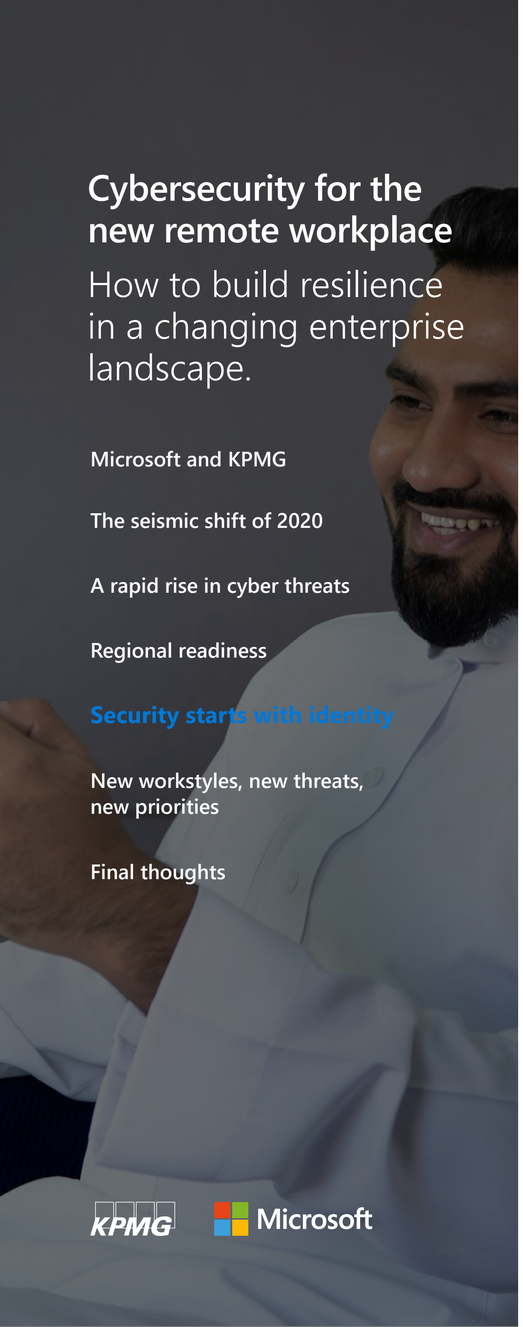


KPMG Microsoft

Security starts with identity

The cloud era is fundamentally changing how businesses think about security. The focus point of protection is no longer the physical network. As traditional network boundaries expand into the cloud, the starting point of security now must be the identity of your users.

This will give you the assurance that the right people are accessing the right resources and doing the right work. Following these five principles will help you implement a robust identity strategy, fit for fully remote or hybrid home-office working.

The first line of defense in a cloud-based, virtual landscape should always be identity.

Embrace open standards

In a virtual working world of different devices, apps, and services, it is important that your approach to identity management supports open standards.

For example, standards like OAuth 2.0, OIDC, and SAML enable single sign-on across apps and clouds, no matter what device users are working on. Similarly, SCIM enables automated user provisioning, and new standards from the FIDO alliance make signing in more secure.

Choosing an identity solution with APIs and protocols that support these open standards, such as Azure AD, will future-proof your security strategy for the evolving changes and challenges of remote work.

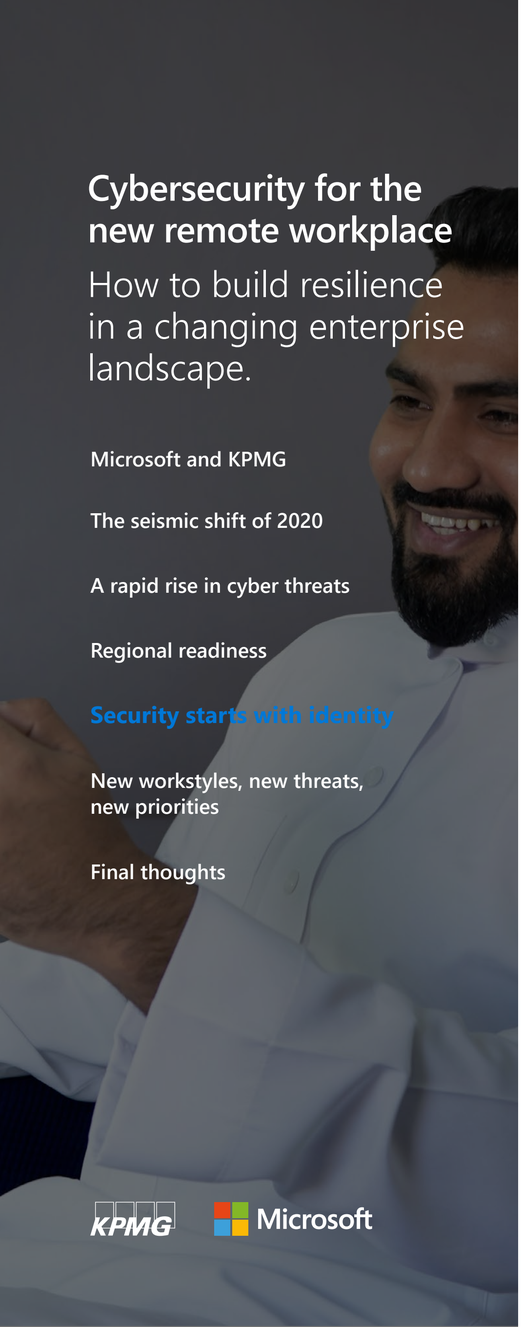
Tap into new technologies

A simple first step to mitigating security risks is to enable **multi-factor authentication** (MFA). This is proven to reduce credential-based breaches by more than 99 percent. MFA asks the user for an additional form of identification during sign-on, such as a code that's sent to their registered mobile phone or a scan of their fingerprint.

While MFA is highly secure, users often get frustrated with the additional security layer, on top of having to remember their passwords. Another option is the use of FIDO (Fast Identity Online) security keys, which—in combination with the WebAuthN standard—can eliminate the use of passwords altogether. FIDO is an open standard for **password-less authentication**, allowing users to sign in using an external security key or a platform key built into a device.

Zero Trust is another security model to specifically address the risks associated with cloud migration and a remote workforce. Within a **Zero Trust architecture**, all users and devices—both inside and outside the corporate network—are assumed to be untrustworthy. Based on the principle of "never trust, always verify", access to resources is only granted after the user's identity and the health of their device has been assessed and approved.

To minimize friction for users and further simplify the identification process, organizations can also tap into **machine learning algorithms**, which—when deployed at scale in the cloud—can process trillions of data points every day to learn each user's behavioral patterns and flag any authentication attempts that are abnormal or high risk.



Cybersecurity for the new remote workplace

How to build resilience in a changing enterprise landscape.

KPMG Microsoft

Security starts with identity

Strengthen and automate your governance

Having **strong governance procedures** in place is essential for keeping on top of identity security. But it can be a daunting task when dealing with thousands of users. Granting access is the easy part, but remembering to remove it when people leave or change roles can be more of a challenge.

Identity systems should automatically provision and deprovision access to resources, based on a user's role, location, and business unit. Employees and partners should be able to request access when they need it, and get a fast and accurate system response.

Administrators should be prompted to review access permissions regularly, specifically when people change roles. And all these processes should be driven and informed by machine learning and AI that constantly monitors for unusual patterns and unrecognized risks. The level of available data and visibility provided by these identity provider technologies simply cannot be matched by on-premises systems, however it does require the organization to adopt a whole new operational approach to identity.

Insist on one holistic solution

If you adopt a modular approach to identity, using different solutions from different vendors, there will inevitably be gaps and vulnerabilities.

In contrast, choosing one holistic solution that supports all applications and different identities will provide full security and control—and more assurance over your critical corporate data.

With a completely **integrated identity and access management suite**, you'll have a single place to manage and protect the identities of all employees, business partners, and customers—plus all the resources they need to access.

Move to decentralized identity

Everyone in an organization should feel that their personal data is secure and private. This can be achieved by giving people ownership of their own digital identity.

By augmenting your identity system with the principle of 'decentralized identity', you can empower users and organizations to have greater control over their data.

With a self-owned identity that integrates into their daily lives, users can choose what they share and with whom—and when necessary, take it back. Instead of granting broad consent to countless apps and services and spreading their identity data across numerous providers, they will have a secure, encrypted digital hub where they can store and manage their identity data.

Microsoft is actively collaborating with members of the Decentralized Identity Foundation (DIF), the W3C Credentials Community Group, and the wider identity community to develop standards and unlock new experiences for Decentralized Identity. Together, we are developing a unified, interoperable ecosystem on which developers and businesses can build a new wave of products, apps, and services that put users in control.

Cybersecurity for the new remote workplace

How to build resilience in a changing enterprise landscape.

KPMG Microsoft

Microsoft Azure Active Directory helps staff at a global transportation company based in Dubai to collaborate as virtual teams and access applications in the cloud—securely.

As part of a business drive shift to reduce its on-premises footprint, the company has moved its legacy HR system to a SaaS solution. Azure AD gives employees a secure and easy way to sign-in and access their information. It also allows HR teams to manage the identities of remotely located contractors for short periods.

"Moving to Azure AD not only simplified administration tasks but—and most importantly—removed a lot of cybersecurity concerns."

One of the world's largest container logistics companies, which operates across 120 countries, needs to keep customer data safe to maintain the trust of its diverse global client base.

Following a cyberattack in 2017, the firm chose to implement the Identity Protection and Conditional Access tools in Microsoft Azure Active Directory. These provide visibility on threats and risky behavior, and make it easy to provide conditional access for each user.

Changes can be activated quickly and seamlessly in the background, so users experience no disruption to their work. It's an integrated intelligent approach to identity that enhances the company's data protection and adds further security to its global operations.

"Working with Azure AD, we had an excellent tool that allowed us to reconfigure our identities. We were then able to look at what applications those users were able to access. In the past, we probably had too much freedom, but with Azure AD we were able to tailor that access."