



How Veeam can help with NIS2 directive

Cornel Popescu

Systems Engineer – South East Europe

cornel.popescu@veeam.com

Disclaimer

- I'm not a lawyer
- Content is condensed
- This presentation covers technical aspects of certain areas of NIS2
- What will be presented is NOT recipe for success



DISCLAIMER

1. What is NIS2
2. Timelines
3. Where does it apply
4. Obligations
5. Where do we fit in

What is NIS2

What is NIS2

L 333/80

EN

Official Journal of the European Union

27.12.2022

DIRECTIVES

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 December 2022

on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

(Text with EEA relevance)

<https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>

What is NIS2?

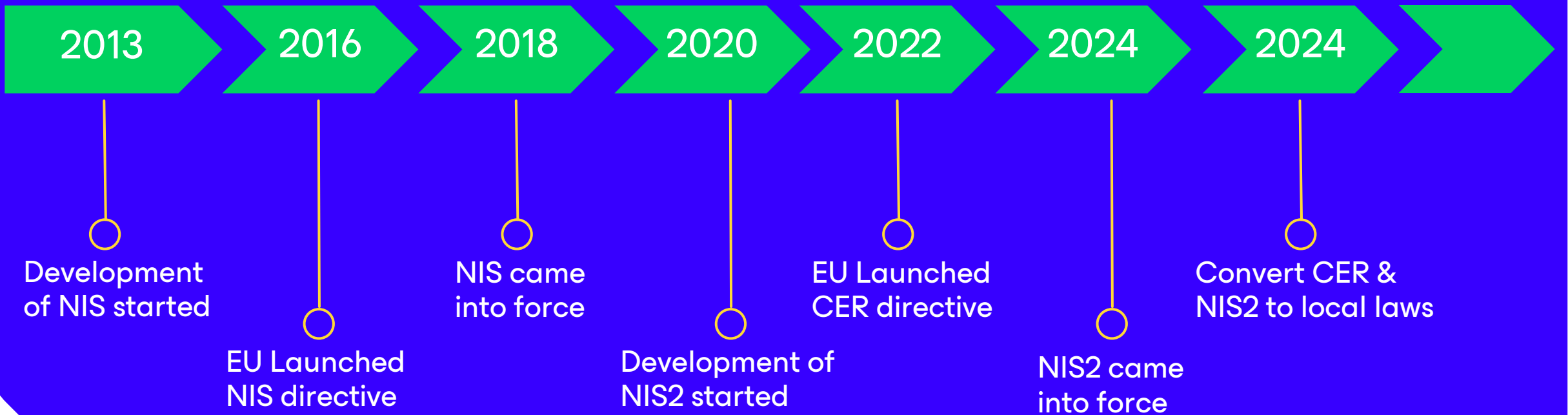
The NIS2 Directive is the EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity in the EU.

NIS2 is “directive” it means that local governments need to pass local legislations according to this directive

It's continuation, stricter version of already valid NIS directive

Strengthens the resilience of critical infrastructure to a range of threats, including natural hazards, terrorist attacks, insider threats, or sabotage.

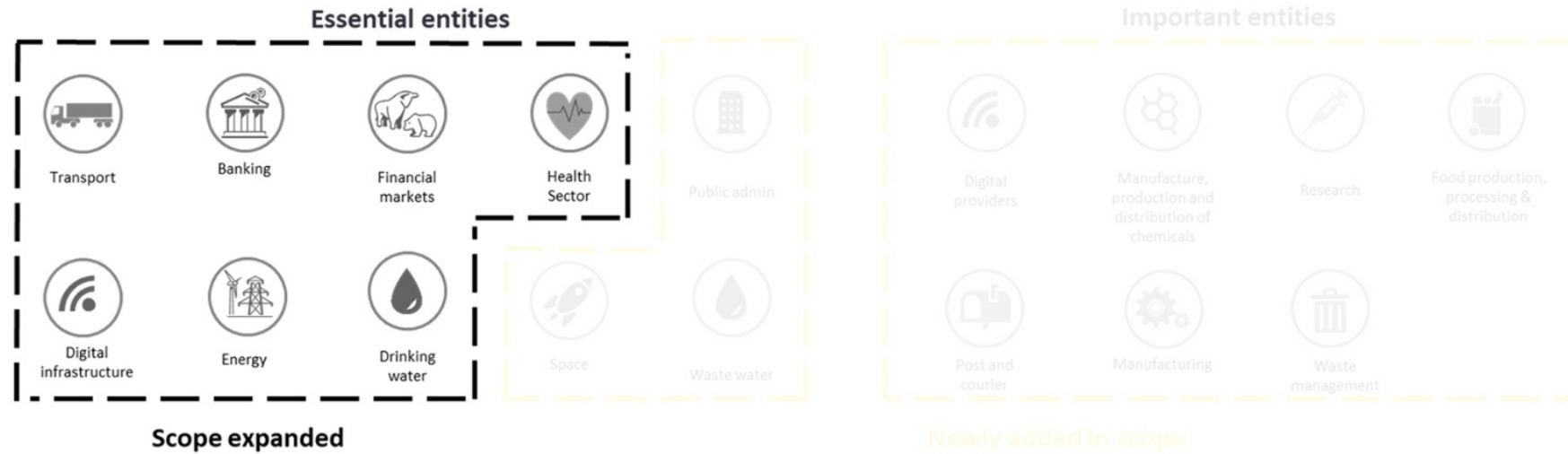
Timelines



Impacted Sectors

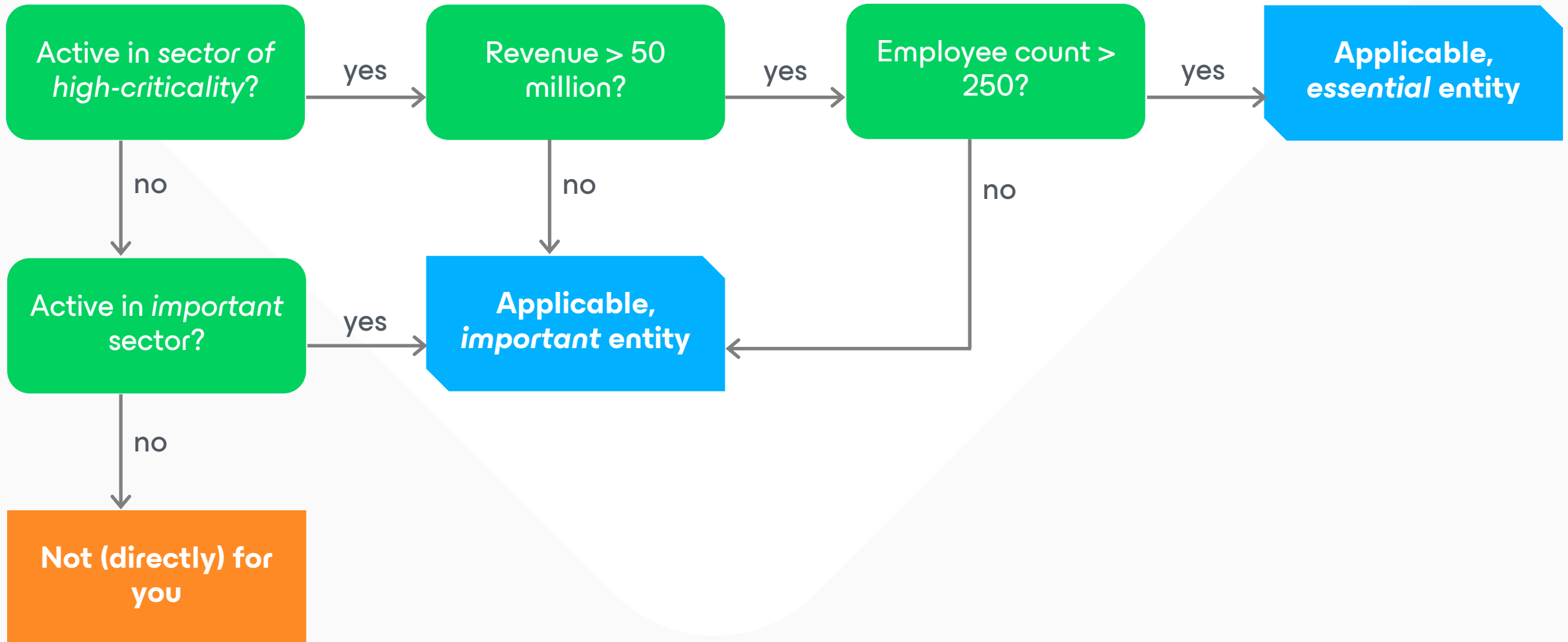
Impacted Sectors

Expansion of NIS



Impacted Sectors

The fingerprint

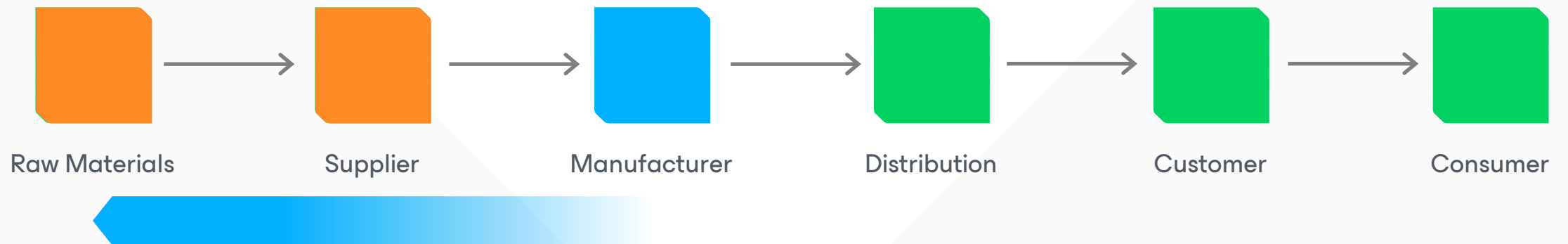


Impacted Sectors

Indirect impact – Supply chain

Not (directly) for
you

?



What does it
mean

What is NIS2

Which obligations does the NIS2 directive impose?

Duty of care

You must carry out a risk assessment. Based on this risk assessment you should take measures to guarantee continuation of services as much as possible and protect the information used.

Duty to report

You have to report incidents to the supervising authority within 24 hours. It concerns incidents that (can) significantly disrupt the provision of the essential services. Does it concern of a cyber incident? Then this must also be reported to the Cyber Security Incident Response Team.

Supervision

Organizations covered by the NIS2 directive will be under supervision. The supervisory body will look at compliance with the obligations of the directive, such as the duty of care and the duty to report. It is currently being worked out which sectors will fall under which supervisory body.

How can Veeam help?

NIS2 goal: Resilience against cyber incidents

Whole Veeam portfolio can help to protect against data loss and ensure service continuity,

- Veeam Data Platform Premium
- Veeam Backup for Microsoft 365
- Veeam Backup for Azure/AWS/Google Cloud
- Kasten by Veeam (backup for Kubernetes)
- Veeam Backup for Salesforce

NIS2 goal: maintaining data integrity; preventing and minimizing the impact of cybersecurity incidents

Veeam immutable backups can help prevent ransomware attacks and unauthorized deletions and changes by making backup data impervious to modifications.

It works **across all supported workloads** in any environment – physical, virtual, cloud

Repository

Repository
Type in path to the folder where backup files should be stored, and set repository load control options.

Location

Path to folder:
/backup Browse...

