Compete 366

Microsoft Partner

Gold Cloud Platform
Gold Small and Midmarket Cloud Solutions
Gold Cloud Productivity

Azure Virtual Desktop

Contents

CHAPTER 1

What is Azure Virtual Desktop and how should you use it? 4

CHAPTER 2

How to Implement Azure Virtual Desktop 7

CHAPTER 3

Optimising AVD for Cost and Performance 11

CHAPTER 4

Eight Tips on how to manage AVD 16

CHAPTER 5

Security Best Practice for AVD.. 21

Introduction

You may already be aware that many organizations are currently leveraging virtual desktops. Right now, they are becoming increasingly popular, when much of the workforce is remote. The fact is, the way we work is rapidly evolving. An increasing number of companies are adapting to these changes and cutting costs with Azure Virtual Desktop, also known as Azure Virtual Desktop and AVD.

However, remote work isn't the only use case for this solution. Windows Virtual Desktops offer an easy and secure way to give your entire team secure access to the information and applications they need on their devices. This saves time, resources and boosts employee efficiency.

Want to know if Azure Virtual Desktop is right for you? We've written this eBook to help you find out if it is.

CHAPTER 1

What is Azure Virtual Desktop and how should you use it?

What is a virtual desktop?

A virtual desktop is a full desktop that runs on a remote server. This enables you to securely access work applications and data from wherever you are and on any device. It expands the possibilities beyond the physical desktop screen in the office.

Azure Virtual Desktop is a desktop app and visualization service that runs on the cloud. It provides all the benefits you might expect from a virtual desktop while offering the same tools and resources your employees already use.

Benefits of a virtual desktop

You may be wondering: How do I determine if my organization will benefit from a virtual desktop solution? If all of your staff have work laptops and you can secure and manage their access to the information and applications they need, using a virtual desktop may not be necessary for your organization. However, for many companies, Compete366's Azure experts highlight that their specific needs are best managed with a virtual desktop. If any of the following apply to you, it's worth considering Azure Virtual Desktop.

>> Your staff need to work remotely

Your team need to be able to work from home, when travelling, on customer sites or in the office and have the same user experience wherever they are. You need to manage and secure access to company data and applications.

>> Simple security management

When you have contractors or part time staff that need access to information, security can become a concern. Azure Virtual Desktop makes it easy for you to provide controlled and secure access to your data and applications. Additionally, your full-time employees can use their home PC (or Mac) to connect to their work virtual desktop. This keeps all your corporate information secure.

>> You have an occasional need for PCs

Don't waste resources on setting up several physical machines if all of your employees don't need a dedicated PC. Azure Virtual Desktop makes it possible to deploy virtual PCs when you need them. As your needs change, you can add or remove virtual desktops to meet the needs of your workforce.

>> You need different types of PCs for different teams in the business

You can deploy different virtual desktops to different user groups. This way, users are only able to access the apps and information they need to do their work. They won't see information that they don't need, and you can give them the computing power that they need for their work.

What makes Azure Virtual Desktop different?

In the past, virtual desktop solutions have been complex and expensive. They were difficult for companies to set up and manage. A large server infrastructure was necessary to run virtual desktops. As a result, most small and medium businesses didn't have the resources to manage virtual desktops in-house. Azure Virtual Desktop makes this accessible and affordable for all businesses.

As Compete366's Azure experts explain, Azure Virtual Desktop is different from other virtual desktop solutions because it is:

Simple to deploy and configure

Now, managing Azure Virtual Desktop is easier than ever before. In the Azure Portal, you can deploy and manage virtual desktops and apps, assign users and have access to monitoring and diagnostics. All of this is available to you in a single interface.

Cost effective

Azure Virtual Desktop can save your organization money, because you only pay for virtual servers when your virtual desktops are on. In addition, when using Azure Virtual Desktop, there is less infrastructure required to run a distributed team.

Easy to scale

You can quickly provide full Windows 10 desktops with all your business applications to your users. You can also increase or decrease the number of virtual desktops you use as your workforce changes.

Flexible

Like with all Microsoft Cloud Services, there are no contractual commitments with Azure Virtual Desktop. The service itself is also more flexible than other available options because it allows you to choose to give your employees the entire desktop experience or only offer specific virtual apps. It's also the only virtual desktop interface that offers Windows 10 Enterprise multi-session.

How much does Azure Virtual Desktop cost?

Our Azure experts outline that the monthly cost will depend on the number of users, the software that they need and their usage patterns. This is what the costs will typically include:

>> A domain controller

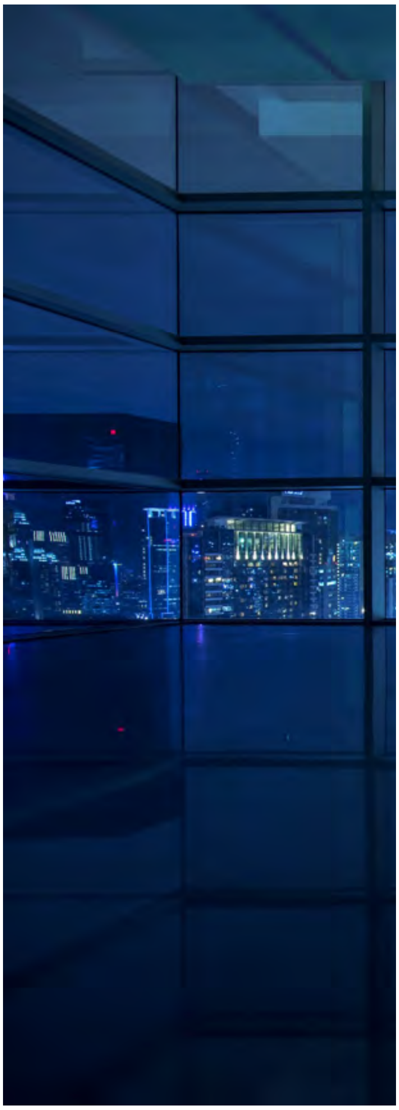
This will manage user access and the Session Hosts. If simplicity is a priority for your organization, one option is to use Azure Active Directory Domain Services. You can learn more about AD and Azure AD here.

>> Session hosts

You will need session hosts to host the virtual desktops. The session host is an Azure Virtual Machine (server) and you can have one or many of these. Typically you will assign a number of users per session host, so for example if you assigned 6, this means that 6 users would have their Virtual Desktop sessions on the same server. So in this example, if you had 30 users then you would need 5 session hosts. Note that you only pay for the session hosts while they are on.

>> Storage for user profile disks

Your user profile is stored centrally and is attached to whichever session host you are allocated to – this means that your desktop and your data looks the same regardless of which session host you are allocated to that time. This user profile uses FSLogix and needs to be stored somewhere, for simplicity we recommend Azure Files.



Licensing

To use Azure Virtual Desktop, you will need licensing for:

- MS Office with Shared Computer Activation (if you are using the Office suite)
- FSLogix
- Windows 10 Enterprise

As our Azure experts explain, your organization may already have access to AVD with a Windows or Microsoft 365 license. For example, the licensing for Office, FSLogix and W10 Enterprise is all included in the M365 Business Premium plan. If you are using a lower plan, then you can upgrade your license and pay the additional amount.

CHAPTER TWO

How to implement Azure Virtual Desktop

Defining your user groups and their needs

Before you implement Azure Virtual Desktop, our Azure experts advise that you need to consider your user groups. Who in your organisation do you want to provide with a Azure Virtual Desktop?

Here are some questions that can help you define your user groups:

- Will everyone get one or just a selected group of users?
- Are these staff all based in the same country or are some on the other side of the world? You need to think about round trip latency for the end users and choose an Azure data centre region accordingly.
- Will everyone get the same Azure Virtual Desktop or will different groups of users need different ones? For example, admin staff get a lower spec Azure Virtual Desktop with just Office and the engineering staff get a higher spec Azure Virtual Desktop with Office and a CAD application.
- Also how will these users access their Azure Virtual Desktops? Will they use existing work or personal PCs / Macs using the available Azure Virtual Desktop clients? Or will you be providing them with thin clients?

Putting it all together: the components you need for Azure Virtual Desktop

Once you define what your organisation's needs are, our Azure experts highlight that you will need to make sure you have all the necessary components. Here's what you need to set up AVD:

- Azure AD
- An Azure subscription
- A Domain Controller that is synced with Azure AD
- A virtual network for the session hosts
- Azure Virtual Desktop session hosts
- FSLogix for user profile containers
- A central storage location for the FSLogix user profile disks

You may already have some of these critical components. For example, when you sign in to the Azure Virtual Desktop service, it authenticates against Azure AD. If you're using Office 365 (O365) or Microsoft 365 (M365), you already have Azure AD.

