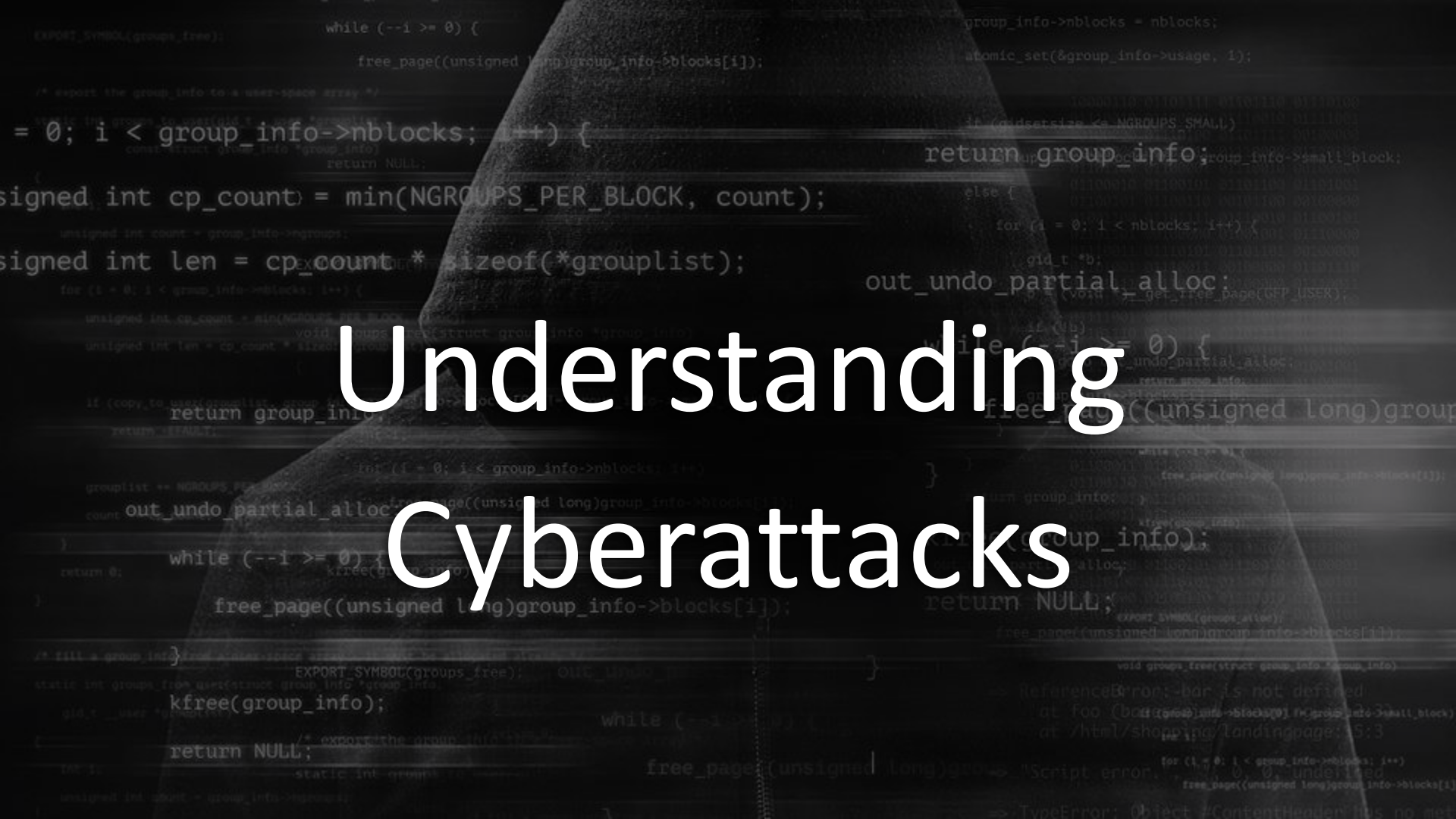
Winning the war on ransomware

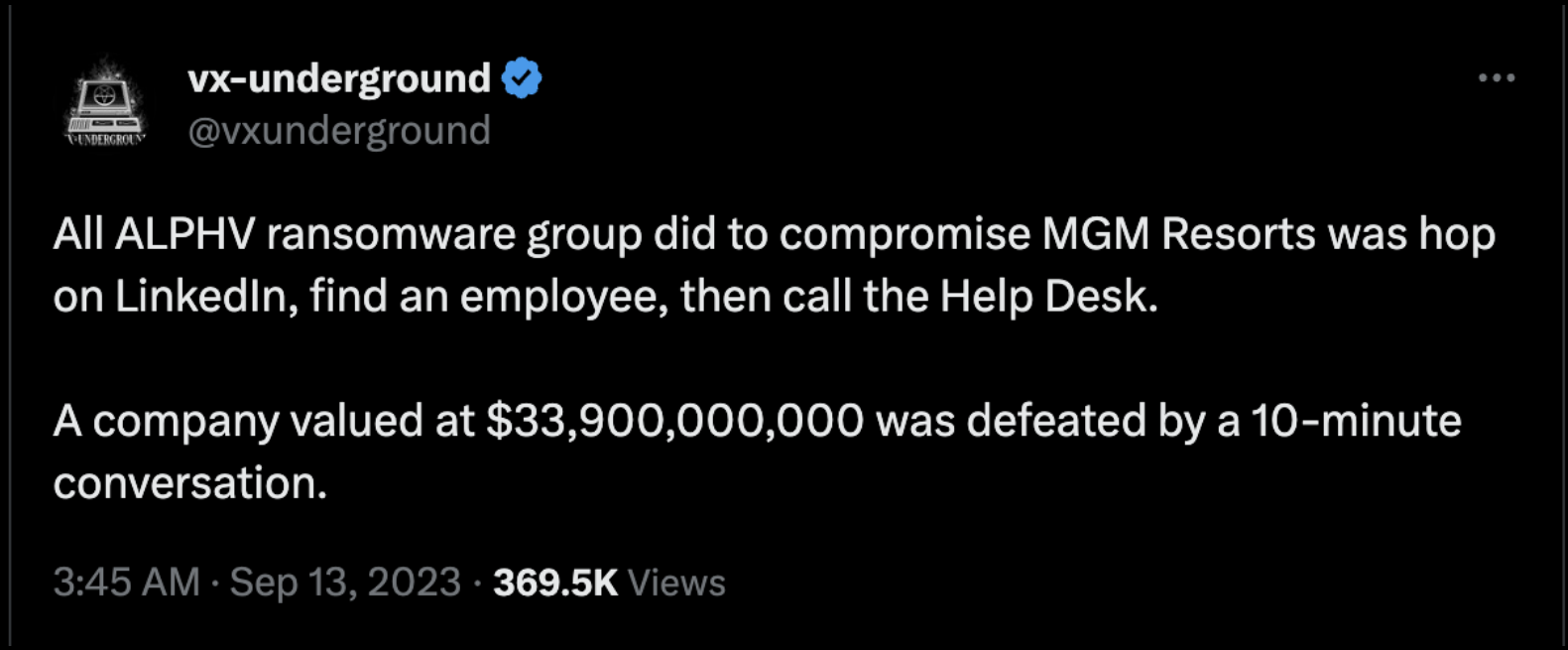
Cornel Popescu

Sr. Syestems Engineer

© 2023 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.


Understanding
