

veeAMON 2023

Ransomware Recovery Unplugged



Rick Vanover

Senior Director, Product Strategy
@RickVanover | **RICKATRON**



Brad Linch

Manager, Enterprise Pre-Sales
@Brad_Linch | www.linchtips.com



Agenda

- Where will you recover?
- What ransomware do we see?
- Four real-world debriefs
- What will you recover from?
- Worst practices to best practices
- Resources for more information



Forms of ransomware

ESXi attacks

Ransomware Detection & Remediation

ESXi Ransomware attack – real use case:

- ESXi Ransomware, ESXi 6.7 update 3 - latest patch
- ESXi hosts and vCenter were on the internal network, nothing exposed
- A Few Webservers in DMZ, Datacenter access via VPN, Edge Firewall
- All Virtual Machine files were encrypted
- All Virtual Machine files were renamed .hjhc2dr
- All Virtual Machines were powered off and could not power on
- Physical Servers were not affected

Veeam Backup Server lost connection to vCenter

- Virtual Machines were restored to a new vCenter and ESXi hosts
- No in-guest infection was detected with another two anti-malware solutions



The last known good backup was the last successful restore point

Time bomb attacks



Encryption attacks



veeAMON2023



Where will you recover?

Design for recovery!

PAST



100%



Restore

3-5%

PRESENT



Backup



Restore

100%

100%

~95% of ALL organizations designed for backup

Why Veeam...

Total **control** over your recovery



Without Veeam

Most companies have limited recovery options, which can cause data loss



With Veeam

The most options for fast recovery after an attack

- Instant Recovery for critical workloads.
- Recover from storage snapshots.
- Recover from replicas.

