Using Azure Virtual Desktop for BCDR in Ransomware Scenarios

A white paper by Marc Wolfson, Director Advanced Migrations, Global Black Belt Team, Microsoft

# Executive Summary

* Ransomware is a growing threat to businesses of all sizes and sectors, disrupting operations and causing financial and reputational damage.
* Business continuity and disaster recovery (BCDR) strategies are essential to mitigate the impact of ransomware and ensure the resilience and availability of critical data and applications.
* Azure Virtual Desktop (AZURE VIRTUAL DESKTOP) is a cloud-based service that delivers a secure and scalable virtual desktop experience to users on any device and from any location.
* AZURE VIRTUAL DESKTOP can be used as a BCDR solution for ransomware scenarios, enabling rapid recovery of desktops and applications, isolation of infected devices, and protection of data and credentials.
* This white paper provides an overview of the benefits and best practices of using AZURE VIRTUAL DESKTOP for BCDR in ransomware scenarios, as well as a reference architecture and a deployment guide.
* This paper is the result of some work I completed with a very large automotive manufacturer that needed a plan if the worst were to occur. The design leverages the elasticity of Azure and creates a very compelling and cost-effective mitigation to a Ransomware attack. This paper is not BCDR for existing AVD deployments. This paper addresses a situation where all users use enterprise devices on premises and need an option for safe computing while the devices have the ransomware removed from the organization.

# Introduction

Ransomware is a type of malicious software that encrypts the victim's data and demands a ransom for its decryption.

Ransomware attacks can compromise the confidentiality, integrity, and availability of data and applications, resulting in operational downtime, data loss, regulatory fines, and reputational damage.

Ransomware attacks are becoming more frequent, sophisticated, and targeted, affecting businesses of all sizes and sectors.

According to a report by Cybersecurity Ventures, ransomware is expected to cost the global economy $20 billion in 2021, up from $11.5 billion in 2019.

BCDR is the process of planning and implementing measures to ensure the continuity of business operations and the recovery of data and applications in the event of a disaster, such as a ransomware attack.

BCDR strategies typically involve backup, replication, and failover of data and applications to a secondary site, either on-premises or in the cloud.

However, traditional BCDR solutions may not be sufficient to cope with the evolving ransomware threat, as they may not provide the required level of security, scalability, and agility.

Cloud-based BCDR solutions, such as AZURE VIRTUAL DESKTOP, offer a more effective and efficient way to protect and recover data and applications in ransomware scenarios.

AZURE VIRTUAL DESKTOP is a cloud-based service that delivers secure and scalable virtual desktop experience to users on any device and from any location.

AZURE VIRTUAL DESKTOP can be used as a BCDR solution for ransomware scenarios, as it enables the following capabilities:

* Rapid recovery of desktops and applications: AZURE VIRTUAL DESKTOP allows users to access their desktops and applications from the cloud, without relying on the availability or integrity of their physical devices. This reduces the downtime and data loss caused by ransomware attacks.
* Isolation of infected devices: AZURE VIRTUAL DESKTOP isolates the user's session from the underlying device, preventing the ransomware from spreading to other devices or networks. This limits the scope and impact of the attack.
* Protection of data and credentials: AZURE VIRTUAL DESKTOP encrypts the data in transit and at rest, and stores it in Azure, not on the user's device. This prevents the ransomware from accessing or encrypting the data. AZURE VIRTUAL DESKTOP also supports multi-factor authentication (MFA) and conditional access policies, which enhance the security of the user's credentials.
* It is critical that all data is safely backed up. Consider anything users that users can access. Ransomware infection will try to encrypt anything the user has access to. User data should always be stored on OneDrive.

This white paper provides an overview of the benefits and best practices of using AZURE VIRTUAL DESKTOP for BCDR in ransomware scenarios, as well as a reference architecture and a deployment guide.

# Benefits of using AZURE VIRTUAL DESKTOP for BCDR in ransomware scenarios

AZURE VIRTUAL DESKTOP offers several benefits for BCDR in ransomware scenarios, such as:

* + Reduced downtime and data loss: AZURE VIRTUAL DESKTOP enables users to access their desktops and applications from the cloud, regardless of the state of their physical devices. This minimizes the disruption and data loss caused by ransomware attacks.
  + Reduced recovery time and cost: AZURE VIRTUAL DESKTOP allows users to restore their desktops and applications from a backup or a snapshot, without requiring the reinstallation or reconfiguration of the operating system or the applications. This reduces the time and cost of recovery.
  + Reduced risk and exposure: AZURE VIRTUAL DESKTOP isolates the user's session from the underlying device, preventing the ransomware from spreading to other devices or networks. This reduces the risk and exposure of the attack.
  + Enhanced security and compliance: AZURE VIRTUAL DESKTOP encrypts the data in transit and at rest, and stores it in Azure, not on the user's device. This protects the data from unauthorized access or encryption by ransomware. AZURE VIRTUAL DESKTOP also supports MFA and conditional access policies, which enhance the security of the user's credentials. AZURE VIRTUAL DESKTOP also complies with various industry standards and regulations, such as ISO 27001, PCI DSS, HIPAA, and GDPR.
  + Increased scalability and agility: AZURE VIRTUAL DESKTOP allows users to scale up or down their desktops and applications according to their needs, without requiring additional hardware or infrastructure. This increases the flexibility and agility of the BCDR solution.
  + Improved user experience and productivity: AZURE VIRTUAL DESKTOP delivers a high-performance and consistent virtual desktop experience to users on any device and from any location. This improves the user experience and productivity, especially for remote and mobile workers.

# Best practices of using AZURE VIRTUAL DESKTOP for BCDR in ransomware scenarios

To use AZURE VIRTUAL DESKTOP effectively and efficiently for BCDR in ransomware scenarios, the following best practices are recommended:

* + Assess the BCDR requirements and objectives: Before deploying AZURE VIRTUAL DESKTOP, it is important to assess the BCDR requirements and objectives of the organization, such as the recovery point objective (RPO), the recovery time objective (RTO), the recovery service level agreement (SLA), and the recovery cost.
  + Design the AZURE VIRTUAL DESKTOP architecture and configuration: Based on the BCDR requirements and objectives, the AZURE VIRTUAL DESKTOP architecture and configuration should be designed, such as the number and type of host pools, the number and size of virtual machines, the storage and network options, the backup and restore policies, and the security and governance policies.
  + Implement the AZURE VIRTUAL DESKTOP deployment and testing: The AZURE VIRTUAL DESKTOP deployment and testing should be implemented, following the deployment guide and the reference architecture provided in this white paper. The deployment and testing should include the creation and provisioning of the host pools, the assignment and personalization of the desktops and applications, the backup and restore of the desktops and applications, and the validation and verification of the BCDR functionality and performance.
  + Monitor and optimize the AZURE VIRTUAL DESKTOP operation and maintenance including updating the custom images so they are fully ready for deployment prior to the event.: The AZURE VIRTUAL DESKTOP operation and maintenance should be monitored and optimized, using the tools and metrics provided by Azure and AZURE VIRTUAL DESKTOP. The operation and maintenance should include the monitoring and management of the host pools, the virtual machines, the desktops and applications, the storage and network, the backup and restore, and the security and governance.
  + Train and educate the users and administrators: The users and administrators should be trained and educated on how to use and manage AZURE VIRTUAL DESKTOP for BCDR in ransomware scenarios, such as how to access and use the desktops and applications, how to backup and restore the desktops and applications, how to report and resolve any issues or incidents, and how to follow the security and governance policies.
  + Setup backups of EVERYTHING BEFORE THE ATTACK. User data should be located on OneDrive so files that got encrypted can be restored to known good.

# AZURE VIRTUAL DESKTOP for BCDR optimization

Understanding how to leverage the elasticity of Azure is key to having a BCDR solution that is cost effective. No one wants to simply deploy all the infrastructure just in case the attack happens. If possible, we can try to meet the RTO/RPO requirements without the overhead of dedicated resources prior to the attack. Here are some recommendations:

* **Configure the components** needed in the landing zone that cost nothing. VNETS, Subnets, NSGs, storage accounts host pools, app groups etc. refer to [https://github.com/Azure/avdaccelerator](https://www.bing.com/ck/a?!&&p=c50389a78d1c6cd7JmltdHM9MTcwOTE2NDgwMCZpZ3VpZD0xMzBhODRjOC0wZDA5LTZmMWUtMWM5Ni05NzZlMGM4ZDZlZTgmaW5zaWQ9NTUxMA&ptn=3&ver=2&hsh=3&fclid=130a84c8-0d09-6f1e-1c96-976e0c8d6ee8&psq=azure+virtual+desktop+landing+zone+accelerator&u=a1aHR0cHM6Ly9naXRodWIuY29tL0F6dXJlL2F2ZGFjY2VsZXJhdG9y&ntb=1" \t "_blank)
* **Determine if some components must be set up in advance** and can they be turned off until needed. Example Azure Firewall. [Stop and start the Azure Firewall (cloudoing.com)](https://cloudoing.com/stop-and-start-the-azure-firewall/)
* **Leverage the Landing Zone accelerator** scripts to deploy the VMs at scale. [Azure Virtual Desktopaccelerator/workload/bicep/brownfield/newSessionHosts/readme.md at main · Azure/Azure Virtual Desktopaccelerator · GitHub](https://github.com/Azure/avdaccelerator/blob/main/workload/bicep/brownfield/newSessionHosts/readme.md#deploy-new-session-hosts) I recommend splitting the deployment across multiple subscriptions. Use our Hub and spoke model so you have subscriptions that only contain host pool VMs. For more information refer to this link on [Azure API limitations](https://learn.microsoft.com/en-us/azure/architecture/example-scenario/wvd/windows-virtual-desktop?toc=%2Fazure%2Fvirtual-desktop%2Ftoc.json&bc=%2Fazure%2Fvirtual-desktop%2Fbreadcrumb%2Ftoc.json#azure-virtual-desktop-limitations). Multiple subscriptions don’t increase costs but ensure that you can meet your RTO/RPO. Leverage Multi-Session if possible to reduce the number of VMs that need to be deployed.
* **Leverage FSLogix and OneDrive** so data is not resident on the VM and can be easily flattened and re-deployed.
* **Leverage FSLogix Cloud Cache using Azure Page Blob Standard**. Our primary recommendation is always to use an SMB share on Azure Files Premium, however customers may choose to leverage Cloud Cache and Page Blob. This is always true for production AVD but if AVD will simply be short term mitigation during the event I recommend investigating using Cloud Cache and PageBlob. The main reason for this is that you don’t pay for storage that’s not used. Until the user logs into the VM and creates a profile the cost is 0 and you don’t pay for users that may never login during the event. Be sure to locate the VMs close or in the same data center as the storage.
* **Use page blob Standard** and set FSLogix to a single CCD location. Remember that identity is not supported on Page Blob so you will be using a storage key. Protect the storage key by using credential manager. [Protect Azure page blob connection string - FSLogix | Microsoft Learn](https://learn.microsoft.com/en-us/fslogix/how-to-protect-connection-string). Leverage Keyvault and rotate the credentials often by scripting a pull from keyvault and pushing the new value to the hosts registry. Setup private link to the storage account and be sure to setup the DNS resolver service attached to the VNET with the Virtual Machines. [Use private endpoints - Azure Storage | Microsoft Learn](https://learn.microsoft.com/en-us/azure/storage/common/storage-private-endpoints) [Quickstart - Create an Azure DNS Private Resolver using the Azure portal | Microsoft Learn](https://learn.microsoft.com/en-us/azure/dns/dns-private-resolver-get-started-portal) so FSLogix can resolve the storage to the private link.

**UseFSLogix XMLRedirection** to exclude anything not needed in the profile. [Custom profile redirections.xml - FSLogix | Microsoft Learn](https://learn.microsoft.com/en-us/fslogix/concepts-redirections-xml)  
Use with CAUTION! Every entry in the XML file forces an evaluation by FSLogix which can impact performance. Go after the biggest hitters to the profile. Unless you know the Software publisher supports the exclusion we don’t recommend using it.

[In Dean Cefelos FsLogix Video](https://www.youtube.com/watch?v=lvBiLj7oAG4&list=PL-V4YVm6AmwUJDWOBwhLNqw4MQjtAZsmx) he shows a very simple Folder Redirections file that is very effective.

<FrxProfileFolderRedirection ExcludeCommonFolders="0">

<Excludes>

<Exclude Copy="0">AppData\Local\Microsoft\Teams\meeting-addin\Cache</Exclude>

<Exclude Copy="0">AppData\Roaming\Microsoft\Teams\media-stack</Exclude>

<Exclude Copy="0">AppData\Local\Microsoft\Outlook</Exclude>

<Exclude Copy="0">AppData\Local\Microsoft\OneDrive</Exclude>

<Exclude Copy="0">AppData\Local\Microsoft\Edge</Exclude>

<</Excludes>

<Includes>

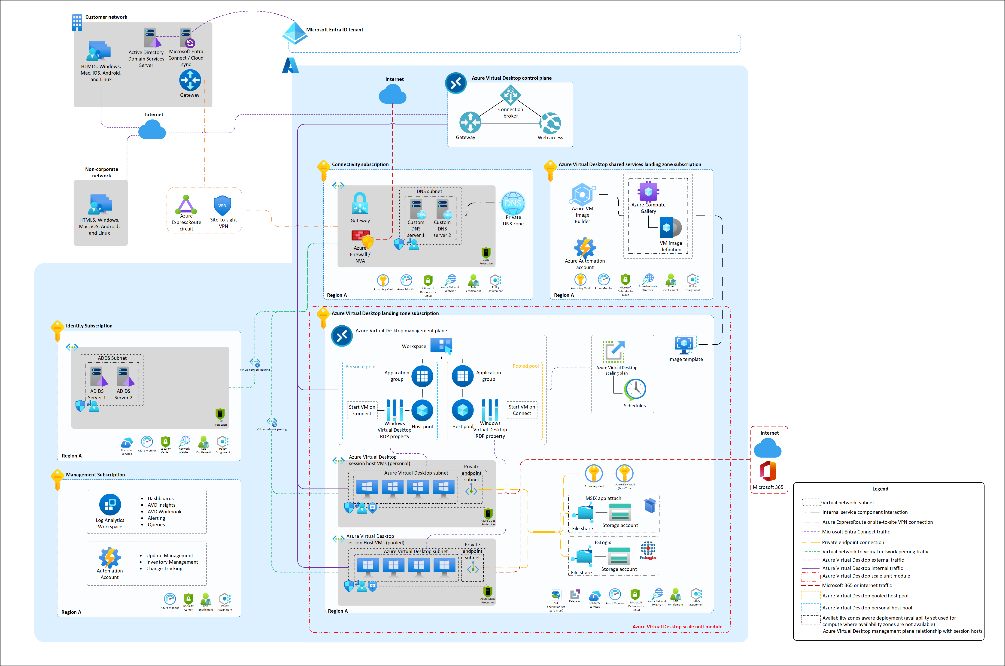
<Include>AppData\Local\Microsoft\Edge\User Data</Include>

</FrxProfileFolderRedirection>

* **Setup and AIB DevOps Workflow**- The AZURE VIRTUAL DESKTOP Landing Zone Accelerator includes scripts on setting this up. It is very important that images get updated regularly and pushed to Azure Compute Galleries so that when the BCDR is needed the deployed AZURE VIRTUAL DESKTOP image is patched, secured and apps are updated to what is being used in production at the time of the event. [AZURE VIRTUAL DESKTOP LZA Custom Image Build](https://github.com/Azure/avdaccelerator?tab=readme-ov-file#custom-image-build). Be sure to back up your custom images so they are available for deployment during the event.
* **Set OneDrive to all online**. Recovering back from an event can be challenging. Better not have any new or updated data on the local VM drives. [Redirect and move Windows known folders to OneDrive - SharePoint in Microsoft 365 | Microsoft Learn](https://learn.microsoft.com/en-us/sharepoint/redirect-known-folders)
* **Very important-** Make sure each subscription has a single Resource Group for all the VMs ONLY. After the event you can simply delete the resource group and all the resources are deleted and no longer charged to your agreement. Don’t put other objects in that resource group like VNETS and subnets so they can be re-used later if needed since they don’t cost anything to leave up.
* **Consider options from our Azure Virtual Desktop ecosystem partners** that enhance the operational capabilities you will need during the event. When the event happens some of these partners can really help reduce the pain of a very bad day.
* **Additional Considerations**-
  1. How critical are the data in profiles. Sometimes it’s a pretty easy task with minimal impact to just setup a new profile, other times all the settings in their software can be very impactful to users. We recommend separating these groups into different Storage accounts and setting up a backup solution to the subset of these users. Due to latency issues synchronizing profiles to multiple FSLogix CCD locations it is not recommended with Page Blob Storage
  2. Page Blob by default can only handle 20,000 requests per second so consider spreading the load across multiple storage accounts or requesting support increase the IOPS cap to meet demand. Page blob uses HDD and azure APIs instead of SMB protocol so there is more overhead and HDD is less performant than SSD but generally the impact to the user is completely hidden due to local caching. However, the design of the cache mode of FSLogix assumes the user will be logged in for a reasonable time to allow the synchronization to complete. If synchronization does not complete before logout it will delay logout until synchronization completes. Therefore, it is recommended that users simply close the session and not logoff. Set RDP property to close inactive sessions and logout after a defined reasonable time period and the logout process will proceed without impacting the end user.

### Security considerations

* + All VMs should have Window Defender or Defender XDR or similar malware protection.
  + VMs should be configured with Azure Virtual Desktop Insights leveraging the Azure Monitor Agent.
  + Defender Cloud should be leveraged to take advantage of Microsoft’s security at scale.
  + Choose VMs that support Secure Boot.
  + Security SIEM tool is recommended like Azure Sentinel
  + Consider deploying AppLocker and restricting user access to non-administrative roles.
  + Keep storage keys secure leveraging a vault like Azure KeyVault and programmatically deploying the Key to the VMs with a call to KeyVault for the key. Keys can be rotated without the script writer having access to the keys.
* Reference Architecture



Download [Visio File](https://github.com/Azure/avdaccelerator/blob/main/workload/docs/diagrams/avd-accelerator-baseline-architecture.vsdx)

### Glossary

|  |  |
| --- | --- |
| Component | Description |
| Entra ID | Entra IDis a cloud-based identity and access management service that provides authentication, authorization, and MFA for users and devices accessing AZURE VIRTUAL DESKTOP. |
| Azure Virtual Network (VNet) | A VNet is a logical isolation of the Azure network that provides connectivity and security for the AZURE VIRTUAL DESKTOP resources. |
| Azure Firewall | Azure Firewall is a cloud-based network security service that provides firewall and network address translation (NAT) capabilities for the VNet. |
| Azure Bastion | Azure Bastion is a cloud-based service that provides secure and seamless remote desktop protocol (RDP) and secure shell (SSH) access to the AZURE VIRTUAL DESKTOP virtual machines. |
| Azure VPN Gateway | Azure VPN Gateway is a cloud-based service that provides site-to-site and point-to-site VPN connectivity between the VNet and the on-premises network. |
| Azure ExpressRoute | Azure ExpressRoute is a cloud-based service that provides dedicated and private network connectivity between the VNet and the on-premises network. |
| AZURE VIRTUAL DESKTOP host pool | An AZURE VIRTUAL DESKTOP host pool is a collection of virtual machines that host the desktops and applications for the users. A host pool can be either pooled or personal, depending on the type of desktop assignment. |
| AZURE VIRTUAL DESKTOP session host | An AZURE VIRTUAL DESKTOP session host is a virtual machine that runs the Windows 10 operating system and the desktops and applications for the users. A session host can be either persistent or non-persistent, depending on the type of desktop personalization. |
| AZURE VIRTUAL DESKTOP application group | An AZURE VIRTUAL DESKTOP application group is a logical grouping of applications that are assigned to users. An application group can be either remote app or desktop, depending on the type of application delivery. |
| AZURE VIRTUAL DESKTOP workspace | An AZURE VIRTUAL DESKTOP workspace is a logical grouping of application groups that are presented to users. A workspace can contain multiple application groups from different host pools. |
| Azure Storage | Azure Storage is a cloud-based service that provides storage and backup capabilities for the AZURE VIRTUAL DESKTOP resources. Azure Storage includes Azure Files, Azure Blobs, Azure Disks, and Azure Backup. |
| Azure Monitor | Azure Monitor is a cloud-based service that provides monitoring and analytics capabilities for the AZURE VIRTUAL DESKTOP resources. Azure Monitor includes Azure Log Analytics, Azure Metrics, Azure Alerts, and Azure Application Insights. |
| Azure Security Center | Azure Security Center is a cloud-based service that provides security and compliance capabilities for the AZURE VIRTUAL DESKTOP resources. Azure Security Center includes Azure Defender, Azure Policy, and Azure Sentinel. |

# Deployment guide of using AZURE VIRTUAL DESKTOP for BCDR in ransomware scenarios

The following steps provide a high-level guide of how to deploy AZURE VIRTUAL DESKTOP for BCDR in ransomware scenarios:

* Step 1: Create and configure an Azure AD tenant and a VNet.
* Step 2: Create and configure an Azure Firewall and an Azure Bastion.
* Step 3: Create and configure an Azure VPN Gateway or an Azure ExpressRoute.
* Step 4: Create and configure an AZURE VIRTUAL DESKTOP host pool and a session host.
* Step 5: Create and configure an AZURE VIRTUAL DESKTOP application group and a workspace.
* Step 6: Create and configure an Azure Storage account and a backup policy.
* Step 7: Create and configure an Azure Monitor workspace and an alert rule.
* Step 8: Create and configure an Azure Security Center policy and a Sentinel workspace.
* Step 9: Test and validate the AZURE VIRTUAL DESKTOP deployment and the BCDR functionality.
* Step 10: Train and educate the users and administrators on how to use and manage AZURE VIRTUAL DESKTOP for BCDR in ransomware scenarios.

For more details and instructions on how to deploy AZURE VIRTUAL DESKTOP for BCDR in ransomware scenarios, please refer to the following resources:

* Azure Virtual Desktop documentation: <https://docs.microsoft.com/en-us/azure/virtual-desktop/>
* Azure Virtual Desktop BCDR best practices: <https://docs.microsoft.com/en-us/azure/virtual-desktop/disaster-recovery-guidance>
* Azure Virtual Desktop BCDR reference architecture: <https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/virtual-desktop-infrastructure/vdi-azure>
* Azure Virtual Desktop BCDR deployment guide: <https://docs.microsoft.com/en-us/azure/virtual-desktop/deploy-azure-virtual-desktop>
* [The growing threat of ransomware - Microsoft On the Issues](https://blogs.microsoft.com/on-the-issues/2021/07/20/the-growing-threat-of-ransomware/)
* [Malware and ransomware protection in Microsoft 365 - Microsoft Service Assurance | Microsoft Learn](https://learn.microsoft.com/en-us/compliance/assurance/assurance-malware-and-ransomware-protection)
* [Ransomware Protection for Businesses | Microsoft Security](https://www.microsoft.com/en/security/business/solutions/ransomware-protection-for-businesses)
* [Responding to ransomware attacks | Microsoft Learn](https://learn.microsoft.com/en-us/microsoft-365/security/defender/playbook-responding-ransomware-m365-defender?view=o365-worldwide)
* [Announcing New OneDrive for Business feature: Files Restore - Microsoft Community Hub](https://techcommunity.microsoft.com/t5/microsoft-onedrive-blog/announcing-new-onedrive-for-business-feature-files-restore/ba-p/147436)
* [Deploy ransomware protection for your Microsoft 365 tenant | Microsoft Learn](https://learn.microsoft.com/en-us/microsoft-365/solutions/ransomware-protection-microsoft-365?view=o365-worldwide)

Acknowledgements:  
I’d like to thank the following for their suggestions and contributions to this paper:  
  
John Kelbley  
Jason Maston  
John Wilson