Achieving Radical Resilience

With the Veeam Data Platform

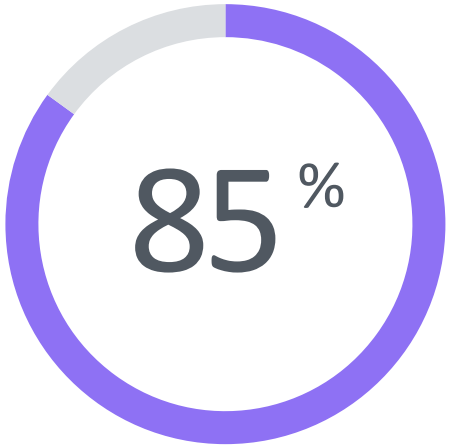
Arjan Henselmans
Senior Pre-Sales Engineer
Veeam Benelux

Agenda

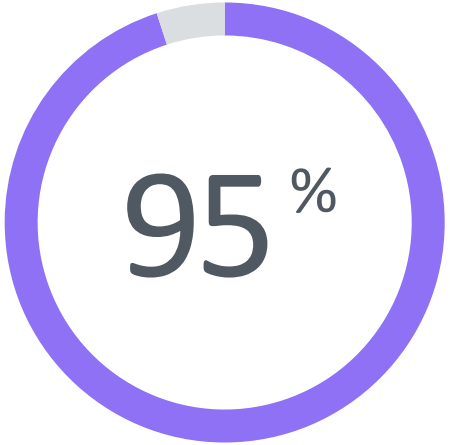
- Disasters
- NIS-2
- Ransomware Trends
- Navigating a Cyber Attack – Assume Breach
- Veeam Data Platform Overview of Features
- Q&A

Disasters

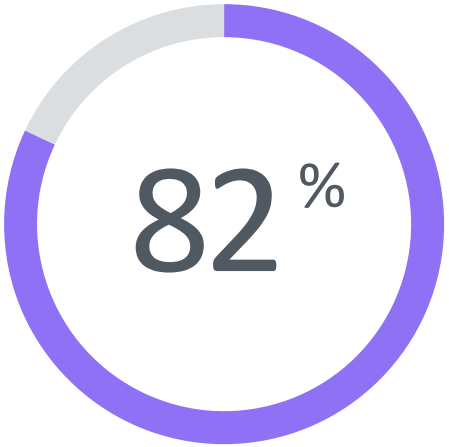
Outages and data loss are an unfortunate reality



