

## Cybersecurity for the new remote workplace

How to build resilience in a changing enterprise landscape.

Microsoft and KPMG

The seismic shift of 2020

A rapid rise in cyber threats

### Regional readiness

Security starts with identity

New workstyles, new threats, new priorities

Final thoughts

# Regional readiness

Across the Middle East and Africa, many organizations had already begun their digital transformation journey prior to the outbreak. The benefits of moving from on-premises infrastructure to cloud services were widely acknowledged, and migration strategies were already commonplace on the business agenda.

According to a Riverbed survey in early 2020, 29% of organizations in the Middle East had already completed migration of workloads to the cloud, with a further 31% still in progress, and an additional 20% planning to migrate within the next two years.<sup>12</sup>

What we are seeing in the region now is a rapid acceleration of those plans. Globally, Microsoft has seen two years of digital transformation activity from customers in just two months.<sup>13</sup>

In March, 35% of firms across the Gulf Cooperation Council were already planning to shift to remote work—with 45% of those planning to do so universally for all employees.<sup>14</sup>

The urgent requirement to provide users with remote access to business-critical services was underlined in Riverbed's findings, where 77% of organizations said it is 'very important' to optimize connections to cloud applications like Microsoft 365.<sup>15</sup>

In early 2020

**29%**

of organizations in the Middle East had already completed migration of workloads to the cloud...

with a further

**31%**



still in progress...

and an additional

**20%**

planning to migrate within the next two years.

<sup>12</sup><https://www.riverbed.com/gb/press-releases/riverbed-research-reveals-cloud-and-network-readiness-of-uae-enterprises-as-organizations-adopt-work-from-home-model.html>

<sup>13</sup><https://www.microsoft.com/en-us/microsoft-365/blog/2020/04/30/2-years-digital-transformation-2-months/>

<sup>14</sup><https://www.utilities-me.com/news/15249-37-of-uae-firms-shift-to-remote-work-due-to-covid-19>

<sup>15</sup><https://www.riverbed.com/gb/press-releases/riverbed-research-reveals-cloud-and-network-readiness-of-uae-enterprises-as-organizations-adopt-work-from-home-model.html>

## Cybersecurity for the new remote workplace

How to build resilience in a changing enterprise landscape.

Microsoft and KPMG

The seismic shift of 2020

A rapid rise in cyber threats

**Regional readiness**

Security starts with identity

New workstyles, new threats, new priorities

Final thoughts

# Regional readiness



## A changing security perspective

As this transformation continues at pace across the region, there will be an equally rapid security adjustment.

As applications and services move to the cloud, security strategies will move with them. Organizations that operate a traditional on-premises approach will increasingly adopt the built-in controls of their cloud tools.

This will be a major cultural change for many security teams, who have spent years protecting a physical infrastructure with a well-defined network edge.

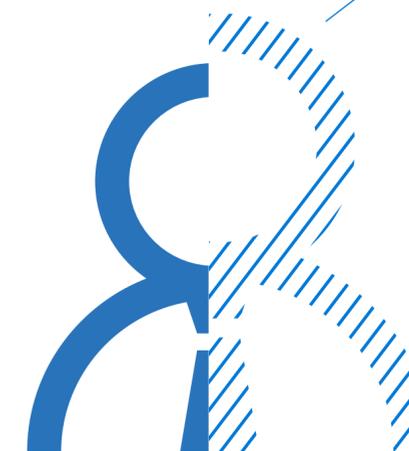
They will now face the altogether different challenge of safeguarding a distributed cloud network, characterized by thousands of end points (both corporate and personal devices), virtual desktops and VPN connections.

VPNs that support split-tunneling, coupled with a secure cloud service endpoint, can help optimize performance for remote users. However, the approach of using VPNs to access certain applications may only be a short-term necessity, as organizations look to modernize and move those applications to the cloud.

To maintain control over sensitive company data and mitigate evolving cybersecurity threats in the new landscape, security teams will need to embrace proven cloud security tools and adopt new processes—such as remote provisioning—to get workers set up appropriately when they can't physically be at the office to collect equipment or receive training.

Instead of defining borders at the edges of a building, the new normal is to provide for protections that are as close to the data as possible—i.e. protection and tracking that lives on the data and on the device where they are consumed.

In March, 35% of firms across the Gulf Cooperation Council were already planning to shift to remote work—with 45% of those planning to do so universally for all employees.



## Cybersecurity for the new remote workplace

How to build resilience in a changing enterprise landscape.

Microsoft and KPMG

The seismic shift of 2020

A rapid rise in cyber threats

**Regional readiness**

Security starts with identity

New workstyles, new threats, new priorities

Final thoughts

# Essential security steps for the new reality

Organizations that encourage remote working or operate a hybrid home-office model need effective security controls, including:

- Email and web security
- Regular patch updates
- Monitoring of shadow IT
- Fraud detection algorithms
- Bespoke tools to monitor home-working tasks

### However...

the most important security step for organizations to get right is identity and access management, which we will explore further in the next chapter.