Ace Cloud Hosting

WHY VDI MAKES SENSE IN TODAY'S WORLD

WHITEPAPER

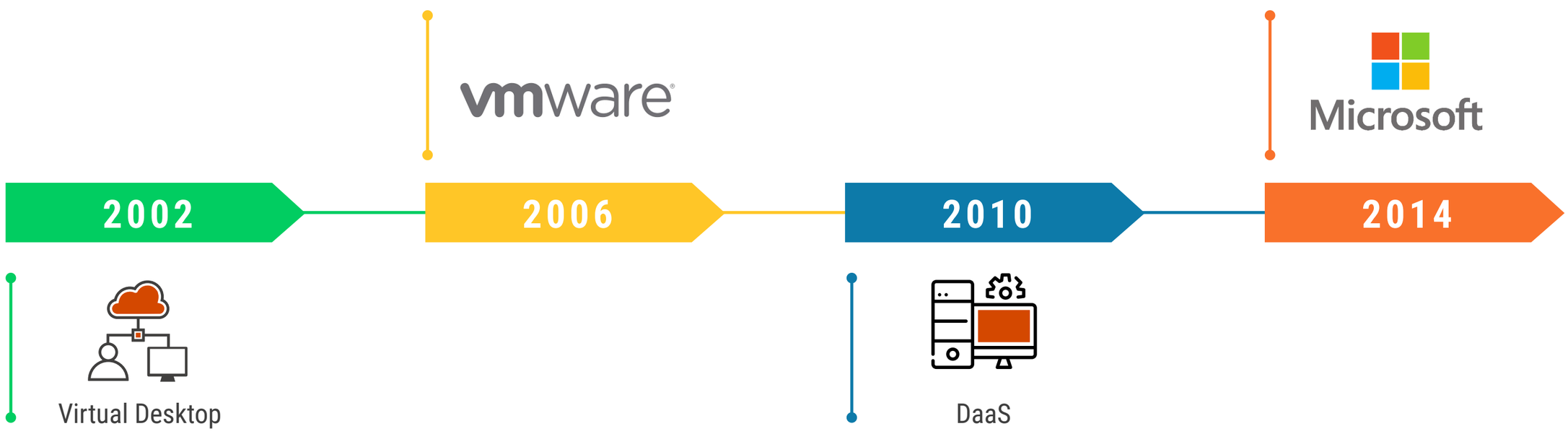
Table Of Contents

Introduction: What is VDI?

With time, we have seen technology bring tremendous changes to our lives. However, providing an optimized desktop environment for the workforce remains a challenge for many organizations. The traditional desktop environment is no longer viable for the current generation. They seek a desktop solution that is mobile, secure, and scalable.

With VDI or Virtual Desktop Infrastructure, industries can cater to the ever-changing needs of their workers and customers alike. VDI is a technological model that enables an organization to provision and deploy virtual desktops over a cloud server. Using VDI brings significant benefits and helps drive up productivity and efficiency in the workplace

VDI History



The term VDI was coined for the first time in 2006 by VMware. But people have been using virtual desktops since as early as 2002. However, at that time, there was no actual connection broker (discussed below), prompting people to use Microsoft Remote Desktop Protocol for connecting to their Virtual Machines (VMs) on VMware and ESX servers. In 2006, VMware coined the term “VDI,” which prompted other prominent organizations like Microsoft and Citrix to push their VDI products for sale.

By the mid-2010s, another desktop virtualization type was introduced, DaaS (Desktop as a Service). DaaS began drawing the attention of various businesses towards VDI and further increasing its outreach.

By 2014, Microsoft eased its licensing restrictions, which solved the excessive licensing fee problems. Other vendors, namely Citrix and VMware, followed similar paths, which provided growth for the VDI industry.

