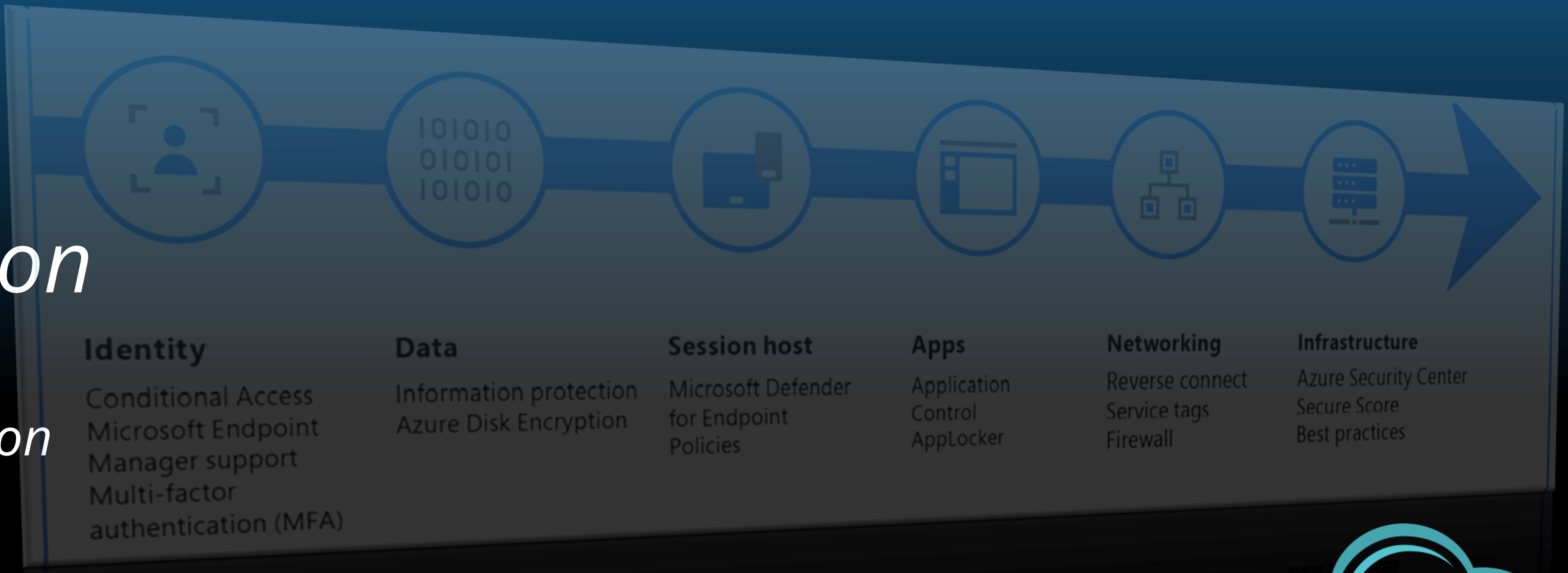
Windows Virtual Desktop does not use port 3389, so we’re secure…. *Right?*

Freek Berson

@fberson

github.com/fberson

Microsoft MVP



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

Thanks to our sponsors!

