THE RANSOMWARE SURVIVAL GUIDE

PRAGMATIC PROTECTION FOR YOUR BUSINESS



BE THE MASTER OF YOUR DOMAIN

Welcome to the ultimate survival guide for navigating the digital wilderness, safeguarding your valuable data in the cloud, and securing your digital future.

Cyber threats can happen quite unexpectedly, and ransomware attackers are the stealthy predators that you must outsmart to safeguard your data and assets.

Let's explore the steps you can take to fortify your defences and ensure resilience in the face of ransomware attacks.

Ransomware has emerged as a widely discussed and extensively publicised security threat in the modern era.

It all began with a few high-profile attacks caused by a limited number of malware variants, but it has now evolved into a pervasive threat landscape, where even less skilled attackers can execute highly effective ransomware campaigns against organisations of all sizes and complexities.

There are several steps that businesses can take to protect themselves from ransomware attacks. These include:

1. ***Disaster recovery as a service (DRaaS):*** DRaaS allows you to quickly and easily restore your data during a ransomware attack.
2. ***Understanding what assets are valuable to your company***: Understand what data is most critical to your operations and take proper steps to protect that data.
3. ***Encrypting valuable data assets:*** Encrypting valuable data makes it much more difficult for attackers to access.
4. ***Using anti-virus software:*** Anti-virus software can help to protect businesses from ransomware attacks by detecting and blocking malicious files.
5. ***Implementing multifactor authentication (MFA)***: MFA adds an extra layer of security to user accounts, making it more difficult for attackers to gain access.
6. ***Using Cybersecurity as a Service (CSaaS):*** CSaaS providers can help businesses to implement and manage a comprehensive cyber security program.
7. ***Security Fortification:*** Configure and secure servers to make them more resistant to attacks. This involves implementing a variety of security measures, such as:
    - Patching software vulnerabilities
    - Disabling unnecessary services
    - Changing default passwords
    - Implementing strong security policies

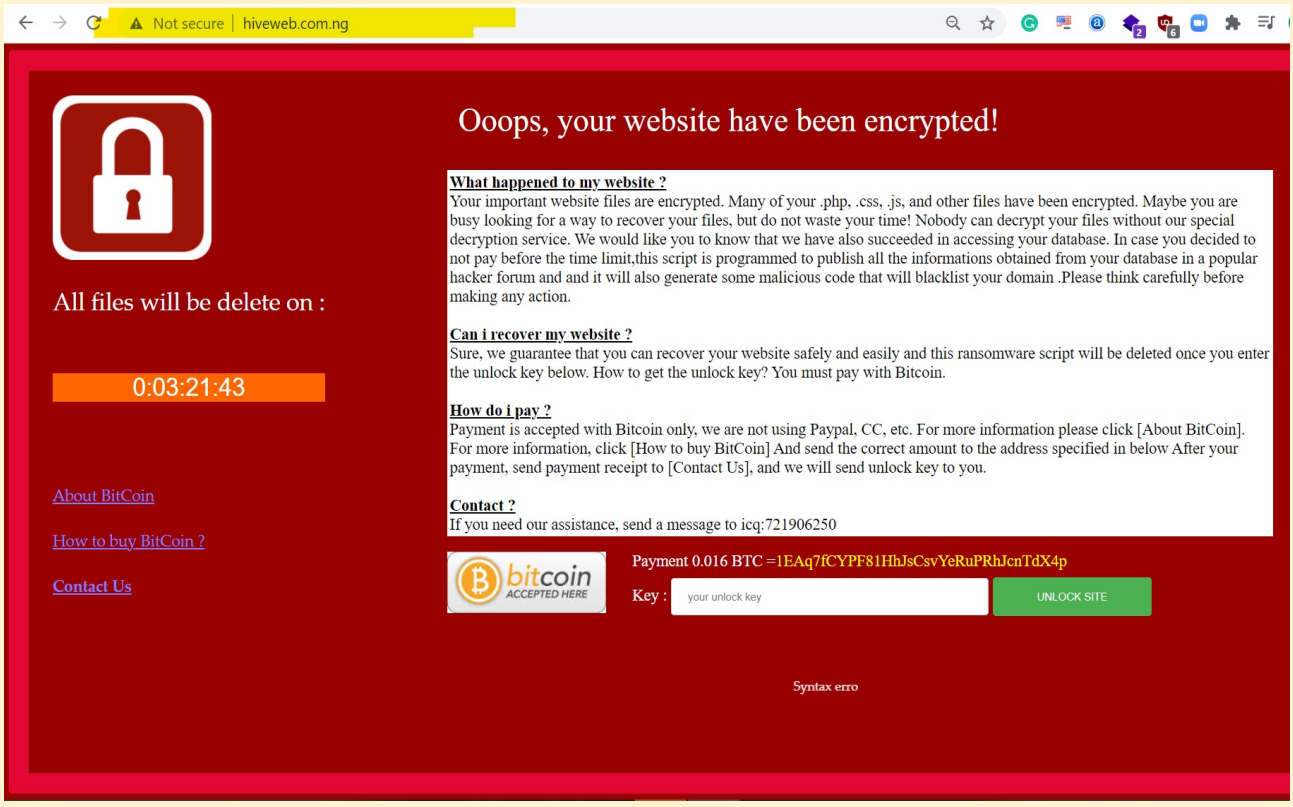
WHAT EXACTLY IS RANSOMWARE?

Ransomware attacks have become a pervasive and costly threat to businesses of all sizes across the globe.

These attacks involve cybercriminals infiltrating a company's systems and encrypting their valuable data, demanding a hefty ransom in exchange for its release. To mitigate the risks associated with such attacks, ransomware protection has become crucial for organisations.

Ransomware is a form of malicious software (malware) designed to block access to a computer system, files, or data until a ransom is paid. It represents a type of cyber extortion where attackers encrypt the victim's files or lock them out of their system, making the data inaccessible. Subsequently, the attackers demand a ransom, typically in cryptocurrency, in exchange for providing the decryption key or unlocking the system.

Various methods can be employed to deliver ransomware, including phishing emails with malicious attachments or links, compromised websites, or exploit kits. Once the malware is executed on the victim's system, it commences encrypting files, and a ransom note is usually displayed, informing the victim of the demand and providing payment instructions.

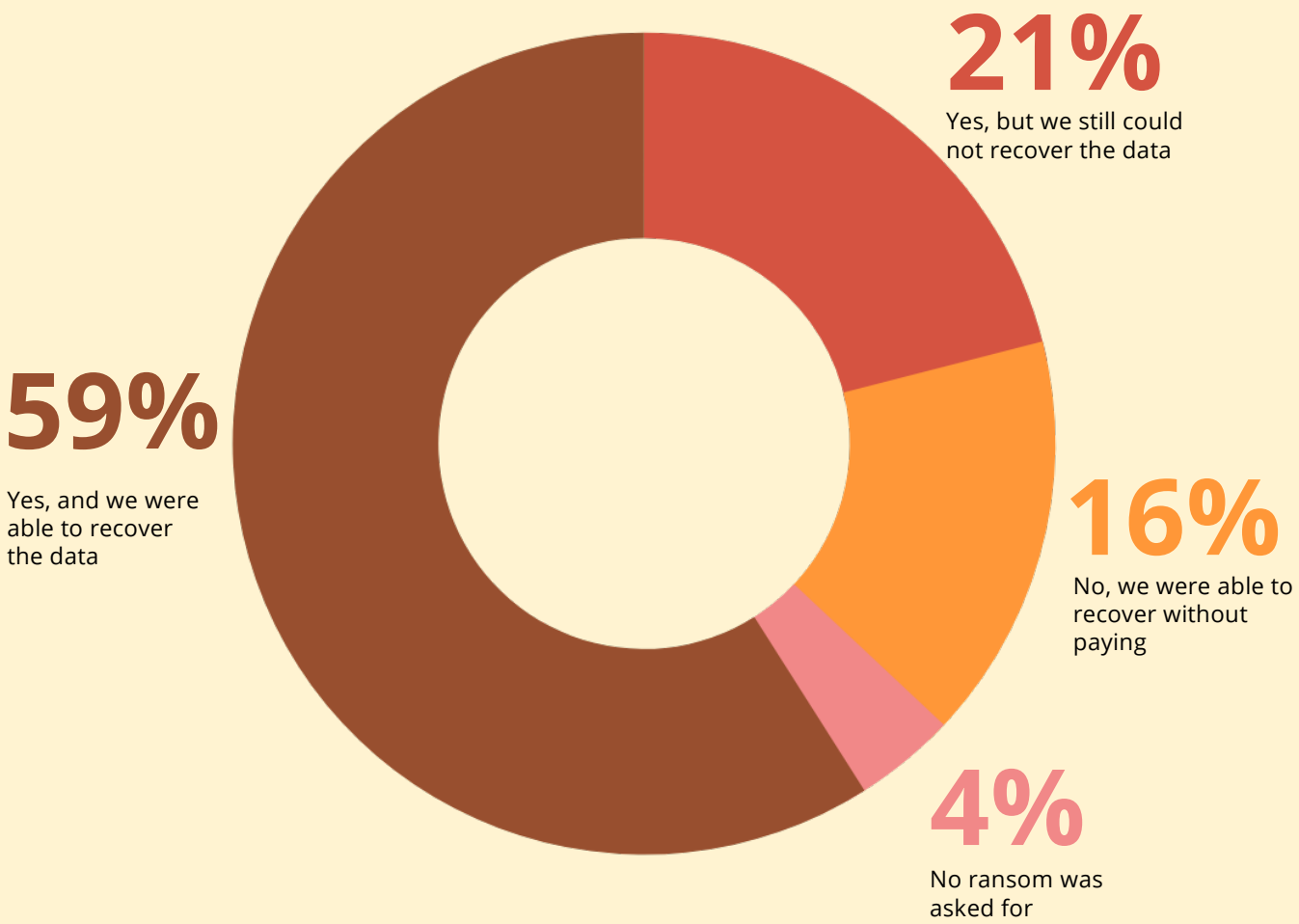


Example of a ransom note, typically with poor grammar. However, with the advent of AI content generation, sentence construction is improving. Image Source: CyberPlural

DID PAYING RANSOMS HELP VICTIMS RECOVER?

Of 1200 firms surveyed in a recent report, 80% paid but many could not recover their data

It is essential to note that paying the ransom **does not guarantee** that the attackers will provide the decryption key or unlock the system. Furthermore, succumbing to the ransom demand encourages further criminal activities and supports the ransomware ecosystem.



Source: Ransomware Trends Report 2023

To safeguard against ransomware, a **IntelliResponsetic** approach is necessary, including robust cybersecurity measures, regular data backups, educating employees on phishing and malware, and employing reputable security software to detect and prevent ransomware infections.

1

DISASTER RECOVERY-AS-A-SERVICE

BACKUP STRATEGY RULE TO LIVE BY

VEEAM

3	2	1	1	0
Three different copies of data	Two different media	One offsite copy	Of which is offline air-gapped immutable	No errors after automated backup

Source: VEEAM

The growing complexities of risk and compliance require more expertise than ever before. Outsourcing this function tends to reduce time and effort spent on solving these problems; however, to do so effectively, you need a partner who can understand and support your business objectives.

Choose a partner with the industry and technical knowledge to ensure your organisation stays on top of risk management practices and frameworks.

