

Understanding all security aspects of Azure Virtual Desktop

Freek Berson
@fberson



Workplace Ninja Virtual Edition 2021



V-Platin Sponsor



RECAST SOFTWARE



Patch My PC
PATCH MANAGEMENT MADE EASY

glueckkanja  gab

Lenovo

V-Gold Sponsor



scopewyse

we are what's next

sepago[®]

baseVISION
SECURE & MODERN WORKPLACE

Patron Sponsors





About Freek Berson

www.wpninjas.eu

Focus

Azure Virtual Desktop, RDS, Windows 365
Bicep and ARM Templates

From

The Netherlands

Books

Getting started with Bicep

AVD Handbook: Security Fundamentals

AVD migration guide for RDS

RDS - The Complete Guide



Awards

Microsoft MVP since 2011

Hobbies

Spending time with my wife & kids

Cycling, soccer, traveling (pre COVID-19)

Contact

@fberson
github.com/fberson





***Azure Virtual Desktop does not use
port 3389, so we're secure...right?***



Key takeaway:

**learn about all security aspects and options
to properly secure your AVD environment!**



INTRODUCTION

What is AVD and what does Windows 365 add?



SECURITY RESPONSIBILITIES

What does Microsoft manage, what do you manage?



6 SECURITY PILLARS

Example & guidance



DEMOS

Various practical examples



TAKEAWAYS & CALL TO ACTIONS

Links to deck, e-book & guidance on getting started!



Azure Virtual Desktop

www.wpninjas.eu

Your subscription—your control

Desktop and remote apps



Full desktop



Remote app



Windows 10 enterprise multi-session



Windows Server 2012 R2 and newer



Windows 10 enterprise



Windows 7 enterprise full desktop

Management and policies



Image, app, and profile management



User density, VM sizing, and scaling policies



User management and identity



Network policies

Managed by Microsoft

Azure Virtual Desktop Service



Clients



Broker



Management



Gateway



Diagnostics



Load balancing

Azure Infrastructure



Compute



Storage



Networking



HTML5



iOS



Android



Windows




Linux



Windows 365 – Cloud PC

www.wpninjas.eu

- ✓ Leveraging the **AVD Platform**
- ✓ Azure AD Joined **personal desktops**
- ✓ Per-user per-month **fixed license (24/7 access)**
- ✓ **MEM** is used to manage all of your Cloud PCs.
- ✓ **Business** and **Enterprise** editions

**Freek Berson**
[Reset password](#)

[Account](#) [Devices](#) [Licenses and apps](#) [Mail](#) [OneDrive](#)

ⓘ The trial subscription for Windows 365 Business 4 vCPU, 16 GB, 128 GB Trial expires on 10/1/2021. Buy this subscription so they won't lose access when the trial ends.
[Buy this subscription](#)

Select location *

Netherlands

Licenses (3)

☒ **Microsoft Power Automate Free**
9999 of 10000 licenses available

☒ **Microsoft Teams Exploratory**
96 of 100 licenses available

☒ **Windows 365 Business 4 vCPU, 16 GB, 128 GB**
0 of 1 licenses available

← → ↻ 🏠 <https://windows365.microsoft.com>

Windows 365

[Home](#) | **Welcome Freek Berson**


Quick actions

Manage your organization
Manage users and assign licenses for Microsoft 365 products.

Download Remote Desktop
Access your cloud PC directly from your device with the Remote Desktop...

Get more cloud PCs
Add more cloud PCs to your subscription for you and your team.

Your cloud PCs

**VSB_Policy_with_Micro...** ⚙️
Last connected 1 day ago

4 vCPU

16GB RAM

128GB Storage

Restart

Reset

Rename

Troubleshoot

[Open in browser](#)



Security Responsibilities

**Security components
Microsoft manages**

Web access

Gateway

**Connection
Broker**

Diagnostics

**Extensibility
components**

**Security components
customers manage**

**Azure Virtual
Network**

Azure AD

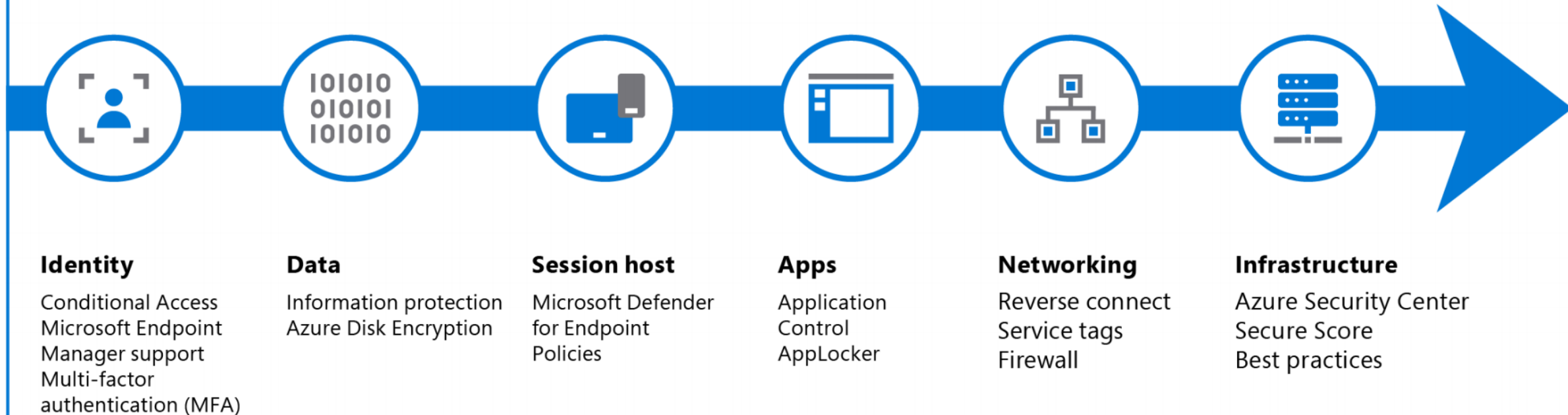
Azure AD DS

**Azure
Virtual Desktop
session hosts**

**Azure
Virtual Desktop
workspace**



End-to-end security for your virtual desktops





Securing Identities

❑ Use Conditional Access and enable **Multi-Factor Authentication (MFA)**

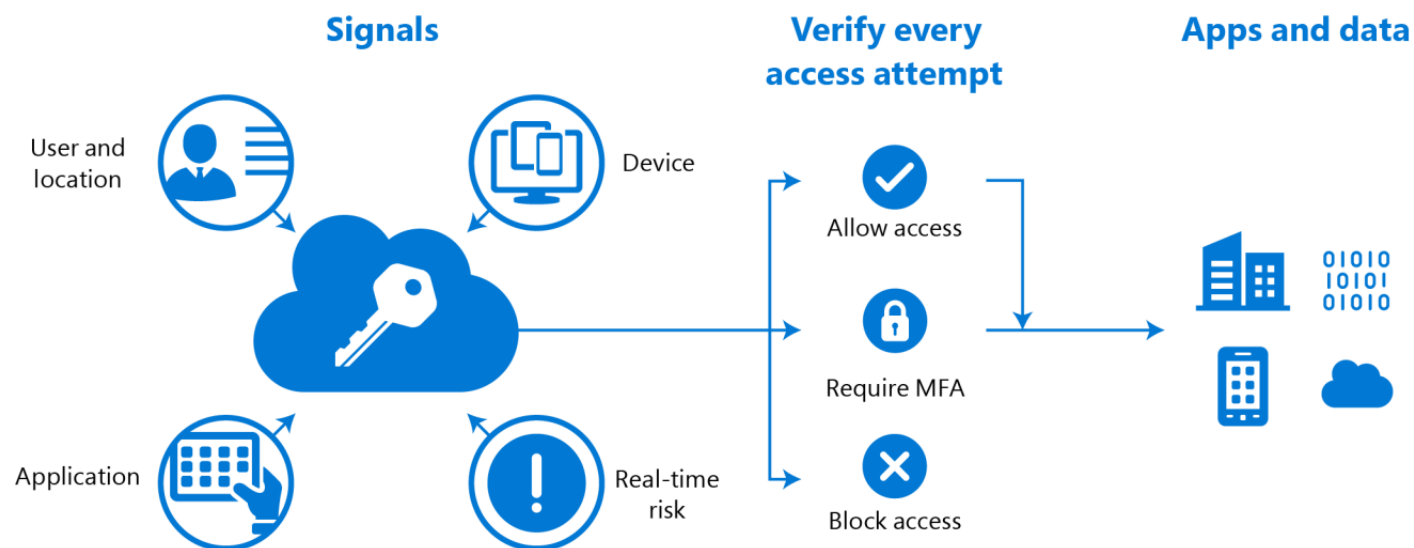
Under Cloud apps or actions > Include, select Select apps and then select Windows Virtual Desktop (App ID [9cdead84-a844-4324-93f2-b2e6bb768d07](#))

<https://docs.microsoft.com/en-us/azure/virtual-desktop/set-up-mfa>

❑ Demo!

❑ Collecting and examining **audit logs** is important too.

<https://docs.microsoft.com/en-gb/azure/virtual-desktop/diagnostics-log-analytics>





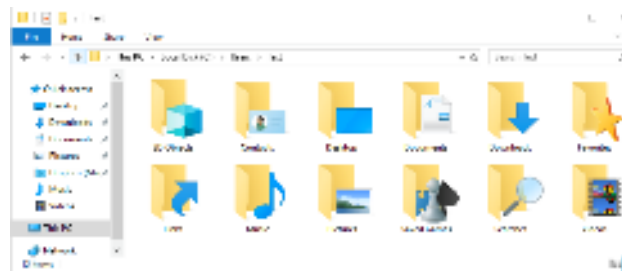
Securing Data

❑ Use Azure Disk Encryption

❑ Use FSlogix Profile Containers

- Places entire user profile in network-based container.
- Fast logon times.
- Virtually eliminates profile corruption.
- Works alongside existing User Environment Management platforms.

<https://docs.microsoft.com/en-gb/azure/virtual-desktop/create-file-share>





Securing applications

- ❑ Review [Security Policy Advisor](#) for Microsoft 365 Apps for enterprise

<https://docs.microsoft.com/en-gb/DeployOffice/overview-of-security-policy-advisor>

- ❑ Implement [AppLocker](#) control policies restriction rules are based on file attributes, product names, file names, or file versions.

<https://docs.microsoft.com/en-gb/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview>

- ❑ Consider [Application Masking](#) can also be used to provide security for applications.

<https://docs.microsoft.com/en-gb/fslogix/implement-application-masking-tutorial>

- ❑ Demo!





Screen Capture Protection

www.wpninjas.eu

The screenshot shows the Local Group Policy Editor window. The left pane displays the tree structure with 'Azure Virtual Desktop' selected under 'Remote Desktop Session Host'. The right pane shows the 'Enable screen capture protection' policy setting, which is currently 'Not configured'. Below the table, there is a description of the policy and its requirements.

Setting	State	Comment
Enable screen capture protection	Not configured	No

Enable screen capture protection

Requirements:
Azure Virtual Desktop

Description:
This policy setting allows you to specify whether protection against screen capture is enabled for a remote session. If you enable this policy setting, the RD Session Host server will instruct the client to enable the screen capture protection for a remote session. If a compatible client is used, it will prevent screen capture of the applications running in the remote session.

If client is not compatible with screen capture protection, connection will be denied.

If you disable or not configure this policy setting, the screen capture protection will be disabled.

<https://docs.microsoft.com/en-gb/azure/virtual-desktop/screen-capture-protection>

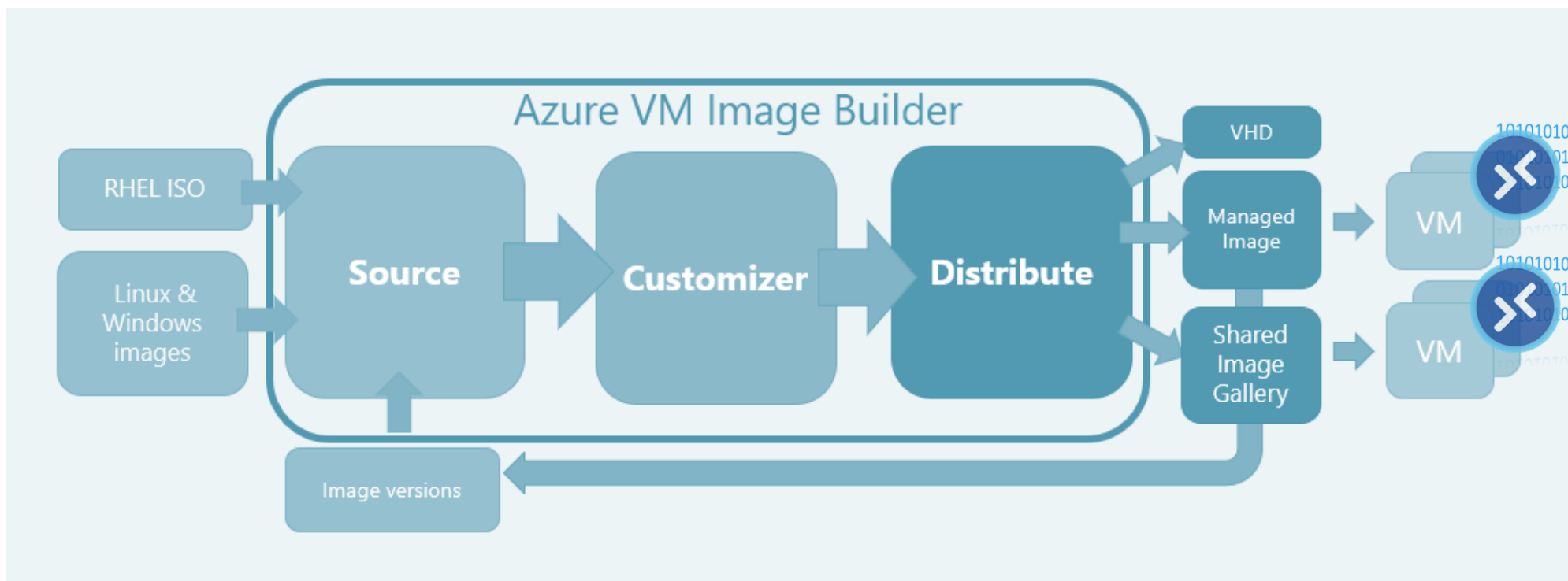


Securing the OS

- ❑ Leverage [Azure Image Builder](https://docs.microsoft.com/en-us/azure/virtual-machines/image-builder-overview) to keep OS image and applications updated.

<https://docs.microsoft.com/en-us/azure/virtual-machines/image-builder-overview>

- ❑ Demo!





Securing the Session Hosts

☐ Lock down your Session Host Servers with GPO, Preferences, MEM, Intune

Maximum inactive/disconnection time policies and screen locks

Device redirection options

Restricting Windows Explorer

Restricting Command prompt, Control Panel

☐ configure Microsoft Defender for Endpoint

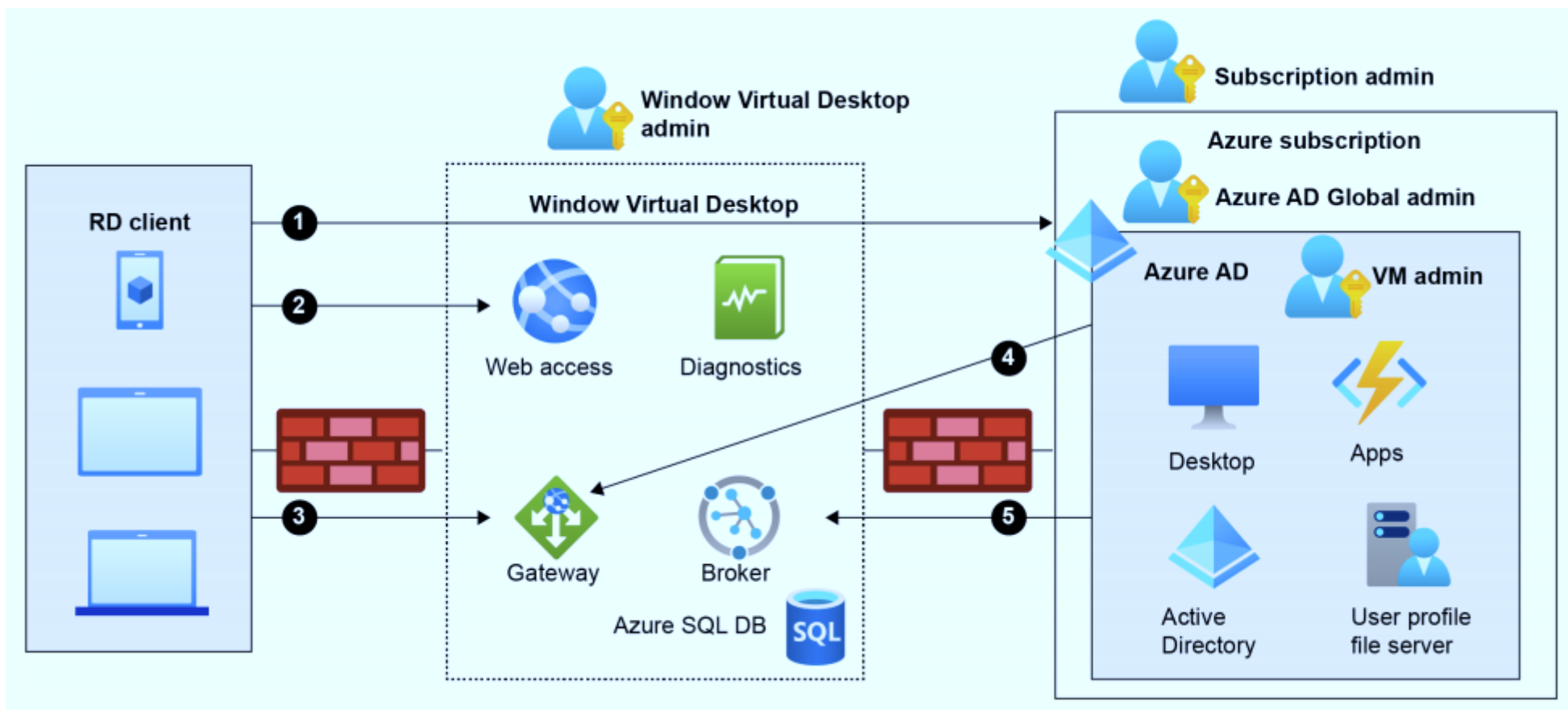
<https://docs.microsoft.com/en-gb/microsoft-365/security/defender-endpoint/Onboard-Windows-10-multi-session-device>

☐ Microsoft Endpoint Manager

<https://docs.microsoft.com/en-gb/mem/intune/fundamentals/tutorial-walkthrough-endpoint-manager>



Securing Network Access





Securing Network Access

- ❑ WVD contain **Reverse connect** transport for establishing the remote session as well as for carrying the RDP traffic

```
Command Prompt
Microsoft Windows [Version 10.0.19042.985]
(c) Microsoft Corporation. All rights reserved.

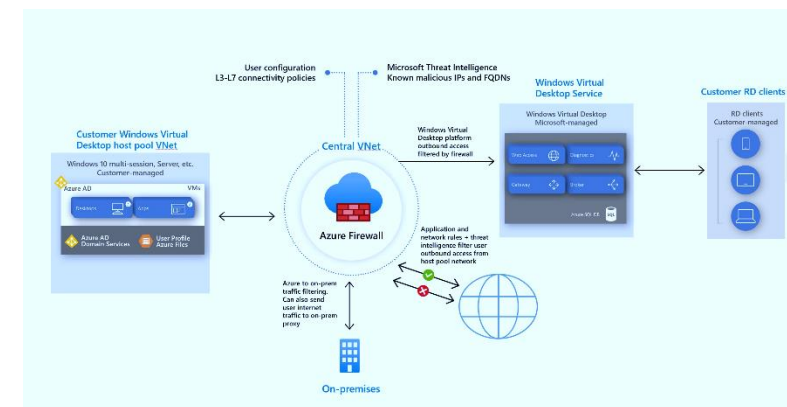
C:\Users\FBerson>qwinsta
SESSIONNAME      USERNAME              ID  STATE  TYPE      DEVICE
services         0                    Disc
console          1                    Conn
>rdp-sxs210326... FBerson              3   Active
31c5ce94259d4...    65536               Listen
rdp-tcp           65537               Listen
rdp-sxs210326006   65538               Listen

C:\Users\FBerson>
```

- ❑ Use **Service tags** to simplify security for Azure VMs.
- Required URL Check tool: WVDAgentUrlTool.exe
<https://docs.microsoft.com/en-us/azure/virtual-desktop/safe-url-list>

Address	Outbound TCP port	Purpose	Service Tag
*.wvd.microsoft.com	443	Service traffic	WindowsVirtualDesktop
gcs.prod.monitoring.core.windows.net	443	Agent traffic	AzureCloud

- ❑ Use **Azure Firewall** to secure outbound traffic
<https://docs.microsoft.com/en-gb/azure/firewall/protect-windows-virtual-desktop>





Azure security best practices

- ❑ Monitoring your [Secure Score](#) to strengthen the overall security of your environment

<https://docs.microsoft.com/en-gb/azure/security-center/secure-score-security-controls>

- ❑ With [Azure Sentinel](#) ingest Windows event logs from your session hosts, Microsoft Defender for Endpoint alerts, and also Azure Virtual Desktop diagnostics.

<https://azure.microsoft.com/en-gb/services/azure-sentinel/>

- ❑ Leverage [Azure security baseline](#) for Azure Virtual Desktop

<https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/windows-virtual-desktop-security-baseline>

Azure security baseline for Windows Virtual Desktop

[NS - Network Security](#)

[IM - Identity Management](#)

[PA - Privileged Access](#)

[DP - Data Protection](#)

[AM - Asset Management](#)

[LT - Logging and Threat Detection](#)

[IR - Incident Response](#)

[PV - Posture and Vulnerability Management](#)

[ES - Endpoint Security](#)

[BR - Backup and Recovery](#)

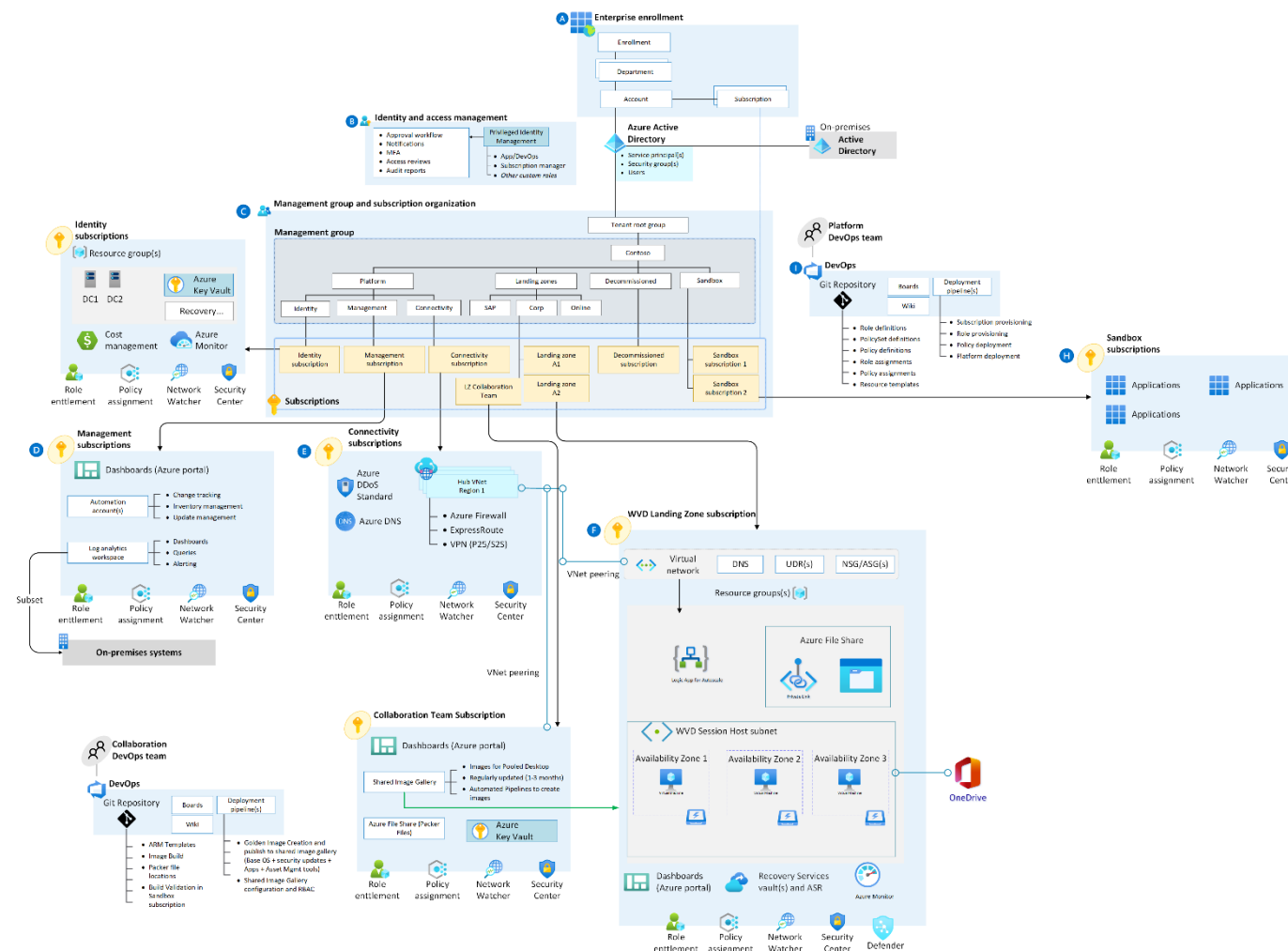
[GS - Governance and Strategy](#)



Enterprise-scale construction sets

www.wpninjas.eu

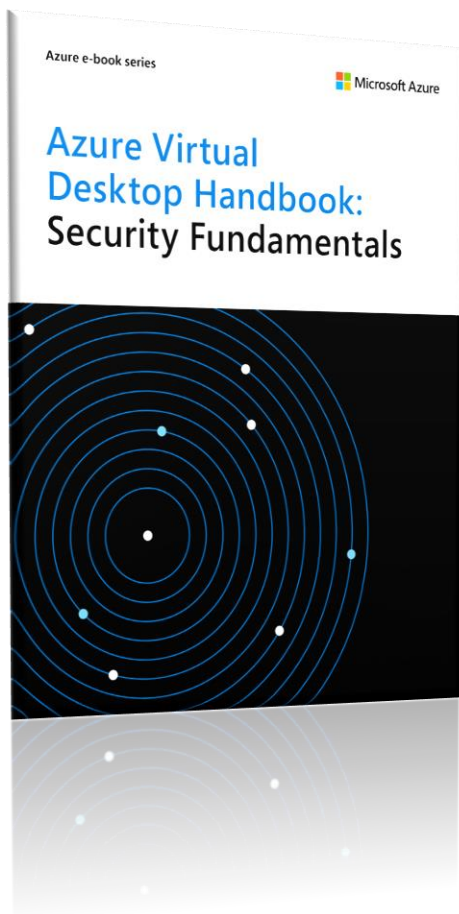
<https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/scenarios/wvd/enterprise-scale-landing-zone>



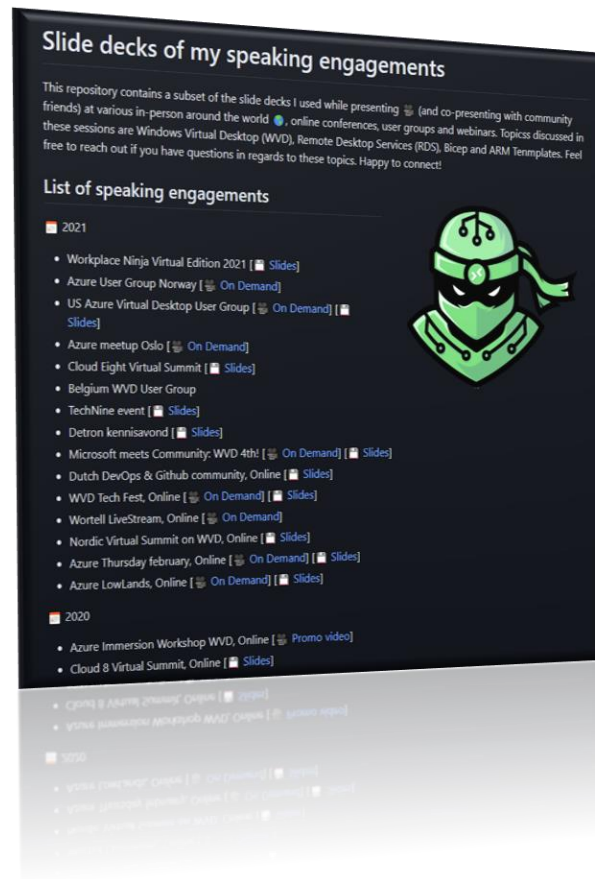


Call to action!

www.wpninjas.eu



<https://bit.ly/3fyiYuB>



<https://github.com/fberson/Slidedecks>





Thank You



Freek Berson
@fberson
freek@wortell.nl
TheMicrosoftPlatform.net



Workplace Ninja Virtual Edition 2021