...než povoláte ZÁLOHY

#ransomware2024

Boris Mittelmann

Senior Systems Engineer
Veeam Software CEE

UNDERSTANDING CYBERATTACKS

Understanding cyberattacks

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

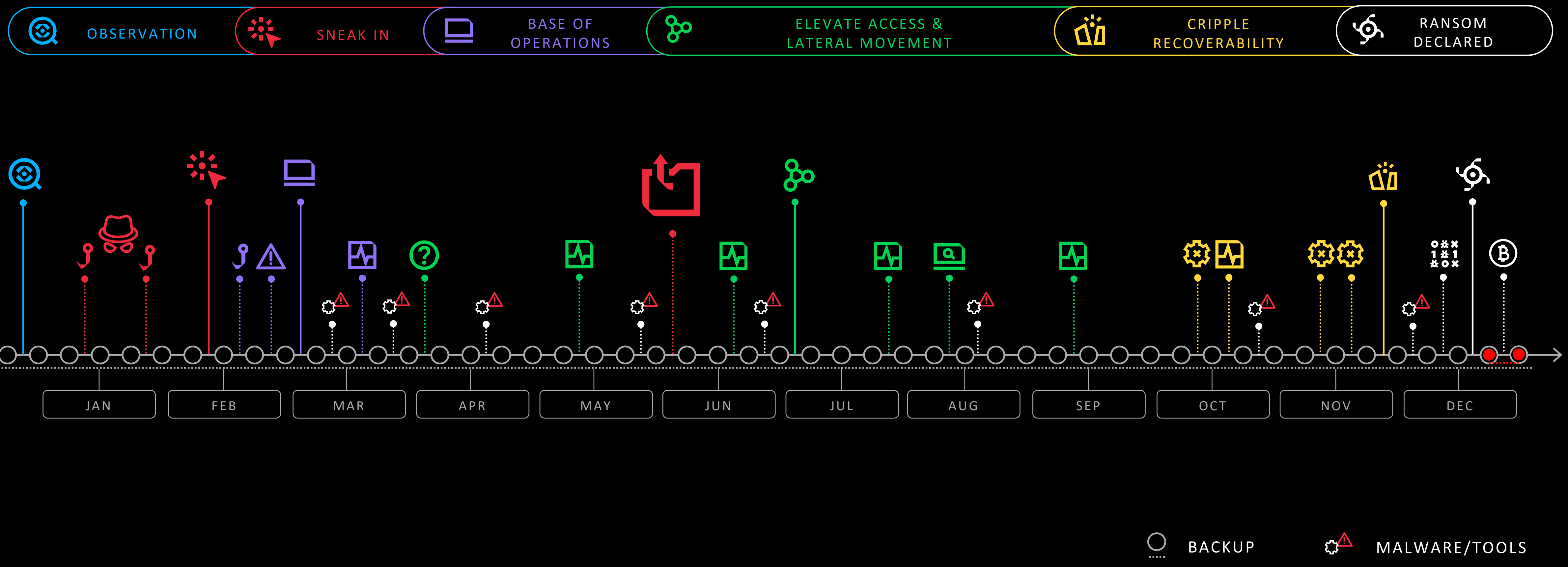
Gain access to the victim by sending phishing emails and let them click a link

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!



OBSERVATION

SNEAK IN

BASE OF OPERATIONS

ELEVATE ACCESS & LATERAL MOVEMENT

CRIPPLE RECOVERABILITY

RANSOM DECLARED

VŽDY predpokladajte úspešný prienik útočníka

[Nová správa zistila, že zločinci používajú umelú inteligenciu na škodlivé účely – a nejde len o deepfakes | (europa.eu)](europa.eu)

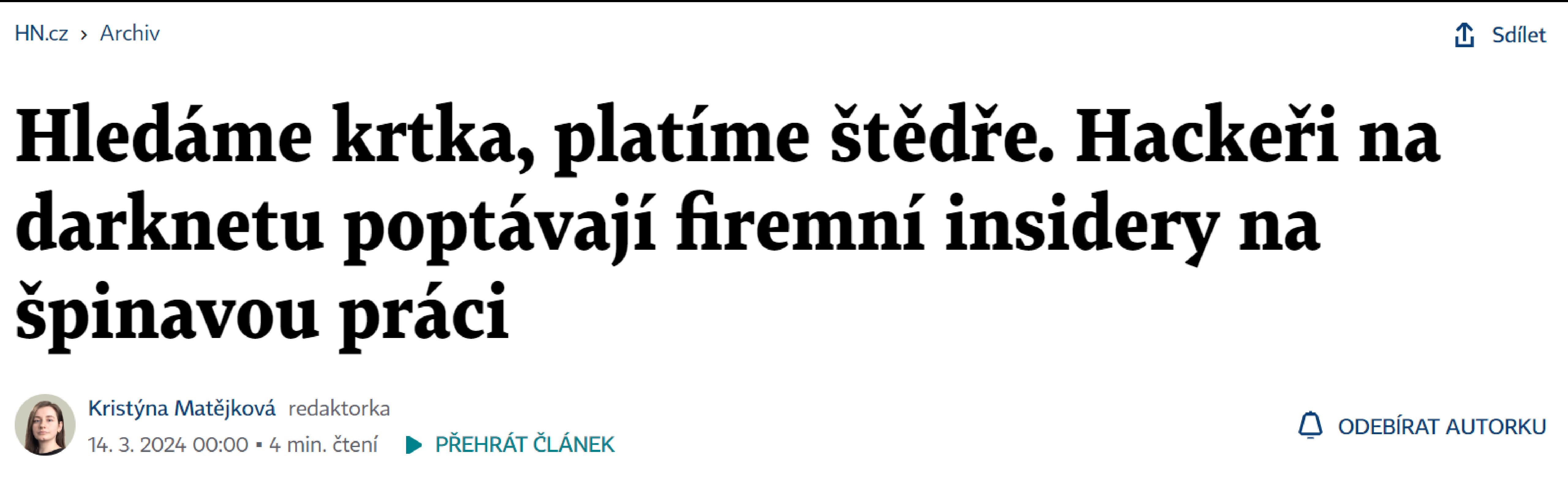
Počiatočné predpoklady návrhu kybernetickej bezpečnosti:

- Nemáte lepšie vybavenie ako útočník
- Nemáte viac vedomostí ako útočník
- Neviete viac o útočníkovi ako on o vás
- Nemáte ani zďaleka toľko času ako útočník
- Musíte minimalizovať dopad útoku

Platby ransomvéru dosiahli v roku 2023 rekordných 1,1 MLD USD

VŽDY předpokládejte úspěšný průnik útočníka

Nová zpráva zjistila, že zločinci využívají umělou inteligenci ke škodlivým účelům – a nejde jen o deep fakes | (europa.eu)



HN.cz › Archiv

Sdílet

Hledáme krtka, platíme štědře. Hackeři na darknetu poptávají firemní insidery na špinavou práci

Kristýna Matějková redaktorka

14. 3. 2024 00:00 ▪ 4 min. čtení

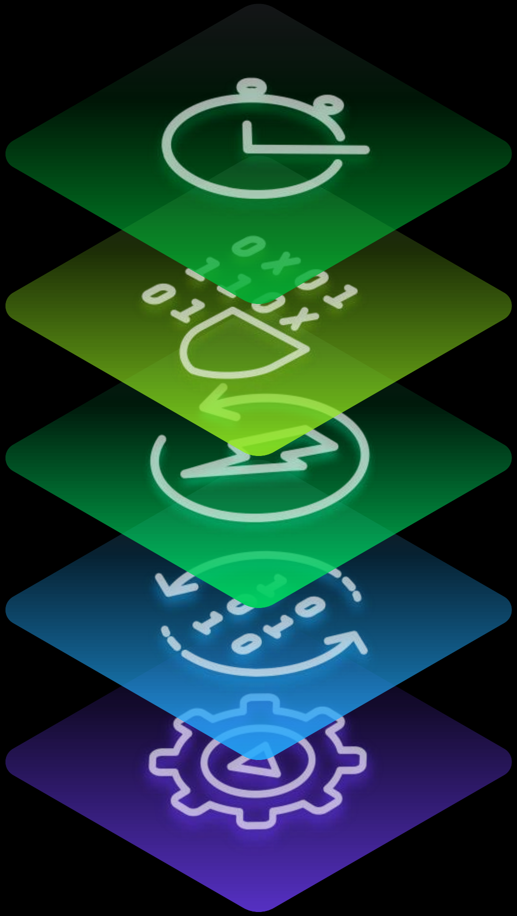
▶ PŘEHRÁT ČLÁNEK

ODEBÍRAT AUTORKU

Platby ransomwaru dosáhly v roce 2023 rekord 1,1 Mld. USD

ReSTORE vs. ReCOVER – KnowBe4!!!

Immutable
Hardened
Air-gapped



Multi-layered immutability

Comprehensive monitoring

Automatic recovery verification

Fastest recovery options

Complete data mobility

...už dnes NESTAČÍ!

Multi-layered immutability

Veeam Ready Object
with Immutability

Veeam READY
Object with Immutability

Veeam Cloud Connect
with Insider Protection

WORM (Write Once Read Many)
– Or Tape media
Physical air gap

Veeam Hardened Repository
with Immutability and single
use credentials

WORM storage snapshots

Offline, Air-Gapped Media copies on disk
(Removable/rotating)

Immutable device on either
dedupe or object repository

Snapshot and CDP replication
dependent on retention but fastest RTO

Backup Target Storage Vendor Immutability Integrations

Ensure that your data is protected from Ransomware

Integrated and Veeam Ready vendor qualified object storages with compliance immutability

11:11 SYSTEMS, aws, Azure, Backblaze, ceph

CLOUDIAN, DELL Technologies, DATACORE, HITACHI, IBM Cloud

IDrive, Infortrend, iTernity, MINIO, NetApp

NUTANIX, NGX, OBJECT FIRST, OSNEXUS, Quest

QNAP, OVHcloud, Quantum, PURESTORAGE, RSTOR

SCALITY, SEAGATE, STONEFLY, SOFTIRON, SPECTRA

SUSE, Ugloo, VAST, wasabi, zadara

EXAGRID

Integrated and Veeam Ready block and deduplication storage vendors with immutability

DELL Technologies, Hewlett Packard Enterprise, Lenovo

EXAGRID

veeam Veeam Hardened Linux Repository

Veeam Hardened Linux Repository is compatible with all major server vendors like …

CISCO, DELL Technologies, Hewlett Packard Enterprise, SUPERMICRO

External controlled immutability (compatible)

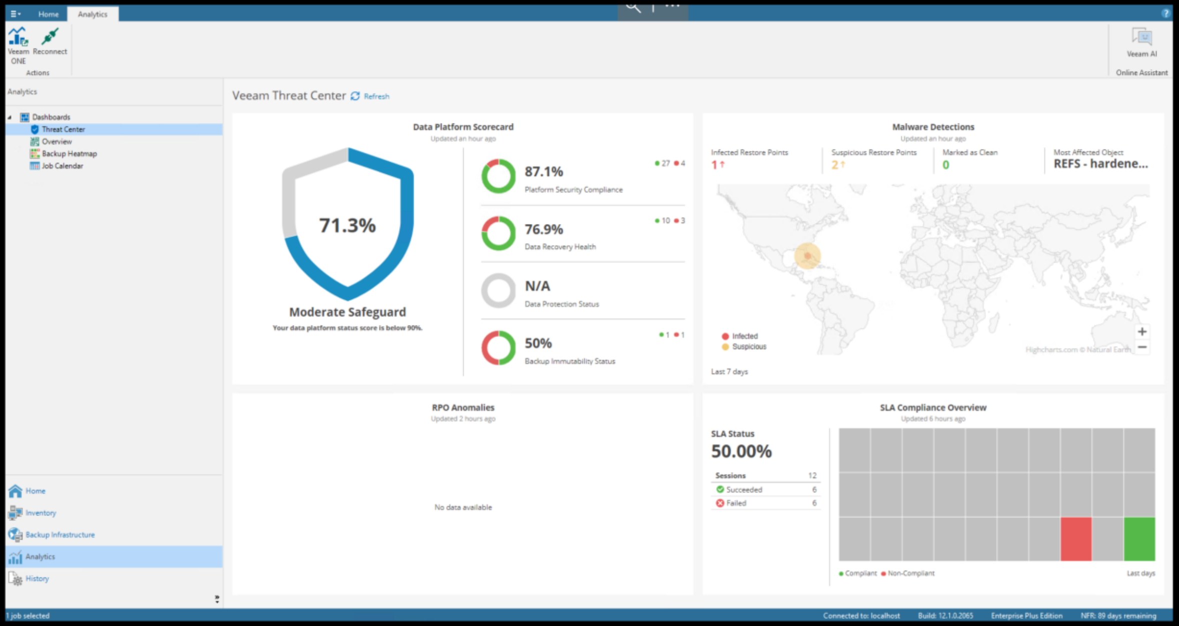
PURESTORAGE, FUJITSU

Hewlett Packard Enterprise, INFINIDAT

Lenovo, NetApp

EXAGRID, VAST

ReSTORE vs. ReCOVER – KnowBe4!!!



Veeam Threat Center

Data Platform Scorecard
Updated an hour ago

71.3%
Moderate Safeguard
Your data platform status score is below 90%.

87.1% Platform Security Compliance ● 27 ● 4
76.9% Data Recovery Health ● 10 ● 3
N/A Data Protection Status
50% Backup Immutability Status ● 1 ● 1

Malware Detections
Updated an hour ago

Infected Restore Points	Suspicious Restore Points	Marked as Clean	Most Affected Object
1 ↑	2 ↑	0	REFS - hardene...

● Infected
● Suspicious
Highcharts.com © Natural Earth
Last 7 days

RPO Anomalies
Updated 2 hours ago
No data available

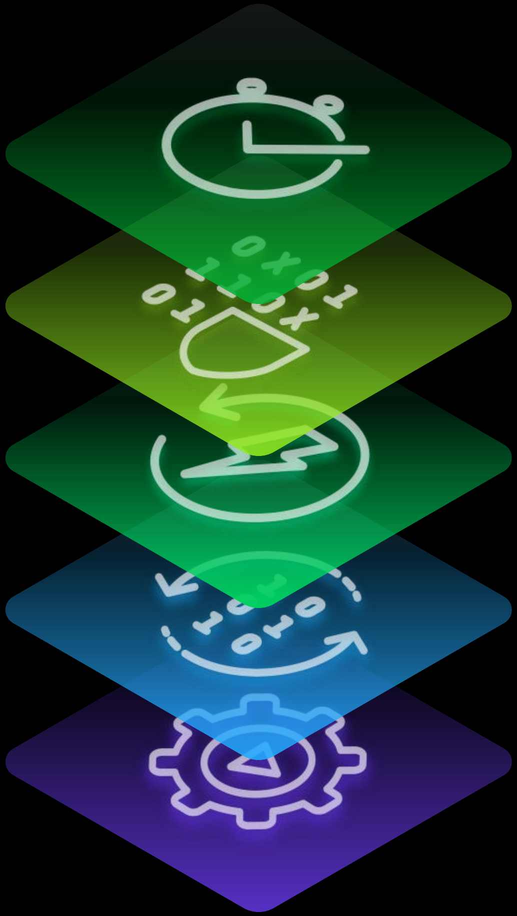
SLA Compliance Overview
Updated 6 hours ago

SLA Status
50.00%

Sessions	12
✓ Succeeded	6
✗ Failed	6

● Compliant ● Non-Compliant
Last days

1 job selected   Connected to: localhost   Build: 12.1.0.2065   Enterprise Plus Edition   NFR: 89 days remaining



Multi-layered immutability

Comprehensive monitoring

Automatic recovery verification

Fastest recovery options

Complete data mobility

Detect + identify cyberthreats

Minimize the devastation of a cyberattack

Data Security

Keep your data safe with multi-layered security that gives you confidence your data is always protected.

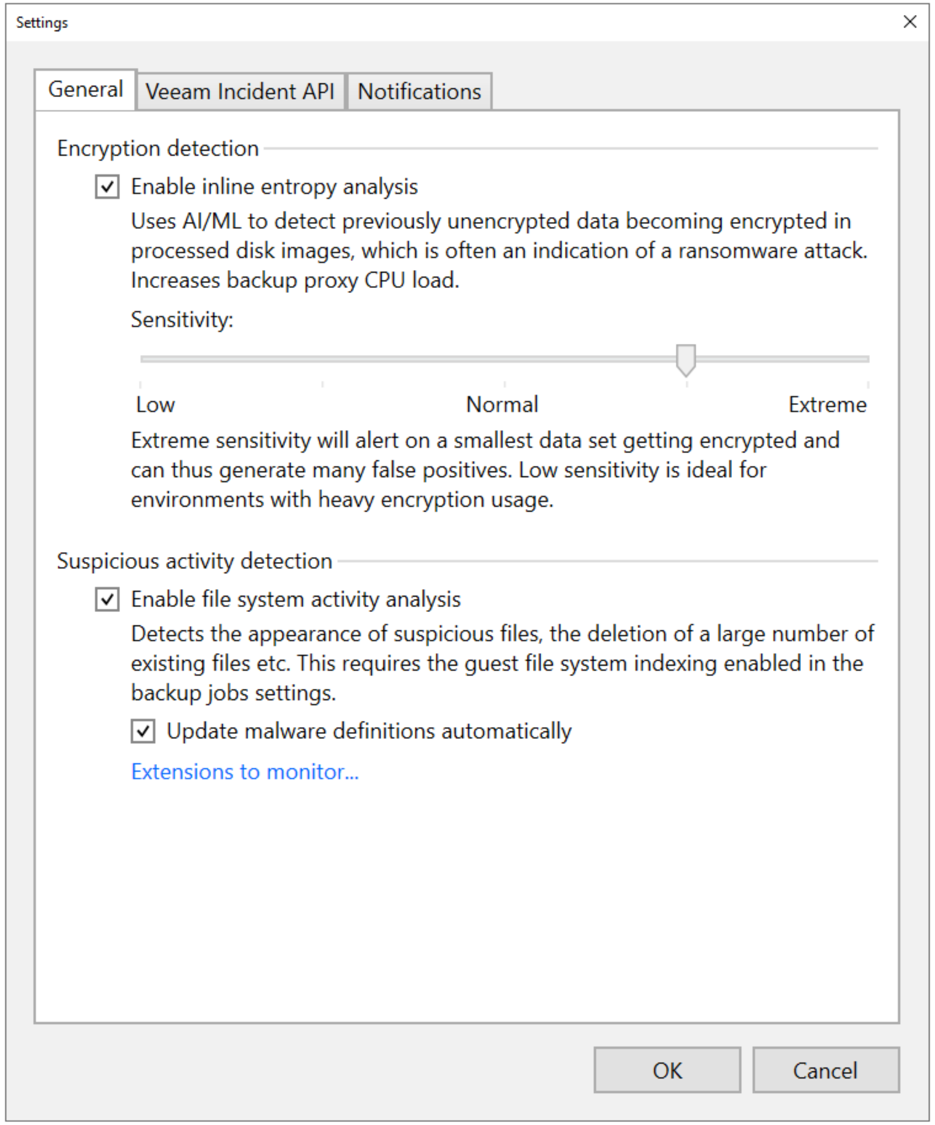
- Malware Detection
- Synchronous communication with ServiceNOW
- Veeam App for Splunk
- Veeam Incident API

Malware Detection

AI-powered inline scanning and file system analysis

Bring detection closer to the time of infection

- Measure and analyze entropy changes
- Detect known indicators of compromise (IoC)
- Mark backups as *clean, suspect,* or *infected*



Encryption detection

☑ Enable inline entropy analysis

Uses AI/ML to detect previously unencrypted data becoming encrypted in processed disk images, which is often an indication of a ransomware attack. Increases backup proxy CPU load.

Sensitivity:

Extreme sensitivity will alert on a smallest data set getting encrypted and can thus generate many false positives. Low sensitivity is ideal for environments with heavy encryption usage.

Suspicious activity detection

☑ Enable file system activity analysis

Detects the appearance of suspicious files, the deletion of a large number of existing files etc. This requires the guest file system indexing enabled in the backup jobs settings.

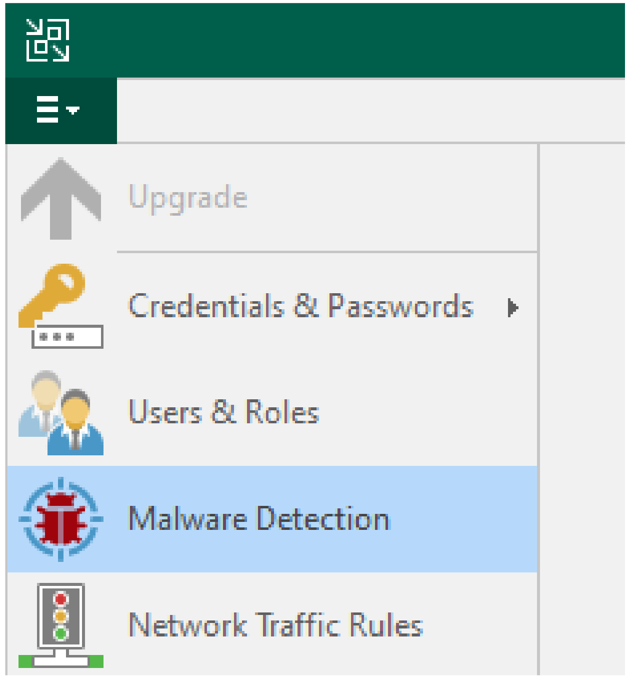
☑ Update malware definitions automatically

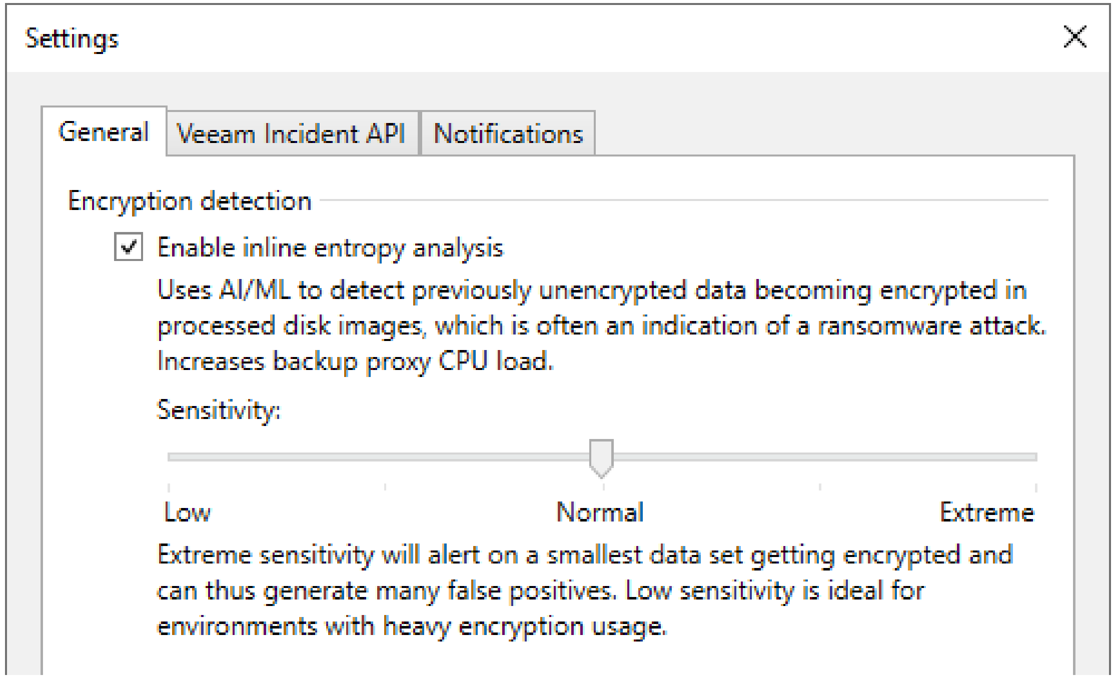
Extensions to monitor...

Inline Malware Detection

encryption detection & text analysis

- analyzes block-level data during backup





Encryption detection

☑ Enable inline entropy analysis

Uses AI/ML to detect previously unencrypted data becoming encrypted in processed disk images, which is often an indication of a ransomware attack. Increases backup proxy CPU load.

Sensitivity:

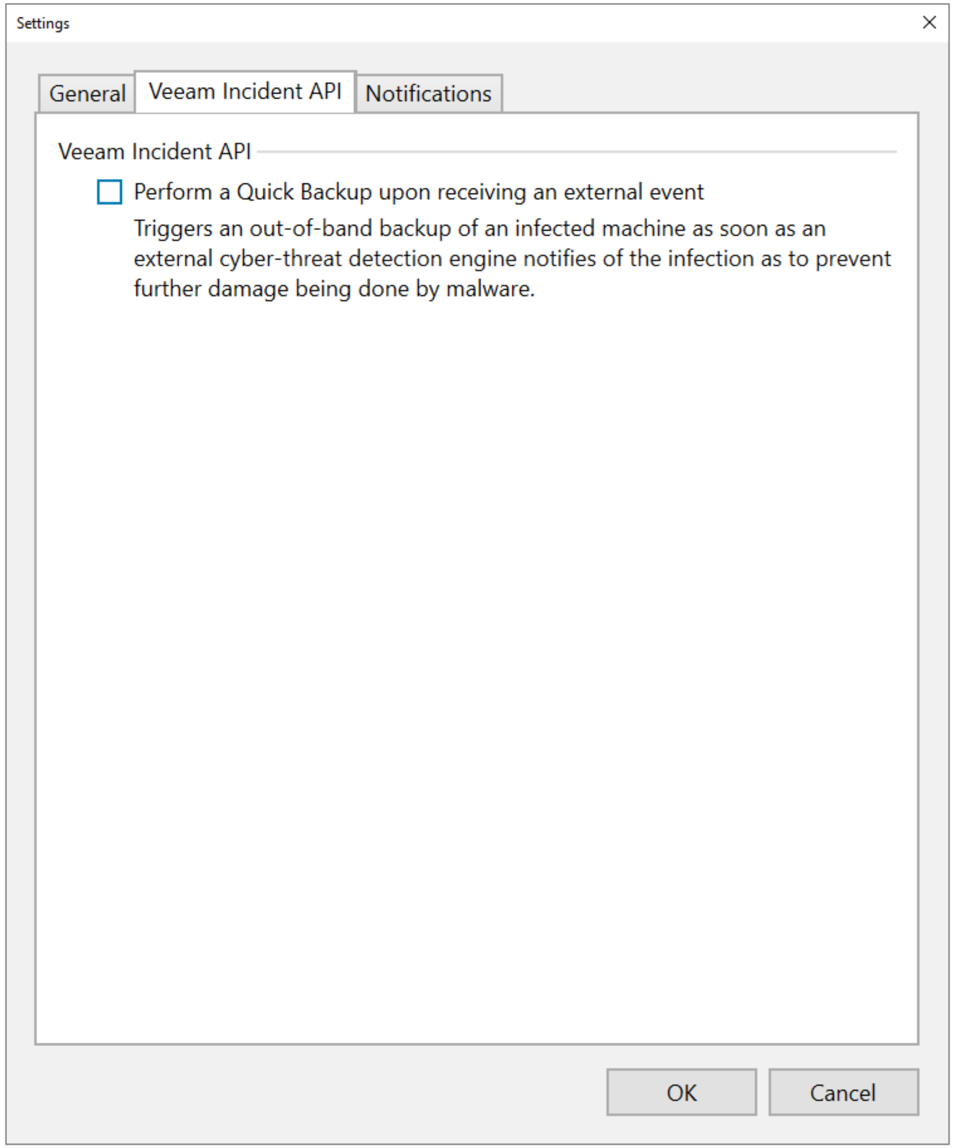
Extreme sensitivity will alert on a smallest data set getting encrypted and can thus generate many false positives. Low sensitivity is ideal for environments with heavy encryption usage.

Veeam Incident API

Get a second opinion

Receive real-time infection reports from third party tools

- Integrate with existing NDR/EDR/XDR tools
- Remove barriers between security and backup teams
- Minimize damage by immediately performing backups upon notification

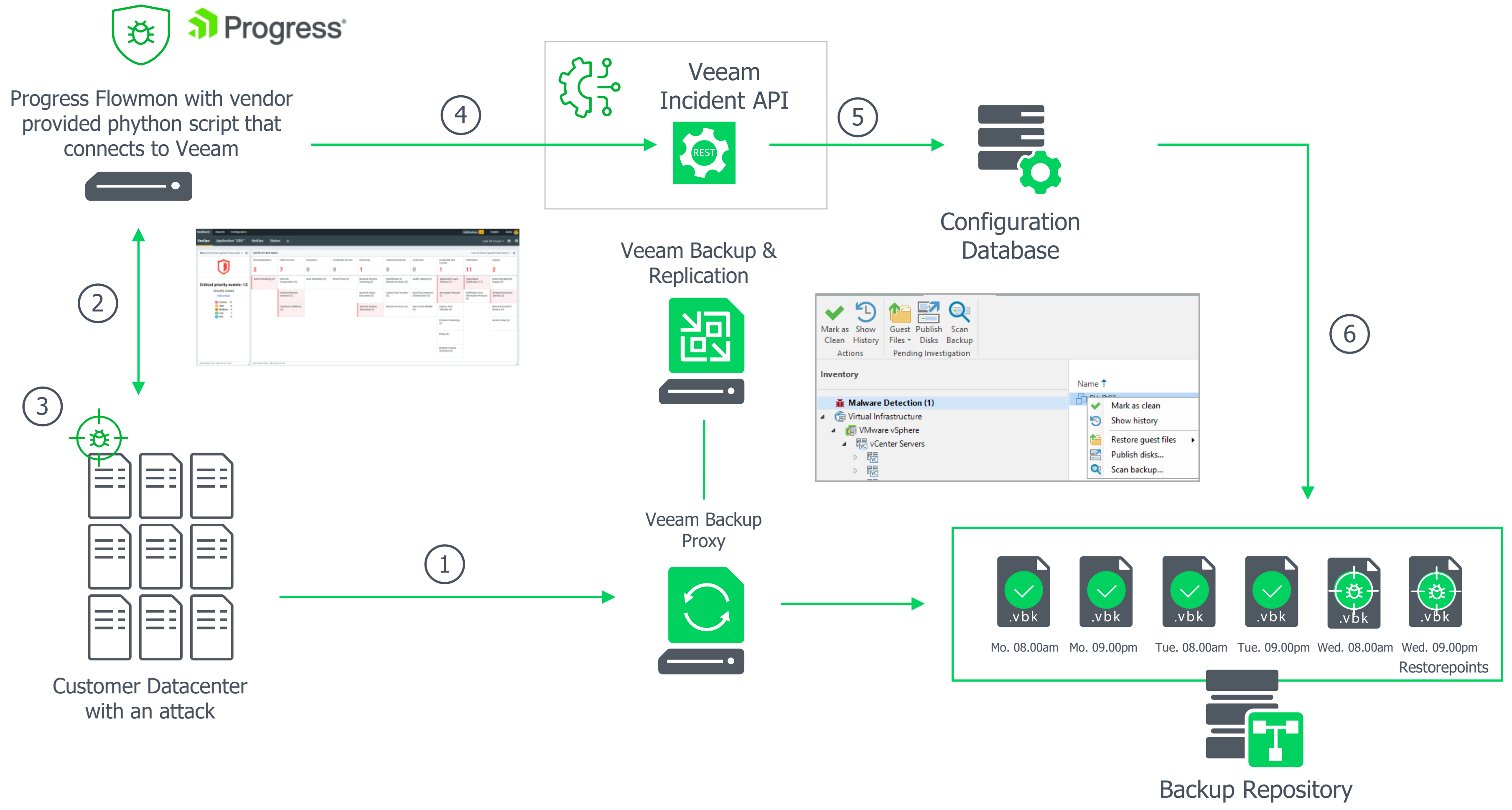


Veeam Incident API

□ Perform a Quick Backup upon receiving an external event

Triggers an out-of-band backup of an infected machine as soon as an external cyber-threat detection engine notifies of the infection as to prevent further damage being done by malware.

Veeam Incident API with Progress Flowmon



1 Veeam Backup & Replication runs regular backups of the source systems

2 External CyberProtection solutions are monitoring the environment

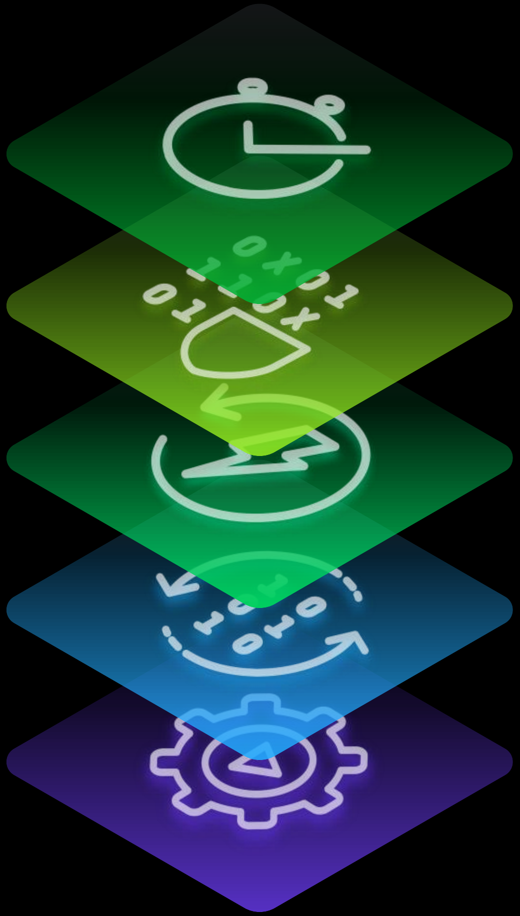
3 The external CyberProtection detects suspicious activities or a Ransomware attack

4 The external CyberProtection calls the Veeam Incident API and sends details of the incident

5 Veeam Backup & Replication flags any restore point created after the detection as potentially infected in the configuration database

6 This is also reflected in the GUI where those restore points now show up as clean or infected

ReSTORE vs. ReCOVER – KnowBe4!!!



Multi-layered immutability

Comprehensive monitoring

Automatic recovery verification

Fastest recovery options

Complete data mobility

Respond + recover from ransomware

Empower your team to slash incident response time

Data Recovery

Breadth and scalability enables you to reliably perform Instant Recovery

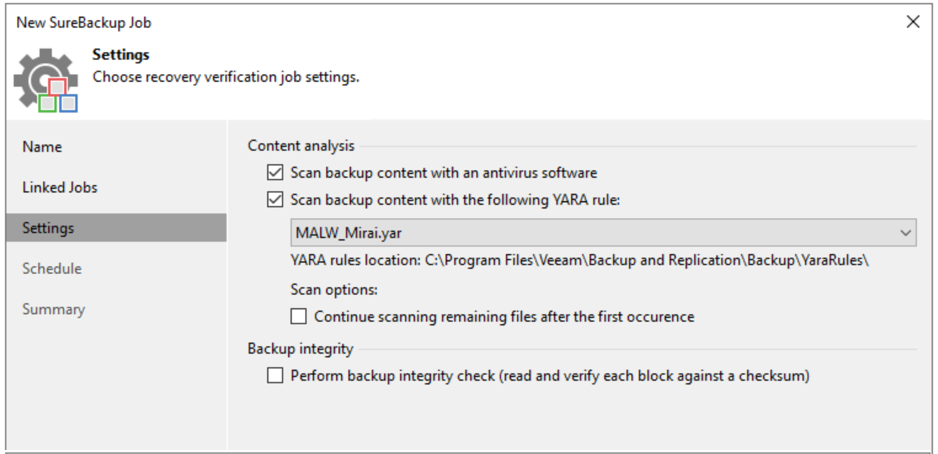
- Avoid reinfection
- YARA content analysis
- Recover clean the first time
- I/O Anomaly Visualizer

Avoid reinfection

Uncover threats before you restore

Automated offline malware detection

- Automated scheduled scans that support the *new* SureBackup® mode
- Orchestrated ad-hoc scans to assist with investigations
- Powered by **both** antivirus engines and/or YARA rules



New SureBackup Job

Settings
Choose recovery verification job settings.

Content analysis

☑ Scan backup content with an antivirus software

☑ Scan backup content with the following YARA rule:

MALW_Mirai.yar

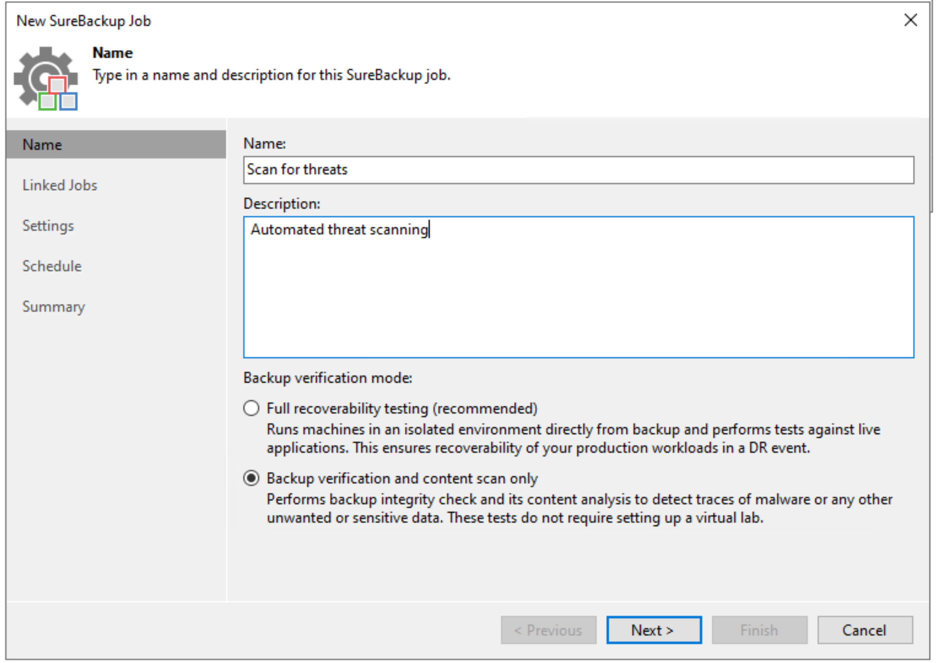
YARA rules location: C:\Program Files\Veeam\Backup and Replication\Backup\YaraRules\

Scan options:

□ Continue scanning remaining files after the first occurence

Backup integrity

□ Perform backup integrity check (read and verify each block against a checksum)



New SureBackup Job

Name
Type in a name and description for this SureBackup job.

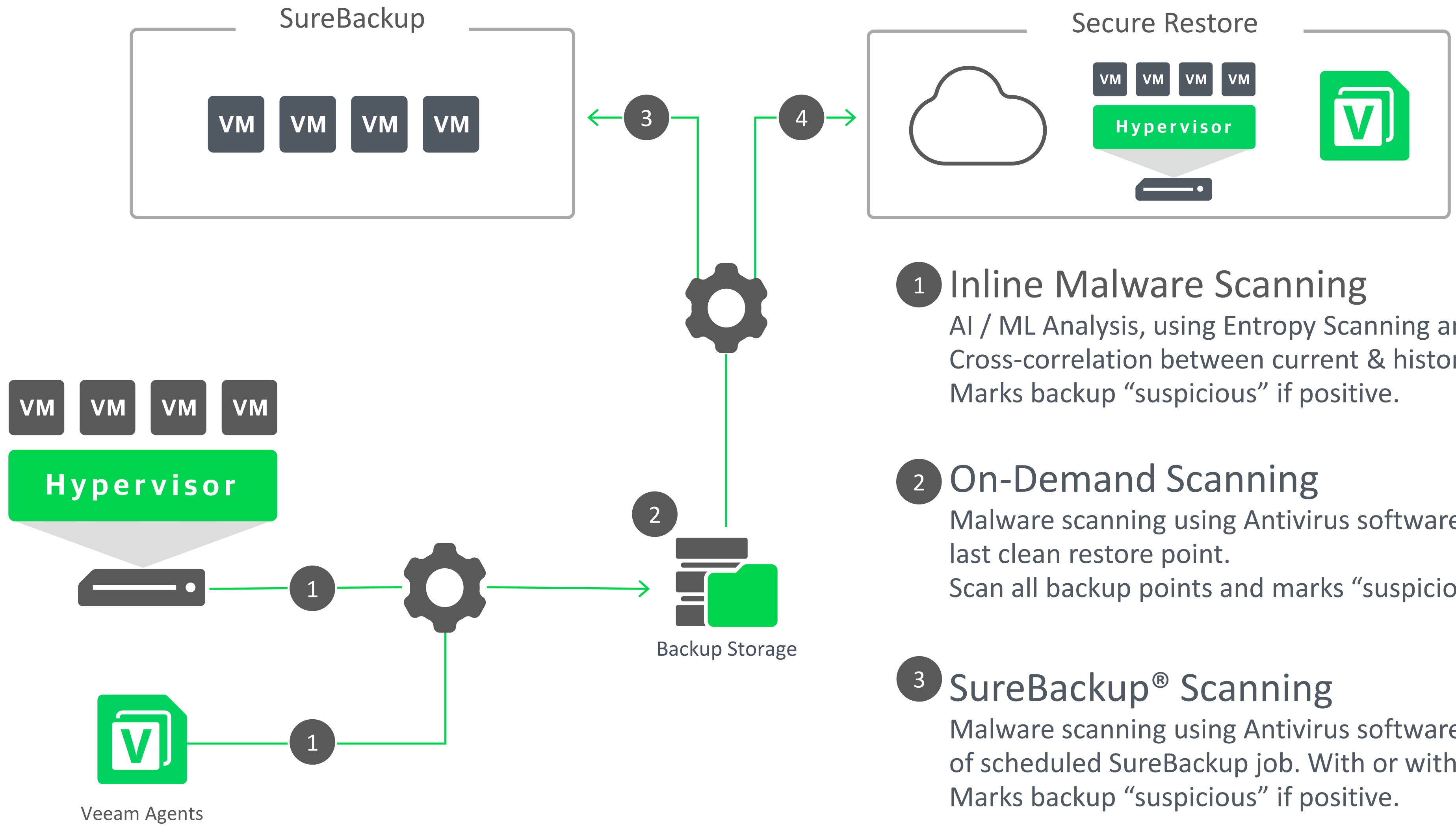
Name: Scan for threats

Description: Automated threat scanning

Backup verification mode:

○ Full recoverability testing (recommended)
Runs machines in an isolated environment directly from backup and performs tests against live applications. This ensures recoverability of your production workloads in a DR event.

● Backup verification and content scan only
Performs backup integrity check and its content analysis to detect traces of malware or any other unwanted or sensitive data. These tests do not require setting up a virtual lab.



1 Inline Malware Scanning

AI / ML Analysis, using Entropy Scanning and in-guest filesystem index.
Cross-correlation between current & historic values.
Marks backup “suspicious” if positive.

2 On-Demand Scanning

Malware scanning using Antivirus software and/or YARA rules to find the last clean restore point.
Scan all backup points and marks “suspicious” if positive.

3 SureBackup® Scanning

Malware scanning using Antivirus software and/or YARA rules as a part of scheduled SureBackup job. With or without DataLabs.
Marks backup “suspicious” if positive.

4 Secure Restore Scanning

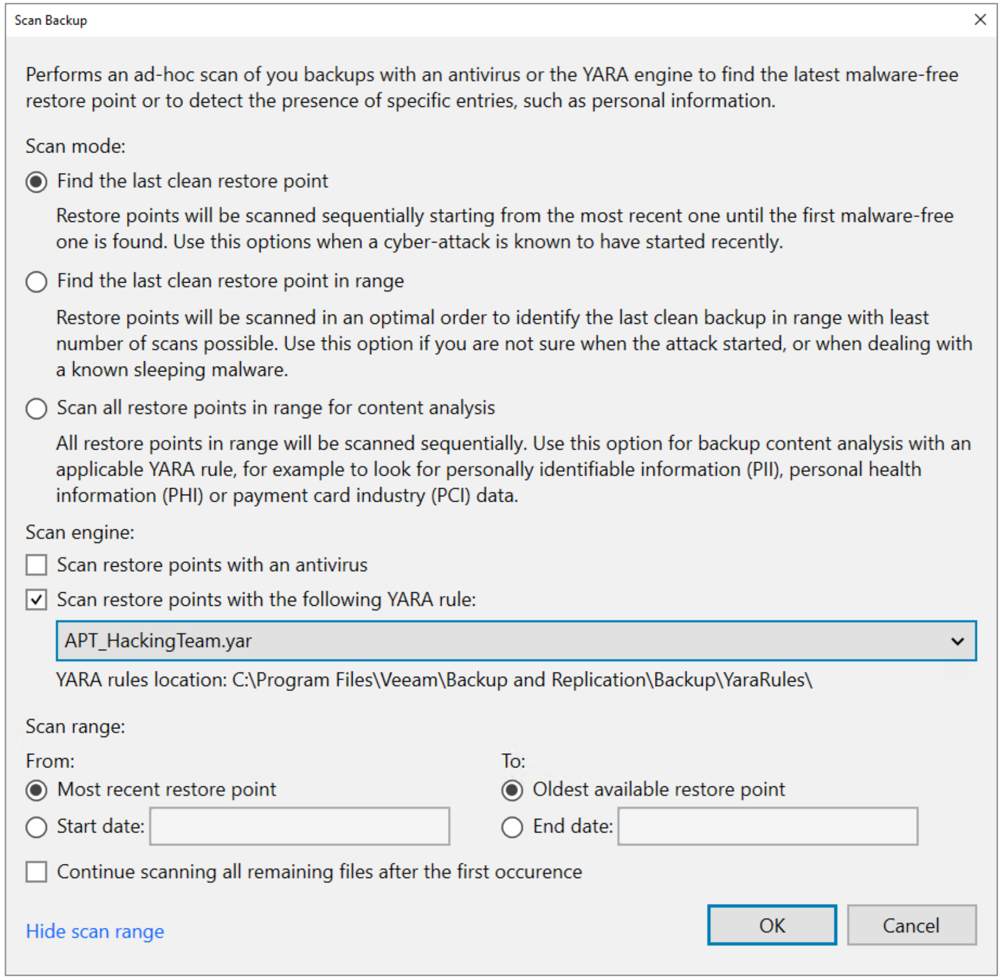
Malware scanning using Antivirus software and/or YARA rules on any Image based restore task. Marks backup “suspicious” if positive.

YARA content analysis

Know what potential risks may be hiding in your backups

Pinpoint ransomware strains in your environment

- Comprehensive and customizable signature-based detection
- Uncover threats almost in real time with Continuous Data Protection (CDP) replicas
- Detect compliance violations



Scan Backup

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:

APT_HackingTeam.yar

YARA rules location: C:\Program Files\Veeam\Backup and Replication\Backup\YaraRules\

Scan range:

From:

● Most recent restore point

○ Start date:

To:

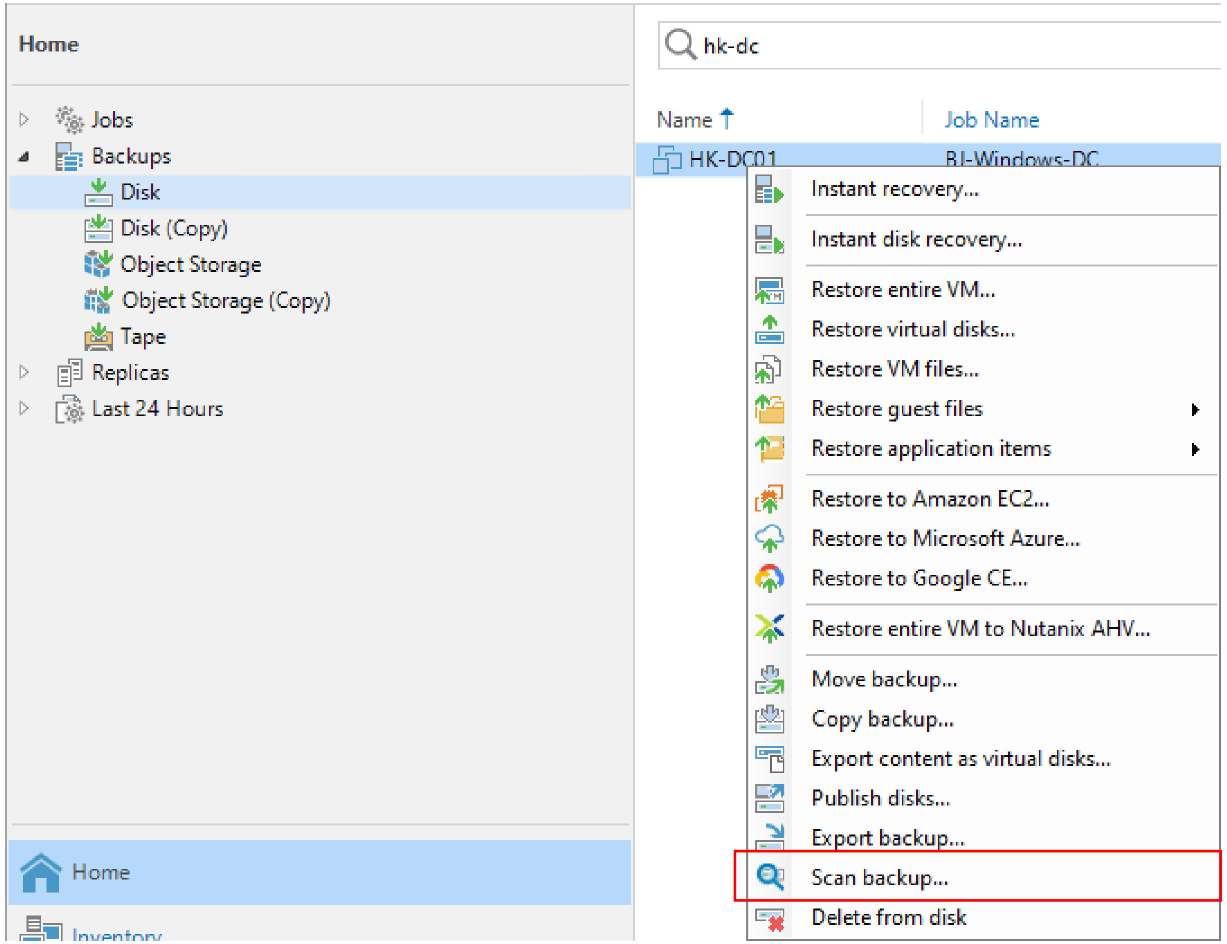
● Oldest available restore point

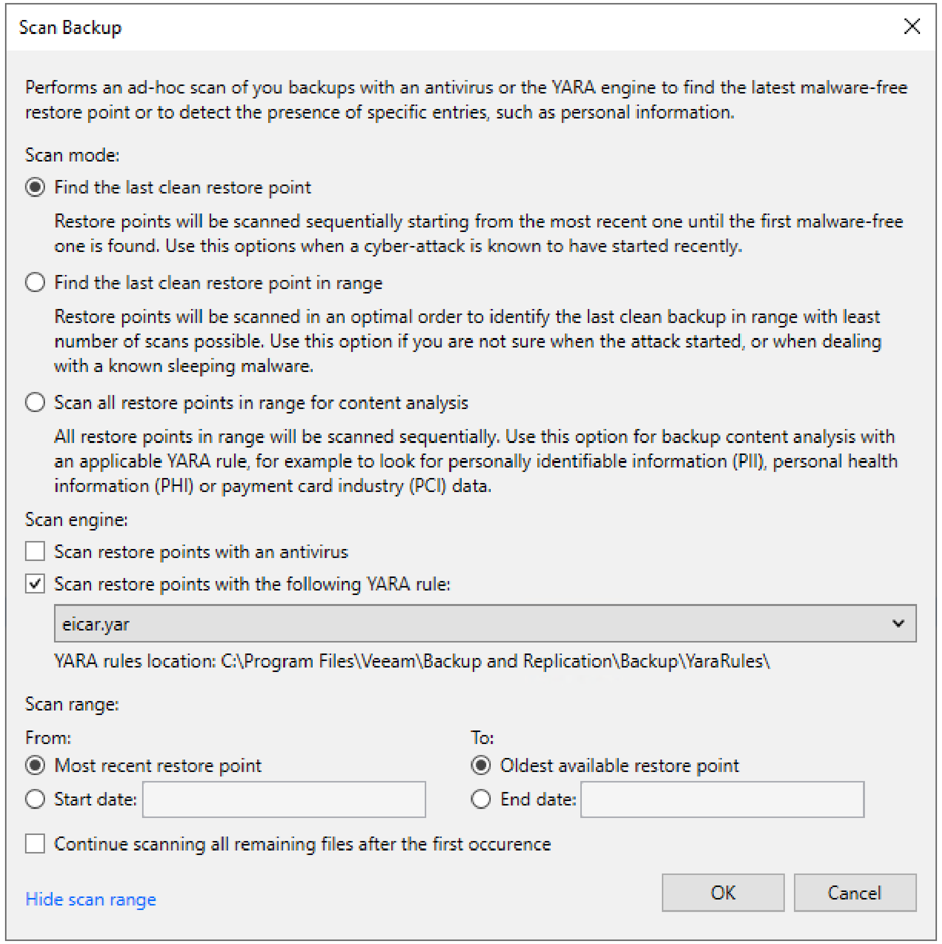
○ End date:

□ Continue scanning all remaining files after the first occurence

On-Demand Scan For Malware & Content

in Backups section





Scan Backup

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

○ Start date:

To:

● Oldest available restore point

○ End date:

□ Continue scanning all remaining files after the first occurence

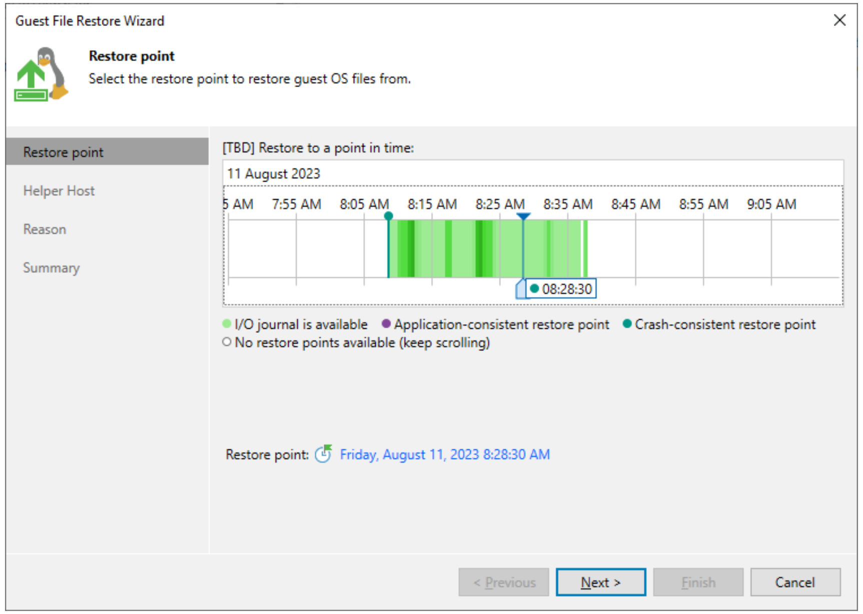
04032024

I/O Anomaly Visualizer

For when seconds matter

Recover from the moment you choose

- Pinpoint variances and recover with exceptional precision
- CDP file-level restores enable the lowest possible data loss
- Standardized application item recovery powered by Veeam Explorers™



Guest File Restore Wizard

Restore point

Select the restore point to restore guest OS files from.

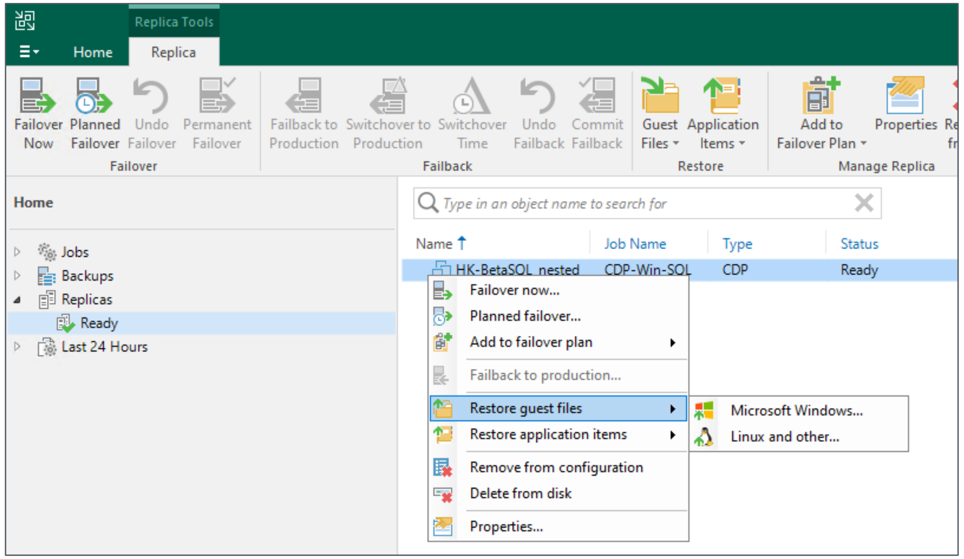
[TBD] Restore to a point in time:

11 August 2023

● I/O journal is available ● Application-consistent restore point ● Crash-consistent restore point

○ No restore points available (keep scrolling)

Restore point: Friday, August 11, 2023 8:28:30 AM



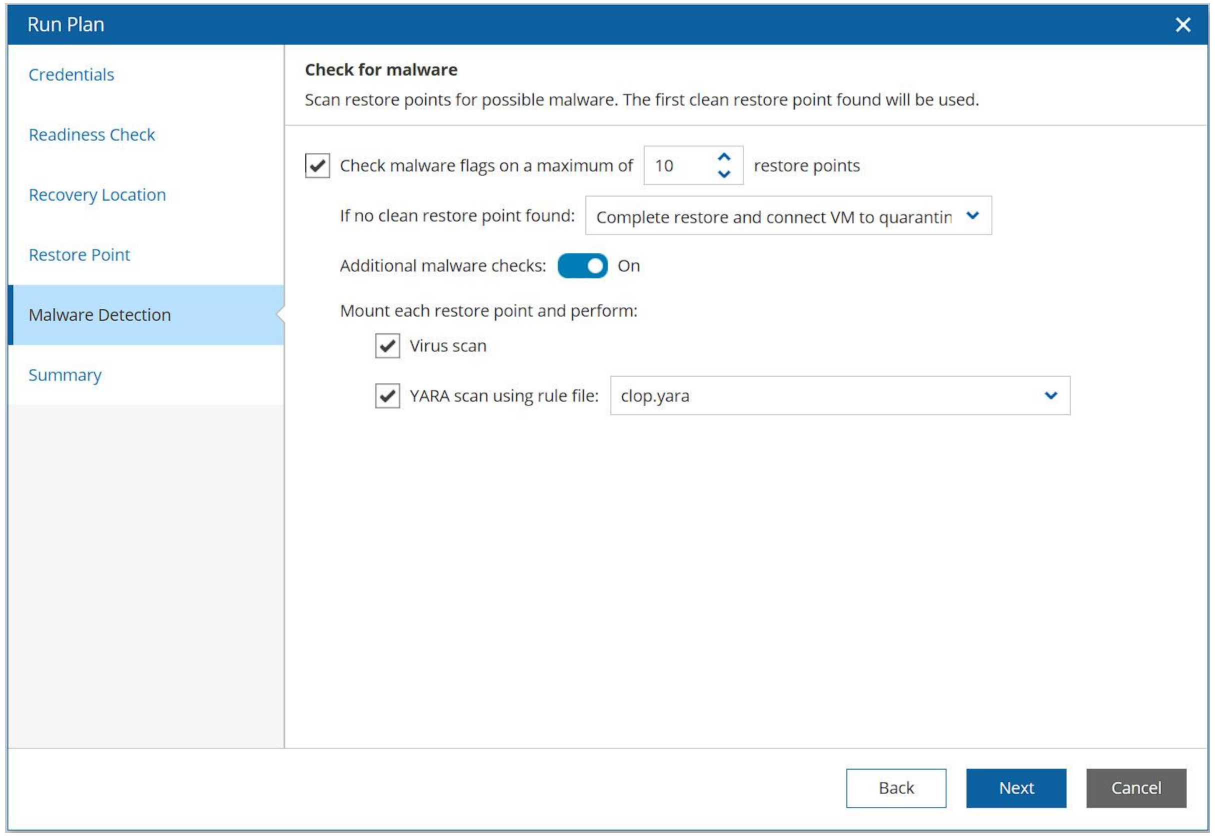
Name	Job Name	Type	Status
HK-BetaSQL_nested	CDP-Win-SQL	CDP	Ready

Recover clean the first time

Orchestrated recovery with malware-free restore points

Proven confidence when disaster strikes

- Expedite recovery by circumventing known-infected restore points
- Flexible recovery on-premises or in the cloud, with post-recovery customizations
- Automated testing proves compliance before you need it



Check for malware

Scan restore points for possible malware. The first clean restore point found will be used.

☑ Check malware flags on a maximum of 10 restore points

If no clean restore point found: Complete restore and connect VM to quarantin

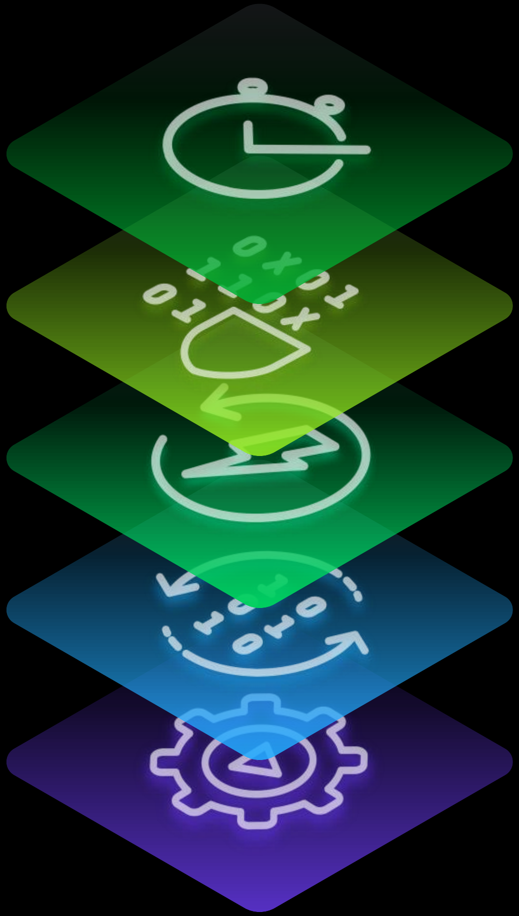
Additional malware checks: On

Mount each restore point and perform:

☑ Virus scan

☑ YARA scan using rule file: clop.yara

ReSTORE vs. ReCOVER – KnowBe4!!!