Cyberattacks

How to breach



vx-underground
@vxunderground

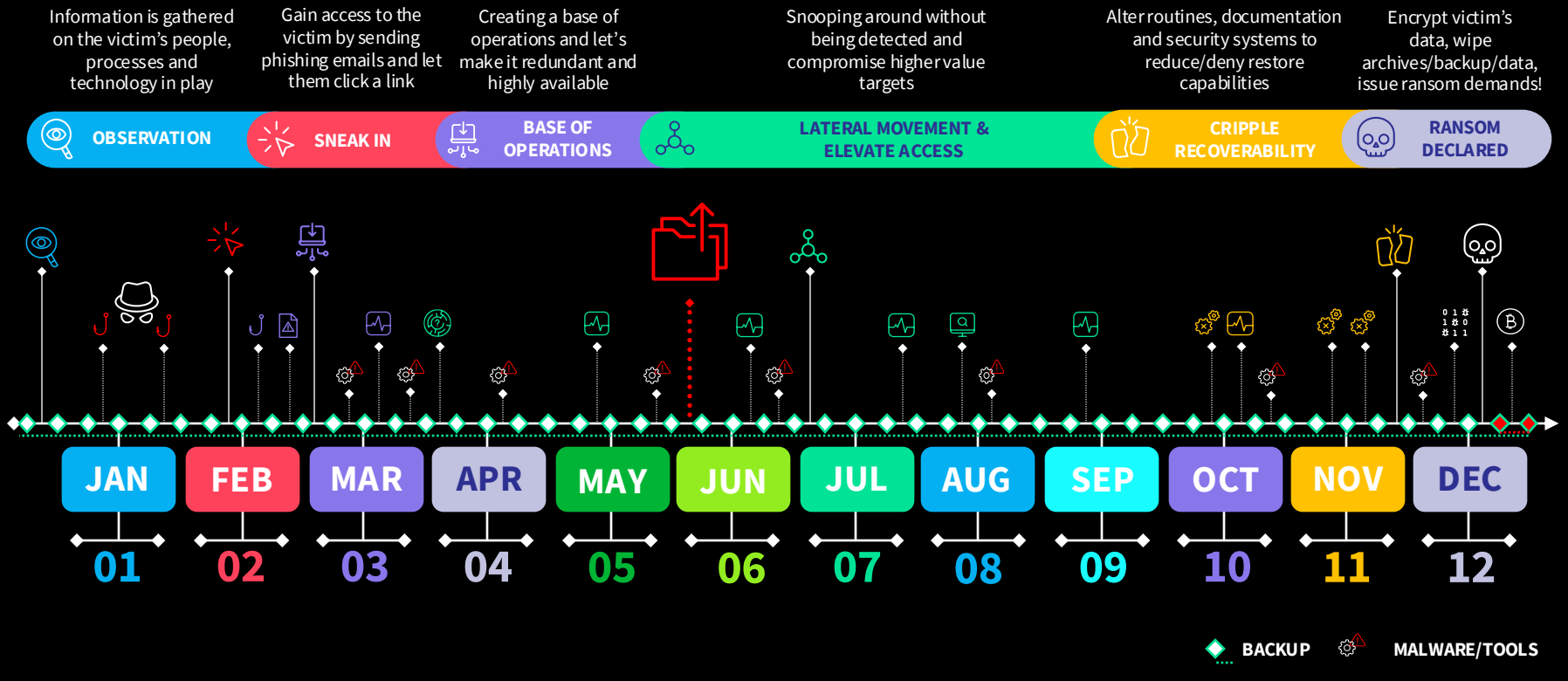
All ALPHV ransomware group did to compromise MGM Resorts was hop on LinkedIn, find an employee, then call the Help Desk.

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

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

© 2023 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Understanding cyberattacks

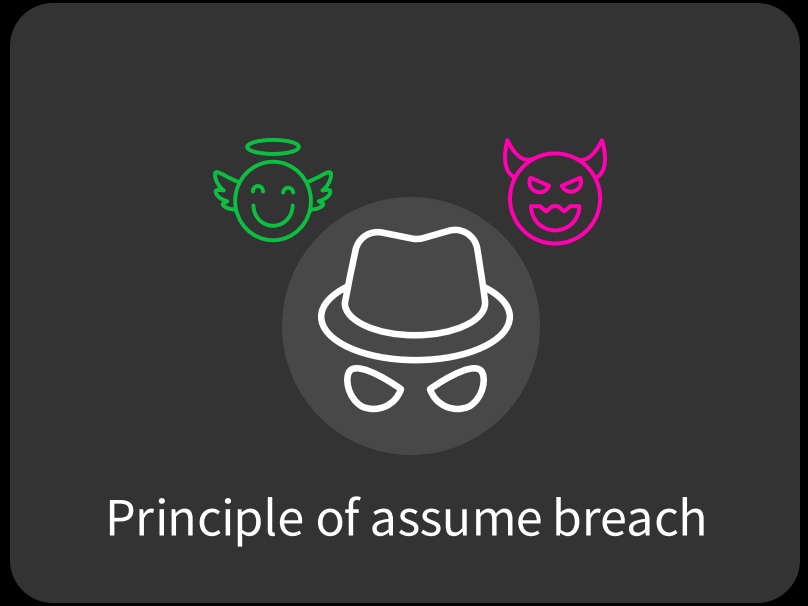


© 2023 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

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.

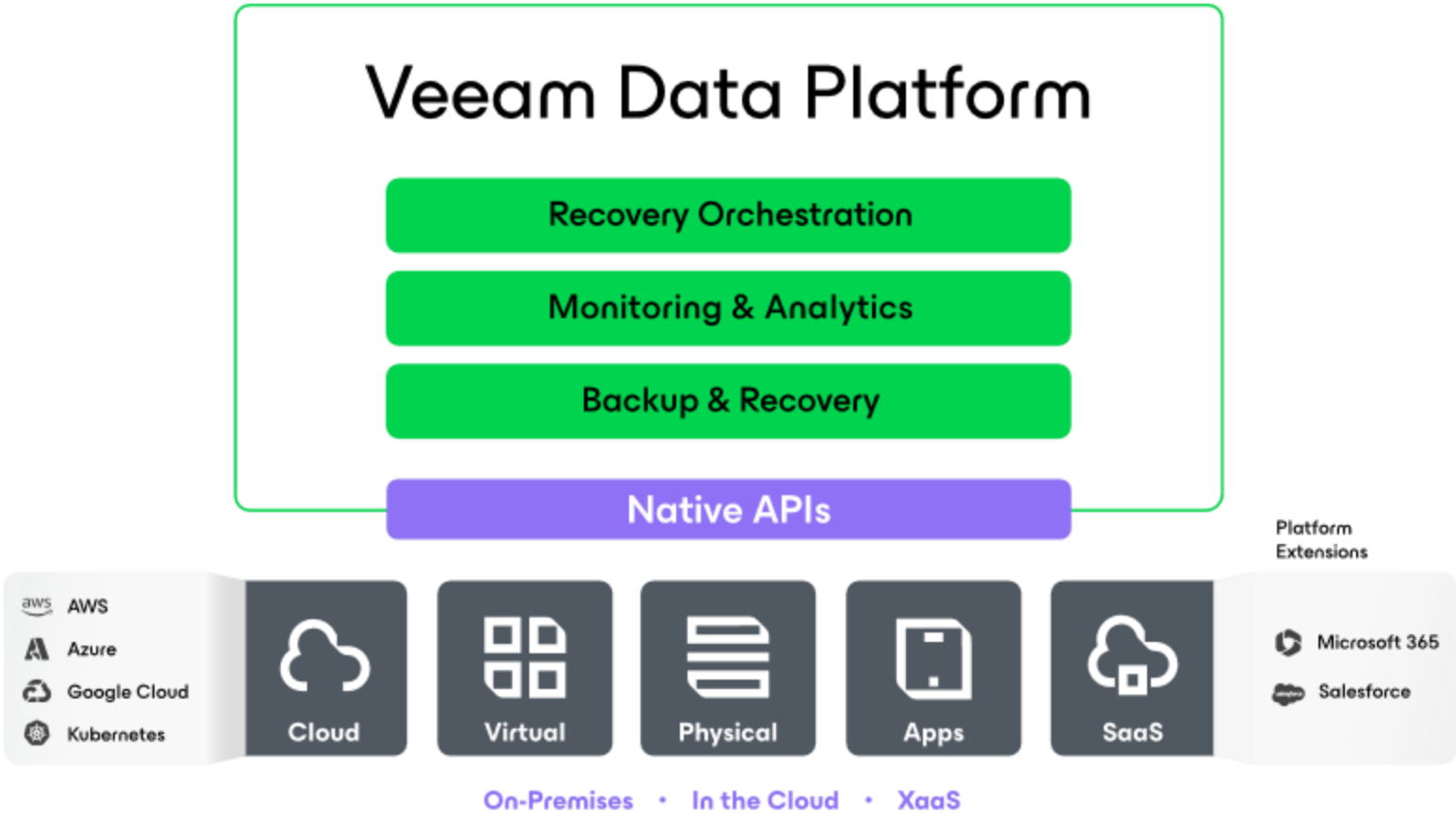


© 2023 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

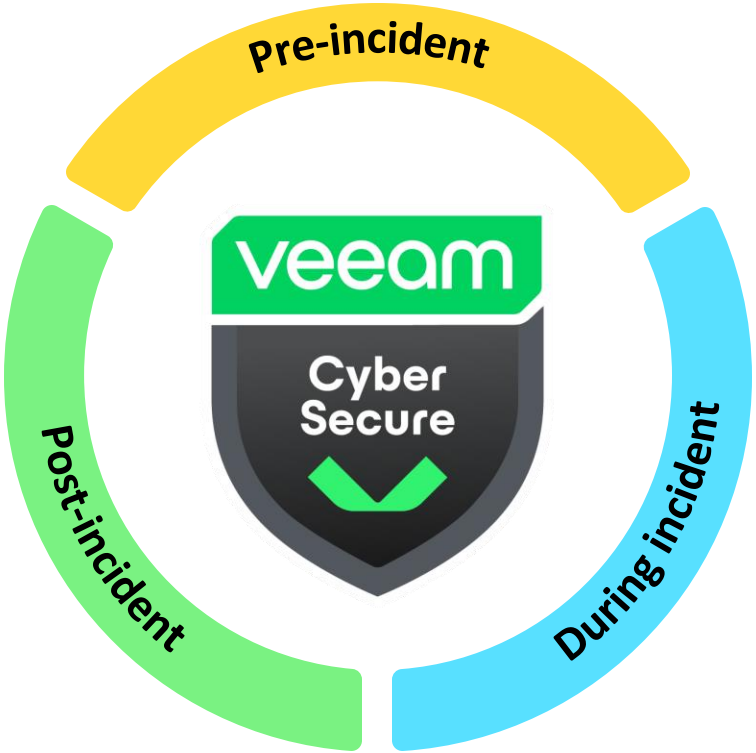
Overview of Features

Veeam Data Platform Security Capabilities

© 2023 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.



