Checklist: Ransomware protection in the age of flexible working

kaspersky BRING ON THE FUTURE

Ransomware remains a growing threat to any organization, with one estimate suggesting 15.45% of all internet users experienced at least one malware-based attack during 2021[1]. Unsurprisingly, cybersecurity is an increasingly important strategic priority for businesses.

The risk of ransomware infection has increased in recent years, particularly as remote working uptake has accelerated in response to pandemic controls. Research suggests that the rush for remote meant that many organizations have reduced oversight – or relaxed many of their usual security protocols.

When it comes to ransomware, most of the focus is on restoring access to encrypted data as quickly as possible. However, it's worth remembering that cybercriminals will often exfiltrate files for additional blackmail purposes, demanding further payments to prevent sensitive information being leaked.

Fewer businesses deployed network security (down 5%) or end user monitoring tools (down 6%) during 2021[2]. Without effective endpoint monitoring and security, the risk of becoming a ransomware victim increases substantially.

Endpoints have always been a weak link in corporate security, often the easiest attack surfaces available to hackers. But remote working practices have moved those endpoints **outside** the network perimeter, making it even harder to manage and mitigate security. The proliferation of endpoints gives attackers a greater choice of potential targets, further increasing their chances of success.

To prevent a significant ransomware outbreak, an effective ransomware strategy must work on several different levels. As remote working becomes a routine aspect of operations, organizations must refine and strengthen their endpoint protections – particularly in relation to how they detect and block ransomware infections.

This guide acts as a practical checklist, helping you to assess how well-protected you are against ransomware at the network edge – and where you must improve your defenses – including:

- **1. Endpoint ransomware detection**
- **2. Endpoint configuration**
- **3. Backup provisions**
- **4. Offloading operations**
- **5. End user training**
- **6. Incident response planning**

[1] Kaspersky Security Bulletin 2021. Statistics – Kaspersky –https://securelist.com/kaspersky-security-bulletin-2021-statistics/105205/

[2] Cyber Security Breaches Survey 2021 – UK Department for Digital, Culture, Media & Sport – https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021

1. Endpoint ransomware detection

Stopping ransomware before it can proliferate is extremely important. The quicker an infection is identified and blocked, the less damage and disruption it will be able to cause.

Generally, your organization can catch malware that has been emailed directly to employees at the mail server – but this does not stop them being tricked into downloading external executables with a well-crafted spear phishing message.

You can improve your ransomware detection capabilities by blocking suspicious executables at the endpoint:

- **Deploy a robust anti-malware toolkit to identify and remove suspicious executables before they can encrypt sensitive files.**
- **Use the machine learning capabilities of Endpoint Detection and Response (EDR) tools to identify and block suspicious system activity automatically.**
- **Consider adopting a Managed Detection and Response (MDR) solution to automate and accelerate ransomware mitigation efforts.**

Deploying these tools will help to contain an infection, preventing it from spreading to other file stores and systems.

It is worth noting that federal bodies and government agencies are hardening their stance on the way victims respond to ransomware infections. In 2019 the FBI Internet Crime Complaint Center (IC3) urged businesses not to pay ransoms[3].

This advice is echoed by Kaspersky: "Do not pay. Each ransom payment represents a financial contribution to malware development and a signal to the cybercriminals that the scheme is profitable. And it may not work — you may get nothing even if you comply."[4]

The German Federal Office for Information Security (BSI) offers some stark advice, "The best protection against ransom demands from cybercriminals is consistently implemented IT security measures."[5]

Consistently implemented IT measures means maintaining similar endpoint protections **outside** the network perimeter as to those inside – in this case, effective, reliable anti-malware and intelligent EDR tools that can automatically detect ransomware-like activity.

2. Endpoint configuration

Endpoint configuration will also help to reduce the potential effect of a ransomware infection. For corporate-issued devices:

- Use application directory allowlisting to ensure that employees can only run authorized software. With the right restriction in place, they cannot install applications – reducing the chance of running infected executables.
- Ensure that endpoint security tools – and any other installed software – is set to update automatically to block new threats and close potential vulnerabilities before they can be exploited[6].

Security best practice suggests applying software updates within 14 days of release. Unfortunately, just 43% of businesses achieve this goal[7]. Relatively easy to implement, this is a significant missed opportunity to prevent ransomware spread.

[3] High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations – FBI Internet Crime Complaint Center –https://www.ic3.gov/Media/Y2019/PSA191002

[4] Five tips for protecting yourself from ransomware – Kaspersky –https://www.kaspersky.com/blog/ransomware-five-tips/41444/

[5] Ibid.

