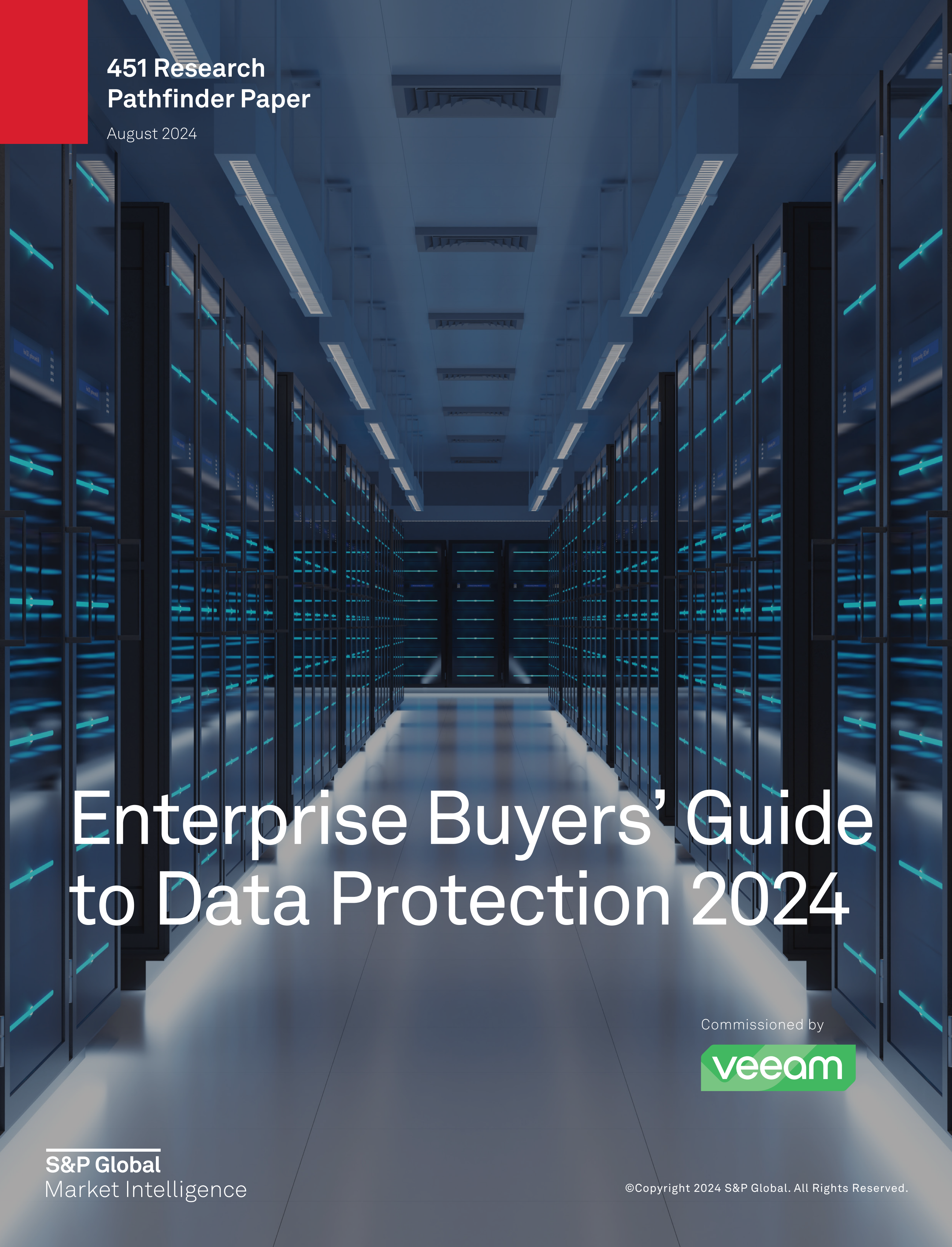


451 Research
Pathfinder Paper

August 2024

Enterprise Buyers' Guide to Data Protection 2024

Commissioned by
veeam

S&P Global
Market Intelligence

Table of contents

Executive summary

Although most organizations already have essential data protection capabilities for backup and disaster recovery, new challenges and emerging innovations are driving progressive companies to modernize their data protection tools and processes. The Enterprise Buyers Guide to Data Protection 2024 is designed to highlight key market trends and challenges while providing information on what capabilities and processes organizations should consider implementing to ensure their investment in data protection not only meets current requirements but can adapt to modern workloads, including software as a service and cloud-native architectures, which require higher levels of scalability and data mobility relative to traditional and legacy applications. Data protection delivery has evolved beyond on-premises software and appliances to include service offerings, such as online backup and disaster recovery as a service (DRaaS), that can help relieve the day-to-day operational and management burden of data protection tasks.

