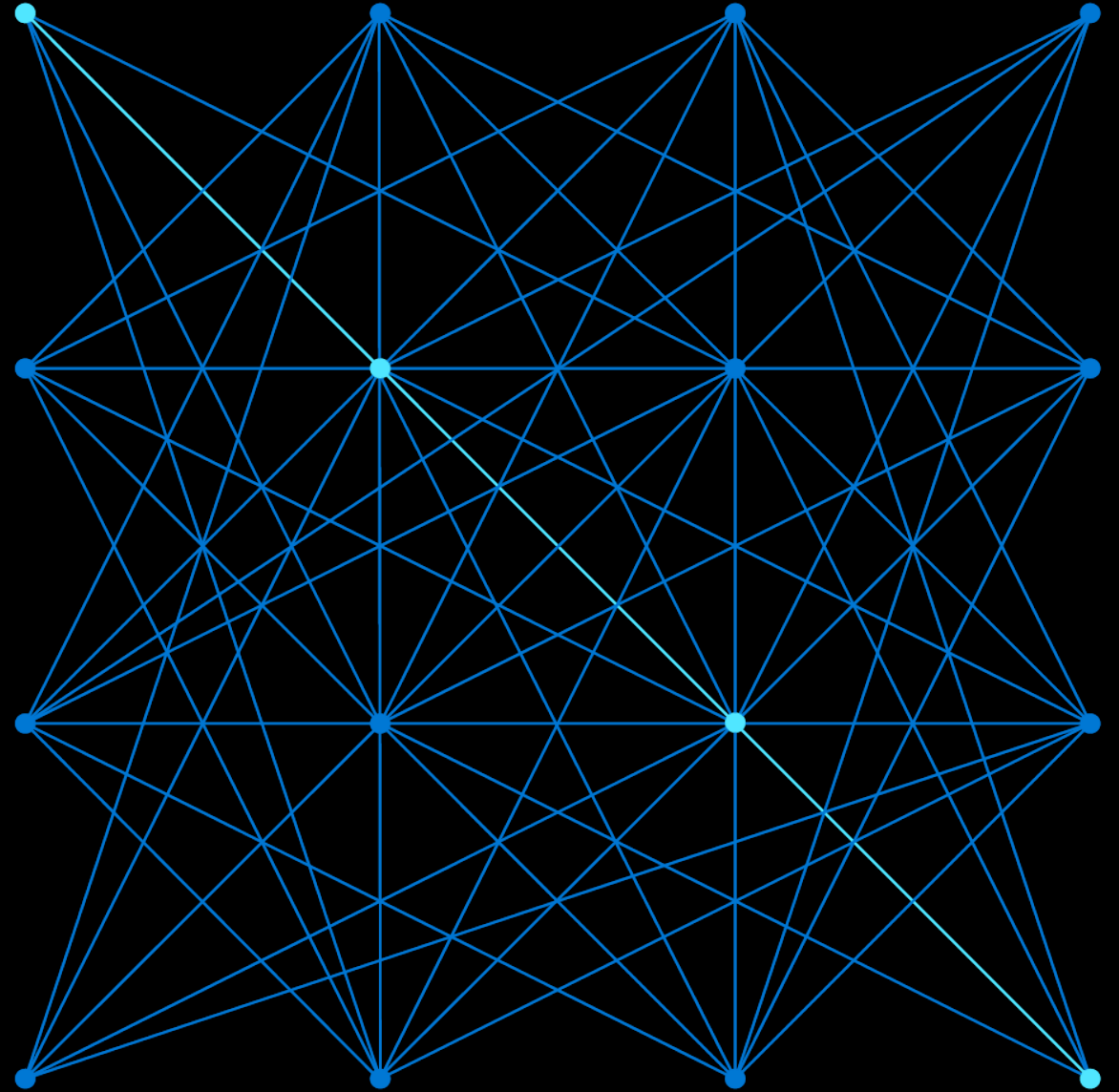


Preparing your organization
for the unpredictable

Business Continuity & Disaster Recovery

Kirillos Sawiras – CSA Azure



Contents

Basic concepts of BCDR

Use cases

- Protect in Azure
- Protect to Azure

Security considerations

Learn more

Introduction to business continuity and disaster recovery

Business Continuity and Disaster Recovery (BCDR)

Processes and tools that protect, restore, and keep your operations running during unpredictable events.

Why BCDR matters

Downtime is inevitable.

Several factors and outside circumstances, like natural disasters, can cause apps to go offline without notice.

Downtime causes tangible impact to business.

When apps are down services become unavailable to organizations and customers.

BCDR can mitigate losses.

Outages may be permanent, and proper BCDR planning not only ensures that business can continue operating but that data is not permanently lost.



High Availability, Disaster Recovery and Business Continuity

Failure event protection options across the recovery and restoration category.

High Availability (HA)

Distribution of an application or workload across a redundant physical or virtual infrastructure

Prevents impact to uptime if one or more nodes should fail

Disaster Recovery (DR)

A combination of tools, backups, replication and asynchronous processes used to recover workloads.

Limits data loss across multiple Azure regions during a catastrophic event.

Business Continuity(BC)

The process, tools and architecture built on top of DR.

Ensures continued uptime of critical business services during a catastrophic event.

BACKUP

Operational restoration processes used in the event of failure.
A low-fidelity DR solution when combined with geo-replication

Why do customers need to protect their IT estate?



Data corruption
and deletion



Outages and
natural disasters



Compliance



Ransomware

Why BCDR matters for your business

\$590_M

Reported ransom paid CY21*

\$11.6k/min

average cost of downtime for large enterprises **

66%

of businesses had some sort of outages in past 3 years***

*Source <https://www.marketsandmarkets.com/Market-Reports/cloud-storage-market-902.html>

** Source: Webtribunal <https://webtribunal.net/blog/data-loss-statistics/>

***Source: Uptime institute report [2021 Data Center Industry Survey Results - Uptime Institute](#)

BCDR Scenarios and Methodologies

Standard BCDR strategies

Your workload setup determines which BCDR strategy you need for protection against disaster events.

SCENARIO ONE

Protect **in** Azure

Strategy for workloads run in Azure.

Uses one or more additional Azure regions as failover locations

SCENARIO TWO

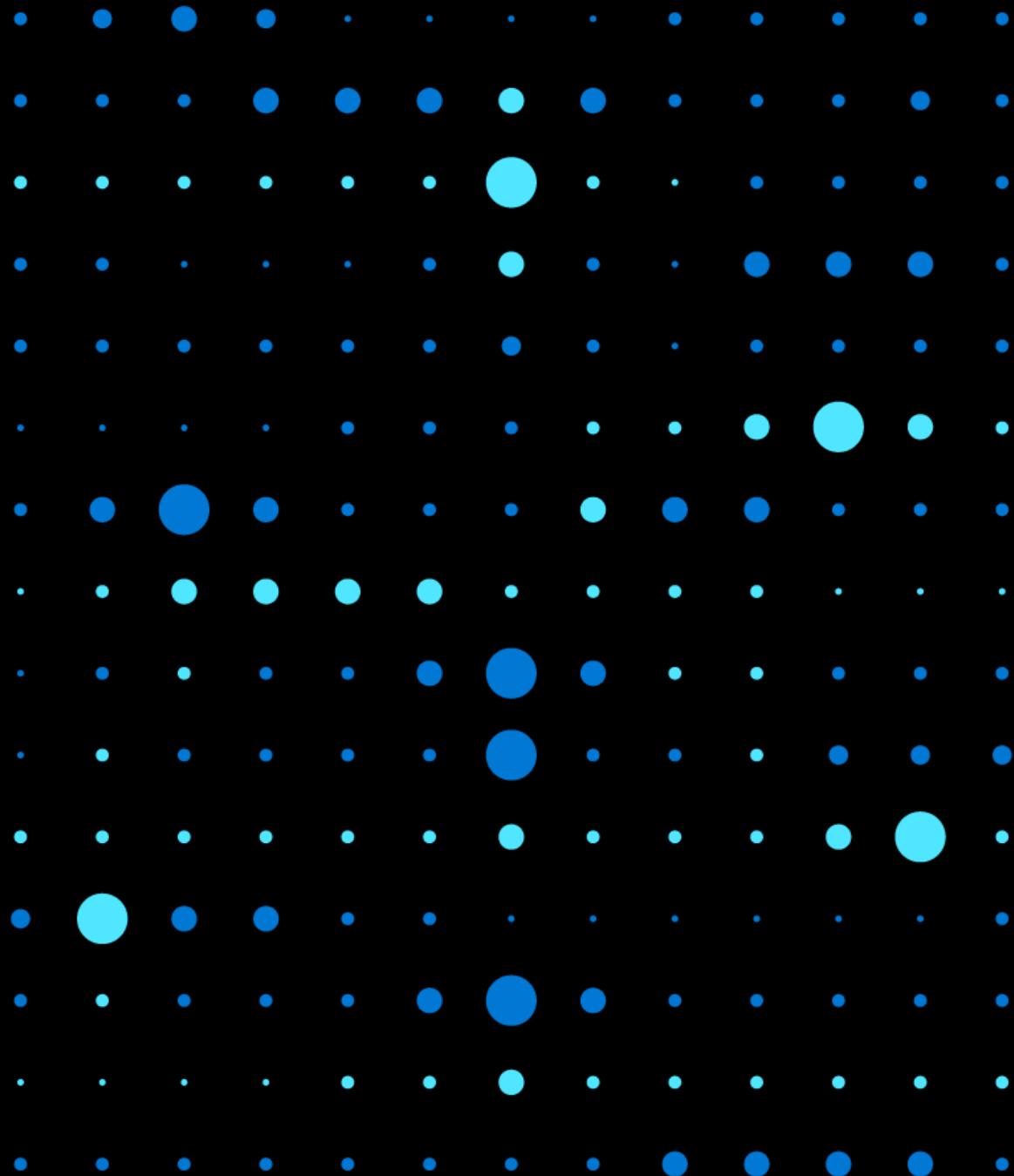
Protect **to** Azure

Strategy for workloads that run on premises.

Uses Azure as a failover location instead of another self-hosted datacenter.

SCENARIO ONE

Protect **in** Azure



SCENARIO ONE

Protect in Azure

The method used to achieve your desired BCDR goals may span across a combination of Azure tools and services, application architecture, and operational processes.



Azure Backup: Modern enterprise-class backup solution!

Azure Backup is a simple, secure, cost-effective manage at-scale built-in backup solution to protect diverse set of workloads in Azure



Simple

Experience less overhead with zero-infra backup solution and self-service restores



Secure

Safeguard backups against ransomware, accidental deletions and outages



Cost-Effective

Predict backup cost with precision and save money with cheaper storage



Manage at-scale

Monitor, operate, govern and plan backups at scale from a central pane of glass



Diverse workload support

Protect database and storage workloads across IaaS and PaaS deployments

Customer success



“As we shift from our on-premises cloud to public cloud, we’ll spend even less time operating that storage backup and compute infrastructure, and more time focusing on more important business needs.”

Tom Voss
IT Operations Manager



“We are able to spin up resources in a few hours instead of months, and we’ve reduced the operational costs of disaster recovery by almost 65 percent. We essentially avoided a half-million-dollar capital purchase.”

Jeff Olson
IS Technical Director



“With the cloud, you don’t need to stock up on components. You can just leverage the technology right away.”

Daniel Breton,
Infrastructure Manager

Diverse business-critical assets protection

Azure Backup and our trusted partners together support protecting multiple workload types to end-to-end across infrastructure, databases, and storage to Azure

Infrastructure, databases, and storage

Backup with ease from a central location
diverse set of workloads – Azure
Windows/Linux VMs, databases (SQL Server, SAP HANA, PostgreSQL, Oracle) and storage
workloads (Azure Files/Disks/Blobs)

Trusted partner ecosystem

Extend your on-premises strategy to Azure
with help from our partners

Azure Backup



Azure VM



On-prem
Servers



Azure
PostgreSQL



SQL/HANA VM



Azure Blob
Storage



Azure Disks



Azure Files

Partner ecosystem



COMMVault™



rubrik



and many more...

Choose from our trusted partners for additional workloads

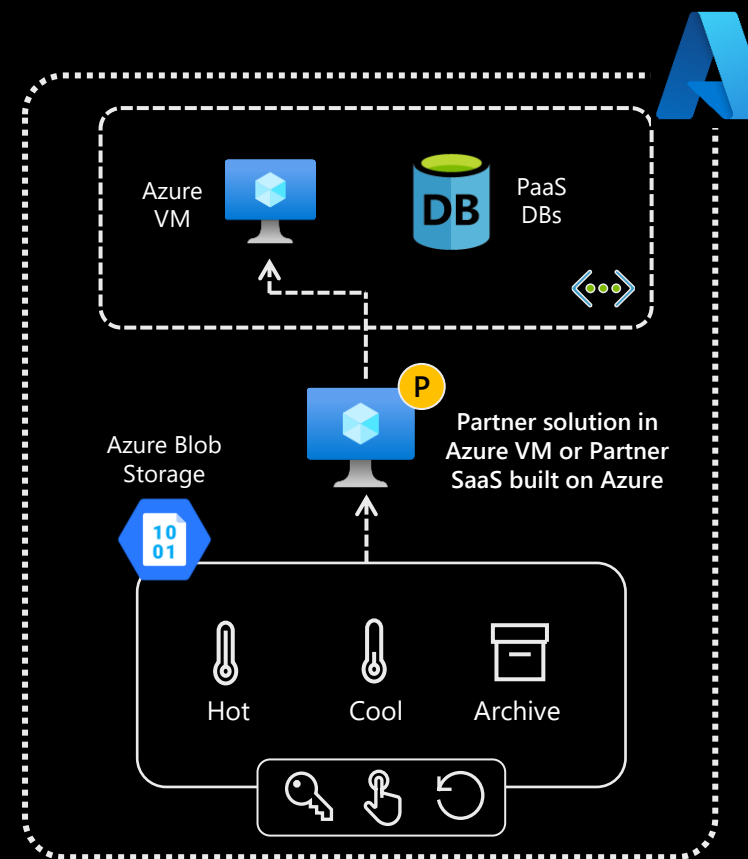
Choose from our ecosystem for your unique workload needs

Continue using your preferred BCDR solution for your migrated workloads

Leverage SaaS on Azure ISV solutions for air gapped storage of your backups

Store cost-effectively on the secure & durable Azure Storage platform

Stay compliant



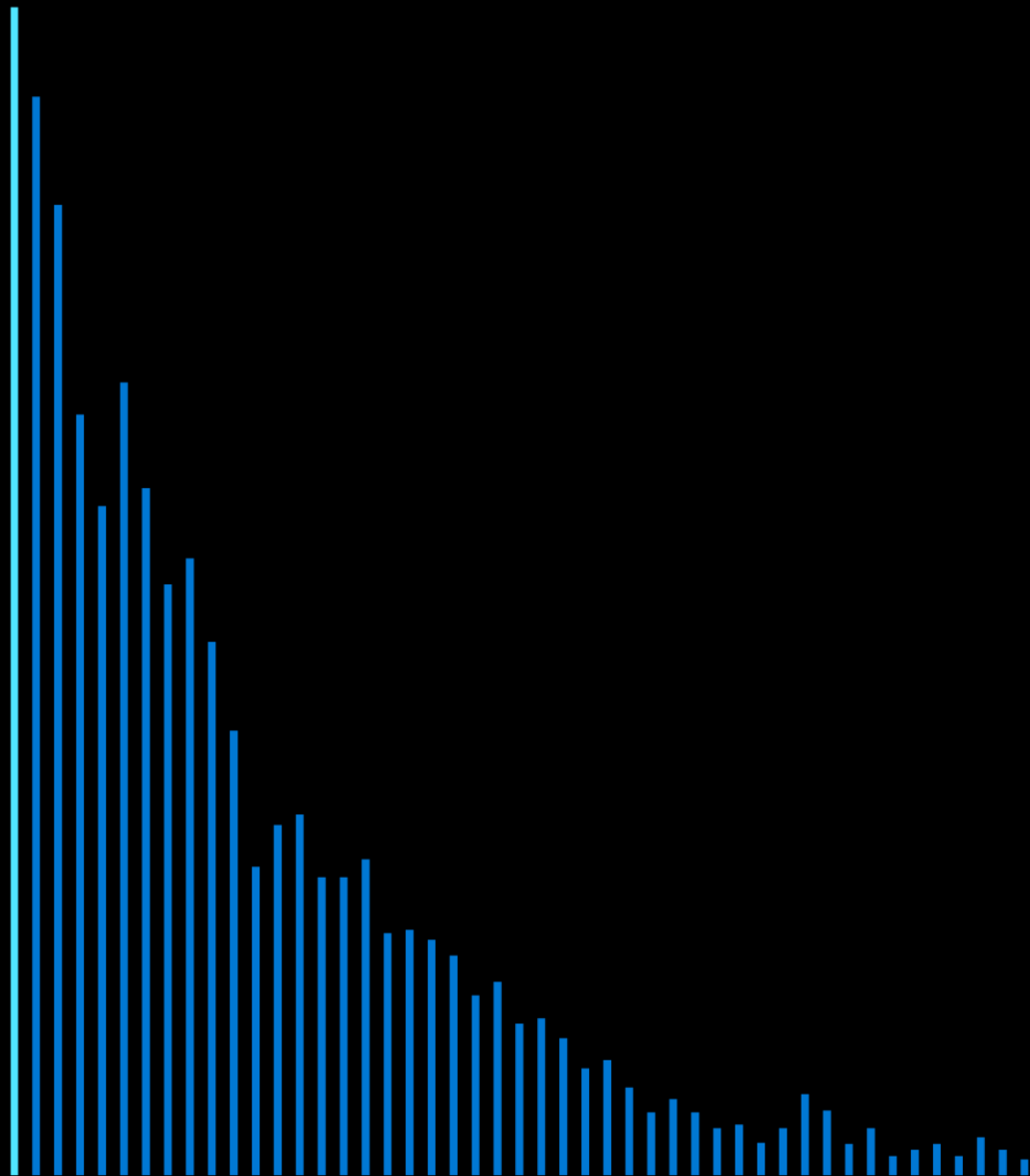
Our trusted
partner ecosystem



and many
more...

SCENARIO TWO

Protect **to** Azure



Protect **to** Azure

Azure can be used as a secondary, highly-resilient failover location for workloads running in your existing datacenters, offering backup and recovery.

The cost of Azure is based on consumption

Azure only charges for resources used at the time of and during failover. By contrast, on-premises datacenters come with upfront costs (e.g., facilities, hardware, electricity and cooling costs).

Resiliency is built in

Azure's fabric is far more resilient than most on-premises datacenters.

Azure gives you options

It offers multiple native and third-party workload protection options by replicating live servers to Azure regions—with no impact on production workloads.

Broad ISV ecosystem

Leading data protection ISVs partner with Azure to help customers protect their critical data

SCENARIO TWO

Protect **to** Azure

Options include:



Independent Software Vendors (ISV)



Azure Site Recovery (ASR)

Extend your BCDR strategy with our trusted partners

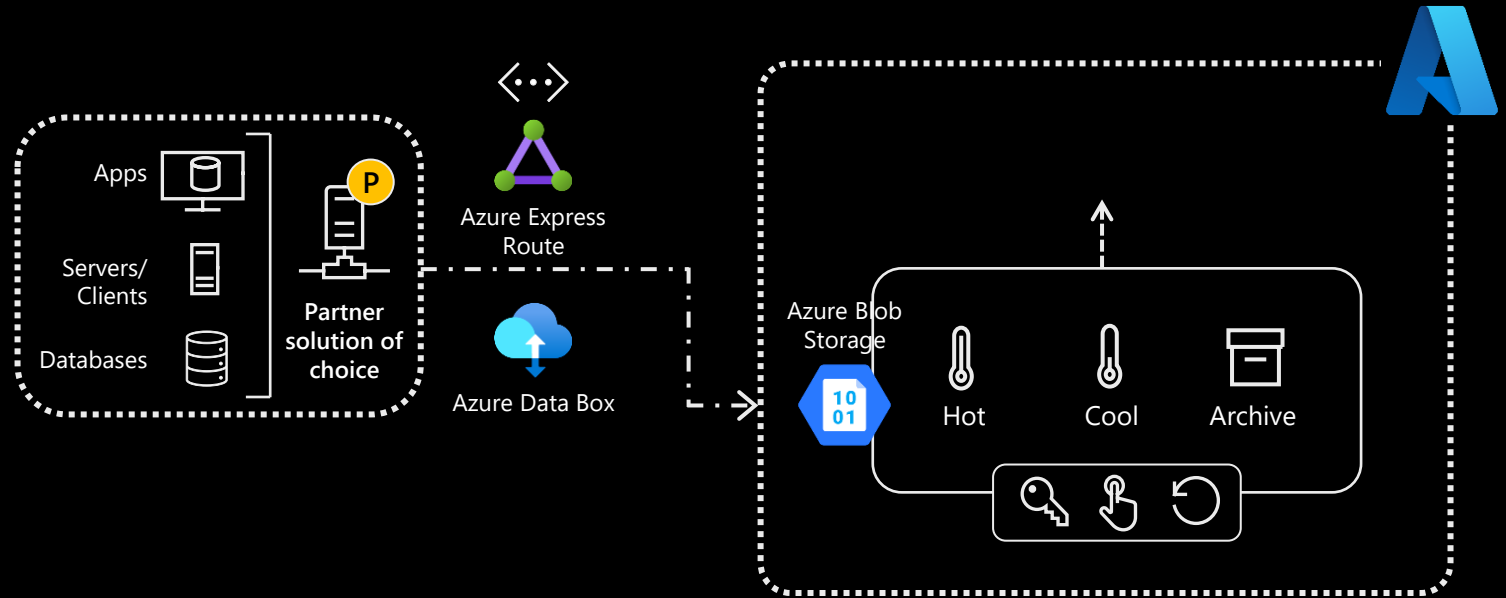
Backup data/apps to Azure as a durable offsite

Store securely & cost-effectively in **Azure Storage**

Use Azure as a secure & cost-effective DR site

Migrate and protect in Azure

Stay compliant

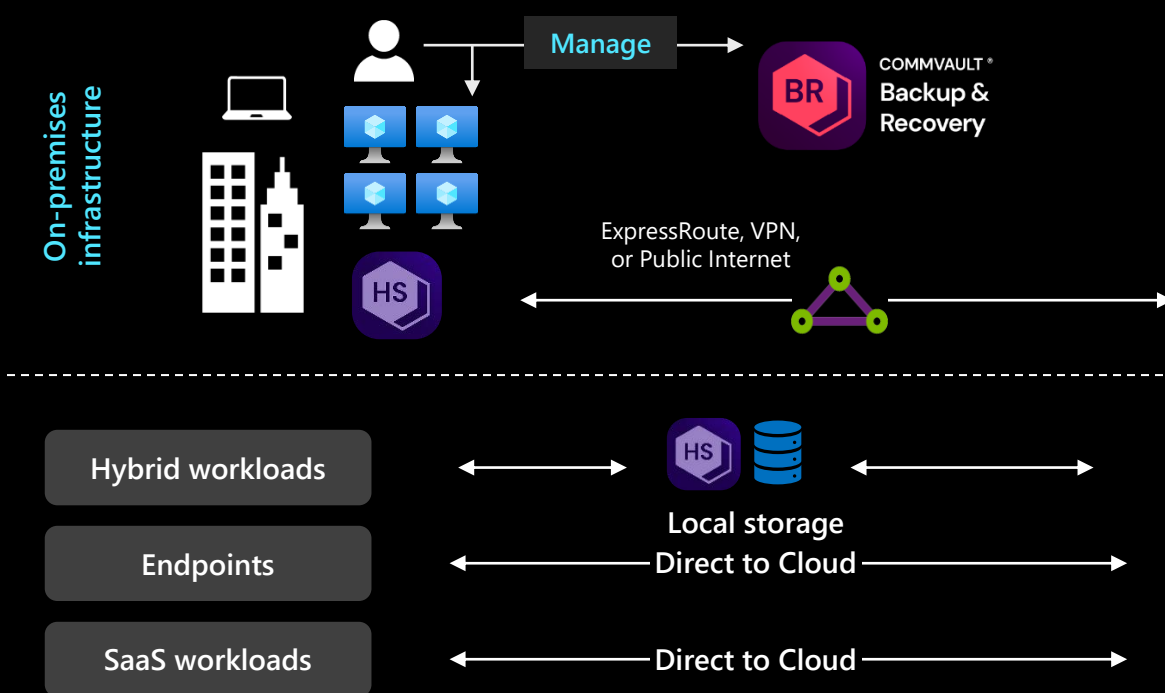


Our trusted
partner ecosystem

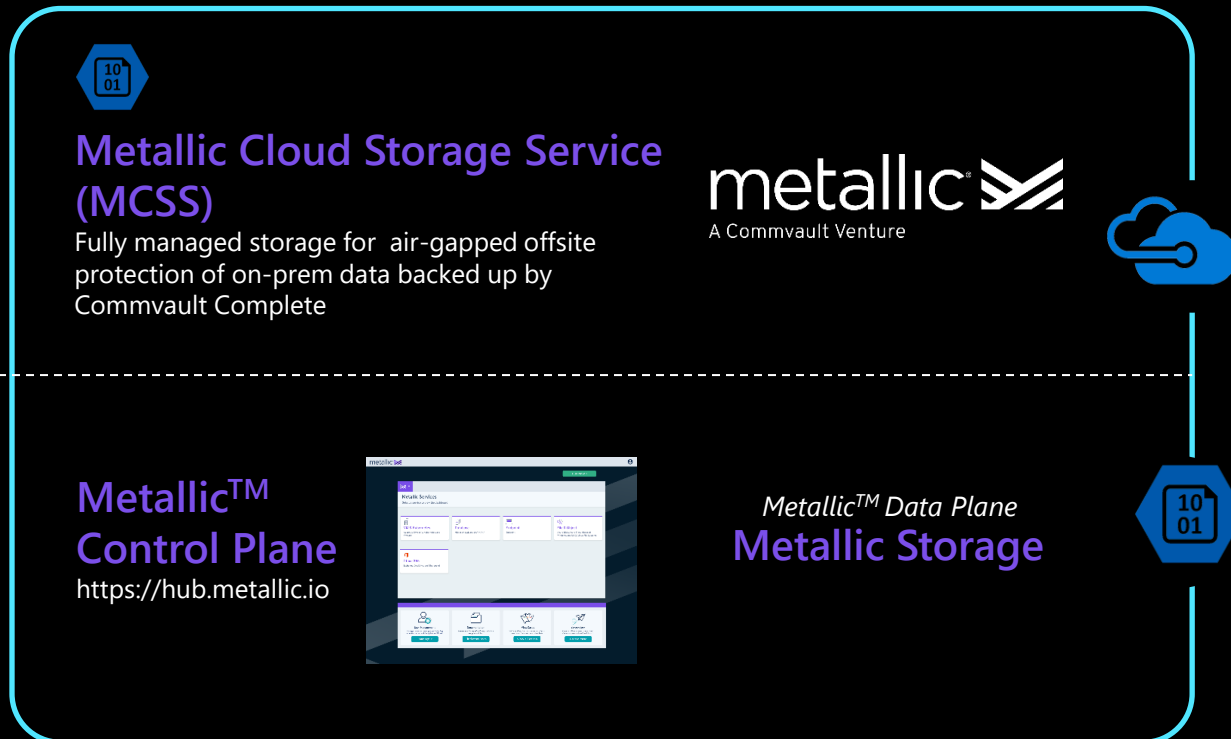


and many
more...

Commvault & Metallic SaaS



- Lightweight / Easy to setup and central management with other Commvault software
- Hosted on Azure for SaaS data, On-prem offsite data, Azure data
- Built on Secure, immutable and scalable Azure Blob foundations (FedRAMP Certified)
- Air-gapped security and ransomware protection
- Simple \$/GB/month pricing



- Protect Azure VMs, Azure Files, Azure Blobs, ADLS Gen2, Azure VMWare Solution and AKS
- Protect Endpoints, M365 (Including Teams) and Hybrid workloads
- Use Azure as a DevTest or Recovery Site with Orchestrate
- All the goodness of proven Commvault Complete features
- Search, Discovery, and Compliance cross-cloud with Activate

Rubrik - Zero Trust Data Security

Instantly secure your data from ransomware with Rubrik Cloud Vault built on Azure

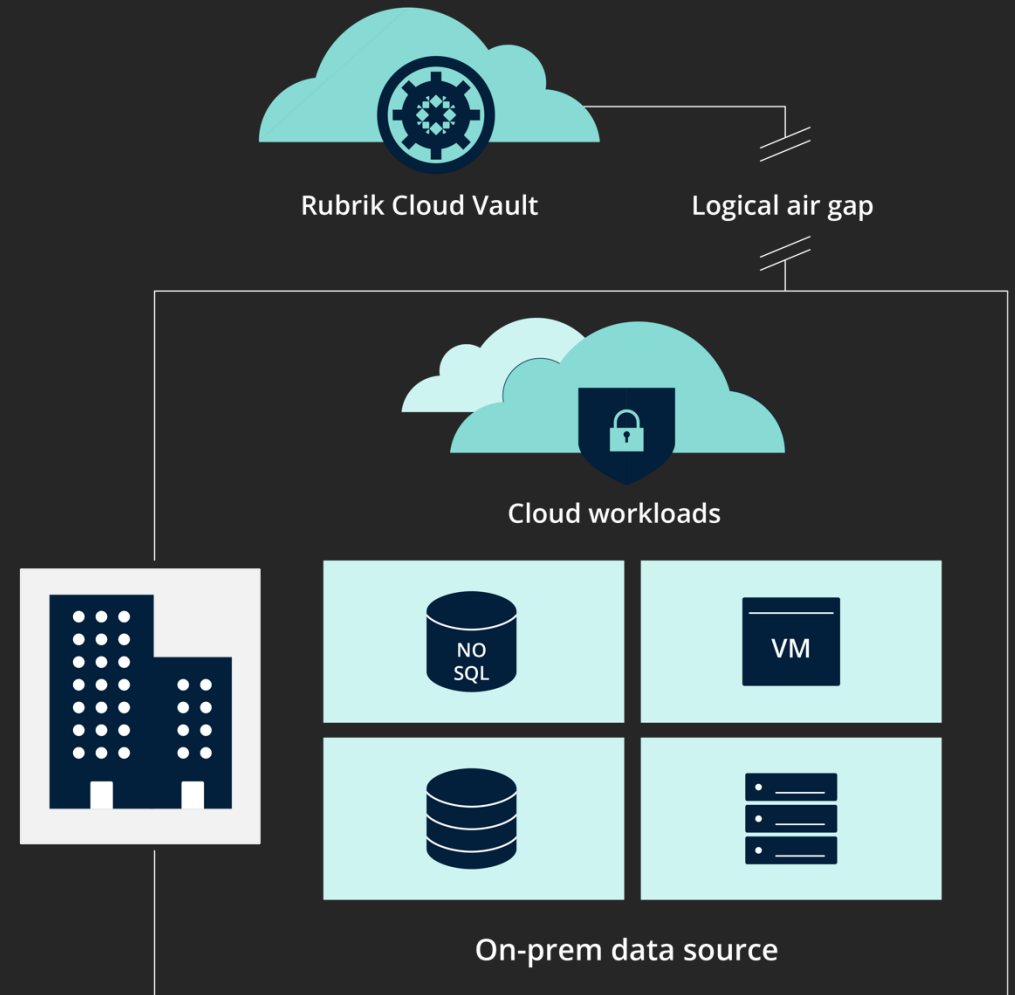
Logically air-gapped & immutable storage so you can always recover from cyber attacks

Fully-managed service that reduces data risk and operational complexity

Predictable cost that includes all storage & egress charges to stay within budget

[Rubrik Cloud Vault | Rubrik](#)

[Instant Application Availability for Microsoft | Azure Backup | Rubrik](#)



Veeam Modern Data Protection



Microsoft Office 365

(SaaS)

Granular protection and item-level recovery for Exchange Online, Sharepoint Online, Microsoft OneDrive, and Microsoft Teams.

Can also protect on-premises Exchange and Sharepoint.

Veeam Backup for Microsoft Office 365



Store metadata cache on disk and data on Azure Blob



Azure-native virtual machines

(IaaS)

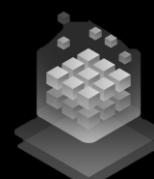
Protect and restore Azure virtual machines

←
Direct restore for Microsoft Azure includes support for restore from other cloud providers and hypervisors

Veeam Backup for Microsoft Azure



Create snapshots and store backups on Azure Blob



Azure Kubernetes Service

(PaaS)

Data portability and application mobility for cloud-native applications.

Automatic application discovery, backup disaster recover, and data portability for Kubernetes workloads.

Kasten K10 by Veeam

Restore via external repository



Virtual and physical environments

(Vmware, Hyper-V, AHV, Windows, Linux, Solaris, and AIX)

Protect and restore workloads with native granular restore via Veeam Explorers™ for Active Directory, Exchange, SharePoint, SQL Server, Oracle, and support for other enterprise applications

Supports agentless backup, replication, and migration for Azure VMware Solution, and Azure Stack HCI

Veeam Backup & Replication®



Direct restore to Microsoft Azure Stack Hub

Veeam Agents for Windows, Linux, Solaris, and AIX



Data can be stored on disk as primary tier and then Azure Blob as capacity tier

[Learn more at Veeam for Microsoft Cloud](#)

Veritas Enterprise Data Services Platform

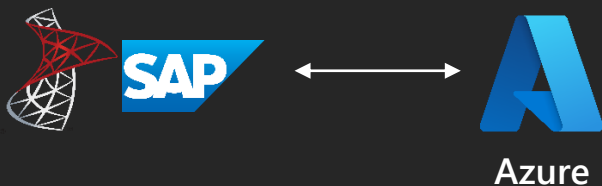
VERITAS™

Availability



Veritas InfoScale™

Low RPO automated migration and disaster recovery to Azure



And more....

Protection



Veritas NetBackup™

Automated application aware backups tiered to Azure



Veritas NetBackup SaaS Protection

Comprehensive SaaS protection run as a service on Azure



Veritas NetBackup Recovery Vault

Secure and resilient data protection storage as a service

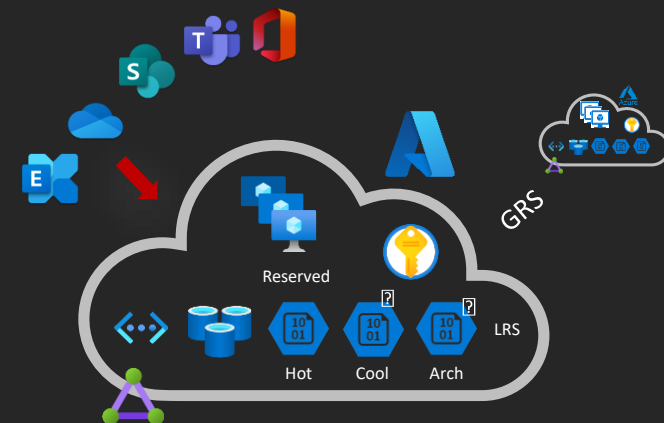


Insights

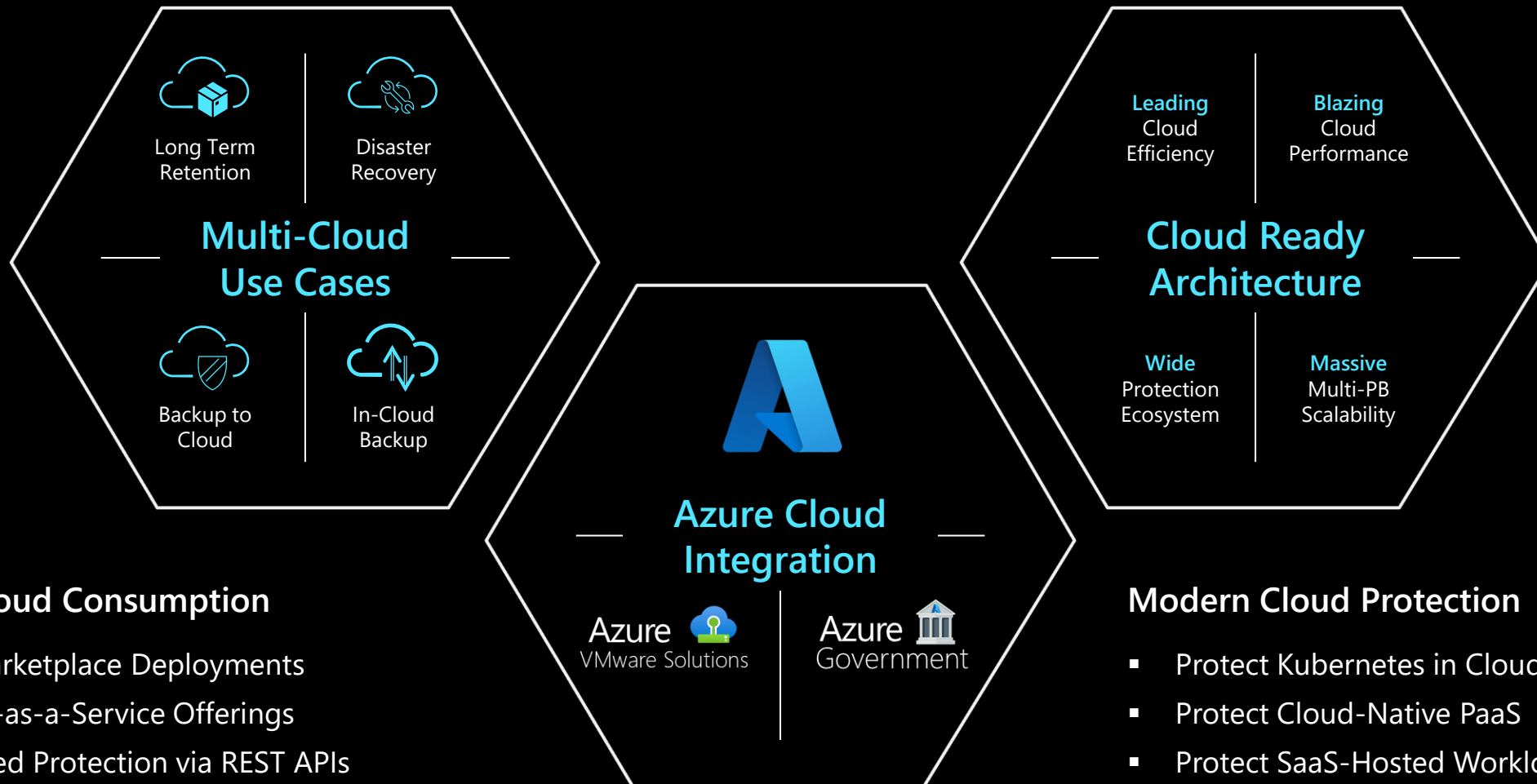


Enterprise Vault.cloud

Content Collection, Classification, Discovery & Supervision
SaaS solution completely hosted in Azure



Data protection for Microsoft Azure



Modern Cloud Consumption

- Azure Marketplace Deployments
- Software-as-a-Service Offerings
- Automated Protection via REST APIs

Modern Cloud Protection

- Protect Kubernetes in Cloud
- Protect Cloud-Native PaaS
- Protect SaaS-Hosted Workloads

Zerto Data Protection Solutions



Disaster Recovery to Azure

Continuous data protection with low-RPO and low-RTO to Azure Virtual Machines and Azure Disks



Massive Scale

Use of Virtual Machine Scale Sets for significant improvement to RTO



Tiered Storage

Integration with Azure Blob storage for cost effective long term retention



Hot

Cool

Archive

Azure Migrate

Integration with unified platform for discovery, assessment and migration



Azure to Azure Protection

Replicates to regions globally in Azure for disaster recovery



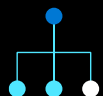
Azure Kubernetes Service

Data protection for stateful applications running on Kubernetes in Azure



Protect to Azure via Azure Site Recovery

Clones your live server to Azure



Easy to deploy and manage



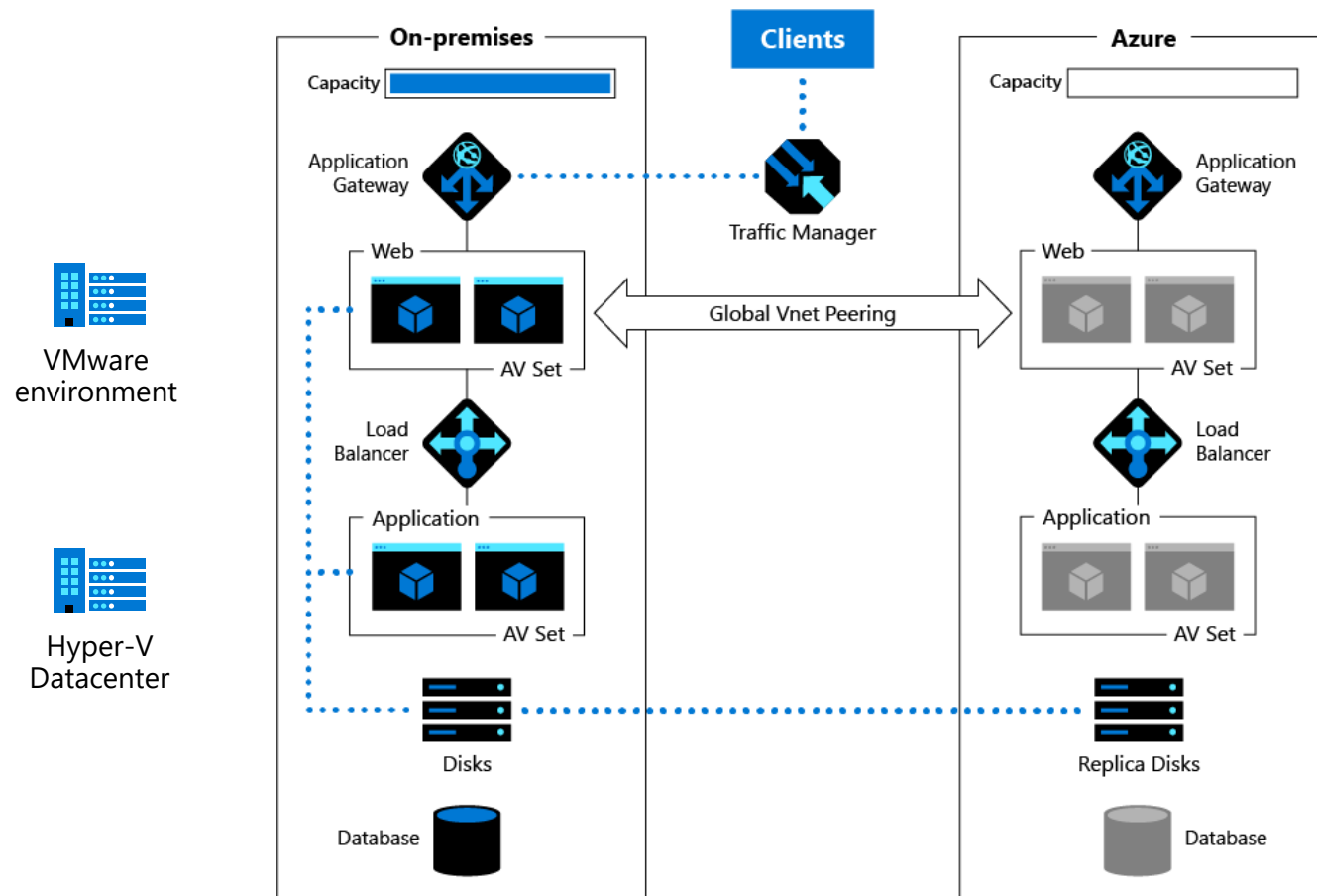
Reduce infrastructure costs

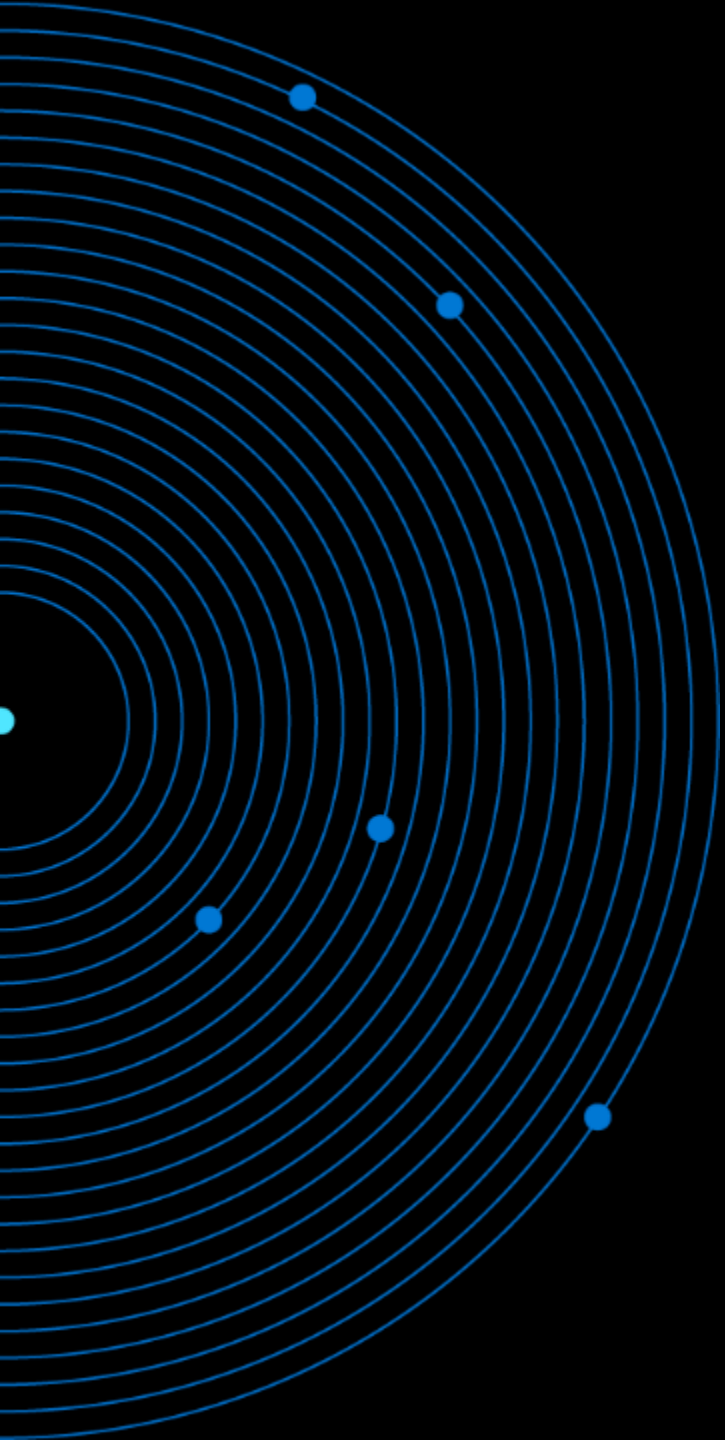


Minimize downtime with
dependable recovery



Heterogenous environment
support





Security considerations

Protect your organization from ransomware

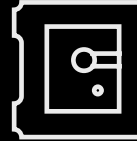


Create a response plan and adopt the right tools

Adopt an internal culture of Zero Trust, assumed breach, and good security hygiene and posture. Implement a system of data recovery/backup and secure access.

Related capabilities

- Remote access
- Zero Trust
- Security posture
- Data backup



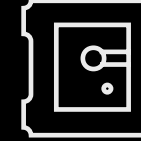
Prevent attackers from getting in

Harden the security perimeter by leveraging best-in-class security workloads.

Deploy comprehensive prevention, detection, and response capabilities.

Related capabilities

- SIEM + XDR for prevention, detection, and response
- Cross-workload security



Protect critical data from compromise

Minimize the potential for lateral movement and privilege escalation should an attacker gain an entry point.

Related capabilities

- Internal process/access management
- Data backup and business continuity

Microsoft Sentinel

Optimize security operations with cloud-native SIEM powered by AI and automation



Harness the scale
of the cloud

56%

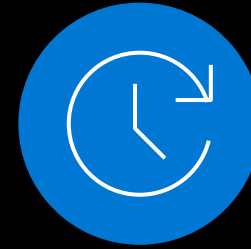
**reduction in management
effort** for infrastructure
and SIEM



Detect
evolving threats

79%

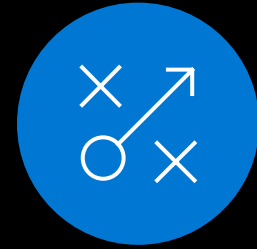
decrease in false positives
over three years



Expedite
incident response

80%

**reduction in investigation
labor effort**



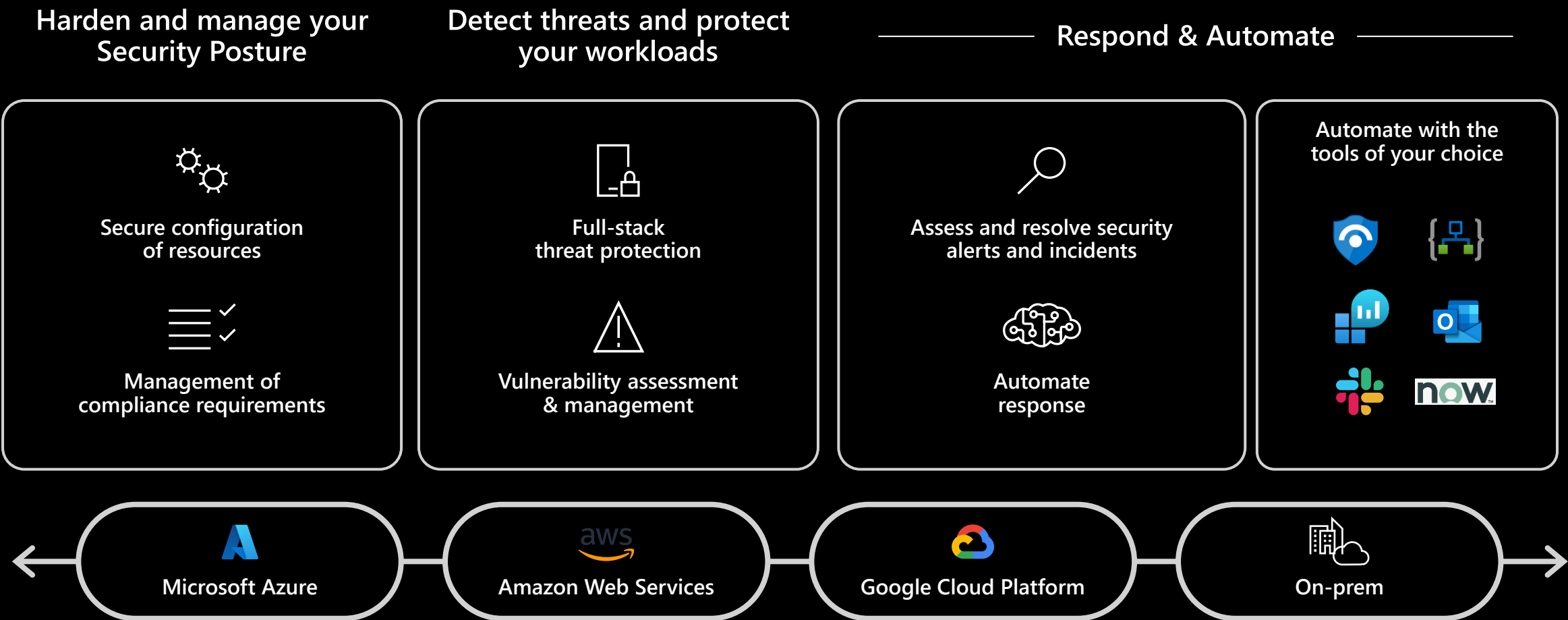
Get ahead
of attackers

67%

**decrease in time to
deployment** with pre-built
SIEM content and out-of-the-
box functionality

Microsoft Defender For Cloud

Cloud-native application protection across clouds and on-prem environments



Secure your network infrastructure and applications

Protection from edge to cloud with cloud-native network security based on Zero Trust

Azure Network Security

Infrastructure Security



Azure
Firewall



Azure DDoS
Protection



Azure
Bastion

Application Security



Azure Web
Application Firewall
(regional & global)



Segmentation
controls

Intelligent
threat protection

Traffic
encryption

Private
access



Defense-in-depth protection from edge to cloud

Resources for Azure Backup and Azure Site Recovery

Landing page	https://aka.ms/azure-backup https://azure.microsoft.com/en-us/services/site-recovery/
Blogs	https://aka.ms/azure-backup-blogs https://aka.ms/siterecovery_blogs
Documentation	https://aka.ms/azure-backup-documentation https://docs.microsoft.com/en-us/azure/site-recovery
Recent Azure Backup releases	https://aka.ms/azure-backup-recent-releases
Guidance and Best Practices	https://aka.ms/azure-backup-best-practices https://azure.microsoft.com/en-us/solutions/architecture/disaster-recovery-smb-azure-site-recovery/
Azure Backup Support Matrix	https://docs.microsoft.com/azure/backup/backup-support-matrix
Training	https://aka.ms/azure-backup-training/
MS Learn: Protect Virtual Machines using Azure Backup	https://aka.ms/AzureBackup-Learn https://aka.ms/siterecovery_mva
Feedback (user voice)	https://aka.ms/azure-backup-user-voice https://aka.ms/ASRuservice



Write to AskAzureBackupTeam@microsoft.com for preview signups

ISV resources



- [Quick Start Guide](#)
- [Instantly protect your data to Metallic Cloud Storage Service](#)
- [Try Metallic for free](#)
- [See demo](#)



- [Quick Start Guide](#)
- [Learn more about Rubrik Cloud Vault](#)
- [Learn more about Rubrik M365](#)
- [See demo](#) of how to use Rubrik Cloud Vault



- [Quick Start Guide](#)
- [Exclusive Azure Offer](#)
- [See demo](#)



- [Quick Start Guide](#)
- [Try NetBackup Recovery Vault on Azure](#)
- [See demo](#)



- <http://delltechnologies.com/Azure>
- [Dell Data Protection Suite offer](#)
- [Dell PowerProtect Cyber Recovery offer](#)
- [DD VE offer](#)



- [Learn more about Zerto on Azure](#)
- [See demos of the Zerto platform](#)
- [Try Zerto for free](#)

Industry leaders to help you on your journey

You can *EASILY & SECURELY* leverage Azure to protect your critical data and apps from ransomware attacks and stay compliant!