Disaster Recovery as a Service (DRaaS) is a cloud-based service that provides organisations with a comprehensive solution for protecting and recovering their critical data, systems, and applications during a disaster.

Instead of relying on traditional, on-premises disaster recovery infrastructure, DRaaS leverages cloud technology to ensure business continuity.

KEY BENEFITS OF DRaaS

- Quickly recover your critical systems and data, minimising impact on business continuity and reducing financial losses
- Scale your infrastructure up or down based on your evolving needs
- Data replication, infrastructure management, and testing tasks all handled by **DRaaS**, relieving your organisation from managing a separate disaster recovery infrastructure
- Provides a secure off-site replication and storage solution, safeguarding data from potential threats
- Eliminates the need for upfront investments in infrastructure like secondary data centres, resulting in significant savings
- Allows you to achieve faster recovery times by quickly accessing and restoring cloud-based systems and data, minimising downtime and enabling rapid resumption of operations.

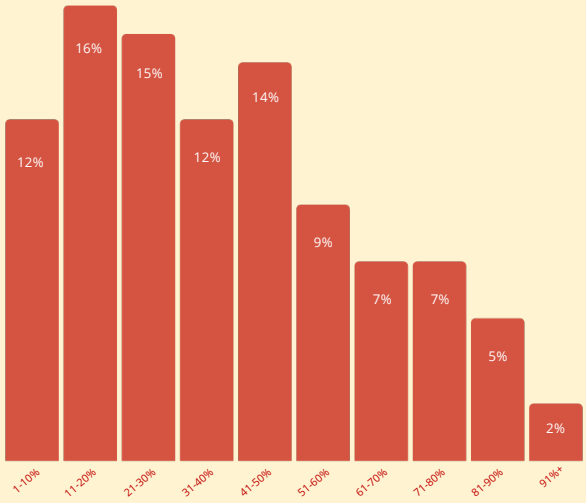
With the many challenges faced in a disaster, adopting DRaaS can help your organisation **protect critical data, ensure fast recovery times, reduce costs, and gain flexibility.**

2 UNDERSTANDING WHAT ASSETS ARE VALUABLE TO YOUR COMPANY

Ransomware attackers typically target critical data. They know that this data is the most valuable to the organisation, and they can use it to extort a ransom payment.

- If critical data is encrypted, the organisation may be unable to operate. This can lead to lost revenue, productivity, and reputational damage.
- Organisations that do not understand their critical data may be more likely to pay a ransom. This is because they may not know how to recover their data without paying the ransom.
- An attack on backup repositories, for example, can lead to a **39% reduction** in your ability to recover vital information

BACKUP REPOSITORIES MODIFIED OR DELETED BY ATTACKERS



Source: Ransomware Trends Report 2023

At IntelliResponse, we use a combination of frameworks such as ISO27001 and the CoBit 5 to help you define critical data as "**data that is essential to the organisation's operations and that, if lost, corrupted, or accessed by unauthorised individuals, could have a significant impact on the organisation**."

ROADMAP TO SUCCESS

- Implementing strong security controls. This includes things like access control, encryption, and disaster recovery.
- Educating employees on how to protect critical data. Employees should be taught how to identify and report phishing emails, how to create strong passwords, and how to avoid clicking on malicious links.
- Having a plan for responding to a ransomware attack. This plan should include steps for identifying the attack, isolating the affected systems, and recovering the data.

