How to Stem the Flow of **Ransomware**

(and other Threats)

Executive summary

Ransomware is not new, but the scale of attacks has grown both in frequency and sophistication over recent years. During the COVID-19 pandemic, ransomware attacks doubled in June 2020 over the previous month, and in 2021 the UK National Cybersecurity Centre reported that “Ransomware became the most significant cyber threat facing the UK”.

Cybercriminals have become more organised, using “Ransomware-as-a-Service” with pre-developed ransomware tools to launch their attacks, enabling an increase in the number of attacks as well as in amounts demanded, up to £31 million on average, according to **research by IBM**. With increased awareness of ransomware following attacks on Colonial Pipeline in the US and the Health Service Executive in Ireland, **for example**, and the increased demands of cybercriminals, what can your company or organisation do to stem the tide of ransomware attacks, whilst still keeping data flowing into and across your business?

Preventing ransomware by taking different approaches to reduce the potential for an attack is preferable to submitting to the demands of cybercriminals which can bring even bigger financial and reputational loss. In this ebook, we will look at the steps you can take to keep ransomware at bay.

Whilst ransomware is extremely difficult to prevent, a multi-faceted approach - via software, IT and business processes, and employee awareness – is possible and will help you to put the right controls in place.

The impact of ransomware on all types of organisations

Ransomware is a threat to both SMBs and larger organisations. A type of malware, ransomware has been a threat since the 1980s but, in recent years, attacks have grown in number and sophistication. During the Covid-19 pandemic, there was a significant step up in cyber-criminal activity, taking advantage of remote workers away from the support of their IT departments.

What is ransomware?

Ransomware is a type of malware that makes data and business systems unusable. It can infiltrate a company via **phishing emails** or **vulnerabilities** in an organisation's network or software. Once the ransomware is installed on a network data is stolen, deleted or encrypted. A ransom (often in cryptocurrency) is demanded before the ransomware is removed or deactivated.

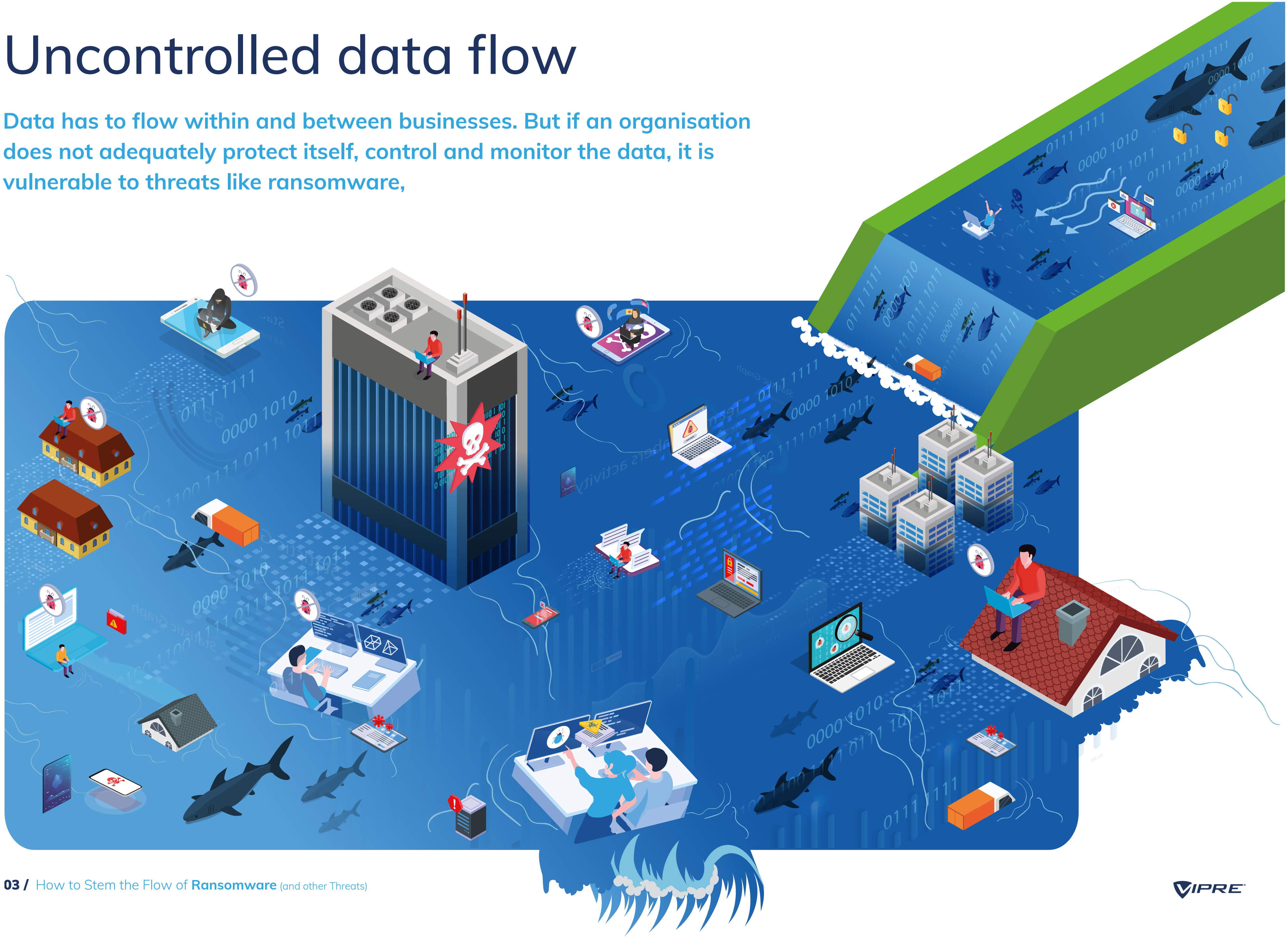
If your organisation pays a ransom, there is no guarantee that your data will be un-encrypted or returned, and, if the data is stolen, it may still be leaked.

