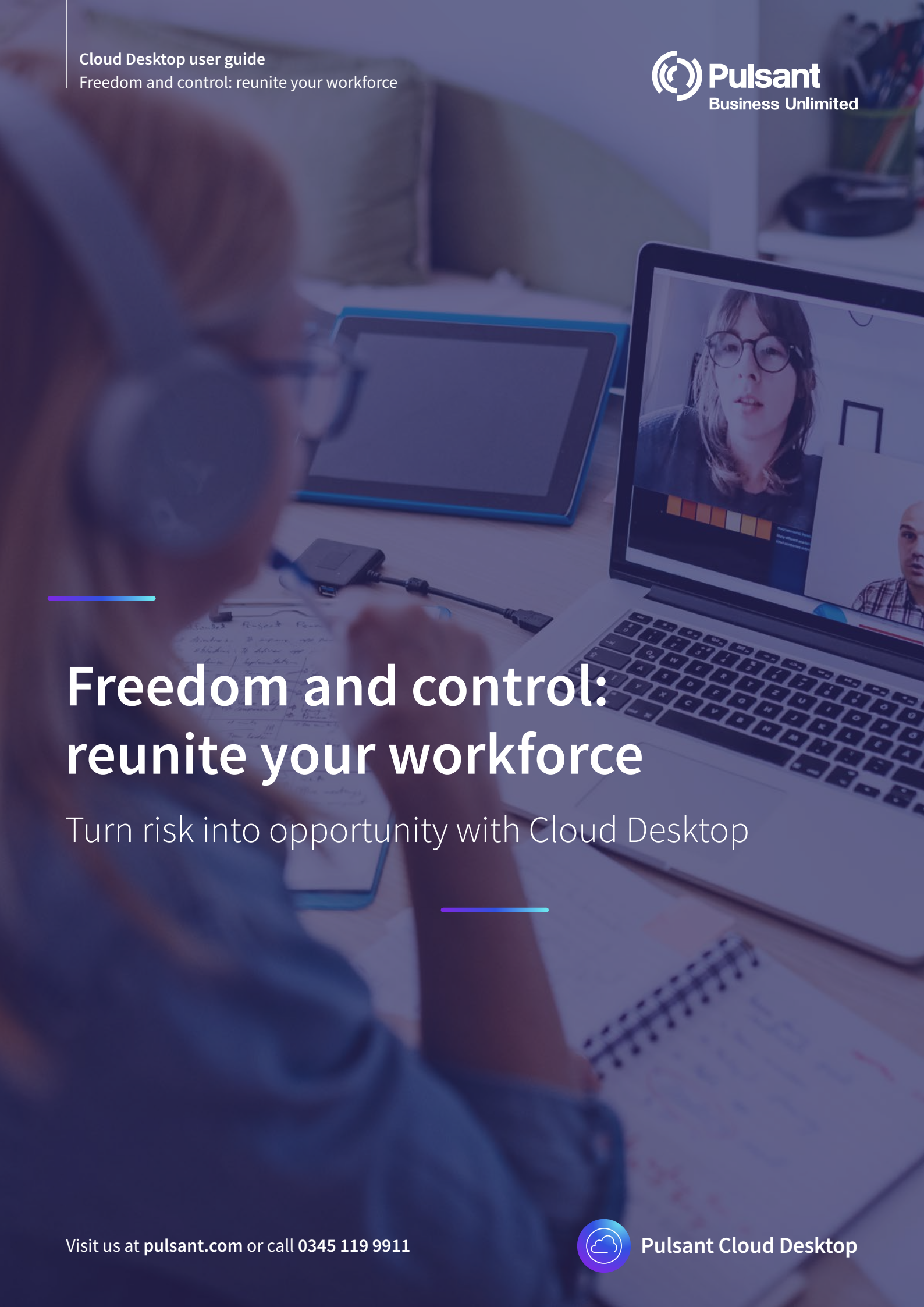
Pulsant
Business Unlimited



# Freedom and control: reunite your workforce

## Turn risk into opportunity with Cloud Desktop

# Navigating the new landscape

Covid-19 has necessitated the inevitable shift to remote working; something which is likely to become one of the permanent legacies of the global pandemic. But whilst the move might not have been foreseen, many benefits of the new working dynamic have now become clear.

For many organisations the new way of working has provided the opportunity to either reduce or reconfigure office space to drive down overheads, improve staff flexibility and attract and retain top talent outside of their traditional catchment area. Some have even reported increases in productivity, with the office rumoured to become a place for training, meeting colleagues and collaborating on occasions, rather than a permanent base for work.