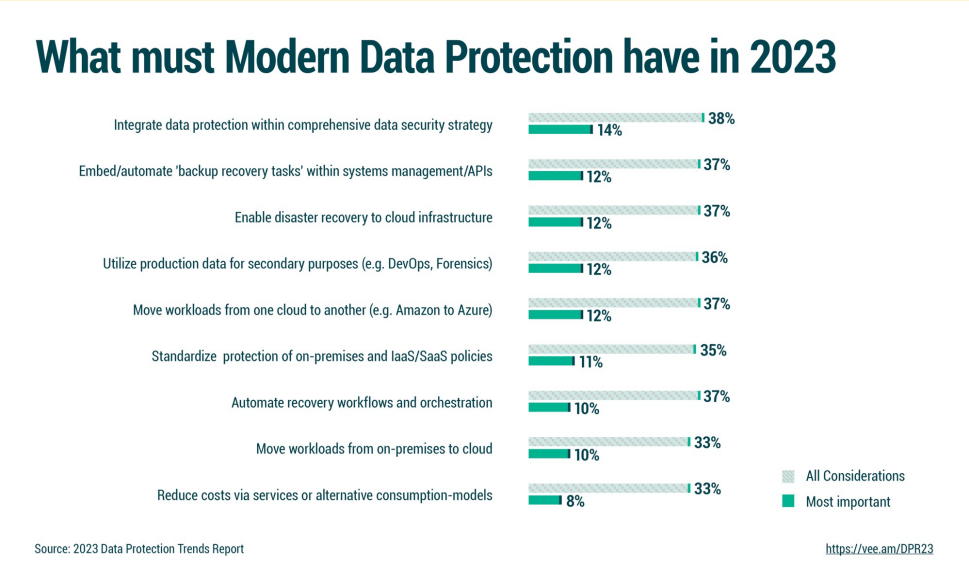
By taking these steps, you can help to protect your critical data and mitigate the risk of a ransomware attack.

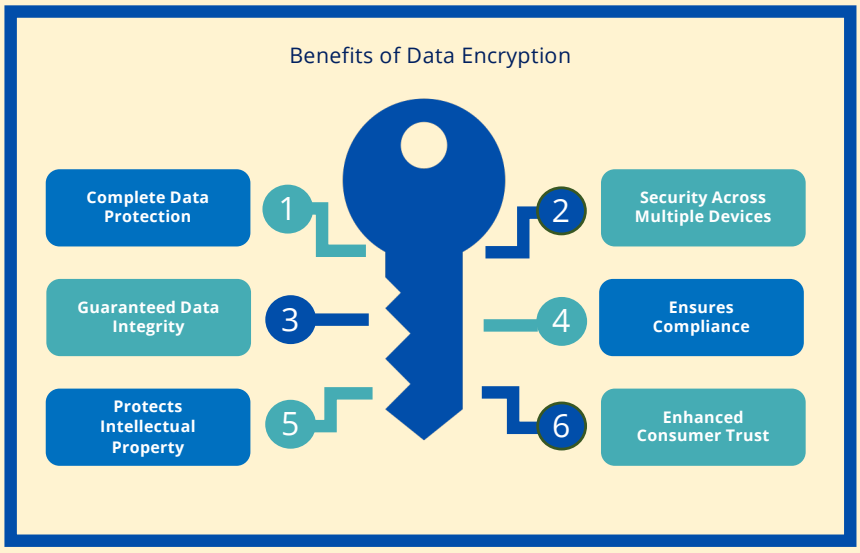
Here are some more reasons why it is important to understand what data is critical to your organisation:

- **To comply with regulations**. Many industries are subject to regulations that require them to protect certain types of data. By understanding what data is critical, you can ensure that you are compliant with these regulations.
- **To protect customer privacy**. Many organisations collect and store personal data about their customers. By understanding what data is critical, you can ensure that this data is protected, and that customer privacy is maintained.
- **To protect your reputation**. A data breach can damage your reputation. By understanding what data is critical, organisations can take steps to protect this data and mitigate the risk of a data breach

3 ENCRYPTION OF IMPORTANT INFORMATION

Encryption is the process of converting important information into an unreadable or scrambled format, known as **ciphertext**, to protect it from unauthorised access or interception. It ensures the confidentiality and integrity of sensitive data, such as personal information, financial transactions, or classified documents, by making it extremely difficult for unauthorised individuals to decipher or make sense of the encrypted data. To strengthen protection further in today's digital landscape:



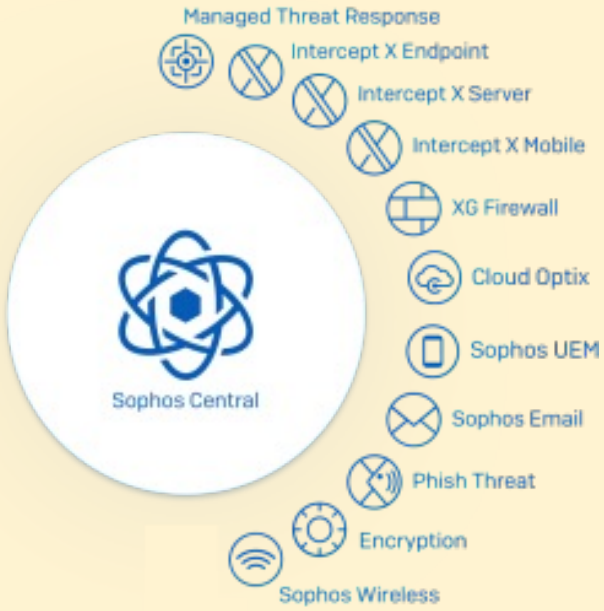


IntelliResponse offers comprehensive data encryption solutions to safeguard your sensitive information and protect it from unauthorised access. With their expertise in encryption technologies, IntelliResponse can assist you in implementing robust encryption algorithms and secure encryption key management systems to ensure the confidentiality and integrity of your important data.

4 SOPHOS ANTI-VIRUS MTR

As cyber threats work as a system, a **cybersecurity system** that delivers defence in depth is crucial in protecting against them. With **Sophos**, the only vendor in Gartner Magic Quadrant Leader for both Endpoint and Network security and #1 in the recent NSS Labs report for endpoint, your organisation is provided security right to the edge of your network.

IntelliResponse and Sophos are committed to bolstering your organisations security stance ensuring breadth and quality of cyber protection.



KEY BENEFITS

- Identifies hidden security risks so you can take action to address them. The automated incident response also slashes exposure to threats.
- The complete portfolio of products eliminates security gaps.
- Sophos products protect Windows, Mac and Linux devices, so you can see the security status of all your platforms at any one time.
- Reveals all network traffic – removing the cloak from the 43% that is currently hidden – enabling IT managers to see exactly what is running on their network.
- Time saving costs due to the automated threat response capabilities and cross-estate insights which reduces the time spent on manual investigations.
- Managing all your security through a single console both reduces day-to-day admin time, as well as eliminating the time and costs of maintaining an on-premises server.

Sophos utilises a synchronised security system managed through Sophos central, an intuitive cloud-based cybersecurity platform that includes all the cybersecurity you need.

With open APIs, extensive third-party integrations, and consolidated dashboards and alerts, Sophos Central makes cybersecurity easier and more effective to manage.

Sophos comprehensive security solutions ensure multiple layers of defence against different types of threats, **allowing for fewer incidents to deal with, and less time spent on managing IT security.**

5 MULTIFACTOR AUTHENTICATION

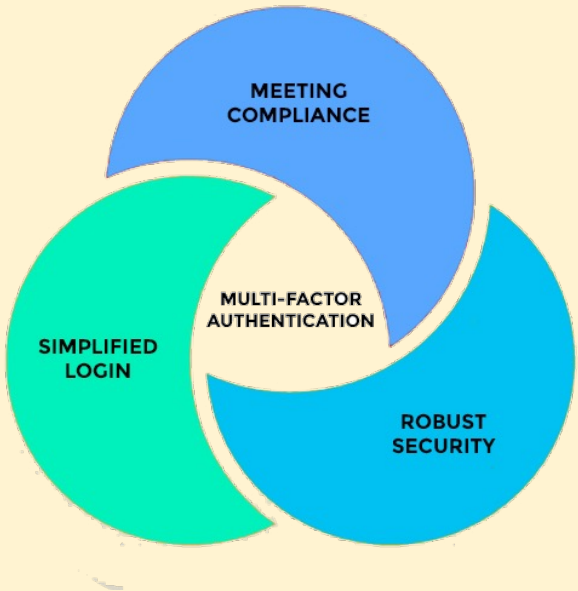
Multi Factor authentication (MFA) is a security measure that adds an additional layer of protection to the authentication process, aiming to verify the identity of users accessing digital systems or services. It goes beyond relying solely on a username and password combination, which can be easily compromised

MFA is crucial because it significantly enhances the security posture and helps mitigate the risk of unauthorised access to sensitive information and systems.

Multi Factor Authentication is an essential measure that enhances authentication security, reduces the risk of unathorised access and strengthens overall cybersecurity defences that ensures the protection of your data.

KEY BENEFITS

- Even if one factor is compromised, an attacker would still need to overcome the additional factor(s) to gain unauthorised access, significantly reducing the likelihood of successful credential theft or brute-force attacks
- Mitigates the impact of password theft or data breaches
- Acts as a deterrent in phishing attacks and provides an additional verification step, making it more challenging for attackers to exploit stolen credentials obtained through phishing emails or deceptive websites
- Inspires greater confidence in the security of financial transactions
- Prevents identity theft and unauthorised access to online services, ensuring that customers' digital identities remain secure.



6

CYBERSECURITY AS A SERVICE
SECUREWORKS TAEGIS MXDR

IntelliResponse has exclusively partnered with SecureWorks to offer you **SecureWorks Taegis Managed XDR**, an industry-leading service. By choosing us as your provider, you gain access to this comprehensive managed detection and response solution, integrating advanced technology, round-the-clock monitoring, proactive threat hunting, and expert incident response.

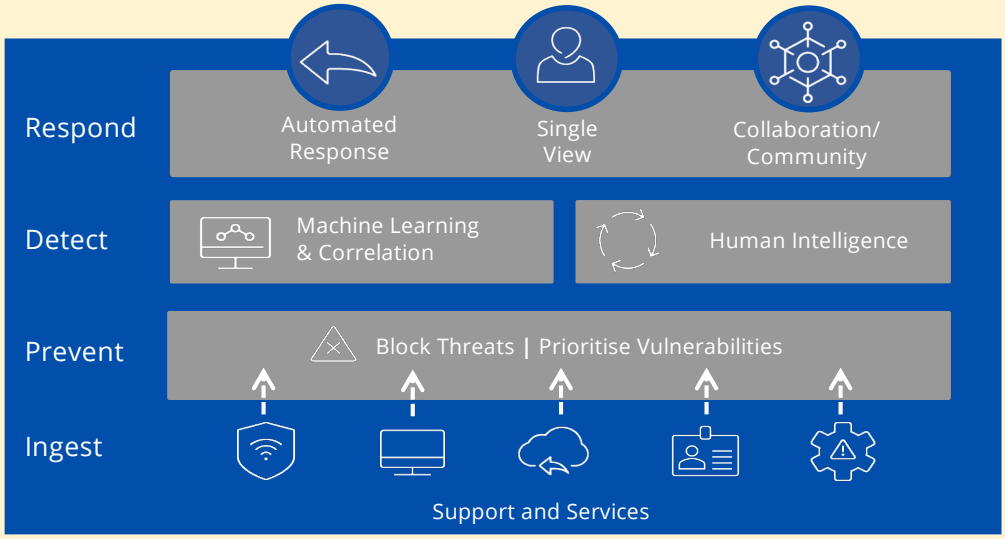
Together, **IntelliResponse** and **SecureWorks** are committed to enhancing your organisation's security posture, ensuring that you receive the highest level of protection and support available with SecureWorks Taegis Managed XDR.

KEY BENEFITS

- Raise the skill level of your team through collaborative investigations and live chat with our analysts
- Receive an unlimited response for in-scope assets, and monthly threat hunting, with an option of continuous managed threat hunting as part of ManagedXDR Elite
- Gain threat knowledge to defend against adversaries
- Improve your security posture as our security experts provide quarterly reviews of your defences, and easy access to comprehensive Secureworks Services for ManagedXDR

Taegis XDR uses threat intelligence, machine and deep learning, and user behavioural analytics for rapid threat detection. Our team will expose adversaries by prioritising endpoint, network, and cloud threat activity and identify which events require action. Receive unlimited responses for in-scope assets. While we fully manage* this technology on your behalf, you will have full access to it so we can collaborate on investigations via live chat.
Threat hunting is an included component of ManagedXDR to proactively isolate any malware that managed to evade your existing controls.

With limited resources at your disposal, protecting your organisation from advanced threats can seem overwhelming. ManagedXDR is designed to alleviate this burden and help you uncover threats 24x7.



Business Results

- Reduce Risk
- Maximise Security Investments
- Navigate Shortage of Security Talent

Purpose built • Broad & deep threat detection • Expertise • Collaboration

7 SYSTEM FORTIFICATION

System fortification plays a vital role in cybersecurity by mitigating the risk of unauthorised access, exploitation, and compromise of computer systems and networks. Here are some key reasons why system fortification is crucial:

Incident Response Readiness

By implementing logging, monitoring, and auditing mechanisms, organisations can detect and respond to security incidents more effectively.

Defence in depth

This approach ensures that even if one security control is bypassed or compromised, other measures are in place to provide additional protection.

Compliance Requirements

Many frameworks and regulatory requirements, such as the PCI DSS or the GDPR, mandate the implementation of specific security controls and measures. By adhering to these requirements, organisations demonstrate their commitment to data protection and privacy.



Vulnerability Reduction

By applying patches, disabling unnecessary services, and configuring secure settings, the attack surface is minimised, making it more challenging for attackers to find and exploit weaknesses.

Risk Mitigation

By implementing security controls and best practices, the likelihood and impact of successful attacks can be significantly reduced. This helps protect sensitive information, prevent financial losses, and maintain business continuity.

Defence against known threats

By regularly updating software, applying security patches, and configuring firewalls and intrusion detection systems, organisations can defend against known threats and exploit attempts.

Overall, system fortification is essential in the cybersecurity world as it helps protect against known vulnerabilities, reduces risk exposure, and enhances an organisation's ability to withstand and respond to cyber threats. It forms an integral part of a comprehensive cybersecurity strategy, ensuring the resilience and integrity of computer systems and networks.

SYSTEM FORTIFICATION ACTIVITIES

Servers	Operating Systems	Applications	Databases
• Install all security patches • Two different network interfaces • Keep backups of all data and files	• Install the latest service packs • File system encryption • Run services with the least privileged accounts	• Install all security patches • Implement an SSL architecture • Install a web application firewall	• Locking and expiring unused accounts • Role-based access control privileges • Perform periodic data-base security audits

HOW IntelliResponse CAN HELP YOU

As we conclude this **Ransomware Survival Guide**, we must remember that staying ahead of cyber threats requires a pragmatics approach. Embracing change and enhancing internal capabilities are vital steps within any organisation and its supply chain.

At IntelliResponse, we stand ready to be your trusted partner in this journey. Together, we'll fortify your defences and ensure your business thrives in the face of evolving cyber challenges.

Reach out to us at contact@intelliresponse.co and let's embark on this transformational cyber journey together.

Secure your future, protect your assets, and unlock the full potential of your organisation with IntelliResponse.

About IntelliResponse | IntelliResponse.co

IntelliResponse is a global incident Response and forensic firm that helps leading businesses, governments, and not-for-profit organisations recover from a breach and restore services.