[6] Ransomware world in 2021: who, how and why – Kaspersky –https://securelist.com/ransomware-world-in-2021/102169/

[7] Cyber Security Breaches Survey 2021 – UK Department for Digital, Culture, Media & Sport – https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021

BYOD endpoints present an additional challenge because your organization can only exert limited control over the device. In this operating model you have a few options:

- Encourage employees to install an approved anti-malware tool on each of their devices. Providing this software free of charge is a good incentive because it will protect the employee's personal data as well as corporate assets.
- Sandbox corporate applications and data so that they are kept separate from personal applications. If an employee accesses malware using their personal applications, the sandbox provides some measure of protection against spread.

Ultimately, protecting personal user devices will be a process of compromise, agreeing to implement measures that are agreeable to company and employee. Where this is not possible, your business will need to consider providing alternative access methods – or supplying employees with owned devices.

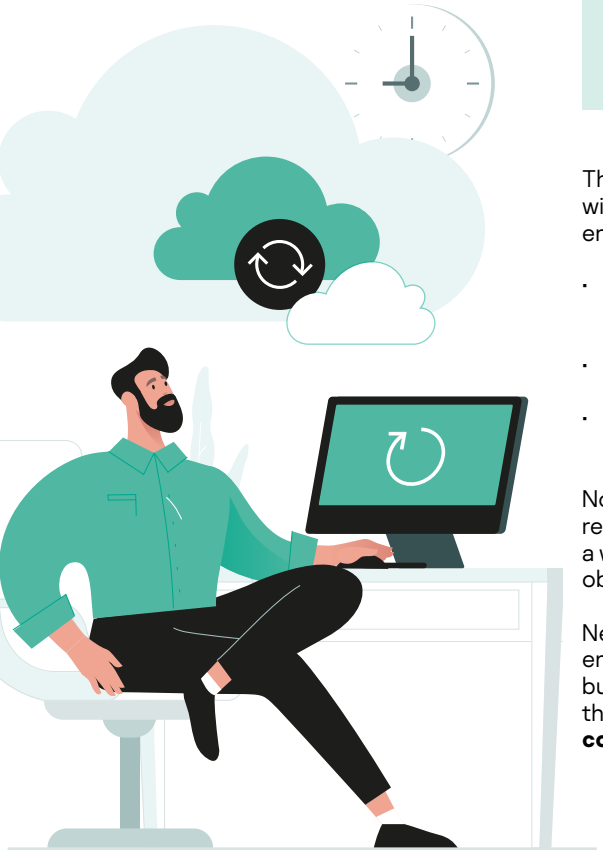
3. Backup provisions

Once files have been encrypted, there are two options: pay the ransom or recover "clean" copies of the files from backup. Which means having a robust, reliable backup routine for your endpoint devices too.

In an ideal deployment, employees would not have the option to store corporate data locally. But the reality is that they probably will save documents to the local drive, often to the Downloads folder or Desktop.

As you prepare for safer remote working you need to consider:

- **How likely is it that corporate data is being stored locally?**
- **What data is being saved?**
- **What are the risks if these files are encrypted or rendered inaccessible?**
- **How can we backup this data?**



This is a significant challenge outside the network perimeter. How you solve the problem will be decided by your technical architecture and, to some degree, the IT abilities of the end user. Options to consider include:

- Synchronizing data in selected folders to cloud storage or other remote service – preferably with immutable backups that cannot be overwritten or amended.
- Backing up to a local removable drive.
- Relying on functionality built into the operating system to create automated shadow copies and rollback points.

None of these potential solutions is ideal because there is the inherent threat of replicating ransomware and encrypted files into the backup. However, you must identify a way to capture locally stored data, not least to meet compliance and data protection obligations.

Never forget –data backup is your very last line of defense against ransomware-encrypted files. Also bear in mind that backup and recovery will not protect your business against data leaks – or doxxing. Criminals may still demand a ransom under threat of exposing sensitive information. The only defense against these attacks against **confidentiality** is to prevent criminals from accessing your endpoints.

4. Offloading operations

The more data and applications held on an endpoint device, the more potential vulnerabilities there are to exploit. And the more attractive that machine becomes to hackers. So by **reducing** the amount of applications and data held locally, the less impact a ransomware infection will have.

