MAKING HYBRID CLOUD REPLICATION WORK FOR YOU

Data protection using the Microsoft Azure replication target

Quest

Introduction

If you could have on-premises data protection or public cloud data protection, which would you choose?

How about both?

Organizations with significant infrastructure investments are moving to a hybrid model that combines on-premises and public cloud data protection. The model offers the predictability and security of the data center with the automation, flexibility and on-demand pricing of public cloud.

In a hybrid cloud data protection strategy, recent copies are stored in the on-premises data center for faster backup and restore. Older backup copies are stored in the public cloud to take advantage of infrastructure as a service (IaaS) for longer-term retention. The combination allows IT teams to enjoy hybrid data protection and disaster recovery (DR) — the best of both worlds.

This paper explains how organizations can effectively protect their systems, applications, and data by backing up on premises and replicating the backups to the public cloud. The featured use case focuses on the ease of buying and configuring replication in the Microsoft Azure public cloud, and the robustness and bring-your-own-license simplicity of Rapid Recovery. In this paper, IT managers and backup administrators will learn about the trends, rationale and benefits around implementing this secure, pay-as-you-grow, hybrid strategy for disaster recovery and data protection.

Why open up your data protection strategy to incorporate public cloud?

Businesses are choosing to extend their backup infrastructure to include public cloud for multiple reasons:

- To ease the crunch of onsite data storage
- To preserve backups safely for DR
- To reduce the CAPEX and OPEX involved in on-site DR
- To reduce the cost of protecting non-core IT assets
- To move beyond tape backup technology and processes

Most IT teams find that the advantages of public cloud — no storage limits, no infrastructure to maintain and pay-as-you-grow pricing — outweigh concerns about control over facilities and reliance on outside entities.[1] They can start out paying for enough capacity to meet their initial needs, then increase or decrease their spending as storage needs change.

INDUSTRY TRENDS

Several IT priorities support the move toward data protection in the public cloud.

Research by ESG reveals that the software-defined data center and the use of the public cloud for applications and infrastructure are among the most important IT initiatives. As shown in Figure 1, ESG also found three high priorities — managing data growth, using cloud infrastructure services and creating business continuity/disaster recovery (BC/DR) programs — that contribute to IT managers' interest in always-on, always-available, public cloud data protection.

A recent ESG survey[2] shows that when it comes to exploring on- and/or off-premises cloud infrastructure, 45 percent of senior IT decision makers report that increased use of on- and/or off-premises infrastructure is a top ten IT priority for 2016.

Demand for hybrid cloud has recently outpaced the growth of IT as a whole[3], and Gartner has predicted that nearly half of large enterprises will have hybrid cloud deployments by the end of 2017[4]. RightScale reports that 82 percent of enterprises surveyed have a multi-cloud strategy and more than half (55 percent) favor hybrid cloud[5].

45 percent of senior IT decision makers report that increased use of on- and/or off-premises infrastructure is a top ten IT priority for 2016.

1 John Waters, "Data Protection in a Hybrid Cloud, Software-Defined and Virtual Era," Redmond Magazine, March 2016

2 Jennifer Gahm, Bill Lundell, Jon Oltsik, "ESG Research Report, 2016 IT Spending Intentions Survey," Enterprise Strategy Group, February 2016

3 Steve Rosenbush, "CIOs Say Hybrid Cloud Takes Off," Wall Street Journal, October 20, 2015

4 Press release, "Gartner Says Nearly Half of Large Enterprises Will Have Hybrid Cloud Deployments by the End of 2017," Gartner Inc., October 1, 2013

5 "RightScale 2016 State of the Cloud Report," RightScale, Inc., May 2016

ESG Research: Top 10 IT Priorities

Top 10 most important IT priorites over the next 12 months.
(Percent of respondents, N=601, ten responses accepted)

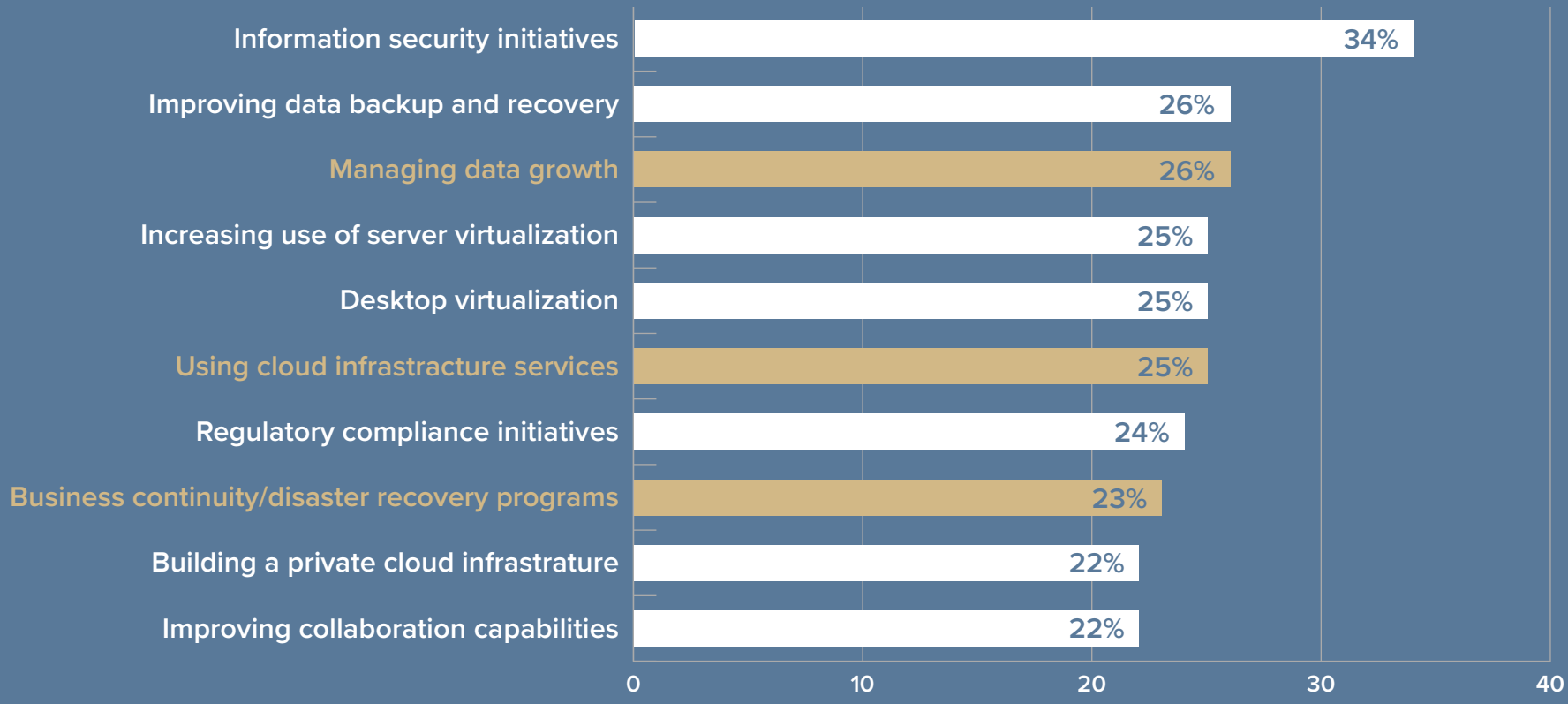
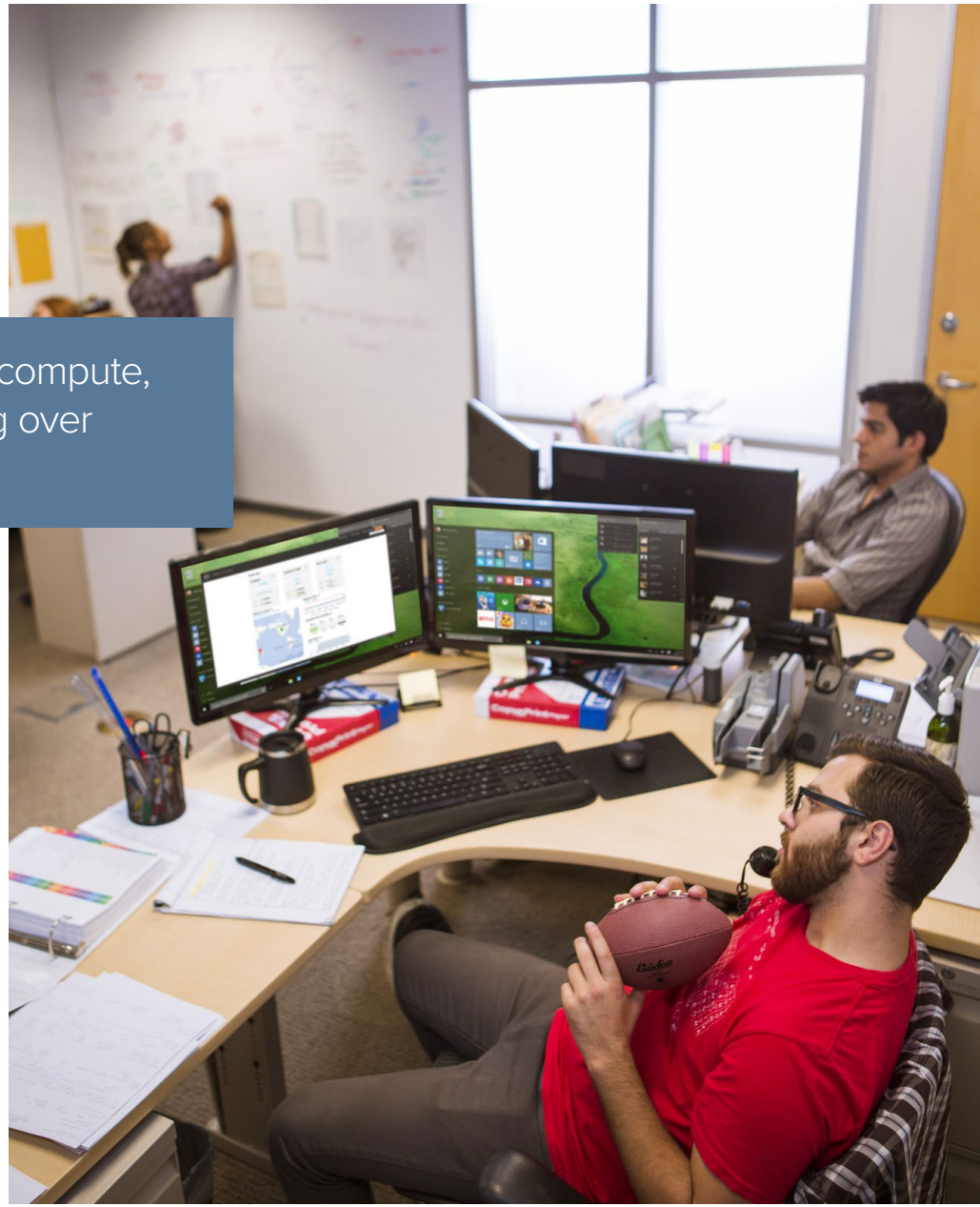


Figure 1: Top IT priorities[6]

6 Jason Buffington, "You Must Modernize Protection When You Modernize Production," Enterprise Strategy Group, March 2015

It's more than the desire to follow a trend that moves IT toward cloud infrastructure; it's the low tolerance for downtime. Among average midmarket and enterprise organizations, 67 percent of production applications have a downtime tolerance of two hours or less[7]. Cloud-based, IT-as-a-service (ITaaS) offerings include warm virtual standby replicas of critical systems that can be spun up nearly instantly in the event of an outage.



IT organizations are accustomed to owning storage, compute, network and applications and may be wary of cutting over suddenly to full dependence on the public cloud.

However, many managers and IT teams have longstanding investments in their own data centers. They've become accustomed to owning storage, compute, network and applications. Many of them are still concerned about security[8] and are wary of cutting over suddenly to full dependence on the public cloud.

GOING HYBRID

The hybrid cloud model has emerged as a viable option in which backup and storage in the public cloud is complemented with backup and storage on premises. It allows companies to enjoy continued return on their investment in data center infrastructure while taking their first steps toward the public cloud.

7 Jason Buffington, Jennifer Gahm, Bill Lundell, "ESG Research Report: The Evolving Business Continuity and Disaster Recovery Landscape," Enterprise Strategy Group, February 2016
8 "Cloud Security Spotlight Report," Crowd Research Partners, 2015

When implemented according to best practices, this model pays off in several ways:

- IT retains copies on premises for prompt disaster recovery while storing copies offsite.
- Users can see, manage and restore from the offsite data.
- The on-site and off-site copies, when kept synchronized, keep the backup safe and highly available.
- Regular backups of data and applications run locally and quickly.

The hybrid approach to data protection brings improved flexibility, support, availability and, most of all, security.

The model allows IT teams to gauge the fit of a new, potentially rich environment while they continue to work in their familiar data center.

Hybrid cloud allows IT teams to gauge the fit of a new, potentially rich environment while they continue to work in their familiar data center.

WHAT TO LOOK FOR IN A HYBRID CLOUD ENVIRONMENT

The variety of cloud-based and hybrid data protection offerings works in favor of IT decision makers, but it can also overwhelm them with a bewildering assortment of pricing plans and service level agreements. Not all executives have enough experience with the cloud to understand pricing and metrics; some report feeling that they are "just making it up as we go along[9]."

In planning a hybrid approach to data protection, an organization should first define its needs for performance, availability and reliability, and then pick a provider with a proven track record of offering the infrastructure, responsiveness and services that meet the organization's needs.

Data protection in the hybrid cloud requires a broader perspective than in the data center alone. DCIG analyst Jerome Wendt has called out several best practices[10], among them:

1. Use on-premises disk as the primary backup target. It results in the fastest backup and restore and in improved recovery time objectives (RTOs) and recovery point objectives (RPOs).
2. Define the scope of cloud services. Some organizations need replication, some need only archiving and some need both.
3. Assess criticality of servers and apps. Which applications, data and entire machines will be needed first when recovering from a disaster? What is the downtime tolerance for each?
4. Use a single solution to manage all recovery types. Using separate tools to recover data from physical, virtual and cloud storage increases recovery time and effort.

9 "Casualties of the Cloud Wars: Customers are Paying the Price," Enterprise Management Associates, cited in Joe McKendrick, "What Cloud Computing Customers Want: Clarity, Simplicity, Support," Forbes, July 19, 2014
10 Jerome Wendt, "Best Practices for Incorporating Cloud Services into a Comprehensive Backup and Recovery Strategy," DCIG, June 2016

BACKUP AND RESTORE PERFORMANCE

The goal of modern data protection should be the recovery of entire systems, apps and data with RTOs of minutes and as little impact on users as possible. RPOs should be as short as every hour — and could be more frequent — to minimize impact on protected servers. Short RPOs not only narrow data loss windows but also reduce backup size and network traffic for each backup job.

> Effective data protection products can safeguard entire virtual machines and not merely the data inside them.

To improve the performance of restore operations, backup and recovery solutions should offer granular restore for files and applications such as Microsoft Active Directory, Exchange and SharePoint. To reduce the WAN/internet bandwidth requirement and enable transfers of large datasets, it should offer incremental-forever backup. Block-based incremental-forever backup is more storage-efficient than file-based incremental-forever backup and can save even more network bandwidth.

As virtual machines become more pervasive, IT wants to be sure it can recover them promptly and easily. Effective data protection products can safeguard entire virtual machines and not merely the data inside them. They keep replicated VMs updated and ready if the primary machine fails.

There are several ways to implement so-called “instant recovery.” Look for a solution that enables instant recovery to physical as well as virtual machines. Rapid Recovery has a Live Recovery feature that restores the operating system volume first, to a target virtual or physical machine, and then makes backup data available to the restored OS on demand. When the recovery sequence restores the OS volume first, it can then make backup data available in the form of volumes and files for recovery as soon as users need them.

Finally, the product should support both bare-metal restore (BMR) and file-level restore (FLR) from archive. BMR reduces admin effort by keeping the server configuration and installed software intact. FLR allows users to recover individual files without waiting for the entire image to be restored.

REPLICATION TO CLOUD

Replication to the cloud can play a prominent role in a data protection strategy for disaster recovery. For instance, if a company suffered a ransomware attack but had replicated multiple recovery points to the cloud, system administrators could look back through them and pick a specific recovery point deemed likely to have been replicated before the attack. They could mount the volume as read-only, scan it for malware and, after determining it was clean, restore from it.

Organizations use cloud replication for disaster recovery because its reliability allows companies to meet higher standards for business continuity without breaking the budget. In replicating to the cloud, IT teams enjoy more flexibility and can protect data off site for longer periods of time.

> Replication to the cloud can play a prominent role in a data protection strategy for disaster recovery.

Microsoft Azure: Advantages for the public and hybrid clouds

Organizations looking for a stable and flexible public cloud should consider Microsoft Azure. Built on decades of enterprise expertise, Azure is public cloud that picks up where the on-premises data center leaves off.

ABOUT MICROSOFT AZURE

Azure is Microsoft's cloud computing platform for developing, managing and hosting applications off site. Azure runs on computers located in Microsoft data centers and provides secure, scalable, efficient storage in the cloud. The Azure Marketplace is an online market for buying and selling finished software-as-a-service (SaaS) applications.

Azure offers both hardware — a set of globally dispersed data centers filled with computers — and software — a set of services representing compute, storage and network (see Figure 2).

