

Safeguarding a post-Covid future

Meeting corporate cybersecurity challenges in the 2020s

Remote working during the pandemic has been a massive success story, with the IT department as its largely unsung heroes. Businesses not dependent on face-to-face interactions have survived and thrived during lockdowns and restrictions, as staff have been able to continue working effectively and securely from home, on their corporate or personal laptops, PCs and other devices.

Adopting home-based working practices has shown a number of benefits, including increased productivity, low levels of absenteeism, improved staff retention and reduced office space costs. So, while for some employees the initial enthusiasm for a fully home-based working life has now worn thin, we can look forward to a future where a 'blended' home/office workstyle may well be the norm.

Kaspersky-commissioned research¹ has found that:

- 74% of employees never want to return to at least some of yesterday's workplace dynamics
- 39% of employees are ready to escape the traditional 9–5 working structure
- 34% no longer want to work at a fixed office desk
- 32% want to rethink the five-day working week

'Cybercrime costs may double due to
Coronavirus outbreak'

[Cybersecurity Ventures](#), July 2020

The cybersecurity story

How has cybersecurity been faring during this dramatic change in working practices? For all the business benefits of remote working, there are downsides. One of these is the increased vulnerability to attack of remotely located and operated endpoints. And, through these, of the whole corporate infrastructure.

In short, cybercriminals have been having a field day.

- Before the pandemic, the FBI's Internet Crime Complaint Center received about 1,000 cybercrime complaints per day. They are now receiving 3,000 to 4,000 per day².
- An Interpol report³ issued in August 2020 has revealed 'an alarming rate of cyberattacks during Covid 19'.
- Phishing scams and remote attacks on employees have been spiking, while home office workers are proving lax about security, according to leading industry magazine Cybersecurity Ventures⁴.

What are the security issues?

- Remote endpoints no longer operate over a corporate LAN. They connect to the internet through domestic routers, or using unsecured Wi-Fi in public places. So they're more vulnerable to man-in-the-middle attacks.
- Corporate devices in the home often double as domestic PCs – used for checking personal emails, pursuing outside interests etc. And, working privately at home rather than in a busy office, employees may be more tempted to visit dodgy and potentially dangerous websites via their business laptop, further exposing the device to cyberthreats.
- If BYOD is being adopted, the risks escalate. Now, the user is also the administrator – you have little or no control over what form of security has been installed on the devices interfacing with your corporate infrastructure, or how they're configured.

¹ [Securing the future of work, Kaspersky, 2020](#)

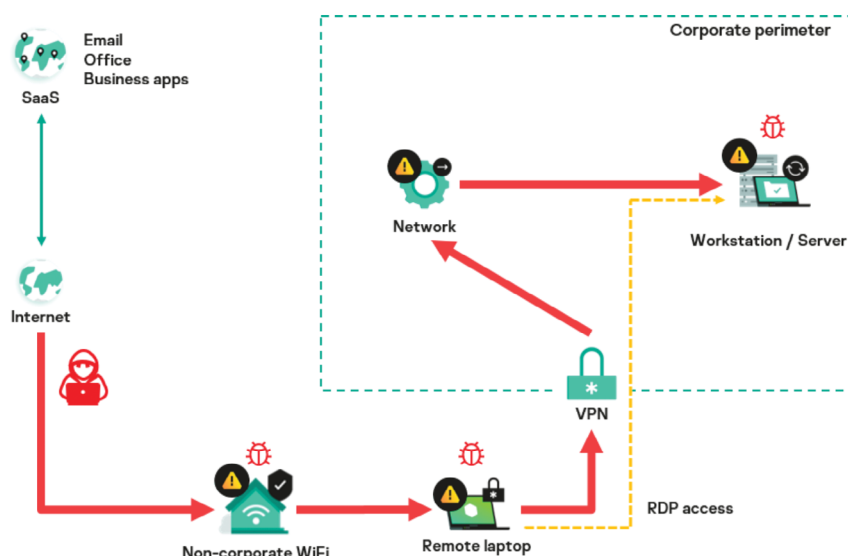
² [Combating Cybercrime During COVID-19, Aspen Digital, 2020](#)

³ [INTERPOL report shows alarming rate of cyberattacks during COVID-19, INTERPOL, August 2020](#)

If an endpoint is compromised, the user can't work, valuable data stored on the device is at risk, and a user's identity can be hijacked to launch attacks on your customers – for example, through their business email account. Even more importantly – if attackers can penetrate your perimeter via a single endpoint, they can start moving laterally throughout your network, embedding and activating malware, and taking command of your systems. This is the standard modus operandi of even the most complex, sophisticated and wide-ranging (and expensive) corporate attacks – initial penetration through just one vulnerable device.

VPNs or RDP provide secure communications between remote endpoints and your network. But these can be compromised. Stolen user credentials – gained through brute force attacks, phishing, or social engineering – are readily available on the dark web to anyone with a few dollars and an interest in attacking you. Or, another example, a RAT (Remote Access Trojan) can be installed on the endpoint without you or the user even knowing.

Any of these entryways can be used to install ransomware, perform illegal financial operations, steal your data – or just gain access to your systems and sell that access online to the highest bidder.



Remember too that, when remotely-based devices are brought into the office and plugged directly into the network, any malware they may have picked up along the way has yet another access route straight into your systems.

The answer

As is so often the case with cybersecurity, the answer lies in a multi-faceted approach employing multi-layered defenses, with a particular emphasis on those vulnerable remote endpoints.

Here are some of the things you can do:

At VPN/RDP level

- **Implement MFA** – Multi-Factor Authentication (e.g. password + security token) – for endpoint access onto the VPN
- **Limit RDP access** only to IP addresses coming from the corporate VPN
- Complicate things for your attacker by **using a non-standard RDP port number** (not 3389)
- Consider **routing all web traffic through your secured proxy server** – assuming you have the resources and capacity which, of course, won't be the case for many.
- **Limit what functionality and applications can be accessed** via the VPN or RDP. The configuration work involved will take time, but should prove well worth it if this approach would be acceptable in your organization.
- **Consider updating your perimeter protection** – email server and web gateway security solutions which block the majority of threats before they can reach endpoint-level are generally a sound investment.

Since the beginning of March, the number of BruteForce.Generic.RDP attacks has rocketed across almost the entire planet⁴

⁴ [Remote spring: the rise of RDP bruteforce attacks, Kaspersky, 2020](#)

Controlling access to websites and applications not relevant to the job in hand has the additional benefit of cutting down on the use of social media, web surfing, online shopping and other time-wasting activities during business hours, and so boosting productivity – often an economic concern where remote working is involved.

At Workstation level

Reduce your attack surface through systems hardening. Limit or ban workstation access to specific websites or block the running of certain applications via 'allow' and 'deny' listing. Or you could consider operating a 'default deny' policy, where only specified work-related and system native applications can be run on the device. This won't make you popular with remote workers whose corporate devices double as personal equipment, but it's a powerful security approach.

Use encryption to protect corporate data. Devices not tied to the office can sometimes go missing, and you need to know that any confidential data they carry has been rendered impenetrable and completely useless to outsiders.

Keep up with patching. It may be mundane – but timely, prioritized patching is absolutely critical. Exploiting vulnerabilities in common applications is still easily the most popular illicit entry point into corporate systems.

Use anomaly control to detect suspicious endpoint activity. Something not quite right? A remote workstation behaving out of character? You need your security solution to be able to spot this automatically and to get onto it fast.

Employ robust detection and remediation tools. It's now widely recognized that EDR (Endpoint Detection and Response), combined with a solid EPP (Endpoint Protection Platform), is fundamental to effective endpoint defenses, especially when talking about evasive cyber-attacks. This needn't eat up a lot of your time – automated detects can in many cases be countered by automated responses. Your team need step in only when your solution detects a serious problem that warrants your attention.

So who's going to do all this?

Employment in the field needs to grow by approximately 89% worldwide, to meet the anticipated demand.⁵

Giving great advice is easier, we know, than implementing it. Particularly when those unsung heroes of the pandemic, the IT professionals and specifically the IT Security professionals needed to undertake all this work, are in such short supply. Many IT Departments are operating below headcount much of the time, simply because recruiting (and retaining) enough IT security staff is such a major challenge.

In a scenario where remote or blended home/office working, with all the additional IT concerns this involves, may well be the future, the cybercrime industry is taking full advantage of the new opportunities being created. So making the very most of your available IT Security staff hours is critical.



Automation

Much of the answer lies in automation. So many of the activities listed above – anomaly control, patching, and other detection and system hardening elements – can be fully or largely automated thanks to developments in machine learning and intelligence. This can even include some of the more advanced processes, like aspects of root cause analysis and response. So your security solution, rather than you and your team, should be doing most of the heavy lifting.

⁵ (ISC)2 Cybersecurity workforce study, (ISC)2, 2020

Integration

Working with one integrated security system is another big time-saver. Deploying a single set of policies across all aspects of the system from a single console is more efficient, as well as reducing risk by leaving less room for administrative error. So think twice before investing in shiny new 'point' products with their own separate consoles – these can eat up time and resources with little to show for it.

Fewer alerts

Chances are your security team also spends a lot of time chasing up routine alerts, when they could be focusing on more dangerous evasive threats. Your choice of foundation EPP will make all the difference here – fundamentals like systems hardening, efficient patching and automated threat prevention all help dramatically reduce the number of alerts your busy team has to deal with. And you have the right to expect a near-zero rate of false positives from your security solution – your team should not be wasting their time on these.

A managed approach

Now may also be a good time to look at a managed security solution. MDR (Managed Detection and Response) is being widely adopted by hard-pressed IT Departments right now. There are a whole raft of benefits to be gained by bringing an expert third party in to manage the most taxing aspects of your security and support your IT Security Team's work. A third party provider should have the bandwidth to offer 24/7 security monitoring, the specialist skills to address tasks like advanced root cause analysis, threat hunting and even guided and remote response scenarios, and the resources and technical expertise on-tap to scale to your growing or fluctuating needs as required. One way and another, employing a reliable third party to support you by taking on some of the load can make for a sound business investment.

A cyber-aware culture

"If remote workers don't immediately self-educate, and if businesses don't immediately provide their employees with security awareness training centered on the home office threat, then we could see global cybercrime damage costs as much as double by the end of this year."

Steve Morgan, founder of [Cybersecurity Ventures](#) and Editor-in-Chief at Cybercrime Magazine

In a corporate culture where users are aware of threats, have the practical skills to avoid compromising the infrastructure due to negligence or a simple lack of knowledge, and practice cyber-hygiene as second nature, wherever they are, IT team workloads naturally decline. Cyber awareness across the board, a culture of cybersafe behavior within the organization, and basic cybersafety skills are key to reducing the attack surface and the number of incidents you need to handle. Organizations often struggle to find the right tools and methods for effective employee training, and creating these from scratch is complex and time-consuming. To achieve a security-aware culture, the right cybersafety training must be deployed – training that employs the latest techniques and technologies for adult education and, most importantly, delivers relevant up-to date content.

A happy, motivated IT department

Security professionals naturally hate wasting their time on boring routine activities, so freeing them up to get on with handling more challenging tasks will increase job satisfaction, resulting in greater levels of retention. Which means you can afford to invest in building up your team's expertise (now they have the bandwidth to attend skills training courses) with less risk of them being poached by others – a true win-win situation.


How we can help

The changes imposed in the information technology (IT) landscape weakened existing cybersecurity measures, turning their speedy adaptation into a challenge. At the same time, cybersecurity is the enabler of trust in emerging use-cases for digital services and thus it has the opportunity to facilitate the transformation.⁶

The most time-saving and cost-efficient approach, whether you choose to go in-house, managed, or both, is generally going to be one of opting for a single supplier – one who can offer a complete multi-layered EPP/EDR platform and more. This also means looking for a solution that can scale with you in the longer term, so you don't have to manage bought-in, bolt-on products with their own consoles and training needs further down the line.

Kaspersky Optimum Security is ready to help your growing IT security team meet and defeat the challenges offered by blended working environments, with scalable, easily managed endpoint protection capabilities.

KASPERSKY OPTIMUM SECURITY




Kaspersky Endpoint Detection and Response Optimum

- Enhanced threat visibility
- Root cause analysis
- Automated response




Kaspersky Managed Detection and Response Optimum

- 24/7 security monitoring
- Automated threat hunting
- Guided and remote response scenarios



Kaspersky Sandbox

- Enhanced automatic detection of evasive threats



Kaspersky Threat Intelligence Portal

- Enriched data for investigation



Kaspersky Security Awareness

- Online training programs for raising employee cybersafety skills

We can offer you a multi-layered endpoint security solution that's highly automated, fully scalable, and based on the reliable foundations of [an award-winning EPP](#), backed by unparalleled MDR expertise, skills and awareness training, and of course our unequalled dedicated support.

⁶ [ENISA Threat landscape - The year in review, European Union Agency for Cybersecurity \(ENISA\), 2020](#)

For more information on how Kaspersky Optimum Security can help you secure your business against evasive threats, please visit: <http://go.kaspersky.com/optimum>.