computing™

THECHANNELCO.

Cyber deception

Why staying one step ahead is crucial to first-class security

MARCH 2023

Sponsored by

COMMVAULT®

CONTENTS

03 EXECUTIVE SUMMARY

04 KEY FINDINGS

06 THE DATA LANDSCAPE

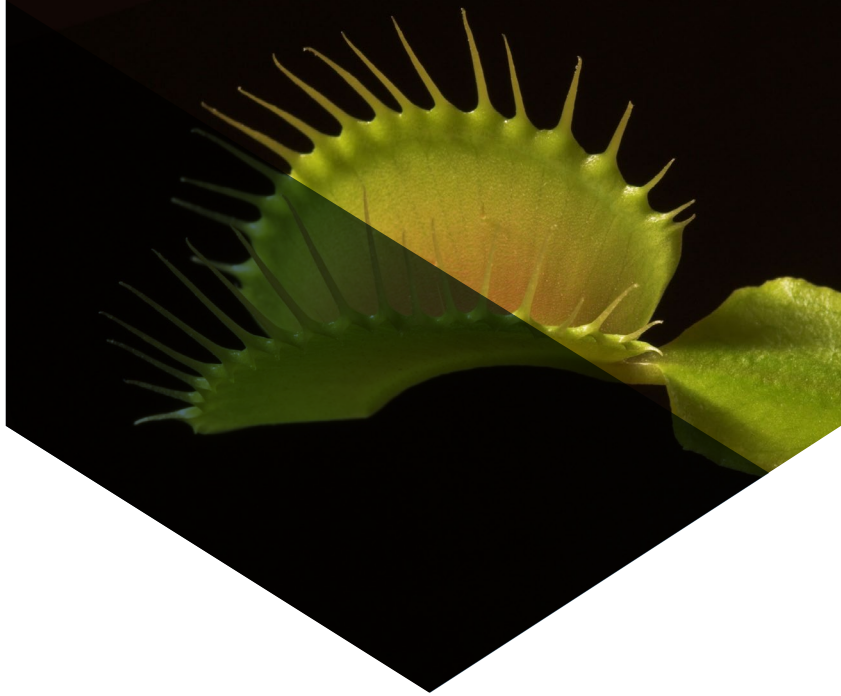
10 THE RANSOMWARE RISK

13 DATA PROTECTION: THINKING OUTSIDE THE BOX

17 CYBER DECEPTION

18 CONCLUSION

19 ABOUT THE SPONSOR - COMMVAULT



computing™

Executive summary

Data is arguably one of the most important resources today's organisations have at their disposal. If managed correctly, data can unlock rich customer insights and lead to better business decisions. However, if data is poorly managed it can lead to data sprawl, poor visibility, and increase the likelihood of a security breach.

While data must be easily accessible to those that need it, security must always be top-of-mind to prevent your organisation's greatest asset falling into the hands of adversaries.

Threat detection, endpoint protection, immutable backups, and disaster recovery are all key pillars of a successful incident response plan regardless of where that data is stored. However, with threat actors deploying increasingly sophisticated attacks, security response teams must think outside the box. Tactics such as cyber deception, in which fake network environments or "honeypots" are used to catch threat actors and learn more about them, enable security teams to respond at speed.

This white paper, featuring bespoke research from Computing, will examine how organisations are keeping increasingly extensive and distributed data environments safe from attack and how investing in the right tools not only reduces risk, but also enables organisations to get the most out of their data. Finally, it will look at how cyber deception can help augment incident detection and response strategies. ■

Key findings

43%

The percentage of organisations mainly storing data on-prem with some cloud storage, with 20 per cent mainly using cloud storage with some on-prem.

37%

The percentage of respondents that currently have a unified solution for data security with a centralised management console.

48%

The percentage of respondents that estimate it would take their organisation two to seven days to fully recover data following a successful ransomware attack.

82%

The percentage of respondents that currently have an incident response plan.

22%

The percentage of organisations that have carried out cyber deception.

The data landscape

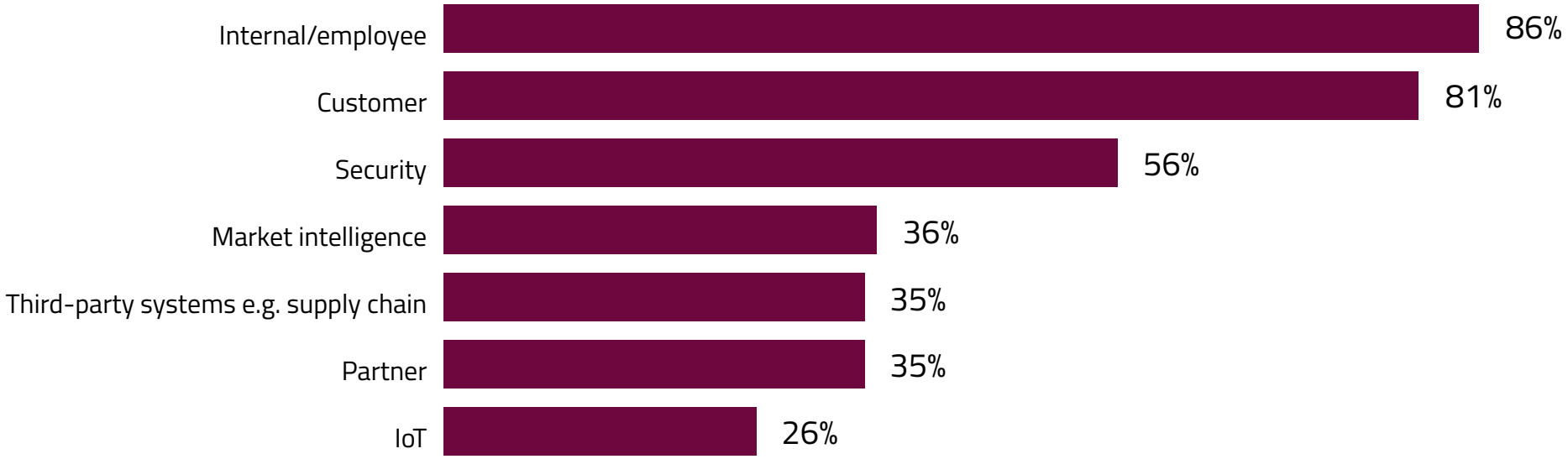
Used correctly, data is a goldmine for organisations, helping them uncover new insights into their customers, gain competitive advantage and create a better-informed business strategy. However, it is also an attractive target for adversaries, with a lack of adequate data security practices exposing organisations to financial loss, a decrease in consumer confidence, and reputational damage.