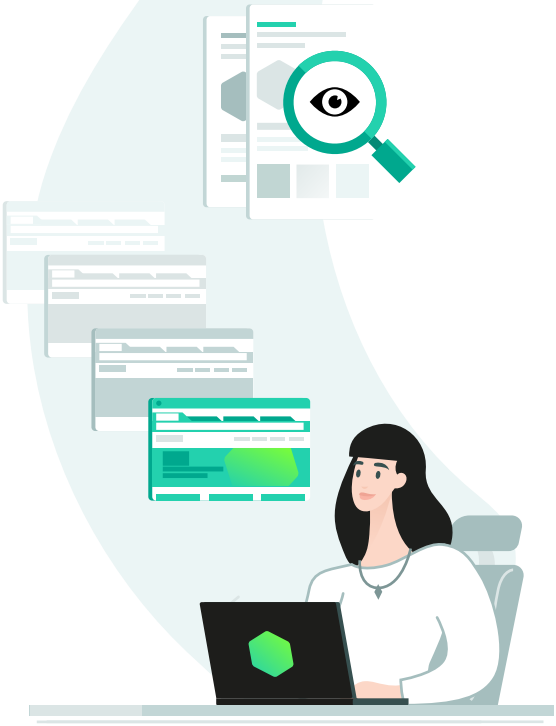
Cloud services have provided a way to offload applications, minimizing the amount of data that is stored on the local device. Email and productivity tools can now be run as web apps in the cloud for instance, ensuring that little or nothing is transferred locally. Many, particularly email services, will also offer advanced malware protection to scan, detect and block suspicious attachments before your users can download them.

Virtualization offers another possibility. Using application and desktop streaming, users can connect to a session hosted in the corporate data center or cloud. The hosted session provides a desktop-like session for the end user – but again, all data and processing is completed inside the virtualized system.

Remote desktop sessions (RDP) are regarded as the single biggest attack vector for ransomware[8]. But when configured correctly, this creates a useful sandbox between the endpoint device and corporate systems – as is evidenced by the extensive use of RDP inside the corporate network.

It is possible to realize the same benefits for remote workers by tightening endpoint security, namely:

- **Enforcing a strong password policy to prevent brute force attacks.**
- **Deploying multi-factor authentication to prevent sessions being hijacked.**
- **Using VPN connections for all traffic between endpoint and RDP servers.**
- **Assessing and tightening network perimeter firewall rules to prevent unauthorized connections.**
- **Using EDR security tools to assess activity to automatically identify and block suspicious activity.**
- **Choosing non-standard RDP connection ports to avoid speculative hacking attempts.**



Ultimately, the key is preventing hackers and malware compromising the RDP connection and session – which means properly securing the user's endpoint.

5. End user training

Employees are the most valuable assets of any business, and they can play an important role in preventing the spread of ransomware – if they know what to do. All employees, not just those working remotely, should receive regular training so they are equipped to identify potential cybersecurity attacks – and what they need to do next. Every day, 2% of employees will click on a phishing link[9] – and we can expect similar figures with regards to ransomware.

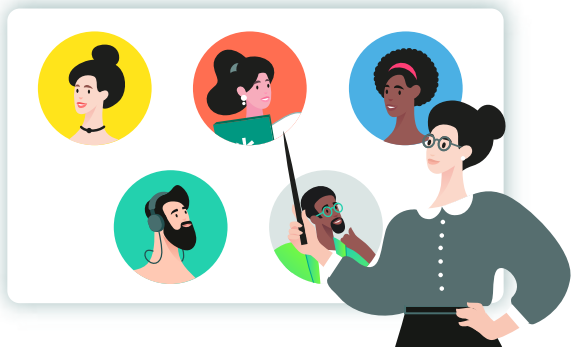
Training needs to be interactive, practical and regular – cybersecurity threats are constantly evolving after all. A one-off presentation about identifying phishing emails and suspicious executables will quickly date (and be forgotten). Here are some factors to consider as you design cybersecurity training for your remote workers.

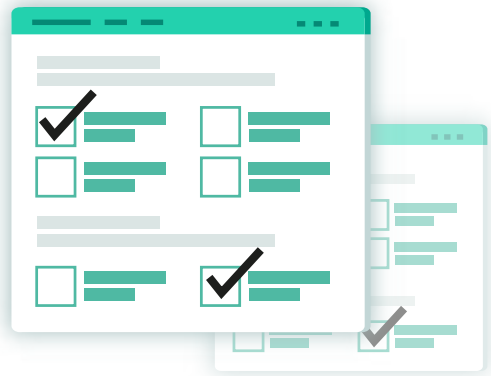
[8] How to secure RDP from ransomware attackers – Emsisoft –https://blog.emsisoft.com/en/36601/how-to-secure-rdp-from-ransomware-attackers/

[9] Mobile Security Index 2020 Report – Verizon – https://www.verizon.com/business/en-gb/resources/reports/mobile-security-index/2020/mobile-threat-landscape/user-threats/

Tailor the training

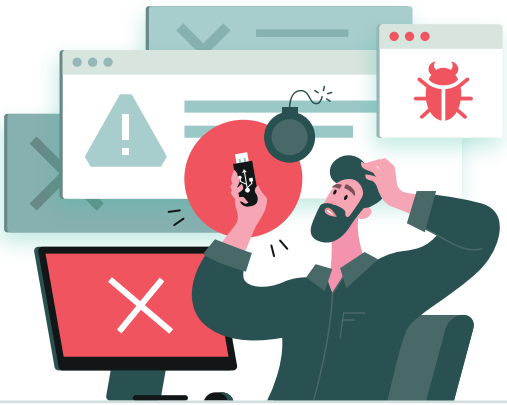
The most effective ransomware attacks are carefully targeted to specific people and roles. It makes sense then to tailor training in the same way. Finance, marketing, HR and executives will all face slightly different attacks, so training them in their own "language" about the threats they are likely to face will be of greater value to them – and more effective to the business too.





Test your employees

Knowledge is of little value until it is put into action – especially when the stakes are so high. Routine, regular testing ensures that your employees can put their training into practice when required. Routine assessments will also highlight knowledge gaps or opportunities to further improve their skills and the security posture of your business.



Go beyond phishing

Phishing and malicious attachments are the most obvious potential source of ransomware infection. However, there are other factors that your end users need to be aware of. Infected removable drives, malicious websites and cross-contamination between work and personal activity can all introduce malware onto the endpoint – and the wider corporate network. You must ensure employees are trained to be aware of these potential issues too.

Make it fun (and/or interesting)

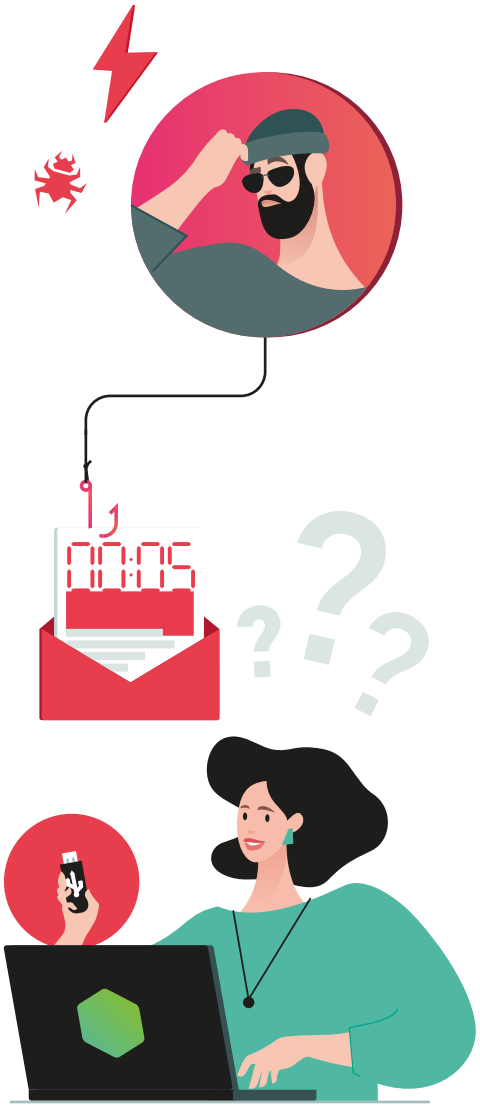
Cybersecurity can be dry and boring, particularly if it is not your core responsibility – it is highly unlikely your end users will read (or understand) weekly briefings from the US National Cyber Awareness System for instance. Using gamification will help to increase interest and engagement, particularly as the concepts being taught get harder. Setting goals and challenges, encouraging competition and making the process fun will encourage employees to stay connected – and to keep improving their knowledge and abilities.

Investing in your end users is an important step towards strengthening the defense of your endpoints. Indeed, minimizing human error is perhaps the most effective form of ransomware prevention. It will also help your employees to play an effective role in the very early stages of a ransomware infection, helping to minimize spread and overall impact on the business.

6. Incident response planning

An astonishing 32% of businesses do not have a formal incident response plan for dealing with cybersecurity incidents like a ransomware outbreak[10]. These organizations are assuming an unjustifiable level of risk because they will all encounter a malware incident at some point in the foreseeable future.

Building an incident response plan will help your business assess vulnerabilities and take appropriate steps to mitigate them. The plan will also help to accelerate your response – critical when dealing with ransomware where every second counts.



Although unique to your organization, every endpoint disaster recovery (DR) plan should include:

- **A communication strategy.** You need to make sure that the right information reaches the right stakeholder at the right time. And that your remote workers are able to connect to experts who can help them in the earliest stages of an infection.
- **A plan of attack.** Decide how the severity of an attack is determined and how you will respond. Will you pay the ransom, or try and recover data from backup?
- **Accessible documentation.** There is a very high probability that an endpoint infection will prevent employees accessing ransomware response playbooks or instructions. You must ensure that there is always a way to get this information, even if their systems are down.
- **Employee guidance.** As soon as an issue is detected, you should assign a specialist who can assist the remote worker. They can talk them through initial mitigation and recovery efforts, and also collect information to include in the report to regulators if the situation demands it.
- **Enhanced vigilance.** As soon as a ransomware infection is detected on a remote endpoint, your IT security team must increase levels of monitoring and reporting to assess whether central systems have also been compromised. They can then trigger the main disaster recovery plan if required.

With a well-designed disaster recovery plan, your business is better positioned to reduce malware impact – ideally containing spread long before it reaches critical systems and data.

[10] Cyber Security Breaches Survey 2021 – UK Department for Digital, Culture, Media & Sport – https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021

Conclusion

IT executives have had concerns about remote working for many years – and rightly so. However, recent events have changed operations forever, and remote working is now a standard aspect of business.

At the same time, ransomware has become a standard tool in the cybercriminal's kit. Attacks against organizations are frequent, effective and potentially devastating. With additional attack surfaces provided by remote workers, it is extremely likely that every business will be affected eventually.

Protecting endpoints against ransomware should therefore be a strategic priority. Otherwise, it may be too late for your business to respond effectively when the inevitable does happen.

The six factors outlined in this paper will immediately help your business to better ready itself for when the ransomware arrives. Addressing these factors will immediately improve your endpoint security posture:

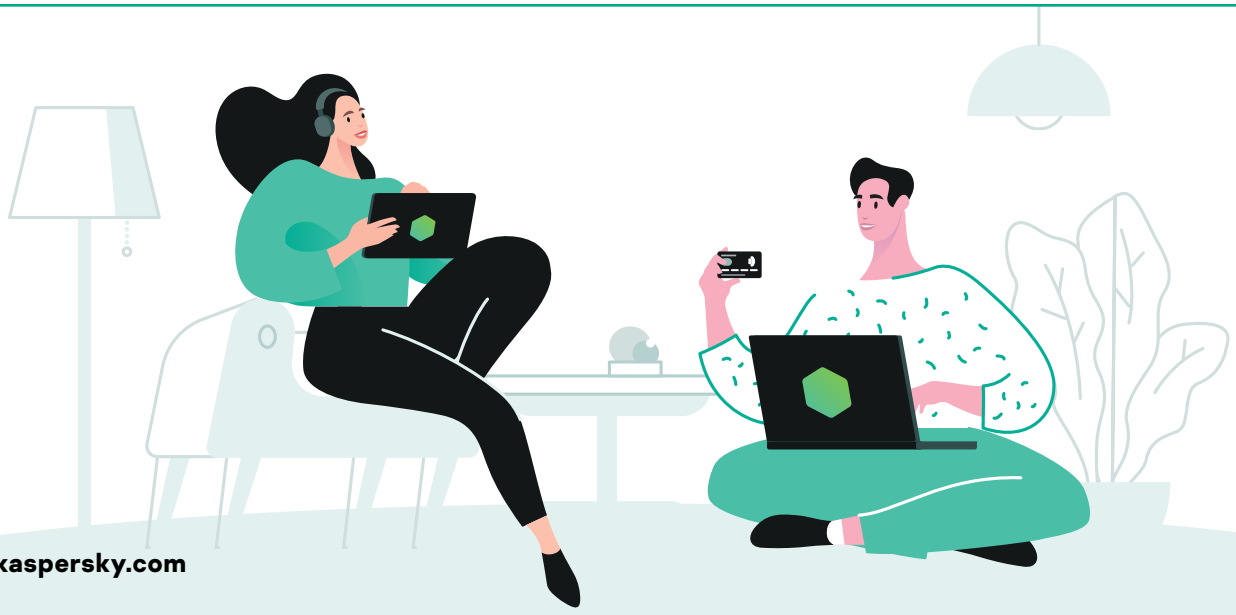
1. Malware detection and removal
2. Device configuration
3. Data backup and recovery
4. Offloading operations
5. Training
6. DR planning

If you would like to learn more about protecting remote workers –and the rest of your organization –against ransomware, 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:

The story of the year: ransomware in the headlines
How to know what level of endpoint protection you need
EDR Buyer's Guide
Boost cybersecurity for remote working teams with system hardening



www.kaspersky.com

kaspersky BRING ON THE FUTURE