Components of the VDI

There are three main components of VDI: **Hypervisor, Connection Broker,** and **End devices.**

Hypervisor

A **hypervisor** is the heart and soul of a VDI environment. It is software that carries out virtualization. The underlying software and hardware are abstracted and virtually divided to create virtual desktops with virtualization. Let's understand this with an example. Suppose you had 16GB RAM and a 1TB hard disk.

With VDI, all the resources are housed as standard units in their data centers. The hypervisor abstracts these resources, which you can then allocate accordingly. So, if you have 16GB of RAM and a 1 TB hard disk, instead of scratching your head on how to partition them, the hypervisor will virtually segment them into the divisions of your choice. You can also create a single golden image and replicate it or create customized virtual images, varying with the needs.

Depending on the modus operandi, a hypervisor can be of two different types:

- Type 1 hypervisor
- Type 2 hypervisor

Type 1 hypervisor - also known as the Native hypervisor or bare-metal hypervisor, this type does not depend upon any underlying OS to carry out virtualization. It can be directly incorporated into your data centers.
Examples: Microsoft Hyper-V hypervisor, Citrix XenServer, etc.

Type 2 hypervisor - also known as the Hosted hypervisor, needs a pre-existing OS to carry out virtualization.
Examples: Parallel Desktops, Oracle VM VirtualBox, etc.

Connection Broker

A **connection broker** is software used to manage incoming user permissions for accessing virtual desktops. Its role is similar to that of a guard in a commercial parking space who validates your entry pass for parking your car at a pre-designated spot. Similarly, a connection broker authenticates the user requests and directs them to virtual desktops. It is essentially your resource manager, responsible for handling your network of virtual desktops.

Thin-Client Device

Strictly speaking, a **thin-client device** is a computer that works by accessing resources from a centralized setup instead of having them installed locally. Imagine this as withdrawing water from a large water tank, where you need to have individual containers for holding water. Similarly, while the hypervisor partitions the hardware resources and creates virtual desktops, you need the thin-client devices to access them. They have double the lifespan of a standard PC and are comparatively less expensive to maintain.

VDI Deployment Models

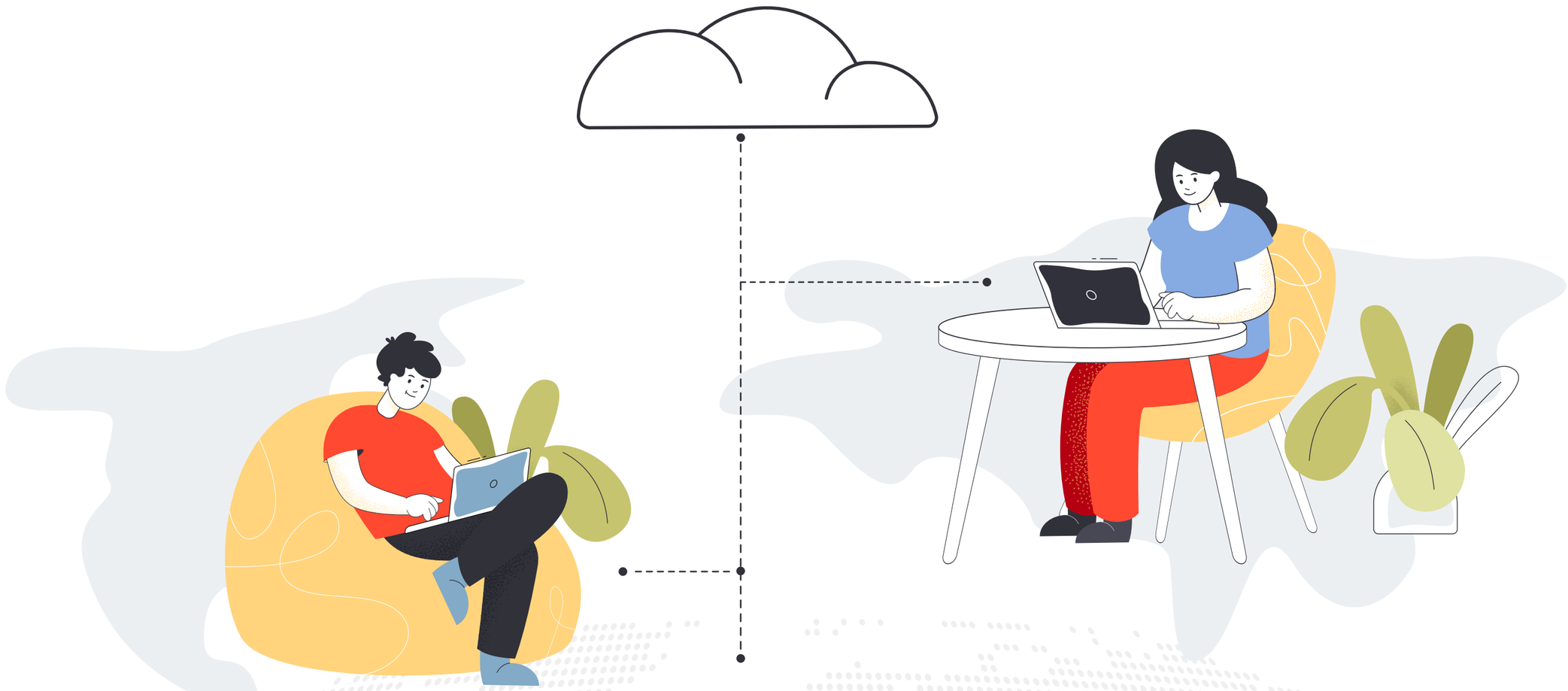
The virtual desktops hosted within a VDI can be of two different types based on their deployment methodologies:

- Persistent VDI: A persistent VDI, also known as a stateful VDI, is a type of VDI in which in-session changes remain after the session termination. Simply speaking, it is similar to using a personal desktop where the changes are carried forward to the next session. So, the next time a user logs in, they can access their previously saved configuration settings or data.

- Non-Persistent VDI: On the contrary, in a non-persistent VDI, a virtual desktop reverts to its base configuration after the user logs out. It is like using a fresh virtual desktop every time you log in. It is not possible to access your previously saved data or permanently change its configuration. For any such changes, you must modify its base image, which then, upon modification, gets reflected next time you log in.

Both deployment models have their unique characteristics and features and cater to different organizational roles. Persistent VDI offers a great deal of end-user customization, making it ideal for power users. Non-persistent VDI requires simpler IT management than the persistent VDI and is comparatively easier to deploy.

The Benefits of Using VDI



- **Device Independence:** Unlike the conventional desktop unit, this is a dedicated 1:1 model and does not allow you to use hardware resources from another device. Users can use thin-client devices or a personal desktop or laptop to access organizational data and applications

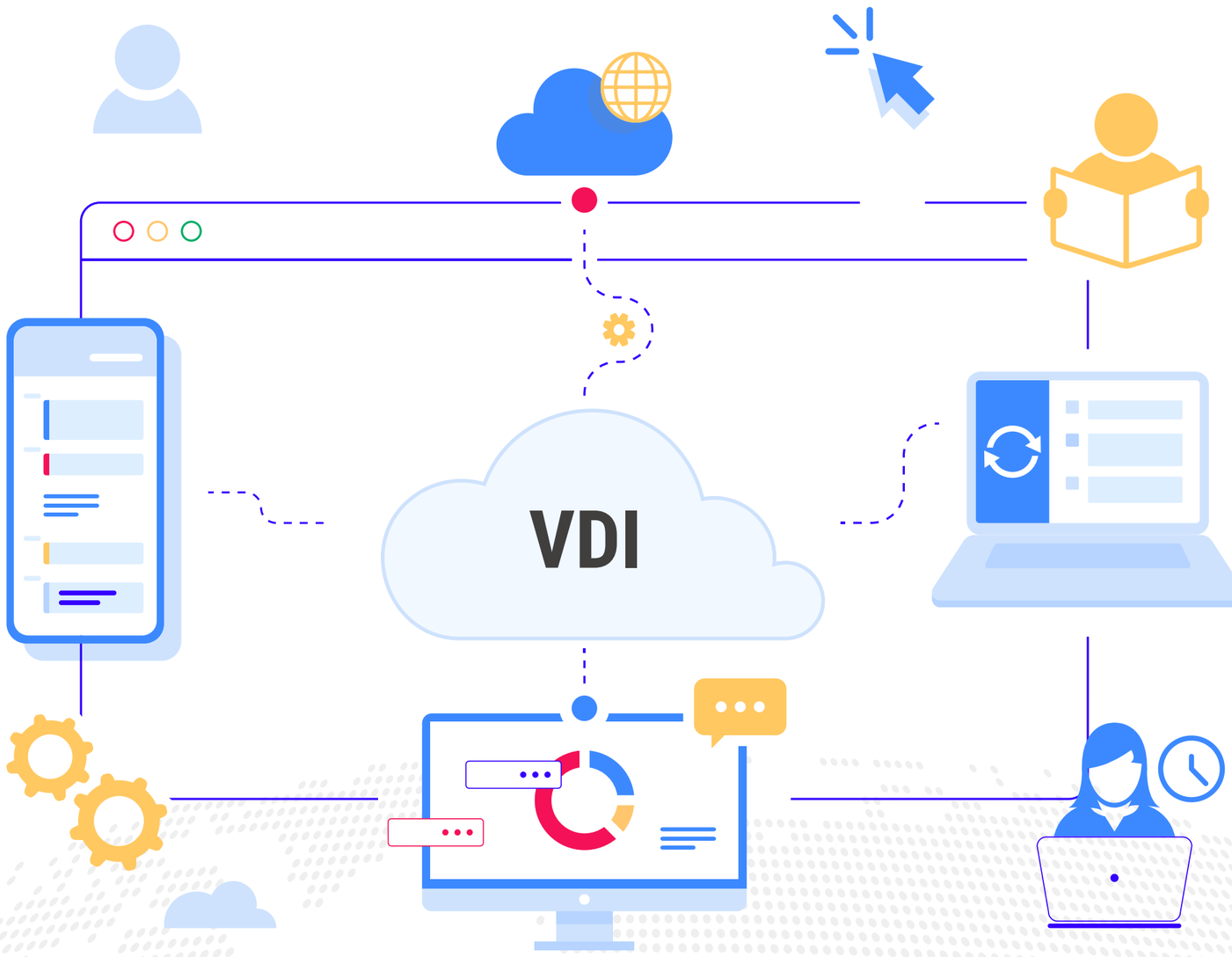
- **Extended Accessibility:** Another benefit of VDI is its accessibility. A traditional desktop environment is device-bound, making it impossible to remotely access. However, in a VDI, you can access a virtual desktop from anywhere, anytime via the Internet. Depending on your network strength, the range of your remote accessibility can vary from within your office space to even faraway geographical positions.

- **Desktop Scalability:** In a hosted VDI solution (when you opt for VDI services from a service provider), scaling up your resources is quite easy. Instead of procuring individual hardware and software components, all you need to do is contact your VDI provider for enhanced resources. This way, you get the flexibility to scale when you need additional resources at an economical price. You can also descale if required and save your finances. However, this benefit is not available with a traditional VDI setup, as procuring new components is an expensive and tedious task.

- **Resource Utilization:** VDI allows you to use your available resources efficiently. Unlike a traditional desktop environment, where the unused storage cannot be used for another device, the hypervisor allows you to track and optimize your resources. You can either set up a new virtual desktop using the unused resources or shift resources from a less-priority device to a higher-priority device. This way, you can also boost your organizational productivity by optimally using the resources.

- **Security Benefit:** On a traditional desktop, getting a particular device compromised or stolen always carries a risk of permanent data loss. However, with VDI, the device only acts as a medium between the user and the server. This means that it does not store any data. So, if your device gets stolen, you can remove its access, and your data will be safe.

How to implement VDI



- **Selecting The Right Platform:** Before you decide to deploy a VDI solution, select which platform you want to work on. For example, while Xen and KVM hypervisors are only Linux-compatible, Microsoft Hyper-V can only host Windows Virtual Desktops.

- **Understanding Your Users:** Another consideration that you need to take into account is the type of users you are supporting. Depending on their role, the users can be classified into four types:

- **Task workers:** Require only a basic set of applications and limited hardware resources. Example: Call center agents.

- **Power workers:** Require maximum customization with immense hardware resource requirements: Example: Graphic designers, software developers.

- **Knowledge workers:** Require greater sophistication and more hardware resources. Example: Scientists, accountants.

- **Kiosk users:** Users are required to share a common network. Example: Students.

- **Assessing Your Resource Requirements:** To avoid under-provisioning of resources, assess the resource requirements of your organization. Check how many resources you need for each virtual desktop, and plan accordingly

- **Monitor Your Network Strength:** The performance of your VDI is closely linked to your network strength and coverage. Identify the peak times where your network gets most loaded, and maintain it within the necessary levels to provide an optimum end-user experience.

- **Perform a Pilot Test:** Before you deploy a VDI solution, it is advised to operate it on a pilot basis. This way, you can get an idea of what to expect from your VDI setup, which platform is best for you, and the resources required.

Use Cases

Due to various benefits, VDI is deployed and actively used across industries. Here are some of its use cases:

- **Highly-Regulated Workspaces:** Certain professions must follow some regulations and compliance standards at their workplace. For example, in healthcare, you must follow HIPAA guidelines, failing which could even revoke your license. With the help of a centralized server in VDI, you can easily regulate who can access /modify your information and adhere to HIPAA measures to safeguard it.

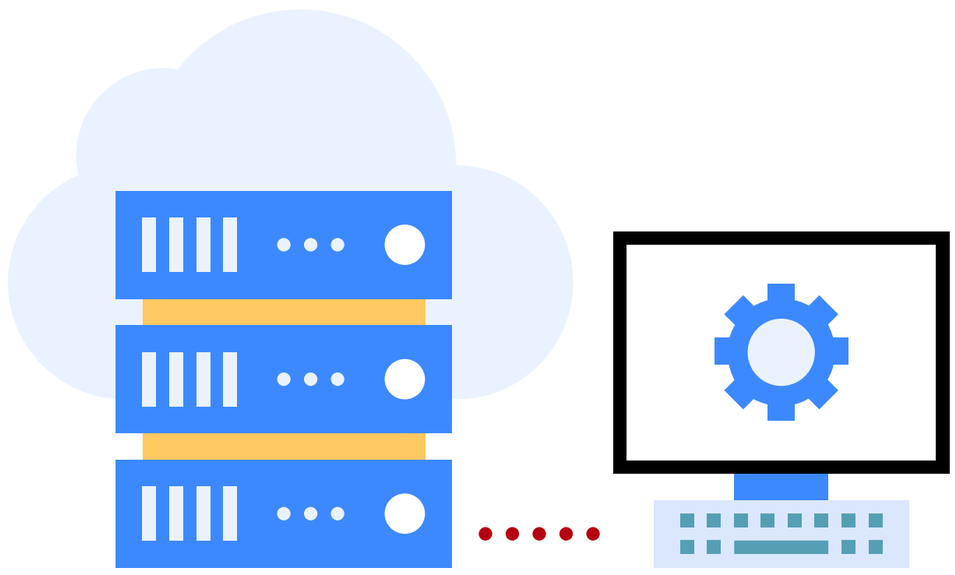
- **BPOs:** In BPOs, the workers require only minimal hardware equipment. The VDI provides an ideal solution for a uniform end-user interface across its virtual desktops, as all you need is to manage a single golden image. Furthermore, with its extended accessibility, BPOs can easily hire remote workers and offer round-the-clock services.

- **BYOD:** Many organizations around the world actively implement BYOD at their workplace. However, letting their employees use their devices directly carries compatibility and security issues. With VDI, they can securely access a virtual desktop without integrating additional applications or modifying their system configurations.

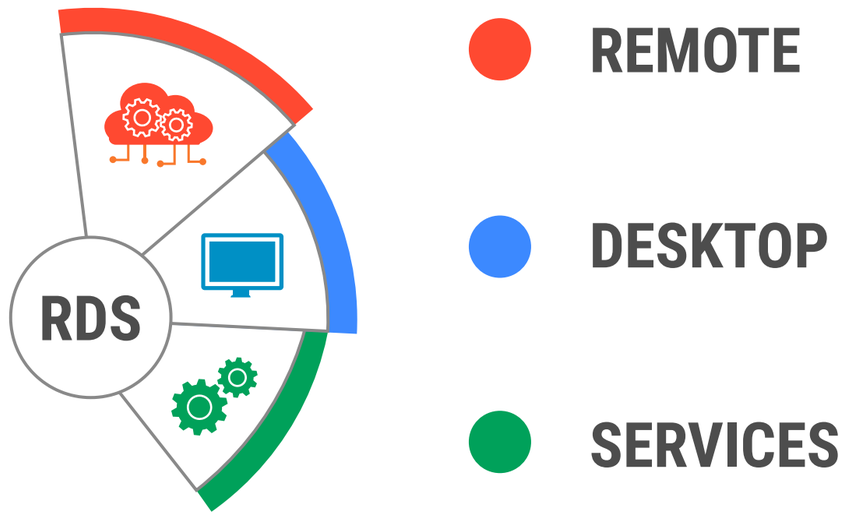
- **Educational Institutions:** With VDI, students can remotely access their educational resources or manage their projects. It is also easier for the management to implement the necessary policies and safeguards to monitor the students and prevent them from accessing malicious sites during class hours.

How is VDI different from desktop virtualization?

Virtual Desktop Infrastructure →



Desktop virtualization

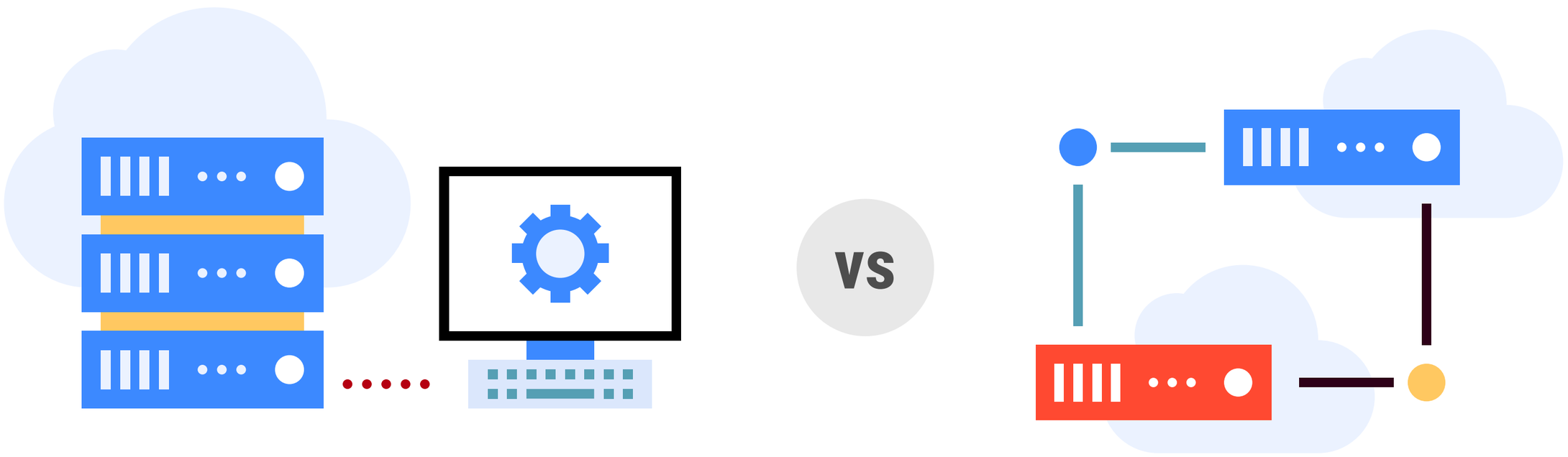


Often confused as the same, desktop virtualization and VDI are two different concepts. VDI is a form of desktop virtualization and uses a hypervisor and other associated technologies to create and deploy a virtual desktop.

Desktop virtualization is an umbrella term encompassing all the technologies that enable you to access a desktop remotely. It has two other types: Remote Desktop Service (RDS) and DaaS (Desktop as a Service).

While DaaS is inherently similar to VDI, the only place where it differs is that a third-party service provider manages the entire infrastructure. Whereas in RDS, users are only limited to using Windows and can access their data and Windows applications through a Microsoft Window Server OS. You must run a Windows Server instance on your virtual server from which you can access a virtual desktop using their network connection, provided your device follows the Remote Desktop Protocol (RDP).

VDI vs. Virtual Machines



Virtual Desktop Infrastructure

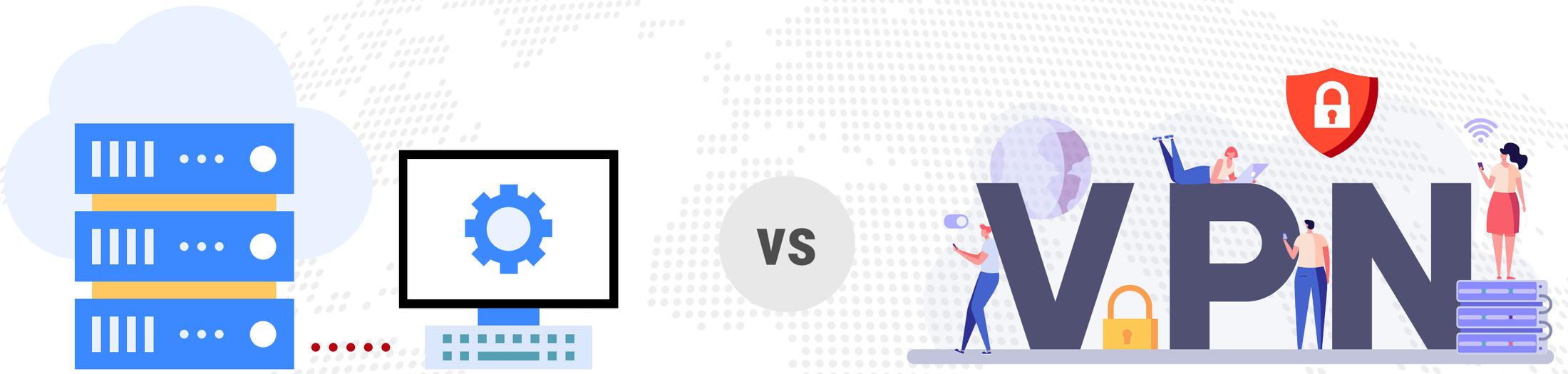
Virtual Machines

Although closely related, VDI and virtual machines (VMs) are not the same.

A virtual machine is a computational entity that functions as a normal computer. On an orthodox CPU, you can only use a single type of OS with predetermined system configurations. However, running a VM is different. You can create varying VMs from a single resource point. For example, if you have a set of 32GB RAM and 2 Terabytes of storage, you can create multiple VMs, each having its unique configuration. You don't need to physically segregate your resources. Everything is done using a hypervisor.

VDI is a type of desktop virtualization that leverages VMs to host applications and resources on a central server. It utilizes a centralized resource point for provisioning and creating virtual machines. This is essentially a building block without which you cannot establish a virtual desktop infrastructure

VDI vs. VPN



“VPN stands for Virtual Private Network. It is a technology that encrypts the network connection from different end-point devices, like laptops and smartphones. It masks your IP address and protects your data from unauthorized third-party access. Since it allows you to remotely access resources from a private network, it is often confused with VDI.

However, both are entirely different technologies. VDI enables you to remotely access a virtual desktop. You can log in from any device and access a virtual desktop with your desired system configurations. Whereas a VPN is simply a secure means to access resources over the network. It creates a safe tunnel for data transfer that cannot be intercepted from outside.

There are other innate differences between them as well. A VPN relies on end-point devices, making it dependent on them. You may suffer from latency issues depending on your system configuration. On the other hand, VDI’s performance is determined by its server components. The end-point device is simply a means to access a virtual desktop and does not affect your desktop performance.

In terms of security, a VPN provides limited protection. It is only responsible for delivering a secure connection during data transfer. The end-user, after accessing the data once, can copy it to their personal devices, leading to a potential insider breach. However, a VDI solution does not allow you to copy data without administrative permission. You can restrict its access outside of your company devices.

Avoiding Common Mistakes During VDI Deployment

We all make mistakes while implementing something new. VDI is no different. Most organizations often end up making some basic mistakes while deploying VDI that can affect their end-user experience in the long run.

However, with correct guidance, you can plan and avoid them altogether. Let’s have a look at the top mistakes that you should avoid during VDI deployment:

1. On-Site Data Storage

Maintaining on-premise data storage is one of the most common mistakes that you can make while deploying VDI. Doing so only perpetuates the limitations originally associated with conventional file storage, like regular data synchronization and backup management. Furthermore, your users experience latency while accessing their files. This ultimately dents their VDI experience. So, when you deploy VDI, it is critical to move the existing network-attached storage and other data resources to the same server infrastructure.

2. Investing Conundrum

The initial upfront costs of VDI setup are high. This may deter you from openly seeking out a VDI solution. However, despite the initial investment, VDI carries numerous cost benefits. The key here is to invest appropriately. Even if the initial upfront cost is high, remember that investing in an ideal solution for your organization will reward you over the long term. This is much better than ending up with a VDI setup that doesn’t cater to your user needs and fails

3. Not Asking For Help

Half-knowledge is more dangerous than ignorance. Does this quote ring a bell? This is certainly true when you avoid seeking out a specialist while establishing your VDI infrastructure. A successful VDI deployment is the result of accurate analysis and technical expertise. Enrolling an expert allows you to have a clearer picture of your organizational needs. So, rather than managing everything yourself, seek third-party assistance in guiding and planning your VDI deployment.

Lift and Shift Migration.

Most organizations opt for “Lift and Shift” migration to move their existing on-premise resources to their VDI environment. While it is one of the easiest and cheapest methods, it comes with some serious flaws. You don’t get to experience a true cloud platform and might run into latency and performance issues. Furthermore, if your on-premise applications are not compatible with your VDI environment, it will eventually lead to migration failure

Future Perspectives

The need for a mobile workforce, BYOD implementation, and the recent COVID-19 pandemic are the various reasons that have tremendously fueled the growth of the VDI industry. Using VDI carries many benefits and helps organizations overcome the limitations of a traditional desktop environment. In short, VDI has become a top-sought solution across different industrial verticals. The growth of virtualization technologies is further easing VDI deployment. It is expected to prompt more and more organizations to adopt VDI for using virtual desktops and revolutionize their end-user desktop experience.

Ace Cloud Hosting

www.acecloudhosting.com