The Enterprise Buyer's Guide to Data Protection 2024 covers five key actions for modernizing and enhancing data protection and resiliency:

1. Integrate cloud resources to boost scalability and flexibility

2. Choose offerings that harden backups and detect cybersecurity threats earlier

3. Leverage services to offload operational data protection burdens

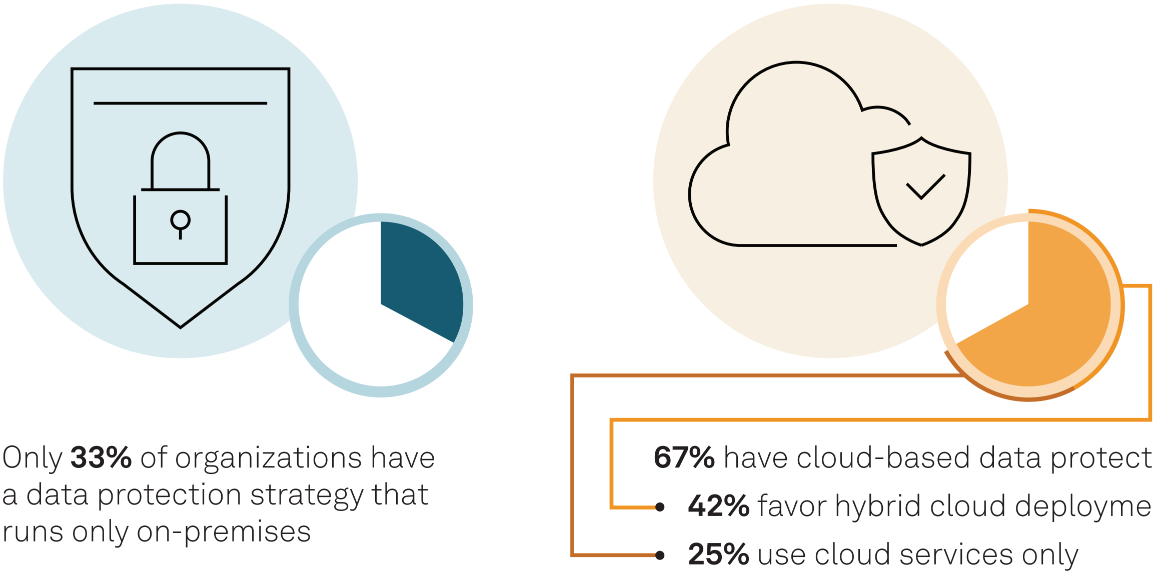
4. Extend and modernize data protection for SaaS and containers

5. Choose platforms with AI enhancements to improve operational efficiency

Integrate cloud resources to boost scalability and flexibility

Data highlight

Figure 1: Cloud and hybrid backup services push ahead of on-premises-only data protection



Only **33%** of organizations have a data protection strategy that runs only on-premises

67% have cloud-based data protection:

- **42%** favor hybrid cloud deployment
- **25%** use cloud services only

Q. Which of the following best describes your organization's current use of data protection (e.g., backup, disaster recovery)?
Base: IT decision-makers whose organizations use on-premises storage systems (n=269).
Source: 451 Research's Voice of the Enterprise: Storage, Disaster Recovery 2023.

Why it matters

Disaster recovery and data protection are top challenges for organizations for several reasons. For example, 71% of respondents to our Voice of the Enterprise: Storage, Disaster Recovery 2023 survey have experienced a significant outage, with a mean cost of $2.15 million. This mean cost increased 34% from the previous year's study. Data protection challenges will only escalate, with data under management expected to grow by 23% in the next 12 months.

