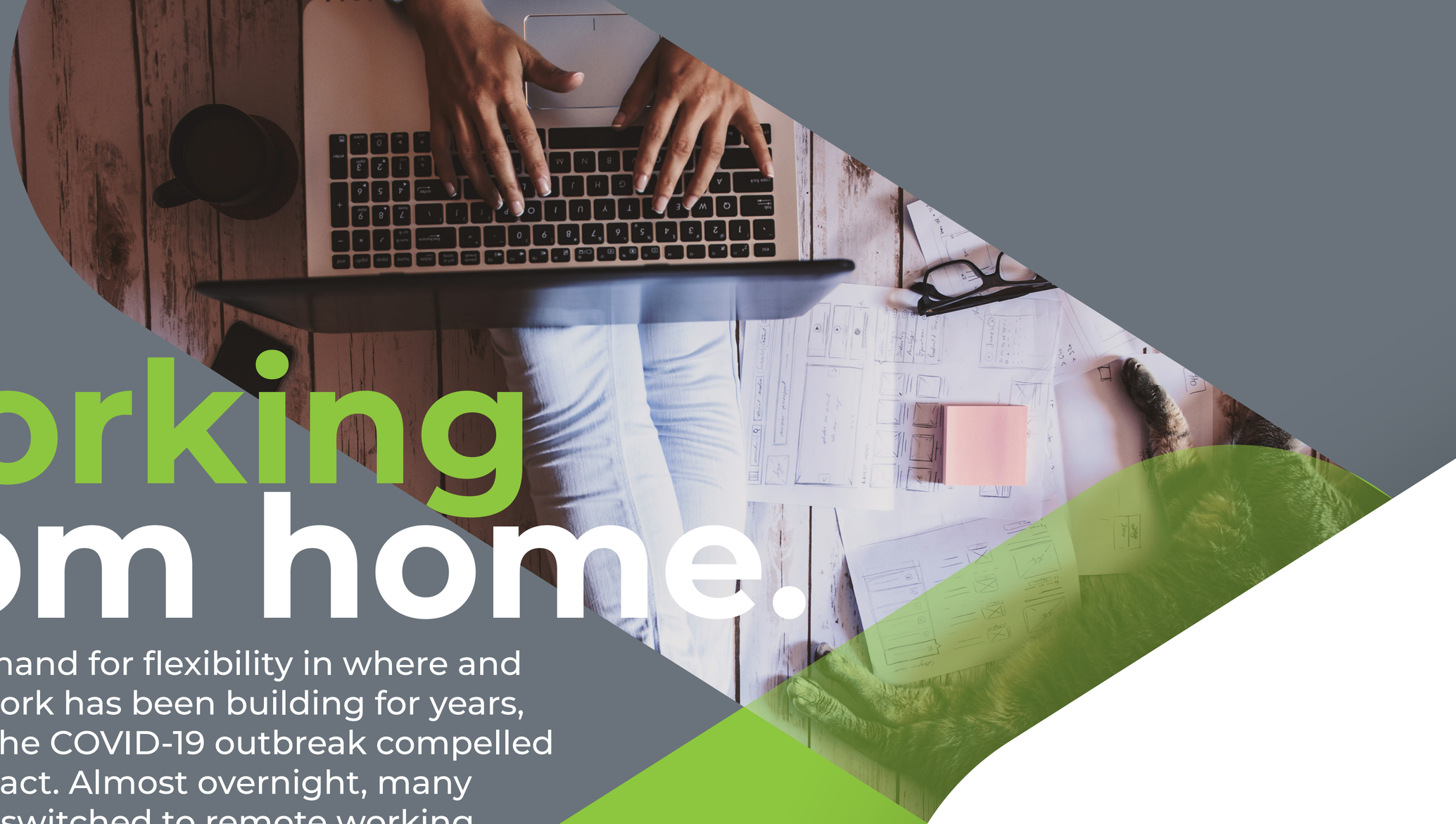


Working from home.

While the demand for flexibility in where and how people work has been building for years, ready or not, the COVID-19 outbreak compelled businesses to act. Almost overnight, many organisations switched to remote working practices as an emergency response to keep the wheels of their business turning.

