ONE OF THE LARGEST CLOUD EVENTS OF THE YEAR

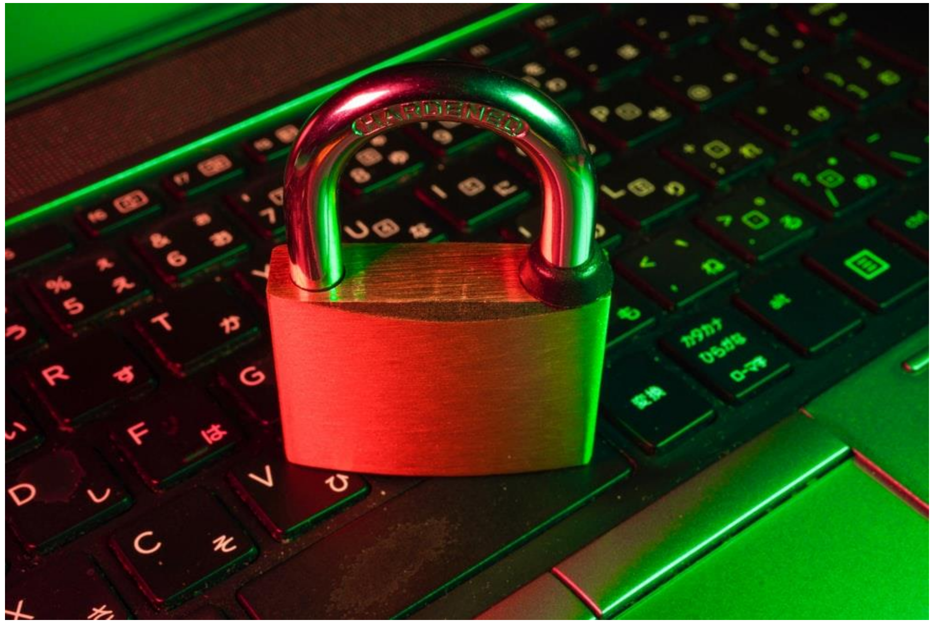
CLOUD SUMMIT 2021

(Azure Focused)

SEPTEMBER 13 - 23

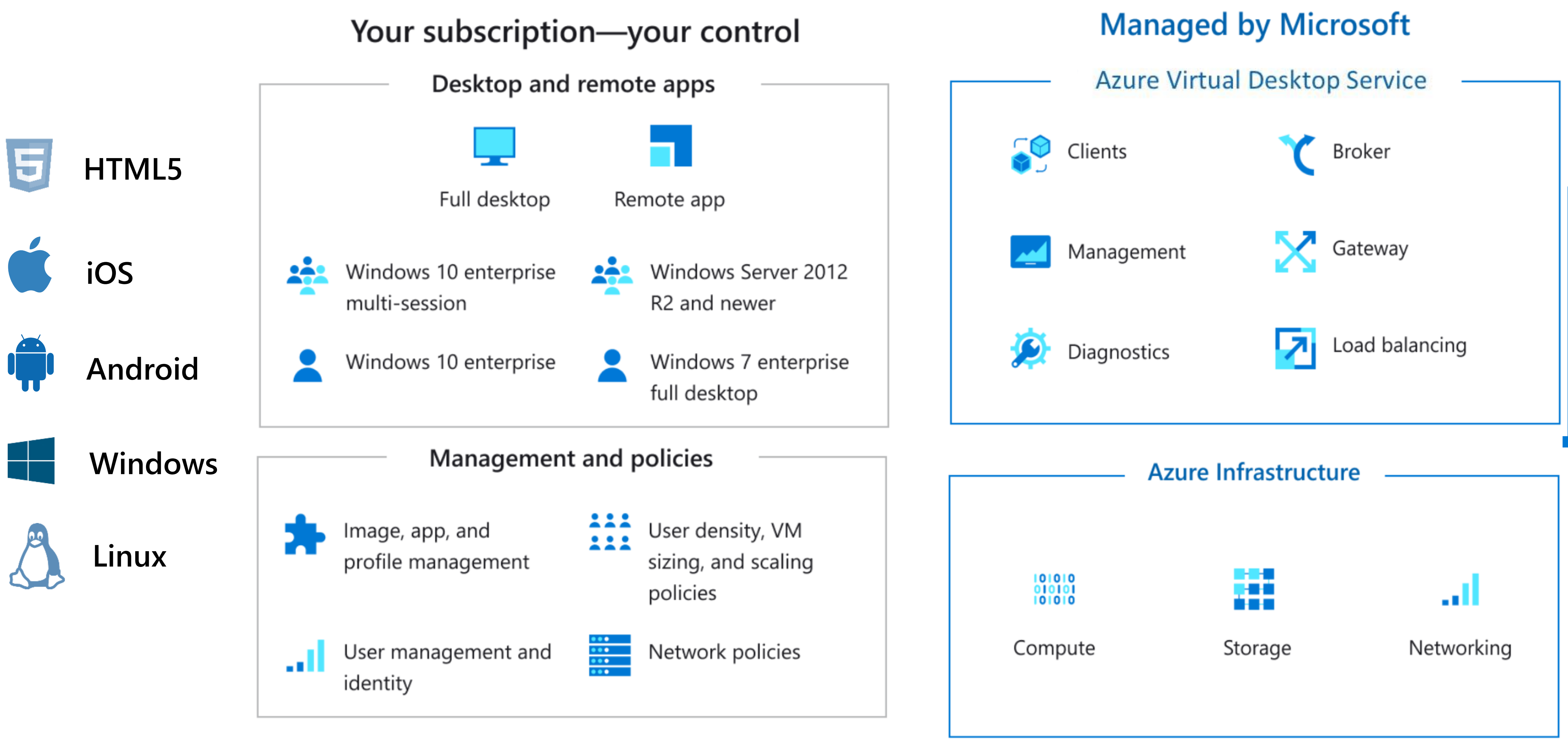
Understanding all security aspects of Azure Virtual Desktop

