Microsoft Security

Microsoft best practices for securing your remote workforce

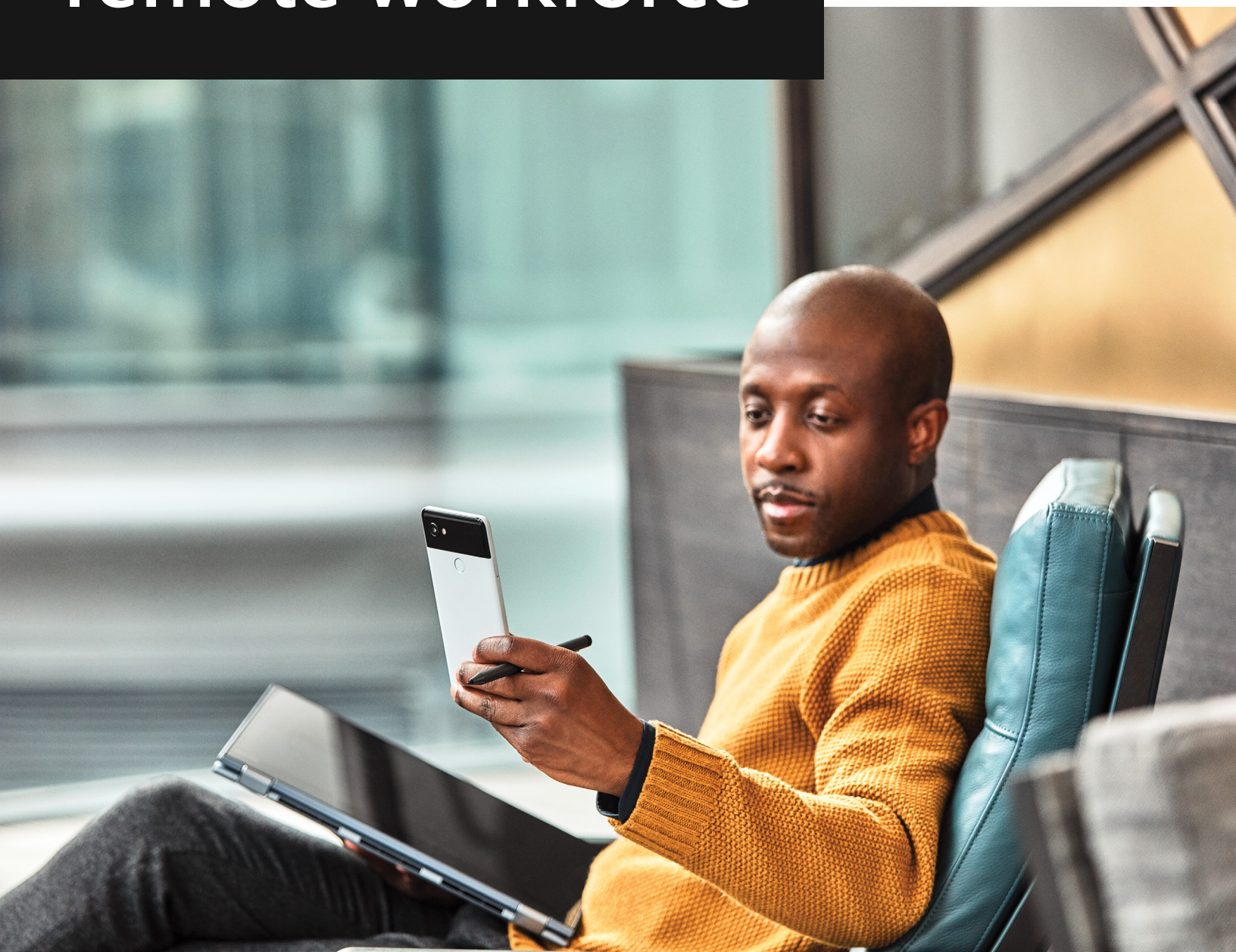


Table of Contents

Transitioning to remote work securely

With the spread of COVID-19 throughout the world, millions of people have moved to remote work, including tens of thousands of Microsoft employees. Our journey to the cloud has changed how we manage identity and network access for all users; helped ensure devices used to access the network are secure and healthy; and created a better end-user experience to access critical productivity apps. This transformation, led by Core Services Engineering and Operations (CSEO), our internal IT team, has helped Microsoft rapidly enable remote work for our vast workforce, while continuing to secure our customers, data, and applications.

Enabling a team to work remotely is an ongoing challenge that looks different for every organization, depending on their size, industry, and stage of digital transformation.

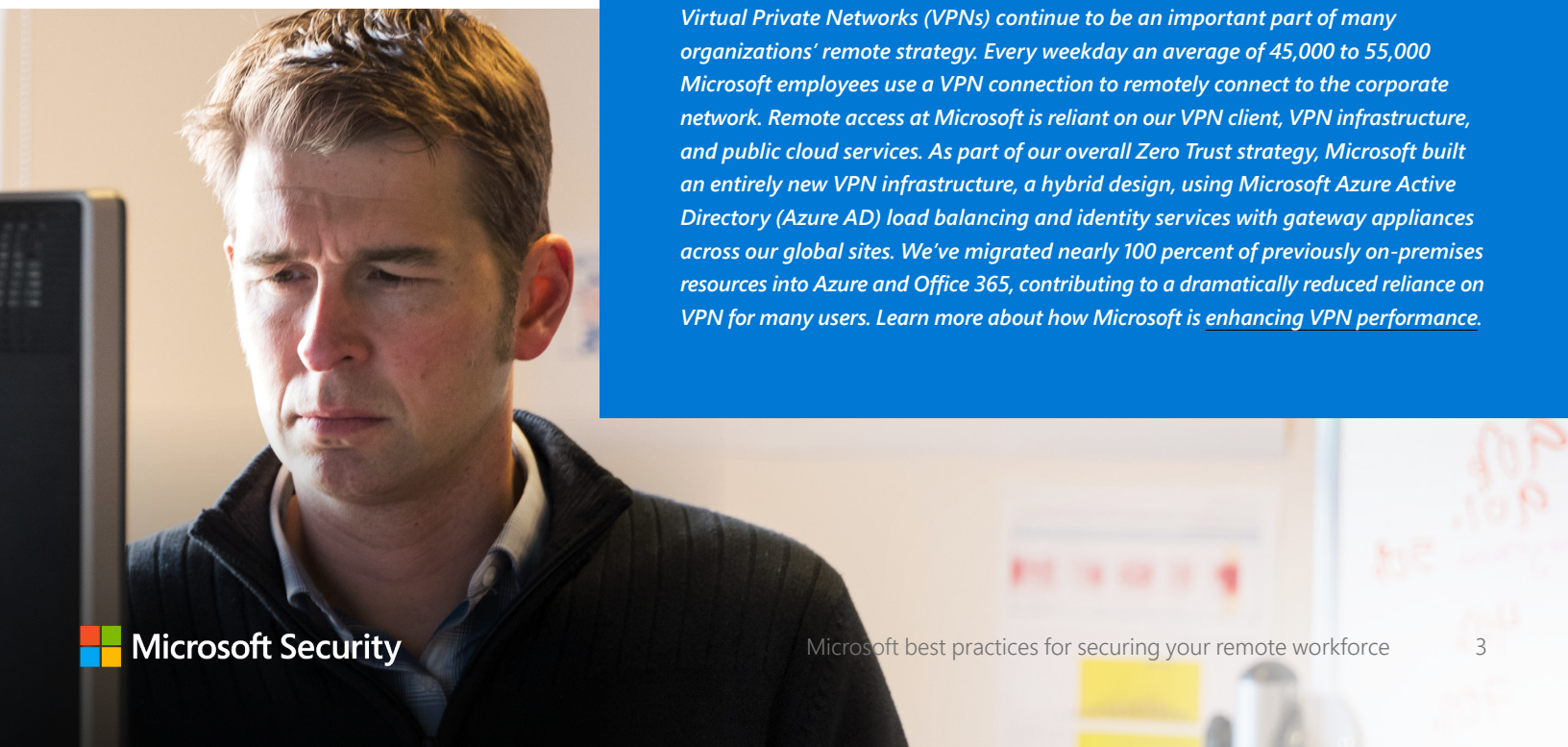
We understand that every IT leader needs to define their own priorities to enable remote productivity across their organization's workforce. While our remote work journey may look different than yours, we want to help by sharing some of our best practices and learnings.

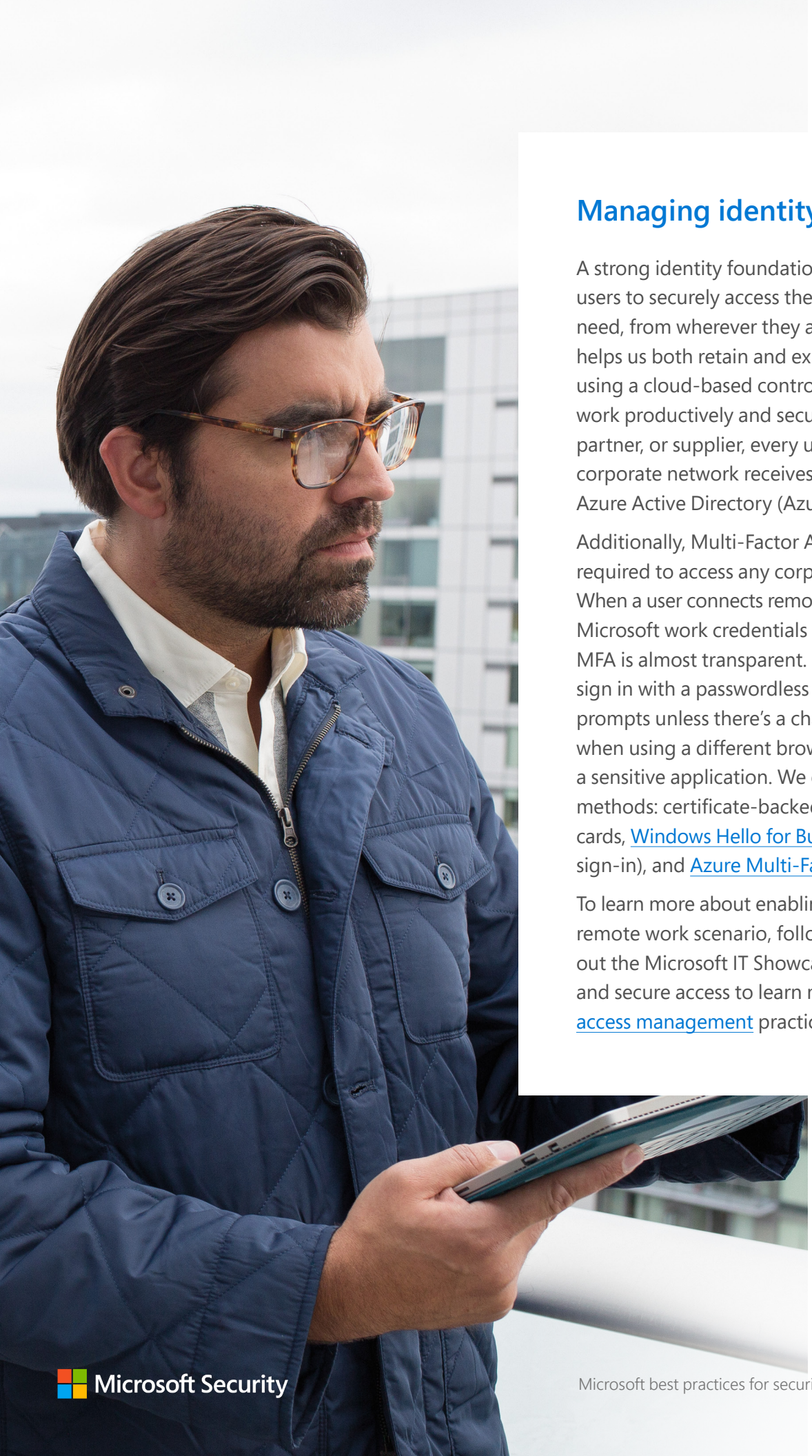
Zero Trust

The complexity of the modern business environment means that our workforce is mobile and expects to be able to work from anywhere. That's why our security approach begins with Zero Trust, which is based on the principle: never trust, always verify. We treat each access request as though it originated from an uncontrolled network. Every access request is strongly authenticated, authorized within policy constraints, and inspected for anomalies before access is granted. Everything from the user's identity to the application's hosting environment is used to verify the request and prevent breach. This approach helps Microsoft protect our employees, devices, applications, and data—and our customers—no matter where our users are located.

Learn more about Microsoft's Zero Trust approach, including how we secure our network with Zero Trust while employees work remotely, and how you can build it into your security model. Because every organization has its unique requirements, existing technology implementations, and security stages, we recommend you use the Zero Trust Assessment tool to determine where you are in your journey and which maturity stage you're at so you can plan your next steps.

Virtual Private Networks (VPNs) continue to be an important part of many organizations' remote strategy. Every weekday an average of 45,000 to 55,000 Microsoft employees use a VPN connection to remotely connect to the corporate network. Remote access at Microsoft is reliant on our VPN client, VPN infrastructure, and public cloud services. As part of our overall Zero Trust strategy, Microsoft built an entirely new VPN infrastructure, a hybrid design, using Microsoft Azure Active Directory (Azure AD) load balancing and identity services with gateway appliances across our global sites. We've migrated nearly 100 percent of previously on-premises resources into Azure and Office 365, contributing to a dramatically reduced reliance on VPN for many users. Learn more about how Microsoft is enhancing VPN performance.





Managing identity and access

A strong identity foundation makes it possible for users to securely access the resources and apps they need, from wherever they are. Our hybrid environment helps us both retain and expand existing systems while using a cloud-based control plane to enable people to work productively and securely. Whether an employee, partner, or supplier, every user who needs to access the corporate network receives a primary account synced to Azure Active Directory (Azure AD).

Additionally, Multi-Factor Authentication (MFA) is required to access any corporate resource at Microsoft. When a user connects remotely to our domain using their Microsoft work credentials on a device that we manage, MFA is almost transparent. Most days, people simply sign in with a passwordless method and won't see MFA prompts unless there's a change in usage—for example, when using a different browser or device, or accessing a sensitive application. We offer three authentication methods: certificate-backed virtual and physical smart cards, Windows Hello for Business (with PIN or biometric sign-in), and Azure Multi-Factor Authentication.

To learn more about enabling Azure MFA to support a remote work scenario, follow this tutorial. And check out the Microsoft IT Showcase covering user identities and secure access to learn more about our identity and access management practices.

Managing devices

Unmanaged devices are a powerful entry point for malicious parties, and it's vital that only healthy devices can access applications and data. At Microsoft, we manage a wide range of devices, including Windows, Mac, Linux, iOS, and Android. Like many of you, we're making the transition to a fully cloud-based management environment. As we make that shift, we've adopted a comanagement approach with Microsoft Endpoint Manager. Endpoint Manager integrates Microsoft Intune and Configuration Manager into a single console where you can manage all your endpoints and applications and take action to ensure they're secure and reliable.

With more employees working from home and across devices, organizations need a strategy to support bring-your-own-device (BYOD) scenarios. We offer self-service enrollment so users can quickly and easily join Azure AD and enroll in Endpoint Manager to access company resources. Once enrolled, Endpoint Manager then applies appropriate policies—for example, to ensure that a device is encrypted with a strong password and has certificates for access to things like VPN and Wi-Fi. Endpoint Manager also ensures 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. Note that while Microsoft company policies require device enrollment, you may roll out a secure BYOD policy without enrollment using Endpoint Manager.

For guidance on deploying and using Endpoint Manager, see our Endpoint Manager documentation and tutorials.

Enable access to productivity and line-of-business apps

Secure and seamless access makes productivity possible while supporting a remote workforce.

At Microsoft, every meeting is now a Teams meeting, with built-in security and privacy safeguards that allow you to manage who participates in your meetings, collaborates on documents, and presents content. Microsoft 365 empowers employees to collaborate through self-service creation of Office 365 Groups or teams within Microsoft Teams while ensuring appropriate security, compliance, and manageability are in place. And when deeper-level collaboration is needed, employees are encouraged to move their chats into a channel.

In addition to making it easy to access Microsoft workplace productivity apps, we've moved many of our legacy line-of-business apps to the cloud. Endpoint Manager can deliver to both Windows and mobile devices, giving employees a seamless experience when accessing their mobile and web, SaaS, desktop, and line-of-business apps. Additionally, we're in the process of rolling out Windows Virtual Desktop (WVD) and are scaling up this offering to support the devices that our developers want to use. For engineers who work exclusively on desktops, we're providing them with laptops that include a WVD solution so they can remotely access their dev environment.

Learn more about how we're enabling our employees to work remotely with Microsoft Teams and about live events in Microsoft 365.

Adapting together

Alongside our customers, Microsoft has adapted the way we support employees working from any location and on any device. To learn more, check out the IT Showcase where we share the blueprint for Microsoft reinvention, so you can benefit from our experiences and accelerate your transformation. Join the new Enabling Remote Work tech community to share your experiences, ask other IT professionals and partners for advice or information, and find additional resources.