Publication date:
May 2024
Author:
Dennis Hahn

Navigating the Complexities of Modern Backups

Commissioned by:

opentext™

Brought to you by Informa Tech

Brought to you by Informa Tech

Contents

Introduction

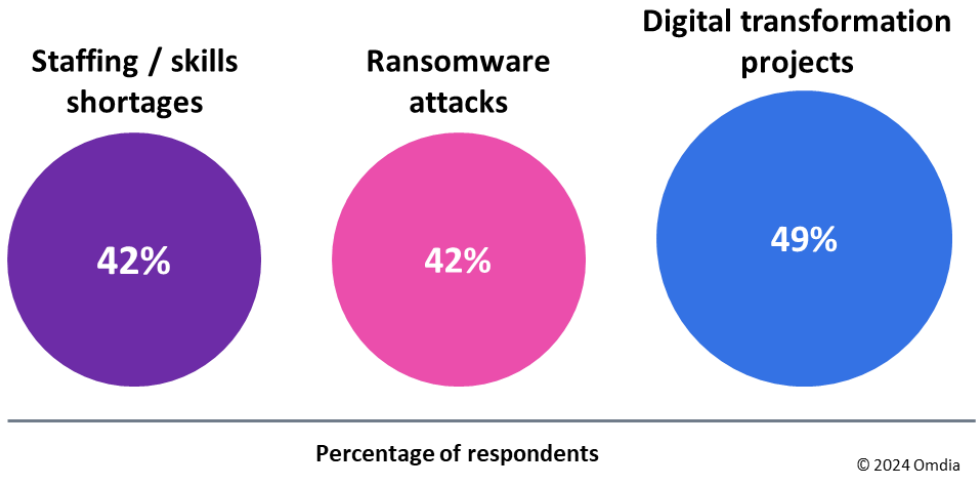
Ransomware attacks have become pervasive

In today's digital landscape, where technology and data permeate nearly every aspect of our lives, cybersecurity has become a critical concern for individuals and organizations alike. Among the myriad threats looming over the horizon, one has emerged as being particularly insidious and pervasive: ransomware attacks.

In a 2022 survey by Omdia, when respondents were asked about the most challenging issues IT is facing, ransomware was ranked joint second. This alarming trend underscores the urgent need for a comprehensive strategy to combat this evolving threat to data. Some overarching items to consider are detection of a ransomware attack, failsafe backups of data, and ransomware recovery workflows.

> *When a recent survey asked what was the most challenging aspect of security, ransomware came joint second. Ransomware is just one reason for backups: others might be data loss, disaster recovery, and so on.*

Figure 1: What are the most challenging issues in IT?



Source: Omdia 2022 survey

Recovery and backup workflow optimization

In the face of escalating ransomware threats, optimizing recovery and backup workflows is vital to ensure swift recovery and minimize downtime. Efficient recovery processes are crucial, underlining the need for strategic backup planning tailored toward recovery objectives. Consistency across all recovery experiences—whether on premises, in the cloud, or at the edge—is essential for workflow optimization. Additionally, having a well-defined contingency plan for recovery in place is imperative to navigate unforeseen challenges data loss of any type can bring.

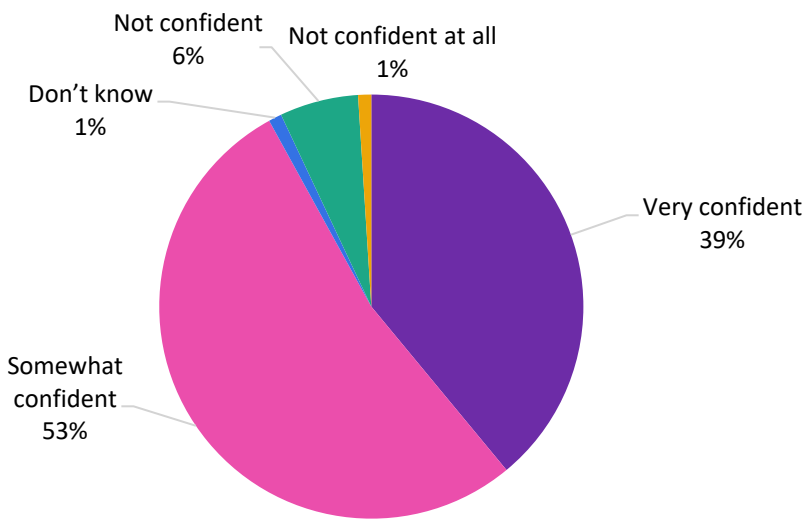
Reflecting on your organization's readiness to respond to ransomware attacks, consider the following key aspects. When evaluating recovery products, prioritize web-based approaches, streamlined workflows, and standardized procedures to enhance recoverability. To ensure the reliability of recovery processes, conduct regular drills to test readiness, and leverage sandboxed data recoveries for added security.

Automation plays a pivotal role in streamlining reporting processes, reducing manual workload, and minimizing the risk of human error. By automating report generation and distribution, organizations can ensure timely access to critical information and facilitate proactive decision-making. Detailed automated backup reporting not only facilitates informed decision-making but also ensures thorough coverage, safeguarding critical data assets against potential loss or corruption.

The findings from Omdia's Cybersecurity Decision Maker Survey 2022 in **Figure 2** underscore the importance of remaining vigilant, even for organizations confident in their response plans. Continuous assessment and refinement are essential to effectively address emerging threats. Regardless of perceived readiness, it is crucial to remain proactive in identifying and addressing potential issues to bolster ransomware resilience.

> *Even those who believe they have a response plan in place need to continually review it and address potential issues to ensure their defenses remain effective. Given the potentially disastrous consequences of a ransomware attack, being "somewhat" confident is probably not enough.*

Figure 2: How confident are you in your organization's plans for responding to a ransomware attack?



Source: Omdia Cybersecurity Decision Maker Survey 2022

Do not let your backup data be compromised by ransomware

Data theft has emerged as a significant concern in today's threat landscape, and organizations are increasingly vulnerable to attacks that target sensitive information. According to Omdia, a considerable proportion of organizations have encountered issues related to data security, including data destruction, ransomware attacks, and theft of information. Organizations should assign the same level of importance to backup data as to primary data, implementing robust measures to protect it against theft and tampering.

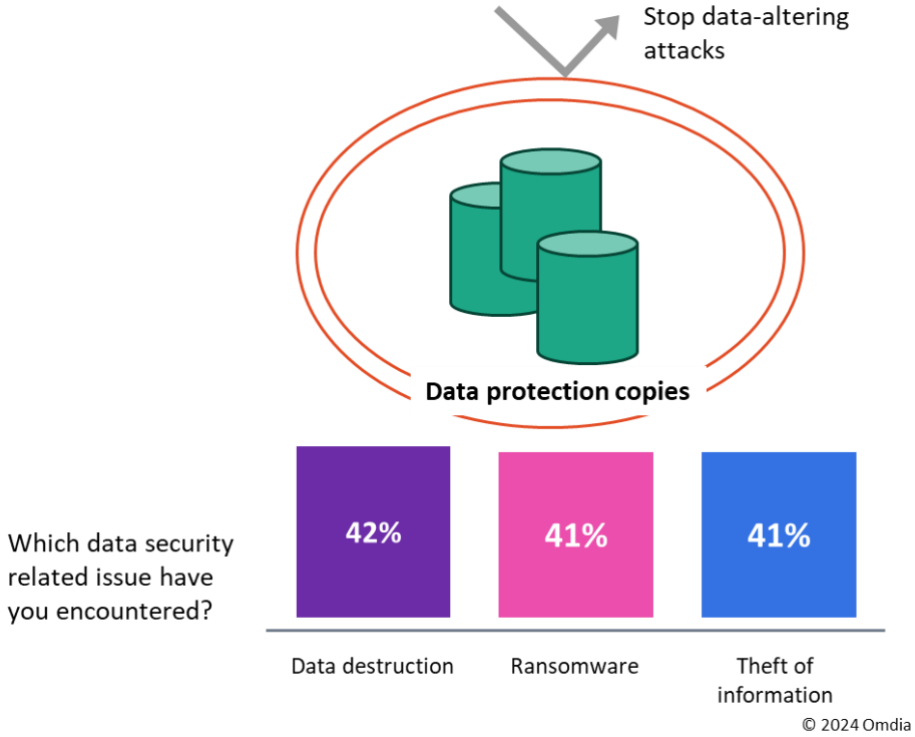
Because data theft has become increasingly prevalent, ensure the access to backed-up data is controlled by cybersecurity measures; this is especially important to data recovery scenarios. When backup products are being evaluated, several key considerations should be taken into account to enhance theft resilience. These include implementing strict access controls, multifactor authentication (MFA), monitoring for unauthorized access attempts, data encryption with AES-256, and the use of secure protocols for data transfer.

Before many attacks, attackers often attempt to neutralize any data backups by turning off backup processes, deleting backup data, encrypting the data, or altering its contents. Foremost, it is essential to safeguard data with air-gapped backup repositories where the data cannot be altered by would-be attackers. Then the backup process controls and control plane need to be secured to prevent unauthorized control over backups to shut down protections. The significance of locking

down the control pane and APIs cannot be overstated: unauthorized access to these backup controls poses a significant risk to possibly needed recoverability.

Figure 3: Data theft has become a huge concern

The survey highlights two huge concerns. One is the theft of data, which needs entirely different protections to guard against ransomware data encryption attacks. The second is the need to lock down the control plane and APIs tightly so backups cannot be turned off or protection data destroyed before the attack.