Recover from multiple platforms



CDP



Replica



Backup



Storage



Reduce risk

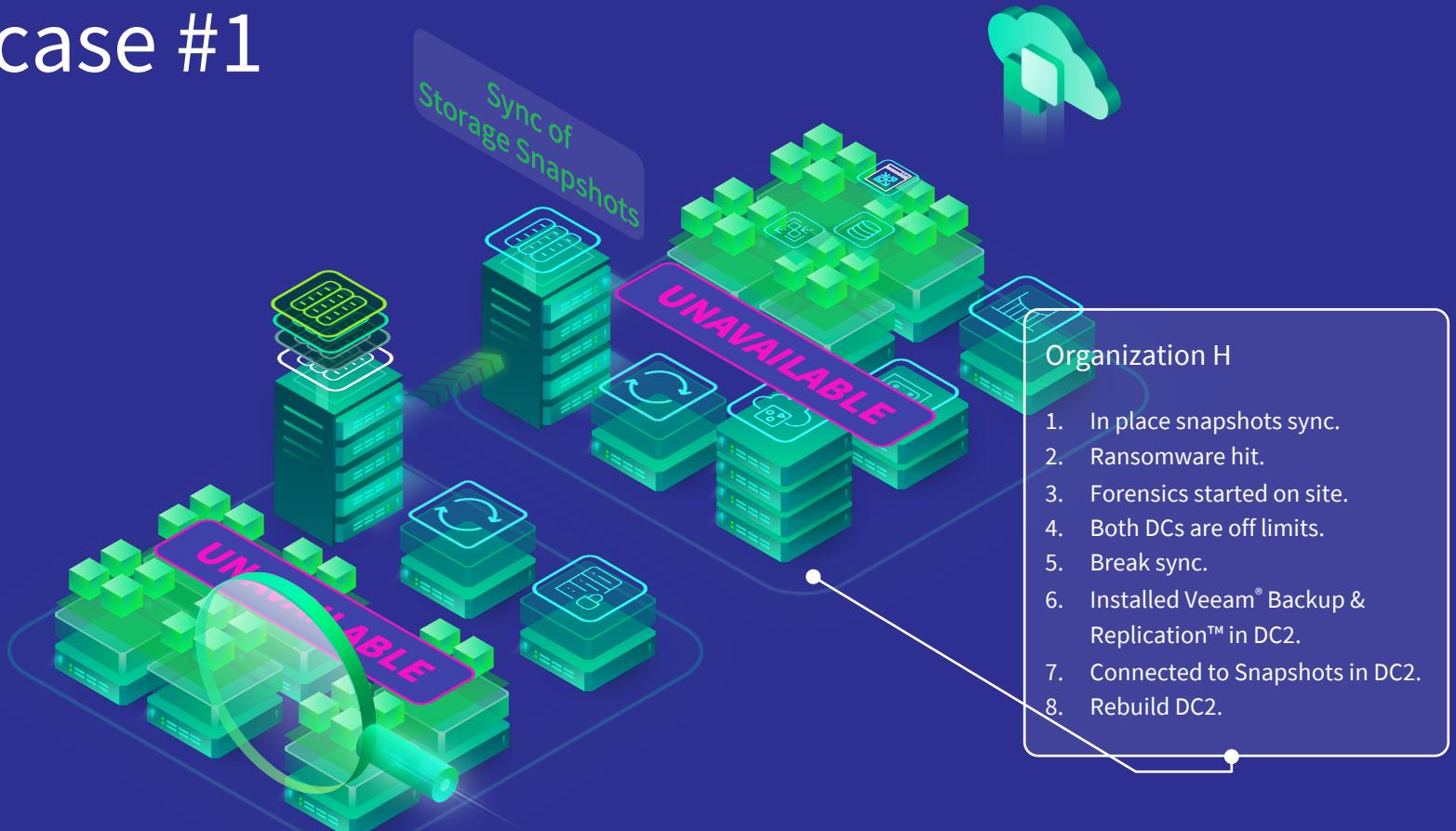


Save time



Restore confidence

Field case #1



Veeam Backup and Replication

VM Tools Home Virtual Machine

Instant Recovery Instant Disk Recovery Guest Files Application Items Restore

Storage Infrastructure

- Storage Infrastructure
 - Pure Storage
 - adcestor09
 - USDEMO/adcestor09-ds2
 - PURE.4627.USDEMO/adcestor09-ds2
 - USDEMO/adcestor09-ds2.VEEAM-ProdSni
 - PURE.4626.USDEMO/adcestor09-ds2
 - USDEMO/adcestor09-ds2.VEEAM-ProdSni
 - PURE.4625.USDEMO/adcestor09-ds2
 - USDEMO/adcestor09-ds2.VEEAM-ProdSni
 - PURE.4624.USDEMO/adcestor09-ds2
 - USDEMO/adcestor09-ds2.VEEAM-ProdSni
 - PURE.4623.USDEMO/adcestor09-ds2

Type in an object name to search for

Name ↑	Host	State
Instant Recovery...	102.usdemo.veeam.local	Crash-consistent snapshot
Instant disk recovery...	104.usdemo.veeam.local	Crash-consistent snapshot
Restore guest files	103.usdemo.veeam.local	Crash-consistent snapshot
Restore application items		

 - Microsoft Active Directory objects...
 - Microsoft Exchange mailbox items...
 - Microsoft SharePoint content...
 - Microsoft SQL Server databases...
 - Oracle databases...

Home Inventory

96+

Storage Integrated
Partners



Veeam Explorer
for Storage Snapshots

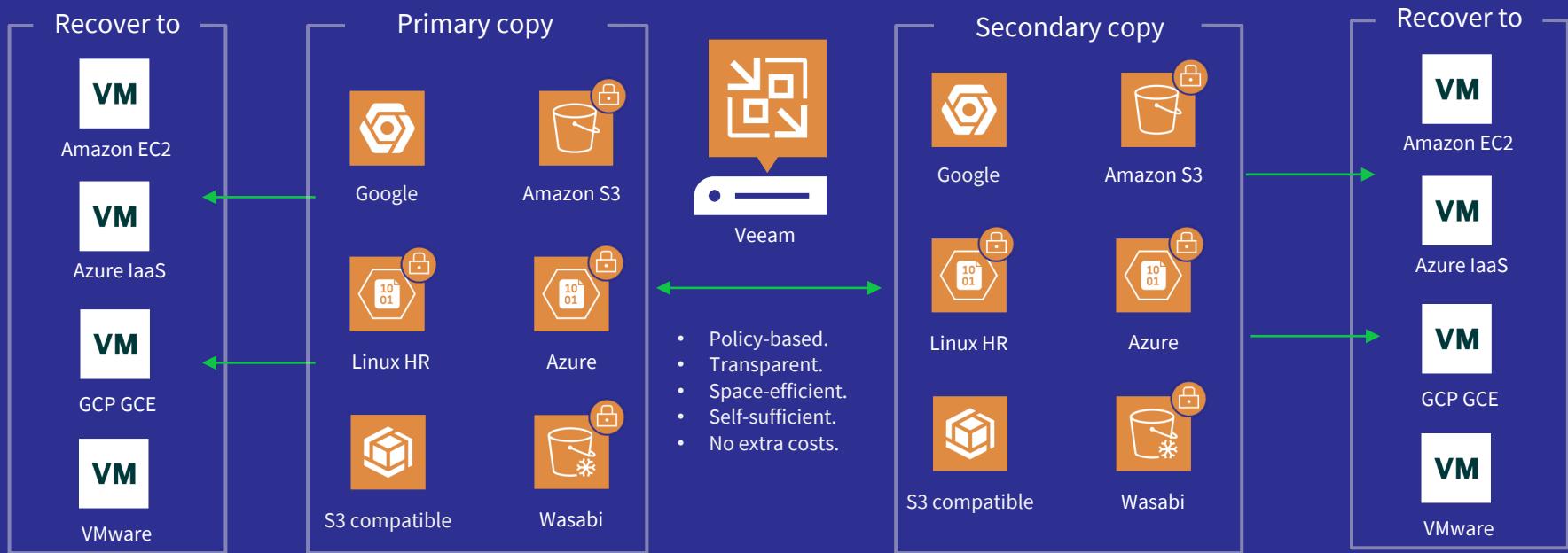
Field case #2



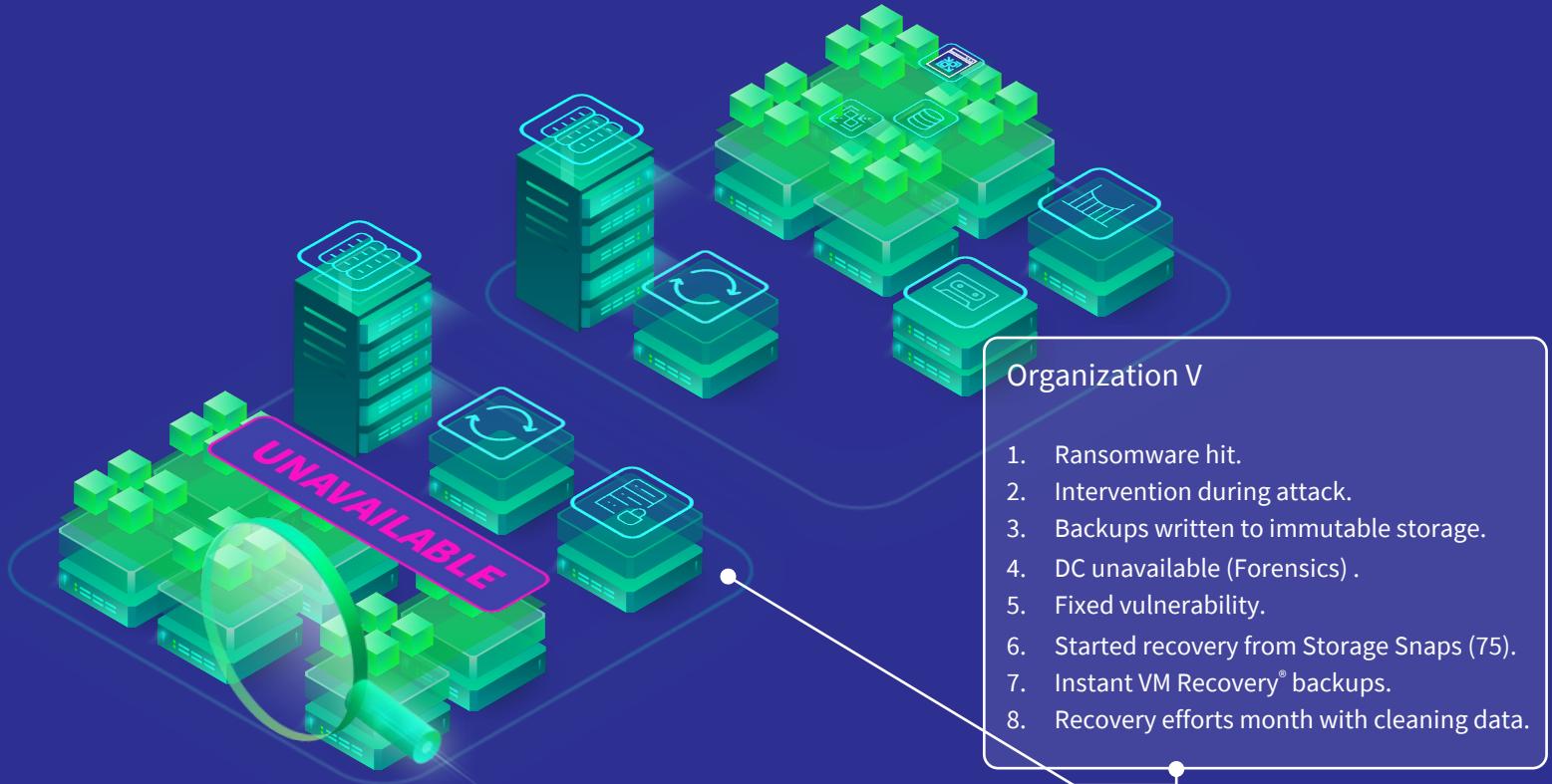
Organization F

1. Ransomware hit.
2. On-premises backups deleted.
3. Primary Veeam Backup & Replication server offline.
4. Turned on Veeam Backup & Replication in Azure.
5. Rescanned offsite copies in Azure.
6. Restored VMs into Azure VMs.
7. Scanned for malware.
8. Back online.

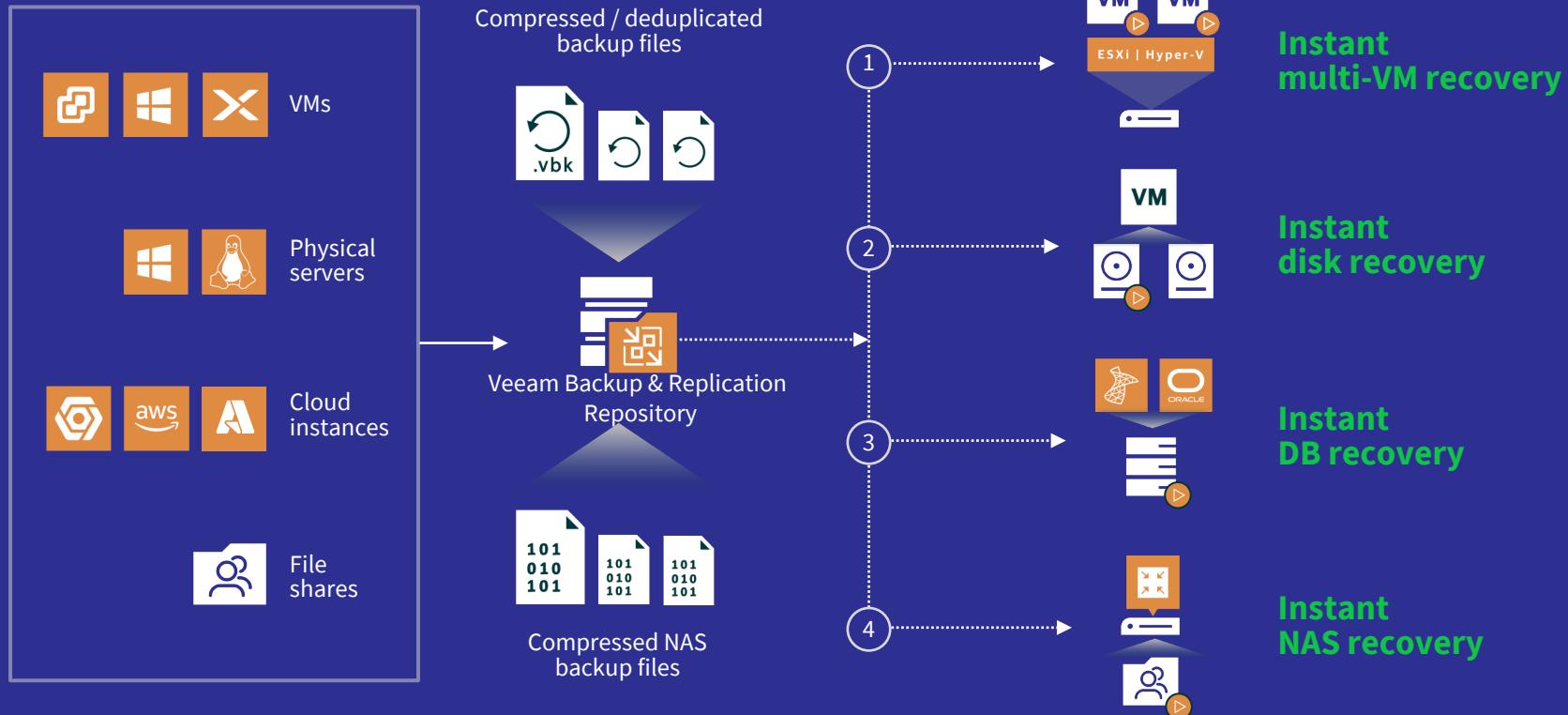
Data mobility



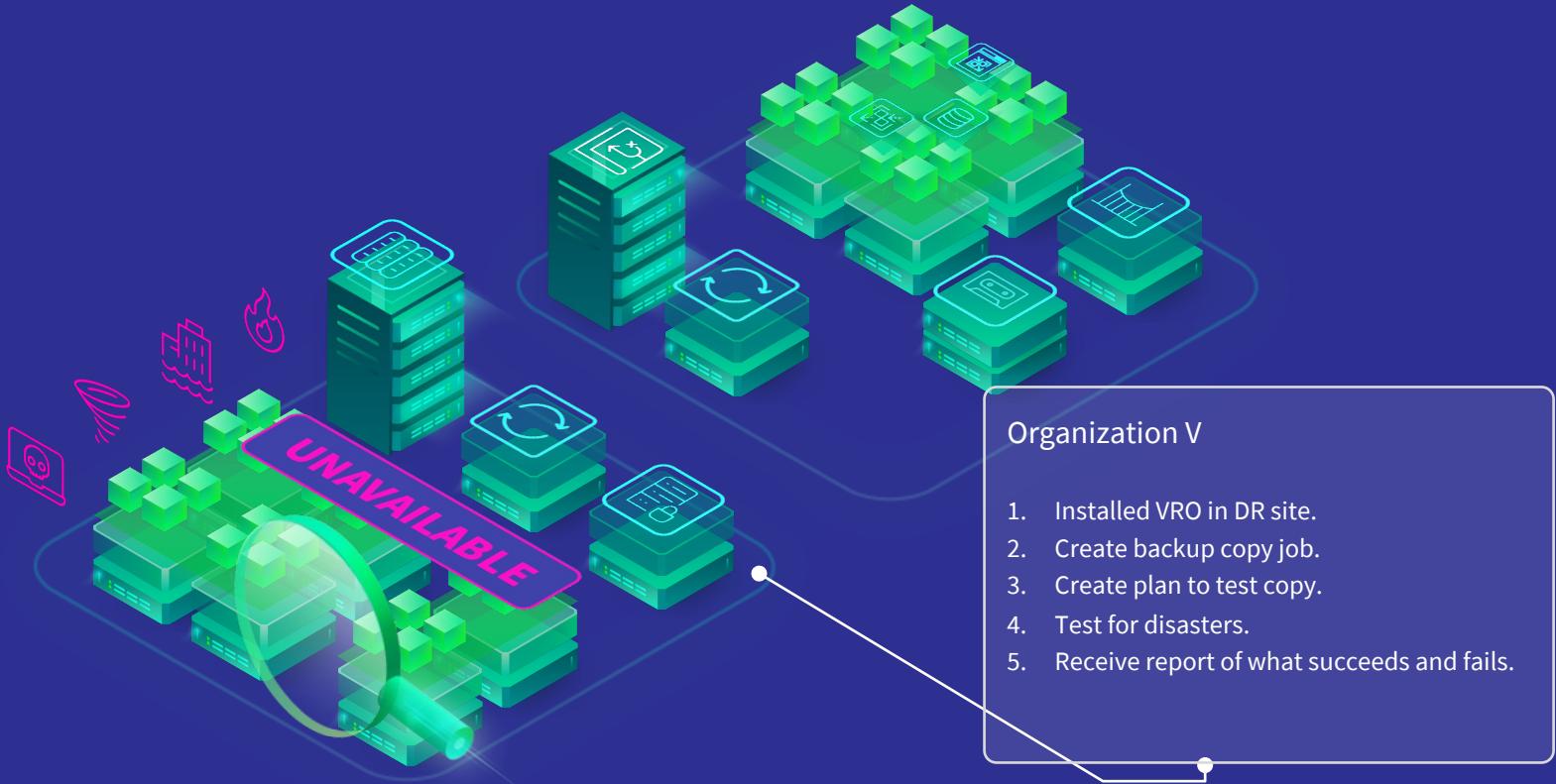
Field case #3



Instant recovery at scale



Field case #4



Clean DR: Veeam Data Platform

Ransomware
scan

Ransomware scan
until clean point

Restore physical, cloud or
virtual after scan

Any CLI scanning SW

No threats detected
Exit code: 0

Plan Details: Restore Agents to ETELLEZ

Plan Type: Cloud Recovery Location: ETELLEZ Lab Restore 72%

Machines - Process 10 in parallel, Halt on error

	Status
GENT01	Running
GENT02	Completed

Steps

Name	Status
Check license and availability	Completed
Create Cloud VM	Running

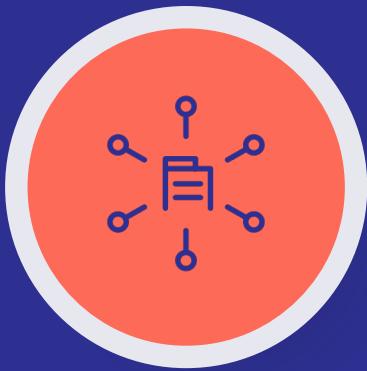
Step Details

Time	Message
8:45:29 PM	[[TBD] Public IP address] [TBD] Cloud VM will be restored without a public IP address
8:45:29 PM	The restored VM will have the name LABAGENT01
8:45:51 PM	[Windows Defender] Antivirus resource has been acquired
8:45:51 PM	Performing antivirus scan for [LABAGENT01]
8:49:03 PM	[Volume{6bbf887b-0000-0000-1000-000000000000}] No threats detected. Exit code: 0
9:16:16 PM	[C] No threats detected. Exit code: 0
9:16:59 PM	Starting restore job
9:17:01 PM	Using Azure proxy ackproxy2.westeurope.cloudapp.azure.com
9:17:01 PM	Queued for processing at 11/14/2022 5:17:01 AM
9:17:01 PM	Processing LABAGENT01
9:17:02 PM	Required backup infrastructure resources have been assigned
9:17:07 PM	Waiting for Azure proxy VM to start
9:17:47 PM	Restoring Disk 0 (100 GB) : 15.9 GB restored at 31 MB/s
9:27:22 PM	Performing conversion
9:29:29 PM	Creating Azure VM

Where will you recover?



Disaster recovery site



Service provider



Cloud

veeAMON 2023



What will you
recover from?



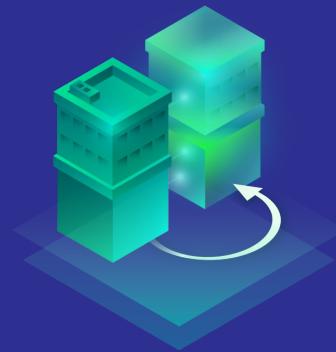
Immutable

\neq



Hardened

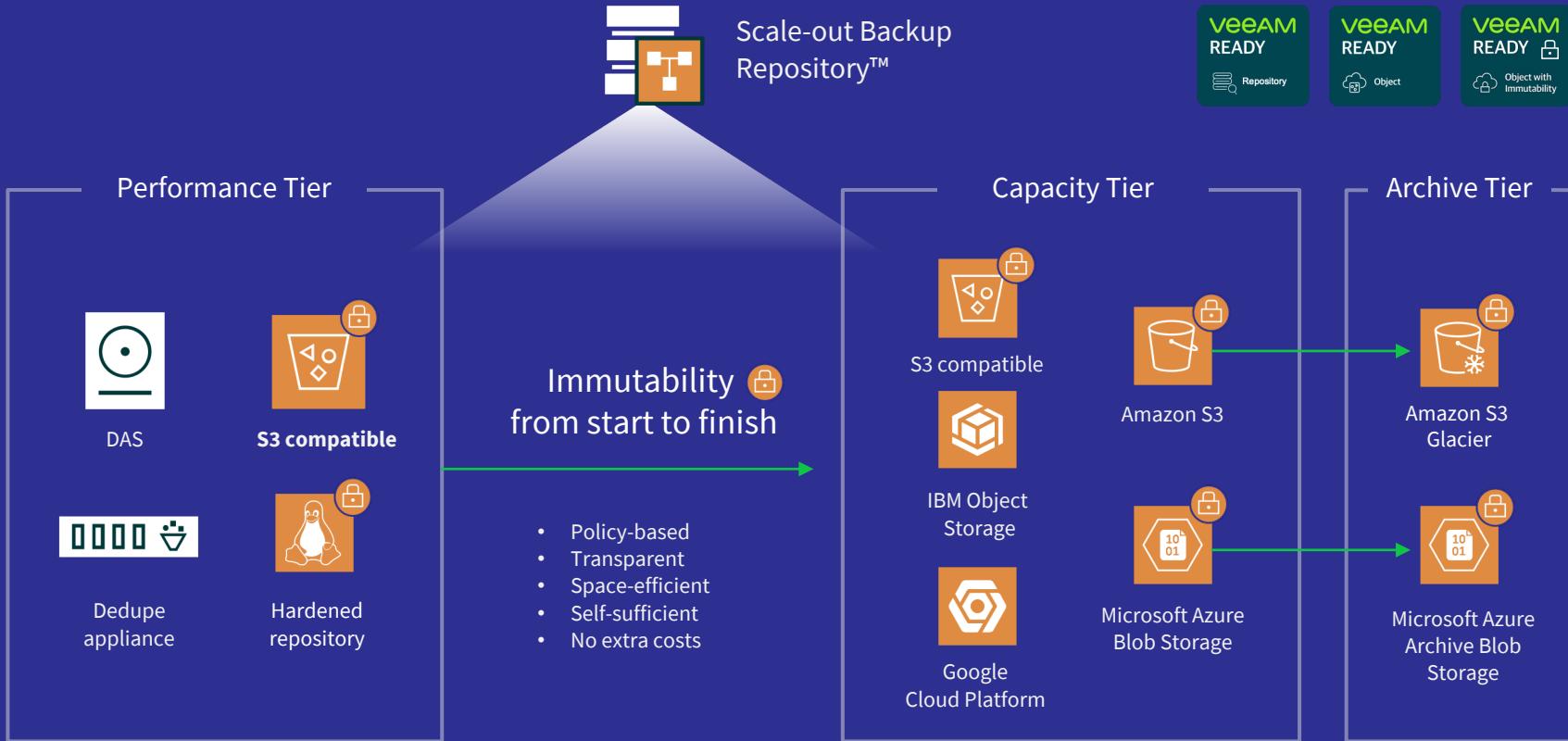
\neq



Air gapped



Flexible immutability options



Ultra resilient media types include....

Veeam Ready Object
with Immutability



Veeam Cloud Connect
with Insider Protection



WORM (Write Once Read Many) –
tape media or tape media
removed/3mm ejected



Veeam Hardened Repository



WORM storage snapshots



Offline, air-gapped media copies
on disk (removable/rotating)



Copies that require
4-Eyes Recovery



Honorable mention:
FC Replication

Caution: replication,
storage snaps

Where will you recover?



Disaster recovery site



Service provider



Cloud