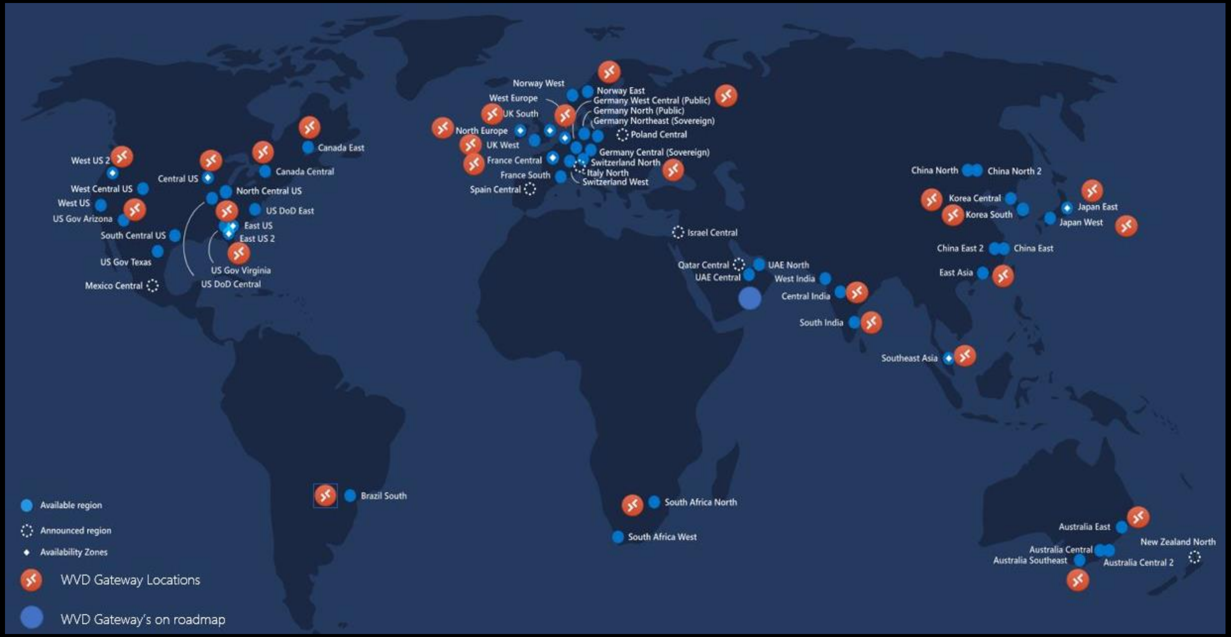
itpoint

365

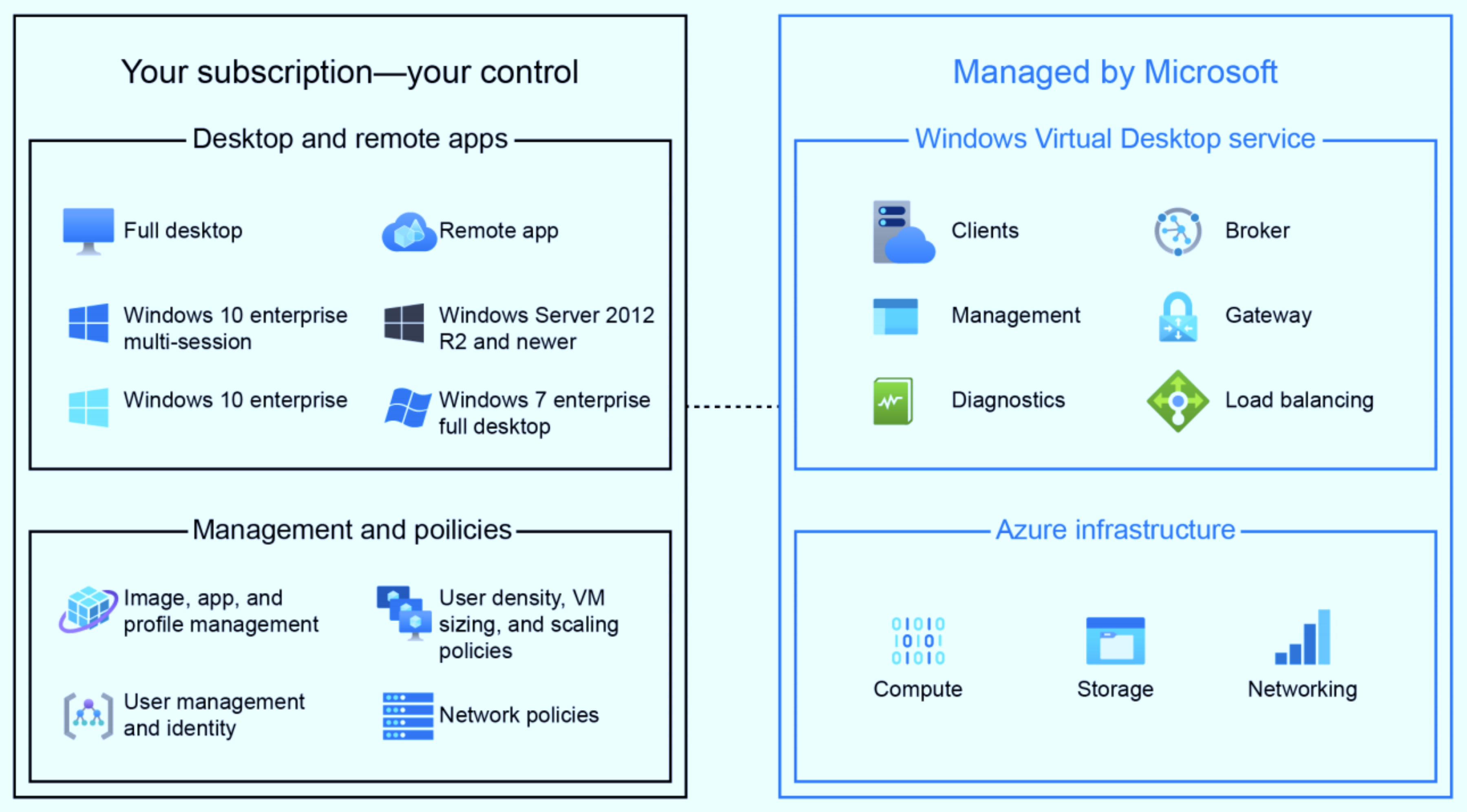
ScriptRunner®

Windows Virtual Desktop

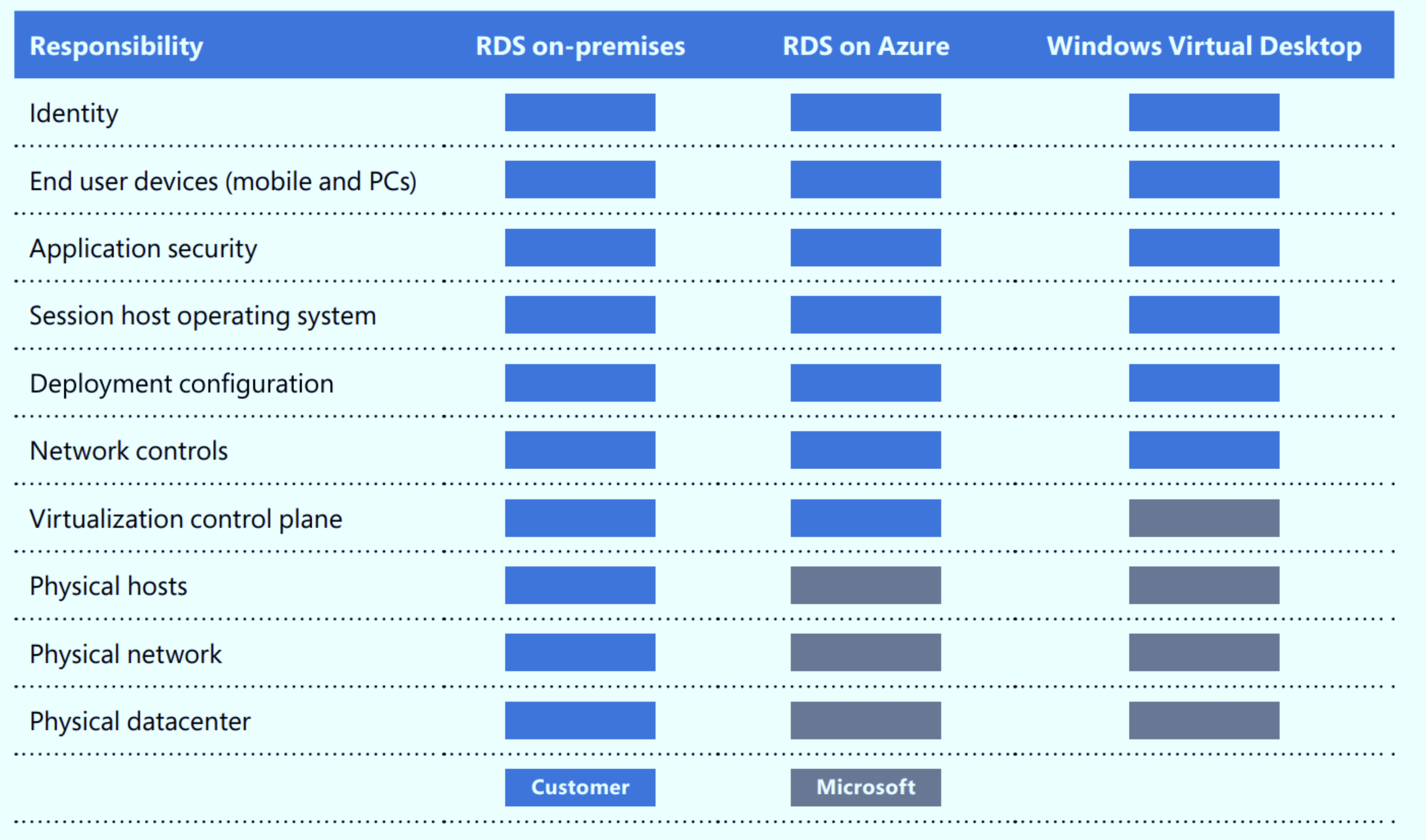
- Provide a full-desktop, authenticated experience for users at every level
- Reduce the costs and time spent managing on-premises infrastructure
- Simplify management, provisioning, and access to corporate data and apps
- Deploy and scale in minutes



Architecture

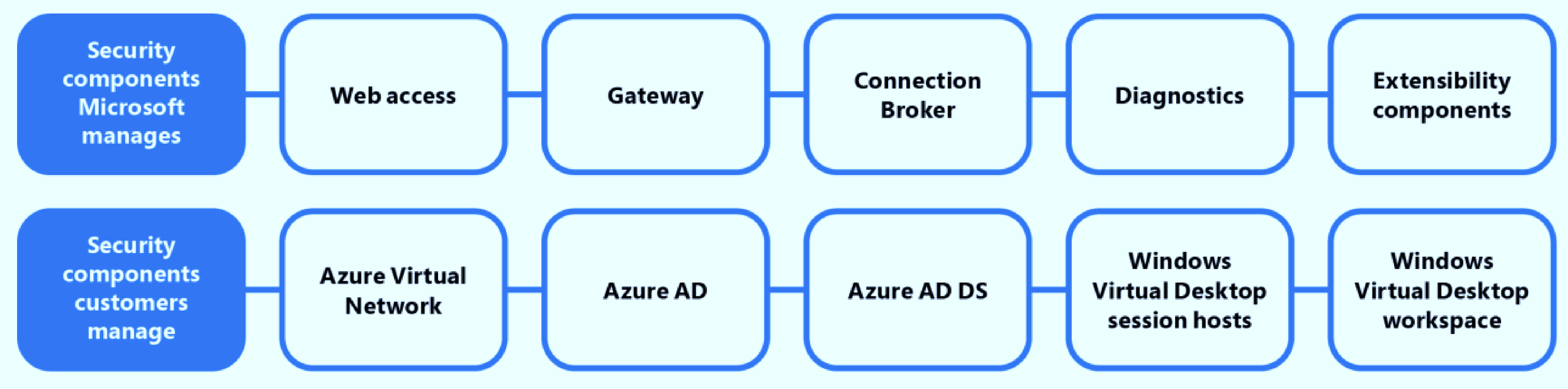

Your subscription—your control
Desktop and remote apps
Full desktop
Remote app
Windows 10 enterprise multi-session
Windows Server 2012 R2 and newer
Windows 10 enterprise
Windows 7 enterprise full desktop
Management and poilicies
Image, app, and profile management
User density, VM sizing, and scaling policies
User management and identity
Network policies
Managed by Microsoft
Windows Virtual Desktop service
Clients
Broker
Management
Gateway
Diagnostics
Load balancing
Azure infrastructure
Compute
Storage
Networking

Responsibilities



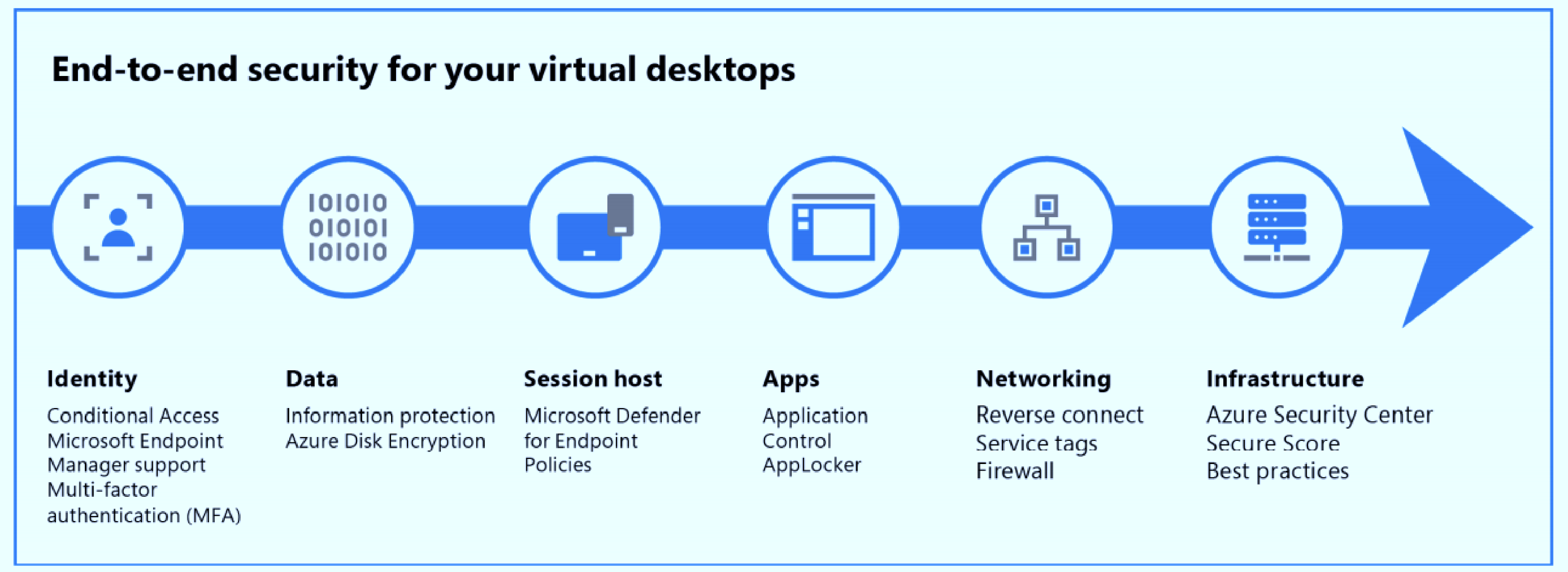
Responsibility	RDS on-premises	RDS on Azure	Windows Virtual Desktop
Identity	🟦	🟦	🟦
End user devices (mobile and PCs)	🟦	🟦	🟦
Application security	🟦	🟦	🟦
Session host operating system	🟦	🟦	🟦
Deployment configuration	🟦	🟦	🟦
Network controls	🟦	🟦	🟦
Virtualization control plane	🟦	🟦	▨
Physical hosts	🟦	▨	▨
Physical network	🟦	▨	▨
Physical datacenter	🟦	▨	▨
	🟦 Customer	▨ Microsoft	

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	Windows Virtual Desktop session hosts	Windows 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