Source: Omdia Cybersecurity Decision Maker Survey 2022

There is a need for ransomware detection everywhere

In the battle against ransomware, comprehensive detection is essential to safeguarding organizational data. Detecting ransomware threats at every possible entry point ensures complete

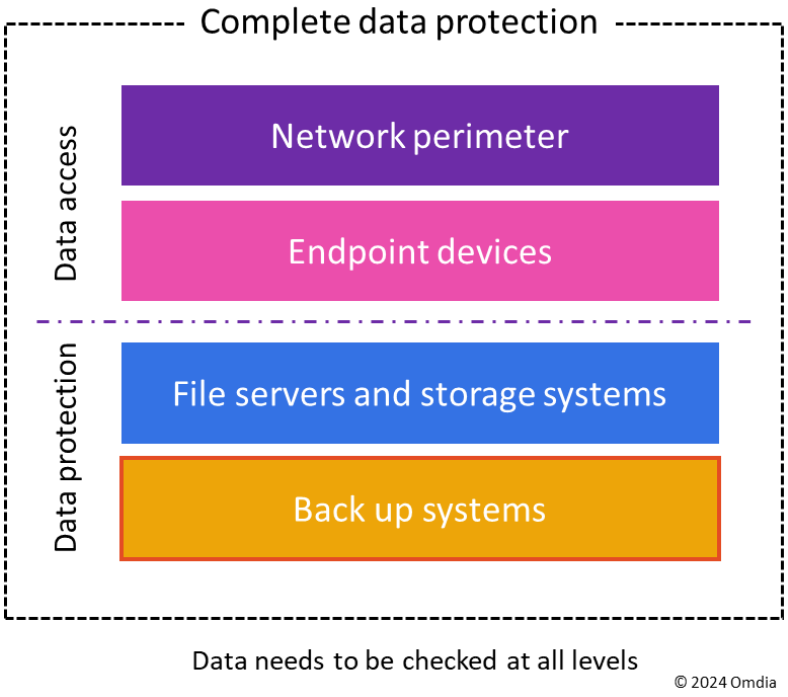
protection and minimizes the risk of data compromise. To achieve this, it is crucial to prioritize solutions that are ransomware aware and that integrate vertically across tools for seamless threat mitigation.

Furthermore, verifying data integrity at each step of the backup process and conducting thorough scans for ransomware across all backup data are both critical measures. Antivirus checks on all files help identify and neutralize potential threats, ensuring that backup data remains secure and free from compromise.

Despite these measures, the direct protection of data can sometimes be overlooked. It is imperative to prioritize data cleanliness and implement checks at all levels to mitigate the risk of ransomware attacks targeting backup systems. By ensuring that data remains untainted and readily available for recovery, organizations can bolster their defenses against ransomware and safeguard their critical assets.

Backups play a crucial role in a comprehensive ransomware protection strategy by ensuring data recovery and minimizing downtime in the event of a breakthrough attack that alters the primary data. The backup can also be a point where an attack can be detected.

Figure 4: Backup plays an important role in a complete data protection framework



Source: Omdia

The need to protect all data within an enterprise's data estate

In today's digital landscape, protecting all data assets is paramount. Organizations must ensure comprehensive coverage across various environments, including virtual machines (VMs), physical servers, Kubernetes clusters, and cloud-based VMs. Deploying tools capable of safeguarding data in multiple scenarios is essential, because different data sources often require distinct backup methods.

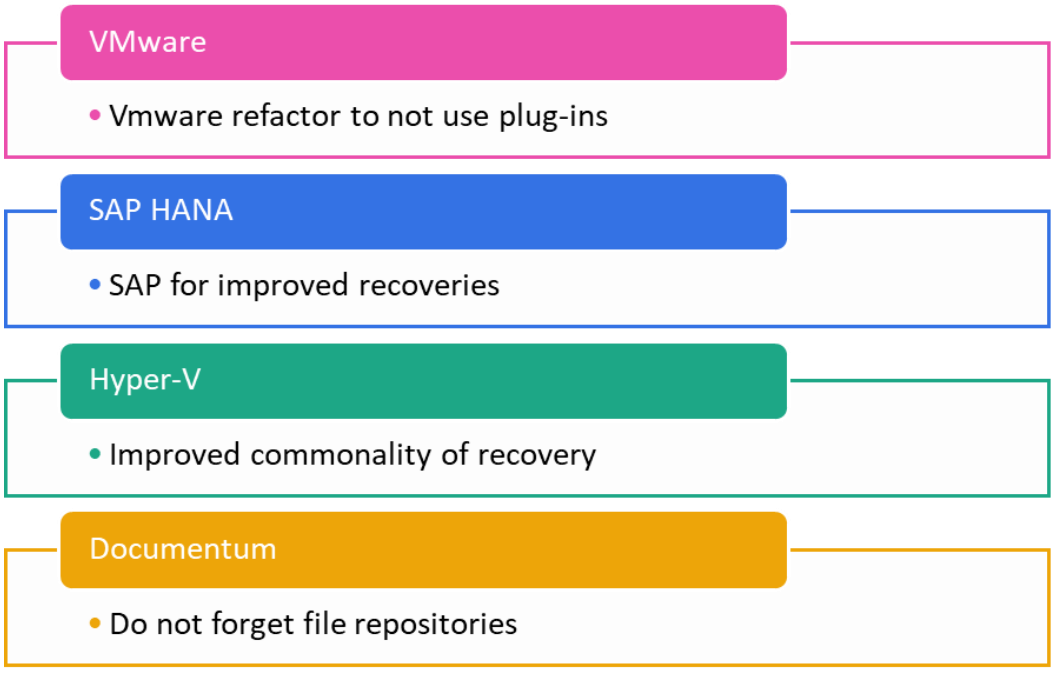
One critical consideration is to refrain from relying on plug-ins for VMware backup, instead opting for solutions that offer native support to enhance efficiency and reliability. Furthermore, organizations should prioritize application-consistent backups, particularly for complex applications such as SAP, to facilitate improved recoveries. Embracing commonality in recovery processes and not overlooking file repositories are both essential steps in ensuring comprehensive data protection.

