INOVASYS

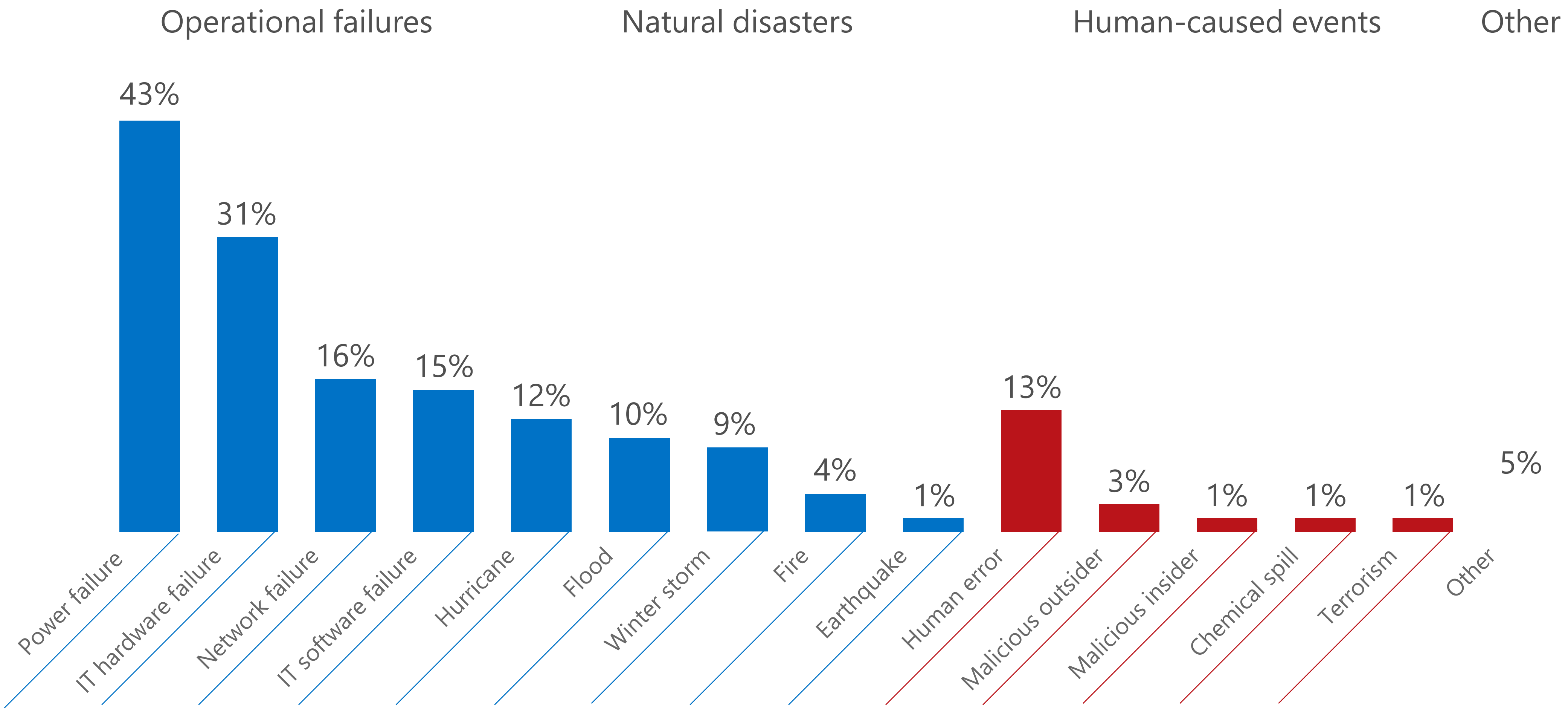
ThinkBIG

Microsoft Business Continuity Solutions

Microsoft Gold Partner

Causes of IT "disasters"

Most are caused by operational failures – not natural disasters



Source: Forrester "The State of Business Technology Resiliency Q2 2014", May 12, 2014

Customer challenges

Without strong backup & disaster recovery solutions, customers are exposed to risk

$1.25B to $2.5B

Average annual cost of downtime for F1000[1]

$500K to $1M

Average hourly cost of a critical application failure[1]

$100K

Average hourly cost of an infrastructure failure[1]

Source:
1: IDC: DevOps and the Cost of Downtime: Fortune 1000 Best Practice Metrics Quantified

Common customer challenges…

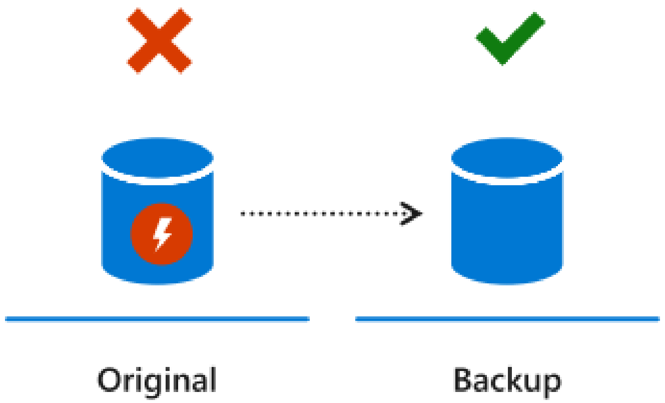
"I need to consolidate vendors and require a partner who can solve my disaster recovery and backup needs under one contract."

"My infrastructure is extremely complex and features a mix of Linux, VMware, and Windows software."

"I am looking to take advantage of a hybrid deployment but it is a complicated process to migrate workloads to the cloud."

"I know the cloud has a number of useful services but it has proven difficult to achieve in reality."

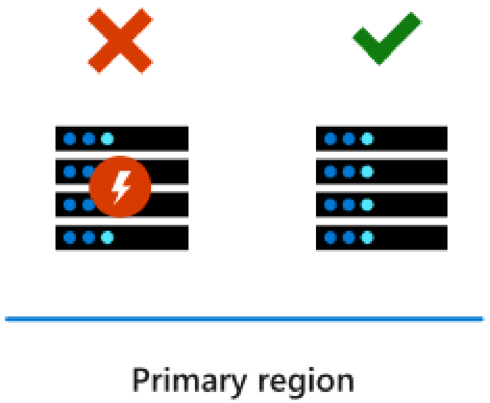
Delivering resilient applications in Azure



Backup

When your data is corrupted, deleted, or lost you can restore it

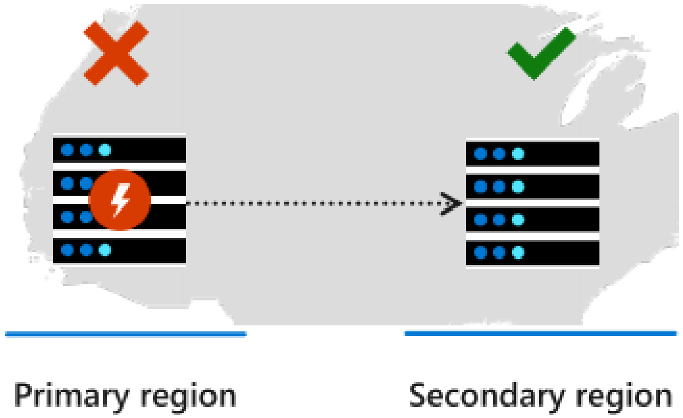
Azure Backup



High availability

When your applications or infrastructure have failure, run a second instance in the primary site

Availability Sets, Zones and Region Pairs



Disaster recovery

When your primary site has failures, run your applications in secondary site

Azure Site Recovery

Common enterprise challenges

Business continuity & data protection are critical issues for every organization

Limiting downtime

Downtime puts your organization’s reputation, finance, and productivity at risk

Reducing costs

The costs of maintaining secondary sites and infrastructure can be prohibitive

Managing complexity

Managing complex environments while meeting RPO and RTO standards is often difficult for IT

Ensuring compliance

Regulatory and compliance demands for data retention and protection may be taxing for your business

Scaling protection

Protection beyond mission-critical apps and data is unrealistic for most businesses

Data Protection Challenges

Rapid Data Growth

Data rates are growing at over 40% per year.

+

Operation Challenges

Cost of storage growing

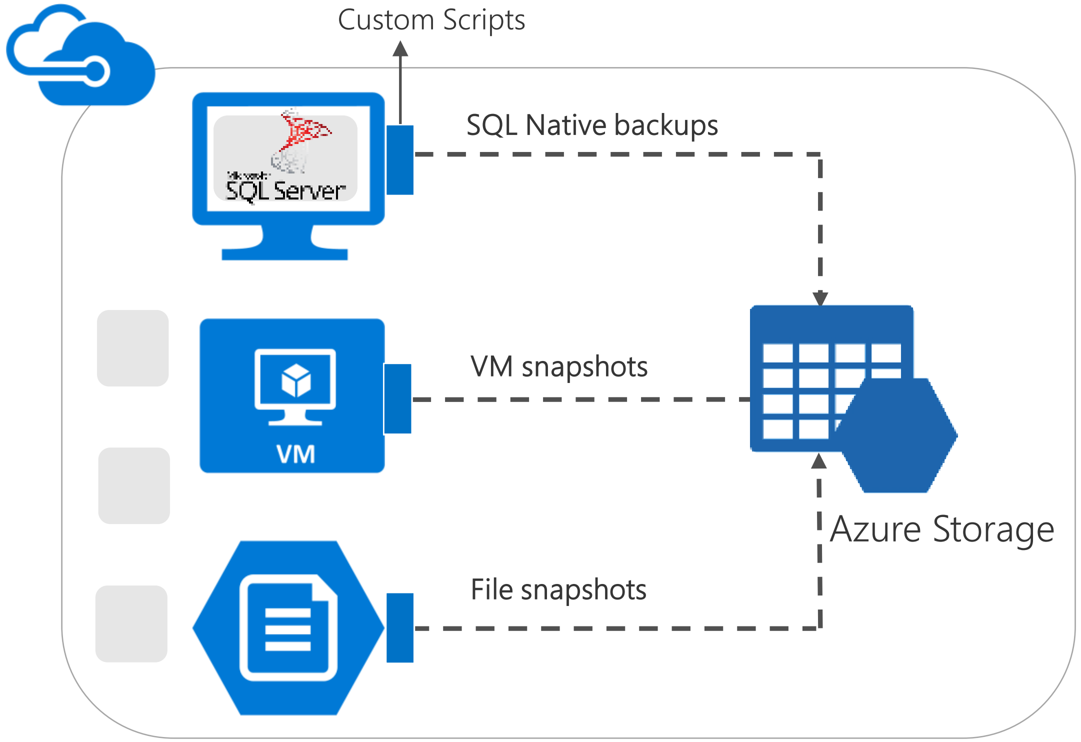
Cost of backup solutions

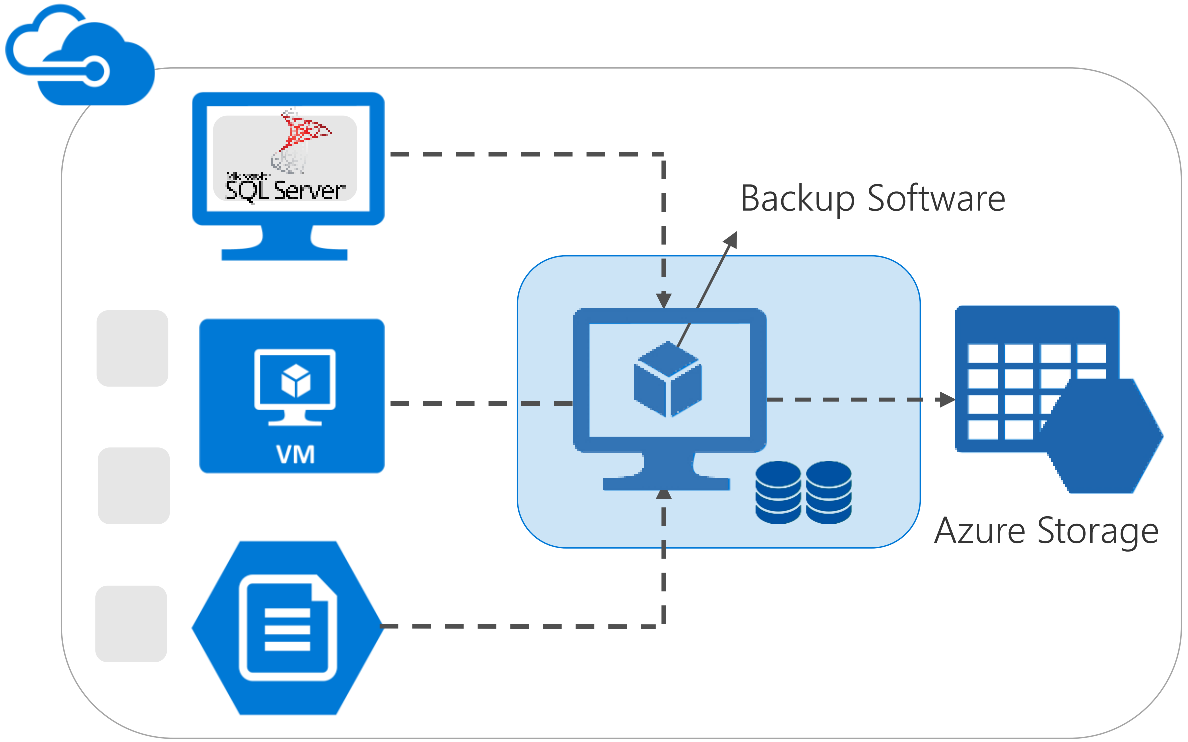
Complexity of managing all that storage

=

Important data may go without the protection it should have

Conventional backup approaches





✗ Need to manage Infrastructure

✗ No Central Management

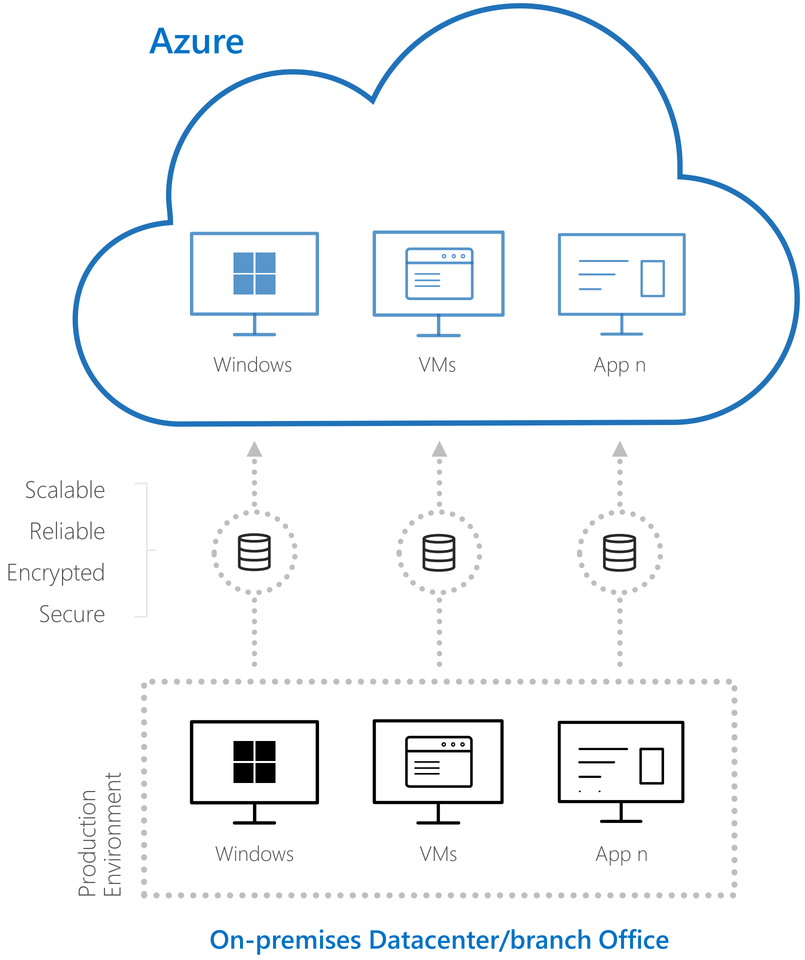
✗ Infrastructure Management

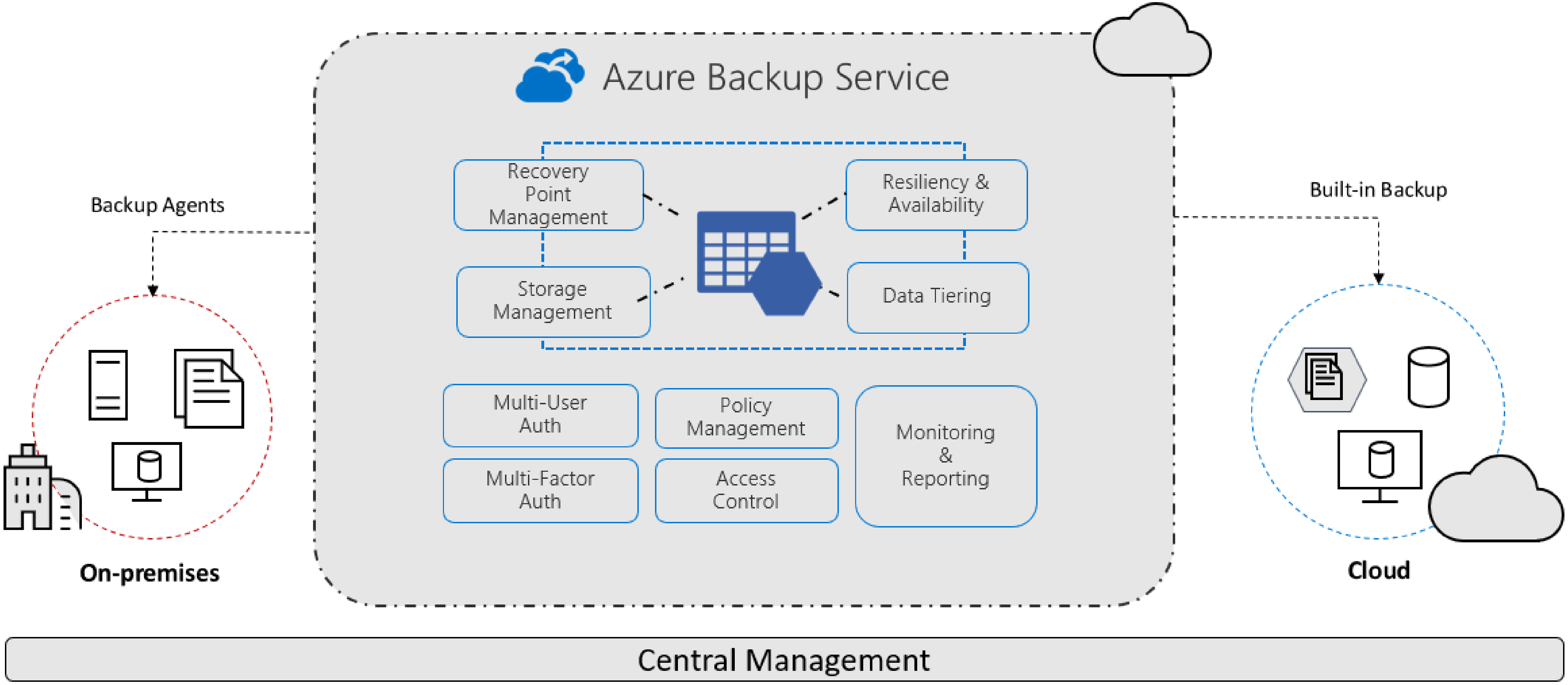
✓ Some Central Management

Cloud first backup

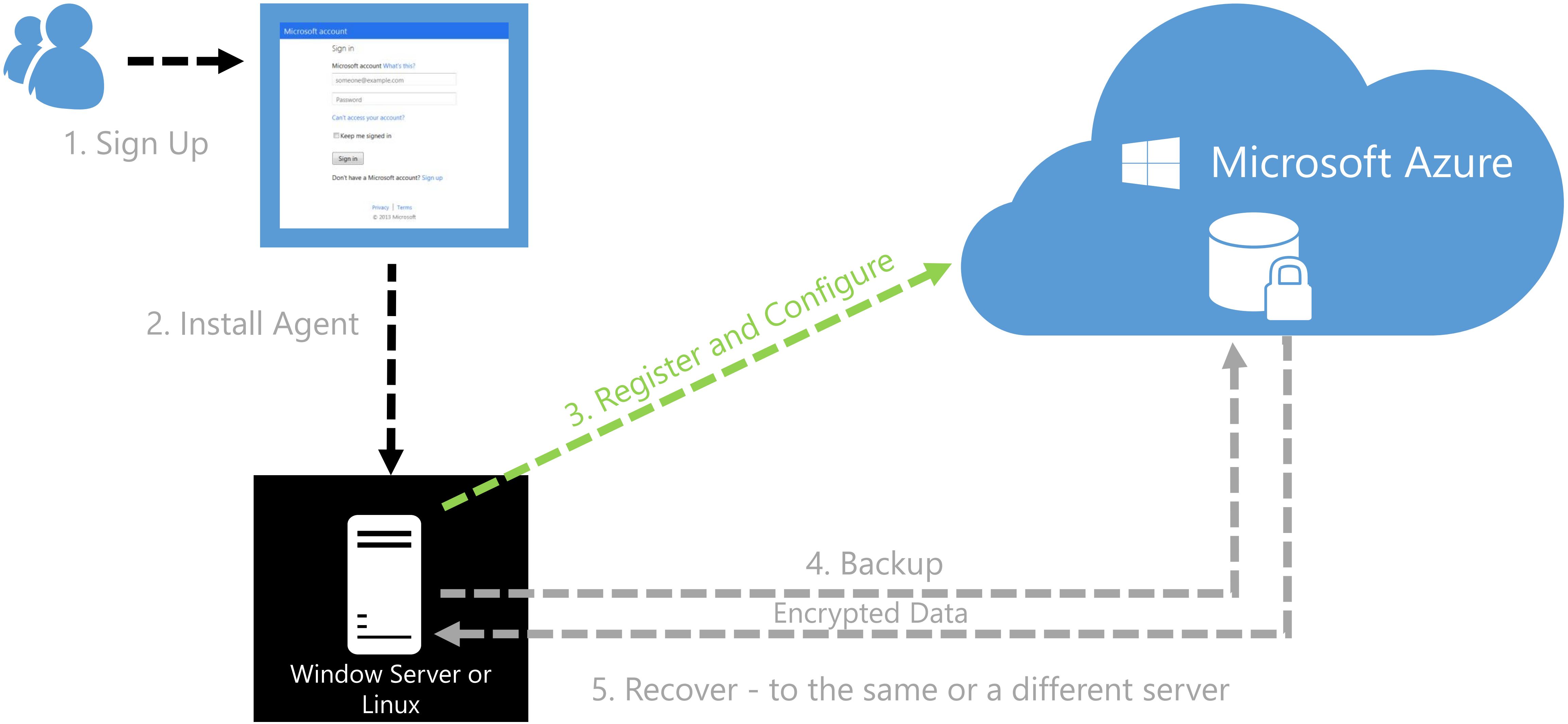
Unifying data protection across the enterprise

- → Gets you out of the business of maintaining backups as your IT strategy shifts to the cloud
- → Supports born-in-the-cloud applications with an all-in-one, cloud-native, backup solution
- → Protects remote offices and branch locations without the complexity of in-house management
- → Delivers faster time-to-value without the overhead and capital expense of standing up a backup solution
- → Stops hardware sprawl in its tracks even when facing severe app proliferation and massive data growth
- → Economical cloud pricing with pay-as-you-go storage




Azure Backup Service
Backup Agents
Built-in Backup
Recovery Point Management
Resiliency & Availability
Storage Management
Data Tiering
Multi-User Auth
Policy Management
Monitoring & Reporting
Multi-Factor Auth
Access Control
On-premises
Cloud
Central Management

How Microsoft Azure Backup Works



1. Sign Up

2. Install Agent

3. Register and Configure

4. Backup

Encrypted Data

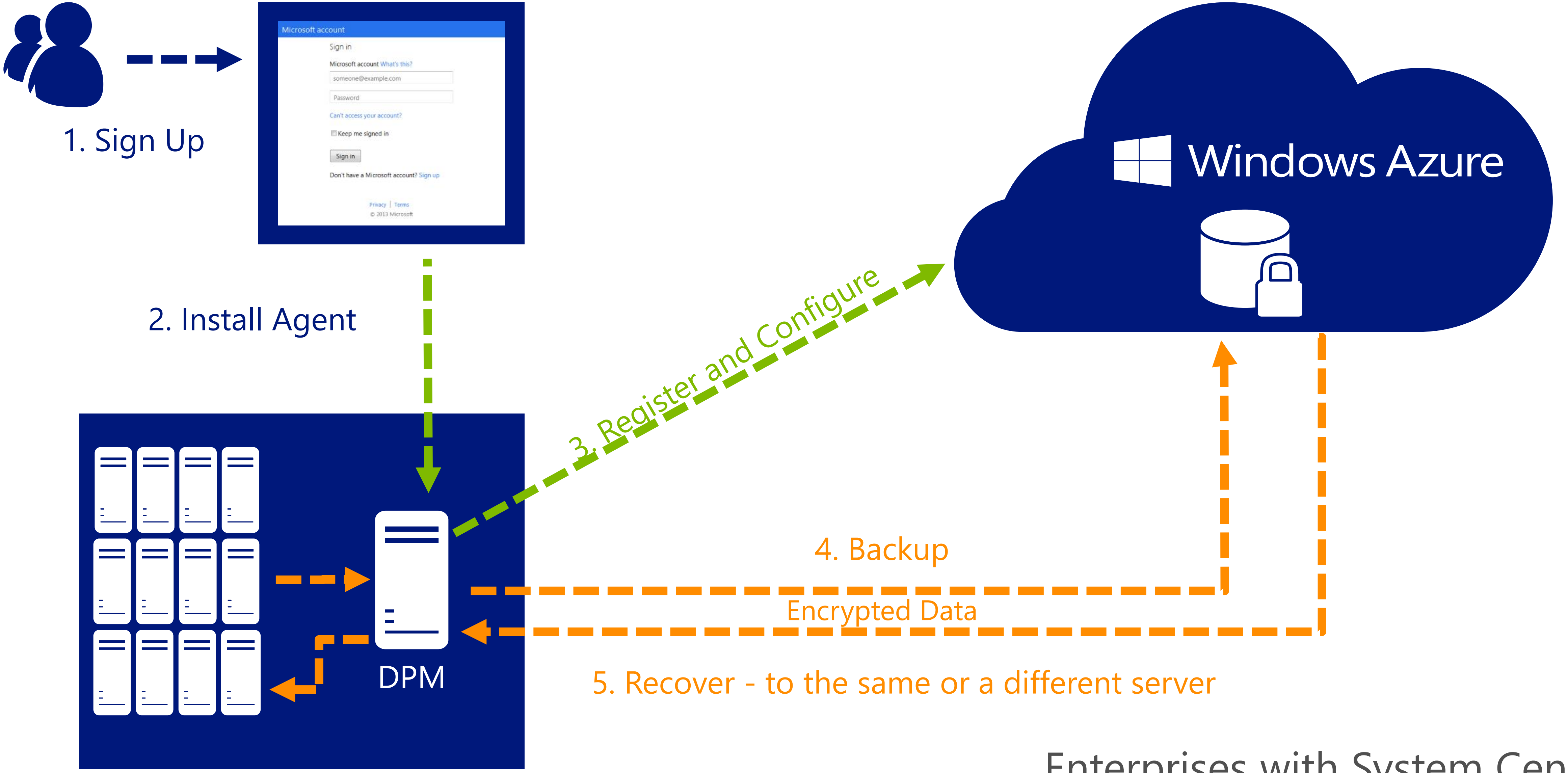
5. Recover - to the same or a different server

Window Server or Linux

Microsoft Azure

Small Business or Branch Office

How Windows Azure Backup Works



1. Sign Up

Microsoft account

Sign in

Microsoft account What's this?

someone@example.com

Password

Can't access your account?

□ Keep me signed in

Sign in

Don't have a Microsoft account? Sign up

Privacy | Terms

© 2013 Microsoft

2. Install Agent

3. Register and Configure

Windows Azure

DPM

4. Backup

Encrypted Data

5. Recover - to the same or a different server

Enterprises with System Center

DPM – Overview

Workload integration

DPM provides agents to protect enterprise workloads :

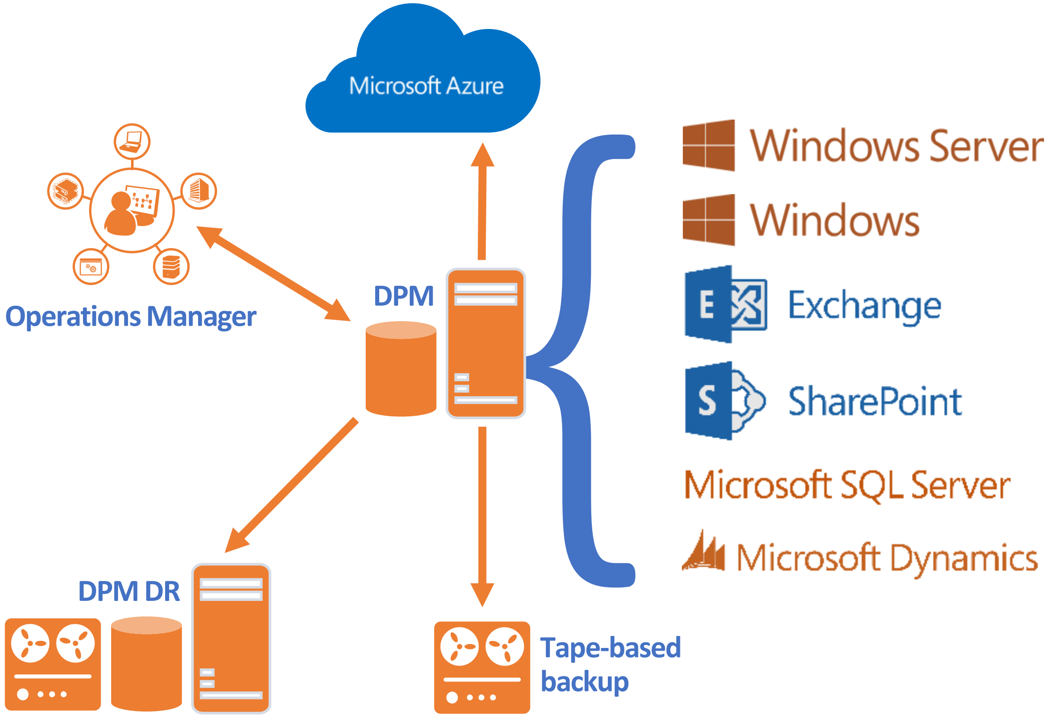
- Windows Server and Windows client
- Microsoft Exchange Server
- Microsoft SQL Server
- Microsoft SharePoint
- Microsoft Dynamics
- Microsoft Hyper-V virtual machines
- Linux (file-consistent only)

Several storage options

Data storage on disks, tapes, and cloud with Microsoft Azure Backup

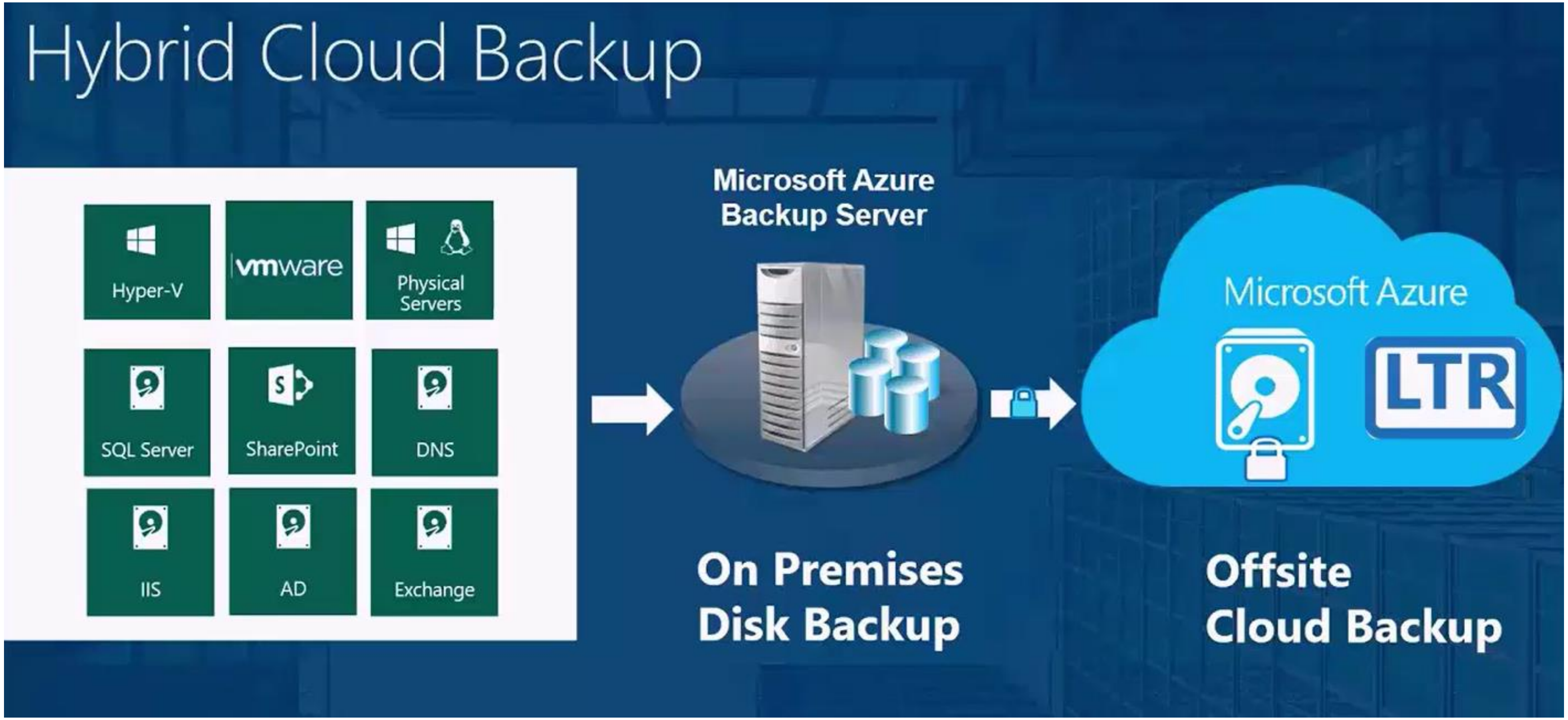
Disaster Recovery Low Cost

Possibility to chain DPM servers for a secondary protection

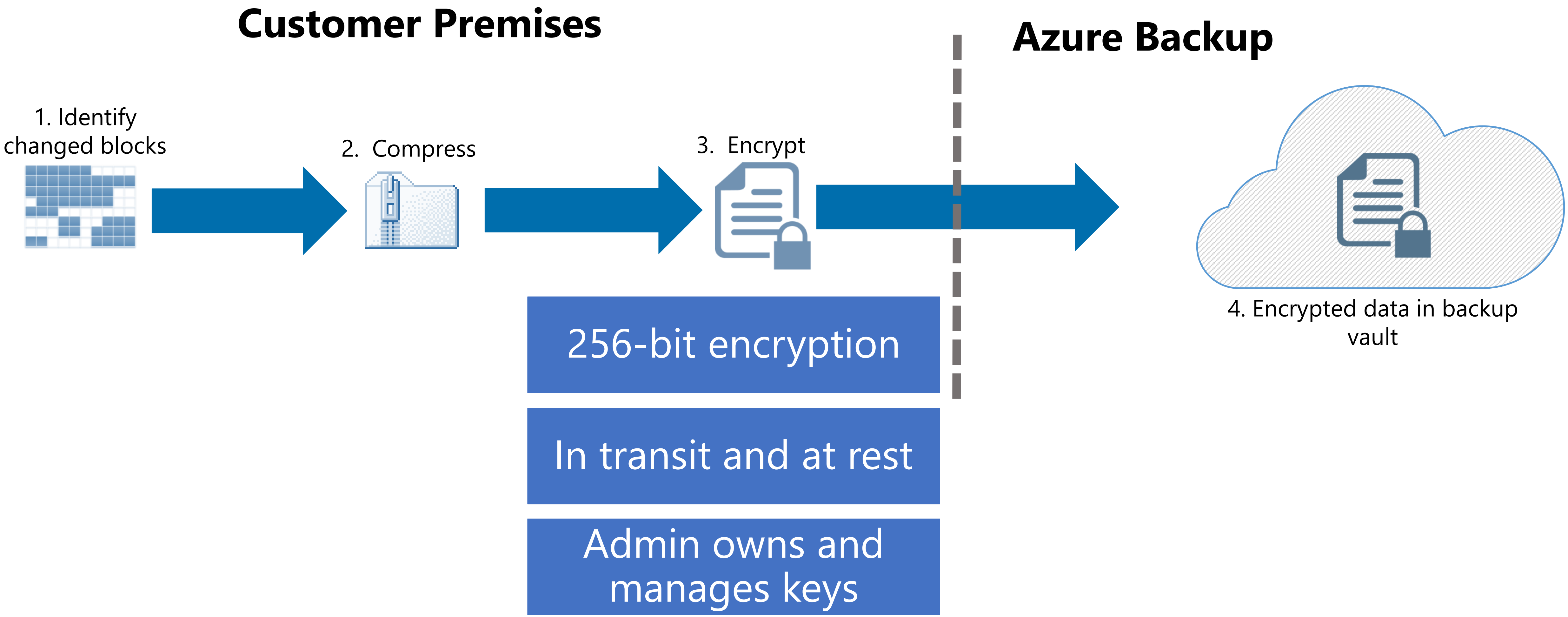


MABS – Overview

Microsoft Azure Backup Server is included as a **free download** with Azure Backup that enables cloud backups and disk backups for key Microsoft workloads such as SQL Server, SharePoint Server, and Exchange Server regardless of whether these workloads are running on Hyper-V, VMware, or physical servers



Azure Backup Security



Customer Premises

Azure Backup

1. Identify changed blocks

2. Compress

3. Encrypt

4. Encrypted data in backup vault

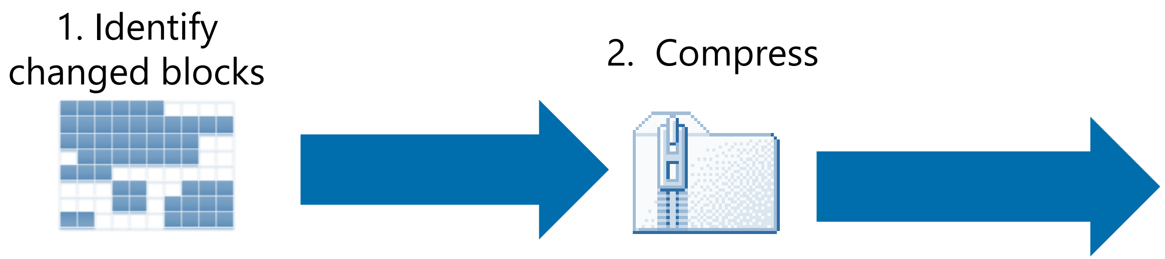
256-bit encryption

In transit and at rest

Admin owns and manages keys

Azure Backup Network Efficiency

Customer Premises



1. Identify changed blocks

2. Compress

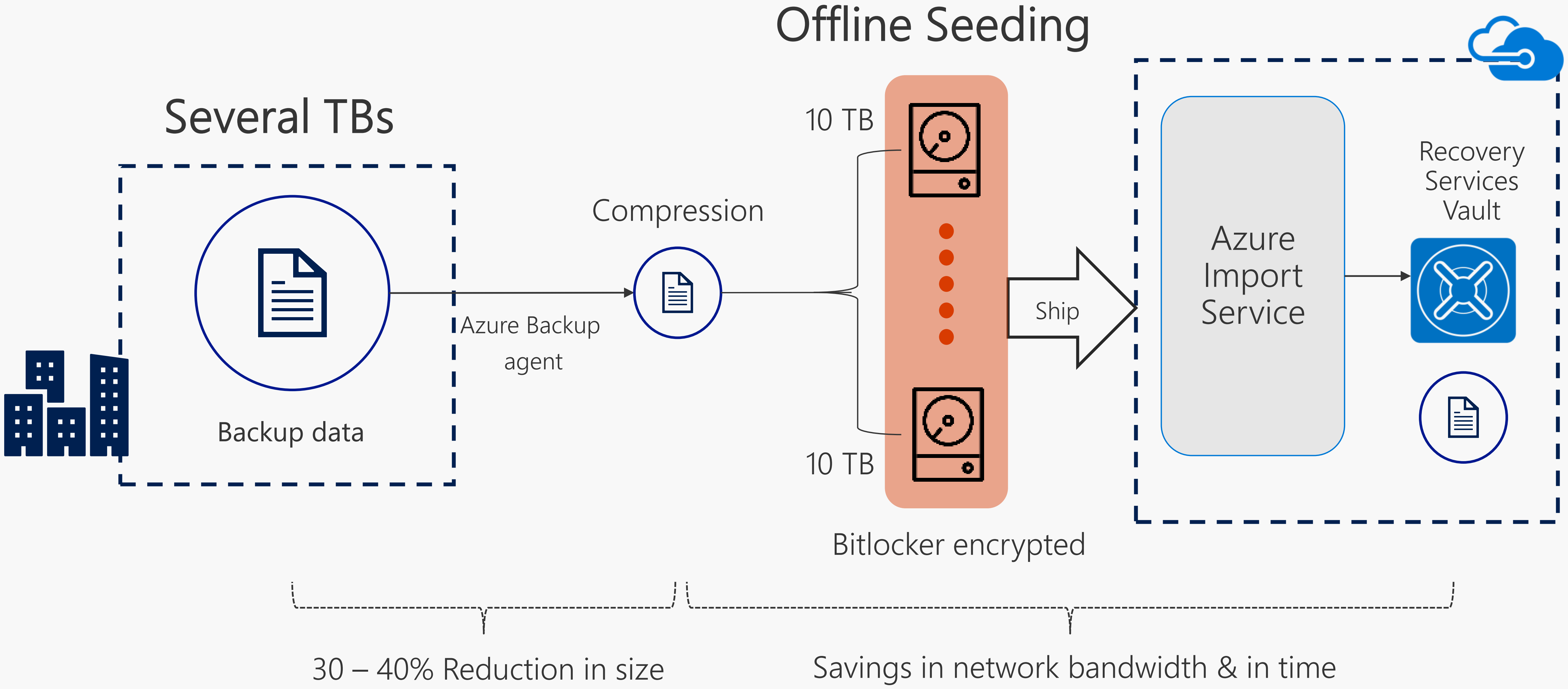
Efficient change tracking

Transfer only changed content

Compression for low bandwidth consumption

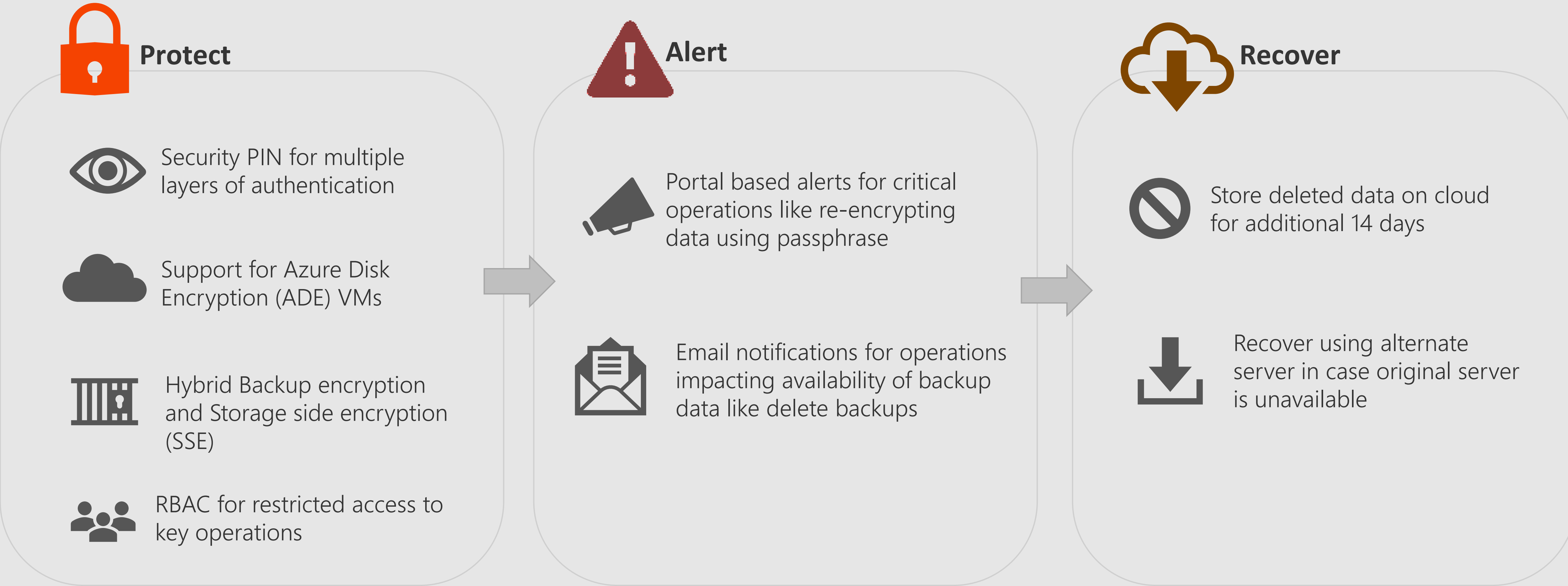
Observed 50-70%

Azure Backup – Sending (large) data efficiently



Security

Enhanced Security for Backups



Protect

- Security PIN for multiple layers of authentication
- Support for Azure Disk Encryption (ADE) VMs
- Hybrid Backup encryption and Storage side encryption (SSE)
- RBAC for restricted access to key operations

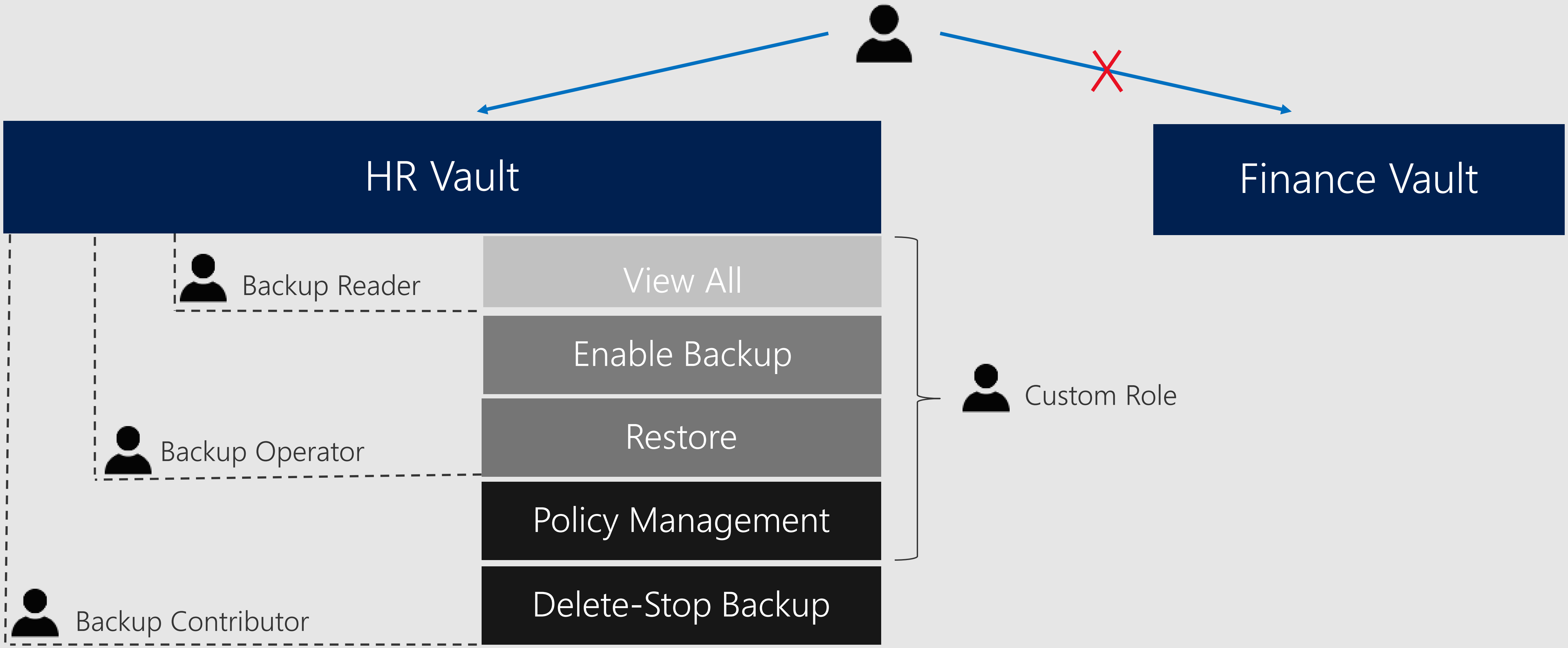
Alert

- Portal based alerts for critical operations like re-encrypting data using passphrase
- Email notifications for operations impacting availability of backup data like delete backups

Recover

- Store deleted data on cloud for additional 14 days
- Recover using alternate server in case original server is unavailable

Isolation and Access Control



HR Vault

Finance Vault

Backup Reader

Backup Operator

Backup Contributor

View All

Enable Backup

Restore

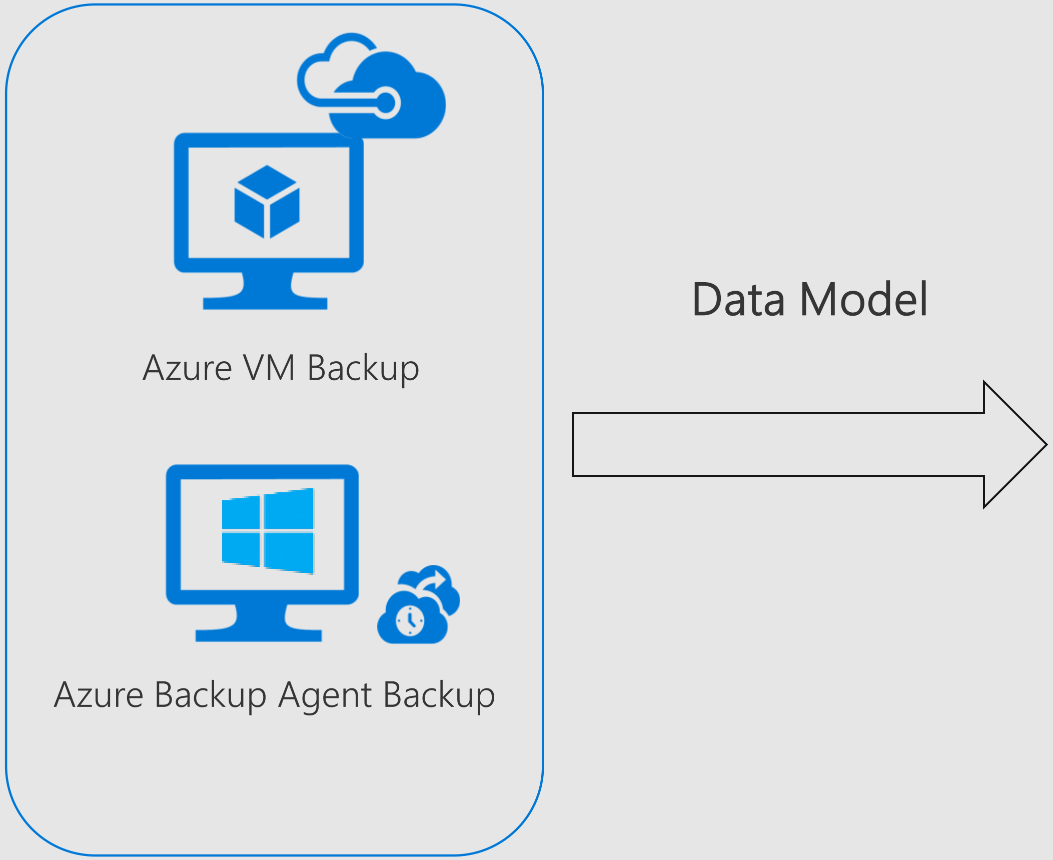
Policy Management

Delete-Stop Backup

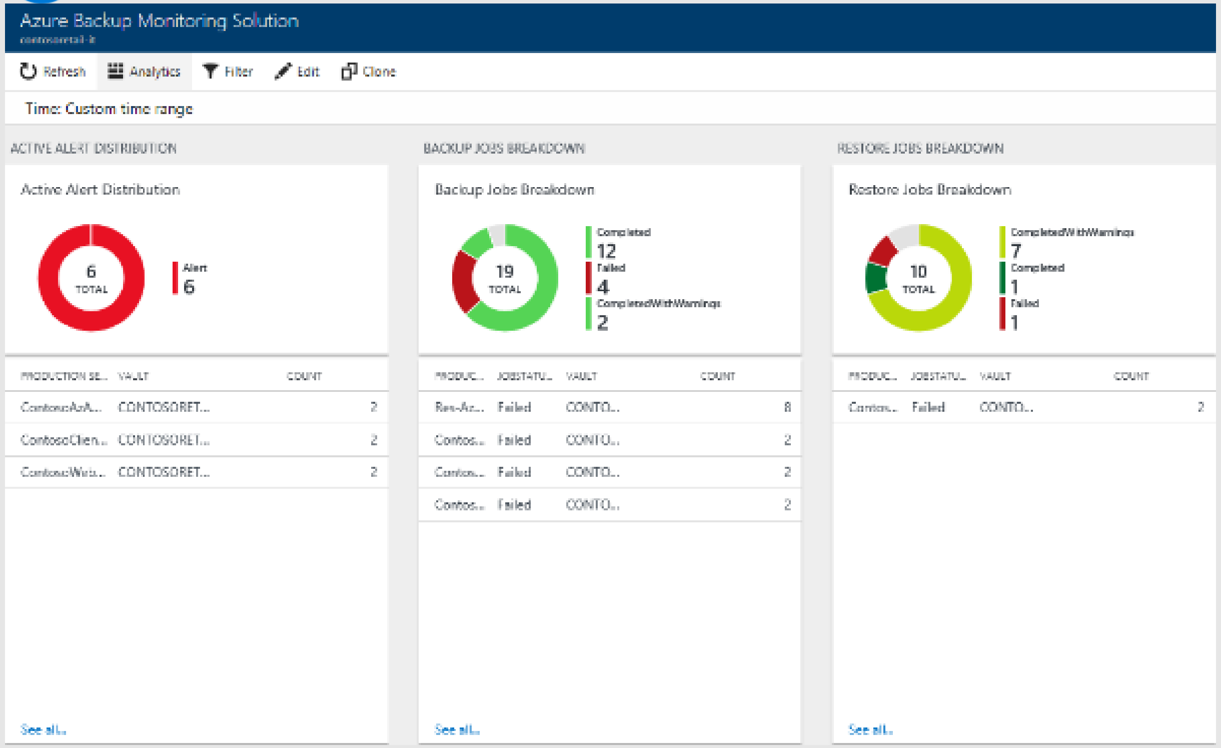
Custom Role

Monitoring and Reporting

Azure Backup Monitoring with Log Analytics



Log Analytics



Azure Backup Monitoring Solution
contosoretail-it

Refresh | Analytics | Filter | Edit | Clone

Time: Custom time range

ACTIVE ALERT DISTRIBUTION

Active Alert Distribution

6 TOTAL

Alert 6

PRODUCTION SE...	VAULT	COUNT
ContosoAzA...	CONTOSORET...	2
ContosoClien...	CONTOSORET...	2
ContosoWeb...	CONTOSORET...	2

See all...

BACKUP JOBS BREAKDOWN

Backup Jobs Breakdown

19 TOTAL

Completed 12
Failed 4
CompletedWithWarnings 2

PRODUC...	JOBSTATU...	VAULT	COUNT
Res-Az...	Failed	CONTO...	8
Contos...	Failed	CONTO...	2
Contos...	Failed	CONTO...	2
Contos...	Failed	CONTO...	2

See all...

RESTORE JOBS BREAKDOWN

Restore Jobs Breakdown

10 TOTAL

CompletedWithWarnings 7
Completed 1
Failed 1

PRODUC...	JOBSTATU...	VAULT	COUNT
Contos...	Failed	CONTO...	2

See all...

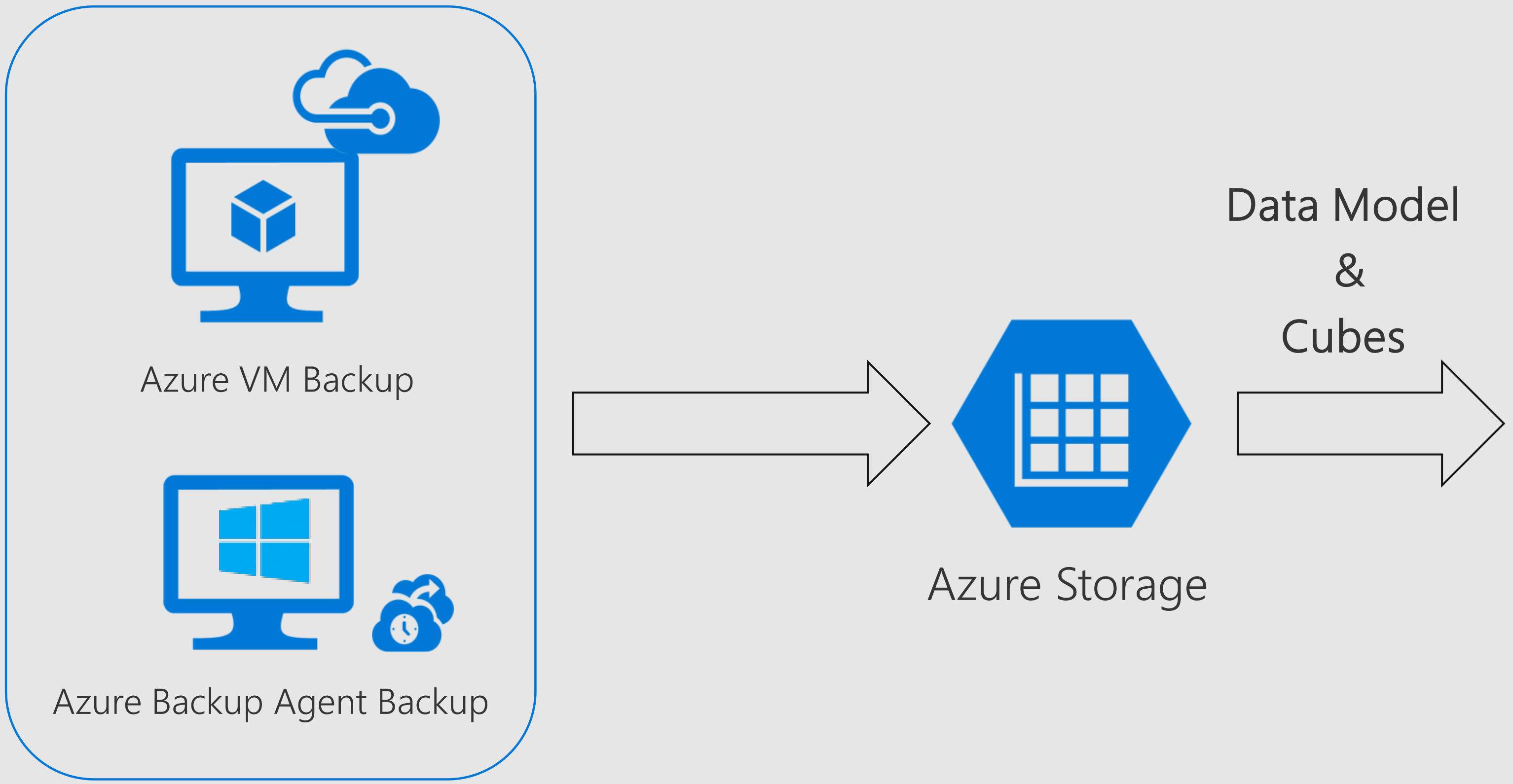
No infrastructure

Enterprise Wide

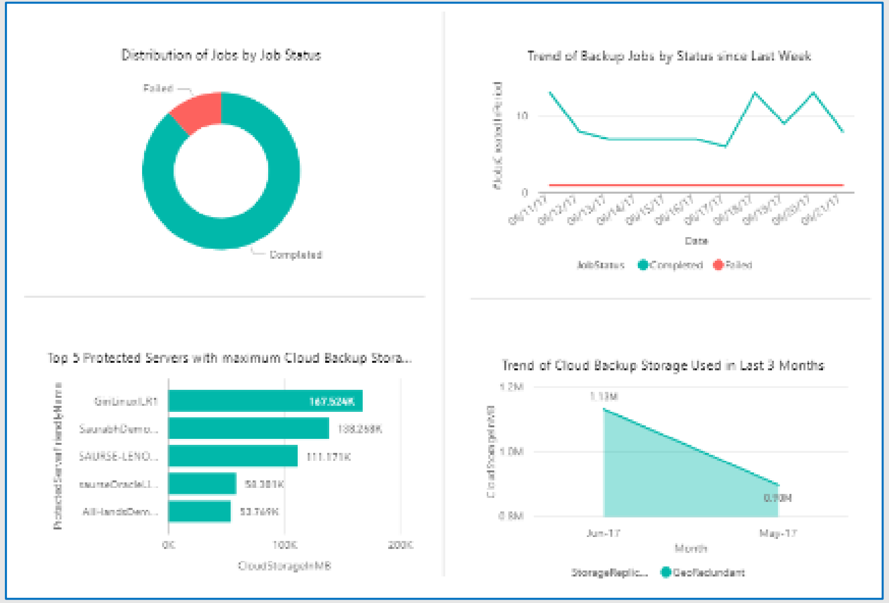
Custom Queries (KQL)

ITSM Integration

Azure Backup Reports with PowerBI



Power BI Reports



No infrastructure

Enterprise Wide

Custom Reports

Access Control

Cloud Backup – Support Matrix

Backup Support	What's backed up	Features
Azure VM backup by using VM extension	Entire VM	**Back up once a day.** App-aware backup for Windows VMs; File-consistent backup for Linux VMs. You can configure app-consistency for Linux machines by using custom scripts. Restore VM or disk. Can't back up an Azure VM to an on-premises location.
Azure VM backup by using MARS agent	Files, folders, system state	**Back up three times a day.** If you want to back up specific files or folders rather than the entire VM, the MARS agent can run alongside the VM extension.
Azure VM with DPM	Files, folders, volumes, system state, app data	**Back up twice a day.** App-aware snapshots. Full granularity for backup and recovery. Linux supported for VMs. Oracle not supported.
Azure VM with MABS	Files, folders, volumes, system state, app data	**Back up twice a day.** App-aware snapshots. Full granularity for backup and recovery. Linux supported for VMs. Oracle not supported.

On-premises Backup – Support Matrix

Backup Support	What's backed up	Features
Direct backup of Windows machine with MARS agent	Files, folders, system state	Back up three times a day No app-aware backup Restore file, folder, volume
Direct backup of Linux machine with MARS agent	Backup not supported	
Back up to DPM	Files, folders, volumes, system state, app data	App-aware snapshots Full granularity for backup and recovery Linux supported for VMs (Hyper-V/VMware) Oracle not supported
Back up to MABS	Files, folders, volumes, system state, app data	App-aware snapshots Full granularity for backup and recovery Linux supported for VMs (Hyper-V/VMware) Oracle not supported

Linux Backup – Support Matrix

Backup type	Linux (Azure endorsed)
Direct backup of on-premises machine that's running Linux	Not supported. The MARS agent can be installed only on Windows machines.
Using agent extension to back up Azure VM that's running Linux	App-consistent backup by using custom scripts. File-level recovery. Restore by creating a VM from a recovery point or disk.
Using DPM to back up on-premises machines running Linux	File-consistent backup of Linux Guest VMs on Hyper-V and VMware. VM restoration of Hyper-V and VMware Linux Guest VMs.
Using MABS to back up on-premises machines running Linux	File-consistent backup of Linux Guest VMs on Hyper-V and VMware. VM restoration of Hyper-V and VMware Linux guest VMs.
Using MABS or DPM to back up Linux Azure VMs	Not supported.

SQL Backup – Support Matrix

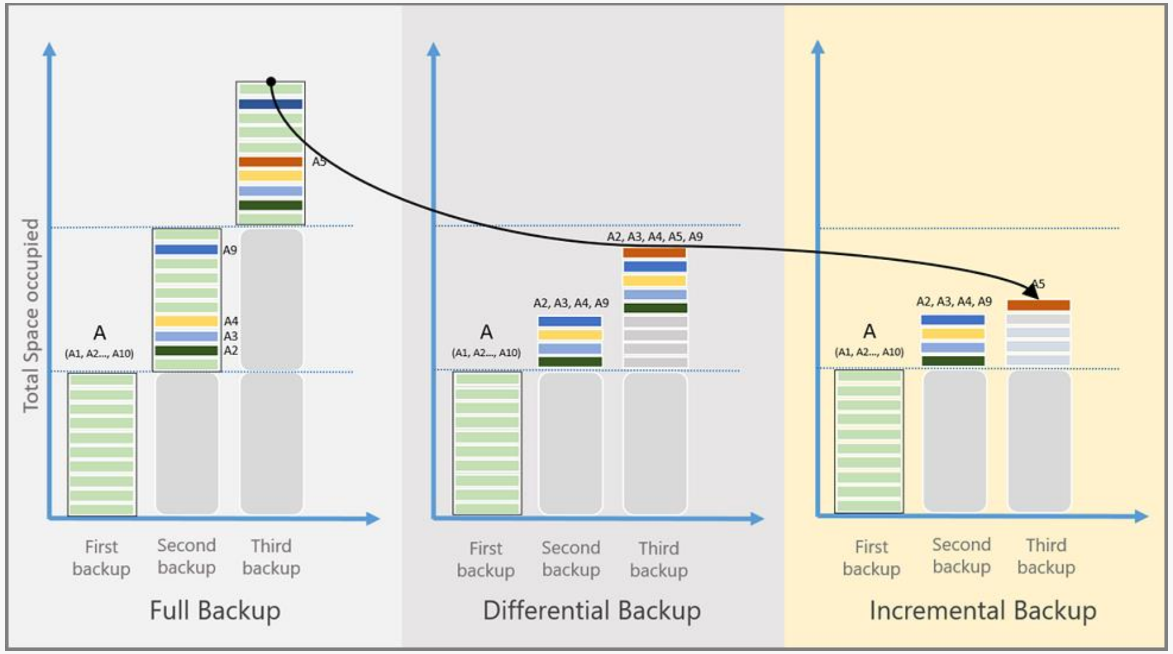
Support	Linux (Azure endorsed)
Supported operating systems	Windows Server 2019, Windows Server 2016, Windows Server 2012, Windows Server 2008 R2 SP1 Linux isn't currently supported.
Supported SQL Server versions	SQL Server 2019, SQL Server 2017, SQL Server 2016, SQL Server 2014, SQL Server 2012, SQL Server 2008 R2, SQL Server 2008 Enterprise, Standard, Web, Developer, Express. Express Local DB versions aren't supported.

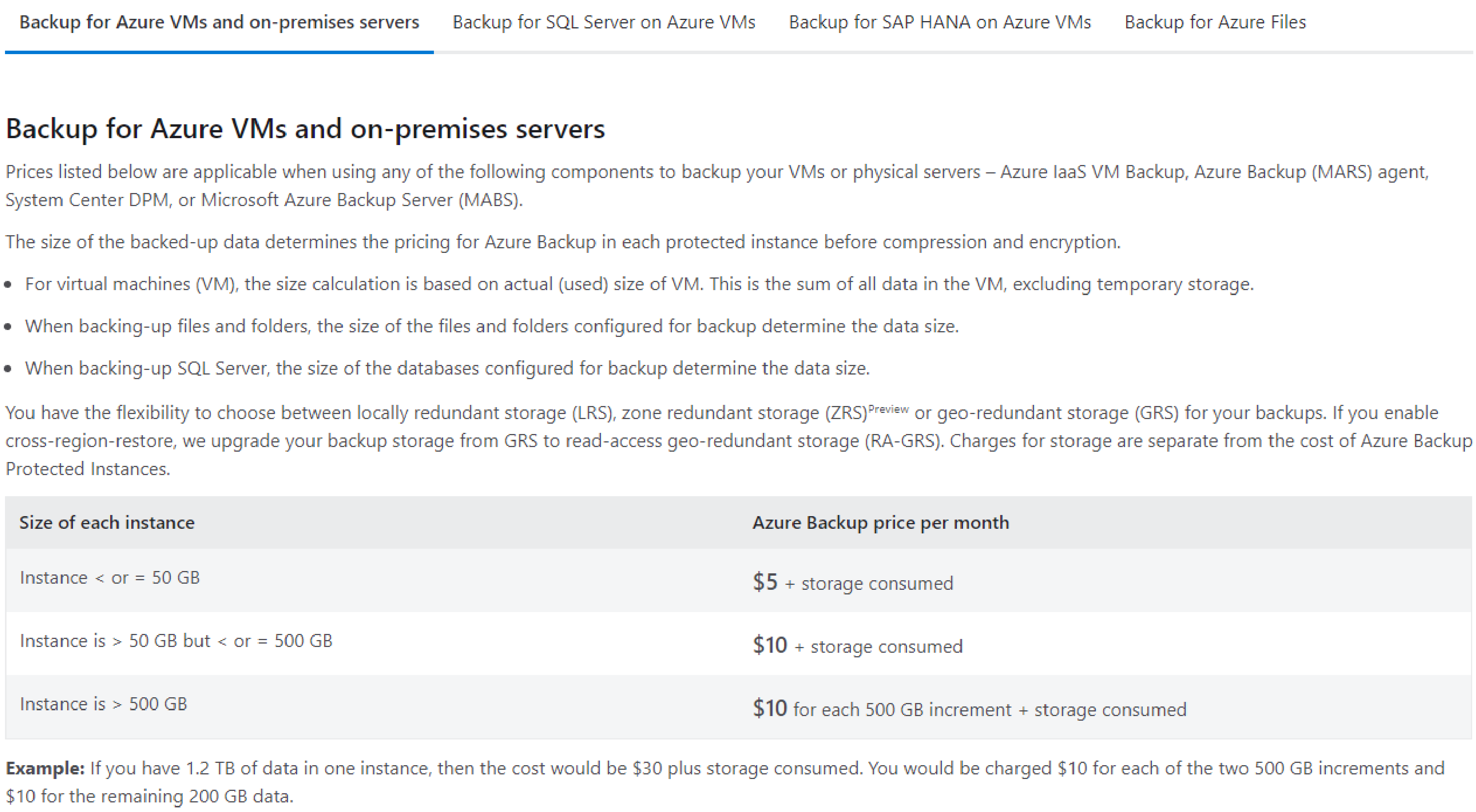
Limitation	Maximum Limit
Number of databases that can be protected	2000
Database size supported (beyond this, performance issues may come up)	6 TB*
Number of files supported in a database	1000

Azure Backup Architecture

The following table explains the different types of backups and when they're used:

Backup type	Usage
Full	Used for initial backup.
Differential	Not used by Azure Backup.
Incremental	Used by DPM/MABS for disk backups and used in all backups to Azure.




Backup for Azure VMs and on-premises servers
Backup for SQL Server on Azure VMs
Backup for SAP HANA on Azure VMs
Backup for Azure Files

Backup for Azure VMs and on-premises servers

Prices listed below are applicable when using any of the following components to backup your VMs or physical servers – Azure IaaS VM Backup, Azure Backup (MARS) agent, System Center DPM, or Microsoft Azure Backup Server (MABS).

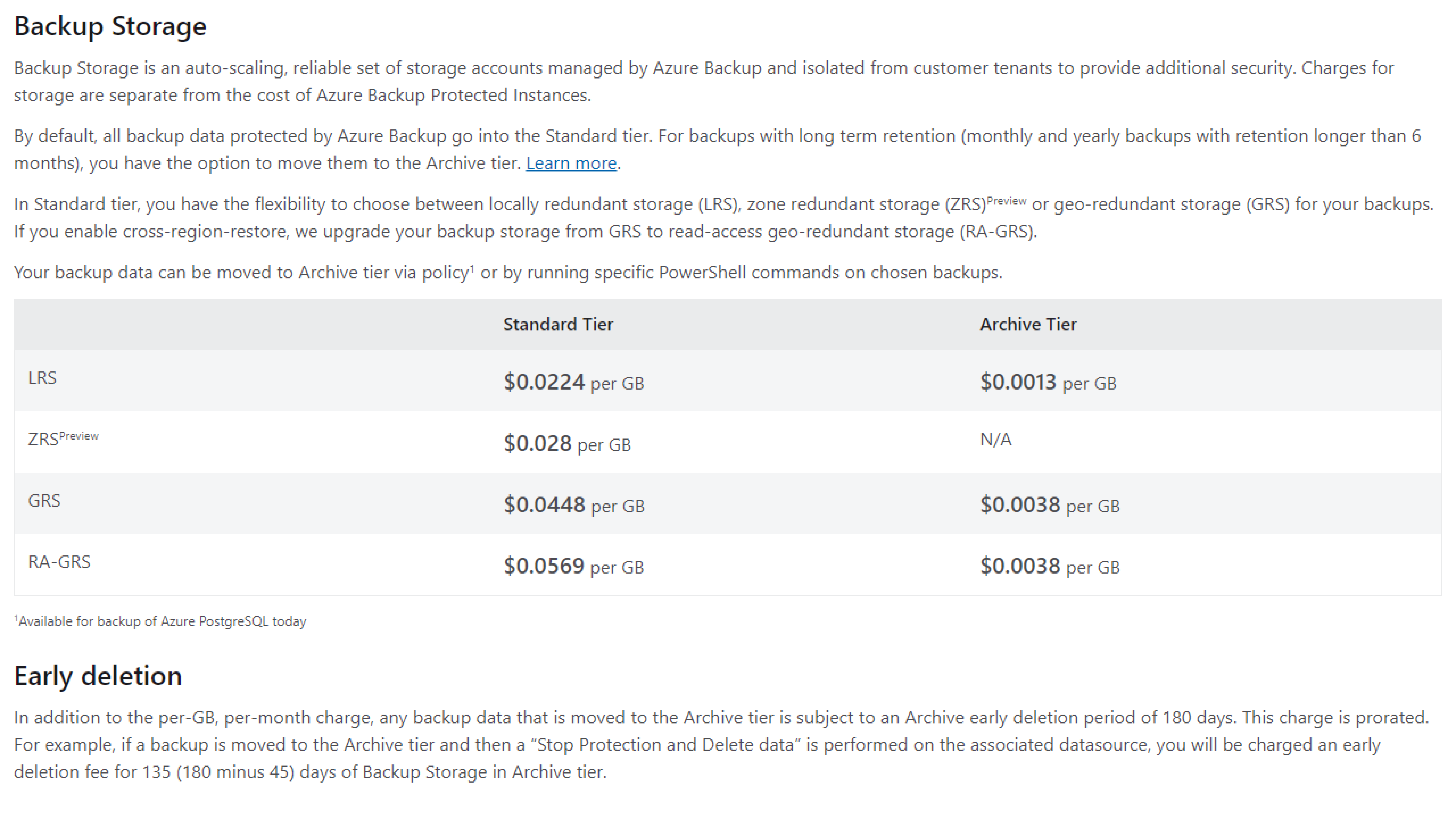
The size of the backed-up data determines the pricing for Azure Backup in each protected instance before compression and encryption.

- For virtual machines (VM), the size calculation is based on actual (used) size of VM. This is the sum of all data in the VM, excluding temporary storage.
- When backing-up files and folders, the size of the files and folders configured for backup determine the data size.
- When backing-up SQL Server, the size of the databases configured for backup determine the data size.

You have the flexibility to choose between locally redundant storage (LRS), zone redundant storage (ZRS)$^{\text{Preview}}$ or geo-redundant storage (GRS) for your backups. If you enable cross-region-restore, we upgrade your backup storage from GRS to read-access geo-redundant storage (RA-GRS). Charges for storage are separate from the cost of Azure Backup Protected Instances.

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

Example: If you have 1.2 TB of data in one instance, then the cost would be $30 plus storage consumed. You would be charged $10 for each of the two 500 GB increments and $10 for the remaining 200 GB data.



Backup Storage

Backup Storage is an auto-scaling, reliable set of storage accounts managed by Azure Backup and isolated from customer tenants to provide additional security. Charges for storage are separate from the cost of Azure Backup Protected Instances.

By default, all backup data protected by Azure Backup go into the Standard tier. For backups with long term retention (monthly and yearly backups with retention longer than 6 months), you have the option to move them to the Archive tier. Learn more.

In Standard tier, you have the flexibility to choose between locally redundant storage (LRS), zone redundant storage (ZRS)$^{\text{Preview}}$ or geo-redundant storage (GRS) for your backups. If you enable cross-region-restore, we upgrade your backup storage from GRS to read-access geo-redundant storage (RA-GRS).

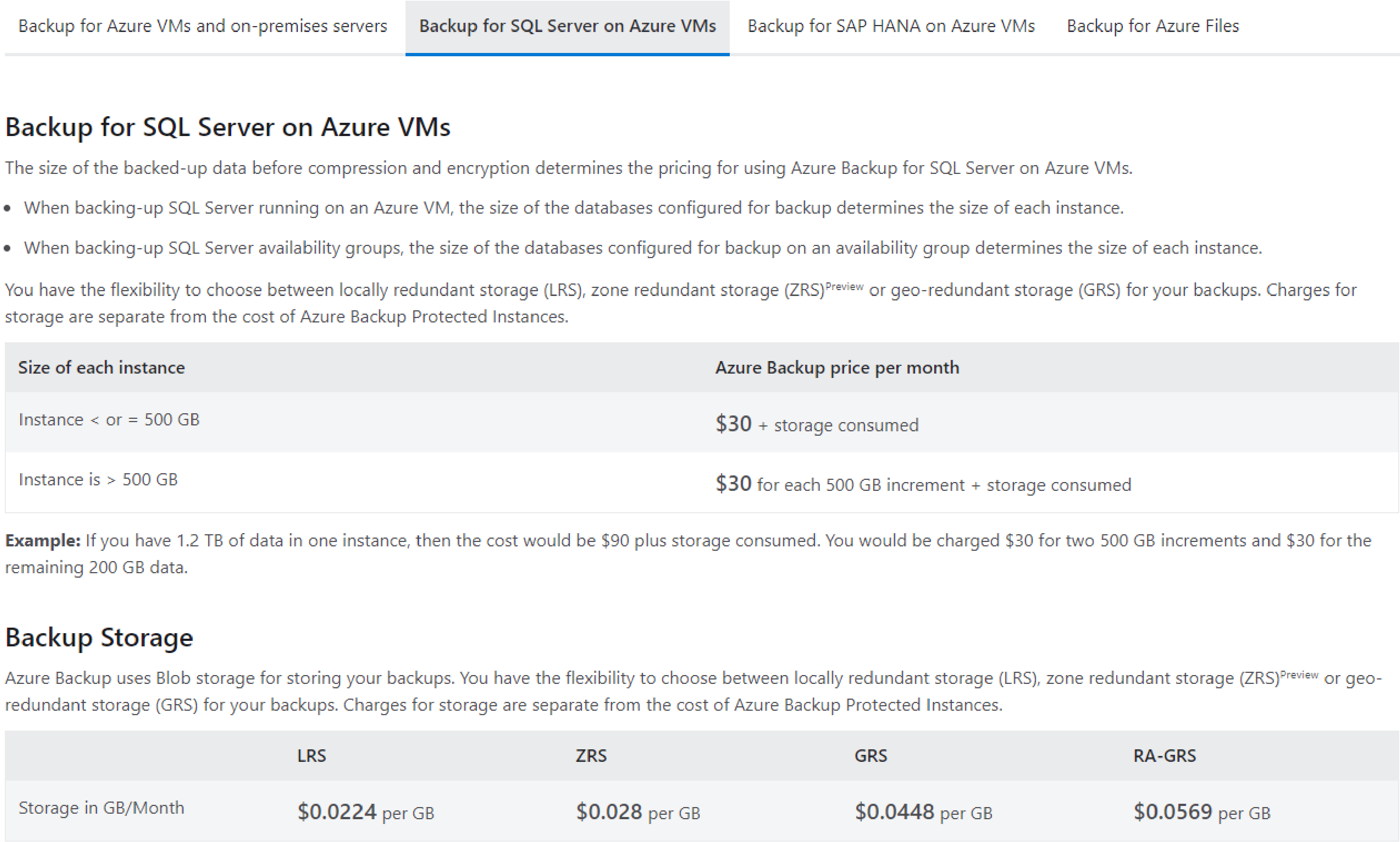
Your backup data can be moved to Archive tier via policy[1] or by running specific PowerShell commands on chosen backups.

	Standard Tier	Archive Tier
LRS	**$0.0224** per GB	**$0.0013** per GB
ZRS$^{\text{Preview}}$	**$0.028** per GB	N/A
GRS	**$0.0448** per GB	**$0.0038** per GB
RA-GRS	**$0.0569** per GB	**$0.0038** per GB

[1] Available for backup of Azure PostgreSQL today

Early deletion

In addition to the per-GB, per-month charge, any backup data that is moved to the Archive tier is subject to an Archive early deletion period of 180 days. This charge is prorated. For example, if a backup is moved to the Archive tier and then a “Stop Protection and Delete data” is performed on the associated datasource, you will be charged an early deletion fee for 135 (180 minus 45) days of Backup Storage in Archive tier.


Backup for Azure VMs and on-premises servers
Backup for SQL Server on Azure VMs
Backup for SAP HANA on Azure VMs
Backup for Azure Files

Backup for SQL Server on Azure VMs

The size of the backed-up data before compression and encryption determines the pricing for using Azure Backup for SQL Server on Azure VMs.

- When backing-up SQL Server running on an Azure VM, the size of the databases configured for backup determines the size of each instance.
- When backing-up SQL Server availability groups, the size of the databases configured for backup on an availability group determines the size of each instance.

You have the flexibility to choose between locally redundant storage (LRS), zone redundant storage (ZRS)Preview or geo-redundant storage (GRS) for your backups. Charges for storage are separate from the cost of Azure Backup Protected Instances.

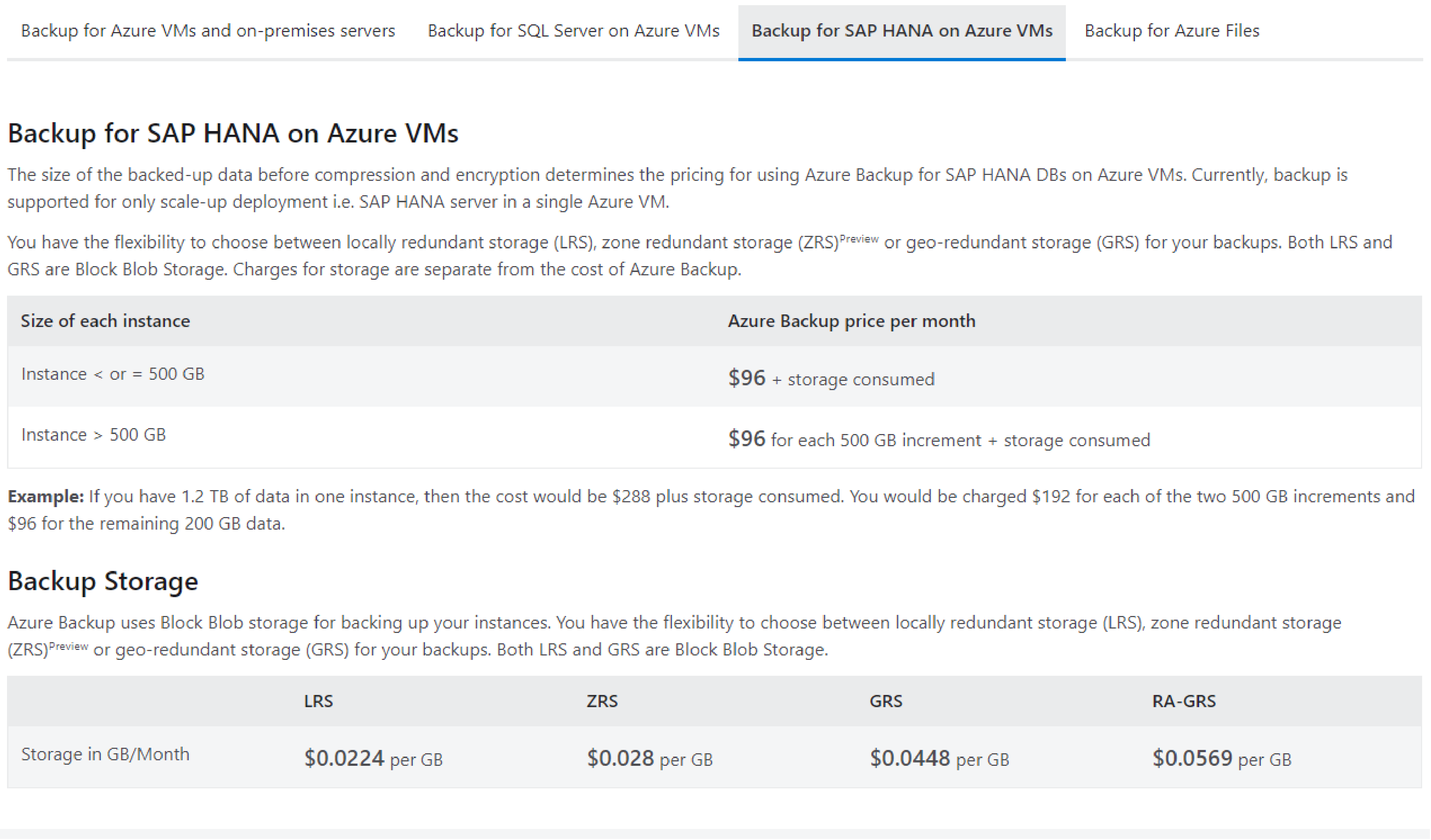
Size of each instance	Azure Backup price per month
Instance < or = 500 GB	$30 + storage consumed
Instance is > 500 GB	$30 for each 500 GB increment + storage consumed

Example: If you have 1.2 TB of data in one instance, then the cost would be $90 plus storage consumed. You would be charged $30 for two 500 GB increments and $30 for the remaining 200 GB data.

Backup Storage

Azure Backup uses Blob storage for storing your backups. You have the flexibility to choose between locally redundant storage (LRS), zone redundant storage (ZRS)Preview or geo-redundant storage (GRS) for your backups. Charges for storage are separate from the cost of Azure Backup Protected Instances.

	LRS	ZRS	GRS	RA-GRS
Storage in GB/Month	$0.0224 per GB	$0.028 per GB	$0.0448 per GB	$0.0569 per GB


Backup for Azure VMs and on-premises servers
Backup for SQL Server on Azure VMs
Backup for SAP HANA on Azure VMs
Backup for Azure Files

Backup for SAP HANA on Azure VMs

The size of the backed-up data before compression and encryption determines the pricing for using Azure Backup for SAP HANA DBs on Azure VMs. Currently, backup is supported for only scale-up deployment i.e. SAP HANA server in a single Azure VM.

You have the flexibility to choose between locally redundant storage (LRS), zone redundant storage (ZRS)[Preview] or geo-redundant storage (GRS) for your backups. Both LRS and GRS are Block Blob Storage. Charges for storage are separate from the cost of Azure Backup.

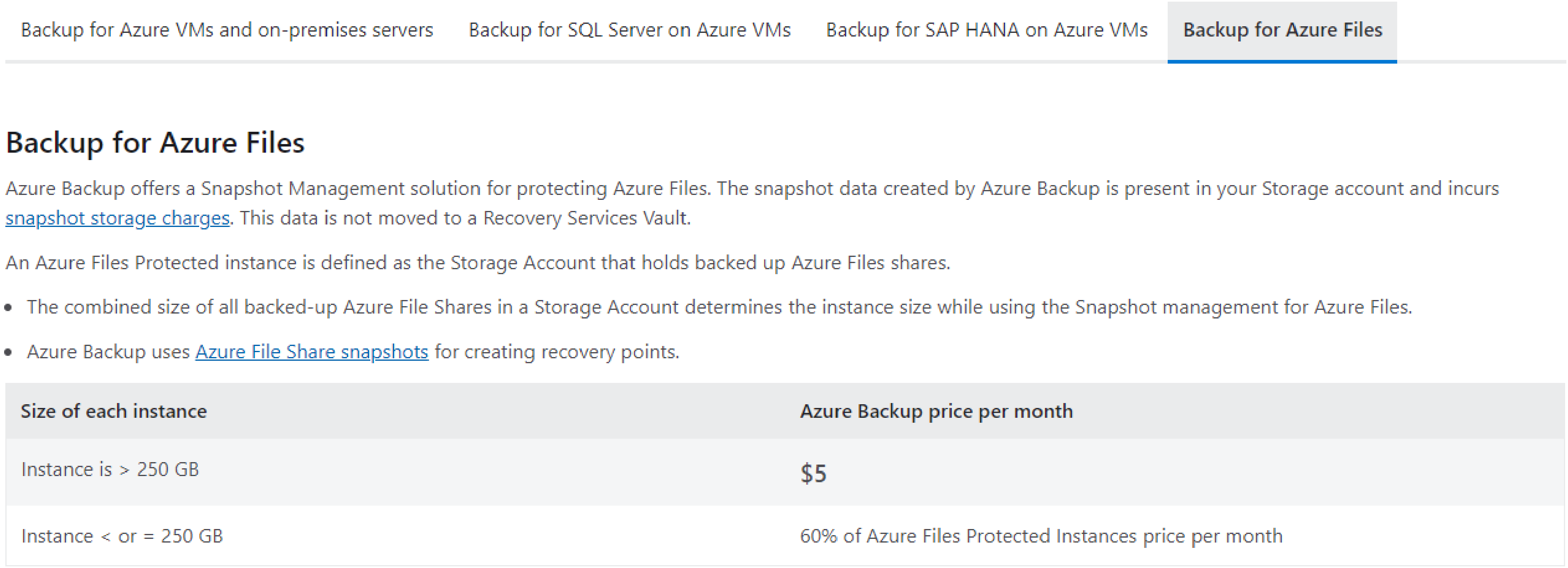
Size of each instance	Azure Backup price per month
Instance < or = 500 GB	$96 + storage consumed
Instance > 500 GB	$96 for each 500 GB increment + storage consumed

Example: If you have 1.2 TB of data in one instance, then the cost would be $288 plus storage consumed. You would be charged $192 for each of the two 500 GB increments and $96 for the remaining 200 GB data.

Backup Storage

Azure Backup uses Block Blob storage for backing up your instances. You have the flexibility to choose between locally redundant storage (LRS), zone redundant storage (ZRS)[Preview] or geo-redundant storage (GRS) for your backups. Both LRS and GRS are Block Blob Storage.

	LRS	ZRS	GRS	RA-GRS
Storage in GB/Month	$0.0224 per GB	$0.028 per GB	$0.0448 per GB	$0.0569 per GB


Backup for Azure VMs and on-premises servers
Backup for SQL Server on Azure VMs
Backup for SAP HANA on Azure VMs
Backup for Azure Files

Backup for Azure Files

Azure Backup offers a Snapshot Management solution for protecting Azure Files. The snapshot data created by Azure Backup is present in your Storage account and incurs snapshot storage charges. This data is not moved to a Recovery Services Vault.

An Azure Files Protected instance is defined as the Storage Account that holds backed up Azure Files shares.

- The combined size of all backed-up Azure File Shares in a Storage Account determines the instance size while using the Snapshot management for Azure Files.
- Azure Backup uses Azure File Share snapshots for creating recovery points.

Size of each instance	Azure Backup price per month
Instance is > 250 GB	$5
Instance < or = 250 GB	60% of Azure Files Protected Instances price per month

We Look Forward to Partnering With You…

A Cloud 9, Mohamed Naguib Axis,
North Investors Area, New Cairo, Egypt.

P +2 02 25 390 467

E info@inovasys.co