White Paper

SaaS Backup and Recovery: Simplified Data Protection Without Compromise

Sponsored by: Commvault

Phil Goodwin
November 2019

IDC Opinion

Modern businesses are constantly looking for an edge in the marketplace. For many, this involves becoming a "data driven" organization, whereby business leaders look for data insights that lead to more quickly exploiting market opportunities, adjusting to changing business circumstances, or solving problems that affect the customer experience and satisfaction. IDC estimates that 60% of organizations have embarked on a digital transformation (DX) strategy with the aim of becoming data driven. Thus these organizations are seeking faster, more accurate, and insightful information to drive better decision making. Successful digital transformation is not possible without data availability, and data protection is foundational to data availability. According to IDC research, more than half of all digital transformation initiatives involve improvements to data protection systems and strategies.

The data protection improvements sought by organizations take several forms: greater reliability (i.e., reduced data loss), simpler operations to reduce human labor, and faster data recovery for less downtime and lower cost. Organizations on a growth curve will also look for data protection solutions with the agility to adapt to new application deployments and platforms (i.e., on-premise and in the cloud), new threats to data vulnerabilities (i.e., malware and ransomware), and changing regulatory and data governance requirements.

Among the most important measures of data protection success is SLA attainment, and three such SLA measures are most important: downtime, recovery time objective (RTO), and recovery point objective (RPO). IDC research finds that the average cost of downtime is $250,000 per hour. Obviously, less downtime is better, and this benchmark helps organizations empirically determine the value of data availability improvements. Currently, the best practice RTO is 1 hour while the best practice RPO is 15 minutes, though these SLAs will vary by application, industry, and other factors. Organizations that meet or beat these SLAs are likely to have a data availability advantage over competitors and, therefore, are in a better position to exploit DX as a competitive differentiator.

IDC research also shows that 70% of CIOs have a "cloud first" strategy. For many, this initially involves cloud-based data protection. In fact, our research further finds that 90% of organizations expect to use cloud for at least a portion of their data protection strategy. Because the majority of critical applications are still on-premise, IT organizations need hybrid cloud data protection for both on-premise and cloud. Moreover, as more applications are deployed in the cloud, organizations will look for cloud-based data protection solutions. Cloud repositories have the inherent advantage of providing off-premise data location for data survivability in the event of an on-premise disaster.

IDC offers the following recommendations for cloud-based data protection initiatives:

- Establish service levels (SLAs) in alignment with business requirements and look for solutions designed to meet them.
- Leverage the cloud for data survivability.
- Consider "as a service" (SaaS and/or backup as a service [BaaS]) solutions to simplify infrastructure requirements and operations while leveraging "on demand" pricing with seamless scaling.
- Calculate your cost of downtime and utilize cloud solutions to reduce downtime and yield a positive ROI.

Situation Analysis

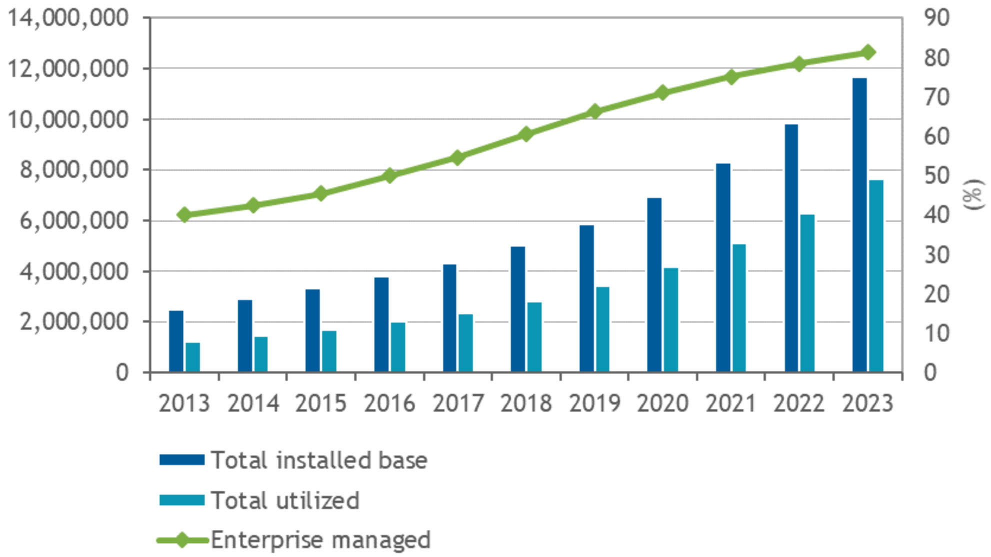
Although the majority of organizations have a "cloud first" strategy, most also continue to manage onsite applications and the backup infrastructure associated with them. However, many are moving away from backup specialists and instead are leaving the task to virtual infrastructure administrators or other IT generalists. Managing backup infrastructure can be labor intensive; devices, updates, upgrades, and so forth can result in many man-hours lost to these activities, which are nothing more than maintenance operations. In fact, these are lost man-hours that could be devoted to higher-value IT activities. With most IT organizations operating with a staff stretched thin, being able to redirect time to more strategic tasks can make a significant difference in overall effectiveness.

