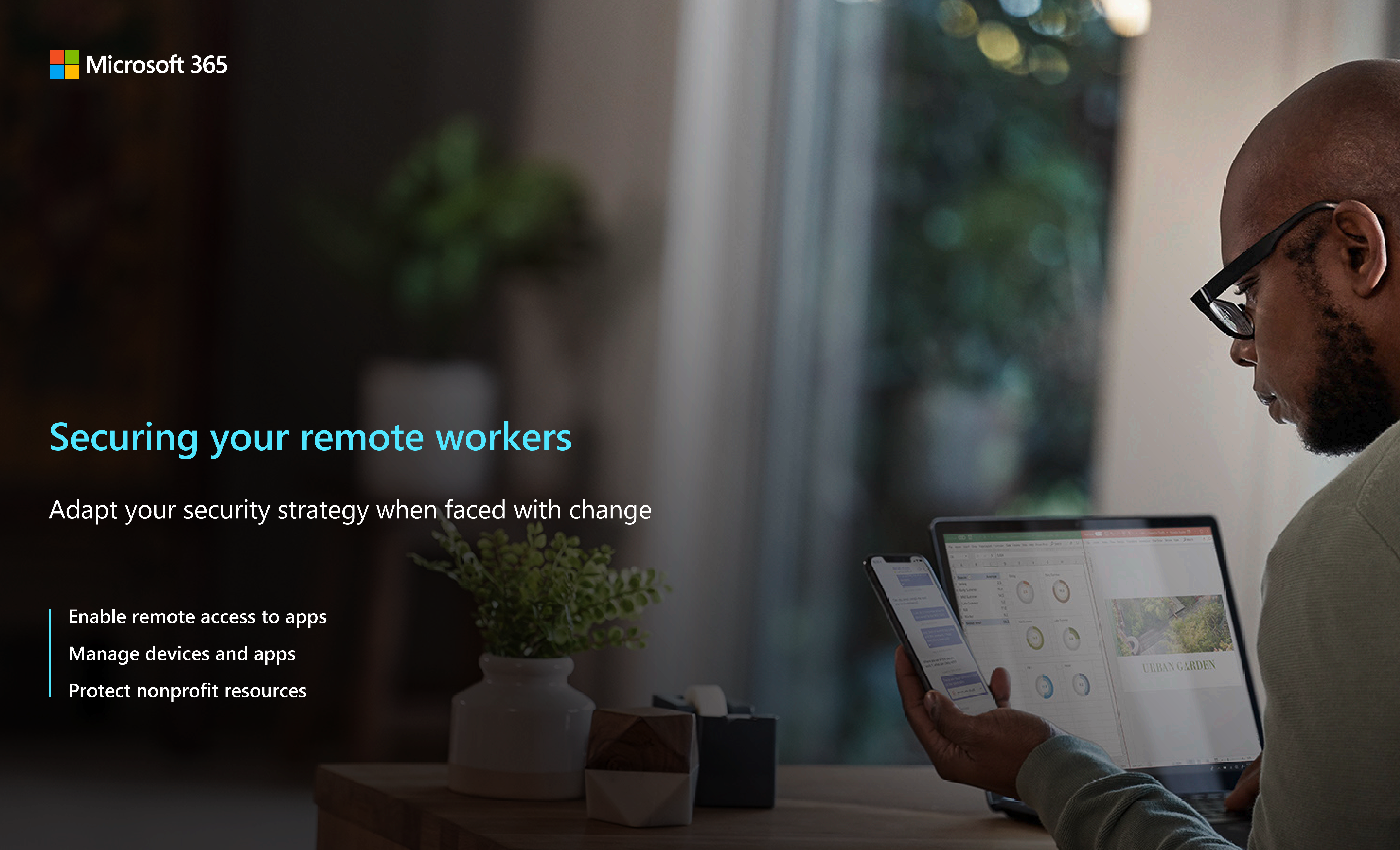
Microsoft 365



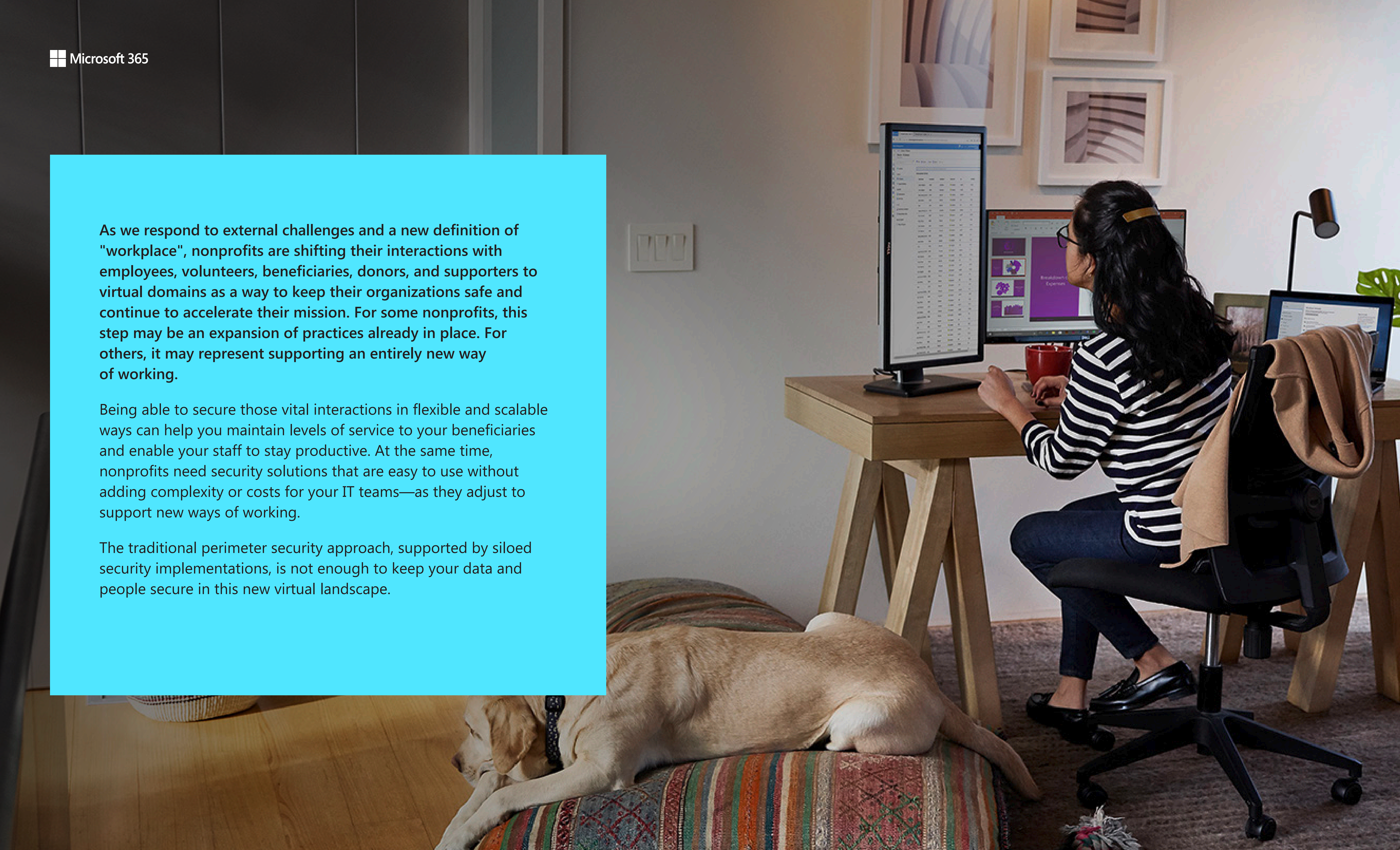
Securing your remote workers

Adapt your security strategy when faced with change

Enable remote access to apps

Manage devices and apps

Protect nonprofit resources



As we respond to external challenges and a new definition of "workplace", nonprofits are shifting their interactions with employees, volunteers, beneficiaries, donors, and supporters to virtual domains as a way to keep their organizations safe and continue to accelerate their mission. For some nonprofits, this step may be an expansion of practices already in place. For others, it may represent supporting an entirely new way of working.

Being able to secure those vital interactions in flexible and scalable ways can help you maintain levels of service to your beneficiaries and enable your staff to stay productive. At the same time, nonprofits need security solutions that are easy to use without adding complexity or costs for your IT teams—as they adjust to support new ways of working.

The traditional perimeter security approach, supported by siloed security implementations, is not enough to keep your data and people secure in this new virtual landscape.

This guide aims to show you how you can use your existing investments in Microsoft 365 to quickly shift your people to remote work while turning on built-in security controls to help them stay secure. Refer to the list on the right to identify areas where you need help, and use the links to jump directly to that information.

Remote access challenges

□ Keeping up with the sheer volume of remote workers who need access to apps and info.

□ Our remote workers are scattered across the globe.

□ We need to provide access to volunteers and third parties to get the work done.

□ We have mixed apps that include on-prem and cloud resources to which it is currently difficult for us to provide consistent access.

□ We are worried about VPN scalability.

Start with:

→ Enable remote access to apps

Microsoft can help you quickly provide secure and scalable access to your apps, whether the platforms are on-prem or in the cloud.

Device management challenges

□ All of our workers are remote, which makes managing their devices a challenge.

□ We expect that some people will be using their own devices to get work done.

□ We need to get new devices quickly provisioned and shipped to our remote workers.

□ We're struggling with managing the device lifecycle remotely.

Start with:

→ Manage devices and apps

Microsoft can help you simplify the management of your remote devices, and protect the apps and organizational data that lives in them.

Protection challenges

□ We are worried about our data now that everyone is working remotely.

□ New cybersecurity threats are rapidly increasing due to the remote work situation–especially phishing.

□ Risk of confidential information getting leaked out of the company.

□ We don't have a handle on all of the cloud resource usage–and the potential security risks.

Start with:

→ Protect nonprofit resources

Microsoft can help you get a handle on protecting your apps and data as work gets done remotely while easing the burden of stopping new attacks.

Microsoft 365

Enable remote access to apps

To successfully connect all your remote workers, you will need secure access across a few different levels of resources. For example, enabling access to cloud applications and resources for people outside your organization's network (and potentially using their own devices). Or providing your remote employees and volunteers with secure access to critical on-premises applications. You may also need to enable continued collaboration with supporters and board members to further your mission.

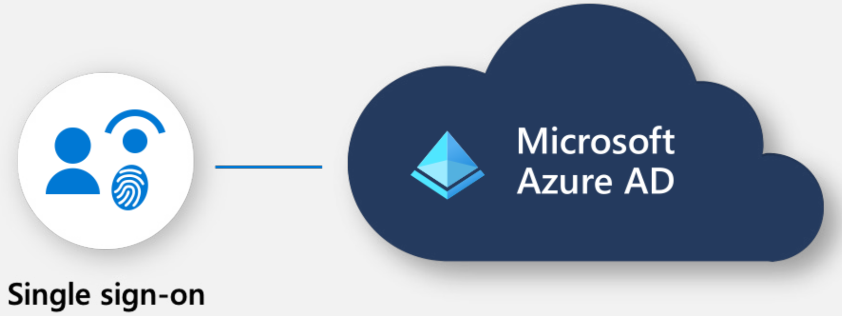
Let's take a look at what's possible.

Secure access to your apps from anywhere

Managing secure access, whether to the cloud, or anywhere else, starts with enforcing secure identities for your people. A control plane for managing all your user identities, Microsoft Azure Active Directory (AD) offers you a comprehensive identity and access management platform and is part of your Microsoft 365 subscription. If you are not already using it, this is a great opportunity to start.

Azure AD provides access control by enabling single sign-on to all your apps. With single sign-on, your users only need to log in once to gain access to all their critical productivity resources without needing to remember separate passwords for each application account.

[Enable single sign-on with Azure Active Directory]



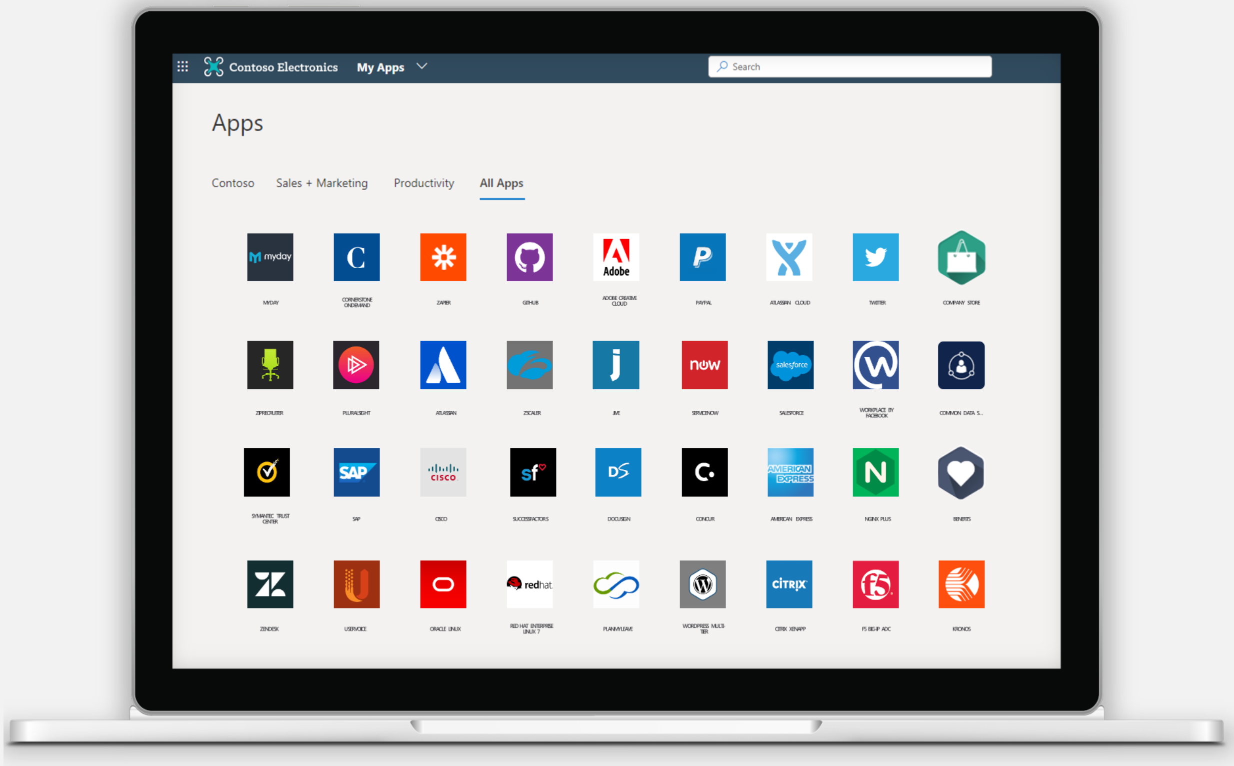
Simplify end user app discovery

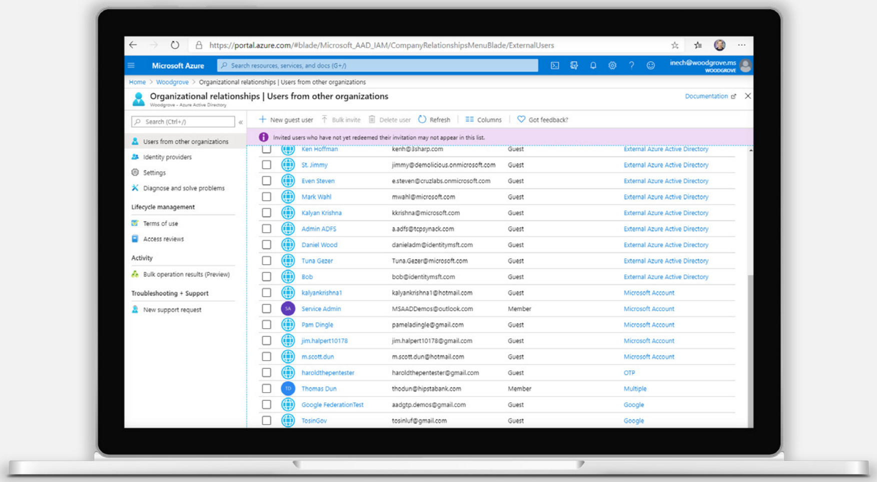
Azure Active Directory has an app gallery of thousands of pre-integrated third-party SaaS apps to simplify single sign-on for your users. From Salesforce, to Workday, Marketo, Adobe, and others, you can use Azure AD to provide a centralized point of protection for your people.

If you are already using Microsoft 365 and Office portal, all applications connected to Azure AD will show up in the Office portal. If you are not using the online Office portal, you can get the same great experience in Azure AD My Apps portal. The My Apps portal makes it easy to deploy new apps across your entire organization or to specific groups, such as new hires or volunteers who need to be productive right away.

In addition, if you're using Microsoft Endpoint Manager, Microsoft Company Portal provides a one-stop location for users to find and provision any installed apps or web/cloud front ends. What's more, deploying apps using Microsoft Endpoint Manager via Company Portal enables you to apply security and data protection policies to MDM-enrolled devices and SDK-enabled apps in MAM-only scenarios.

[Help your people find their apps from a single location]




https://portal.azure.com/#blade/Microsoft_AAD_IAM/CompanyRelationshipsMenuBlade/ExternalUsers
Microsoft Azure
Search resources, services, and docs (G+/)
inech@woodgrove.ms
WOODGROVE
Home > Woodgrove > Organizational relationships | Users from other organizations
Documentation
Search (Ctrl+/)
Users from other organizations
Identity providers
Settings
Diagnose and solve problems
Lifecycle management
Terms of use
Access reviews
Activity
Bulk operation results (Preview)
Troubleshooting + Support
New support request
New guest user
Bulk invite
Delete user
Refresh
Columns
Got feedback?

Organizational relationships | Users from other organizations

Woodgrove - Azure Active Directory

Invited users who have not yet redeemed their invitation may not appear in this list.

Ken Hoffman	kenh@3sharp.com	Guest	External Azure Active Directory
St. Jimmy	jimmy@demolicious.onmicrosoft.com	Guest	External Azure Active Directory
Even Steven	e.steven@cruzlabs.onmicrosoft.com	Guest	External Azure Active Directory
Mark Wahl	mwahl@microsoft.com	Guest	External Azure Active Directory
Kalyan Krishna	kkrishna@microsoft.com	Guest	External Azure Active Directory
Admin ADFS	a.adfs@tcpsynack.com	Guest	External Azure Active Directory
Daniel Wood	danieladm@identitymsft.com	Guest	External Azure Active Directory
Tuna Gezer	Tuna.Gezer@microsoft.com	Guest	External Azure Active Directory
Bob	bob@identitymsft.com	Guest	External Azure Active Directory
kalyankrishna1	kalyankrishna1@hotmail.com	Guest	Microsoft Account
Service Admin	MSAADDemos@outlook.com	Member	Microsoft Account
Pam Dingle	pameladingle@gmail.com	Guest	Microsoft Account
jim.halpert10178	jim.halpert10178@gmail.com	Guest	Microsoft Account
m.scott.dun	m.scott.dun@hotmail.com	Guest	Microsoft Account
haroldthepentester	haroldthepentester@gmail.com	Guest	OTP
Thomas Dun	thodun@hipstabank.com	Member	Multiple
Google FederationTest	aadgtp.demos@gmail.com	Guest	Google
TosinGov	tosinluf@gmail.com	Guest	Google

Securely collaborate with external partners, for any app

You can also use Azure AD to simplify collaboration with external parties, such as board members, subject matter experts, donors, and others that need access to specific apps as part of the day-to-day rhythm of the organization.

With Azure AD, you can

- Enable employees to invite their external parties to access internal resources.
- Allow nonprofit partners to request access.
- Connect external partners to your SharePoint Online and Office 365 applications, in addition to other SaaS apps, or custom, on-prem Line-of-Business (LOB) applications.

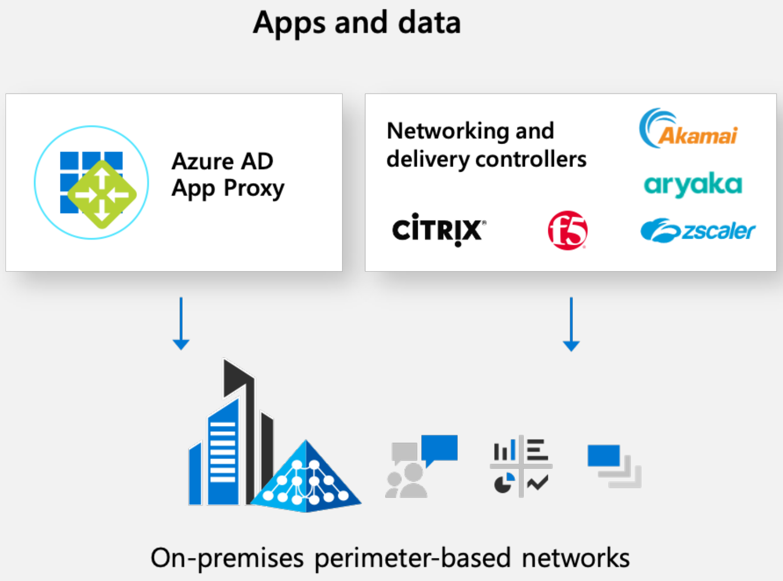
Enable external access in Azure AD

Secure access to critical on-premises apps for remote users

Many nonprofits also manage legacy on-premises applications (apps that are not perhaps practical to modernize). To make it easier to connect any application to Azure AD, you can use solutions like Azure AD App Proxy and integrations with networking security companies–Akamai, Arayaka, Citrix, F5, and Zscaler.

Azure AD App Proxy is a feature of Azure AD that supports single sign-on and enables users to access on-premises web applications from a remote client, removing the need for a VPN or a reverse proxy.

Enable Azure AD App Proxy


Apps and data

Azure AD App Proxy

Networking and delivery controllers

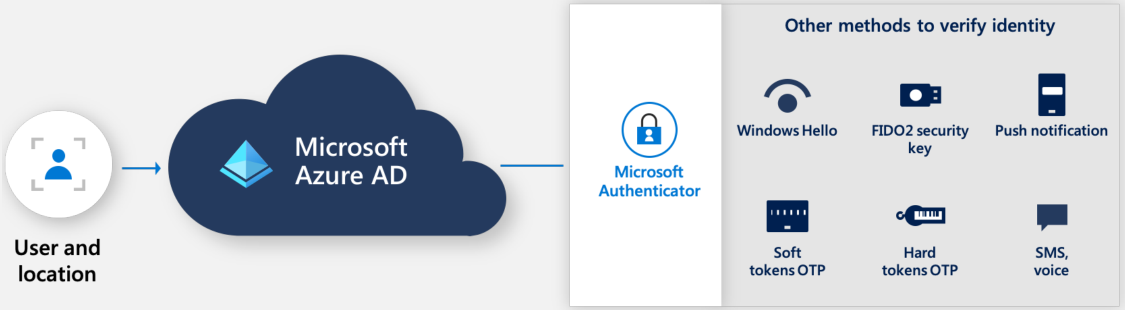
On-premises perimeter-based networks

Enable strong authentication

To keep your people secure while working remotely, you'll also want to ensure your end-user authentication is secure. Passwords are the weakest link in the security chain and are also, without any additional verification, a single point of failure. Multi-factor authentication (MFA), however, can reduce the risk of being breached by 99.9%. If there's only one thing you do to help protect your people, turn on MFA for your organization.

You can further fortify security by using Azure AD Conditional Access to deploy fine-tuned adaptive access policies based on user context, device, location, and session risk information. With Conditional Access, you can define the specific conditions for how users authenticate and gain access to your apps and data.

Enable MFA



Actions you can take today to get started

- Connect your on-premises infrastructure to the cloud.
- Connect all apps to Azure AD to enable single sign-on.
- Turn on MFA with Conditional Access.

For a more detailed walkthrough to get started in providing secure remote access to your applications, visit the Application management with Azure AD guide on Microsoft Docs.

Microsoft 365

Manage devices and apps

Managing devices and apps is a critical aspect of securing your remote workforce. Yet the rapid transition to remote work during this crisis has given organizations little time to find the best approach for managing all the devices that are remotely accessing apps and data.

Many nonprofit workers may be using a mix of organization-issued and personal devices. At the same time, your IT team may be struggling to provision and deploy new devices remotely. You need a way to securely manage apps, multiple types of devices, and virtual desktop experiences across the entire lifecycle.

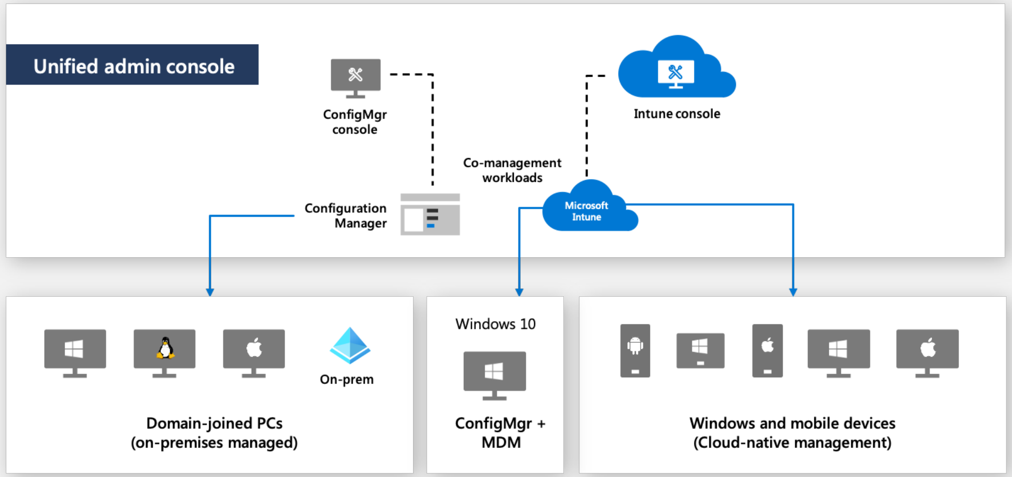
Deploy and manage devices and virtual desktops

One of the biggest challenges in managing a heterogeneous mix of devices is the different “panes of glass” that are required. Microsoft Endpoint Manager brings together all your endpoints and apps under a single pane of glass and combines the on-premises capabilities of Microsoft Configuration Manager and the cloud-native benefits of Microsoft Intune into the Microsoft 365 Admin Center.

With Microsoft Endpoint Manager, you can deploy and manage all your apps and endpoints, extend on-premises infrastructure with cloud security, and securely enable BYO to access resources. As well, you’ll be able to automate deployment for any device directly from the manufacturer to the user and automate the provisioning of user settings, configurations, and apps.

[Get started with Microsoft Endpoint Manager]()

Microsoft Endpoint Manager



Beyond devices, organizations may opt to provide access via virtual desktops. Azure Windows Virtual Desktop provides virtualization infrastructure as a managed service, enabling you to deploy and manage VMs in your Azure subscription, and manage experiences using tools like ConfigMgr or Intune.

Learn more about Windows Virtual Desktop

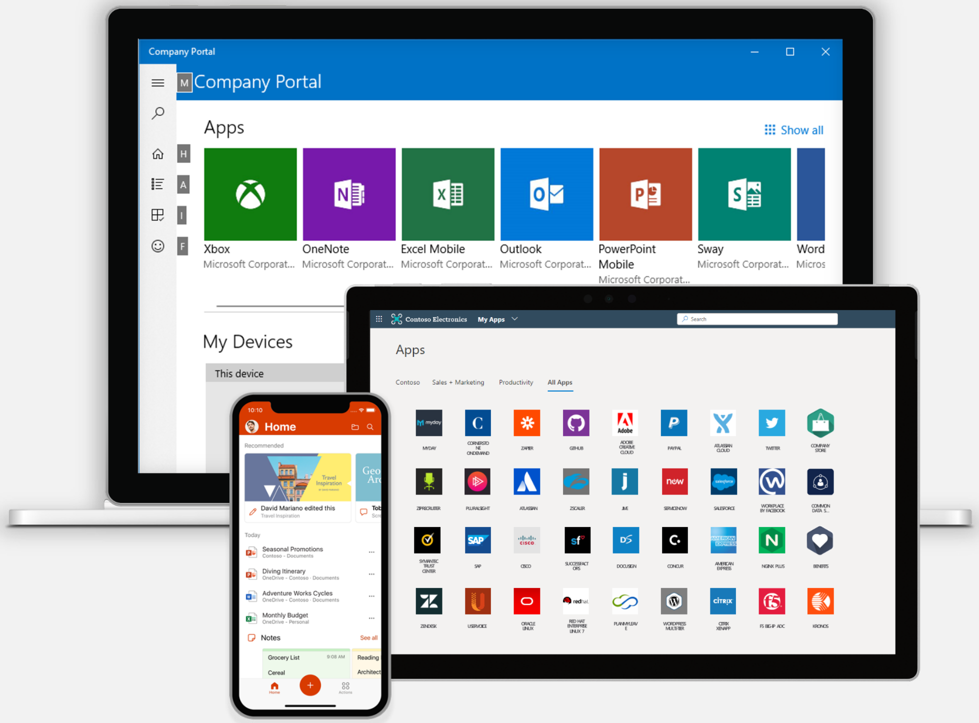
You can also offer a centralized place for your users to find and access their work apps by using My Apps, Company Portal, or the Office 365 portal.

Learn more about Intune app management

Deploy and manage apps on any device

Some organizations want more control of managing devices and the apps that live on them. Others may have BYO policies in place. Microsoft provides two approaches to protect the apps and data that live on mobile devices.

- **Mobile Device Management** (MDM) provides you with the ability to manage at the device level. With MDM, you can use conditional access to restrict access to and from the managed device.
- **Mobile Application Management** (MAM) is ideal for BYO scenarios. You manage at the application layer, without having to enroll the device in MDM. For example, using MAM, you provide secure access to Office apps and their associated data on personal devices. That data is protected and you can remove it from the device without affecting any personal data or apps. You can apply information protection policies to control how the data is accessed and used.



Proactively manage updates, patching, and policies

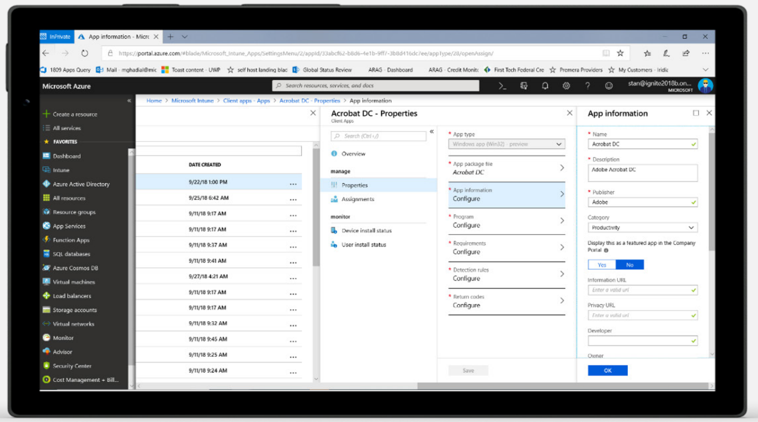
As entire nonprofit organizations work remotely, it can be challenging to remotely manage the device and app lifecycle—to make sure that all devices and apps are up to date with required updates, patches, and policies.

You can configure co-management in Endpoint Configuration Manager and Intune for a more flexible and centralized experience managing remote devices and apps.

For example, you'll be able to:

- Manage OS updates on Windows PCs and macOS and set up update policies for supervised mode iOS and iPad devices.
- For Windows 10 PCs, you have the options to configure immediate, automated, or prompted updates.
- For iOS and iPadOS devices, you can update apps and set software update policies for supervised mode.

Learn more about how co-management works



DATE CREATED
9/22/18 1:00 PM
9/25/18 6:42 AM
9/11/18 9:17 AM
9/11/18 9:17 AM
9/11/18 9:37 AM
9/11/18 9:41 AM
9/27/18 4:21 AM
9/11/18 9:17 AM
9/11/18 9:17 AM
9/11/18 9:32 AM
9/11/18 9:45 AM
9/11/18 9:25 AM
9/11/18 9:24 AM

* App type: Windows app (Win32) - preview

* App package file: Acrobat DC

* App information: Configure

* Program: Configure

* Requirements: Configure

* Detection rules: Configure

* Return codes: Configure

* Name: Acrobat DC

* Description: Adobe Acrobat DC

* Publisher: Adobe

Category: Productivity

Display this as a featured app in the Company Portal: Yes ● No

Information URL: Enter a valid url

Privacy URL: Enter a valid url

Developer:

Owner

Actions you can take today to get started

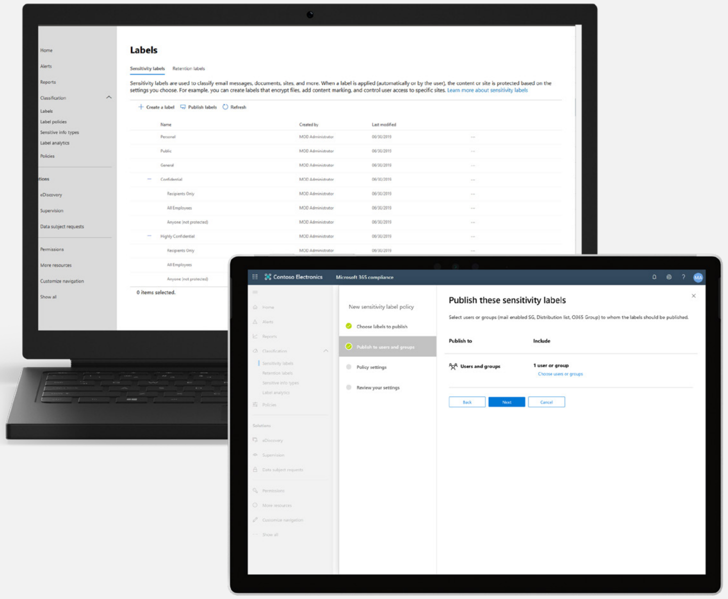
- Remotely provision and deploy new devices.
- Enforce access policies on unmanaged devices with Intune.
- Deploy and manage virtual desktops.

Microsoft 365

Protect nonprofit resources

With nearly everyone working remotely now, the surface area for protecting your organization's resources just got more complicated. Unfortunately, we also know that bad actors are going to take advantage of the situation. Protecting your data, apps, and endpoints against threats and security risks is paramount.

Let’s explore a few areas where you can keep your people productive while ensuring your apps and endpoints are safe.



Labels

Sensitivity labels | Retention labels

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. Learn more about sensitivity labels

Name	Created by	Last modified
Personal	MOD Administrator	06/30/2019
Public	MOD Administrator	06/30/2019
General	MOD Administrator	06/30/2019
Confidential	MOD Administrator	06/30/2019
Recipients Only	MOD Administrator	06/30/2019
All Employees	MOD Administrator	06/30/2019
Anyone (not protected)	MOD Administrator	06/30/2019
Highly Confidential	MOD Administrator	06/30/2019
Recipients Only	MOD Administrator	06/30/2019
All Employees		
Anyone (not protected)		

0 items selected.

New sensitivity label policy

- Choose labels to publish
- Publish to users and groups
- Policy settings
- Review your settings

Publish these sensitivity labels

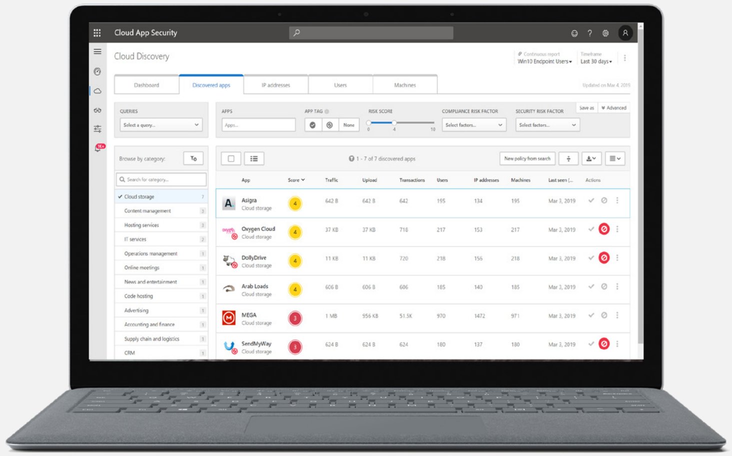
Select users or groups (mail enabled SG, Distribution list, O365 Group) to whom the labels should be published.

Publish to	Include
Users and groups	1 user or group Choose users or groups

Protect data while your remote workers collaborate

Due to stay-at-home mandates, nonprofit employees and volunteers have now shifted much of their collaboration to working through digital tools like Microsoft Teams. This transition has helped people stay productive while providing information protection, as much of the communication and content being shared is contained within the Teams collaboration environment. At the same time, you need to ensure that the communication happening inside Teams, Office products, and other third-party productivity tools complies with any industry regulations that are relevant to you.

With Microsoft Information Protection, you can protect your sensitive data wherever it lives and travels. One example is Data Loss Prevention (DLP) for Teams that automatically blocks messages that contain sensitive information. Microsoft Information Protection provides over 90 out-of-the-box sensitive-information definitions that you can use to detect common data types like credit card numbers.



Secure data in cloud applications and resources

Most organizations rely on cloud-based apps, whether SaaS apps or apps hosted in the cloud. Now, with the quick shift to remote work, people in your organization may be looking for new tools and apps to fill in the gaps they face to get things done working remotely. Having a handle on which cloud applications and resources are being used and how they're being used is critical to protecting yourself against risks.

With Microsoft Cloud App Security, you can discover and control access to your cloud applications and resources. It allows you to monitor and control web sessions in real time from threats such as the download of sensitive files from an unmanaged device. You also have visibility and control over the usage of cloud apps. You may discover that an app is being used that does not comply with your organization's policies and block that specific app.

Protect against phishing and malware attacks

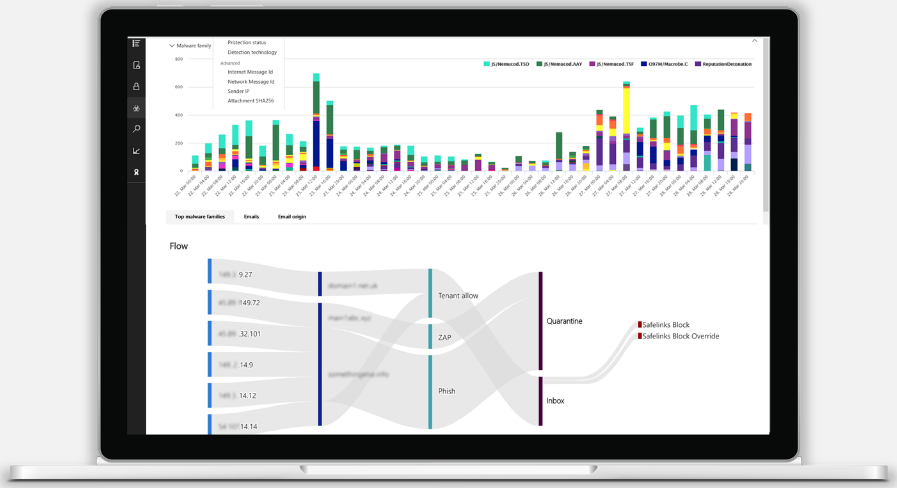
Before the pandemic, email phishing and malware attacks were at the top of the list of cybersecurity threats. Now, attackers are capitalizing on fear, leveraging this time of uncertainty and change as an opportunity. Phishing and malware attacks are on the rise, many of which now include COVID-19-related lures. In the circumstances we are living through, these threats continue to be some of the most considerable risks to organizations.

With Microsoft Office 365 Advanced Threat Protection (ATP), you can protect your organization from these threats while helping your security teams be more productive through the automation and AI capabilities inherent in Office 365 ATP.

Here are a few recommendations on how to protect against phishing and malware attacks:

1. **Enable "Safe Links and Attachments,"** which provides time-of-click protection of URLs. Safe Attachments provides detonation of attachments.
2. **Use the "Recommended Configuration Analyzer."** Approximately 20% of all phishing delivered to users' mailboxes is a result of misconfigurations. This tool reviews configurations to ensure your policies are up to date.
3. **Visualize the threats to your organization.** With Office 365 ATP, you can visualize and understand attacks and how they are were prevented.

[Learn more how you can protect your organization against phishing and malware attacks]



Protect your endpoints

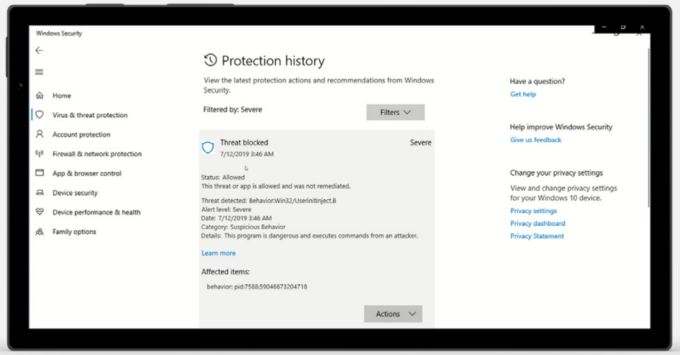
With most work happening remotely, ensuring that all of your workers' endpoints are protected has become more complex than it was before. At the same time, the threat landscape continues to evolve.

With Microsoft, you benefit from our industry-leading threat and malware capabilities built into Windows. These capabilities provide behavioral-based, real-time protection which blocks file-based and fileless malware, and stops malicious activity from attacking trusted and untrusted applications. Microsoft Defender Advanced Threat Protection (ATP), our unified endpoint security solution, provides an integrated suite of pre- and post-breach capabilities that help security teams to scale and operate efficiently in the current circumstances.

A few highlights include

- **Threat and Vulnerability Management** to discover, prioritize, and remediate endpoint vulnerabilities.
- **Attack Surface Reduction** to harden your systems and to regulate access to potentially malicious IPs, domains, and URLs.
- **Auto Investigation and Remediation** to reduce alert threat fatigue and to respond to threats quickly.

Learn more about securing your remote workforce with Microsoft Defender ATP



Protection history

View the latest protection actions and recommendations from Windows Security.

Filtered by: Severe

Threat blocked Severe
7/12/2019 3:46 AM

Status: Allowed
This threat or app is allowed and was not remediated.

Threat detected: Behavior:Win32/UserinitInject.B
Alert level: Severe
Date: 7/12/2019 3:46 AM
Category: Suspicious Behavior
Details: This program is dangerous and executes commands from an attacker.

Affected items:
behavior: pid:7588:59046673204718

Have a question?

Help improve Windows Security

Change your privacy settings

View and change privacy settings for your Windows 10 device.

Actions you can take today to get started

- Turn on Microsoft Teams Data Loss Prevention policies.
- Protect web sessions with Microsoft Cloud App Security.
- Enable Safe Links and Safe Attachments.
- Take advantage of built-in endpoint security.

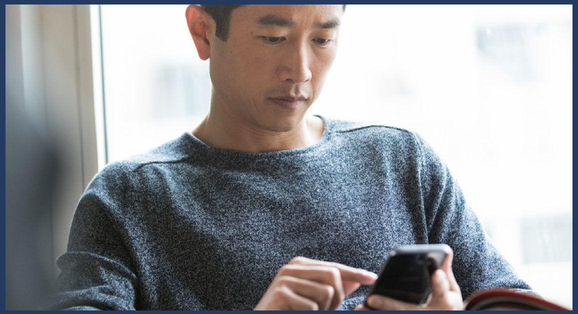
Get started enabling a more secure remote work experience

We know that every organization has different needs and is in a different place when it comes to securing its remote workers. The guidance in this ebook represents some of the top recommended actions you can take that will yield significant security benefits for your organization. We've summarized the top steps for each priority area that you can get started on today.

Enable secure remote access

Top actions

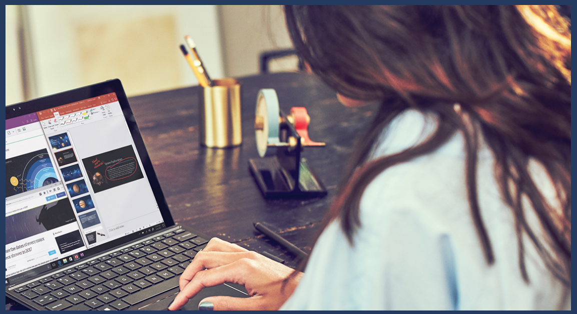
1. Connect your on-premises infrastructure to the cloud.
2. Connect all apps to Azure AD to enable single sign-on.
3. Turn on MFA with Conditional Access.



Manage devices and apps

Top actions

1. Remotely provision and deploy new devices.
2. Enforce access policies on unmanaged devices with Intune.
3. Deploy and manage virtual desktops.

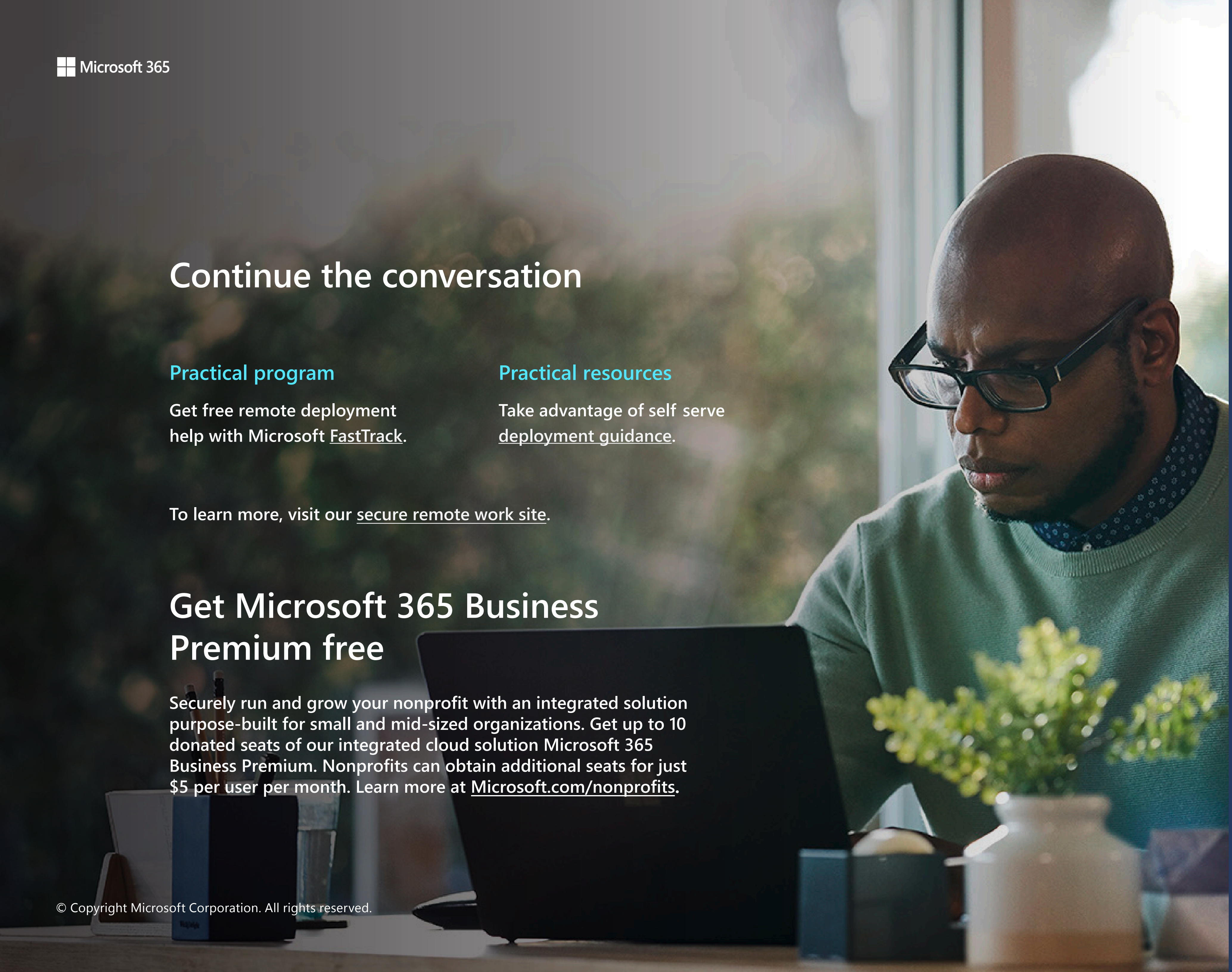


Protect nonprofit resources

Top actions

1. Turn on Microsoft Teams Data Loss Prevention policies.
2. Protect web sessions with Microsoft Cloud App Security.
3. Enable Safe Links and Safe Attachments.
4. Take advantage of built in endpoint security.

Microsoft 365



Continue the conversation

Practical program

Get free remote deployment help with Microsoft FastTrack.

Practical resources

Take advantage of self serve deployment guidance.

To learn more, visit our secure remote work site.

Get Microsoft 365 Business Premium free

Securely run and grow your nonprofit with an integrated solution purpose-built for small and mid-sized organizations. Get up to 10 donated seats of our integrated cloud solution Microsoft 365 Business Premium. Nonprofits can obtain additional seats for just $5 per user per month. Learn more at Microsoft.com/nonprofits.

Contact us

Contact us to learn about nonprofit offers for your organization

Visit Microsoft.com/nonprofits

Submit an inquiry at
aka.ms/nonprofits.contact

Find a partner at
aka.ms/nonprofits.partners

Follow us
@msftnonprofits
facebook.com/msftnonprofits