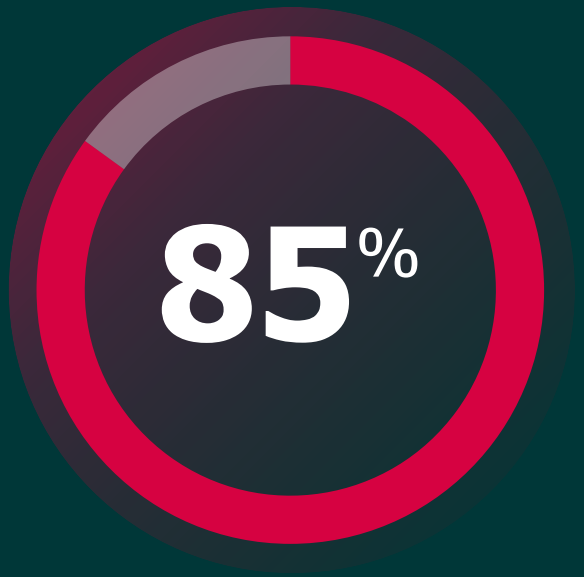
Ransomware protection strategy

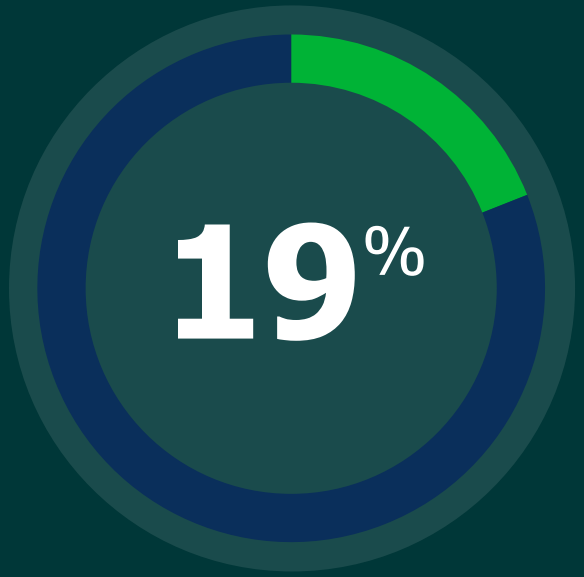
secure your backup with Veeam

Marcin Dudziak
Inside Systems Engineer | Veeam

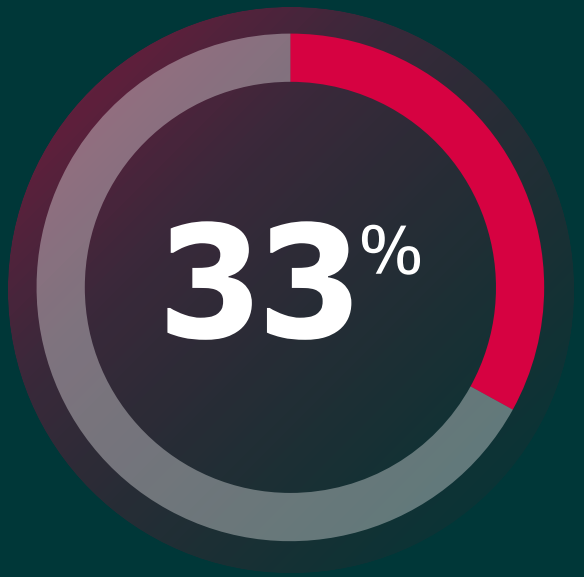
Ransomware is the worst kind of disaster



of companies have experienced at least 1 ransomware attack in the past year*



of companies were able to recover without paying the ransom**



of companies paid the ransom but didn't recover their data

*2023 Veeam Data Protection Report; **2022 Veeam Ransomware Trends Report

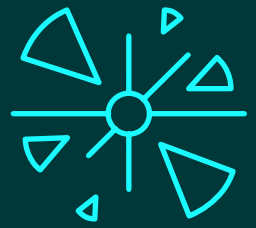
Ransomware is REAL

Ransomware is a

DISASTER

What are you most concerned about with ransomware?

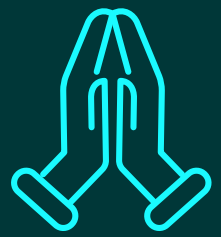
Unable to service customers



Brand damage

Loss of profits

How are you protecting?



Good luck

Anti-malware

Oh, that’s very complex

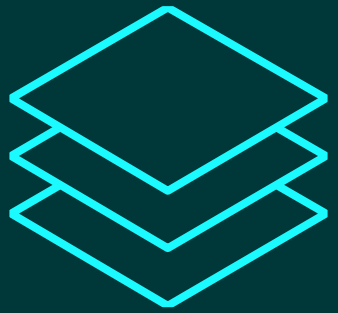
What's your plan in the unfortunate event?

Execute plan

Give up

Pay the ransom

Draw Up Your Battle Plans!



Layered defense!

There is no one magic bullet!

Attackers only need to be right once!

Defenders need to be right all the time!

Secure Backup is your last line of Defense

Data Management Protection Strategy

VEEAM

3 Different copies of data

2 Different media

1 Offsite copy

1 Of which is: offline air-gapped or immutable

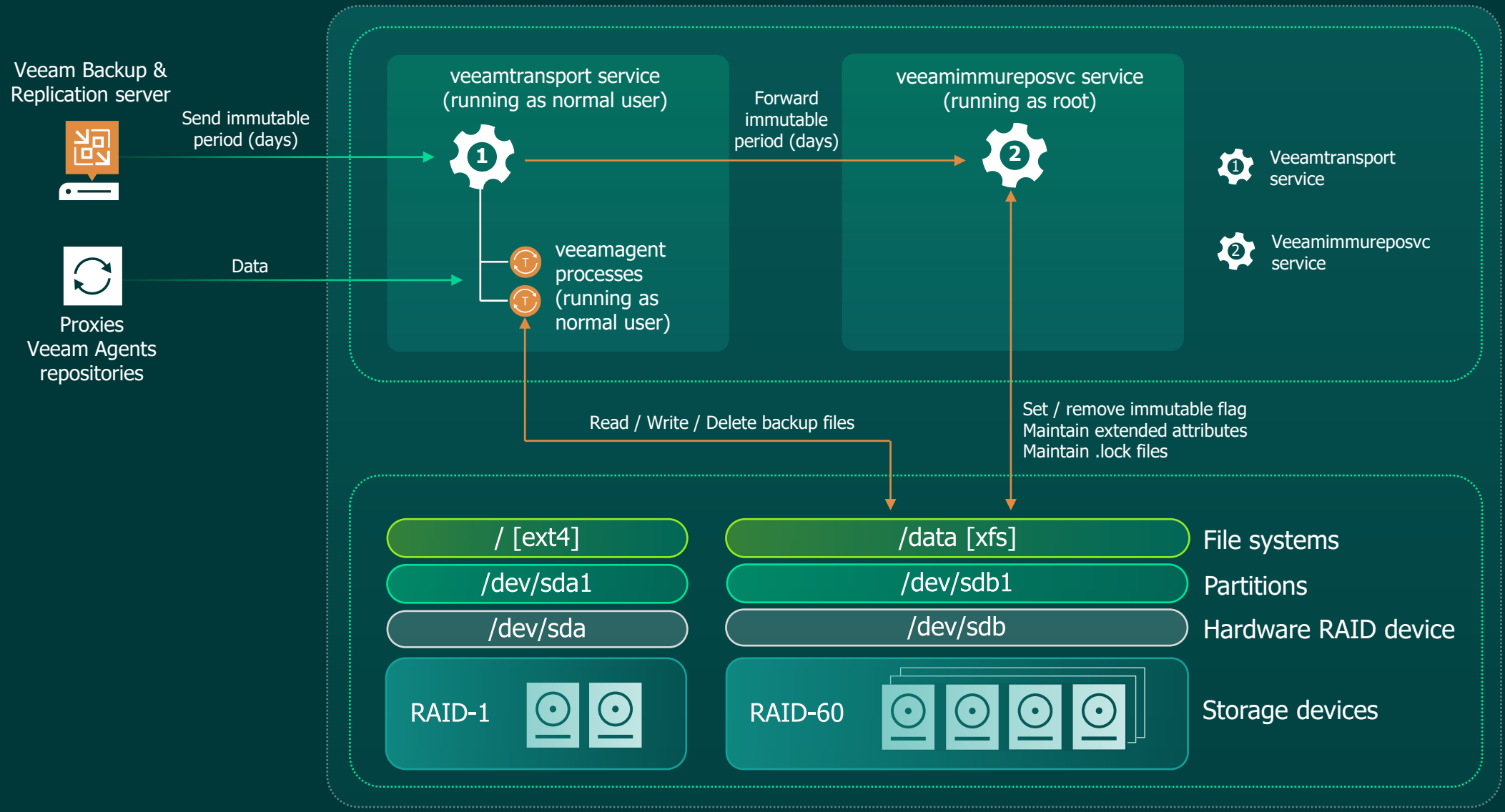
0 No errors after backup recoverability verification

VEEAM PROPARTNER SUMMIT 2022

Offline, Immutable & Air-gapped

Likely the single most effective resiliency technique is to have some form of offline storage tape, removable disk, etc. as an ultra-resilient copy.

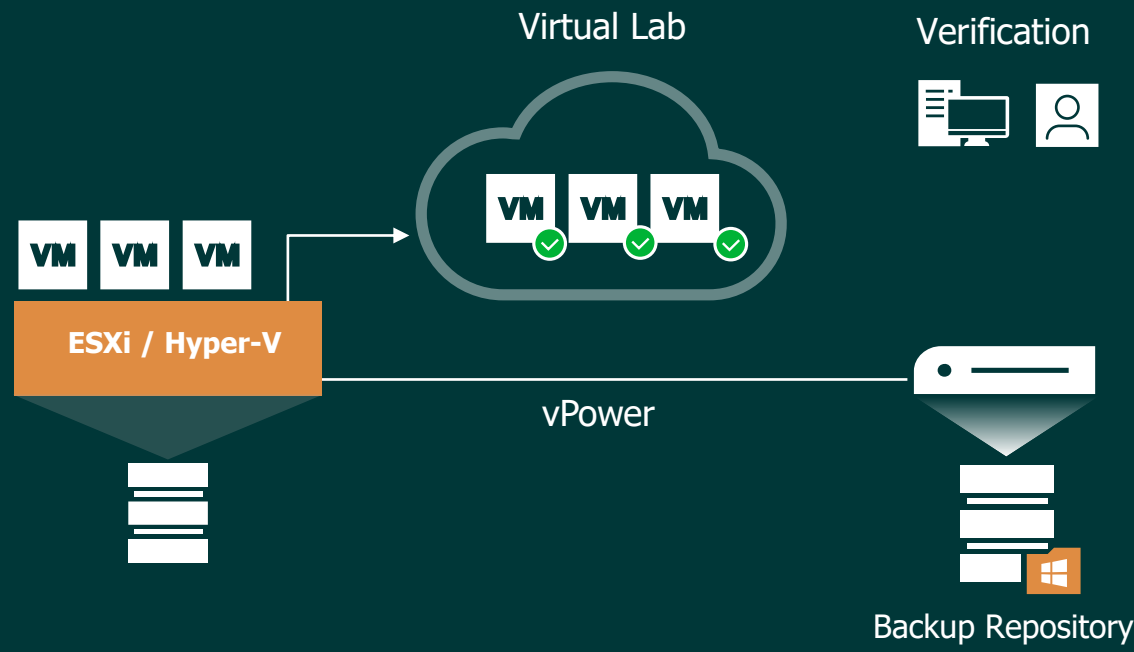
Media type	Characteristic
Tape media	Completely offline when not being written to or read from and WORM
Replicated VMs	Powered off and, in most situations, can be a different authentication framework (ex: vSphere and Hyper-V hosts are on a different domain)
Primary storage snapshots	Can be used as recovery techniques and usually have a different authentication framework
Veeam Cloud Connect backups +Insider Protection	Not connected directly to the backup infrastructure and uses a different authentication mechanism along with different API
Rotating hard drives (rotating media)	Offline when not being written to or read from (similar to tape)
Immutable Backups	Backups in AWS S3, Azure Blob, some S3-Compatible storage and HW appliances can keep backup data immutable
Hardened Linux Repository	Linux immutable flag on Veeam backups


Veeam Backup & Replication server
Send immutable period (days)
Data
Proxies Veeam Agents repositories
veeamtransport service (running as normal user)
Forward immutable period (days)
veeamimmureposvc service (running as root)
veeamagent processes (running as normal user)
Veeamtransport service
Veeamimmureposvc service
Read / Write / Delete backup files
Set / remove immutable flag
Maintain extended attributes
Maintain .lock files
/ [ext4]
/dev/sda1
/dev/sda
/data [xfs]
/dev/sdb1
/dev/sdb
File systems
Partitions
Hardware RAID device
RAID-1
RAID-60
Storage devices

SureBackup

- With SureBackup technology you can automatically verify the recoverability of every backup.

1. Starts VMs in an isolated Datalab environment
2. Performs a set of tests
3. Sends a status report to your mailbox



Create virtual lab → Create application groups → Create SureBackup Job(s) → Specify Tests within the jobs → Schedule SureBackup jobs → Receive verification report

Complete Ransomware Protection

Veeam

Possible Ransomware Activity Alarms

Secure backups

Validated recovery tests

Secure Backup

Immutable Backup Repositories

Protect Veeam backups with built-in HW services like SafeMode, Retention Lock, etc

Fast Restore

Veeam Instant Recovery of critical workloads

Recover from replicas

Recover from snapshots

When you just want to check off the box

Thank you!

VEEAM