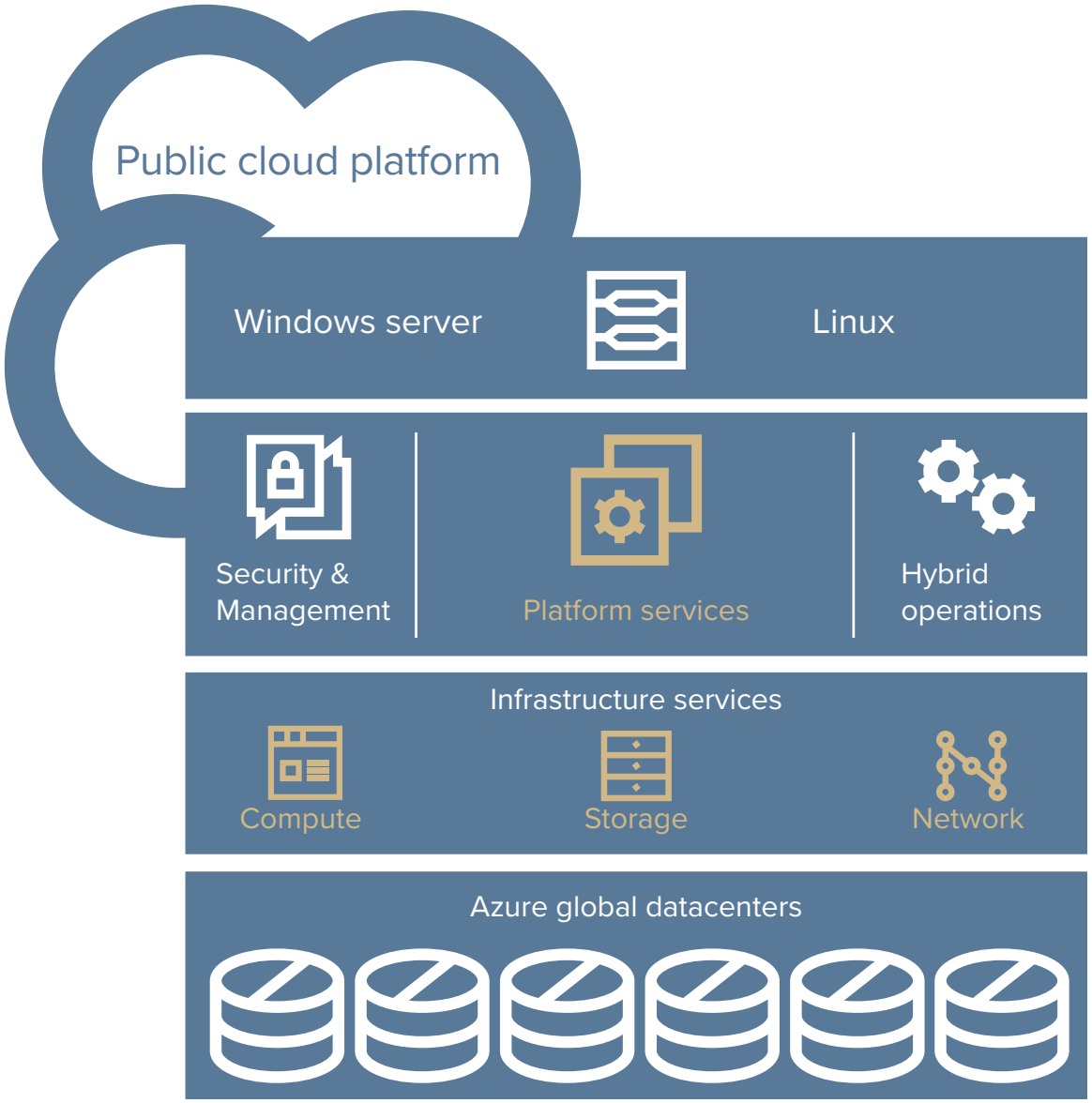
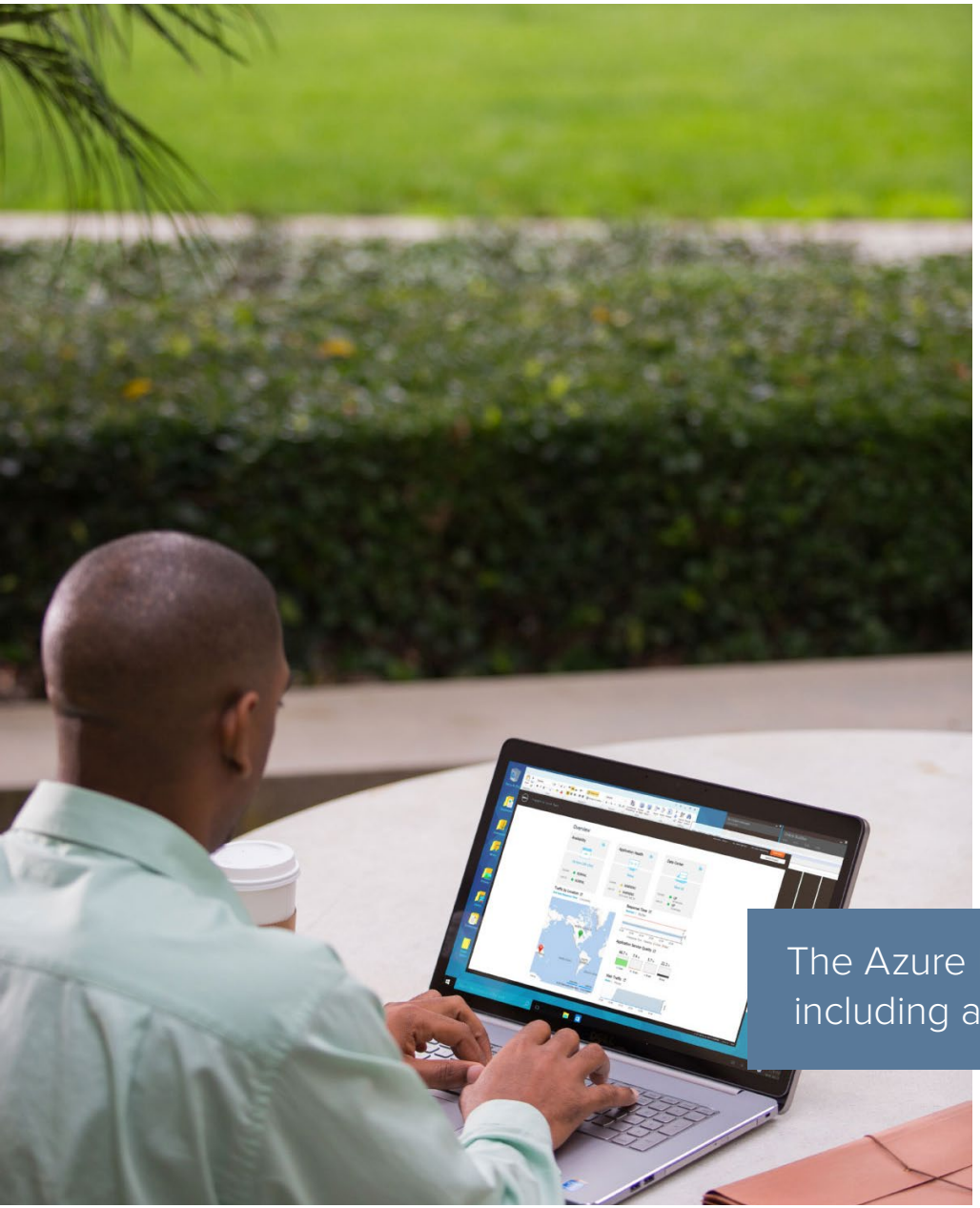


Figure 2: Microsoft Azure public cloud

Quest



Through Azure, IT teams can easily accomplish the same things they can in their own on-premises data center, provisioning machines, services and entire applications without the burden of installing, configuring and updating them for users scattered across the organization.

THE AZURE DIFFERENTIATORS: GROWTH, STABILITY AND INNOVATION

Azure offers enterprises flexibility as they begin to develop and implement their cloud strategy, and it meets the requirement for stability and longevity that IT organizations considering public cloud should be looking for:

- Fortune 500 companies using Azure: More than half (57 percent)
- New customer subscriptions: Approximately 120,000 per month
- SQL databases deployed to Azure: More than 1.4 million (excluding Oracle and MySQL instances and NoSQL databases)

The Azure Marketplace contains more than 3,500 products, including applications for data protection. Microsoft's prominent role in enterprise computing is strong assurance that it — and the data entrusted to its cloud — will remain a powerful force for the foreseeable future.

The Azure Marketplace contains more than 3,500 products, including applications for data protection.

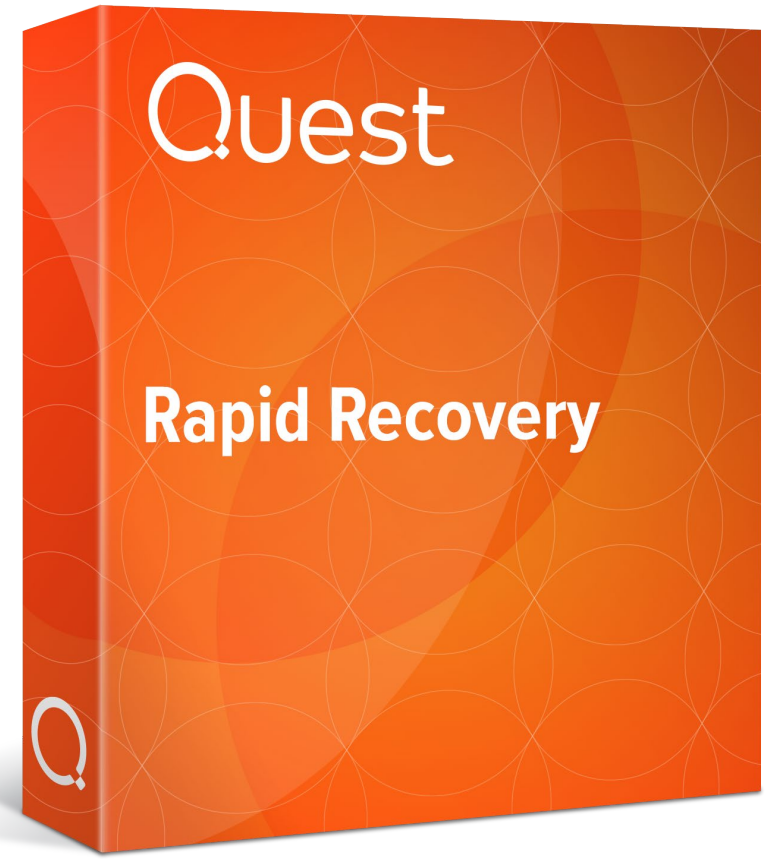
Quest

Rapid Recovery software and the Rapid Recovery Replication Target VM in Azure — A use case for hybrid cloud data protection

Rapid Recovery software provides advanced data protection on premises and in the cloud, enabling organizations to:

- Protect systems, applications and data anywhere – physical, virtual and in the cloud
- Recover at any level, including entire systems, in as little as 15 minutes
- Recover cross-platform: physical to virtual, physical to physical, virtual to physical, and virtual to virtual – even across hypervisors
- Connect to public cloud simply and easily
- Perform bare-metal restore and file-level restore from local and cloud-based archives in just a few clicks

Quest has a specialized Rapid Recovery core, available in the Azure Marketplace, to allow organizations to streamline setup and configuration of replication targets: the Rapid Recovery Replication Target VM for Azure.



Quest

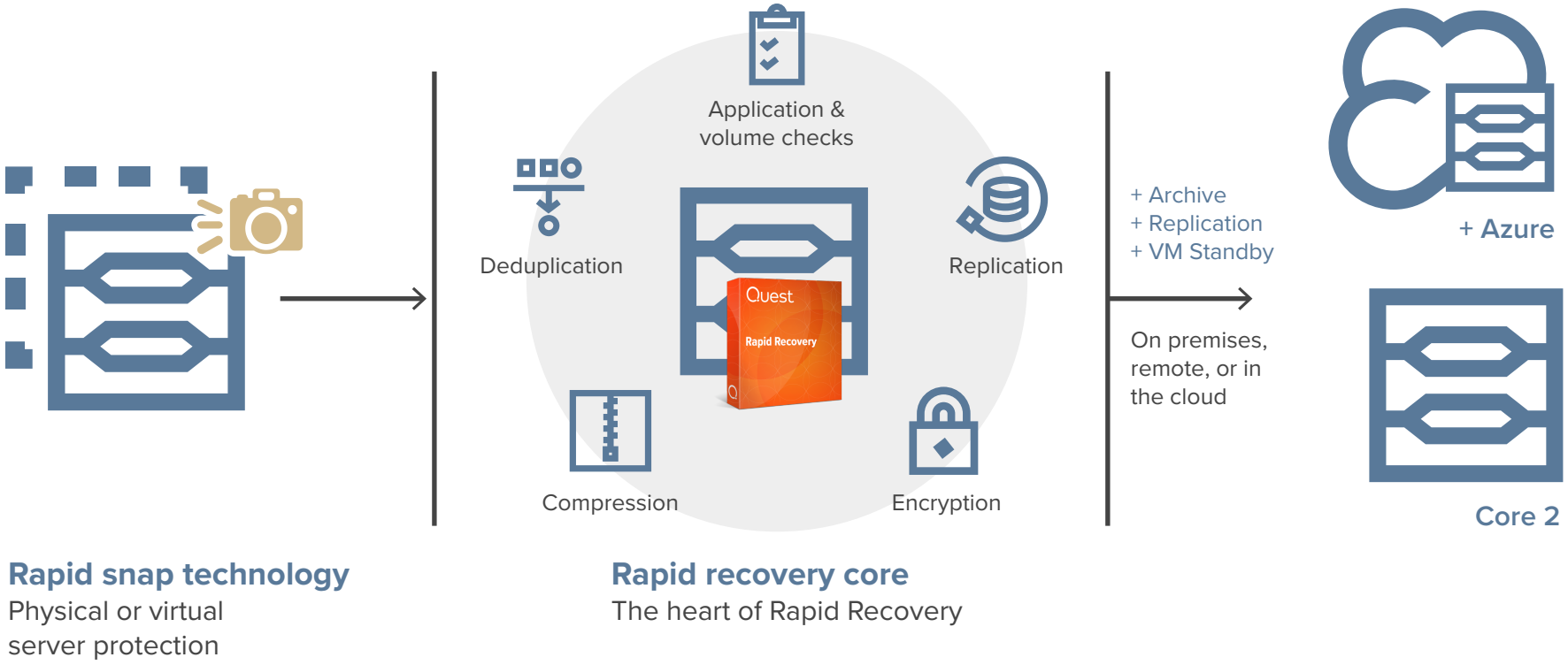


Figure 3: How Rapid Recovery software works for hybrid data protection

RAPID RECOVERY ARCHITECTURE

As shown in Figure 3, the heart of Rapid Recovery is its core software, which writes, compresses, encrypts and deduplicates data. Rapid Snap technology provides incremental-forever backup, taking up to 288 snapshots per day. Rapid Snap for Applications is agent-based protection that captures the entire application and its relevant state, enabling complete application and system recovery with near-zero RTOs and aggressive RPOs. Rapid Snap for Virtual is agentless protection for VMware VMs.

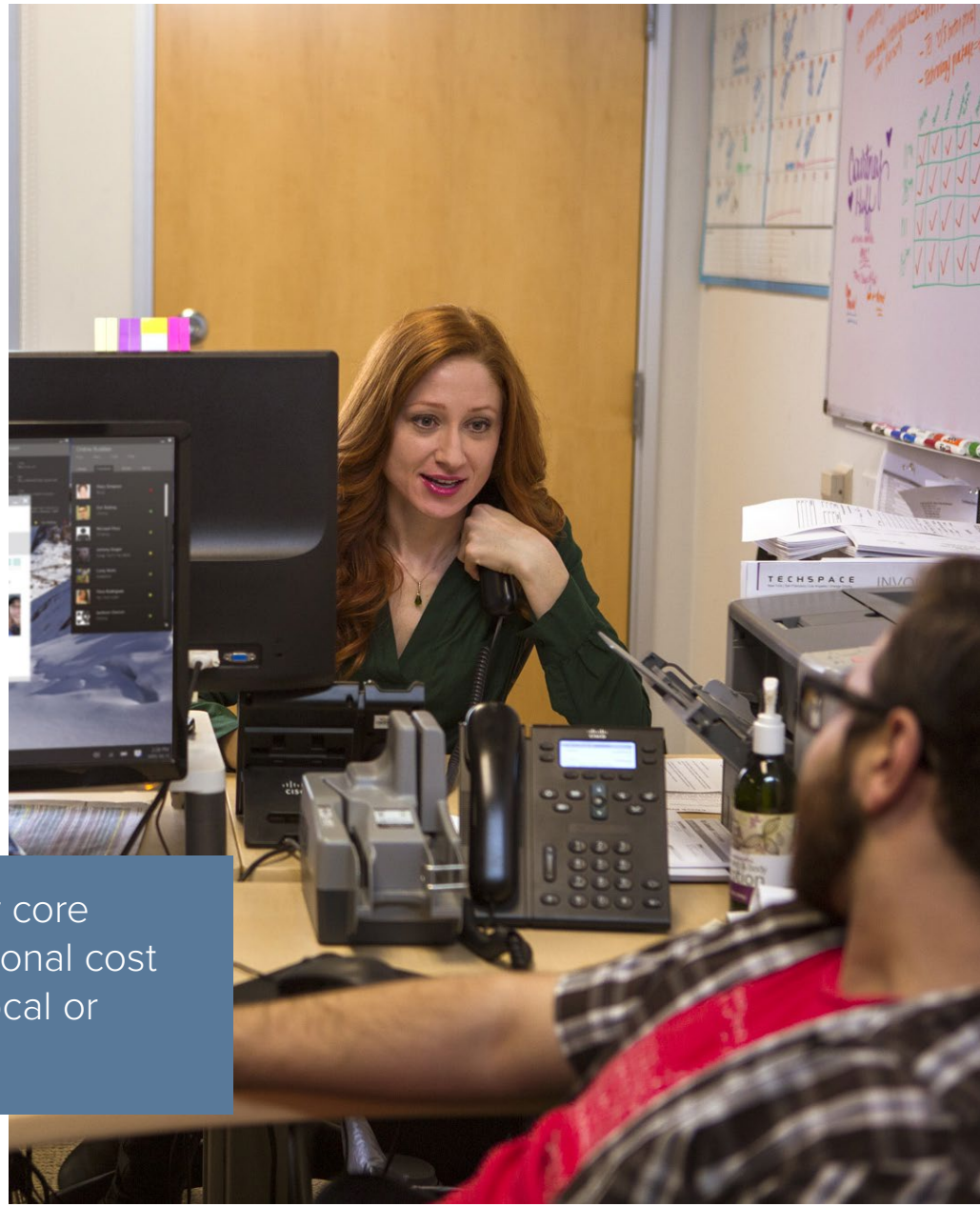
The Rapid Recovery core software also creates virtual standby machines, replicates data to additional Rapid Recovery cores, performs application checks and recovers systems, applications and data. Replicas and virtual standbys may be on premises, offsite or in the cloud. The core must be properly sized and configured for successful implementation.

Quest

With Rapid Recovery, IT teams can create as many core servers, physical or virtual, as they like at no additional cost and use them as virtual standby machines or for local or cloud-based archives and replicas for DR.

Administrators can apply their own variations to hybrid cloud replication:

- Outbound replication to the organization's own data center, to a remote disaster recovery site or to a managed service provider (MSP) implementing off-site backup and DR services
- AES-256 encryption of sensitive data prior to transmission
- Workflows that request connections and receive automatic notifications
- Retention policies on replicas in the data center that differ from those on replicas in the cloud. This is advantageous for organizations that need to keep backups for regulatory compliance but do not have the space on premises to keep them as long as required.



With Rapid Recovery, IT teams can create as many core servers, physical or virtual, as they like at no additional cost and use them as virtual standby machines or for local or cloud-based archives and replicas for DR.

Quest

How replication in Azure and Rapid Recovery work together

Hybrid cloud replication using the Rapid Recovery replication target in Azure works on a paired, source-target relationship between two Rapid Recovery cores. As depicted in Figure 3, the Rapid Recovery Core resides on premises and the Target Core (or "replication target") runs in Azure.

> Businesses that do not have (or do not want to use) a secondary site of their own can replicate to Azure and introduce enterprise-caliber redundancy to their data protection strategy.

The replication target in the Azure Marketplace includes an easy-to-use, pre-configured Rapid Recovery Core, optimized for replication. Administrators license Rapid Recovery and install it on premises, then they take the same license to Azure Marketplace and apply it to the replication target. They choose a size for the VM, which automated scripts configure.

BENEFITS OF CLOUD-BASED REPLICATION WITH AZURE AND RAPID RECOVERY

With Rapid Recovery, organizations can use Azure to manage the remote core as a service.

The benefits of cloud-based replication to Azure include:

- **Scalability** — Cloud-based object storage in Azure is virtually unlimited in capacity, with little to no additional overhead. Adding more storage is either a matter of contacting your cloud storage provider or provisioning the space using a self-service web portal that the cloud storage provider hosts. Of course, adding storage usually increases cost.
- **Flexible service-level agreements (SLAs)** — Cloud storage can be set up with different SLAs to meet different storage requirements. For example, some cloud storage providers like Azure target long-term storage of data, while others are suited to more immediate needs and can be connected to a cloud service provider. Cloud storage generally has built-in redundancy that provides an additional layer of data protection.
- **Disaster recovery** — Cloud-based replication to Azure offers the inherent high reliability and availability of cloud storage to meet higher business continuity standards economically. In a disaster, the environment can failover to an off-site, managed cloud location that usually comes at a fraction of the cost of maintaining a physical data center at a secondary location.

Businesses that do not have (or do not want to use) a secondary site of their own can replicate to Azure and introduce enterprise-caliber redundancy to their data protection strategy. They enjoy the flexibility of the cloud without incurring more infrastructure ownership and maintenance. Azure requires no up-front costs or termination fees, so companies pay for only what they use as their needs change over time.

Conclusion

More enterprises are adopting the hybrid model of using both on-premises and public cloud storage in their data protection strategy. Microsoft Azure offers them the options and flexibility to make the most of the public cloud while continuing to make the most of their own data center investment. Rapid Recovery provides flexible, on-premises data protection and easy replication to the cloud. The Rapid Recovery replication target in Azure is an easy way to implement hybrid data protection.

Organizations can use the replication capabilities of data protection software like Rapid Recovery and the Rapid Recovery Replication Target VM in Azure to implement hybrid cloud data protection.

Microsoft Azure offers enterprises the options and flexibility to make the most of the public cloud while continuing to make the most of their own data center investment.

Quest

ABOUT QUEST

Quest helps our customers reduce tedious administration tasks so they can focus on the innovation necessary for their businesses to grow. Quest® solutions are scalable, affordable and simple-to-use, and they deliver unmatched efficiency and productivity. Combined with Quest's invitation to the global community to be a part of its innovation, as well as our firm commitment to ensuring customer satisfaction, Quest will continue to accelerate the delivery of the most comprehensive solutions for Azure cloud management, SaaS, security, workforce mobility and data-driven insight.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (www.quest.com) for regional and international office information.

Ebook-MakingHybridCloudReplication-US-GM-21031

Quest