WRITER INFORMATION

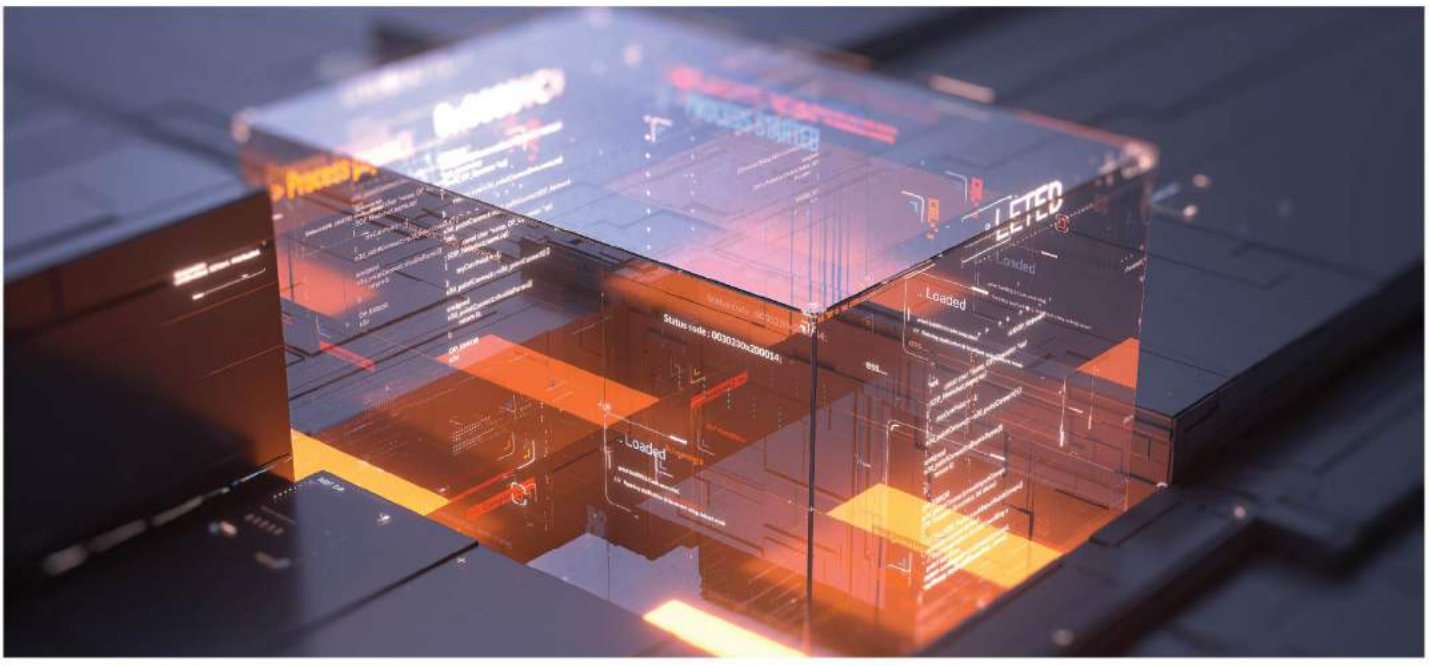
# Are you assured of the safety of your data in a Public Cloud?

Whitepaper

# Making use of IaaS data protection can help mitigate the shared responsibility

In today's world of tech advancements, can your business afford the rising revenues and productivity loss that are mostly associated with technology outages? The market scenario is hypercompetitive, and in the given circumstance, few businesses can. Most IT professionals expect to address this problem of business downtime by moving the increasing workloads to the cloud. But the cloud provider has limited ability to protect your precious data. Most cloud providers take up responsibility only for the underlying infrastructure. Such backup procedures mostly aren't designed as adequate measures to protect the data in case of an outage or disaster. That is why cloud service providers subscribe to the "shared responsibility" model when it comes to data protection.

With shared responsibility, the service provider is accountable for maintaining infrastructure and the enterprise is completely responsible for protecting the cloud-based data from the various challenges and that include human errors, cyber security threats and retention policy misconfigurations. In this white paper we discuss the necessity of data protection in IaaS public cloud environments and why complete reliance on cloud providers is not enough.



WRITER INFORMATION

# Why Data Protection Strategy Is Crucial To Business Operations

Data protection is not only essential when it comes to business continuity, but also for competitiveness, complying with regulations, and handling your brand reputation. Business surveys have shown the following concerns that figure among the top priorities when it comes to moving to a cloud environment:


**61%**

cite security issue as a top concern.

**61%**

cite backup and recovery of cloud workloads challenges.

**54%**

are apprehensive about compliance and other industry regulation challenges.

Many enterprises move their workloads to the cloud with an expectancy that the cloud will boost their workload availability and often incorrectly assume that their cloud provider will restore their cloud-based applications or data.

Although most providers employ secondary locations that act as disaster recovery sites, their sole responsibility is to restore the instances in the respective accounts, not particularly the data housed in them. Businesses bear the onus to back up and offer continuity, compliance and security measures when it comes to their data and applications. Unless that isn't done, businesses are most vulnerable to security threats, human error and technical mishaps, which can lead to corrupt data.

WRITER INFORMATION

# Understanding Business Liability For Data Protection In The Cloud

The cloud indeed holds the guarantee of substantial business benefits. However, to make that happen, the business must take direct action when it comes to protecting its crucial data and facilitate business continuity in case there is any unforeseen situation. Therefore, it becomes crucial for IT leaders to comprehend their specific roles when it comes to infrastructure and workload protection.

Most providers' shared responsibility language asserts that the provider is wholly responsible for its own hardware that comprises of its global infrastructure, and any other software that mostly defines infrastructure like storage, computes networking, or mostly database resources. However, specific applications, platforms, workloads or services, which the subscriber loads onto their instances are not usually the responsibility of the provider. Businesses are most responsible when it comes to their own personal data and server-side encryption; network traffic security (encryption of data, data integrity); OS; platforms, applications; network and firewall configurations; as well as the security and backup of their customers' data.

## Impacts On Disaster Recovery

Shared responsibility models mostly have effects on disaster recovery and security strategies and their responsibility mostly applies to recovery and backup of cloud-hosted data. In the event of an untoward incident, under most shared responsibility models, cloud providers mostly restore a customer's infrastructure that they have subscribed to. The provider is not completely responsible when it comes to the applications and data stored within that same infrastructure. So, if the cloud workloads haven't been backed up appropriately, business-impacting downtime is a possibility.

# How To Prevent It?

Back up of workloads by replicating and saving them in a secondary environment is the need of the hour. For this, the enterprise must actively initiate a data protection plan, which is secure, compliant, and convenient. Some businesses feel that the cloud is a proposition that is done once and for all, mostly if the security aspect is to be considered. But this isn't the correct inference. The respective IT teams of the businesses must monitor the security of businesses of its various workloads for any kind of breaches.

# Infrastructure-as-a-service (Iaas) Data Protection

IaaS data protection solutions of various businesses offer the power to protect your data that's in the cloud. IaaS data protection services help to automate the process of making viable backups when it comes to your public cloud-based data, whereby you can minimise manual effort from the IT team. A sophisticated software platform helps the IT department to organise and set policies that revolve on specific workloads or infrastructure resources that need to be backed up. It's also essential to know how often the backup is required and the number of copies of the backup that need to be retained. It also helps the business to specify where the backups need to be stored. The most efficient data protection platforms offer an easy-to-understand and graphical interface. This helps you to effortlessly set backup policies for your workloads that are cloud-based, without the help of a specialist who is dedicated for backup and recovery.

# Benefits of IaaS Data Protection Services

The right IaaS data protection service comes with various benefits. With it, businesses can effortlessly:

### Increase application availability

It is easy to configure your applications so that any kind of cloud outages does not end up in any kind of downtime. Just a few clicks, and you can restore data to a new cloud region with the help of the backup that is created by the chosen IaaS data protection service.

### Flexible backup and recovery

Just a few mouse clicks and you can choose the best possible IaaS data protection service with the right protection level for every application workload, cloud instance or database based on your business needs.

### Improved security

Added security for your profiles that are across the IT environments, including those in the public cloud.

### Manage expenses

The right levels of protection can help you allocate tasks better and manage expenses for improved backup and further to that recovery of data.

# Choosing The Right Iaas Data Protection Solution

Evaluating the right IaaS data protection services is crucial for your business. What are the things you look forward to in a provider?

- Support for all major public cloud providers – The IaaS data protection provider you will shortlist, must support all the import public cloud providers. In case you wish to migrate your workload from a provider to the next, you need to opt for the one whose protection extends from the one you use today, to any that you may use in the future.

- A range of restoration target environments – Look for a provider that can restore your cloud-based workloads to the required infrastructure be it public or private cloud, or it may be your business premises.

- Formidable relationships with public cloud providers – You need to find the right IaaS data protection provider that has resilient relationships with the cloud providers supporting those specific environments. Strong linkages between the cloud and service providers often help them to request for the necessary customisations of the environment.

- Facilitate the backup and recovery of different types of environments — hosted, premises-based or private clouds; as well as the potential to repeat the data that is stored.

- Offer a robust partner ecosystem consisting of complimentary services.

Overall, the IaaS data protection provider must offer comprehensive services, which can add that extra protection to the workloads that you have on your public cloud.

To ensure stability and uniformity and bring down the maintenance hassles on your organisation, look for a provider that has the potential to not only protect your IaaS workloads, but others as well. So, when you choose a provider with a strong and capable suite of services to protect your IT environment, you gain a thorough IT protection in a singular service, which can for sure add protection to your company data and help you meet all your business goals.

However, these benefits can be best realised if your stored data remains uncorrupted and the workloads are accessible. Some sort of infrastructure outages, disasters or security breaches can also make it inaccessible. Savvy IT leaders have understood that IaaS data protection solutions are the best when it comes to enabling easy backup, storage and finally restoration of cloud-based workloads. The IaaS data protection orchestrates and automates backups of your public cloud-based data, sans the manual efforts from your IT team. This enables your team to focus on higher-value innovation, while at the same time ensuring that your workloads remain secure and available during any type of an outage situation. Therefore, it's important to look for a provider that offers more than IaaS protection, whether hosted, cloud-based, or on the premises. This will lead to a comprehensive data protection plan, which secures your IT environment, and empowers it to be restored in just a few minutes, should the need ever come up.