When evaluating backup products, organizations should prioritize solutions that offer protection across multiple scenarios, including integration agents, native application integrations, and agentless options with appliances. Ensuring consistency in recovery workflows and regularly refreshing backup approaches is crucial for maintaining operational resilience.

Given the ever-evolving nature of data environments, organizations must remain vigilant and adaptable in their backup strategies. By embracing innovative solutions and staying abreast of emerging trends, they can effectively safeguard their data assets and adapt to evolving challenges in the digital landscape.

A critical component of any effective ransomware protection strategy is selecting the right data protection scheme for each data center application. The way the data is backed up often dictates how it is recovered. Continuous evaluation and adaptation of these schemes, combined with robust data protection solutions, will safeguard data and ensure business resilience.

Figure 5: Application data protection is always evolving



Source: Omdia

The necessity of detailed automated backup reporting

The sheer volume and complexity of backup operations poses a significant challenge, particularly for IT teams already stretched thin. Keeping track of backups, monitoring their status, and ensuring their effectiveness demands meticulous attention to detail and timely intervention.

To alleviate the burden on administrators and enhance operational efficiency, backup solutions must offer robust reporting capabilities. When products are being evaluated, scalability should be a primary consideration, offering the ability to generate reports for potentially tens of thousands of session instances without compromising performance or accuracy.

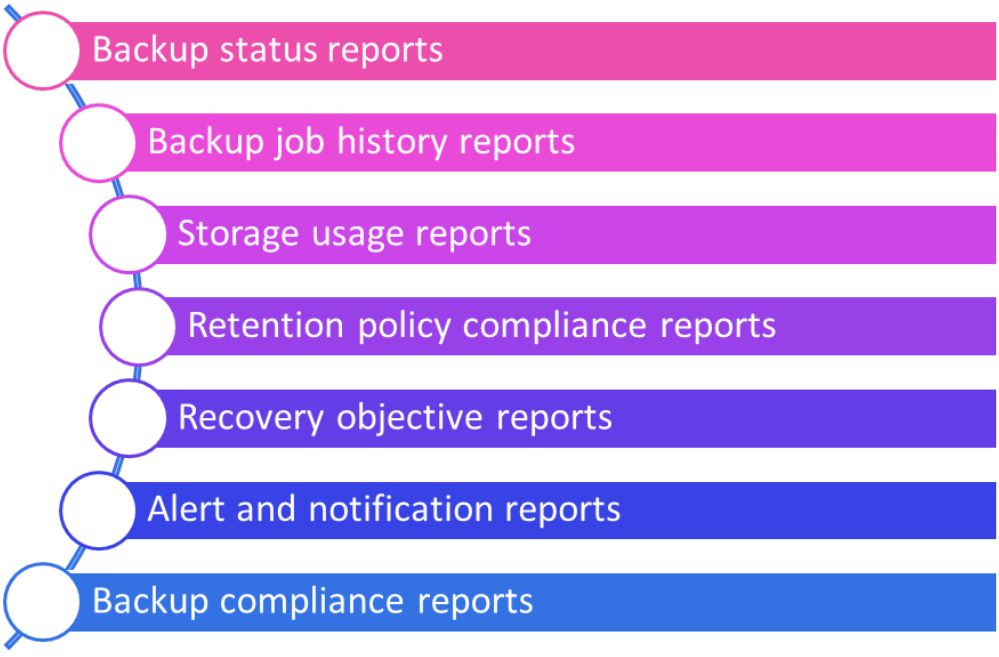
At the enterprise level, comprehensive backup reporting encompasses a diverse range of metrics and insights:

- **Backup status reports:** Providing real-time visibility into the status of backup operations, including successful completions, failures, and pending tasks
- **Backup job history reports:** Offering a detailed overview of backup job execution history, facilitating trend analysis and performance optimization
- **Storage usage reports:** Assessing storage utilization trends and identifying opportunities for capacity optimization and cost savings
- **Retention policy compliance reports:** Ensuring adherence to data retention policies and regulatory requirements, minimizing compliance risks
- **Recovery objective reports:** Assessing the effectiveness of backup strategies in meeting recovery objectives and minimizing downtime
- **Alert and notification reports:** Notifying administrators of critical events, errors, or anomalies requiring immediate attention
- **Backup compliance reports:** Providing insights into backup policy enforcement and adherence to best practices
- **Trend analysis reports:** Identifying patterns and trends in backup performance, enabling proactive optimization and resource allocation

In summary, detailed automated backup reporting is indispensable for organizations seeking to maintain data integrity, meet compliance requirements, and mitigate operational risks. By investing in solutions that offer comprehensive reporting capabilities and automation features, organizations can empower their IT teams to effectively monitor, manage, and optimize backup operations, ensuring the resilience and availability of critical data assets.

