kaspersky BRING ON THE FUTURE

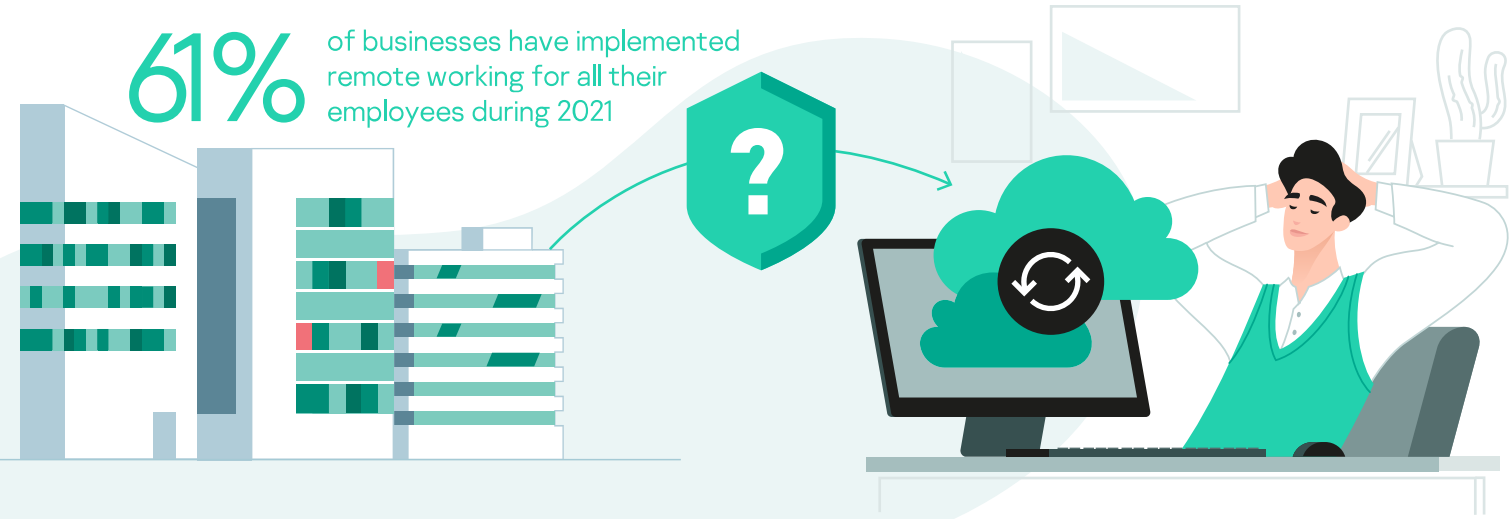
Cybersecurity: Lessons learned in making remote working work

Flexible and remote working options have always been popular with employees. But when the global pandemic disrupted operations, virtually every business was forced to open their networks and systems for remote operations.

One report suggests that 61% of businesses have implemented remote working for all their employees during 2021[1]. Businesses are also keen to encourage the trend – 24% intend to increase their use of remote working in future[2].

But many businesses rushed their remote working deployments. The priority was to maintain some level of productivity – virtually every other consideration was sidelined in favor of speed.

If this was the case for your business, can you be sure that your remote working provisions are secure?



90% of IT professionals believe remote workers pose a security risk – and 54% believe they are a greater danger than their onsite counterparts[3]. Clearly there is an awareness that remote working may involve elevated risks – but at the same time, 26% of companies report that they do not have enough security staff to properly support their remote workforce[4].

The truth is that as lockdown mandates came into force, businesses were forced to implement mass remote working provisions as fast as possible. Even when there were existing remote working systems in place, most were unable to properly deploy at scale.

In many cases this led to an explosion in the use of shadow IT, as employees scrambled to find tools that were 'good enough' for collaboration and data sharing. Security and encryption did not figure prominently in many of these choices, leading to the selection of insecure, inappropriate applications[5]. These bad choices dramatically increased risk of data being lost, stolen or leaked – especially as they had no centralized control mechanisms that would allow the IT security team to monitor uses and abuses.

