www.wpninjas.eu

Top 10 Azure Security Best Practices

By Gregor Reimling

Workplace Ninja Summit 2022

About “Gregor Reimling”

www.wpninjas.eu

Azure Meetup BONN
www.azurebonn.de

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

Agenda

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

Key takeaways:

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

Azure AD Hardening

Identity Attacks rising

www.wpninjas.eu

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

- Azure AD
- ADFS
- MSA
- Google ID
- Android
- iOS
- MacOS
- Windows
- Windows Defender ATP
- Geo-location
- Corporate Network
- Browser apps
- Client apps

Conditions

- Employee & Partner Users and Roles
- Trusted & Compliant Devices
- Physical & Virtual Location
- Client apps & Auth Method

171TB

Machine learning

Session Risk

3

Real time Evaluation Engine

Policies

Effective policy

Controls

- Allow/block access
- Limited access
- Require MFA
- Force password reset
- Block legacy authentication

Microsoft Cloud

Microsoft Cloud App Security

Cloud SaaS apps

On-premises & web apps

Identity Secure Score

www.wpninjas.eu

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+/)

Learn more | Got feedback?

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)
- ...n-ins
- ...ctions

Troubleshooting + Support

- New support request

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%

Score history

7 days | 30 days | 60 days | 90 days

50 40 30 20

July 17 | July 24 | July 31 | August 7

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

New policy | New policy from template (Preview)

Search policies | Add filters

Policy Name

- 01-CA-EnableMFAforallGlobalAdminswithoutBreakGlass
- 10-CA-EnableMFAforallUsers
- 20-CA-Devices-Requires-mustbeCompliant

Manage

Named locations

...blems

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

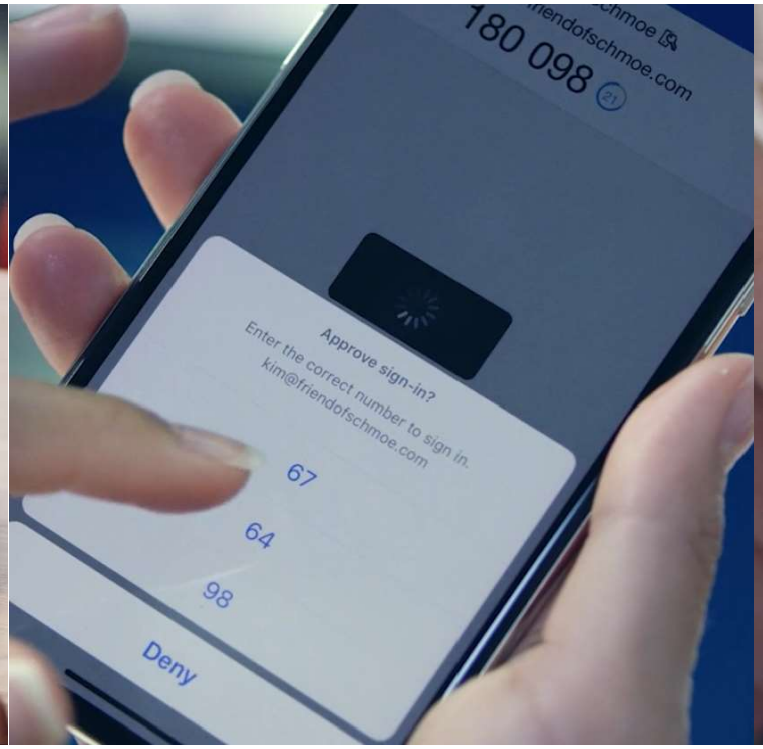
The following is a brief summary of updates to protected logins available in AD FS 2019:

Passwordless Options

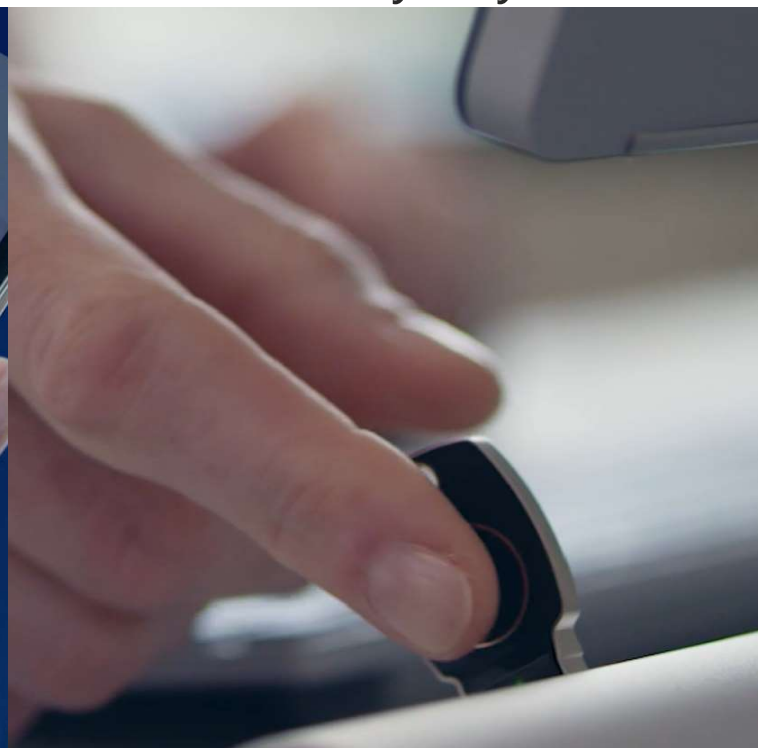
www.wpninjas.eu

Windows Hello for Business

Microsoft Authenticator



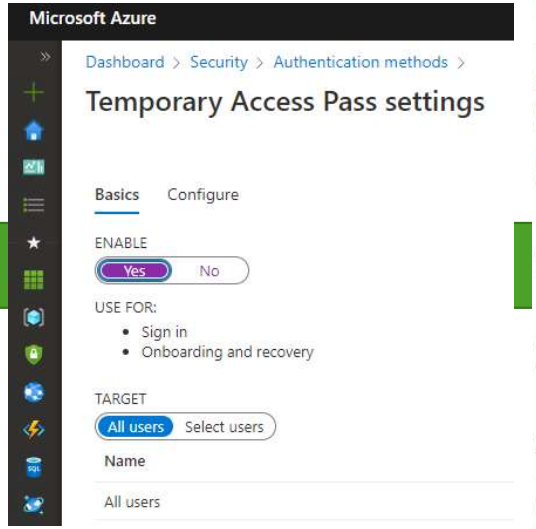
FIDO2 Security Keys

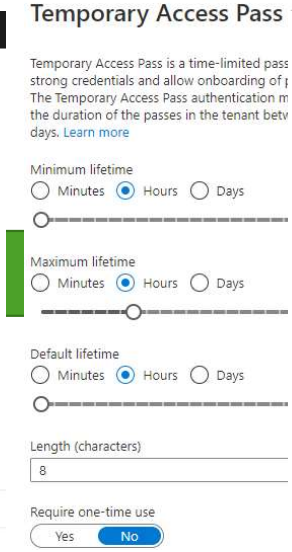


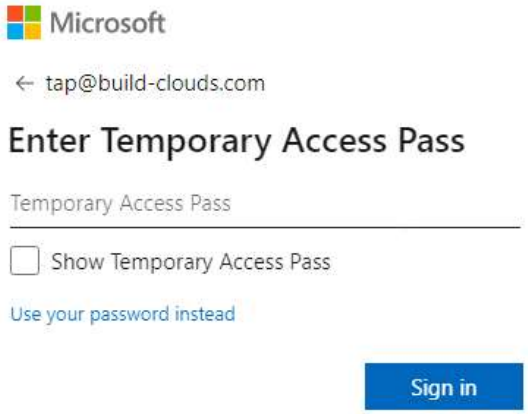
Azure Active Directory passwordless sign-in - Microsoft Entra | Microsoft Docs

