



Optimising your hybrid working infrastructure

A hybrid working guide



Introduction

According to a [Microsoft survey](#), more employees and managers than ever are embracing the flexibility of hybrid work. The only problem? Many companies that are already trying their hand at hybrid collaboration could be better at it. While well-equipped offices used to be the main way people would experience your organisation, leaders must now reevaluate their processes to offer a true, remote working infrastructure.

As expected, this isn't an easy task, with hybrid work comes a host of distinct challenges including a balance of cloud services for your teams, productivity issues and an increasing number of cyber security risks. To stay ahead of the game, more is needed to optimise the set-up and support better collaboration and productivity.

In this guide we will cover the various challenges associated with hybrid work and show you how to optimise your hybrid working infrastructure with a range of Microsoft services and solutions.

Contents

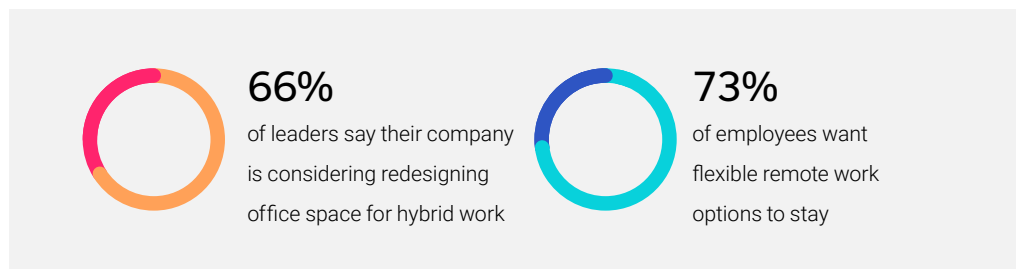
- › The shift to hybrid working
- › Creating your hybrid working strategy
- › Putting hybrid work into action
- › Microsoft solutions available



Section 1

The shift to hybrid working

According to [data from the Office of National Statistics](#), before the COVID-19 pandemic, a mere 5% of the UK workforce were working from home and around 65% of employers either did not offer regular working from home at all or offered it to less than 10% of their workforce. Fast forward to now where all that has changed. [Microsoft reports](#) 66% of business decision makers are redesigning their physical spaces to better accommodate hybrid working environments and 73% of employees want flexible and remote working options to continue. The data is clear. Extreme flexibility and hybrid work is the future.



While some employees want to work from home all the time, most would prefer a balance where they are in the office for some of the week and at home for the remainder. For most organisations, hybrid working will require a significant culture shift and new ways of working with associated policies and practices.

It's not enough to simply convert physical interactions into virtual meetings. Hybrid work is the new normal, but it can be difficult to equip the new workplace. Some common challenges we come across with our own clients include:

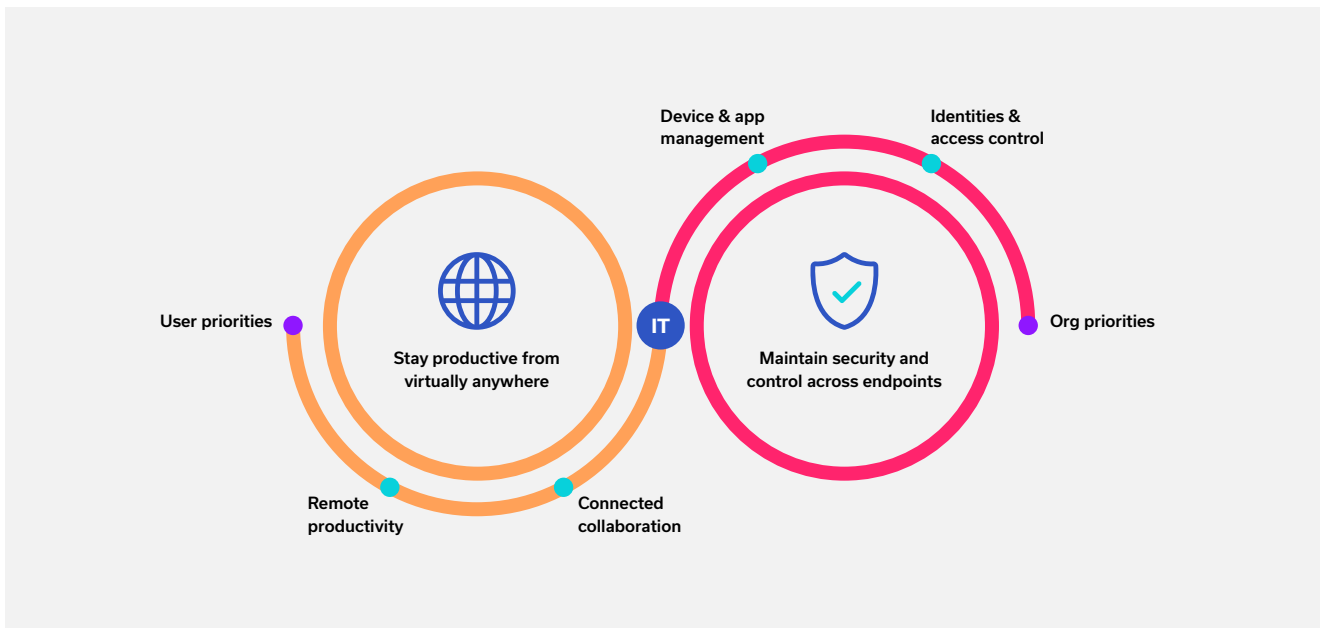
- › **Communication challenges and difficulties in collaboration** - A lack of reliable tools for remote collaboration and productivity.
- › **Reduced productivity** – According to a McKinsey report, employees spend about 20% of their work week searching for internal information which can hinder your team from being productive and completing tasks. With our own clients we notice this can be down to slow connections and capacity issues with internal systems.
- › **Trouble accessing information** – You could describe the cloud as the backbone of your hybrid workforce. If your cloud provider is unable to provide high quality solutions, chances are your teams may struggle to access key systems remotely and stop the seamless operation of collaboration tools.
- › **Inconsistent experience** - Employees working from home require an internet connection just as fast as at the office and a laptop that can handle the office technology stack. A good virtual desktop interface is another factor that would make the work from home experience as seamless as possible. However, too often we see employees using outdated virtual desktop interfaces or VPNs which means the portals you are accessing give you a poor working from home experience and accessing core apps can be a struggle.
- › **Security issues** - According to a study, 67% of cyber-attacks target remote employees. The sites they visit using their work laptop, the links they click on, the way they store personal and business information, this increases the vulnerability of the company's data. Some clients who do not have antivirus software, VPNs or firewalls, are an easier target for hackers, making it simpler to gain access to devices and aim for your corporate network.



Section 2

Creating your hybrid working strategy

So, what should organisations think about when implementing a hybrid approach? It may seem like a minefield, but there is no single way to implement hybrid working, and its exact form is likely to vary from business to business. In this section we cover some areas to consider when thinking about potential approaches towards a more hybrid future



- › **User priorities** – Consider when and how your teams work. What is the working day like and how would you define it? What applications and processes are most important to users.
- › **Remote productivity** – To remain productive you must ensure to provide everyone with a connected experience, especially when it comes to working together.
- › **Connected collaboration** – It should be easy to access what you're working on, to get back to what you're working on and to connect to others.
- › **IT** – IT sits at the heart of your hybrid working strategy. How can IT help provide a better experience for remote workers. Is IT moving to the cloud and working on productivity with the business?
- › **Device and app management** – No matter which device people log in from, can they do this safely and securely?
- › **Identities and access control** - Identity is a key cyber security component. Organisations must be able to provide secure access for contractors and business partners, remote and mobile users, and customers.
- › **Organisation priorities** – Ensure that all the points mentioned match up towards the priorities of your organisation.
- › **Security** – Whatever route you take you must ensure the highest level of security across all touchpoints.



Section 3

Putting hybrid work into action

Once you have some key questions covered, to successfully implement the hybrid working model we have identified 4 key pillars to help you get started.



Collaboration

Working as a team is hard enough when everyone is in the same room, never mind when they are working from home. Add in varying time zones, poor connectivity and audio issues and you've got a real challenge on your hands. Some ways you can deal with this issue is looking at the following points.

- › Reimagine meeting culture for a hybrid way of work
- › Level up meetings with the power of asynchronous tools
- › Create norms that work best for your team

There are also a whole host of collaboration tools including Microsoft Teams and SharePoint which you could be using. The transition to hybrid working may seem difficult to begin with but remember there are several tools available that you can start using.



Communication

As with collaboration, communication can also be a struggle with hybrid working. It is very easy for employees to become siloed when working in different locations. Traditional platforms like email are particularly focused on legacy ways of communication and cause a drain on your staff and productivity.

In the absence of an office environment, it's difficult for teams to have an awareness of what's going on. Employees working together may choose to cc other team members into communications which can cause a drain on productivity. They may also choose to use one to one communication that could then make it difficult for other members of the team to contribute valuable ideas or experience to assist their team.



Productivity/Experience

Most organisations have legacy on-premise applications that are out of date and struggling to keep up with your business. Hybrid working compounds these challenges as providing access to these applications via virtual desktop solutions or VPNs can create more issues. When it comes to productivity and experience, we have narrowed it down to 3 main areas: access, experience and performance.



Access

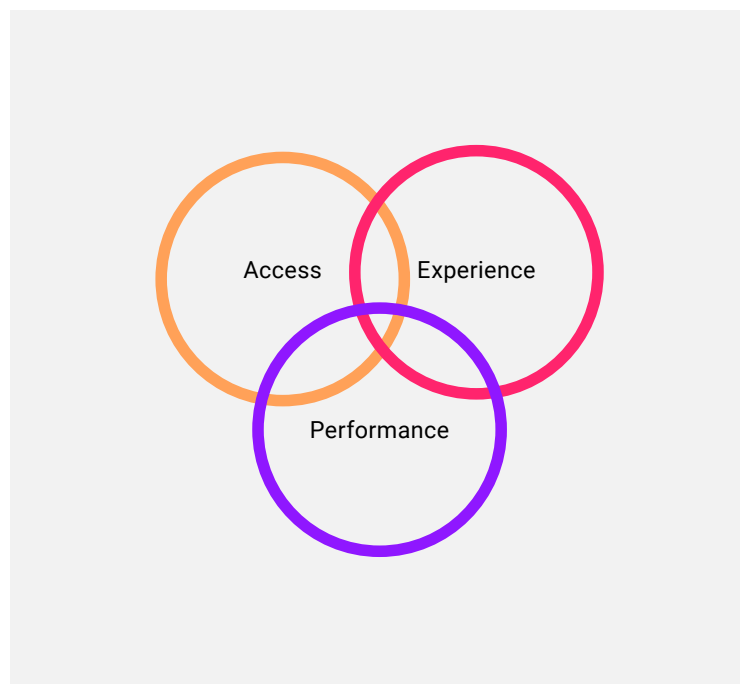
Access is a challenge when using legacy applications. These applications are almost exclusively on-premises limiting access to inside your organisation. For organisations with employees working from home, this presents a challenge. An example of something you can do to improve access to legacy applications is to start using Azure Virtual Desktop. Azure Virtual Desktop provides a desktop virtualization solution using the familiar Windows experience, while keeping the application on-premise. We'll talk more about this solution later in this guide.

Experience

Legacy applications generally have a poor experience and with evolving business processes and a lack of internal knowledge this only worsens over time. When you compound this by delivering the app via a remote working solution this can be even harder to use and navigate. When you compound this by delivering the app via a remote working solution this can be even harder to use and navigate.

Performance

Legacy applications regularly operate slowly and rarely have process automation or notification processes to help employees save time and be more productive. Productivity is a key criteria for system implementation and is critical in achieving a return on your investment.





Security

When it comes to security, gone are the days of the traditional 'castle and moat' approach used by most offices. It's now imperative that all touchpoints are identified and secured in newly expanded networks.

Remote work has expanded the definition of company perimeter and there are now an increasing number of security challenges we need to be aware of.

Loss of sensitive data – Data breaches are probably the most concerning of security threats as they affect the business, employees and most importantly your customers. The worst part is these can be triggered by the smallest thing. Say an employee hasn't switched to a secure network when working from home, or when out and about they have misplaced their device, companies are responsible for implementing practical solutions on how to strengthen the organisational cybersecurity landscape to overcome this.

Remote access for your hybrid workforce – Everyday operations require teams to share files and data and connect to devices on-site amongst other things. An explicit trust in endpoints accessing a company network with a once-granted entry is among the most significant security vulnerabilities. Remote means there is no confidence in how and who someone operates within the network. Manual monitoring of user activities is time-consuming, especially when it takes many users, leading to potentially more errors.

Device security risks - Little or no knowledge of who sits behind a screen is an issue, yet not a final one. Mobile device management is another security threat category for remote and hybrid work.

We cover some of the security solutions offered by Microsoft later in this guide to help give you peace of mind.



“You must treat identity as the new security boundary, not the network perimeter”



Section 4

Microsoft solutions for hybrid working

Microsoft Teams

Where would we be without Teams? With over 270 million active monthly users, of course, Microsoft Teams is the first thing we recommend for effective collaboration. The solution allows you to meet, chat, call, and collaborate in a single place.

- › **Instant messaging and video conferencing** – This has now become second nature to most of us and is the bare minimum to expect from a collaboration tool. Teams allows you to instant message, make a video call or video clip, screenshare and add multiple people into a chat.
- › **Collaboration and knowledge sharing tools** - Multiple people/departments can work together in a shared space for a more flexible, focused and long-term collaboration. Use shared channels to have conversations, chat, meet, share and co-author files, collaborate on apps without ever switching tenants.
- › **Task and project management planner** – An app within Teams we recommend to users is the task and project management planner. Here you can write tasks and assign them to people and keep track of deadlines. Managers and Leaders can see all progress on a single dashboard and see in list form who is assigned what. Planner comes with Teams and you can get notifications about tasks to keep you updated as well.
- › **Personal reports and analytics** - On a wider level, you can bring Power BI capabilities into Teams to discern findings and collaborate on reports. Bring data to every corner of your organisation in a matter of several taps and empower your teams to experiment with self-service analytics.

While the transition to a hybrid work environment can seem daunting at first, tools like Microsoft Teams are available to make the experience as seamless as possible.

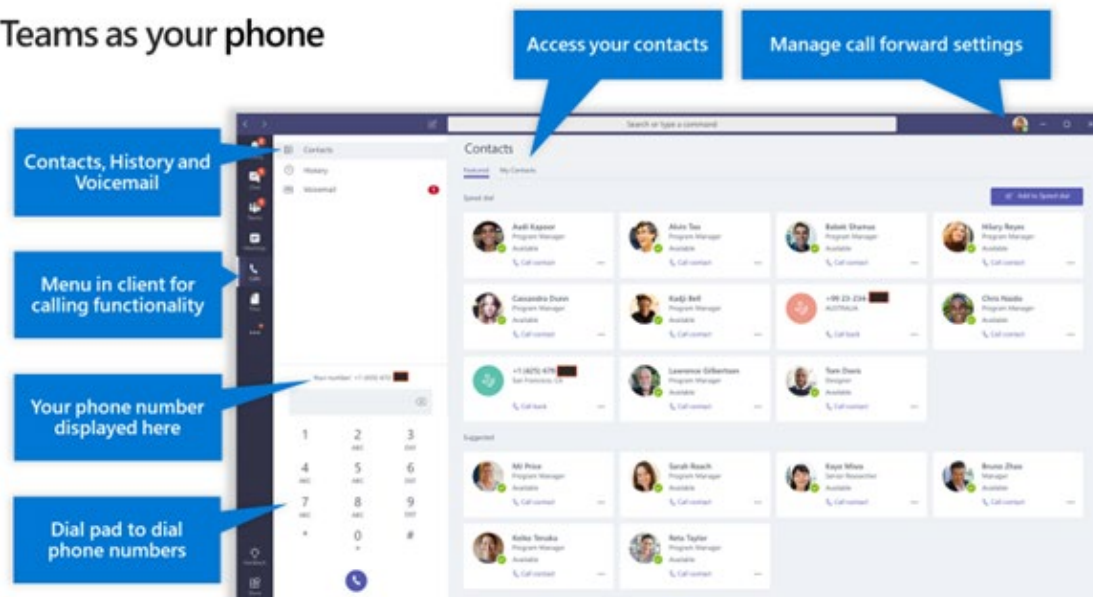




Microsoft Teams Phone

Teams can be more than just meetings and chats; you can also integrate your phone system and remove desk phones. The great thing about using Teams as your main calling solution is that you quickly create an all-in-one application. Microsoft Teams integrates with Outlook and allows collaboration across the wider Office apps and all of that can be done in calls the exact same way you would in a meeting. Teams also makes it easy to start a call from a chat, contact card within Outlook or Teams.

Teams as your phone



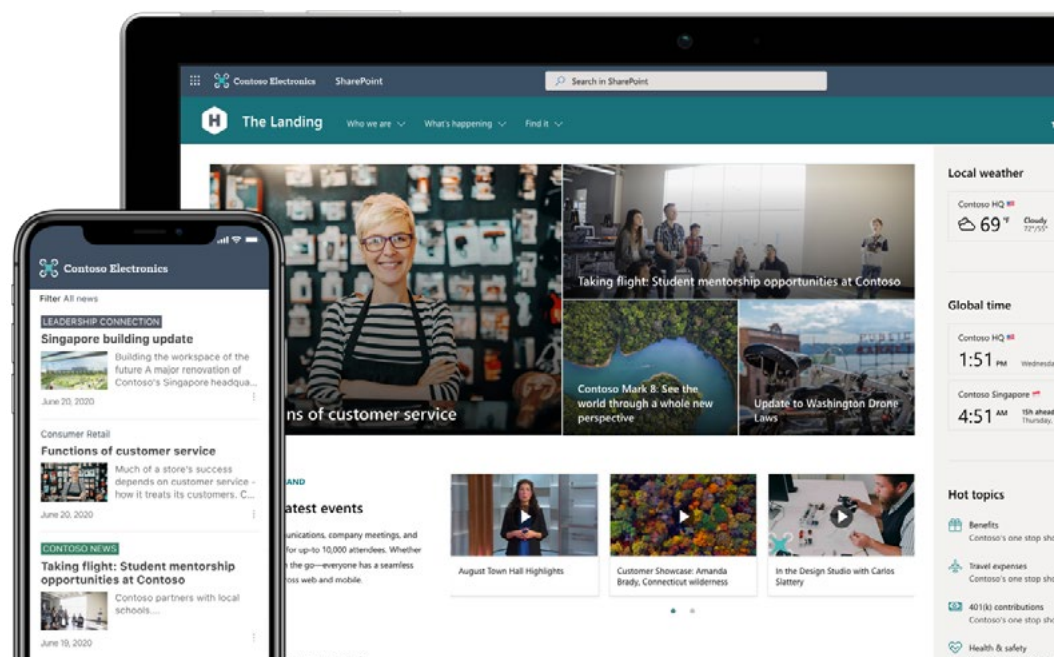


SharePoint

When it comes to virtual collaboration, SharePoint has been known as Microsoft's gold standard for years now. It directly facilitates collaboration, content management and security which makes it great for hybrid working. Teams and SharePoint offer similar but different capabilities to your business – and you don't have to choose one or the other. In fact, every Team comes with a corresponding SharePoint Online site, allowing quick storage and easy sharing of documents with your coworkers. Here are just some of the features you can benefit from:

- › **SharePoint intranet** - When you utilise SharePoint as your intranet, it'll significantly boost the ease with which new and existing employees can access your assets.
- › **Communication sites** - Communication sites are designed for communicating information to a wide range of end-users or audiences. You can use them to create portals, department or project-specific sites, and public-facing sites for sharing company news, announcements, or events. You can choose from Topic, Showcase, or blank templates for internal communications, while Publish Enabled site templates can be used to manage public-facing content or when a site needs to be managed and populated with content for review and approval.
- › **Collaboration sites** - The site type most SharePoint users are familiar with, collaboration sites allow users to track and stay up to date with project and task statuses, co-author and maintain documents and content, and leverage other Microsoft 365 services to access team resources.
- › **File sharing inside SharePoint** – You can easily copy links from files to Microsoft Teams to share internally.
- › **Collaboration** – You won't encounter any issues with multiple people opening documents at once. These restrictions don't exist anymore.
- › **SharePoint modern for collaboration** - Modern SharePoint is faster, easier to use and has been optimised for mobility built from mobile up. Microsoft continues to invest heavily in the Modern experience, with all new SharePoint sites being Modern by default. Some businesses may already be using a classic version of SharePoint, if this sounds like you, we encourage you to think about a move to modern SharePoint. Not only to take advantage of the new functionality but to reduce the risk of the classic version not being supported in the future.

It's important to utilise platforms in a way that not only aligns with your organisation's goals and policies but also meets your evolving needs. We believe SharePoint is a crucial part of that hybrid work puzzle.





Microsoft Viva

Along with Teams, Microsoft Viva is the second of the two main Microsoft products aimed at online collaboration. Microsoft Viva, a tool designed to empower employees, support remote working and enhance wellbeing. This platform is yet another development in the future of the modern workplace, bringing tools for employee engagement, learning, wellbeing and knowledge discovery directly into the M365 apps that your staff are already working with every day.





Azure Virtual Desktop

Many IT managers are addressing their remote and hybrid employee challenges by implementing VDI solutions. Hosted and managed centrally, VDI enables remote users to run fully functional virtual desktops to access their work desktops and applications from any device anywhere. There are several benefits to this including:

Deploy and scale in minutes – Quickly deploy desktop apps to the cloud, whether modern or legacy with unified management in the Azure portal. Scale access up or down to suit peak times.

Optimise costs – You only need to pay for your Azure virtual desktops, machines and Azure storage consumed by users as they use the service. Select and scale deployment options to match your organisations needs.

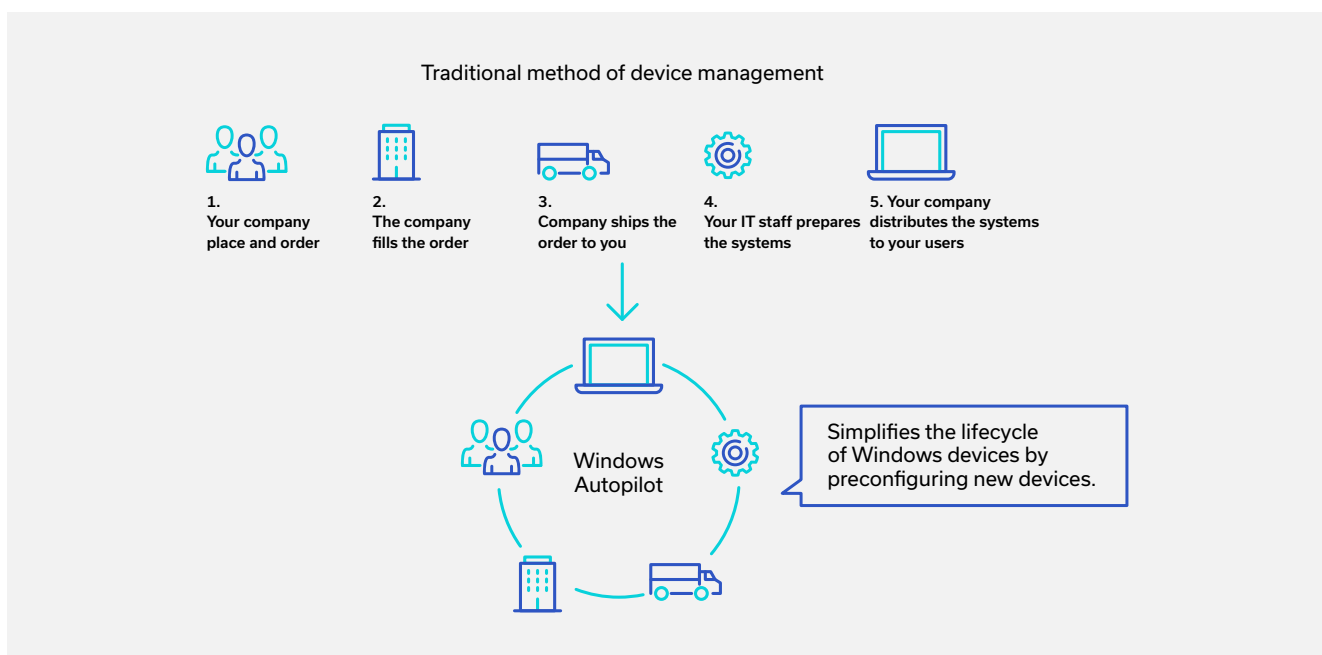
Security – With more compliance certifications than any other cloud provider, Microsoft has more than 3500 security experts dedicated to protecting your data. AVD with multi factor authentication (MFA) also allows users to securely access their work from anywhere.

Seamless end user experiences – Whether your users are loading their desktop on a tablet at home, shared laptop or a workstation anywhere, the Windows interface is the same and the experience is seamless and protected.

Windows Autopilot

When it comes to hybrid working, configuring and deploying end-user devices for your staff can be slow and present real problems for your business. The new device experience often requires manually configuring a host of time-consuming processes. It's a hassle for both end-users and IT admins, especially when mass deployment is needed, such as for remote employees.

This is where Windows Autopilot is a great option. Whereas a traditional procurement process would take a lot of time and effort, Windows Autopilot simplifies the lifecycle of Windows devices by preconfiguring new devices for production use & for resetting & recovering existing devices.





Endpoint Manager

Microsoft Endpoint Manager is a Microsoft Azure service that provides you with a wide range of features and services to manage and monitor a full range of devices including: mobile devices, desktop computers, virtual machines, embedded devices and servers. It allows you to secure your devices and data on devices.

Microsoft Endpoint Manager offers a seamless, end-to-end management solution without the complexity of a migration or disruption to productivity. It is perfect for organisations looking to provide greater security, monitoring and updates across a full range of devices.

Endpoint Manager combines services you may know and already be using, including Microsoft Intune, Configuration Manager, Desktop Analytics, co-management and Windows Autopilot. These services are part of the Microsoft 365 stack to help secure access, protect data, as well as respond and manage risk.

Going serverless with Azure

Digital transformation has made waves in many industries, with revolutionary models like Infrastructure as a Service (IaaS) and Software as a Service (SaaS) that make digital tools much more accessible and flexible, allowing you to rent the services you need rather than taking on large commitments of owning them. Rather than owning and managing everything through a private cloud, organisations can go serverless with one of many cloud service providers like Microsoft Azure.

Azure allows you to deliver more value to the core of your business by minimising the time and resources you spend on infrastructure-related requirements. Use fully managed, end-to-end Azure serverless solutions to boost developer productivity, optimize resources, and accelerate the pace of innovation. There are countless benefits of using a service like Azure including:

Enhance security - Protect your legacy apps with advanced security capabilities, including Conditional Access, identity protection, and multi-factor authentication.

Centralise access management - Simplify app management by centralising access controls across your cloud and legacy apps with a single identity solution.

Reduce costs - Reduce your on-premises identity infrastructure, retire web access management solutions and use modern access methods for your legacy apps.

Streamline access - Provide seamless access with single sign-on to cloud and on-premises apps and help your workforce be more productive.





Managing threats with Microsoft

With cybercriminals constantly looking for ways to exploit your IT systems, as an organisation you must be confident with your ability to quickly identify and mitigate any potential security risks. Microsoft offer several security solutions to make your life so much easier. We have listed some common problems that we encounter with our clients and have listed a range of Microsoft solutions to help combat these issues.

	Issue	Solution
User	<ul style="list-style-type: none">› Compromised user credentials – weak user passwords	<ul style="list-style-type: none">› Multi-factor authentication› Risk-based conditional access
Device	<ul style="list-style-type: none">› Compromised device› Unmanaged device – BYOD –contains your corporate data› Weak pin – anyone can access the device	<ul style="list-style-type: none">› Full centralised management of mobiles and laptops with Intune› Remote wipe of data lost & stolen devices› Enforce strong pin requirements with wifi, VPN profiles
Apps	<ul style="list-style-type: none">› Users can copy/paste/save corporate data to personal apps› Using third party apps with weak security	<ul style="list-style-type: none">› Intune application management restricts copy/paste/save to personal apps› Azure information protection
Email	<ul style="list-style-type: none">› Email malware vulnerabilities› Ransomware threats/phishing› Protecting sensitive data from being sha	<ul style="list-style-type: none">› Office 365 Advanced Threat Protection› Data loss prevention› Email restrictions
Docs	<ul style="list-style-type: none">› Important documents need to be protected internally and externally› Making sure only the right people have access› Making sure people leaving the organisation don't have access	<ul style="list-style-type: none">› Azure Information Protection protects, classifies documents for secure sharing› Revoke access to documents› Track sensitive documents

Hybrid working is here to stay, is your infrastructure optimised to the fullest? Use this guide to help you in your journey towards a better hybrid working strategy. If you'd like to speak to a member of our team, contacts us for a hybrid working technology assessment where we can work with you to improve your hybrid working environment.

What's next?

Hybrid working technology assessment

Our hybrid working technology assessment is perfect for organisations looking to improve their hybrid working infrastructure.

[FIND OUT MORE >](#)

Since 2003 Bridgeall has delivered advisory, development, implementation and support services to our clients on 100's of successful projects. We're a multiple Microsoft Accredited Gold Partner and ISO9001, ISO27001 and Cyber Essentials accredited.

WE'LL HELP YOU BUILD YOUR MODERN INTELLIGENT WORKPLACE QUICKLY AND SECURELY.

[bridgeall.com](https://www.bridgeall.com)



[linkedin.com/company/bridgeall](https://www.linkedin.com/company/bridgeall)



twitter.com/bridgeall



Glasgow Head Office

George House

50 George Square

Glasgow, G2 1EH

www.bridgeall.com