avanade

Remote working challenges

Frequently asked security 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 security 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.

- **Employee security**
- **Secure collaboration**
- **Information security**
- **Access and applications**

avanade

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 explore our Security solutions and 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