Streamlining and automating the creation of comprehensive backup reports can greatly increase productivity and guarantee that administrators have easy access to critical data. Organizations can increase visibility into backup operations, expedite backup reporting procedures, and improve the overall dependability and efficacy of their backup strategies by using automated and user-friendly reporting methods.

Figure 6: The top enterprise-level backup reports



Source: Omdia

The future: More use of artificial intelligence and machine learning in backup

As companies strive to do more with less, the integration of artificial intelligence (AI) and machine learning (ML) into backup processes is gaining momentum. This shift toward AI-powered backups is driven by the imperative to drive operational efficiencies while enhancing data protection measures.

One key area where AI and ML are making an impact is in semicustom reporting. By leveraging AI algorithms, companies can generate tailored reports that provide deeper insights into backup performance and data integrity, empowering decision makers with actionable information.

Moreover, AI is revolutionizing alert response by guiding users in real time. With AI-driven alerts, IT teams can swiftly identify and address potential issues before they escalate, minimizing downtime and optimizing resource allocation.

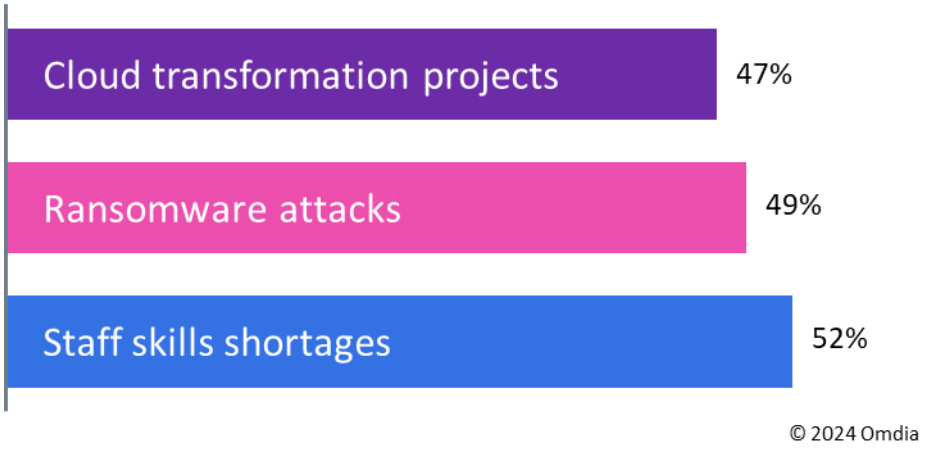
AI's influence extends across various facets of backup operations:

- Intelligently scheduling backups based on data usage patterns and workload priorities, optimizing resource utilization and minimizing disruption
- Early detection of ransomware compromises through anomaly detection algorithms, enabling prompt response and containment measures
- Conducting deep threat analysis to identify and mitigate potential security vulnerabilities and data breaches
- Identifying misconfigurations in backup settings and infrastructure, reducing the risk of data loss and ensuring compliance with best practices
- Removing malware before initiating data recovery processes, safeguarding restored data from potential contamination
- Identifying unattached remediation copies and unclassified data, enabling organizations to enact proper controls and ensure data governance
- Leveraging natural language processing (NLP) for support and troubleshooting, enhancing user experience and streamlining issue resolution processes

Data protection vendors are actively working to incorporate AI and ML capabilities into their products, recognizing the transformative potential of these technologies in enhancing backup efficiency and resilience. Looking ahead, it is reasonable to expect that threat hunting and risk analysis capabilities will become "table stakes" features within the next few years, further cementing the role of AI in shaping the future of backup operations.

The incorporation of AI capabilities into data protection products represents a significant advance. With AI-driven technologies, organizations can overcome the challenges posed by skills shortages and enhance their data protection posture in an increasingly complex threat landscape. It is reasonable to expect AI-based threat-hunting and risk analysis capabilities to be table stakes within the next few years.

Figure 7: There is a high level of skills shortage in many data centers



Source: Omdia Cybersecurity Decision Maker Survey 2022

How best to back up in a multicloud world

In the dynamic landscape of multicloud environments, effective application of backups requires a nuanced approach that addresses the unique challenges posed by public cloud infrastructure. These challenges include data transfer limitations, the need to navigate data silos across different cloud providers, and the varied mechanisms employed by individual applications for backup and recovery.