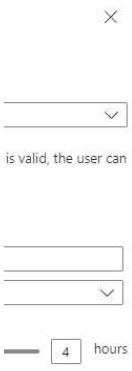
Temporary Access Pass

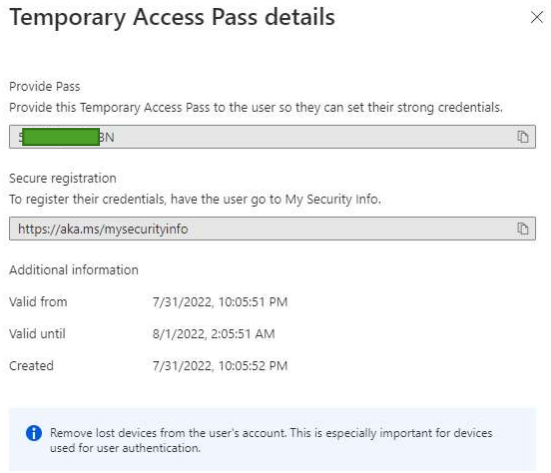
www.wpninjas.eu











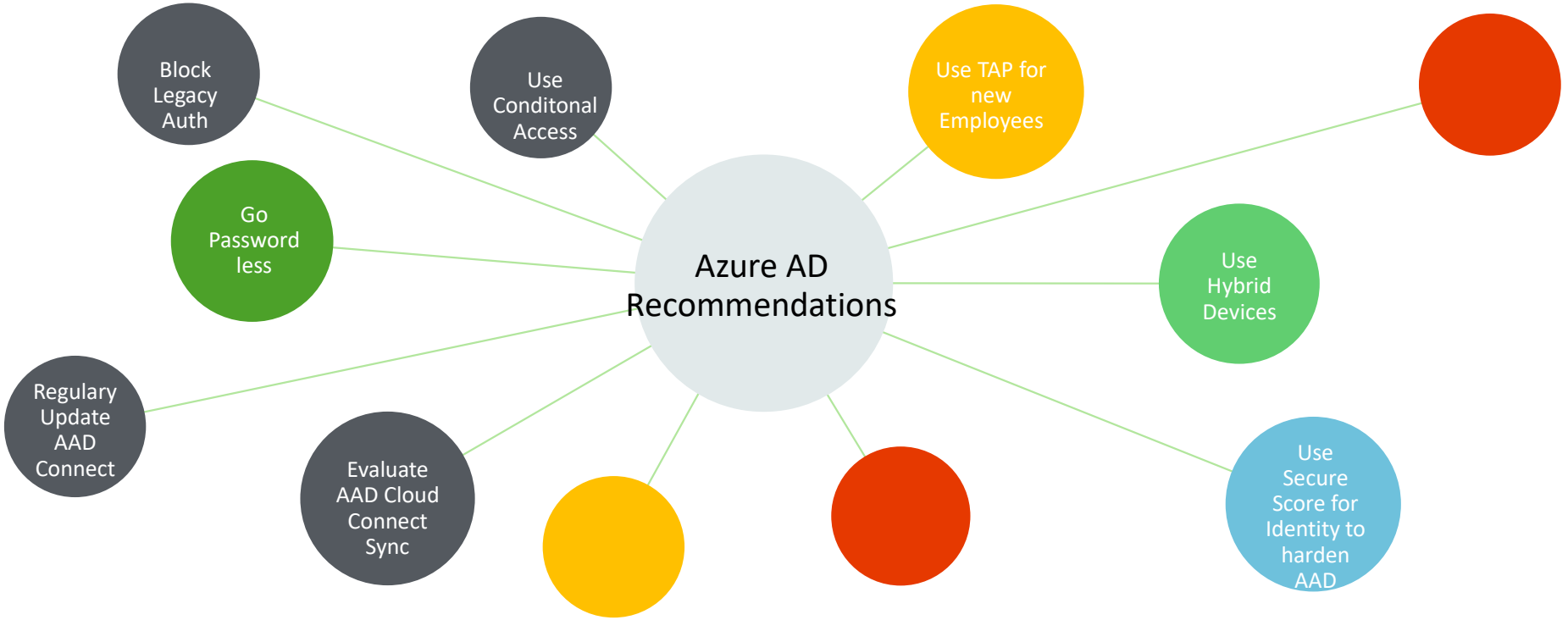
https://aka.ms/mysecurityinfo

Show following settings

