Microsoft

Microsoft hybrid business continuity and disaster recovery solutions

An overview of Azure Backup and Azure Site Recovery advantages when compared to VMware solutions

Executive Summary

In this white paper, you will learn about the features and benefits of Azure Backup and Azure Site Recovery and how they can help protect and recover VMware in a more cost-effective and simple way across hybrid environments.

Azure Backup and Azure Site Recovery reduce costs because by storing backups in Azure and replicating workloads to Azure rather than a secondary site. Contrastingly, VMware does not provide automatic storage management and requires purchasing a secondary site.

Azure Backup and Azure Site Recovery reduce the complexity involved in building disaster recovery solutions. In just a few minutes, you can protect your data and test your disaster recovery plan to have confidence that Azure meets your compliance needs. VMware solutions typically require a slower time onboarding.

Azure Backup and Azure Site Recovery support hybrid environments. These services support on-premises and cloud workloads running on VMware and Hyper-V and using Windows and Linux. VMware primarily supports VMware and private clouds.

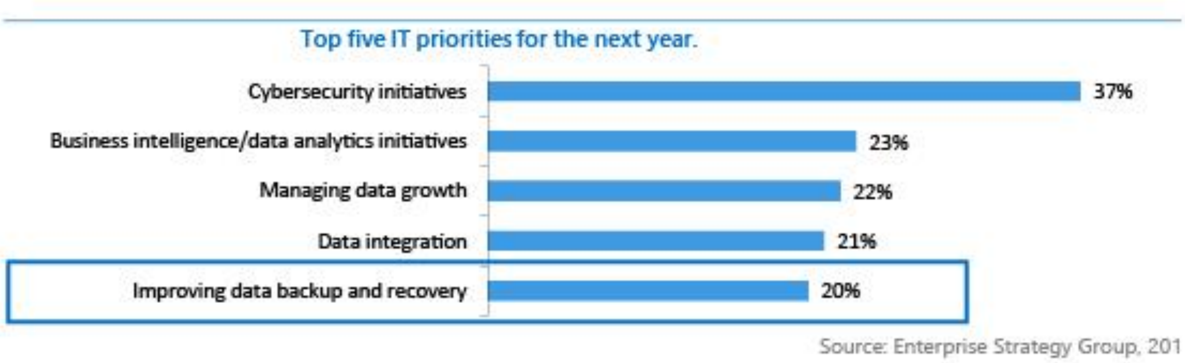
Continue reading the white paper to learn more about Azure Backup and Azure Site Recovery differentiate against VMware.

Contents

Today's challenges drive data protection innovation

With the transformation of business IT from traditional datacenter to hybrid cloud and the advent of big data, social media, mobility and the Internet of Things (IoT), there's an ever-increasing flow of data. This increase in data presents new challenges and opportunities. Organizations face an immense challenge in providing enough storage, capacity and backup for this data. Furthermore, many organizations understand that the traditional patchwork of point products does not provide enough protection for the current volume and variety of data.

Enterprise IT is also evolving at a rapid pace, with new platforms to address these emerging business demands. Organizations are looking to allocate budget resources to increase their IT agility so they can ultimately cut costs, glean new value from these digital transformations, and invigorate other important business drivers that affect strategic IT spending today. Several IT leadership mandates tie directly into data protection, as shown in Figure 1. ESG's 2016 report validates that 20% of survey respondents selected backup and recovery as one of the top five priorities that IT admins currently have.[1]


Top five IT priorities for the next year.

Source: Enterprise Strategy Group, 201

Figure 1: Top five IT priorities for 2016

Meeting executive-level mandates while simultaneously addressing cost concerns could require purchasing new technologies, considering new approaches, assessing new vendors or re-evaluating familiar vendors that could support the desired improvements.

[1] Source: Enterprise Security Group. "Research Report: 2016 IT Spending Intentions Survey." February 2016. http://www.esg-global.com/hubfs/irp/abstracts/ESG-Research-Report-Abstract-2016-IT-Spending-Intentions-Survey-Feb-2016.pdf.

Why a modern backup and disaster recovery solution for your business?

IT infrastructure gets wide and complex as your business grows. When you have a wide array of operating systems, hypervisors, and physical servers, maintaining your environment is challenging. Business applications are critical, and unplanned downtime can have devastating effects on your business' customer relations, revenue, reputation and regulatory compliance. Even a short period of downtime can cost thousands to hundreds of thousands of dollars, or more.

The cost of ICT downtime is substantial, from $1 million a year for a typical midsize company to over $60 million for a large enterprise.

IHS report, January 25, 2016

In-depth survey-based IDC research shows that the average annual revenue loss per hour of downtime in midsize companies varies significantly by industry sector: nearly $60,000 for manufacturing firms, $158,000 for healthcare businesses, as much as $400,000 for retail businesses, and nearly $10 million for financial firms.

IDC Report, 2015

Legacy local backup and secondary site replication for disaster recovery (DR) cannot support all your applications, make performing disaster recovery drills difficult, and risk affecting your production workloads. Loss of data and application errors often occur during failover to your datacenter.

You need a modern IT data-protection platform to keep business up and running with zero downtime. With such a tight competitive edge for business, even a minute of downtime can have a heavy impact. Because the risks associated with being unprotected in today's business climate are more serious, you cannot be dependent on time-consuming and limited disaster recovery plans that are susceptible to error. The conventional solutions to backup and disaster recovery are not as reliable.

The cloud has become an important part of data protection strategies

The modern data protection landscape is becoming increasingly complex, with its mix of hypervisors and physical assets. Multiple data protection and disaster recovery solutions are often required to address these increasingly multifaceted environments, and this adds further complexity. And technology innovation has greatly extended the definition of data protection. It's no longer sufficient to just make copies of data. The focus is not only on business continuity, but also on the speed and simplicity of disaster recovery.

With advanced data protection approaches in the cloud, organizations need to be able to recover data and also have applications and business services available from multiple datacenters and cloud locations. This allows organizations to obtain maximum levels of protection at an acceptable cost. ESG research shows[2] the “tape versus cloud” comparison: cloud usage is growing faster and tape is declining. (See Figure 2.) While both tape and the cloud have their place in IT strategy, cloud-based data protection is quickly becoming a prominent solution for backup and disaster recovery.

Media	2012 reported usage	2017 anticipated usage	Five-year change
Tape	56%	45%	-22%
Cloud	7%	22%	+314%

Figure 2 : Data backup process, 2012 versus 2017

The modern approach to cloud data protection integrates various data protection functions like replication, automation virtualization, de-duplication, orchestration tools and centralized management. A growing number of organizations have already recognized the potential for unlocking the business value that comes with using a cloud-based data protection.

Azure Backup and Azure Site Recovery

Microsoft Azure provides a unified solution to protect data on-premises and in the cloud. Azure Backup and Azure Site Recovery provide disaster protection for data and applications to ensure business continuity.

Azure Backup

Azure Backup is a simple and reliable cloud-integrated backup service that serves as a unified solution to protect the data, providing an alternative to tape that saves money and ensures compliance. Azure Backup delivers data protection no matter where data resides—in the enterprise datacenter, in remote and branch offices, or in the public cloud—while being responsive to the unique requirements these scenarios pose. Protect your critical applications, including Microsoft SharePoint, Exchange, and SQL Server; files and folders; servers and clients running Windows; and Azure Infrastructure-as-a-Service (IaaS) virtual machines. With Azure Backup, you can focus on your business needs and not manage or pay for infrastructure on cloud.

[2] Source: Enterprise Security Group. “ESG Research Report: 2015 Trends in Data Protection Modernization.” September 2015. http://research.esg-global.com/reportaction/2015dataprotectionmodernization/Marketing.

Figure 3 shows the key capabilities of Azure Backup.

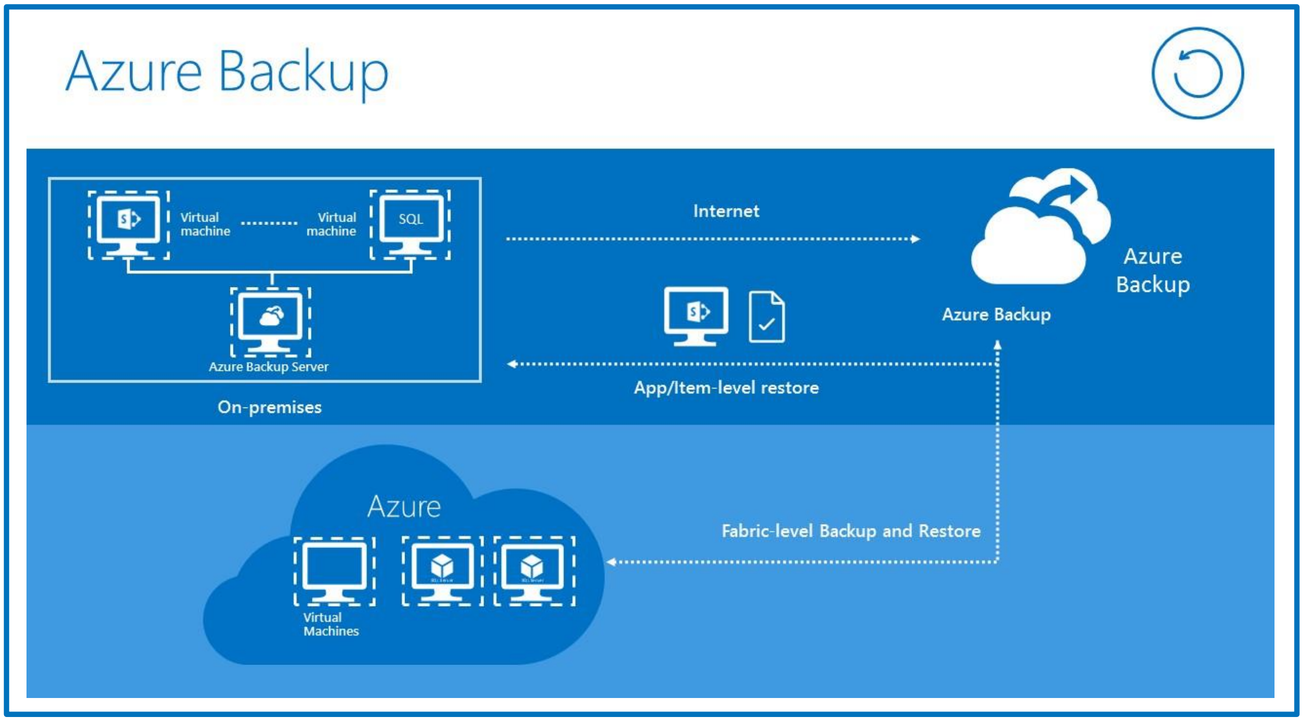


Figure 3: Key capabilities of Azure Backup

- **Cost-effective storage management.** With Azure Backup, there's no cost for using on-premises storage devices. Azure Backup automatically allocates and manages backup storage, and it uses a pay-as-you-use model, so you pay only for the storage you consume.
- **Integration into Azure.** Azure Backup as a SaaS service, fully integrated into Azure, alleviates the need to run updates or patch the service and allows for faster onboarding.
- **Unlimited scaling.** Azure Backup uses the underlying power and nearly unlimited scale of the Azure cloud to deliver high availability with no maintenance or monitoring overhead. You can set up alerts to provide information about events, but you do not need to worry about high availability for your data in the cloud.
- **Multiple storage options.** One aspect of high availability is storage replication. Azure Backup offers two types of replication: locally redundant storage and geo-redundant storage.
- **Unlimited data transfer.** Azure Backup doesn't limit the amount of inbound or outbound data you can transfer, and you won't be charged for data that's transferred.
- **Data encryption.** Data encryption helps you to securely transmit and store your data in the public cloud. You store the encryption passphrase locally; it's not transmitted or stored in Azure.
- **Protection against ransomware.** Azure Backup has built-in protection from ransomware. Backups deleted by malware result in a permanent loss of data, causing organizations to have to spend time and money dealing with the aftermath.
- **Application-consistent backup.** Azure Backup provides application-consistent backup, which ensures that additional fixes are not needed to restore data. Restoring application-consistent data reduces restoration time, allowing you to quickly return to a running state.

- **Long-term retention.** You can use Azure for short-term and long-term retention. Azure doesn't limit the length of time data remains in a Backup or Recovery Services vault.

Azure Backup vs. VMware vCloud Air Data Protection

Azure Backup provides data protection across hybrid and heterogeneous environments. It helps you protect Windows files and folders in addition to enterprise workloads like SharePoint, Exchange, and SQL Server. VMware vCloud Air Data Protection helps to protect data that resides in dedicated cloud or Virtual Private Cloud instances. It's limited to VMware VM-level protection.

These are some of the competitive advantages that Azure Backup has over VMware vCloud Air Data Protection:

- **Protection across hybrid environments.** Azure helps protect data across hybrid environments, protecting files, folders, applications, and VMs throughout on-premises and the cloud. VMware vCloud Air Data Protection is limited to VMware hypervisor–level protection in vCloud Air by means of a combination of inline I/O quiescing and snapshot techniques.
- **File-level and folder-level protection for Windows.** Back up your Windows files and folders to Azure by using Azure Backup. The backup is stored in the Recovery Services Vault. VMware vCloud Air Data Protection can back up applications like SQL Server, SharePoint, and Exchange.
- **Heterogeneous storage for backup.** Azure Backup provides automatic storage management and allocation across on-premises and the cloud. With Azure Backup, there's no cost for using on-premises storage devices.
- **VMware backup.** Azure Backup supports VMware VM backup to disk and to cloud for offsite copy or long-term retention, which provides value beyond the capabilities of vCloud Air Data Protection. Azure Backup uses the VMware vSphere Storage APIs to protect VMware VMs remotely without installing agents on vCenter or ESXi servers. You can also seamlessly discover and protect VMware VMs residing on external storage targets like NFS and cluster storage. Other features of VMware backup are available for vCloud Air Data Protection as well.
- **Granular restore.** Azure Backup provides granular restore capabilities, like mailbox recovery for Exchange, database-level recovery for SQL Server, and item-level recovery for SharePoint. VMware vCloud Air Data Protection provides VM-level and vApp-level protection but it doesn't provide application-level protection.
- **Data retention for compliance**. For business compliance and retention requirements, Azure Backup provides data retention for up to 99 years. VMware provides retention policies between 1 and 365 days.
- **Third-party services for backup.** Azure Backup has a single management pane, real self-service, instant restore, enhanced secure backups, and no storage egress charges or infrastructure. All backups across an enterprise, including backups at remote and branch offices and in the cloud, can be managed from the Azure portal. This gives you visibility and control of your environments from one centralized location without the involvement of third-party services. VMware uses third-party services like Veeam and Commvault for its backup solution. This adds extra complexity, tim, and resources to the backup process and makes it more expensive.

Azure Site Recovery

Azure Site Recovery natively integrates into Azure. It allows you migrate workloads from on-premises to Azure, manage your DR solution from Azure and take advantage of hybrid disaster recovery capabilities across multiple platforms.

Azure Site Recovery is a customizable disaster recovery solution that gives you the means to orchestrate an effective DR plan and ensures that your vital applications are available. To ensure your customized disaster recovery plan works, you can test it whenever and as many times as you want without effecting production workloads or end users. Azure Site Recovery provides a single DR solution that works across platforms (Hyper-V, VMware, and physical), across clouds (public, private, and service provider) running on Windows or Linux to provide a range of recovery time objectives (RTOs) and recovery point objectives (RPOs) by using multiple channels (host-level, guest-level, application-level replication and others).

You can replicate the following to Azure:

- VMware: On-premises VMware VMs running on supported hosts. VMs must be running supported operating systems.
- Hyper-V: On-premises Hyper-V VMs running on supported hosts.
- Physical machines: On-premises physical servers running Windows or Linux. You can replicate Hyper-V VMs running any guest operating system supported by Hyper-V and Azure.

Azure Site Recovery allows for DR replication and orchestrated recovery for the following cloud-enabled scenarios. (See Figure 4.)

- Private cloud. VMware to VMware or Hyper-V to Hyper-V.
- Hybrid cloud. Physical / VMware / Hyper-V to Azure.
- Public cloud. AWS to Azure migration or Azure to Azure

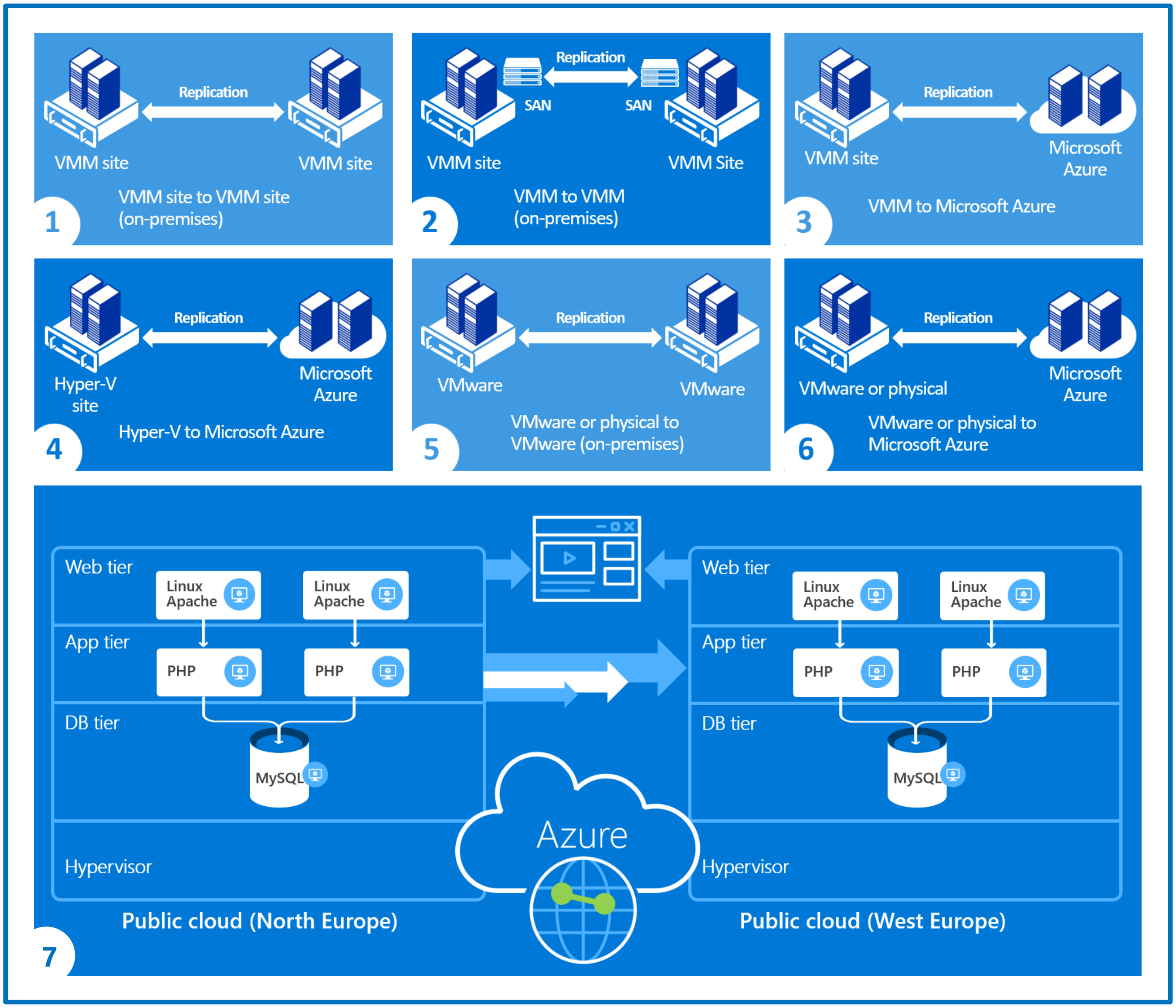


Figure 4: Supported Azure Site Recovery replication scenarios

Key capabilities of Azure Site Recovery

- **Disaster recovery to Azure.** You can replicate workloads running on VMs and physical servers to Azure rather than to a secondary site. This eliminates the cost and complexity of maintaining a secondary datacenter or having to pay for a secondary site that replicates to the cloud.
- **Flexible replication for hybrid environments.** You can replicate any workload running on supported on-premises Hyper-V VMs, VMware VMs, and Windows or Linux physical servers.
- **Migration.** You can use Azure Site Recovery to migrate on-premises workloads to Azure.
- **Simplified business continuity and disaster recovery.** You can deploy replication from a single location in the Azure portal. You can run simple failover and failback operations of single and multiple machines.

- **Resilience.** Azure Site recovery orchestrates replication and failover without affecting production applications. Replicated data is stored in Azure storage, which provides resilience. When failover occurs, Azure VMs are created based on the replicated data.
- **Replication performance.** Azure Site Recovery provides replication as frequently as every 30 seconds for Hyper-V and continuously for VMware. You can set RPO thresholds to control how often data recovery points are created, and you can reduce RTOs with the Azure Site Recovery automated recovery process.
- **Application consistency.** Machines replicate using application-consistent snapshots. In addition to capturing disk data, application-consistent snapshots capture all data in memory and all transactions in process.
- **Testing without disruption.** You can easily run test failovers to support disaster recovery drills without affecting production environments or end users.
- **Flexible failover and recovery.** You can run planned failovers for expected outages with zero data loss (supported for Hyper-V only) or unplanned failovers with minimal data loss (depending on replication frequency) for unexpected disasters. You can easily fail back from Azure to on-premises when your primary site is available again.
- **Custom disaster recovery plans.** Disaster recovery plans allow you to model and customize failover and recovery of multitier applications that are spread over multiple VMs. Disaster recovery plans can be automated with Azure Automation runbooks.
- **Multitier apps.** You can create disaster recovery plans for sequenced failover and recovery of multitier apps. You can group machines in different tiers (for example, database, web, app) within a disaster recovery plan and customize how each group fails over and starts up.
- **Integration with existing BCDR technologies.** Azure Site Recovery integrates with other business continuity and disaster recovery (BCDR) technologies. For example, you can use it to protect the SQL Server backend of corporate workloads, including native support for SQL Server AlwaysOn, to manage the failover of availability groups.
- **Automated disaster recovery plans.** The Azure Automation runbook gallery provides production-ready, application-specific scripts that can be downloaded and integrated with Azure Site Recovery.

Azure Site Recovery .vs vCloud Air Disaster Recovery

Azure Site Recovery provides business continuity by orchestrating the replication of on-premises virtual machines—Hyper-V VMs, VMware VMs, and Windows or Linux physical servers—to Azure, or to a secondary site. vCloud Air Disaster Recovery is a disaster recovery services offering owned and operated by VMware and built on vSphere Replication and vCloud Air. It’s intended only for vSphere Replication.

These are some of the advantages that Azure Site Recovery has over vCloud Air Disaster Recovery:

- **Replicate workloads running on VMs and physical servers.** With Azure Site Recovery, you can replicate workloads running on VMs and physical servers to Azure, and to a secondary site. This includes replication of any workload running on supported on-premises Hyper-V VMs, VMware VMs, and Windows or Linux physical servers. vCloud Air Disaster Recovery is built on vSphere Replication and vCloud Air for the disaster recovery of hybrid cloud platforms for the VMware environment.

- **Migrate VMs to the cloud.** Azure Site Recovery migrates on-premises and other cloud (AWS instances) to Azure VMs. (See Figure 5.) vCloud Air Disaster Recovery with Hybrid Cloud Manager extends on-premises vSphere VM migration to and from vCloud Air.

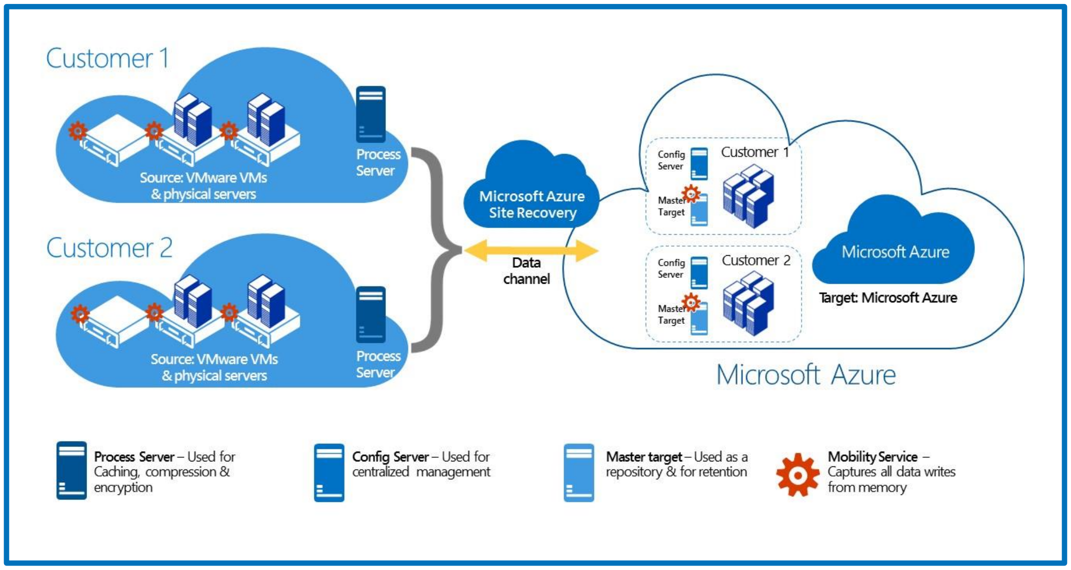

Customer 1
Process Server
Source: VMware VMs & physical servers
Customer 2
Process Server
Source: VMware VMs & physical servers
Microsoft Azure Site Recovery
Data channel
Config Server
Customer 1
Master Target
Config Server
Customer 2
Master Target
Microsoft Azure
Target: Microsoft Azure
Microsoft Azure
Process Server – Used for Caching, compression & encryption
Config Server – Used for centralized management
Master target – Used as a repository & for retention
Mobility Service – Captures all data writes from memory

Figure 5: Migrating VMs to the cloud

- **Fine tune replication frequency.** Azure Site Recovery provides replication as frequently as every 30 seconds for Hyper-V and continuously for VMware. You can set RPO thresholds to control how often data recovery points are created, and you can reduce RTOs. VMware vCloud Air Disaster Recovery supports RPO thresholds allowed in vSphere Replication—from 15 minutes to 24 hours.

Advantages of Azure BCDR solutions over VMware solutions

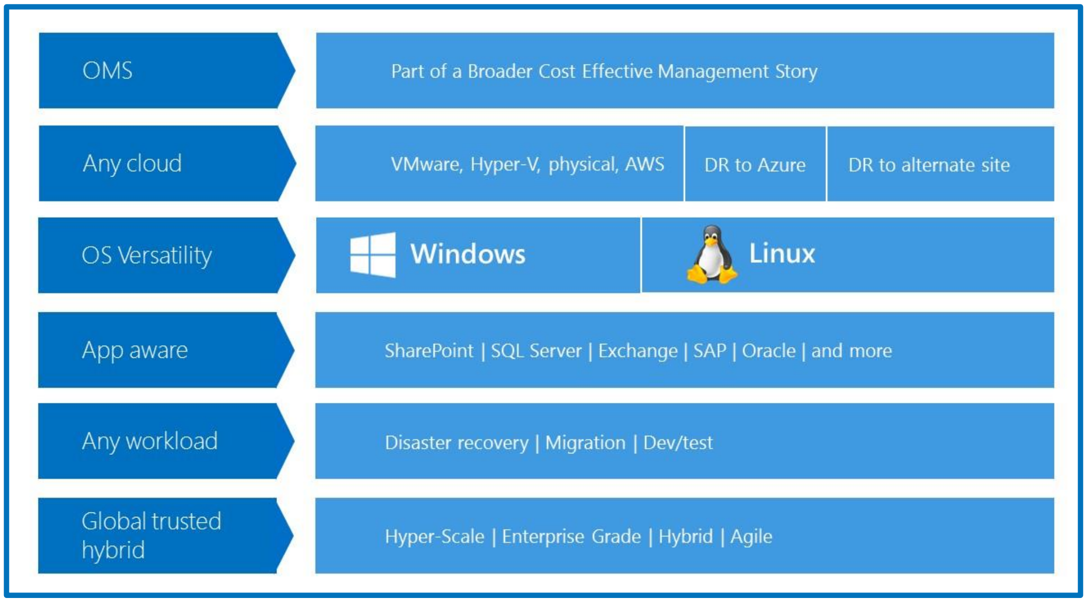
Azure business continuity and disaster recovery solutions provide advantages above and beyond what VMware solutions provide.

Supported scenarios in Azure Site Recovery vs. VMware Site Recovery Manager

Azure Site Recovery is a complete disaster recovery solution. (See Figure 6.)

- **Any cloud.** Azure Site Recovery protects physical servers and VMs (VMware and Hyper-V). It protects VMs on Azure and other cloud platforms, including AWS.
- **OS versatility.** Azure Site Recovery supports both Windows and Linux.

- **Any workload.** From small dev/test projects to global product launches, Azure is engineered to handle any workload, including SharePoint, Exchange, Dynamics, SQL Server, Active Directory, Oracle, SAP, IBM, Red Hat, and many more.
- **The power of Azure.** Azure Site Recovery is deployed at cloud scale, is backed by an enterprise-grade SLA and currently has more global datacenters than any other hyper-scale cloud provider.



OMS	Part of a Broader Cost Effective Management Story		
Any cloud	VMware, Hyper-V, physical, AWS	DR to Azure	DR to alternate site
OS Versatility	Windows	Linux	
App aware	SharePoint | SQL Server | Exchange | SAP | Oracle | and more		
Any workload	Disaster recovery | Migration | Dev/test		
Global trusted hybrid	Hyper-Scale | Enterprise Grade | Hybrid | Agile		

Figure 6: Azure Site Recovery—Complete disaster recovery solution

Feature comparison—VMware Site Recovery Manager vs. Azure Site Recovery

Feature	VMware Site Recovery Manager	Azure Site Recovery
Heterogeneous protection: support for Hyper-V, VMware, AWS, and physical servers Notes: • Azure Site Recovery can support heterogeneous protection and on-premises VMware VMs, Hyper-V VMs, AWS, and Windows or Linux physical servers. • VMware Site Recovery Manager and VMware vCloud Air Disaster Recovery can support VMware and VMware environments that use vSphere or array-based replication. They are not ideal for heterogeneous environments.	✗	✓

Hybrid support and experience across public, private, and service provider clouds Notes: • Azure Site Recovery provides the same experience across private, public, and service provider clouds. • Site Recovery Manager is the primary VMware DR product and has limited integration with vCloud Air. It supports VMware environments that use vSphere or array-based replication. It's not ideal for hybrid environments.	–	✓
Number of regions supported Notes: • Azure currently supports the largest number of regions. • Azure includes 38 regions while VMware has 11 regions.	9 sites + 2 government-only sites	38
No on-premises DR software needed	X	✓
Physical server (support for Windows and Linux)	X	✓
Requires a secondary site for failover Notes: • Azure Site Recovery can replicate to Azure storage or to a secondary datacenter. Azure Site Recovery supports both site-to-site and site-to-cloud replication. • VMware Site Recovery Manager offers a site-to-site DR option that requires the purchase of an expensive secondary site. If a you want to use cloud DR with VMware, you need to use vCloud Air and give up guaranteed recovery as well as sufficient and scalable storage.	X	✓
Security and encryption available both in transit and at rest Note: • VMware Site Recovery Manager provides security and encryption during transit, not at rest.	–	✓
Short recovery point objective Note: • vCloud Air DR RPO thresholds are at least 15 minutes. Azure Site Recovery thresholds are as short as 30 seconds.	–	✓
Limitless VM protection for site-to-cloud DR Notes: • Azure Site Recovery helps you protect 1000s of VMs with a few simple steps. • vCloud Air DR enables self-service protection for up to 500 VMs per subscription.	–	✓
Certified support for Microsoft applications	–	✓
New features as they become available	X	✓

N-tier consistency Note: • VMware supports only array-based replication.	⊖	✓

Feature comparison—VMware vCloud Air Data Protection vs. Azure Backup

Feature	VMware vCloud Air Data Protection	Azure Backup
Long-term retention policy Notes: • Azure Backup provides a retention policy of up to 10 years. Long-term retention is up to 99 years. • VMware provides a retention policy of 1 to 365 days.	⊖	✓
Solution for any cloud Notes: • Azure Backup supports heterogeneous backup on-premises. • Azure Backup supports VMware VMs, Hyper-V VMs, AWS, and Windows and Linux physical servers. • VMware supports dedicated and virtual private clouds.	⊖	✓
Heterogeneous storage Notes: • Azure Backup provides automatic storage management. • Azure Backup backs up data on-premises and synchronizes data in the cloud.	⊖	✓
Application-consistent backup Notes: • With Azure Backup, no additional fixes are required to restore application data.	⊖	✓

Flexible, simple and cost-effective

Azure Site Recovery and Azure Backup disaster recovery plans are deployed and managed from Azure and backed by an enterprise-grade SLA. You can be confident that if an application, server, or datacenter fails, the workload is backed up and replicates to Azure, ensuring business quickly returns to normal.

Because of the scalability, support for hybrid environments, certified workload support for popular workloads and sensible pricing model, Microsoft competes favorably in these scenarios:

Flexibility and support for hybrid IT

Microsoft business continuity and disaster recovery services are integrated into Azure, and Azure Backup and Azure Site Recovery are managed from the Azure portal. VMware does not offer first-class integration—it offers basic services with limited hybrid use. Microsoft helps to provide data protection solutions to replicate across any workload running on supported on-premises Hyper-V VMs, VMware VMs, and Windows and Linux physical servers, including physical to virtual, virtual to hybrid cloud, hybrid cloud to public cloud, and on-premises AWS instances to Azure VMs. (See Figure 7.) You can replicate on-premises workloads to Azure with Azure Site Recovery for 31 days at no charge, effectively making migration to Azure free.

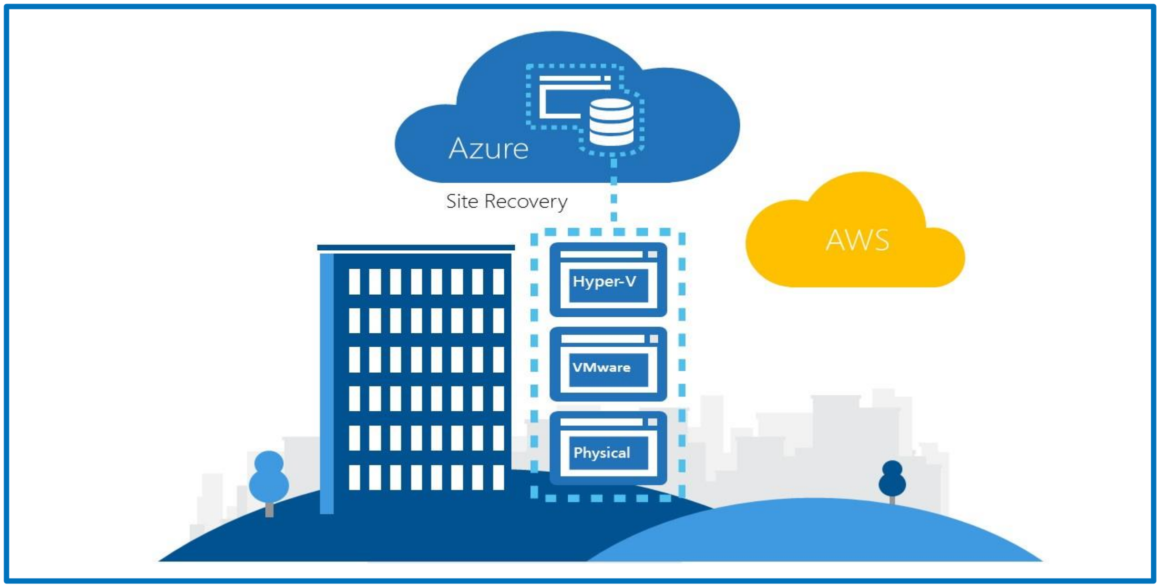


Figure 7: Flexible replication and migration to Azure

Support for heterogeneous environments: VMware to Azure

Many customers have large VMware deployments as part of heterogeneous environments and have not yet committed to public clouds, either as components in datacenters or for disaster recovery. By using Azure Site Recovery, you can coordinate replication, failover and recovery of on-premises VMware virtual machines to Azure storage. To migrate VMware VMs and physical servers, you perform almost the same steps as those used for regular replication.

Cost-effective

With Azure Site Recovery, ensure applications are available in Azure, and with Azure Backup, backups are protected in Azure. This means that you don't have to pay for infrastructure or maintenance costs and that you have one centralized location for managing your disaster recovery plans. Azure Backup is cost-effective for both short-term operational recovery and long-term retention and archive because storage is charged on a pay-as-you-go basis. With Azure Site Recovery, you pay for the workloads running in Azure.

The following information details the pricing for each product and provides an illustration of the cost differences between the VMware DR solution and Microsoft Azure Site Recovery and Azure Backup.

vCloud Air Data Protection pricing

Service	**Included resources**	**Price per month**	**Price per unit**
Data protection	1 TB	$430	$0.43/GB/month

Source: VMware Cloud Computing Pricing Guide

Azure Backup pricing

The pricing model for Azure Backup has two components: the number of *instances* that are protected by the Azure Backup service, and *storage,* which is the amount of data stored with the service.

Size of each instance	**Azure Backup price per month**
Instance <= 50 GB	$5 + storage consumed
Instance > 50 but <= 500 GB	$10 + storage consumed
Instance > 500 GB	$10 for each 500 GB increment + storage consumed

Note: Prices are current as of April 2017 and are subject to change.

Source: Azure Backup Pricing

VMware vCloud Air DR pricing

Service	Included resources	Price per month	Price per unit
Compute	20 GB VRAM, 10 GHz CPU	$226	$0.02/GB/hour
Storage & support	1 TB storage	$265	$0.27/GB/month
Bandwidth	10 Mbps	$229	$0.03/Mbps/hour
Public IPs	Priced per IP (2 included)	$50	$25 each

Source: VMware Cloud Computing Pricing Guide

VMware SRM pricing

License options	License cost[1]	One-year support cost
VMware SRM Standard (v6)	$4,875 per 25-pack OSI	Basic—$1,024; Production—$1,219
VMware SRM Enterprise (v6)[2]	$12,375 per 25-pack OSI	Basic—$2,599; Production—$3,094
vCloud Suite Enterprise (includes VMware SRM Enterprise)	$11,500 per processor	Basic—$2,414; Production—$2,874

[1] "Per processor" is for virtual environments with high consolidation ratios. "Per VM" or "per OSI" (for virtual machine or physical server) is for virtual environments with low consolidation ratios.

[2] Enterprise includes Stretched Storage Support, orchestrated cross-vCenter vMotion, VMware NSX integration, and storage profile protection groups; the Standard version does not include these features.

Source for VMware SRM Standard (v6) pricing:
VMware Store—Site Recovery Manager Standard Edition

Source for VMware SRM Enterprise (v6) pricing:
CDW—Site Recovery Manager Enterprise Edition

Azure Site Recovery pricing

	Price for first 31 days	Price after 31 days
Azure Site Recovery to customer-owned sites	Free	$16/month per instance protected
Azure Site Recovery to Azure	Free	$25/month per instance protected

Note: Prices are current as of April 2017 and are subject to change.

Source: Azure Site Recovery Pricing

Test case: Total cost of ownership (TCO) competitive pricing for VMware Site to vCloud Air DR and VMware Site to Azure Site Recovery

To help you assess the pricing of the previously mentioned solutions, here's a comparison of the costs of Azure Site Recovery / Azure Backup with those of VMware vCloud Air DR:

Parameter	Test case	VMware site to vCloud Air DR	VMware site to Azure Site Recovery / Azure Backup
Basic parameters	6 VMs (1 core each) 3-tier application (e.g., SharePoint)	$226/month for computer resources $229/month for bandwidth	**$25/month** for Azure Site Recovery **$268/month** for 2 VMs **$335/month** for computer resources
Storage	2 TB	$530/month for storage resources	**$49/month** for storage resources
Test failovers	Quarterly testing, 4 days per test	$265/year	$25/year
Failover/failback	5% churn rate with 3 – 4 week run time	$455/year	$603/year
1-year TCO	N/A	$12,540	$8,752
3-year TCO	N/A	$37,620	$26,256

Note: Prices are current as of April 2017 and are subject to change.

Source: Azure Site Recovery Pricing

Azure Site Recovery eliminates the cost of maintaining a secondary datacenter

Figure 8 compares the costs of maintaining 400 VMs in an enterprise with no site-recovery solution with the costs of using a do-it-yourself solution and the costs of using Azure Site Recovery.

By using Azure Site Recovery, you can replicate workloads running on VMs and physical servers to Azure rather than replicating them to a secondary site. This eliminates the cost and complexity of maintaining a secondary datacenter. When you use Azure as your secondary DR site, capital and operating expenses are replaced with a pay-as-you-go model, so you only pay for the workloads running in Azure when you need them.

Figure 10 compares the costs of maintaining 400 VMs in an enterprise with no site-recovery solution, a do-it-yourself solution, and ASR.

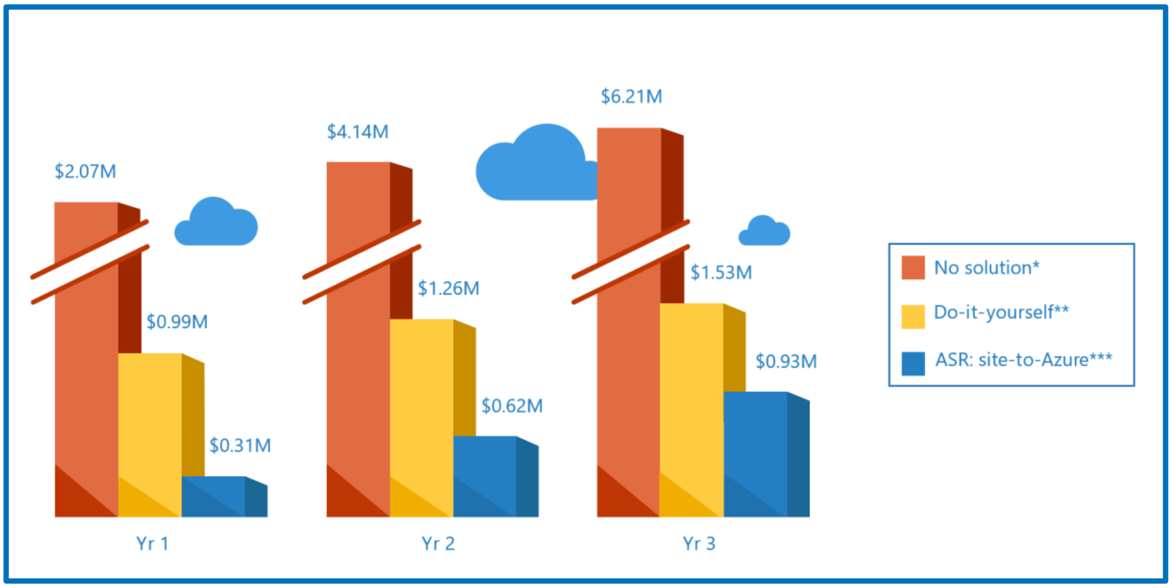


Figure 8: Cumulative costs over three years, 400 VMs

*Assumes average cost of datacenter outage ($690,000), multiplied by number of outages (3).

**Assumes licensing costs, hardware expenses, heating and cooling expenses, and one Operations Engineer salary for 400 mid-sized VMs.

***Assumes list pricing and ½ Operations Engineer salary for 400 mid-sized VMs.

All cost scenarios are estimates based on internal Microsoft analysis and calculations.

Source: Azure Site Recovery Datasheet

Conclusion

In a world of emerging data and heterogeneous multi-OS, multi-hypervisor, and even multi-cloud architectures, dynamically protecting data and applications is imperative, regardless of industry or company size. The penalty for downtime or data loss can be severe so IT groups need a reliable solution to transform their data protection.

With cloud disaster recovery solution offerings emerging as viable, more affordable and more scalable alternatives, it can help you start protecting your data in a more robust yet affordable way. Azure is the fully integrated, end-to-end, holistic backup and disaster recovery solution with simplified management. Businesses that implement Azure Backup and Azure Site Recovery can transform disaster recovery from operational overhead to a convenient service-based framework with a pay-as-you-go model, ensuring business continuity.

With Azure Backup and Azure Site Recovery, storing data in Azure alleviates the costs associated with paying for and managing a secondary site. Azure Site Recovery and Azure Backup are deployed at cloud scale and backed by an enterprise-grade SLA with more global data centers than any other cloud provider. Azure's scalability, support for hybrid environments and popular workloads and affordable pricing ensure that the combination of Azure Site Recovery and Azure Backup provide business continuity.

References and next steps

Explore Azure Site Recovery

Azure Site Recovery overview

Documentation

Pricing

Explore Azure Backup

Azure Backup overview

Documentation

Pricing

Get started with Azure Backup and Azure Site Recovery today

Azure portal