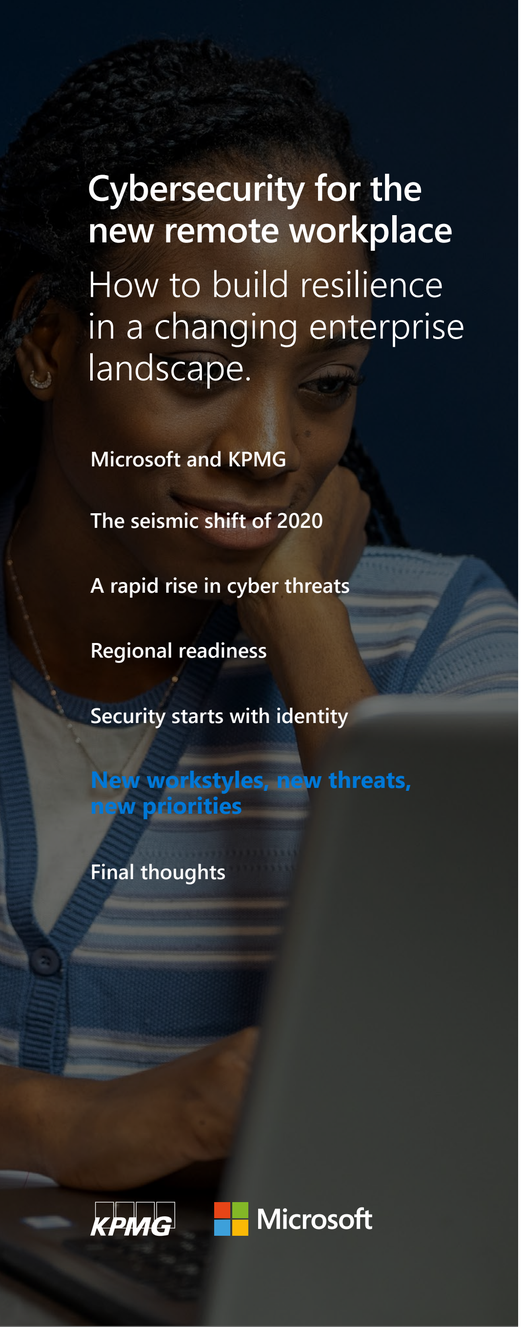


KPMG Microsoft

New workstyles, new threats, new priorities

As we have seen, the health crisis is accelerating the digital transformation of the workplace. It is now a global imperative.

Business leaders across the Middle East and Africa are embracing digitalization and cloud adoption—and there are many strong security tools, identity technologies, and governance policies available to help mitigate security concerns and cyber risks.

However, with the threat landscape evolving at pace, it is important to embed dynamic and adaptive security into your permanent enterprise strategy.

Here are four key trends that will shape the landscape moving forwards:

Automating the security function

By bringing together disparate data sets, and improving the management and accessibility of enterprise information, security teams can start to automate various tasks—such as user authentication and threat detection.

For example, AI and machine learning will automatically verify that remote employees are who they say they are, and detect if they have a virus on their computer or if they have recently opened a phishing email.

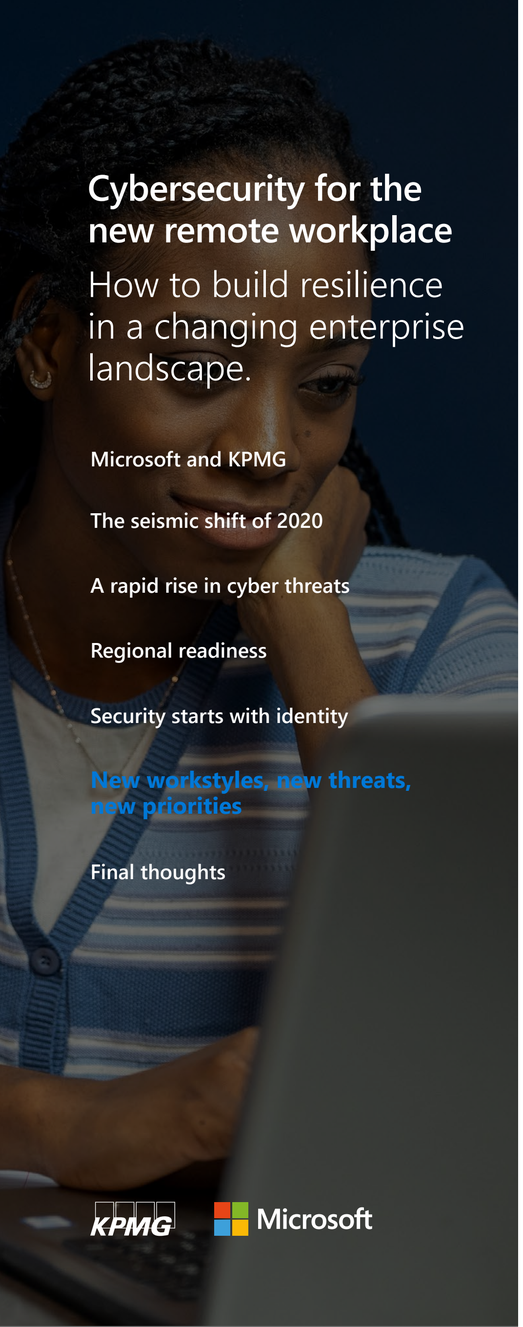
Automating your first and second lines of defense via the cloud means that threats can be addressed without a human having to do that work. It is more cost effective too.

Aligning security to business goals

Security risk models are often misaligned with the business strategy, operating in IT-driven silos. They tend to plan for worst-case scenarios, whereas most incidents have a relatively minor business impact. As a result, organizations are starting to reassess their cybersecurity spending—and seek greater value by ensuring controls are embedded end-to-end across the business.

This new approach requires an ongoing dialog between security and business teams. For example, promoting ‘privacy by design’ will encourage DevOps teams to build security directly into new applications and services. This will move cybersecurity away from being an IT-driven function, towards a business-led function.

Organizations will also seek opportunities for cybersecurity orchestration, using robotic process automation and workflows to automate manual tasks. New models for third-party security will be required too, allowing for dynamic risk management and scoring, and better tracking of supply chain stresses.



KPMG Microsoft

New workstyles, new threats, new priorities

Enhancing digital trust

For remote workers to remain productive and engaged, it is important that they have a smooth and convenient experience when accessing systems and resources. This is especially important when competing for the top talent, who will be more drawn to employers that offer the best working conditions.

A balance must therefore be struck between managing security and reducing employee friction. For example, while it's important to verify who is requesting a password reset, it can be frustrating for the user if they have to wait for a code to be sent to a different device.

As seen earlier, there are frictionless alternatives. Machine learning can be used to understand a user's unique characteristics and behaviors, and shorten the authentication process. There are also password-less technologies, such as security keys and biometrics.

The goal is to establish the right level of digital trust for different scenarios. By aggregating the data you have on each user, you can decide which authentication steps will provide both the smoothest user experience and the requisite level of security. For regular daily tasks, the sign-in process could be short and simple—whereas for atypical processes, you could add in more steps to provide extra assurance.

Strengthening resilience across teams

Historically in an enterprise, the disconnect between IT and security has impacted overall operational resilience. There has often been a time lag in IT teams sharing an up-to-date threat list, so security teams know which infrastructure components to scan.

This challenge is heightened as IT assets move to the cloud and new services can be provisioned far quicker. It is more important than ever to get different teams on the same page, and operating at the same pace.

The key will be to move from long-term, slow-moving security strategies, to small, fast, incremental projects. Security must be built directly into the development stage of every IT deployment, so it is inherent in your software code and not bolted on after the fact.

Building a culture that is open to innovation and experimentation will attract the right cloud security talent for the future. This will enable you to build high levels of resilience against evolving cyber threats in all areas of your business.

Quick wins for secure remote working today

Here are some practical steps you can take now to help employees remain productive when working remotely, without increasing your cybersecurity risk.

- Enable an official 'chat' tool for your organization, so employees know where to congregate for work. Look for opportunities to upgrade for free, so you can remove limits on the number of users who can join a team or video call.
- When sharing tools and resources to help people work remotely, avoid sending download links via email. This could lead to users falling for phishing emails. Instead, make sure you provision tools via a single-sign-on solution instead.
- Look at any policies you have set for access to cloud applications to make sure they do not block users who are working from home.
- Protect company data, while enabling employees to be productive on their personal device, using a Mobile Device Management service.

KPMG Microsoft

As we have seen, the health crisis is accelerating the digital transformation of the workplace.

It is now a global imperative.