© 2023 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.



Full Support for Every Stage

Pre-incident

- Malware detection
- ServiceNow and Syslog integration
- Incident API

During incident

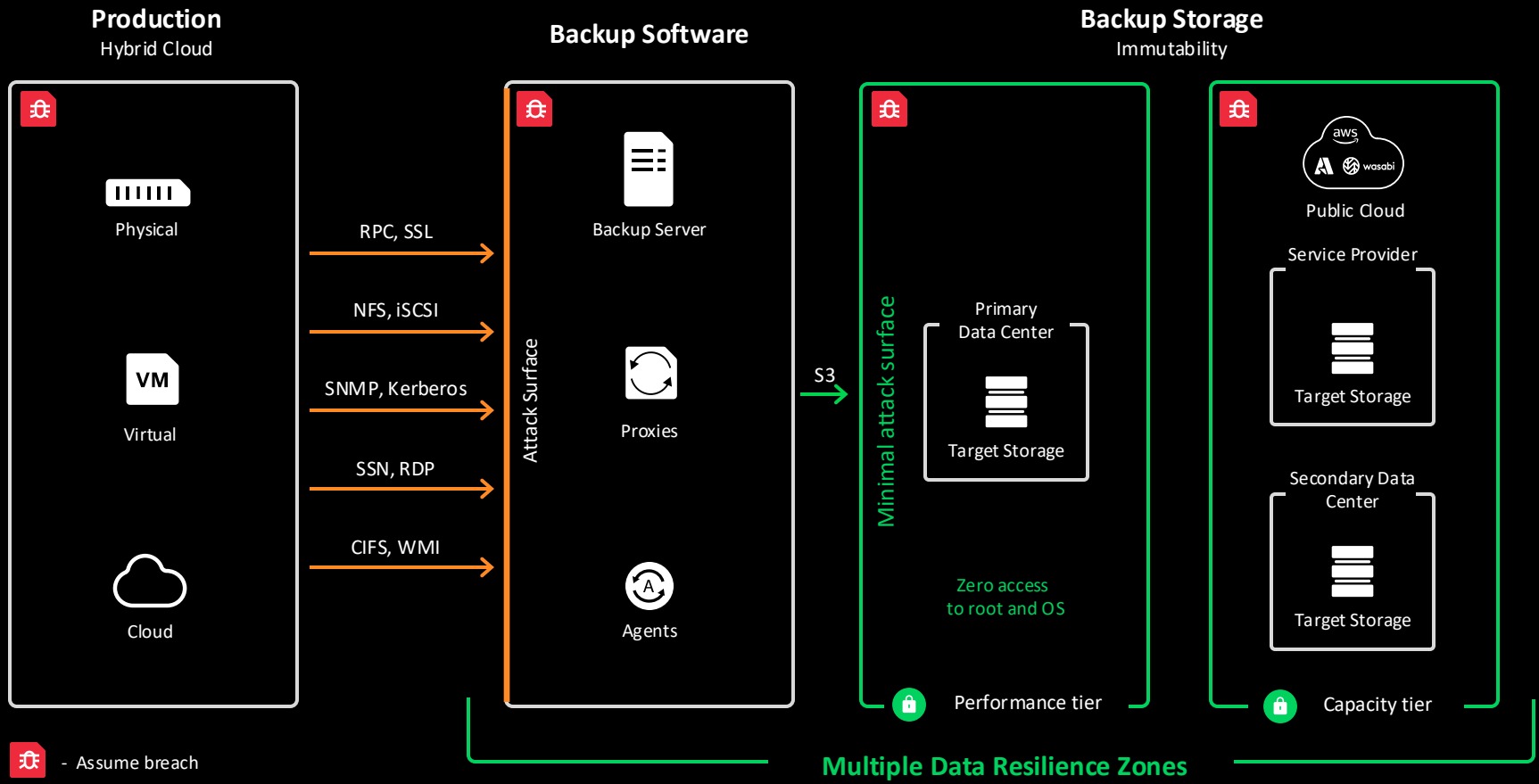
- Avoid reinfection
- Fast recovery
- YARA and AV scans

