



ESG WHITE PAPER

How to Enhance AWS Workload Protection with Third-party Cloud Backup

Seamlessly Meeting Business Continuity and Compliance Mandates

By Christophe Bertrand, ESG Senior Analyst
and Monya Keane, ESG Senior Research Analyst

August 2020

This ESG White Paper was commissioned by Druva
and is distributed under license from ESG.

Contents

Market Landscape	3
Cloud Data Protection Considerations	4
Key Adoption Factors.....	4
Downtime and Recoverability	5
Granular Recovery.....	5
Who Is in Charge? Avoiding a Big Disconnect	6
The Shared Responsibility Model	6
Key Challenges for Data Governance on AWS	6
Compliance Mandates.....	7
The Druva Solution	7
An Enterprise-grade SaaS Platform	7
Optimized for Cost and Efficiency	7
Intelligent Data Management.....	7
The Bigger Truth	8

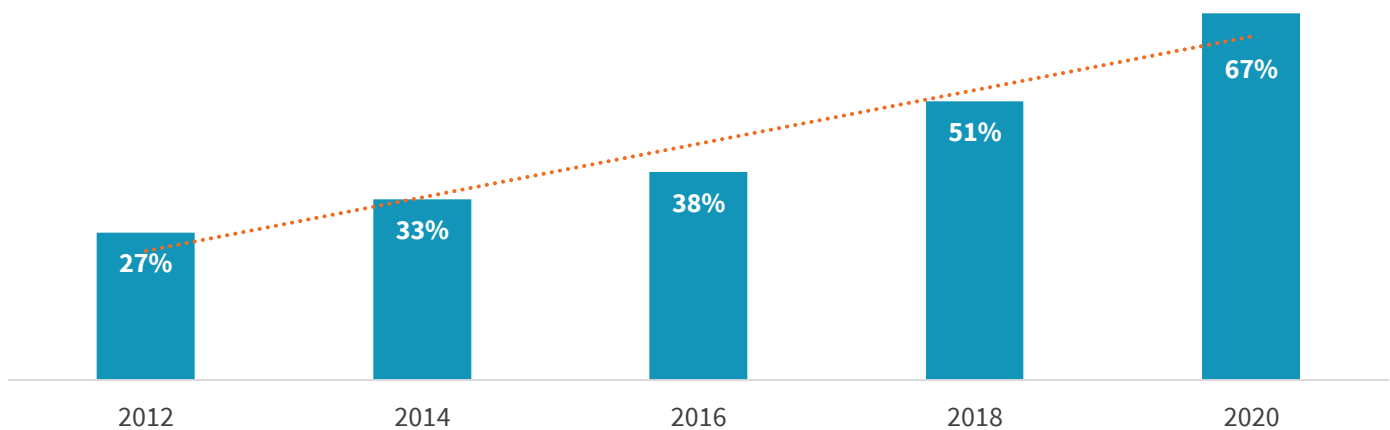
Market Landscape

Cloud usage is now ubiquitous. In fact, ESG survey respondents expect most remaining on-premises workloads (nearly three-quarters of them) will be cloud candidates over the next five years. And among IT decision makers surveyed by ESG, 94% report that their organizations currently use cloud services.¹

This year has brought another significant increase in public cloud infrastructure adoption (see Figure 1).²

Figure 1. Public Cloud Adoption Has Accelerated Significantly

Percent of organizations currently using infrastructure-as-a-service (IaaS), 2012-2020.



Source: Enterprise Strategy Group

Currently, the top use cases for IaaS include analytics, backup and archiving, running production applications, testing and development, and disaster recovery.³

In particular, the use of IaaS to support mission-critical applications is on the rise. The cloud has become a busy place, with more than one-quarter of mission-critical applications owned by ESG survey respondents now residing on IaaS. Similarly, 32% of mission-critical applications are in SaaS environments.⁴

IT professionals overwhelmingly recognize the positive impact that cloud services can have on their data protection strategies. The vast majority of respondents to an ESG survey said they consider cloud computing helpful to their organization’s data protection strategy.⁵ Disaster recovery-as-a-service and backup-as-a-service have each seen a significant rise, too.

Figure 2 illustrates the significant uptake across the board that has been evident in the past three years in regard to use of cloud backup targets, backup-as-a-service, and disaster recovery-as-a-service.⁶

¹ Source: ESG Master Survey Results, [2020 Technology Spending Intentions Survey](#), February 2020.

² *ibid.*

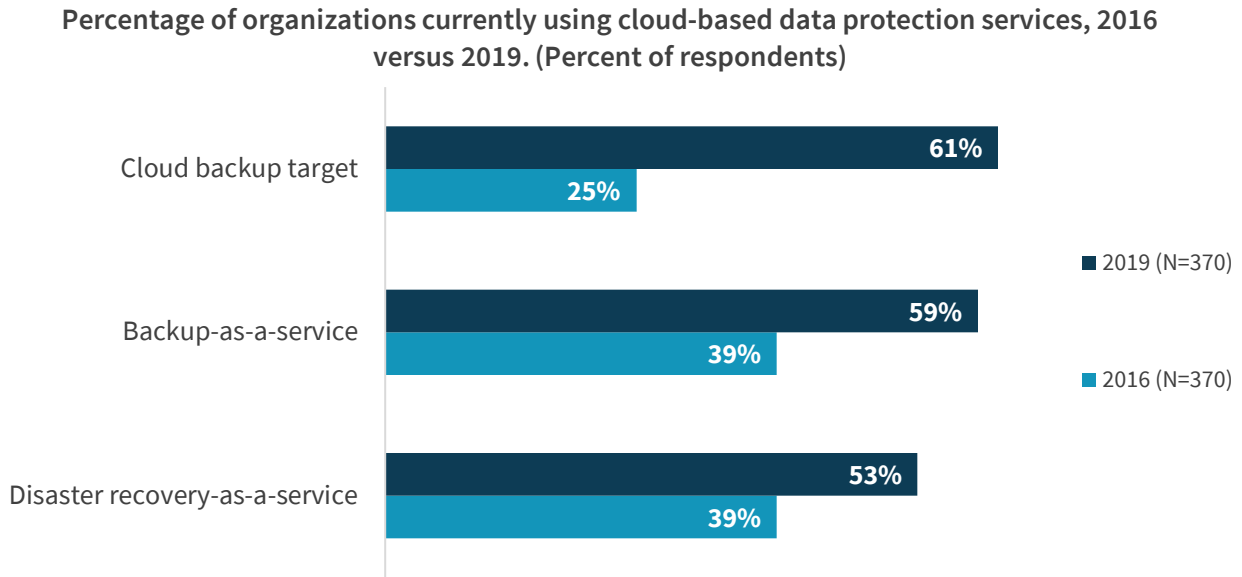
³ *ibid.*

⁴ Source: ESG Master Survey Results, [Real-world SLAs and Availability Requirements](#), August 2020.

⁵ Source: ESG Master Survey Results, [Data Protection Cloud Strategies](#), June 2019.

⁶ *ibid.*

Figure 2. Cloud-based Services for Data Protection Are on the Rise



Source: Enterprise Strategy Group

Cloud Data Protection Considerations

Cloud-based workloads are no different than on-premises workloads in that an organization needs an effective data protection strategy in place for business continuity. And when it comes to protecting data in the cloud, several considerations are important, including cost of the service, its operational efficiency, and its ability to support recoverability and keep downtime to a minimum.

Key Adoption Factors

Cost—as well as the ability to optimize processes, workflows, and operations for data protection—are key factors for organizations to consider as they move to the cloud for data protection. IT professionals already deal with so much complexity; the promise of the cloud is that it will provide simplicity, lower CapEx, more functionality, and ultimately improved SLAs.

The cloud certainly does come with a number of operational efficiency benefits. The most commonly realized ones relate to lower costs, better SLAs, and improvements in deployment times—i.e., hastening “time to first backup.” But other benefits are evident, too—for example, having an easy-to-use interface for ongoing management and easy configuration of data protection workflows. That benefit means IT generalists can quickly become proficient and efficient when performing cloud-based protection operations.

In particular regard to cost, one of the basic qualities of cloud IT is that it can help organizations optimize the cost of backup and recovery through tiering—specifically, long-term retention of infrequently accessed data, which can be stored on lower-tier, more economical storage.

Downtime and Recoverability

According to ESG research, acceptable downtime for mission-critical applications has to be kept to a minimum, with 15% of surveyed organizations reporting that they can tolerate no downtime for mission-critical applications. Even 35% of respondents report that their non-mission-critical applications must be back online in one hour or less.⁷

Clearly, uptime requirements are very stringent. Organizations are moving to cloud-based protection (using SaaS and/or IaaS), but they are not altering those uptime requirements: They expect similarly stringent performance for recovery time objectives and recovery point objectives. Basically, just because an organization goes to the cloud, that doesn't mean it is willing to renegotiate its mission-critical SLAs. And that's why these organizations need a backup/recovery solution that can meet those uptime requirements.

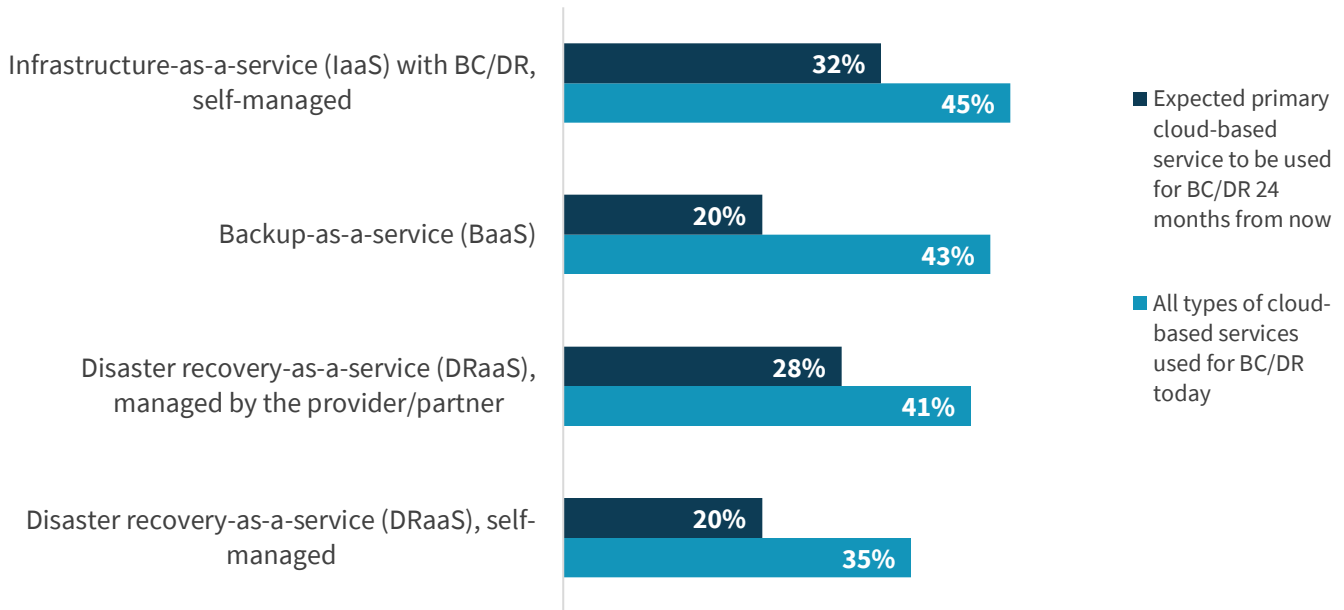
Granular Recovery

As Figure 3 shows, leveraging infrastructure-as-a-service for self-managed BC/DR is a very popular approach, as is leveraging additional services, and even make use of a partner network that specializes in certain cloud topologies and methodologies.⁸

It's also worth noting that BC/DR recoverability is not just about recovering all data at once. That is unrealistic. It is important (from a capability standpoint) that the chosen solution's recoverability features include some granular recovery capabilities for key applications. In that way, when only a part of a data set is lost or certain components need to be recovered, IT won't find itself in the inefficient and potentially costly position of having to recover more data than is necessary.

Figure 3. Cloud Service-based Approaches for Recoverability

Which types of cloud services does your organization utilize for BC/DR today? Which method do you anticipate being your organization's primary cloud mechanism for BC/DR 24 months from now? (Percent of respondents, N=212)



Source: Enterprise Strategy Group

⁷ Source, ESG Master Survey Results, [Real-world SLAs and Availability Requirements](#), August 2020.

⁸ *ibid.*

Who Is in Charge? Avoiding a Big Disconnect

Organizations' cloud architects and cloud admins are responsible for their own AWS backup, recovery, retention, and data management. It is *your organization's data*. Additionally, you, not AWS, are responsible for adhering to compliance and data protection mandates. Don't confuse "service availability" with actual data backup availability.

The Shared Responsibility Model

To distinguish what client organizations versus AWS are responsible for, AWS introduced the AWS Shared Responsibility Model. This model defines a separation of power when it comes to data security and compliance. Essentially, AWS takes responsibility for the security and stability of the cloud service itself: the hardware, software, networking, and physical protection of the facilities that run AWS Cloud services. But the customer organization is responsible for protecting (backing up) all data; managing the platform, operating systems, and relevant applications; and providing access management for users.

For example, AWS is responsible for patching and fixing flaws within the infrastructure, but customers are responsible for patching their guest OS and applications. And while AWS maintains the configuration of its infrastructure devices, customers are responsible for configuring their own guest operating systems, databases, and applications.

It is a sensible approach. But it means that a third-party data protection provider such as [Druva](#) is going to be a vital resource in ensuring that essential data is properly protected and managed.

Key Challenges for Data Governance on AWS

The consequences of downtime affect more than IT. Downtime's negative consequences extend to lost revenue, a lack of operational productivity, and reputational damage at a company level. Other impacts of downtime include:

- Loss of employee confidence.
- Damage to brand integrity.
- Loss of intellectual property.
- Increased insurance premiums.
- Reduced stock price.
- Legal action.
- Revocation of industry or governmental accreditations.

Those are all fundamental business operational efficiency issues that divert IT resources from other projects. Leveraging a strong IaaS-based infrastructure, such as AWS, is an excellent way to mitigate and minimize these issues. With AWS, an organization can mitigate the consequences of downtime and improve business efficiency, IT productivity, and end-user productivity.

An AWS environment, especially one supported by Druva, offers a lot of capabilities to keep protection and recovery on track so that no one's productivity is affected. At a time when budgets may be contracting due to recent economic and health-crisis situations, it is particularly important to be as optimized as possible.

Compliance Mandates

In regard to compliance, it is important for organizations to remember that the data is always theirs, not AWS's. Organizations will be audited, and so they must demonstrate that they are protecting and deleting data properly—that they know what data they have, where it is, and that it is being retained according to compliance requirements or erased according to privacy regulations.

Additionally, it is not possible to achieve most modern formal IT compliance certifications (i.e., HIPAA Compliant or GDPR Compliant certifications) without a strong data protection/retention layer. Fortunately, AWS is a great platform for certification-achievement purposes. Its massive cloud storage capability allows organizations to retain a lot of data, as well as optimize and classify it. Such a capability really helps in meeting compliance mandates.

The Druva Solution

Druva is different, innovative, and critical to protecting data in an AWS environment.

An Enterprise-grade SaaS Platform

Druva is an enterprise-grade SaaS platform designed from inception for native AWS Cloud workloads. It boasts impressive cloud scalability, breadth, security, and cost-efficiency. In fact, Druva reports that it considers its solution to be infinite in scale and capable of growing with a business as that business adds more AWS workloads, AWS regions, and AWS accounts.

Druva serves as the single protection vendor for unified protection and rapid recovery of AWS workloads including Amazon EBS, EC2, RDS, DynamoDB, NeptuneDB, DocumentDB, and Redshift. It also possesses what Druva calls “best-in-class” certifications for security and privacy standards including SOC2, HIPAA, and AWS Storage Partner.

This solution supports all AWS regions apart from China—including AWS Govcloud to meet data residency, compliance, and data isolation needs. Organizations can be sure they are using a solution that complies with the most stringent security, privacy, and compliance regulations.

Optimized for Cost and Efficiency

Druva allows organizations to lower their AWS-related costs. The software requires no additional servers to run within the organization's AWS Cloud environment.

It is a particularly smart solution for data archiving on AWS: Organizations can archive their EBS snapshots to S3 storage tiers, including Glacier, for long-term retention on less expensive AWS storage. Instead of paying \$0.05 per gigabyte for EBS snapshots, the organization pays the regular cost of using Amazon S3 (with the most “expensive” class being S3 Standard, priced at \$0.023 per gigabyte stored, and the even more economical Glacier, priced at \$0.004 per gigabyte).

An organization's internal IT admin costs should shrink, too, thanks to Druva's operational simplicity.

Intelligent Data Management

Druva supports data agility across AWS accounts and AWS regions that the organization's IT admin can manage from a single pane of glass.

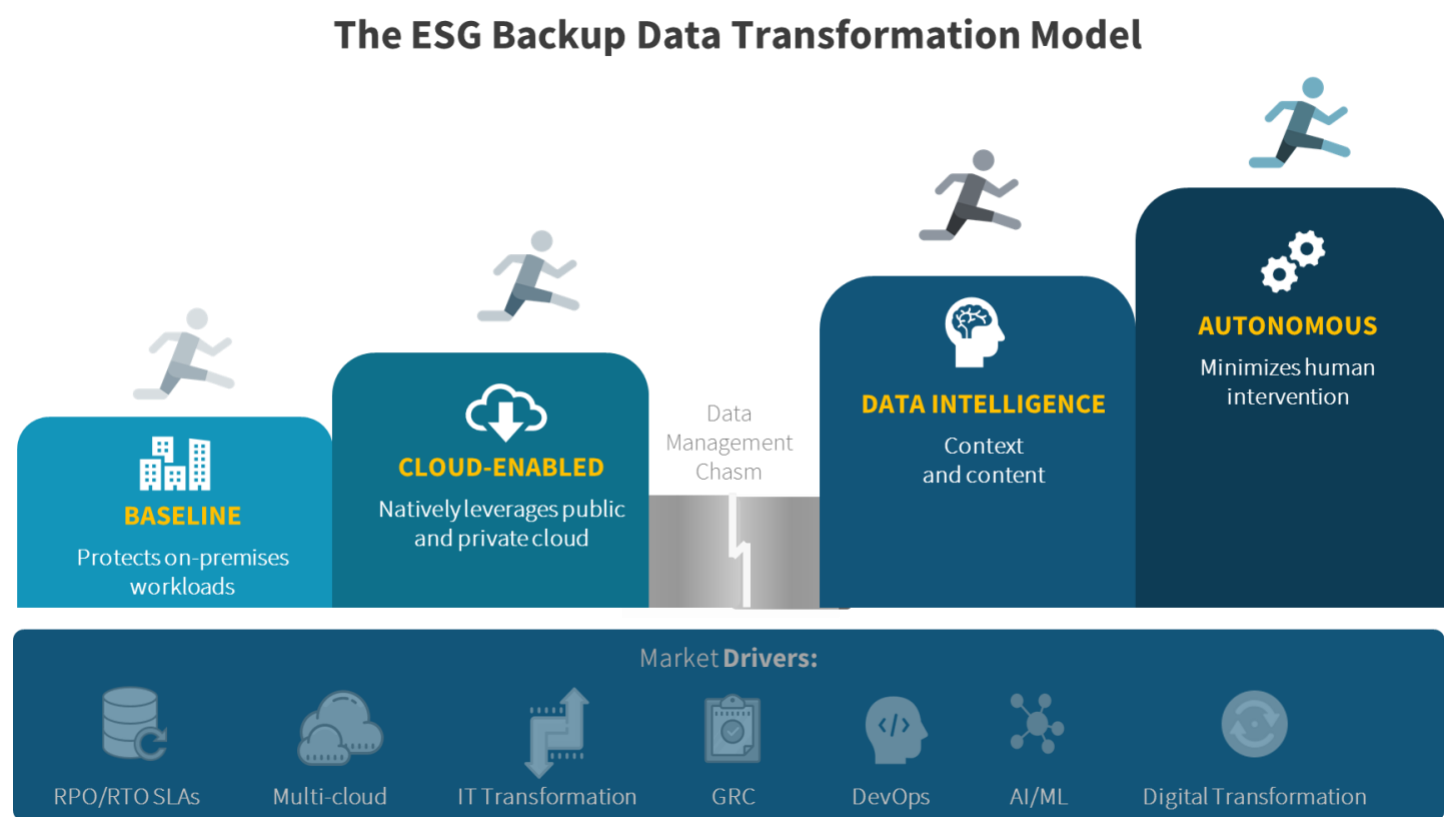
Administrators can apply unified global backup policies across multiple accounts in the AWS environment based on include/exclude rules/criteria. They can also administer cross-region and cross-account disaster recovery plans across the AWS environment.

It's possible as well to automate scheduled tests of DR plans to validate RTO and RPO requirements and ensure compliance and disaster readiness.

And when it comes to search functionality, Druva offers file-level search capabilities for snapshots based on metadata, with instant file-level recovery.

Essentially, Druva is going far beyond standard cloud backup with its ability to help admins perform tasks such as cloning environments, creating DR plans, leveraging automated DR testing, performing file-level search and file-level recovery, and establishing global backup policies (see Figure 4).

Figure 4. Intelligent Data Management: Going Beyond Backup



Source: Enterprise Strategy Group

The Bigger Truth

Every organization that moves to the cloud for data protection will experience some challenges. AWS offers great capabilities and tools to help overcome those challenges. But organizations also need to have a data protection strategy that allows them to maximize AWS. It turns out that [Druva](#) is a great platform to make that happen.

With all of the data stewardship, governance, and sound business best practices in play that apply to AWS-hosted data, you need *more than just AWS backup to protect your AWS-stored assets*. Protecting data in the cloud and leveraging cloud-based data protection is a natural combination. Druva brings the key components to the table to get it done correctly and address both business and technical mandates. That's because [Druva](#) goes beyond backup and recovery into intelligent data management.


All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.



Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

 www.esg-global.com

 contact@esg-global.com

 508.482.0188