It's clear remote working is here to stay, however, when operating with a dispersed workforce it is a challenge to maintain the same levels of security, standardisation and control that you may be used to in an office environment. And in industries where data security is paramount and reputation is everything, there is no room for error.

**As an IT leader, you need to free your remote workforce and provide a scalable, secure, and flexible environment.**

As an IT leader, you need to free your remote workforce and provide a scalable, secure, and flexible environment, without increasing your IT management overheads, adding complexity and still retaining control. So where should you start?

This guide will provide all the information you need to help you combine the freedom of remote working with enterprise level control and capitalise on the benefits of a remote workforce.

## The guide will cover:

- Understanding the risks
- How to turn risk into opportunity
- What is VDI?
- Key benefits of VDI
- Is VDI right for me?
- Choosing the right VDI platform
- Why Pulsant Cloud Desktop?
- Key features of Cloud Desktop
- Combining freedom and control

# Understanding the risks

In a remote working environment, staff need to be able to connect from anywhere, using different devices, whilst receiving the same end user experience. However, whilst this flexibility has many business benefits, it also has risks.

## Some of the most common risks you are likely to face in this environment include:

**Greater attack surface**
Employees are working from uncontrolled environments and, as a result, perimeters have expanded making effective cyber security more difficult.

**Risks to the confidentiality and integrity of your data**
You need to consider whether remote working has implications on the confidentiality, integrity and availability of your data. While workers are still bound by the same policies, the measures to implement and control them are not present outside of the office, so you're placing a lot of trust in employees to take the right precautions.

**Access via home broadband and unsegregated networks**
You no longer have control over the networks employees are using. With users accessing their desktops remotely over networks that are not as secure, your chances of being compromised increase significantly.

**Data loss from employees**
With employees now outside of your line of sight, there's an added risk information could be misused or misplaced, particularly if they are unused to remote working or using their own devices.

**An increase in cyber attacks**
Cyber criminals are already seizing the opportunity presented by mass remote working to gain access to breach systems and exfiltrate data - more than 90% of enterprises reported an increase in cyber attacks with more employees home working amidst the coronavirus outbreak.

**Reputational and financial damage**
Any form of data breach could significantly erode trust and have a critical impact on your organisations' ability to operate, generate new business or retain clients. And with the average cyber breach costing $3.86 million and taking 280 days to identify and contain according to IBM, you cannot afford to be complacent.

# How to turn risk into opportunity

In the face of these new challenges, you need to find a balance between freedom and control. Overly tight restrictions risk alienating your users and restricting productivity, but too loose controls can expose your business to unacceptable levels of risk.

You also need to maintain consistency of configuration across an estate of devices with a traditionally installed application environment in a highly dispersed environment. This can be costly in terms of tooling and resource to manage so you need to consider a solution that could reduce your real estate footprints and costs whilst centralising and standardising access.

This is why many organisations are turning to hosted or cloud desktop services, commonly known as Virtual Desktop Infrastructure (VDI).

## What is VDI?

VDI technology is a form of desktop virtualisation that uses dedicated virtual machines (VMs) to provide and manage virtual desktops. Essentially the desktop operating system is hosted on a central server in a data centre - whether that be your own, in a hosting facility or within one of the hyperscale public clouds. The virtual desktop image is then delivered over a network to the endpoint device, giving users the same experience as if the operating system and its applications were running locally. Those endpoints may be PCs or devices like tablets or thin client terminals.

The technology is not new – VDI has been around for well over a decade in one form or another, progressing from shared remote desktop or terminal services. Historically its usage was limited to niche use cases and defined user segments. Only recently has the technology been used in a company wide fashion.

## Key benefits of VDI

The traditional model of desktop computing involves an expensive, power-hungry machine on every desk, running the operating system and applications that your users' needs. In addition, the requirement to install, manage, secure, patch, and otherwise support these machines can be a massive drain on your IT department and budget.

## VDI removes this burden and offers a number of advantages including increased user mobility and ease of access, scalable computing power, consistent user experience and centralised security and control.

### In particular, key benefits include:

**Reduced costs**
VDI can significantly reduce costs and improve ROI. Users can connect to a virtual desktop via existing PC infrastructure or thin-client devices, while desktop management is centralised, allowing consistent roll-out of patches, upgrades and new applications. Management overheads are reduced through centralisation and less time spent managing or visiting endpoint devices.

**Improved performance**
Moving desktop applications into the same data centre as the servers running applications can achieve significant improvements in performance. Only the display and keyboard traffic between the user's device and the virtual desktop is sent over the connection between the user and the data centre, providing an enhanced performance and end-user experience.

**Increased mobility**
Users can connect from any location, even using their own personal devices, and still see the same desktop. The experience is the same, regardless of location or device.

**Greater security and control**
In a VDI environment, data resides on the server rather than the user's device, ensuring it remains protected even if a device is stolen or compromised. Centralised management also provides greater control over desktop configurations and permitted application stacks.

**Ensured business continuity**
VDI minimises the disruption caused by a disaster. Users can simply reconnect to the virtual desktop from a new device or to the secondary data centre and can continue working seamlessly.

## Is VDI right for my organisation?

**The benefits of virtual desktops are clear, but VDI is not a fit for every business or situation. In particular, VDI is well suited to organisations that:**

- Are moving to variable staffing, hotdesking, mobile or remote working models
- Are struggling to manage and support the IT of a large distributed or mobile workforce
- Need to control and reduce user support costs
- Want to improve the responsiveness of remote applications
- Would like to make a desktop hardware refresh and turn CapEx into OpEx
- Operate in highly regulated sectors and need to manage and control applications installed on user desktops, as well as provide extra security and business continuity for mobile workers
- Are undergoing mergers or acquisitions where a quick roll-out of a standardised application platform is key to operational alignment
- Have strong business continuity and compliance needs

# Weighing up costs vs benefits

When building a business case for VDI you need to consider the costs versus benefits. The up-front cost of a VDI implementation may not seem outwardly justifiable, however, when you consider the bigger picture, it will be much more cost effective in the long term than traditional desktop hardware.

Traditional desktop computing architectures carry a high cost, driven up largely by the capital expense of purchasing new hardware and the burdensome and inefficient support models. Add to this include indirect costs, such as facilities, power consumption, procurement and tax accounting that are not so easy to identify or quantify and costs are considerate.

With VDI, you can lower capital and operating expenses by lowering acquisition costs, reducing the infrastructure needed to support a distributed workforce and enabling centralised support. Furthermore, VDI allows old or low-powered desktop clients to continue in service while the computing power becomes a monthly OpEx that scales with your needs.

When weighing up the costs versus benefits of a VDI implementation don't forget to consider the following:

- The amount of time and money currently spent on device support and how long it takes to apply, configure and test patches on all desktops in your organisation
- Budget currently spent on PC refresh cycles for all users
- Any costs resulting from security breaches caused by lapses in security from remote working
- Cost savings that can be made on overheads from allowing employees to work remotely and enabling BYOD to decrease real estate, IT hardware and energy costs
- The long-term savings in time, as well as the huge benefits to productivity that VDI can bring

**With VDI, you can lower capital and operating expenses by lowering acquisition costs, reducing the infrastructure needed to support a distributed workforce and enabling centralised support.**

# Choosing the right VDI platform

A number of different VDI offerings exist from leading companies including Microsoft, Citrix, AWS and VMWare so it's important to select the right solution.

A number of different VDI offerings exist from leading companies including Microsoft, Citrix, AWS and VMWare so it's important to select the right solution.

There are two primary VDI platforms: persistent and non-persistent. Persistent platforms enable users to log into the same desktop image every time with all changes to applications and data retained. In contrast, non-persistent VDI does not save changes so is better suited to one-off desktop access rather than replicating traditional physical desktops.

VDI solutions can either be operated and maintained by your in-house IT teams and located in an on-site data centre managed by IT staff, or you can opt for a fully outsourced, managed infrastructure solution which is delivered by a provider and hosted in their data centre.

The benefits of an in-house model is that you retain complete control. However, while managing hardware and software internally is convenient, it can require a huge IT team to look after the maintenance, setup, and upgrade. Plus, hardware failure, software issues, and other unexpected problems have to be handled in-house which can be expensive.

**With a managed solution the service provider manages all of the hardware, so you don't have to worry about rackspace, hardware breakdown or maintenance.**

There are many questions to consider when choosing the right VDI solution for your business, but there are three that matter the most:

1. Can it deliver the rich, high-quality experience users depend on to be fully productive?
2. Will it help my organisation protect corporate data, comply with security regulations and reduce risk wherever people work?
3. Does it make management simple, flexible and efficient so IT can focus on strategic initiatives?

Other considerations include storage and disaster recovery requirements, the level of security provided, integration with existing IT management solutions and unified communications solutions, desktop performance levels, customisation and support and management provided.

# Why Pulsant Cloud Desktop?

Built on Citrix Virtual Apps and Desktops technology, Cloud Desktop places your desktop computing in a secure Pulsant data centre.