See our blog post on the difference between Azure AD and AD if you're not familiar with Azure AD.

You will also need licensing for:

- Office with shared computer activation (if you're planning to use Office)
- FSLogix
- W10 Enterprise

The licensing for Office, FSLogix and W10 Enterprise is all included in the M365 Business Premium plan. If you are using a lower plan, then you can upgrade your license and pay the additional amount.

Domain controller

Your Azure Virtual Desktops need to be joined to a domain, which is why you need a domain controller (DC). Our Azure experts outline three options:

- Azure Active Directory Domain Services (Azure AD DS)
- An Azure Virtual Machine configured as a DC
- An existing on-premises DC with a site to site VPN from on-premises to the Azure Vnet

Whichever option you choose they need to synchronize with Azure AD. For either of the Domain Controller options you install and configure Azure AD Connect, whereas Azure AD DS synchronizes with Azure AD directly.

Which option is best will depend on your existing set up and requirements.

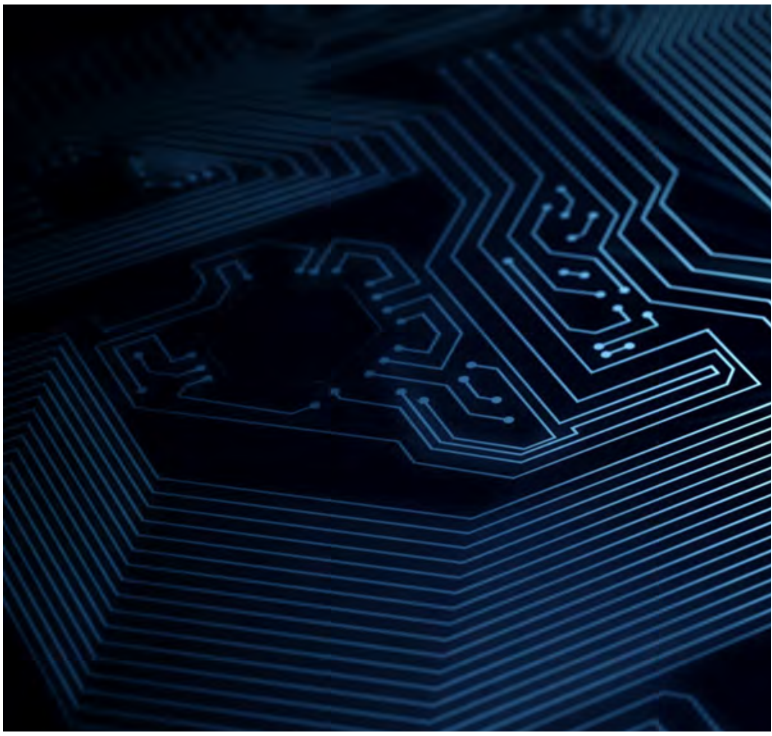
For cloud based organisations we usually recommend Azure AD DS because it is simple to set up, there is no ongoing management (it is a Platform as a Service offering), it is resilient and it costs about the same as having a pair of Domain Controller Virtual Machines.

If you use Azure AD DS, then in order to set up any Group Policies for fine grained control of the Virtual Desktops (for example to deny user access to Control Panel) you need an additional Azure VM which is domain joined and has the Active Directory administrative tools installed. These policies are then synced to Azure AD DS, and you can then shut down this VM to save money, and spin it up again next time you want to edit or create any Group Policies.

User profile containers

Microsoft recommends FSLogix profile containers as the user profile solution to use withAzure Virtual Desktop.

At sign-in, this container is dynamically attached to the session host. Then, the user profile is immediately available. It appears in the system exactly as a native user profile would.



Creating the images

To create your image, you deploy a normal Azure VM and use this to create the image for your Azure Virtual Desktop Session Hosts. If you want the Office suite on your image, then deploy the VM from the Azure gallery image for Windows 10 Enterprise multi-session with Office, and it comes pre-installed.

Once the VM is created and joined to the domain, you install and configure the following:

- FSLogix
- Access and rights for the users that will use this
- Your applications

Then you sysprep the VM and create an image from this. At this point the VM can no longer be used and you can delete it.

If you want a different image (say with different applications on) for different groups of users then you would create a second image for them in the same way.

You now have your image(s) from which you will create your session hosts.

Choosing the size and number of session hosts

The AVD Session Hosts are Azure VMs and they host the Virtual Desktop sessions.

You can dedicate an individual session host to each user – so in this instance there would just be one Virtual Desktop session running on the Session Host. But in most cases people choose to have multiple Virtual Desktop sessions supported on each Session Host.

You need to decide how much computing power to allocate to each Azure Virtual Desktop. This will depend on what the users' workloads require.

Say for example each user needed 0.5 vCPUs and 2 GB of RAM, and you wanted 8 users per Session Host, then you would choose a VM size with 4 vCPUs and 16 GB of RAM for the Session Host. If you had 32 users then your hostpool would need to contain 4 of these Session Hosts.

Deploying host pools

Host pools are a collection of one or more identical virtual machines (Session Hosts) within the Aure AVD environment.

Creating and deploying the host pool all happens in the Azure portal. You choose your image, the size and number of session hosts. Then, you decide which virtual network to add them to and which domain to join. Azure will then deploy the host pool for you.

This usually takes about 5 minutes and then your session hosts will be up and running.

Application groups

An Application Group is associated with a host pool. The default app group created for a new host pool publishes the full desktop. So you can now assign users to that app group (again in the Azure portal GUI), and once you've done this they can sign into the AVD service to access their virtual desktop session.

If you have a number of different applications on the image and you would like to publish one of them as a remote application (e.g. Outlook, Chrome, or one of your Line of Business apps), then you just create a remote app group (in the GUI) for that application. You then assign users to that remote app group and it will be visible and available to them when they sign in to the Azure Virtual Desktop service. You can do this for some or all of the available applications on the session host image.

Using Azure Virtual Desktop

Now the setup is complete, and users can access Azure Virtual Desktop. There are clients for Azure Virtual Desktop that you can install on Windows, Macs, iOS and Android devices, and there is also a web client. Or you may be using a Thin Client solution.

All users have to do is sign in with their Azure AD credentials and they can get to work.

CHAPTER THREE

Optimising Azure Virtual Desktop for cost and performance

This third chapter gives the IT lead in your organisation high-level guidance on optimising the cost and performance of Azure Virtual Desktop according to your particular business needs. The only IT knowledge you will need to manage this environment is traditional desktop management skills.

You may be looking for a virtual desktop or remote app solution or your organisation may have already set up Azure Virtual Desktop, we outline how you can make the most of Microsoft's best-in-class solution.

Want advice from a trusted Azure Virtual Desktop expert? We are an Azure Gold Partner and can help. Book a free, no-obligation consultation or read on to find out about the key considerations for optimising Azure Virtual Desktop in your business.

As many IT professionals will know, there is often a trade-off between cost and performance – if you want better IT performance, it usually costs more. While this is true for many elements of Azure Virtual Desktop, there are some key ways to optimise the performance of your Azure Virtual Desktop environment that won't cost a penny.

1. Optimising performance

For optimizing Azure Virtual Desktop, there are two, key performance considerations – latency and speed.

Latency

Latency is the round-trip time (RTT) and primarily based on the physical distance from your users to the virtual desktop session host (or server) and back again. All things being equal, the latency decreases the closer the network points of a connection are to each other. Therefore, it is important to consider which Azure region your session host is deployed in.

For a decent virtual desktop experience, the round-trip latency should be less than 100ms. Between 100ms and 200ms is still reasonable, however anything above 200ms will be noticeable by the end-user.

Choose the right location for your session hosts

The Microsoft AVD Experience estimator allows you to estimate the connection round-trip time (RTT) from your current location, through the Windows Virtual Desktop service, to each Azure region in which you can deploy virtual machines.

For example, if your users are in the UK, logically you'll choose a UK data centre for your session hosts. If you also have a set of users on another continent, then you can deploy their session hosts in an Azure datacentre that's local to them.

However, if you have a set of users on another continent that need access to back-end systems in the UK, you'll need to balance the user latency to the virtual desktop and the virtual desktop latency to the back-end system. Therefore, you may want to consider locating your session hosts between the back-end system and your users. Our Azure Virtual Desktop specialists can help you identify the right option for your requirements.

Consider RDP Shortpath for direct connectivity

RDP Shortpath is a new Microsoft service in public preview designed to establish direct connectivity between the remote desktop client and the session host with a number of potential benefits:

- reduces dependency on the Windows Virtual Desktop gateways
- improves the connection's reliability
- increases the bandwidth available for each user session

The removal of additional relay reduces RTT, which can improve user experience with latency-sensitive applications and input methods.

Speed of your Azure Virtual Desktop

The second key consideration is the speed at which your virtual desktop is running your applications and performing tasks such as opening Outlook or creating a new Word document for example.

>> Size session hosts according to user needs

The speed your virtual desktop runs at is determined by how resource intensive the workload is (according to the applications that you're running and how intensively you use them) and how much compute resource (processors and memory) you allocate to each user. The more compute resource you allocate to a user, the faster their virtual desktop will run.

To help estimate the amount of compute resource you need, Microsoft have published this useful guidance on the types of remote desktop workloads from 'light' through to 'power' with corresponding recommendations for virtual machine sizing.

For example, if your workloads are deemed to be 'heavy' then the recommendation is a maximum of two virtual desktop sessions (users) per vCPU, with a minimum virtual machine specification of four vCPUs and 16 GB of RAM such as the D4s_v3, which is a commonly used virtual-machine size for AVD session hosts. Therefore, you could have eight virtual desktop sessions on this session host. Our Azure Virtual Desktop consultants will advise you on how best to scale your deployment depending on the expected need of each type of user.

>> Test performance and refine

Once you've deployed your virtual machines, the first priority is to test their performance for your users. If the virtual desktop sessions are performing well, you can try increasing user density per processor – either by allocating more users per session host or by decreasing the size of the session host. Whilst this decreases your cost, you will need to monitor and ensure the trade off on performance.

Optimising Windows 10 for Azure Virtual Desktop

Windows 10 comes with a number of pre-installed applications. Removing those that aren't wanted and not running unnecessary processes will make virtual desktop sessions more efficient. This will improve performance for the allocated compute resource, or alternatively, you can reduce the amount of compute resource and its costs accordingly. By optimising in this way, you can increase user density by up to 15%. Watch this 10-minute video from the Azure Academy for a useful overview of this optimisation plus Virtual Desktop Optimization tool with the scripts and instructions you'll need.

NB. You can't use this code to optimise the image itself as some of the code won't survive the sysprep process, instead run the code against the Azure Virtual Desktop session hosts once you've deployed them from the image.

2. Optimising cost

Your Azure virtual machines or session hosts represent the primary cost of an Azure Virtual Desktop environment. Therefore, increasing user density as discussed above will reduce your costs. Once you've identified your optimum user density, there are steps you can take to reduce your costs further.

>> Switch off your virtual machines when they're not in use

Azure virtual machines are billed on a pay-as-you-go basis, so there can be considerable cost savings if you're able to switch your machines off outside working hours. You'll continue to pay for any virtual machine discs, however this is typically a minor cost in comparison to the virtual machine.

If you only need your Azure Virtual Desktop environment to be available to users during office hours i.e. 08.30 to 17.30, Monday to Friday, and you're able to switch off your virtual machines outside those hours, then you may pay as little as 27% of the full monthly virtual machine cost.

>> Autoscale to minimise your costs

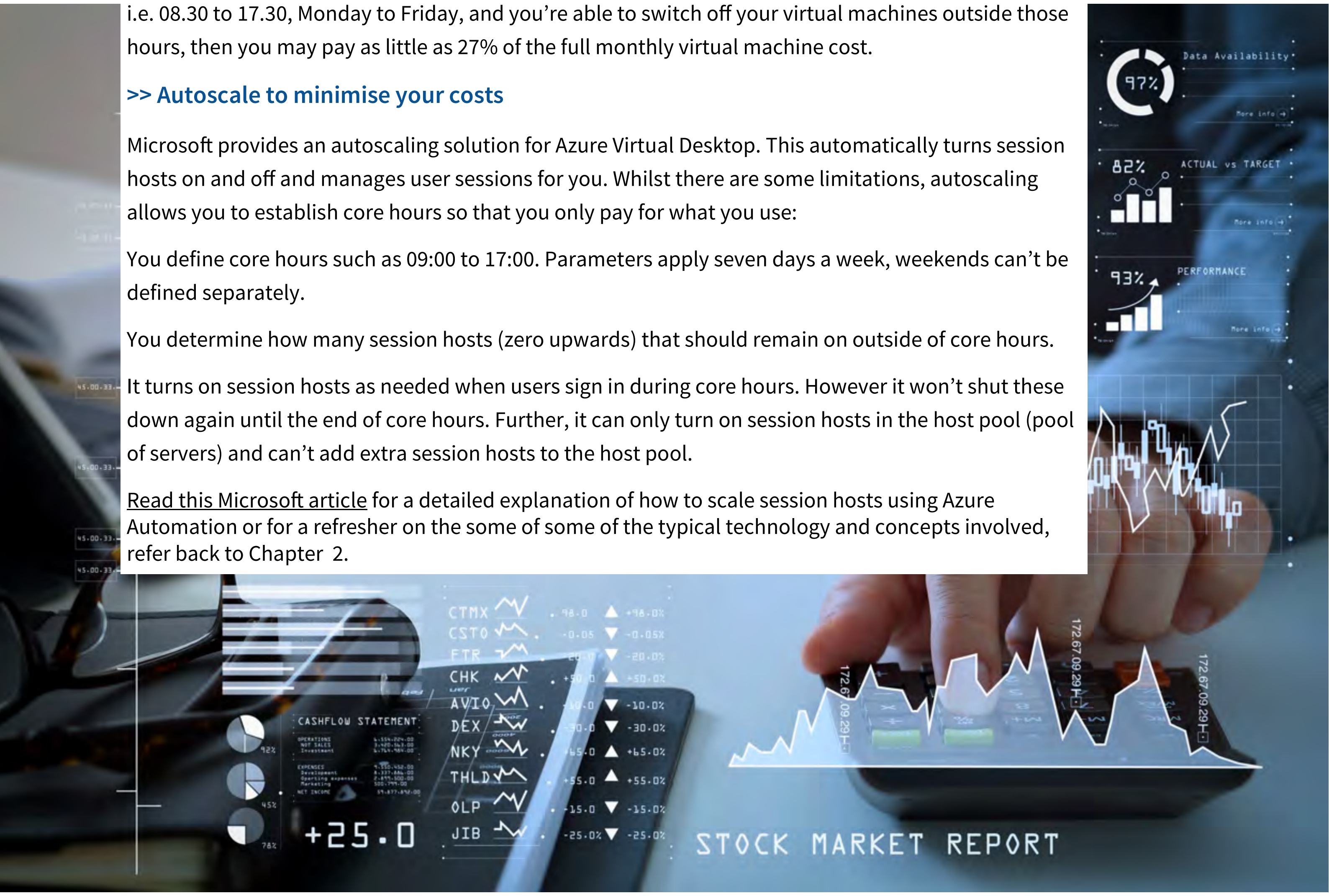
Microsoft provides an autoscaling solution for Azure Virtual Desktop. This automatically turns session hosts on and off and manages user sessions for you. Whilst there are some limitations, autoscaling allows you to establish core hours so that you only pay for what you use:

You define core hours such as 09:00 to 17:00. Parameters apply seven days a week, weekends can't be defined separately.

You determine how many session hosts (zero upwards) that should remain on outside of core hours.

It turns on session hosts as needed when users sign in during core hours. However it won't shut these down again until the end of core hours. Further, it can only turn on session hosts in the host pool (pool of servers) and can't add extra session hosts to the host pool.

Read this Microsoft article for a detailed explanation of how to scale session hosts using Azure Automation or for a refresher on the some of some of the typical technology and concepts involved, refer back to Chapter 2.



>> Gain discounts by committing to reserved instances

By default, all the resources you deploy in Azure are Pay As You Go (PAYG) and without minimum commitments or tie-ins. However, Azure also offers other pricing options such as Reserved Instances (RI) for virtual machines. This means that you can benefit from a significant discount in return for committing to resources for one or three years. You can still pay monthly and have the flexibility to cancel within the agreed period, subject to a cancellation fee.

The key point to note is that if you buy an RI for a virtual machine, then you pay for it whether you turn the virtual machine on or not. So the idea is that you apply RIs to the virtual machines that are going to be on all the time, as you don't make any saving by turning them off with RI pricing.

For further details of how to save more with RI read Microsoft's article [Azure Reserved Virtual Machine Instances | Microsoft Azure.]

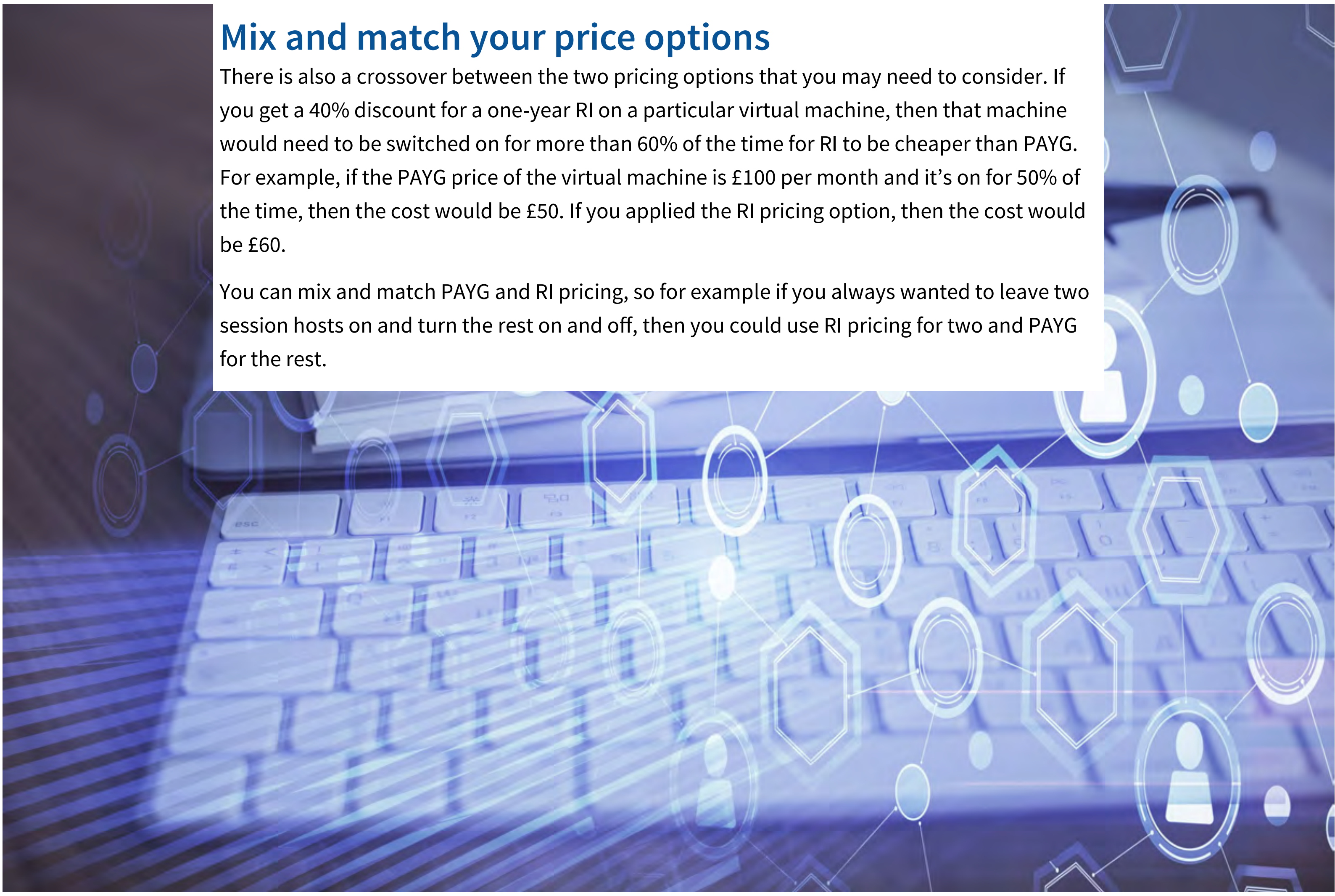
We normally recommend:

- Use PAYG pricing for virtual machines that you can switch on and off because you don't pay when they are turned off.
- Use RI pricing for virtual machines that are on 24×7 when you can commit to usage for at least one year.

Mix and match your price options

There is also a crossover between the two pricing options that you may need to consider. If you get a 40% discount for a one-year RI on a particular virtual machine, then that machine would need to be switched on for more than 60% of the time for RI to be cheaper than PAYG. For example, if the PAYG price of the virtual machine is £100 per month and it's on for 50% of the time, then the cost would be £50. If you applied the RI pricing option, then the cost would be £60.

You can mix and match PAYG and RI pricing, so for example if you always wanted to leave two session hosts on and turn the rest on and off, then you could use RI pricing for two and PAYG for the rest.



Choose the right Azure Virtual Desktop license

Wondering what license you need for Azure Virtual Desktop and what is the most cost-effective licensing option for you? When deploying resources in Azure, typically the costs are included in the monthly bill for the solution you're deploying and there are no additional licensing fees. For example, if you deploy an Azure virtual machine running a Windows Server, your monthly Azure consumption bill will include the cost of the compute part of the virtual machine (CPU and memory) and the operating system (Windows Server) - you essentially pay for what you use.

However, with Azure Virtual Desktop you may need additional licensing for services purchased outside Azure such as Office 365 or Microsoft 365.

>> Windows 10 licensing

Azure Virtual Desktop session hosts are automatically charged at the Linux compute rates so you won't be charged for the Windows 10 license as part of the virtual machine cost. However, each AVD user will need to be licensed for Windows 10 with one of the following licenses which include it:

- Microsoft 365: E3, E5, A3, A5, F3, Business Premium
- Windows: E3, E5, A3, A5

Licenses are automatically applied when you deploy from an Azure marketplace image. The following article explains how to apply a Windows license to your session host virtual machines.

>> Office 365 licensing

If you're going to deploy the Office suite on your virtual desktops, you'll need to be licensed for Office with shared computer activation. This means you will need an O365 E3 or E5 plan or M365 Business Premium and above plans which include this.

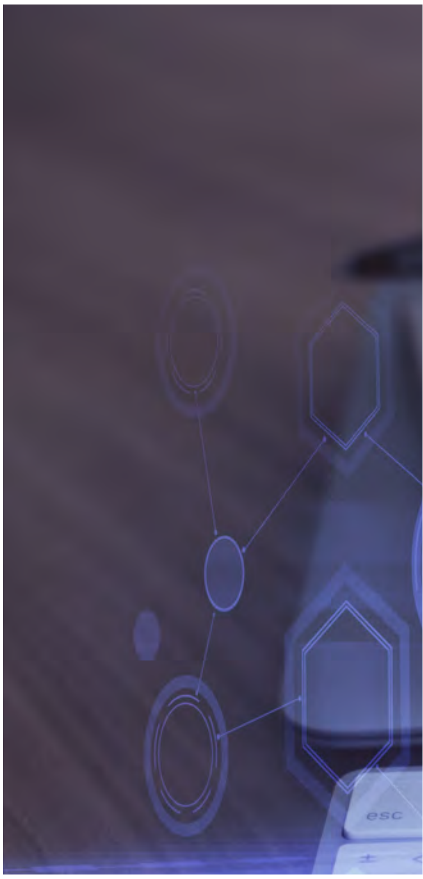
>> FSLogix

If you're going to use FSLogix for the user profile container, each AVD user will need to be licensed for FSLogix with one of the following licenses which include it:

- Microsoft 365: E3, E5, A3, A5, F3, Business Premium
- Windows: E3, E5, A3, A5

Microsoft's guide to Windows Virtual Desktop Pricing gives full details on Azure Virtual Desktop licensing requirements.

You can certainly optimise your costs by choosing the right licensing. In practice we find that Microsoft 365 Business Premium is often the best option in the most common scenarios. It does of course depend on what licensing you already have and which of the above you need to be licensed for in your Azure Virtual Desktop environment.



CHAPTER FOUR

Eight tips on how to manage Azure Virtual Desktop

This Chapter provides high-level guidance on the day-to-day management of Microsoft's best-in-class solution.

Azure Virtual Desktop key management tasks

Once you've set up Azure Virtual Desktop, we've identified a number of key management tasks to keep the environment performing at its best, including how to:

- Administer Group Policy
- Manage images
- Update your desktops and applications or deploy new applications
- Validate updates before users access them
- Add or remove session hosts from the host pool
- Create new host pools
- Monitor and receive alerts for the environment
- Backup the environment

1. Administer Group Policy

Settings for user and computer objects in Active Directory Domain Services (AD DS) are managed using Group Policy Objects (GPOs). If you are using a domain controller (whether that be an Azure virtual machine or an on-prem one accessed via a site-to-site VPN) to domain join the AVD session hosts to, then you can control them with Group Policy on the domain controller.

If you're using Azure AD DS instead of a domain controller, you can manage Group Policy by installing Group Policy Management Tools on a domain-joined Windows server. These settings will synchronise with the Azure AD DS service so that you could then shut down your virtual machine until you next need to implement changes.

Azure AD DS includes built-in GPOs for the AADDC users and AADDC computer containers. You can customise these built-in GPOs to configure Group Policy as needed for your environment. Members of the Azure AD DC administrators group have Group Policy administration privileges in the Azure AD DS domain and can also create custom Group Policy Objects (GPOs) and Organisational Units (OUs). This useful article from Microsoft explains in more detail how to create and manage Group Policy in Azure AD Domain Services.

2. Manage images

Creating the image that you use to deploy your AVD session hosts from is the most time-consuming element of managing AVD. Chapter Two gives more details on creating images. Once you have the image, deploying session hosts from it is straightforward. Having put the effort into creating the images, you need to put some care into managing them.

Provided that you have a fairly simple set up, you can manage images manually with your own naming system while deleting older ones that you no longer need. However, if you have a larger, more complex set up, with host pools in multiple geographies or host pools with large numbers of session hosts, then you can use the Shared Image Gallery. This is a good way to organise images and offers a number of benefits:

Replication to other regions: If you've deployed host pools on different continents, you can replicate images to those regions and keep them up to date, so that your session hosts all use the same one.

Deploy at scale: If your host pool has 20 or more session hosts, then it is recommended to have multiple copies of the image. One managed image supports up to 20 simultaneous deployments. Attempting to create more than 20 virtual machines concurrently, from the same managed image, may result in provisioning timeouts due to the storage performance limitations of a single virtual hard disk (VHD). To create more than 20 virtual machines concurrently, use a Shared Image Galleries image configured with one replica for every 20 concurrent virtual machine deployments. Take a look at Microsoft's article on Shared Image Galleries for a good overview of this service.

3. Update the desktop and applications or deploy new applications

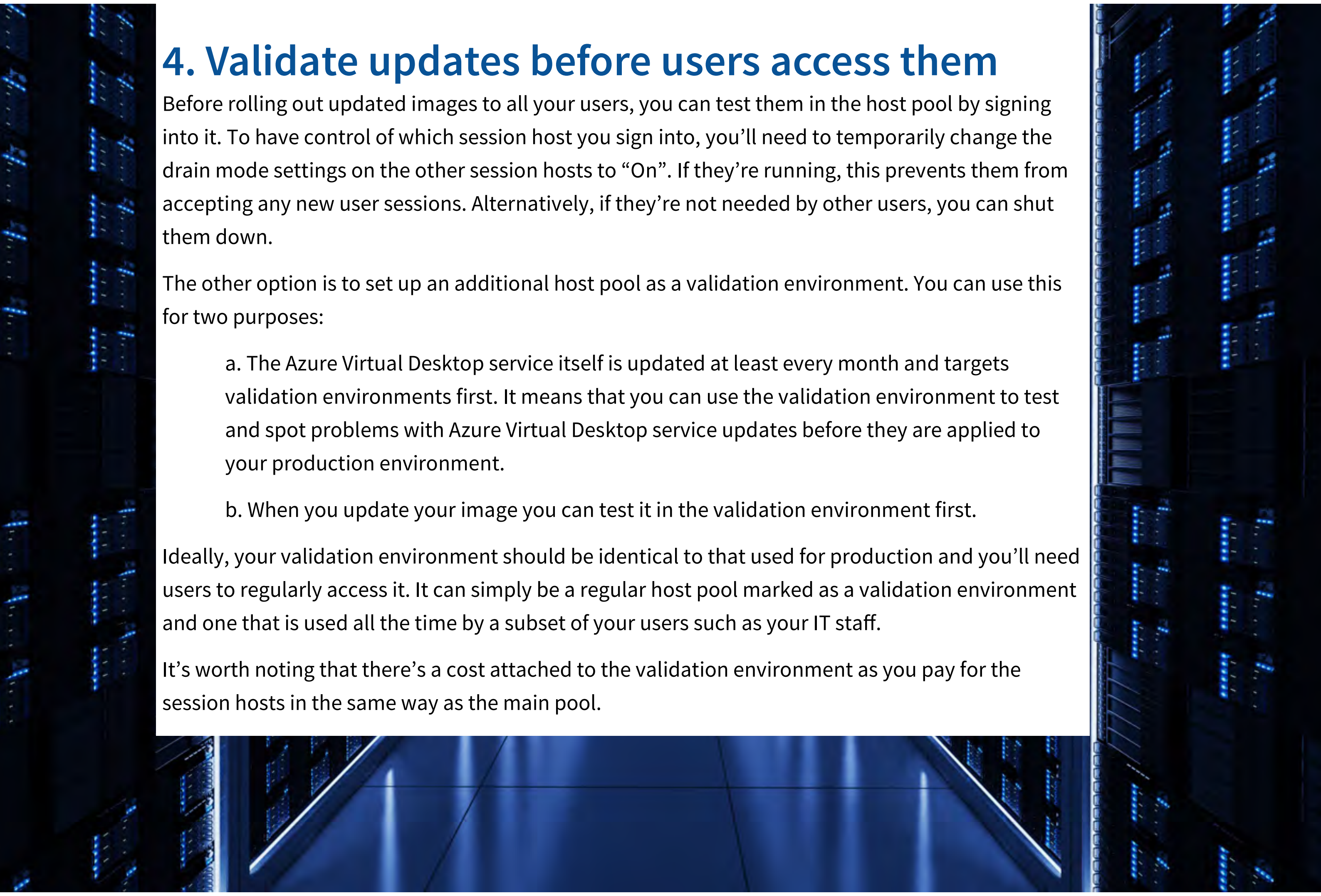
By default users don't have the ability to re-start the virtual desktop to apply any Windows 10 updates – and you wouldn't want this as it would re-start the session host and thus kick off any other users on it. By default users do, however, have the ability to check for Windows 10 updates and download and install them. You can of course use Group Policy to control this as you wish, and it is wise to only allow IT admin staff to manage updates.

You can patch or update your Windows 10 virtual desktop sessions by signing into each session host with an admin account. Alternatively, you can create a new image with all the updates and re-deploy to the host pool.

We advise updating session hosts with Windows patches and potentially updating applications on a monthly basis. Occasionally, you may also need to add a new application and we recommend the following approach:

- update the image including Windows and application patches and any new applications.
- add new session hosts created from the updated image to the host pool.
- remove the session hosts with the "old" image from the host pool.

You can update the image by creating a new Azure virtual machine from it, make the updates to this virtual machine, then create the updated image from this virtual machine. See below for how to add and remove session hosts.



4. Validate updates before users access them

Before rolling out updated images to all your users, you can test them in the host pool by signing into it. To have control of which session host you sign into, you'll need to temporarily change the drain mode settings on the other session hosts to "On". If they're running, this prevents them from accepting any new user sessions. Alternatively, if they're not needed by other users, you can shut them down.

The other option is to set up an additional host pool as a validation environment. You can use this for two purposes:

a. The Azure Virtual Desktop service itself is updated at least every month and targets validation environments first. It means that you can use the validation environment to test and spot problems with Azure Virtual Desktop service updates before they are applied to your production environment.

b. When you update your image you can test it in the validation environment first.

Ideally, your validation environment should be identical to that used for production and you'll need users to regularly access it. It can simply be a regular host pool marked as a validation environment and one that is used all the time by a subset of your users such as your IT staff.

It's worth noting that there's a cost attached to the validation environment as you pay for the session hosts in the same way as the main pool.

5. Add or remove session hosts from the host pool

If, for instance, you currently have 30 users spread over five session hosts in your host pool, and now need to add capacity for another 12 users, then you'd need to add another two session hosts to the host pool.

In the Azure portal, adding or removing session hosts couldn't be simpler. To add a session host, in the session hosts blade:

- Click to add new ones.
- Enter the quantity.
- Select the image from which you wish to create these.

NB. This must be the same image that you used to create the existing session hosts.

Similarly, if the number of users who need a virtual desktop has decreased and you now have more session hosts than you permanently need, you can remove them. For example, if you simply want to decrease the number of session hosts by one:

- Switch on drain mode for the session host that you want to remove to stop any new connections to it.
- Force a log-off or wait for users to do so.
- Click the Remove button on the session host blade.
- Shut down and delete the virtual machine, its OS disk and network interface.

6. Create new host pools

There are a number of reasons for creating a new host pool in addition to those you already have:

Your organisation may have a new set of users in a different geographical location and you need a host pool that's local to them either for performance or data residency reasons.

You may want to provide a set of users with a more or less powerful PC or a different set of applications, while other users continue with their existing PCs in the first host pool.

You may have a set of users for which you want to apply a different auto-scaling schedule – read our blog post on How to optimise the cost and performance of Azure Virtual Desktop for more about auto-scaling.

One of the advantages of the Azure portal is that you can create as many host pools as you like, and once a host pool is set up, creating another one is quick and simple. Go to the host pool blade, click to add another one, then go through the wizard.

If you're deploying a new host pool in a different Azure region but using the same image, the image needs to be available in the target region so that you can deploy session hosts from it. Simply go to the Shared Image Gallery and replicate the image to your target region.

If you're creating a new host pool to provide a group of users with a new application, then you'll need to update your image accordingly and deploy the new host pool using that image.

7. Monitor and receive alerts

If you have a large or complex Azure Virtual Desktop environment, you'll benefit from setting up monitoring and alerts. This can be done using Microsoft's Azure Monitor for Windows Virtual Desktop, an out-of-the box solution that's currently in public preview.

Relatively straightforward to set up, it will help you optimise cost and performance and assist with trouble-shooting. Further, the only cost associated with Azure Monitor is the Log Analytics Workspace and once set up it gives you dashboards covering:

- connection diagnostics
- connection performance
- host diagnostics
- host performance
- user report
- utilisation report
- client report

Watch this Azure Monitor Insights video from Microsoft's Azure Academy for guidance on how to set it up.

8. Back-up the environment

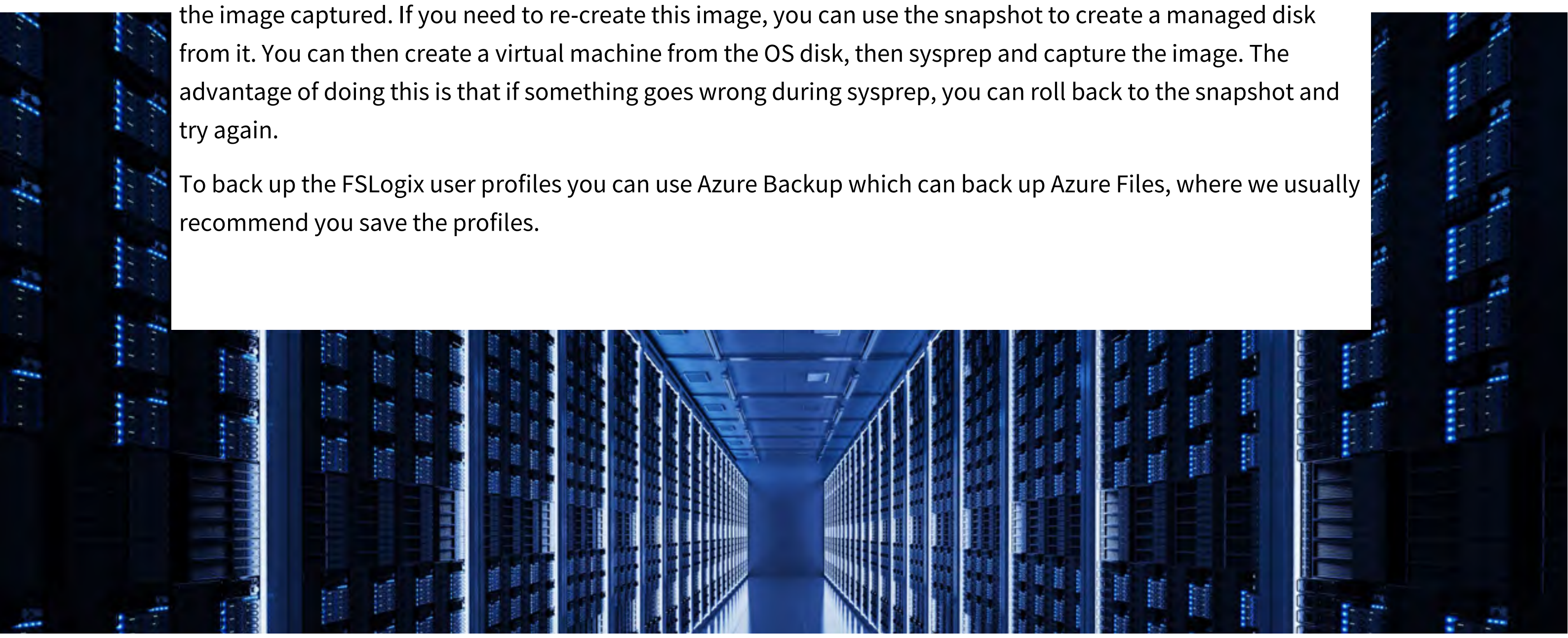
The main elements of your AVD set-up that need to be backed up are the images, session hosts and the FSLogix user profiles. You should also back up domain controllers, file servers and any other systems and data that your virtual desktop sessions are accessing.

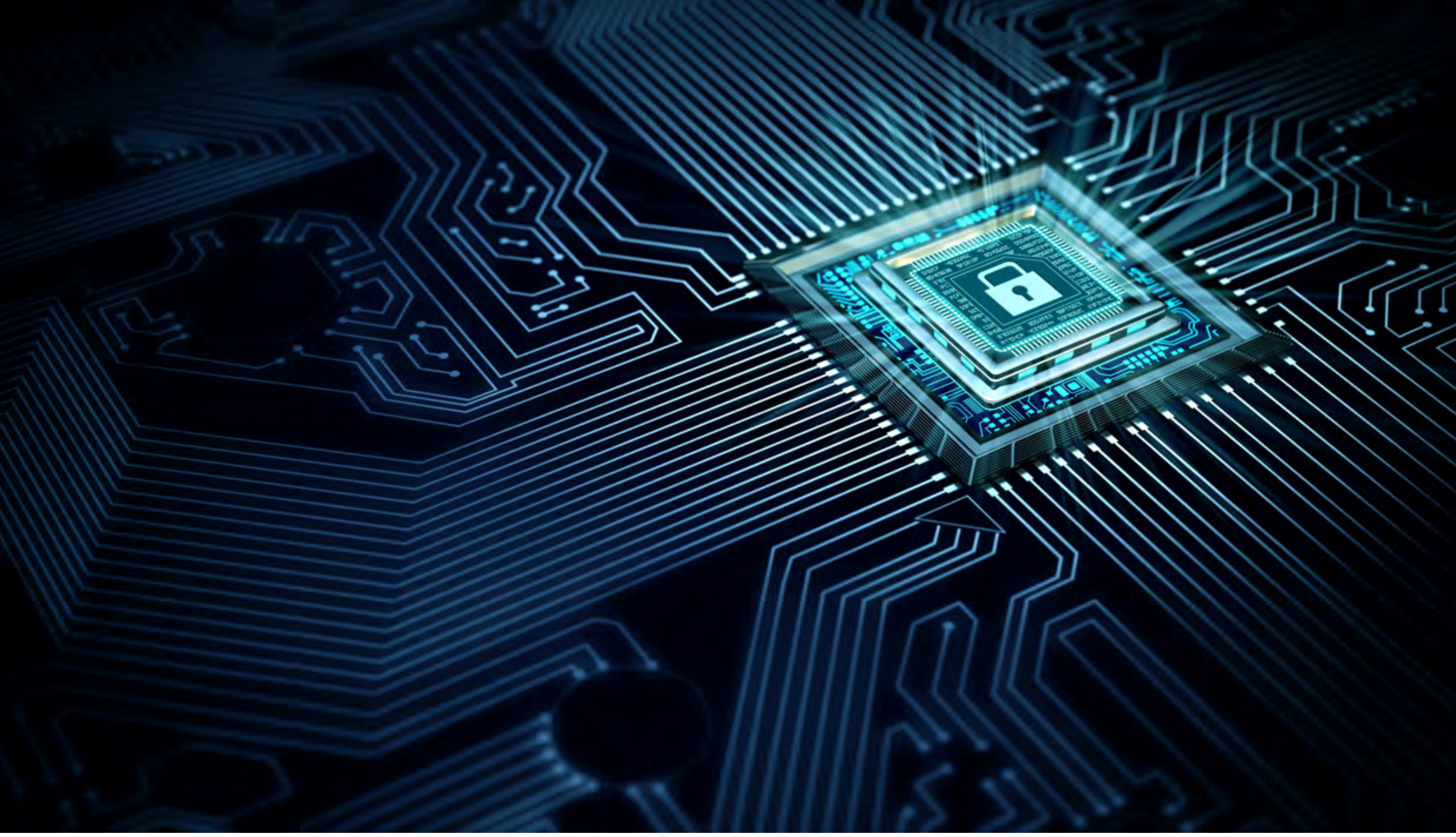
Session hosts are disposable, so there's no need to back them up. However, the images you've created are vital for creating new session hosts and we recommend that you protect them. By default, Azure keeps at least three copies of your images, however this won't prevent accidental deletion, which also deletes the replicas. To protect against this, set up a Deletion Lock in the Azure portal:

- Go to the image blade.
- Click on Locks to set it up.
- Remove the Lock first if you do want to delete the image.

Azure doesn't offer a way to back up the image itself, therefore the best work around for this is to take a snapshot of the OS disk of the virtual machine being used to create the image just before it is sysprepped and the image captured. If you need to re-create this image, you can use the snapshot to create a managed disk from it. You can then create a virtual machine from the OS disk, then sysprep and capture the image. The advantage of doing this is that if something goes wrong during sysprep, you can roll back to the snapshot and try again.

To back up the FSLogix user profiles you can use Azure Backup which can back up Azure Files, where we usually recommend you save the profiles.





CHAPTER FIVE

Security best practice for Azure Virtual Desktop

With the unprecedented and sustained rise in remote working in the UK and the rest of the world over the last year, IT security is more of a hot topic than ever. Not only has Azure Windows AVD (AVD) made Virtual Desktops accessible and affordable for all businesses, state-of-the-art security gives you peace of mind that your IT infrastructure can be set up with a secure foundation from the outset. This Chapter shows the IT lead in your organisation how to set up Azure Virtual Desktop securely, to keep your IT environment and data in safe hands. You may be looking for a virtual desktop or remote app solution. Alternatively, you may have already got Azure Virtual Desktop set up and want to ensure security best practice from day one.

Security is a continuous process of ensuring that you have robust checks and balances in place to protect your Azure Virtual Desktop environment. In this Chapter we give you an overview of the four key areas to look at:

>> Managing identity and devices

>> Protecting session host virtual machines from external threats

>> Addressing your organisation's data and information security

>> Monitoring security on an ongoing basis

Managing identity and devices

Users always sign into their Azure Virtual Desktop sessions using their Azure AD credentials, so it's vital that you protect this identity. You'll also need to consider which devices they'll be using to connect to their sessions.

You can protect your users' ID and control the devices they can use to access the virtual desktops in two ways – by enabling multi-factor authentication (MFA) for users in Azure AD, then by using Conditional Access to apply MFA for the Azure Virtual Desktop client itself. This mitigates risk and significantly improves overall AVD security.

MFA: enabling MFA for all users and admins in Azure Virtual Desktop improves the overall security of your Azure Virtual Desktop deployment.

Conditional Access: along with MFA, Conditional Access enables your admin to select which specific users should be granted access based on which devices they are using, their location and how they sign in etc.

For further guidance, these Microsoft tutorials explain how to setup MFA and Conditional Access when using Azure Virtual Desktop. This video from The Azure Academy also provides useful guidance about setting up MFA and conditional access.

Protecting session host virtual machines from external threats

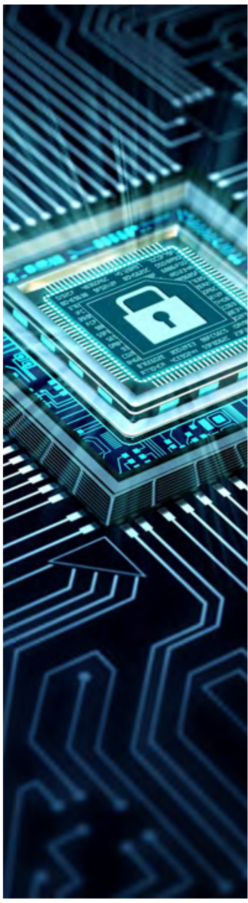
Having protected the identity of the users accessing the Azure Virtual Desktop service, it is important to protect the session hosts themselves including your operating system, applications and network.

Use Network Security Groups and firewalls

The virtual machines and virtual network deployed as part of your Azure Virtual Desktop deployment are key endpoints and securing these determines the overall effectiveness of your security. The inbound and outbound networking rules and regulation of your overall network traffic to the virtual machines affects their exposure to external threats and hackers.

You should at least configure a Network Security Group (NSG) and attach it to the subnets that your Azure Virtual Desktop session hosts are deployed in to protect them.

NSGs can contain multiple inbound and outbound security rules. As described in Microsoft's article, Network Security Groups, these enable you to filter traffic by source and destination IP address, port, and protocol. Therefore, your NSG should contain the outbound rules required for Azure Virtual Desktop and detailed in this Required URL list.



An NSG is free and is simply an access control list (ACL), it is not intelligent like a Firewall. However, if you need application rules and web filtering, you can configure all the Azure Virtual Desktop traffic to go through a firewall using a route table.

This could be your own, on-premise firewall if you're connecting to your Azure environment across a site-to-site VPN or a network virtual appliance (NVA) in Azure. There are a range of third-party solutions in Azure Marketplace or Azure Firewall, which provides managed, cloud-based network security and is a fully stateful firewall service.

See the following video from The Azure Academy on Azure Virtual Desktop network security using VNet, NSGs and Azure Firewall as well as this Microsoft article for more information on using Azure Firewall to protect Azure Virtual Desktop deployments.

Protect against operating system, application and software vulnerabilities

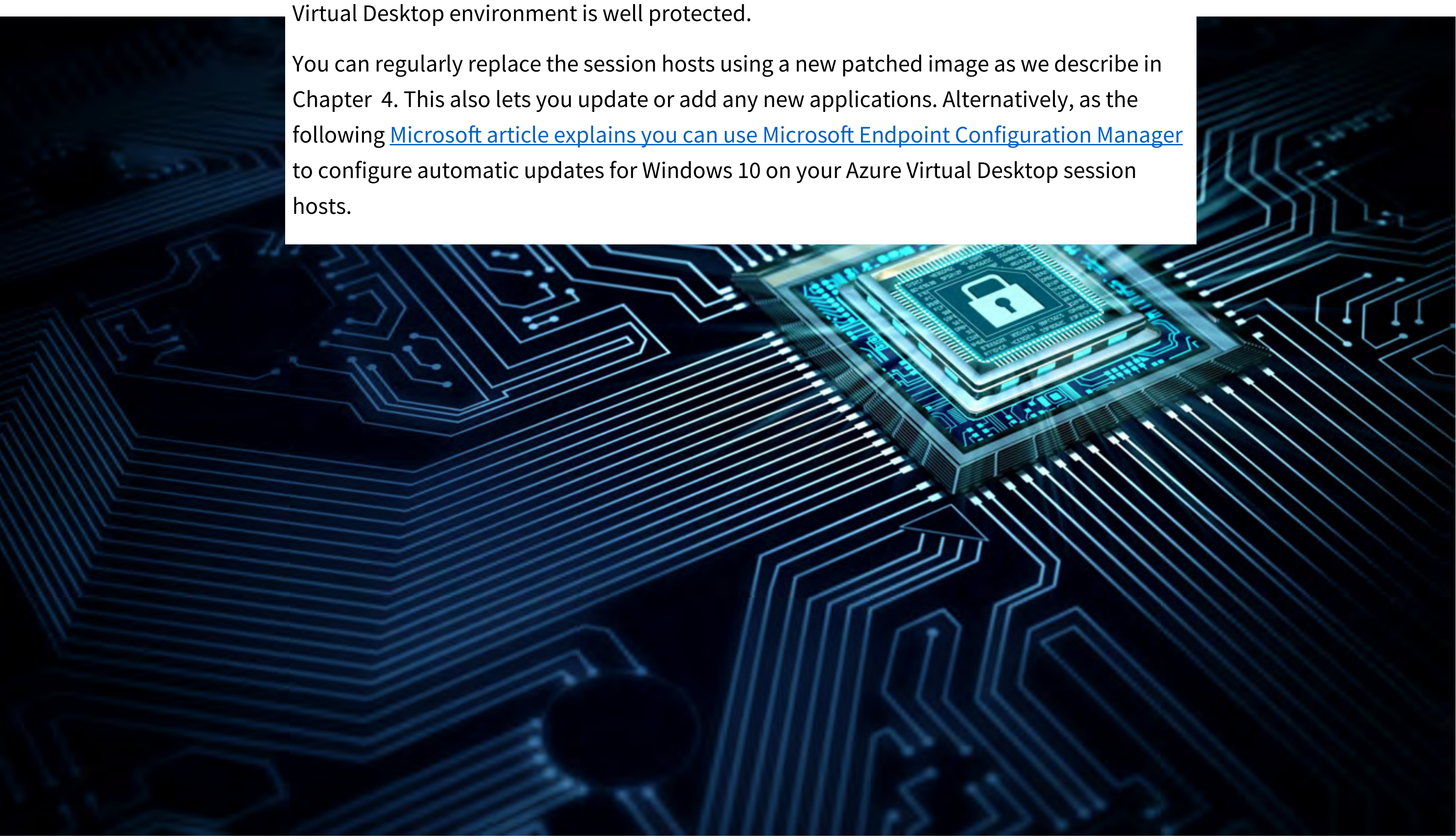
Identifying malicious software and software vulnerabilities within your operating system (OS) and applications is the key to proactive, preventive security measures to keep your Azure Virtual Desktop environment safe.

Enabling end point security for your session host virtual machines (VMs) protects your overall Azure Virtual Desktop deployment from malicious software. Tools like Windows Defender and ATP (Advanced Threat Protection) proactively address OS and application-level vulnerabilities, identifying problem spots through vulnerability assessments for server operating systems. Read the deployment guide for Microsoft Defender Antivirus in a virtual desktop infrastructure (VDI) environment to configure your VMs for optimal protection and performance.

Apply patches and security updates

Regular patches and security updates to your OS and applications ensure that your Azure Virtual Desktop environment is well protected.

You can regularly replace the session hosts using a new patched image as we describe in Chapter 4. This also lets you update or add any new applications. Alternatively, as the following Microsoft article explains you can use Microsoft Endpoint Configuration Manager to configure automatic updates for Windows 10 on your Azure Virtual Desktop session hosts.



Addressing your organisation’s data security

It is vital to consider the company data that users are able to access via their virtual desktop sessions and whether this is secure.

Control how users copy and transfer data

You can protect your organisation’s data from being copied or transferred to local devices and disable any features which compromise data security. This can be done by controlling access and setting the RDP properties in the Azure Virtual Desktop host pool from Azure Virtual Desktop to the following external devices:

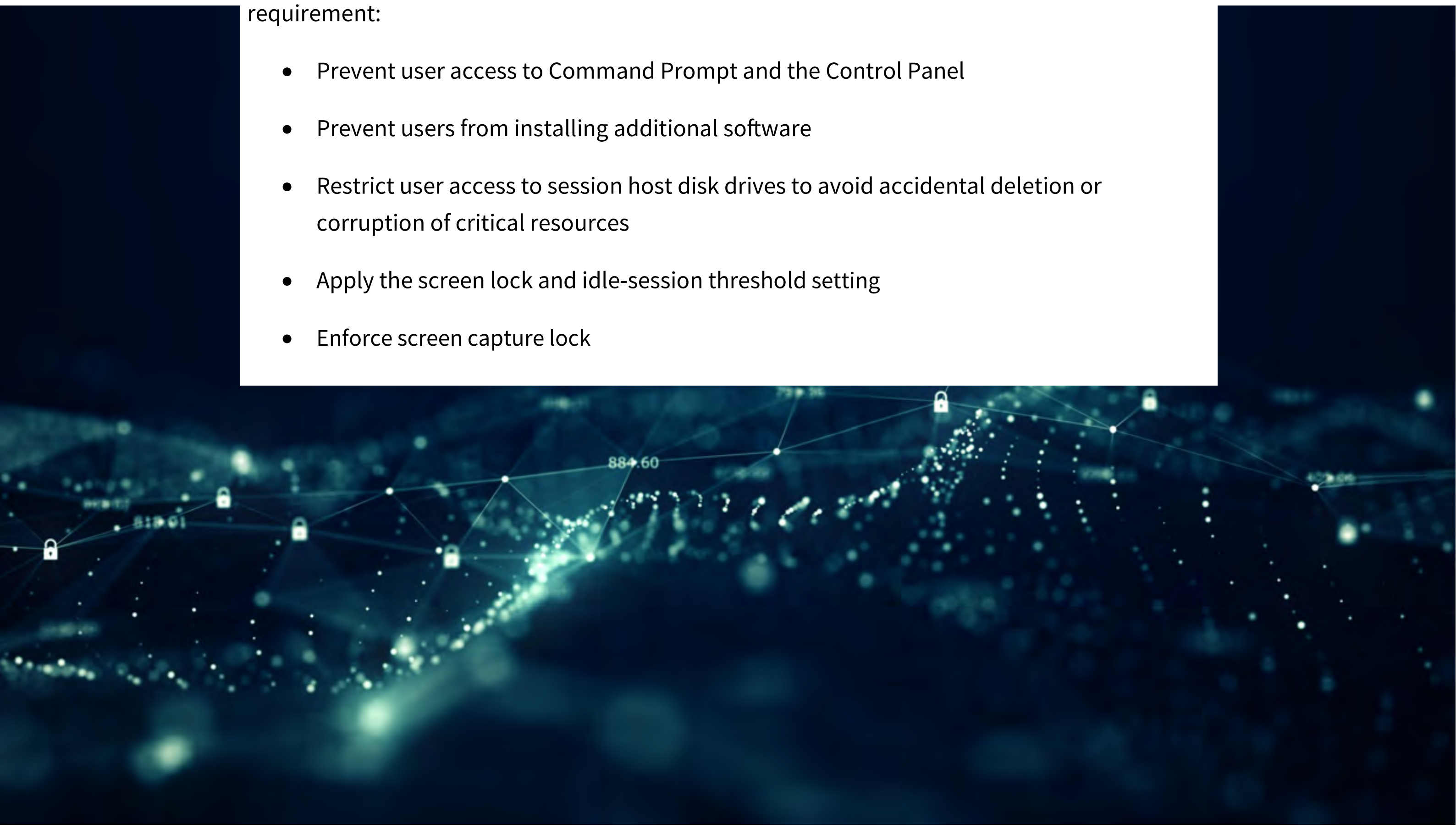
- Printers
- Local drives
- USB drives
- Clipboard
- Screenshots
- Camera

The following table details which settings are needed for Azure Virtual Desktop device redirection.

Control user access in Azure Virtual Desktop sessions

You can leverage Azure AD DS or Windows AD domain services based on your deployment model and enforce group policies that regulate which actions are allowed by your Azure Virtual Desktop users. Below are just some of the policies that you can apply according to your requirement:

- Prevent user access to Command Prompt and the Control Panel
- Prevent users from installing additional software
- Restrict user access to session host disk drives to avoid accidental deletion or corruption of critical resources
- Apply the screen lock and idle-session threshold setting
- Enforce screen capture lock



Encrypt your VM disks

Encryption will protect your organisation’s session host OS and data disks from unauthorised users gaining access and copying them.

For disks on session host VMs, you can achieve this with Azure Disk Encryption. Using the Bitlocker feature of Windows, it provides volume encryption for the OS and data disks of Azure virtual machines (VMs). It is also integrated with Azure Key Vault to help control and manage disk encryption keys and secrets. This quick-start tutorial shows you how to enable Azure Disk Encryption for session host VMs disks using Azure Key Vault.

Monitoring security on an ongoing basis

Securing your environment isn’t something that you can do once and then forget about. As threats change, you’ll need to continue monitoring and evolving the security for your Azure Virtual Desktop environment accordingly.

Azure Security Center

Enabling Azure Security Center provides a unified management platform to secure all your Azure resources including AVD. A wealth of tools and services proactively manage vulnerabilities and perform assessments of your overall Azure Virtual Desktop configuration to check whether you are compliant and implement preventive solutions to strengthen your overall security. The following quick-start tutorial shows you how to setup Azure Security Center.

Audit Logs collection and Azure Monitor

It is recommended to enable audit log collection and leverage Azure monitor. Azure Monitor helps to identify any issues in operations of the infrastructure, including checking your applications maps, network latency and error exceptions which indicate security issues and authentication errors. Find out more about Azure Monitor and using Log Analytics for the Diagnostic feature in this article.

There is not a one-off answer to IT security, it must evolve over time to proactively respond to ever-changing security threats. For more useful insights from Microsoft read the following articles on Security Best Practises and the Azure Security Baseline for AVD.

Contact Us

Compete366 are a Microsoft Cloud specialist with Gold Competencies in Azure and Office 365.

Please contact us for a free, no-obligation discussion with one of our certified Azure consultants. They will guide you on how to set up and manage Azure Virtual Desktop.

When you work with Compete366 to implement Azure Virtual Desktop, we provide free guidance on the Azure and Microsoft Office 365 elements including how to optimise Azure Virtual Desktop for cost and performance. The only IT knowledge you'll need to implement and manage this environment are traditional desktop management skills.

☎ 020 3282 7186

✉ engage@compete366.com

🌐 compete366.com

Compete366 Ltd

Registered Office: Heathmans House, 19 Heathmans Road, London , SW6 4TJ

Compete 366

Microsoft Partner | Gold Cloud Platform
Gold Small and Midmarket Cloud Solutions
Gold Cloud Productivity