Multi-layered immutability

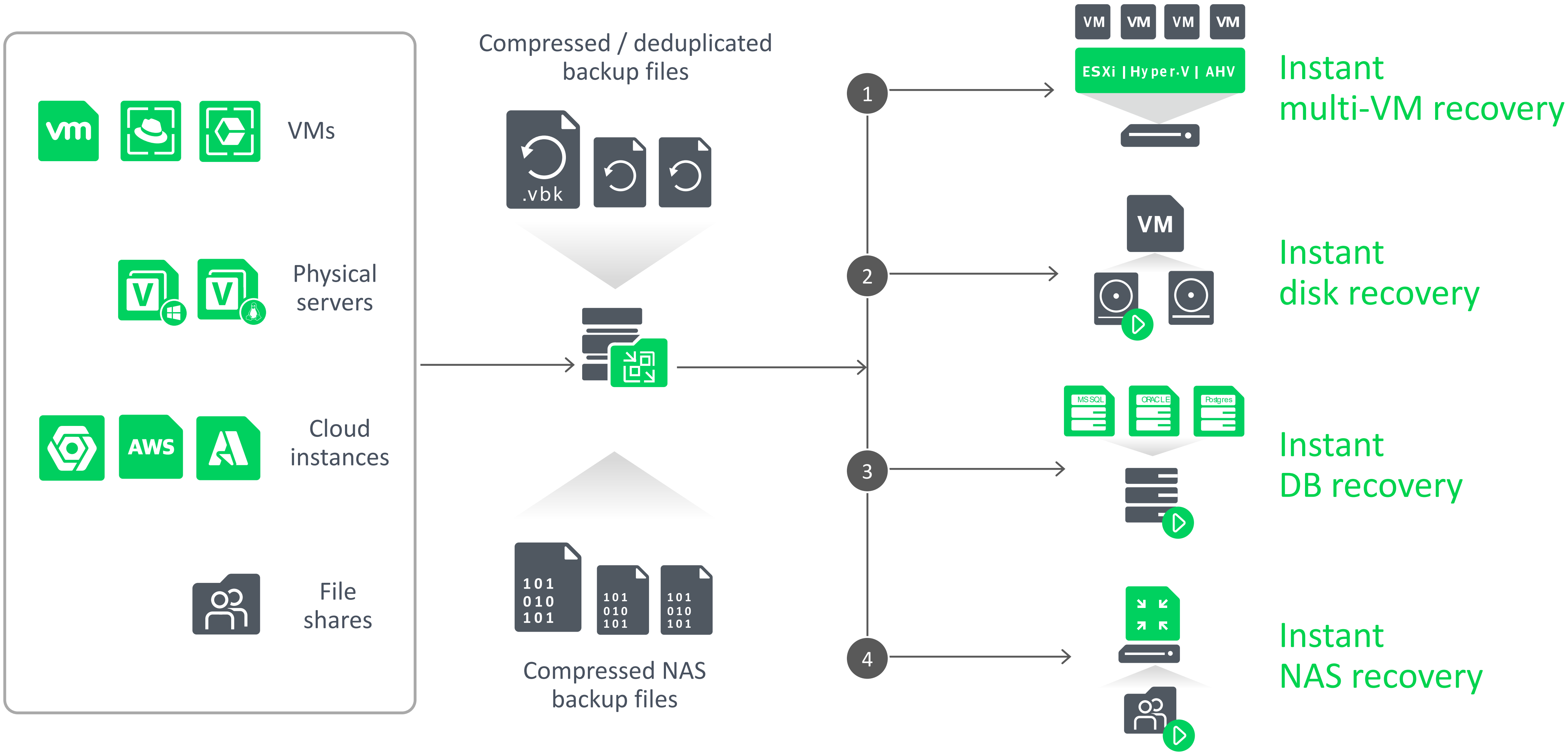
Comprehensive monitoring

Automatic recovery verification

Fastest recovery options

Complete data mobility

Instant recovery at scale



VMs

Physical servers

Cloud instances

File shares

Compressed / deduplicated backup files

Compressed NAS backup files

Instant multi-VM recovery

Instant disk recovery

Instant DB recovery

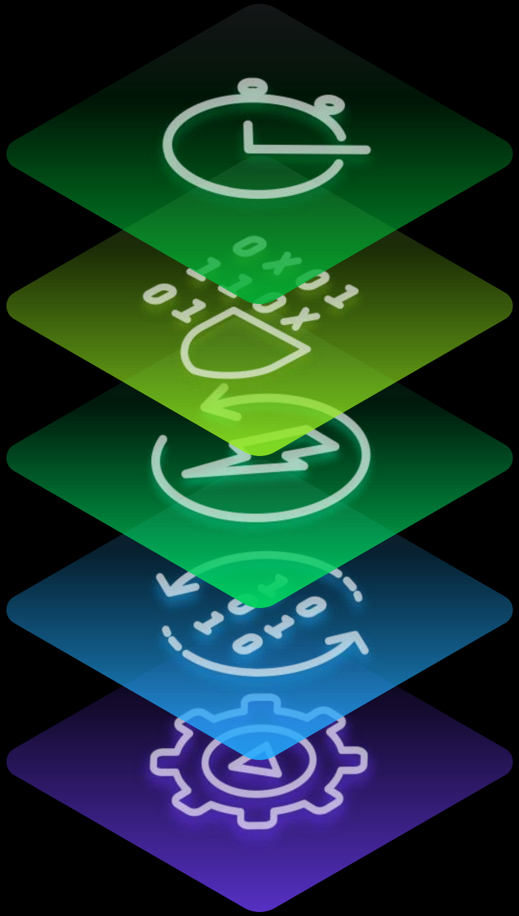
Instant NAS recovery

Veeam Explorers

Veeam Explorers Suite rozširuje funkčnosť Veeam Backup for Microsoft 365 a Veeam Backup & Replication, čo vám umožňuje obnoviť alebo exportovať údaje na úrovni aplikácie z image-based zálohovaných alebo replikových súborov.

- Veeam Explorer for Microsoft Active Directory
- Veeam Explorer for Microsoft SQL Server
- Veeam Explorer for Oracle
- Veeam Explorer for PostgreSQL
- Veeam Explorer for SAP HANA (NEW in v12.1)
- Veeam Explorer for Storage Snapshots
- Veeam Explorer for Microsoft Exchange
- Veeam Explorer for Microsoft Sharepoint
- Veeam Explorer for OneDrive for Business
- Veeam Explorer for Microsoft Teams

ReSTORE vs. ReCOVER – KnowBe4!!!



Multi-layered immutability

Comprehensive monitoring

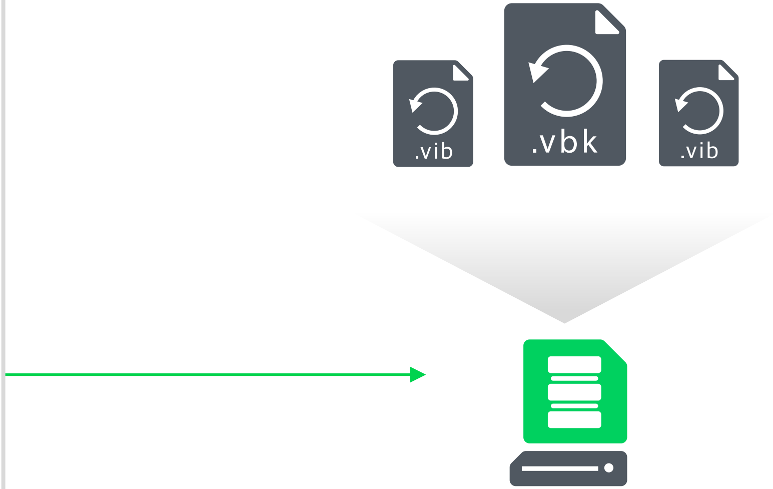
Automatic recovery verification

Fastest recovery options

Complete data mobility

Veeam Backup File Format

- Veeam Backup & Replication
- Veeam Backup & Replication Community Edition
- Veeam Agent for Microsoft Windows
- Veeam Agent for Linux
- Veeam Backup for AHV
- Veeam Backup for RHEV
- Veeam Backup for Cloud



Any on-premises VMware vSphere, Microsoft Hyper-V, Nutanix AHV VMs, physical servers and workstations…

Veeam mobility matrix

To From	vSphere	Hyper-V	Nutanix AHV	Azure VM	AWS EC2	Google Cloud VM
vSphere	✓	✓	✓	✓	✓	✓
Hyper-V	✓	✓	✓	✓	✓	✓
Nutanix AHV	✓	✓	✓	✓	✓	✓
Red Hat / Oracle KVM	✓	✓	✓	✓	✓	✓
Windows Agent	✓	✓	✓	✓	✓	✓
Linux Agent	✓	✓	✓	✓	✓	✓
Azure VM	✓	✓	✓	✓	✓	✓
AWS EC2	✓	✓	✓	✓	✓	✓
GCP VM	✓	✓	✓	✓	✓	✓
Other Clouds (agent based)	✓	✓	✓	✓	✓	✓

✓ Supported ✓ Supported via Backup Copy

Secure + compliant protection

Complete your security and compliance standing

Data Freedom

Support for hybrid- and multi-cloud infrastructures that help protect all your data with zero lock-in. Your data should be protected wherever you need it — in the cloud, on-premises, or at the edge.

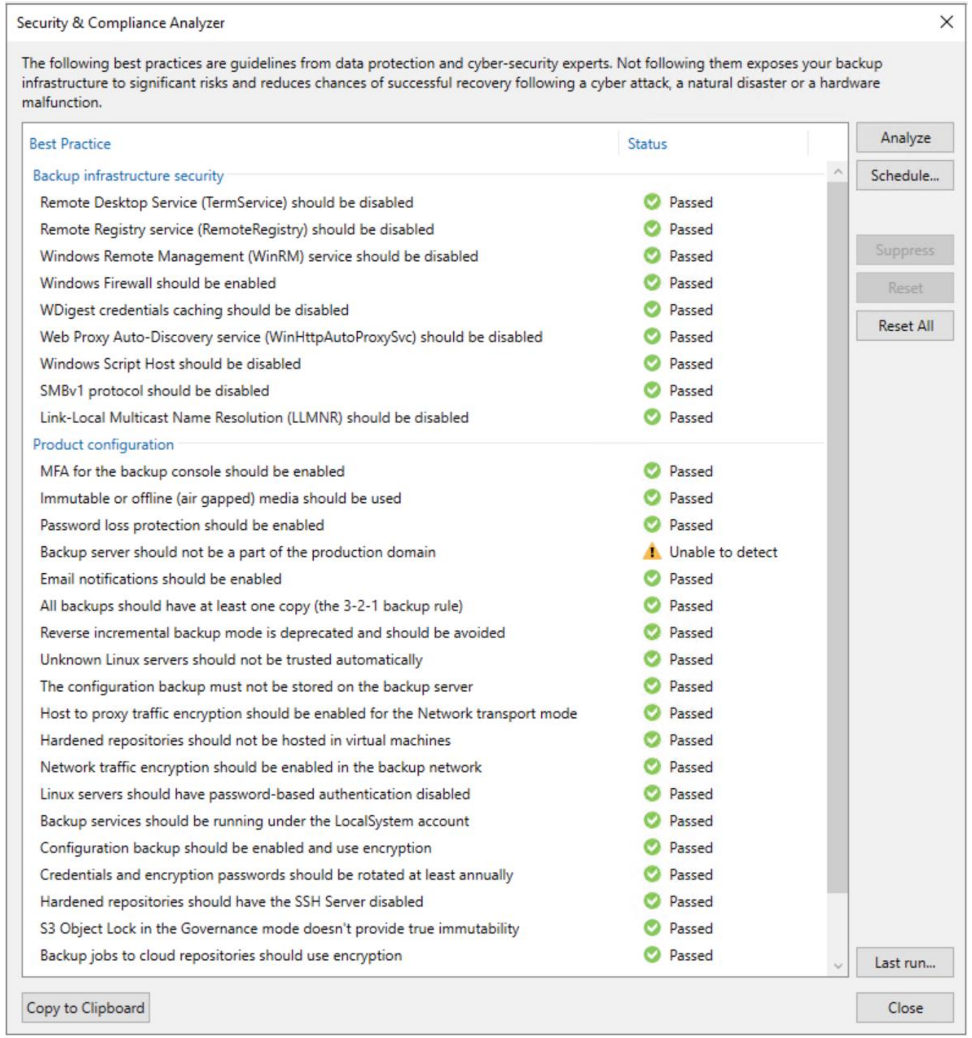
- Security and compliance analyzer
- “Four-eyes” principle protection
- Veeam Threat Center
- Veeam ONE Audit Reports

Security and compliance analyzer

Align to cybersecurity best practices

Verify security and compliance

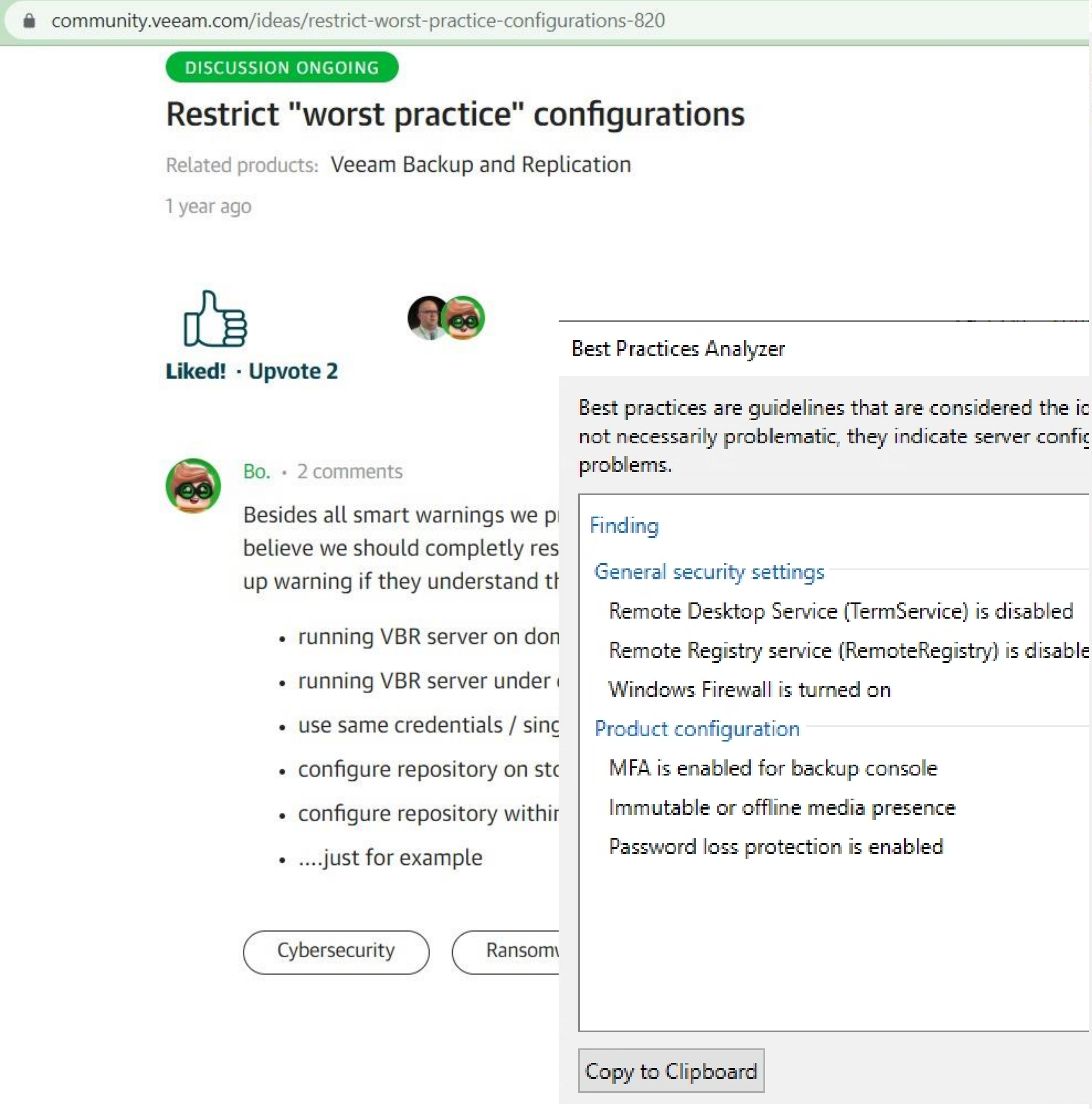
- Uncover and identify risks to your backup infrastructure
- Perform ad hoc scans or execute based on a flexible schedule
- Comprehensive and powerful best practices for backup administrators



Security & Compliance Analyzer

The following best practices are guidelines from data protection and cyber-security experts. Not following them exposes your backup infrastructure to significant risks and reduces chances of successful recovery following a cyber attack, a natural disaster or a hardware malfunction.

