THE OFFICIAL

WINGMAN GUIDE
TO REMOTE WORK

TIPS AND INFORMATION TO
SUCCESSFULLY WORK REMOTELY

pax8

ABOUT THIS GUIDE

This guide offers recommendations to help your clients adapt to remote work by optimizing their remote collaboration experience while ensuring they stay productive and secure.

INTRODUCTION

THE CHALLENGES OF ADAPTING TO THE SURGE IN REMOTE WORK

Microsoft Teams hit 44 million daily active users on March 18, 2020, up from 32 million just a week earlier on March 11 – and a 120% increase from 20 million daily active users in November 2019.[1]

While remote work adoption has been steadily increasing across industries and business of all sizes for the past ten years, rapidly changing market conditions in Q1 2020 have led to a drastic global spike in companies turning to remote work to stay productive. Remote work has proven benefits, such as increased productivity and employee satisfaction, but it also brings increased security challenges as employees remotely access the company network, files, and data. Your clients may be struggling to extend existing remote work capabilities to a larger set of employees or trying to kick off remote work programs from scratch within a short window.

BENEFITS OF REMOTE WORK

77%

of remote employees say they're more productive when working from home.[2]

76%

of employees prefer to avoid their office completely when they need to concentrate on a project.[3]

98%

of remote workers want to continue to work remotely (at least some of the time) for the rest of their careers.[4]

CHALLENGES OF REMOTE WORK

Less than half of remote employees say they receive proper internet security training – despite receiving confidential business data![5]

46%

of employees admitted to transferring files between work and personal computers when working from home.[6]

36%

of organizations have dealt with a security incident due to an unsecured remote worker.[7]

INTRODUCTION

OPTIMIZE REMOTE WORK PRODUCTIVITY – AND KEEP CLIENTS SECURE

As a trusted technology advisor, you are well-situated to help your clients optimize their teams' remote productivity and, most critically, help them stay secure as their suddenly distributed workforce begins to access corporate data from remote networks and locations. So, how can you best enable your clients' rapid transition to remote work?

1 OPTIMIZE REMOTE PRODUCTIVITY AND COLLABORATION TOOLS.

- **Recommend UCaaS and cloud file storage tools** best suited for each client's business needs.
- **Offer guidance on remote work best practices** to help employees stay productive and connected.
- **Provide training resources** so that end users are comfortable with new tools and workflows.

2 HELP CLIENTS ESTABLISH AND FOLLOW REMOTE SECURITY BEST PRACTICES.

- **Educate clients** on remote security best practices.
- **"Harden" productivity apps** by configuring them to the optimal security settings for remote work.
- **Use a layered approach** to secure remote work environments using leading cloud security solutions.
- **Encourage clients to create policies** around proper network access, file sharing, and cloud storage hygiene to protect company data.

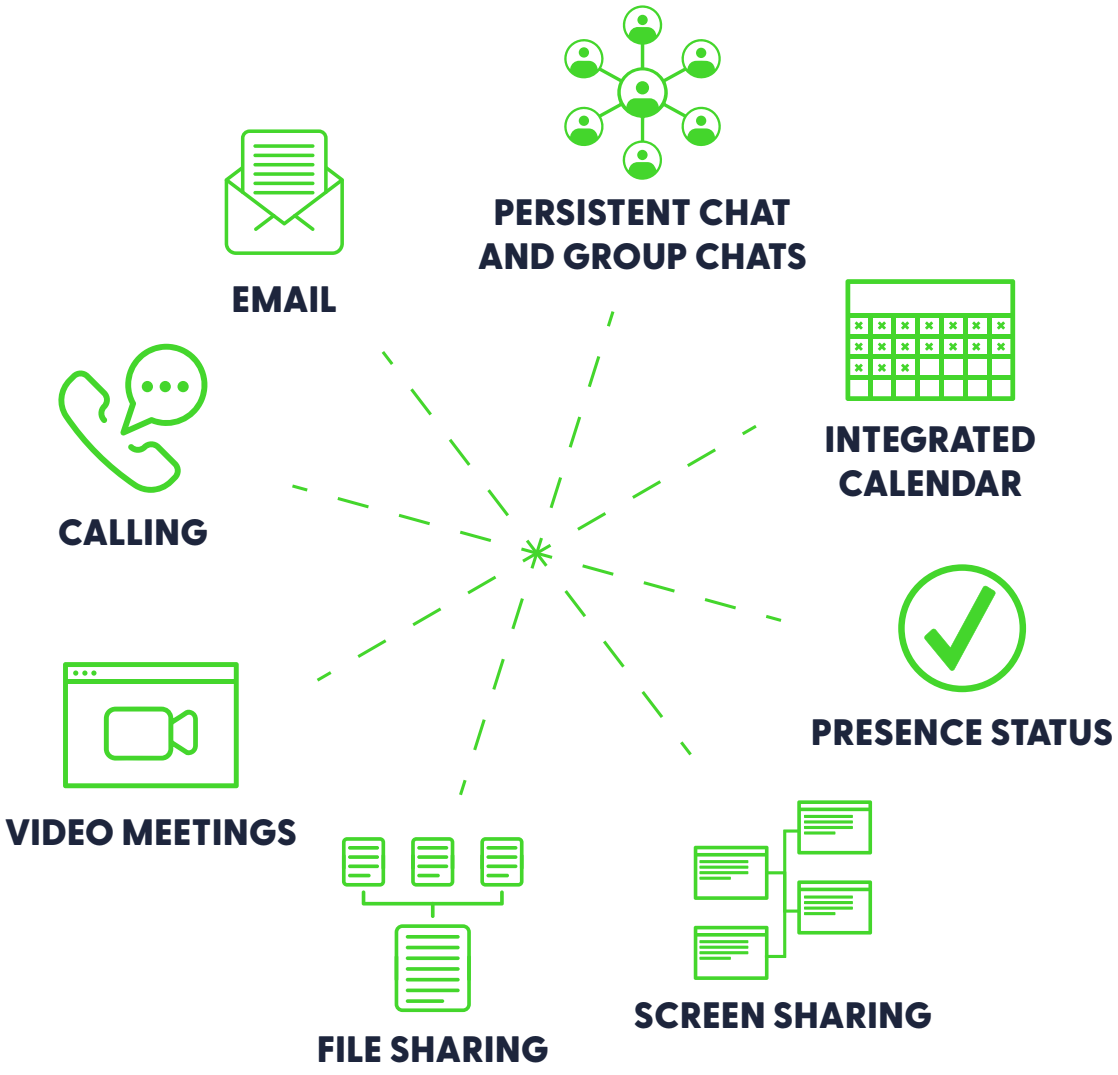
3 SUPPORT YOUR CLIENTS THROUGH THE TRANSITION.

- **Expect an influx of helpdesk tickets** as users adjust to new tools and security protocols – so ensure support continuity by following best practices when setting up remote work on your own team.
- **Stock up on spare laptops** to support the surge in clients' remote work hardware needs.

REMOTE PRODUCTIVITY & COLLABORATION

THE POWER OF UNIFIED COMMUNICATIONS

Unified communications as a service (UCaaS) solutions integrate communication and collaboration tools, such as email, VoIP calling, video conferencing, screen sharing, instant messaging, file sharing, and scheduling, into a single cloud interface. The goal of UCaaS is to make collaboration seamless, streamlining processes and unifying communications channels so that employees can work from anywhere without interrupting their workflow.



REMOTE PRODUCTIVITY & COLLABORATION

RECOMMENDED UCAAS SOLUTIONS

MICROSOFT TEAMS

Teams is the hub for collaboration within the Microsoft environment, bringing everything together in a shared workspace where users can chat, meet, create, and make decisions as a team. Paired with the cloud file storage capabilities of SharePoint/OneDrive, Teams creates a seamless experience for sharing and collaborating on documents.

BEST FIT:

- Internal collaboration needs
- Remote meetings with small groups of participants
- Clients already on M365, O365 E3, or O365 E5

In 2019, Microsoft Teams was used by 500,000 organizations, including 91 Fortune 100 companies.[10]

ZOOM

Zoom offers leading enterprise video communications, with a reliable cloud platform for video and audio conferencing, chat, and webinars.

BEST FIT:

- Internal collaboration needs
- Substantial need for external collaboration with partners, clients, and/or prospects
- Remote meetings with large groups of participants (up to 1,000 video participants and up to 10,00 viewers!)

EVOLVE IP

Evolve IP seamlessly integrates cloud collaboration services with enterprise-quality voice communications, including voice-enablement for Microsoft Teams with a native platform integration.

BEST FIT:

- Heavy-duty calling requirements (e.g. large sales teams, call centers, or support teams)
- Need for PBX replacement, fully integrated with Teams

REMOTE PRODUCTIVITY & COLLABORATION

BEST PRACTICES FOR WORKING FROM HOME

20% of remote workers say their biggest challenge is collaboration and communication, and 20% say it is loneliness.[8] By encouraging employees to follow these established best practices for remote work, you can foster a sense of teamwork and connection, while maintaining efficiency.

DEFINE YOUR HOME WORKSPACE

Establish a dedicated, quiet area of your home as your workspace. Doing so can help you define boundaries for when you're working and when you're off-duty at home, and it can help you get into the rhythm of work each day by stepping into your "office."

ESTABLISH ONLINE MEETING ETIQUETTE

For conference calls, encourage the use of muting when not speaking and be sure to announce yourself and speak clearly. Video meetings are the best way to connect and collaborate remotely but can offer distractions – try to keep your room well-lit and look at the camera while speaking. It can be tempting to multi-task during online meetings, but other participants can tell if you aren't focused – stay engaged and present!

LEARN TO USE IDENTITY & STATUS

To avoid distracting a busy colleague or wasting time by trying to reach someone who is unavailable, learn to check their presence status. Teams integrates with your calendar to automatically update your presence when "In a meeting", but you should make it a habit to change your status to "Be right back" or "Do not disturb" so your colleagues know you when you can't be reached. Setting status messages can provide even further context to your team.

COMMUNICATE!

Clearly communicate your availability schedule to your colleagues and use group chats to keep relevant team members up to date on project progress.

STANDARDIZE CLOUD FILE STORAGE

To keep remote collaboration efficient, establish guidelines for cloud file storage, including file structures and document naming conventions, so that colleagues can easily find and collaborate on documents.

DON'T LOSE THE SOCIAL ASPECT!

Without in-office meetings, drive-by desk conversations, and chats by the coffeemaker, you can quickly feel disconnected from your colleagues. Set aside time for video meetings just to chat and catch up as a team face-to-face. And keep things fun by using emojis and gifs in your chats and emails!

REMOTE SECURITY

SECURING MICROSOFT FOR REMOTE WORK

Microsoft cloud services see 300 million fraudulent sign-in attempts every day![9] To ensure that end users are as secure as possible when collaborating through Teams and SharePoint/OneDrive, deploy these Microsoft features and settings.

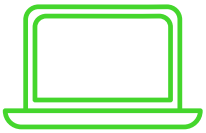
1. **Harden Teams:** Configure these recommended settings to secure Teams:
    - Ensure Advanced Thread Protection (ATP) for Teams is enabled to provide safe links and email security
    - Ensure external domains are not allowed in Teams, but only whitelist-approved organizations
    - Ensure Data Loss Prevention (DLP) policies are created for Teams
    - Ensure external file sharing in Teams is enabled only for approved cloud storage services
2. **Multi-factor authentication (MFA):** By requiring a second form of authentication, MFA is the best defense to strengthen access security. Make sure that MFA is required for all employees when off-network.
3. **Conditional access (CA):** Use conditional access to control who can access which apps and data, and from which networks and locations.
4. **Device management:** Restrict corporate network access to approved devices.
5. **Intune:** Set up Intune to provide the ability to remotely wipe or encrypt company data if a laptop or mobile device is lost or stolen.
6. **Azure AD Sync with on-prem:** If employees are remote without a VPN, no devices are checking in to an on-prem active directory. Use Azure AD sync for better control and visibility.
7. **SharePoint/OneDrive:** Enable data protection policies to ensure employees can safely and seamlessly collaborate on files.

Microsoft reports that 99% of account hacks are blocked using multi-factor authentication (MFA).[9]

NEED A BOOST TO ROLL OUT REMOTE WORK SOLUTIONS TO YOUR CLIENTS?

THERE'S A WINGMAN FOR THAT!

If you feel stretched thin by the influx of clients transitioning to remote work, take advantage of our cost-effective Pax8 Professional Services bundles for remote work! We'll augment your team to configure and drive adoption of Microsoft Teams and other technology solutions so that you can empower successful and secure remote work for all your clients.



TEAMS REMOTE WORKER STARTER BUNDLE
to set up and configure Microsoft Teams. Includes admin and end user training videos to help drive adoption.

M365 SECURE REMOTE WORKER BUNDLE
to set up Intune and Mobile Application Management to protect data within Teams, SharePoint, and OneDrive.

M365 HARDENING BUNDLE
to optimally configure Advanced Threat Protection (ATP) and Advanced Information Protection (AIP).

CUSTOM END USER TRAINING
to drive Teams adoption and/or offer guidance around remote security best practices.

GET STARTED

REMOTE SECURITY

SECURING MICROSOFT FOR REMOTE WORK

The following tools can provide additional layers of security for remote employees.

1. **Virtual private network (VPN):** A VPN provides an encrypted, private connection so employees can securely access company resources and applications from home or public networks.

2. **Windows Virtual Desktop (WVD):** WVD (which is included with M365) enables central management and security of users' desktops by creating Windows 10 virtual desktops in Azure, allowing end users to work remotely with a secure connection and securely store data in the cloud rather than on their local device. WVD separates the compute environment from user devices, greatly reducing the risk of confidential information being left on a personal device. Pax8 works with Nerdio and CloudJumper to help estimate costs, deploy, manage, and optimize a WVD deployment.

   nerdio Cloud Jumper

3. **Endpoint security:** As a last line of defense against incoming malware, deploy an endpoint security solution to actively discover and remediate threats across devices, desktops, and servers.

   Bitdefender WEBROOT SentinelOne

4. **DNS filtering:** Since users working remotely on company devices don't have the protection of the company firewall, use DNS filtering to protect them from malicious websites and prevent them from visiting inappropriate websites on company devices.

   TitanHQ WEBROOT Bitdefender

5. **Phishing prevention:** Email is the top delivery mechanism for 96% of phishing attacks, so protect users with real-time anti-phishing email security.

   IRONSCALES

6. **End user security training:** Make sure users are trained to spot phishing attempts and are able to recognize and report other common cyber threats.

   IRONSCALES Breach BSN Secure Now!

ADVANCING THE CONVERSATION

REMOTE SECURITY CHECKLIST

In the rush to roll out remote work capabilities, many businesses have left security considerations behind. But with remote users "in the wild" and unprotected by the company firewall, security is more critical than ever. This checklist can help you guide the conversation to make your clients aware of their security needs while transitioning to remote work.

- [ ] Is multi-factor authentication (MFA) enabled? Did employees receive guidance on how to use MFA (and authenticator apps, if applicable)?
- [ ] Is conditional access enabled and configured?
- [ ] Do you have the ability to remotely wipe company data from lost or stolen laptops and mobile devices? Are you using whole disk encryption to encrypt the physical hard drive of company laptops?
- [ ] Do you have an email security product in place? Were employees trained to recognize and report phishing attempts?
- [ ] Have you installed a web security app to prevent users from visiting malicious sites?
- [ ] Have you set up data loss prevention policies and/or set applicable restrictions on external file sharing?
- [ ] Have you created a remote work and data protection policy for employees to sign?
- [ ] Have you conducted end user training on remote security policies and best practices?
- [ ] Do you have endpoint protection installed for all remote machines?
- [ ] If you are subject to compliance regulations, do you have policies and procedures in place to ensure compliance? Are employees trained to enforce those policies?
- [ ] What is your incident response plan during times of company-wide remote work?

ADVANCING THE CONVERSATION

MICROSOFT TEAMS EMAIL TEMPLATE FOR CLIENTS WITH M365, O365 E3, OR O365 E5

Do you have clients who are on M365, O365 E3, or O365 E5, but are not utilizing their included access to Teams and SharePoint/OneDrive? This email template can help you start a discussion around optimizing their remote work experience with the Microsoft suite of tools.

New Email

To: Customer

Subject: Working remote? You already have the tools you need

Dear [Client Contact First Name],

If you're looking for ways to improve remote work so that your business can stay productive during the challenges of the COVID-19 pandemic, I wanted to make sure you knew that since [Client Company Name] is already using [SELECT: M365, O365 E3, or O365 E5], you have built-in access to the Microsoft suite of tools – including Teams and SharePoint/OneDrive.

Together, Teams + SharePoint/OneDrive create a collaboration hub for Microsoft, integrating email, chat, meetings, calls, file sharing, screen sharing, and scheduling. There's no need to pay for another productivity app!

I'd like to set up a call to discuss configuring Teams and SharePoint/OneDrive to create a better remote collaboration experience for your employee – and steps to protect your company data as employees remotely access and share files. What's your availability this week?

Thanks,
[Partner Name]

Send

ADVANCING THE CONVERSATION

EMAIL TEMPLATE FOR NON-MICROSOFT CLIENTS

You may have other clients who are using cloud apps and services, such as G-Suite or Slack, to enable remote work. This email template can help you start a discussion around securing their remote work experience by moving to M365.

New Email

To: Customer

Subject: Staying secure during remote work?

Dear [Client Contact First Name],

If [Client Company Name] has enabled remote work to stay productive during the challenges of the COVID-19 pandemic, I wanted to check in to see if you've taken measures to secure employees and protect your company data.

Turning on multi-factor authentication (MFA) for company apps is my #1 security recommendation for remote work – Microsoft reports that 99% of account hacks are blocked using MFA.

My team is standing by to assist with your remote work initiatives in any way we can. If you'd like to have a call to discuss tools to improve your remote security posture and/or discuss how moving to M365 can create a better (and more secure) remote collaboration experience for your employees, I'm happy to talk it over. What's your availability this week?

Thanks,
[Partner Name]

Send

GET A WINGMAN

Just as your clients need you to be their Wingman to help them successfully adapt to remote work, know that you're not alone in this either! Rest assured, as a born-in-the-cloud company, the Pax8 team is fully remote-enabled and standing by to assist you with product guidance and technical support.

And, if your team is running low on resources and you need a boost to enable and secure your clients' Microsoft Teams environments, our **Professional Services team** is available to serve as an extension of your team.

Want to learn more about Microsoft Teams, Zoom, or EvolveIP to improve remote collaboration? Have a question about security solutions for remote work?

YOUR CLOUD WINGMAN IS HERE TO HELP.

SCHEDULE A CALL

OTHER RESOURCES

WATCH:
On-Demand Webinar– How to Optimize Your Clients' Remote Workforce

LEARN:
Resource Hub – How to Empower a Productive and Secure Remote Workforce

DOWNLOAD:
Guide – MSP's Guide to Selling M365

MICROSOFT TEAMS RESOURCES

TEAMS QUICK START GUIDE

TEAMS WALKTHROUGH VIDEOS

TEAMS END USER TRAINING

GUIDE TO INSTALLING AND USING THE MOBILE TEAMS APP

TIPS FOR WORKING FROM HOME AND RUNNING ONLINE MEETINGS

HOW TO TURN TEAMS ON

REMOTE WORKFORCE FAQ

REMOTE WORK CHECKLIST

SOURCES

1. CNBC, Microsoft says Teams communication app has reached 44 million daily users, March 2020
2. CoSo, CoSo Cloud Survey Shows Working Remotely Benefits Employers and Employees, February 2015
3. Atlassian, The me in team: Drawing on the strengths of the individual to unleash the power of teams
4. Buffer, 2019: The State of Remote Work, 2019
5. GetApp, GetApp Unveils Results of Workforce Trends Study, Uncovering Shifts in Remote Work, Privacy and AI SMB Perceptions, January 2020
6. Heimdal Security, What Are The Cybersecurity Issues With Remote Work, October 2019
7. OpenVPN, Remote Work Is the Future – But Is Your Organization Ready for It?, 2019
8. Buffer, The 2020 State of Remote Work, 2020
9. ZDNet, Microsoft: Using multi-factor authentication blocks 99.9% of account hacks, 2019
10. Microsoft, Microsoft Teams wins Enterprise Connect Best in Show award and delivers new experiences for the intelligent workplace , March 2019