Capacity: <Unknown> Populate
Free space: <Unknown>

Use fast cloning on XFS volumes (recommended)
Reduces storage consumption and improves synthetic backup performance.

Make recent backups immutable for: 7 days
Protects backups from modification or deletion by ransomware or hackers. GFS full backups are made immutable for the entire duration of their retention policy.

Load control

Running too many concurrent tasks against the repository may reduce overall performance, and cause I/O timeouts. Control storage device saturation with the following settings:

Limit maximum concurrent tasks to: 4

Limit read and write data rate to: 1 MB/s

Click Advanced to customize repository settings. Advanced...

< Previous Next > Finish Cancel

NIS2 goal: safe recovery from incidents

Veeam offers **secure restore** features that can verify the backup integrity and scan for malware before data is restored, thus helping to avoid reintroducing threats into the environment.

The image displays several overlapping windows from the Veeam Backup & Replication console. On the left, a sidebar menu includes 'Upgrade', 'Credentials & Passwords', 'Users & Roles', 'Malware Detection' (highlighted), and 'Network Traffic Rules'. The 'Malware Detection' window shows details for an event: Object: HK-1944-ency, Activity date: 10/2/2023 11:05 AM, Type: Built-in detection engine, Initiated by: LAB\SYSTEM, Status: Suspicious, and Details: Possible malware activity detected. The 'Settings' window for 'Veeam Incident API' shows 'Enable inline entropy analysis' checked, with a sensitivity slider set to 'Normal'. The 'New SureBackup Job' dialog is open, showing the 'Settings' tab where 'Content analysis' is enabled, including 'Scan backup content with an antivirus software' and 'Scan backup content with the following YARA rule: eicary.yara'. The YARA rules location is specified as 'C:\Program Files\Veeam\Backup and Replication\Backup\YaraRules\'. The 'Backup integrity' section has 'Perform backup integrity check' unchecked. The 'Process simultaneously no more than' is set to 3 machines at a time. The 'Backup verification' section has 'Backup verification and content scan only' selected. The Veeam logo is in the bottom right corner.

NIS2 goal: safe recovery from incidents

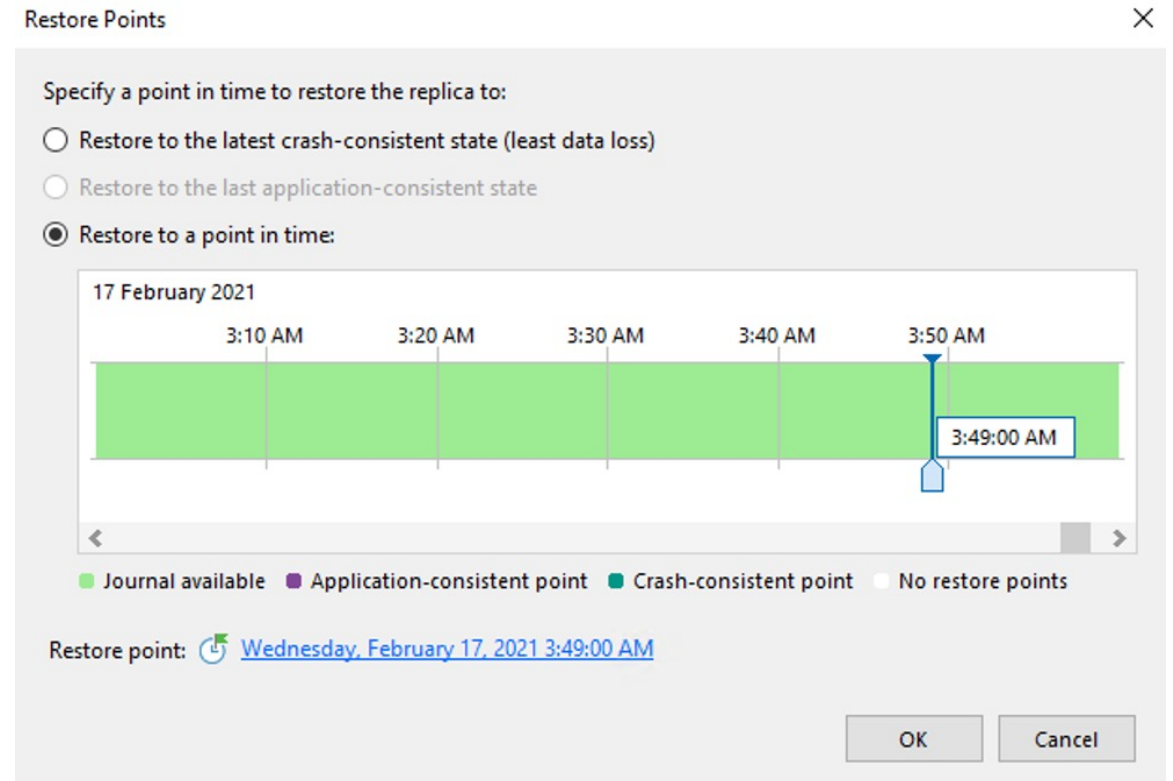
Veeam allows to scan backups **on demand** giving flexibility of scanning any restore point at any given time. This is applicable to backups created **with older versions of our products**.

The image shows a screenshot of the Veeam Backup & Replication console. On the left, the 'Home' view is active, showing a tree structure with 'Backups' expanded to 'Disk'. A context menu is open over a backup job named 'HK-DC01', with the 'Scan backup...' option highlighted by a red rectangle. On the right, the 'Scan Backup' dialog box is displayed. It contains the following information:

- Title:** Scan Backup
- Description:** Performs an ad-hoc scan of you backups with an antivirus or the YARA engine to find the latest malware-free restore point or to detect the presence of specific entries, such as personal information.
- Scan mode:**
 - Find the last clean restore point: Restore points will be scanned sequentially starting from the most recent one until the first malware-free one is found. Use this options when a cyber-attack is known to have started recently.
 - Find the last clean restore point in range: Restore points will be scanned in an optimal order to identify the last clean backup in range with least number of scans possible. Use this option if you are not sure when the attack started, or when dealing with a known sleeping malware.
 - Scan all restore points in range for content analysis: All restore points in range will be scanned sequentially. Use this option for backup content analysis with an applicable YARA rule, for example to look for personally identifiable information (PII), personal health information (PHI) or payment card industry (PCI) data.
- Scan engine:**
 - Scan restore points with an antivirus
 - Scan restore points with the following YARA rule: eicar.yar
- YARA rules location:** C:\Program Files\Veeam\Backup and Replication\Backup\YaraRules\
- Scan range:**
 - From:** Most recent restore point
 - To:** Oldest available restore point
 - Start date:
 - End date:
 - Continue scanning all remaining files after the first occurrence
- Buttons:** Hide scan range, OK, Cancel

NIS2 goal: resilience and quick recovery

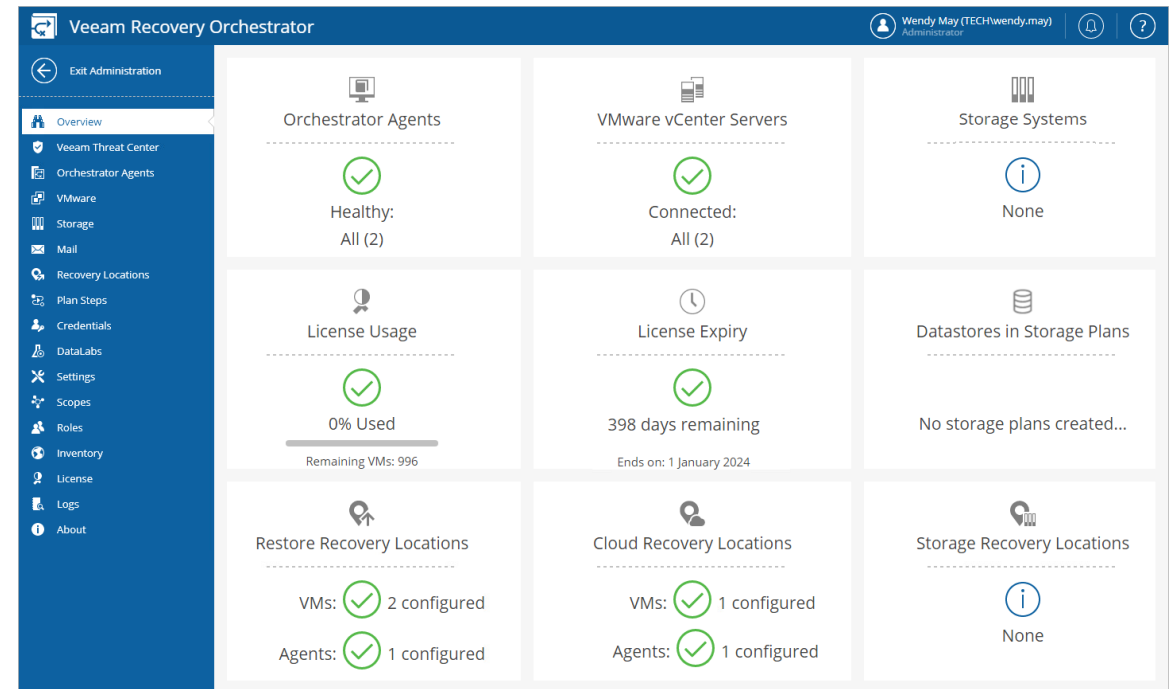
Veeam's **Continuous Data Protection** can provide near-zero recovery point objectives (RPOs) for critical workloads, ensuring that businesses can recover their data quickly in the event of cyber incidents or data corruption.



NIS2 goal: resilience and quick recovery

Through **Veeam Recovery Orchestrator**, businesses can automate and simplify disaster recovery planning, ensuring that they are prepared for a wide variety of scenarios

- With VRO organisation can **create** DR plans and **test** them to ensure they will work when they need it most
- Documentation of DR plans is **updated automatically**
- VRO can **automate** recovery, orchestrating **all recovery workflows** and help to speed up recovery regardless where DR site is (on-prem or cloud)



NIS2 goal: compliance with risk management and reporting obligations

Utilizing Veeam ONE, the Veeam Data Platform Premium offers solutions for real-time monitoring, reporting, and capacity planning for the backup infrastructure.

VEEAM

Malware Detection

Description

This report provides a precise overview of detected malware anomalies in the infrastructure. It logs all incidents across workloads and restore points allowing you to quickly identify compromised and clean data.

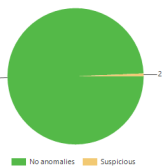
Report Parameters

Scope: Backup Infrastructure
 Workload status: All
 Events to show: 5

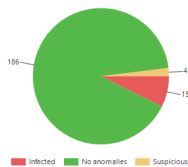
Summary

Malware-analyzed workloads		Malware-analyzed restore points		Top 5 Backup Servers with workloads anomalies		
Total workloads:	301	Total restore points:	205	Backup Server	Suspicious	Infected
Suspicious:	2	Infected:	15	mmf-win16vbr.tech.local	2	0
No anomalies:	299	Suspicious:	4			
		No anomalies:	186			
		No anomalies:	186			

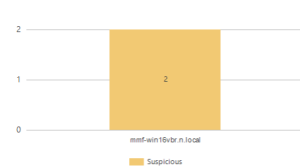
Malware-analyzed workloads



Malware-analyzed restore points



Top 5 backup servers with workloads anomalies



Security Scorecard
 Updated 3 hours ago
 93.2%
 Well done
 Your Data Platform Status Score is above 90%.
 One or more Backup Servers have not been updated to the latest release. Please consider upgrading for an accurate score.

- 91% Platform Security Compliance (230 up, 12 down)
- 100% Data Recovery Health (120 up, 0 down)
- 89% Data Protection Status (29 up, 236 down)
- 93% Backup Integrity Status (246 up, 19 down)

Malware Detections
 Updated 3 hours ago
 640† Infected Restore Points
 356† Suspicious Restore Points
 360 Marked as Clean
 Most Affected Object: workload-1299
 There are some repositories without mapping. Go to widget settings.

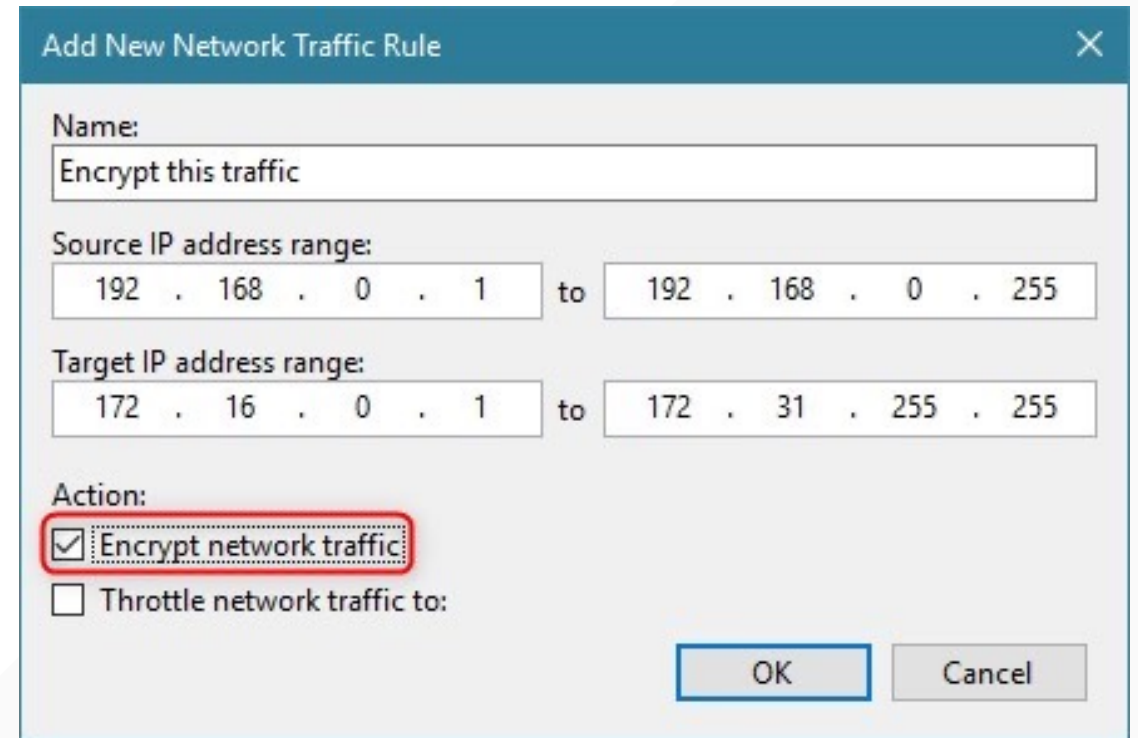
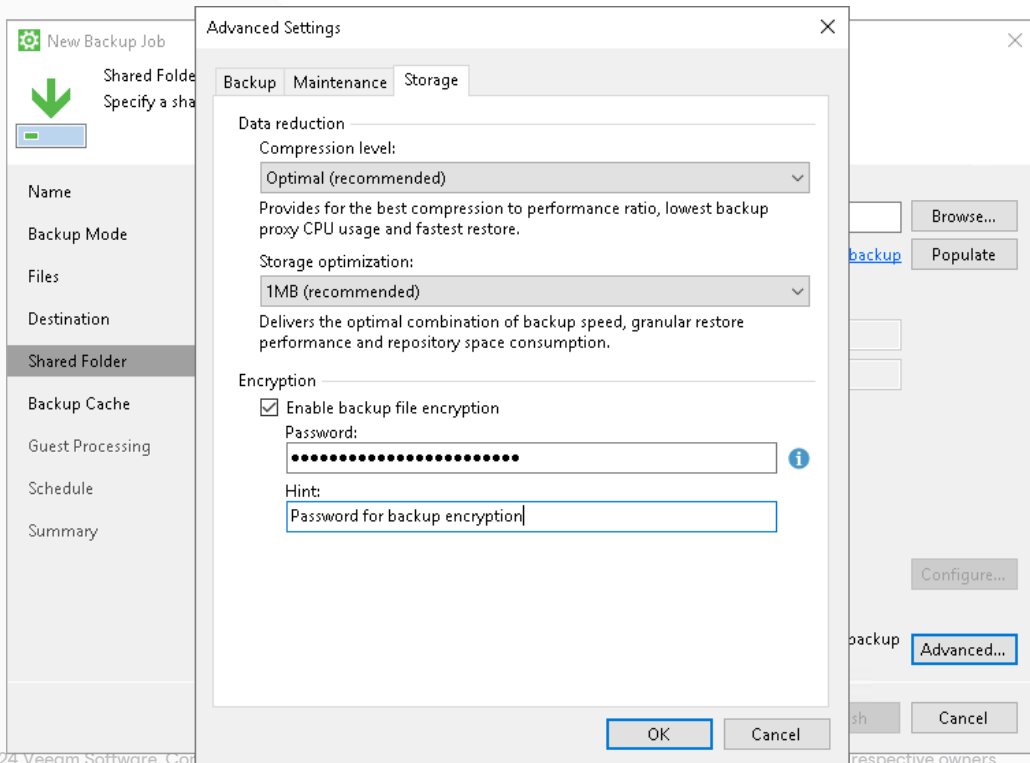
RPO Anomalies
 Updated 35 minutes ago

Workload	Type	Backup Server	Last Success	Missing RPO
ES-win12-vo.tech.local	Computer	ES-win2016-WS.tech.local	11/20/2023 9:00:00 AM	Less than an...
azure-files	Cloud Instance	mmf-win16vbr.tech.local	11/20/2023 11:20:01 AM	8 hours
ES-win19-orac2.tech.local	Computer	ES-win19-vbr2.tech.local	11/19/2023 7:44:18 PM	14 hours
ES-win19-V10_5.tech.local	Unstructured Data	ES-win19-V10_5.tech.local	11/19/2023 6:25:19 PM	15 hours
shared-empty-multi-disks-d-04	Virtual Machine	mmf-win16vbr.tech.local	11/19/2023 7:03:33 AM	A day
shared-empty-multi-disks-d-01	Virtual Machine	mmf-win16vbr.tech.local	11/19/2023 7:01:59 AM	A day
shared-empty-multi-disks-d-03	Virtual Machine	mmf-win16vbr.tech.local	11/19/2023 7:01:57 AM	A day
shared-empty-multi-disks-d-02	Virtual Machine	mmf-win16vbr.tech.local	11/19/2023 7:00:47 AM	A day
shared-empty-d-12	Virtual Machine	mmf-win16vbr.tech.local	11/19/2023 7:00:37 AM	A day
ES-win19-orac3.tech.local	Computer	ES-win2016-WS.tech.local	11/18/2023 5:03:53 PM	A day

SLA Compliance Overview
 Updated 3 hours ago
 Total SLA: 92.6%
 Sessions: 20,565
 99.8% Success Percentage
 Total Sessions: 58
 Succeeded Sessions: 56
 Failed Sessions: 2

NIS2 goal: data confidentiality and integrity

Veeam provides options to **encrypt backup data at rest and in transit**, helping to protect sensitive data from unauthorized access or interception.





Follow us!



Join the community hub:

