

# Winning against Ransomware

## The Veeam Way



Mario Zimmermann

Regional Director Austria, Veeam Software



Blockchain and Cryptocurrency

**Social Media**

**Big Data and Analytics**

**Cloud Computing**

**Remote Work and Collaboration Tools**

Artificial Intelligence and Machine Learning

Augmented Reality (AR) and Virtual Reality (VR)

**Software-as-a-Service**

**Mobile Revolution**

**Internet of Things**

**Cybersecurity**

What is the **worst fear** of any business relying on digital systems and data?



# OFFLINE

Unplanned downtime

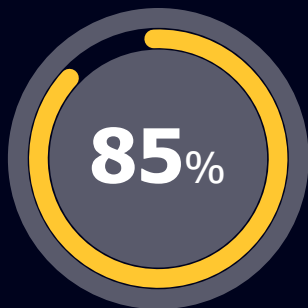


# Ransomware Report

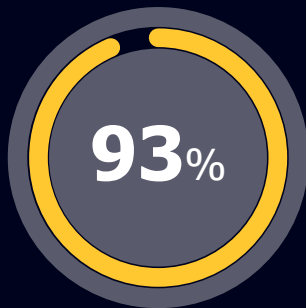
**1,200**

Organizations hit  
with Ransomware  
in prior 12 months

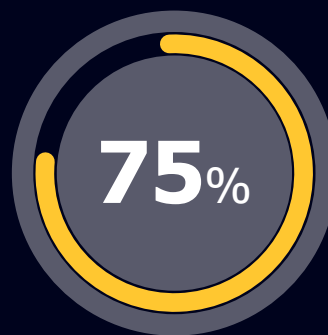




of organizations suffered at least one cyberattack in the preceding 12 months (**up from 76%** in prior years)



of cyber-events, the criminal attempted to attack the backup repositories first



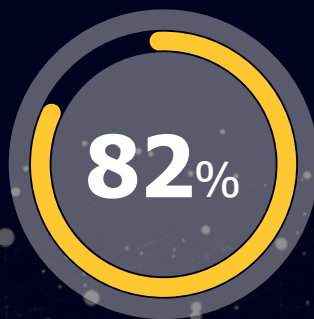
of orgs lost at least some of their backup repositories during an attack



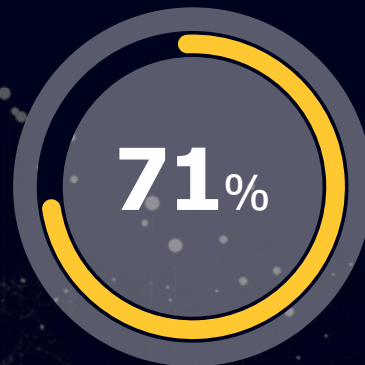
of organizations were able to recover themselves without paying (**down from 19%** last year's survey)



paid the ransom but could not recover data



of organizations use immutable cloud repositories



have plan to recover to cloud cloud-hosted infrastructure or DRaaS



of organizations run the risk of re-infection.

# Ransomware event frequency

How many ransomware attacks has your organization suffered in the last 12 months? (n=1,932)



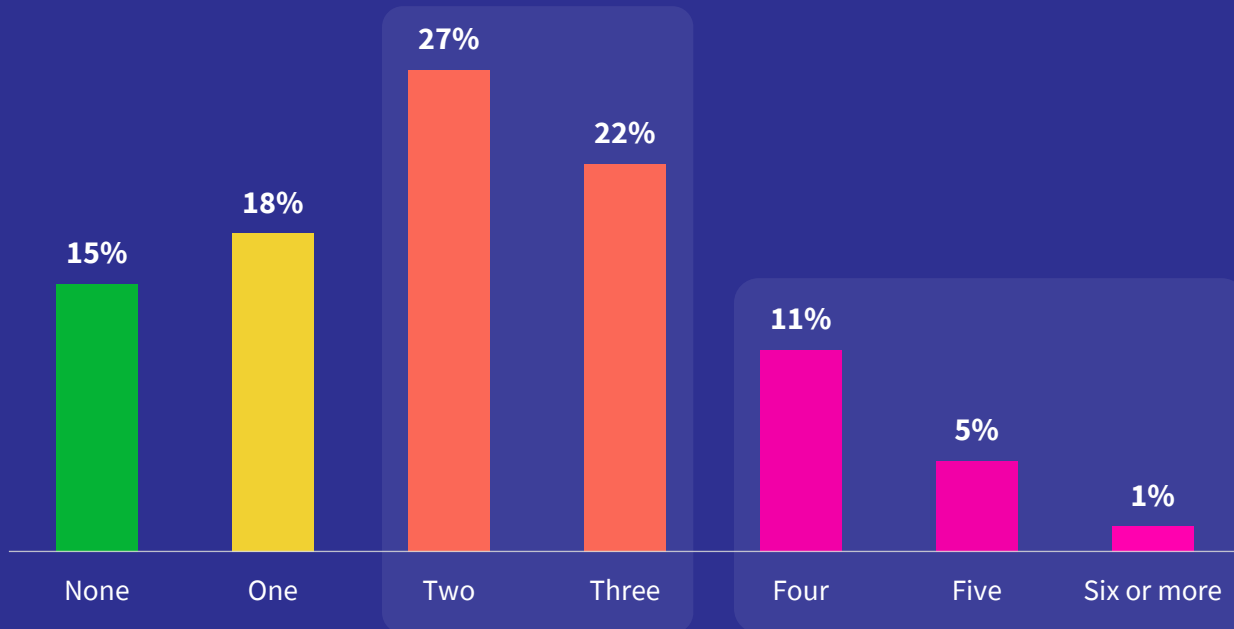
**85%**

of organizations suffered at least one ransomware attack

More people (**17%**) suffered four or more attacks than had zero attacks (**15%**)

**49%**

of organizations suffered two to three ransomware attacks



Source: Data Protection Trends Report 2023  
<https://vee.am/DPR23>

© 2023 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

**veeam** ON TOUR

# Connectivity has consequences

**DARK**Reading

The EdgeDR TechSectionsEventsResourcesNEWSLETTER


Vulnerabilities/Threats4 MIN READNEWS

## Tesla Model 3 Hacked in Less Than 2 Minutes at Pwn2Own Contest

In two days, ethical researchers from 10 countries have unearthed more than 22 zero-day bugs in a wide range of technologies at the annual hacking contest.

**Jai Vijayan**  
Contributing Writer, Dark Reading

March 24, 2023



Source: The Bold Bureau via Shutterstock


[Twitter](#) [LinkedIn](#) [Facebook](#) [Reddit](#) [Print](#) [RSS](#)


Researchers from France-based pen-testing firm Synacktiv demonstrated two separate exploits against the Tesla Model 3 this week at the Pwn2Own hacking contest in Vancouver. The attacks gave them deep access into subsystems controlling the vehicle's safety and other components.


One of the exploits involved executing what is known as a time-of-check-to-time-of-use (TOCTTOU) attack on Tesla's Gateway energy management system. They showed how they could then – among other things – open the front trunk or door of a Tesla Model 3 while the car was in motion. The [less than two-minute attack](#) fetched the researchers a new Tesla Model 3 and a cash reward of \$100,000.


The Tesla vulnerabilities were among a total of [22 zero-day vulnerabilities](#) that

### Editors' Choice


**Microsoft Outlook Vulnerability Could Be 2023's 'It' Bug**  
Nathan Eddy, Contributing Writer, Dark Reading


**Okta Post-Exploitation Method Exposes User Passwords**  
Elizabeth Montalbano, Contributor, Dark Reading


**Chinese Warships Suspected of Signal-Jamming Passenger Jets**  
Tara Seals, Managing Editor, News, Dark Reading


**ChatGPT Gut Check: Cybersecurity Threats Overhyped or Not?**  
Becky Bracken, Editor, Dark Reading


### Webinars

 **Building Out the Best Response Playbook for Ransomware Attacks**

 **ChatGPT: Defending Your Business Against AI-Supercharged Ransomware**

 **Ten Emerging Vulnerabilities Every Enterprise Should Know**

 **How Applications Are Attacked: A Year in Application Security**

 **Managing Identity in the Cloud**

[More Webinars](#)

### Reports



## Principle of assume breach

# Understanding Cyberattacks

# Understanding cyberattacks

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

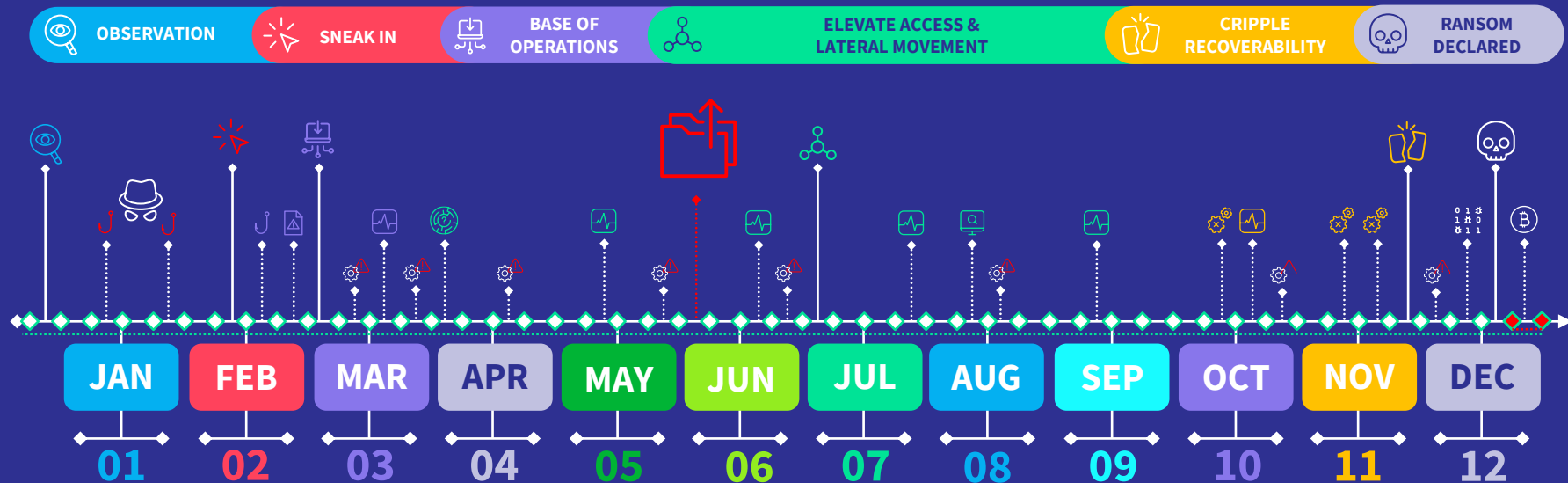
Gain access to the victim by sending phishing emails and let them click a link

Creating a base of operations and let's make it redundant and highly available

Snooping around without being detected and compromise higher value targets

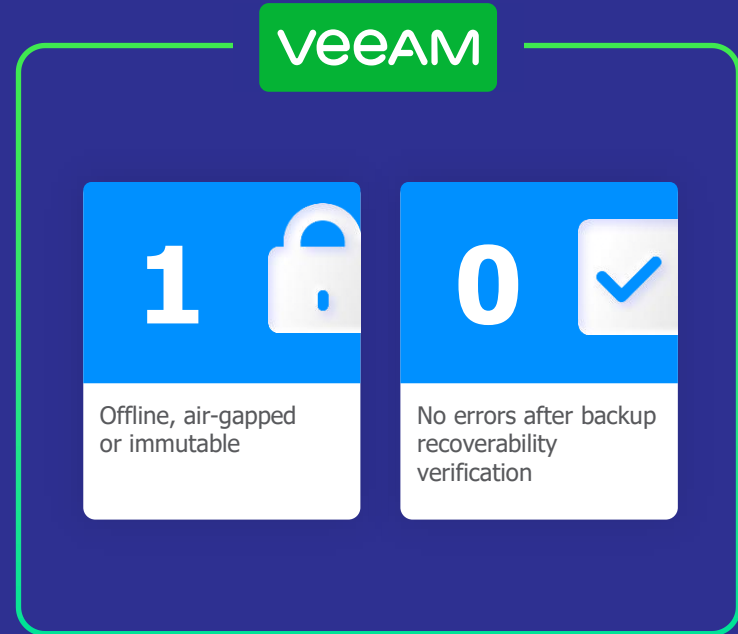
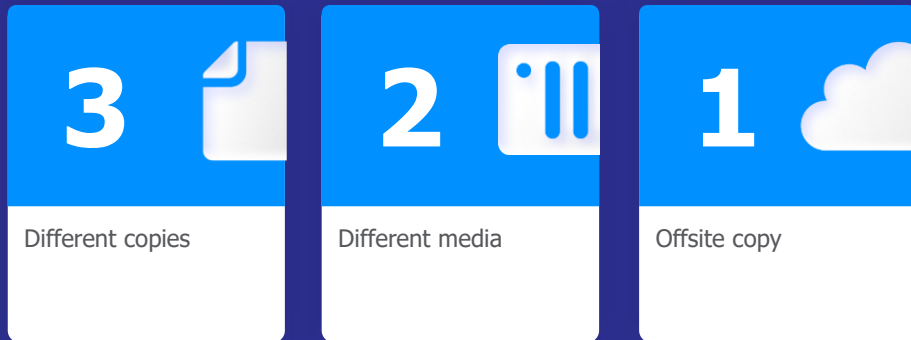
Alter routines, documentation and security systems to reduce/deny restore capabilities

Encrypt victim's data, wipe archives/backup/data, issue ransom demands!



# Backups are Target #1

# 3-2-1 Rule



1



Trusted immutability  
to protect against  
backup data being  
modified or deleted

Offline, air-gapped  
or immutable



0



No errors after backup  
recoverability  
verification

Backups are only  
as good as they  
are being verified!



# Stealing the Backups

# Encryption

Protect against backup data being readable after being exfiltrated



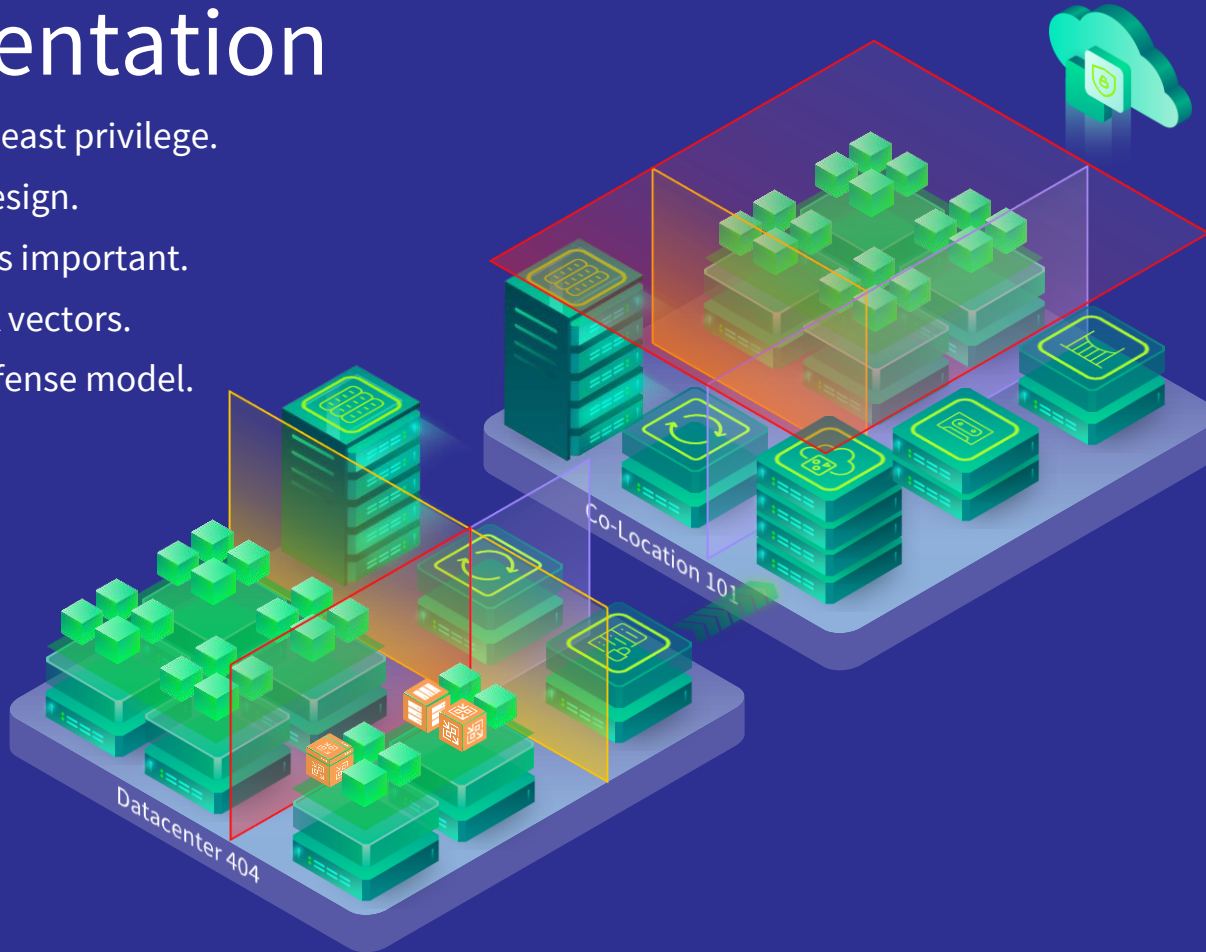
# Taking over Control

# Principle of Least Privilege



# Segmentation

- Principle of least privilege.
- Secure by design.
- Know what is important.
- Know attack vectors.
- Strategic defense model.



# The Easy Route!

# Patches & updates

## Updates & upgrades

- Is it new functionality only?
- Is the old version going to be End of Support (EOS) or End of Life (EOL)?

## Patches

- Is it a high-ranking security patch? (CVSS score 7.0 - 10.0)
- Regular patch to fix a software bug affecting a function in the product?

The screenshot displays the vSphere Client interface. On the left, a navigation pane shows the hierarchy: vcsa.corp.local > Datacenter > Homelab > srv-esx01.corp.local. The main panel shows the 'Summary' tab for the host 'srv-esx01.corp.local'. The 'Uptime' field is highlighted with a pink box, indicating 1728 days. Other fields include Hypervisor (VMware ESXi, 7.0.1, 17551050), Model (SYS-E200-8D), Processor Type (Intel(R) Xeon(R) CPU D-1528 @ 1.90GHz), Logical Processors (12), NICs (4), Virtual Machines (14), and State (Connected). On the right, resource usage bars are shown for CPU (Used: 4.83 GHz, Free: 6.57 GHz, Capacity: 11.4 GHz), Memory (Used: 28.89 GB, Free: 35.01 GB, Capacity: 63.9 GB), and Storage (Used: 14.16 TB, Free: 17.25 TB, Capacity: 31.41 TB).

Resource	Used	Free	Capacity
CPU	4.83 GHz	6.57 GHz	11.4 GHz
Memory	28.89 GB	35.01 GB	63.9 GB
Storage	14.16 TB	17.25 TB	31.41 TB

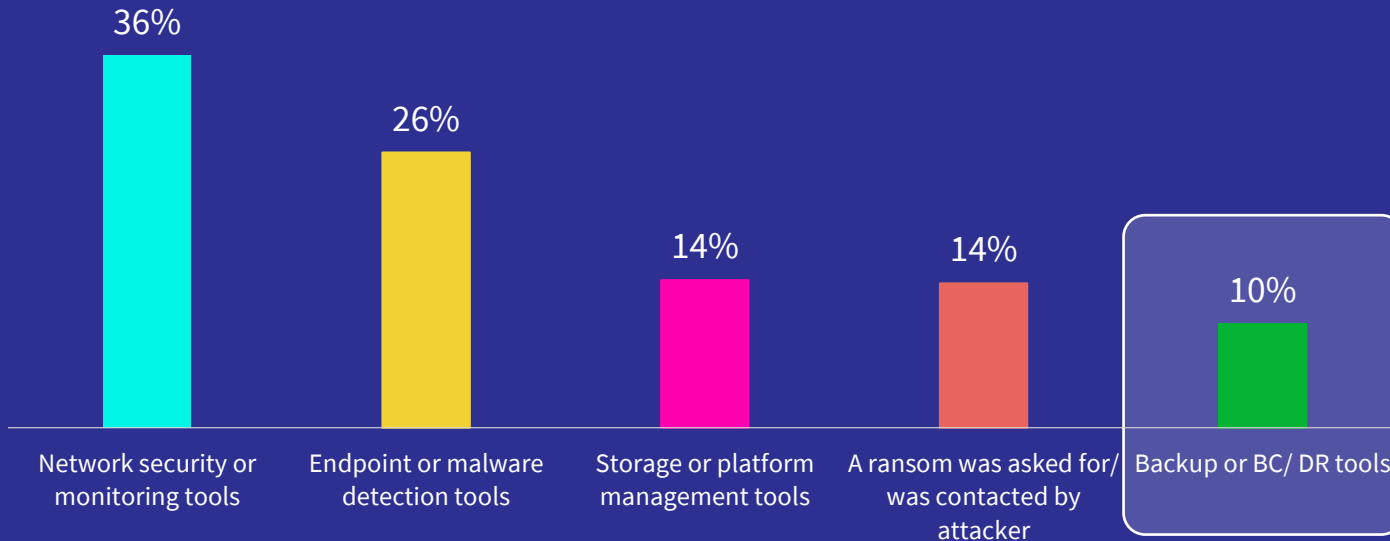
# Hide & Seek



# How did you first discover the attack?



How did you first become aware that ransomware had entered your organization's IT environment? (n=950)



Source: Ransomware Trends Report 2023  
<https://vee.am/RW23>

# Backup Object Change Tracking



## Backup Objects Change Tracking

### Description

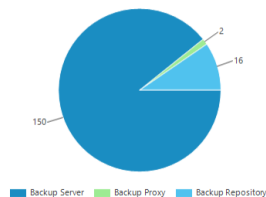
This report provides detailed information on backup infrastructure configuration changes that occurred during a specified period, including the exact time and the account name of the user who made the changes.

### Report Parameters

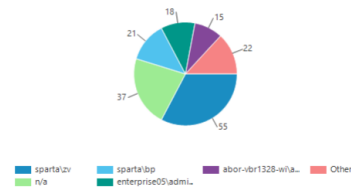
Scope: Backup Infrastructure  
Interval: 12/1/2022 - 12/31/2022  
Object types: All objects  
Object inclusion rule:  
Users: All

### Summary

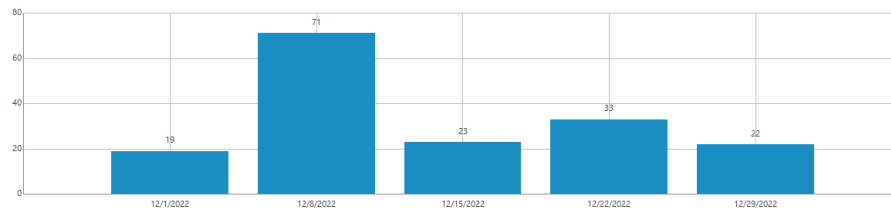
Modifications by Object Types



Modifications per Initiator



Modifications by Day



# Veeam ONE ransomware detection

## Veeam ONE™ Alarms

Possible ransomware  
activity

Suspicious backup  
increment size

Unusual job duration

The screenshot shows the Veeam ONE Client interface. The top navigation bar includes buttons for Back, Forward, Refresh, Add Server, Notifications, Reports, Modeling, Settings, Full Screen, and Help. The left sidebar shows the Alarm Management section with a tree view of infrastructure resources. The main area displays a table of alarms. One alarm is highlighted: 'Suspicious incremental backup size' for source 'ATLOSEWEST' at 4:38:58 AM. Below the table, the 'Alarm Details' section provides a description of the issue, listing several backup jobs with their sizes and creation times. A red box highlights the 'ATLWIKI01' job with a size of 159.5%. The 'Cause' section explains that the size of the recently created incremental restore point is significantly different from previous ones, and a red arrow points to the 'Possible ransomware activity' bullet point in the list.

Veeam ONE Client Logged in as: USDEMO\mark.polin

Search...

Alarm Management

- All Alarms
- VMware

Infrastructure View

- Demo
  - adcseesx01.usdemo.veeam
  - adcseesx02.usdemo.veeam
  - adcseesx03.usdemo.veeam
  - adcseesx04.usdemo.veeam
- Resources
  - Agents
  - Core
  - Demo Stations
  - Prod
    - ATLBEM01
    - ATLDEMOC01
    - ATLEXCH2016
    - ATLFILE01
    - ATLFILE01\_restored

Service: ATLWONE connected

Status	Time	Source	Type	Name	Repeat
Error	4:49:21 AM	performance tier for demo		Backup repository free space	
Error	4:49:21 AM	kasten		Backup repository free space	
Error	4:38:58 AM	ATLOSEWEST		Suspicious incremental backup size	

Page 3 of 19

### Alarm Details

#### Description

Incremental backup size of "ATLWIKI01" (159.5%) created by "VMware - Immutable/Immediate Move" job is above the configured threshold (150.0%)

Incremental backup creation time 2022-08-03 01:00:46 (UTC-7:00)

Incremental backup size of "usdemo-worker-2" (151.3%) created by "VMware - Immutable/Immediate Move" job is above the configured threshold (150.0%)

Incremental backup creation time 2022-08-03 01:00:39 (UTC-7:00)

Incremental backup size of "ATLWIKI01" (159.9%) created by "VMware - Wasabi Object Lock" job is above the configured threshold (150.0%)

Incremental backup creation time 2022-08-03 01:00:30 (UTC-7:00)

Incremental backup size of "ATLOSEWEST-WINAGENT.usdemo.veeam.local" (56.6%) created by "Agent Backup - Windows" job is below the configured threshold (70.0%)

Incremental backup creation time 2022-08-03 01:00:39 (UTC-7:00)

Incremental backup size of "ATLDEMOC01" (41.6%) created by "VMware - Veeam Explorers" job is below the configured threshold (70.0%)

Incremental backup creation time 2022-08-03 01:00:39 (UTC-7:00)

Incremental backup size of "UbuntuServer-BeJX" (44.3%) created by "VMware - vCloud Director - vApp" job is below the configured threshold (70.0%)

Incremental backup creation time 2022-08-03 01:00:41 (UTC-7:00)

#### Knowledge

The size of the recently created incremental restore point is significantly different from the previously created ones

#### Cause

The size of the recently created incremental restore point may be different in comparison with the previously created ones due to the following reasons:

- Possible ransomware activity
- A significant amount of data blocks of the VM has been changed since the previous backup job session



# Design for recovery



# How to recover?

## Duration

How fast would you be able to restore your business?

<1 day <1 week

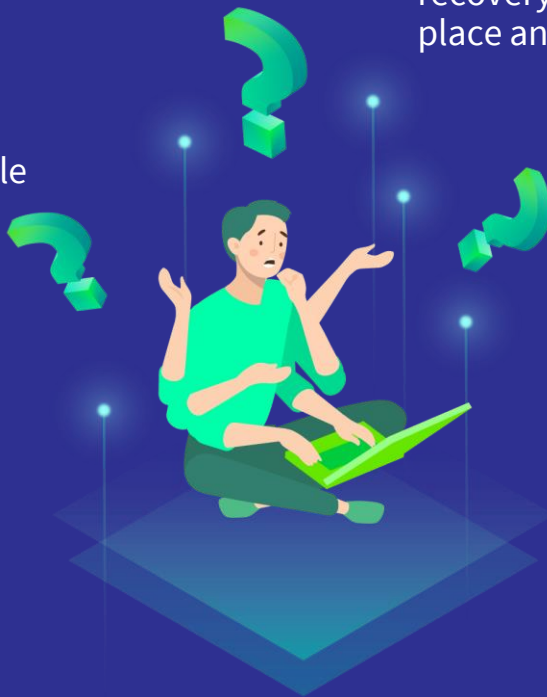
<1 month or longer?

## How

Manual or automated recovery processes in place and in which order?

## Where

Which location have you designated for recovery?  
Going to the cloud, service provider or second datacenter?

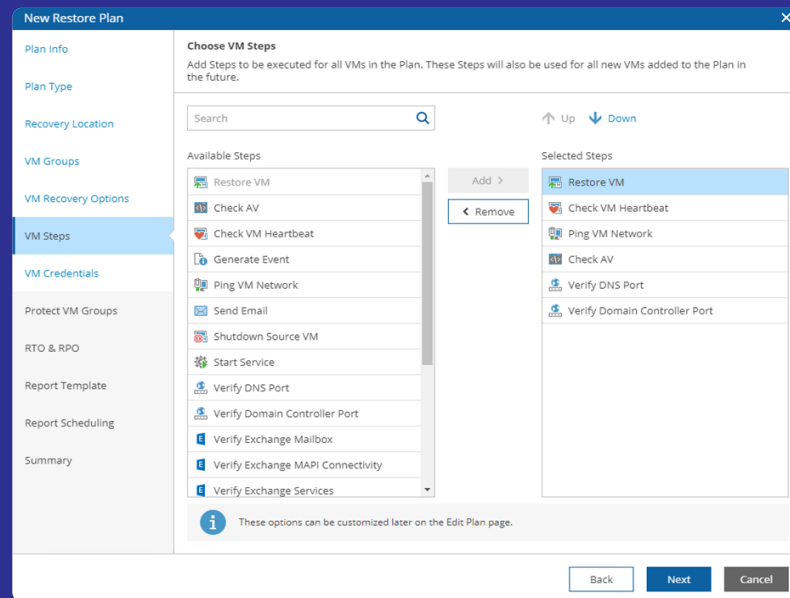


# Recovery (Orchestration) plans



Someone with a plan can beat  
a genius without a plan. **Warren Buffet**

- ✓ Dynamically restore VMware and/or Agent backups created by Veeam® Backup & Replication™.
- ✓ Define and establish RPO and RTO in alignment with business requirements.
- ✓ Inject any number of in-guest operations or custom scripting.



# The Report

VEEAM

## Restore Linux

Restore

Readiness Check-Report

Umfang: Admin Scope  
Generiert: 02.06.2023 11:23, [UTC+01:00] Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

Readiness Check. Inhalt.

02.06.2023 11:23

### Inhalt

Orchestrierungsplan-Report für Restore Linux.....	3
Dokumentinformationen .....	3
Overview .....	4
Summary .....	5
Recovery Locations.....	6
Restore Location .....	6
Pre-Plan Steps.....	7
All Groups .....	9
Group Details.....	10
Agent Backup Job PostgreSQL-vbr12.homelab.local.....	10
Post-Plan Steps .....	12

### Summary

Result	Details
✖ Not ready	1 Errors, 5 Warnings

### Execution Details

Item	Details
Run/Scheduled By	HOMELAB\administrator
Duration (HH:mm:ss)	00:12:21

### Plan

Result	Group	Details
[!] Warning	<a href="#">Pre-Plan Steps</a>	3 Warnings
✖ Not ready	<a href="#">Agent Backup Job PostgreSQL-vbr12.homelab.local</a>	1 VM(s) with errors
✓ Ready	<a href="#">Post-Plan Steps</a>	No errors

### RPO

Result	Check	Details
[i] Info	RPO	Target RPO is 24:00:00 (HH:mm:ss)
✓ Ready	Target RPO Met	Yes
✓ Ready	Number of RPO failures	None
✓ Ready	Worst RPO failure	None

### Ransomware scan

Result	Details
✓ Ready	The scanned restore points do not contain ransomware.

### Recovery Locations

Result	Resource	Details
[!] Warning	<a href="#">Restore Location</a>	3 Warnings

### Licensing

Result	Check	Details
[i] Info	Summary	2 of 20 license instances used
✓ Ready	Usage	1 licenses are used in this plan
✓ Ready	Expiry	The license will expire in 319 days
✓ Ready	Exceeded	The license limit is not exceeded on the Orchestrator

# Ressourcen



Ransomware Assessment Kit



Allgemeine Informationen zu Ransomware



Content Library (Executive und Technical)

## DOWNLOAD:

### Ransomware Trends Report 2023

Der Ransomware Trends Report 2023 ist der aktuellste und umfassendste Forschungsbericht in der Geschichte von Datensicherung und -verfügbarkeit und basiert auf den Erfahrungen von Opfern von Cyberangriffen. Die Befragung, die von einem unabhängigen Marktforschungsunternehmen durchgeführt wurde, umfasst 1.200 Unternehmen aus 14 Ländern und damit Informationen zu fast 3.000 Cyberangriffen.