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



of organizations are moderately to extremely concerned about cloud security**



of companies use manual processes to recover their data after an outage*

*2024 Veeam Data Protection Trends Report
**2022 Fortinet Cloud Security Report

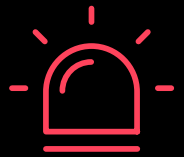
Disasters happen all the time

Ransomware

Fire

Hardware failure

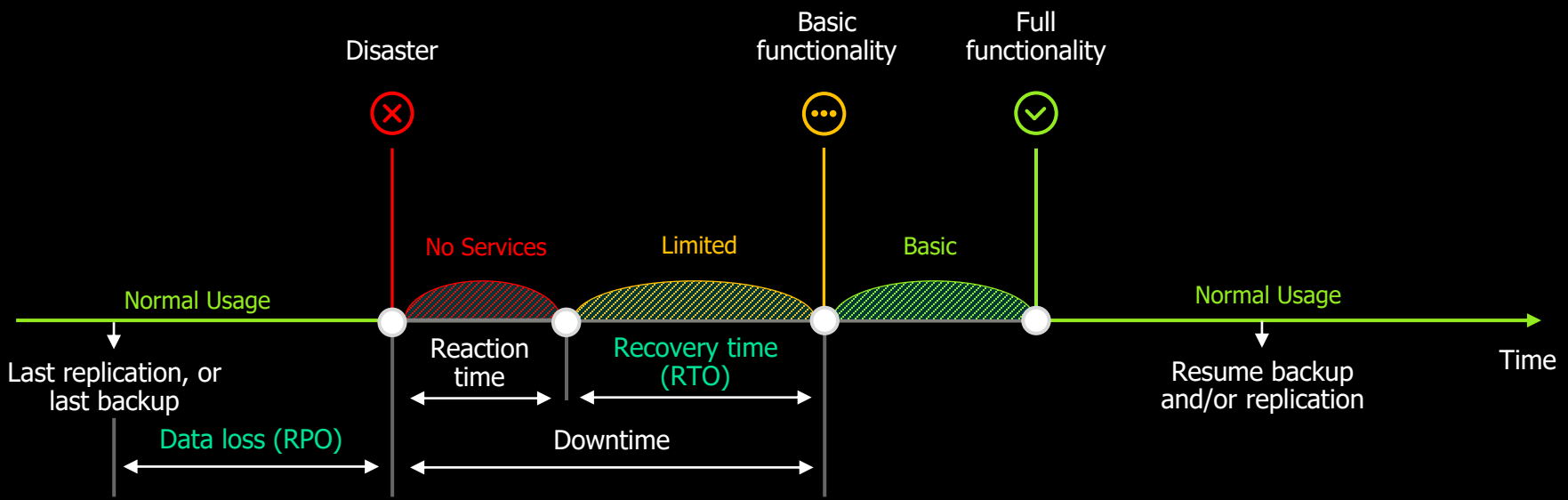
Flood



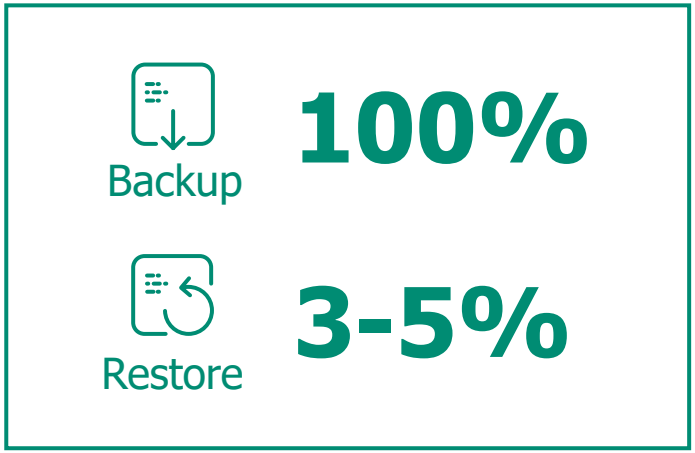
Corruption

Stor m

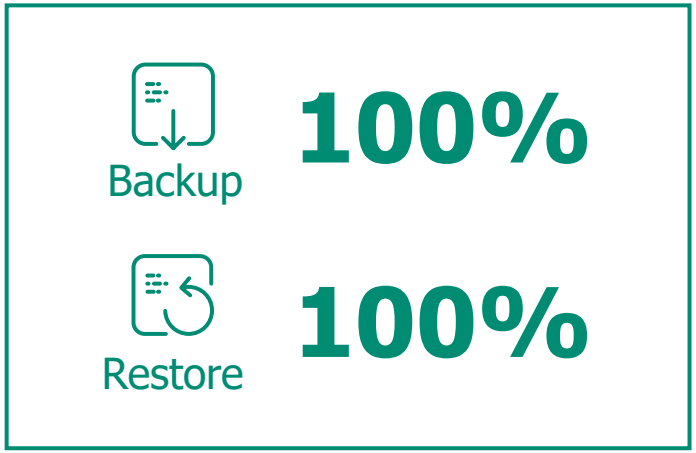
Recovery timeline



Design for Mass Recovery!



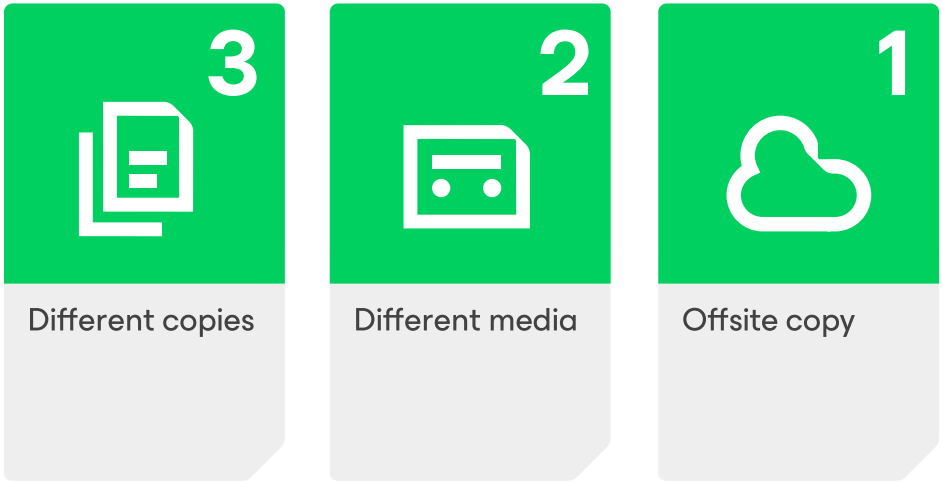
PAST



PRESENT

~95% of ALL organizations designed for backup

Veeam's 3-2-1 Backup Rule



NIS-2

NIS-2 – Dit begrijpt toch iedereen…

(31) Tot de digitale-infrastructuursector behorende entiteiten zijn in wezen gebaseerd op netwerk- en informatiesystemen en daarom moeten de hun uit hoofde van deze richtlijn opgelegde verplichtingen op een omvattende manier betrekking hebben op de fysieke beveiliging van dergelijke systemen in het kader van hun maatregelen voor het beheer van cyberbeveiligingsrisico's en rapportageverplichtingen. Aangezien die aangelegenheden onder deze richtlijn vallen, zijn de verplichtingen van de hoofdstukken III, IV en VI van Richtlijn (EU) 2022/2557 niet van toepassing op dergelijke entiteiten.

([11]) Verordening (EG) nr. 300/2008 van het Europees Parlement en de Raad van 11 maart 2008 inzake gemeenschappelijke regels op het gebied van de beveiliging van de burgerluchtvaart en tot intrekking van Verordening (EG) nr. 2320/2002 (PB L 97 van 9.4.2008, blz. 72).

([12]) Verordening (EU) 2018/1139 van het Europees Parlement en de Raad van 4 juli 2018 inzake gemeenschappelijke regels op het gebied van burgerluchtvaart en tot oprichting van een Agentschap van de Europese Unie voor de veiligheid van de luchtvaart, en tot wijziging van de Verordeningen (EG) nr. 2111/2005, (EG) nr. 1008/2008, (EU) nr. 996/2010, (EU) nr. 376/2014 en de Richtlijnen 2014/30/EU en 2014/53/EU van het Europees Parlement en de Raad, en tot intrekking van de Verordeningen (EG) nr. 552/2004 en (EG) nr. 216/2008 van het Europees Parlement en de Raad en Verordening (EEG) nr. 3922/91 van de Raad (PB L 212 van 22.8.2018, blz. 1).

([13]) Richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad van 14 december 2022 betreffende de weerbaarheid van kritieke entiteiten en tot intrekking van Richtlijn 2008/114/EG van de Raad (zie bladzijde 164 van dit Publicatieblad).

NIS-2 – Wat betekent het voor u?

… en voor uw toeleveranciers?

Zorgplicht

Bescherm uw data
Zorg voor toegangscontrole
Maak recovery plannen

Rapportage

Aantonen van effectief beheer
Informatie voor toezichthouders
Bij cyberaanval; Voorlopige en definitieve rapportages

Toezicht

Er worden audits uitgevoerd. Bij herhaaldelijk overtreden kan dit ook persoonlijke consequenties hebben

KPMG

pwc

EY

veeam

Ransomware

Ransomware event frequency

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

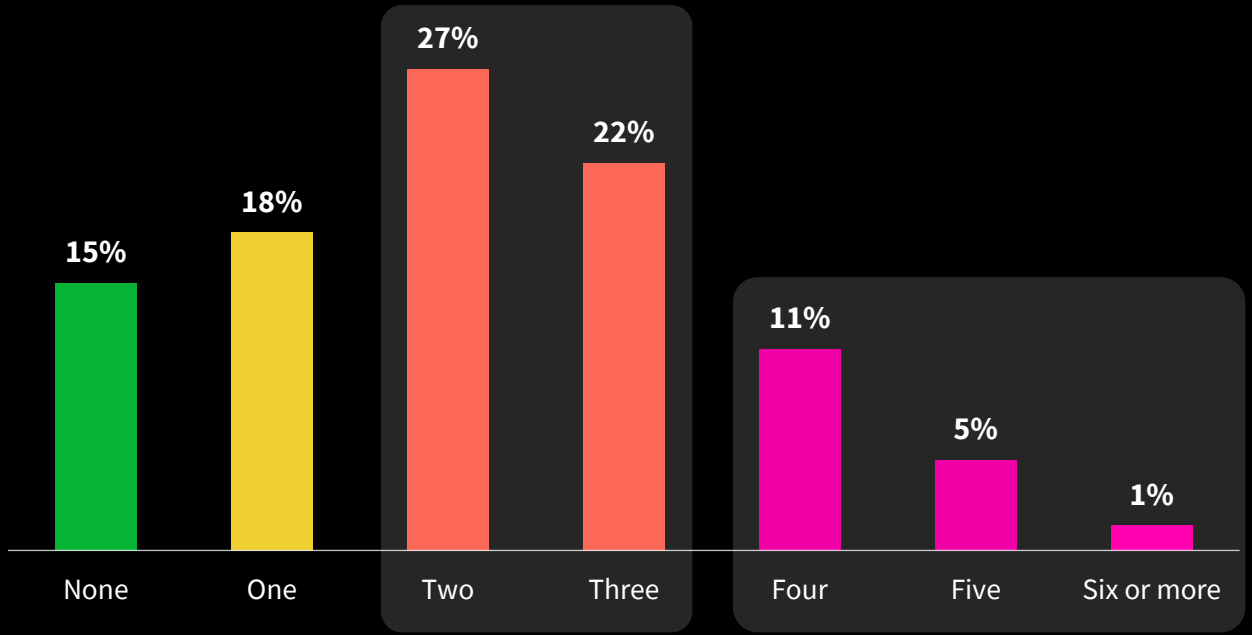
85%

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

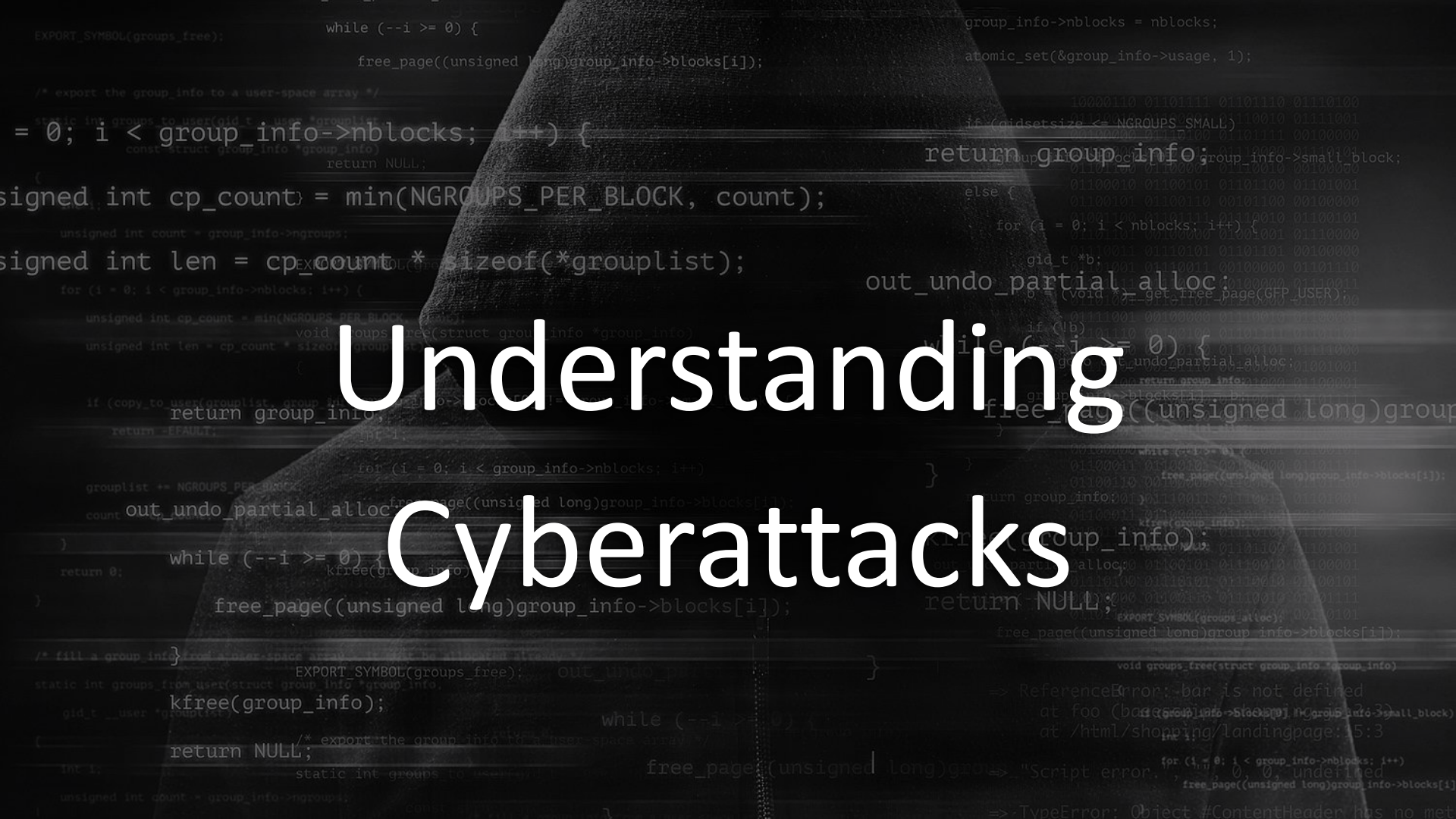


Source: Data Protection Trends Report 2024
https://vee.am/DPR23

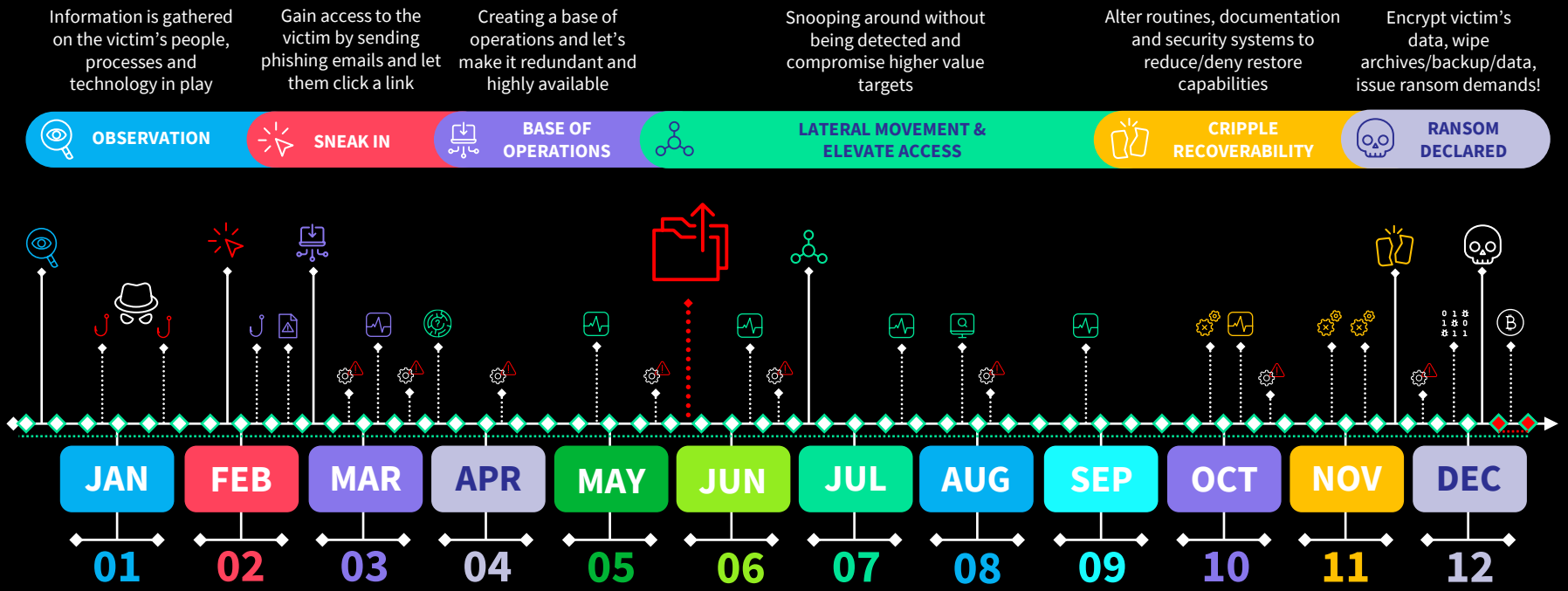
(Ransomware) Recovery is a team effort

Who's involved:

1. Sr. Leadership is driving the process
2. Legal, HR, and public relations determine the course of action
3. Incident responders drive the investigation and the recovery process
4. The backup team supports the recovery with clean data


Understanding
Cyberattacks

Understanding cyberattacks

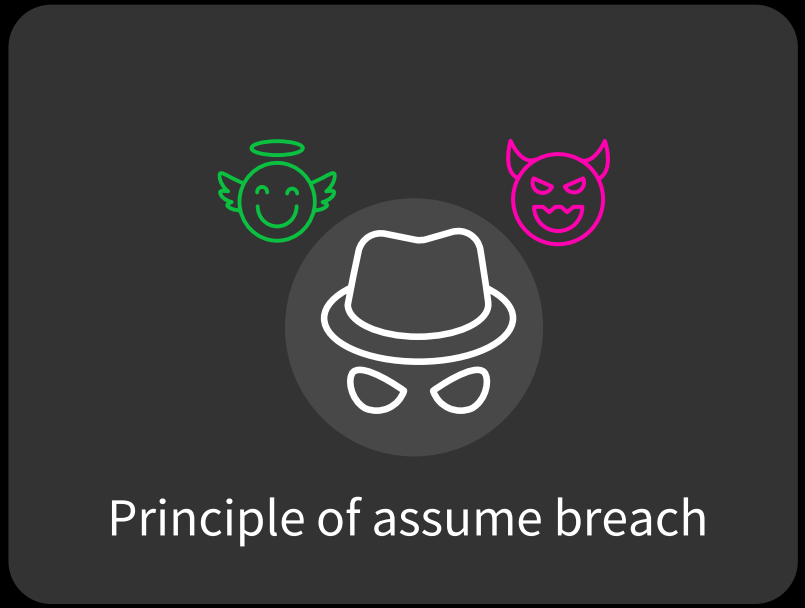


Assume Breach

Embrace the Breach

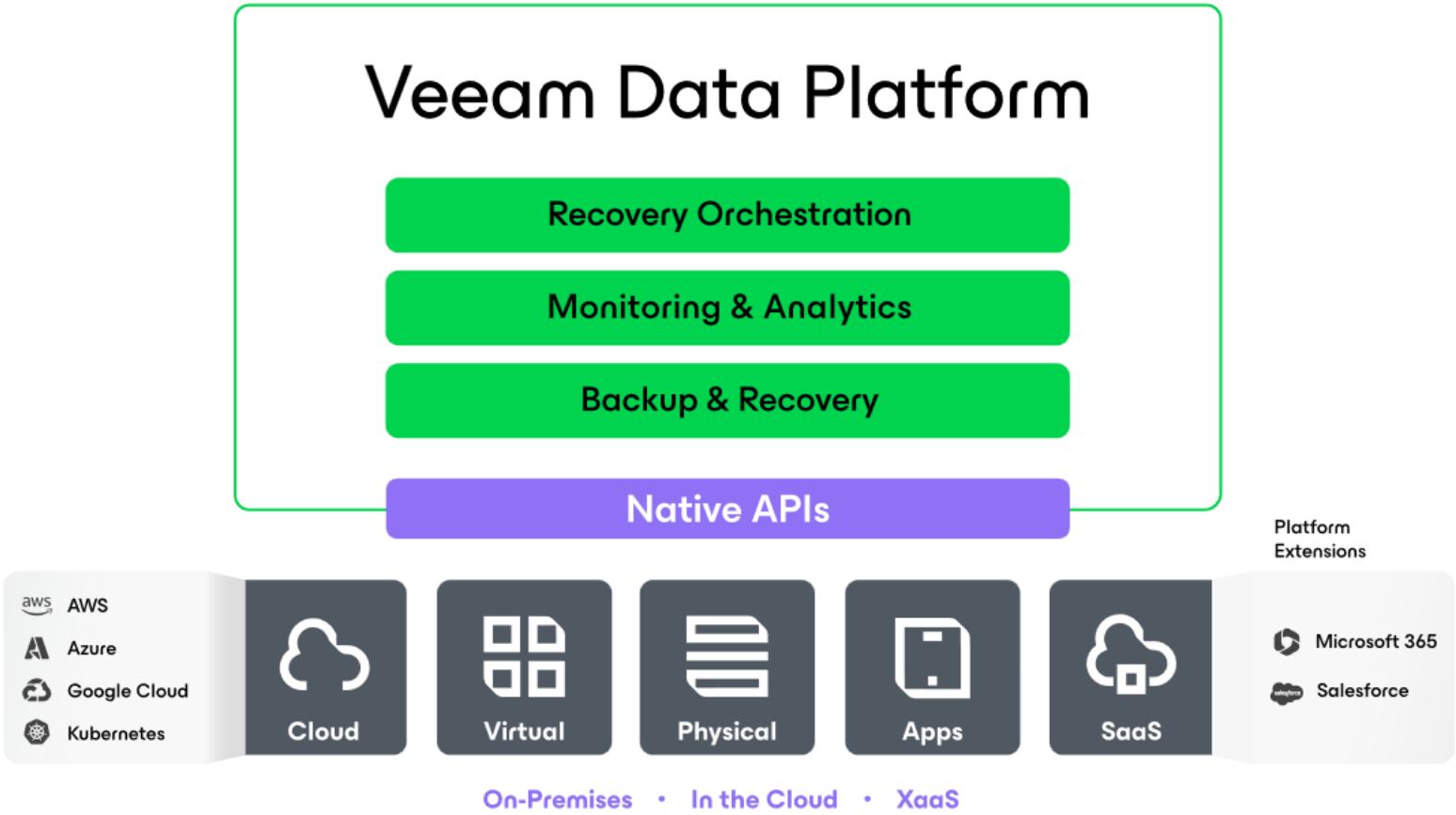
Cyber Security Design Principles

- Establish the context before designing a system.
- Make compromise difficult.
- Make disruption difficult.
- Make compromise detection easier.
- Reduce the impact of compromise.



Overview of Features

Veeam Data Platform (Security) Capabilities



Why Veeam...

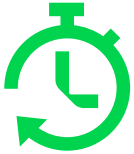
Secure Backup and Fast Recovery

Own, control, backup and recover all your data, anywhere in the hybrid cloud

Reduce risk with comprehensive data security

Secure Backup

Meet recovery objectives with confidence



Instant Recovery

Accelerate your move to the hybrid cloud

Multi-cloud Mobility

Why Veeam...

Proactive Monitoring and Analytics

Maintain full visibility for proactive management and recovery success

Quickly mitigate potential issues before they become threats

Real-time Monitoring

Stay secure by always knowing your protection status

Suspicious Activity Alerts

Minimize downtime by eliminating the need for manual responses

Automated Remediation

Why Veeam...

Proven Recovery Orchestration

Be compliant and ready for disaster with orchestrated recovery

Automate test to highlight potential impacts to your recovery

Automated Testing

Take the headache out of documentation and compliance

Automated Documentation

Recover faster from any disaster

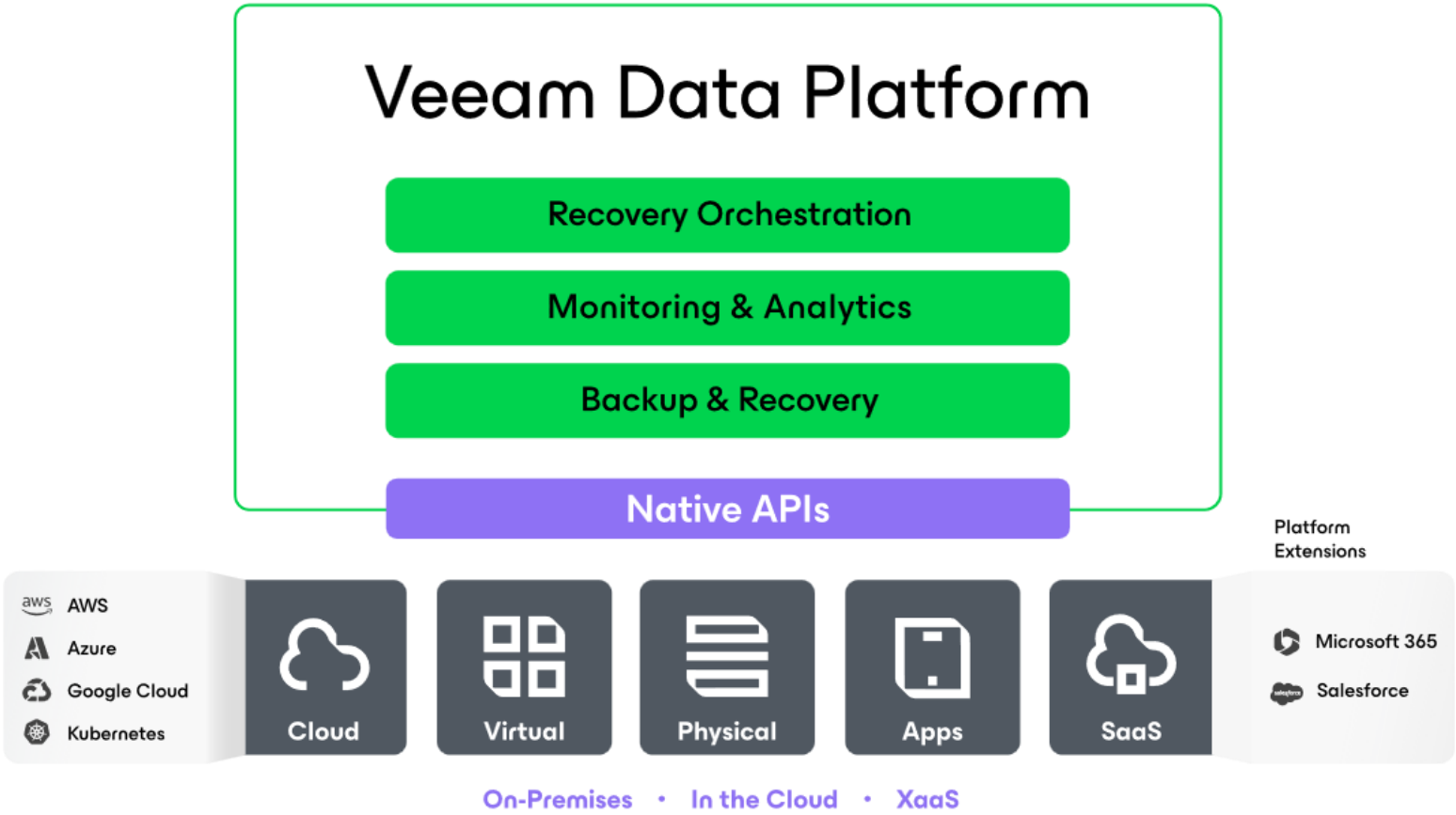
One-click Recovery

We keep your business running

Data Security

Data Recovery

Data Freedom



VDP Detect + Identify cyberthreats

Minimize the devastation of a cyberattack

(New)
Early threat detection

AI-powered built-in **Malware Detection Engine** performs low-impact inline entropy and file extensions analysis during backup for immediate detection

(New)
Proactive threat hunting

Backup anomalies are instantly reported into **ServiceNow** and other **SIEM** tools of your choice so you can immediately perform triage and reduce further risk to your data

(New)
Get a second opinion

Let your cyber-threat tool report infections directly into the **Veeam Incident API**, marking existing restore points as infected or trigger backup

VDP Respond + Recover faster from ransomware

Empower your team to slash incident response time

(New)

Avoid recovery reinfection

YARA content analysis helps to pinpoint identified ransomware strains to prevent reintroduction of malware into your environment

(Enhanced)

Automate clean recovery

Perform orchestrated recovery of an entire environment using **malware-free restore** points

(New)

Recover with precision

Perform point-in-time recovery to the moment prior to infection with the **I/O Anomaly Visualizer**, ensuring the lowest possible data loss thanks to Veeam CDP

VDP Secure + Compliant protection for your data

Complete your security & compliance standing

(New)

Guarantee your survival

Prevent accidental or malicious deletion or encryption of backups by employing a zero-trust architecture, **“Four-eyes” admin protection** and immutable backups

(Enhanced)

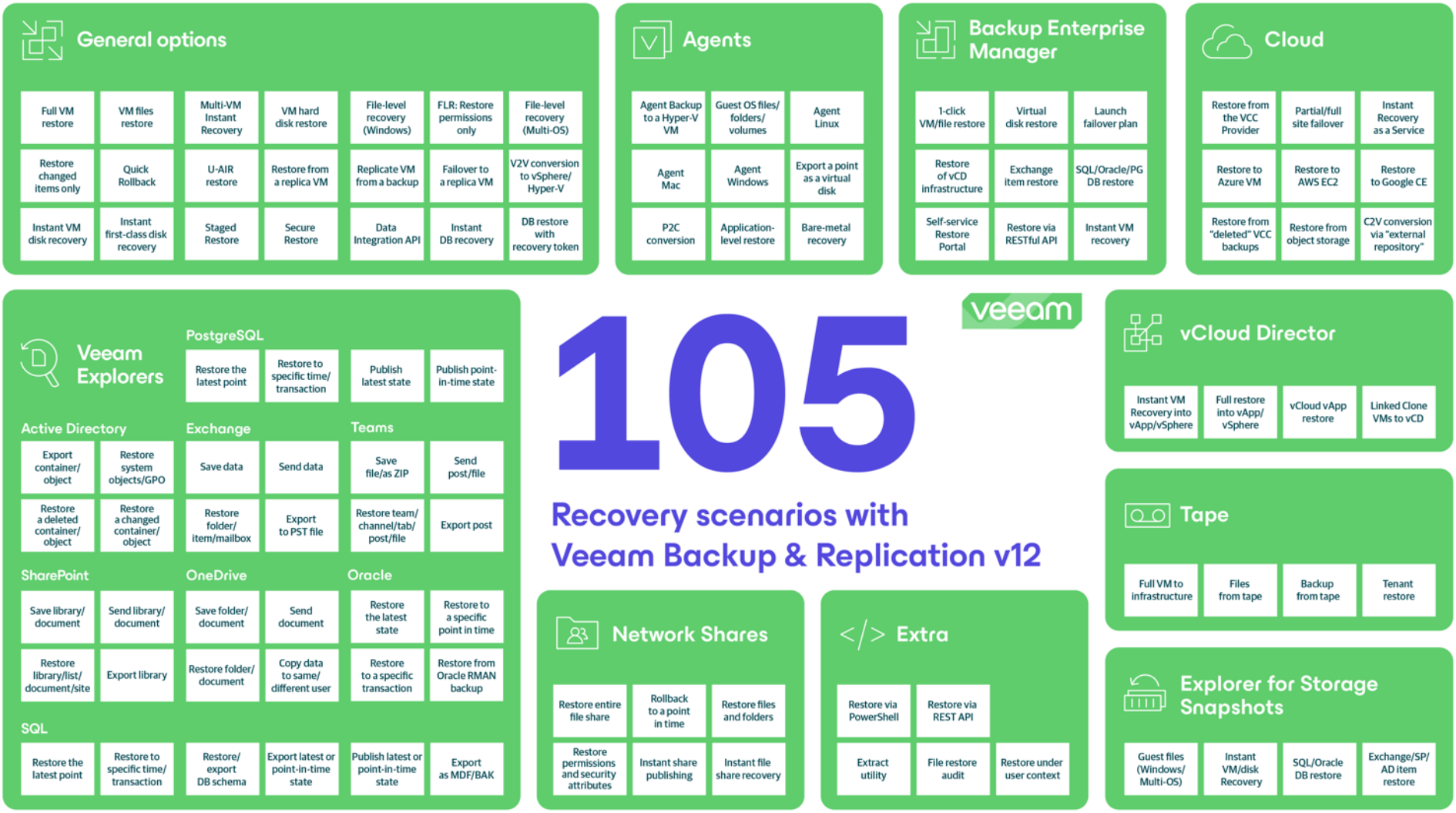
Verify security and compliance

Ensure recovery success with automated scans using the **Security & Compliance Analyzer**, leveraging infrastructure hardening and data protection best practices

(New)

Put the spotlight on malware

Highlight threats, identify risks and measure the security score of your environment in the **Veeam Threat Center**


General options
Full VM restore
VM files restore
Multi-VM Instant Recovery
VM hard disk restore
File-level recovery (Windows)
FLR: Restore permissions only
File-level recovery (Multi-OS)
Restore changed items only
Quick Rollback
U-AIR restore
Restore from a replica VM
Replicate VM from a backup
Failover to a replica VM
V2V conversion to vSphere/ Hyper-V
Instant VM disk recovery
Instant first-class disk recovery
Staged Restore
Secure Restore
Data Integration API
Instant DB recovery
DB restore with recovery token
Agents
Agent Backup to a Hyper-V VM
Guest OS files/ folders/ volumes
Agent Linux
Agent Mac
Agent Windows
Export a point as a virtual disk
P2C conversion
Application-level restore
Bare-metal recovery
Backup Enterprise Manager
1-click VM/file restore
Virtual disk restore
Launch failover plan
Restore of vCD infrastructure
Exchange item restore
SQL/Oracle/PG DB restore
Self-service Restore Portal
Restore via RESTful API
Instant VM recovery
Cloud
Restore from the VCC Provider
Partial/full site failover
Instant Recovery as a Service
Restore to Azure VM
Restore to AWS EC2
Restore to Google CE
Restore from "deleted" VCC backups
Restore from object storage
C2V conversion via "external repository"
Veeam Explorers
PostgreSQL
Restore the latest point
Restore to specific time/ transaction
Publish latest state
Publish point-in-time state
Active Directory
Export container/ object
Restore system objects/GPO
Restore a deleted container/ object
Restore a changed container/ object
Exchange
Save data
Send data
Restore folder/ item/mailbox
Export to PST file
Teams
Save file/as ZIP
Send post/file
Restore team/ channel/tab/ post/file
Export post
SharePoint
Save library/ document
Send library/ document
Restore library/list/ document/site
Export library
OneDrive
Save folder/ document
Send document
Restore folder/ document
Copy data to same/ different user
Oracle
Restore the latest state
Restore to a specific point in time
Restore to a specific transaction
Restore from Oracle RMAN backup
SQL
Restore the latest point
Restore to specific time/ transaction
Restore/ export DB schema
Export latest or point-in-time state
Publish latest or point-in-time state
Export as MDF/BAK
105
Recovery scenarios with Veeam Backup & Replication v12
veeam
Network Shares
Restore entire file share
Rollback to a point in time
Restore files and folders
Restore permissions and security attributes
Instant share publishing
Instant file share recovery
Extra
Restore via PowerShell
Restore via REST API
Extract utility
File restore audit
Restore under user context
vCloud Director
Instant VM Recovery into vApp/vSphere
Full restore into vApp/ vSphere
vCloud vApp restore
Linked Clone VMs to vCD
Tape
Full VM to infrastructure
Files from tape
Backup from tape
Tenant restore
Explorer for Storage Snapshots
Guest files (Windows/ Multi-OS)
Instant VM/disk Recovery
SQL/Oracle DB restore
Exchange/SP/ AD item restore

previder

Even voorstellen

- Lead Consultant
- d.vanderaalst@previder.nl
- Dennis van der Aalst

it starts here.

Samenwerking Previder <-> Veeam

Preferred partner t.a.v. Backup

- Backup klantomgeving
- Backup IaaS-platform
- Cloud Connect
- Microsoft 365 Backup

previder

Samenwerking Previder <-> Veeam

Heb je vragen over:

- Backup
- Disaster recovery / Uitwijk
- Ransomware
- Of iets anders

previder

Q&A

veeam

Follow us!

Join the community hub: