The Best Practices of Ransomware Recovery

Chris Wong
Regional Channel Systems Engineer
Veeam

Veeam is the clear market leader

83%

of the Fortune 500 trust Veeam with their data

#1

Market Share in #1 worldwide IDC, 2H2021

200+

Top Industry Awards

450K+

Customers worldwide

HQ in Columbus, Ohio

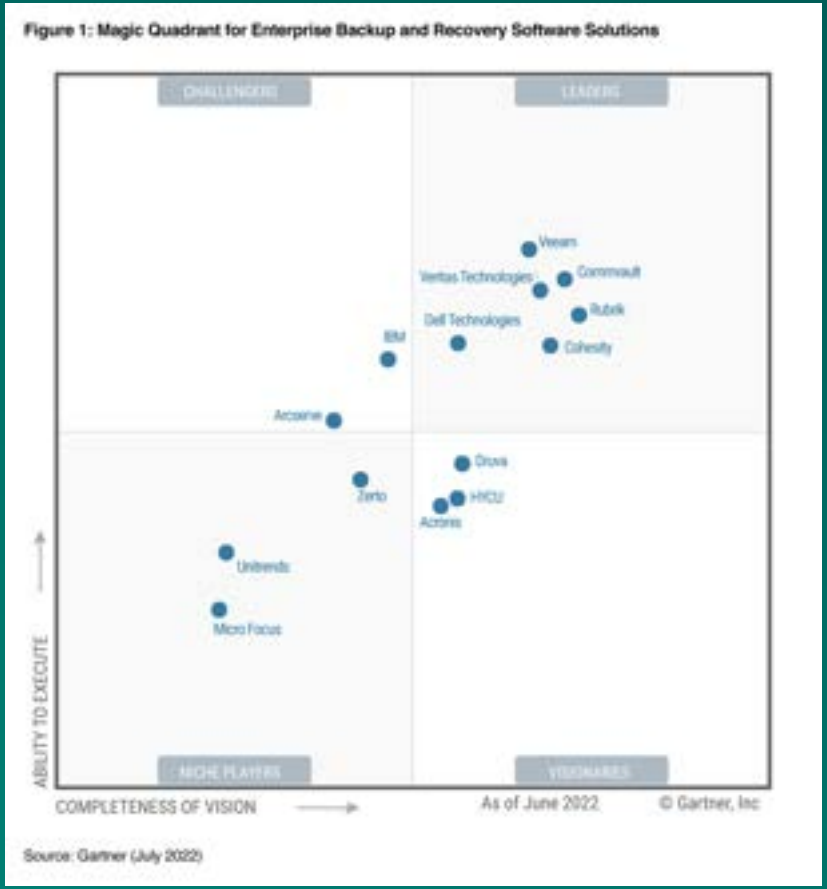
FORRESTER®

"Forrester showcases Veeam as a market leader in Data resiliency solutions (Q3 2019)"

Gartner®

2021 (6 years in a row): "Gartner Magic Quadrant for Data Center Backup and Recovery recognizes Veeam as a Leader."

Veeam named a Leader for the 6th time!



Gartner named Veeam as a Magic Quadrant
Leader for the sixth time
for its highest Ability to Execute and Completeness of Vision

Veeam is a Leader in Enterprise Backup & Recovery Solutions!

#1
Market Share Worldwide

450K+
customers worldwide and counting

200+
top industry awards

DISCLAIMER

Gartner Magic Quadrant for Enterprise Backup and Recovery Software Solutions, Michael Hoeck, Nik Simpson, Jerry Rozeman, Jason Donham, 28th July 2022. Gartner and Magic Quadrant are registered trademarks of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.
This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Veeam. https://www.veeam.com/2022-gartner-magic-quadrant.html Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

VEEAM

Data Protection Trends Report 2022

244

Organizations

1000+

Employees

Hong Kong and Taiwan

The Ransomware Threat

40%

of servers have at least one unexpected outage

60%

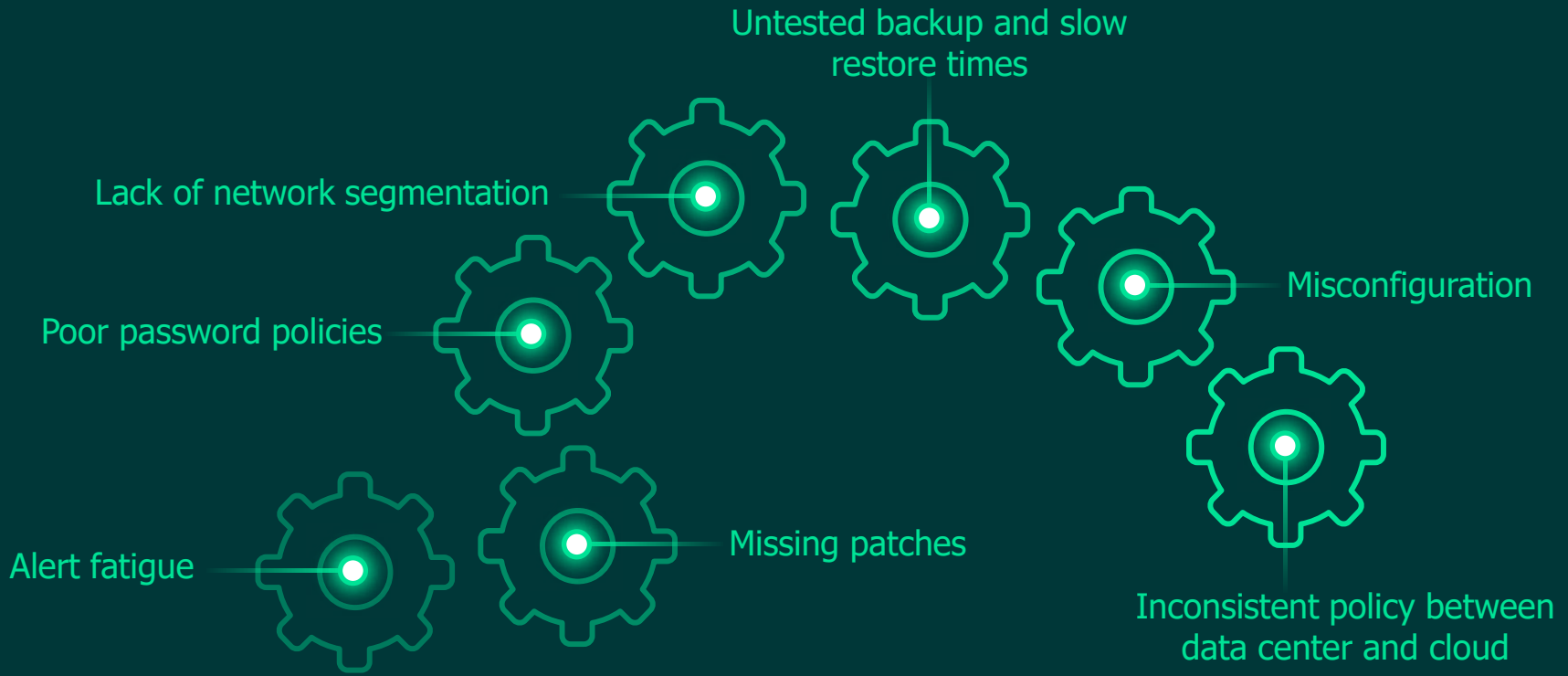
of organizations had outages caused by ransomware

36%

of data on average was unrecoverable after a ransomware attack

Why is ransomware effective?

People, processes, technology



6 Stages of an Advanced Ransomware Attack

Stage 1: Observation

Information is gathered on the victim's people, processes and technology in play

6 Stages of an Advanced Ransomware Attack

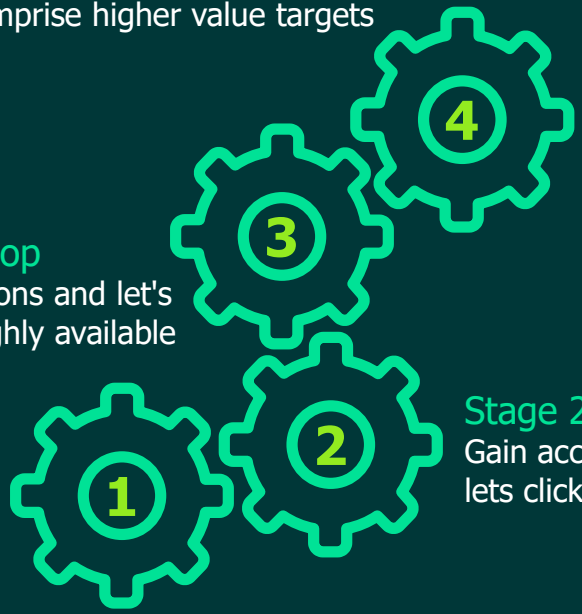
Stage 3: Setting up Shop
Creating a base of operations and let's make it redundant and highly available

Stage 2: Sneak in
Gain access to the victim, lets click a link!