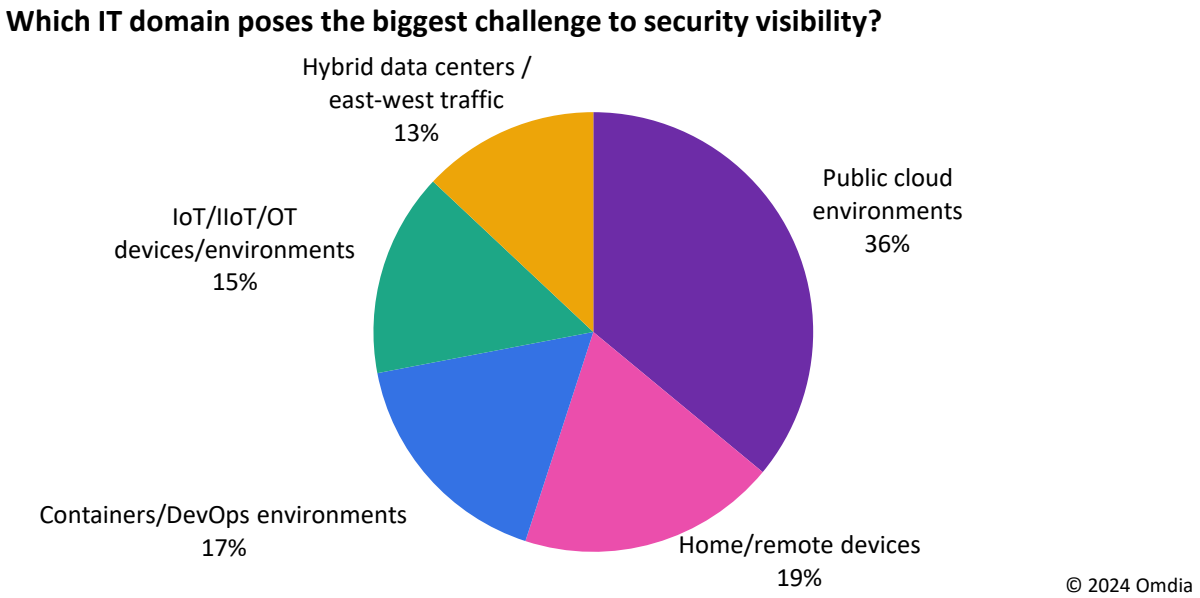
To navigate these challenges, organizations must bear in mind some key considerations:

- Centralization of backups, essential to streamline management and ensure consistency across diverse cloud environments
- Establishing recovery sites in new locations to enhance resilience and mitigate the risk of localized disruptions
- Leveraging movable media and backup servers to facilitate data mobility and enable seamless backups across multiple cloud platforms
- Maintaining synchronized copies of data in the cloud to ensure data consistency and availability for recovery purposes
- Redirecting recovery processes to compatible platforms to accommodate the unique infrastructure requirements of different cloud providers
- Embracing relocatable media and media migration capabilities to facilitate data movement and adaptability in multicloud environments

By proactively addressing these considerations, organizations can optimize their backup strategies in the multicloud era, ensuring data resilience, availability, and agility across diverse cloud ecosystems.

Public cloud data centers have transformed the IT landscape in recent years, but with the benefits come unique security challenges. Visibility is the most pressing concern. Public cloud environments are highly dynamic, and resources are provisioned, scaled, and decommissioned rapidly in response to changing demand. This can lead to security blind spots. Also, because the cloud provider and user share data security responsibilities, there may be misunderstandings and protection lapses because of a lack of clarity around responsibilities.

Figure 8: Public and hybrid clouds present their own security challenges



Source: Omdia Cybersecurity Decision Maker Survey 2022

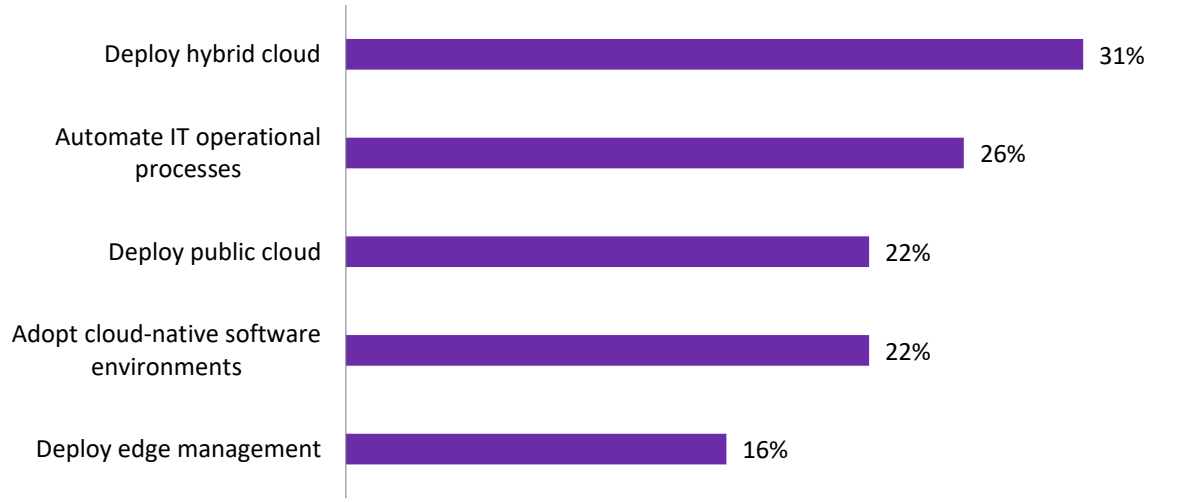
The effectiveness of quality hybrid solutions

Quality hybrid solutions offer a powerful combination of benefits, combining the strengths of on-premises infrastructure with the scalability and flexibility of the cloud. Hybrid solutions provide scalable storage capacity, allowing organizations to adapt to changing data requirements while optimizing retention through intelligent data placement strategies. Moreover, they enable organizations to manage the blast radius for disaster recovery (DR) scenarios by leveraging the cloud as a secondary site for recovery, thereby enhancing resilience and reducing downtime.

When hybrid solutions from an independent software vendor (ISV) are being evaluated, several key factors should be considered. These include support for a broad set of cloud targets, encompassing major providers such as Microsoft Azure, AWS S3, Google Cloud, Alibaba Cloud, Ceph, Scality, and Cloudian. Additionally, capabilities for seamless synchronization and resynchronization to and from the cloud are essential for maintaining data consistency and availability across hybrid environments. Furthermore, the flexibility of media that can be moved and executed upon anywhere is crucial for enabling agile data management and ensuring compatibility with diverse infrastructure configurations. By prioritizing these considerations, organizations can harness the full potential of quality hybrid solutions to address their evolving data management needs and drive business innovation.

Adoption of hybrid clouds is a key priority for infrastructure development because it provides an adaptable, scalable, and economical way to modernize IT environments. In the data protection area, it also helps meet the need for a remote air-gapped data vault, data sovereignty, compliance, and DR. Hybrid cloud strategies often allow organizations to enhance the agility, efficiency, and innovation of their IT operations while retaining control over their data.

Figure 9: Top initiatives for developing infrastructures



Note: Excludes security, cost reduction, and AI/ML.

Source: Omdia Data Center and Operations study

Consider cloud-based backups as an important copy

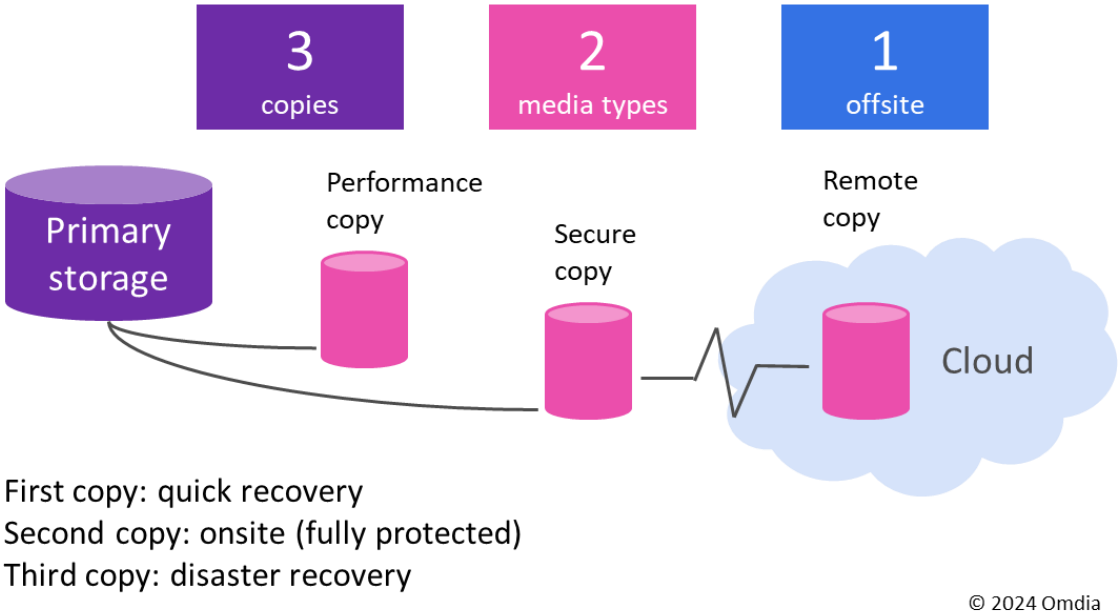
Incorporating cloud-based backups into your data protection strategy offers several advantages, making it an indispensable component of a robust backup solution. Automated backup copy processes streamline data replication, reducing manual intervention and enhancing operational efficiency. Cloud backups that leverage continuously updated copies of data ensure that critical information is always current and accessible. Additionally, cloud backups offer a range of recovery options, enabling organizations to tailor their recovery strategies to suit users' specific needs and preferences.

When a backup product is being selected, several factors should be considered to ensure optimal performance and reliability. Cloud-based data synchronization capabilities are crucial for maintaining consistency across backup copies and facilitating seamless recovery processes. Adhering to a 3-2-1 backup architecture enhances data protection and resilience.

One thing to ensure is that cloud connections have sufficient internet bandwidth, because that is essential for efficient data transfer to cloud storage. Also enforcing compliance with object store standards, such as S3 compliance, ensures multicloud interoperability and compatibility. Ultimately, by prioritizing these considerations and selecting a backup solution that aligns with enterprise requirements, organizations can leverage the benefits of cloud-based backups to safeguard their data effectively and mitigate the risk of data loss or downtime.

Even when the cloud is used as part of a backup, the 3-2-1 data protection strategy should be used. Three copies of data are stored on two different media, with one copy stored offsite. The cloud store can be included as one of the three copies.