IDC's Global DataSphere research shows that data *creation* will continue to grow unabated, roughly 26% through 2023. We also forecast that data *stored* (StorageSphere) will grow at an even faster CAGR, 30% through 2023. At this rate, the volume of data stored more than doubles every three years on average. Figure 1 shows this growth in terms of the total amount of worldwide installed capacity, stored data, and the percentage that organizations will need to manage.

Figure 1 illustrates that IT organizations will be responsible for storing and managing an increasing percentage of the world's stored data. In fact, IDC projects that by 2023, organizations will need to manage over 80% (up from 40% in 2013) of the world's stored data, which equates to 6.2ZB across disk, flash, tape, and optical environments. Of course, any given organization on a business growth path may deal with substantially higher data growth rates. Because of this substantial rate of growth and data volume, organizations will seek data protection solutions that scale seamlessly, eliminating the need for disruptive forklift upgrades or changes in infrastructure platforms. These same organizations will value solutions that do not require them to overbuy capacity initially but rather solutions that can be provisioned with on-demand capacity and pricing that allows them to pay only for what they use.

FIGURE 1

Global StorageSphere Total Installed Capacity and Stored Data Forecast, 2013–2023 (PB)



Source: IDC's Global DataSphere and StorageSphere, 2019

In addition to data volume increasing, data protection is being further complicated by more diverse application environments. Data protection, by nature, is reactive in support of applications. Thus as the deployments become more diverse, data protection becomes more complicated. In addition to traditional on-premise applications, organizational data is being created by cloud-native apps, SaaS apps, IoT apps, and edge device apps. In many cases, these applications may be under the control of third-party application providers. In these situations, the IT organization has no direct control of the data and how it is protected, retained, or recovered. Moreover, data sovereignty requires organizations to control data location. The default data protection scheme is unlikely to meet organizational data retention and recovery SLAs. Some providers may offer enhanced data protection capabilities (usually at additional cost). Ultimately, however, it is the organization's responsibility to assure that all data — regardless of origin — is protected and retained according to organizational requirements.

Among the greatest concerns for many senior leaders, both IT and business, is ransomware. IDC research shows that 84% of organizations have suffered a malicious attack within the past 12 months. Recent ransomware attack strategies have been to first corrupt or encrypt the backup copies before attacking the production copy, making data restore difficult or impossible. To thwart these attacks, organizations need to implement an "air gap" between the primary copies and the backup copies so that the two are physically disconnected and cannot be attacked simultaneously. Utilizing cloud as the disconnected secondary copy is proving to be an attractive method for implementing the air gap.

Future Outlook

Our research finds that backup and recovery software as a service represents one of the fastest-growing segments of the data protection market. Software-only solutions for data protection and replication, delivered through the public cloud, will grow at a 9% CAGR through 2023. SaaS data protection solutions are cloud-based services that provide and manage a backup infrastructure in a multitenant environment. The data being backed up may be either on-premise or in the cloud. In fact, a common configuration is to have the backup control in the cloud for both on-premise and cloud workloads. Many organizations choose to keep a data copy on-premise for rapid restore while positioning a second copy in the cloud for data survival, DR preparation, or other purposes. Services include backup infrastructure management, with the implementation and management of backup policies and jobs handled by the organization, either internally or through a partner.

There are several reasons for the rising popularity of SaaS solutions. These include:

- **Almost limitless scale:** SaaS solutions are offered for the smallest organizations up to the very largest. Capacity is normally available on demand and charged on a consumption basis. Because SaaS is managed by a third party, IT organizations do not need to worry about keeping the infrastructure up to date, upgraded or updated.
- **Service flexibility and tailored solutions:** SaaS providers allow customers to choose solutions for their specific use case and allow customers agility and price flexibility to get what they need, when they need it, without having to purchase it in perpetuity.
- **Outsource infrastructure maintenance:** With SaaS, IT organizations can reduce the need for specialized backup activities. Rather than attending to the daily care and maintenance of backup infrastructure, IT staff can be freed up for other, higher-value tasks. IT staff members will also reduce risk as they no longer need to architect backup infrastructure, which becomes out of date, or other maintenance efforts.

Considering Metallic

Metallic is a new SaaS backup and recovery solution based on Commvault's data protection software suite, proven in the marketplace for more than 20 years. It is designed specifically for the needs of medium-scale enterprises but is architected to grow with them based on data growth, user growth, or other requirements. Metallic initially offers either monthly or annual subscriptions through reseller partners; it will be available through cloud service providers and managed service providers over time. The initial workload use cases for Metallic include virtual machine (VM), SQL Server, file server, MS Office 365, and endpoint device recovery support; the company expects to add more use cases and supported workloads as the solution evolves.

Metallic is designed to offer flexibility as one of the service's hallmarks. Aspects of this include:

- **On-demand infrastructure:** Metallic manages the cloud-based infrastructure components and software for the backup environment, though the customer will still manage any of its own on-premise infrastructure. This environment will support on-premise, cloud, and hybrid workloads. IT organizations are relieved of the daily task of managing the infrastructure components and do not have to worry about upgrades, OS or firmware updates and the like, for the cloud infrastructure, so people can repurpose that time saved toward other activities.

  Metallic offers preconfigured plans designed to have users up and running in approximately 15 minutes, eliminating the need for a proof-of-concept test. These preconfigured systems have Commvault best practices built into the design, or organizations can configure their own.

  With this option, the IT organization retains full control over the backup/recovery job management. Administrators manage backup policies and execute restore operations as well as daily backup administration.
- **Partner-delivered services:** Metallic plans to go to market with resellers that can offer a range of services on top of the basic solution's capabilities. These services will vary by provider and will give users a variety of choices when selecting a provider to match the services offered with the organization's needs.
- **"Bring your own storage":** Among the flexible options of Metallic, including VM and file or SQL database use cases, users can deploy their own storage, either on-premise or in the cloud, while utilizing the backup/recovery services of Metallic. The company refers to this option as "SaaS Plus."

Regardless of deployment option, Metallic includes a customer dashboard that provides visibility into the entire data protection estate that is managed by Metallic or its partners. This dashboard can help organizations assure service-level attainment (i.e., RPO and RTO) and measure uptime delivery improvements.

When data losses do occur, Metallic offers sophisticated and granular data restores. This can be all the way down to the individual file level to any desired target, whether on-premise or in the cloud. Restores can also be configured to choose the best storage option automatically without sacrificing performance.

Challenges and Opportunities

Although backup as a service (BaaS) is a rapidly growing market, it is also highly competitive. We estimate that more than 2,000 cloud service providers currently offer a data protection-as-a-service (DPaaS) solution. Thus consumer choice in such solutions is already very broad. Even so, the 2,000 providers represent a small fraction of the estimated 45,000 cloud service providers worldwide. Many of these providers desire a DPaaS solution, and a ready-to-go service such as Metallic is likely to be attractive to them, especially as they don't need to manage the back-end infrastructure, and there is an opportunity for Metallic to build out an ecosystem of providers. To be successful in the BaaS market, Metallic must enable an ecosystem of providers that layer a range of services on top of the solution to offer a rich range of service options.

Conclusion

Metallic represents Commvault's direct entry into one of the fastest-growing segments of the data protection market. Its hallmarks are simplicity and flexibility of deployment and use. IT organizations can rid themselves of the hassle of managing backup infrastructure without losing control of the backup/recovery policies and processes. Configuration and deployment can be completed in as little as 15 minutes, with Commvault best practices built into the configuration. Importantly, Metallic data protection extends to both on-premise and cloud workloads. For many organizations, this will equate to simpler data protection operations with less downtime and seamless scaling.

Commvault's 20-year heritage of backup/recovery and data protection gives Metallic the backing of a trusted brand. Commvault has architected a baseline of solid functionality, yet it has provided plenty of room for partners to build differentiating services on top of the platform. By fostering a diverse ecosystem of provider partners, Metallic has an opportunity to develop a strong position in a burgeoning market.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com

Copyright Notice