The most common consequence of recent outages was lost worker productivity, cited by 48% of respondents, while 32% of respondents lost data. As customer experience grows in importance across industries, it is worth noting that outages leading to lost revenue from missed business opportunities (30%), damaged business reputation (20%) and lost customer loyalty (14%) all negatively impact how customers rate their vendors.

The 3-2-1 rule, an industry standard for backup operations, calls for organizations to have three copies of data, stored in two different storage mediums with one copy stored in a remote site.

Recently, the 3-2-1 rule has been enhanced to include immutable storage capabilities, which prevent backup repositories from being deleted or corrupted, either intentionally by attackers or accidentally by staff members with credentials. Leveraging immutable storage for every workload, regardless of where it resides, is made easier by the broad availability of immutable cloud storage services.

What to look for

- Data protection that facilitates hybrid cloud or cloud-only architectures
- Immutable storage in a remote geographic location
- Cloud and datacenter providers with sustainable infrastructures

Data protection workloads such as backup, disaster recovery and data archiving now use public cloud resources and service providers to fulfill off-site storage requirements and to act as a second storage medium that complements on-premises repositories that facilitate rapid, local restoration operations.

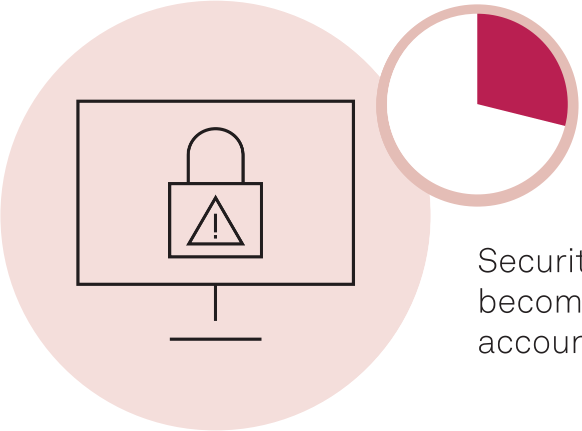
In data protection use cases, only 33% of respondents favor on-premises-only deployments. This contrasts with 42% who favor hybrid cloud deployments, in which a smaller on-premises backup repository is maintained for rapid recovery while cloud storage handles long-term storage of backups and acts as the off-site repository. For organizations averse to maintaining a remote recovery site for protection against natural disasters, cloud-based data protection offloads the cost burden of building and maintaining those sites.

A quarter of respondents would prefer to completely rely on cloud-based services such as online backup and DRaaS and avoid having on-premises backup appliances or software. With rapidly emerging environmental, social and governance (ESG) requirements driving organizations to reduce their energy consumption, the migration of workloads to public clouds is likely to continue. More than three-quarters (80%) of respondents to our Voice of the Enterprise: Storage, ESG Attitudes 2023 study agree that their organization is moving data and workloads to public clouds to help meet their company's ESG strategy.

Choose offerings that harden backups and detect cybersecurity threats earlier

Data highlight

Figure 2: Security issues are the leading cause of outages



Security issues such as ransomware have become the leading cause of outages, accounting for **29%** of recent outages

Q. What was the cause of your organization's most recent outage that resulted in lost data or affected worker productivity? Please select all that apply.
Base: IT decision-makers whose organizations experienced an outage/downtime that resulted in lost data or productivity (n=183).
Source: 451 Research's Voice of the Enterprise: Storage, Disaster Recovery 2023.

Why it matters

Many companies have recently put effort into hardening their recovery infrastructure with immutable storage and remote backup repositories. But attackers are now seeking out soft targets, such as administrator accounts and other vulnerabilities, that can compromise data protection from within. Even if organizations set up frequent backups and immutable storage, a compromised administrator account would allow an assailant to delete data and orchestration information, catastrophically hindering recovery operations.

What to look for

Solutions that proactively detect security issues

The ability to create isolated testing and forensics environments

Ransomware recovery guarantee programs

By implementing zero-trust principles, organizations can create a stronger foundation for their resiliency practices. Least-privilege access should be used to limit user, device and application access to short durations and just enough access to get tasks accomplished. Resiliency systems and software should never implicitly trust and should always authenticate and authorize using identity and access management contexts together with multi-factor authentication to ensure unauthorized users cannot disable data recovery capabilities, even if an administrator password is stolen.

Data protection tools should also integrate well with security information and event management platforms. Often, threat actors attack backup infrastructure as part of their penetration strategy. By leveraging insights from data protection tools, behavioral anomaly detection is better positioned to detect suspicious actions, such as backup encryption and deletion, before attackers can act.

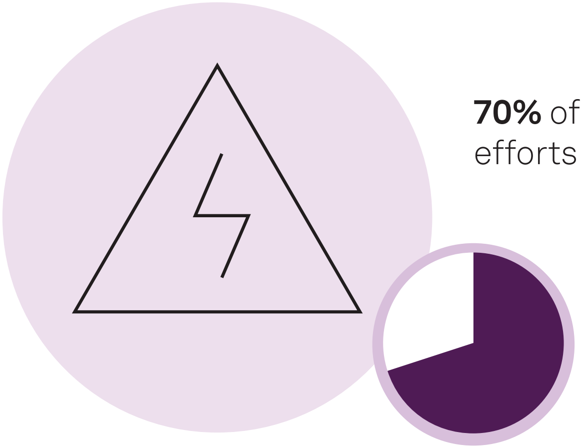
The ability to create a secure and isolated testing environment is a key requirement that comes into play after an attack has occurred. Using such an environment, security and data protection professionals can ensure that recovered data is clear of infections and run tests without the risk of spreading malware to production environments.

Ransomware recovery guarantee programs are becoming common, providing customers with reimbursement if their data protection platform is unable to restore company data from its most recent and usable backup. But the true value of these programs is not limited to reimbursement. These programs also require a services and support commitment — including quarterly assessments by the vendor — to ensure that security best practices are implemented and maintained.

Leverage services to offload operational data protection burdens

Data highlight

Figure 3: Most outages require substantial recovery efforts



70% of outages require moderate to significant efforts to complete failback

Q. How much effort is required to resume normal operations after a failure (i.e., a failback)?
Base: IT decision-makers whose organizations use on-premises storage systems (n=260).
Source: 451 Research's Voice of the Enterprise: Storage, Disaster Recovery 2023.

Why it matters

A fifth of respondents say that a lack of skilled staff is among their top pain points. Some organizations report difficulty meeting disaster recovery requirements and completing jobs within their backup windows. Data protection challenges will only become more difficult as data growth continues, and although new hybrid and multicloud infrastructures facilitate distributed environments and workload portability, they also add a new layer of complexity.

> **"We have outages all the time. Big environment, so they're not necessarily serious outages, but... [teams] spring into action when there's an outage. And then a more senior team that springs into action if it's got serious financial implications or regulatory, or impact our customers might view negatively."**

IT engineering manager/staff
10,000 – 49,999 employees, $10 billion+ revenue, financial services

Source: 451 Research's Voice of the Enterprise in-depth interview, April 2024.

In some cases, such as the one described by the financial services customer quoted above, outages have become extremely common. Senior staff often only have time to focus on mission-critical workloads. For organizations with highly geographically distributed environments, the inability to hire employees to fill skill gaps becomes glaring, particularly in remote regions.

Many organizations have issues with disaster recovery testing, including 8% of respondents who say they either do not have a disaster recovery plan or never test it. Only 27% of respondents say they test their disaster recovery more than twice a year, while 39% say they only do annual testing.

What to look for

DRaaS and online backup services to reduce the data protection burden

Service providers that can facilitate DR testing

MSPs and other service providers with geographic reach and expertise to accelerate recovery

An online backup service can provide an entry point for organizations to reduce the burden of day-to-day backup operations. Much of the operational labor lies with the underlying infrastructure management of backup storage. Online backup services offer a turnkey "easy button" to get started fast, especially for cloud-native and SaaS-based workloads.

Many organizations are turning to cloud services and managed service providers (MSPs) to reduce their data protection burden. They can leverage managed data protection services to fulfill requirements when hiring a dedicated data protection specialist is not possible. Cloud-based disaster recovery services can also serve as a cost-efficient alternative to maintaining remote recovery sites with infrastructure components to facilitate a failover.

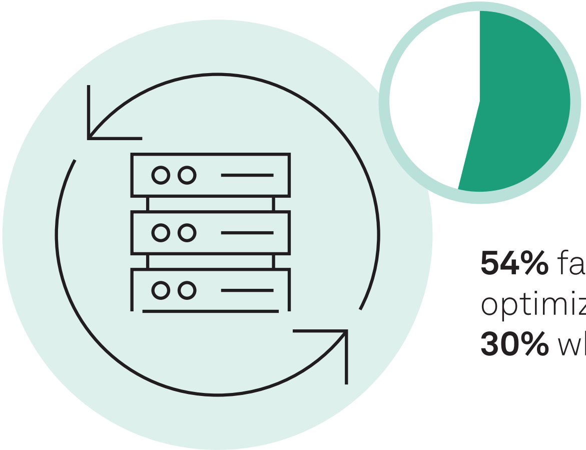
Protracted outages negatively impact an organization's recovery point objectives and recovery time objectives, which leads to increased losses when recovery operations are slow or unsuccessful. In addition to helping improve day-to-day operations, experienced data recovery service providers can provide great value when an incident occurs.

Service providers can manage scheduled backups and ensure that they consistently run to completion to meet service-level agreements required by customers. Through expertise and automation, service providers also help organizations with time-consuming and tedious tasks (such as disaster recovery testing and runbook documentation, which are both essential for ensuring healthy recovery operations).

Extend and modernize data protection for SaaS and containers

Data highlight

Figure 4: Most organizations prefer tailored backup and recovery tools for containerized workloads



54% favor using backup and disaster recovery tools optimized for container platforms, in contrast to just **30%** who rely on legacy data protection tools

Q. What is your organization's primary data protection strategy for containerized applications and data volumes?
Base: All respondents, excluding respondents whose organizations do not use containers (n=381).
Source: 451 Research's Voice of the Enterprise: Cloud Native, Resiliency 2023.

Why it matters

Modern enterprise data protection must go beyond virtual machines, legacy workloads and network-attached storage/file servers running on physical systems. It must account for newer architectures such as SaaS platforms and containers.

SaaS platforms such as Microsoft 365 and Salesforce have hosted important workloads for years. But the infrastructure and software running these platforms is the responsibility of the SaaS vendor, and many customers do not factor in the importance of third-party backup capabilities. With the increasing threat of ransomware — and with the potential for data loss due to accidental or malicious deletion, whether by employees or attackers — the need for SaaS backups has become widely acknowledged.

Data protection must also extend to cloud-native technologies such as containers to protect the persistent data being created on these platforms. From modern AI and large language model (LLM) workloads to critical DevSecOps functions, the need for data protection designed for cloud-native platforms will only increase.

What to look for

- Data protection tools designed for containers and cloud-native environments
- Third-party tools and services that can protect SaaS workloads
- Data protection vendors that are expanding their modern workload coverage

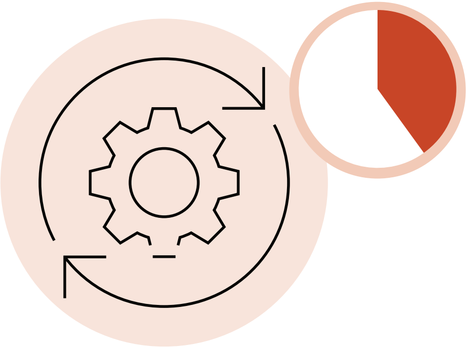
More than a third (35%) of respondents to our Voice of the Enterprise: Storage, Disaster Recovery 2023 study rely primarily on third-party backup tools for data protection with SaaS applications. We expect to see these third-party backup tools expand offerings and add coverage across infrastructure as a service, platform as a service and SaaS workloads (i.e., Google Workspace, ServiceNow and Microsoft Dynamics 365).

