IDC

SPOTLIGHT

Sponsored by: Arcserve

Data protection can be an afterthought for SaaS applications. Too often, users assume the provider's data protection is adequate. Unfortunately, these default solutions are insufficient for data protection, retention, and governance. As a result, organizations are turning to commercial data protection to fill the gap.

Backing Up SaaS Applications: What You Don't Know Can Cost You

September 2022

Written by: Phil Goodwin, Research Vice President, Infrastructure Systems, Platforms, and Technologies Group

Introduction

SaaS applications are becoming an increasingly important component of an organization's application estate. These applications include key areas such as messaging, CRM, ERP, and many others that are industry specific or often regarded as mission critical. Unfortunately, few organizations fully understand the implications of the "shared responsibility" model inherent in many SaaS applications. Under shared responsibility, the SaaS vendor provides basic data protection and retention. The customer's responsibility is anything further than the basics, whether for granular data restore, long-term retention, or data governance.

IDC estimates that as many as 80% of new application deployments will be cloud native, many of which are SaaS. SaaS deployments are driving the adoption of various clouds, causing most organizations to operate in a multicloud environment, where they must support more than one public cloud provider. This includes both the dominant hyperscalers and industry clouds. Because of this multicloud dynamic, data can become isolated in silos and disconnected from the central IT umbrella of support, resulting in poor governance, inconsistent data protection, and vulnerability to malware and ransomware.

Although SaaS is rising in importance, most organizations still deploy and support on-premises workloads and plan to do so for the foreseeable future. These deployments may be on premises alone or combined with on premises and public cloud in a hybrid cloud configuration. For cloud-native applications, IT may also need to support cloud-to-cloud implementations, mainly as intracloud (i.e., zone to zone or region to region) or, more rarely, intercloud (i.e., one hyperscaler platform to another).

For many companies, Microsoft 365, Salesforce.com, Google Workspace, and others have become mission-critical applications. Moreover, the data from these applications is subject to the governance and policy requirements of the organization for data retention, discovery, and the like. Yet, unknown to many customers, most SaaS provider data protection solutions offer minimal protection and retention as part of the base package. The default can be as little as a daily backup with 30-day retention and "best efforts" data recovery with either no SLA or a very long SLA. More extensive capabilities may not be available or may have a substantial cost.

AT A GLANCE

WHAT'S IMPORTANT

SaaS applications often have inadequate data protection compared with corporate standards and SLAs. It is incumbent on the IT group to ensure that data in SaaS applications is adequately protected and governed.

KEY TAKEAWAY

IT executives are looking for solutions to protect SaaS data that fit with existing data protection efforts and architectures and that do so in the simplest manner possible.

Because SaaS data is so critical, IT leaders need to take control of data protection, archive, and governance themselves, even when a third party manages the application. Even in cases where an organization considers the extended data protection option from the SaaS vendor, an organization may still experience siloed data that is not in sync with other organizational policies. Thus, taking direct control of the data protection and management activities of SaaS apps is a "must" in many situations. Using a single vendor to protect on-premises, hybrid cloud, and SaaS workloads offers consolidation, consistency, and streamlined operations advantages.

Benefits

Many important business benefits exist for organizations that take control of their SaaS data. Organizational leaders may have several of the following motivators for taking control:

- Data retention and governance requirements vary by industry and organization. The one-size-fits-all approach by many SaaS vendors is unlikely to meet these requirements. This may include the need to archive the data separately.
- Organizations may need to restore data to the SaaS application. In the case of discovery orders, for example, it may be necessary to restore the data to the original state.
- Disaster recovery and cyber-recovery preparedness may also necessitate taking control of the data as few SaaS vendors offer either capability. This may be as simple as facilitating region-to-region replication or replication to separate secure, air-gapped, and/or immutable repositories.
- Data from SaaS applications may have significant secondary value through analytics. Replicating the data to a data lake or other repository allows organizations to extract this value, which would not be possible if the data remained siloed in the SaaS vendor's environment.

Above all, it can offer peace of mind to IT leaders knowing their data is safe and in conformance with organizational guidelines. Whether the need for data recovery is triggered by user error or cyberattack, having data protected in multiple places with different methods can help ensure data survival and reduce the risk of data loss and impact on staff time.

Key Trends

Modern organizations of almost any size have data at the core, cloud, and edge. Core repositories (on-premises private cloud) continue to hold the most data, but data is growing faster at the edge and in the cloud. SaaS is one of the main drivers of cloud and edge data growth. Irrespective of the location or applications, IT organizations are responsible for managing and protecting that data.

Data protection has evolved to much more than backup/recovery. Organizations need solutions that meet a complex matrix of requirements: cloud, on-premises, and edge repositories, as mentioned; multiple operating environments including virtual, physical, and legacy; file system, traditional database, and NoSQL database; and cloud-native applications, including SaaS and containers. Data protection solutions must be able to do it all, including supporting cyber-recovery, disaster recovery, and governance mandates.

IT leaders prefer to avoid a complex array of single-purpose tools to address the various data protection environments. Instead, they look for the greatest degree of consolidation possible to cover as many scenarios as possible. The preference is for integrated hardware and software systems that can provide routine data protection, cyber-recovery, and disaster recovery.

Considering Arcserve

Arcserve has a decades-long history of providing complete, integrated data protection solutions for modern workloads. Through its merger with StorageCraft in 2021, the company now offers a wide range of integrated data protection and object storage appliances and solutions designed to simplify deployment and operations while addressing data protection and governance across the enterprise (core, cloud, and edge). Arcserve's products cover nearly all data types and any application deployment, whether on premises, cloud, or SaaS. The company offers integrated cyber-protection and data protection via its partnership with Sophos Intercept X Advanced and the integration of that product with X Series, N Series, and 9000 Series appliances plus UDP.

Key components of the Arcserve platform include the following:

- **Unified data protection (UDP).** Arcserve Unified Data Protection is the center of the Arcserve platform. This software solution provides data protection, ransomware recovery, and disaster recovery. It provides immutable cloud storage via AWS S3 Object Lock and integration with Sophos Intercept X cyberprotection.
- **SaaS protection.** Arcserve SaaS backup offers backup for popular SaaS applications, including Microsoft 365, Salesforce.com, Google Workspace, Microsoft Dynamics 365, and Microsoft 365 Azure Active Directory. Arcserve's SaaS protection facilitates a single point of control for all SaaS backup operations to drive consistent backup policies across these apps, ensure data sovereignty, and support cloud-to-cloud replication for data survival. Arcserve claims its SaaS protection can be set up in five minutes.
- **Arcserve appliance family.** The Arcserve appliance family consists of the 9000 Series, X Series, and N Series to offer fully integrated data protection and/or cyberprotection for any size organization, from small businesses to large-scale enterprises.
- **As a service.** Arcserve offers both backup as a service and disaster recovery as a service for organizations interested in fully managed cloud-based services that support both cloud and hybrid cloud applications.

Challenges

The data protection market is highly dynamic and competitive. Currently, IDC tracks more than 40 vendors in the data replication and protection software market. Because of their importance to organizations, SaaS applications have become a particular focus of data protection vendors, and the competition is heating up. Arcserve's partnership with Keepit for SaaS backup gives Arcserve a faster route to market with a company focused on best-of-breed SaaS solutions. However, the two companies must maintain close collaboration to ensure market responsiveness and competitive positioning.

Cyberprotection is an area of high interest for IT and businesspeople alike. Cyberprotection for SaaS applications is becoming especially critical as cybercriminals are finding ways to simultaneously attack data in these applications to impact many potential victims. Arcserve has many cyberprotection strengths, but these are from partnerships with Sophos and Keepit, which may result in different methodologies. Arcserve has a long history of successful partnerships, and managing them appropriately to provide a consistent user experience will be critical to ongoing success.

Conclusion

Too often, organizations overlook data protection for SaaS applications, perhaps because they just don't think to consider it, don't think it is necessary, or don't want to take on the burden. Unfortunately, this can lead to lost data, unnecessary legal risk, and a missed opportunity to leverage the data for analytical purposes.

While it is possible to find boutique solutions for individual SaaS applications, most organizations prefer consolidating their backup operations to the greatest extent possible to simplify vendor management and operations and have a consistent experience across the enterprise. Organizations looking for a single vendor to provide their on-premises and cloud data protection, cyberprotection, and SaaS data protection will want to consider a company such as Arcserve that can satisfy the breadth of all three requirements.

About the Analyst

Phil Goodwin, *Research Vice President, Infrastructure Systems, Platforms, and Technologies Group*

Phil Goodwin is a Research Vice President within IDC's Infrastructure Systems, Platforms, and Technologies Group, with responsibility for IDC's infrastructure software research area. Mr. Goodwin provides detailed insight and analysis on evolving infrastructure software trends, vendor performance, and the impact of new technology adoption.

MESSAGE FROM THE SPONSOR

More About Arcserve

Find out more at www.arcserve.com, contact us at info@arcserve.com, or view our global office contact information here.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.