



Winning the war on ransomware



Cornel Popescu
Sr. Systems Engineer

Understanding Cyberattacks

How to breach



vx-underground 

@vxunderground



All ALPHV ransomware group did to compromise MGM Resorts was hop on LinkedIn, find an employee, then call the Help Desk.

A company valued at \$33,900,000,000 was defeated by a 10-minute conversation.

3:45 AM · Sep 13, 2023 · **369.5K** Views

Understanding cyberattacks

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

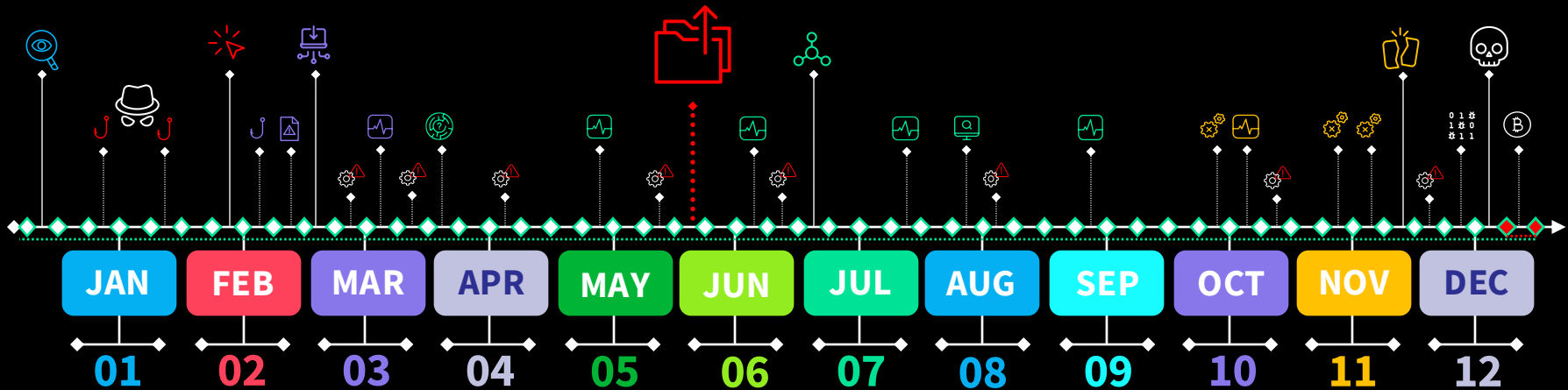
Gain access to the victim by sending phishing emails and let them click a link

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!



BACKUP **MALWARE/TOOLS**

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.



Principle of assume breach

Overview of Features

Veeam Data Platform Security Capabilities

Veeam Data Platform

Recovery Orchestration

Monitoring & Analytics

Backup & Recovery

Native APIs

Platform
Extensions

aws AWS

Azure

Google Cloud

Kubernetes



Cloud



Virtual



Physical



Apps

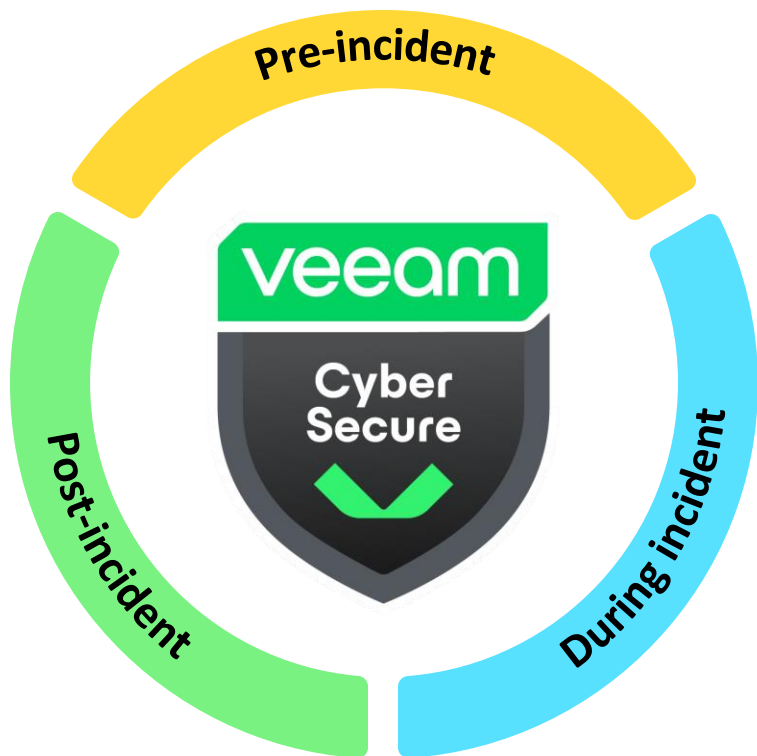


SaaS

Microsoft 365

Salesforce

On-Premises • In the Cloud • XaaS



Full Support for Every Stage

Pre-incident

- Malware detection
- ServiceNow and Syslog integration
- Incident API

During incident

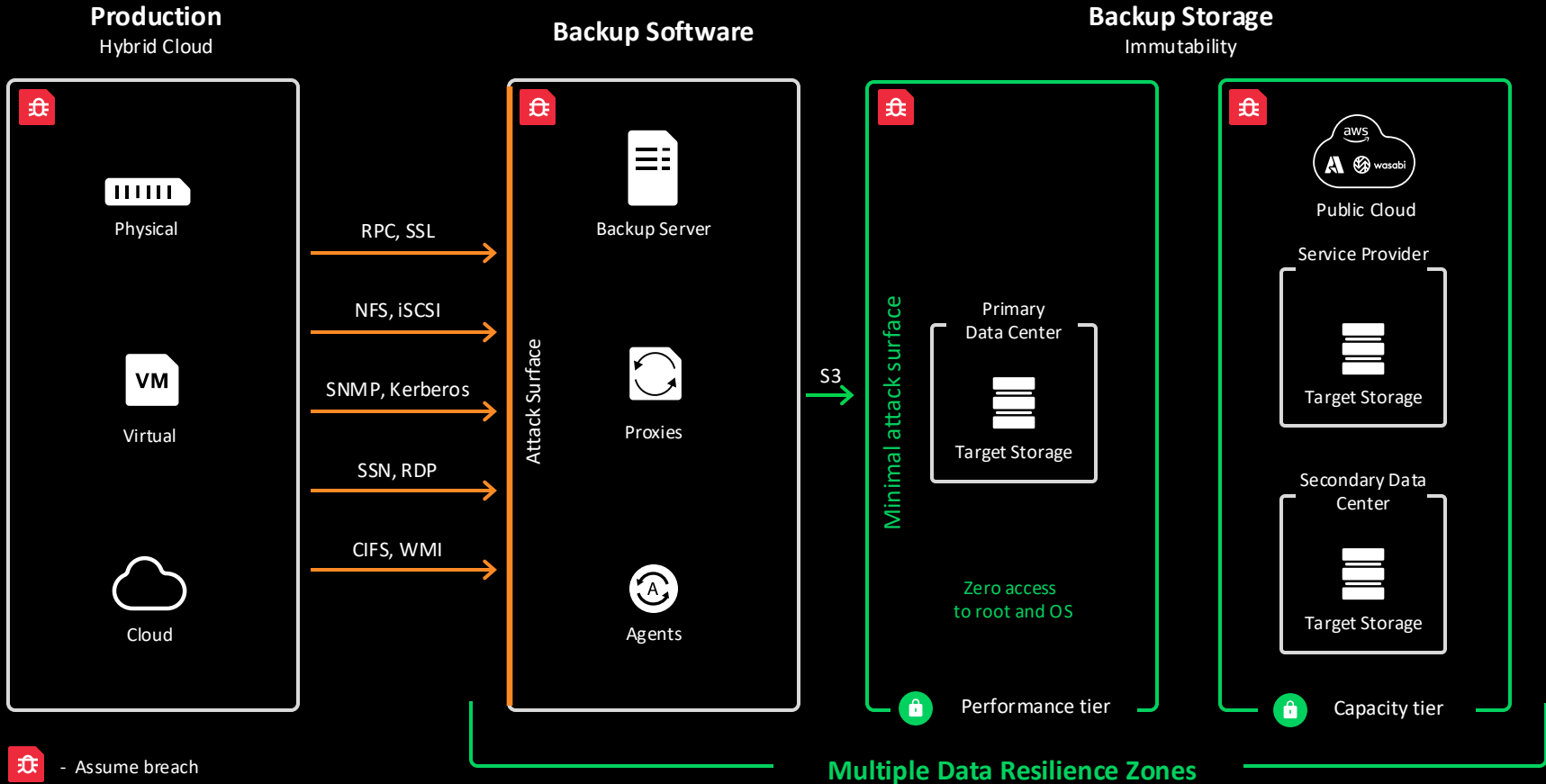
- Avoid reinfection
- Fast recovery
- YARA and AV scans

Post-incident

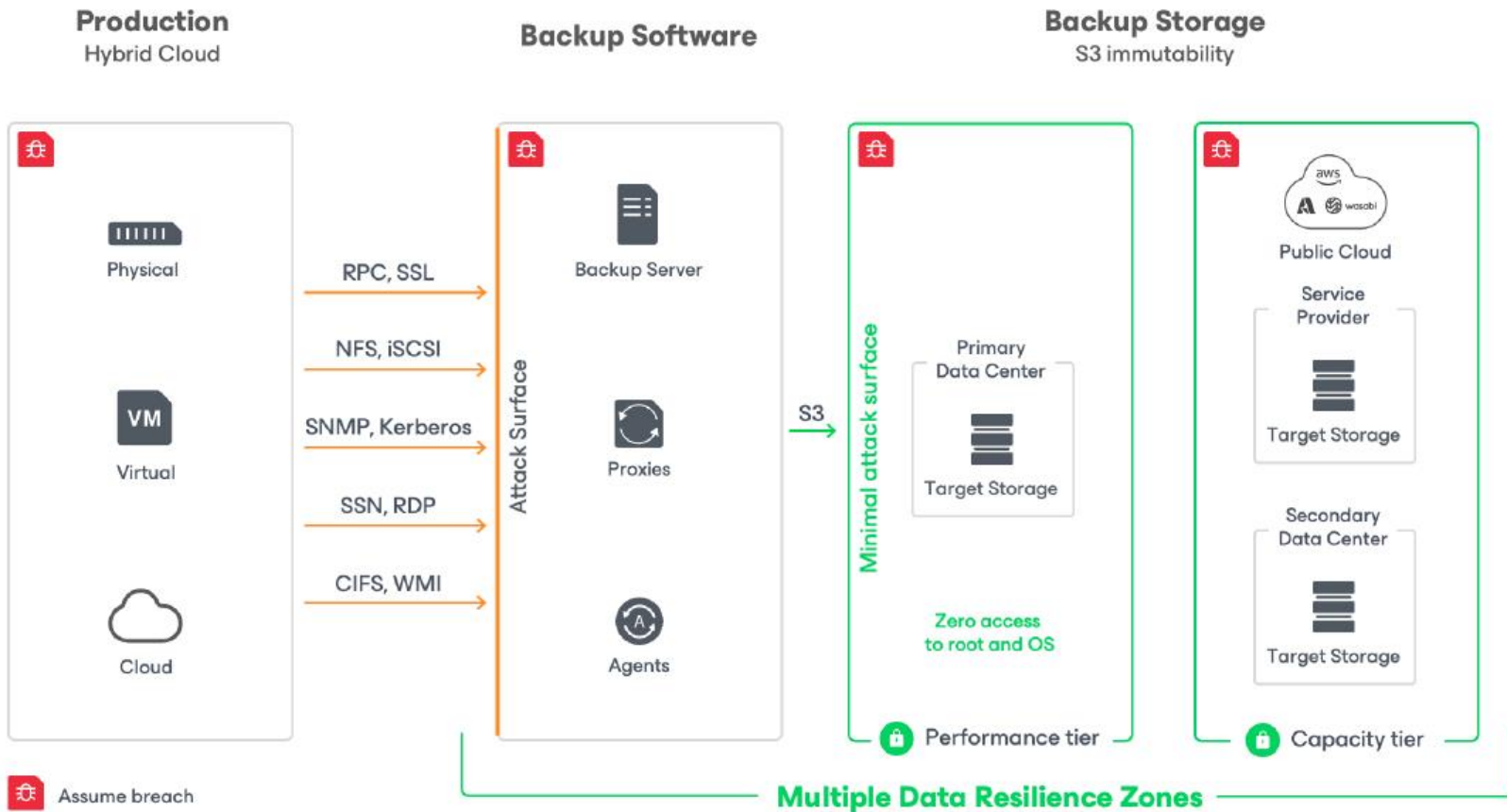
- Security and compliance analyzer
- Threat center dashboard
- Four-eyes authorization



Zero Trust Data Resilience (ZTDR) Architecture



Zero Trust Data Resilience (ZTDR) Architecture





Pre-incident

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.

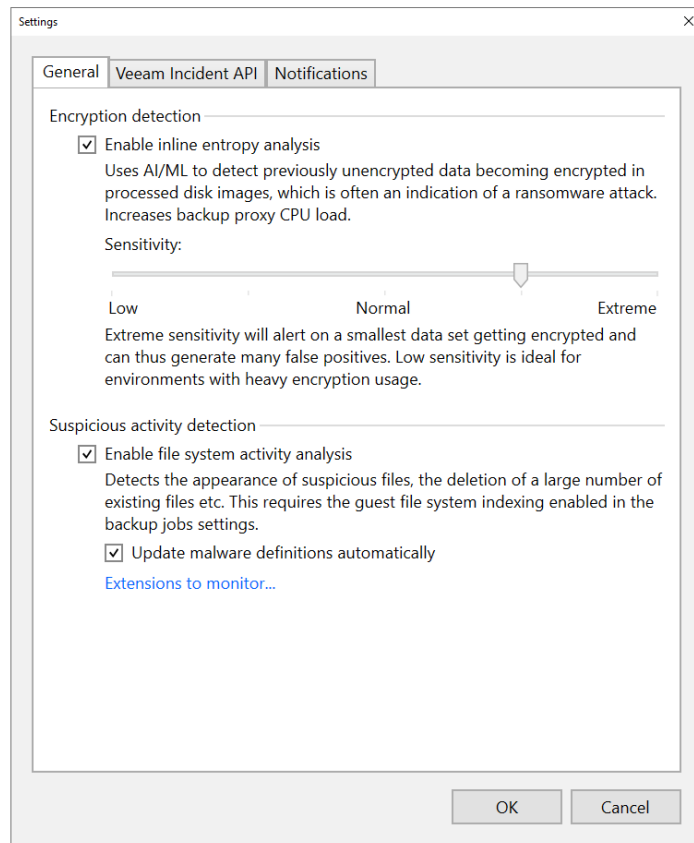
- Malware Detection
- ServiceNow and Syslog integration
- Veeam Incident API

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)
- Signature based detection



Integration with ServiceNow

Platform observability for the enterprise

Cross-incident lifecycle support

- Seamless integration for Veeam ONE™
- Leverage existing workflows and increase visibility across teams
- Two-way integration ensures both platforms are up to date

The screenshot shows the 'Server Settings' configuration page in ServiceNow. The left sidebar lists various settings categories, with 'ServiceNow' selected. The main content area is titled 'Configure ServiceNow server settings to send alarm notifications as incidents'. It includes sections for 'Enable ServiceNow integration', 'ServiceNow credentials', 'ServiceNow incident configuration', and 'ServiceNow incident additional fields'. The 'Instance URL' is set to 'https://yoursnowinstance.service-now.com'. Under 'ServiceNow credentials', 'Veeam ONE Admin (Last edited: Today)' is listed. The 'ServiceNow incident configuration' section has 'Caller' set to 'Veeam ONE', 'Assignment group' set to 'Veeam ONE Support', and 'Close code' set to 'Resolved by Caller'. The 'Include Veeam ONE knowledge base information' checkbox is checked. There is a 'Test ServiceNow integration' button at the bottom.

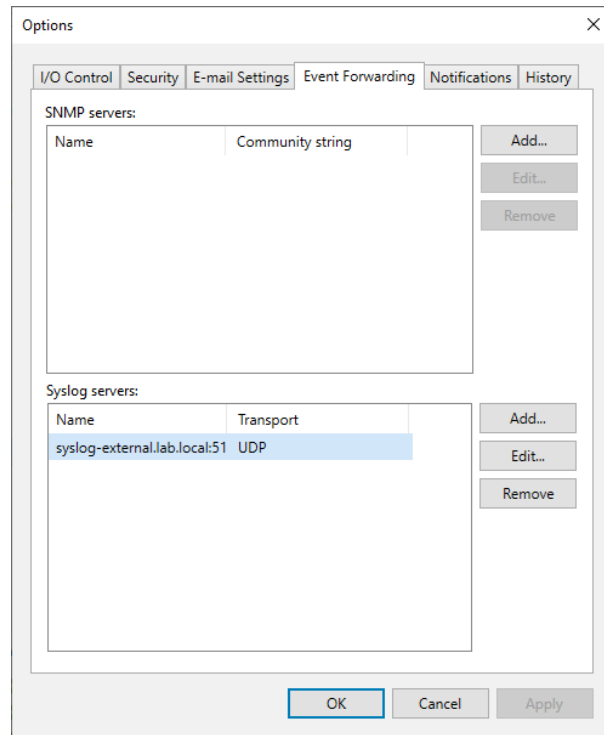
The screenshot shows the ServiceNow Incident record for 'Incident - NC0010038'. The incident details include: Number: NC0010038, Opened: 2023-10-01 15:04:42, Closed: (empty), Urgency: 2 - Medium, State: New. The short description is 'Potential infrastructure malware activity'. The 'Additional comments (Customer-visible)' section contains a comment from 'System Administrator' dated 2023-10-01 15:04:42. The comment text describes a summary of Veeam Backup & Replication integration with the backup system, mentioning that it provides an API for other services to check and mark VMs as infected. It also mentions that Veeam ONE can identify and quarantine infected VMs and that Veeam ONE can be used to identify and quarantine infected VMs. The comment also mentions that Veeam ONE can be used to identify and quarantine infected VMs. The incident is assigned to 'System Administrator' with a priority of '3 - Moderate'.

Syslog Event Forwarding

Leverage your existing tools

Broaden the visibility of your protection

- Provide data to SIEM tools for collection, aggregation, and analysis
- Effortless configuration removes the burden of deployment and management
- Streamline and centralize Day 2 operational monitoring

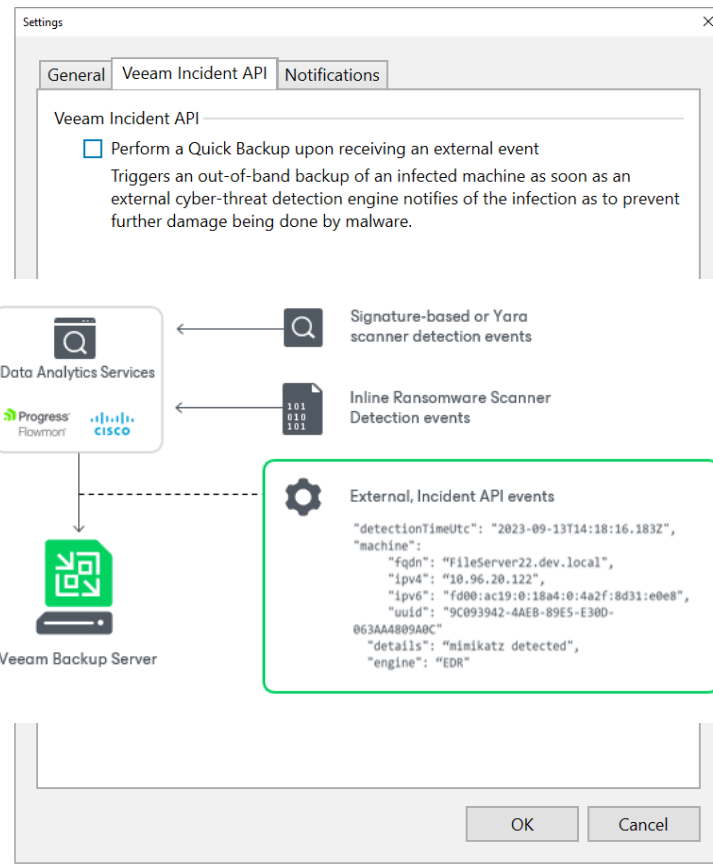


Veeam Incident API

Get a second opinion

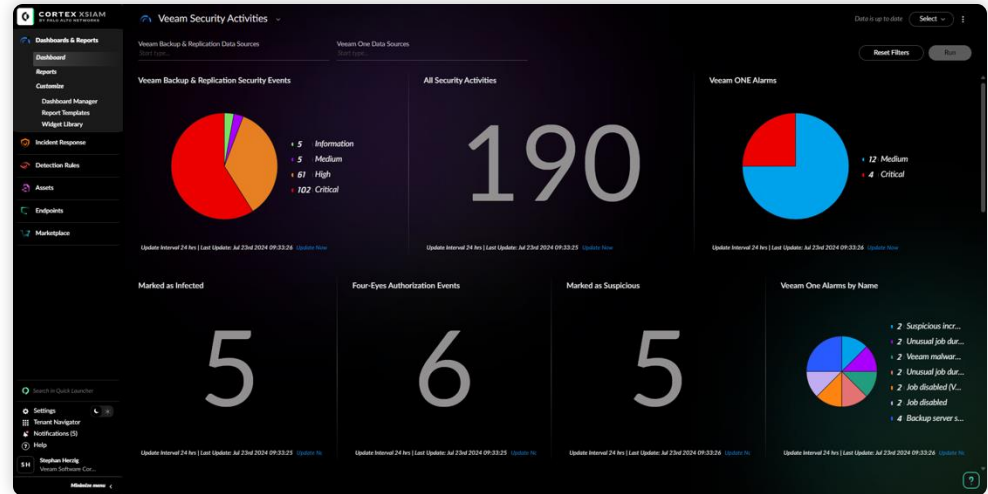
Receive real-time infection reports from third party tools

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



Veeam App for Palo Alto XSIAM and XSOAR

- Centralized view of security-related activity across your environment, now including your Veeam backups
- Pre-configured monitoring and security dashboards allow for easy setup and installation
- Automated, AI-powered investigation saves analysts from alert fatigue and manual processes
- Scalable, AI-powered incident response





During Incident

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
- Fast recovery

Quickly find a clean backup

YARA content analysis

Pinpoint ransomware strains in your environment

- Comprehensive and customizable backup queries
- Critical path in cyber recovery is finding a clean backup
- 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 To: Oldest available restore point

Start date: End date:

Continue scanning all remaining files after the first occurrence

[Hide scan range](#)

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.

Name

Linked Jobs

Settings

Schedule

Summary

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 occurrence

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

Linked Jobs

Settings

Schedule

Summary

Name: Scan for threats

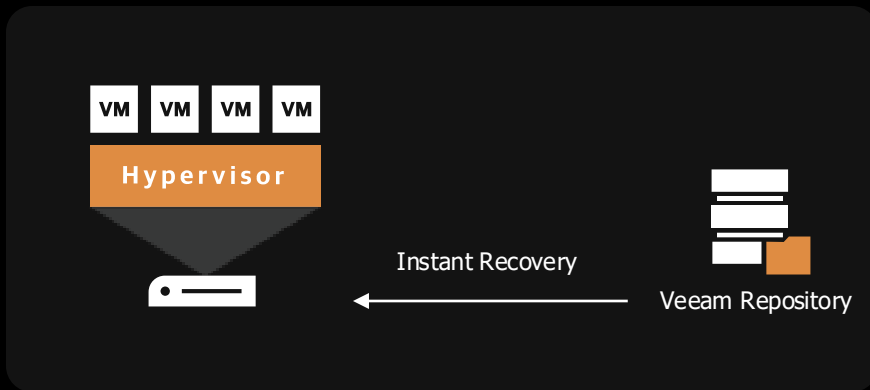
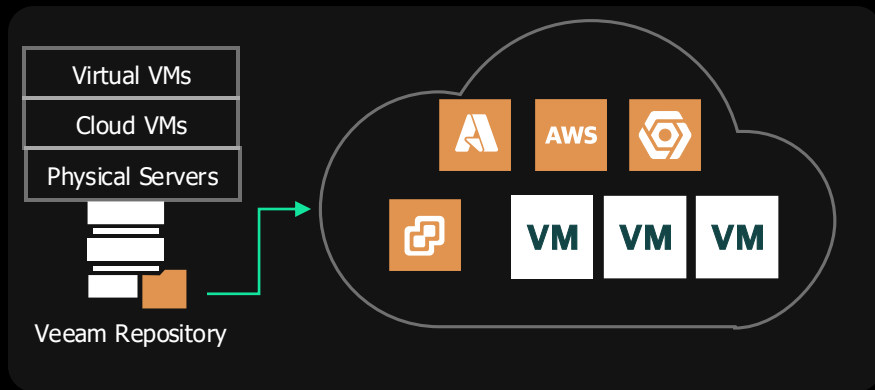
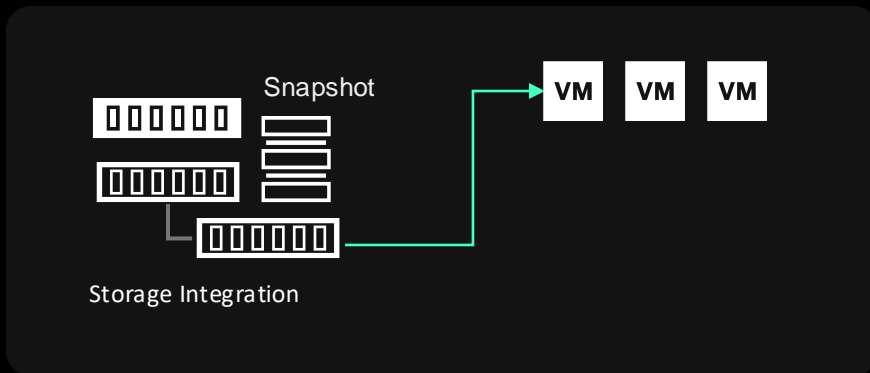
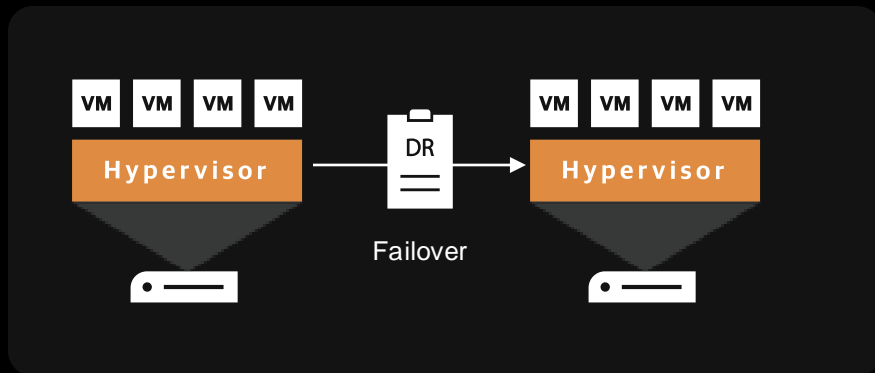
Description: Automated threat scanning

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.

< Previous Next > Finish Cancel

Fastest Recovery Options





Post-incident

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.

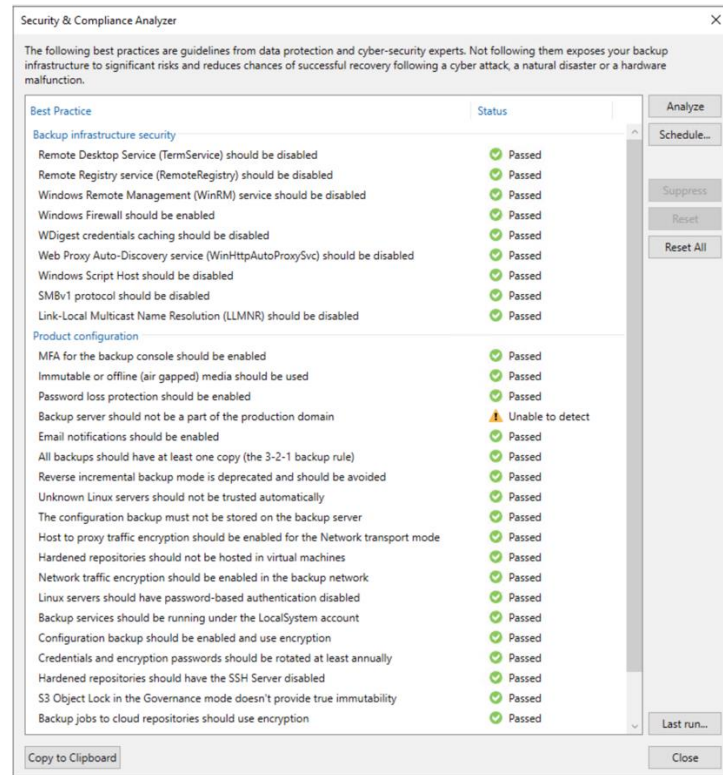
- Security and compliance analyzer
- “Four-eyes” principle protection
- Veeam Threat Center

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



“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

The screenshot displays the Veeam Backup and Replication console. The 'Users & Roles' window is open, showing the 'Authorization' tab. Under 'Four-eyes authorization', the checkbox 'Require additional approval for sensitive operations' is checked. Below it, a text box explains: '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.' A dropdown menu shows '7' days for 'Automatically reject pending approvals after:'. A modal dialog box titled 'Veeam Backup and Replication' is in the foreground, containing a question mark icon and the text: '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?'. It has 'Yes' and 'No' buttons.

The background interface shows the 'Approvals' section with a table of pending requests:

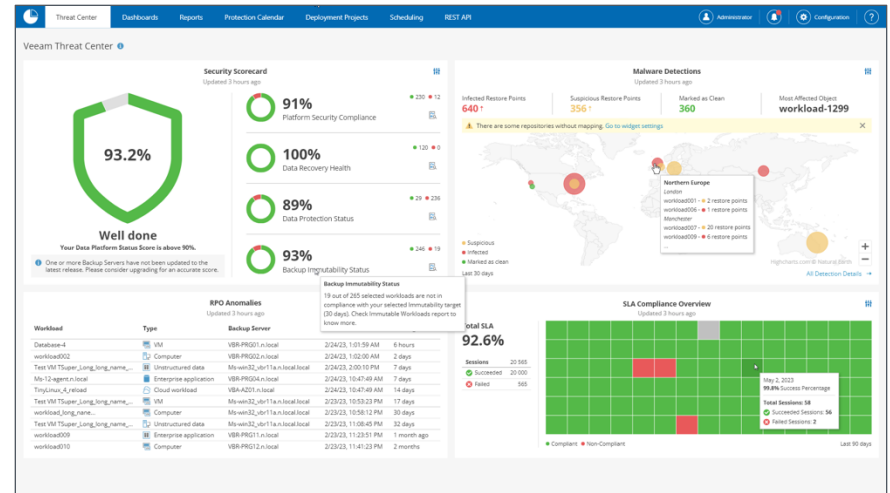
Event	Initiated by	Initiated at	Expires at
Delete backup NAS...	LAB\hannes	9/20/2023 10:31:59 AM	9/27/2023 10:31:59 AM
Delete repository S...	LAB\hannes	9/20/2023 10:33:50 AM	9/27/2023 10:33:50 AM

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 keeps
your business
running.