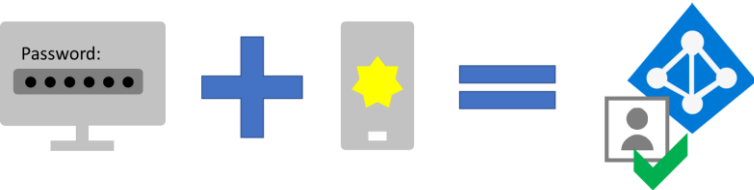**Microsoft**

Empower remote workers with Microsoft 365

Features in Microsoft 365 and other Microsoft cloud services enable you to work from anywhere and at any time in a highly collaborative, productive, and secure way. Follow the steps below to empower remote workers.
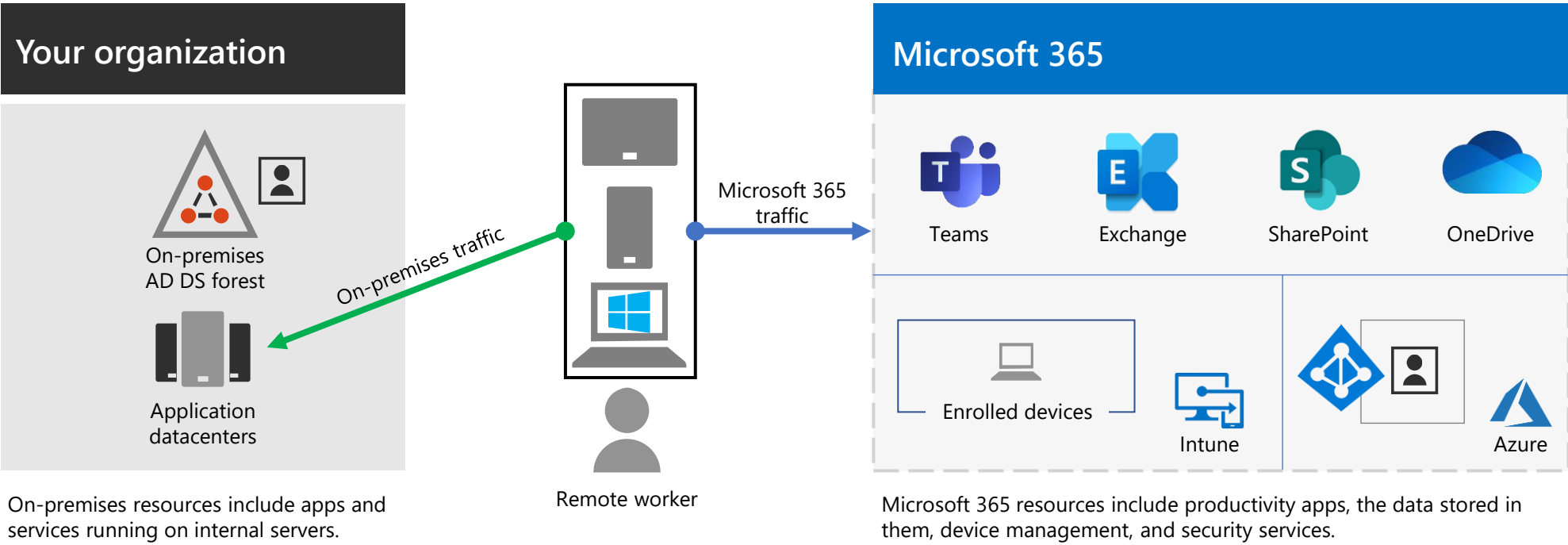
Step 1. Increase sign-in security with multi-factor authentication and Conditional Access
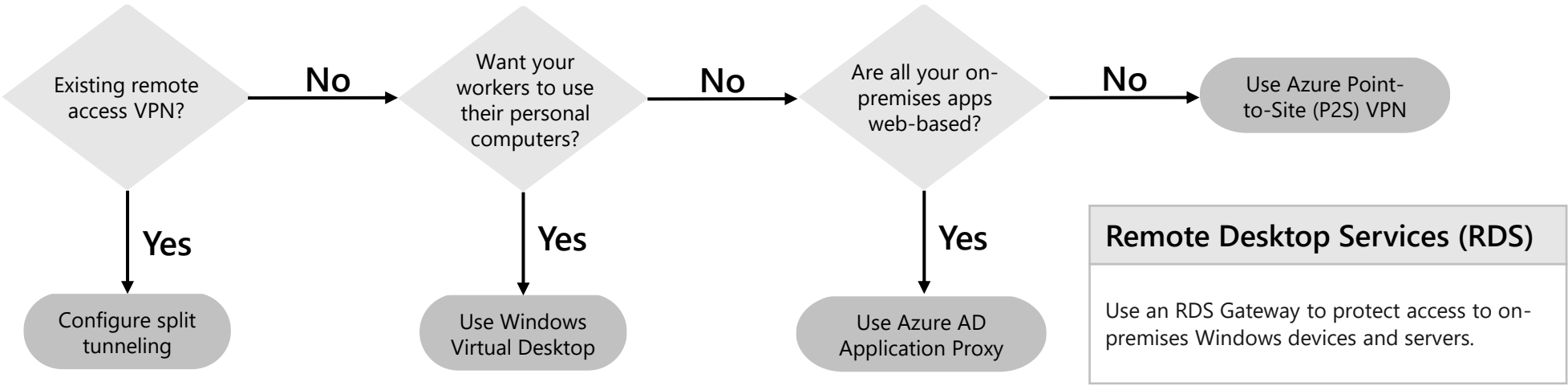
Use Conditional Access to require remote workers to sign in using a password and an additional verification method such as Microsoft Authenticator, a phone call, or a text message.

Step 2. Provide remote access to on-premises apps and services

For many organizations, remote workers need access to both on-premises and cloud apps and resources.

Your organization

On-premises AD DS forest

Application datacenters

On-premises resources include apps and services running on internal servers.

On-premises traffic

Remote worker

Microsoft 365 traffic

Microsoft 365

Teams   Exchange   SharePoint   OneDrive

Enrolled devices

Intune

Azure

Microsoft 365 resources include productivity apps, the data stored in them, device management, and security services.

Use this flowchart to determine how to provide remote access:

Existing remote access VPN? — **No** → Want your workers to use their personal computers? — **No** → Are all your on-premises apps web-based? — **No** → Use Azure Point-to-Site (P2S) VPN

- Existing remote access VPN? — **Yes** → Configure split tunneling
- Want your workers to use their personal computers? — **Yes** → Use Windows Virtual Desktop
- Are all your on-premises apps web-based? — **Yes** → Use Azure AD Application Proxy

Remote Desktop Services (RDS)

Use an RDS Gateway to protect access to on-premises Windows devices and servers.

Step 3. Deploy security and compliance

Security	• Office 365 Advanced Threat Protection (ATP) to protect your Microsoft 365 apps and data from attack • Malware protection for Windows 10, SharePoint files, and Exchange email • Microsoft Defender ATP to detect and respond to advanced cyberthreats • Cloud App Security to protect both Microsoft 365 and other SaaS apps • Azure Active Directory (Azure AD) Identity Protection to detect and remediate identity-based risks ✔ docs.microsoft.com/microsoft-365/compliance/compliance-quick-tasks
Compliance	• Sensitivity labels to classify your data for levels of protection • Data Loss Protection (DLP) to prevent inappropriate sharing of data • Conditional Access App Control to keep sensitive data off personal devices • Data retention labels and policies to implement data governance • Office message encryption (OME) for secure email to internal and external mailboxes • Communication Compliance to prevent inappropriate messages and Insider Risk Management to address malicious and inadvertent risks • Compliance Manager and Compliance Score (preview) to manage and improve your subscription's compliance configuration ✔ docs.microsoft.com/microsoft-365/security/top-security-tasks-for-remote-work

For deployment guidance, visit aka.ms/m365eremoteworkers

Empower remote workers with Microsoft 365

Step 4. Deploy endpoint management

Microsoft Intune	Configuration Manager	Co-management	Desktop Analytics	Windows Autopilot
Use app protection policies for granular control over data and allow access only for the right people under the right conditions.	Deploy apps, software updates, and operating systems to manage desktops, servers, and laptops from on-premises or the cloud.	Attach your existing Configuration Manager deployment to the Microsoft 365 cloud to concurrently manage Windows 10 devices.	Use Desktop Analytics to inventory apps running in your organization and deploy Windows 10 to pilot and production-managed devices.	Simplify the lifecycle of Windows devices by pre-configuring new devices for production use and for resetting and recovering existing devices.

Microsoft Endpoint Manager includes Microsoft Intune and Configuration Manager.

Step 5. Deploy remote worker productivity apps and services

Microsoft Teams	Exchange Online and Outlook	SharePoint and OneDrive	Microsoft 365 Apps
• Chat and conversations • Meetings, events, and conferences • Calling • Apps and workflows	• Send and receive email • Manage calendars, contacts, and tasks	• Migrate files to SharePoint and OneDrive • Collaborate on, store, and manage documents • Work from Teams, Office desktop apps, or a web browser	• Create and co-author in real time on documents • Get the latest security and feature updates

Includes PCs and mobile devices such as smartphones and tablets.

Step 6. Train remote workers

Sign-in	• How to use MFA with an additional verification method • How sign-ins can be blocked for users that use legacy authentication • How risky sign-ins can be blocked or force the employee to change their password
Remote access	• How to use your organization's remote access VPN client, an Azure virtual desktop, or RDS
Endpoint management	• How endpoint management policies can be used to block access for non-compliant devices • The use of allowed apps and how app polices can be used to block the use of apps • How to use and interact with Windows 10 Enterprise security features
Productivity apps and services	• How to install and use Microsoft 365 Apps • How to use Teams for chat, video-based conferencing, document sharing, and threaded conversations • How to use Outlook for email and scheduling • How to use SharePoint team or communication sites and OneDrive folders to browse and collaborate on files in a user's library and those belonging to a group 🎓 support.microsoft.com/training

For deployment guidance, visit aka.ms/m365eremoteworkers