IRIS | Anywhere

Unlock the Power of **Azure Virtual Desktop**

The IRIS Guide to Azure Virtual Desktop

Contents

IRIS | Anywhere

Introducing **Azure Virtual Desktop**

The IRIS Guide to Azure Virtual Desktop

What is Azure Virtual Desktop?

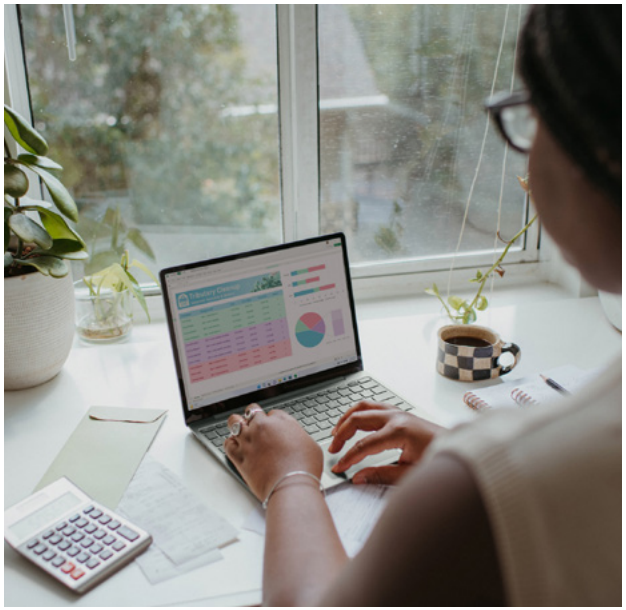
Azure Virtual Desktop (AVD) is a flexible cloud desktop infrastructure platform that securely delivers virtual desktops and remote apps with maximum control. AVD enables a secure remote work environment with a fully optimised Windows experience in minutes, providing you and your users the same flexible experience that you would have on a local desktop or laptop.

AVD offers greater flexibility and mobility for your employees to connect from any location, as well as offering enhanced security and data protection. This makes Virtual Desktops a key technology for many organisations worldwide, especially as 58% of organisations intending to deploy AVD in the next 24 months.

Azure Virtual Desktop also allows for the entire desktop environment to be managed centrally, streamlining IT management and support, saving you time and resources as opposed to managing and maintaining each individual device in traditional desktop environments.

AVD is also highly scalable and therefore, you can provision and deprovision virtual desktops quickly and easily, making sure you have the ability to scale up on-the-fly ensuring your organisation always has the resources that it needs to operate at peak efficiency.

The Microsoft ecosystem is another huge reason why Azure Virtual Desktop is massively popular among modern businesses. Azure Virtual Desktop is fully integrated with the Microsoft Azure ecosystem, letting you take advantage of the powerful Azure platform and all the capabilities that come with it including rapidly onboarding and enabling access remotely to company desktops and apps with an optimised Microsoft 365 and Microsoft Teams experience for your hybrid or remote workforce. Your employees will be able to work in an environment that is completely familiar to them.



58%

of organisations intending to deploy AVD in the next 24 months

Source: eG Innovations

How does AVD work?

Key Features

Azure Virtual Desktop is packed with features and capabilities that will allow your business to take advantage of the power of cloud-based virtualisation.

Full Desktop Virtualisation

Azure Virtual Desktop lets you set up full desktops within a cloud-based environment, meaning that you can fully implement powerful cloud-based remote desktops to be accessed using any device — with the ability to fully configure your cloud setup.

However, not all businesses require all their users to have a complete desktop environment, if you would like to deliver and manage individual apps to users instead of a full desktop, you can use AVD remote app streaming.

Remote App Streaming

Remote application streaming allows you to run your app in Azure and stream it to a remote device soyou can deliver your organisation's applications as a Software as a Service (SaaS) solution for users inside and outside of your organisation.

Some of the benefits of using AVD Remote App Streaming include:

Reduced latency – app streaming allows your users to use remote apps with little to no lag because data is compressed, only the data needed to run the app is sent rather than the entire application.

Improved performance – there is no lag, or slow load time with AVD remote app streaming as apps are streamed directly to target devices.

Increase flexibility – AVD remote app streaming is not tied to a single device or location, any device with an internet connection can stream your apps.

No multi-installation required – With AVD, you can install the app once and use it on any compatible device.

Improved productivity – Users can access their apps from any location, so with AVD remote app streaming, your users can be productive even away from their desks.

Enhanced security – AVD provides a secure connection to support remote app streaming, minimising the risk of data theft or other security threats.

Reduced cost – by streaming apps remotely, users can avoid the need to purchase and install multiple copies of their apps.

AVD remote app streaming can be a great solution for those who need to use a specific app that is unavailable and unsupported on certain devices, or simply for saving battery life. As remote work becomes more frequent, AVD can keep everyone connected and productive.

Access External Peripherals

Using a virtual desktop on a remote device, you can utilise any peripheral that you would on that device within the virtual environment.

This means that any mice, keyboards, microphones, webcams, etc. that you'd use within the office can also be used remotely meaning that you never have to sacrifice any functionality for remote working.

Access from Any Device/OS

Flexibility is a vital aspect of the modern business world. With remote working and the ability to work on the go, more flexibility allows your business to thrive.

Azure Virtual Desktop allows access from any device or OS that can utilise remote access programs, making flexibility easier than ever. Whether it be a home computer, mobile device, or even simply a computer in another office, Azure Virtual Desktop makes it far easier to work flexibly.

Auto-Scaling of Resources

As a business, your needs will fluctuate as your business grows and expands. Scalability is a massive part of this — it allows your business to adapt to new changes with complete flexibility, meaning that you're easily able to expand and scale up without overspending when it's required.

With Azure Virtual Desktop, you can scale your session host pool based on user demand, this is particularly useful if you have a lot of users who need access to your pool during peak times but don't need it during off-peak.

AVD allows you configure two types of autoscaling:

- Scale based on a schedule
- Scale based on load

Remote management

Working with cloud-based environments means that you can manage anything remotely.

This allows your management to be more flexible and applicable to your organisation's needs and means that you can far more easily make sure that important management functions can be done remotely.

Create a Golden Image for all Virtual Desktops

Azure Virtual Desktop allows you to create a custom image to use for all of your Azure environments.

This is known as a 'golden image' and is an Azure image that is configured and set up in the manner that you'd like to deploy the rest of your virtual hosts.

300m

people globally have used Microsoft Teams in the past 12 months

Source: Microsoft

Benefits of Azure Virtual Desktop

Sensitive Data is Never on the Endpoint

Azure Virtual Desktop lets you store your sensitive data on cloud servers hosted by Microsoft, which means that data will never be stored on-premises.

This means that you can ensure that the data that is stored on the cloud can never be breached physically through hardware, as it will be stored in the protected Microsoft cloud server hardware, making it near impossible for that data to become compromised.

The Ability to Work From Anywhere on Any Device

Azure Virtual Desktop will allow you to work from anywhere on any device, adding great flexibility to your organisation.

Whether you want to access your virtual desktop from home, during travel, or even from other locations, Azure Virtual Desktop makes it simple to do so. All you need is a remote desktop connection application, which will easily let you access your virtualised desktop no matter what device you are using.

Reduce Hardware Costs with Thin Clients OR Enable BYOD

High-performance hardware is important for modern organisations but can get quite costly when supplying every employee. Azure Virtual Desktop gives you access to high-powered hardware without having to spend on hardware, instead allowing you to use any computer to access the virtual desktop.

With Azure Virtual Desktop, you can use lower-powered hardware to simply access the cloud-based virtual machine — or even introduce bring-your-own-PC to your organisation. This will save costs on hardware all around, without sacrificing operating power.

82%

of organisations worldwide have enabled a Bring-Your-Own-Device (BYOD) program to some extent

Source: Bitglass

IRIS | Anywhere

The Azure Virtual Desktop Implementation Journey

The IRIS Guide to Azure Virtual Desktop

Define Strategy

The first step in the implementation journey is defining your strategy for implementing Azure Virtual Desktop. This includes:

Motivation for Implementation

Knowing why you're implementing Azure Virtual Desktop into your organisation, and what you want to do with it, is vital to creating your strategy.

Business Justification

Part of strategising is understanding the business justification for implementing Azure Virtual Desktop into your business. Why would it be beneficial to your business?

Business Outcomes, Goals and KPIs

Going on from this, working out tangible goals to ensure that your business is successful is vital. Using Key Performance Indicators (KPIs) is a great way for you to measure this — what are your metrics of success, and how will you measure them?

Assess

Once you've defined your organisation's strategy, the next step is to assess your organisation's current position to ensure that your long-term strategy can be deployed effectively.

Evaluation

Here, you'll need to evaluate your business's current position and what needs to be implemented into the Virtual Desktop. This includes key stakeholders and the most critical parts of your business' infrastructure, to ensure that your organisation can effectively move forward.

Plan

Planning is vital, as you'll have to assess everything that the Virtual Desktop setup will include. This is a complex process, and so working with an established partner to ensure that your organisation's assessment and planning are thorough is the best way to move forward here.

Configure

The next step is to configure Azure Virtual Desktop within your organisation, which is a process that has multiple steps. There are multiple steps to this process, the first being setting up your host pool.

A host pool is a collection of multiple identical virtual machines within Azure Virtual Desktop. These machines contain an app group that users can interact with as they would on a physical desktop, to which you can send resources equally.

Personal

Personal host pools are pools where session hosts are signed to individual users.

Pooled

Session hosts can accept connections from any authorised user in the host pool.

After configuring your host pool, the next step is to deploy. The process of deployment is a multi-step process.

Session hosts

Adding session hosts to your existing pool will increase the number of VMs accessible within your host pool.

Golden Image

A golden image will be the basis for all session hosts and will be the default configuration for all host sessions.

Application Group, Workspaces, and Users

You'll need to make an application group, then add it to a workspace and assign users to the workspace through the Azure portal.

Adoption

The final stage is adoption, which is the process of getting your organisation ready at an infrastructural level to use and implement Azure Virtual Desktop.

The key steps for adoption are:

End-user training

Your employees will also need to know how to work with the new Azure Virtual Desktop environment and so end-user training to get everyone informed is vital.

Management and Optimisation of Infrastructure and Security and Compliance

Your Azure Virtual Desktop environment is set up, however managing it correctly is another important aspect of ensuring that your Azure Virtual Desktop setup is sustainable for your business. There are many steps that you can take to ensure that management is done correctly with benefits to your organisation.

IRIS | Anywhere

Managing and Optimising Azure Virtual Desktop Infrastructure

The IRIS Guide to Azure Virtual Desktop

Ensuring that your Azure Virtual Desktop infrastructure is managed and optimised correctly is important to consider, as this will help you get the most out of your AVD system.

These steps are vital to ensuring that your Azure Virtual Desktop Infrastructure is maintained properly to benefit your organisation economically and infrastructurally.

Right-sizing VMs

Right-sizing a virtual machine is when you optimise the size of your VM to ensure that you get the best performance from your Azure Virtual Desktop infrastructure.

The process of doing this will allow you to optimise your allocation of resources to ensure that your VMs have the resources they need in an efficient manner. This will optimise running costs in the long term.

Turn Off VMs When Not in Use

Leaving your virtual machines running when not being used is a way to waste power and resources — your virtual machine will cost you whenever it's in use, and so leaving it running will cause your business to haemorrhage resources.

The best way to stop this is to simply turn off virtual machines when not in use. This will stop your virtual machines from running and stop these extra costs from accruing.

Delete Unused vDisks

Unused vDisks will take up space and resources even when not being used by a virtual machine. You'll often build up unused vDisks as time goes on, and these can take up lots of space within your host pool.

By deleting your unused vDisks, you reclaim the space within your pool, meaning that the storage space can be used by other vDisks.

Use Reserved Instances

A reserved instance is a billing concept that gives massive discounts when compared to 'on-demand' pay-as-you-go prices.

However, the reason that reserved instances are far cheaper is that you're essentially paying for a fixed level of usage, meaning that you do lose a bit of flexibility. The cost-saving aspects of this often do make it still worth using reserved instances, however.

Monitor Usage

The best way of knowing exactly what your usage is and what your needs are is by tracking and monitoring your Azure Virtual Desktop setup.

Azure Monitor lets you do exactly that, providing you with a powerful data platform which you can use to analyse and even diagnose and troubleshoot your system.

You can use this to receive alerts and notifications based on aspects of your Azure setup throughout your organisation, to ensure that you're up to date on every aspect of your Azure Virtual Desktop infrastructure.

IRIS | Anywhere

Enhancing Security and Compliance

The IRIS Guide to Azure Virtual Desktop

Let's now delve into a topic that remains of paramount importance in today's digital landscape - security and compliance.

The security of your cloud-based infrastructure isn't something to be taken lightly, and keeping your Azure VD infrastructure secure can help avoid significant losses and optimise your costs.

Here are some essential steps for ensuring security and compliance:

Control access and identity

Identity and control access for Azure VD systems is handled by Azure Active Directory (AD) - Microsoft's cloud-based identity and access management service.

One key method to enhance the security of your AVD infrastructure is to enable Multi-Factor Authentication (MFA).

MFA demands that users provide two or more verification factors to gain access to a resource, making it more difficult for unauthorised users to break in. It combines something the user knows (like a password), something the user has (like a phone), and sometimes even something the user is (like a fingerprint). Microsoft claims that enabling MFA can prevent 99.9% of attacks on accounts.

On top of MFA, Azure AD also offers Conditional Access. This security feature further enhances the control over your environment by enforcing certain conditions that must be met before access is granted.

Here, the principle of 'least privilege' should be followed diligently, meaning users should only have access to the resources they need to carry out their tasks - nothing more, nothing less.

Protect from external threats

In an increasingly interconnected world, the risk of external threats to your Azure Virtual Desktop (AVD) environment has never been greater.

Businesses must take necessary measures to protect themselves from such threats to minimise potential damage to their operations and reputation.

Encrypt All VMs

The first step in protecting your AVD from external threats is to encrypt all Virtual Machines (VMs).

Encryption transforms your data into unreadable text, which can only be converted back to its original form with the right decryption key.

Azure offers built-in capabilities to encrypt data at rest using Azure Disk Encryption and data in transit using Azure Network Platform Service Endpoints.

By encrypting your VMs, you significantly enhance the security of your AVD environment. Even if a malicious entity manages to gain access to your data, they will find it extremely difficult to interpret it without the decryption key.

99.9%

of account compromise attacks can be prevented with MFA

Source: Microsoft

Use Microsoft Defender

Microsoft Defender for Cloud is another robust tool for shielding your AVD from external threats.

It provides unified security management and advanced threat protection across hybrid cloud workloads. Microsoft Defender can detect unusual behaviour, provide actionable security recommendations, and improve the security posture of your AVD environment.

Control of How Users Copy and Transfer Data

In an AVD environment, it's essential to regulate how users copy and transfer data to protect against data leakage.

Azure's security configurations allow you to control these activities, enabling you to prevent unauthorised data copying or transferring that could expose sensitive information to external threats.

For instance, you can restrict clipboard access in your AVD settings or limit the types of devices that can be redirected.

Remain Compliant

In the complex and ever-evolving landscape of regulatory compliance, adhering to necessary standards and requirements is not just a good practice but a business imperative.

When using Azure Virtual Desktop (AVD), ensuring ongoing compliance is essential to avoid costly penalties, protect your reputation, and provide assurance to your clients.

Collect Audit Logs

The first step towards remaining compliant is to regularly collect and review audit logs. Azure provides comprehensive logging of activities within your AVD environment, making it easier to monitor and track user activities.

Audit logs offer valuable insights into who did what and when, aiding in investigations and helping to identify potential misuse or anomalies. Consistent logging and monitoring are also requirements under several regulatory standards.

Microsoft Defender for Cloud Built-in Regulatory Standards

Microsoft Defender also offers built-in compliance dashboards to help meet the most pertinent regulatory standards.

These dashboards provide an easy-to-understand compliance score, detail compliance recommendations, and provide insight into the steps required to improve your compliance posture.

For AVD environments, key standards to consider might include PCI-DSS for handling payment information, UK OFFICIAL and UK NHS for UK government and health data, HIPAA/HITRUST for health data in the US, and ISO 27001 for information security management.

Data Residency Requirements

Compliance also extends to where your data is stored. Data residency requirements dictate that certain types of data must remain within specific geographic boundaries.

Azure offers a broad range of regions worldwide, allowing you to store your data where required to meet these legal and regulatory obligations.

IRIS | Anywhere

How to Get Started with Azure Virtual Desktop

The IRIS Guide to Azure Virtual Desktop

Embarking on your journey with Azure Virtual Desktop might seem daunting at first, but with the help of an expert Managed Service Provider (MSP), this process can be a breeze!

MSPs bring extensive knowledge and expertise in deploying and managing AVD environments, ensuring that businesses can smoothly transition to this powerful platform without any hiccups.

We will guide you through the initial setup, including the configuration of your network, setting up user identities and access controls in Azure Active Directory, and configuring your virtual machines.

We'll also help you implement key security measures, like enabling multi-factor authentication and setting up conditional access policies, to ensure your environment is secure from the outset.

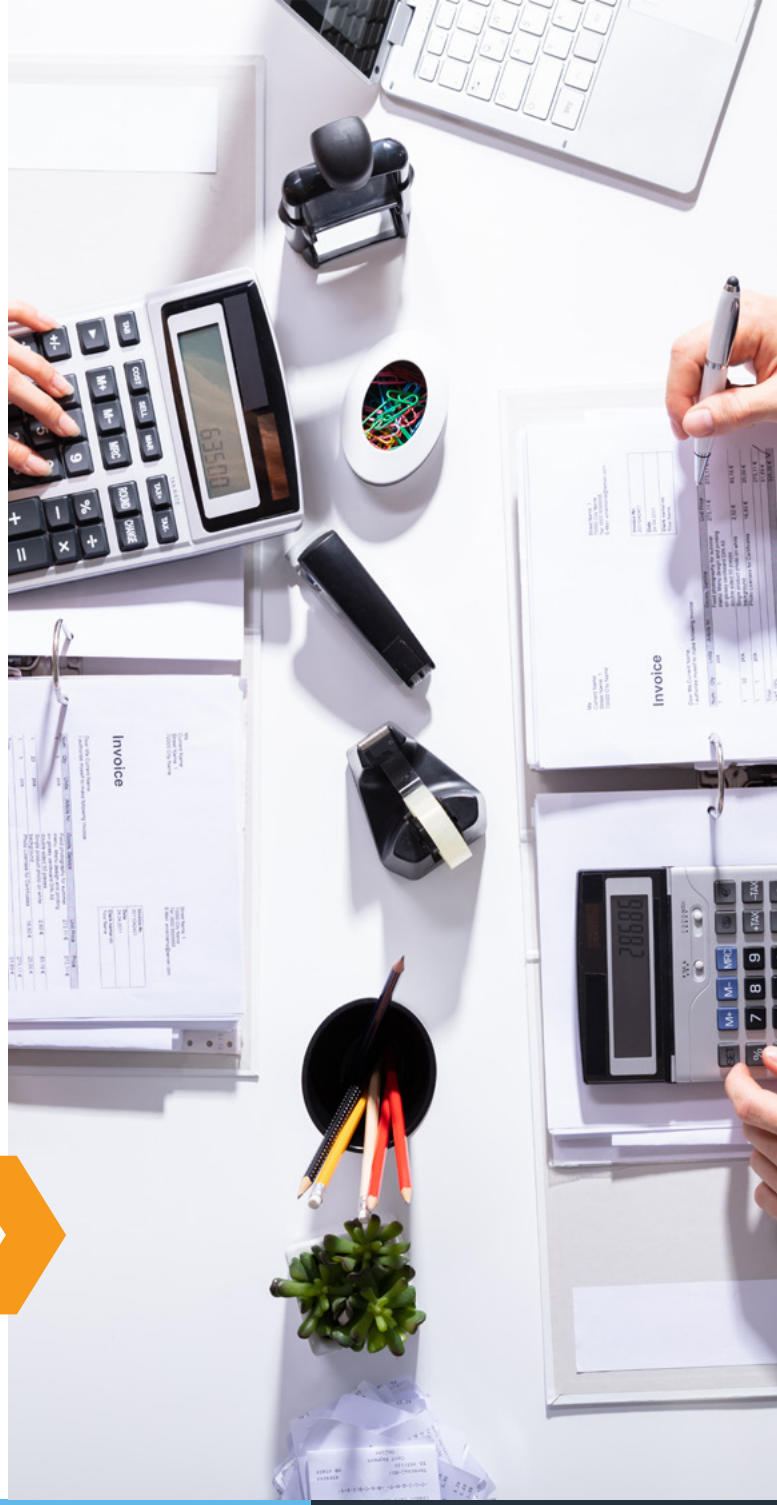
Additionally, we can provide invaluable support in maintaining compliance and set up your Microsoft Defender for Cloud to meet various regulatory standards, guide you through the necessary audit procedures, and help address data residency requirements.

We'll also offer ongoing support and management by monitoring your AVD environment, handle routine maintenance, and quickly resolving any issues that arise.

This allows your team to focus on core business tasks, instead of dealing with technical issues.

So, if you're considering AVD, don't go it alone. Partner with us to help you get started and reap the full benefits of this powerful platform while maintaining a secure, compliant, and cost-effective virtual desktop environment.

Get in touch today to see how we can help!



IRIS | Anywhere

How We Can **Help**

IRIS Anywhere empowers your accountancy firm to thrive wherever you need to work, through the combined power of the cloud and world class accountancy software.

Bringing together industry leading accountancy software with productivity boosting Microsoft tools into one single cloud-based platform, which is so much more than a hosted desktop.

iris.co.uk/products/iris-anywhere/

0344 815 5555