Is Your Data Safe in an IaaS Public Cloud?

Mitigating Shared Responsibility Using IaaS Data Protection

FROST & SULLIVAN

An Executive Brief Sponsored by Veeam

Karyn Price
Senior Analyst & Associate Fellow – Cloud Computing
Frost & Sullivan

DYNAMIC GROUP - INDIA
www.dynamicgroup.in
+919025 66 55 66

July 2018

INTRODUCTION

Can your business afford the revenue and productivity loss associated with technology outages? In a hypercompetitive market, few businesses can. Many IT professionals expect to address the problem of business downtime simply by moving workloads to the cloud; they assume their cloud provider replicates customer data within their cloud centers as a matter of course. But in truth, your cloud provider has limited ability to protect your data. Most cloud providers assume responsibility only for the underlying infrastructure. Such backup procedures aren't designed as an adequate means to protect your data in the event of an outage or disaster.

Instead, cloud service providers and IT professionals subscribe to the "shared responsibility" model for data protection. With shared responsibility, the cloud service provider is responsible for maintaining infrastructure, and the enterprise is responsible for protecting its cloud-based data from productivity-impacting challenges, including human error, retention policy misconfigurations, and cyber security threats.

This white paper discusses the need for data protection in IaaS public cloud environments, including common shared responsibility models employed by many cloud providers, and why relying on your cloud provider is not enough. We discuss how shared responsibility impacts both disaster recovery and security; as well as steps that businesses can take to protect their data in a public cloud environment.

WHY A SOLID DATA PROTECTION STRATEGY IS CRITICAL TO BUSINESS OPERATIONS

For businesses like yours, protecting data is not only key to business continuity, but also to maintaining competitiveness, complying with regulations, and managing your brand reputation.

Businesses surveyed in the Frost & Sullivan 2018 Cloud User Survey cite such concerns among their top priorities when moving to a cloud environment:

- 61% cite security or unauthorized access to their data as a top concern.
- 61% cite challenges with backup and recovery of cloud workloads.
- 54% are concerned with ensuring compliance with appropriate industry regulations.

Many businesses move workloads to the cloud with an expectation that the cloud will enhance workload availability. Specifically:

- 70% of IT decision-makers rate "high availability SLAs" as a top selection criterion for a cloud service provider.
- 67% stated that they believe a move to the cloud will help improve business continuity and disaster recovery capabilities.
- 64% believe a move to the cloud will help them deliver applications and services faster.

Unfortunately, the high expectations regarding the cloud service provider's role in data protection are often misplaced. Many organizations incorrectly assume that their cloud provider will restore cloud-based applications or data in the event of an outage.

In fact, although most providers replicate their environments and employ secondary locations that act as disaster recovery sites, their only responsibility is to restore the instances contained in your account, not the data housed on them. Businesses still have responsibility to back up and provide continuity and security/compliance measures for their applications and data. Unless they do so, businesses are vulnerable to human error, security threats, and technical mishaps that can cause outages and corrupt data.

UNDERSTANDING BUSINESS RESPONSIBILITY FOR DATA PROTECTION IN THE CLOUD

While the cloud holds the promise of significant business benefits, the business itself must still take direct action to protect its critical data and enable business continuity in the event of an outage or disaster. Therefore, it's important for IT leaders to understand their role in infrastructure and workload protection.

Shared Responsibility in the Public Cloud: What Is It?

Most, if not all, major cloud providers have a Shared Responsibility Model as part of their Terms & Conditions. Shared responsibility clauses outline which parts of the cloud environment the provider is responsible for protecting and which parts the business customer is responsible for protecting.

Provider Responsibility

Most providers' shared responsibility language states that the provider is responsible for its own hardware that comprises its global infrastructure, and any software that defines infrastructure as compute, storage, networking, or database resources. For example:

- AWS states that it "is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services."[1]
- For customers using Azure IaaS services, Microsoft takes responsibility for the physical security of the infrastructure, and partial responsibility for the host infrastructure and the network controls.[2]

In general, providers take responsibility for security and backup of the infrastructure itself. Specific platforms, applications, workloads or services that the subscriber loads onto their instances are not the responsibility of the provider.

Business Subscriber's Responsibility

Businesses are responsible for their own data and server-side encryption; network traffic security (encryption of data, data integrity); OS, network and firewall configurations; platforms, applications, and identity and access management; as well as the backup and security of their customers' data. Shared responsibility models have impacts on disaster recovery and security strategies.

Business Continuity/Disaster Recovery

Shared responsibility applies to backup and recovery of cloud-hosted data. In the event of an outage, under most shared responsibility models, cloud providers only need to restore a customer's instances—meaning, the size and

[1] AWS Shared Responsibility Model

[2] Microsoft Cloud Computing Shared Responsibility

configuration of infrastructure that they subscribed to. The provider is *not* responsible for the applications and data stored within those instances. In the event of an outage, if your cloud workloads are not backed up appropriately, you may experience business-impacting downtime. To prevent this, you must back up those workloads by replicating and saving them in a secondary environment. This requires the enterprise to actively initiate a data protection plan that is secure, compliant, and easy to restore in the event of an outage.

Application and Data Security in the Cloud

Based on the terms of shared responsibility, cloud providers do not have the obligation to manage security settings for customers, beyond securing the actual infrastructure (hardware) on which the cloud environment is hosted.

Some businesses feel that security in the cloud is a "once and done" proposition: once they configure security policies for their public cloud instances, nothing further is required.

This is not an entirely correct assumption. Your IT team must still monitor security of your businesses' workloads on an ongoing basis for security threats or breaches; and handle any potential issues, whether on a proactive or reactive basis.

So what is the best way to proactively manage backups and security policies in the cloud?

INFRASTRUCTURE-AS-A-SERVICE (IAAS) DATA PROTECTION

For many businesses, IaaS data protection solutions offer the ability to protect your data that's already in the cloud, and address your shared responsibility with your cloud service provider.

What does an IaaS Data Protection Platform do?

IaaS data protection services automate and orchestrate the process of making viable backups of your public cloud -based data, minimizing manual effort from your IT team. A sophisticated software platform enables the IT department to schedule and set policies around what workloads or infrastructure resources get backed up, how often they need to be backed up, and how many copies of the backup should be retained. It also allows the business to define where backups will be stored, in terms of region, in order to ensure that they are compliant with data sovereignty regulations.

Such services may offer very granular backup and recovery capabilities, enabling the business to recover any part of infrastructure, from a single file or instance, to a full volume or a complete site.

The best data protection platforms offer a graphical, easy-to-understand and administer interface. This allows you to quickly and easily set backup policies for your cloud-based workloads, without a specialist on your team who is dedicated solely to backup and recovery.

What are the benefits of IaaS Data Protection Services?

With the right IaaS data protection service, businesses can:

- **Increase application availability** – You can configure your applications so a cloud outage does not result in downtime. Just restore to a new cloud region using the backup created by your IaaS data protection service, with just a few mouse clicks.

- **Flexible backup and recovery** – An IaaS data protection service allows you to choose, with just a few mouse clicks, the right protection levels for each application, workload, database, or cloud instance, based on your business needs.
- **Improved security** – Ensure consistent security profiles across your IT environments, including those in the public cloud.
- **Manage costs** – By choosing the right levels of protection for each specific workload, you can better allocate and manage costs for backup and recovery.
- **Reduce your management burden** – By reducing the staff needed to manually facilitate backup and recovery of your cloud workloads, you can reduce your internal IT management burden and enable your own staff to focus on innovative, business-supporting activities.

CHOOSING THE RIGHT IAAS DATA PROTECTION SOLUTION

When evaluating IaaS data protection services, what should you look for in a provider? Below are some specifics to help guide your choice:

- **Support for all major public cloud providers** – Your chosen IaaS data protection provider should support all major public cloud providers. Should you choose to migrate a workload from one provider to another, you will want a provider whose protection extends from the provider you use today, to any you may use in the future.
- **A range of restoration target environments** – Look for a provider that can restore your cloud-based workloads to whatever infrastructure you have up and available to accept the workload, whether public cloud, private cloud, or on your business premises.
- **Replication capabilities for multiple cloud instance types** – You'll want a provider that can replicate data regardless of whether it is compute or storage data.
- **Easy-to-configure backup and security through a graphical user interface** – Your chosen provider should offer an easy, intuitive online interface, which includes the ability to set backup & recovery and security policies, as well as encrypt backups.
- **Strong relationships with public cloud providers** – Look for an IaaS data protection provider that has strong relationships with the cloud providers whose environments it supports. Tight linkages between cloud and service providers often enable the service providers to request needed customizations of the environment, or to beta test new features relevant to their service before they are available to the general market.

Also consider your chosen provider's ability to:

- **Facilitate the backup and recovery** of other types of environments—premises-based, hosted, or private clouds; as well as the ability to replicate storage data.
- **Offer a strong partner ecosystem** of complimentary services that will interoperate well with its service.

As a whole, your IaaS data protection provider should offer comprehensive services that can protect your public cloud workloads—both where they reside today, and where they may reside in the future. To ensure consistency and minimize the maintenance burden on your organization, seek a provider that can not only protect your IaaS workloads, but other types of workloads as well. By choosing a provider with a robust suite of services that can protect your complete IT environment, you gain comprehensive IT protection in a single service that will protect your company data and meet your business goals.

THE LAST WORD

Businesses like yours move workloads to the cloud for a variety of benefits, chief among them being easy scalability and savings. But these benefits will not be realized if your data becomes corrupted or workloads become inaccessible because of infrastructure outages, security breaches, or disasters.

Savvy IT leaders have found IaaS data protection solutions to be the best solution to enable easy backup, storage and restoration of cloud-based workloads. IaaS data protection automates and orchestrates the process of making viable backups of your public cloud-based data, without the manual effort from your IT team—allowing you the freedom to "set and forget," while the software handles each aspect of the backup process. This enables your team to truly focus on higher value innovation, while ensuring that your workloads will remain secure and available in the event of any type of outage situation.

Not all IaaS data protection is the same, however. Look for a provider that goes beyond IaaS protection, allowing your business to protect any sort of workload—whether cloud-based, hosted, or on the premises—using its solution. The result will be a comprehensive data protection plan that secures your IT environment, and enables it to be restored in minutes, should the need arise.

Karyn Price

Senior Analyst & Associate Fellow – Cloud Computing
Frost & Sullivan
karyn.price@frost.com

Silicon Valley
3211 Scott Blvd
Santa Clara CA, 95054
Tel: 650.475.4500
Fax: 650.475.1571

San Antonio
7550 West Interstate 10, Suite 400
San Antonio, Texas 78229-5616
Tel 210.348.1000
Fax 210.348.1003

London
4, Grosvenor Gardens,
London SWIW ODH,UK
Tel 44(0)20 7730 3438
Fax 44(0)20 7730 3343

877.GoFrost • myfrost@frost.com
http://www.frost.com

www.dynamicgroup.in
+919025 66 55 66

ABOUT FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies? Contact Us: Start the Discussion