Post-incident

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

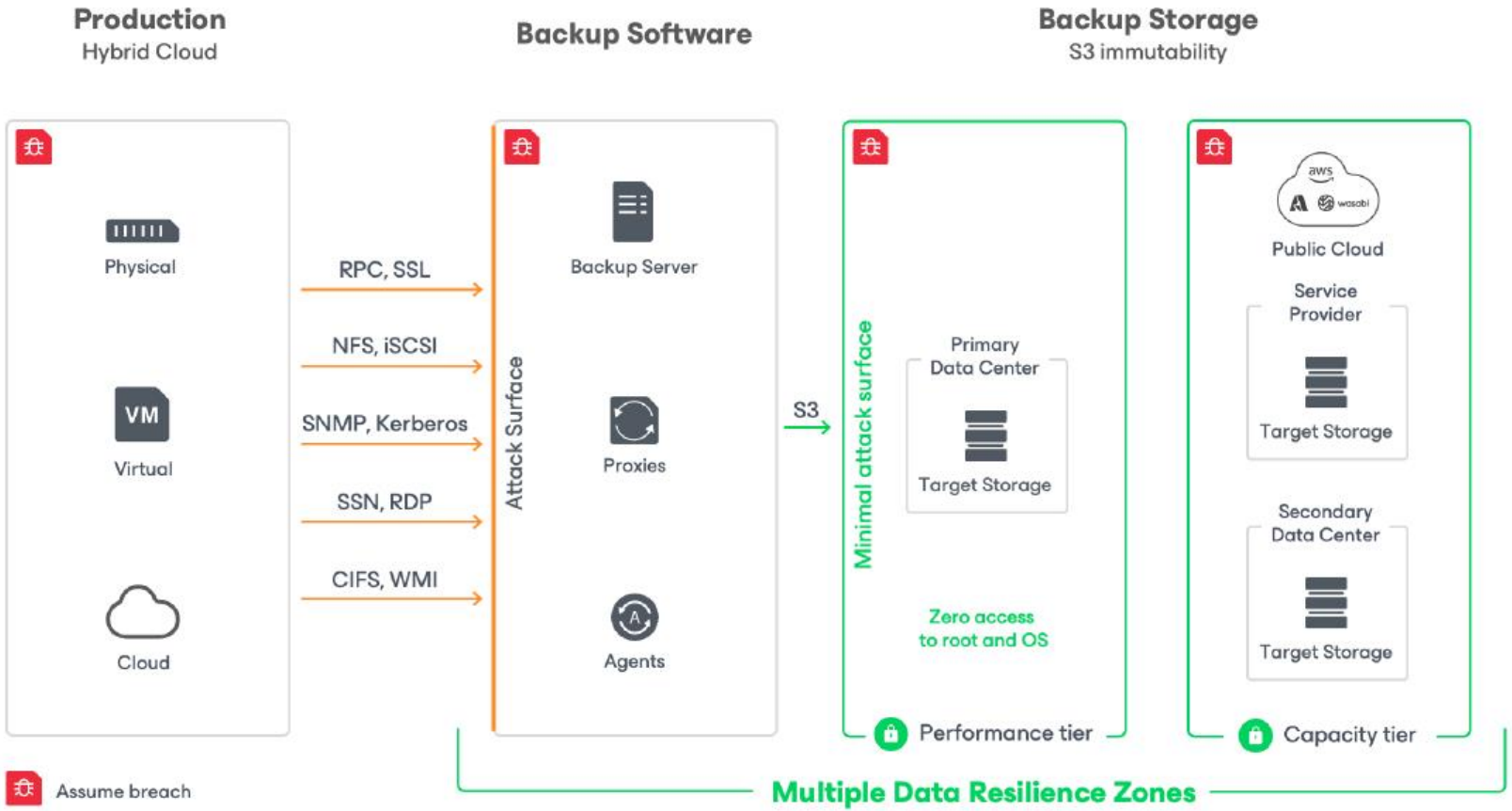
© 2023 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Zero Trust Data Resilience (ZTDR) Architecture



© 2024 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Zero Trust Data Resilience (ZTDR) Architecture



© 2024 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

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

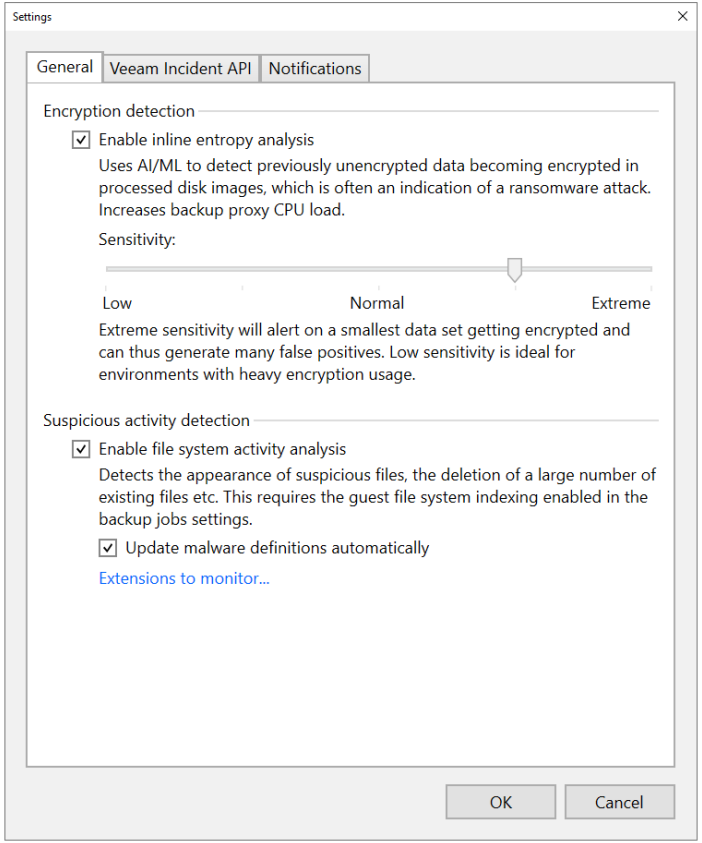
© 2023 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

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



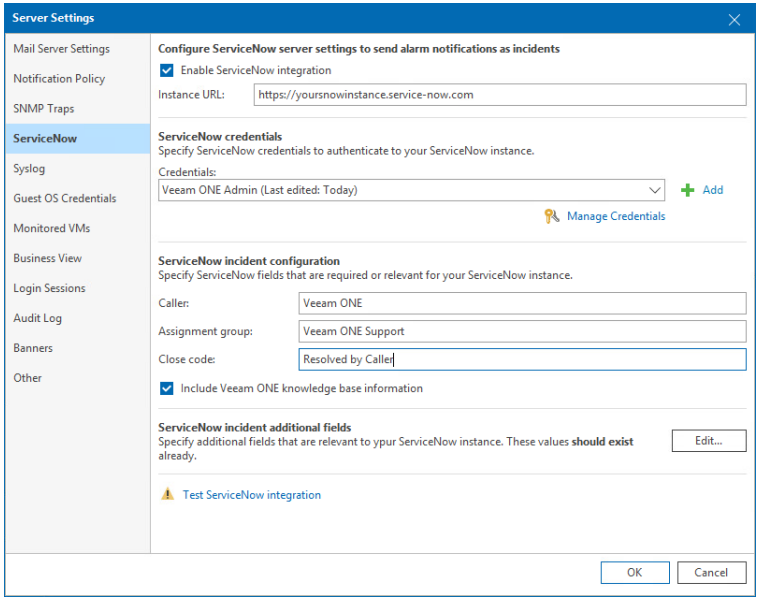
© 2023 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

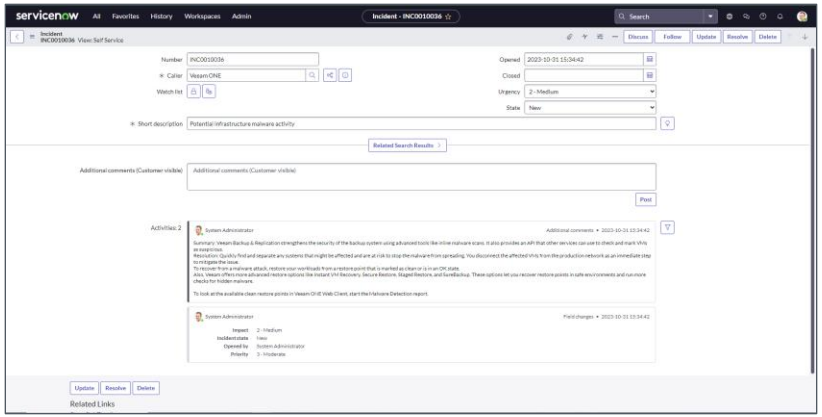
Integration with ServiceNow

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





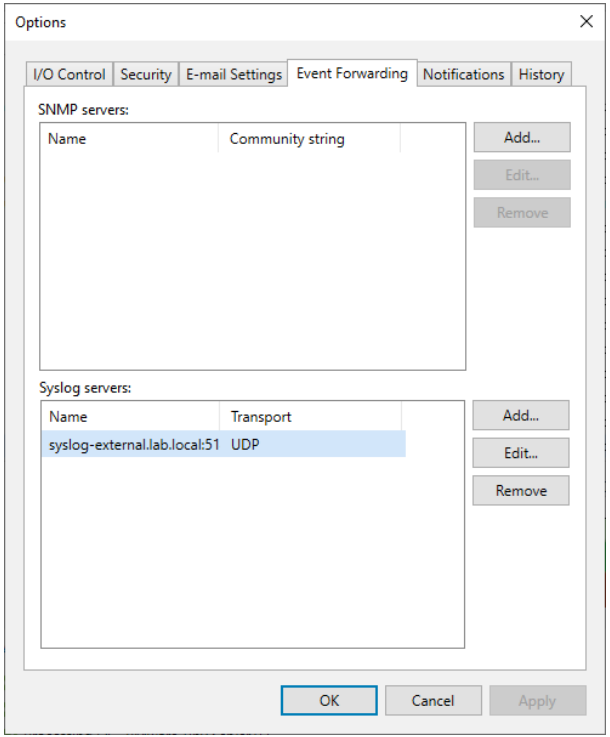
© 2023 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

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



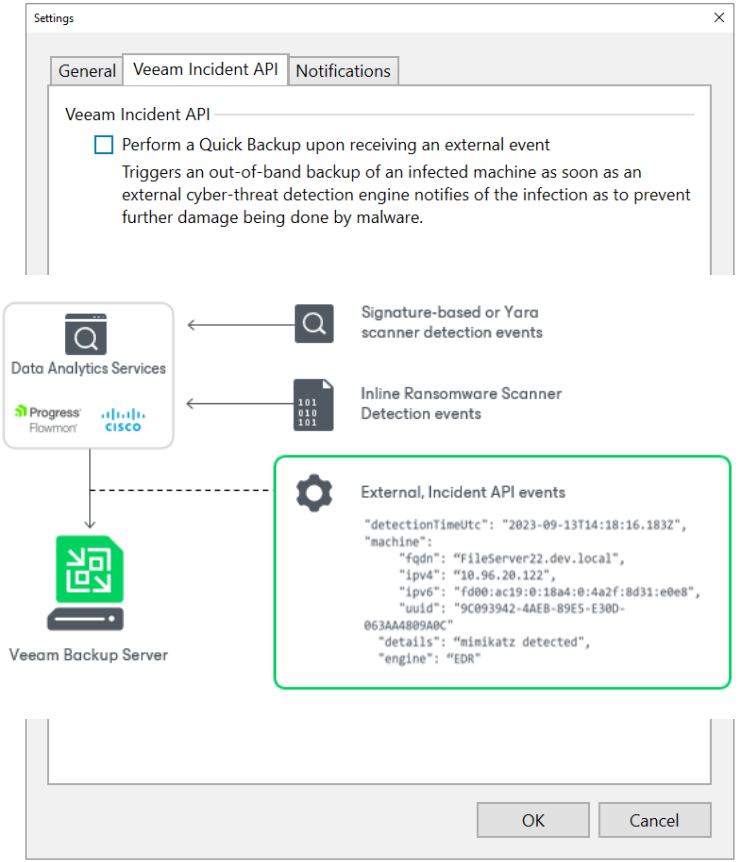
© 2023 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

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



© 2023 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

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

© 2023 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

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

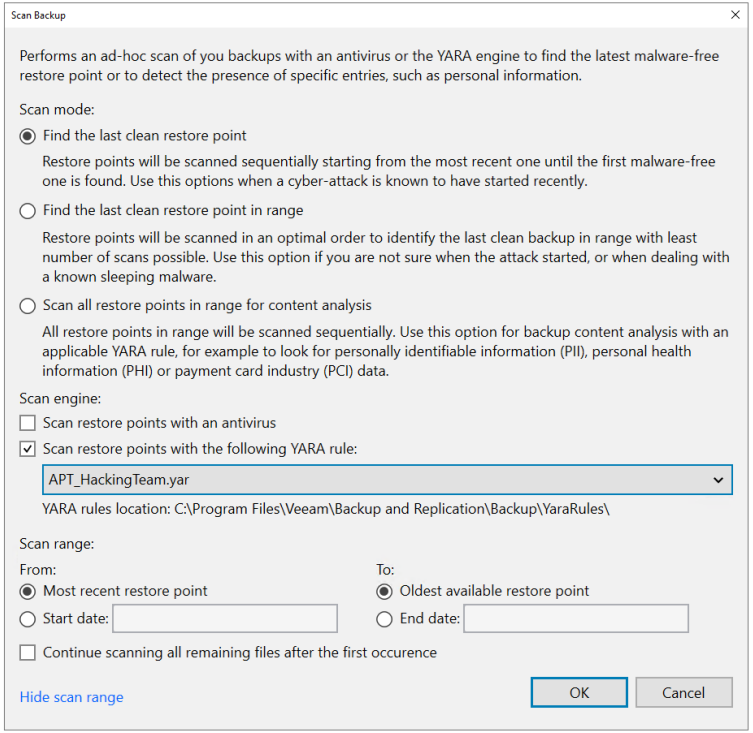
© 2023 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

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



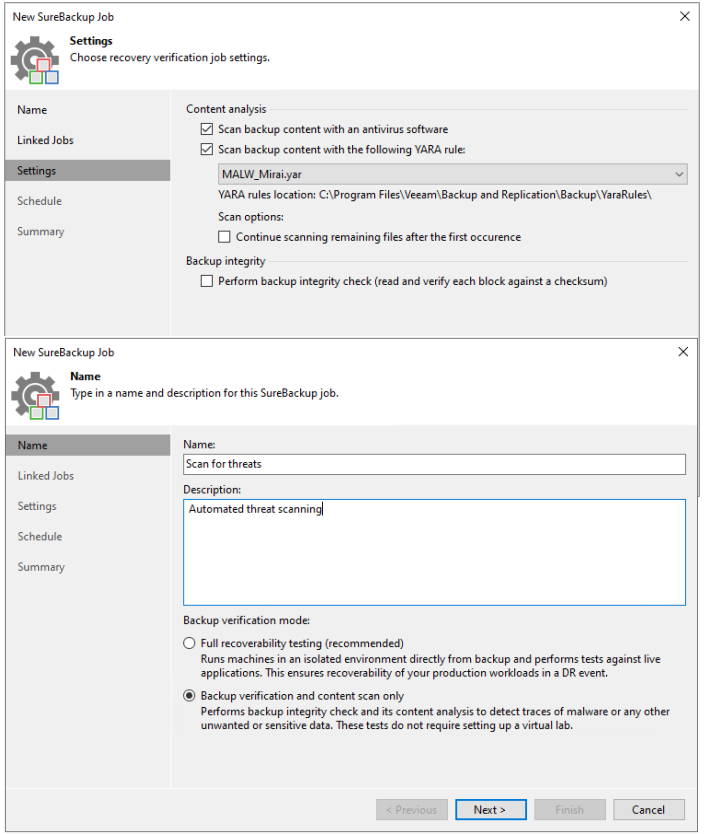
© 2023 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Avoid reinfection

Uncover threats before you restore

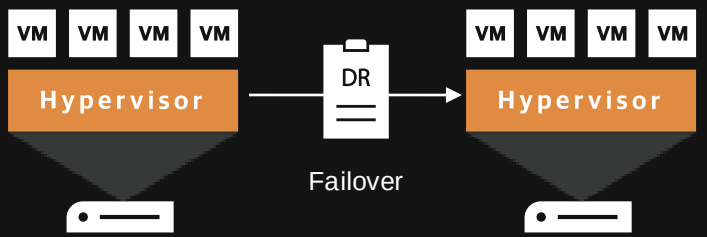
Automated offline malware detection

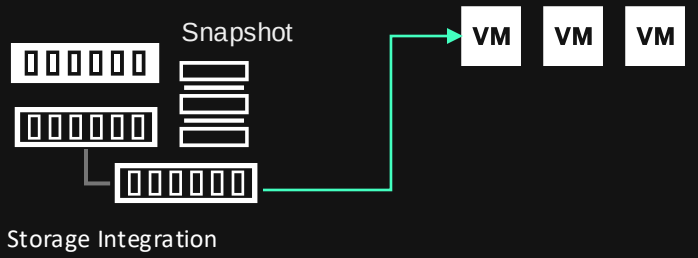
- Automated scheduled scans that support the *new* SureBackup® mode
- Orchestrated ad-hoc scans to assist with investigations
- Powered by **both** antivirus engines and/or YARA rules

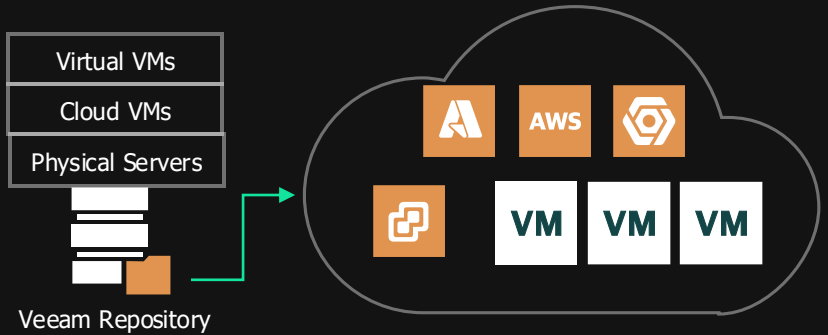


© 2023 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Fastest Recovery Options







© 2023 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

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

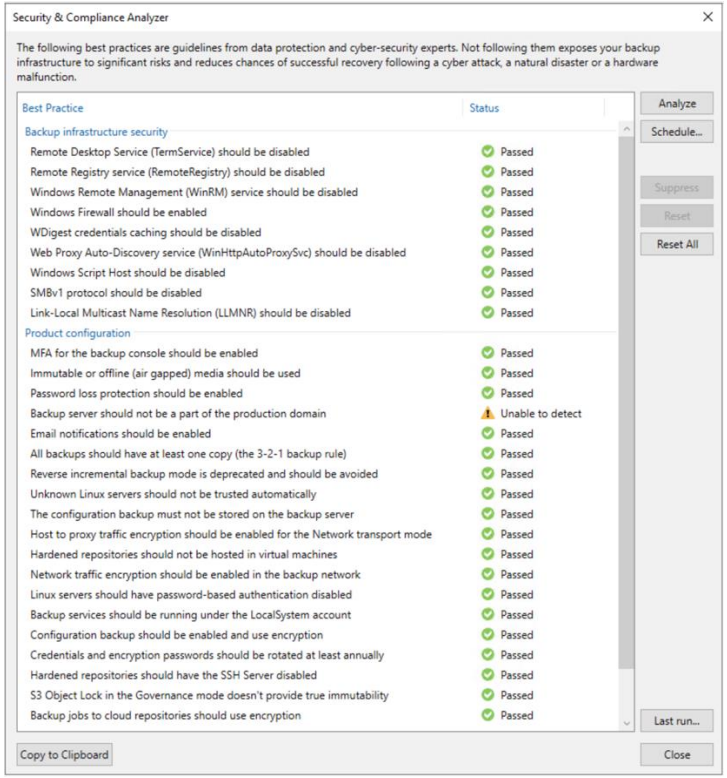
© 2023 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

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



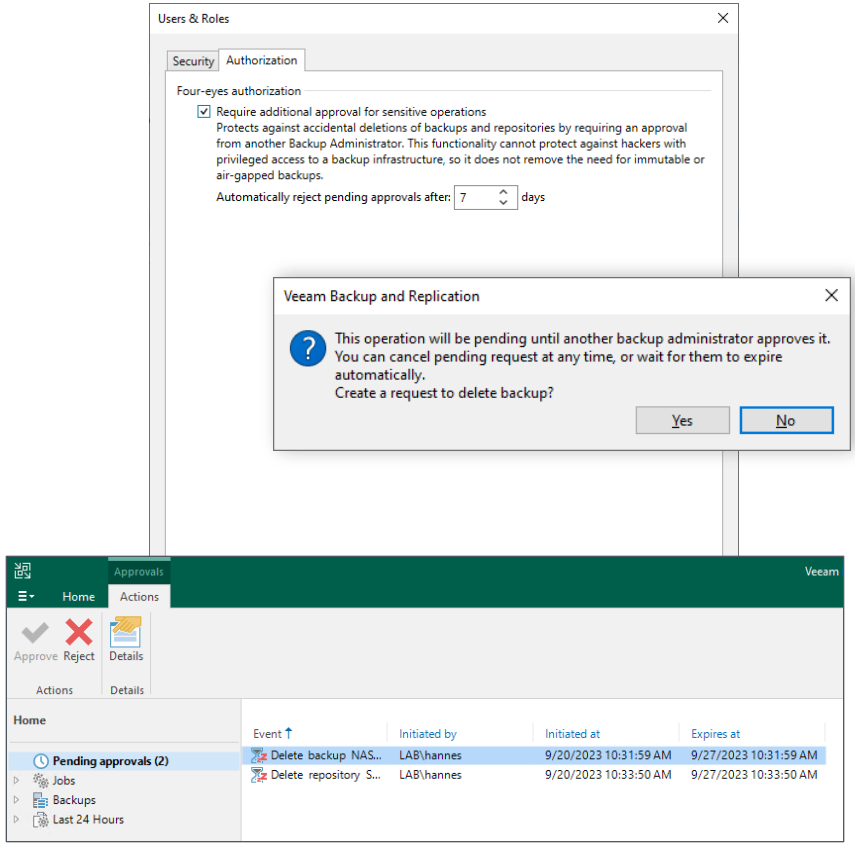
© 2023 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

“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



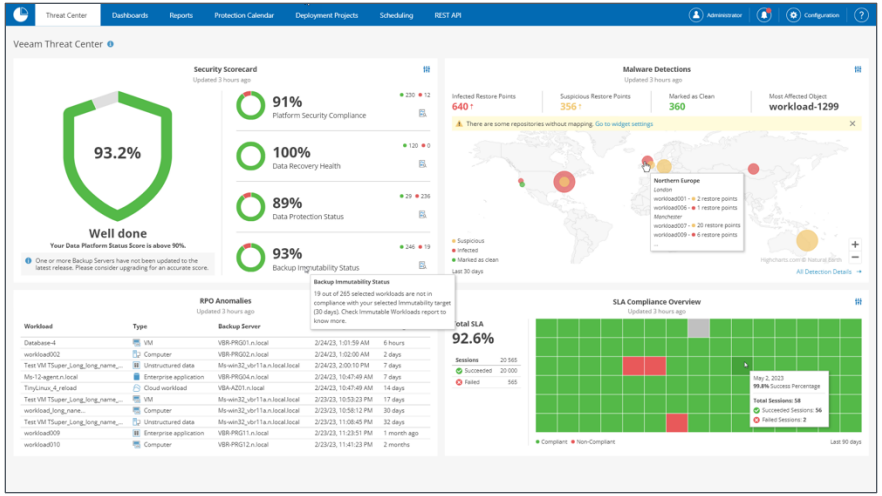
© 2023 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

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



© 2023 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Veeam keeps your business running.

© 2023 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.