Mindtree
A Larsen & Toubro Group Company

Securing Windows Virtual Desktop

Welcome to possible

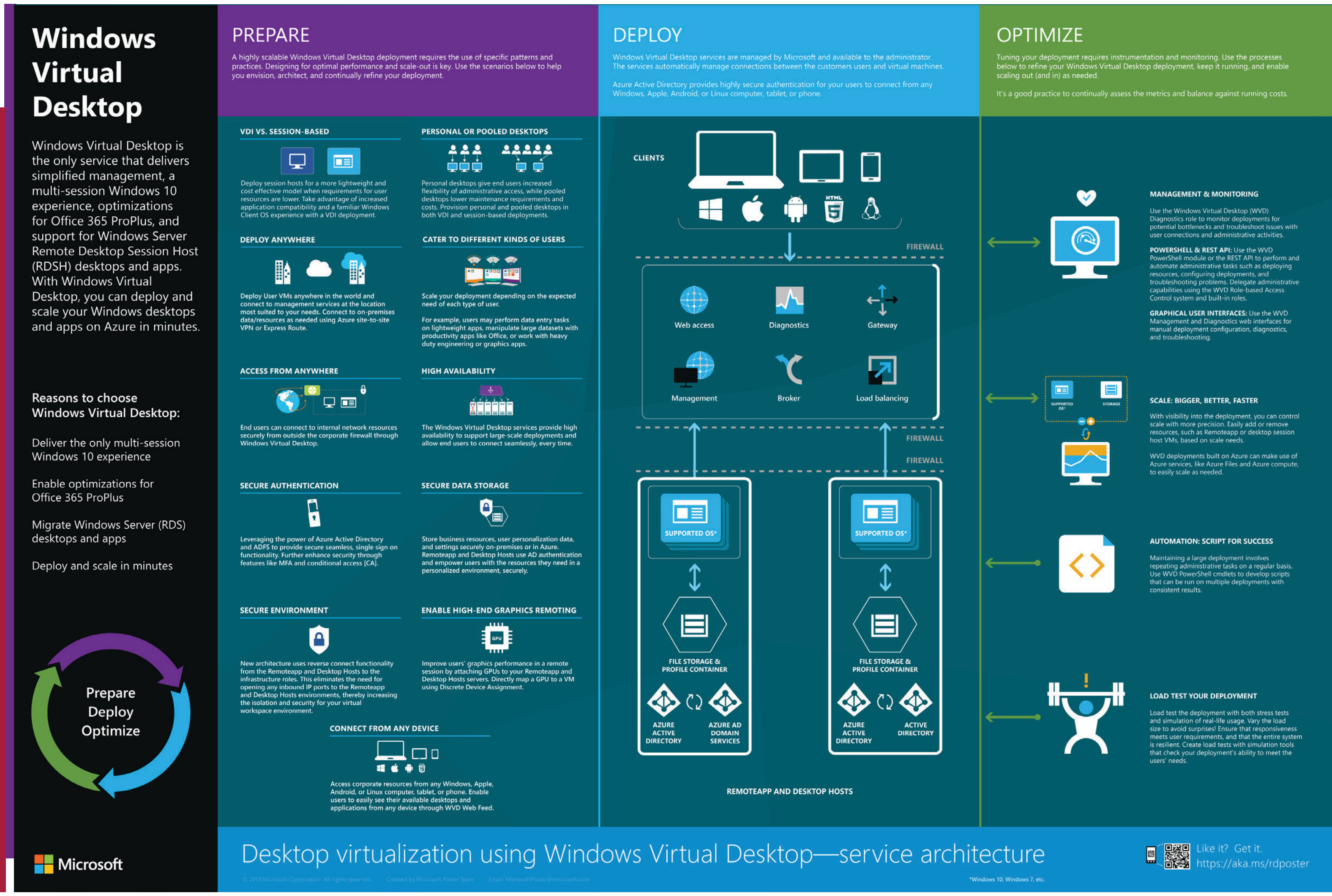
A Mindtree Point of View

Table of Contents

WINDOWS VIRTUAL DESKTOP

WVD helps us to manage the virtual machine desktop and application as a virtualization platform.
WVD is an Azure service, and it's developed for providing secure remote work.
WVD supports (Windows, macOS, Android, iOS, and HTML5)

Windows Virtual Desktop – Service Architecture



Windows Virtual Desktop

Windows Virtual Desktop is the only service that delivers simplified management, a multi-session Windows 10 experience, optimizations for Office 365 ProPlus, and support for Windows Server Remote Desktop Session Host (RDSH) desktops and apps. With Windows Virtual Desktop, you can deploy and scale your Windows desktops and apps on Azure in minutes.

Reasons to choose Windows Virtual Desktop:

Deliver the only multi-session Windows 10 experience

Enable optimizations for Office 365 ProPlus

Migrate Windows Server (RDS) desktops and apps

Deploy and scale in minutes

Prepare
Deploy
Optimize

Microsoft

PREPARE

A highly scalable Windows Virtual Desktop deployment requires the use of specific patterns and practices. Designing for optimal performance and scale-out is key. Use the scenarios below to help you envision, architect, and continually refine your deployment.

VDI VS. SESSION-BASED

Deploy session hosts for a more lightweight and cost effective model when requirements for user resources are lower. Take advantage of increased application compatibility and a familiar Windows Client OS experience with a VDI deployment.

PERSONAL OR POOLED DESKTOPS

Personal desktops give end users increased flexibility of administrative access, while pooled desktops lower maintenance requirements and costs. Provision personal and pooled desktops in both VDI and session-based deployments.

DEPLOY ANYWHERE

Deploy User VMs anywhere in the world and connect to management services at the location most suited to your needs. Connect to on-premises data/resources as needed using Azure site-to-site VPN or Express Route.

CATER TO DIFFERENT KINDS OF USERS

Scale your deployment depending on the expected need of each type of user.

For example, users may perform data entry tasks on lightweight apps, manipulate large datasets with productivity apps like Office, or work with heavy duty engineering or graphics apps.

ACCESS FROM ANYWHERE

End users can connect to internal network resources securely from outside the corporate firewall through Windows Virtual Desktop.

HIGH AVAILABILITY

The Windows Virtual Desktop services provide high availability to support large-scale deployments and allow end users to connect seamlessly, every time.

SECURE AUTHENTICATION

Leveraging the power of Azure Active Directory and ADFS to provide secure seamless, single sign on functionality. Further enhance security through features like MFA and conditional access [CA].

SECURE DATA STORAGE

Store business resources, user personalization data, and settings securely on-premises or in Azure. Remoteapp and Desktop Hosts use AD authentication and empower users with the resources they need in a personalized environment, securely.

SECURE ENVIRONMENT

New architecture uses reverse connect functionality from the Remoteapp and Desktop Hosts to the infrastructure roles. This eliminates the need for opening any inbound IP ports to the Remoteapp and Desktop Hosts environments, thereby increasing the isolation and security for your virtual workspace environment.

ENABLE HIGH-END GRAPHICS REMOTING

Improve users' graphics performance in a remote session by attaching GPUs to your Remoteapp and Desktop Hosts servers. Directly map a GPU to a VM using Discrete Device Assignment.

CONNECT FROM ANY DEVICE

Access corporate resources from any Windows, Apple, Android, or Linux computer, tablet, or phone. Enable users to easily see their available desktops and applications from any device through WVD Web Feed.

DEPLOY

Windows Virtual Desktop services are managed by Microsoft and available to the administrator. The services automatically manage connections between the customers users and virtual machines.

Azure Active Directory provides highly secure authentication for your users to connect from any Windows, Apple, Android, or Linux computer, tablet, or phone.

OPTIMIZE

Tuning your deployment requires instrumentation and monitoring. Use the processes below to refine your Windows Virtual Desktop deployment, keep it running, and enable scaling out (and in) as needed.

It's a good practice to continually assess the metrics and balance against running costs.

MANAGEMENT & MONITORING

Use the Windows Virtual Desktop (WVD) Diagnostics role to monitor deployments for potential bottlenecks and troubleshoot issues with user connections and administrative activities.

POWERSHELL & REST API: Use the WVD PowerShell module or the REST API to perform and automate administrative tasks such as deploying resources, configuring deployments, and troubleshooting problems. Delegate administrative capabilities using the WVD Role-based Access Control system and built-in roles.

GRAPHICAL USER INTERFACES: Use the WVD Management and Diagnostics web interfaces for manual deployment configuration, diagnostics, and troubleshooting.

SCALE: BIGGER, BETTER, FASTER

With visibility into the deployment, you can control scale with more precision. Easily add or remove resources, such as Remoteapp or desktop session host VMs, based on scale needs.

WVD deployments built on Azure can make use of Azure services, like Azure Files and Azure compute, to easily scale as needed.

AUTOMATION: SCRIPT FOR SUCCESS

Maintaining a large deployment involves repeating administrative tasks on a regular basis. Use WVD PowerShell cmdlets to develop scripts that can be run on multiple deployments with consistent results.

LOAD TEST YOUR DEPLOYMENT

Load test the deployment with both stress tests and simulation of real-life usage. Vary the load size to avoid surprises! Ensure that responsiveness meets user requirements, and that the entire system is resilient. Create load tests with simulation tools that check your deployment's ability to meet the users' needs.

Desktop virtualization using Windows Virtual Desktop—service architecture

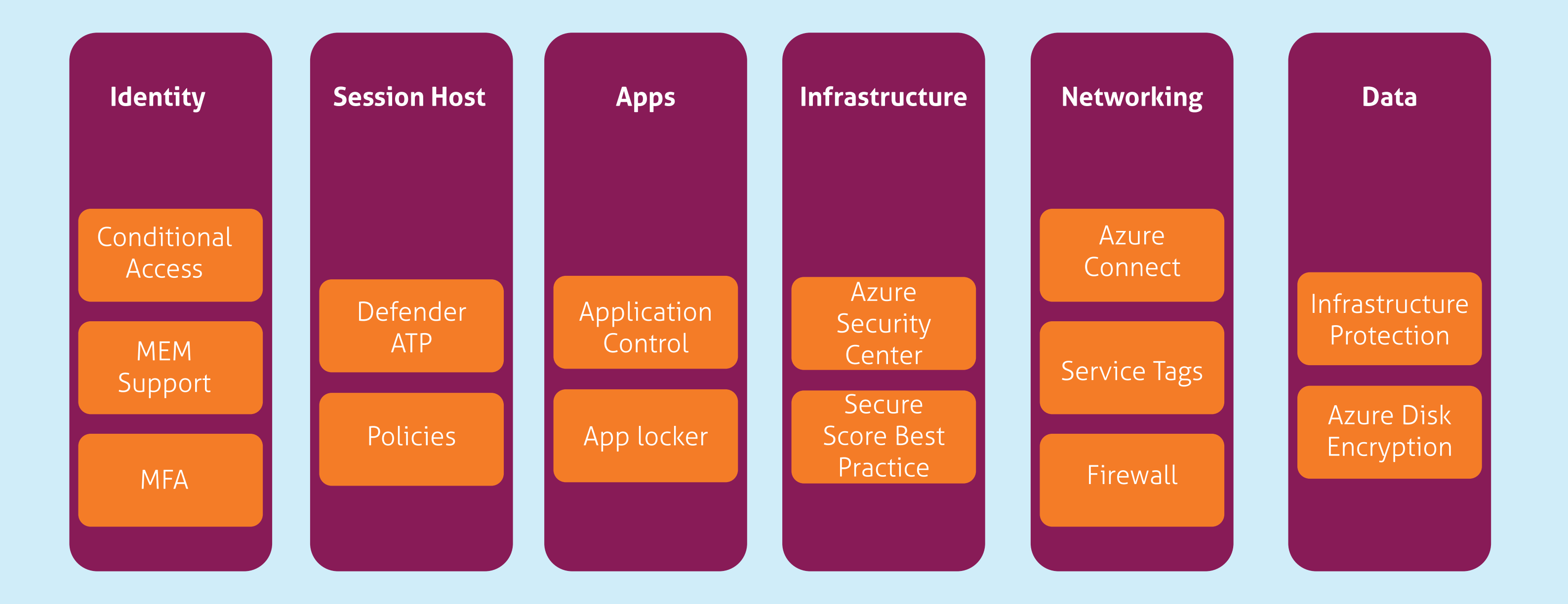
Created by Microsoft Poster Team Email: MicrosoftPoster@microsoft.com

*Windows 10, Windows 7, etc.

Like it? Get it.
https://aka.ms/rdposter

Source Image Reference: Microsoft

END TO END SECURITY FOR YOUR VIRTUAL DESKTOPS



Identity	Session Host	Apps	Infrastructure	Networking	Data
Conditional Access	Defender ATP	Application Control	Azure Security Center	Azure Connect	Infrastructure Protection
MEM Support	Policies	App locker	Secure Score Best Practice	Service Tags	Azure Disk Encryption
MFA				Firewall	

SECURING OS IMAGES

While creating the WVD host pool, you can select the windows multi-session images, or else you can use the hardened OS images as per your organization's security standards to meet your requirements and these images are placed in the image gallery.

IDENTITY SECURITY

Enable Multifactor Authentication and Conditional Access

Azure AD must be configured by MFA to protect against credentials leaking, fishing attacks and to ensure enabled conditional access to provide more security for user account login.

MEM Support for WVD Machines

Customers can integrate with the Windows Virtual Desktop for deploying Applications in a secure way, controlling devices, efficiently deploying their deployments, and accelerating the move to a secure remote work solution.

SESSION HOST SECURITY

Session Host has a number of virtual machines inside the Azure subscription and VNET, and also as part of the host pool. To keep the Session host more secure, it requires updates in a timely manner.

Enable Microsoft-Defender ATP

To ensure all the information inside your Virtual Machines is secure and comes with the additional feature named Next Generation Anti-Virus, which is enabled by default.

Enable Endpoint Detection and response

To secure the deployment from the software, ensure endpoint protection is enabled in all the session hosts.

Note: For Antivirus, the existing E3 license is enough, but to enable EDR it requires an E5 license. Kindly install an endpoint detection and response (EDR) to get advanced detection and response capabilities.

Server operating systems, you can integrate or enable this with the Azure Security Center, as well as by installing an EDR product.

Client operating systems, you can install Defender ATP or other third-party tools to endpoints.

Threat Vulnerability Management

Threat Vulnerability helps to find the software vulnerabilities, which exist in the operating system and applications to make a secure environment. Azure security center will help you analyze the vulnerabilities caused by the operating systems and use Defender ATP for your desktop operating system to manage the threat and vulnerability.

Patch Software Vulnerabilities

Ensure all Virtual machines are up to date and also ensure security updates are installed or re-deployed using the latest gallery image (Microsoft updates gallery image every month on Tuesday).

Group Policies

Once the WVD host pool has joined AD, then you have full control over group policy options, and you can also enforce the policies through the GPO.

APP SECURITY

AppLocker

It helps you control the apps and files which can be run by the users, and you can also create rules based on the file path and hash to provide more security.

Application Control

Similar to AppLocker but it provides control over which driver and application can run.

NETWORKING SECURITY

Reverse Connect

To setup RDP on WVD, we recommend not to configure any inbound ports however, the communication will happen through TCP (HTTPS).

NSG Firewall

NGSs have a default route, and security can be controlled through the firewall itself. If it requires NSGs you can use them as default outbound ports such as TCP/UDP 53 – DNS, TCP 389 – LDAP, TCP 445 – SMB, TCP 443 – HTTPS, and also recommends no need of inbound connectivity for WVD.

NSG Firewall service tags

you can limit the network traffic and WVD traffic with service tags.

Azure Firewall helps you lock your WVD environment and also filters the outbound traffic. Consider the Azure Firewall for application-level protection with the WVD FQDN tag. Outbound internet access should be provided for WVD service to operate properly which is required for end users. Virtual Machine created by you in the WVD has access to multiple Fully Qualified Domain Names (FQDNs) to function properly. Azure firewalls help to simplify the windows virtual desktop FQDN Tag configuration.

INFRASTRUCTURE SECURITY

Azure Security Center

WVD infrastructure elements should be integrated into Azure Security Center for threat detection, patch management, security alerts, and Defender-ATP. Azure Security Center will save time and reduce costs and provide security monitoring solutions.
Azure Security Center will help us to:

- Manage vulnerabilities
- Boost up the overall security of the environment

If azure security center is integrated with azure sentinel, it acts as the replacement of SOC.

Enabling Azure Defender and Azure Security center

It offers threat and vulnerability management.

Integration with SIEM solution-

It will keep records of all the operations in WVD. Security plays a key role in this; audit logs will be recorded using this. Following logs will be collected, which are mentioned below:
Azure Activity Log, Azure Active Directory Activity Log, Session hosts logs, Windows Virtual Desktop Diagnostic Log, Key Vault logs, Specific Application logs.

Integrate Azure Monitor with WVD

Integrating azure monitor provides features for monitoring the WVD infra and helps to detect and identify the issues in operation.

Secure Score

Provides the best practices and set of recommendations for improving security in the infrastructure.

DATA SECURITY

Microsoft Information Protection (MIP) helps us to discover and protect sensitive information wherever it lives or is in transit. You can customize the policies to meet the security and compliances, and also it provides the functionality to discover sensitive information across locations such as devices, cloud services, etc.

Azure Disk Encryption for Windows VMs uses Windows' BitLocker feature to provide full disk encryption of the OS disk and data disks, which helps to safeguard and protect your data.

About Mindtree

Mindtree [NSE: MINDTREE] is a global technology consulting and services company, helping enterprises marry scale with agility to achieve competitive advantage. “Born digital,” in 1999 and now a Larsen & Toubro Group Company, Mindtree applies its deep domain knowledge to 275+ enterprise client engagements to break down silos, make sense of digital complexity and bring new initiatives to market faster. We enable IT to move at the speed of business, leveraging emerging technologies and the efficiencies of Continuous Delivery to spur business innovation. Operating in more than 15 countries across the world, we’re consistently regarded as one of the best places to work, embodied every day by our winning culture made up of over 22,000 entrepreneurial, collaborative and dedicated “Mindtree Minds.”