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

Azure AD Recommendations

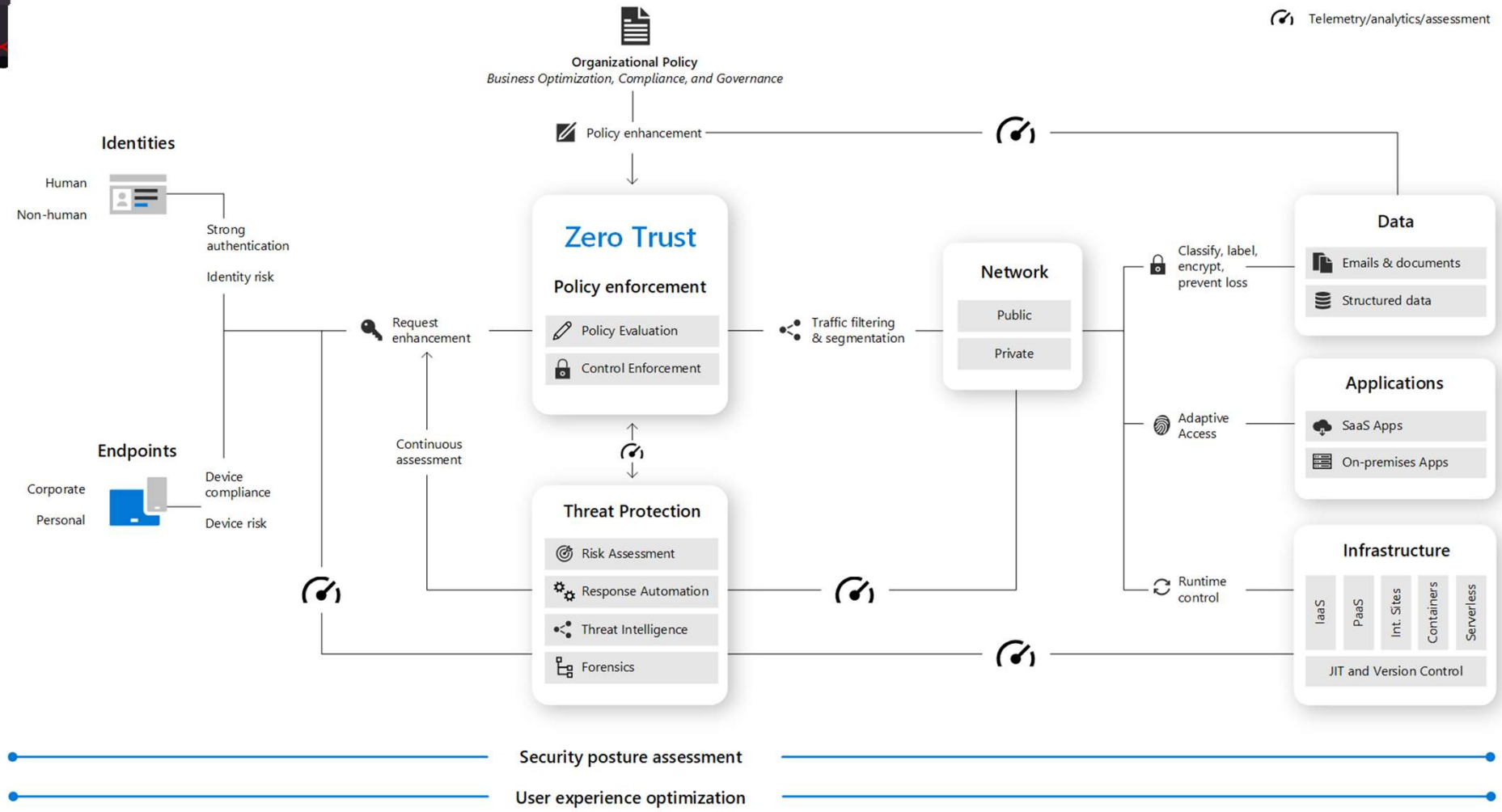
www.wpninjas.eu



Azure Tenant Hardening

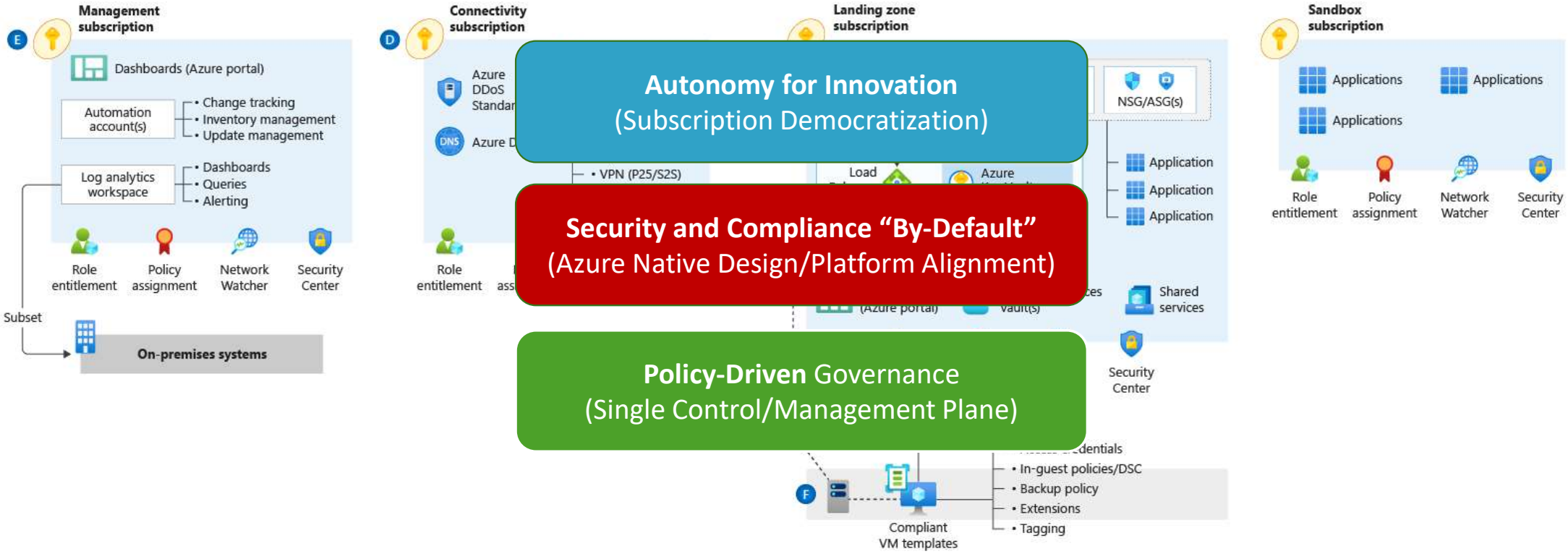
Zero Trust architecture

www.wpninjas.eu



Enterprise-Scale - Design Principles

www.wpninjas.eu



Well-architected Framework

www.wpninjas.eu

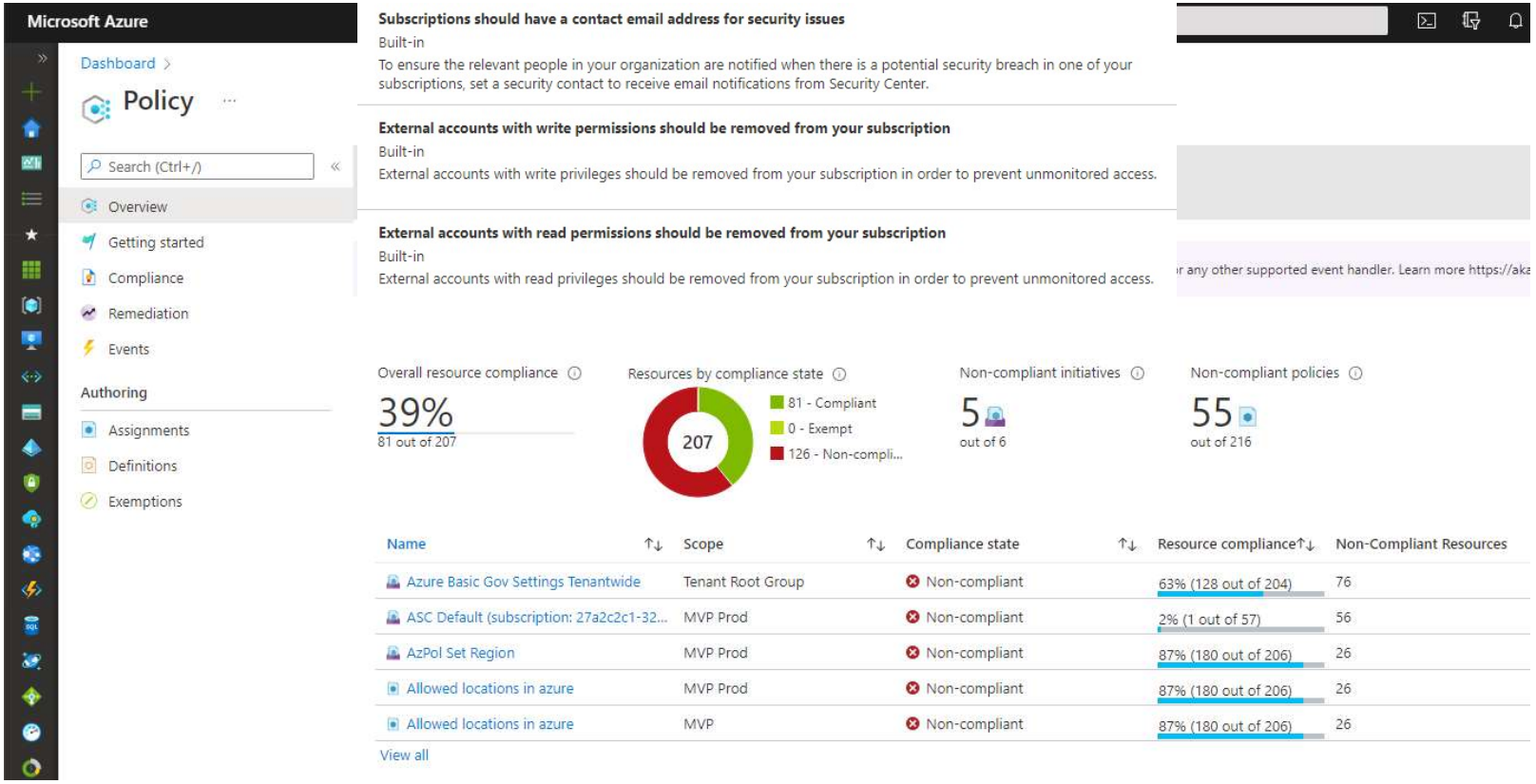
"The Azure Well-Architected Framework is a set of guiding tenets that can be used to improve the quality of a workload."