Data security is the process of protecting your organisation's data from unauthorised access. This includes protecting data from attacks capable of encrypting data, such as ransomware, ensuring that data can be restored swiftly and easily in the event of an attack, and making sure backups cannot be tampered with. A robust incident response plan, which is regularly reviewed and updated to reflect advances in technology is key.

Computing surveyed 146 IT leaders involved with data security at their organisations. 16 per cent were C-suite professionals, with 63 per cent IT directors or managers, and the rest other IT or cybersecurity professionals.

> A ROBUST INCIDENT RESPONSE PLAN, WHICH IS REGULARLY REVIEWED AND UPDATED TO REFLECT ADVANCES IN TECHNOLOGY, IS KEY.

Fig. 1: Types of data collected



The most common type of data organisations are collecting is internal or employee data, being collected by 86 per cent of organisations, closely followed by customer data at 81 per cent. 56 per cent are collecting security data, with around a third collecting market intelligence, third party data, partner data, or IoT data respectively.

Regardless of the types of data being stored, it is important to identify business-critical and sensitive data across environments and ensure it is not exposed to vulnerabilities. The data may need to be moved or new security measures put in place to remediate the risk of a breach.

86%

THE MOST COMMON TYPE OF DATA ORGANISATIONS ARE COLLECTING IS INTERNAL OR EMPLOYEE DATA.

In terms of where this data is being stored, 43 per cent are mainly storing it on-prem but with some cloud storage. Conversely, 20 per cent are mainly using cloud storage with some on-prem. Ten per cent said they are entirely on-prem, with 12 per cent entirely in the cloud.

Most organisations have not wholly made the switch to the cloud for their data storage and are instead opting for a mix and match approach, with data dispersed across different environments. When data is stored in this way, it is important to ensure it can be cross-referenced when analysed, can be securely moved to and from the cloud, and that issues related to data duplication are avoided. Security solutions must be able to protect data across SaaS, devices, databases, virtual machines (VMs), and containers, and must be easily scalable to protect growing environments.

With today's evolving IT environments meaning data is more distributed than ever before, a unified cyber security platform protecting data across public, private, hybrid, and multi-cloud is a must.

Deploying a patchwork of different solutions means IT teams must manage multiple interfaces at once, reducing productivity and ▸

Fig. 2: Data storage

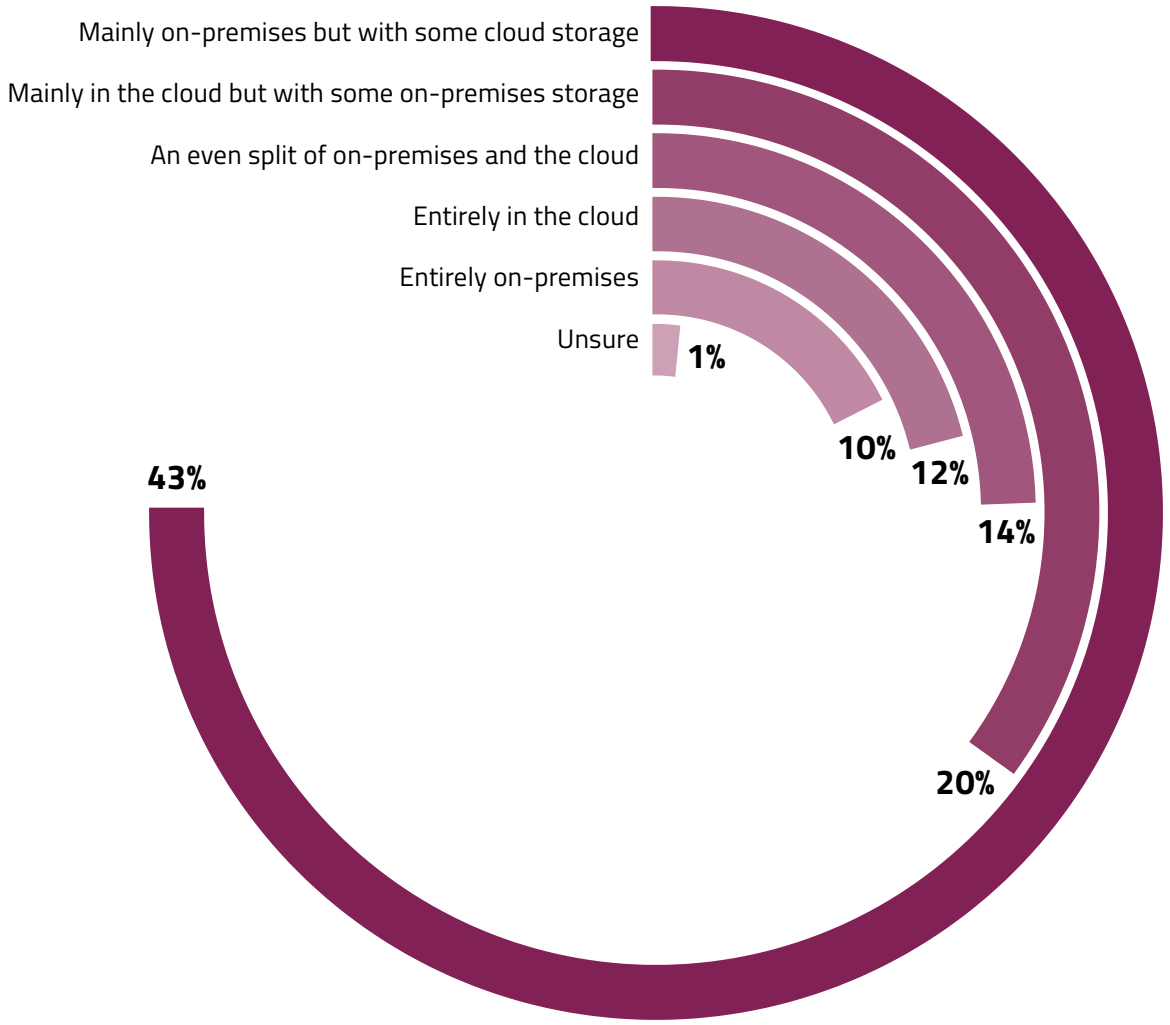


Fig. 3: Does your organisation currently have a unified solution for data security with a centralised management console?

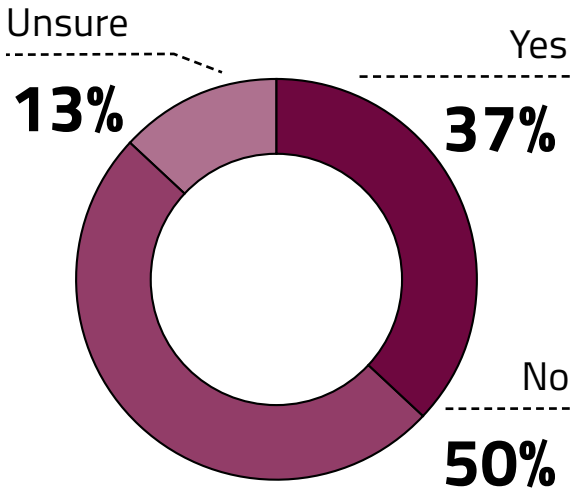
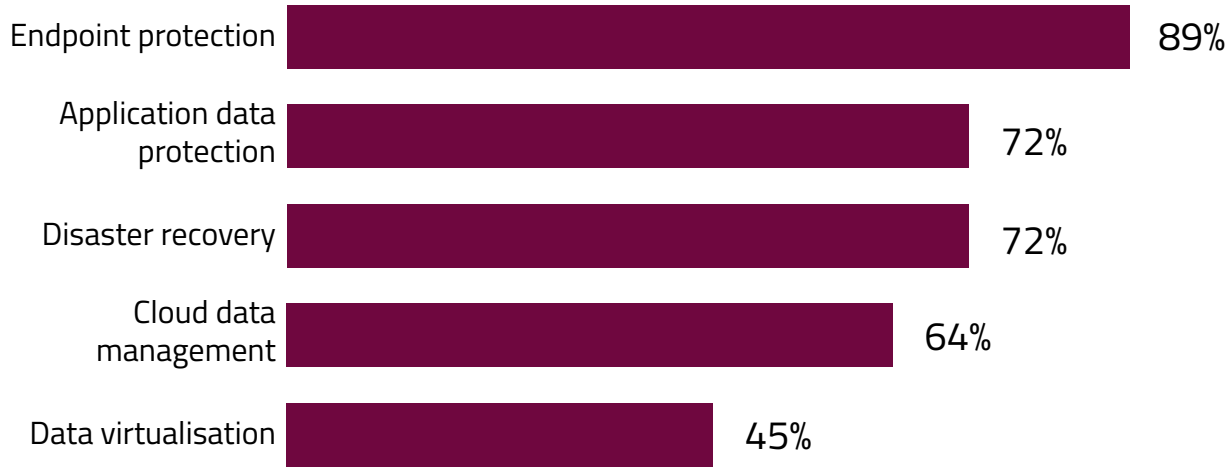


Fig. 4: Which of the following does your unified security solution cover?



increasing risk, as well as increasing data siloes and fragmentation. Having end-to-end visibility from a central control panel can help reduce complexity in your data management, meaning teams can focus their attention elsewhere.

As seen in figure 3, just 37 per cent of respondents were confident that their organisation currently has a unified solution for data security with a centralised management console.

For organisations that have not yet invested in this type of solution, it is important to assess whether their current process for managing and protecting data is fit-for-purpose, and how having a single control centre could help simplify disaster recovery, data migration and data protection.

For those that do currently have a unified data security solution, 89 per cent said it covers endpoint protection, as seen in figure 4, with 72 per cent answering application data protection and disaster recovery respectively. 64 per cent said their solution covers cloud data management and 45 per cent said it covers data virtualisation. This indicates that many organisations are missing crucial aspects of data protection and recovery from their security solutions, which may leave them vulnerable to attack. ■