Figure 10: Making cloud a part of the protection strategy



Source: Omdia

Ease some of the IT burden with backup as a service

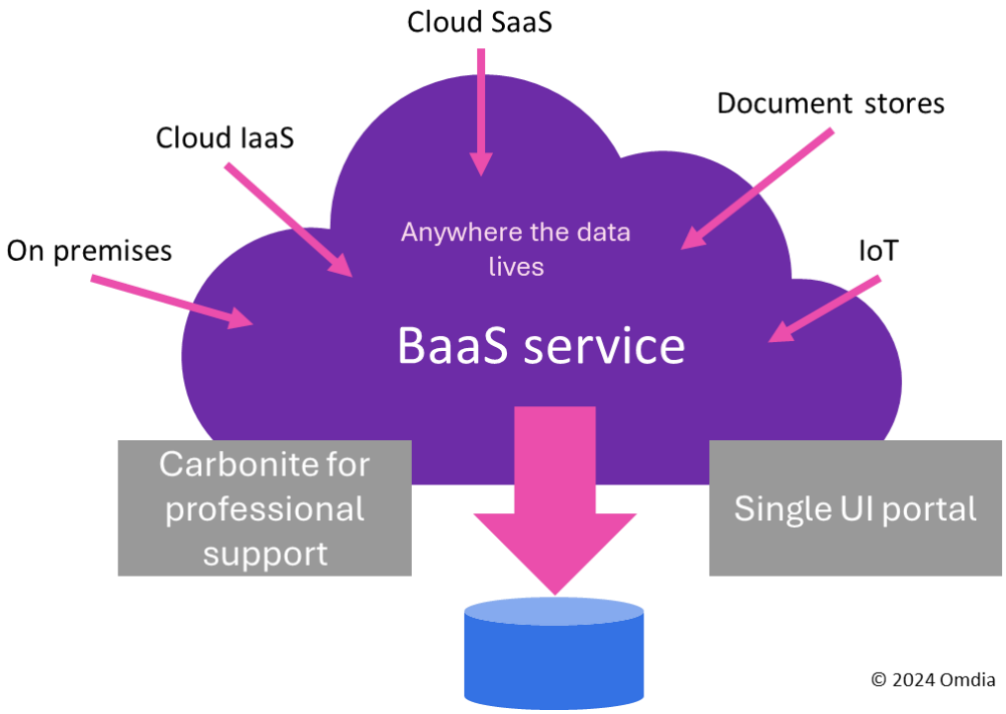
Embracing backup-as-a-service (BaaS) methods offers organizations a way to alleviate IT burdens by entrusting backup responsibilities to a fully managed service provider. By offloading backup tasks, IT teams can focus their efforts on driving innovation rather than managing routine operations. Moreover, BaaS eliminates the need for upfront capital expenditure, improves financial flexibility, and can reduce IT costs.

BaaS providers bring specialized expertise to the table, enhancing security measures and bolstering reliability to safeguard critical data. This managed service model extends across various environments, including on-premises infrastructure, cloud infrastructure as a service (IaaS), and software-as-a-service (SaaS) applications, ensuring comprehensive coverage regardless of data location.

When considering BaaS solutions, organizations should prioritize established services and seek vendors with robust management capabilities. Professional support partners can further enhance the reliability and effectiveness of BaaS implementations, ensuring that organizations receive the necessary assistance and expertise.

You can stop managing backups onsite by using a BaaS provider to handle and maintain the backup process. Install copy software on your systems and select the desired service level, then the service provider does the rest. The local server software sends data copies to a backup target. In the event of data loss, the necessary files are recovered by the BaaS provider back to the original local or cloud servers.

Figure 11: Offload work to a fully managed backup service



Source: Omdia

Final thoughts

Organizations face new possibilities and difficulties as the data protection and backup landscape continues to change quickly. Businesses are keeping their data in multiple clouds and on premises, and there has never been a more pressing demand for flexible backup solutions. Not only that, but backup solutions that are also resistant to ransomware attacks—which have become more frequent in recent years—are serving as undefeatable data repositories, ensuring recovery from attack incidents. Additionally, there is a rising need for data governance tools to assist enterprises in adhering to data sovereignty laws by tracking data lineage and ensuring placement controlled to sovereignty regulation compliance.

Innovations in backup technology are essential to address these evolving needs effectively. Organizations require backup solutions that can seamlessly operate across various cloud platforms and on-premises infrastructure, providing guaranteed data protection across a variety of environments, including VMs, bare metal, containers, and edge devices.

Comprehensive monitoring and deep insight into backup operations are crucial for organizations to maintain visibility and control over their data protection processes. Additionally, automation and orchestration capabilities enable organizations to improve overall process efficiency, streamline operations, and reduce manual intervention.

In conclusion, as organizations navigate the complexities of modern data environments, they must embrace innovative backup solutions that offer comprehensive protection, seamless operation, and advanced features to address the evolving landscape of data protection and backup effectively.

Appendix

To learn more

Webinar team will update this page

Watch this free webinar

"Automating networks with intent, AI, and machine learning"

presented by Omdia and our partner(s) Frinx and Fujitsu

The webinar can be accessed at: link

For additional Omdia events, visit:

https://technology.informa.com/Events

Follow the conversation: @OmdiaHQ, @Omdia_Cloud

Author

Dennis Hahn
Principal Analyst, Cloud & Data Center Research Practice
customersuccess@omdia.com

Get in touch

www.omdia.com
customersuccess@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa Tech, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

Copyright notice and disclaimer