Azure Advisor

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

Azure Policy

www.wpninjas.eu



Manage Subscription Policies

www.wpninjas.eu

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

Demo

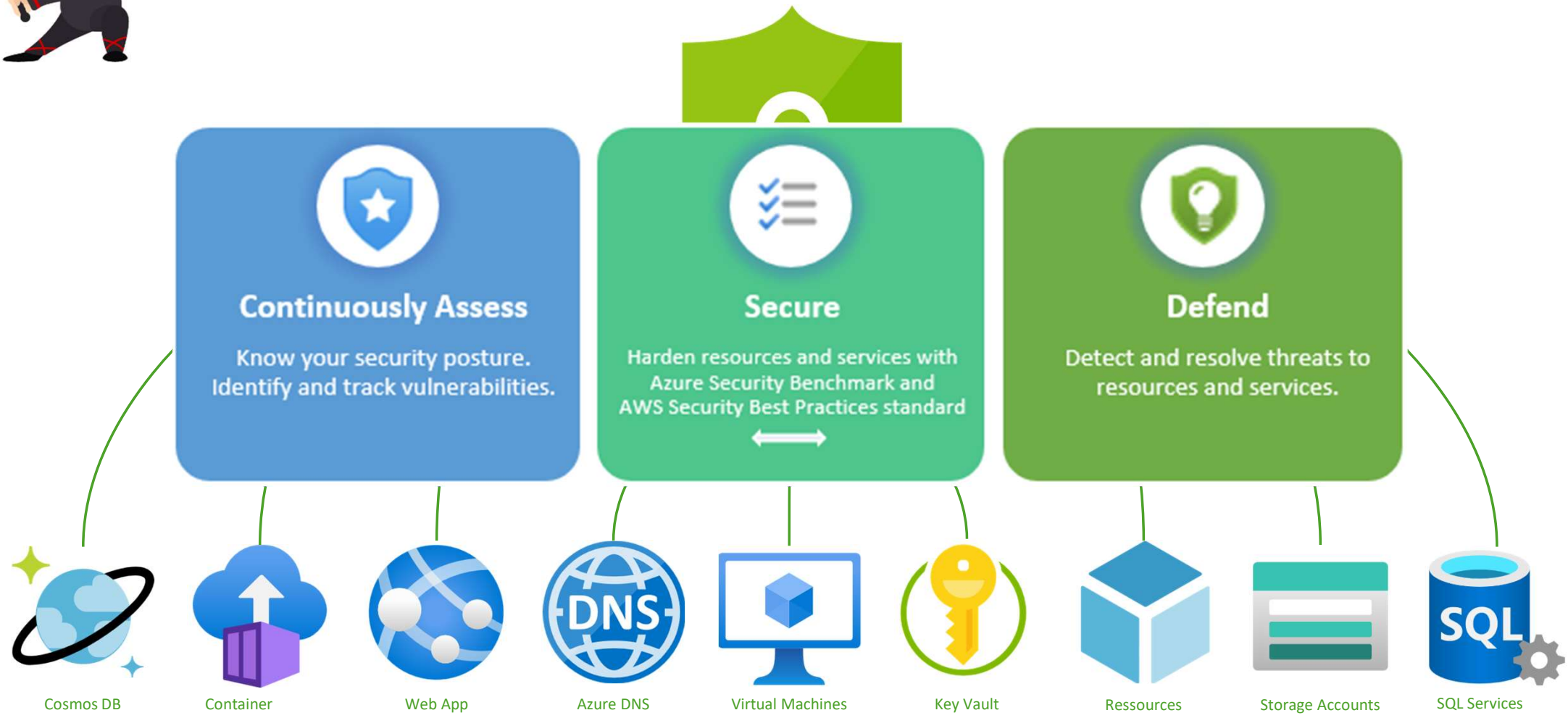
Dive into the Azure Portal

- Azure Advisor
- Azure Policy

Microsoft Defender for Cloud

Microsoft Defender for Cloud

www.wpninjas.eu



MS Defender for Cloud

www.wpninjas.eu

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

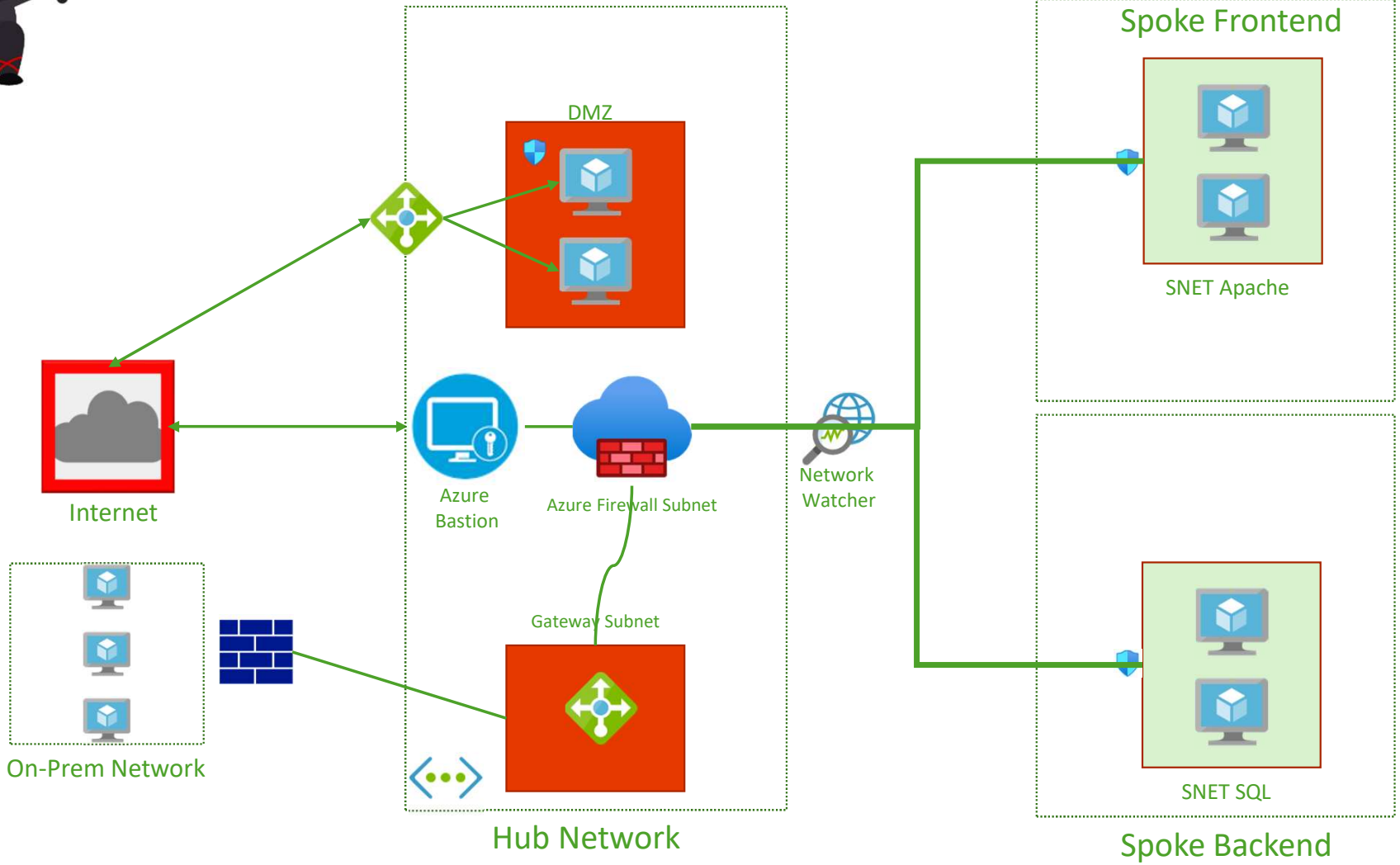
Dive into the Azure Portal

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

Azure Network Hardening

Network Protection

www.wpninjas.eu