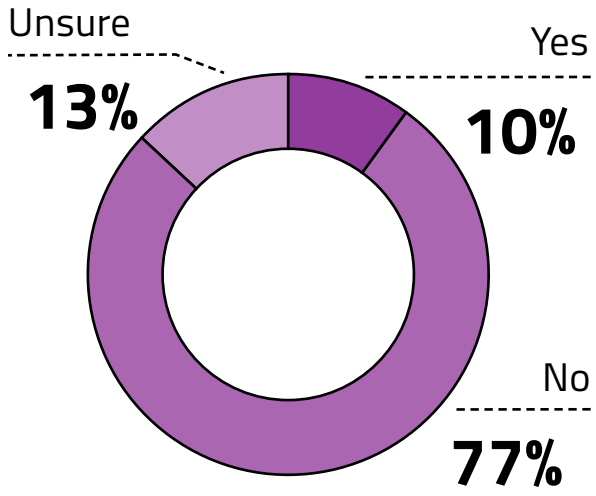
The ransomware risk

10 per cent of respondents said that their organisation has been hit by a successful ransomware attack, with 77 per cent saying that they haven't and 13 per cent unsure. While the proportion of organisations that have been hit may appear small, this still represents a large volume of data that has been compromised. Furthermore, it is concerning that a number of organisations are unaware of whether they have been affected by ransomware, indicating a lack of visibility.

According to the 2022 Verizon Data Breach Investigations Report, ransomware attacks rose dramatically in 2022, with ransomware involved in 25 per cent of all breaches. So even those that have not yet experienced a ransomware attack must remain vigilant.

> SINCE THERE'S NO WAY TO COMPLETELY PROTECT YOUR ORGANISATION AGAINST RANSOMWARE AND OTHER TYPES OF MALWARE, YOU SHOULD ADOPT AN "IF NOT WHEN" MINDSET.

Fig. 5: Has your organisation experienced a successful ransomware attack?



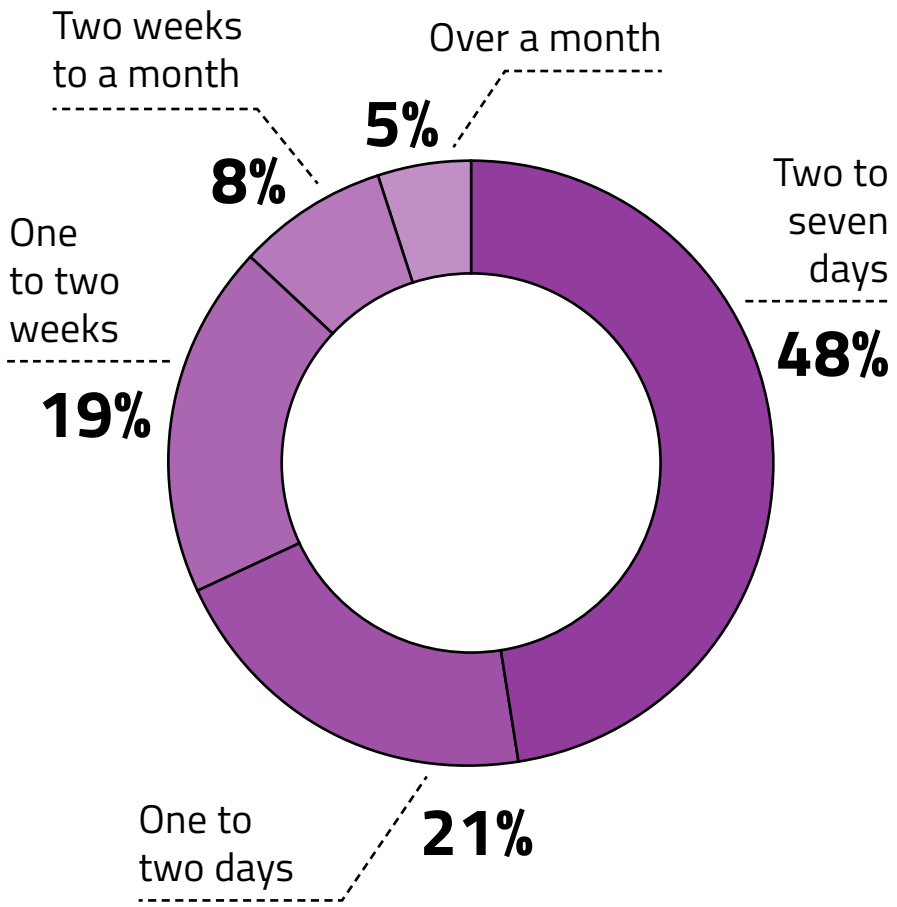
Sponsor insight:

COMMVAULT

The reality is your organisation needs to become less vulnerable and take proactive steps to protect your data and work with a provider who offers ransomware protection and recovery solutions. How prepared are you?

Take our **free risk assessment** to find out.

Fig. 6: Time it would take to fully recover data following a ransomware attack



Since there's no way to completely protect your organisation against ransomware and other types of malware, you should adopt an "if not when" mindset. A growing number of attackers are now carrying out double extortion, in which a victim's data is exfiltrated as well as encrypted, meaning a layered approach to defence is more important than ever.

Just over two-thirds of survey respondents (67 per cent) estimate it would take their organisation somewhere between 2 to 14 days to fully recover data following a successful ransomware attack. Twenty-one per cent are confident that they'd be back up and running within 2 days. Concerningly, 10 per cent predict it would take them over two weeks to fully recover.