Freek Berson
@fberson
github.com/fberson



Azure Virtual Desktop does not use port 3389, so we’re secure…right?

Azure Virtual Desktop



- HTML5
- iOS
- Android
- Windows
- Linux

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

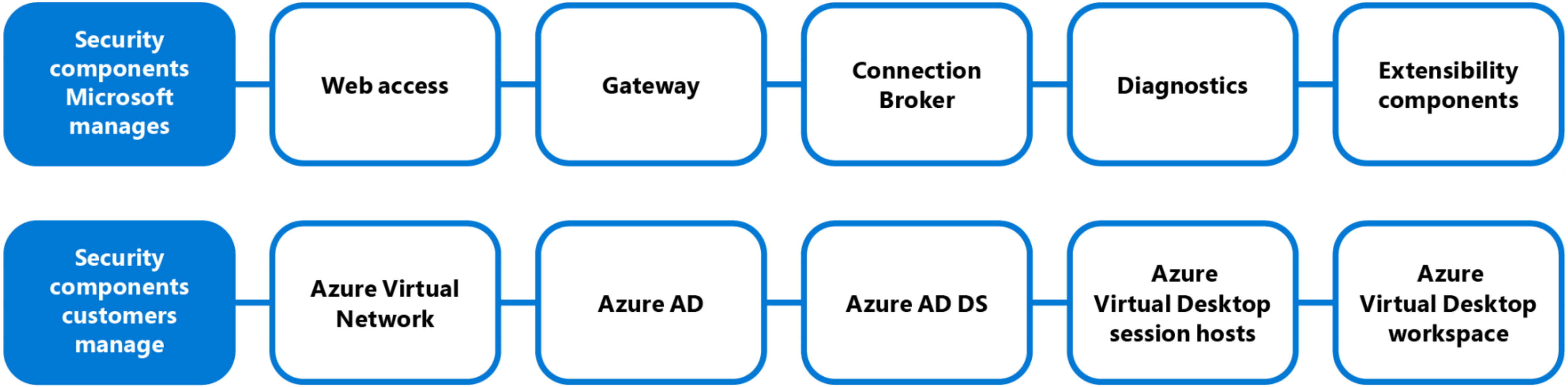
Azure Infrastructure

Compute

Storage

Networking

Security Responsibilities



Security components Microsoft manages

Web access

Gateway

Connection Broker

Diagnostics

Extensibility components

Security components customers manage

Azure Virtual Network

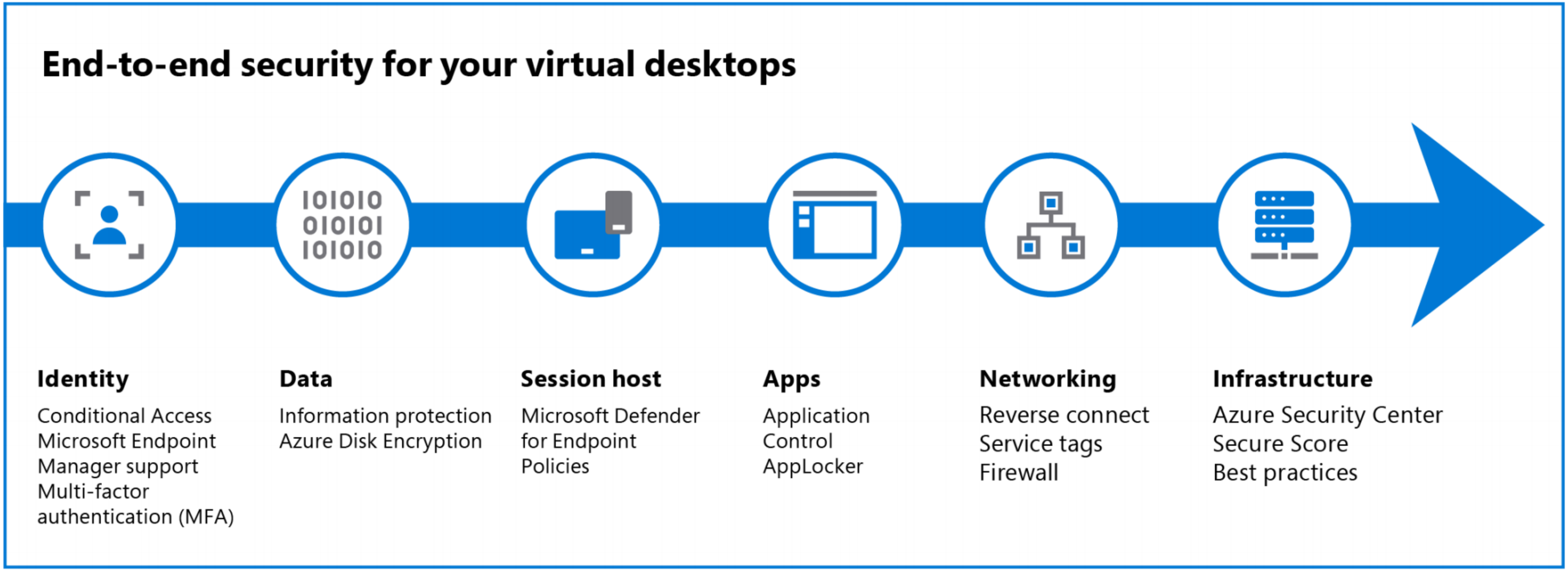
Azure AD

Azure AD DS

Azure Virtual Desktop session hosts

Azure Virtual Desktop workspace

End-to-end security



End-to-end security for your virtual desktops

Identity
Conditional Access
Microsoft Endpoint Manager support
Multi-factor authentication (MFA)

Data
Information protection
Azure Disk Encryption

Session host
Microsoft Defender for Endpoint
Policies

Apps
Application Control
AppLocker

Networking
Reverse connect
Service tags
Firewall

Infrastructure
Azure Security Center
Secure Score
Best practices

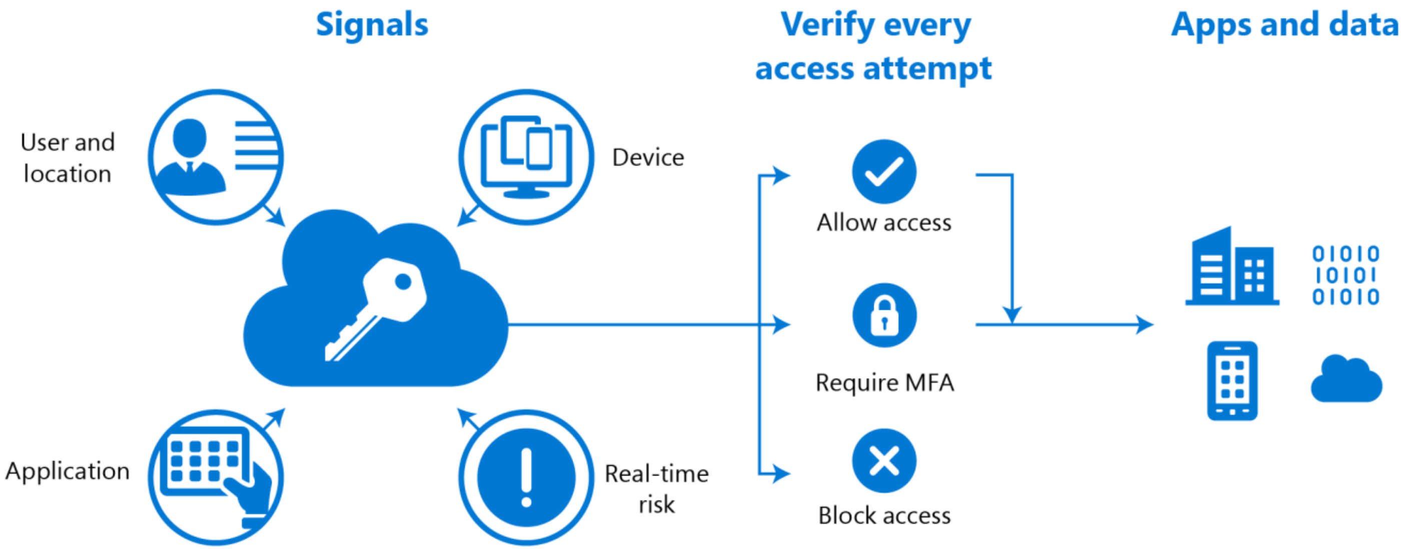
Securing Identities

❑ 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

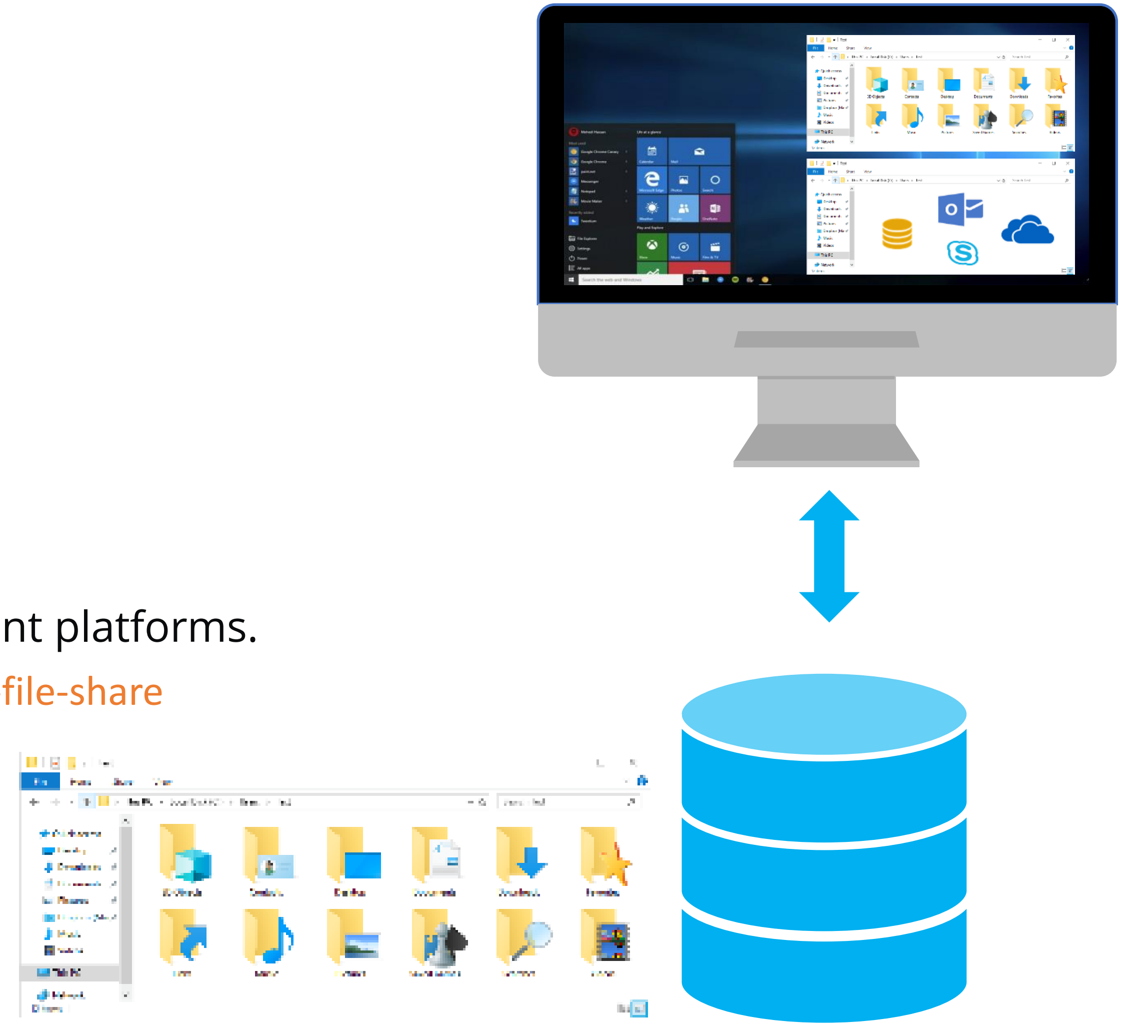
Securing Data

❑ 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.

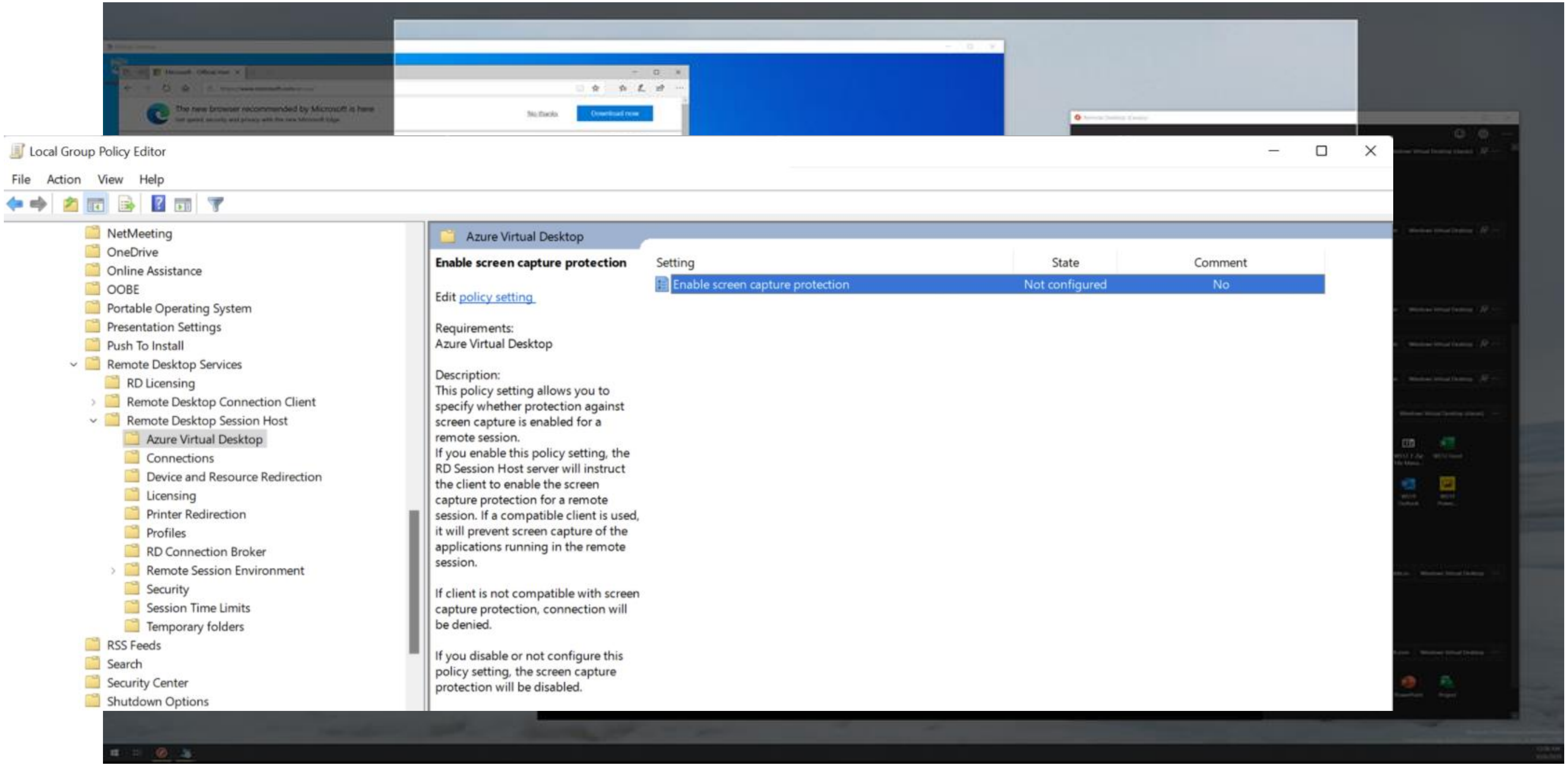
https://docs.microsoft.com/en-gb/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview

❑ 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



Enable screen capture protection

Edit policy setting

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.

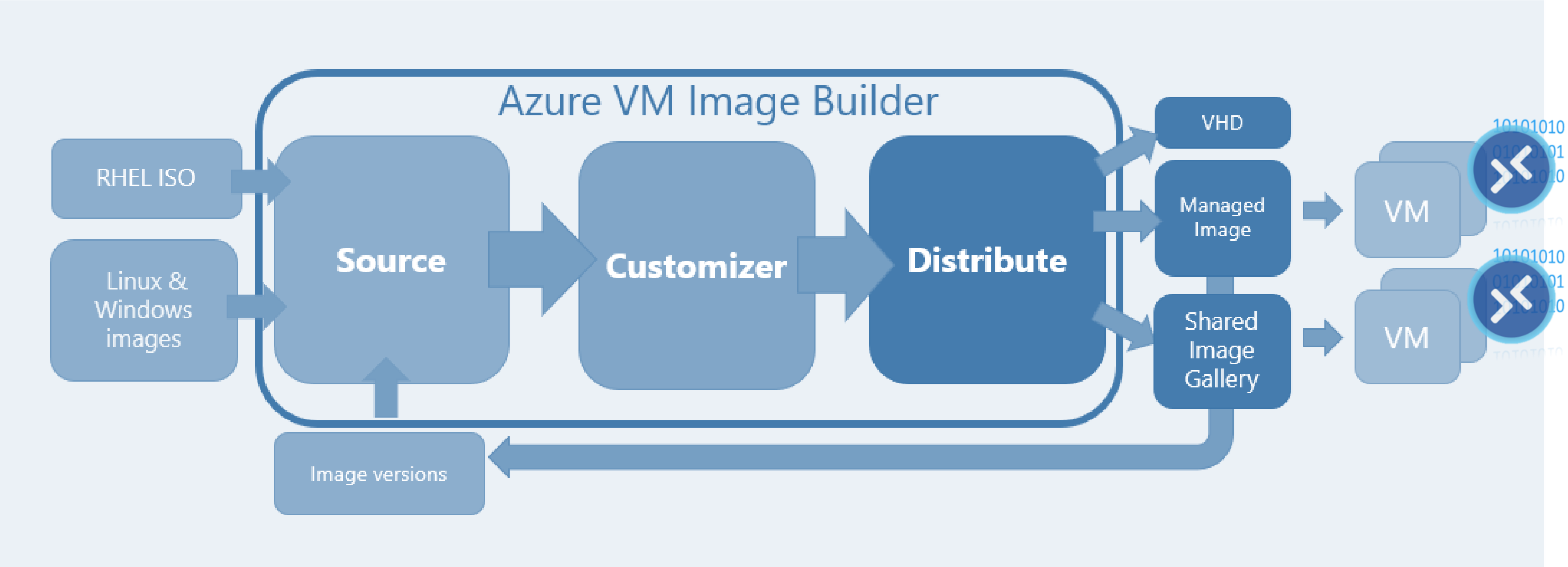
If you disable or not configure this policy setting, the screen capture protection will be disabled.

Setting	State	Comment
Enable screen capture protection	Not configured	No

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

Securing the OS

- ❑ Leverage Azure Image Builder 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

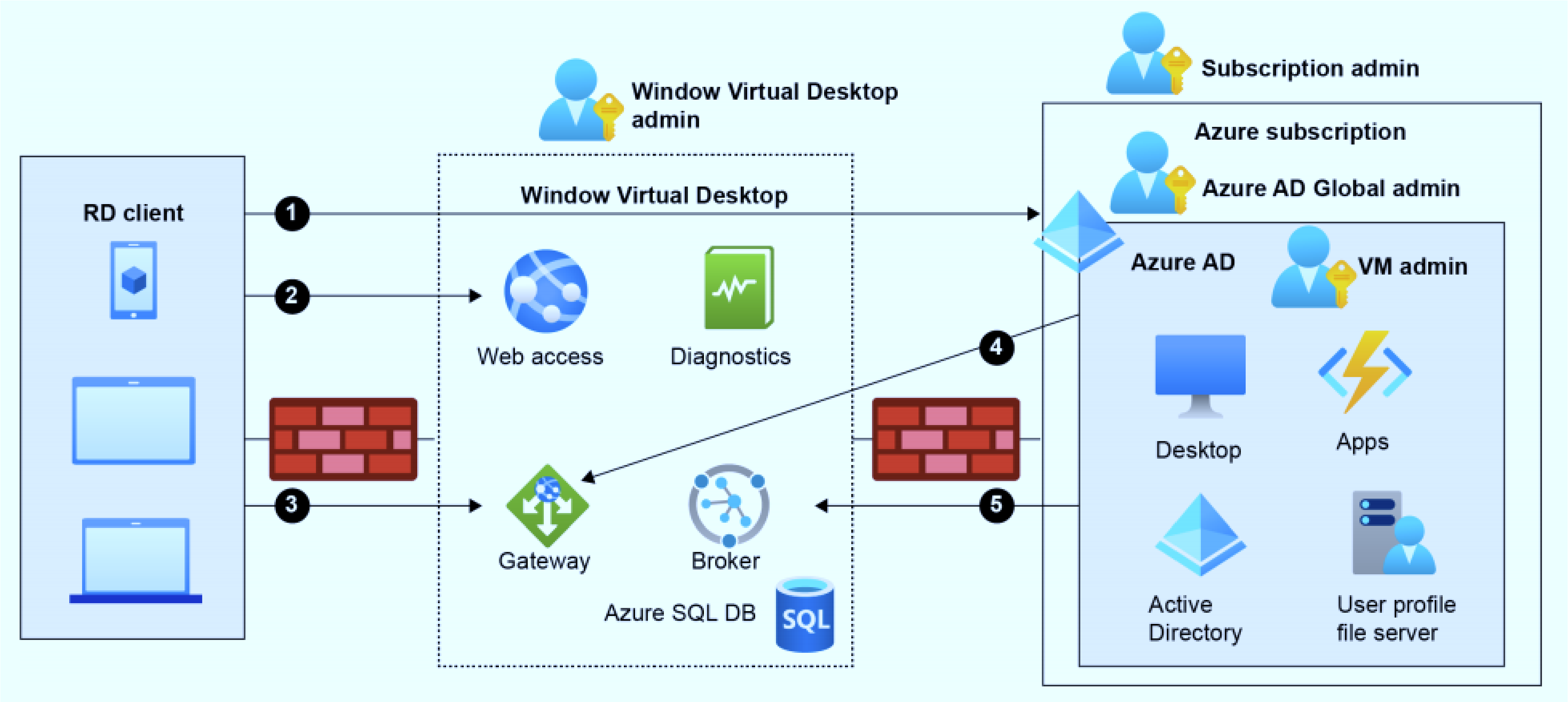
❑ configure Microsoft Defender for Endpoint

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

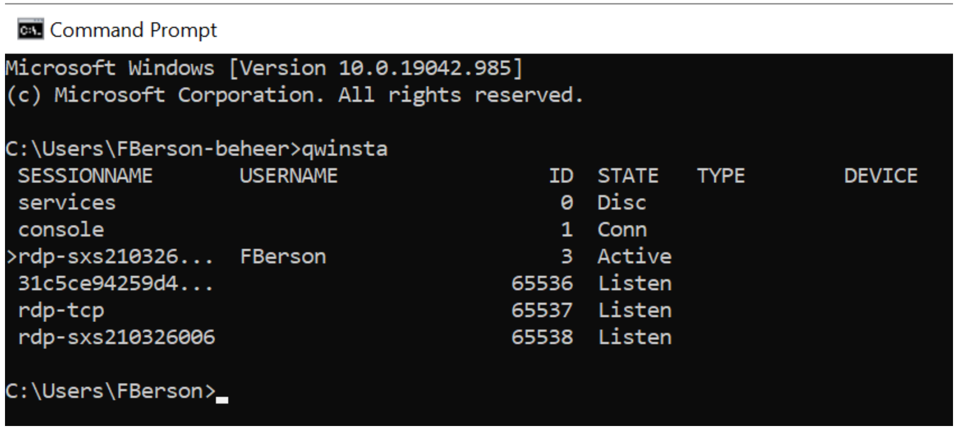
❑ Microsoft Endpoint Manager

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

Securing Network Access



Securing Network Access



Command Prompt

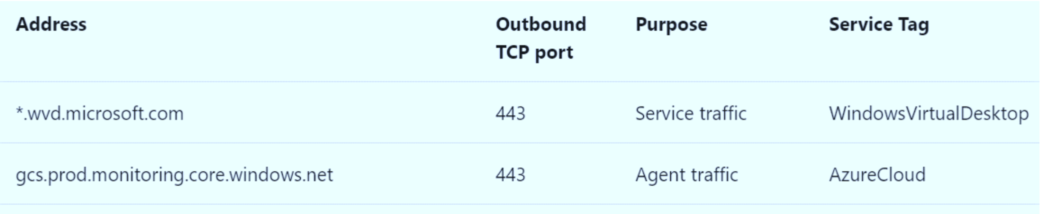
```
Microsoft Windows [Version 10.0.19042.985]
(c) Microsoft Corporation. All rights reserved.

C:\Users\FBerson-beheer>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>_
```

- ❑ AVD contains Reverse connect transport for establishing the remote session as well as for carrying the RDP traffic

- ❑ Use Service tags to simplify security for Azure VMs.

- Required URL Check tool: WVDAgentUrlTool.exe

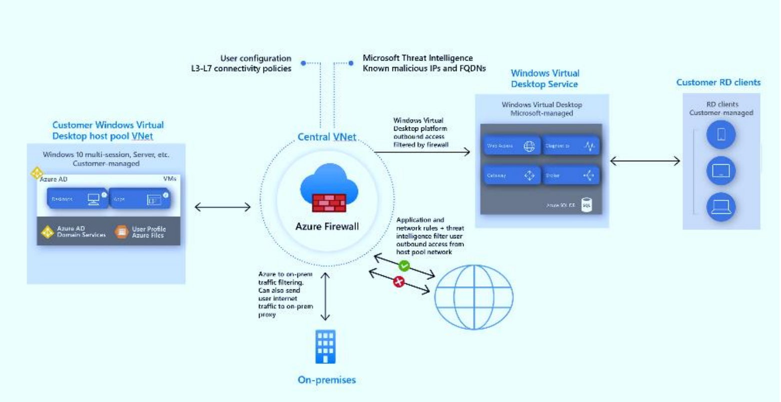
  https://docs.microsoft.com/en-us/azure/virtual-desktop/safe-url-list



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

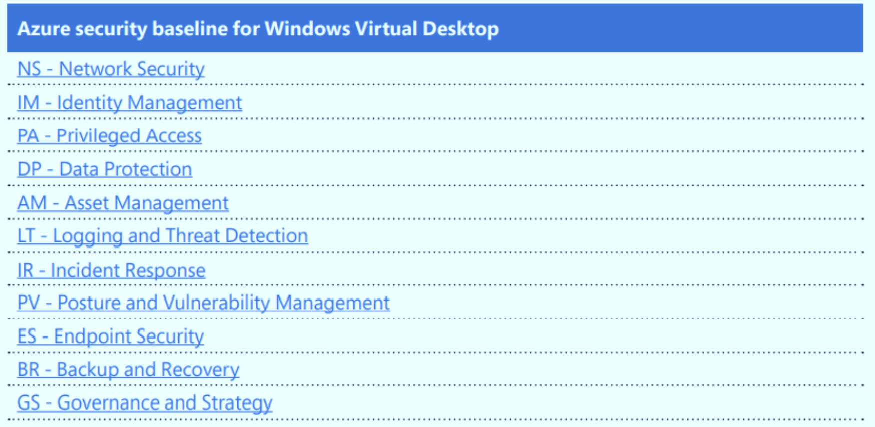

User configuration
L3-L7 connectivity policies
Microsoft Threat Intelligence
Known malicious IPs and FQDNs
Windows Virtual Desktop Service
Windows Virtual Desktop Microsoft-managed
Web Access
Diagnostics
Gateway
Broker
Azure SQL DB
Customer RD clients
RD clients Customer-managed
Customer Windows Virtual Desktop host pool VNet
Windows 10 multi-session, Server, etc. Customer-managed
Azure AD
VMs
Desktops
Apps
Azure AD Domain Services
User Profile Azure Files
Central VNet
Azure Firewall
Windows Virtual Desktop platform outbound access filtered by firewall
Application and network rules + threat intelligence filter user outbound access from host pool network
Azure to on-prem traffic filtering. Can also send user internet traffic to on-prem proxy
On-premises

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/

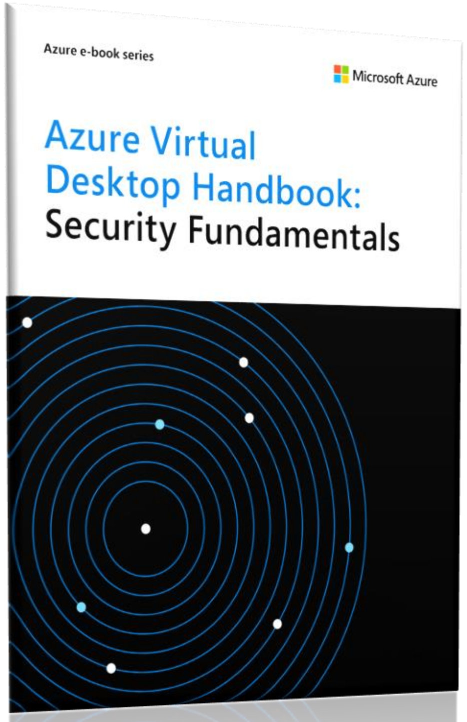
- □ Leverage Azure security baseline for Azure Virtual Desktop
  https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/windows-virtual-desktop-security-baseline



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

Call to action!

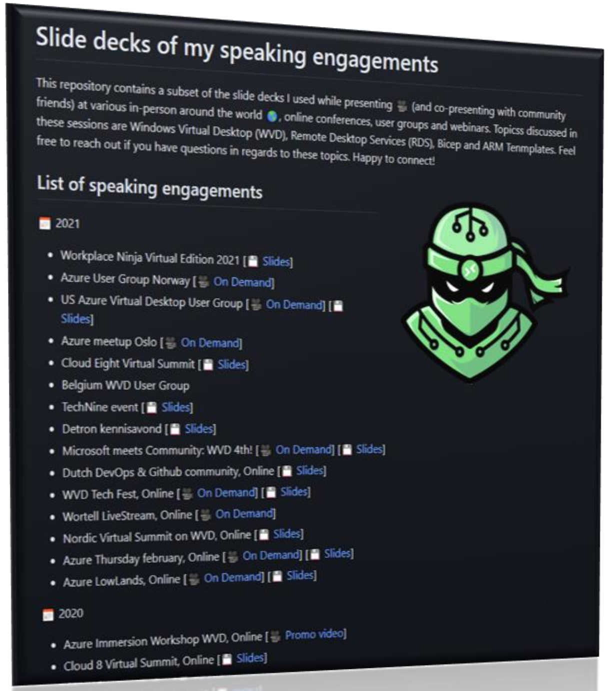


Azure e-book series

Microsoft Azure

Azure Virtual Desktop Handbook: Security Fundamentals

https://bit.ly/3fyiYuB



Slide decks of my speaking engagements

This repository contains a subset of the slide decks I used while presenting 🎥 (and co-presenting with community friends) at various in-person around the world 🌍, online conferences, user groups and webinars. Topicss discussed in these sessions are Windows Virtual Desktop (WVD), Remote Desktop Services (RDS), Bicep and ARM Tenmplates. Feel free to reach out if you have questions in regards to these topics. Happy to connect!

List of speaking engagements

📅 2021

- Workplace Ninja Virtual Edition 2021 [💾 Slides]
- Azure User Group Norway [🎥 On Demand]
- US Azure Virtual Desktop User Group [🎥 On Demand] [💾 Slides]
- Azure meetup Oslo [🎥 On Demand]
- Cloud Eight Virtual Summit [💾 Slides]
- Belgium WVD User Group
- TechNine event [💾 Slides]
- Detron kennisavond [💾 Slides]
- Microsoft meets Community: WVD 4th! [🎥 On Demand] [💾 Slides]
- Dutch DevOps & Github community, Online [💾 Slides]
- WVD Tech Fest, Online [🎥 On Demand] [💾 Slides]
- Wortell LiveStream, Online [🎥 On Demand]
- Nordic Virtual Summit on WVD, Online [💾 Slides]
- Azure Thursday february, Online [🎥 On Demand] [💾 Slides]
- Azure LowLands, Online [🎥 On Demand] [💾 Slides]

📅 2020

- Azure Immersion Workshop WVD, Online [🎥 Promo video]
- Cloud 8 Virtual Summit, Online [💾 Slides]

https://github.com/fberson/Slidedecks

THANK YOU!

Freek Berson
@fberson
freek@wortell.nl
github.com/fberson
TheMicrosoftPlatform.net