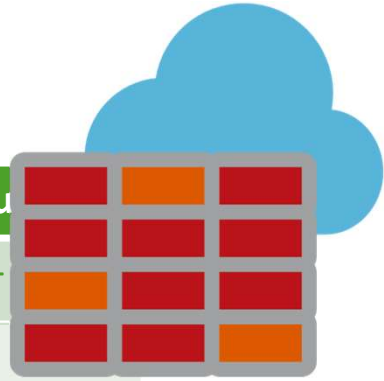


Azure IaaS Recommendations

www.wpninjas.eu

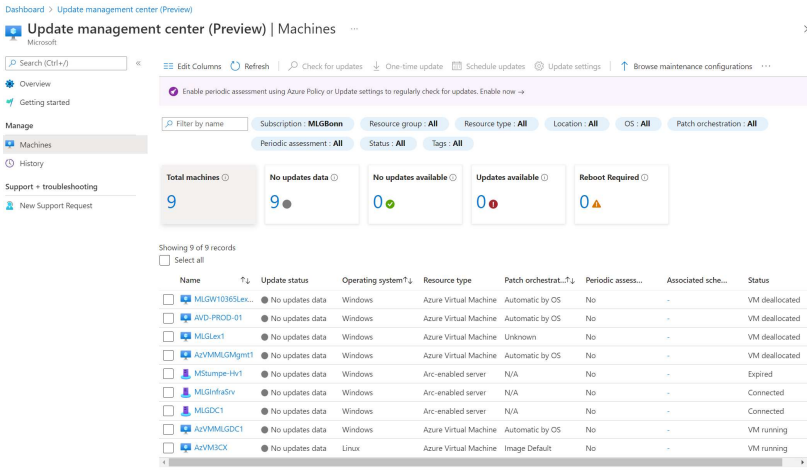
- Segmentation of Virtual Networks
- Define Subnets and use NSG at Subnet Level
- Use a NVA or Azure Firewall at the Hub Network
- Define UDR to Route traffic over the Hub Network and Firewall
- Use Azure Web Application Firewall for Internetapplications
- Use DDoS Protection for Web Applications
- Use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

www.wpninjas.eu



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

Demo

Dive into the Azure Portal

- Update Management Center

Harden Azure on different Layers

www.wpninjas.eu

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)

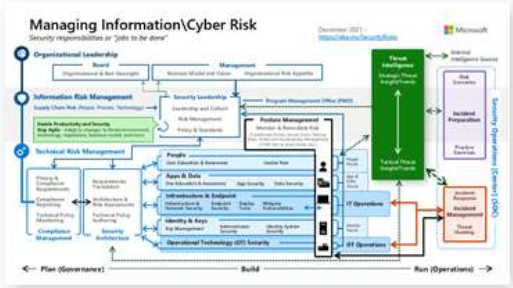
Capabilities

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

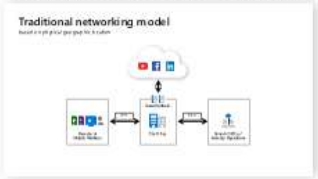
How to enable rapid incident response?

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

- 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

Platin Sponsor

Patch My PC
PATCH MANAGEMENT MADE EASY

Microsoft

Gold Sponsor

glueckkanja gab

LIQUIT

baseVISION
SECURE & MODERN WORKPLACE

Lenovo

RECAST SOFTWARE

Silver and Special Sponsors

SD:>_
SwissDev Jobs

sepago®

EPIC FUSION

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