Modern Data Protection for Healthcare Secure, Recover, and Defend Against Ransomware

Sanya Boonruen
Senior Technology Consultant
sanya.boonruen@veeam.com

The World...

- Cybersecurity threats (Ransomware, Phishing)
- Compliance requirements
- Data growth in EHR and PACS systems
- Downtime and disaster recovery concerns

Ransomware Protection for Critical Healthcare Infrastructure

Ransomware Threats in **Healthcare**

Targeted Healthcare Sector

Healthcare organizations are prime targets for ransomware attacks due to sensitive patient data and critical services they provide.

Importance of Understanding Threats

Recognizing the specific ransomware threats to healthcare is essential for developing effective security measures and defenses.

Building Effective Defenses

Strengthening defenses against ransomware involves a multi-faceted approach, including staff training and advanced security protocols.

Electronic Health Records (EHR) Protection and Compliance

Challenges in EHR Protection

Cybersecurity Threats

Healthcare organizations are increasingly targeted by sophisticated cyberattacks aimed at compromising electronic health records (EHRs).

Human Errors

Human errors remain a significant challenge in EHR protection, often leading to accidental data leaks or breaches.

Regulatory Compliance

Compliance with complex and continuously evolving regulations adds to the challenges that healthcare organizations face in protecting EHRs.

Hybrid Cloud Data Protection for Medical Imaging (PACS)

Challenges in **Protecting Medical Imaging Data**

Large File Sizes

Medical imaging data files are often very large, creating storage and management challenges that require robust solutions.

Rapid Data Growth

The volume of medical imaging data is growing rapidly, necessitating scalable data protection strategies to keep up with demand.

Need for High Availability

Healthcare providers require high availability of medical imaging data for timely diagnoses and treatments, which adds complexity to data protection.

Veeam Data Platform

Veeam Product Portfolio

Veeam Data Platform

Veeam Backup & Replication

Veeam ONE

Veeam Recovery Orchestrator

Cloud

Veeam Backup *For AWS*

Veeam Backup *For Microsoft Azure*

Veeam Backup *For Google Cloud*

SaaS

Veeam Backup *for Microsoft 365*

Veeam Backup *for Salesforce*

Kubernetes

Veeam Kasten

Veeam Data Cloud (BaaS)

VDC Microsoft 365

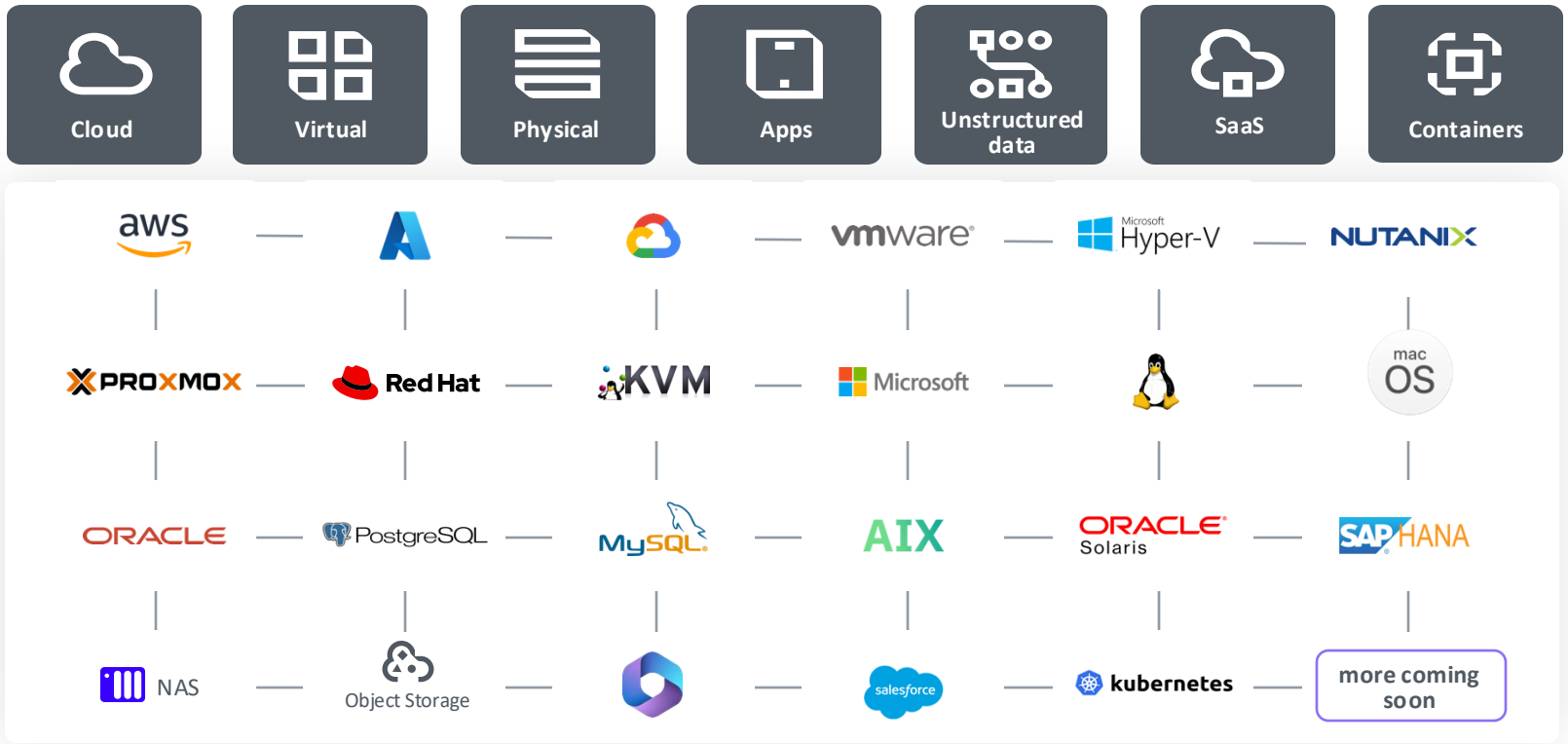
VDC Microsoft Azure

VDC Veeam Vault

VDC Microsoft Entra ID

VDC Salesforce

Extensive workload coverage unmatched in the industry



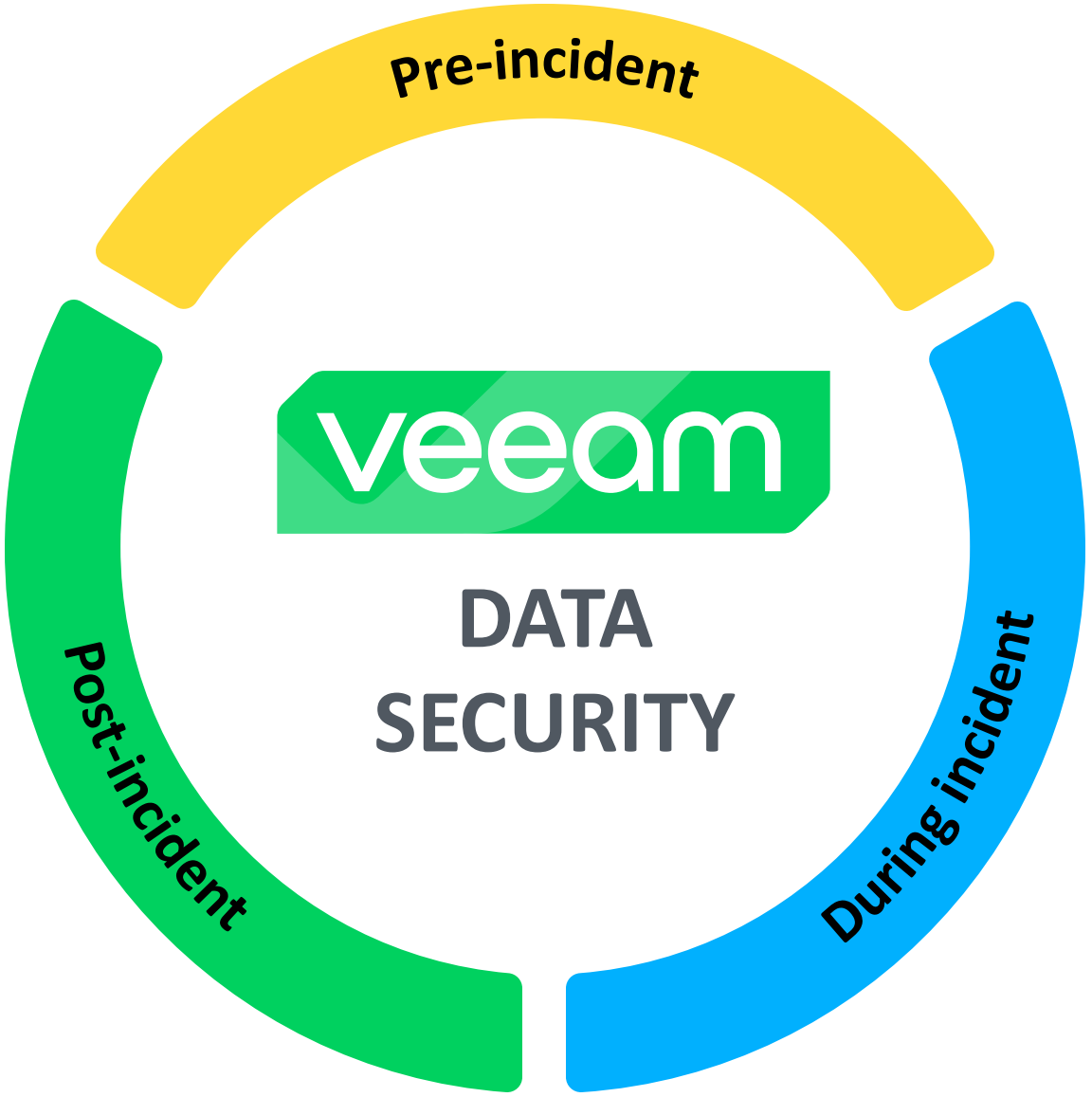
Newly Introduced:

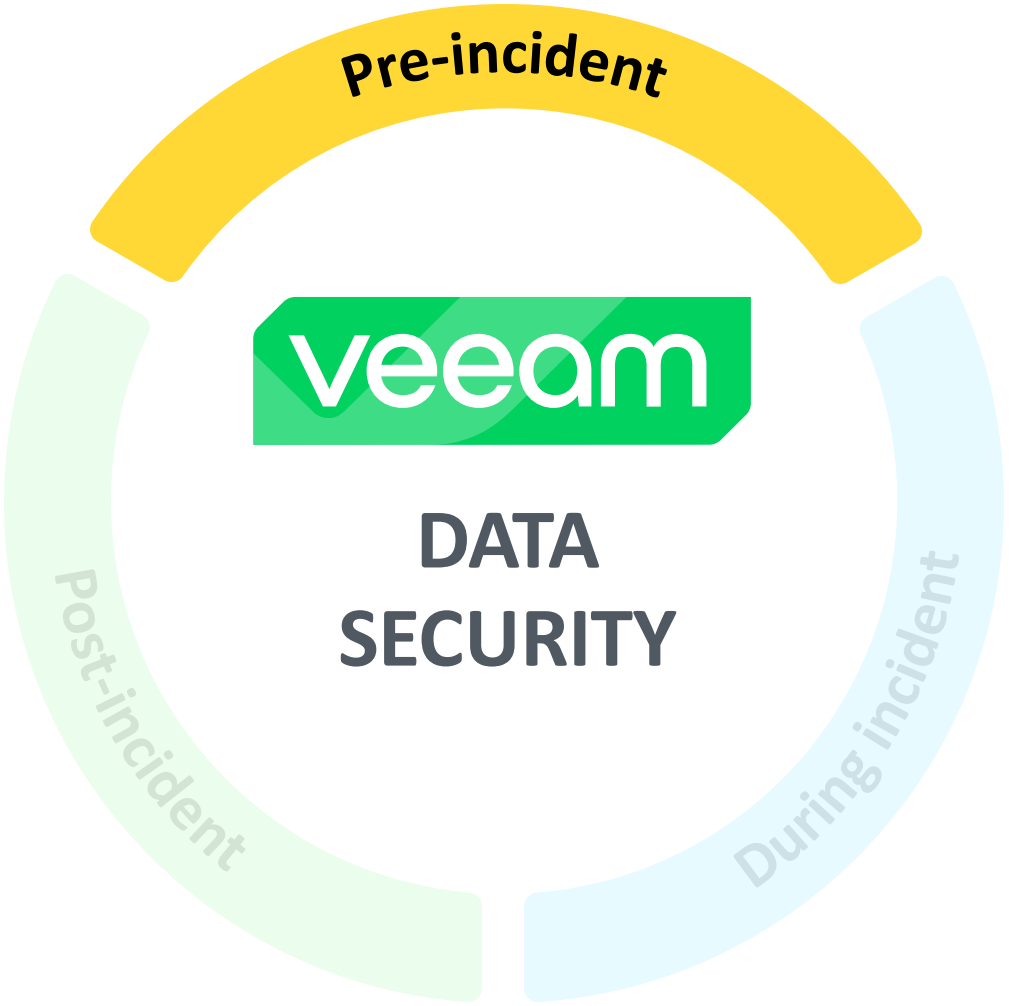
- Microsoft Entra ID
- Proxmox VE
- MongoDB

Cloud

- Amazon FSx
- Amazon RedShift
- Azure Cosmos DB
- Azure Data Lake Storage Gen2

Veeam is purpose-built for powering data resilience





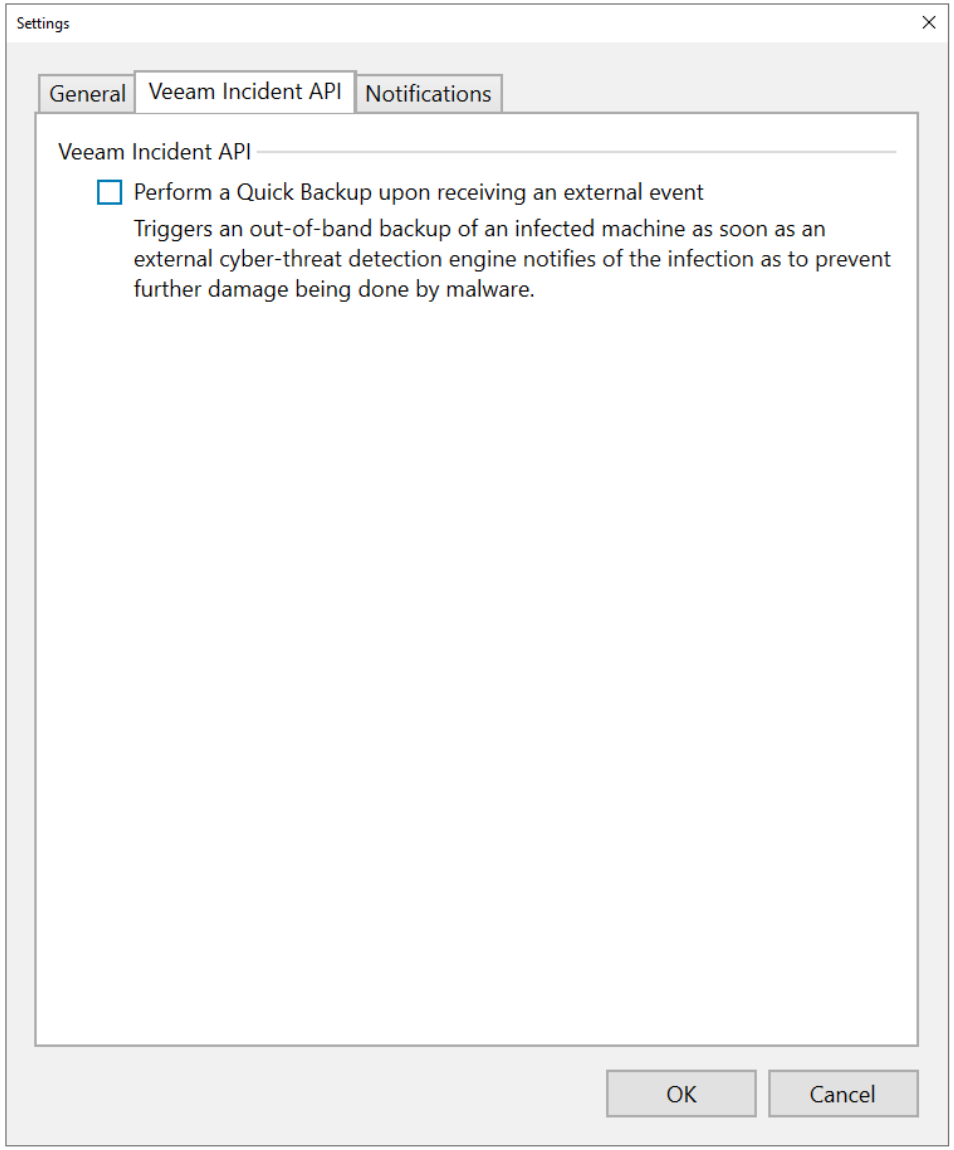
- Veeam Incident API
- Data Observability & Analytics
- Security & Compliance Analyzer
- Recon Scanner from Coveware by Veeam

Veeam Incident API

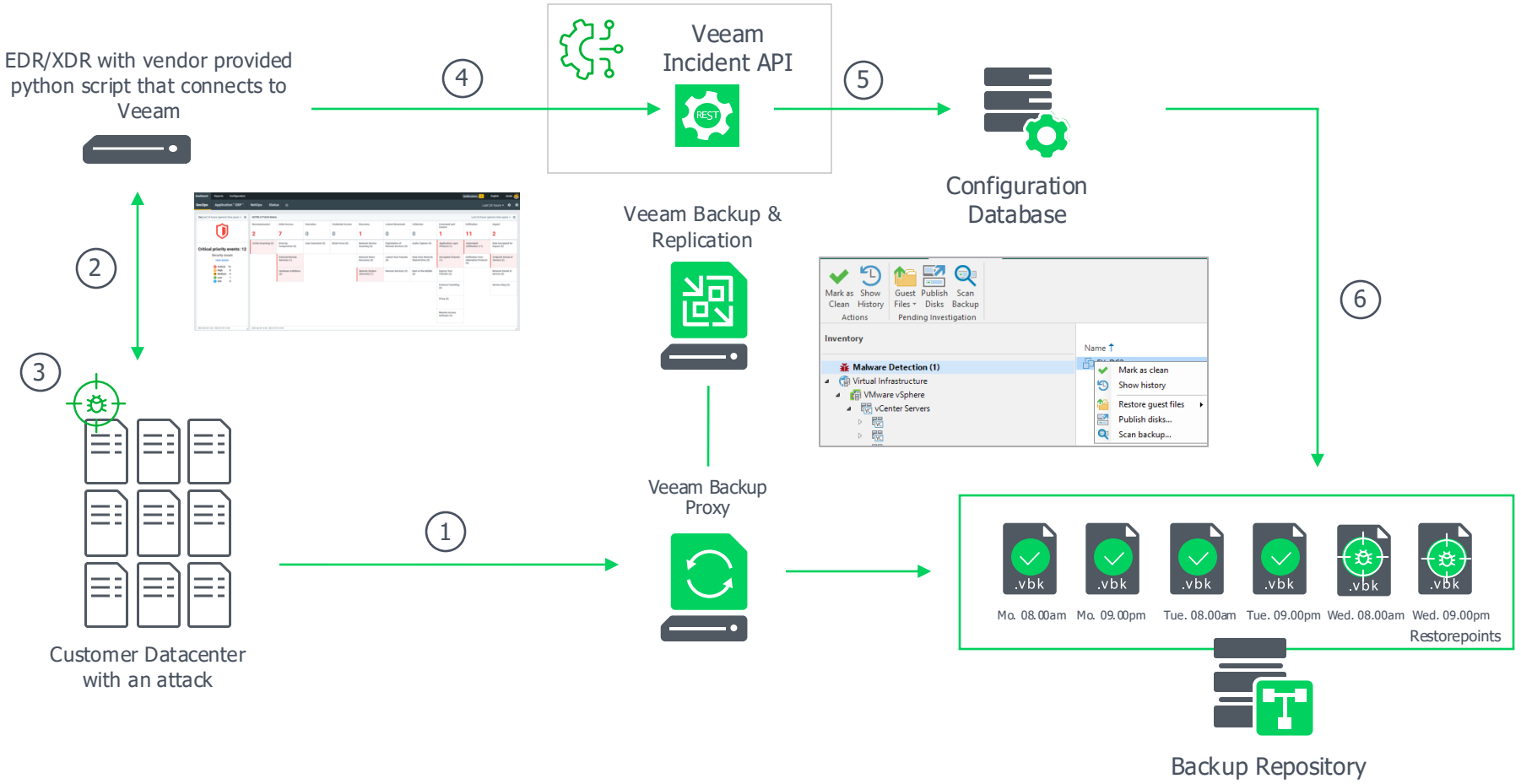
Get a second opinion

Receive real-time infection reports from third party tools

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



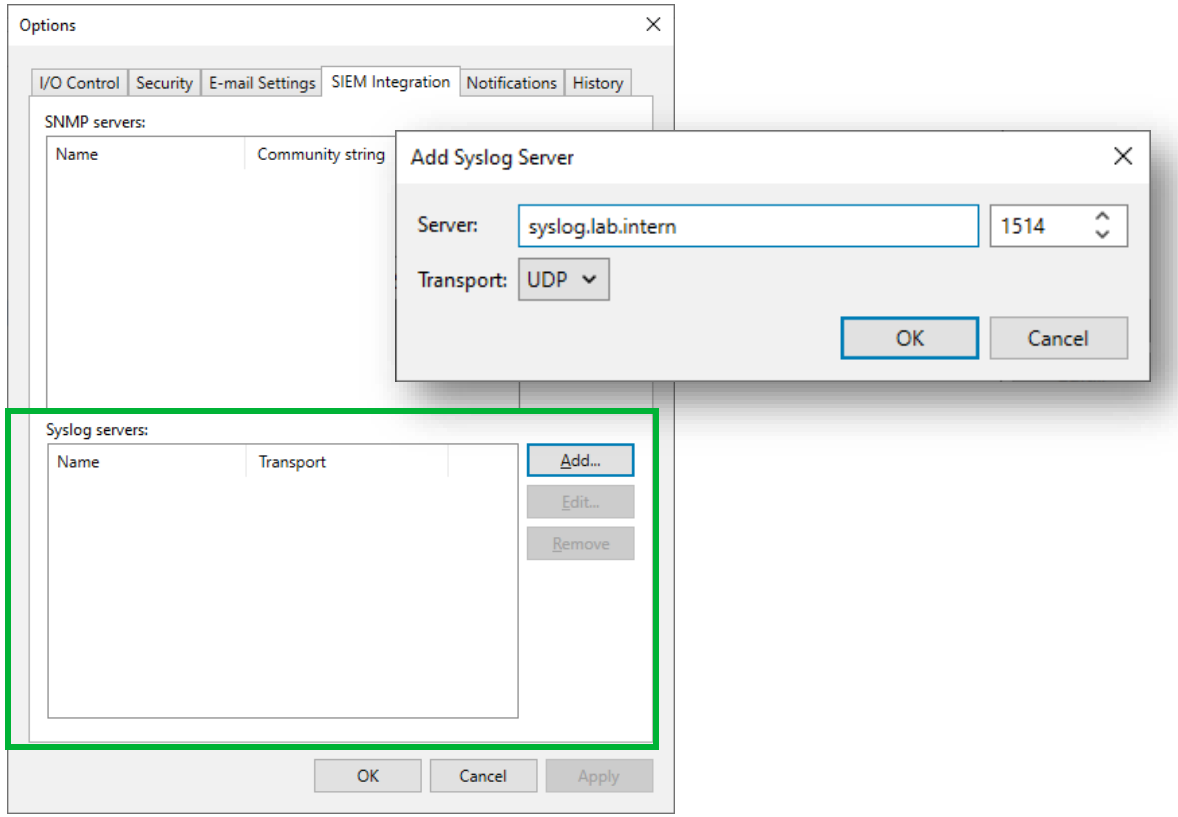
Veeam Incident API with EDR/XDR



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

Better Integration With SIEM Systems

Configuration



Example output

2023-08-10 07:42:56.264

Session BJ-nano (Full) has been completed.

85809820-3751-11ee-8192-00505699beb4

Timestamp
2023-08-10 07:42:56.264

Received by
syslog udp 1514 on dc657e32 / HK-greylog.lab.intern

Stored in index
graylog_0

Routed into streams
- Default Stream

application_name
Veeam_Backup

enterpriseId
31023

facility
user-level

facility_num
1

level
6

message
Session BJ-nano (Full) has been completed.

source
HK-1839-VBR

Easily Check Configuration Best Practices

Built-in Security & Compliance Analyzer

Over 30 security checks:

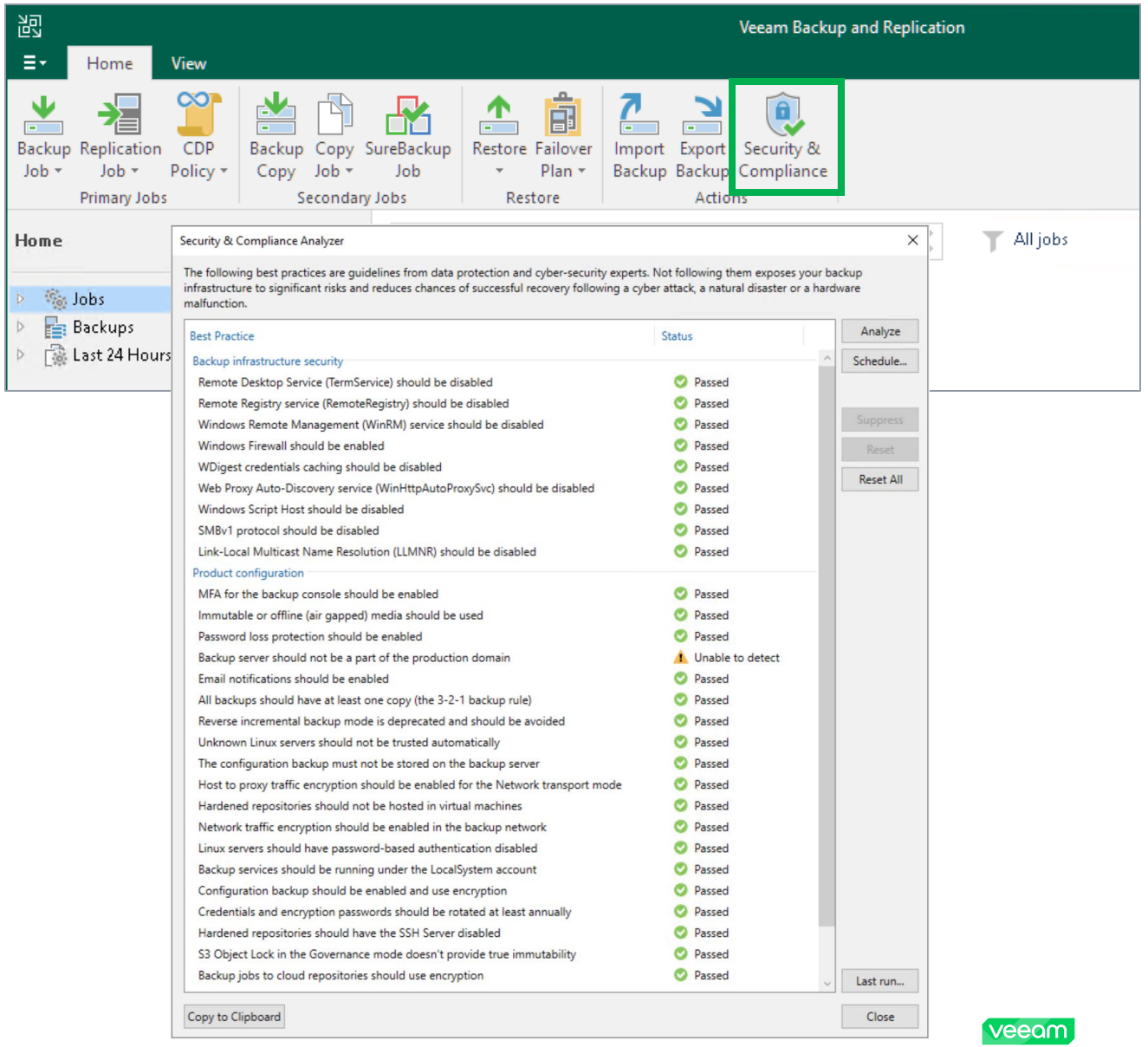
a) Veeam Backup server hardening

b) Environment configuration verification

c) Built-in scheduler and email notifications

d) Veeam Monitoring & Analytics alerts

Your data becomes safer as you successfully clear more security checks



Veeam ONE

Proactive notifications and visibility for critical workloads

New alarms:

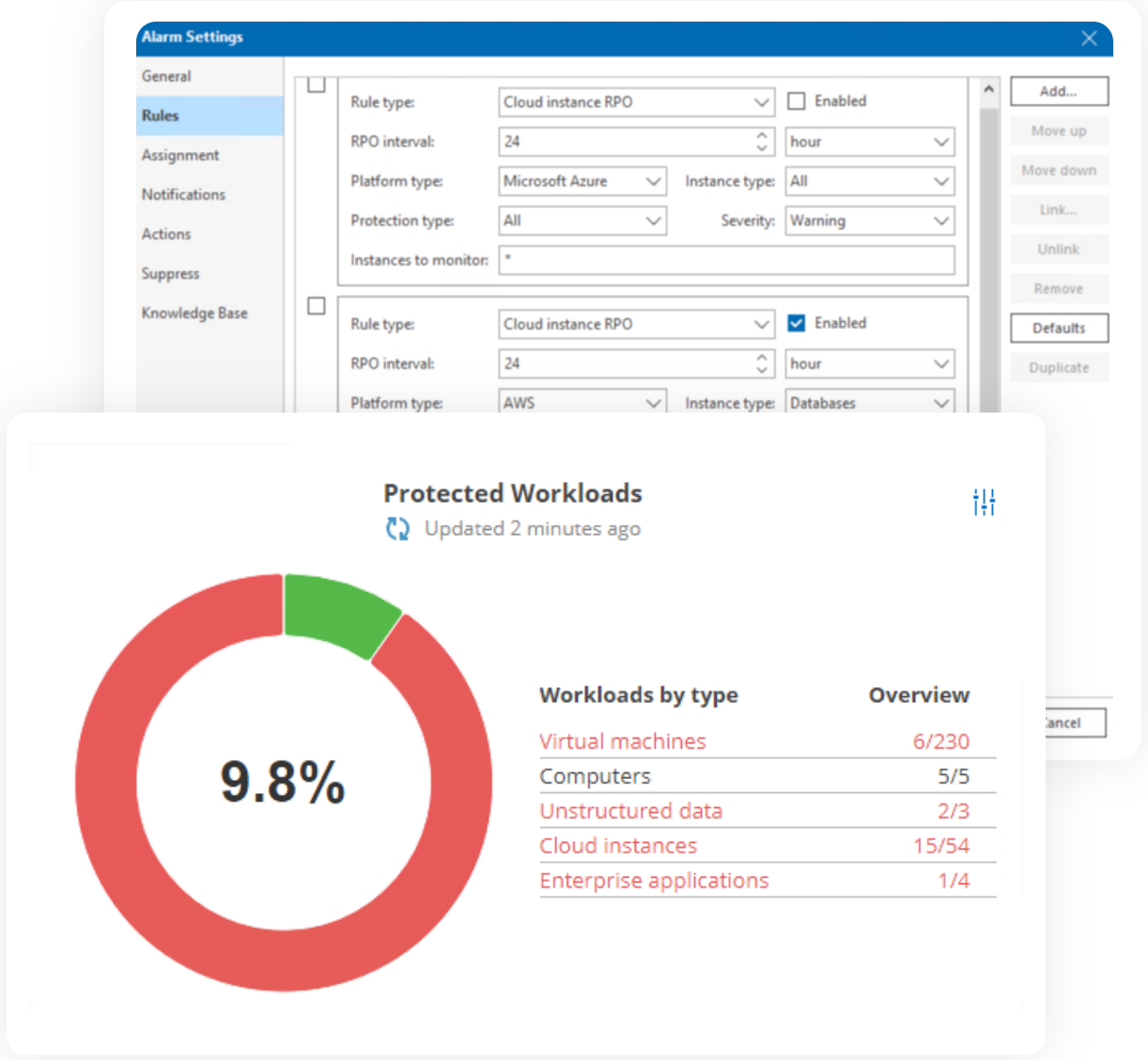
- VM with no backup (*AHV, KVM, and Proxmox)*
- Cloud Instance RPO

New widget:

- Protected workloads

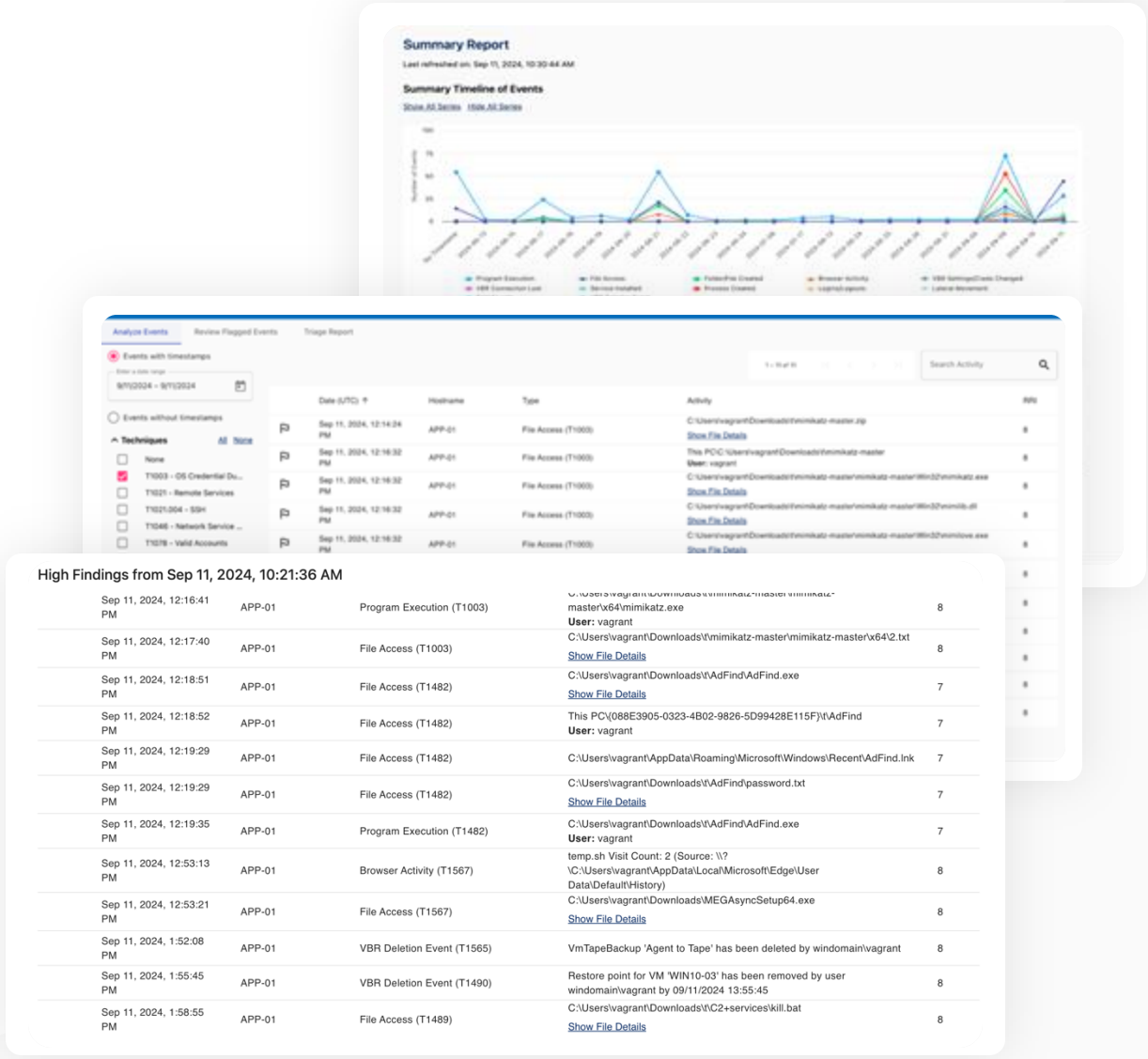
Other enhancements:

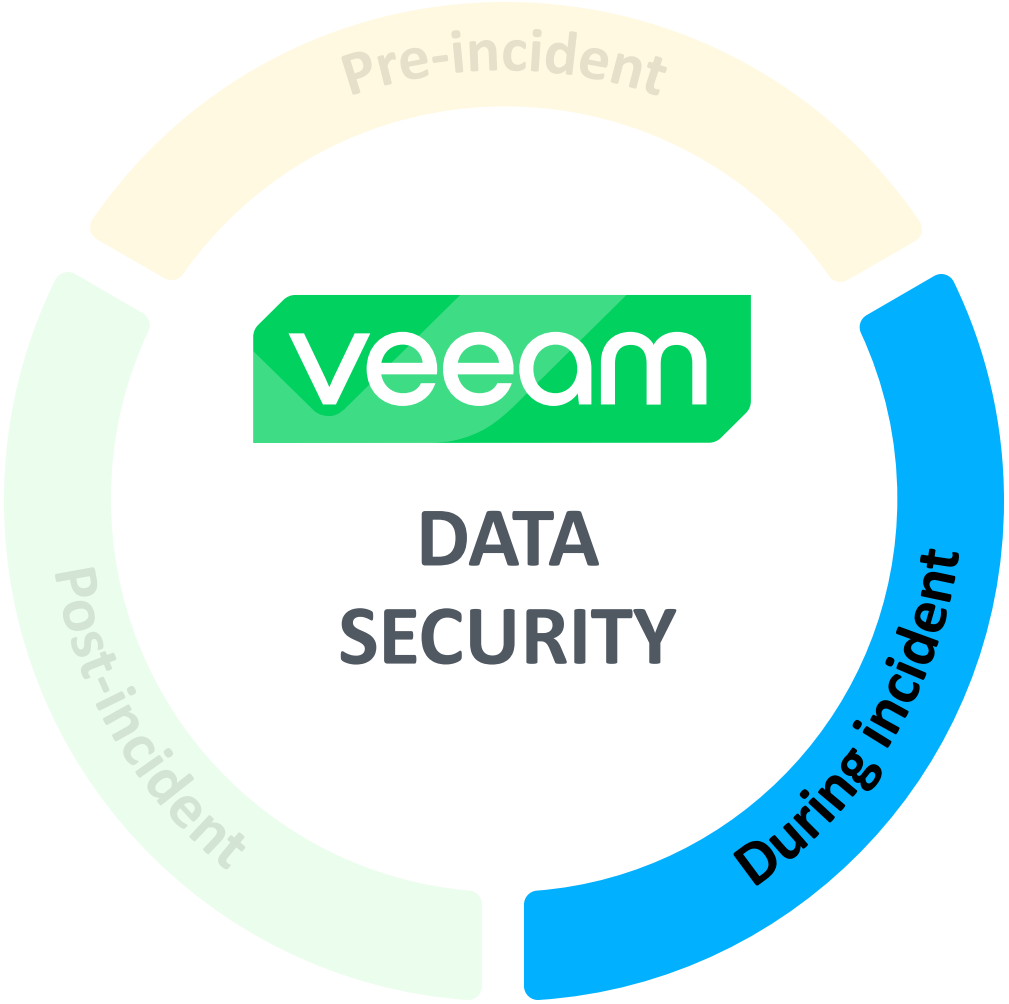
- Support for 11:11 Cloud Object Storage
- Customizable ServiceNow severity settings



Proactive Threat Assessment with **Recon Scanner**

- Exclusive proactive threat assessment technology for Veeam Backup & Replication servers
- Easy deployment and scans with minimal overhead at runtime
- Secure uploads with fast collection of logs, events, and potential adversary content
- Automatic mapping of data to MITRE ATT&CK and Coveware ransomware indicators
- Timeline of activity and remediation report available for security review





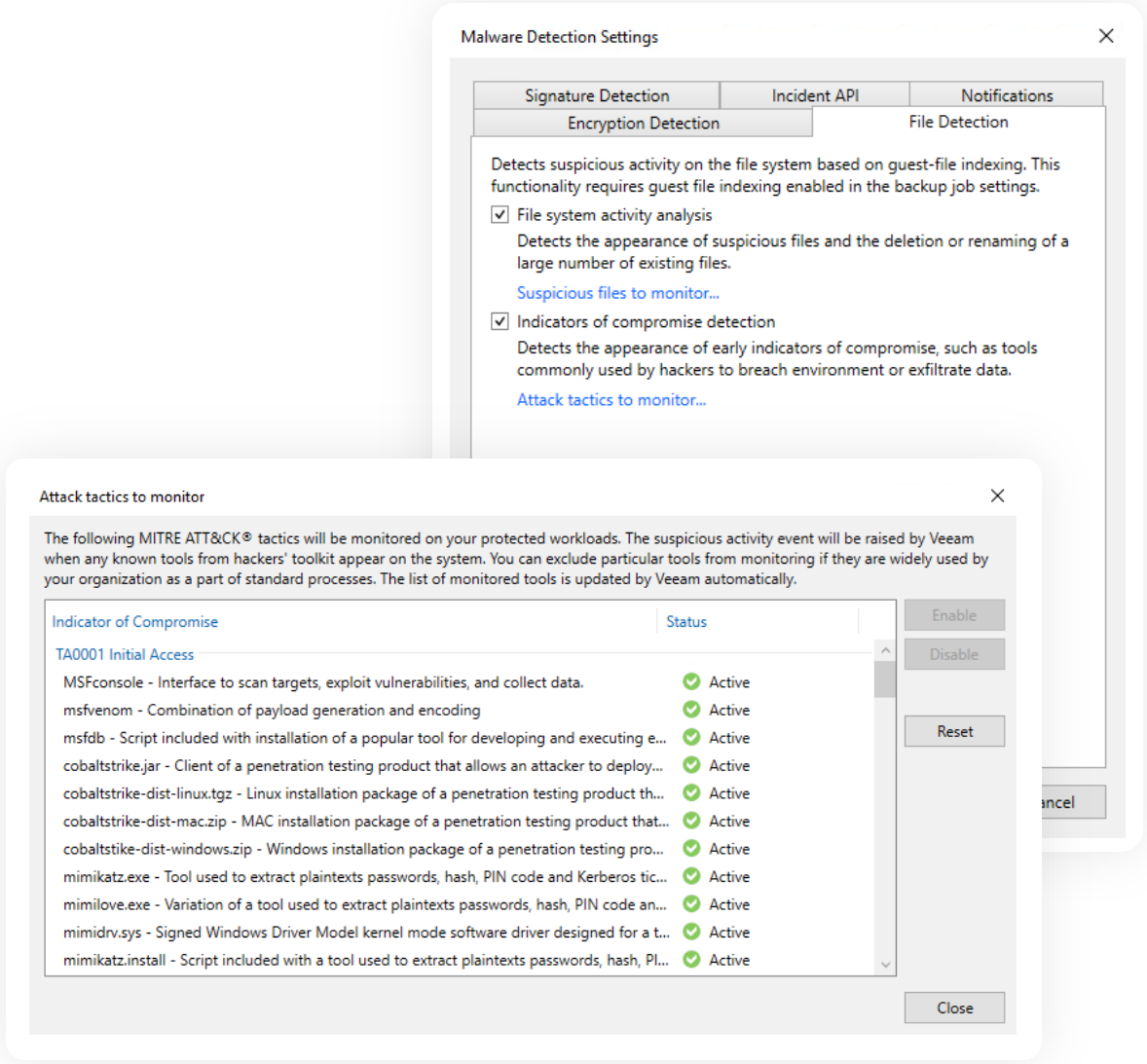
- **NEW** IoC Tools Scanner
- AI-Powered Inline entropy analysis
- Immutability combined with single-use credentials

IoC Tools Scanner

Expand the hunt for Indicators of Compromise

Key features:

- Detect and uncover suspicious tools and tactics closer to the time of compromise
- Aligns to MITRE ATT&CK framework
  - List of threats is constantly updated
  - Checks can be customized to fit your environment
- Works in conjunction with Veeam Threat Hunter
  - File signatures remain the same despite filename changes

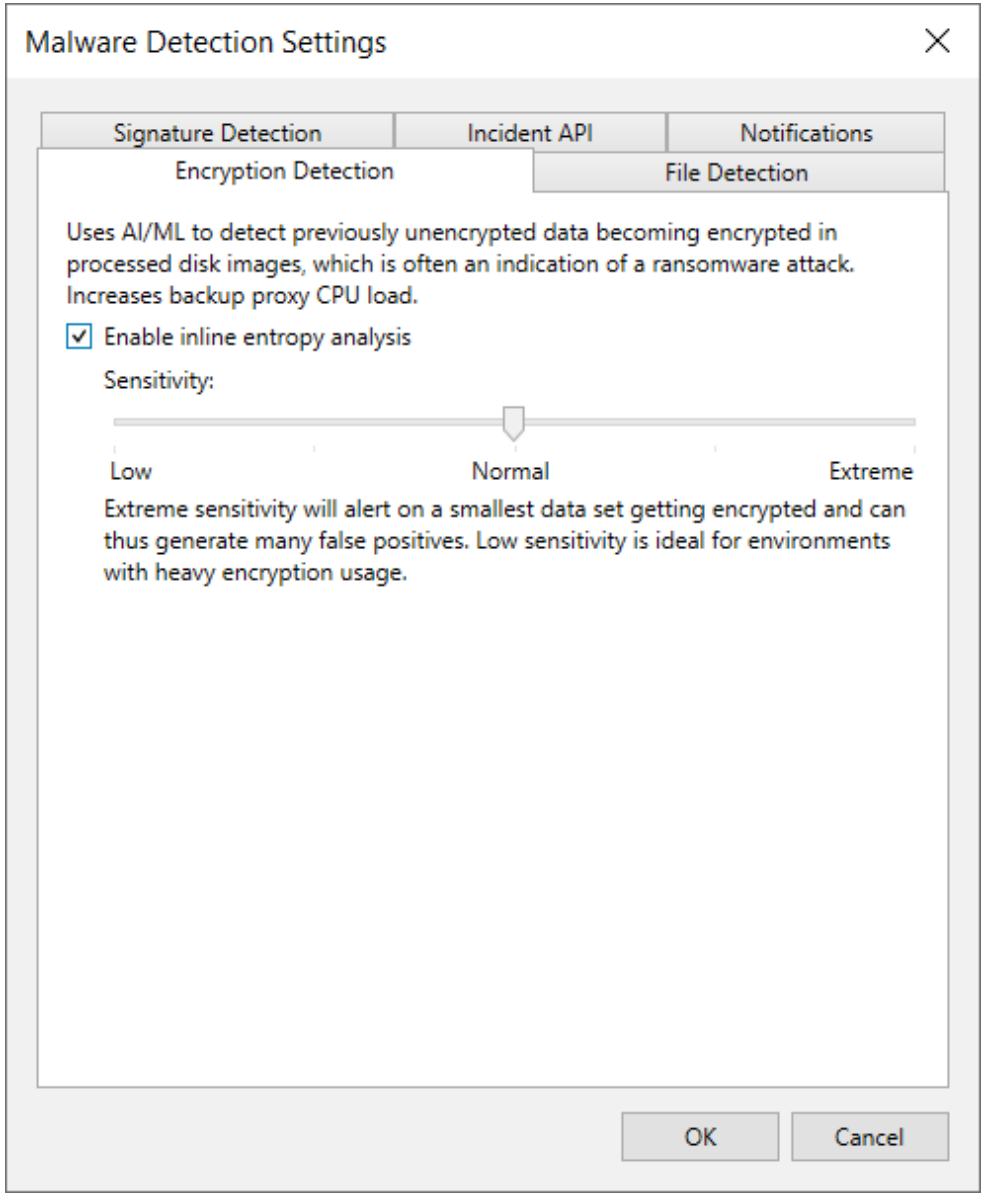


Malware Detection

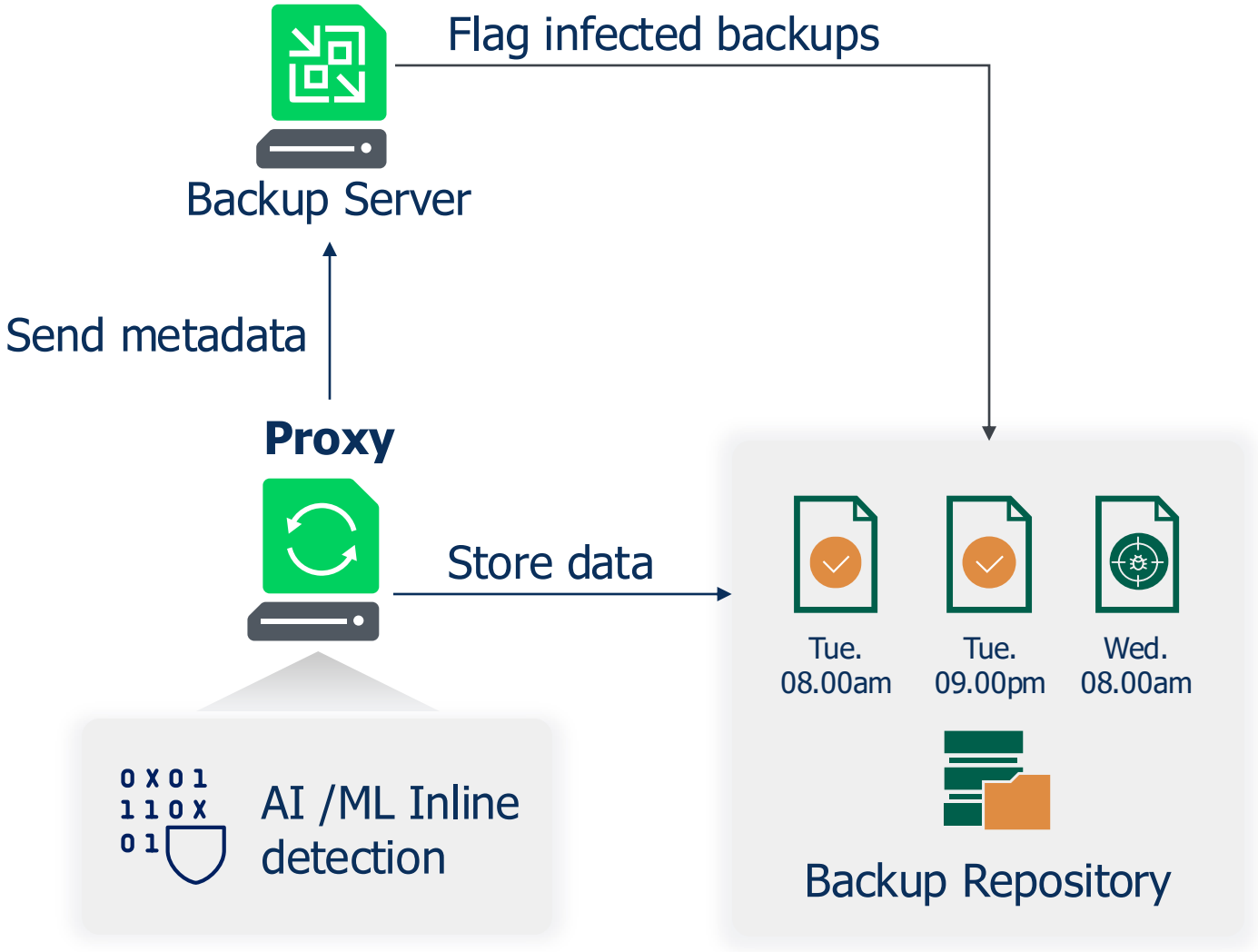
AI-powered inline scanning and file system analysis

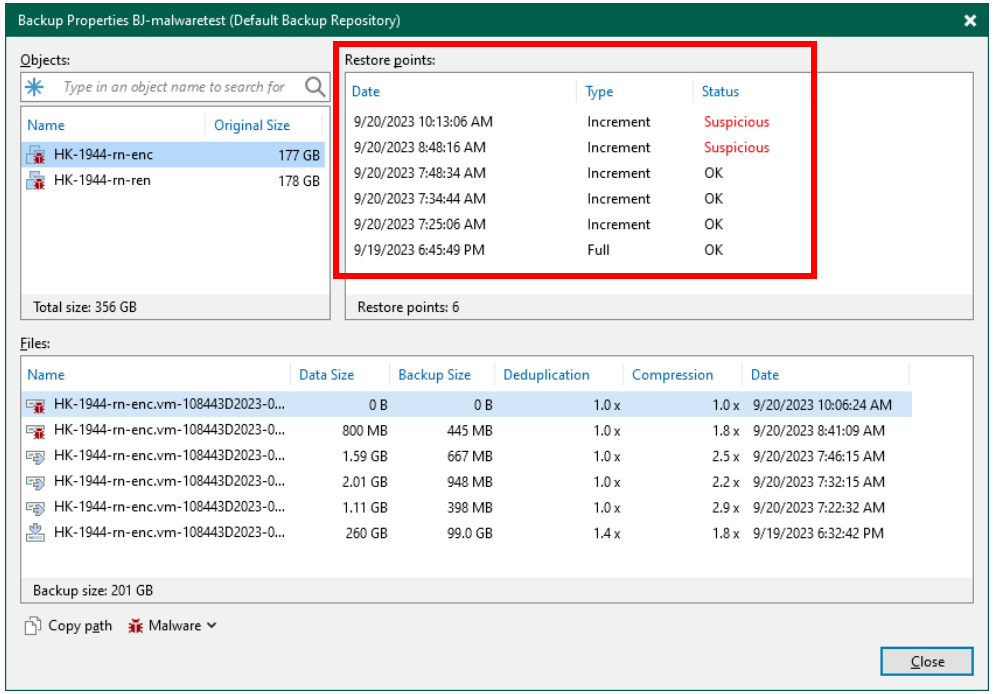
Bring detection closer to the time of infection

- Measure and analyze entropy changes
- Mark backups as *clean, suspect,* or *infected*



Inline Malware Detection Overview





Hardened Linux repository overview (Immutability)

Why?

Malware-safe repositories

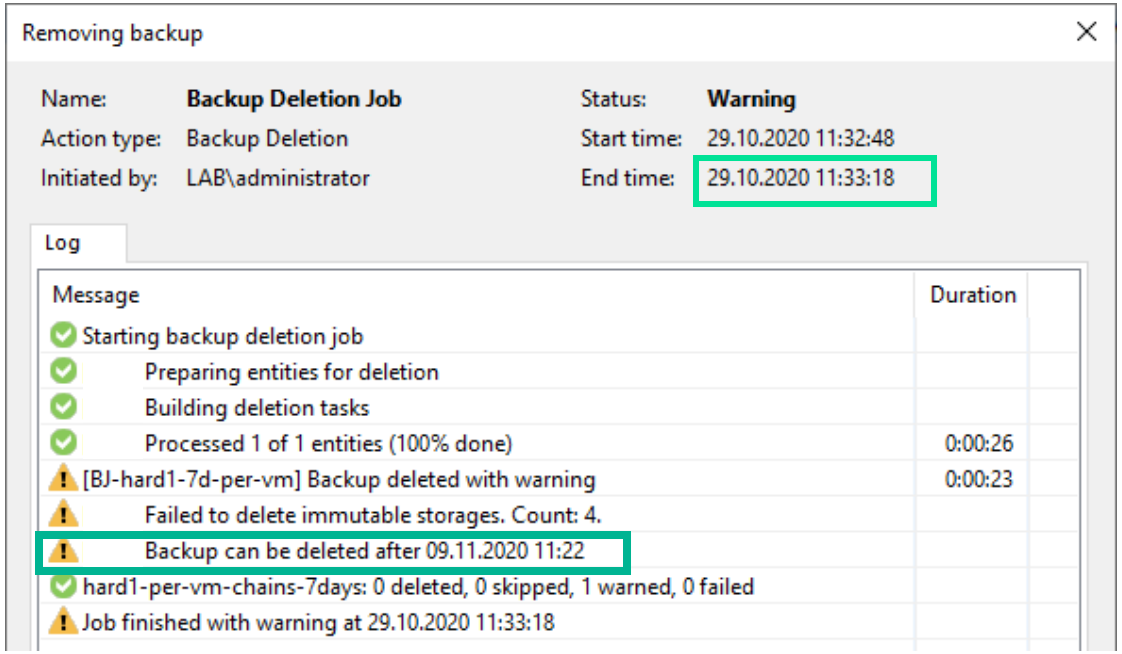
If set up properly: insider protection

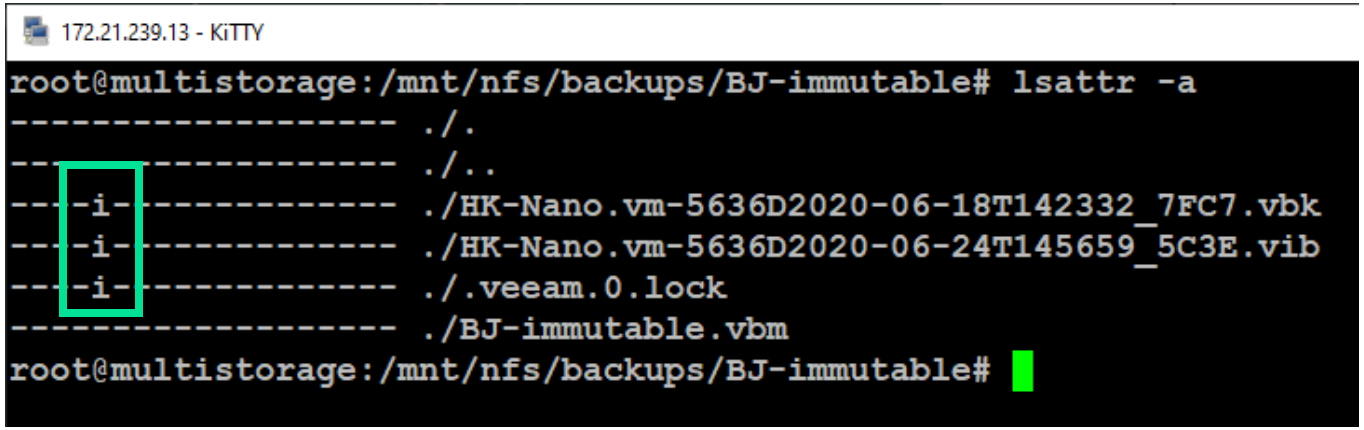
What

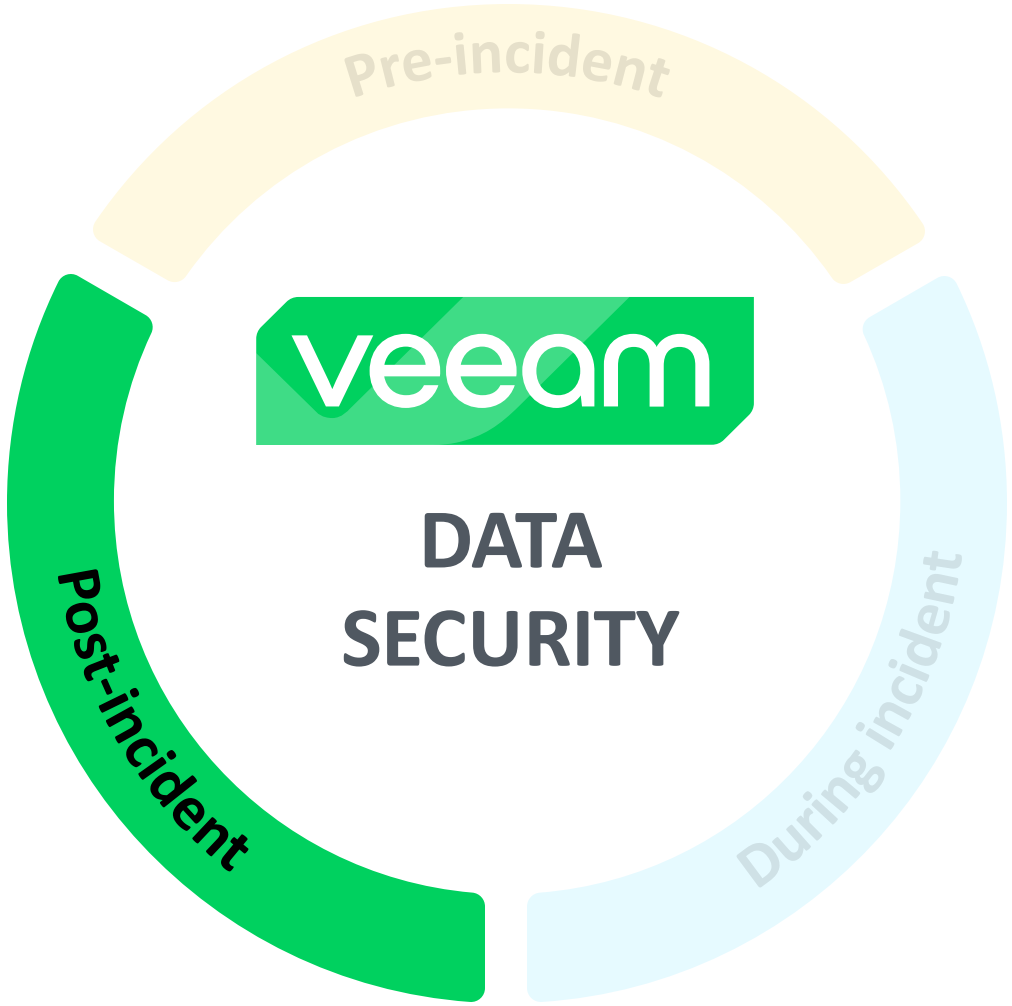
Deny deletion of backups

How

Use “immutable flag” in Linux







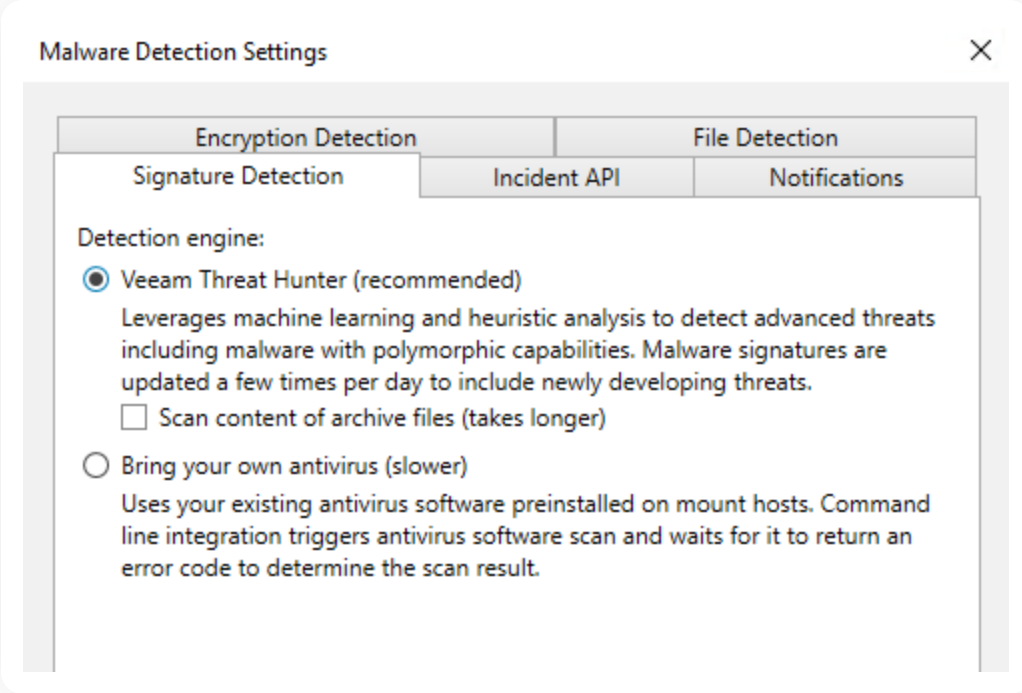
- **NEW** Veeam Threat Hunter
- YARA Rule-Based Scanning
- Secure Restore to Prevent Reinfection
- Recovery Verification with SureBackup

Veeam Threat Hunter

Protection against millions of malware threats

Key features:

- Enables an opportunity for dual AV scans (production system + Veeam Threat Hunter)
  - Provides a “second opinion” for false positives
  - Casts a wider net when looking for threats with a secondary signature-based scan
- Faster processing compared to external scanners
  - Deployed on Windows repository mount hosts
  - Improves performance for Secure Restore operations



What Are YARA Rules?

- Signature based detection
- Yes / no result
- Anyone can write rules
- Not a silver bullet

- Can be used to find “anything” e.g. credit card numbers

https://github.com/Yara-Rules/rules/blob/master/malware/APT_Blackenergy.yar

rules / malware / APT_Blackenergy.yar ↑ Top

Code | Blame | Raw

```
12
13  rule BlackEnergy_BE_2
14  {
15
16      meta:
17          description = "Detects BlackEnergy 2 Malware"
18          author = "Florian Roth"
19          reference = "http://goo.gl/DThzLz"
20          date = "2015/02/19"
21          hash = "983cfcf3aaaeff1ad82eb70f77088ad6ccedee77"
22
23      strings:
24          $s0 = "<description> Windows system utility service  </description>" fullword ascii
25          $s1 = "WindowsSysUtility - Unicode" fullword wide
26          $s2 = "msiexec.exe" fullword wide
27          $s3 = "WinHelpW" fullword ascii
28          $s4 = "ReadProcessMemory" fullword ascii
29
30      condition:
31          uint16(0) == 0x5a4d and filesize < 250KB and all of ($s*)
32  }
```

smaller 250KB

Windows binary

All $s conditions

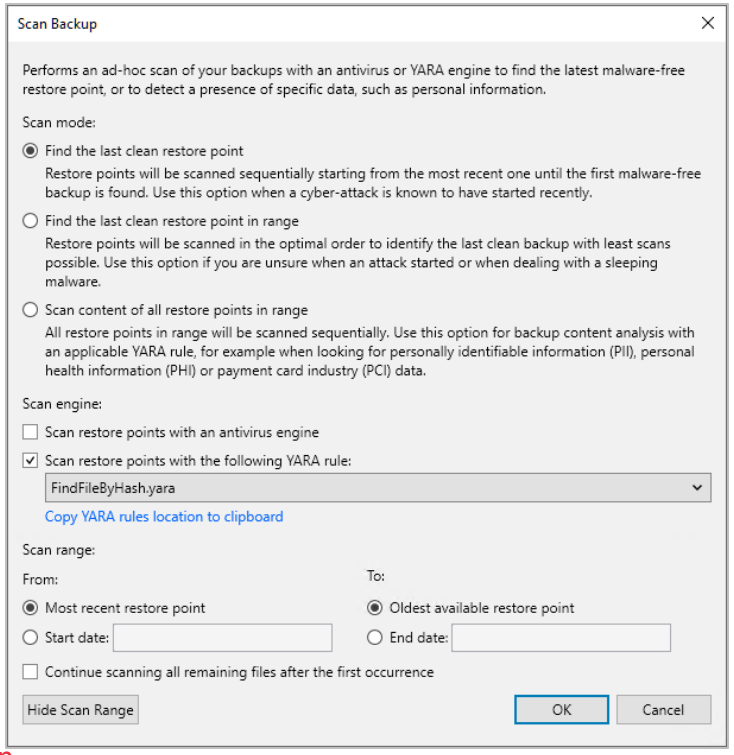
Yara Threat Detection Engine

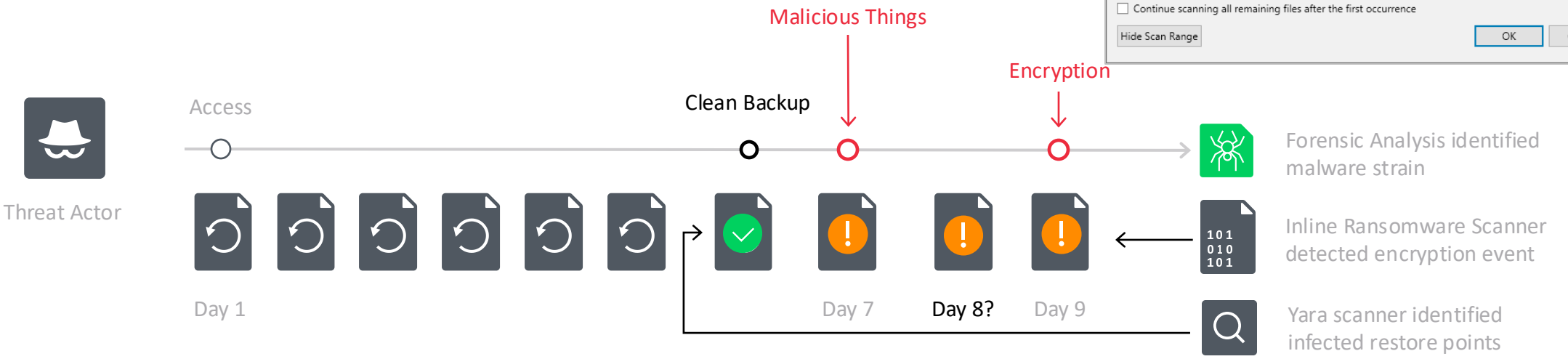
a) Yara is used in digital forensics and incident response

b) Ad-hoc Yara scan for a specific backup

c) Integrated into Surebackup and secure restore

d) Can be used daily or during incident response



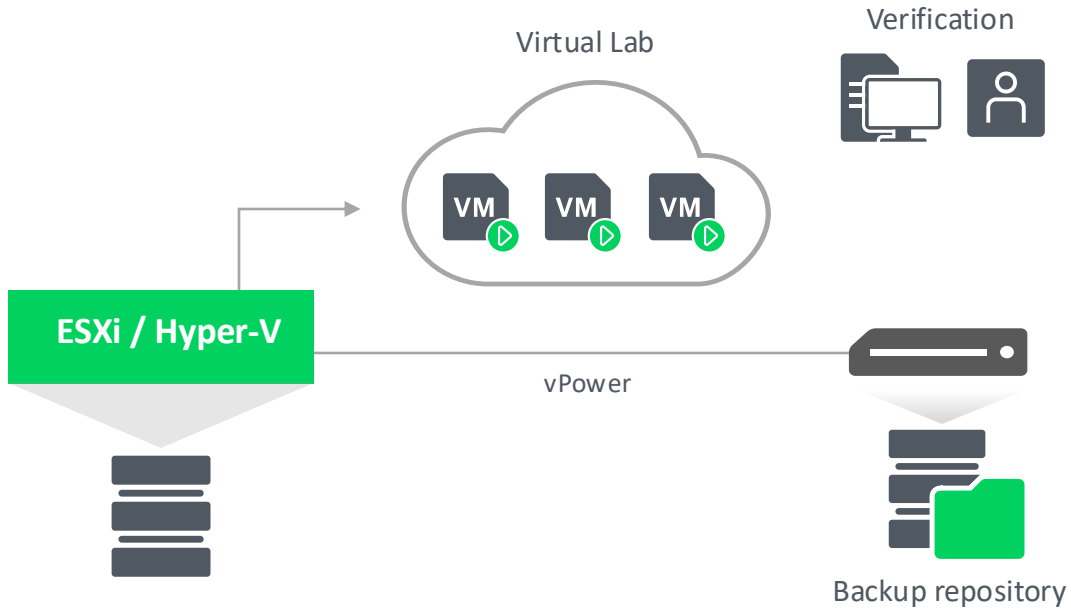


Accelerates clean recovery from ransomware while reducing the chance of reinfection

SureBackup

With SureBackup technology you can automatically verify the recoverability of every backup.

1. Starts VMs in an isolated Datalab environment
2. Performs a set of tests
3. Sends a status report to your mailbox



Create virtual lab → Create application groups → Create SureBackup Job(s) → Specify Tests within the jobs → Schedule SureBackup jobs → Receive verification report

SureBackup Report

SureBackup: Exchange SureBackup Job

Session Details

Status	Success	**Start time**	12/29/2018 2:03:30 PM	**Details**
Total tasks	4	**End time**	12/29/2018 3:21:05 PM	
Processed tasks	4	**Duration**	1:17:34	
Successful tasks	4	**Warning tasks**	0	
Failed tasks	0	**Skipped tasks**	0	
Progress	100 %			

Virtual machines status

VM name	Status	Start time	End time	Heartbeat test	Ping test	Custom script test	Validation test	Malware scan test
dns01	Success	12/29/2018 2:03:31 PM	12/29/2018 3:19:48 PM	Success	Success	Disabled	Disabled	Disabled
dc03	Success	12/29/2018 2:03:31 PM	12/29/2018 3:19:39 PM	Success	Success	Disabled	Disabled	Disabled
exch01	Success	12/29/2018 2:03:31 PM	12/29/2018 3:19:28 PM	Success	Success	Disabled	Disabled	Disabled
fileserv03	Success	12/29/2018 2:03:31 PM	12/29/2018 3:20:55 PM	Success	Success	Disabled	Success	Success

Veeam Recovery Orchestrator

Compliance

RTO and RPO reporting help meet compliance standards and SLA targets

Clean Recovery

Restore the most recent clean recovery point, powered by iterative ransomware scans and VBR-backed intelligence

Dynamic Documentation

Automatically updated reports for checks, tests and executions help correct issues with DR readiness

Recovery to Cloud

Orchestrated Direct Restore to Microsoft Azure gives your business resiliency with DR to the cloud.

Supported platforms and applications:

Azure, vSphere, Hyper-V

Veaam Agents: Windows & Linux

Apps: Exchange, SQL, SharePoint

Storage: NetApp, HPE, Lenovo

Custom scripting

Resilience Throughout Your Data's Lifecycle

Before

During Backup

Recovery

Veeam Threat Center

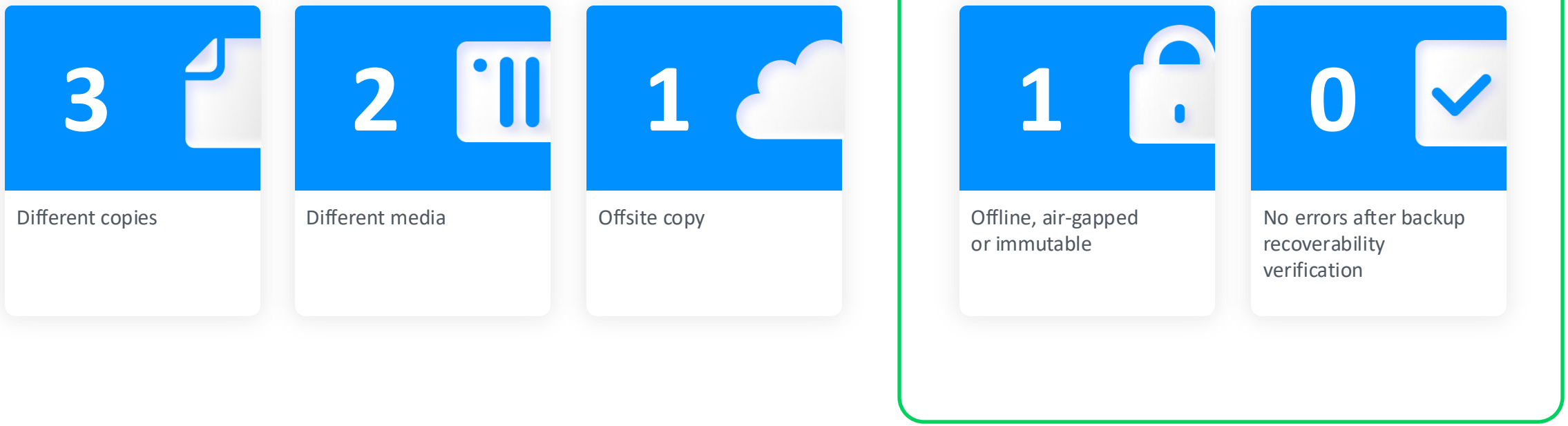
- Veeam Incident API
- Security & Compliance Analyzer
- Data Observability & Analytics
- Recon Scanner by Coveware

- Inline malware detection
- File system activity analysis
- Immutability
- IoC Tools Scanner

- Secure Restore
- YARA rule-based scanning
- Signature-based scanning
- Orchestrated Restore & Clean Room Recovery
- Incident Response by Coveware

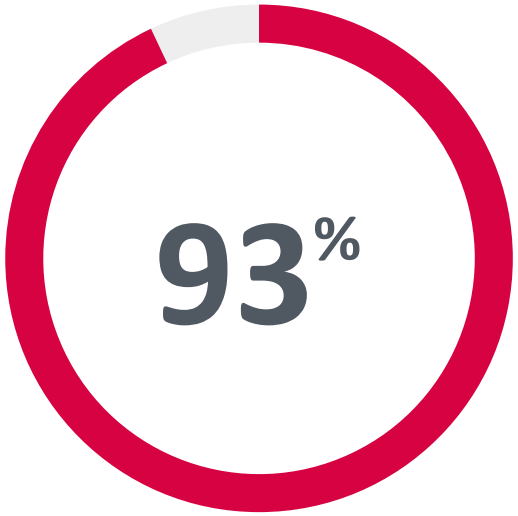
- Veeam Data Platform - Foundation
- Veeam Data Platform - Advanced
- Veeam Data Platform - Premium
- Veeam Cyber Secure

Prepare: the data protection zip code

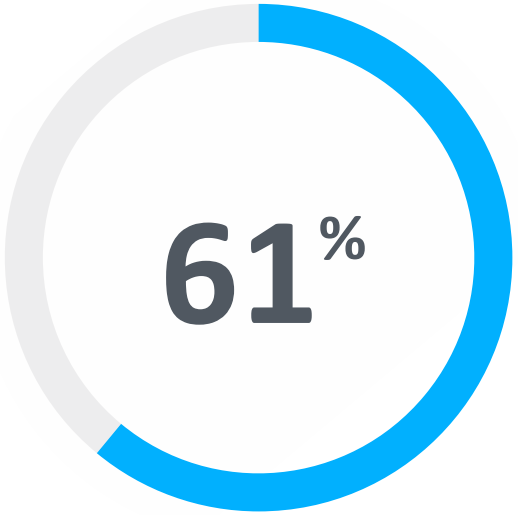


Veeam Data Cloud
Veeam Vault

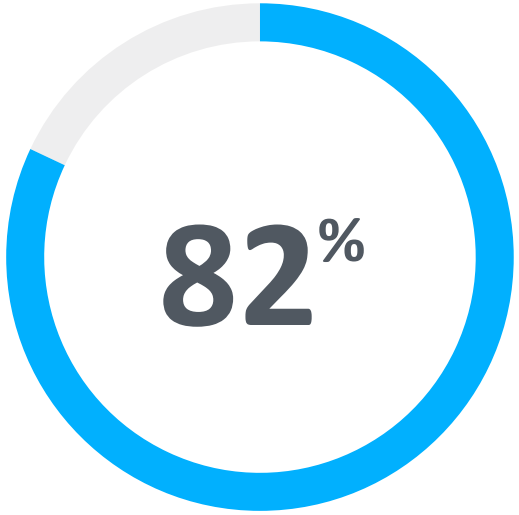
Backups need a resilient, secure place to land



of ransomware attacks explicitly target backups[1]



of organizations use cloud storage in addition to disk-based backup[2]



of organizations use immutable cloud storage[2]

1 Veeam Ransomware Trends 2023 report
2 Veeam Data Protection Trends 2024 report

3-2-1-1-0 Rule Made Easy

with Veeam Data Cloud Vault

3 COPIES OF DATA

- ✓ Supports direct, copied and tiered backup from VDP
- ✓ Synchronously copied in cloud for up to 12 nines of durability

2 DIFFERENT MEDIA

- ✓ Built on object storage to compliment on-premises disk

1 COPY OFFSITE

- ✓ Stored securely in cloud

1 COPY OFFLINE

- ✓ Logically air-gapped from your data center
- ✓ Always immutable

0 ERRORS

- ✓ Works with all Veeam backup and recovery verification tests

Conclusion

Importance of Data Security

Enhancing healthcare data security is essential to protect electronic health records and critical infrastructure from threats.

Understanding Challenges

Healthcare organizations need to understand various challenges posed by evolving cyber threats to safeguard sensitive patient data.

Implementing Solutions

Effective solutions can help healthcare organizations ensure compliance and protect against evolving threats to patient data.

Follow us!

Join the community hub: