

AZURE COST SAVINGS WEBINAR

# Why native Azure tools are your **most expensive** backup strategy

*And what to do instead...*

# What we'll cover today

Native-tool costs, the fix, ASR's gaps, and a framework to size protection per workload.

**01**

## Azure Backup's hidden costs

Why the bill you've stopped questioning is bigger than it should be.

**02**

## How N2W fixes it

Zero Managed Disk, automated Blob tiering, flat per-VM pricing.

**03**

## Where ASR falls short

Replication buys availability. Not the same as recoverability.

**04**

## A framework to size protection

Six questions to match spend to what each workload needs.

# The Azure Backup cost problem, in 3 parts.

Limited storage options

Complex licensing fees

Monthly recurring billing

## Licensing fees for one 1.1 TB VM · backup + retention

### Azure Backup

Tiered by VM size, plus extra per 500 GB.

**\$30**

plus backup costs

### N2W flat-rate

Flat per VM, any size.  
Simple, predictable.

**\$5**

**>83%** cost savings

Same VM, same backups, pure savings.

# N2W slashes backup storage \$\$\$ in 3 parts.

No need to park a full 1 TB backup in costly managed-disk storage for your whole retention window.

**01**

## Zero Managed Disk

Keep only the incrementals and delete the full backup—no redundant full copy sitting in expensive managed-disk storage.

**02**

## Archive to Azure Blob

Automate tiering of long-term backups into low-cost Azure Blob storage (the same 1 TB, a fraction of the cost).

Managed Disk



Azure Blob

**03**

## Kill the license fee

Eliminate the Azure Backup licensing fee entirely. It is no longer part of your monthly bill.

# Fixed pricing. Automated tiering.

- ✓ **Fixed, transparent licensing**— a flat fee per VM.
- 🔗 **Automated Cold blob tiering**— set it and let it run.
- 💰 **Significant cost savings**— for long-term retention.
- 🛡️ **Compliance, accelerated**— hit retention without Azure Backup license fees.

**Up to 90%** savings

AZURE BLOB STORAGE TIERING

**Hot**  
Active backups, fastest access.

EXISTING

**Cool**  
Infrequent access.

NEW IN V4.6

**Cold**  
Rarely accessed, lowest cost.

NEW IN V4.6

Higher cost / fast access

Lower cost / cold archive

Daily < 14 days  
Hot

Weekly < 90 days  
Cool

Monthly + 7 yrs  
Cold

USING N2W

90% up to savings

- ✓ Fixed, transparent licensing
- 🔗 Automated Cold blob tiering
- 💰 Significant cost savings
- 🛡️ Compliance, made easier

AZURE BLOB STORAGE TIERING



Higher cost / fast access

Lower cost / cold archive

| POLICY             |   |      |
|--------------------|---|------|
| Daily, < 14 days   | → | Hot  |
| Weekly, < 90 days  | → | Cool |
| Monthly, + 7 years | → | Cold |

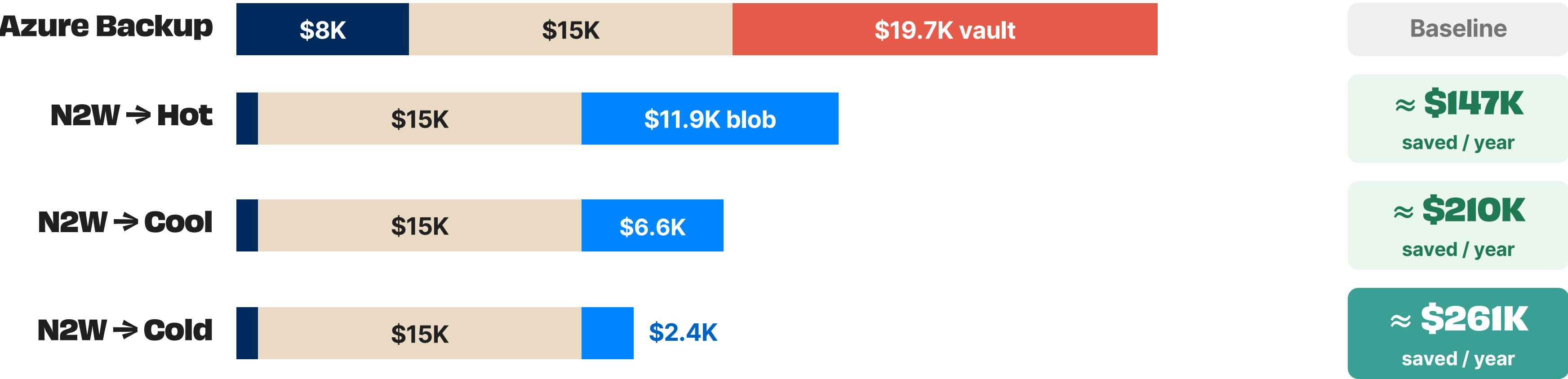
# Savings for 90-day retention.

200 VMs

1.5 TB avg / VM

Daily backups

90-day retention



Licensing fee

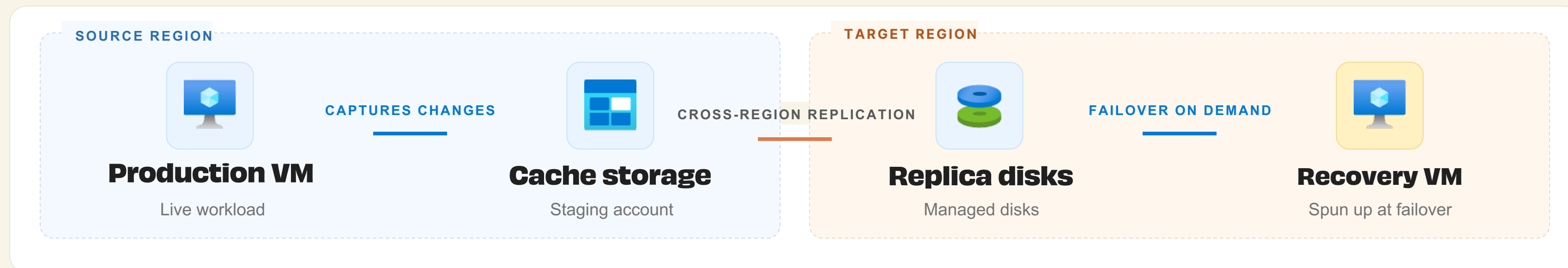
7-day snapshot (shared)

Azure Vault storage

N2W → Azure Blob

# What was ASR intended for?

ASR is Azure's native replication and failover service for VMs and apps.



## What does ASR do well at?

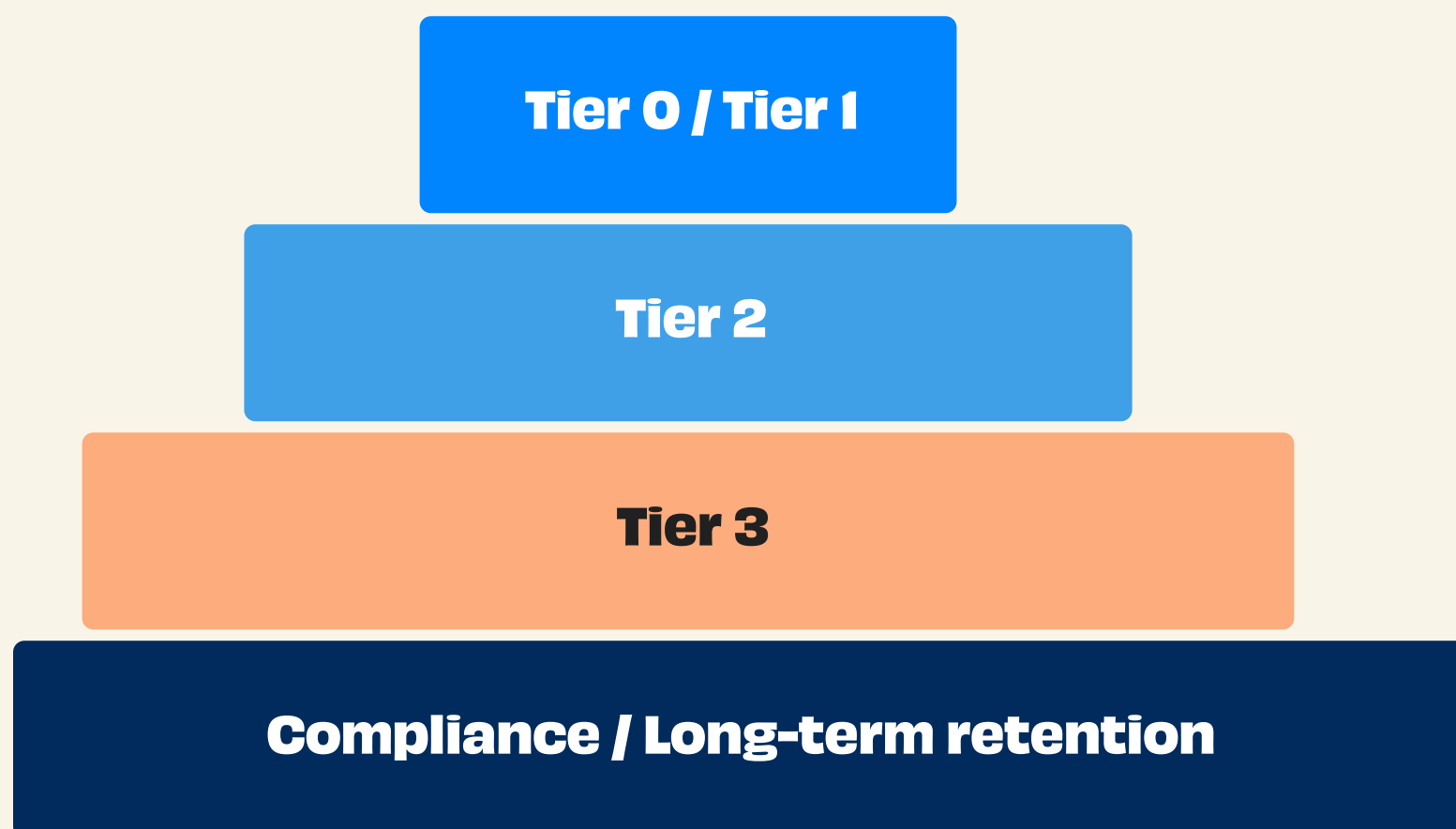
- ✓ Low-RPO VM replication between Azure regions
- ✓ Planned and unplanned failover orchestration
- ✓ Crash-consistent recovery points for IaaS workloads

## Where is it lacking?

- ✗ Not a backup — no long-term retention or archive
- ✗ Limited cyber recovery: corrupted or encrypted writes can replicate
- ✗ RTO has many dependencies that make it hard to pin down

# Protecting workload tiers

How should workload tiers be protected?



Most environments only need near-continuous replication for a thin slice at the top yet ASR is often applied to **everything**.

## Tier 0 / Tier 1

Identity, core databases, revenue systems, customer-facing apps

Good fit for: [ASR or DR-based replication](#)

## Tier 2

Important internal applications, departmental systems

Good fit for: [Snapshot-based DR, frequent backups, orchestrated restore](#)

## Tier 3

Dev/test, QA, reporting, low-use systems

Good fit for: [Backup, lower-frequency restore points, archive](#)

## Compliance / Long-term retention

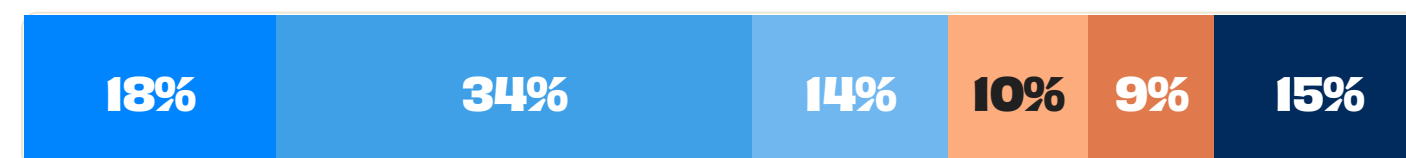
Monthly/yearly retention, audit recovery

Good fit for: [Backup/archive, immutable retention, lower-cost storage](#)

# Hidden costs involved

## Not just the protected VM charge.

### EXAMPLE ASR MONTHLY COST COMPOSITION



- Protected instance fee 18%
- Replicated storage 34%
- Storage transactions 14%
- Test failover compute 10%
- Network / data transfer 9%
- Operational effort 15%

*Illustrative split.*

- ASR protected instance fee** Monthly fee per protected workload after the free initial period
- Replicated storage** Disks and recovery point data in the target region
- Storage transactions** Ongoing replication activity
- Test failover compute** VMs started during DR testing
- Network and data transfer** Architecture-dependent
- Operational effort** Runbooks, testing, validation, cleanup, compliance evidence

# Replication vs DR.

## Is availability enough?



### Recovery point strategy

Replication gives recent recovery points, but you may also need older clean points.



### Application dependencies

Apps rely on databases, identity, DNS, networking, certificates, and integrations.



### Network readiness

VNets, subnets, NSGs, routing, and connectivity must be planned and tested.



### Testing realism

A test failover may require isolated networking and may not perfectly mirror production.



### Long-term retention

Replication is not a replacement for monthly/yearly backup retention.



### Cyber recovery

If corruption is replicated, a recent replica may not be the desired recovery point.

**Cost alignment** Not every workload needs the same RPO / RTO profile. So why pay as if it does?

# ASR can support low RPO.

## But what about RTO?

### RPO

HOW MUCH DATA LOSS

## Low

Replication delivers recent recovery points.



### RTO

HOW LONG TO BE BACK ONLINE

## It depends.

Dependencies, sequencing and validation extend the wall clock.



### WHAT ACTUALLY HAPPENS DURING RECOVERY

**01**

#### VM startup

Replicated VMs still need to be started and validated.

**02**

#### Application order

Databases, app servers, middleware, and front ends need sequencing.

**03**

#### Network mapping

VNets, subnets, DNS routing & connectivity must work.

**04**

#### Identity dependencies

AD, Entra ID integration, service accounts, certificates.

**05**

#### Manual validation

Teams need to confirm the application is usable.

**06**

#### Runbook quality

Tested runbooks reduce recovery time.

**07**

#### DR test frequency

Untested recovery usually takes longer.

# ASR drills are useful but...

A proper drill must have:

**01**

## Isolated test network

Avoids production conflicts but requires extra planning.

**02**

## DNS & routing setup

Test systems need realistic connectivity.

**03**

## Identity access

Apps may depend on AD, Entra ID, service accounts or domain controllers.

**04**

## Application validation

Teams must confirm the app stack actually works.

**05**

## Temporary compute

Test VMs may incur cost while running.

**06**

## Cleanup

Test artifacts need to be removed afterward.

**07**

## Evidence collection

Compliance teams often need proof of test results.

**7**

distinct workstreams in a single defensible drill

**\$\$\$**

test compute, networking, and time stack up



Drill skipped → real recovery takes longer

# What are the options?

N2W can replace (or build on) your existing ASR. Start with six questions:

**Q1**

## What's the required RPO?

Determines whether replication is necessary.

**Q2**

## What's the required RTO?

Determines how much orchestration is needed.

**Q3**

## How long must points be retained?

Determines whether backup / archive is required.

**Q4**

## Is the workload cyber-sensitive?

Determines need for immutability and clean rollback.

**Q5**

## Does it need network-aware recovery?

Determines whether environment restore matters.

**Q6**

## Is it dev / test or production?

Determines the appropriate cost level.

# Calculate your backup savings with N2W

Run the numbers for your own environment.



## Azure Cost Savings Calculator Guide

[n2ws.com/blog/fixing-azure-storage-costs](https://n2ws.com/blog/fixing-azure-storage-costs)



## Azure Cost Savings Calculator

[n2ws.com/azure-cost-savings-calculator](https://n2ws.com/azure-cost-savings-calculator)



**Scan to calculate  
your savings**

# Next steps

Currently using ASR or Azure Backup? Talk to us.

- ✓ Which VMs are protected by ASR but may not require low RPO.
- ✓ Workloads that need longer retention with point-in-time flexibility.
- ✓ How to eliminate high monthly licensing fees and optimize retention tiering.
- ✓ Flexible point-in-time recovery for VMs and network configs.
- ✓ Policy-based recovery vs a replication-only mindset.
- ✓ A live view of all protected and unprotected resources.

 **Sign up for a demo**

See how N2W protects any-tier workload.

[n2ws.com/demo](https://n2ws.com/demo)



ALREADY A CUSTOMER?

**Explore N2W v4.6 → [n2ws.com/blog/n2w-v4-6](https://n2ws.com/blog/n2w-v4-6)**