Best Practice	Status
Backup infrastructure security	
Remote Desktop Service (TermService) should be disabled	✓ Passed
Remote Registry service (RemoteRegistry) should be disabled	✓ Passed
Windows Remote Management (WinRM) service should be disabled	✓ Passed
Windows Firewall should be enabled	✓ Passed
WDigest credentials caching should be disabled	✓ Passed
Web Proxy Auto-Discovery service (WinHttpAutoProxySvc) should be disabled	✓ Passed
Windows Script Host should be disabled	✓ Passed
SMBv1 protocol should be disabled	✓ Passed
Link-Local Multicast Name Resolution (LLMNR) should be disabled	✓ Passed
Product configuration	
MFA for the backup console should be enabled	✓ Passed
Immutable or offline (air gapped) media should be used	✓ Passed
Password loss protection should be enabled	✓ Passed
Backup server should not be a part of the production domain	⚠ Unable to detect
Email notifications should be enabled	✓ Passed
All backups should have at least one copy (the 3-2-1 backup rule)	✓ Passed
Reverse incremental backup mode is deprecated and should be avoided	✓ Passed
Unknown Linux servers should not be trusted automatically	✓ Passed
The configuration backup must not be stored on the backup server	✓ Passed
Host to proxy traffic encryption should be enabled for the Network transport mode	✓ Passed
Hardened repositories should not be hosted in virtual machines	✓ Passed
Network traffic encryption should be enabled in the backup network	✓ Passed
Linux servers should have password-based authentication disabled	✓ Passed
Backup services should be running under the LocalSystem account	✓ Passed
Configuration backup should be enabled and use encryption	✓ Passed
Credentials and encryption passwords should be rotated at least annually	✓ Passed
Hardened repositories should have the SSH Server disabled	✓ Passed
S3 Object Lock in the Governance mode doesn't provide true immutability	✓ Passed
Backup jobs to cloud repositories should use encryption	✓ Passed



community.veeam.com/ideas/restrict-worst-practice-configurations-820

DISCUSSION ONGOING

Restrict "worst practice" configurations

Related products: Veeam Backup and Replication

1 year ago

Bo. • 2 comments

Besides all smart warnings we p
believe we should complety res
up warning if they understand t

- running VBR server on don
- running VBR server under
- use same credentials / sing
- configure repository on sto
- configure repository withi
- ....just for example

Best Practices Analyzer

Best practices are guidelines that are considered the ic
not necessarily problematic, they indicate server config
problems.

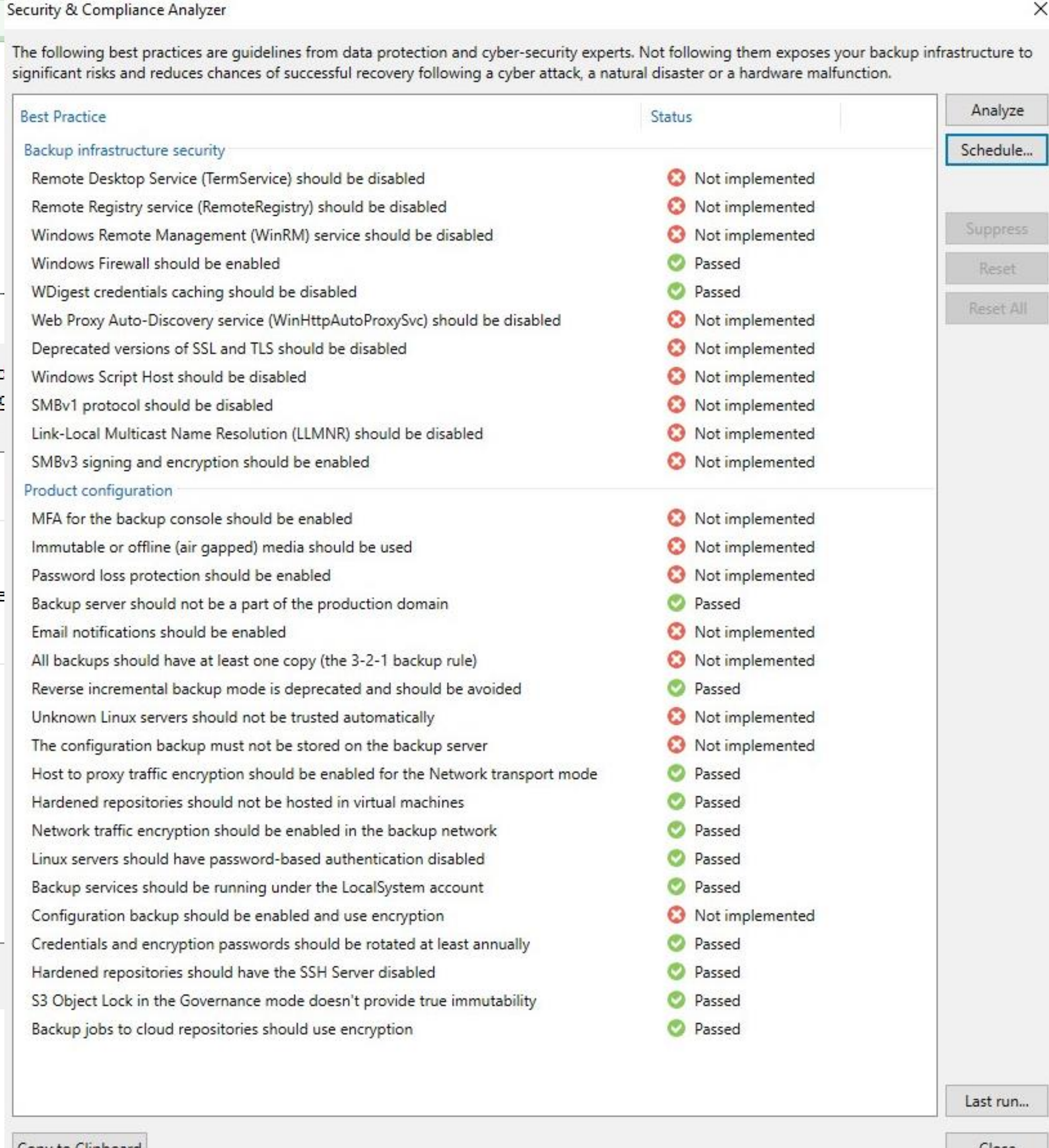
Finding

General security settings

- Remote Desktop Service (TermService) is disabled
- Remote Registry service (RemoteRegistry) is disable
- Windows Firewall is turned on

Product configuration

- MFA is enabled for backup console
- Immutable or offline media presence
- Password loss protection is enabled



Security & Compliance Analyzer

The following best practices are guidelines from data protection and cyber-security experts. Not following them exposes your backup infrastructure to significant risks and reduces chances of successful recovery following a cyber attack, a natural disaster or a hardware malfunction.

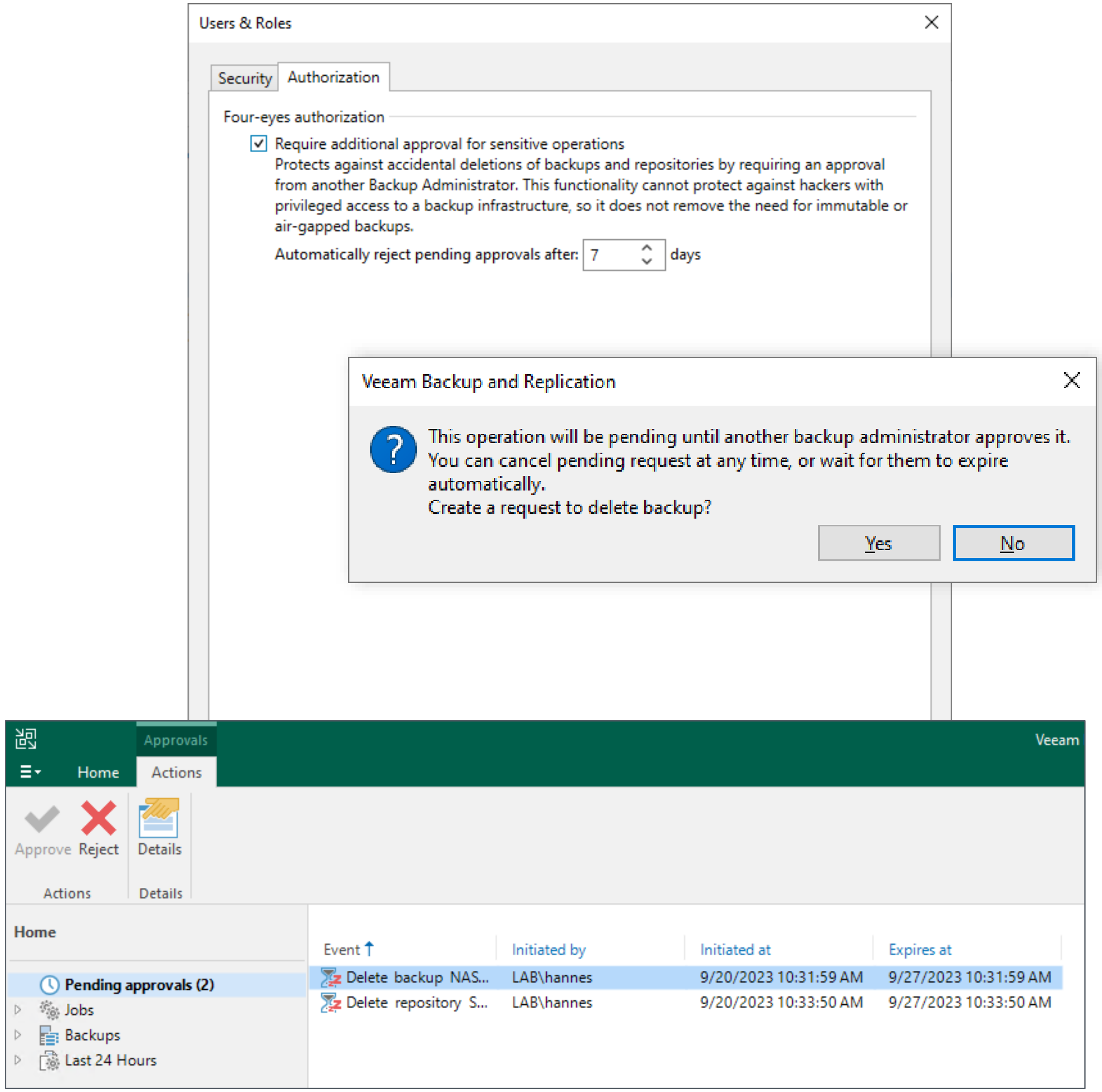
Best Practice	Status
Backup infrastructure security	
Remote Desktop Service (TermService) should be disabled	✗ Not implemented
Remote Registry service (RemoteRegistry) should be disabled	✗ Not implemented
Windows Remote Management (WinRM) service should be disabled	✗ Not implemented
Windows Firewall should be enabled	✓ Passed
WDigest credentials caching should be disabled	✓ Passed
Web Proxy Auto-Discovery service (WinHttpAutoProxySvc) should be disabled	✗ Not implemented
Deprecated versions of SSL and TLS should be disabled	✗ Not implemented
Windows Script Host should be disabled	✗ Not implemented
SMBv1 protocol should be disabled	✗ Not implemented
Link-Local Multicast Name Resolution (LLMNR) should be disabled	✗ Not implemented
SMBv3 signing and encryption should be enabled	✗ Not implemented
Product configuration	
MFA for the backup console should be enabled	✗ Not implemented
Immutable or offline (air gapped) media should be used	✗ Not implemented
Password loss protection should be enabled	✗ Not implemented
Backup server should not be a part of the production domain	✓ Passed
Email notifications should be enabled	✗ Not implemented
All backups should have at least one copy (the 3-2-1 backup rule)	✗ Not implemented
Reverse incremental backup mode is deprecated and should be avoided	✓ Passed
Unknown Linux servers should not be trusted automatically	✗ Not implemented
The configuration backup must not be stored on the backup server	✗ Not implemented
Host to proxy traffic encryption should be enabled for the Network transport mode	✓ Passed
Hardened repositories should not be hosted in virtual machines	✓ Passed
Network traffic encryption should be enabled in the backup network	✓ Passed
Linux servers should have password-based authentication disabled	✓ Passed
Backup services should be running under the LocalSystem account	✓ Passed
Configuration backup should be enabled and use encryption	✗ Not implemented
Credentials and encryption passwords should be rotated at least annually	✓ Passed
Hardened repositories should have the SSH Server disabled	✓ Passed
S3 Object Lock in the Governance mode doesn't provide true immutability	✓ Passed
Backup jobs to cloud repositories should use encryption	✓ Passed

“Four-eyes” principle protection

Prevent accidental or malicious deletion

Remove single points of destruction

- Requires approval by a second backup administrator
- Restrict backup and repository deletions and access setting modifications
- Logged in Veeam history, Windows event log, and email



Users & Roles

Four-eyes authorization

☑ Require additional approval for sensitive operations

Protects against accidental deletions of backups and repositories by requiring an approval from another Backup Administrator. This functionality cannot protect against hackers with privileged access to a backup infrastructure, so it does not remove the need for immutable or air-gapped backups.

Automatically reject pending approvals after: 7 days

Veeam Backup and Replication

This operation will be pending until another backup administrator approves it. You can cancel pending request at any time, or wait for them to expire automatically.
Create a request to delete backup?

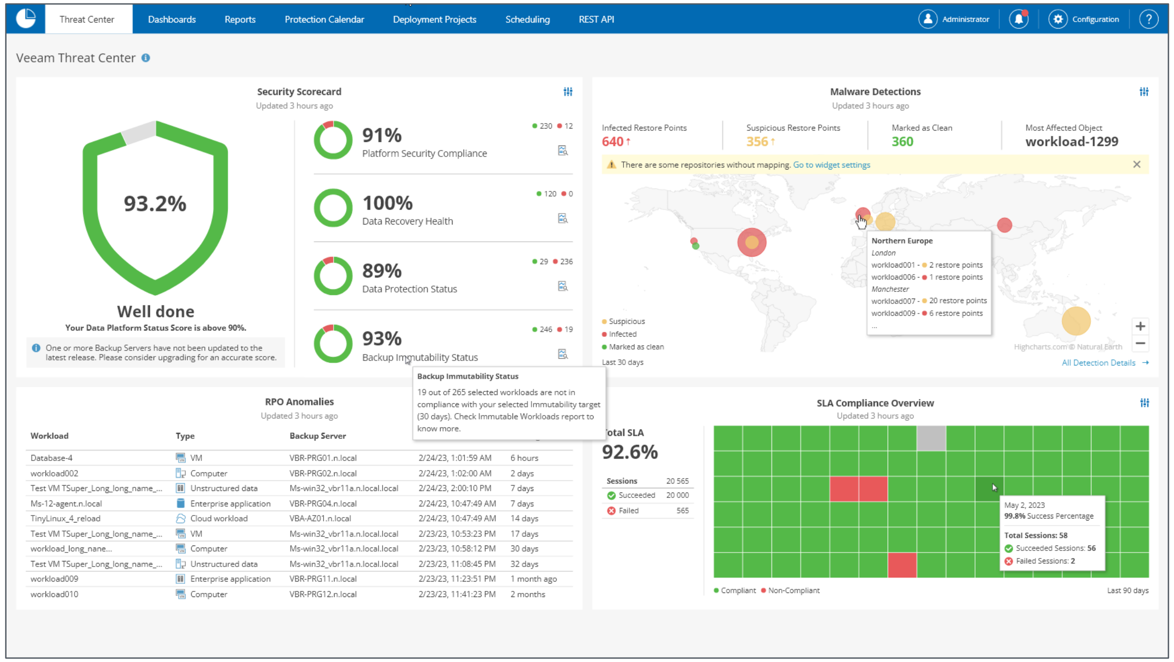
Event	Initiated by	Initiated at	Expires at
Delete backup NAS...	LAB\hannes	9/20/2023 10:31:59 AM	9/27/2023 10:31:59 AM
Delete repository S...	LAB\hannes	9/20/2023 10:33:50 AM	9/27/2023 10:33:50 AM

Veeam Threat Center

Put the spotlight on malware

Comprehensive data protection visibility

- Complete platform security score
- Global Malware Detection Map
- Measure compliance and identify recovery point objective (RPO) anomalies



Veeam Threat Center

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 ● 12

100% Data Recovery Health ● 120 ● 0

89% Data Protection Status ● 29 ● 236

93% Backup Immutability Status ● 246 ● 19

Backup Immutability Status
19 out of 265 selected workloads are not in compliance with your selected Immutability target (30 days). Check Immutable Workloads report to know more.

Malware Detections
Updated 3 hours ago

Infected Restore Points	Suspicious Restore Points	Marked as Clean	Most Affected Object
640 ↑	356 ↑	360	workload-1299

There are some repositories without mapping. Go to widget settings

Northern Europe
London
workload001 - ● 2 restore points
workload006 - ● 1 restore points
Manchester
workload007 - ● 20 restore points
workload009 - ● 6 restore points
...

● Suspicious
● Infected
● Marked as clean

Last 30 days

Highcharts.com © Natural Earth

All Detection Details →

RPO Anomalies
Updated 3 hours ago

Workload	Type	Backup Server		
Database-4	VM	VBR-PRG01.n.local	2/24/23, 1:01:59 AM	6 hours
workload002	Computer	VBR-PRG02.n.local	2/24/23, 1:02:00 AM	2 days
Test VM TSuper_Long_long_name_...	Unstructured data	Ms-win32_vbr11a.n.local.local	2/24/23, 2:00:10 PM	7 days
Ms-12-agent.n.local	Enterprise application	VBR-PRG04.n.local	2/24/23, 10:47:49 AM	7 days
TinyLinux_4_reload	Cloud workload	VBA-AZ01.n.local	2/24/23, 10:47:49 AM	14 days
Test VM TSuper_Long_long_name_...	VM	Ms-win32_vbr11a.n.local.local	2/23/23, 10:53:23 PM	17 days
workload_long_nane...	Computer	Ms-win32_vbr11a.n.local.local	2/23/23, 10:58:12 PM	30 days
Test VM TSuper_Long_long_name_...	Unstructured data	Ms-win32_vbr11a.n.local.local	2/23/23, 11:08:45 PM	32 days
workload009	Enterprise application	VBR-PRG11.n.local	2/23/23, 11:23:51 PM	1 month ago
workload010	Computer	VBR-PRG12.n.local	2/23/23, 11:41:23 PM	2 months

SLA Compliance Overview
Updated 3 hours ago

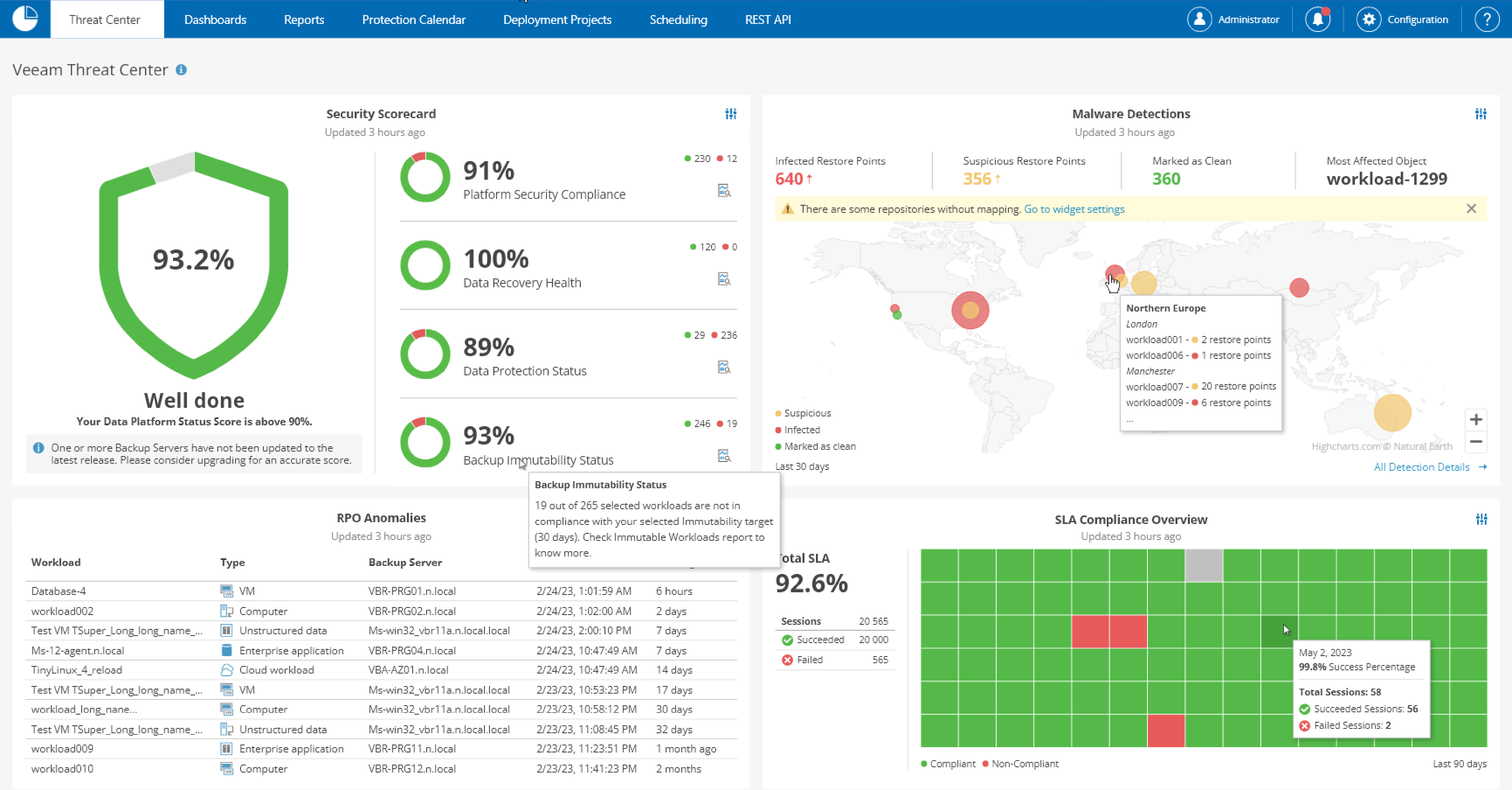
otal SLA
92.6%

Sessions	20 565
✓ Succeeded	20 000
☒ Failed	565

May 2, 2023
99.8% Success Percentage
Total Sessions: 58
✓ Succeeded Sessions: **56**
☒ Failed Sessions: **2**

● Compliant ● Non-Compliant

Last 90 days



Veeam Threat Center

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	12
100%	Data Recovery Health	120	0
89%	Data Protection Status	29	236
93%	Backup Immutability Status	246	19

Backup Immutability Status

19 out of 265 selected workloads are not in compliance with your selected Immutability target (30 days). Check Immutable Workloads report to know more.

Malware Detections

Updated 3 hours ago

Infected Restore Points	Suspicious Restore Points	Marked as Clean	Most Affected Object
640 ↑	356 ↑	360	workload-1299

⚠ There are some repositories without mapping. Go to widget settings

Northern Europe

London

workload001 - ● 2 restore points

workload006 - ● 1 restore points

Manchester

workload007 - ● 20 restore points

workload009 - ● 6 restore points

...

Last 30 days

All Detection Details →

RPO Anomalies

Updated 3 hours ago

Workload	Type	Backup Server		
Database-4	VM	VBR-PRG01.n.local	2/24/23, 1:01:59 AM	6 hours
workload002	Computer	VBR-PRG02.n.local	2/24/23, 1:02:00 AM	2 days
Test VM TSuper_Long_long_name_...	Unstructured data	Ms-win32_vbr11a.n.local.local	2/24/23, 2:00:10 PM	7 days
Ms-12-agent.n.local	Enterprise application	VBR-PRG04.n.local	2/24/23, 10:47:49 AM	7 days
TinyLinux_4_reload	Cloud workload	VBA-AZ01.n.local	2/24/23, 10:47:49 AM	14 days
Test VM TSuper_Long_long_name_...	VM	Ms-win32_vbr11a.n.local.local	2/23/23, 10:53:23 PM	17 days
workload_long_nane...	Computer	Ms-win32_vbr11a.n.local.local	2/23/23, 10:58:12 PM	30 days
Test VM TSuper_Long_long_name_...	Unstructured data	Ms-win32_vbr11a.n.local.local	2/23/23, 11:08:45 PM	32 days
workload009	Enterprise application	VBR-PRG11.n.local	2/23/23, 11:23:51 PM	1 month ago
workload010	Computer	VBR-PRG12.n.local	2/23/23, 11:41:23 PM	2 months

SLA Compliance Overview

Updated 3 hours ago

Total SLA

92.6%

Sessions	20 565
✓ Succeeded	20 000
✗ Failed	565

May 2, 2023

99.8% Success Percentage

Total Sessions: 58

✓ Succeeded Sessions: **56**

✗ Failed Sessions: **2**

veeam

Follow us!

Join the community hub: