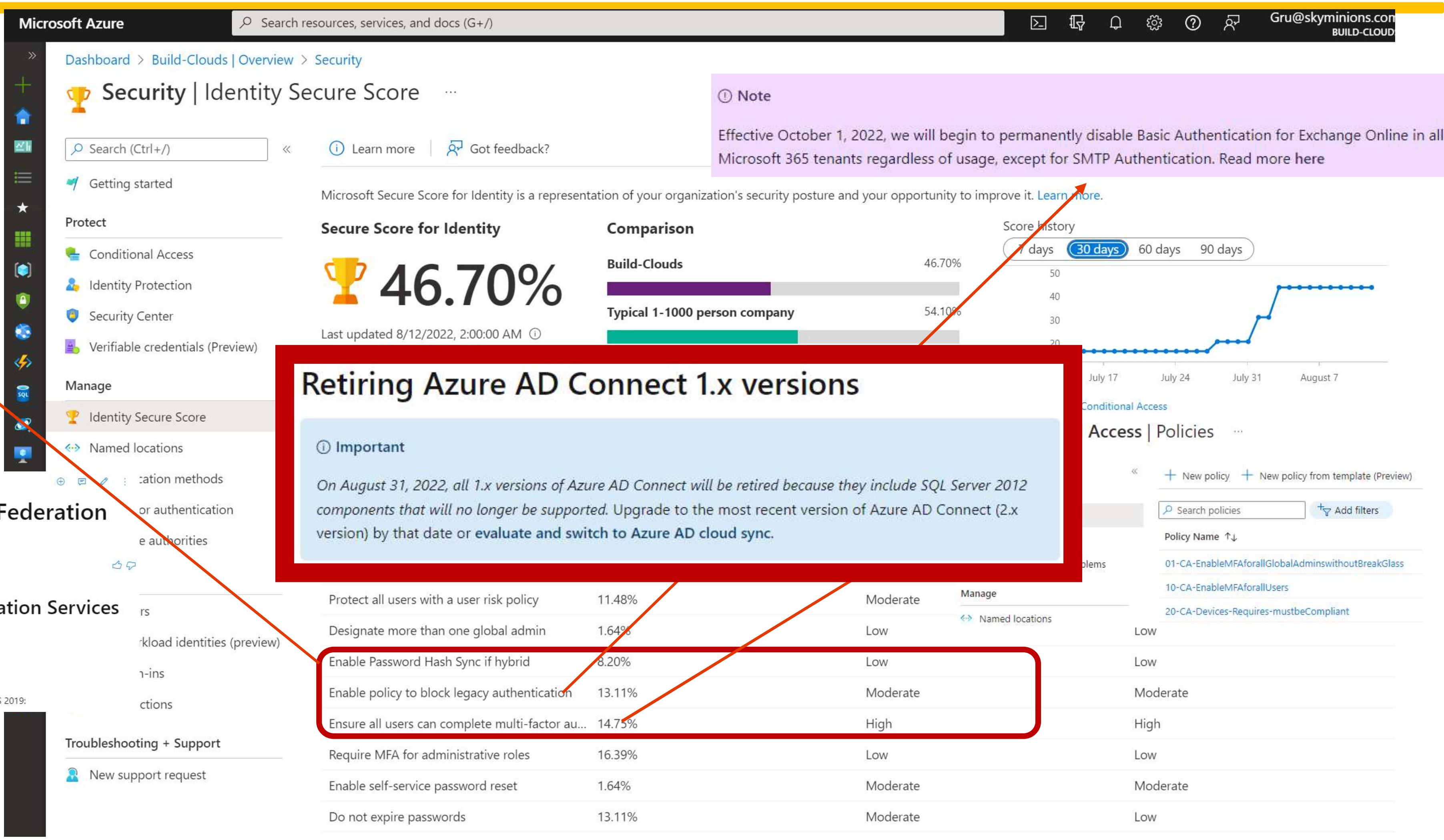
Identity Protection with Conditional Access

www.wpninjas.eu



Identity Secure Score

www.wpninjas.eu



Dashboard > Build-Clouds | Overview > Security

Security | Identity Secure Score

ⓘ 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

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

Comparison

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

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.**

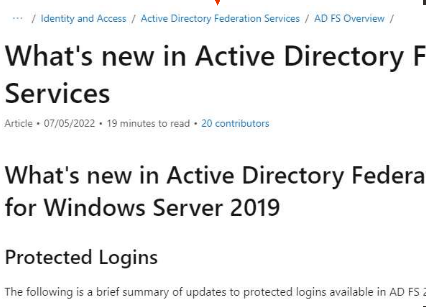
Protect all users with a user risk policy	11.48%	Moderate	
Designate more than one global admin	1.64%	Low	Low
Enable Password Hash Sync if hybrid	8.20%	Low	Low
Enable policy to block legacy authentication	13.11%	Moderate	Moderate
Ensure all users can complete multi-factor au...	14.75%	High	High
Require 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

Conditional Access

Access | Policies

Policy Name ↑↓
01-CA-EnableMFAforallGlobalAdminswithoutBreakGlass
10-CA-EnableMFAforallUsers
20-CA-Devices-Requires-mustbeCompliant

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

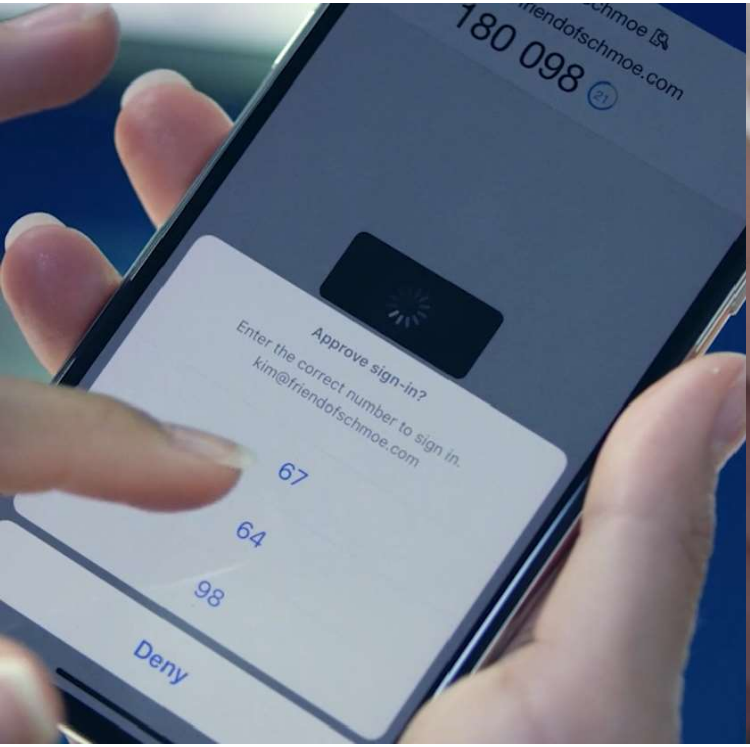
Protected Logins

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

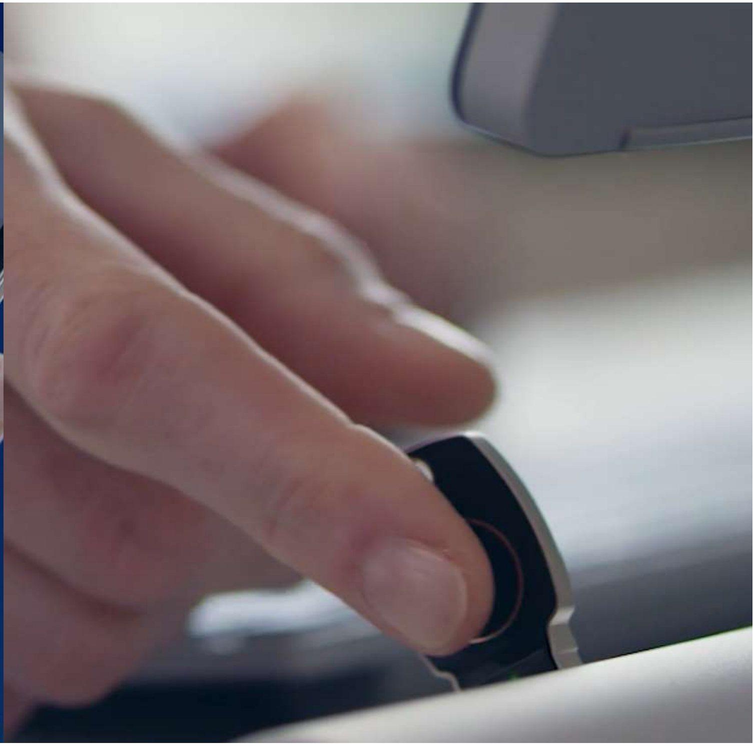
Passwordless Options

Windows Hello
for Business

Microsoft
Authenticator



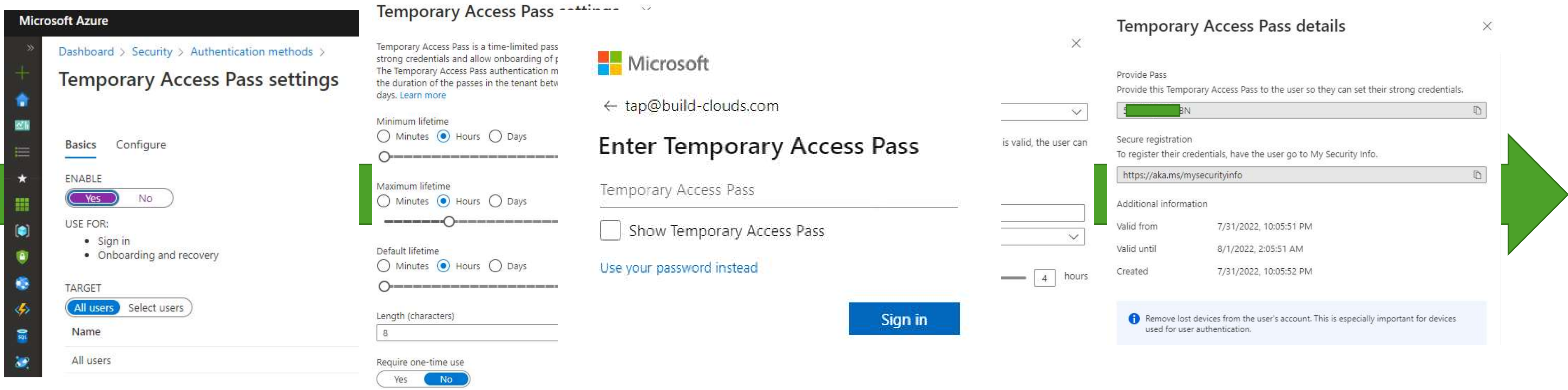
FIDO2
Security Keys



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

Temporary Access Pass

www.wpninjas.eu



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.

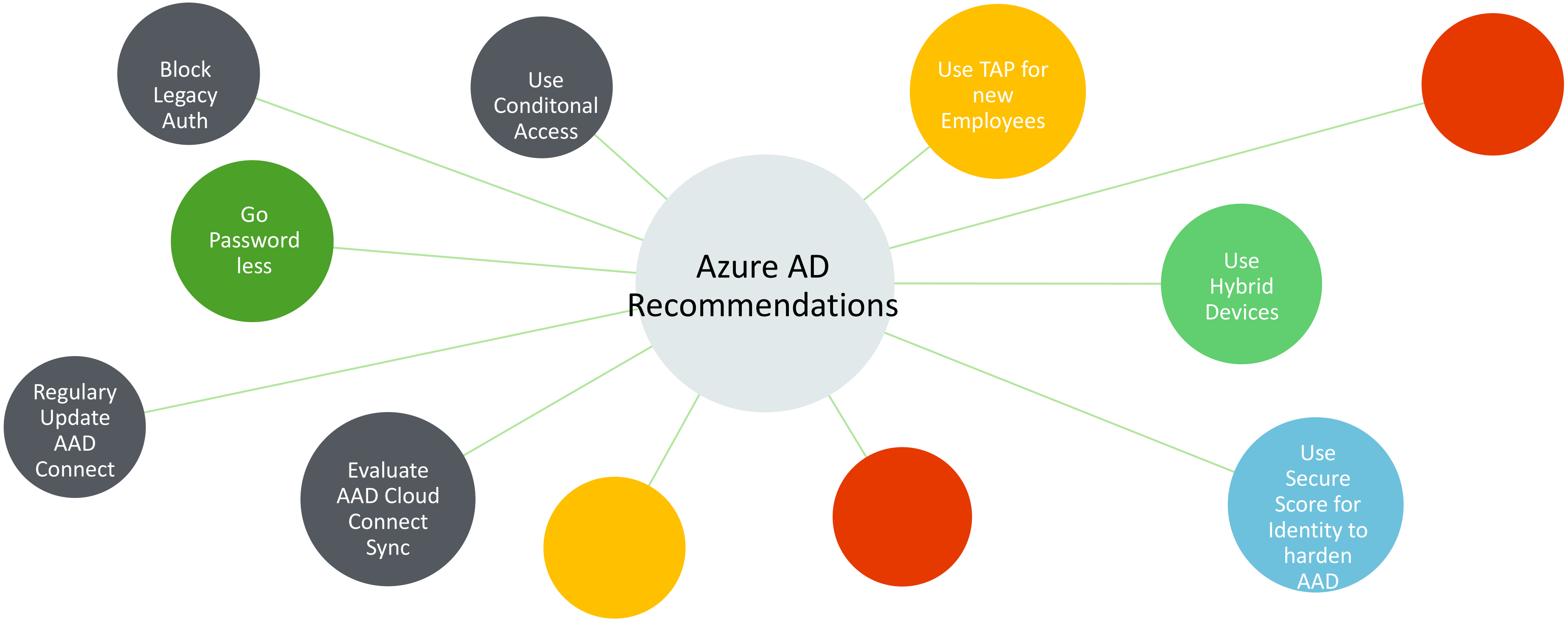
https://aka.ms/mysecurityinfo

Show following settings

- Identity Secure Score
- Conditional Access rules
- Temporary Access Pass

Azure AD Recommendations

www.wpninjas.eu

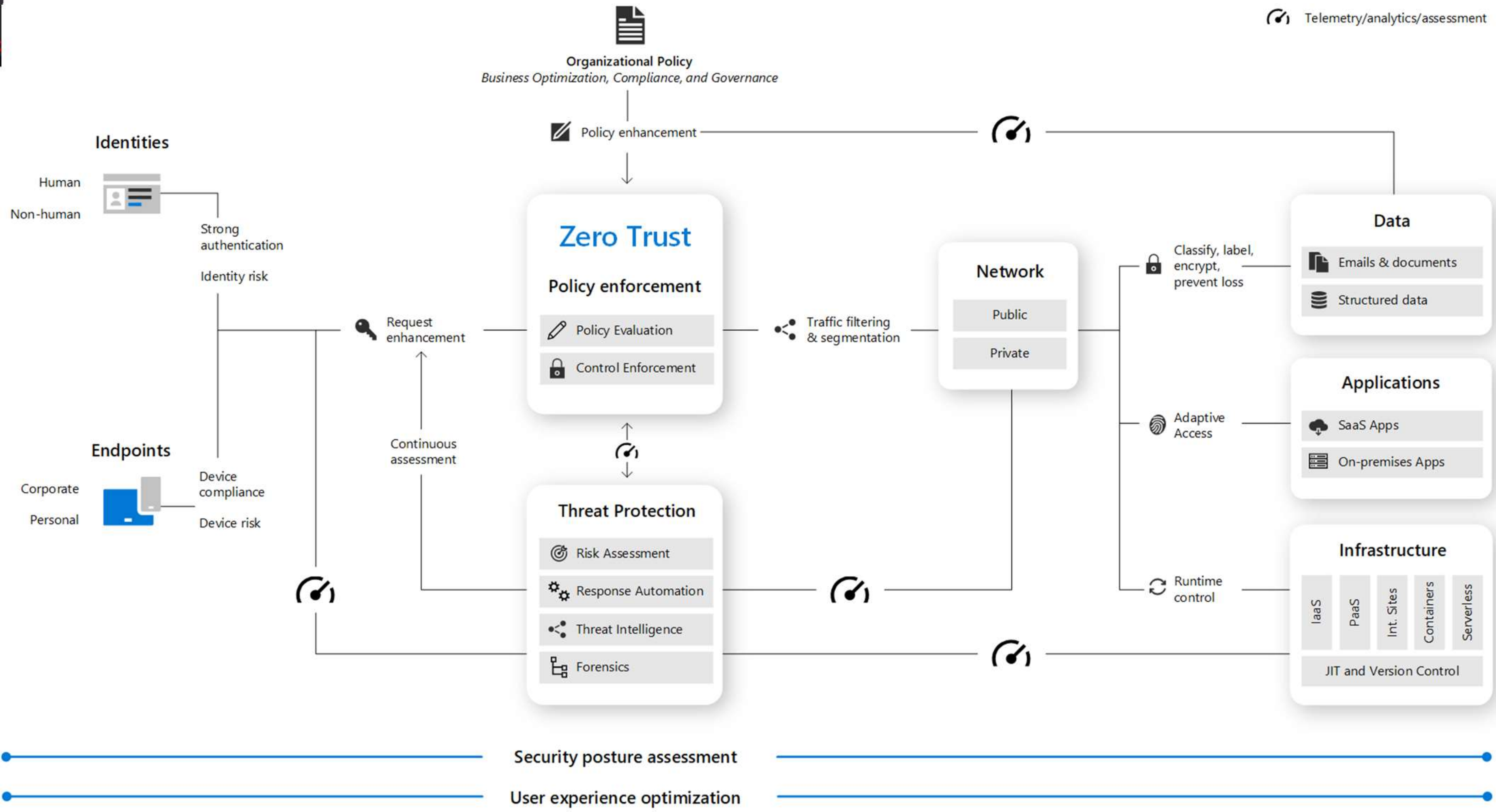


Azure AD Recommendations
Block Legacy Auth
Use Conditonal Access
Use TAP for new Employees
Go Password less
Use Hybrid Devices
Regulary Update AAD Connect
Evaluate AAD Cloud Connect Sync
Use Secure Score for Identity to harden AAD

Azure Tenant Hardening

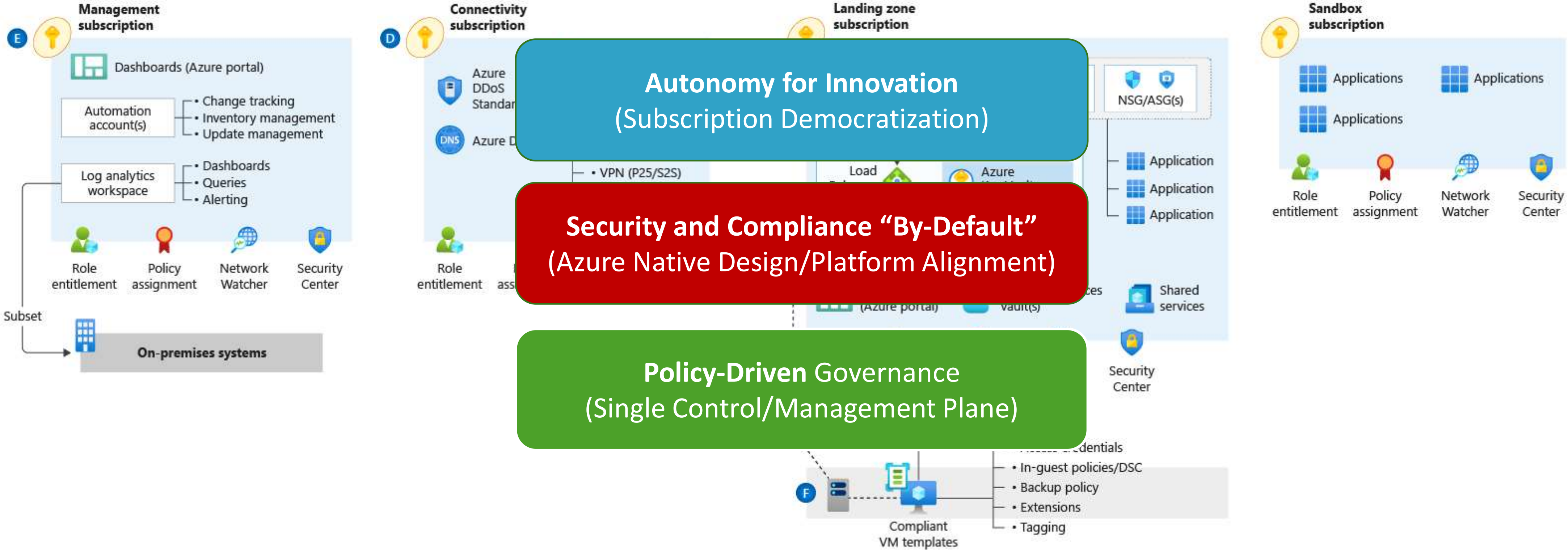
Zero Trust architecture

www.wpninjas.eu



Enterprise-Scale - Design Principles

www.wpninjas.eu



Autonomy for Innovation
(Subscription Democratization)

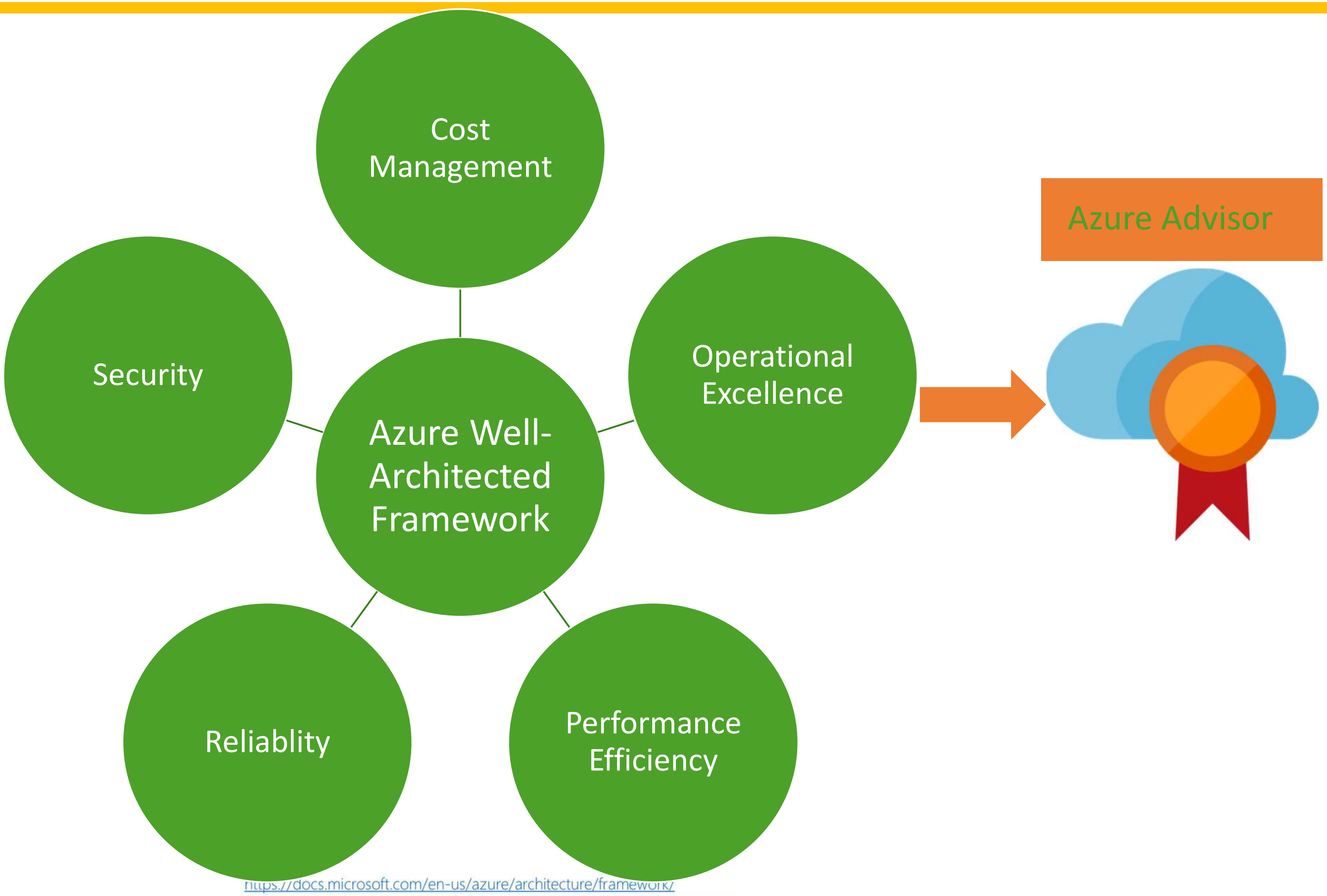
Security and Compliance “By-Default”
(Azure Native Design/Platform Alignment)

Policy-Driven Governance
(Single Control/Management Plane)

Well-architected Framework

www.wpninjas.eu

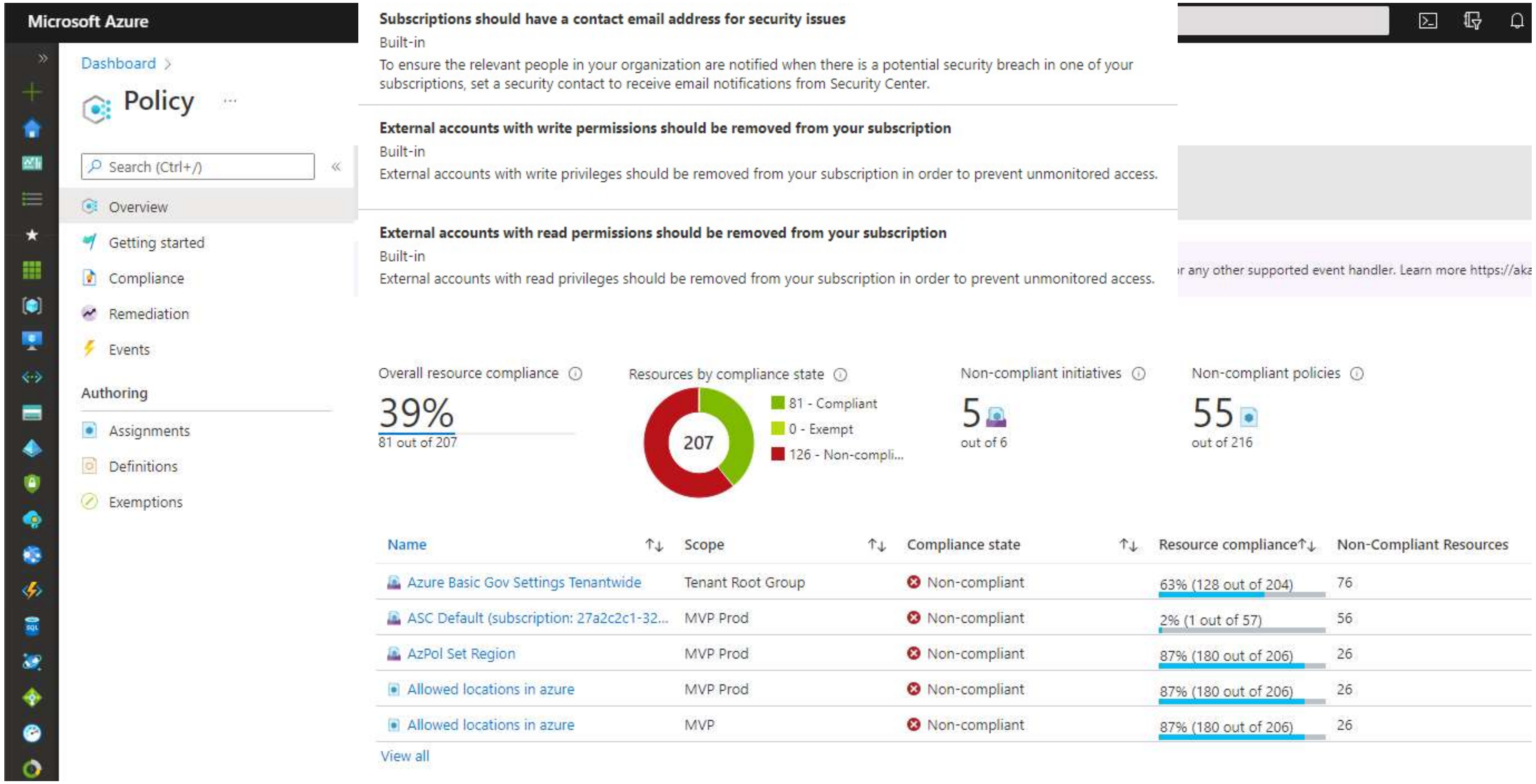
"The Azure Well-Architected Framework is a set of guiding tenets that can be used to improve the quality of a workload."



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

Azure Policy

www.wpninjas.eu



Subscriptions should have a contact email address for security issues

Built-in

To ensure the relevant people in your organization are notified when there is a potential security breach in one of your subscriptions, set a security contact to receive email notifications from Security Center.

External accounts with write permissions should be removed from your subscription

Built-in

External accounts with write privileges should be removed from your subscription in order to prevent unmonitored access.

External accounts with read permissions should be removed from your subscription

Built-in

External accounts with read privileges should be removed from your subscription in order to prevent unmonitored access.

r any other supported event handler. Learn more https://aka

Overall resource compliance ⓘ

39%

81 out of 207

Resources by compliance state ⓘ

207

🟩 81 - Compliant

🟩 0 - Exempt

🟥 126 - Non-compli...

Non-compliant initiatives ⓘ

5

out of 6

Non-compliant policies ⓘ

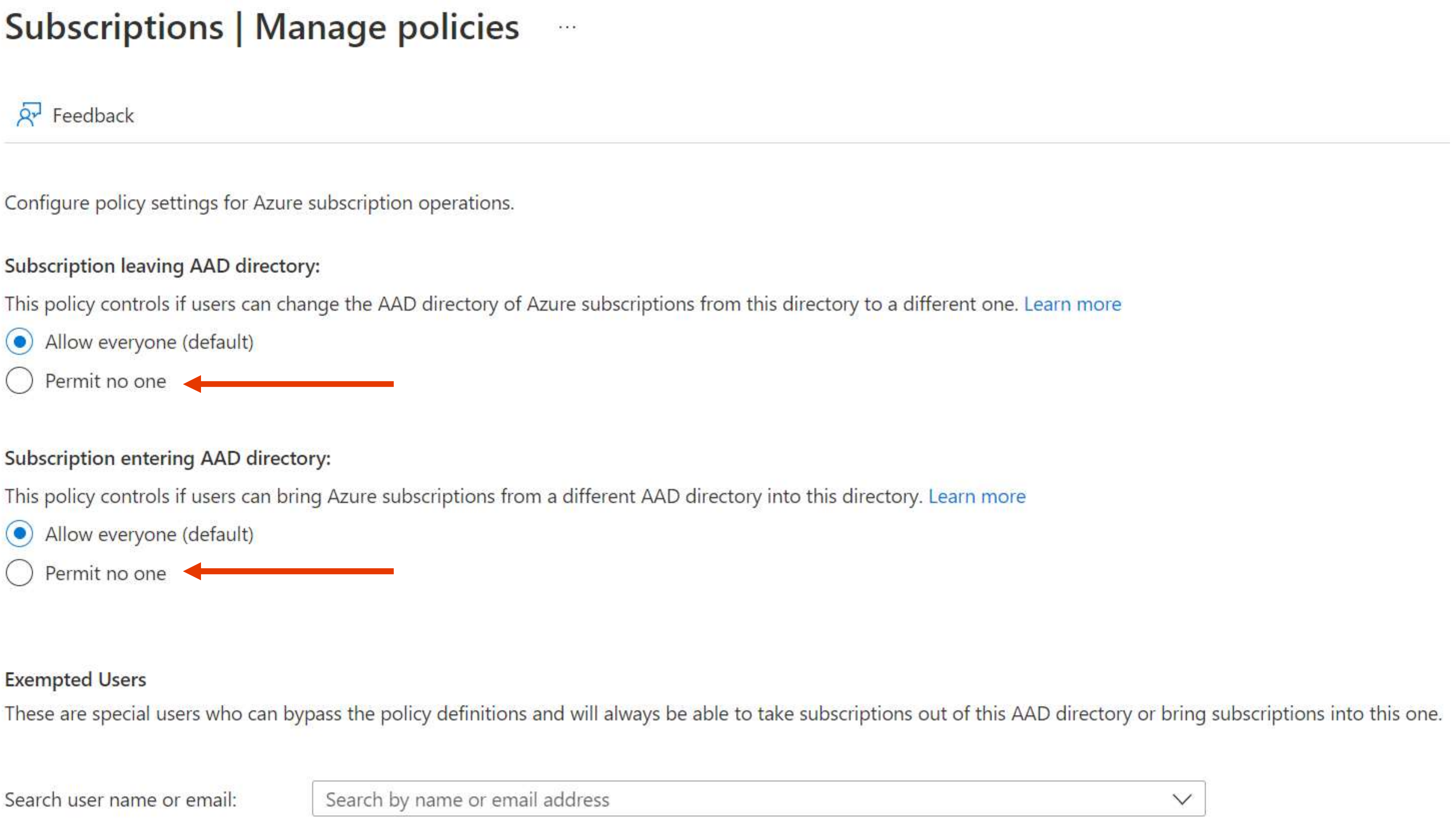
55

out of 216

Name ↑↓	Scope ↑↓	Compliance state ↑↓	Resource compliance↑↓	Non-Compliant Resources
Azure Basic Gov Settings Tenantwide	Tenant Root Group	⊗ Non-compliant	63% (128 out of 204)	76
ASC Default (subscription: 27a2c2c1-32...	MVP Prod	⊗ Non-compliant	2% (1 out of 57)	56
AzPol Set Region	MVP Prod	⊗ Non-compliant	87% (180 out of 206)	26
Allowed locations in azure	MVP Prod	⊗ Non-compliant	87% (180 out of 206)	26
Allowed locations in azure	MVP	⊗ Non-compliant	87% (180 out of 206)	26

View all

Manage Subscription Policies



Subscriptions | Manage policies

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

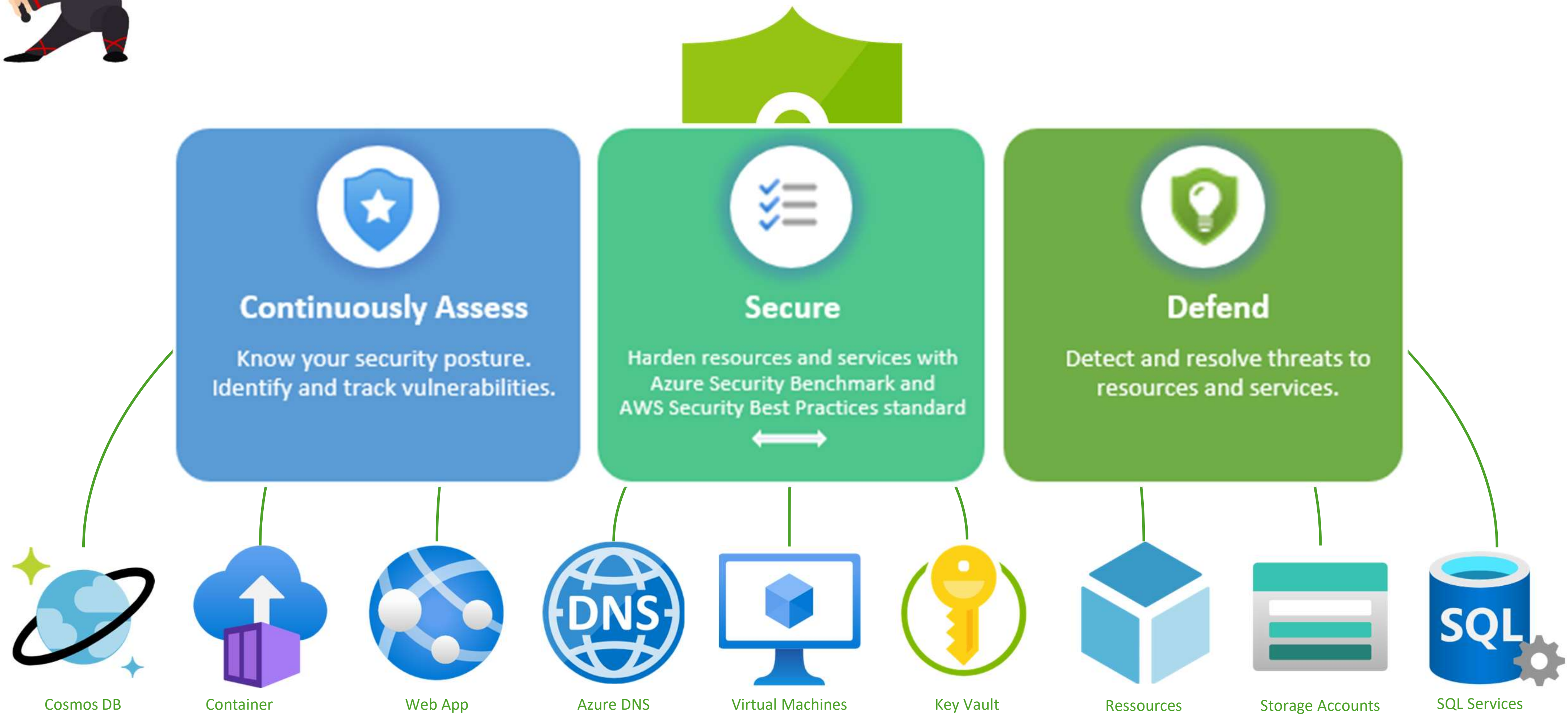
Demo

Dive into the Azure Portal

- Azure Advisor
- Azure Policy

Microsoft Defender for Cloud

Microsoft Defender for Cloud



Continuously Assess

Know your security posture.
Identify and track vulnerabilities.

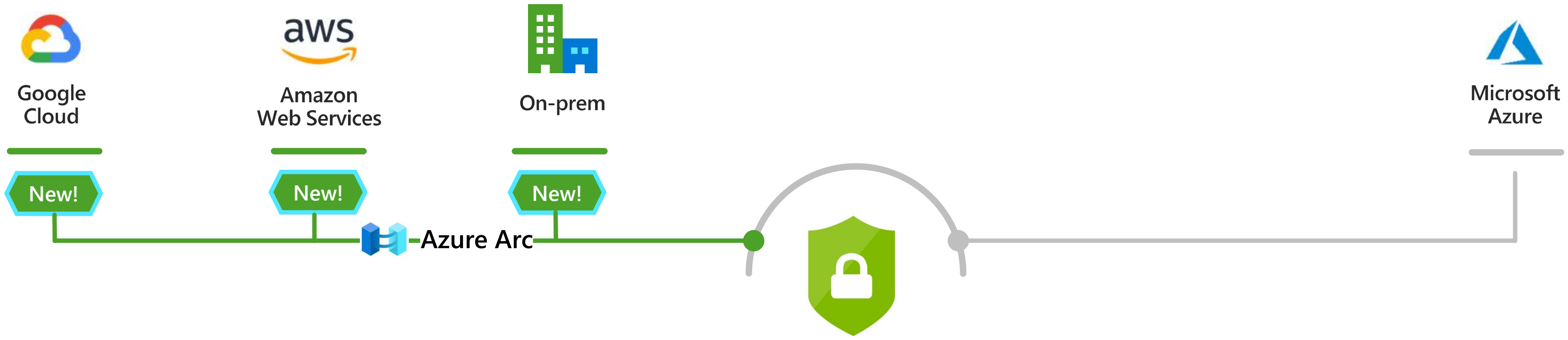
Secure

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

Demo

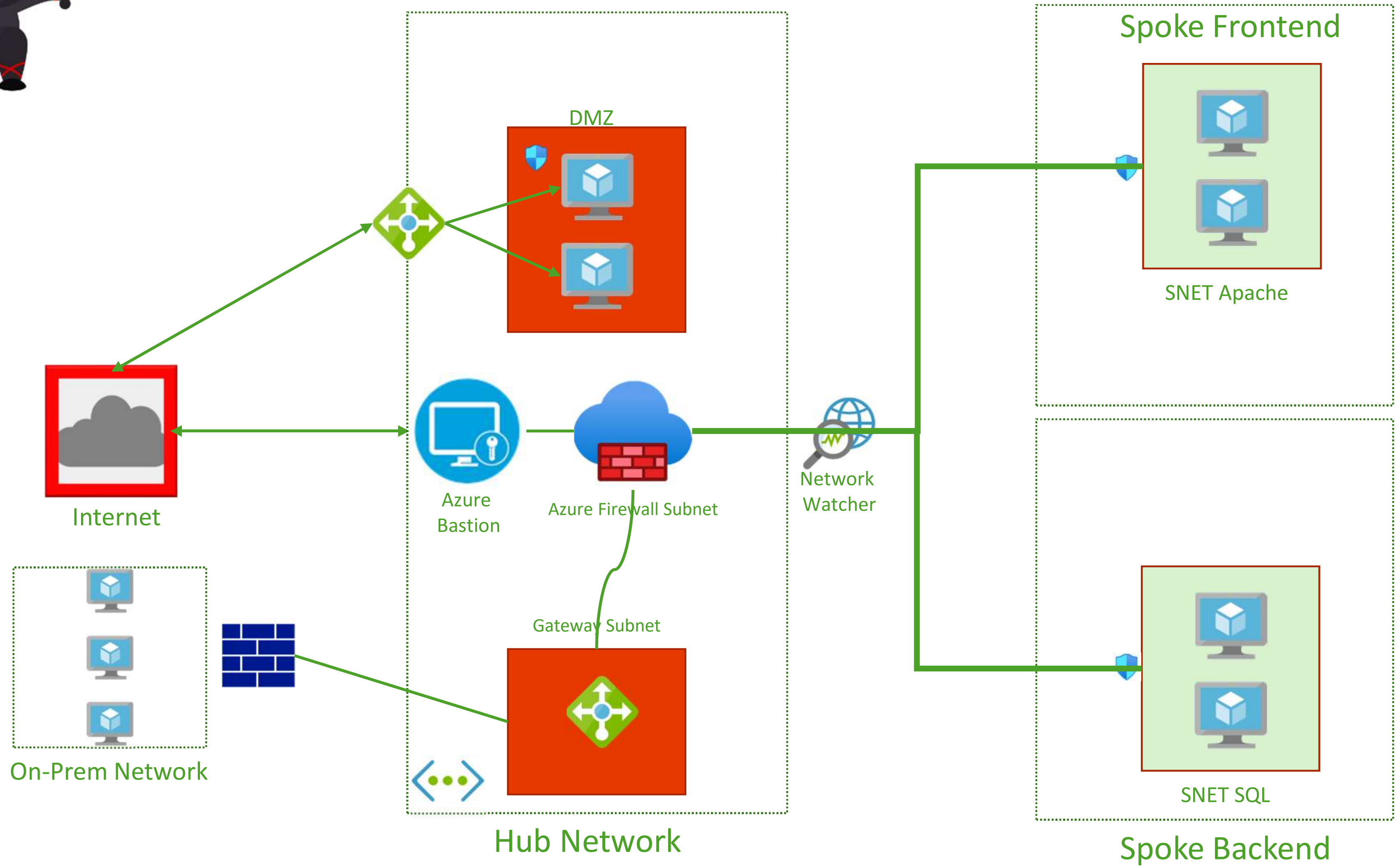
Dive into the Azure Portal

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

Azure Network Hardening

Network Protection

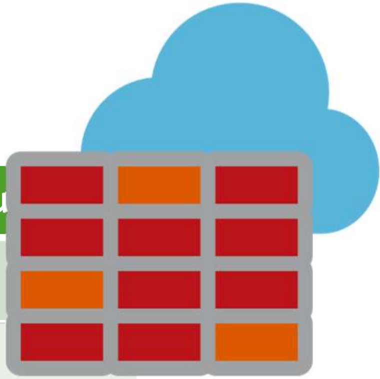
www.wpninjas.eu



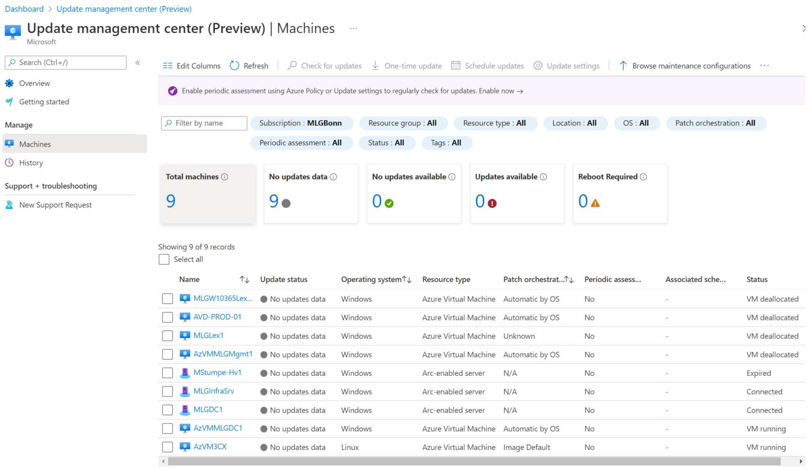
Azure IaaS Recommendations

- 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



Azure Firewall Standard	Azure Firewall Premiu
Built-in high availability	All from Standard +
Availability Zones	TLS Inspection
Application FQDN Filtering Rules	IDPS
Unrestricted Cloud Scalability	URL Filtering
Threat Intelligence	Web categories
FQDN in Network rules	FQDN in Network rules
30GBps	30GBps
901,24€ per month	1.262,29€ per month



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 ⚠

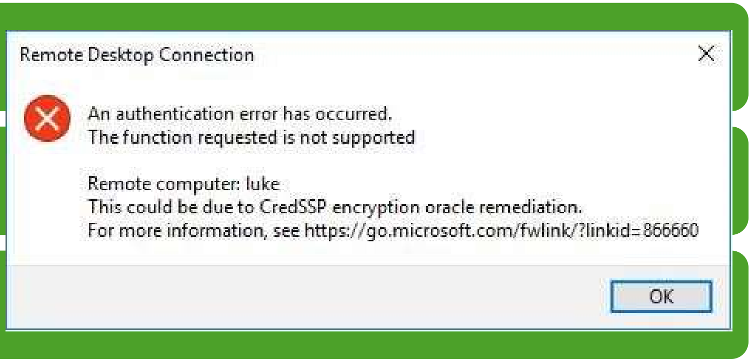
Showing 9 of 9 records

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

Update Management (Center)

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

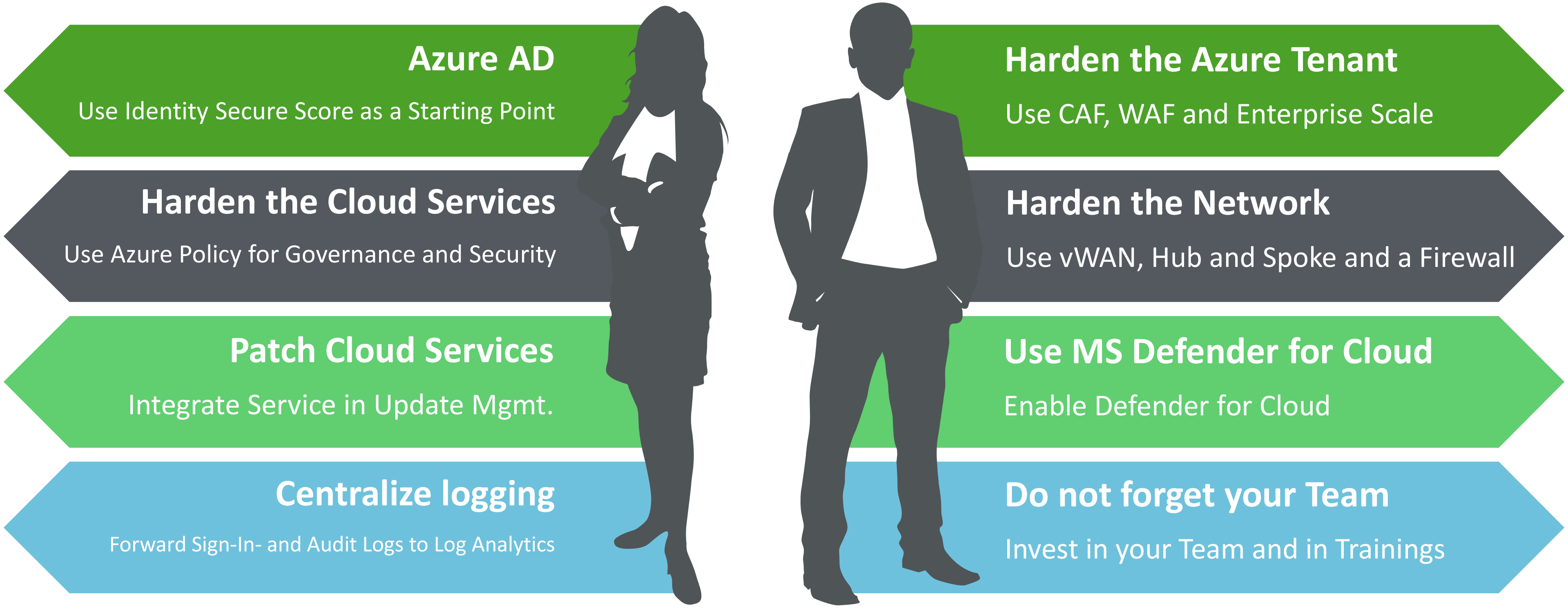
Remote computer: luke
This could be due to CredSSP encryption oracle remediation.
For more information, see https://go.microsoft.com/fwlink/?linkid=866660

Demo

Dive into the Azure Portal

- Update Management Center

Harden Azure on different Layers



Azure AD

Use Identity Secure Score as a Starting Point

Harden the Cloud Services

Use Azure Policy for Governance and Security

Patch Cloud Services

Integrate Service in Update Mgmt.

Centralize logging

Forward Sign-In- and Audit Logs to Log Analytics

Harden the Azure Tenant

Use CAF, WAF and Enterprise Scale

Harden the Network

Use vWAN, Hub and Spoke and a Firewall

Use MS Defender for Cloud

Enable Defender for Cloud

Do not forget your Team

Invest in your Team and in Trainings

Microsoft Cybersecurity Reference Architectures (MCRA)

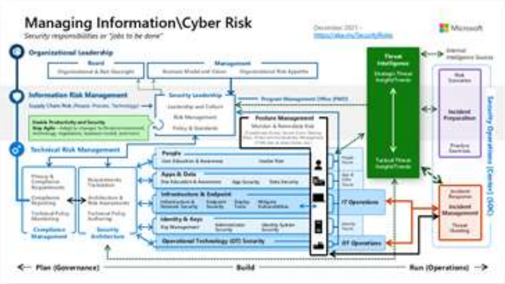
Capabilities

What cybersecurity capabilities does Microsoft have?

Build Slide

People

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



Zero Trust User Access

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

Azure Native Controls

What native security is available?

Security Operations

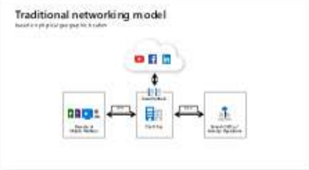
How to enable rapid incident response?

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

CLOUD IDENTITY SUMMIT ‘22

Thu, September 22nd, 2022

Deep-Dive and Q&A sessions on #AzureAD
Free Hybrid Event in Bonn, Germany
www.identitysummit.cloud

Links

www.wpninjas.eu

- Reimling.eu – Microsoft will disable Basic auth – What this means and what you have to do
  - https://www.reimling.eu/?p=4435
- MS Docs – Block legacy authentication access to Azure AD with CA
  - Block legacy authentication - Azure Active Directory - Microsoft Entra | Microsoft Docs
- MS Docs - Deprecation of Basic authentication in Exchange Online
  - Deprecation of Basic authentication in Exchange Online | Microsoft Docs
- MS Docs – Configure Temporary Access Pass
  - Configure a Temporary Access Pass in Azure AD to register Passwordless authentication methods - Microsoft Entra | Microsoft Docs
- MS Docs – Retiring Azure AD Connect 1.x versions
  - Azure AD Connect: Version release history - Microsoft Entra | Microsoft Docs
- MS Docs – Zero Trust Security in Azure
  - Zero Trust security in Azure | Microsoft Docs
- MS Docs – Passwordless options for Azure AD
  - Azure Active Directory passwordless sign-in - Microsoft Entra | Microsoft Docs
- MS Docs – Update Management Center (preview)
  - Update management center (preview) overview | Microsoft Docs
- MS Cybersecurity Rerference Architecture
  - https://aka.ms/MCRA
- Join the MS Security Community
  - Join Our Security Community - Microsoft Tech Community

www.wpninjas.eu
#WPNinjaS

Platinum Sponsor

PATCH MY PC

Microsoft Security

Gold Sponsor

glueckkanja gab

LIQUIT

baseVISION
SECURE & MODERN WORKPLACE

Lenovo

RECAST SOFTWARE

Snapdragon

Silver and Special Sponsors

SD:>_
SwissDev Jobs

LUZERN
DIE STADT. DER SEE. DIE BERGE.

sepago®

EPIC FUSION

SCAPPMAN

AppManagEvent.com
2022 October 7 NETHERLANDS

dinext.

About “Gregor Reimling”

Azure Meetup BONN

www.azurebonn.de

Thank You

Cloud Inspires Podcast

Stories and people behind Cloud Transformation

www.cloudinspires.me

Blog

- https://www.Reimling.eu

Contact

- @GregorReimling
- @CloudInspires