In the cloud-native space, persistent container workloads have become commonplace. Only 2% of respondents to our Voice of the Enterprise: Cloud Native, Resiliency 2023 study are not backing up containerized applications and data volumes. More than half (54%) favor using backup and disaster recovery tools optimized for container platforms — in contrast to 30% who rely on legacy data protection tools. While 14% of respondents choose to run automated snapshots through their own scripts, this method could lead to data loss if policies are not adjusted to match application changes or if the DevOps professional that created the scripts leaves the organization.

Choose platforms with AI enhancements to improve operational efficiency

Data highlight

Figure 5: Use of automation in backup and recovery is increasing



40% of respondents already use IT automation to enhance their backup and recovery management

Nearly **1 in 5 (19%)** identify backup and recovery management among their top three IT processes that would benefit the most from automation

For which of the following processes — if any — does your organization use IT automation technology? Please select all that apply.
Base: Respondents whose organization has DevOps in use or in discovery/POC (n=476).
Source: 451 Research's Voice of the Enterprise: DevOps, IT Automation 2023.
And which of the following IT processes at your organization would benefit the most from automation technology?
Please select up to three.
Base: Respondents whose organization has DevOps in use or in discovery/POC (n=451).
Source: 451 Research's Voice of the Enterprise: DevOps, IT Automation 2023.

Why it matters

High operational costs and lack of skilled staffing clearly indicate that data protection processes must become easier to maintain, less time-consuming and increasingly automated.

Many organizations already leverage IT automation to enhance their data protection and recovery capabilities. For example, many teams use automated alerts to remediate backup job failures. In addition to time savings, automation can reduce the potential for human error and ensure that backup and recovery operations are executed successfully, consistently, securely and efficiently.

We have discussed how organizations could use service providers to reduce the operational burdens of data protection. But for those unwilling to use service providers or unable to find adequate service offerings, AI-enhanced tools could help handle the data protection burden with IT generalists in place of dedicated specialists.

What to look for

- Data protection tools that provide APIs and other tools to facilitate IT automation
- AI-enhanced management tools that proactively identify vulnerabilities and configuration errors
- Tools that employ generative AI to improve product adoption and user experience

Data protection is resource-intensive and time-consuming, even before an incident occurs. Automation helps organizations offload many tasks, including provisioning, the implementation of new software and hardware, and backup and disaster recovery maintenance. Disaster recovery orchestration — which is required to prepare execution venues and ensure processes are brought back correctly to production — is another key process that can benefit from automation. Testing and documentation can also be streamlined, reducing downtime and compliance burdens for organizations.

Proactive tools that detect vulnerabilities before they become outages are more important than ever, given that many companies cannot acquire the skilled IT staffers they need to maintain operations. Tools with AIOps capabilities, for instance, have become commonplace. These offerings learn from previous outages and configuration mistakes to warn organizations of potential issues and provide recommendations to eliminate vulnerabilities.

As organizations seek to optimize spending and reduce technical debt, data protection tools breathe new life into capabilities by building GenAI assistants into their user workflows. These assistants often query product documentation, community articles, and more via LLMs, to suggest answers to common user-experience questions and reduce time spent in research.

Content provided by veeam

As data explodes year on year and sprawls across multiple clouds, countless endpoints, and diverse geographic locations, enterprise organizations are faced with a perfect storm of complexity and threats.

As the #1 Global Leader in Data Protection & Ransomware Recovery, Veeam offers unparalleled support to enterprise-size organizations, enabling 74% of the Global 2,000 to achieve faster recovery from data disruption so they can keep their business running.

Join the 92% of organizations increasing their data protection budgets for 2024 and discover how Veeam uniquely powers data resilience. Explore how Veeam seamlessly protects cloud, virtual, physical, SaaS, and Kubernetes environments through deployment models that meet your teams where they are today — and tomorrow.

Want to learn more? Here are 5 Reasons to Switch to Veeam for Cyber Resilience.

About the author

Henry Baltazar

Research Director, Storage

Henry Baltazar is research director of the 451 Research Storage channel within S&P Global Market Intelligence, with a focus on data storage. In his current role, Henry analyzes the market trends around environmental, social and governance (ESG) storage challenges, infrastructure modernization and resiliency. He publishes reports on trends in data storage, disaster recovery and hybrid cloud. He is often cited as a subject expert by publications such as MIT Technology Review, Forbes and TechTarget.

Henry arrived at S&P Global Market Intelligence through its 2019 acquisition of 451 Research, where he began working as an analyst in August 2006. After spending three years running the storage research practice at Forrester, he returned to 451 Research in 2015 to fill the research director role and lead the storage practice.

Henry graduated from the University of California, Berkeley with a bachelor's degree in environmental sciences.

About this paper

A Pathfinder paper navigates decision-makers through the issues surrounding a specific technology or business case, explores the business value of adoption, and recommends the range of considerations and concrete next steps in the decision-making process.

About S&P Global Market Intelligence

At S&P Global Market Intelligence, we understand the importance of accurate, deep and insightful information. Our team of experts delivers unrivaled insights and leading data and technology solutions, partnering with customers to expand their perspective, operate with confidence, and make decisions with conviction.

S&P Global Market Intelligence is a division of S&P Global (NYSE: SPGI). S&P Global is the world's foremost provider of credit ratings, benchmarks, analytics and workflow solutions in the global capital, commodity and automotive markets. With every one of our offerings, we help many of the world's leading organizations navigate the economic landscape so they can plan for tomorrow, today. For more information, visit www.spglobal.com/marketintelligence.

CONTACTS

Americas: +1 800 447 2273
Japan: +81 3 6262 1887
Asia-Pacific: +60 4 291 3600
Europe, Middle East, Africa: +44 (0) 134 432 8300

www.spglobal.com/marketintelligence
www.spglobal.com/en/enterprise/about/contact-us.html

These materials have been prepared solely for information purposes based upon information generally available to the public and from sources believed to be reliable. No content (including index data, ratings, credit-related analyses and data, research, model, software or other application or output therefrom) or any part thereof (Content) may be modified, reverse engineered, reproduced or distributed in any form by any means, or stored in a database or retrieval system, without the prior written permission of S&P Global Market Intelligence or its affiliates (collectively S&P Global). The Content shall not be used for any unlawful or unauthorized purposes. S&P Global and any third-party providers (collectively S&P Global Parties) do not guarantee the accuracy, completeness, timeliness or availability of the Content. S&P Global Parties are not responsible for any errors or omissions, regardless of the cause, for the results obtained from the use of the Content. THE CONTENT IS PROVIDED ON "AS IS" BASIS. S&P GLOBAL PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, FREEDOM FROM BUGS, SOFTWARE ERRORS OR DEFECTS, THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED OR THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION. In no event shall S&P Global Parties be liable to any party for any direct, indirect, incidental, exemplary, compensatory, punitive, special or consequential damages, costs, expenses, legal fees, or losses (including, without limitation, lost income or lost profits and opportunity costs or losses caused by negligence) in connection with any use of the Content even if advised of the possibility of such damages.

S&P Global Market Intelligence's opinions, quotes and credit-related and other analyses are statements of opinion as of the date they are expressed and not statements of fact or recommendations to purchase, hold, or sell any securities or to make any investment decisions, and do not address the suitability of any security. S&P Global Market Intelligence may provide index data. Direct investment in an index is not possible. Exposure to an asset class represented by an index is available through investable instruments based on that index. S&P Global Market Intelligence assumes no obligation to update the Content following publication in any form or format. The Content should not be relied on and is not a substitute for the skill, judgment and experience of the user, its management, employees, advisors and/or clients when making investment and other business decisions. S&P Global keeps certain activities of its divisions separate from each other to preserve the independence and objectivity of their respective activities. As a result, certain divisions of S&P Global may have information that is not available to other S&P Global divisions. S&P Global has established policies and procedures to maintain the confidentiality of certain nonpublic information received in connection with each analytical process.

S&P Global may receive compensation for its ratings and certain analyses, normally from issuers or underwriters of securities or from obligors. S&P Global reserves the right to disseminate its opinions and analyses. S&P Global's public ratings and analyses are made available on its websites, www.standardandpoors.com (free of charge) and www.ratingsdirect.com (subscription), and may be distributed through other means, including via S&P Global publications and third-party redistributors. Additional information about our ratings fees is available at www.standardandpoors.com/usratingsfees.