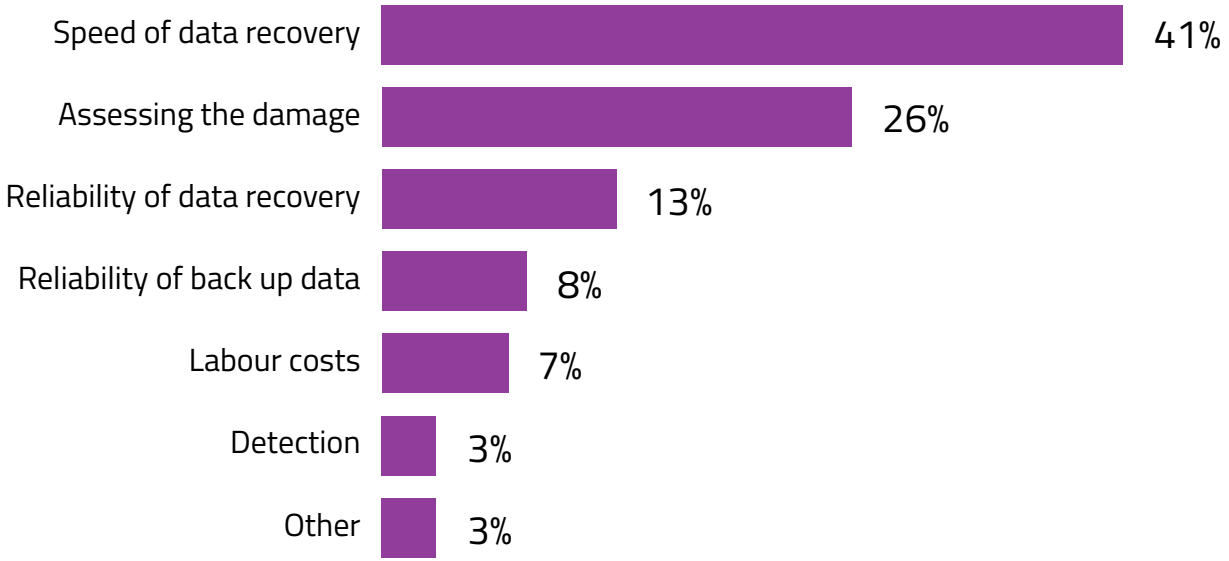
It is imperative that organisations are able to return to business as usual as quickly as possible after an incident to avoid downtime and high costs, and reliable backups and a thorough incident response plan are key to achieving this.

Those that are taking a while to recover data must be proactive in reducing the time taken by preparing in advance for a ransomware attack, using third party tools to prevent ransomware from entering and attacking systems, and enforcing strict IT security policies. Without an effective response strategy, organisations could experience huge damages to productivity, reputation, and potential opportunities.

Respondents said that the hardest part of recovering from a ransomware attack would be the speed of data recovery, followed by assessing the damage, and the reliability of data recovery. "Other" responses include reputational damage, ensuring a clean base to reload, and loss of business.

When ransomware or another form of malware strikes, speed is of the essence. Organisations require tools (such as anomaly detection, immutable backups, air gap, and multi-factor authentication controls) to monitor their environment, determine their recovery readiness state and get back up and running quickly and painlessly. ■

Fig. 7: The hardest part of recovering from a ransomware attack



Sponsor insight:

COMMVAULT

Ransomware is a prominent and real threat that brings daily business operations to a halt. **Watch this demo** and learn how Commvault may help your organisation perform a complete restore to recover all files or even just those needed in the event to a ransomware attack without recovering the infection.

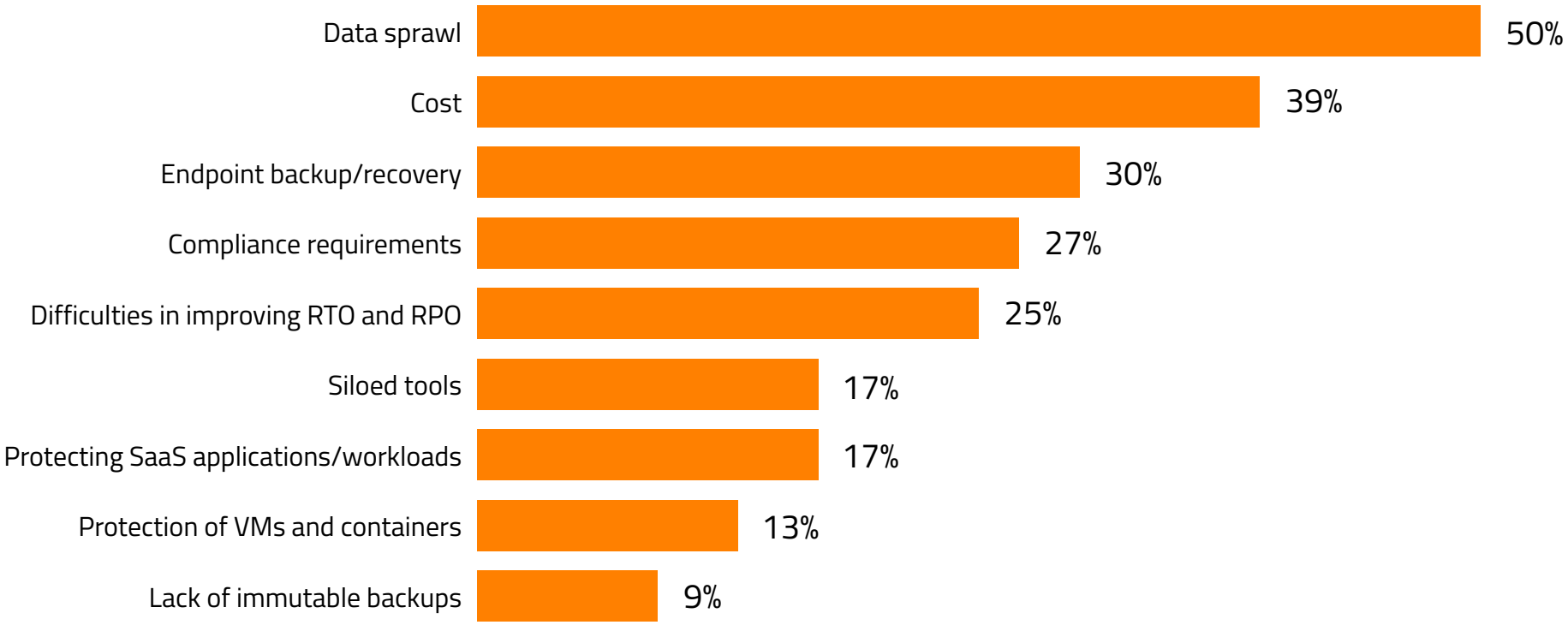
Data protection: thinking outside the box

Sprawl is a common issue for organisations storing data across multiple environments and using point solutions with inconsistent data management policies. As well as creating security blind spots, data sprawl can leave data under-utilised, so must be avoided by using the right management tools to ensure correct data usage, storage, and governance.

