avanade

Remote working challenges

Frequently asked questions from our clients

At Avanade, we are committed to sharing our expertise and insight so that you can keep your business productive and your employees engaged during this time.

Here we share the most **frequently asked questions** we are hearing, from our clients in IT and business leadership roles across the globe, about remote working. These cover everything from questions around managing cultural considerations, to enabling effective collaboration to securing the workplace.

- Managing Culture
- Scaling Technology
- Collaboration
- Microsoft Teams
- Productivity
- Security

Managing Culture

How can I successfully manage culture and awareness during this time?

We recommend that organizations focus on welcoming change. This means including a democratic and proactive aspect in your culture as part of your remote working initiative. Encourage employees to challenge the status quo and suggest ways of doing things differently. Ask your team to come up with ways to enhance communication and conduct regular "team retrospectives" to reflect on what can be improved.

Take the time to educate your people on how to effectively and productively work from home and leverage collaboration tools and other technologies – and ensure that leaders act as role models for virtual behaviour. Also ensure that IT can help employees with any potential issues they may have - a service desk SWAT team is ideal.

Bear in mind that employees who aren't used to working from home may find the change to their usual ways of working a challenge, so it's important to try to keep engagement high. Some things to consider are:

- Create a support network and assign remote working champions to help colleagues understand how best to work from home within the context of their role.
- Use video as much as you can – seeing people can make a big difference.
- Use meetings to also do fun events, such as virtual networking in the evening or at lunchtime.

How can I keep my employees informed about my organization's remote working strategy?

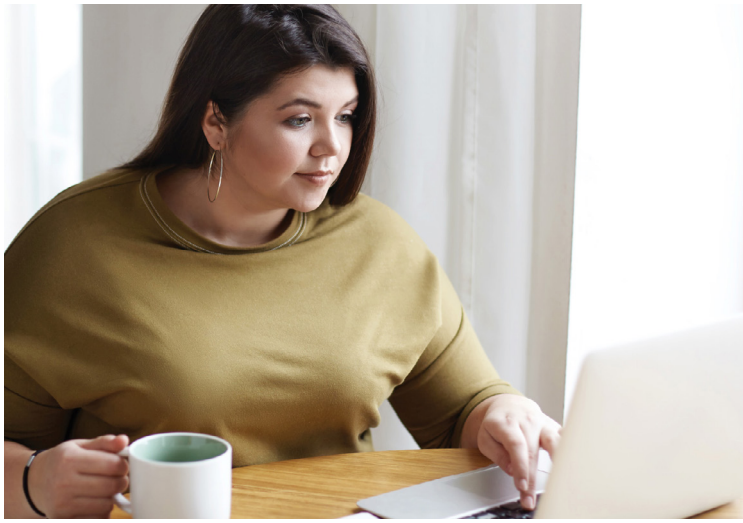
In our experience, when people can hear and see each other they are much more engaged. We recommend enabling interactive broadcast and web conferencing for events to support the shift from physical to virtual working, meetings, workshops and conferences.

On a project or department level a hub for teamwork is ideal, to enable multiuser texting, voice calling and video conferencing on the desktop, on tablets and smartphones so employees can stay connected and informed.

What can I do to help maintain employee trust in leadership?

Open, frequent communication and close collaboration are crucial. Using a hub for teamwork to enable virtual connections between employees, suppliers and customers is a great way to help maintain trust and manage the business impact. A transparent leadership style and regular communications work best. Be open about the situation and the plan moving forward and provide regular updates on topics that affect the business and employees directly, such as personal time off and flexible working.

It's also important to focus on the human element. Broadcast to various levels in your organization about how leaders have responded with messaging focused on flexi-time, taking care of families, etc. And keep a check on employee well-being by having more regular touch points than before. At the same time, prepare contingency plans to cover any absence of critical employees.



Scaling Technology

How can I scale my existing technology to enable remote working in response to COVID-19?

You're likely to experience a much higher demand for virtual communications and collaboration, including virtual meetings, conferences and broadcast events during this time. And for IT leaders, supporting the needs of the business may present a challenge.

There are several key considerations around scaling existing technology. You can try to rapidly expand your existing technologies, by assessing and scaling networking and VPN/NG firewalls to handle the foreseeable growth in load. Analyze your team's capability to rapidly scale and consider whether leveraging a partner would be worthwhile.