Users have a low-powered thin client device or PC on their desk, or a portable device such as a laptop or tablet, which communicates back to the data centre where powerful servers take the load of running the desktop operating system and applications.

This pushes all desktop processing and storage requirements into the data centre, meaning the connecting device only needs a minimum hardware specification to run the connection software.

Pulsant takes on the deployment, configuration, and day-to-day management of the operating system to provide you with a secure, stable, and reliable desktop platform for running your business applications.

**This leaves you free to focus on the end user experience as opposed to managing and maintaining the underlying infrastructure.**

## Key benefits of Cloud Desktop include:

**Trusted technology**
Cloud desktop is built on trusted technology from Citrix - a virtualisation leader for more than 30 years and named leader in the IDC Marketspace for virtual client computing. Used by more than 100 million people worldwide, Citrix Virtual Apps and Desktops technology provides a better user experience, enhanced security and compliance capabilities and greater support and app and system management than competitive solutions.

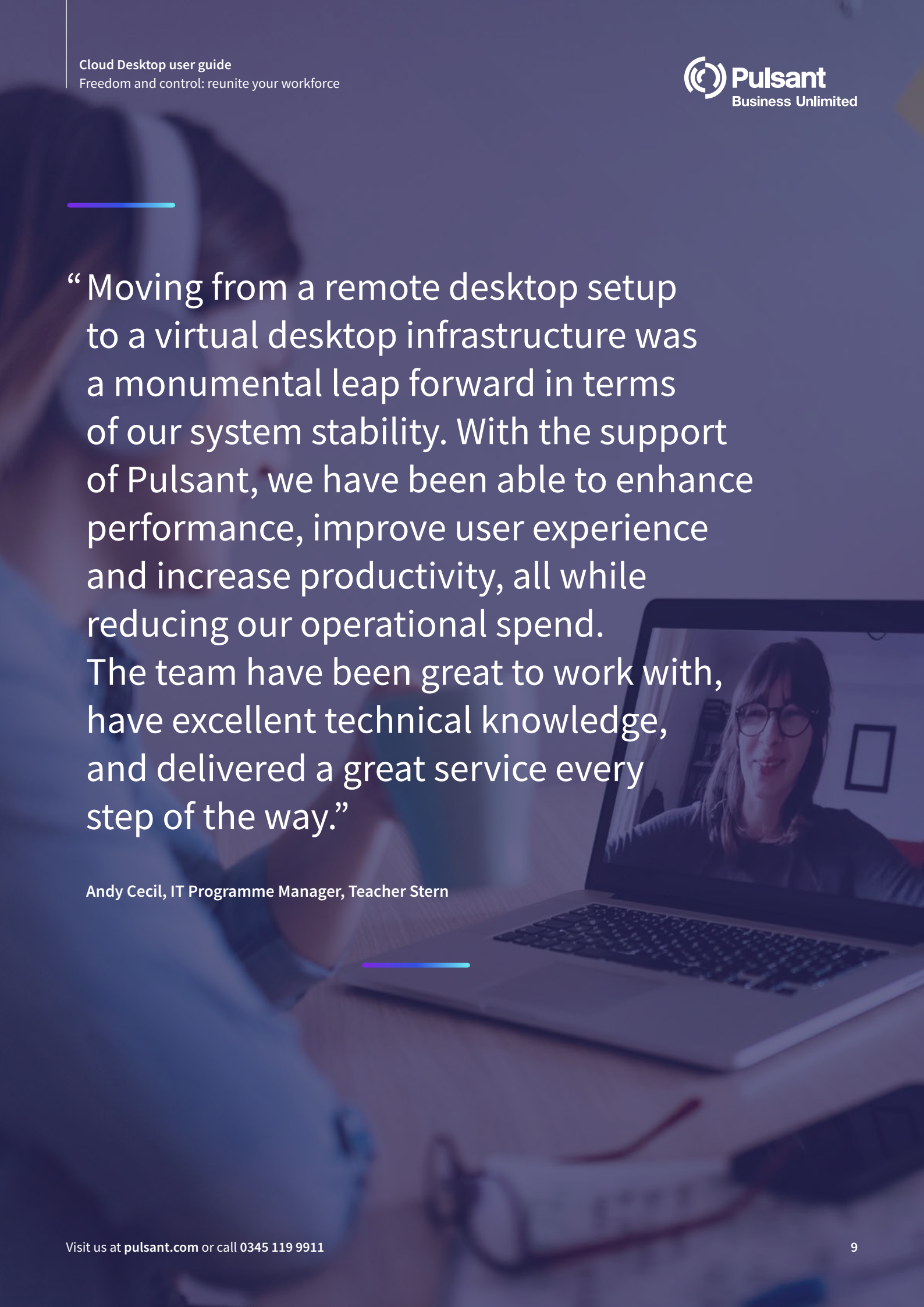
**First-class service and support**
Cloud Desktop is a fully managed infrastructure solution, providing peace of mind that your infrastructure will remain secure and available 24x7. Pulsant will configure and manage the operating system, as well as manage and maintain all aspects of the VDI platform, quickly resolving any issues that affect the delivery of the service.

**Enhanced performance**
With Cloud Desktop you can access a range of VM options to select machine specs that meet the needs of your application stack. Processing is all performed by the data centre infrastructure and if your applications are already hosted with Pulsant, the desktop is now in the same data centre as the servers, leading to better performance and responsiveness.

**Improved reliability and business continuity**
Cloud Desktop comes with guaranteed availability SLAs plus optional disaster recovery (DR) infrastructure in a secondary Pulsant data centre to minimise the disruption caused by a disaster. This enables a seamless switch-over to the secondary data centre should the worst happen, ensuring that your users can continue to use their virtual desktops with minimal loss of service.

**Strengthened security**
Pulsant's data centres are UK-based and ISO 27001 accredited, providing reassurance that infrastructure remains resilient, scalable, and highly available. Users access the Cloud Desktop using a secure multi-factor authentication service from Azure Active Directory as standard and all data transmitted between the data centre and the user device is encrypted, whatever the network.

Pulsant
Business Unlimited



"Moving from a remote desktop setup to a virtual desktop infrastructure was a monumental leap forward in terms of our system stability. With the support of Pulsant, we have been able to enhance performance, improve user experience and increase productivity, all while reducing our operational spend. The team have been great to work with, have excellent technical knowledge, and delivered a great service every step of the way."

**Andy Cecil, IT Programme Manager, Teacher Stern**

# Key features of Cloud Desktop

Built on Citrix Virtual Apps and Desktops technology, Cloud Desktop places your desktop computing in a secure Pulsant data centre.

## Pulsant Cloud Desktop provides you with:

- Cloud desktop infrastructure provided and managed in a Pulsant data centre
- Choice of pre-defined VM profiles (2 cores with 5GB of RAM or 4 cores with 10GB of RAM)
- Secure authentication with Azure AD MFA (Duo MFA available at additional cost)
- A Windows 10 desktop for each user
- Anti-virus as standard on every desktop
- Access from any client device of sufficient hardware specification
- A resilient hardware platform offering a high level of service availability
- Customised desktop template(s) with tailored configuration and application stack created in consultation with the Pulsant team
- 24x7 support, maintenance and management of the VDI platform and operating system
- Monthly patching and updates
- Optional disaster recovery capacity in second data centre (additional charge)
- Optional, deployment and management of Office 365 E3 (additional charge)

**Allocated Resources**
Each desktop is allocated resources (virtual CPUs and memory) from Pulsant's shared Cloud Desktop infrastructure. You can select configurations optimised to different requirements, so you don't pay for more computing power than you require.

**Storage**
Storage for application data, such as file storage for office documents may be provided through Microsoft OneDrive for Business, SharePoint Online, or deployed locally using Pulsant's own cloud storage at an additional cost. Storage must be located in the same data centre as the virtual desktop infrastructure.

**Software**
Cloud Desktop supports any software application certified to run on Windows 10. Where exceptions are identified, Pulsant can help identify alternate solutions to ensure your operating model is maintained.

**Managed Templates**
Cloud Desktop uses templates to configure each user's desktop, including the application stack available to them. A template can "hold" any number of applications, subject to acceptable use policy and storage limitations.

# Combining freedom and control

Remote working isn't going away and to remain competitive you need to provide your employees with the right IT to enable them flexibility in where and how they work.

Whether you are looking to control and reduce user support costs, maximise performance, or provide a consistent user experience, with the right VDI solution you can give your dispersed workforce the freedom they need whilst minimising IT management.

With the support of a trusted partner like Pulsant, you can align your business objectives with VDI deployment models, implement the right technology for your unique needs and remove the burden from ongoing management.

More than that, with Pulsant Cloud Desktop, you benefit from the peace of mind that staff can be productive regardless of location, your infrastructure is fully managed and supported and your data - and ultimately reputation – is protected.

**With the right VDI solution you can give your dispersed workforce the freedom they need whilst minimising IT management.**

Pulsant
Business Unlimited

Visit us at **pulsant.com** or call **0345 119 9911**

Pulsant Cloud Desktop