



**INOVASYS**

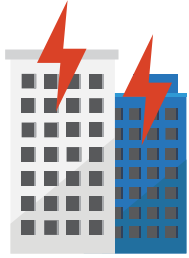
Think**BIG**

# Microsoft Business Continuity Solutions



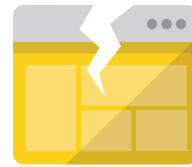
# Customer challenges

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



\$1.25B to \$2.5B

Average annual cost of downtime for F1000<sup>1</sup>



\$500K to \$1M

Average hourly cost of a critical application failure<sup>1</sup>



\$100K

Average hourly cost of an infrastructure failure<sup>1</sup>

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."

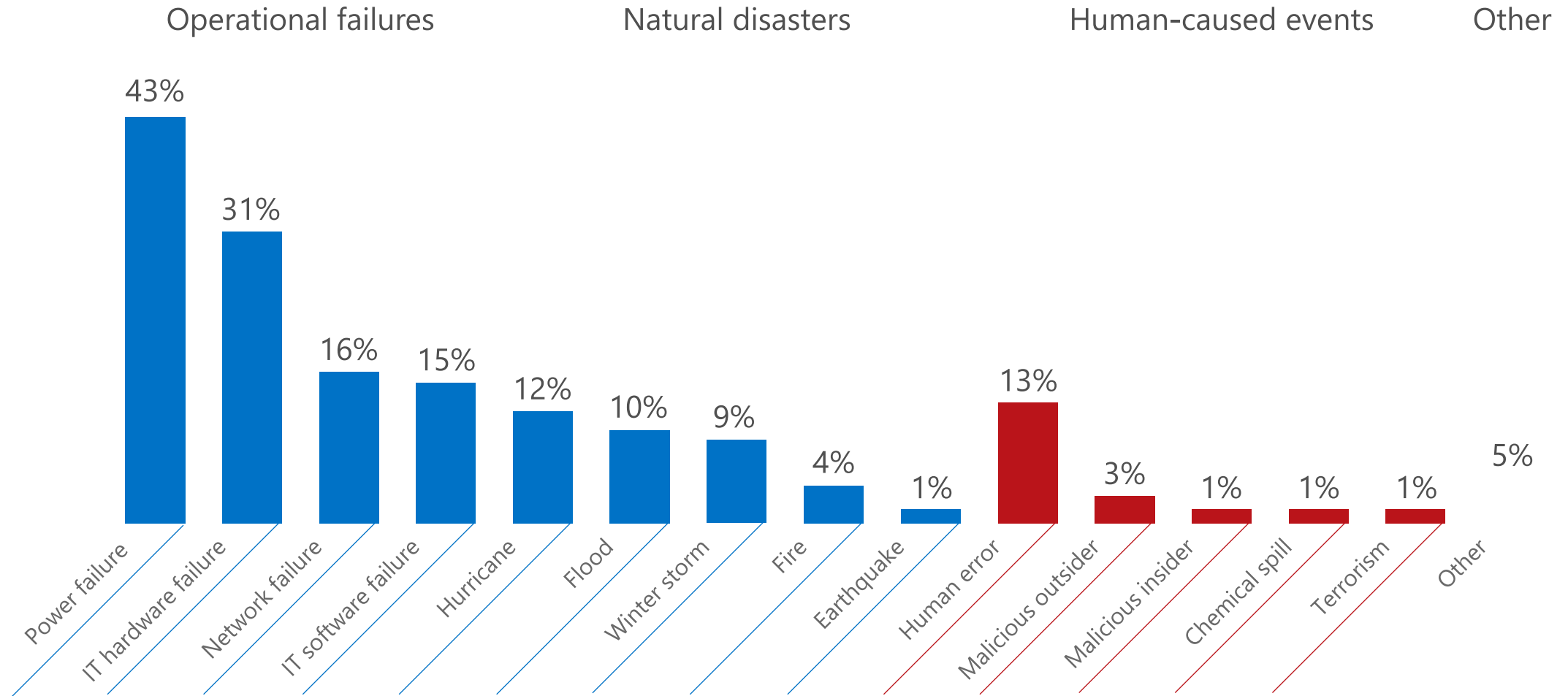
"My infrastructure is extremely complex and features a mix of Linux, VMware, and Windows software."

"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."

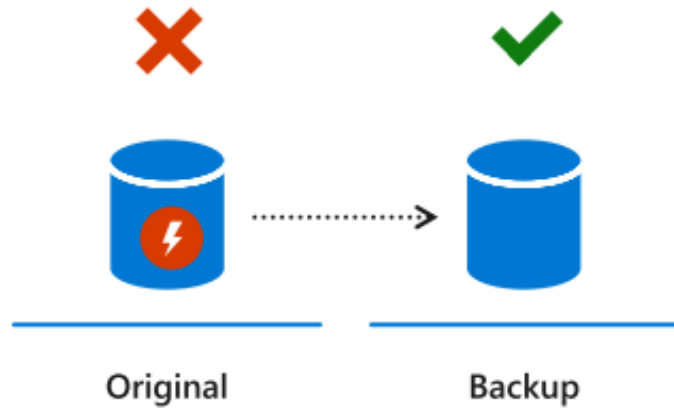
# Causes of IT “disasters”

Most are caused by operational failures – not natural disasters



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

# Delivering resilient applications in Azure



## Backup

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

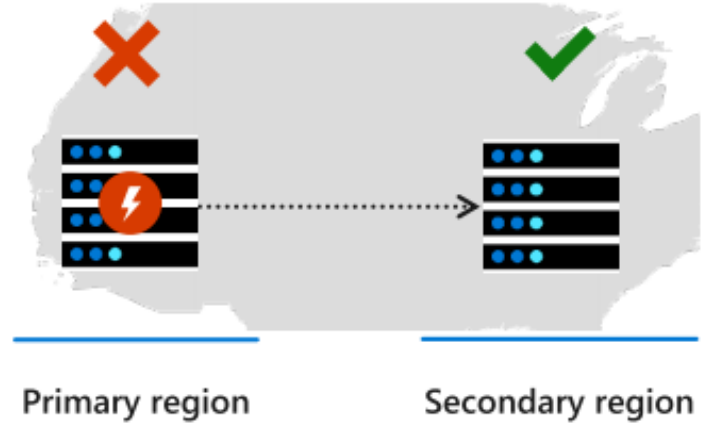
Azure Backup



## 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

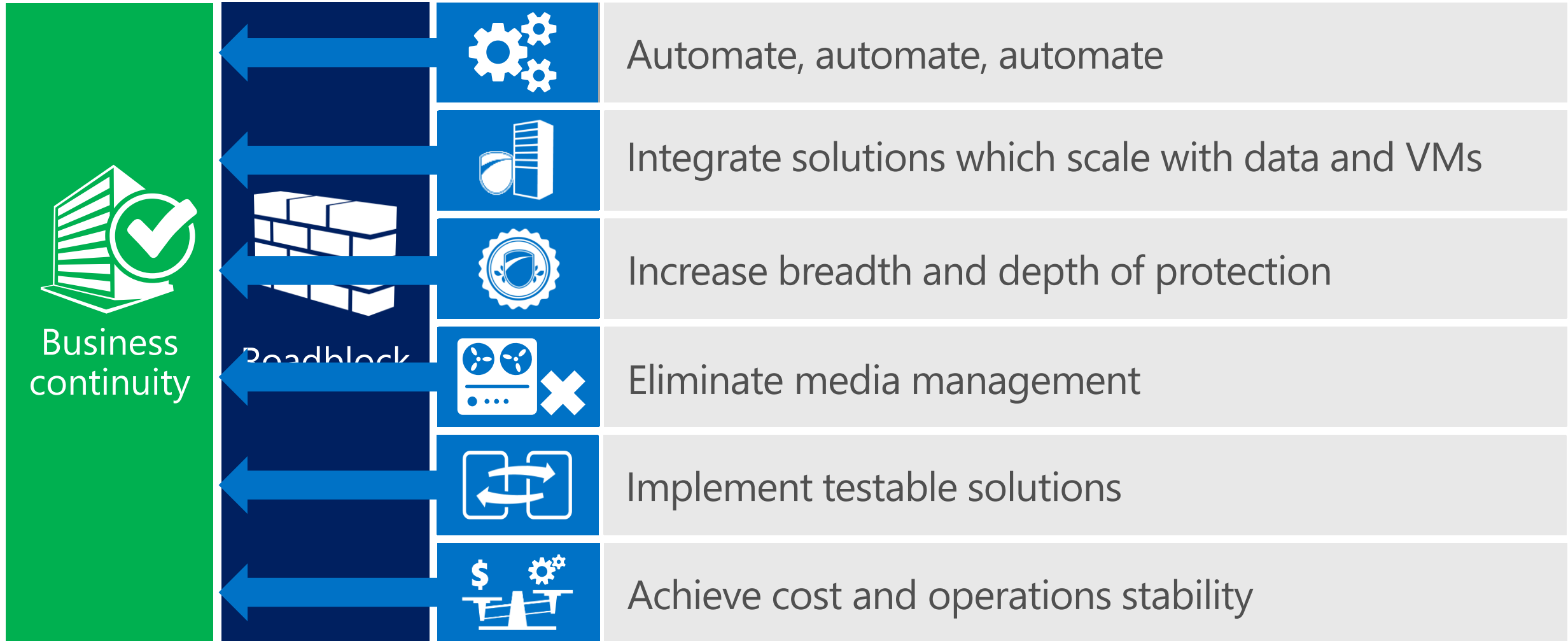
When your primary site has failures, run your applications in secondary site

Azure Site Recovery

# Business continuity challenges

 <p>Business continuity</p>	 <p>Roadblock</p>		Protecting data and applications is complex
			Too much data—often with insufficient protection
			Long data retention requirements
			Time-intensive media management
			Untested plans decreasing recovery confidence
			Costs scale with data size and number of VMs

# Business continuity challenges



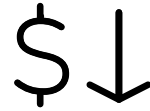
# Common enterprise challenges

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

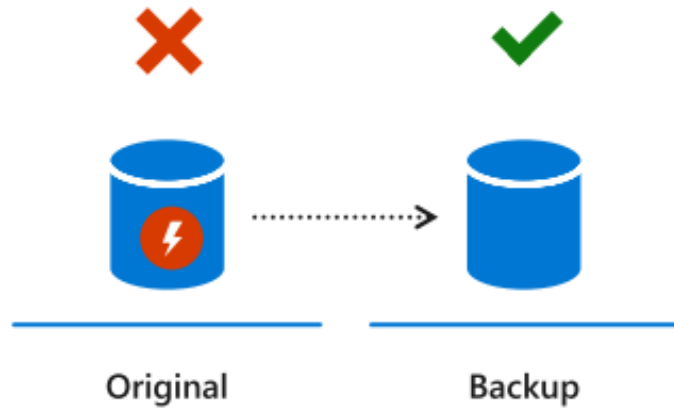


## Scaling protection

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



# Delivering resilient applications in Azure



## Backup

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

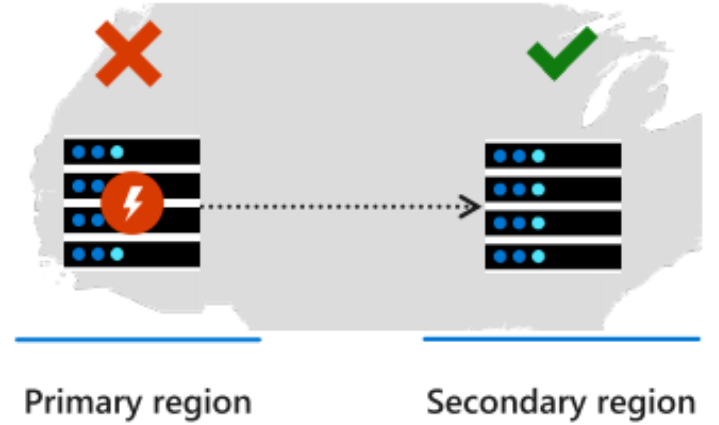
Azure Backup



## High availability

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

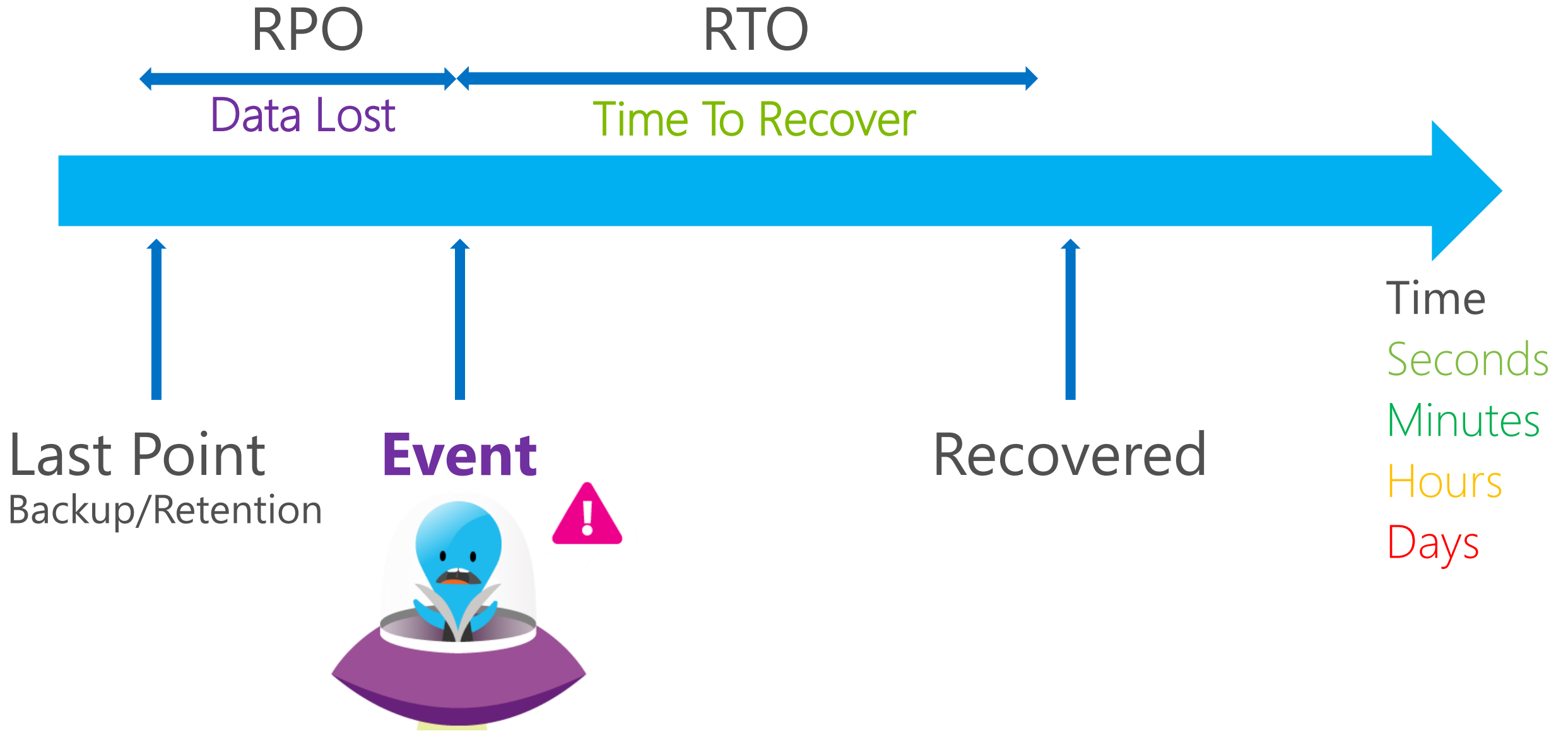
Availability Sets, Zones and Region Pairs



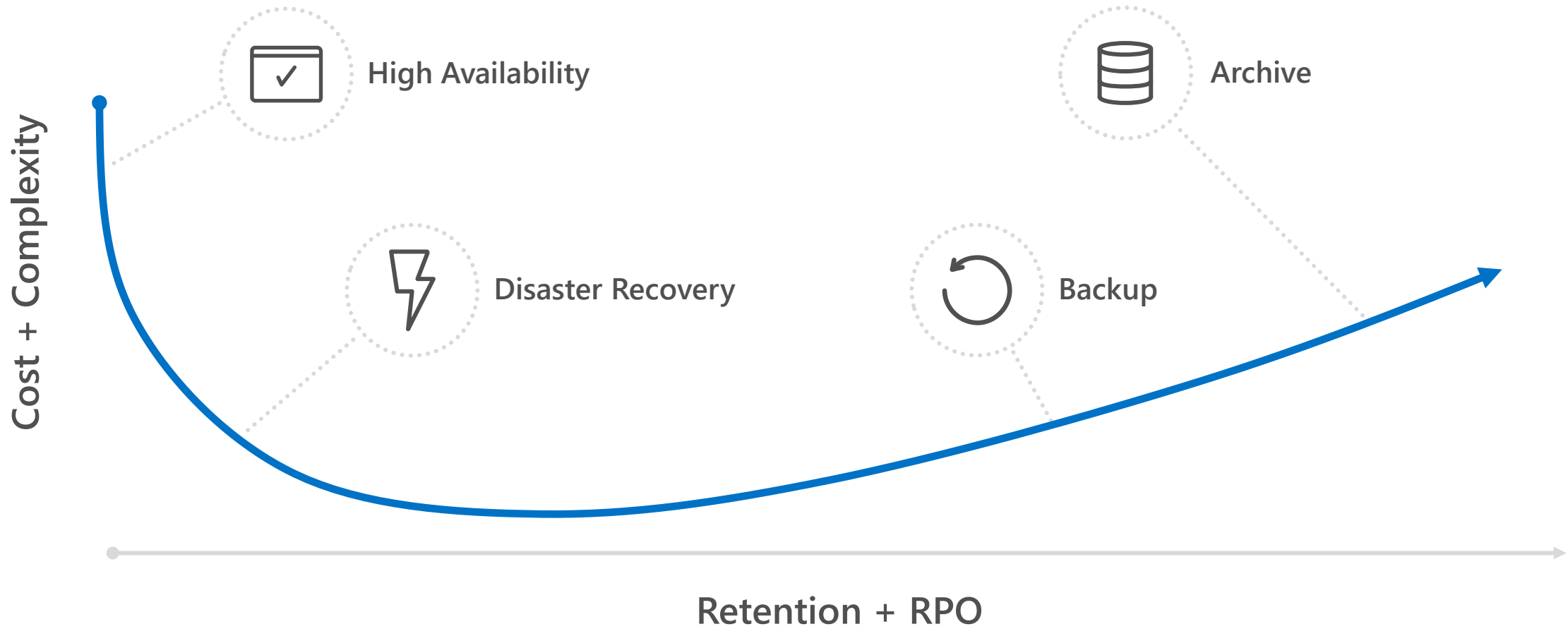
## Disaster recovery

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

Azure Site Recovery



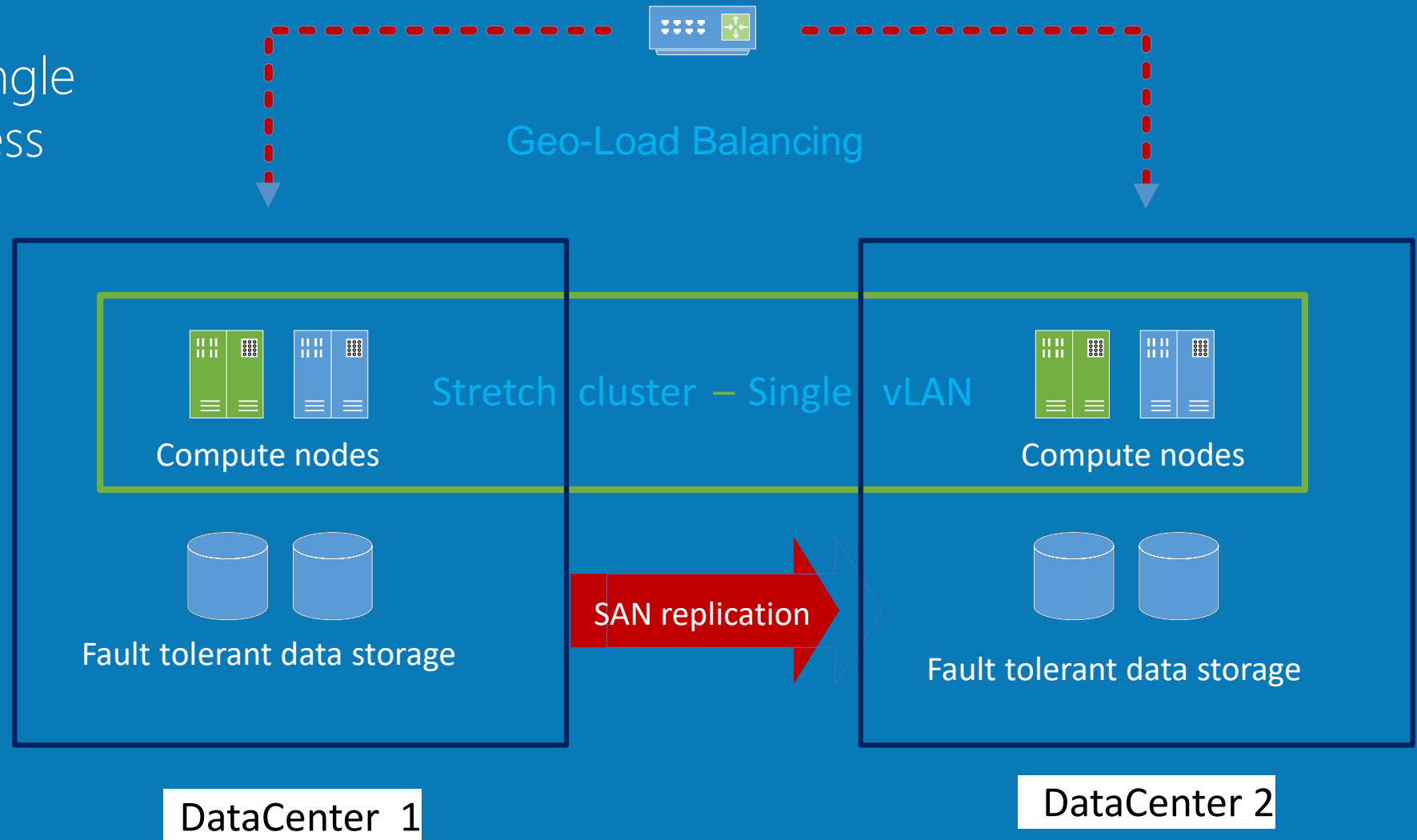
# Traditional enterprise protection



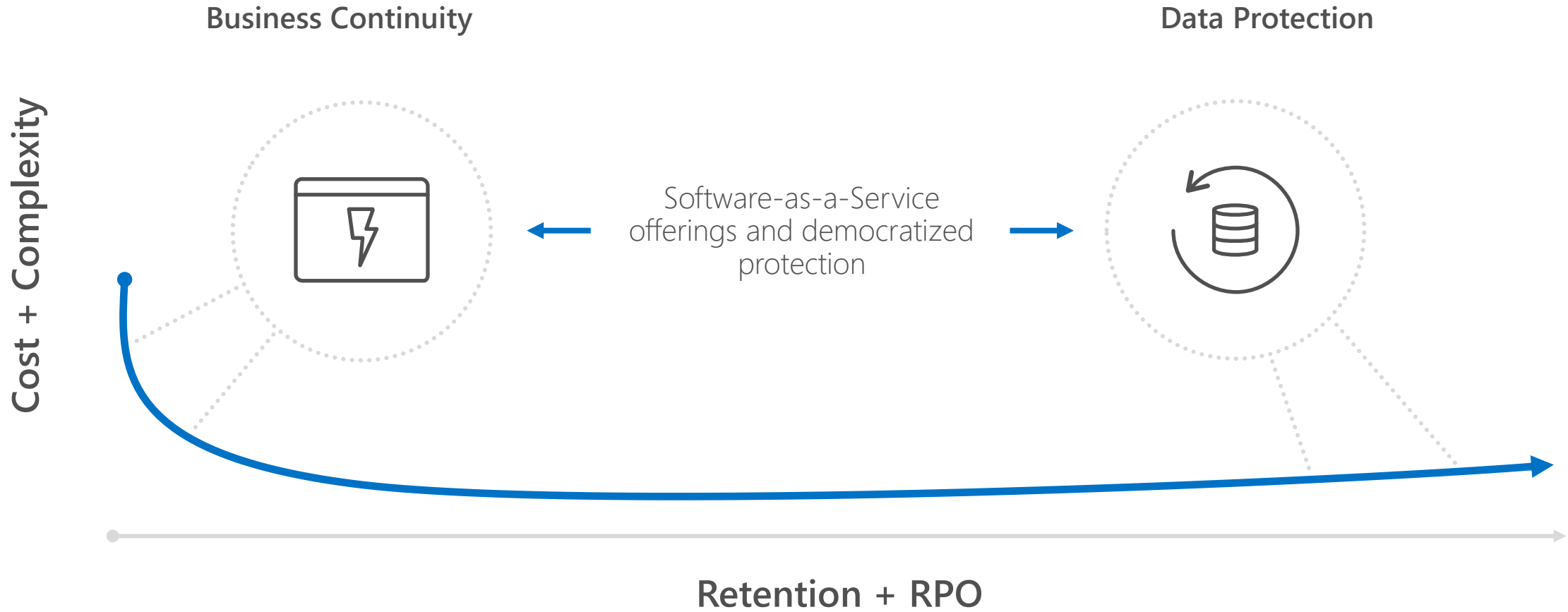
# "Familiar" DR Solutions

- Storage replication
- Stretch cluster using single vLAN with single address space
- Active / passive
- Dynamic incoming connection failover

- Effective, although expensive to deploy and maintain
- Normally tied to hardware vendor specific technologies
- Difficult to perform partial failovers



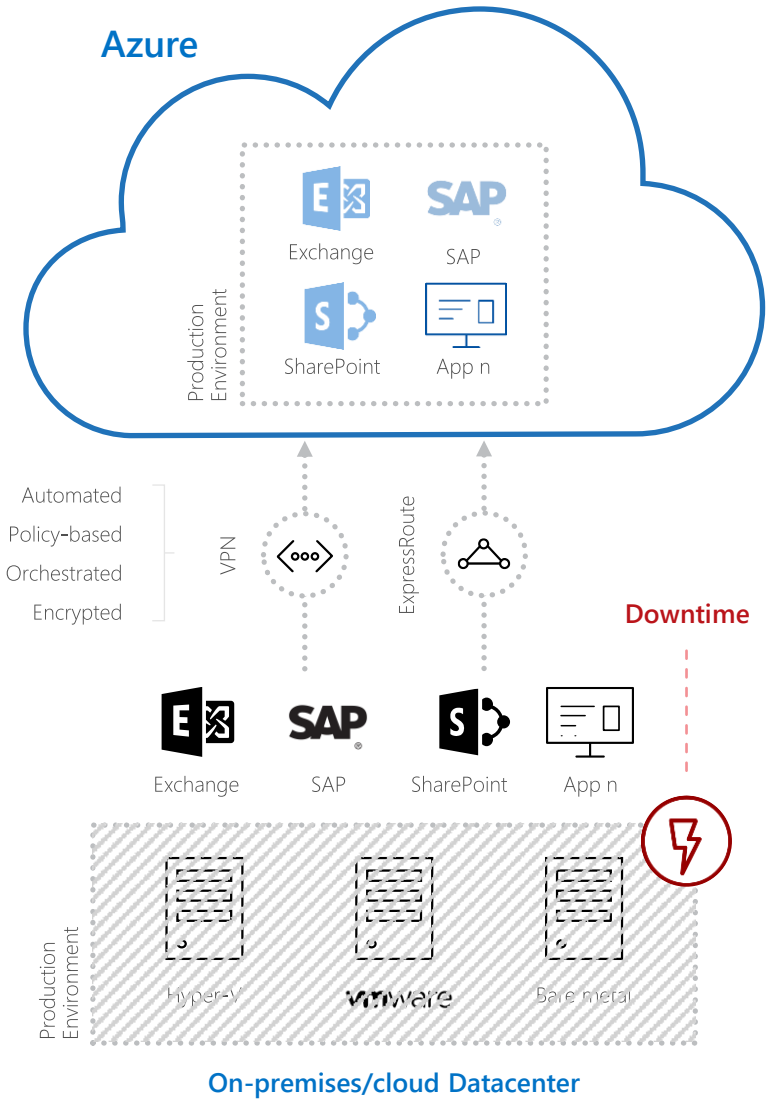
# Introducing Azure-based protection



# Cloud-first disaster recovery

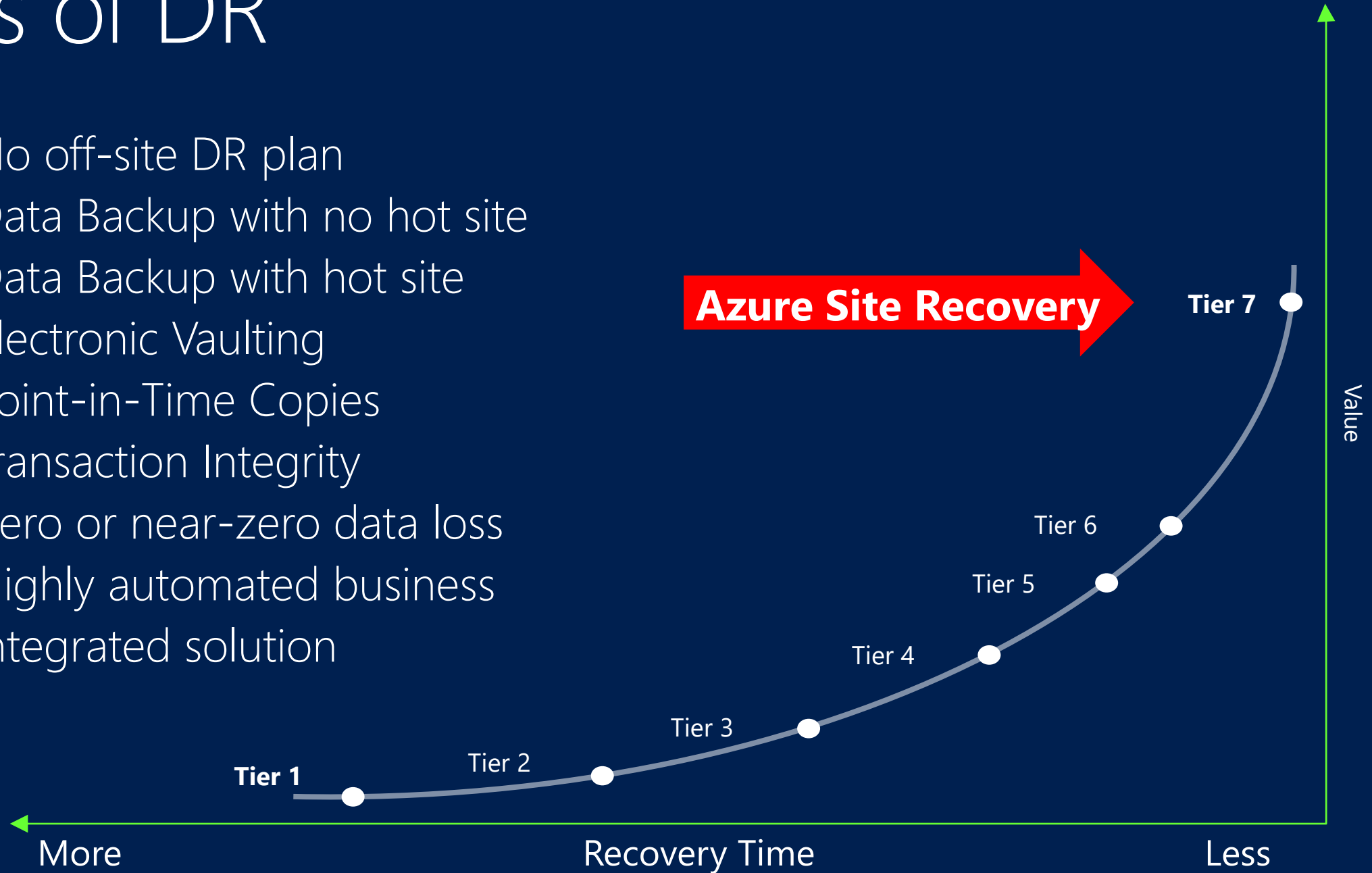
## Democratizing disaster recovery

- No infrastructure required—affordable, enterprise-grade protection for all apps
- No need to sacrifice RPO and RTO goals
- Supports critical workloads—Exchange, SharePoint, SAP, etc.
- Works with what you have—Hyper-V, VMware, or bare metal
- Easy to manage—automated replication, policy-based protection, and one-click orchestrated recovery
- Premium protection against operational and human errors with intra-cloud disaster recovery and backup



# 7 Tiers of DR

- Tier 0 No off-site DR plan
- Tier 1 Data Backup with no hot site
- Tier 2 Data Backup with hot site
- Tier 3 Electronic Vaulting
- Tier 4 Point-in-Time Copies
- Tier 5 Transaction Integrity
- Tier 6 Zero or near-zero data loss
- Tier 7 Highly automated business integrated solution



# Azure Site Recovery

One solution for your entire Infrastructure



Business  
Continuity



**DR Support for any Infrastructure on your on-premises (Hyper-V, VMWare, Physical)**



**Zero RPO/Near sync RPO solutions with Azure Site Recovery**



**Support for Enterprise Class Applications**



**Support for Enterprise scenarios: Shared Storage, raw devices, clustering, group consistency**



**Low TCO DR to Public Cloud or Service Provider Cloud**

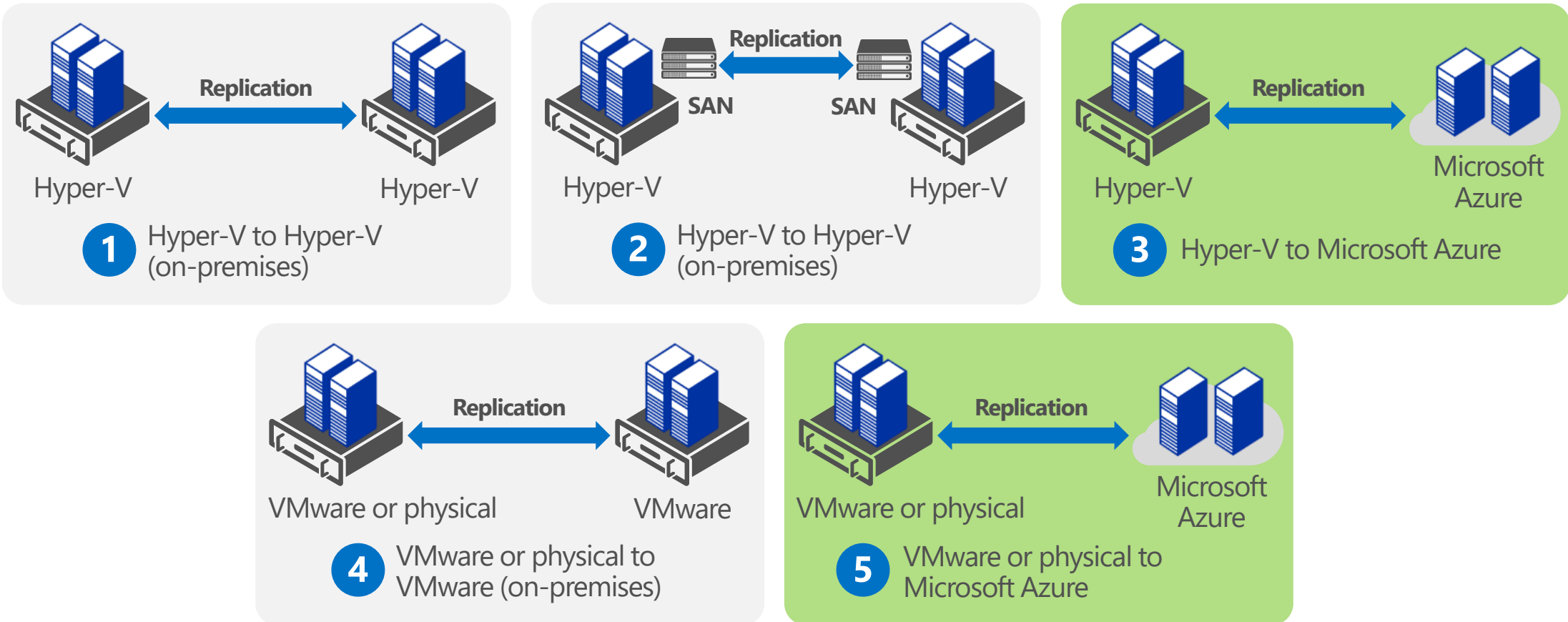


**Simple, consistent, unified management experience**



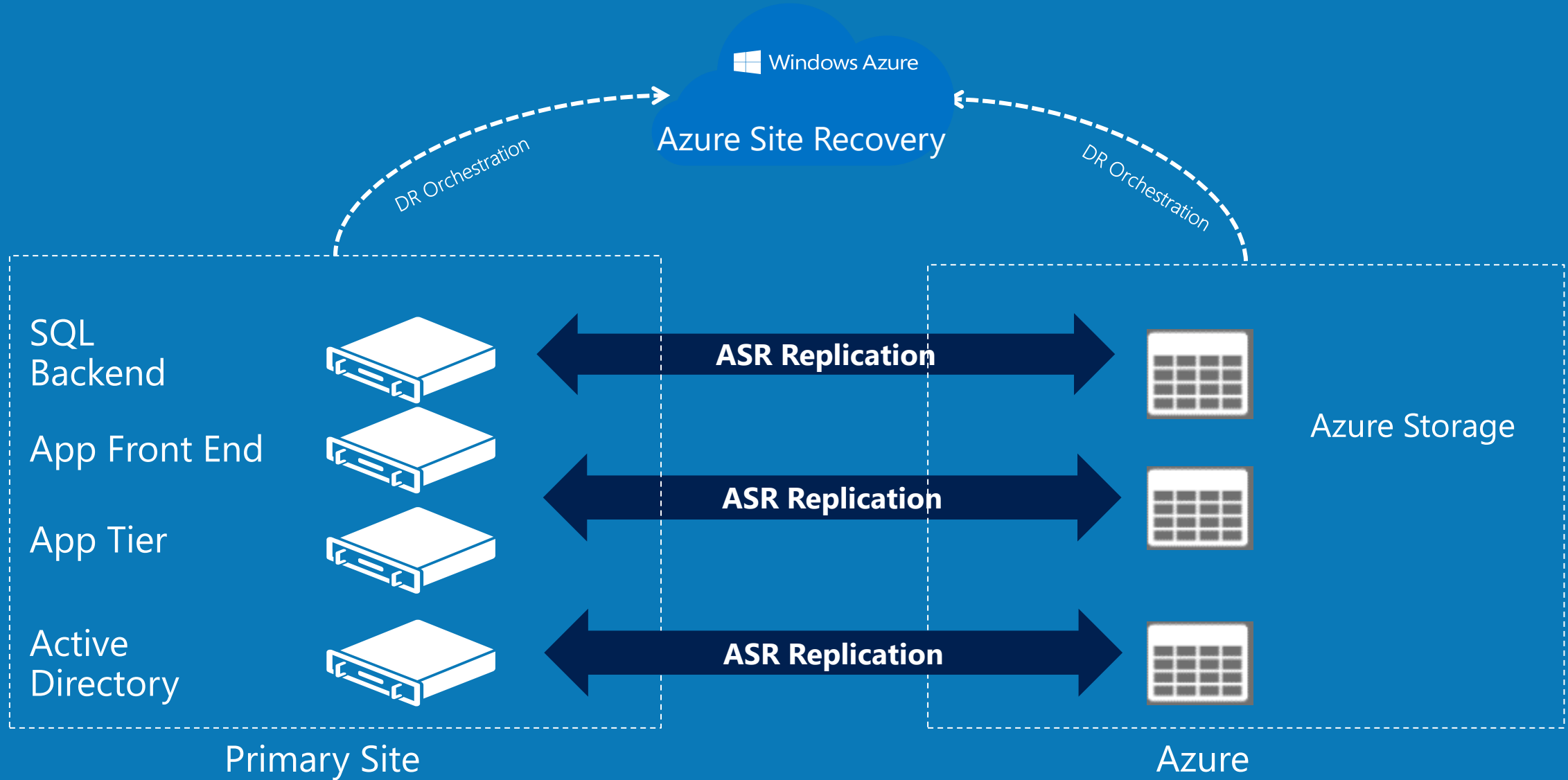
# Microsoft Azure Site Recovery

One solution for multiple infrastructures



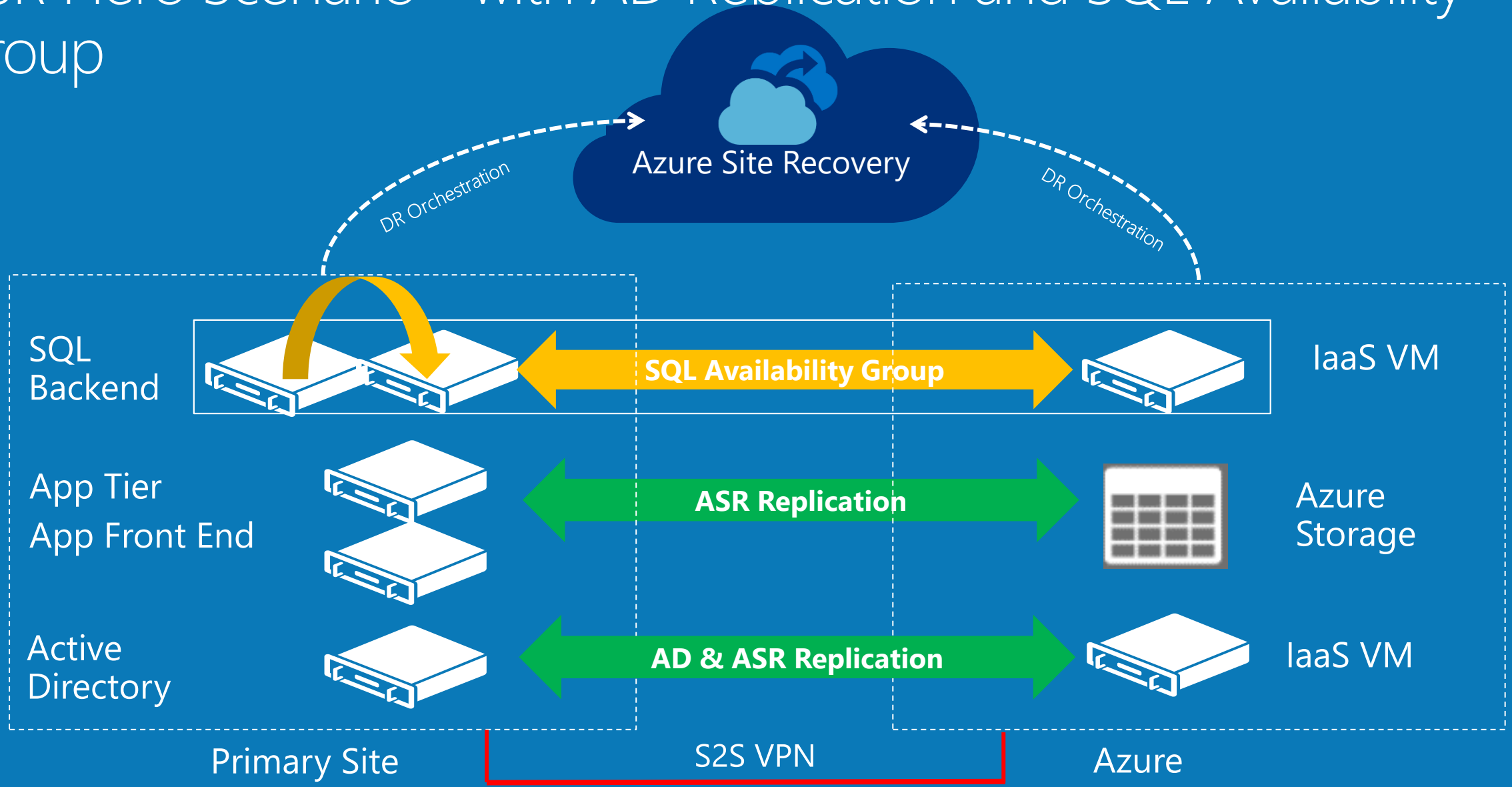
Protect important applications by coordinating the replication and recovery of private clouds across sites. Protect your applications to your own second site, a hoster's site, or even use Microsoft Azure as your disaster recovery site.

# ASR Hero Scenario – Typical 3 Tier Web App



Above shows DR to Azure however same Hero scenario is applicable for On Premise to On Premise DR.

# ASR Hero Scenario - with AD Replication and SQL Availability Group





# Supported applications

Workload		Hyper-V		VMware	
		Site-to-site	Site-to-Azure	Site-to-site	Site-to-Azure
AD, DNS Infrastructure		▲	▲	▲	▲
Web Apps	IIS	▲	▲	▲	▲
	SQL	▲	▲	▲	▲
SCOM		▲	▲	▲	▲
SharePoint		▲	▲	▲	▲
SAP*		■	■	■	■
Exchange**		▲	▲	▲	▲
Remote Desktop/VDI		▲	▲	▲	▲ (Excluding Horizon)
Linux (OS & Apps)		■	■	■	■
Dynamics AX	AX	▲	▲	▲	▲
	CRM	▲	COMING SOON	▲	COMING SOON
Oracle***		■	■	■	■
Windows File Server		▲	▲	▲	▲

▲ Supported and certified by workload team

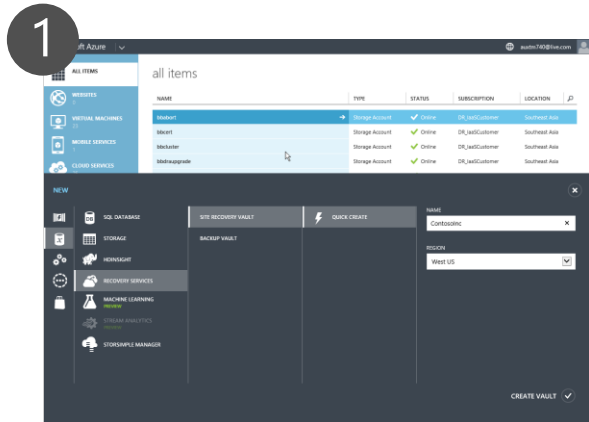
■ Supported – Tested by Microsoft

\*SAP site-to-Azure for un-clustered setups

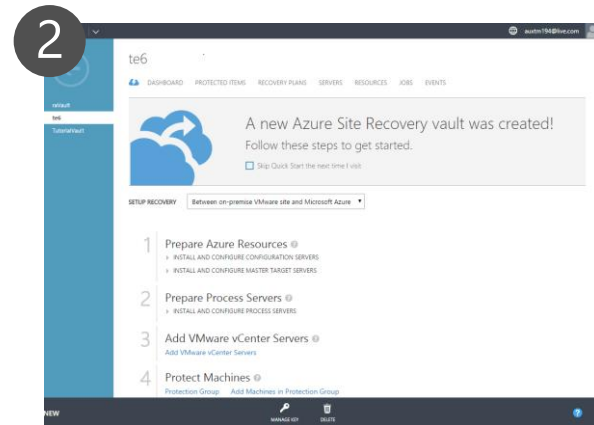
\*\*Exchange 2013 non-DAG setups

\*\*\*Oracle Stand-alone – Oracle Data Guard based solution coming soon

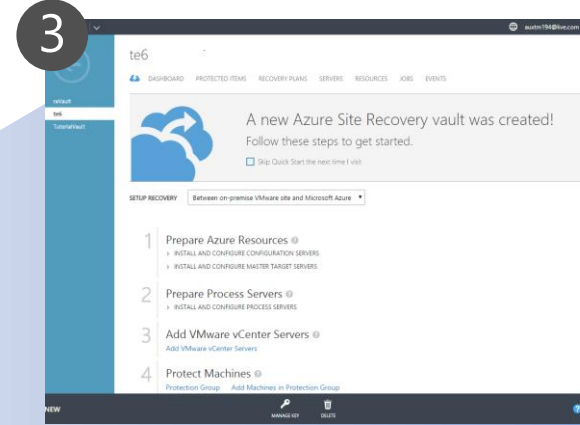
# Protection Steps



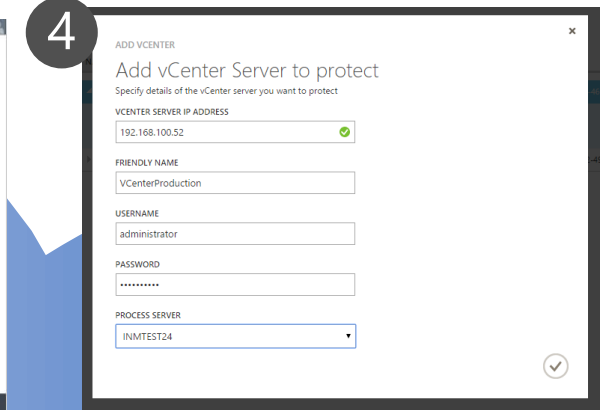
## CREATE VAULT



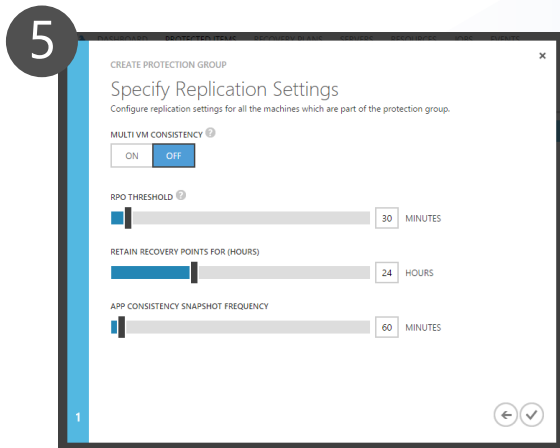
## QUICK START



## SETUP SERVERS

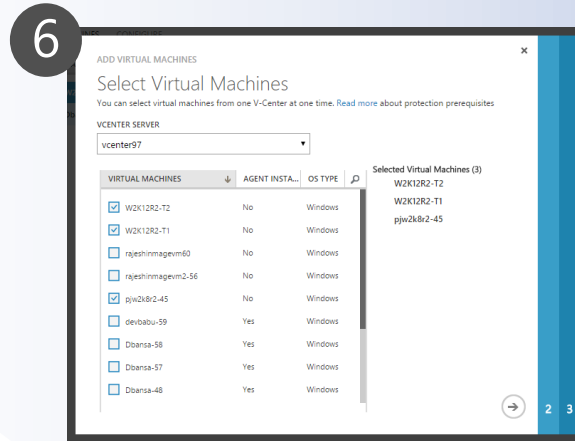


## REGISTER



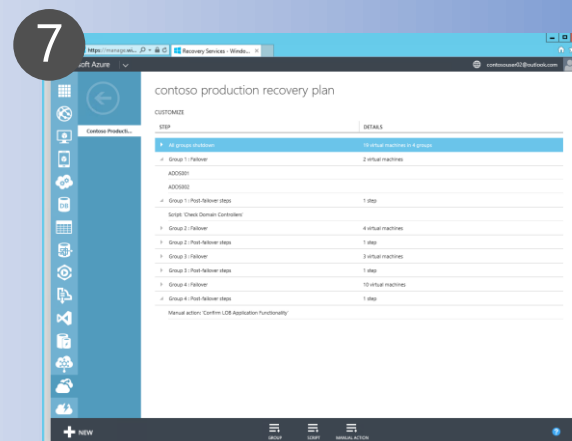
## CONFIGURE PROTECTION

Define protection policy



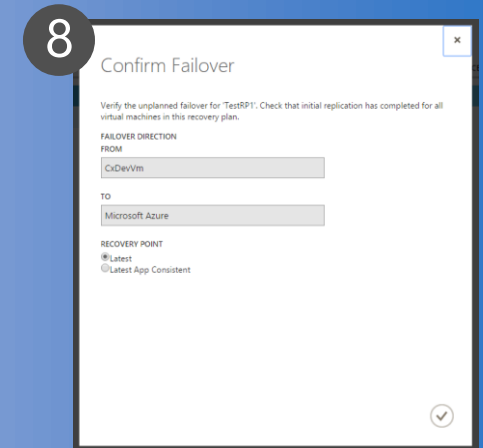
## PROTECT VIRTUAL MACHINES

Replicate disks to Azure



## CREATE RECOVERY PLAN

Define DR Plan



## FAILOVER

Perform failover

# Microsoft Azure Site Recovery

## Executing recovery plans

**Test failover:** Useful to verify that your recovery plan and virtual machine failover strategy are working as expected.

Simulates your failover and recovery mechanism into an isolated network(s), that you define, or that can be created automatically.

**Unplanned failover:** Run an unplanned failover when a primary site experiences an unexpected incident, such as a power outage.

**Planned failover:** Perform a complete failover and recovery in your recovery plans in a proactive, planned manner. Non-replicated changes are applied to the replica virtual machine loss before bringing the VM online ensuring zero data loss

**Flexible Failback:** Flexible options for failback into on-premises environment.

Confirm Planned Failover of  
SharepointAppServer

FAILOVER DIRECTION  
FROM  
Microsoft Azure

TO  
VMME2A.fareast.corp.microsoft.com (Protected Cloud)

DATA SYNCHRONIZATION  
Failover in this direction requires a large data synchronization. Specify how synchronization occurs:

- Synchronize data before failover (minimize downtime)  
Synchronization will be performed without shutting down the virtual machine. After synchronization is complete, clicking 'Complete Failover' performs an additional synchronization that shuts down the virtual machine.
- Synchronize data during failover only (minimize synchronization)  
With this setting enabled, the virtual machine will begin shutdown immediately. Synchronization will start after shutdown to complete the failover.

# Limitations and Recommendations

# Azure Site Recovery Support Matrix

- Supported MS Operating Systems

- Windows Server 2019
- Windows Server 2016 64-bit
- Windows Server 2012 R2 / Windows Server 2012
- Windows Server 2008 with SP2 or later (64-bit/32-bit)
- Windows 7 (x64) with SP1, Windows 8 / 8.1, Windows 10

- Linux Distributions

- SUSE Linux Enterprise Server **11** till 15SP1
- Red Hat Enterprise Linux **6.7** till **8.2**
- Oracle Enterprise Linux **6.4** till **8.1**
- Ubuntu **14.04**, **16.04** and **18.04**
- CentOS **6.5** till **8.2**

**Only 64-bit Linux systems is supported. 32-bit system isn't supported.**



# Azure Site Recovery Support Matrix

- **Storage**

- Standard and Premium Storage
- Encryption at rest (SSE is the default setting on storage accounts)
- OS disk maximum size **2048 GB**
- Data disk maximum size **4095 GB**
- Data disk minimum size **2 GB**
- Data disk maximum number Up to **16**
- Redundancy LRS and GRS are supported. ZRS isn't supported.
- Hot add Supported for VMWare (Only one disk can be hot added at a time)
- Hot remove disk Not supported
- Exclude disk Supported
- Shared cluster disk Not supported (roadmap)
- NVMe disks Not supported

# Azure Site Recovery Support Matrix

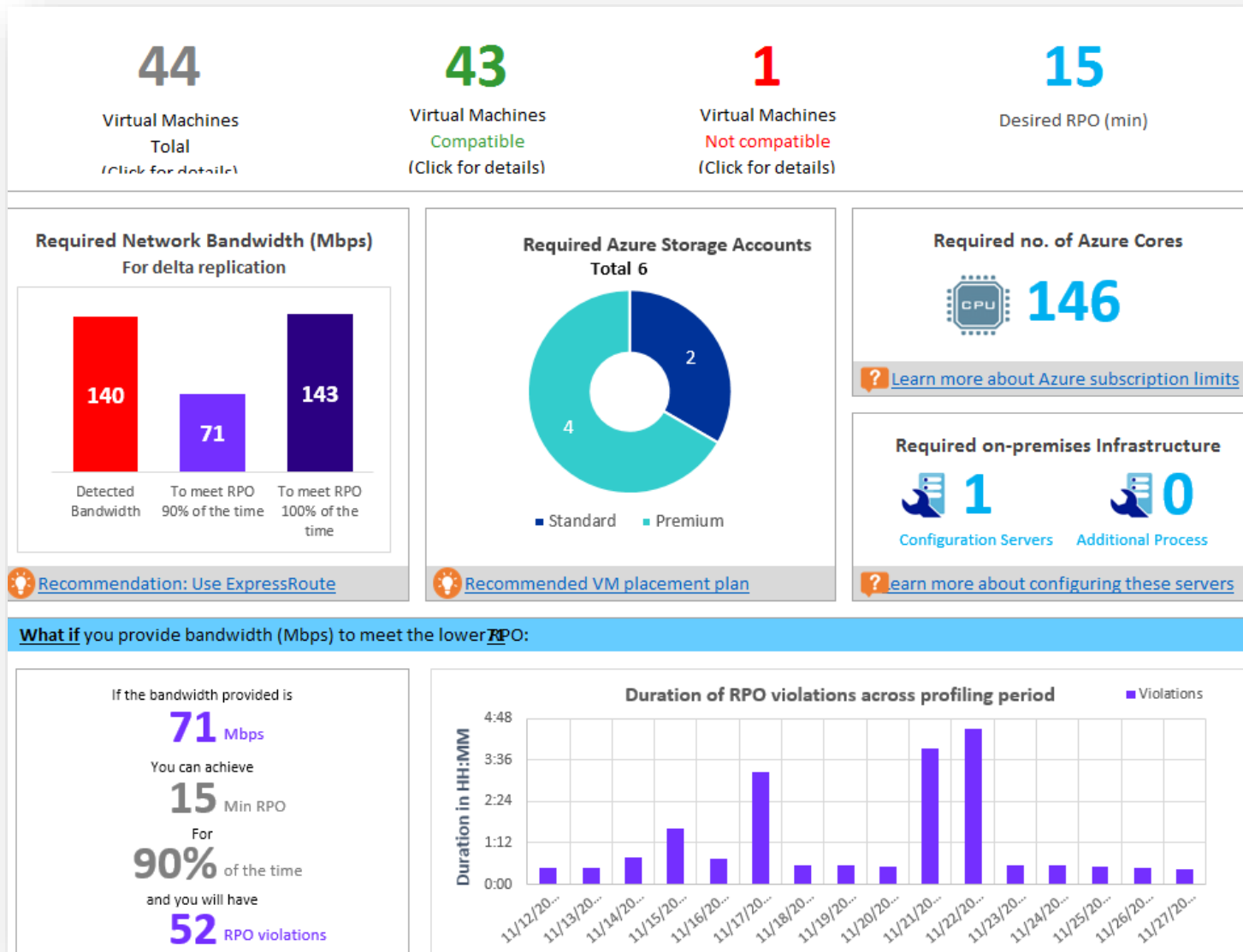
- **Storage (Continued)**

- OS disk must be a basic disk.
- Data disks can be dynamic disks
- Host NFS for Virtual only (not supported for physical)
- Supported to Host SAN (iSCSI/FC)
- Supported to Host multipath (MPIO)
- Supported to host Guest/server VMDK, VHD, VHDX + Gen2
- Encrypted disk not Supported

- **Network**

- Supported for Host network NIC Teaming (Not supported for physical machine)
- Supported for Guest/server network static IP
- Supported for Guest/server network multiple NICs
- Not Supported to Host network IPv6

# Deployment Planner



It is recommended to use a three character prefix for storage account names for performance and scalability optimization

<https://aka.ms/storage-performance-checklist>

Naming convention

<https://aka.ms/guidance-naming-conventions>

SQL Server workload

<https://aka.ms/azure-storage-scalability-performance>

Other high performance workloads

<https://aka.ms/azure-storage-scalability-performance>

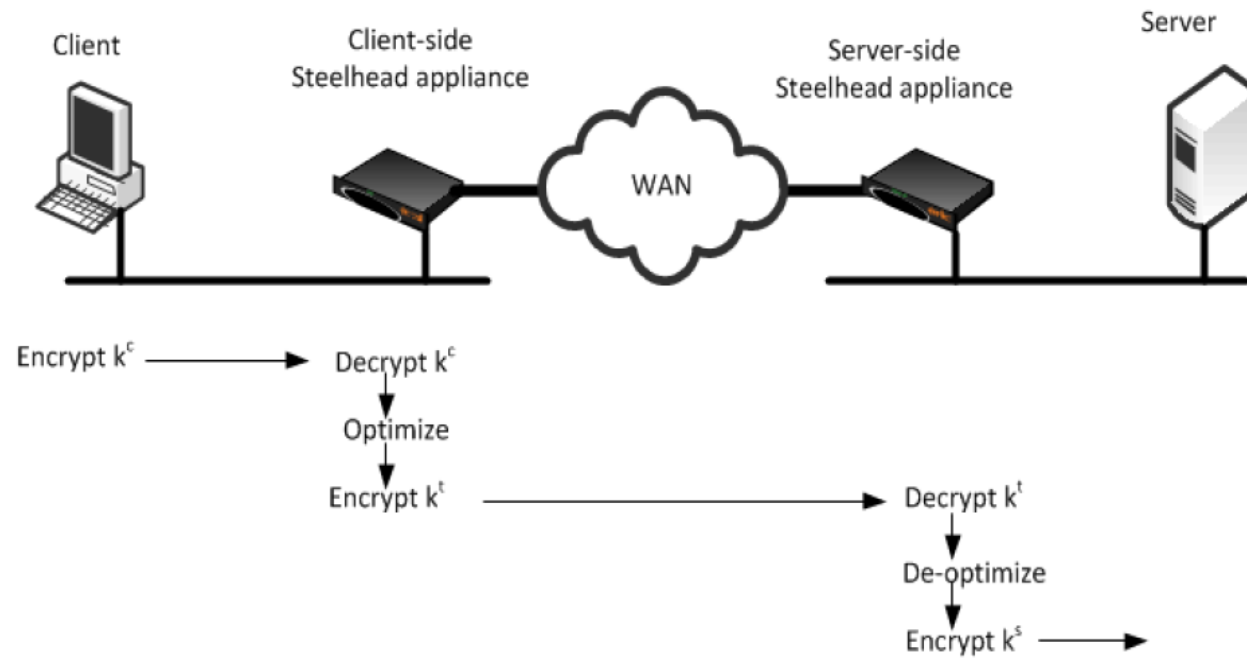
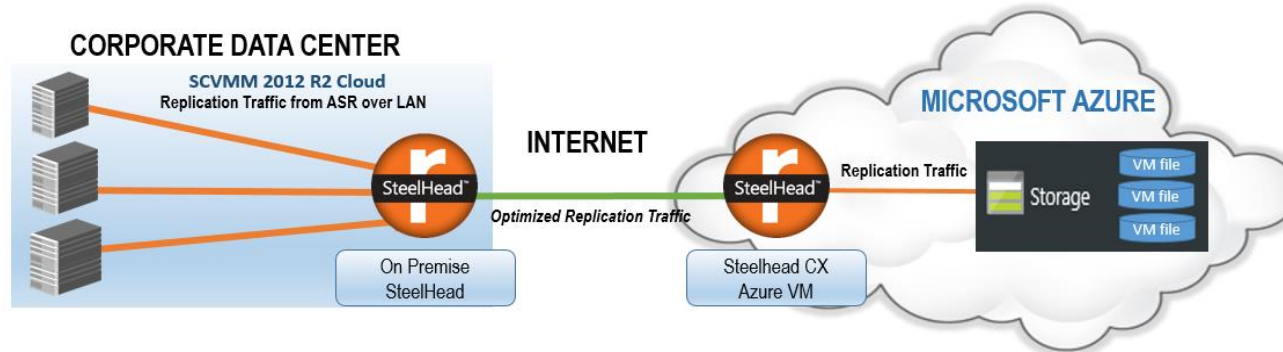
Storage scalability and performance

<https://aka.ms/azure-storage-scalability-performance>

# Deployment Planning

- Estimate **network bandwidth** required for initial and delta replication
- Identify Azure **storage type** (standard or premium) required for virtual machines
- Estimate the total **number of** standard and premium **storage accounts** that need to be provisioned
- Estimate the total **number of Configuration and Process Servers** that need to be deployed while protecting VMware workloads
- Virtual machine **eligibility assessment** based on number of disks, size of the disks and IOPS
- Profile the **actual churn** on the source virtual machine **without any impact** to the production workload

# ASR with Riverbed



## Data Reduction

Average: 72.1%

Peak: 99.7%

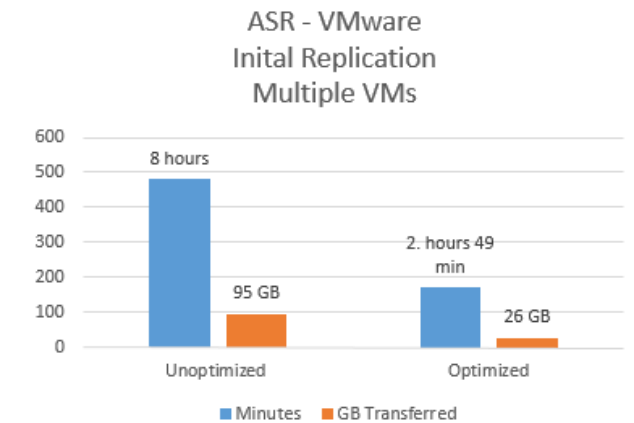
3.6x capacity increase

## LAN Throughput

Total: 95.4 GB

## WAN Throughput

Total: 26.6 GB



Source: Microsoft and Riverbed whitepaper: <https://gallery.technet.microsoft.com/Optimizing-Azure-Recovery-8da50893>

# Networking

- Saturate Available bandwidth
- Throttling
  - [More details](#)
- Retain IP vs. Change IP
  - With full subnet failover -> Retain IP
  - For partial subnet failovers -> Change IP
  - [More details](#)
- Client routing
  - ASR + Azure Traffic Manager
  - [More details](#)

The image shows a Windows desktop environment. In the background, a Task Manager window is open, displaying system performance metrics: CPU at 21% (2.27 GHz), Memory at 10.8/64.0 GB (17%), and Ethernet network activity. In the foreground, the 'Compute and Network' settings window is open, showing configuration for a virtual machine named 'ASRVC2AZ-WS7'. The 'Compute properties' section is visible, with 'Name' set to 'ASRVC2AZ-WS7' and 'Size' set to 'F2 (2 cores, 4 GB memory, 1 NICs)'. Below this, the 'Endpoints' section contains a table with the following data:

NAME	STATUS	MONITOR S...	TYPE	PRIORITY
asremailonpre...	Enabled	Online	External endpo...	1
exchangerp.clo...	Enabled	Degraded	External endpo...	2

## 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](mailto:info@inovasys.co)