Some parts may be easy and some not, but it's important to do the appropriate due diligence. Consider the implications for all the following:

- Mobile contracts (in terms of data volume)
- Wireless configuration for home networks
- Bandwidth considerations
- VPN configuration

You will also need to provide a good experience to your employees, so it's important to implement rigor around monitoring items such as available capacity and quality of service. Be sure to also provide training to help employees use the tools that they need.

And if you do encounter limitations, provide guidance to your organization to help ease some of the pressure on your network.

For example, you can move non-essential audio calls to PSTN – which allows you to maintain one-to-one meetings, collaboration, document sharing and access to whiteboarding features. You can also consider turning off video if necessary, as it may consume a huge amount of bandwidth especially during peak hours in the morning.

If I am using Skype for Business on premise, how can I check my capacity?

If you're using Skype for Business on premise, you can do a quick check of the capacity you have according to the infrastructure you've deployed. To review your edge server capability and bandwidth from your data center, you can use the Skype for Business Bandwidth Calculator to run these calculations. From the tool, you'll be able to roughly calculate how many audio sessions can transit your network and the number of sessions and conferences you can support. If you need help, call us or seek guidance from your technology partner.

How can I solve capability gaps to ensure business continuity in response to COVID-19?

Create a task force to close gaps in your infrastructure landscape. For example, you can take a closer look at cross-company integration and consistency. You can also explore options to source devices to mobilize your workforce and establish virtualization technology like Virtual Desktops. This will push company resources locked in the back-end towards your remote users

Collaboration

How can I quickly provide my employees with tools to communicate and collaborate?

Use the Microsoft Office 365 (O365) platform and tools to enable your employees to work remotely and guarantee business continuity. Each employee will only need a standard device, like smartphone, tablet, PC/ laptop with internet access. The **Office 365 E1 license** contains the following services:

- Office applications (web-based) on tablets and phones (Office Online)
- Email and calendars (Exchange Online)
- Hub for teamwork (Microsoft Teams)
- Workflow automation (Power Automate)
- Online meetings (Microsoft Teams)
- Professional digital storytelling (Sway)
- File storage and sharing (SharePoint and One Drive for Business)

The minimal requirement is that organizations need Azure Active Directory (AD) to be set up and configured to enable employees to access Office 365 cloud services (with E1 license).

How can my employees collaborate securely with their external partners?

Deploy an external sharing solution (with Microsoft Azure B2B) to allow employees to keep minimal business continuity with their external business partners, customers or suppliers.

The solution provides additional control/management over Office 365 platform services and has identity lifecycle capabilities such as onboarding and deleting Azure B2B accounts, modifying permission, etc.

As a requirement your organization needs to have an active Office 365 platform and purchase Azure Active Directory licenses (AAD Premium P1 or P2).

Users will need help from business and IT leaders, so our recommendation is for IT leaders to establish a SWAT team to quickly provide, or to expand, business-to-business connectivity solutions to strategic partners. Federation is key and this needs to be done with the partner organization's Office 365 tenant. Ensure your data is secure and classified in the right way.

How can I quickly provide my employees with an application to communicate during a crisis period?

Consider deploying Microsoft Power Apps Platform, which can be used to create a communications capability that can be customized in line with your company's specific requirements. You can also deploy the Microsoft Crisis Communication app to keep your employees informed and up to date with the latest information during the crisis period.

In the event you have already deployed Office 365 and Power Platform, they can also be used for enhanced rapid app development. As part of the platform, Power Automate can also continuously provision information for urgent needs through an automated workflow – overlaid with 24/7 conversation to a chatbot. As an example, consider using Power Virtual Agents provided by Microsoft in response to COVID-19 that use data gathered from leading institutes like the CDC or NHS.

As a requirement you need an active Office 365 platform and have approval from a security perspective to deploy Power Platform.

At Avanade we have set up a specific SharePoint site to share information on recent events. This includes working procedures, processes and remote working guidance. We are also heavily using Teams for all meetings and events. For business continuity, we are moving engagements that have previously been in person to a virtual environment. As an example, we have conducted interactive meetings via Teams in combination with whiteboard technology from Microsoft or MURAL to run design thinking workshops.

How can I quickly provide my employees remote access and connectivity to corporate applications?

We recommend that you implement and/or scale Microsoft Windows Virtual Desktop or Citrix environment to allow employees' connection to desktop machines and web applications on the corporate network.

As a requirement you will need an Azure subscription and connectivity to an Azure data center (Site-2-Site VPN).

In the medium term, you could consider delivering the applications via digital hubs for ease of access in a highly personalized way. Leveraging our partner Akumina, you can rapidly set up a foundational experience and configure core capabilities such as search and workflow.

You can format your homepage, department sites, video library, company calendar, content pages, user dashboard, FAQ page, announcements and more. You can consider virtual workshopping to put requirements on a fast track, get aids in Akumina adoption and create a value map to guide your next steps to innovate for your people.

How can I accelerate device enablement and mobility for my employees?

Our recommendation is to prioritize employees who have critical roles in driving the business and ensure they have the tools and access they need. Reclaim devices from users with more than one device and use contractor devices or creative options such as sourcing Device as a Service or a bring your own device (BYOD) policy to support retail purchases. Some organizations have had employees take their desktop PC home with them.

What if I have only a limited number of corporate mobile devices in place that are not sufficiently managed?

To enable corporate data access on managed and/or non-managed mobile devices and to enable BYOD scenarios, it is necessary to implement an appropriate mobile device and application management capability. This will provide app protection policies, appropriate governance, security and data protection measures for mobile applications and devices.

Quickly enabling, securing and managing virtual work environments can be further orchestrated with management solutions such as BitLocker or Intune. Microsoft Intune enables identity-driven access to applications and devices and data protection for mobile devices. It integrates with other services, including Microsoft 365 and Azure Active Directory (Azure AD) to control who has access to what.

How can my employees have remote access and connectivity to corporate applications without disrupting the corporate network (minimal VPN access)?

Deploy and configure an Application Proxy (based on Azure AD) to rapidly allow employees to remotely access applications inside the corporate network without VPN and with seamless authentication.

As a requirement you will need to have an Azure AD license (P1/P2) and Azure AD connect synchronization.

How can my employees establish connectivity from their mobile devices (company or privately owned)?

Many users may have to rely on mobile networks for connectivity and the use of mobile apps to connect to the corporate network. Mobile users face challenges such as cellular network coverage, mobile access, security and computer tethering. To allow users to access the corporate network, two-factor authentication such as Microsoft Company Portal can be used to secure data. Educate employees that mobile tethering may result in data charges that exceed their plan limits.

How can I provide my employees with a secure environment for collaboration?

Implement a security layer in Office 365 such as Azure Information Protection, which allows you to configure policies and protect company data from social and cyberattacks. Provide guidance to employees on best practices regarding security on their home network. With Microsoft Defender Advanced Threat Protection (ATP) on the employee's devices you will have visibility to the risks before they become issues. Each employee will need a company or personal device, like a smartphone (that ensures their biometrics) to receive the necessary codes to access corporate data (via multifactor authentication, MFA).

As a requirement you will need to subscribe to the P1 plan (included in Office 365 Business) or P2 (included in Office 365 E5, A5 and Microsoft 365).

Microsoft Teams

How do I get access to Microsoft Teams?

Most workplaces will have access to Skype for Business or Teams as part of their Office 365 subscription. If you do not have access to Microsoft Teams, Microsoft is making six-month free usage available. Click here for more information.

How can I enable meetings for large groups?

Teams and Skype for Business enable meeting of up to 250 users, where all can fully collaborate. But if you need more capacity, these are the steps you can take:

Enable broadcast meetings through Teams live events or Skype Meeting Broadcast. These are streamed and don't place as much pressure on your network. Only a small number of people will be able to present or share video, but everyone will be able to ask questions. You don't need to have Teams or Skype for Business fully deployed at your organization to use these. And users may be able to join with minimal setup from a browser. Learn more about Teams live events here.

Where can I find the best training resources for Microsoft Teams?

You can download our Teams rapid resource guide here which features how-to videos, key recommendations and best practices to help you put Teams to work.

Microsoft also has a dedicated training site that can be accessed here.

Six months of free Teams training videos with Avanade's partner CoreView is also available. Click here for more information.

How can I troubleshoot and proactively manage the performance of Teams and related cloud services?

Our partner ThousandEyes is offering help to get remote working activated and analyze or monitor end-user experience. The endpoint agents are empowered to:

- Visualize end-to-end SaaS and web application performance
- Get real-time insights into Wi-Fi, WAN and the internet
- Quickly identify and triage network issues

Furthermore, we can support you to configure and learn about:

- Monitoring Office 365 service status and message center for outages reported by Microsoft
- Monitoring Call Quality Dashboard proactively for audio/video quality
- Monitoring usage to identify unexpected usage drops

Productivity

How do I help my employees remain secure while being productive?

For your employees to stay productive, you will need to address a number of key aspects of the virtual working environment. Start by educating employees about security initiatives and encourage open communication with operational teams. This means making sure that access policies, permissions and audit logs are in place to enable the use of a virtual work environment.

In addition, offer virtualized workspaces that allow secure access to remote applications and data for employees who do not have access to secure mobile devices. Finally, consider establishing dedicated service management teams enabled with remote user-specific standard operating procedures/FAQs to effectively support the workforce in a high-touch environment.

How can I keep my organization's workplace performance high while a big part of my user population is working from home - potentially in an uncontrolled environment?

Provide clear and prescriptive guidance to employees about broadband connectivity options and packages in their home locations. Consider subsidizing higher bandwidth and quality of service solutions. As most network issues start at home, provide guidance to employees on the best Wi-Fi home network solutions.

Give advice on where to place the gateways and direct people to use 5 GHz frequencies to avoid interference. Guide them on how to configure the solutions to prioritize voice, video and collaboration traffic, and help them troubleshoot issues.

How can I make sure that employees can be productive with no face-to-face interaction?

Establish state-of-the art tooling that allows employees to make decisions and produce content efficiently; this will allow them to collaborate and establish multimodal communications.

Consider creating a framework to adopt and measure collaboration. This will require a detailed collaboration strategy as well as an education program if employees are new to the platform.

Key business-to-business interaction should be established using the same tooling that people use internally – don't use unsecure tools like WhatsApp, for example - and also make it a priority to have a SWAT team available to help.

Employee security

How do I scale remote working capabilities securely?

The unprecedented demand for accessing company resources remotely puts extra pressure on access points and VPN services. The user experience and the ability to work remotely depend on your infrastructure's ability to scale in order to meet the demand.

A modern born-in-the-cloud Application Proxy solution that enables secure remote access to internal web applications – with additional security checks via conditional access and MFA – is highly scalable. And it can support a broad range of authentication capabilities.

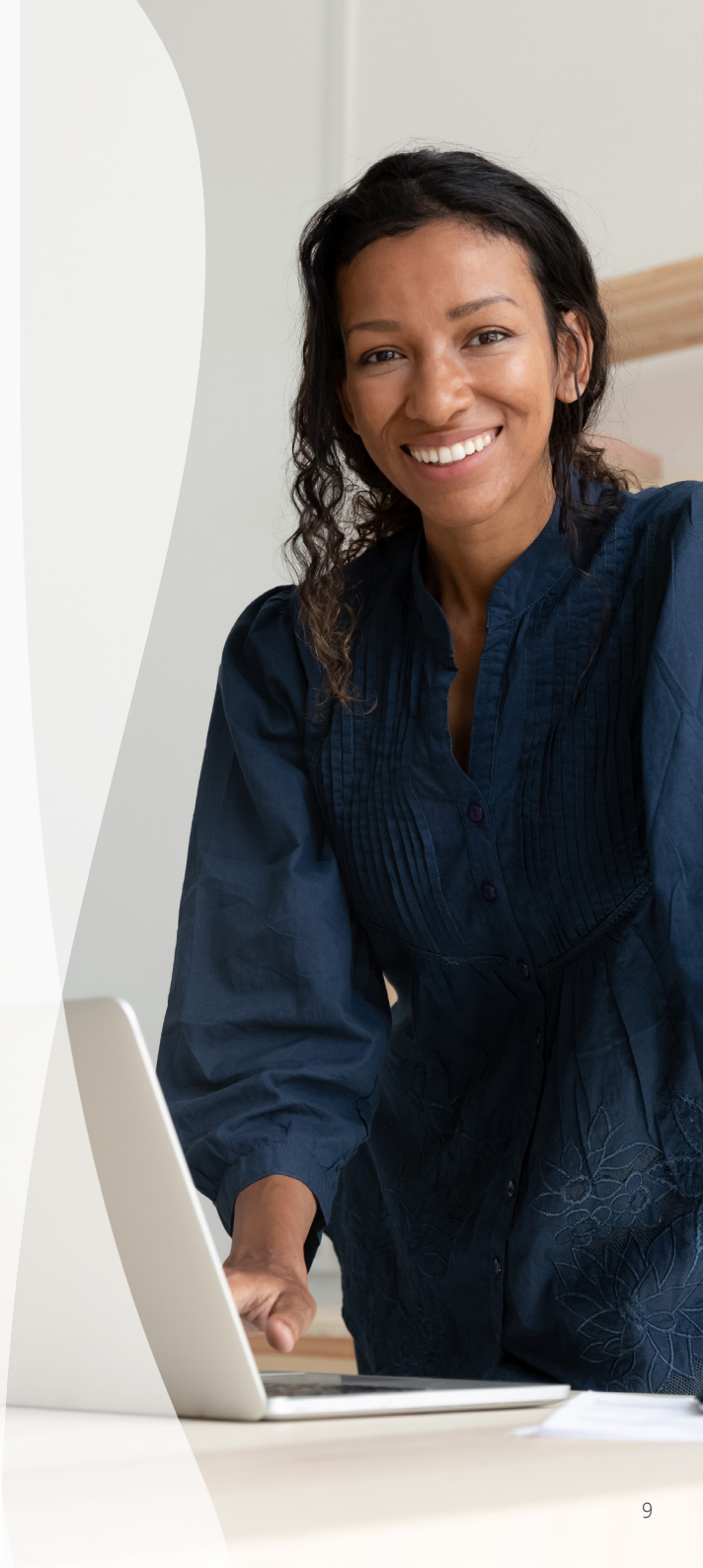
You can also complement your traditional VPN technology with new cloud remote access solutions that will improve remote worker security while alleviating capacity risks on your legacy VPN solution.

Enable split tunneling where possible so users can get the fastest access to cloud services and alleviate traffic to a central VPN solution. At the same time, confirm your capacity on traditional remote access technologies, such as VPN concentrators, next-generation layer 7 firewalls and circuits.

What other security challenges do I need to consider when more of the workforce is working from home?

Provide guidance to employees on best practices regarding security on their home network. Understand the users who have increased requirements for security, such as those handling sensitive data. Help employees to control where data resides and is processed by considering what security policies should be extended to corporate-owned devices or even personal devices.

Configure information protection for classifying and managing sensitive corporate data at rest and in motion. Enabling BYOD for employees and partners may require enhanced security and compliance controls for corporate assets through an endpoint management solution. Finally, consider reviewing and assigning policies to ensure and enforce secure behaviors. To achieve that, provide employees with clear, prescriptive guidance to help them adopt the behaviors required to remain secure in any remote working scenario.



Secure collaboration

How can I provide my employees with an advanced protected environment for collaboration?

Implement a security layer in Office 365, such as Azure Information Protection, which allows you to configure policies and protect company data from cyberattacks.

Microsoft Defender Advanced Threat Protection (ATP) on the employee's devices gives you visibility into risks before they become issues. Also ensure each employee has a company or personal device, like a smartphone (ideally enabled with biometric authentication), to receive the necessary codes to access corporate data (via multifactor authentication). This requires a subscription to the P1 plan (included in Office 365 Business) or P2 (included in Office 365 E5, A5 and Microsoft 365).

How can my employees interact and collaborate securely with their external partners?

Deploy an external sharing solution (with Microsoft Azure B2B) to allow employees to maintain business continuity and collaborate with external partners, clients or vendors. This solution provides additional control and management over Office 365 platform services. It also features identity lifecycle capabilities, such as onboarding and deleting Azure B2B accounts, modify permission and more.

This needs an active Office 365 platform as well as Azure Active Directory licenses (AAD Premium P1 or P2).

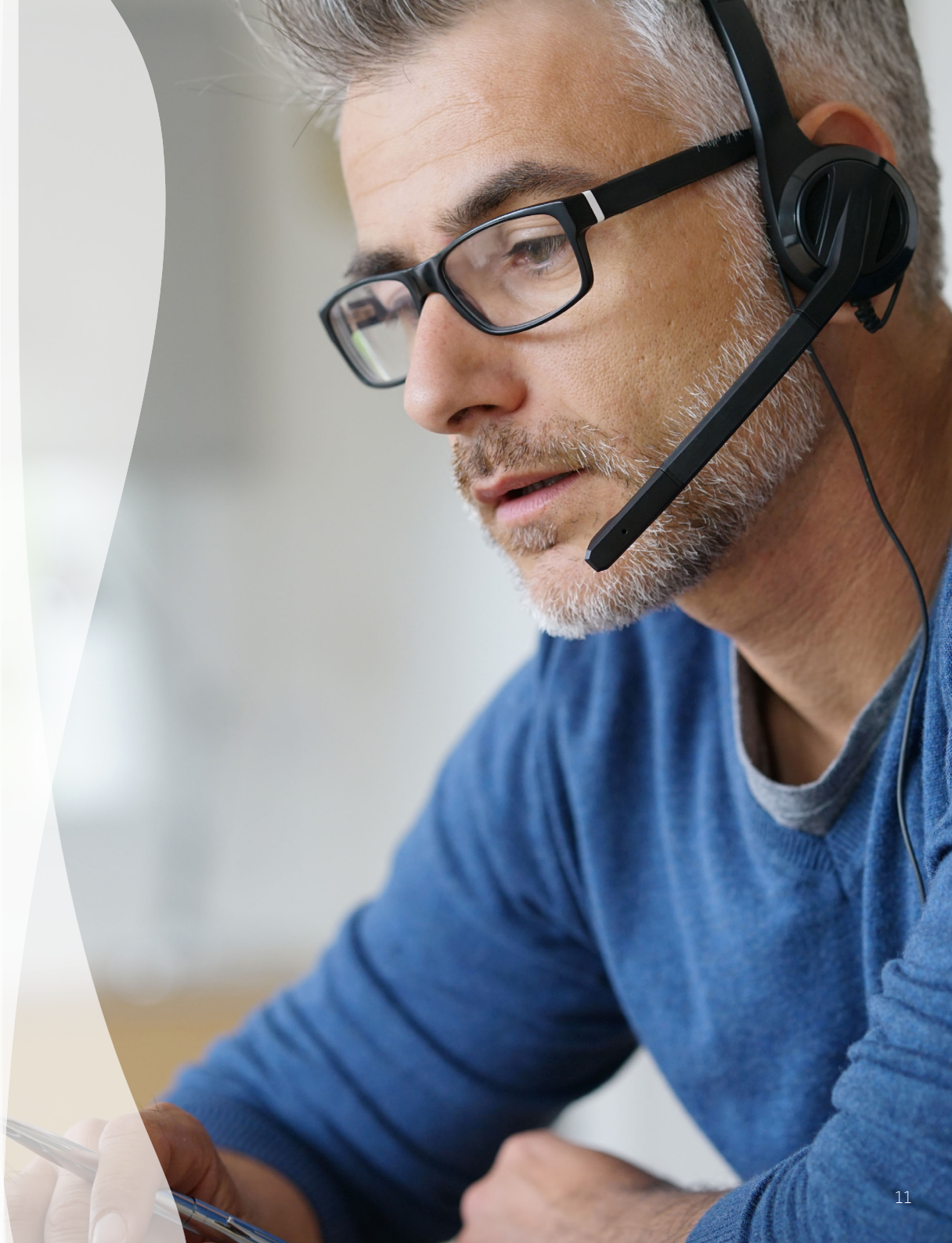
Information security

How do I protect my information if it leaves the organization?

Company data that can be accessed remotely or sent remotely can remain "containerized" and be managed securely by using Microsoft Intune, Information Protection and Azure AD.

This enables users to access Office applications from their home laptop or mobile by protecting information with Microsoft Application Management (MAM) and Windows Information Protection (WIP), securing Office 365 data within Office desktop and mobile applications.

Microsoft Information Protection can further protect information by classifying and protecting assets using document-level encryption and access control lists. This is supported cross-platform and cross-device.



Access and applications

Can I monitor who has access to data and applications, and monitor what they're doing with them?

If you're concerned that employees are using external file sharing services to work around internal IT limitations, you can monitor and assess this with Cloud App Security Broker, which can discover the cloud applications being used in your enterprise. It identifies and combats cyberthreats and enables you to control how your data travels.

How do I ensure the right people get the right access to resources?

It all starts with managing identities. Whether your organization has a hybrid environment or is fully in the cloud, checks and balances can be put in place around identification, authentication and authorization and to ensure monitoring continually takes places.

Policies and conditional access rules will ensure that the right people get access to the right resources (applications, data, services) at the right time.

How do I securely enable access to my organization's applications remotely?

Most organizations are running lots of business-critical apps on-premises, many of which may not be accessible from outside the corporate network.

Azure AD Application Proxy is a lightweight agent that enables internet access to your on-premises apps, without opening up broad access to your network. You can combine this with your existing Azure AD authentication and Conditional Access policies to help keep your users and data secured.

How do I enable access to resources on BYOD devices?

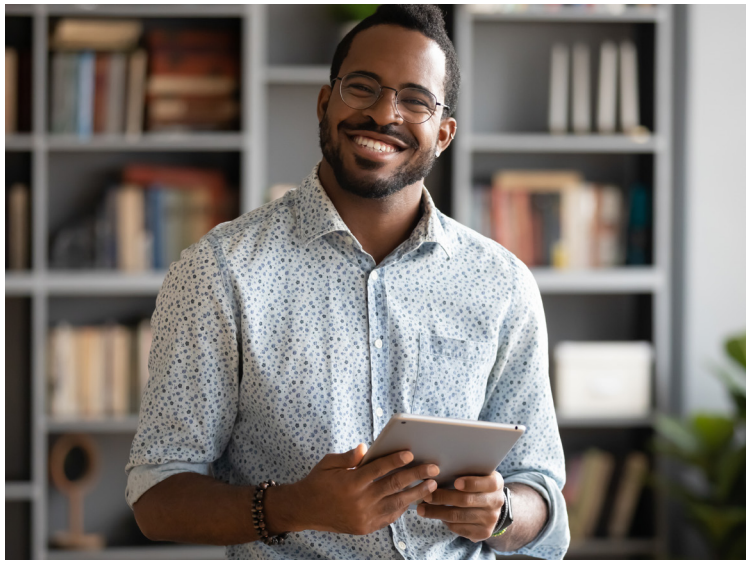
With more employees working remotely and across devices, it's important to support BYOD scenarios. You can offer self-service enrollment so users can quickly and easily join Azure AD and enroll in Microsoft Endpoint Manager (MEM) to access company resources.

Once enrolled, MEM then applies appropriate policies, for example, to ensure that a device is encrypted with a strong password and has certificates to access things like VPNs and Wi-Fi. MEM can also ensure that devices are adhering to policy by checking-in the device's health compliance status to Azure AD as it processes the user's authentication.

How can I enroll my employee's personal mobile devices to securely access corporate applications?

Our recommendation is to deploy an enterprise mobile device management platform such as Microsoft Intune to securely enable employees to get access to corporate applications. This will allow a separation of corporate data and personal data at a device level while maintaining business productivity.

You'll need an active Office 365 platform with Azure Active Directory and Microsoft Intune licenses (either standalone or as part of EMS E3/E5).



We hope you find these answers useful.

If you have any specific remote working challenges please reach out to us. You can also find more guidance and advice around remote working on Avanade.com.

North America
Seattle
Phone +1 206 239 5600
America@avanade.com

South America
Sao Paulo
AvanadeBrasil@avanade.com

Asia-Pacific
Australia
Phone +61 2 9005 5900
AsiaPac@avanade.com

Europe
London
Phone +44 0 20 7025 1000
Europe@avanade.com

About Avanade
Avanade is the leading provider of innovative digital and cloud services, business solutions and design-led experiences on the Microsoft ecosystem. Our professionals bring bold, fresh thinking combined with technology, business and industry expertise to help make a human impact on our clients, their customers and their employees. We are the power behind the Accenture Microsoft Business Group, helping companies to engage customers, empower employees, optimize operations and transform products, leveraging the Microsoft platform. Avanade has 38,000 professionals in 25 countries, bringing clients our best thinking through a collaborative culture that honors diversity and reflects the communities in which we operate. Majority owned by Accenture, Avanade was founded in 2000 by Accenture LLP and Microsoft Corporation. Learn more at www.avanade.com

avanade


avanade