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

VEEAMON 2023

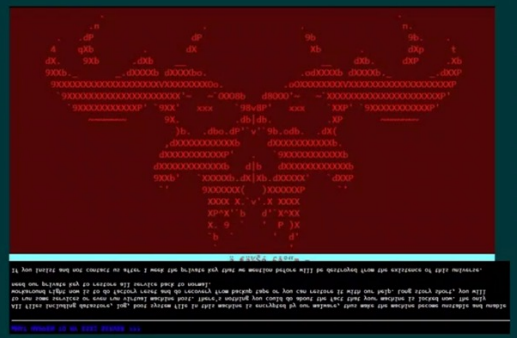
Forms of ransomware

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

VEEAMON 2023

Where will you recover?

Design for recovery!

PAST

Backup **100%**

Restore **3-5%**

PRESENT

Backup **100%**

Restore **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

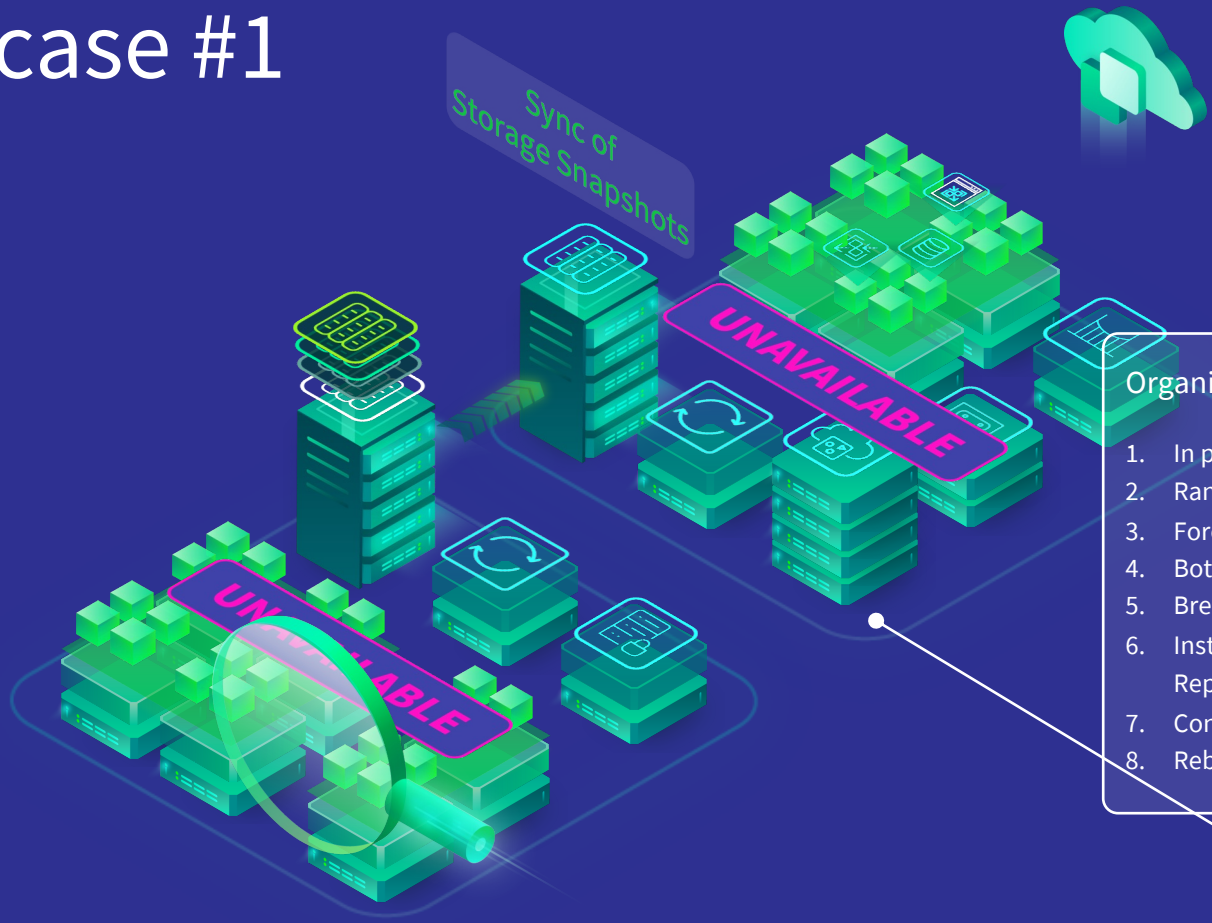
Storage

Reduce risk

Save time

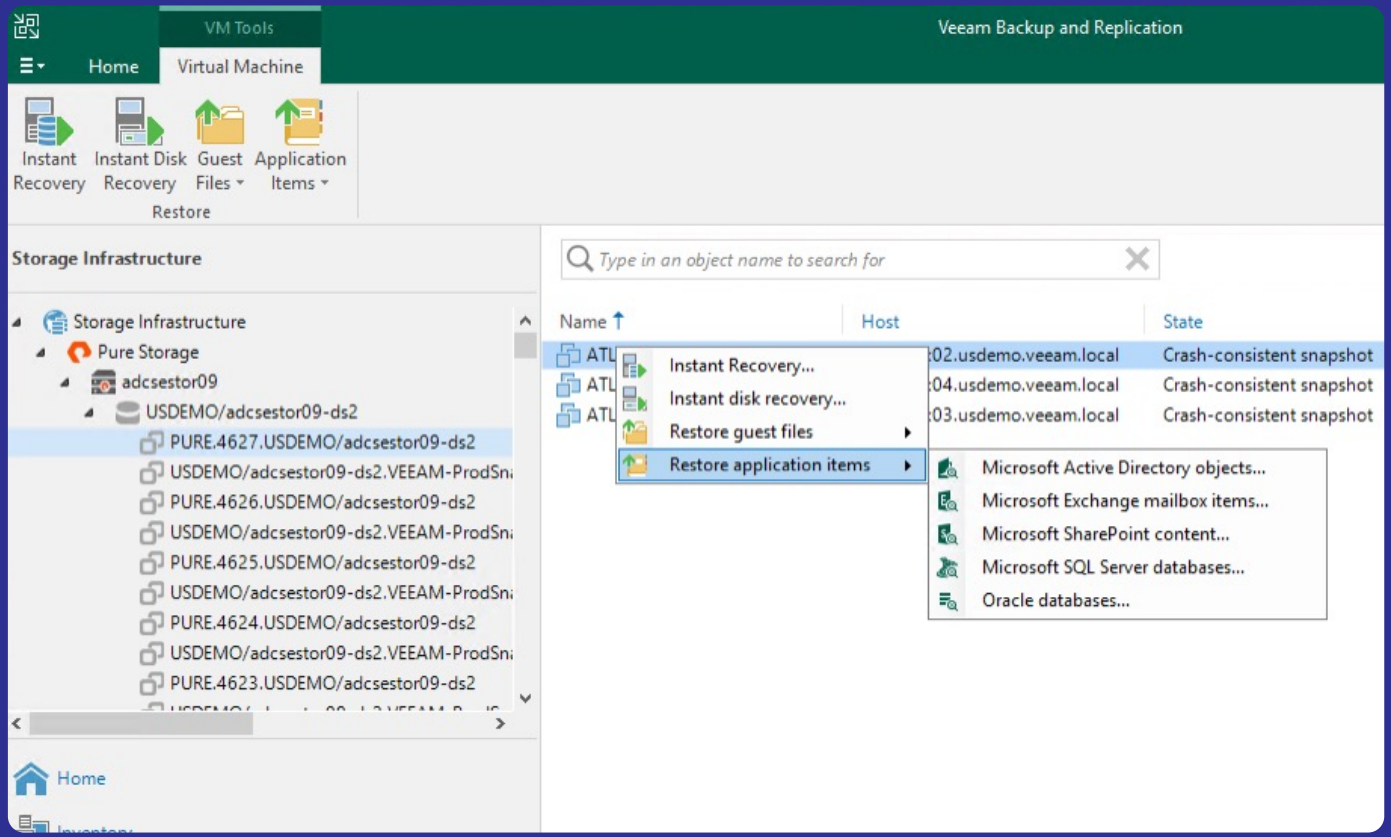
Restore confidence

Field case #1



Organization H

1. In place snapshots sync.
2. Ransomware hit.
3. Forensics started on site.
4. Both DCs are off limits.
5. Break sync.
6. Installed Veeam® Backup & Replication™ in DC2.
7. Connected to Snapshots in DC2.
8. Rebuild DC2.

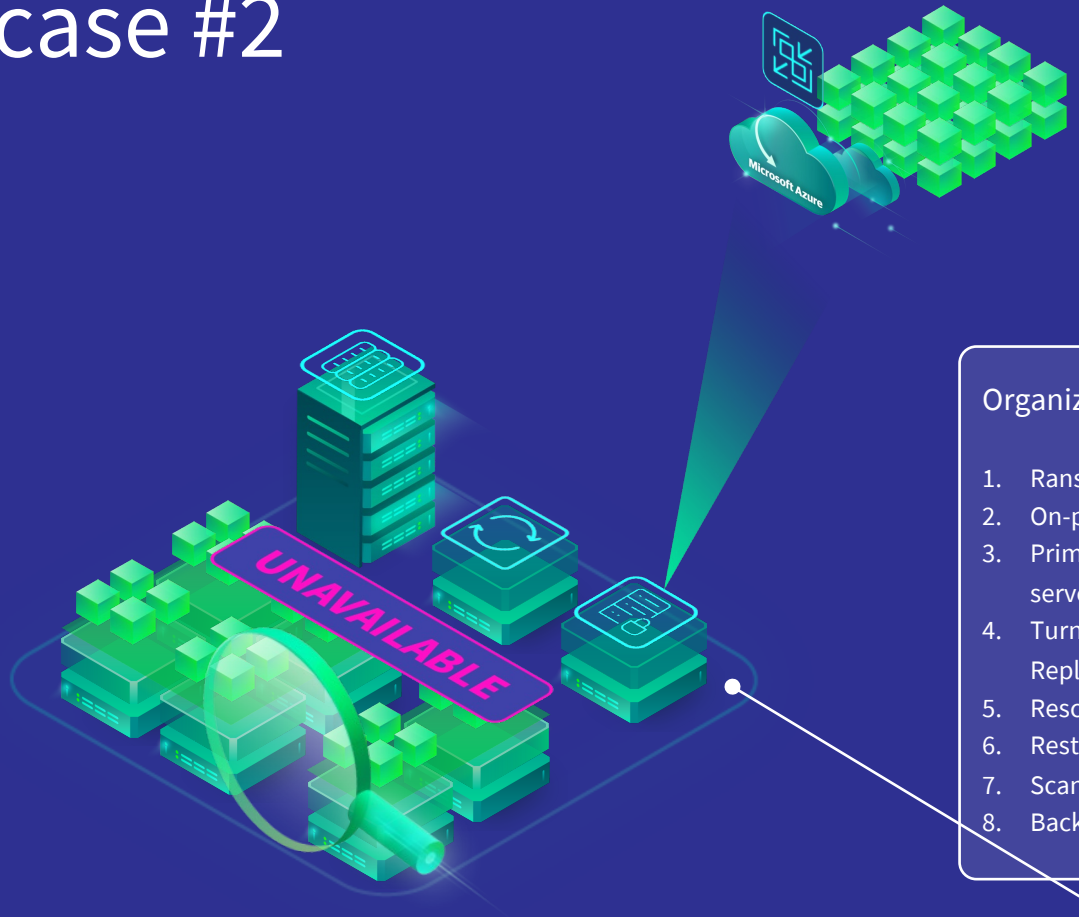


96+

Storage Integrated Partners

Veeam Explorer
for Storage Snapshots

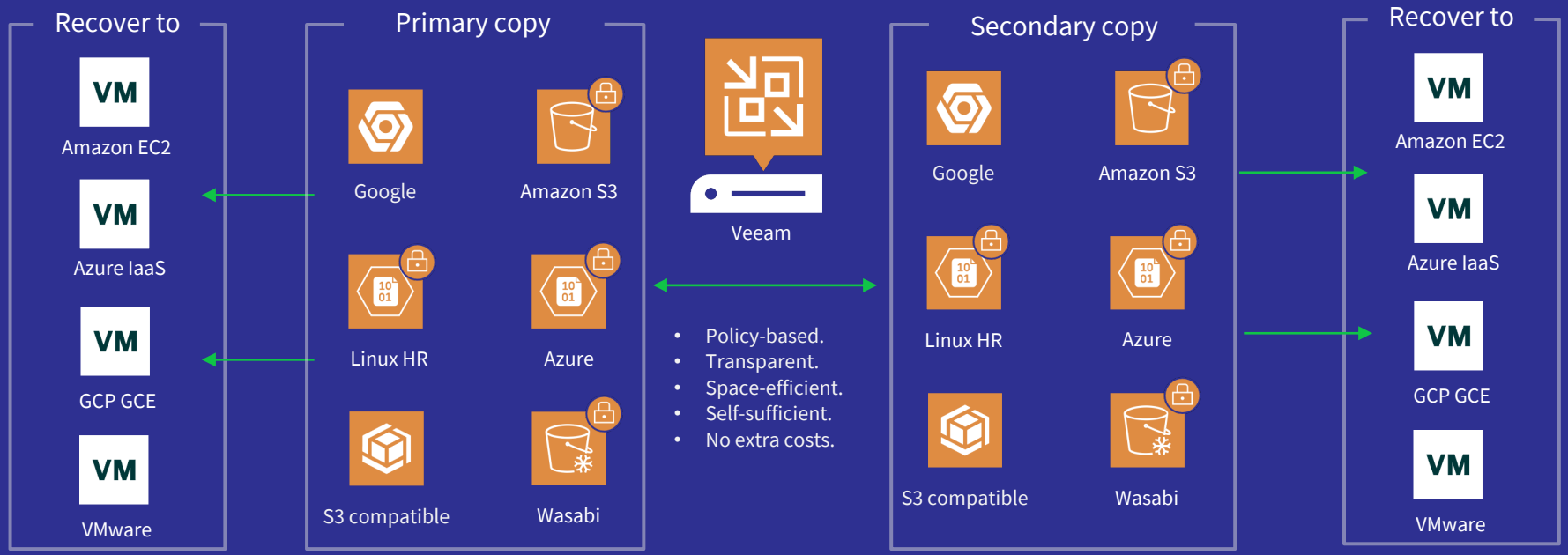
Field case #2



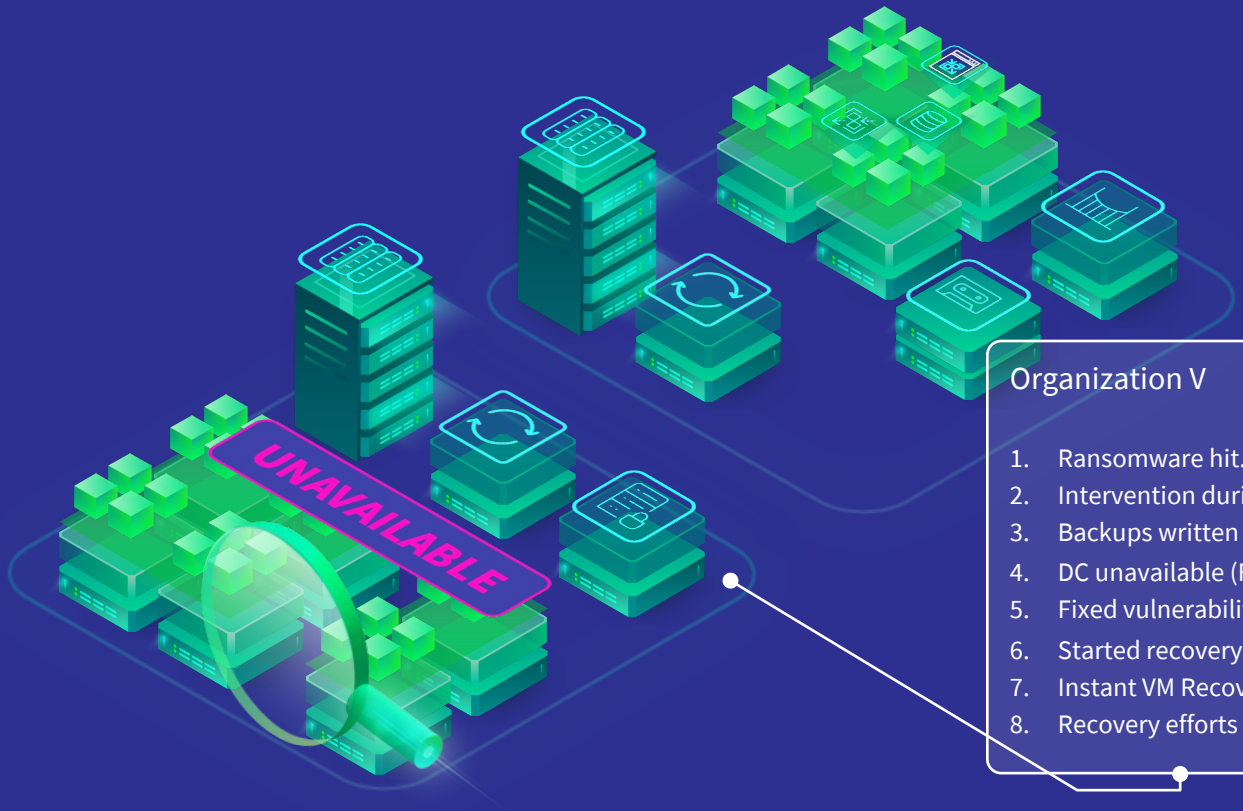
Organization F

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



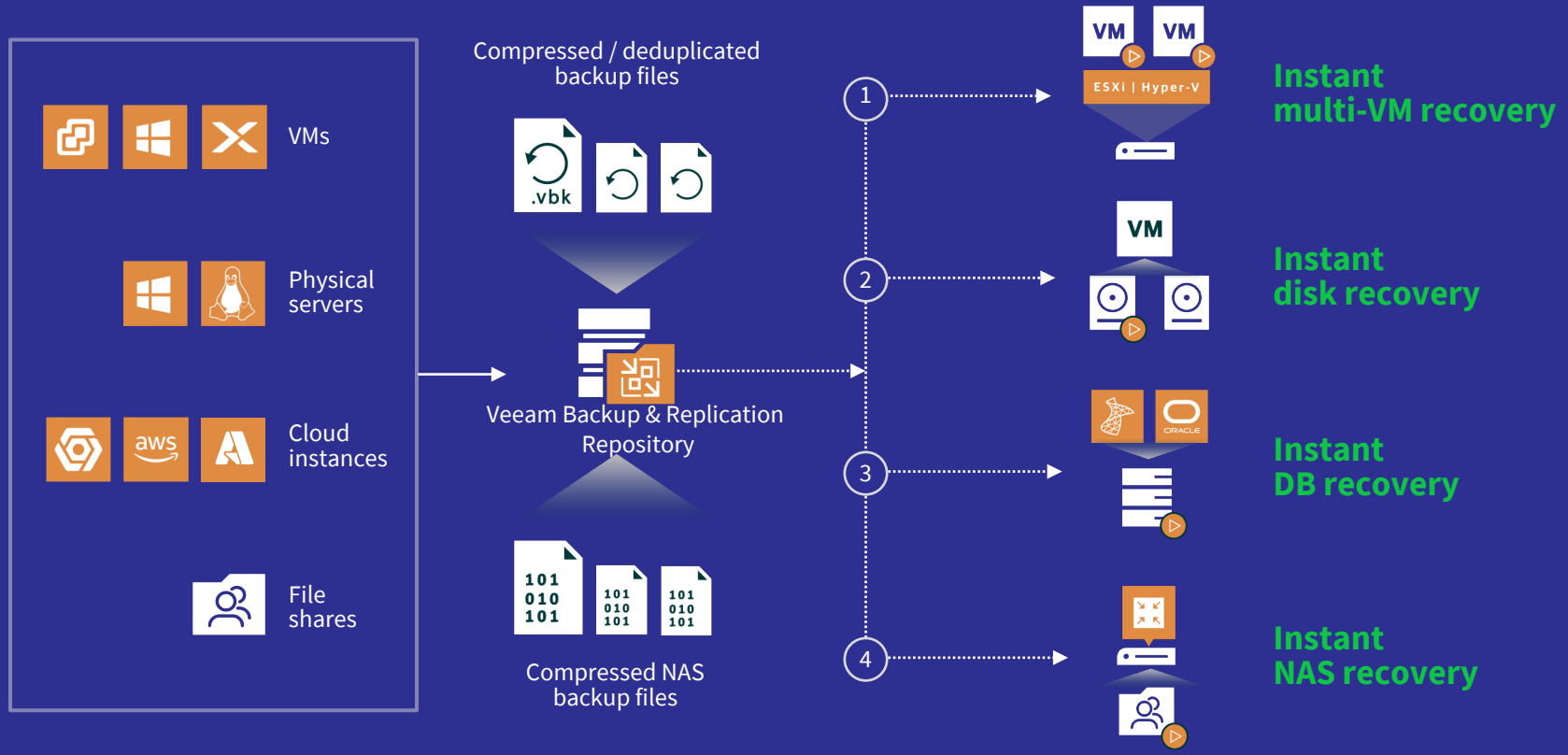
Field case #3



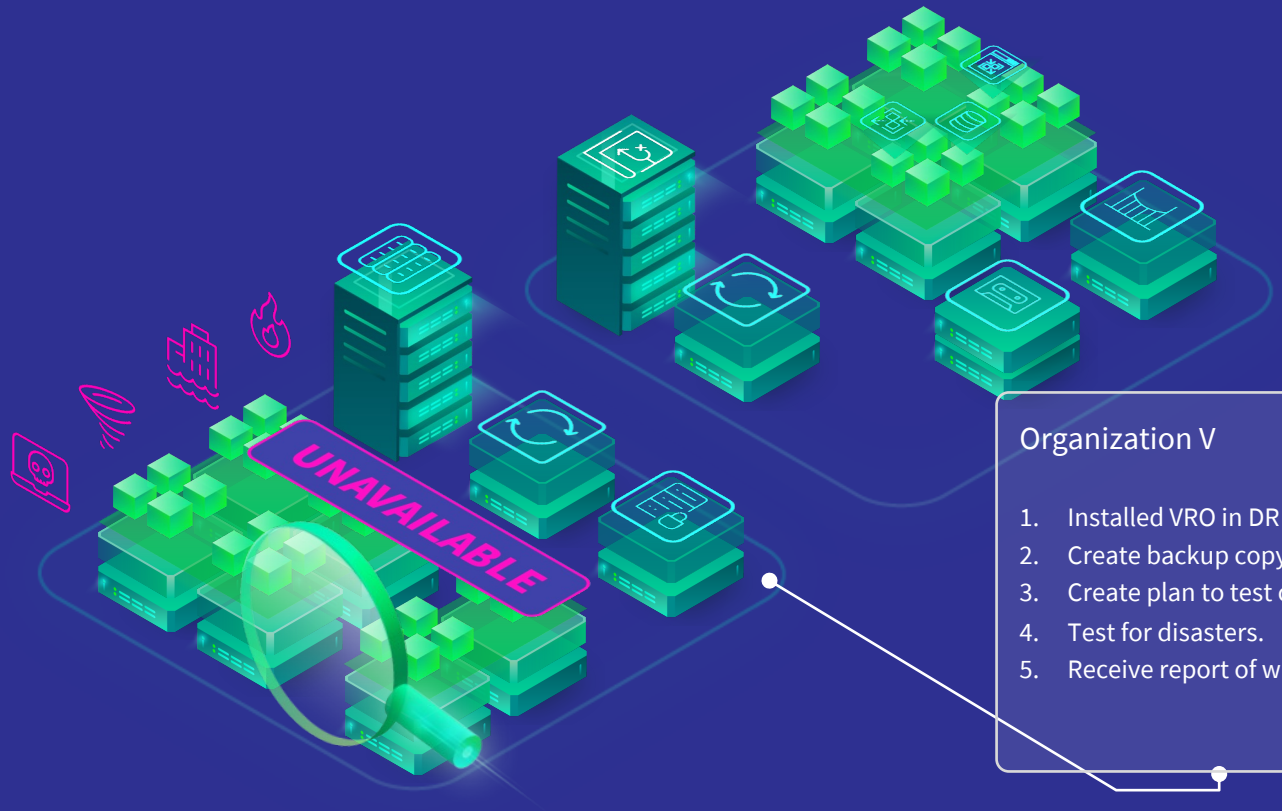
Organization V

1. Ransomware hit.
2. Intervention during attack.
3. Backups written to immutable storage.
4. DC unavailable (Forensics) .
5. Fixed vulnerability.
6. Started recovery from Storage Snaps (75).
7. Instant VM Recovery® backups.
8. Recovery efforts month with cleaning data.

Instant recovery at scale



Field case #4



Organization V

1. Installed VRO in DR site.
2. Create backup copy job.
3. Create plan to test copy.
4. Test for disasters.
5. Receive report of what succeeds and fails.

Clean DR: Veeam Data Platform

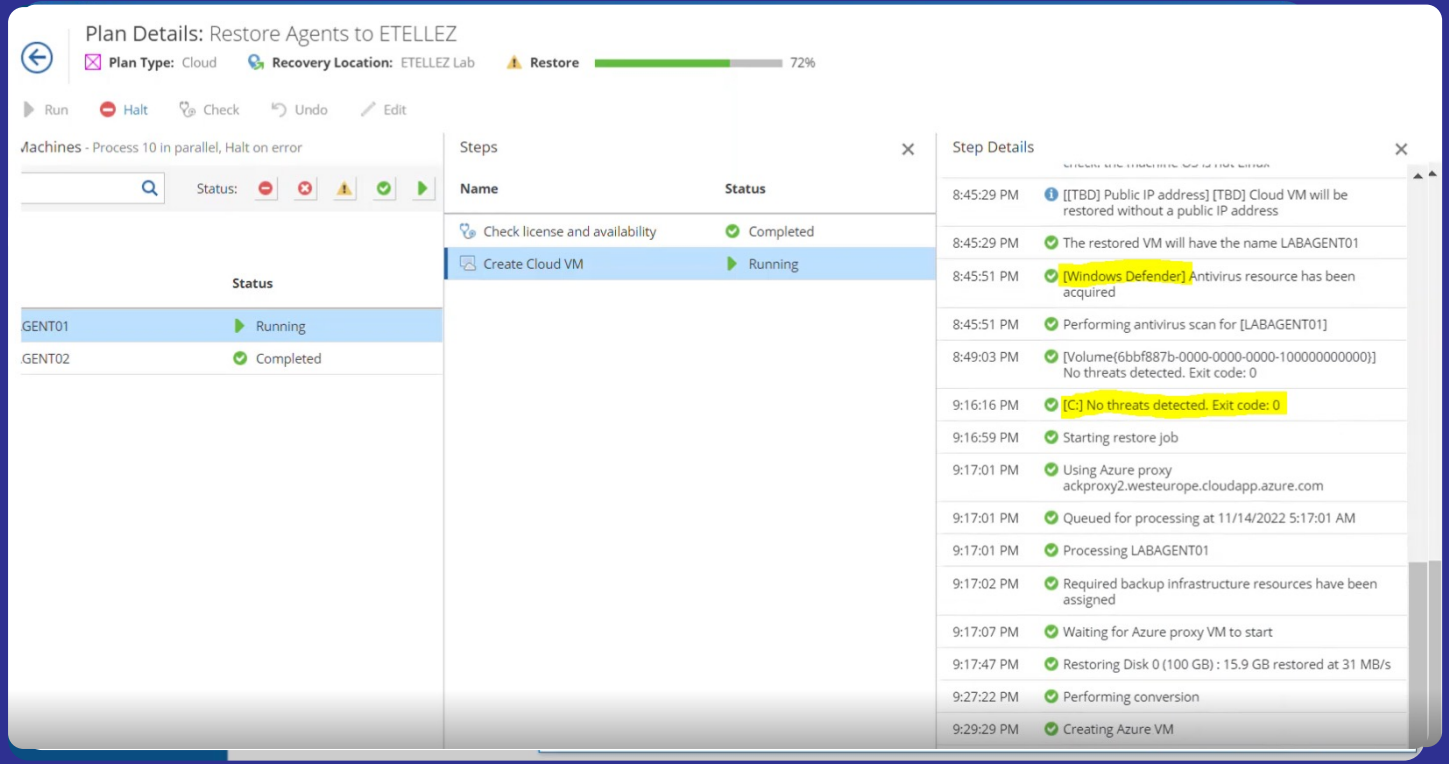
Ransomware scan

Ransomware scan until clean point

Restore physical, cloud or virtual after scan

Any CLI scanning SW

No threats detected
Exit code: 0



Where will you recover?

Disaster recovery site

Service provider

Cloud

VEEAMON 2023

What will you recover from?

Immutable

≠

Hardened

≠

Air gapped

Immutable

+

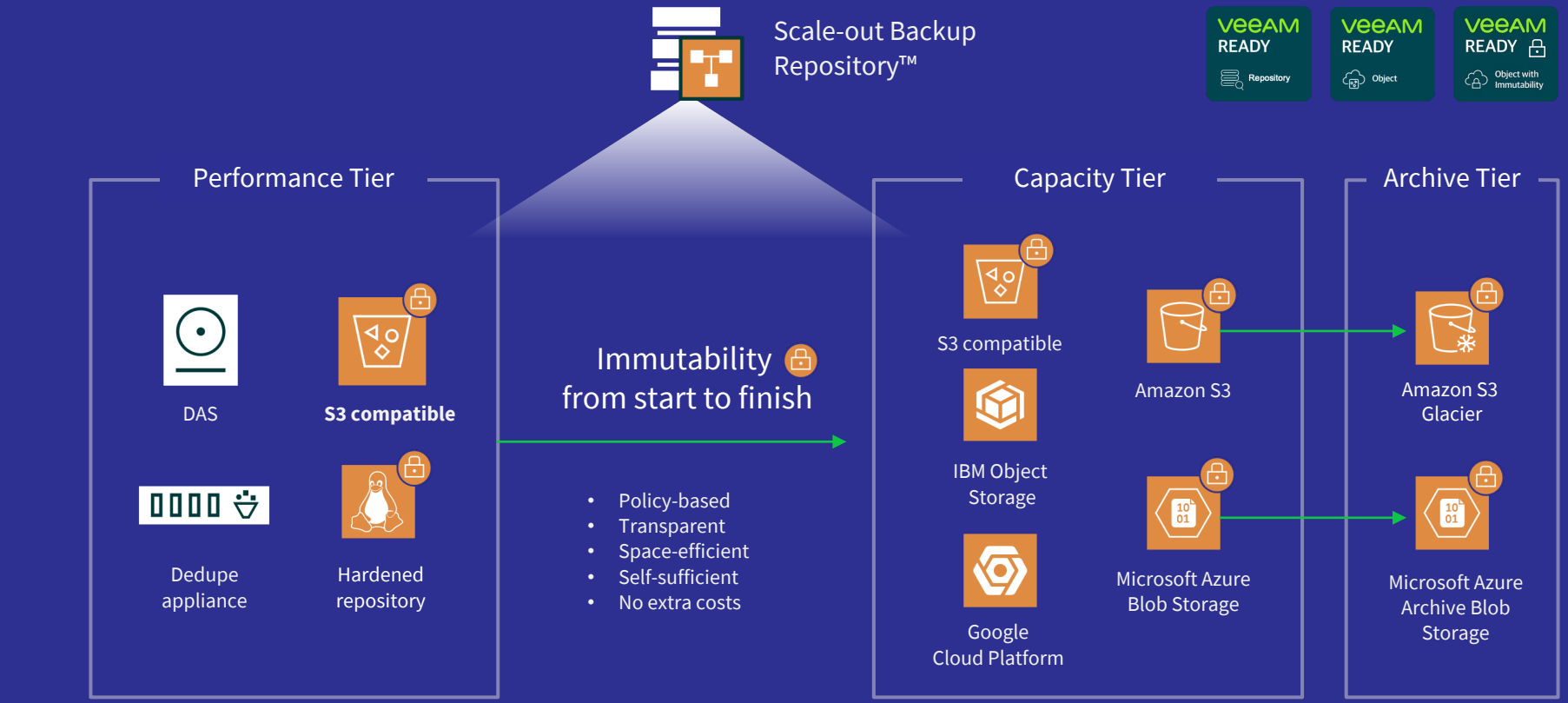
Hardened

+

Air gapped

Secure

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


Thank you
VEEAMON 2023