Stage 1: Observation
Information is gathered on the victim's people, processes and technology in play

6 Stages of an Advanced Ransomware Attack

Stage 4: Preparation (30days)
Snooping around without being detected and comprise higher value targets

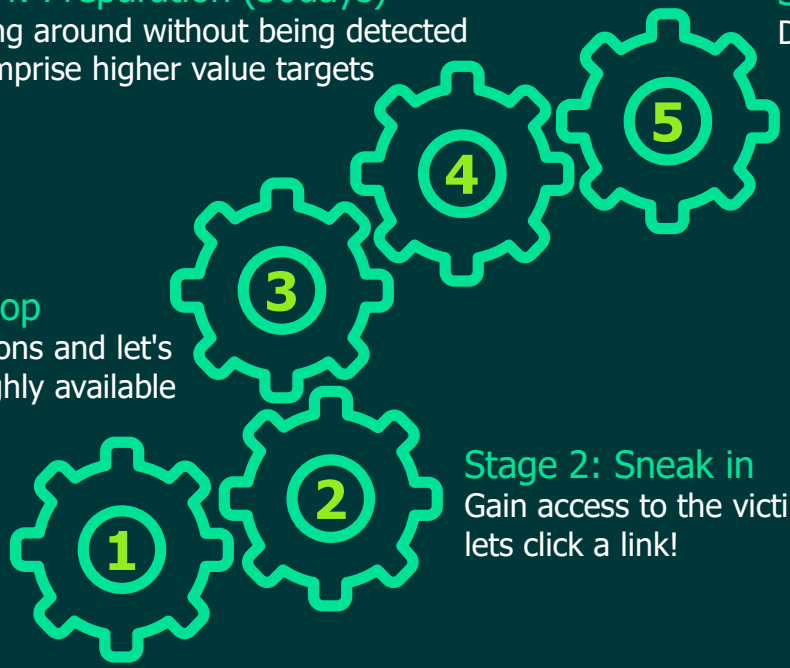


Stage 3: Setting up Shop
Creating a base of operations and let's make it redundant and highly available

Stage 2: Sneak in
Gain access to the victim, lets click a link!

Stage 1: Observation
Information is gathered on the victim's people, processes and technology in play

6 Stages of an Advanced Ransomware Attack



Stage 1: Observation
Information is gathered on the victim's people, processes and technology in play

Stage 2: Sneak in
Gain access to the victim, lets click a link!

Stage 3: Setting up Shop
Creating a base of operations and let's make it redundant and highly available

Stage 4: Preparation (30days)
Snooping around without being detected and comprise higher value targets

Stage 5: Cripple Recoverability
Destroy all the backup copies

VEEAM

6 Stages of an Advanced Ransomware Attack

Stage 1: Observation
Information is gathered on the victim's people, processes and technology in play

Stage 2: Sneak in
Gain access to the victim, lets click a link!

Stage 3: Setting up Shop
Creating a base of operations and let's make it redundant and highly available

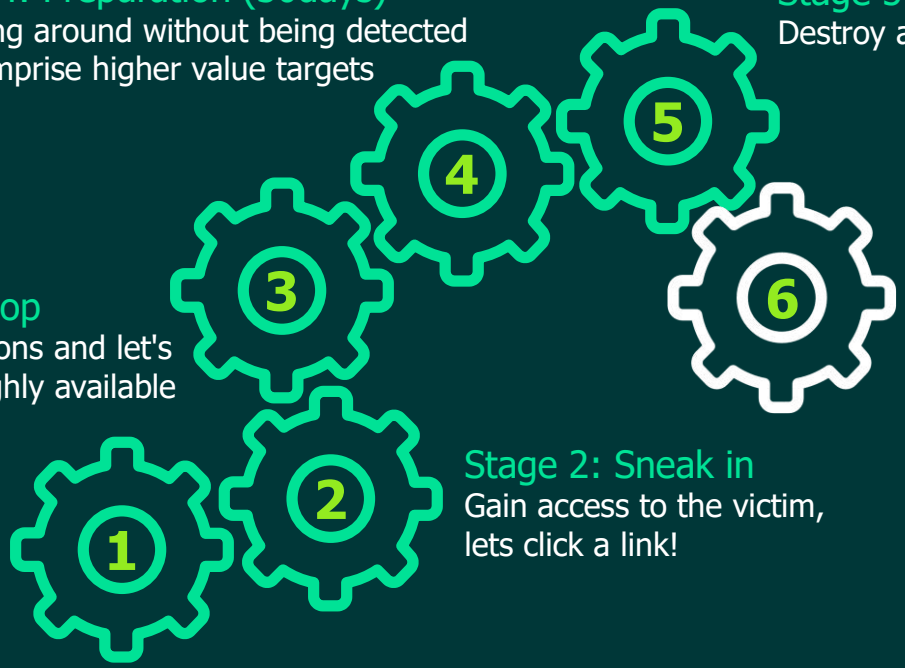
Stage 4: Preparation (30days)
Snooping around without being detected and comprise higher value targets

Stage 5: Cripple Recoverability
Destroy all the backup copies

Stage 6: Ransom Declared!
Encrypt victim's data, wipe archives/backup/data, issue ransom demands!

VEEAM

6 Stages of an Advanced Ransomware Attack



Stage 1: Observation
Information is gathered on the victim's people, processes and technology in play

Stage 2: Sneak in
Gain access to the victim, lets click a link!

Stage 3: Setting up Shop
Creating a base of operations and let's make it redundant and highly available

Stage 4: Preparation (30days)
Snooping around without being detected and comprise higher value targets

Stage 5: Cripple Recoverability
Destroy all the backup copies

Stage 6: Ransom Declared!
Encrypt victim's data, wipe archives/backup/data, issue ransom demands!

VEEAM

Ransom Declared

ClopReadMe.txt - Notepad

File Edit Format View Help

```
Your network has been penetrated.
All files on each host in the network have been encrypted with a strong algorithm.
Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.
We exclusively have decryption software for your situation
No decryption software is available in the public.
DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE readme files.
This may lead to the impossibility of recovery of the certain files.
Photorec, RannohDecryptor etc. repair tools are useless and can destroy your files irreversibly.
If you want to restore your files write to emails (contacts are at the bottom of the sheet) and a
(Less than 5 Mb each, non-archived and your files should not contain valuable information
(Databases, backups, large excel sheets, etc.)).
You will receive decrypted samples and our conditions how to get the decoder.

Attention!!!
Your warranty - decrypted samples.
Do not rename encrypted files.
Do not try to decrypt your data using third party software.
We don`t need your files and your information.

But after 2 weeks all your files and keys will be deleted automatically.
Contact emails:
[redacted]
or
[redacted]

The final price depends on how fast you write to us.

Clop
```

The Best Practices of Ransomware Recovery

Immutable Backup

Backup Data should not be able to modify or erased during the retention period.

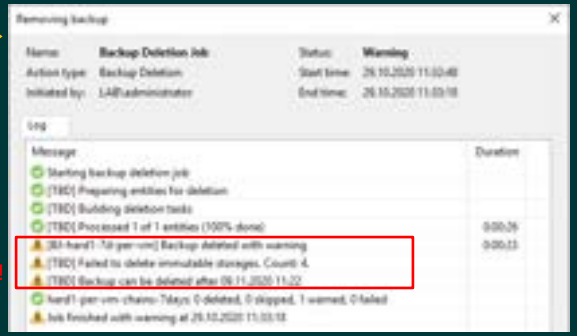
Veeam 's suggestions

- Make use Veeam 's hardened Linux repository (WORM Storage)
- Software feature, no additional costs

Hacker

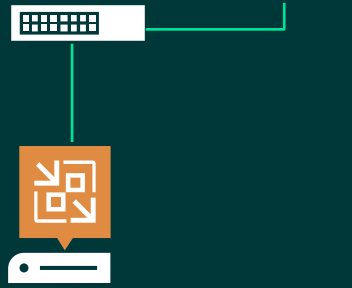
Access Veeam Console via Privileged Account

Try to DELETE the backup images



DELETE failed!!

Immutable Linux Repository



Backup server Console

- SEC 17a-4(f), FINRA 4511(c) and CFTC 1.31(c)-(d)

Best practices for ransomware protection

3

Three different copies of data

2

Two different media

1

One offsite copy

VEEAM

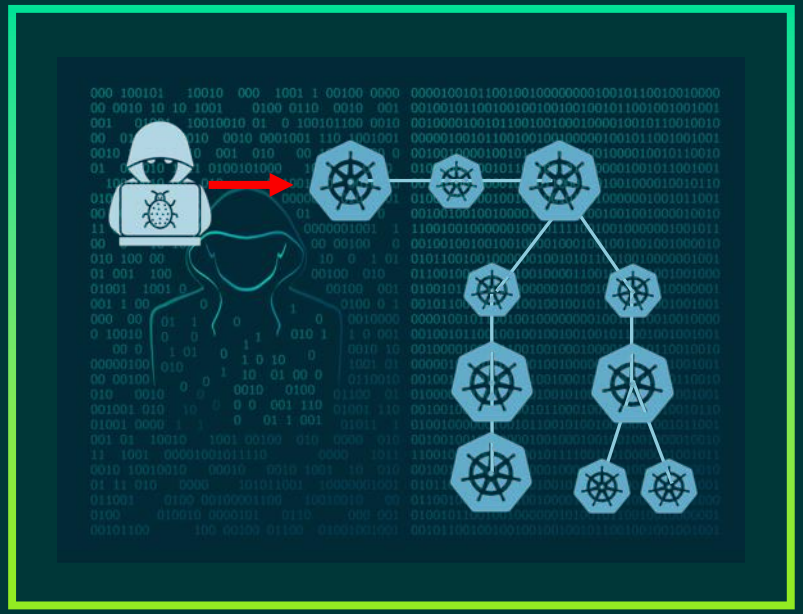
1

Of which is: offline air-gapped or immutable

0

No errors after automated backup testing & recoverability verification

Don’t skip your containers backup



Kubernetes Security Issues: Nearly a Million Instances Exposed on Internet

Julien Maury June 29, 2022

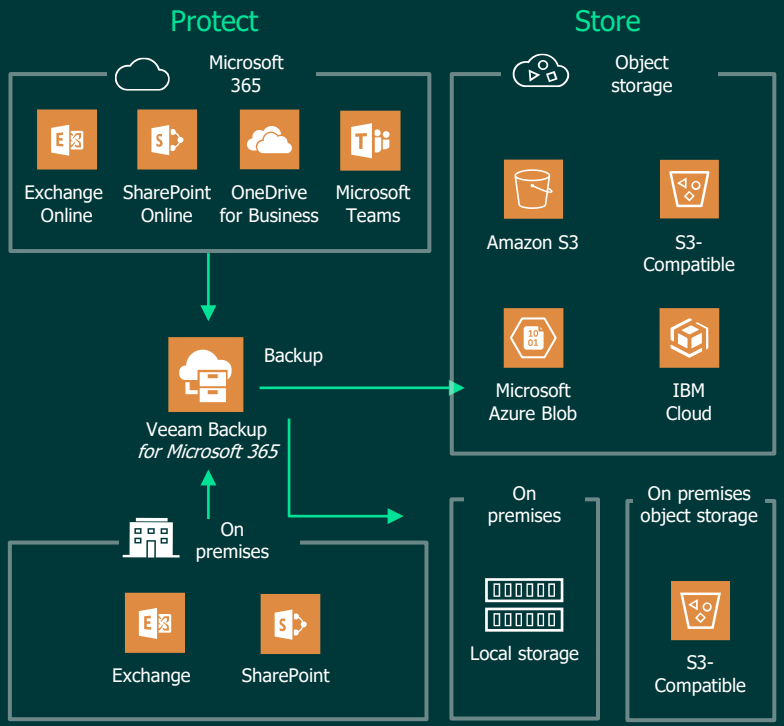
```
HTTP/1.1 401 Unauthorized
Content-Type: application/json
Www-Authenticate: Basic realm="kubernetes-master"
Date: Tue, 21 Jun 2022 11:13:29 GMT
Content-Length: 165
```

Cybersecurity researchers have found more than 900,000 instances of Kubernetes consoles exposed on the internet.

Cyble researchers detected misconfigured Kubernetes instances that could expose hundreds of thousands of organizations. The researchers found a number of indicators of exposure in the open source container orchestration platform

Source: https://www.esecurityplanet.com/applications/kubernetes-exposed-on-internet/

Regain control of Your Microsoft 365 data



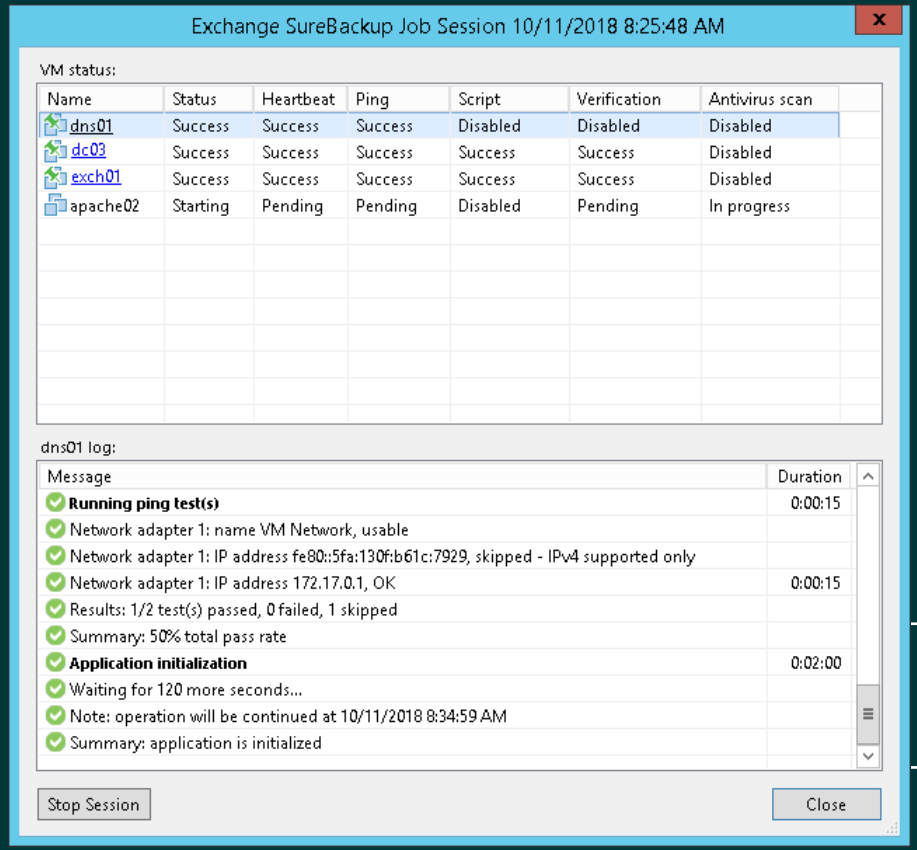
I thought SaaS cannot be attacked ?

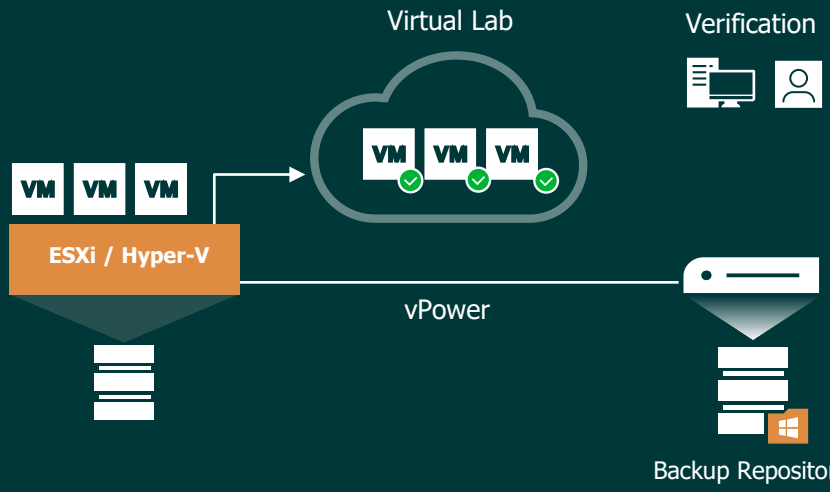
Malicious software through API

VEEAM

Make a backup copy to your datacenter or cloud storage

Automated Verification

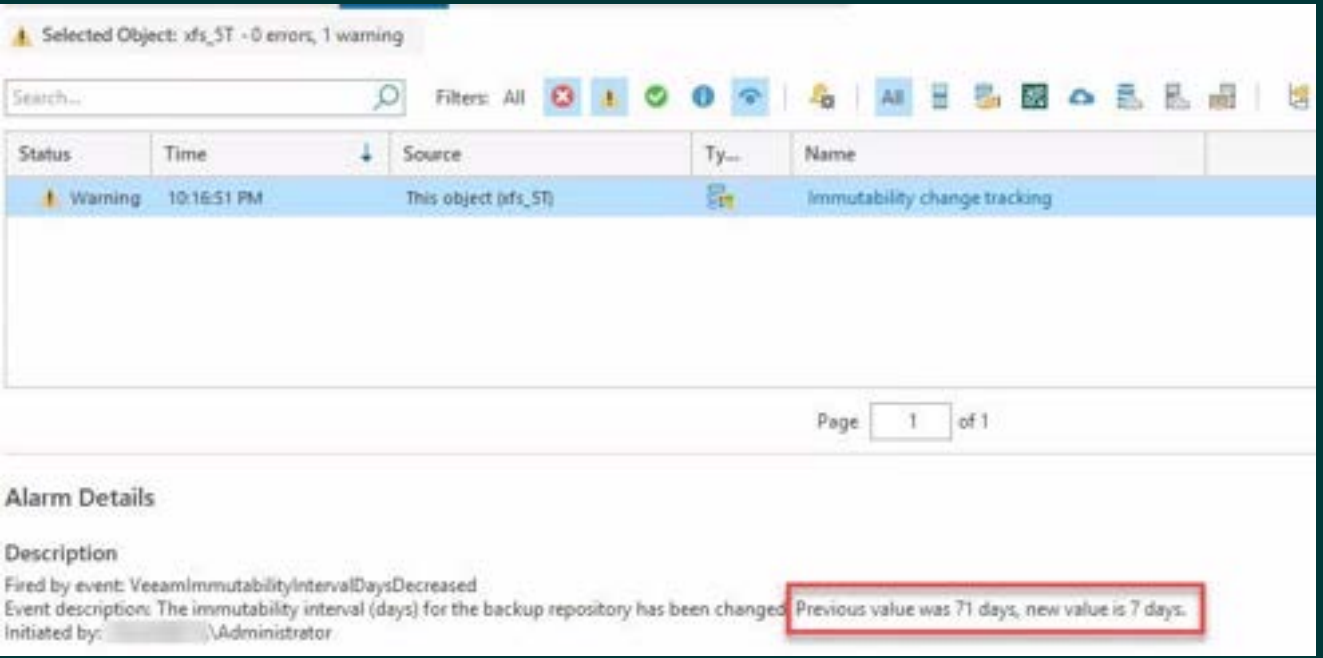




Specify Tests within the jobs → Schedule SureBackup jobs → Receive verification report

VEEAM

Any unprotected VMs?



Unexpected Changes ?

How fast is your restore ?

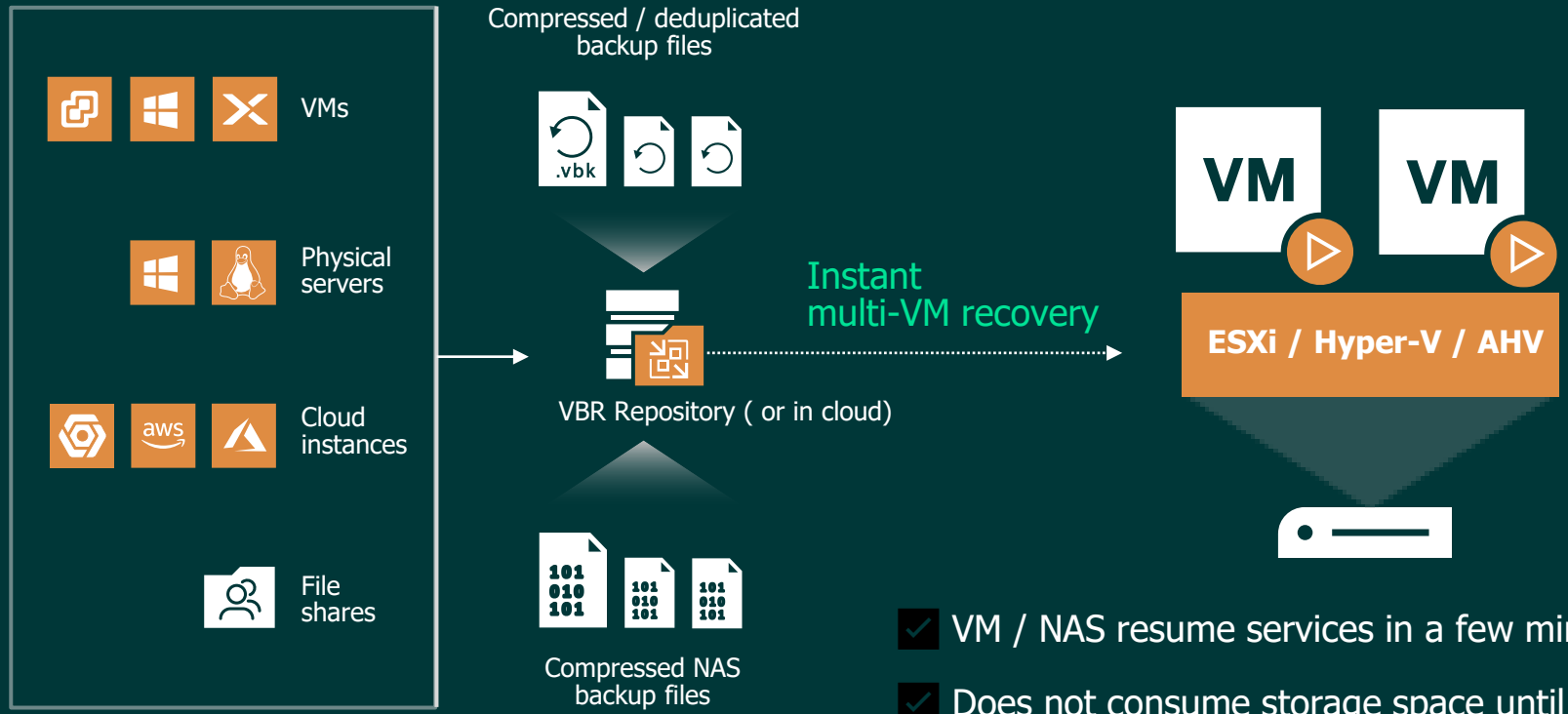
How long will it take to transfer **10 TB** of data over a **10 Gbps** link?

10 TB = 10 * 1,024 (GB) * 1,024 (MB) = 10,485,760 MB
10,485,760 MB / 900 MB/s = 11,651 seconds
11,651 seconds / 60 seconds = 195 minutes

195 minutes / 60 minutes
= 3 hours 15 minutes

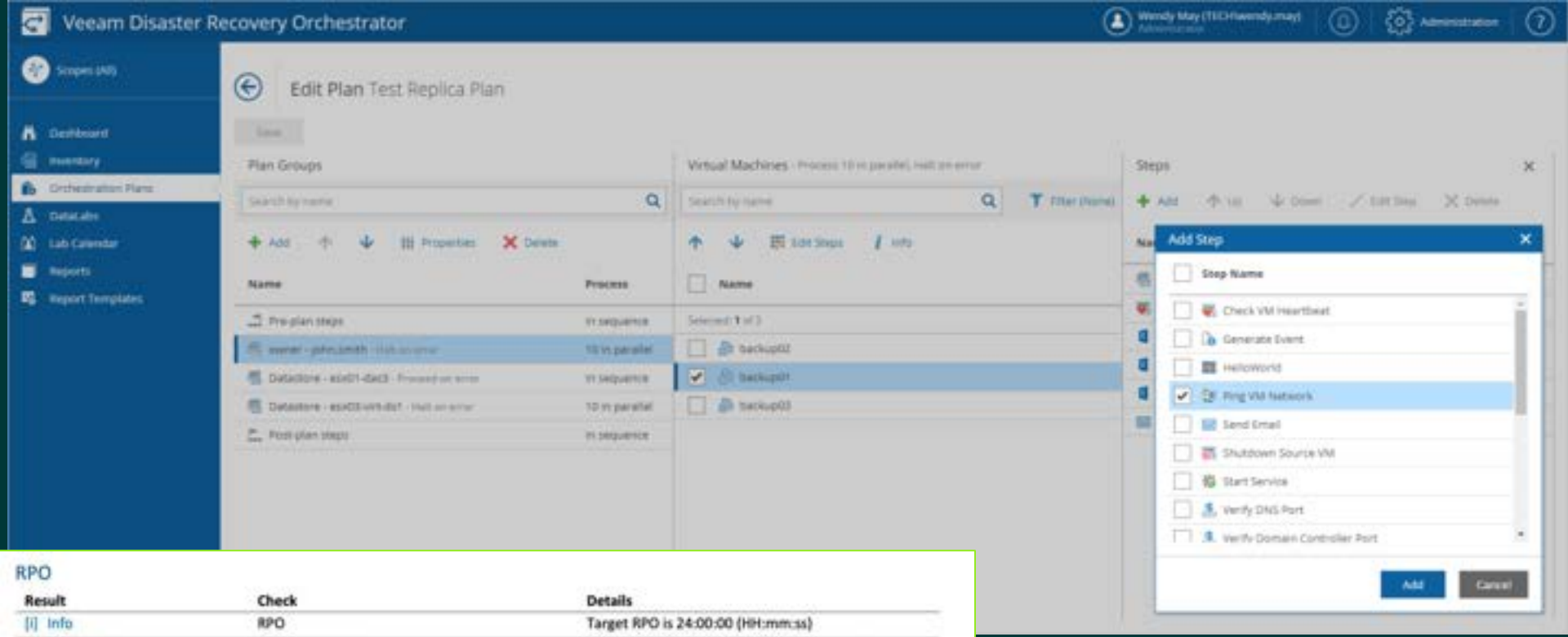
Enough Space to restore ?

Restore your service ASAP



- ✓ VM / NAS resume services in a few minutes
- ✓ Does not consume storage space until migration

What else ?



RPO

Result	Check	Details
[i] Info	RPO	Target RPO is 24:00:00 (HH:mm:ss)
✓ Success	Target RPO Met	Yes
✓ Success	VMs not meeting RPO	None
✓ Success	Worst RPO failure	None

RTO

Result	Check	Details
[i] Info	RTO	Target RTO is 01:00:00 (HH:mm:ss)
[i] Info	Duration	Plan execution duration was 00:18:17 (HH:mm:ss)
✓ Success	Target RTO Met	RTO achieved

Meet Your RTO and RPO

VM Demo-MSSQL

Back to VM Group Members

Detailed Documentation of your Verification test/ Restore Execution

Step Results and Duration

Result	Step	Start Time	End Time	Duration
✓ Success	Check VM license and availability	11:28:43	11:28:43	00:00:00
✓ Success	Shutdown Source VM	11:28:43	11:28:45	00:00:02
✓ Success	Restore - Recovery	11:28:45	11:32:44	00:03:59
✓ Success	Check VM Heartbeat	11:32:44	11:33:19	00:00:35
✓ Success	Verify SQL Port	11:33:19	11:33:51	00:00:32
✓ Success	Restore - Migrate	11:33:51	11:46:56	00:13:05

Check VM Heartbeat

Timestamp	Details
11:32:44	Step 'Check VM Heartbeat' execution started
11:32:44	Execution attempt 1 of 1
11:32:44	Connecting to the vCenter Server imvmvc01.im.lab
11:32:44	Poll 1: The VM Heartbeat check completed successfully
11:32:54	Poll 2: The VM Heartbeat check completed successfully
11:33:04	Poll 3: The VM Heartbeat check completed successfully
11:33:14	Poll 4: The VM Heartbeat check completed successfully
11:33:14	VM Heartbeat checked successfully
11:33:19	Step 'Check VM Heartbeat' execution finished

Verify SQL Port

Timestamp	Details
11:33:19	Step 'Verify SQL Port' execution started
11:33:19	Execution attempt 1 of 11
11:33:25	Starting PowerShell script
11:33:36	Trying connect to server '10.122.0.251' and port '1433'
11:33:36	Successfully established a connection with the server '10.122.0
11:33:51	Step 'Verify SQL Port' execution finished

Ransomware:

Secure Backup is your last line of Defense

Ransomware is a **disaster**

Backup:

1. Protect with immutable backups
2. 3-2-1-1-0 Rule
3. Detect, monitoring and alert for visibility

Recovery:

1. Restore ASAP
2. Do I have enough space to restore ?
3. Automation

Thank you

VEEAM