

ZONES
First Choice for IT™



6 REASONS
**AZURE VIRTUAL
DESKTOPS**
**ARE IDEAL FOR
YOUR BUSINESS**

In the era of remote work, you need a secure and flexible solution that enables employee productivity.

Azure Virtual Desktop.

Azure Virtual Desktop (AVD) provides a virtualized environment in which your workers access their desktops and applications through a centralized cloud portal. With this approach, the programs you use don't actually run on your local computers, but in the cloud.

6 Reasons Azure Virtual Desktops are Ideal for Your Business.



1 Full Windows Compatibility

With AVD you won't have to make any substantial changes to the way your employees work, or the applications they are used to running.

AVD is fully compatible with Windows 7, Windows 10 and 11. All of your present Windows programs, whether commercial or home-grown, plus familiar productivity applications like Office 365 (now Microsoft 365), can run under AVD exactly the way they currently run on your Windows computers.

AVD also offers a Windows 10 and 11 multi-session feature that allows multiple users to log into the same Windows virtual machine (VM). This means your employees can all share the same desktop and applications. It also lowers your costs since your AVD charges will depend, in part, on the number of VMs you are running.



2 Flexibility

In these days when the coronavirus pandemic has caused large numbers of employees to work from home, AVD provides them with the ability run the applications they need from literally anywhere there's an internet connection.

All that's required is a supported device with the AVD app installed, or even just a web-enabled device such as a laptop, tablet or smartphone that can support an HTML-5 browser. AVD client apps are available for Windows, MacOS, iOS, and Android devices.

This is one of those aspects of AVD that truly can be called game-changing.

The ability to run Windows applications from non-Windows devices provides a level of flexibility that was never before available, at least not with the ease of use and cost effectiveness AVD provides. Many of your employees will be able to work remotely without your business having to supply them with company-owned laptops or other devices. In many cases, if not most, they can use their own personal desktop computer, laptop, tablet, or smartphone with minimal adjustments for accessibility and security.



Scalability

Provisioning and scaling are areas in which cloud-based services excel. Traditionally, as your business grew you'd have to go through a cycle of purchasing new IT equipment and integrating it into your operations.

This took substantial amounts not only of money, but of time as well. But with cloud services like AVD, the cloud services provider (Azure in this case) is responsible for bringing additional resources online as needed.

In many cases it requires little more than the click of a mouse to instantly scale to the level required. And, as previously mentioned, until you actually use additional resources, you don't have to pay for them.



Security

With hundreds of thousands of employees now working remotely for the first time, data security has become an even greater concern than it previously was. Although business owners are sometimes concerned that using the cloud might make their data more vulnerable to being compromised by cybercriminals, in reality the opposite will almost certainly be the case.

According to Microsoft, the AVD security program benefits from Azure's long-established, industry-leading security profile. This includes a \$1 billion annual cybersecurity expenditure, 3,500 full-time security professionals, and continuous security updates. This robust security infrastructure can be a major asset to any business, large or small.

A particular advantage of AVD is that it does not require (in fact, need not allow) sensitive data to be downloaded to workers' devices.

All the applications and data remote workers use to perform their jobs are kept secure in the cloud. Workers use the AVD remote desktop to initiate and manage the applications they run without either the applications or the data they work with ever being brought into the user's device.

Although keeping endpoint devices free of malware should always be a high priority, with AVD the consequences of a failure in that regard will be much less than if sensitive information actually resided on the device.

One of the most important security benefits of AVD is that it allows centralized security management. Administrators need not worry about securing data that's being held on client devices. Security standards can be enforced from one place, and are much less dependent on the efforts of inexperienced end users.



Reduced Cost

Simply put, not having to purchase a fully equipped Windows-compatible computer for each worker who needs to run Windows applications can save you a lot of money.

First of all, AVD allows use of what are called “thin clients.” These are devices that don’t necessarily have the hard drives or the amounts of RAM a normal computer requires in order to operate on its own. These resources are not needed because all the real computing work is being done in the cloud, not on the device.

Thin client devices can cost substantially less than traditional desktop computers. For example, because a high degree of compute power is not required, a relatively inexpensive laptop might meet your employees’ needs as well as a high-powered desktop computer could.

Plus, in many cases you won’t need to purchase hardware at all if workers use their own personal devices to do their jobs remotely. In such cases, not only is your business relieved of the need to make capital expenditures for hardware, but it also avoids the ongoing operating expenses required to support those devices.

Like most cloud-based services, AVD operates on a pay-as-you-go basis. You pay only for the resources you actually use. You never have to purchase.



Disaster Recovery

An unforeseen disaster can be devastating to your business.

It can damage your physical infrastructure, disrupt your employees’ workflows, and present a major threat to the health of your data. But AVD makes achieving a high degree of disaster recovery and business continuity readiness much easier for corporate IT leaders.

Even if a fire or flood should destroy your business facility, with AVD your IT resources in the cloud would be unaffected. Employees could continue their work from any location with an internet connection. That means that in many cases, with proper planning, your business will be able to continue serving customers even while its physical facilities (and computer equipment) remain unavailable.