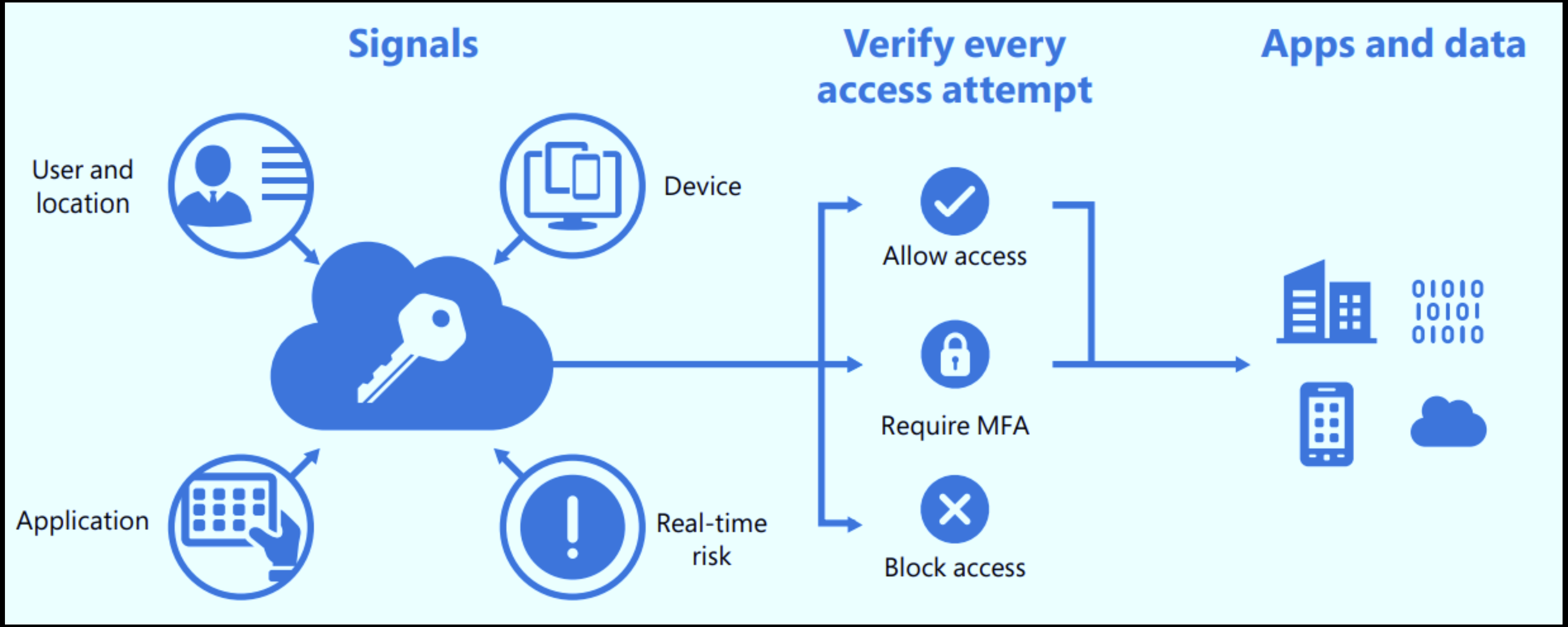
Securing Identities

❑ 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.

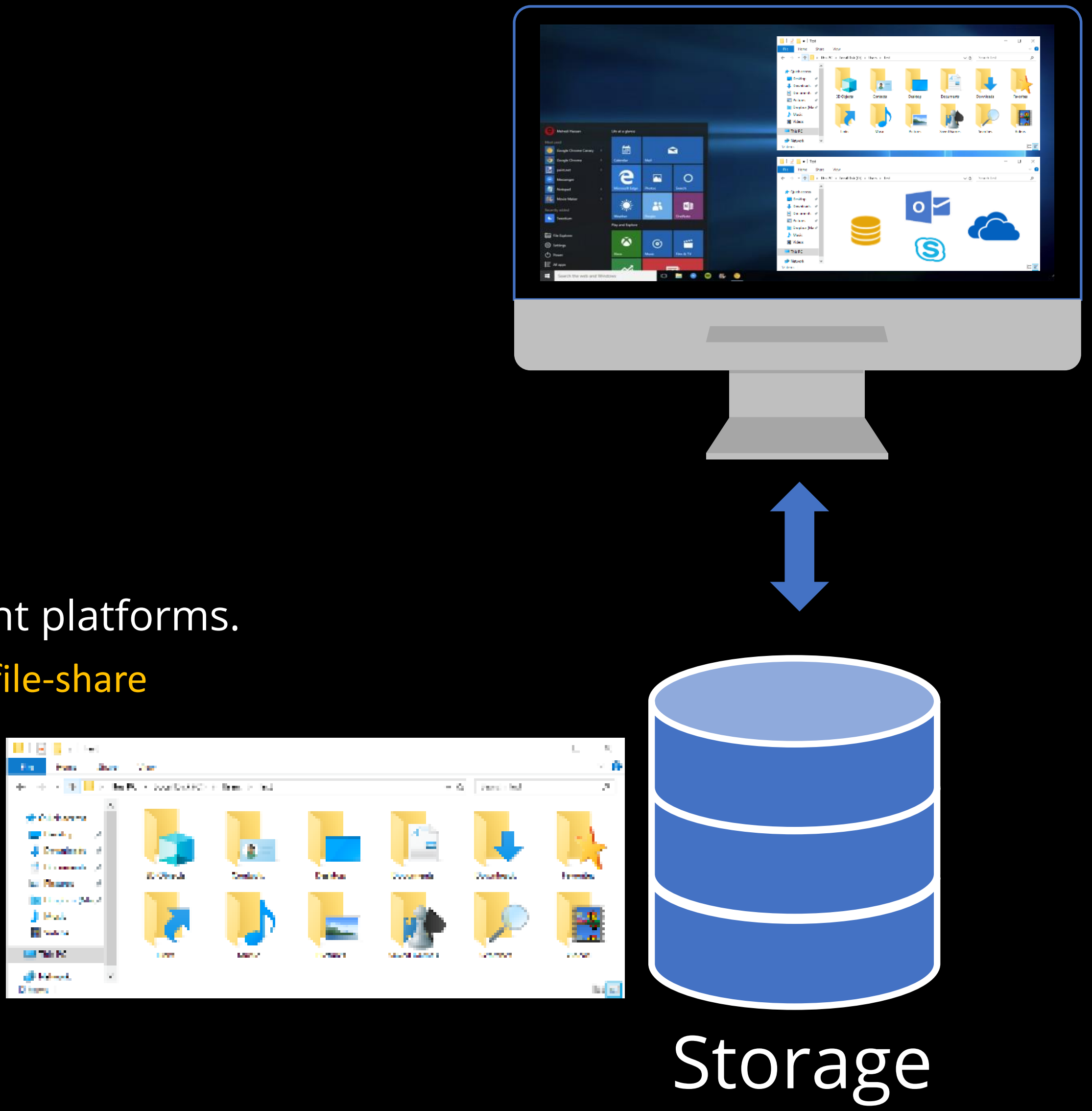
https://docs.microsoft.com/en-gb/azure/virtual-desktop/diagnostics-log-analytics

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.

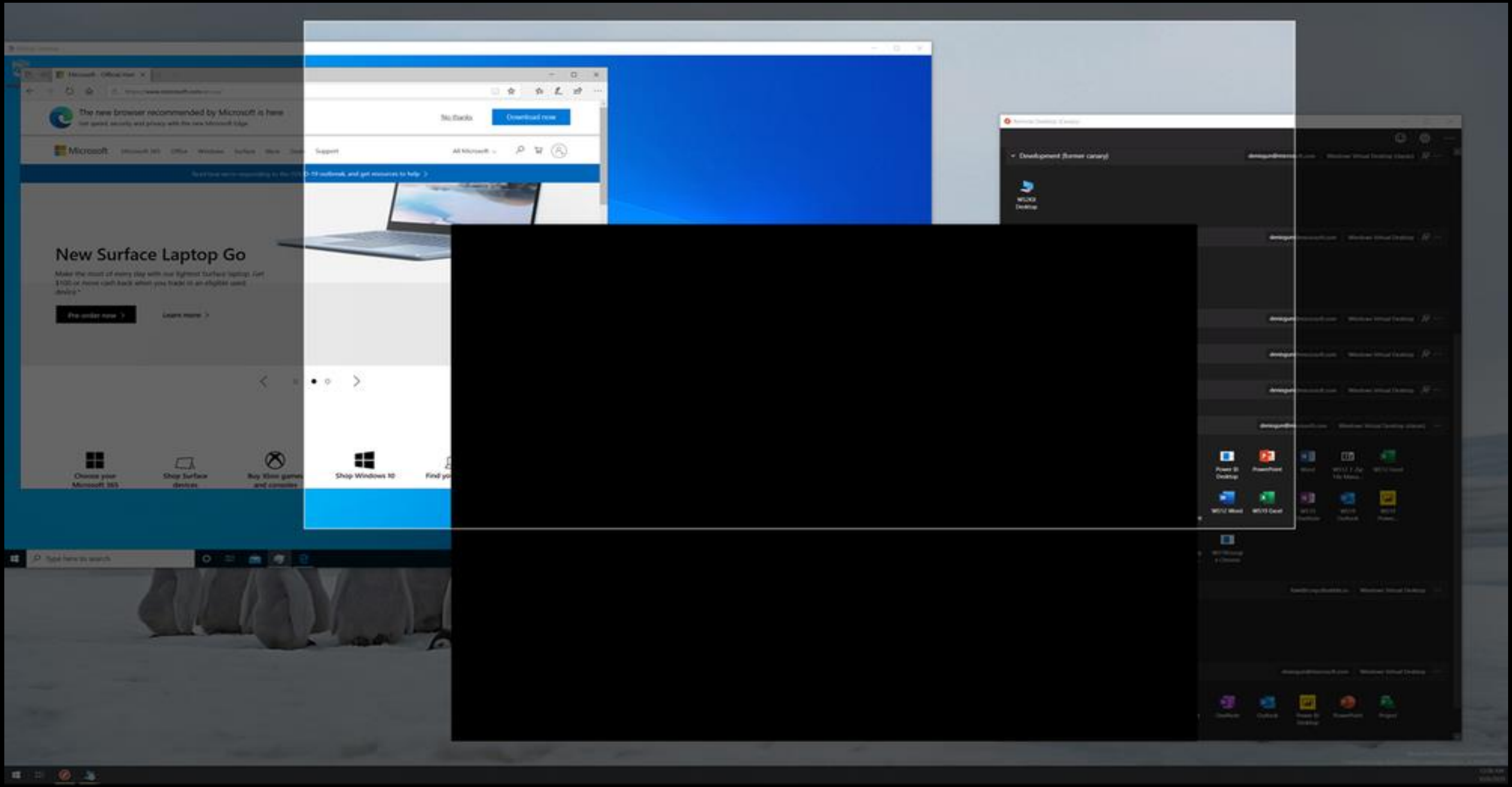
https://docs.microsoft.com/en-gb/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview

□ Consider Application Masking can also be used to provide security for applications.

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

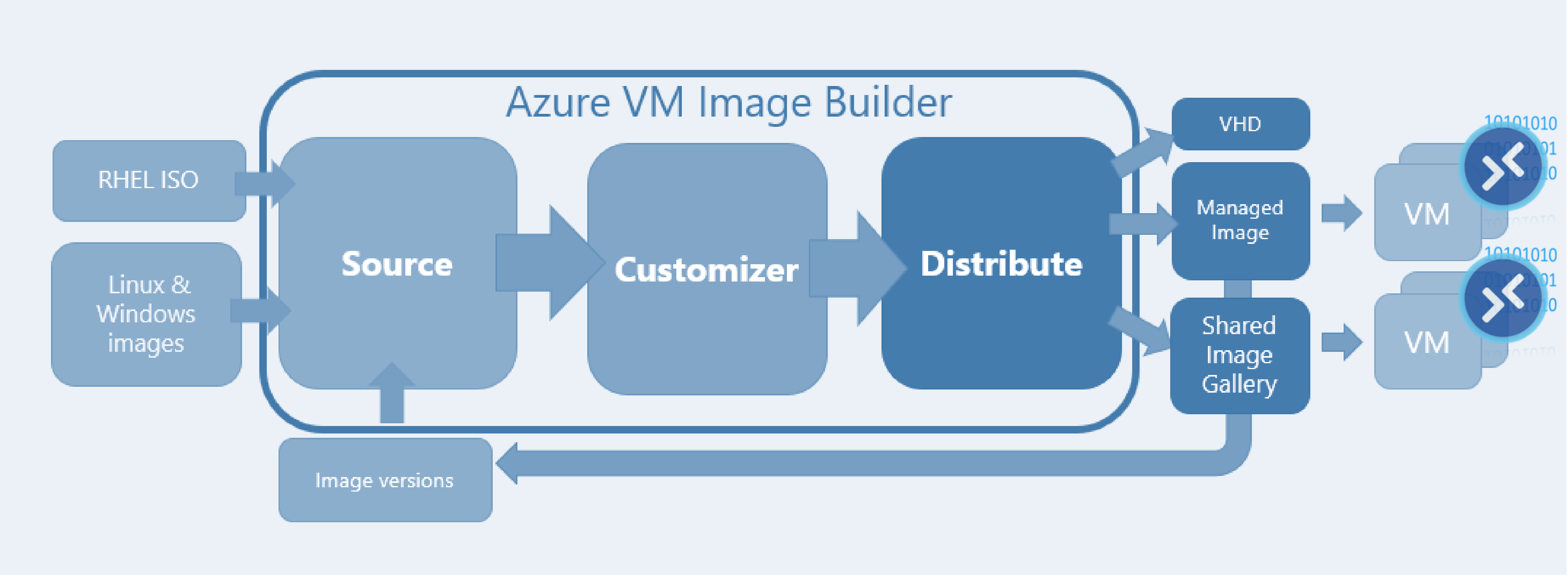
□ Demo!

Screen Capture Protection


The new browser recommended by Microsoft is here
Microsoft
No thanks
Download now
Support
New Surface Laptop Go
Pre-order now >
Learn more >
Choose your Microsoft 365
Shop Surface devices
Buy Xbox games and consoles
Shop Windows 10
Development (former canary)

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

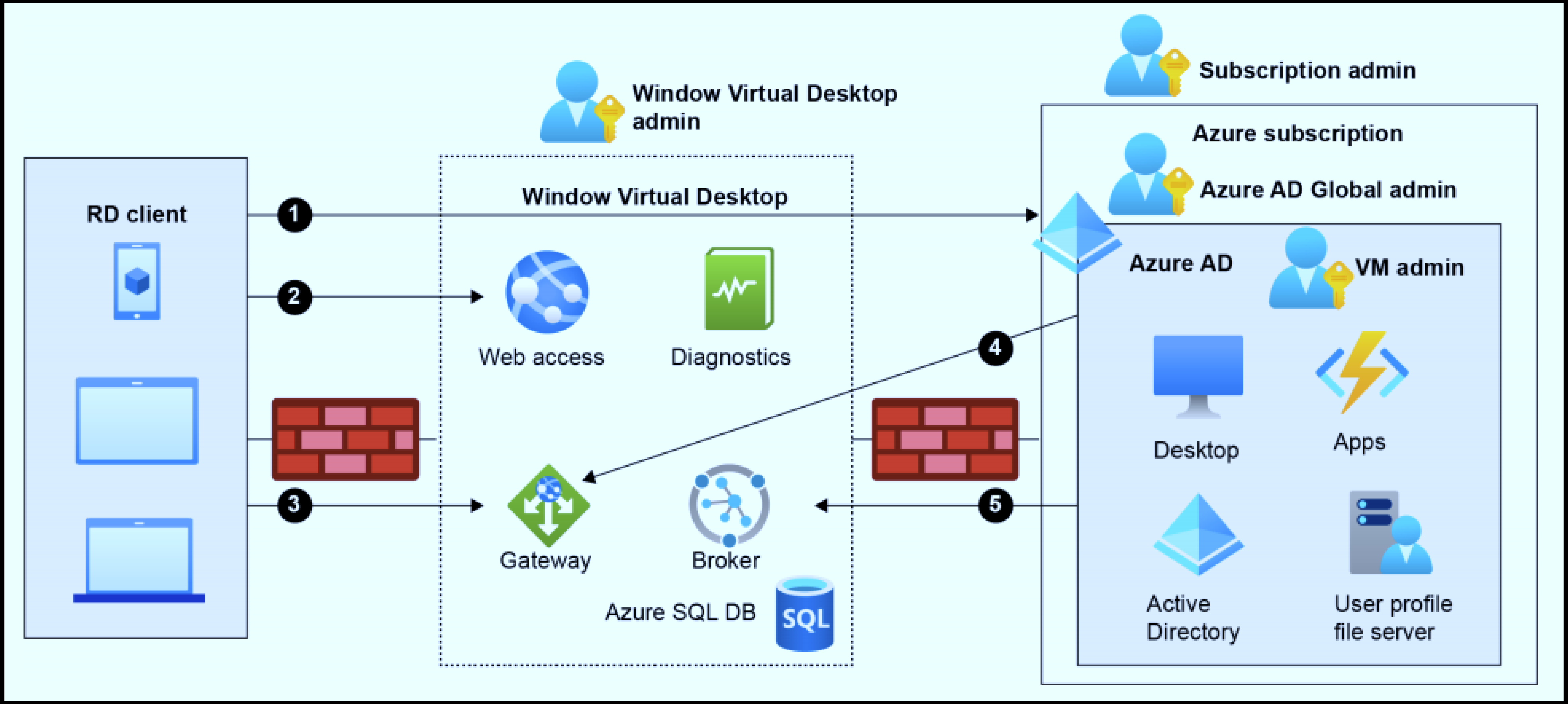
❑ configure Microsoft Defender for Endpoint

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

❑ Microsoft Endpoint Manager

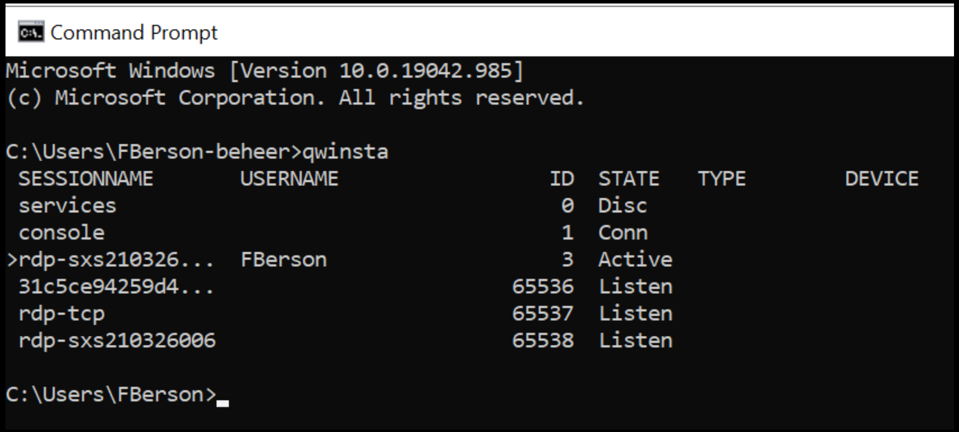
https://docs.microsoft.com/en-gb/mem/intune/fundamentals/tutorial-walkthrough-endpoint-manager

Securing Network Access



Windows Virtual Desktop does not use port 3389, so we're secure…. Right?

Securing Network Access



Command Prompt

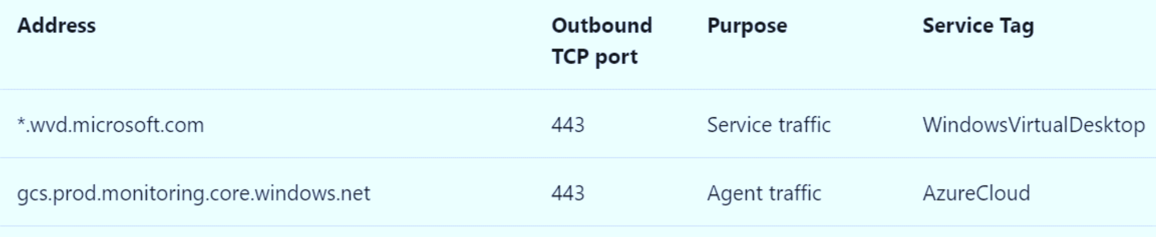
```
Microsoft Windows [Version 10.0.19042.985]
(c) Microsoft Corporation. All rights reserved.

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>_
```

- ❑ WVD contain 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

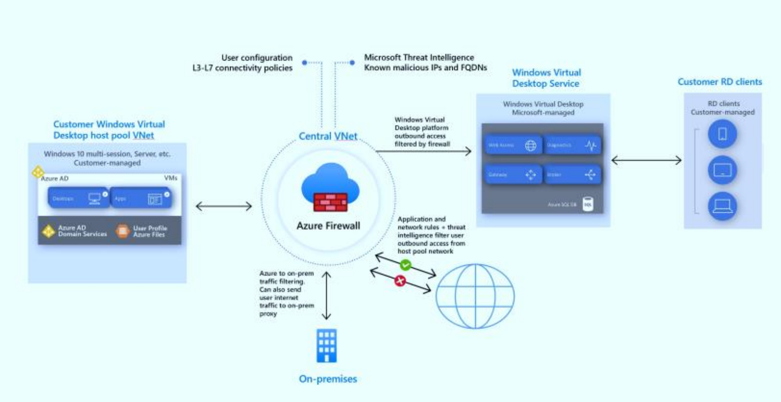
https://docs.microsoft.com/en-us/azure/virtual-desktop/safe-url-list



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
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
Windows Virtual Desktop Service
Windows Virtual Desktop
Microsoft-managed
Web Access
Diagnostics
Gateway
Broker
Azure SQL DB
Customer RD clients
RD clients
Customer-managed
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

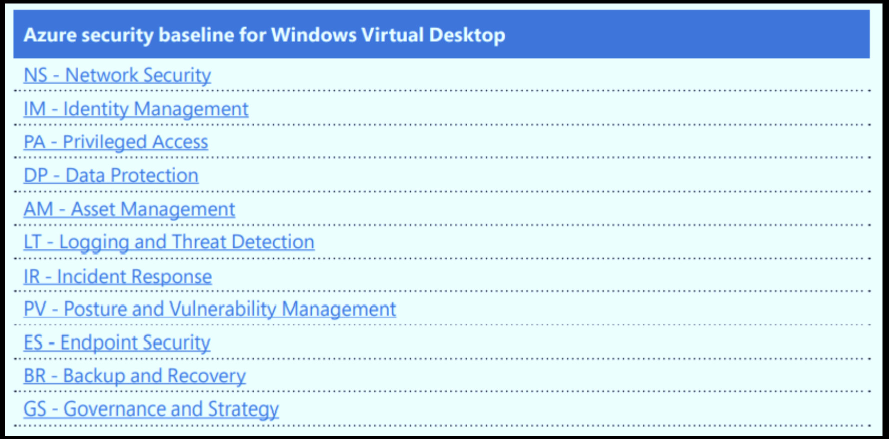
Windows Virtual Desktop does not use port 3389, so we're secure…. Right?

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 Windows Virtual Desktop diagnostics.
  https://azure.microsoft.com/en-gb/services/azure-sentinel/

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

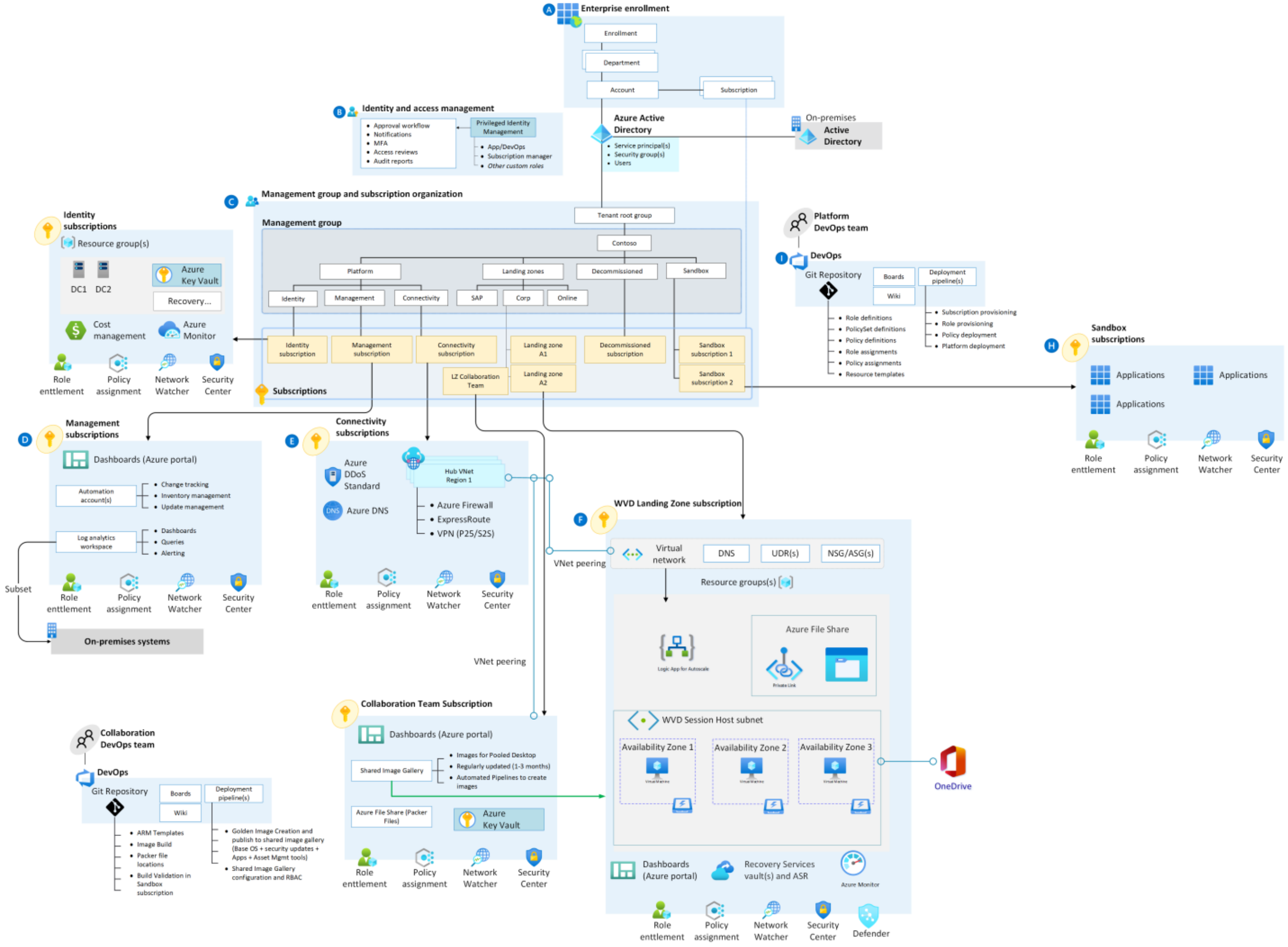


Azure security baseline for Windows Virtual Desktop

- 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

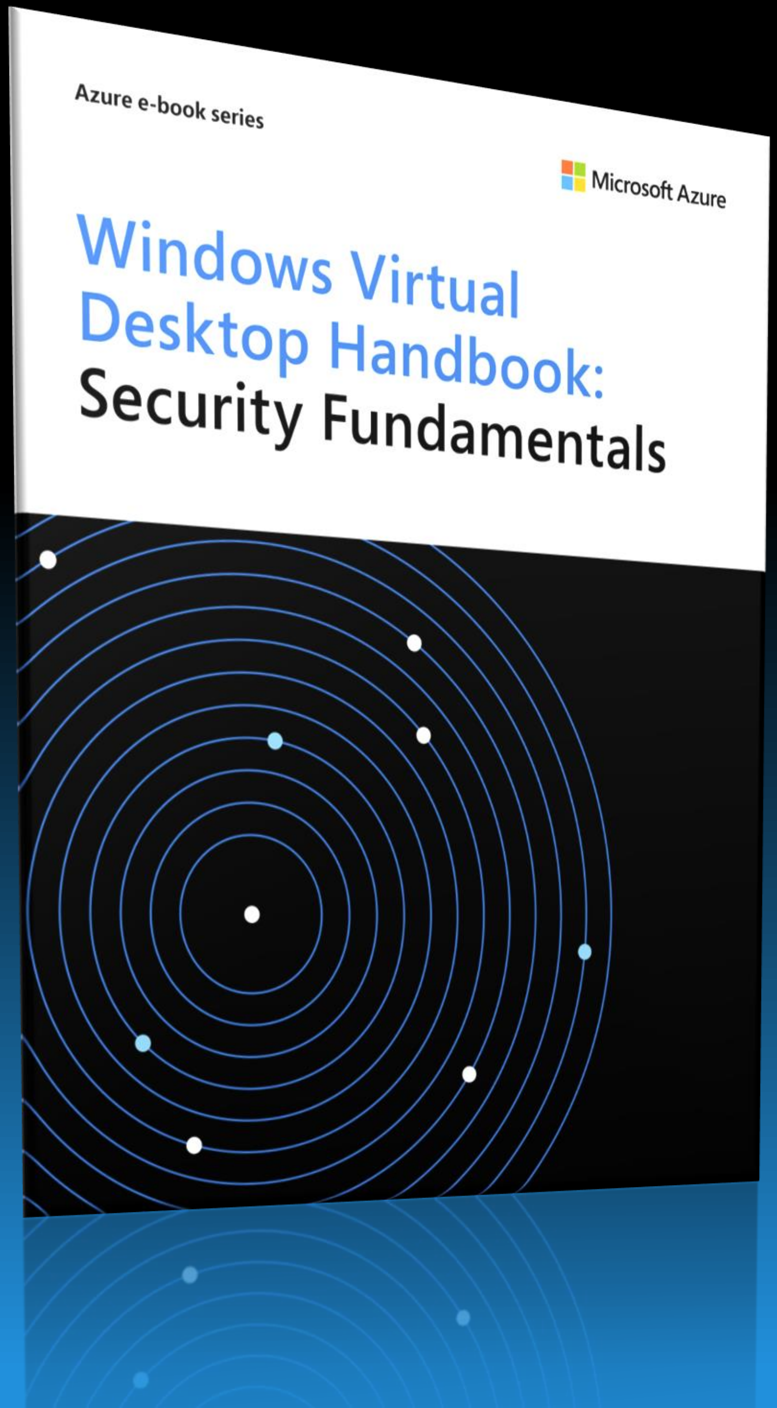
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/scenarios/wvd/enterprise-scale-landing-zone



CALL TO ACTION

https://azure.microsoft.com/en-gb/resources/windows-virtual-desktop-handbook-security-fundamentals/

https://bit.ly/3fyiYuB



Azure e-book series

Microsoft Azure

Windows Virtual Desktop Handbook: Security Fundamentals

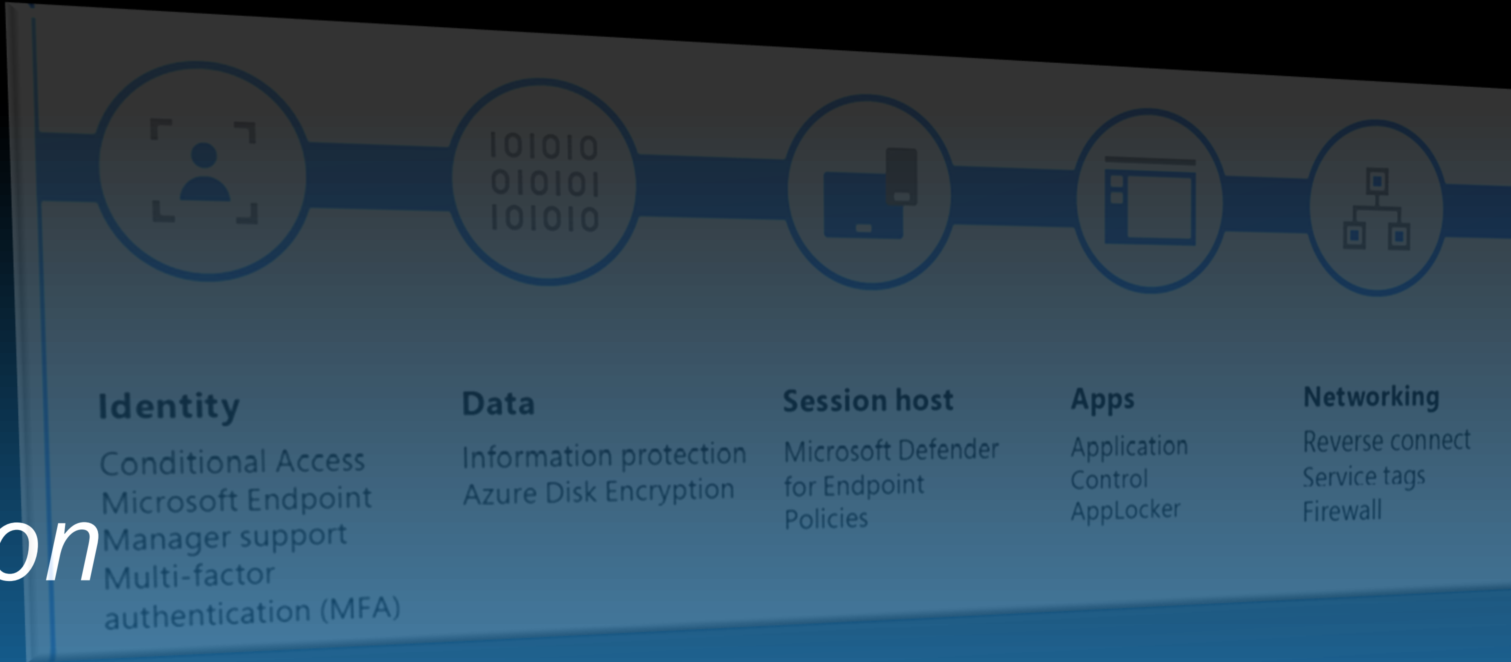
THANK YOU!

Freek Berson

@fberson

github.com/fberson

Microsoft MVP



Identity

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

Data

Information protection
Azure Disk Encryption

Session host

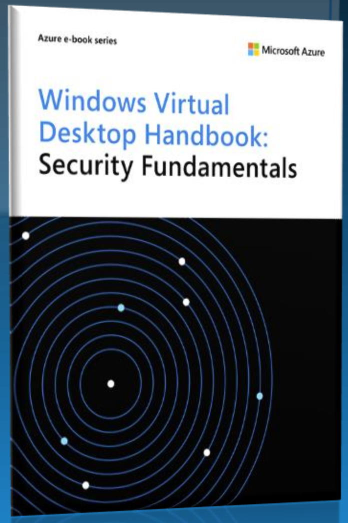
Microsoft Defender for Endpoint
Policies

Apps

Application Control
AppLocker

Networking

Reverse connect
Service tags
Firewall



Azure e-book series

Microsoft Azure

Windows Virtual Desktop Handbook: Security Fundamentals

https://bit.ly/3fyiYuB