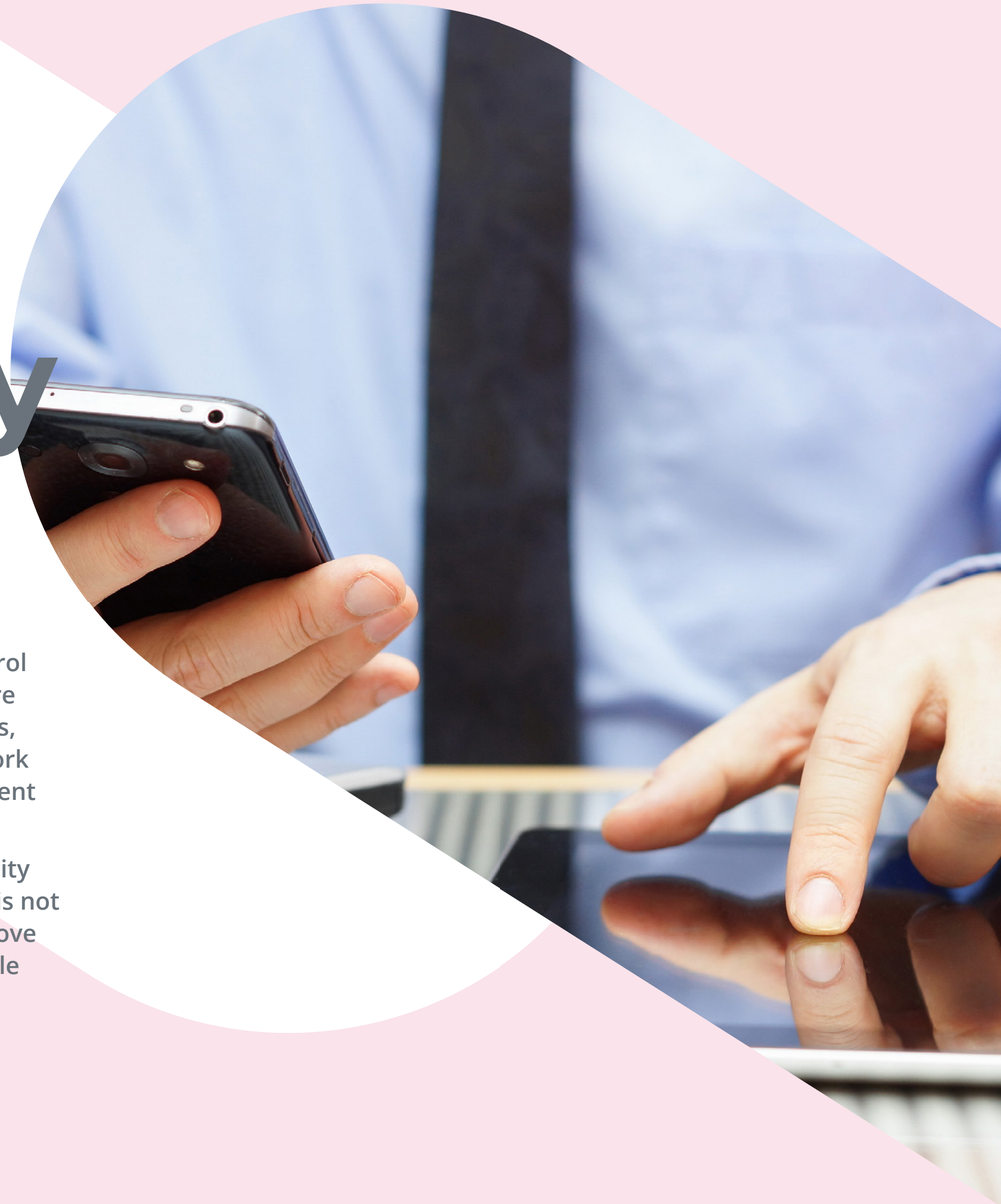
qolcom

Remote working: Solving technology challenges.

Modern technology has made remote working a possibility for everyone, creating an upside for businesses and employees alike.

Studies show that workers who have more control over their schedules and places of work are more satisfied and productive. For many organisations, offering flexibility and allowing employees to work remotely makes them more attractive to top talent and they see retention rates soar.

However, despite the significant benefits flexibility offers, supporting employees to work remotely is not yet universal. Some businesses still resist the move to offer more flexibility because they yet to tackle the technology, support, and remote workforce needs to maintain work quality, culture, and collaboration outside the office.



Tackling remote working challenges with modern connectivity

With business applications and data stored in the cloud, secure and fast access is more important than ever. Delays in loading pages or lengthy document download times can impinge on productivity, user experience and employee morale. So, it's essential to have secure, reliable connectivity between your mobile workers and your critical applications.

For areas connected to the NBN, the frustrations of dealing with slow internet connections that frequently drops out is thankfully a thing of the past.

Likewise, the shift from 4G to 5G will change how, where, and when your people work. 5G's potential for faster speeds and lower latency means your remote workers can experience optimal performance away from the office. This means smooth connectivity using business applications and downloading large files wherever they are.

Tackling remote working challenges with the right tools

To enable knowledge sharing, information gathering and collaboration no matter where your employees are, you need to adopt the right technologies. To get your remote workers collaborating more effectively, unified communication and collaboration tools are essential and include:

- Video conferencing
- Messaging
- IM and presence
- Screenshare

Tackling remote working challenges with end user support

Systems can and do go down. Laptops, mobile devices, and tablets all require troubleshooting and security patches. With your people working remotely, it's important to give them access to immediate support. As such, remote management is vital and integral to business continuity.

Resolving tickets on the helpdesk quickly and efficiently, without interrupting either the support professional or end user, is crucial to meeting service levels and maintaining a good relationship with your workforce.

Tackling remote working challenges with enhanced security

With your employees accessing corporate information from outside your corporate domain, it's critical that your remote access system fully secures access to that data. It's important to identify remote access risks across your organisation and create and enforce remote working security policies.

To mitigate risks, using two-factor authentication is the gold standard for securing remote desktop connections. It keeps data secure by ensuring user authenticity before providing access to remote networks and sensitive data. Likewise, it's essential to keep on-device software completely up to date. Outdated and unpatched remote access devices are vulnerable to attack and can expose your organisation's data and networks to cyberattacks.

Free checklist to maximise remote access

Secure company data for remote working, with our Work from Home Communications Checklist.

Get this free tool to guide you through equipment checks, network requirements, and support services.

Download here

Remote working: Establishing a secure and productive work environment.

Remote working has been accelerating across many different professions and industries for quite some time. The coronavirus pandemic has, however, put the practice into sharp focus. With governments pressing for all those who can work from home to work from home, the COVID-19 outbreak has fast-tracked a trial run of remote working at an unprecedented scale.

Ready or not, businesses everywhere are urgently working out how to support a remote working program and are putting these plans into immediate effect. This includes:

Provisioning desktops and devices

Securing endpoints and data

Providing end-user support

1. Provisioning remote laptops and devices for remote working

For IT professionals, never has it been more important to provision mobile devices and laptops to ensure employees can productively work in these challenging times of COVID-19. Employees need secure remote access to devices, data, business applications, and unified communication and collaboration tools like video conferencing, messaging, and IM and presence.

Whether you offer company-owned devices or support Bring Your Own Devices (BYOD), an enterprise mobility management (EMM) application is essential. It helps to centrally managing large deployments of devices with minimal IT resources – allowing companies manage remote technology, devices, apps, content and security.

The EMM toolset enables IT teams to increase the speed in which they can deploy devices to employees with the right software and security settings which frees up IT from hours of provisioning effort. This also means employees can get started right away while the IT team maintains critical control over all remote devices.

2. Securing endpoints and data

Maintaining your organisation's cyber security framework when the majority of your workers are working from home, creates new challenges. With so many employees working from home, setting up a variety of new security measures and robust user controls is critical.

This includes ensuring all endpoints are secure, patched, and up-to-date, and that the systems will only run authorised applications.

Of course, whenever an employee is working remotely, they should be accessing your organisation's network and any software-as-a-service (SaaS) resources via a virtual private network (VPN). The use of Virtual Private Networks (VPNs) prevents core systems being compromised via the internet.

As it's important to ensure your VPN solution works on most target devices, it's a good idea to test all the service providers, devices, and locations to ensure performance is sufficient.

In addition, multifactor authentication is essential when staff work from home using company laptops. Multifactor authentication provides an added layer of protection and makes it harder for an attacker who gains access to someone's credentials to use them.

3. Providing end-user support for remote workers

Whenever work conditions change, you need to provide additional support. For remote workers who encounter basic technical issues and have no means to resolve them without having to wait on the helpdesk can be incredibly frustrating. Likewise, for the support team, having to rely on unstructured issue descriptions from a user who isn't technical can prolong user downtime.

So, with the move to remote working, it's important to boost your help-desk support team to meet your increased support requests. You can do this by moving staff internally to bolster the team or by partnering with an outsourced provider.

It's also best practice to provide self-service options wherever possible so that employees can change their password if they're locked out of the system, reset a failed device, or log a service ticket. It's also smart to make it easy to get support through multiple channels, including bots, chat, email, and phone.

Remote working: securing sensitive data

For many enterprises, the COVID-19 outbreak has triggered an emergency response to establish and enable a remote workforce. Businesses everywhere are supporting remote working practices, yet in many cases, without laying strong foundations for robust data security.

This scenario, says Dr. Barbara Rembiesa, president and CEO of the International Association of IT Asset Managers (IAITAM), exposes companies to significant risk. “The impulse to send employees home to work is understandable, but companies and agencies without business continuity (BC) plans with a strong IT Asset Management (ITAM) component are going to be sitting ducks for breaches, hacking and data that is out there in the wild beyond the control of the company.”

Securing sensitive data

Without rigid controls, too many businesses are now exposed to potential data security breaches an unauthorised data access:

- Allowing workers to use BYOD devices and work across public Wi-Fi systems is far from ideal if you want to safeguard company data. So, it's essential to ensure your people use an enterprise-class virtual private network (VPN) when working remotely. It routes traffic through a secure network which encrypts the data even while your employees are connected to public Wi-Fi. In addition, multifactor authentication is essential when staff work from home, providing an added layer of protection that makes it harder for an attacker who gains access to someone's credentials to use them.
- In the absence of an enterprise mobility management (EMM) system, companies lack control over access to corporate data. With only scant information about the personal devices being used to conduct company business, it's impossible to secure mobile devices, applications, and the data on them. EMM solutions can prevent critical data loss and unauthorised data access and reduce risk should an employee lose a device that contains commercially sensitive data.
- It's not enough to issue a security policy document. Without regular training and ongoing guidance on security, the sensitive data on personal devices could be at considerable risk of phishing and social engineering attacks. As a matter of course, all employees need security training at regular intervals to ensure they are confident of identifying and responding to potential threats.
- It can be hard to keep track of company data on multiple personal devices. In many cases, company information may remain on a personal device long after the employee returns to the workplace. If the device is handed down, sold to a third-party, or improperly disposed of, who knows who could get their hands on your sensitive company data?

With many of the country's workers potentially working at home for some time to come, it's essential to prioritise these data security challenges. IT assets should not be allowed to leave your company site without formally accounting for each of them.

The smart way to track all IT assets that are being taken home – and the data stored on them – is using modern EMM tools which include:

Mobile Device Management (MDM)

MDM tools allow you to monitor, manage and secure your employees' mobile devices. MDM also allows you to remotely erase data which is a huge benefit when managing devices used by staff working at home.

Mobile Application Management (MAM)

MAM tools enable the remote management of applications on a mobile device.

Mobile Identity Management (MIM)

MIM allows IT to manage accessibility, ensuring only approved users and devices are allowed to access secure corporate data.

Mobile Information Management (MIM)

MIM plays a big role in keeping sensitive corporate information secure. It ensures only approved applications and data are made available to your employees.

Mobile Content Management (MCM)

MCM enables employees to work efficiently from their mobile devices while protecting corporate information from unauthorised access.

Remote working: Delivering benefits to your business

Love it or hate it, remote working has become the new normal for many businesses and employees.

As we (hopefully) move into less restrictive times, many businesses are starting to weigh up the possibility of supporting remote working practices on an ongoing basis. Across many industries, companies are discovering many advantages of supporting remote working and the benefits of working from home.

Business benefits of working from home

Higher retention

Providing employees with flexible work practices can be critical to retaining your best people. Having arrangements where you allow employees to work from home instead of coming into the office gives your employees the opportunity to fit work around their other commitments – which is key to greater happiness at work. If employees are happier, turnover rates will be lower and associated hiring and training costs will decrease.

Enhanced productivity

Trusting your people to work away from the office engenders greater commitment from them. Ask any HR professional, with a more motivated workforce, you wind up with highly productive, efficient staff, with lower absenteeism and its associated costs.

Larger talent pool

Offering remote working arrangements gives you the freedom to hire outside of your local area. This gives you access to a far deeper talent pool and more quality talent. Once hired, you can expect greater productivity and innovative thinking.

Reduced floor space

When you minimize the number of people required to work on site, you may be able to downsize your business workspace requirements, reducing real estate and associated operating costs.

Technology to support your remote workforce

Of course, setting up your business to run at optimal levels with a remote workforce requires a commitment to enterprise mobility, security, and supporting employees with right technology and tools to help them succeed.

Businesses need to review their security policies to ensure employees only have access to the critical data and systems they need to do their work. Employees must also play their part and ensure all work and communication is conducted only on approved devices, applications and collaboration tools.

Essential communication tools include:

Video conferencing

Video conferencing is a boon to remote working teams, allowing workers to communicate face-to-face and read body language and other nonverbal cues that are essential to effective communication. Taking advantage of video conferencing allows your remote workers to easily join meetings, collaborate on documents, and share screens ¬– wherever they are.

Messaging and presence

Dedicated instant messaging tools allow remote employees to stay connected while keeping data safe and secure. Using enterprise-grade tools, help keep vital communications flowing outside of the email inbox. Using instant messaging, messages are received in real time, allowing recipients to action the message without delay.

Multi-party voice

Modern audio-conferencing tools enable quality communications between multiple parties in various locations, conducted via mobile phones or landlines.

Streamlining business communications

Streamlining the use of these tools using unified communications as a service (UCaaS) simplifies the management of multiple applications and vendors. You keep communications up and running with a single UCaaS solution that supports everything from instant chat and messaging, to SMS, presence, and voice, as well as web and video conferencing.

qolcom

Remote working: Enhancing mobile data security in 2021.

The advent of COVID-19 forced many companies to pivot and modernise, adopting new technologies at a rapid pace to keep the wheels of their business turning.

Many organisations are now looking at what they can learn from the pandemic so they can continue to do what they did out of necessity last year as a standard way of doing business this year. With work-from-home models being adopted as the new normal, it's more critical than ever to secure your organisation's data while supporting remote access. Take the time now to take a close look at mobile data security.

Enhancing endpoint management

Long-gone are the days when your IT department only had to support a fleet of corporate-owned devices with one operating system (OS) type. Providing safe connectivity and mobile data security requires seriously scaling up enterprise mobility management across an increasing variety of devices, OSs, users, and remote access tools.

Now, with multiple platforms including Mac, Windows, iOS, and Android being used across any business with who knows how many outdated OS versions, it's a significantly different job.

For instance, according to Wandera's Cloud Security Report 2021, companies with fewer than 500 devices run 11.3 different OS versions on average, on 1.4 different OSs, across 1.8 different device models. While companies with more than 500 devices run 39.4 different OS versions, on 1.6 different OSs, across 2.6 different device models.

At the same time, physically controlling access to the corporate network with remote access tools such as VPN and RDI are no longer enough without a robust method for verifying the user's identity or checking the device's security posture.

Heightening remote access

According to IDC's Remote Access and Security Challenges & Opportunities report, 40% of cyber breaches originate with authorized users accessing unauthorized systems. Whereas in 68% of major incidents involving remote access tools, a VPN was used.

With mobile devices making up the fastest-growing attack surface and with cybercriminals targeting enterprises through vulnerable smartphones and tablets, the widespread shift to remote working has only made matters worse.

As such, adopting a Zero Trust Network Access model and running continuous risk assessments are a critical part of today's remote access strategy. The Zero Trust model of not trusting any network or data access request by default and securing all entry points has emerged as the most reliable way for companies to tackle evolving cyberthreats within their remote and immediate environment.

Configuring business tools for fast and safe connectivity in 2021

According to Wandera's report, 52% of organisations experienced a malware incident on a remote device in 2020, up from 37% in 2019. And of those devices compromised by mobile malware in 2020, 37% continued accessing corporate emails after being compromised and 11% continued accessing cloud storage.

With remote access and work-from-home models becoming the new normal, it's important to understand cyber risks and how they can be introduced to your organisation.

Start by considering what you want to enable your people to do on their devices and what you need to know about users, devices, networks, and apps before you grant them access to corporate resources. As a baseline, make sure you:

4 practical ways to enhance mobile data security

1. Limit users to only the business tools they need – preventing hyper-privileged accounts being exploited to attack large numbers of systems
2. Deploy endpoint protection across all devices – leveraging a cloud-based security solution to protect against the broad spectrum of cyber threats and usage risks
3. Use a security solution to address both external cyber threats (such as phishing, man-in-the-middle attacks, malware) and usage behaviour risks
4. Configure access to address the threat vectors that are appropriate to your business while respecting the privacy of your end users.