Learn more about Commvault's immutable infrastructure architecture here.

> ADVERSARIES ARE CONSTANTLY EVOLVING, SO STAYING PROTECTED INVOLVES THINKING OUTSIDE THE BOX.

Fig. 8: Biggest data protection challenge

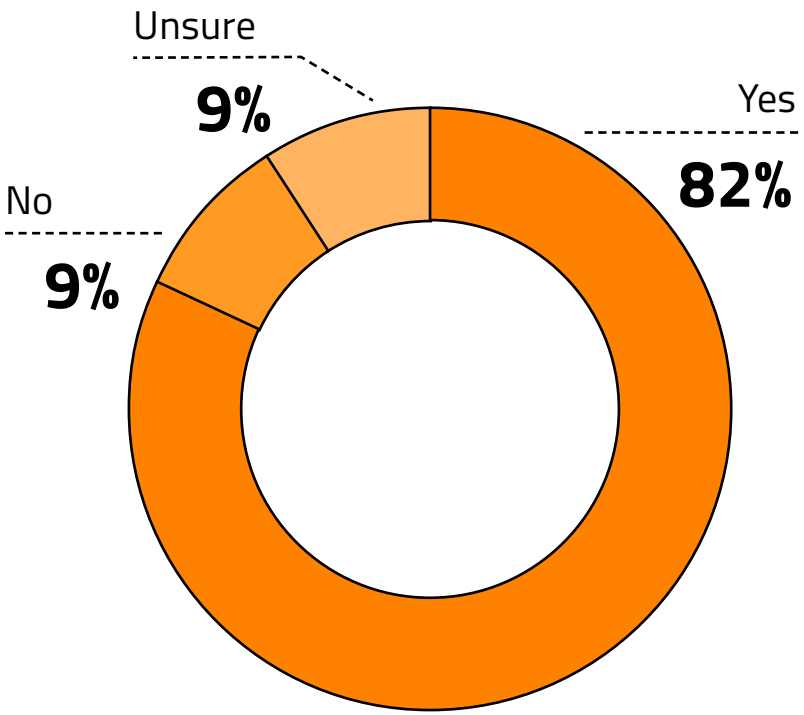


50%

VIEWED DATA SPRAWL AS THE BIGGEST DATA PROTECTION CHALLENGE.

Data sprawl was viewed as the biggest data challenge, followed by cost, endpoint recovery, compliance requirements, and difficulties in improving recovery point objective and recovery time objective. At the other end of the scale, just 9 per cent viewed a lack of immutable backups as a data protection challenge.

Fig. 9: Does your organisation have an incident response plan?



Eighty-two per cent of survey respondents said they currently have an incident response plan in place, with 9 per cent admitting they do not and a further 9 per cent worryingly unsure of their organisation's response practice.

A cyber incident response plan is a document outlining what an organisation should do in the event of a data breach or security incident. They are a crucial part of an organisation's information security strategy and crucially, ensure business continuity following an attack.

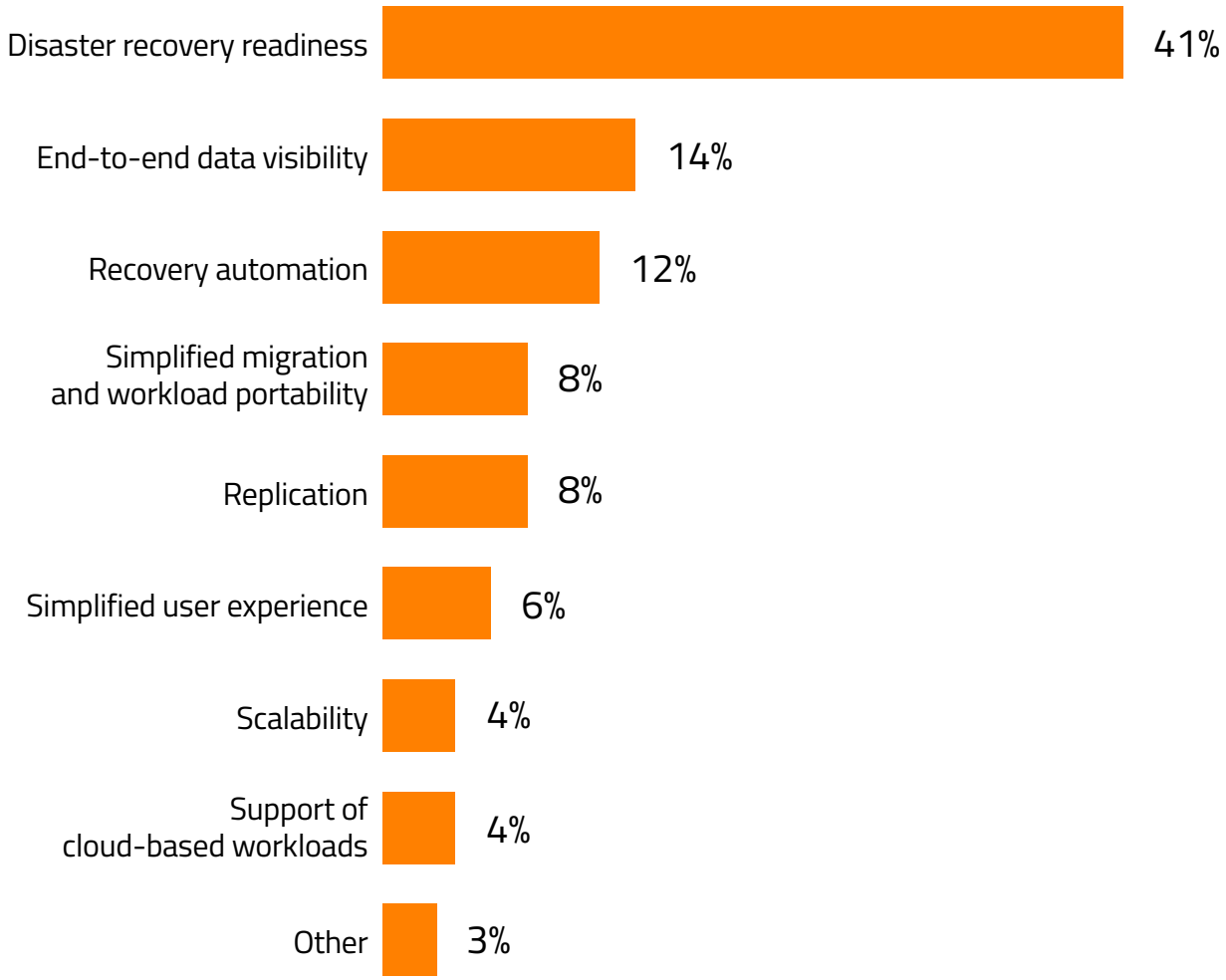
If an organisation does not have an incident response plan, dealing with a cyber attack can be a long and complex process, further intensifying the consequences. While it is encouraging that the majority of organisations have one, the remaining respondents should look to develop their incident response strategies – sooner rather than later. All organisations should prioritise developing a plan. A good place to begin is assessing the people, process, and technology impact of a cyber event, identifying what needs to be part of the recovery plan, identifying teams that need to be engaging with security teams, and putting together detailed processes to be followed after a cyber attack.

Once a plan in place, make sure it's going to work in the event of an attack by testing and updating it frequently. Consider also where those plans are being stored – if your systems become compromised, will you still be able to access your plan? ▸

> IF AN ORGANISATION DOES NOT HAVE AN INCIDENT RESPONSE PLAN, DEALING WITH A CYBER ATTACK CAN BE A LONG AND COMPLEX PROCESS.

The most critical feature of a data protection solution was deemed to be disaster recovery, chosen by 41 per cent of survey respondents. Twelve per cent chose end-to-end visibility and 12 per cent chose recovery automation. "Other" responses included cost, ability to assess the damage, and backups. Less than ten per cent chose simplified migration and workload portability, replication, simplified user experience, scalability and support of cloud-based workloads respectively.

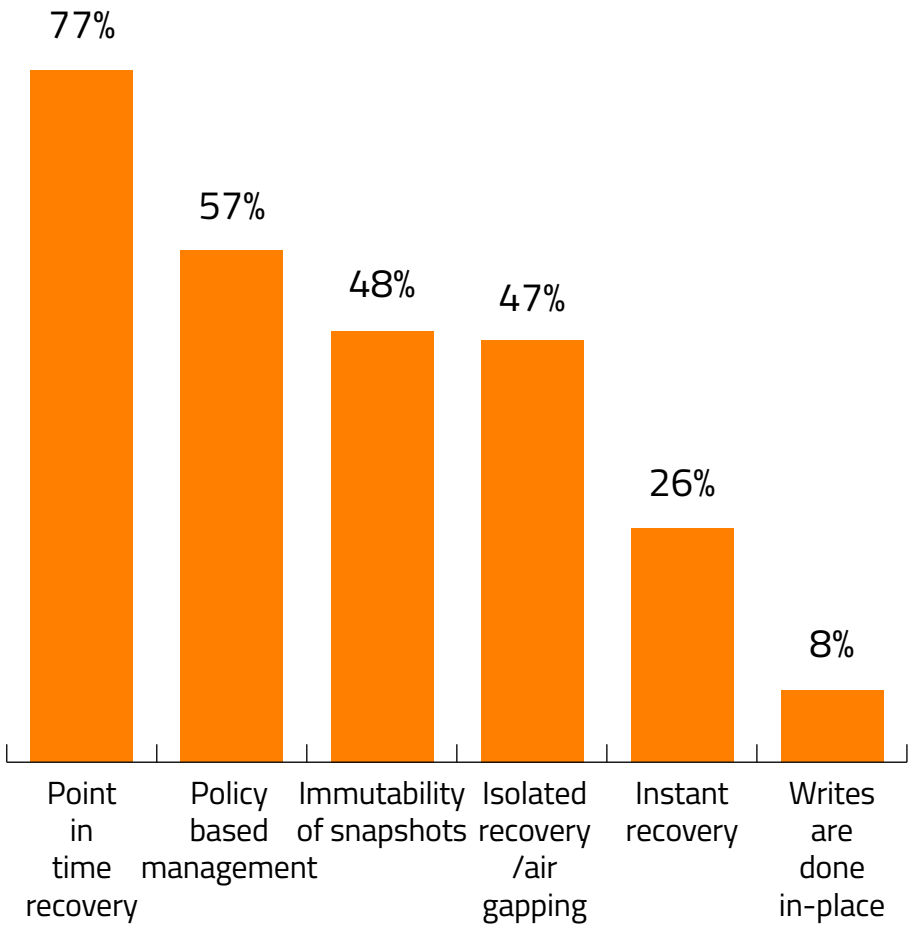
Fig. 10: Most important elements of a data protection solution



41%

THE MOST CRITICAL FEATURE OF A DATA PROTECTION SOLUTION WAS DEEMED TO BE DISASTER RECOVERY.

Fig. 11: Does your backup solution have any of the following features?



> ANOTHER VITAL FEATURE OF A DATA RECOVERY STRATEGY IS IMMUTABILITY.

Another vital feature of a data recovery strategy is immutability. Seventy-seven per cent of respondents said their current backup solution has point in time recovery, with 57 per cent having policy-based management, 48 per cent immutability of snapshots, and 47 per cent isolated recovery or air-gapping.

These are all features of immutable backups. For a backup to be truly immutable, it cannot be accessed or changed by administrators or threat actors alike, meaning it is protected from attackers who will often encrypt or delete data during their attack. If a backup is not immutable, it threatens your organisation's ability to fully restore data quickly and easily and should therefore be integral to systems architecture.

Data backups also need to follow a 3-2-1 backup strategy: 3 copies of your data, on 2 different media types, with a copy off-site and preferably air-gapped. ■

Learn more about how to prevent a ransomware attack and how air gapping adds a layer of security to help safeguard your data and mitigate ransomware risk.

Cyber deception

While having an incident response plan and central data management system are important building blocks for data security success, adversaries are constantly evolving, so staying protected involves thinking outside the box. This further highlights the need to consistently test and update recovery response plans, this will ensure your organisation has the best defence in place at all times.

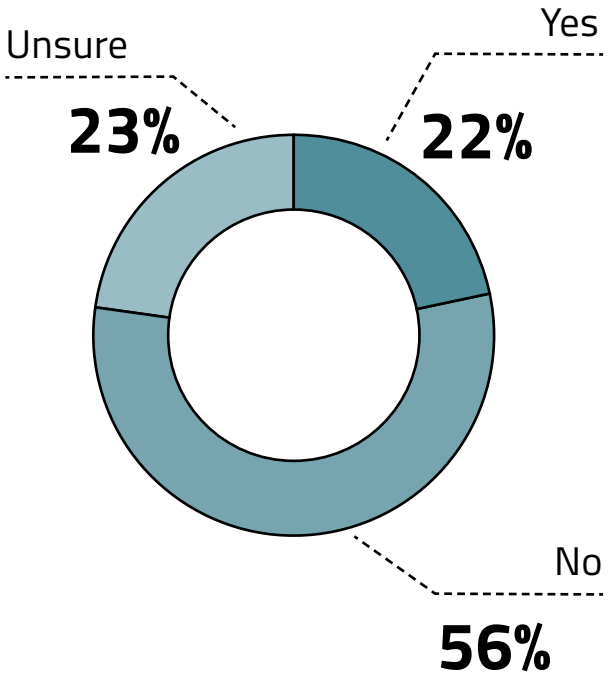
Cyber deception refers to the use of decoys across a system's infrastructure to better understand attack vectors and detect suspicious activity. Fifty-five per cent of survey respondents said their organisation has not carried out cyber deception, with 22 per cent answering "yes" and 23 per cent unsure.

For those that have carried out cyber deception, applications included internal exercises such as sending fake phishing emails, using honeypots and canary services to see what attack attempts were made, penetration testing conducted by a third party, and white hat analysis.

When it comes to detecting and responding to an incident, being proactive is key. But many detection solutions only send alerts once an asset has been compromised, and often do not offer important information such as how an attacker was able to enter a system.

Cyber deception, on the other hand, allows organisations to detect attackers and learn key information about their actions, such as lateral movement and privilege escalation, before a system is actually compromised. Organisations may not have the resources or expertise to carry out cyber deception themselves, so getting the perspective of a third party can be a valuable addition to a cyber strategy. ■

Fig. 12: Has your organisation ever carried out cyber deception?



Data protection starts before you're compromised. Learn more about Commvault's new Metallic® ThreatWise™ platform offering cyber deception technology.

Conclusion

Data is the lifeblood of modern organisations and as such, managing and protecting it must be a priority across all teams. At best, poorly managed data means an organisation is not living up to its potential, missing valuable business insights data can provide. At worst, it can lead to catastrophic data breaches, causing reputational and financial damage that may be difficult to repair.

Therefore, organisations must ensure they have the tools and strategies to prepare for future data protection challenges. Unified data management solutions enable greater visibility across all environments, reducing data management hurdles such as data sprawl and security blind spots. Implementing layers of infrastructure protection and controls that can be easily managed by your security team can also help improve your security posture and speed of recovery following an attack.

However, technology can only solve part of the problem. Having an incident response plan and zero loss strategy that is tested and updated regularly, and one which people across your organisation are engaged with, helps ensure your organisation can quickly return to business as usual.

Keeping one step ahead of attackers also involves keeping abreast of the latest innovations in data security, and assessing how they can be applied to your organisation. Tactics such as cyber deception ensure security teams can respond faster to incidents and remediate them as soon as possible. ■

About the sponsor

Commvault (NASDAQ: CVLT) is a global leader in cloud data protection. Our Intelligent Data Services protect customers' data in a difficult world. We provide a simple and unified Data Protection Platform that spans all your data – regardless of whether your workloads live on-premises, in the cloud, or spread across a hybrid environment. Commvault solutions are available through any combination of software subscriptions, integrated appliances, partner-managed offerings, or Software as a Service via our Commvault-built Metallic portfolio. In addition, integrations are available for O365, Salesforce, ServiceNow, and other leading business applications. For over 25 years, more than 100,000 organisations have relied on Commvault to keep their data secure and ready to drive business growth. ■

Visit **commvault.com** or follow us **@Commvault**