As remote working has matured, businesses are beginning to catch up. Over the past 18 months they have had time to assess tools and select those which best protect the organization's interests. However, there remain inherent weaknesses in these remote working provisions because of the way they were initially assembled.

This guide will help you understand some of the risks you face in terms of endpoints, infrastructure and networking. It will also provide a useful roadmap for improving your security posture as the network perimeter erodes and more unknown, untrusted devices are used to access corporate resources.

Section 1 – Are your endpoints in order?

The devices used by workers are a fundamental pillar in your remote working strategy. Many IT managers regard this as the hardest problem to solve because employees will often use their personal devices for work purposes. This only serves to make scalable administration even harder.

40% of IT managers report difficulties sourcing the right equipment for their remote workers[6], which is why 61% of remote workers had to supply their own[7]. Where this happened, 27% have struggled with the logistics of installing management agents on them[8]. Nevertheless, there must be some degree of endpoint control to protect corporate resources.

Among the questions you need to address are:

- **Are we locking down OS and applications to prevent compromise?**
- **Are our users tampering with settings, placing corporate systems at risk?**
- **How can we prevent crossover of personal and professional data on shared purpose devices?**
- **Are we too focused on PCs? What about smartphones and tablets?**
- **How are we ensuring client devices are properly patched and secured?**
- **How can we ensure employees are 'playing by the rules' and not increasing risk through negligence or malicious activities?**
- **How do we support and administer personal devices? Where do we draw the line between professional and personal responsibility?**

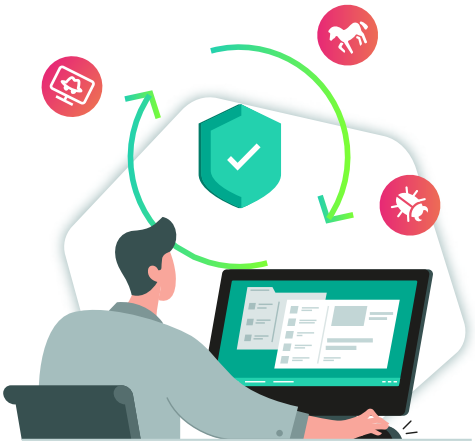
In many ways, the endpoint is the hardest part of the remote working technology stack to manage. The division of personal property and corporate operations relies on compromise from both parties – which is completely at odds with general principles of IT security. It is also why 20% of hacking attempts are directed at end user devices[9].

Nevertheless, 48% of businesses have already implemented strict user and device access policies, with another 24% set to follow suit next year[10]. It may be that these organizations are rolling out corporate devices or VDI sessions to their users, rather than continuing with higher risk personal devices.

Anti-malware

Every endpoint device connecting to corporate resources must be secured with an anti-malware tool. Preventing viruses and ransomware from entering the network is key to containing spread and preventing potential damage – 27% of security incidents are caused by ransomware for instance[11]. Astonishingly, 91% of remote workers in one survey claimed that their employer **did not** provide them with an antivirus solution to install on their personal device that was being used for work purposes[12].

Intelligent anti-malware tools that employ advanced heuristics and machine learning to identify and block suspicious files and activity automatically are essential. These proactive tools dramatically reduce the risk of compromise – particularly when the IT security team cannot always manually update or control remote devices.



Phishing and impersonation

Phishing and email scams continue to be popular with cybercriminals because they work – 22% of reported incidents during 2020 involved phishing[13]. The good news is that most existing email defenses will continue to work, regardless of where remote workers access their inboxes, because they are hosted within the corporate network (or secured cloud platform).

However, where the employee has a mixed-use device, there is always a risk that they fall victim to a phishing email or infected attachment from their personal account. By circumventing the corporate defenses, hackers can still acquire valuable data and credentials by fooling employees with well-crafted email.

Again, installing anti-malware at the desktop level will help, but employees should also receive regular retraining in how to identify and manage email. They should be actively encouraged to apply their knowledge to personal email too – not least because it will help them avoid suffering loss personally as well.

Endpoint updates and patching

Another serious concern will be keeping connected devices patched and updated. Leaving machines unpatched is an open invitation to criminals to take advantage.

It may be that remote workers must be recalled to the office for regular 'health checks'. Or a schedule will need to be drawn up so that devices can be updated overnight according to a pre-agreed routine.

Further into the future, migrating to a hosted VDI system may be a better strategic option. Centralized images remain under your control at all times, and can be managed and maintained in the same way as existing on-premises devices.

End user behavior

Employee behavior has always been one of the biggest concerns surrounding remote working – generally in terms of productivity. But behavior tops IT leaders' lists of concerns, higher than phishing, weak passwords, poor endpoint security and shadow IT[14]. Worse still, 52% of IT managers have experienced employees finding workarounds for security systems and policies[15]. This is not usually malicious behavior, instead it is workers trying to manage barriers to efficiency and productivity. However, each time-saving shortcut is also a potential threat to system integrity.

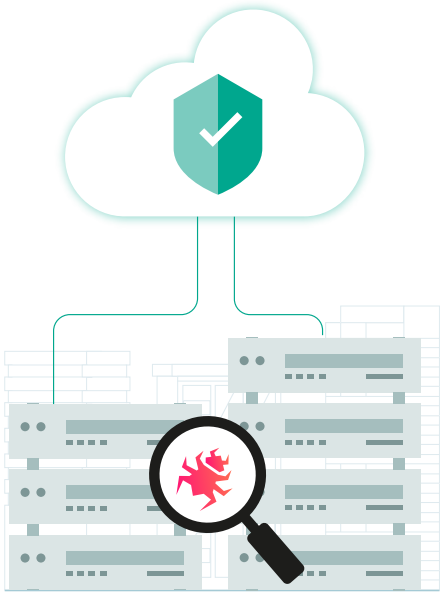
This issue is complicated when dealing with mixed-use devices owned by the employee. Businesses will need to negotiate a compromise with their workers about how they interact with corporate systems – especially when users have spent an average of $348 of their own money to upgrade or improve technology while working at home due to COVID-19[16]. Again, VDI or locally sandboxed sessions may provide additional controls that prevent workarounds without overstepping the boundary between professional and personal. 93% of businesses have a remote work security policy in place[17] – now they need to enforce them.

Zero Trust at the desktop

Although Zero Trust is deployed at the infrastructure level, it still has a role to play at the endpoint level too. Systems need to be configured to carefully monitor and verify remote activity to control and limit access when required.

Zero Trust mechanisms will help to address many of the uncertainties related to 'unknown' devices. Remote employees are assigned least-privileged access, ensuring they can use the resources they need to do their jobs, without exposing other systems that they don't. Controls can be applied at desktop, network and infrastructure level for granular security and increased protection of corporate resources.

Section 2 – Is your infrastructure in order?



For most businesses, their core infrastructure should already be well secured – at least for use internally. However, the shift to remote working has effectively punched holes in perimeter security to provide access to centralized resources.

As your remote working capabilities mature, your IT security team needs to ask some tough questions:

- **Should we be migrating remote workers towards a Virtual Desktop Infrastructure (VDI) setup?**
- **Are there any internal applications that could be better secured by migrating to a cloud-hosted/SaaS alternative?**
- **How are we controlling access to internal resources?**
- **How is data being protected – particularly if it is stored outside the network perimeter?**
- **How can we mitigate the effects of malware and ransomware?**

Keeping data inside the network

By keeping systems and data within the corporate network, you immediately reduce the risk of loss, theft or leak. The use of VDI solutions provides your end users with a desktop-like experience and ensures that data remains within your thin client infrastructure; there is no need to transfer files or data to the local device where it is at greater risk of compromise.

Use the power of the cloud

Cloud-based applications and SaaS are typically protected by enterprise-class security defenses. It may be more appropriate and effective to migrate applications away from the on-premises data center. As well as simplifying remote access to these applications, cloud-enablement can increase the overall security of your data.

Strengthen account control

Passwords remain a continued source of problems – businesses experience an average 922,331 credential stuffing attempts each year[18], while 37% of breaches involve stolen credentials[19]. Maintaining password security within the network perimeter has always been difficult. But remote endpoints simply increase the risk of credentials being exposed or stolen. Upgrading account controls to use single sign-on (SSO) and multifactor authentication (MFA) or passwordless alternatives offers an additional layer of protection if credentials are compromised.

You can further strengthen defenses using continuous authentication and anomaly analysis. These tools monitor user activity to automatically identify and block suspicious behavior to limit damage in the event of a successful breach.

File sharing

As well as being able to access data easily, remote workers must be able to collaborate with their colleagues. There is a serious risk that users will gravitate towards personal accounts with platforms like Dropbox or Google Drive, placing that data outside your controls – and increasing risk of exposure.

You will need to identify and deploy approved file sharing systems for remote workers – including paid-for, centrally controllable versions of services like Dropbox and Google Drive. Your file sharing provisions should apply encryption to all data in transit and at rest.

You can further protect data using a cloud access security broker (CASB). The CASB acts like a proxy to apply policies to data as it is transferred to and from the cloud. In this way, you can ensure data is being used responsibly from any device – including unmanaged personal smartphones and tablets.

Data vaulting

Ransomware represents a real and significant threat to all of your systems. An uncontrolled infection can take production systems and backups offline, making full recovery almost impossible.

Data vaulting – using immutable backups – prevents files being encrypted. This is an important layer of protection for when remote users do inevitably introduce ransomware into the network.

Adopting a Zero Trust posture

Perhaps the most important strategic change your business needs to adopt in the era of remote working is the adoption of a Zero Trust security posture. According to guidance issued by the US National Security Agency, the Zero Trust security model operates according to three core principles:

1. **Never trust, always verify** – Treat every user, device, application/workload, and data flow as untrusted. Authenticate and explicitly authorize each to the least privilege required using dynamic security policies.
2. **Assume breach** – Consciously operate and defend resources with the assumption that an adversary already has presence within the environment. Deny by default and heavily scrutinize all users, devices, data flows and requests for access. Log, inspect and continuously monitor all configuration changes, resource accesses and network traffic for suspicious activity.
3. **Verify explicitly** – Access to all resources should be conducted in a consistent and secure manner using multiple attributes (dynamic and static) to derive confidence levels for contextual access decisions to resources[20].

Using Zero Trust principles will help to identify and mitigate issues more quickly – and to design safer, more secure infrastructure for your remote workers to use. Monitoring goes beyond simply assessing user activity too; any operation or interaction is assessed, identifying misconfigurations alongside active hacking attempts.

Section 3 – Is your networking in order?

Your users need secure, reliable connectivity to ensure they can access corporate resources to do their jobs. Rolling out VPN connections is relatively straightforward, but managing, maintaining and policing them is a significant administrative overhead.

To help assess whether your networking is properly secured for remote working, you need to know:

- **Are all incoming and outgoing connections secured on our remote workers' devices?**
- **How are we dealing with phishing and fake websites?**
- **How are our end users accessing the internet?**
- **What threats exist inside our users' home offices?**

The connection between end user and corporate resources is another key weak point in your remote working provisions.

Encrypt connections

Virtual private network (VPN) connections are now a standard connectivity method, used by 72% of businesses to grant access to the corporate network[21]. By encrypting traffic between endpoints, you can prevent most common eavesdropping attacks. Moving forward, you need to ensure that similar levels of encryption are applied to every remote resource – including cloud platforms and SaaS.

One small note of concern however – just 43% of remote workers surveyed said they used a VPN when working from home[22]. It is likely that many users do not realize that their connections are encrypted. Instead, it indicates a lack of training and knowledge in basic security that would help them play their part in better protecting the business.

Secure Access Service Edge (SASE)

VPNs are useful for securing connections between endpoints and the corporate data center, but the modern network makes heavy use of distributed assets like cloud services. Secure Access Service Edge technology unifies WAN technology with network security services like CASB (see above), Firewall as a Service and Zero Trust into a centralized control panel.

SASE is delivered as a cloud service, monitoring the identity of the entity, providing real-time context, and enforcing enterprise security/compliance policies and continuous assessment of risk/trust throughout the sessions. SASE is flexible, scalable and able to protect data assets on-premise, in the cloud and at any point during transit.

Filter requests

Endpoint antivirus applications will typically detect and block suspicious network requests – but what happens if the end user disables local protections? Enabling DNS filtering provides an additional layer of network security, preventing malware from dialing home and reducing the risk of users being tricked into visiting malicious sites.

Wi-Fi policies

Remote working is not always restricted to the home office. Co-working spaces and even coffee shops are now considered viable work locations by your employees. However, the potential for man-in-the-middle attacks and other connection hijacking attacks is a serious security risk.

VPN connectivity as default will provide some protection, but you must also educate users about using public Wi-Fi safely – if at all – and draw up policies accordingly.

Home network usage

In the age of cloud-controlled home automation, your users' home networks are also increasingly insecure. When working from home, your business has very little direct control over the shared network which could be used to compromise connected corporate devices – often through IoT devices that are improperly secured.

You must invest in technologies that will harden the local devices so they are better defended against local malware, external attacks and other exploits that could be used to piggyback connections into the corporate network. Most home Wi-Fi routers now offer dual network capabilities – encouraging remote workers to configure and use the secondary network to segregate personal and professional traffic will help to prevent crossover. Just 7% of businesses currently use this method, representing a significant missed opportunity to improve end-to-end security[23].

Conclusion: Strengthening your remote working security strategy

As we have seen, effective security for remote working is a three-part process. Your strategy must encompass infrastructure, networking and the devices used by employees to access corporate resources.

The use of personal devices creates a dual challenge. First, you need to address the concerns of employees who may feel that their privacy and autonomy is being violated. Then you have to identify a way to manage and control an ever-expanding network that operates outside your existing controls.

The organic approach to remote working deployment is inherently unsafe and unscalable. In future, businesses will need to strengthen their defenses at every level – data center, network and endpoint. Tools like CASB and Zero Trust are helping to address some of these issues – as are efforts to standardize the applications and tools being used by remote employees.

Looking further forwards, SASE will be crucial, allowing businesses to scale security as their demands change. Adoption is currently very low (approximately 1%[24]), but this is expected to accelerate rapidly as organizations consolidate toolkits to simplify security management and coverage. Security will finally achieve ubiquity, protecting systems and assets consistently, regardless of where they are located. And when this happens, the difference between remote working and office-based operations – from a security standpoint – will be negligible.

Is remote working dissolving your corporate perimeter? Too many urgent tasks and not enough time to action them? Want (and need) EDR but worried about the complexity? Here at Kaspersky we can help tackle these challenges head-on.

Whether you want to strengthen your internal defenses or combat the latest threats with expert external guidance, Kaspersky can help. Our cloud-native Kaspersky Optimum Security lets you upgrade protection against new, unknown and evasive threats, through effective threat detection and response and 24/7 security monitoring, without prohibitive costs or complexity. More visibility. More power. More control.

Learn more at go.kaspersky.com/optimum

Recommended reading:

Machine Learning in Cybersecurity
How to know what level of endpoint protection you need
EDR Buyer's Guide
Boost cybersecurity for remote working teams with system hardening

[1] ISC Cybersecurity Workforce Study 2021 – (ISC)2 – https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx
[2] Business and individual attitudes towards the future of homeworking, UK: April to May 2021 – Office for National Statistics – https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/articles/businessandindividualattitudestowardsthefutureofhomeworkinguk/apriltomay2021
[3] The Flexible Revolution: Are You Ready? – OpenVPN – https://openvpn.net/images/open-vpn-quick-poll/openvpn-remote-workforce-poll.pdf
[4] 2021 Remote Workforce Security Report – Cybersecurity Insiders – https://f.hubspotusercontent10.net/hubfs/8541268/2020_%20Guides/2021-Remote-Workforce-Security-Report-Axiad-Final.pdf
[5] Zoom security issues: Everything that's gone wrong (so far) – Tom's Guide – https://www.tomsguide.com/news/zoom-security-privacy-woes
[6] 2021 Remote Workforce Security Report – Cybersecurity Insiders – https://f.hubspotusercontent10.net/hubfs/8541268/2020_%20Guides/2021-Remote-Workforce-Security-Report-Axiad-Final.pdf
[7] COVID-19 Cybersecurity in the Remote Workforce – PC Matic – https://www.pcmatic.com/news/covid-19/
[8] 2021 Remote Workforce Security Report – Cybersecurity Insiders – https://f.hubspotusercontent10.net/hubfs/8541268/2020_%20Guides/2021-Remote-Workforce-Security-Report-Axiad-Final.pdf
[9] 2020 Data Breach Investigations Report – Verizon – https://enterprise.verizon.com/en-gb/resources/reports/2020-data-breach-investigations-report.pdf
[10] Digital Distancing: Why remote working demands better cybersecurity in a changed world – Computing – https://view.computing.co.uk/carbon-black-digital-distancing/p/1
[11] 2020 Data Breach Investigations Report – Verizon – https://enterprise.verizon.com/en-gb/resources/reports/2020-data-breach-investigations-report.pdf
[12] COVID-19 Cybersecurity in the Remote Workforce – PC Matic – https://www.pcmatic.com/news/covid-19/
[13] Ibid.
[14] Digital Distancing: Why remote working demands better cybersecurity in a changed world – Computing – https://view.computing.co.uk/carbon-black-digital-distancing/p/1
[15] 2021 Remote Workforce Security Report – Cybersecurity Insiders – https://f.hubspotusercontent10.net/hubfs/8541268/2020_%20Guides/2021-Remote-Workforce-Security-Report-Axiad-Final.pdf
[16] People are Working More by Not Going to Work, but Worry about Home Tech, Data Security and Personal Costs – Lenovo – https://news.lenovo.com/pressroom/press-releases/new-lenovo-research-people-are-working-more-by-not-going-to-work-but-worry-about-home-tech-data-security-and-personal-costs/
[17] The Flexible Revolution: Are You Ready? – OpenVPN – https://openvpn.net/images/open-vpn-quick-poll/openvpn-remote-workforce-poll.pdf
[18] 2020 Data Breach Investigations Report – Verizon – https://enterprise.verizon.com/en-gb/resources/reports/2020-data-breach-investigations-report.pdf
[19] 2020 Data Breach Investigations Report – Verizon – https://enterprise.verizon.com/en-gb/resources/reports/2020-data-breach-investigations-report.pdf
[20] Embracing a Zero Trust Security Model – National Security Agency – https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF
[21] Digital Distancing: Why remote working demands better cybersecurity in a changed world – Computing – https://view.computing.co.uk/carbon-black-digital-distancing/p/1
[22] COVID-19 Cybersecurity in the Remote Workforce – PC Matic – https://www.pcmatic.com/news/covid-19/
[23] Ibid.
[24] Hype Cycle for Enterprise Networking, 2020 – Gartner – https://www.gartner.com/en/documents/3987266

www.kaspersky.com

kaspersky BRING ON THE FUTURE