The availability of platforms for cybercriminals, such as Ransomware-as-a-Service and other subscription-based services, make it even easier for them to launch an attack. In addition, more sophisticated methods are being employed, for example, fileless attacks which exploit the tools and features in a network environment, alongside well-known social engineering tactics, such as phishing emails and spear-phishing attacks.

Ransomware is extremely difficult to prevent. It only takes one employee clicking on the wrong link in an email or downloading a malicious attachment for ransomware to take your business hostage. The result of ransomware attacks can be devastating, no matter the size or type of your organisation. Ransomware can inflict financial damage, not just through potential ransom demands, but also through loss of system downtime, loss of productivity, loss of data, and loss of business reputation in the longer term. With our reliance on large amounts of data, which need protecting, and with data flowing into and out of the organisation, across offices, sites, and to remote workers, setting up controls to help prevent and contain ransomware attacks, is the best course of action. Without controls in place and adequate data protection, your business could be swamped by a deluge of cyberattacks...

Uncontrolled data flow

Data has to flow within and between businesses. But if an organisation does not adequately protect itself, control and monitor the data, it is vulnerable to threats like ransomware,



Solutions for security and data control

Prevention of potential attacks is always preferable to the cure. As the United States' President, Joe Biden, highlighted in his 2021 letter to business leaders around ransomware: "*... companies that view ransomware as a threat to their core business operations, rather than a simple risk of data theft will react and recover more effectively.*"

> "The most important takeaway from the recent spate of ransomware attacks on U.S., Irish, German and other organizations around the world is that companies that view ransomware as a threat to their core business operations, rather than a simple risk of data theft will react and recover more effectively."
>
> **Joe Biden,**
> **US President in his 2021 letter to business leaders.**

Containment and damage limitation are important right from the outset.

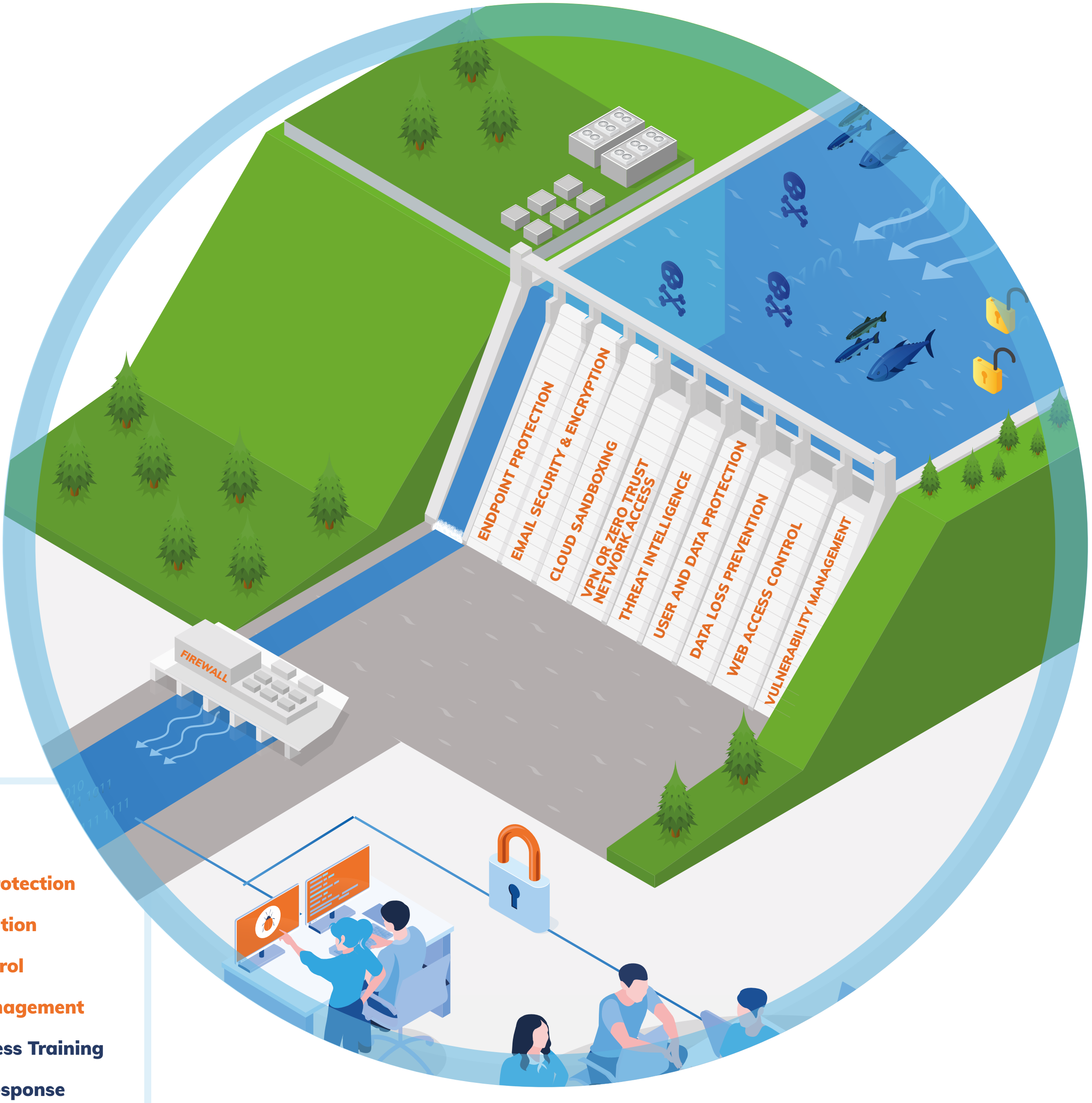
Without controls in place, the flow of data into an organisation can be likened to an uncontrollable river. To mitigate risk the river needs to be dammed into a manageable stream or small pipe of water coming into and out of the organisation. Building the dam starts from the bottom, ensuring that you have the right foundations in place, such as firewalls and gateways, onto which you can add endpoint and email security, for example. By building a dam brick by brick, with the right building blocks, you can advance from fighting off the full flow of water wearing just a wetsuit, to controlling the stream and plugging the remaining small trickle of water simply by putting a finger over the pipe.

Putting the dam in place, with security tools and other technology, enables you to have control over your data and your full IT environment. The remaining data and threats that come through can then be stopped more easily by human intervention, through employee awareness training and, just in case the very worst happens, through a pre-prepared ransomware response plan.

Solutions for security and data control

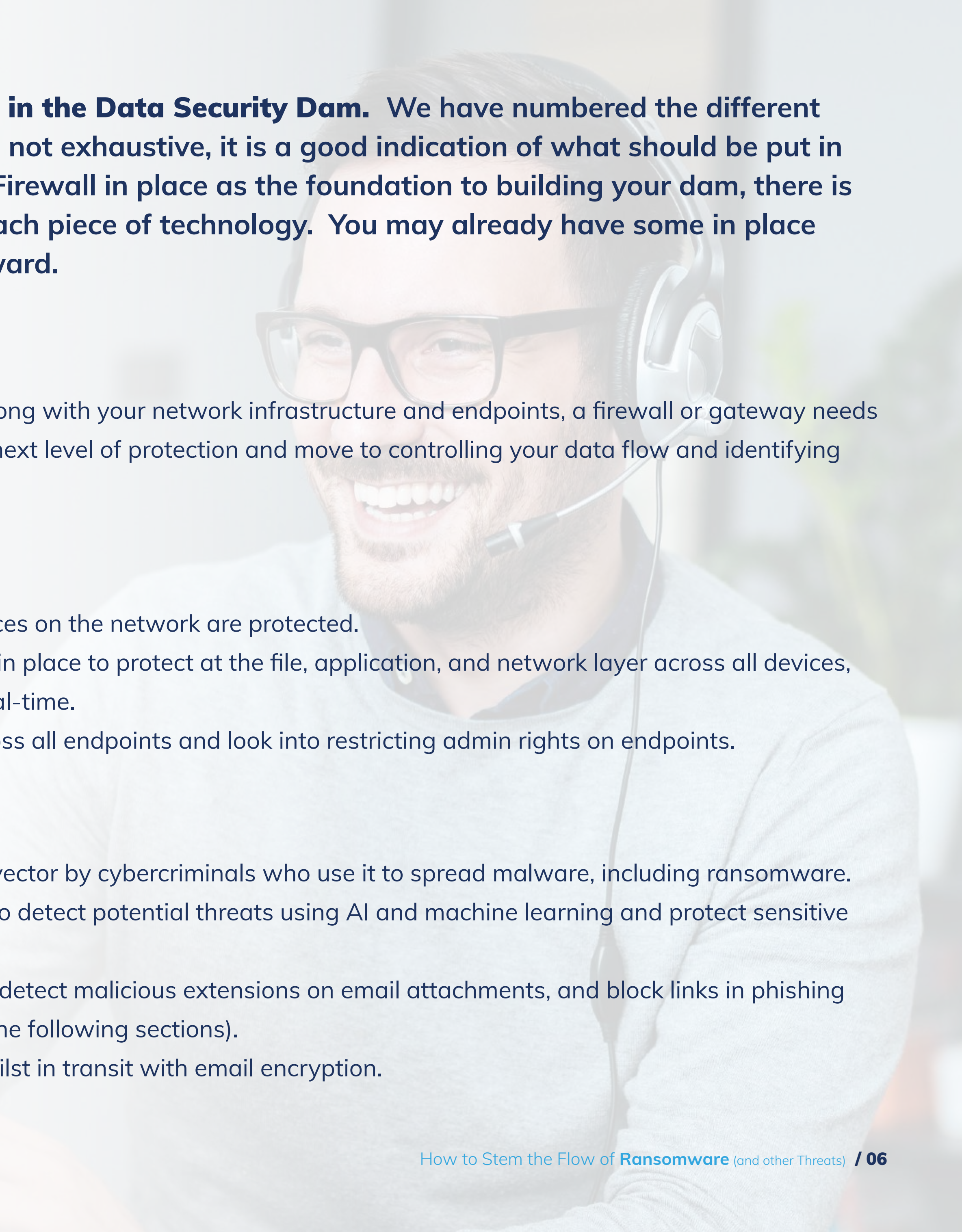
The correct combination of technologies to deliver performance and cyber security

By ensuring you have the right technology in place, you can control and monitor the flow of data into and out of your organisation. The smaller the stream of uncontrolled data, the easier it is to manage, and, whilst ransomware might still infiltrate via emails or slip through technology barriers, the threat can still be stemmed through a well-trained and alert workforce, or, in the worse case scenario, managed with a solid ransomware recovery plan.



KEY

01. Firewall
02. Endpoint Protection
03. Email Security & Encryption
04. Cloud Sandboxing
05. VPN or Zero Trust Network Access
06. Threat Intelligence
07. User and Data Protection
08. Data Loss Prevention
09. Web Access Control
10. Vulnerability Management
11. Security Awareness Training
12. Ransomware Response



Let's take a look at the different controls available in the Data Security Dam. We have numbered the different building blocks for convenience, and whilst this list is not exhaustive, it is a good indication of what should be put in place. Apart from always ensuring that you have a Firewall in place as the foundation to building your dam, there is no particular order in which you should implement each piece of technology. You may already have some in place and just need to improve by adding to it moving forward.

01.

Firewall

The foundation of building data protection, along with your network infrastructure and endpoints, a firewall or gateway needs to be in place before you can move on to the next level of protection and move to controlling your data flow and identifying potential threats.

02.

Endpoint Protection

The logical next step is to ensure that all devices on the network are protected.

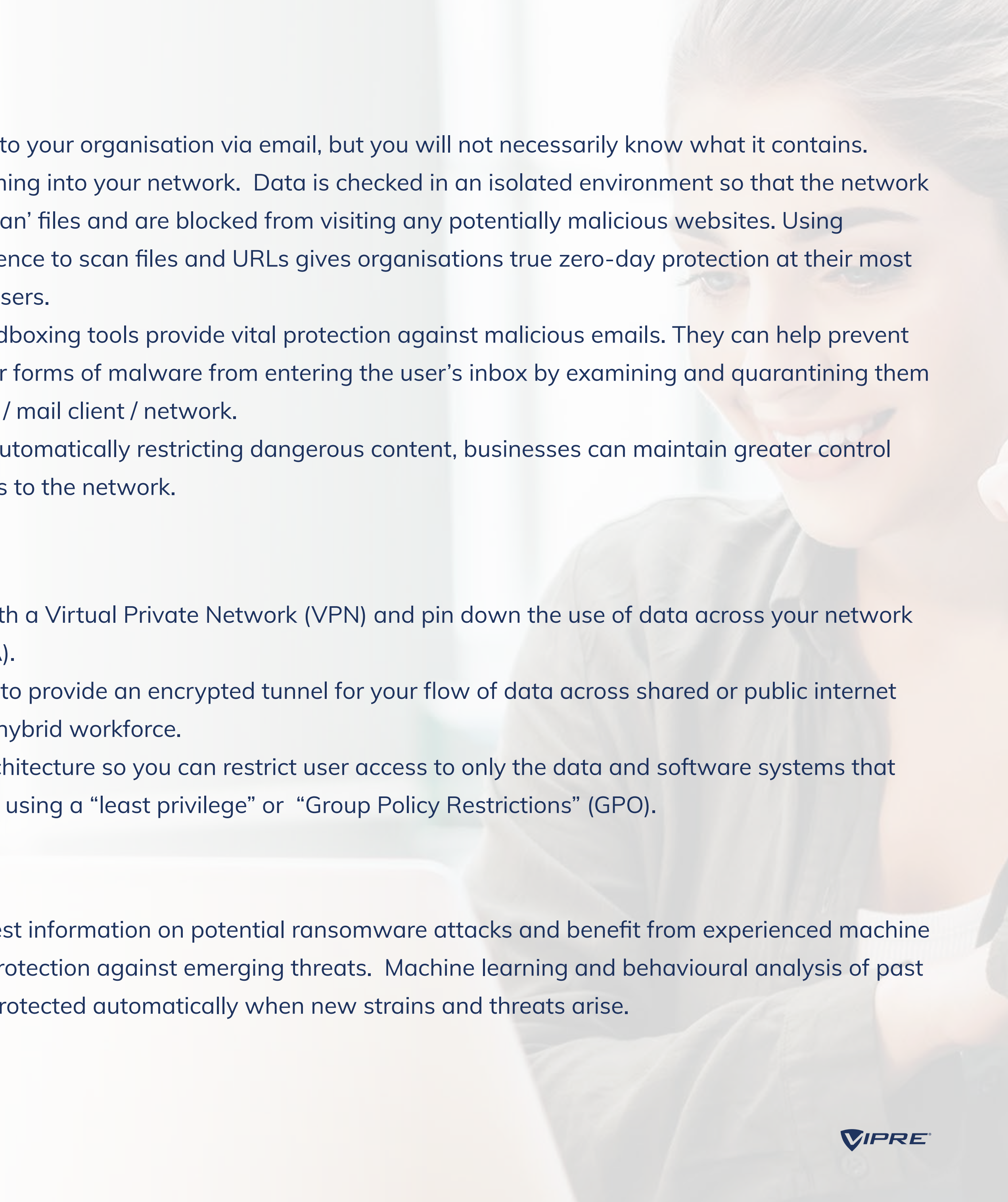
- ✓ Secure endpoint protection should be in place to protect at the file, application, and network layer across all devices, and to respond to security alerts in real-time.
- ✓ Install endpoint security software across all endpoints and look into restricting admin rights on endpoints.

03.

Email Security and Encryption

Email is the most commonly exploited threat vector by cybercriminals who use it to spread malware, including ransomware. An additional layer of security can be added to detect potential threats using AI and machine learning and protect sensitive emails via encryption.

- ✓ Scan emails for viruses and malware, detect malicious extensions on email attachments, and block links in phishing emails. (We will explore this more in the following sections).
- ✓ Protect private and customer data whilst in transit with email encryption.



04.

Cloud Sandboxing – files and links

You will still have data coming through to your organisation via email, but you will not necessarily know what it contains. Sandboxing checks the data that is coming into your network. Data is checked in an isolated environment so that the network is protected, and, users only receive 'clean' files and are blocked from visiting any potentially malicious websites. Using behavioural analysis and threat intelligence to scan files and URLs gives organisations true zero-day protection at their most vulnerable point - emails coming in to users.

- ✓ Email attachment and URL sandboxing tools provide vital protection against malicious emails. They can help prevent dangerous links, attachments, or forms of malware from entering the user's inbox by examining and quarantining them before they even get to the user / mail client / network.
- ✓ By filtering out this traffic and automatically restricting dangerous content, businesses can maintain greater control over email and the access points to the network.

05.

VPN or Zero Trust Network Access

Put a security ring around your data with a Virtual Private Network (VPN) and pin down the use of data across your network with Zero Trust Network Access (ZTNA).

- ✓ Implement a VPN or equivalent to provide an encrypted tunnel for your flow of data across shared or public internet networks – key for protecting a hybrid workforce.
- ✓ Adopt a Zero Trust Network Architecture so you can restrict user access to only the data and software systems that they need to carry out their role, using a "least privilege" or "Group Policy Restrictions" (GPO).

06.

Threat Intelligence

Make sure you are plugged into the latest information on potential ransomware attacks and benefit from experienced machine learning and behavioural analysis for protection against emerging threats. Machine learning and behavioural analysis of past and present malware, means you are protected automatically when new strains and threats arise.

07.

User and Data Protection Tools

Empower your users with tools to help them protect your organisation's data from inadvertent distribution inside and outside of the organisation.

- ✓ Enable users to check and confirm their emails are being sent out to the right person.
- ✓ Alert users at the point of potential data leakage if there is sensitive data in the email and attachment they want to send.

08.

Data Loss Prevention

In our unprotected large river of data, it is hard to capture one specific piece of data that might be moving upstream. Sensitive data moving across and out of the organisation can be detected with Data Loss Prevention tools.

- ✓ DLP tools can be used to detect confidential or sensitive information that might be sent inadvertently by users or stored on inappropriate devices, either at the gateway or at the point of potential leakage (the user).
- ✓ Set up policies to detect data such as credit card numbers, bank account details and national insurance numbers which may be sent via email, for example.

09.

Web Access Control

Web Access Control tools reduce the risk of users accessing inappropriate or malicious websites.

- ✓ Stop inadvertent download of potentially bad software and access to malicious URLs.
- ✓ Controls can also be used to remove online distractions for employees during work hours.

10.

Vulnerability Management

Use Vulnerability Management tools to regularly monitor your network, operating systems and applications for potential weak points.

- ✓ Vulnerability Management tools can be used to scan all types of assets connected to a network, including servers, desktops, laptops, virtual machines, containers, firewalls, switches, and printers.
- ✓ Regular scanning will reveal weak points, such as outdated software which requires patching, open ports and other vulnerabilities.

11.

Security Awareness Training

As you build the different component pieces of your Data Security Dam, the remaining data flow is controlled and stopped by the IT team and data gatekeepers, but this can never eliminate every threat and can sometimes overwhelm these data gatekeepers.

- ✓ With phishing being the most common entrance mechanism for ransomware, users are the last line of defence. Everyone needs to think twice about clicking a link in an email or on a website. Even with technology controls in place and the flow of data controlled, users need to be kept aware of the dangers.
- ✓ Ensure that you have regular cybersecurity awareness training in place for all your employees. Don't settle for once-a-year training...people forget.
- ✓ Conduct phishing penetration tests on a regular basis to check if your employees are able to identify phishing emails and to measure the success of your security awareness training.

> ***See our Help Stop Ransomware Quick Reference Guide at the end of this document for useful tips to share with employees.***

> ***Read The Next Generation Human Firewall White Paper for more about improving security awareness.***

12.

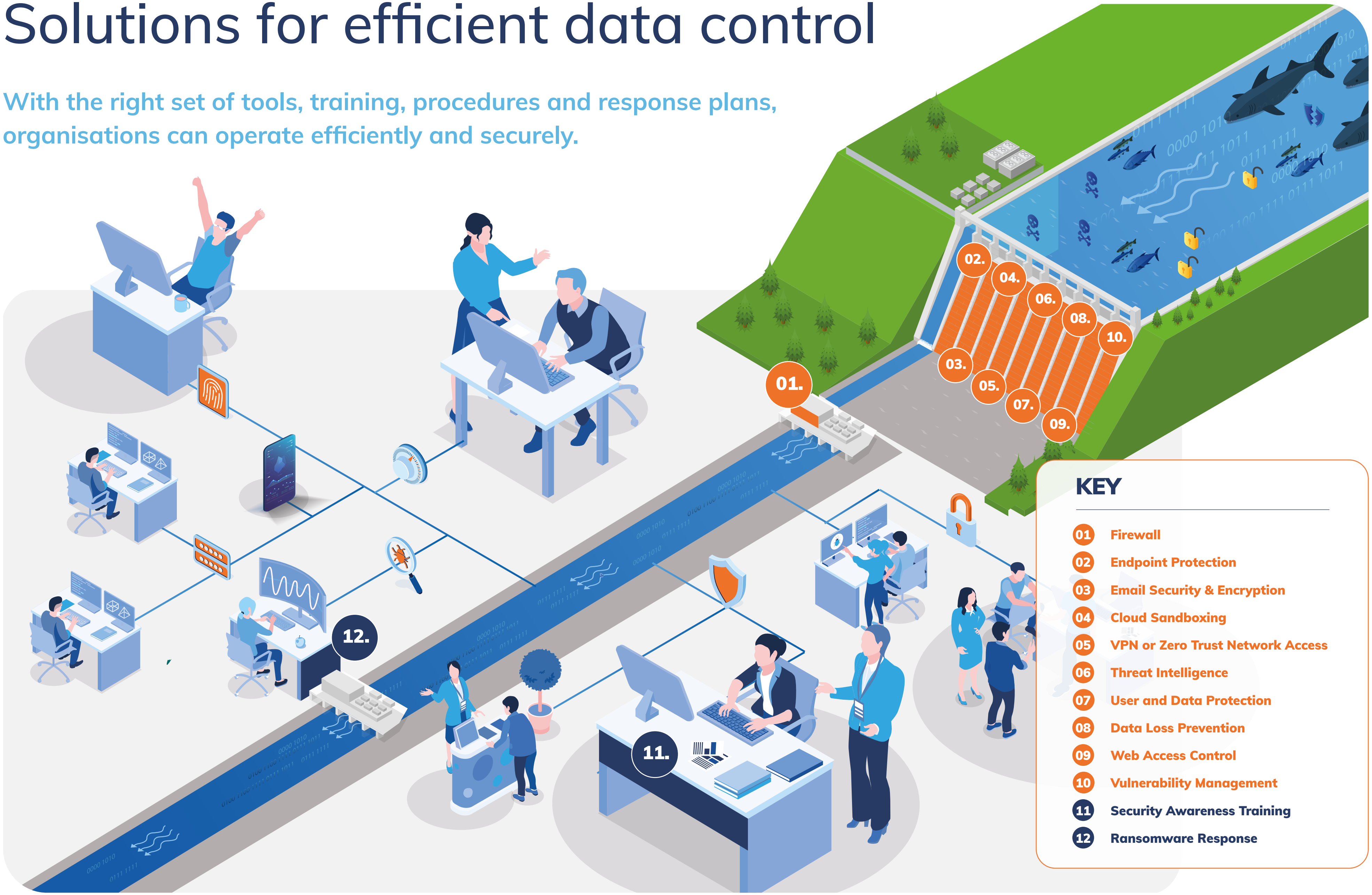
Ransomware Response

Should the worst still happen, be prepared with a ransomware response.

- ✓ Ensure you have a detailed disaster recovery plan in place and regular backups to ensure business continuity.
- ✓ Conduct a retrospective audit of what happened, once the threat has passed.
- ✓ Share your findings so that other companies can learn from your experience and regain the confidence of your customers, clients or patients.

Solutions for efficient data control

With the right set of tools, training, procedures and response plans, organisations can operate efficiently and securely.



KEY

01	Firewall
02	Endpoint Protection
03	Email Security & Encryption
04	Cloud Sandboxing
05	VPN or Zero Trust Network Access
06	Threat Intelligence
07	User and Data Protection
08	Data Loss Prevention
09	Web Access Control
10	Vulnerability Management
11	Security Awareness Training
12	Ransomware Response

Conclusion

Ransomware is becoming ever more sophisticated, morphing to infiltrate many different types of environments, but the good news is that there are steps that you can take to reduce the risk of ransomware attacks to your business.

Constructing a technology barrier or Data Security Dam will enable you to reduce vulnerabilities across your IT infrastructure, help protect all endpoints, reduce the risk of threats from malicious websites and emails, enable you and your users to monitor the information being sent out and coming in.

By implementing the right technology you can reduce the flow of uncontrolled information into your business. Any data, coming in via the digital sluice gate, can be controlled and managed more easily by your IT team and, with security awareness training and the right tools your users will be able to spot suspicious emails and other security threats.

Prevention is definitely better than the cure, but should the worst happen, you will have a ransomware response plan in place for business continuity and minimised the impact of data loss for your customers or patients.

Further reading...

>
See our Help Stop Ransomware Quick Reference Guide at the end of this document for useful tips.

>
Read The Next Generation Human Firewall White Paper for more about improving security awareness.

Quick Reference - Help Stop Ransomware

What is ransomware?

Ransomware is a type of **malware** than can **hijack the data** on your computer or on your company's network. In return for recovering the data, cyber criminals ask for a **ransom to be paid**.

A ransomware attack can be devastating for organisations, with computer systems no longer available and data irrecoverable or taking several weeks to recover. In addition, an attack can have a negative, long-term impact on your organisation's reputation and brand.

How can I help prevent ransomware attacks?

Even though your IT department will have taken steps to ensure the threat of ransomware is reduced as much as possible through the use of technology solutions, these can **never be 100% effective.**

Cybercriminals play on human nature, with phishing emails being one of the most common methods of infiltrating and infecting computer systems organisation-wide. But phishing is not the only method of attack.

Beware of:

01 **Infected websites** – these may have been designed to look like a familiar website. Do not click on banner ads, which are a favourite with cybercriminals for delivering different types of malware, including ransomware.

02 **Downloads** – from websites and emails can also lead to malware and ransomware infections. Ensure you are expecting the attachment in an email and it is from a trustworthy source and make sure you trust the website if you are going to download anything from it. If in doubt, contact your IT Department.

03 **Phishing emails** – claiming to be from a colleague, your boss, a familiar supplier or delivery company, for example. If ANYTHING seems out of place, question it, we are all busy and can fall prey to the urgent wording in a phishing or spear-phishing email, but if you are aware of what to look out for, the attack will be less likely to succeed.

Quick Reference - Help Stop Ransomware (Contd.)

How to spot a phishing email?

Here are a few questions you should ask yourself when receiving an email, to make sure you do not fall for a potential ransomware attack:

1) **Is the email a strange request?** Even if the email looks like it is coming from someone or an organisation you know, is the request urgent, or something that they would not normally ask?
2) **Have you unexpectedly won a substantial amount of money?**
3) **Is the email scaremongering to get you to open it or click on a link?**
4) **Do you know the sender?** If you have not been addressed personally in the email, the chances are that the sender does not know you.
5) **Bad grammar and spelling?** If the email itself does not appear right, with lots of spelling mistakes and incorrect grammar, chances are high that it is a phishing email.
6) **Does the email contain a link or a file to download?** Beware of links and attachments. If you are in any doubt, it is best not to open.
7) **Do you recognize the email address?** Even if you do recognise the sender, be careful and check that the "From" email address actually tallies with the email address you would expect from that person or company.

What should I do if ransomware does infect my workstation or laptop?

If you do receive a message on your screen saying that your files are encrypted and requesting you to pay within a specific number of hours, ***what should you do?***

01 **DO NOT** shut down your computer, otherwise data may be lost

02 **DO** immediately unplug your network cable and/or DO shut off your WiFi connection,

03 **DO** contact IT support immediately.

With your help, we can reduce the risk of ransomware attacks.

VIPRE

For more information on how VIPRE can help protect your organisation and users from ransomware, get in touch with a member of the VIPRE team.

se.sales@VIPRE.com / +46 8-5000 94 20