Technical Validation

Cybersecurity with Veritas

Veritas Ransomware Protection

By Craig Ledo, IT Validation Analyst

September 2022

Introduction

This ESG Technical Validation documents the detailed evaluation of the Veritas solution for cybersecurity, including protecting data, detecting threats, and recovering at scale. Specifically, this evaluation involved validating 12 test scenarios across the Veritas cybersecurity solution portfolio.

Background

Ransomware attacks continue to be top of mind for business and IT leaders, and for good reason. They compromise access to an organization's lifeblood—data. The ongoing ransomware attacks have resulted in tremendous costs for organizations, including downtime, productivity, device costs, network cost, lost opportunity, ransom paid, brand value, and so on. With millions of dollars spent annually to guard entry points to data, many organizations still underestimate the strategic value of augmenting data protection. ESG research shows that 36% of survey respondents said their organization experienced such probing attacks on at least a monthly basis over the past 12 months, including 9% that were targeted daily and 12% that were attacked weekly (see Figure 1).[1]

Figure 1. Recurring Ransomware Attacks Are Common

Source: ESG, a division of TechTarget, Inc.

Another 27% of respondents experienced ransomware attacks more sporadically. Therefore, it's critical for organizations to implement strong proactive and defensive measures against ransomware attacks to prevent their success, especially since victims can and will be revisited by these criminals.

In addition, with demands becoming excessive and the risk of data loss increasing, an advanced multi-layered resiliency strategy is needed to help ensure that IT services are secure, resilient, and recoverable while providing the smooth experience that end-users expect. For example, solutions that have been hardened from a software and hardware perspective and that support immutable (can't be changed) and indelible (can't be deleted) storage help provide a comprehensive, multi-layered cybersecurity strategy.

[1] Source: ESG Research Report, *2022 Technology Spending Intentions Survey*, November 2021.

Veritas Cybersecurity Solution Overview

Veritas provides a unified, multi-layered, platform approach that seamlessly integrates proactive protection, detection, and backup and recovery. Specifically, Veritas provides organizations with a zero trust security model, which allows organizations to implement better access control, contain breaches, protect assets, and mitigate the potential for damage.

Protect:

- Ensures critical data and the IT infrastructure is protected from the unknown and unexpected by making sure all parts of the environment are backed up with universal protection that is applied intelligently and managed automatically to scale properly.
- Backup infrastructure and backed-up data enable organizations to elevate backup and recovery infrastructure to an essential component of resiliency success.
- Veritas NetBackup offers support from edge to core to cloud, with 800+ data sources, 1,400+ storage providers, and 60+ cloud providers, so that the most demanding and broad-ranging environments can be protected.
- Veritas Intelligent Policies bring increased levels of automation that provide greater levels of efficiency to administrators.
- Veritas provides an air gap solution to safeguard data integrity to help ensure backup files remain safe and untouched from malicious invaders.
- Backup images are immutable and indelible with an internally managed secure compliance clock.

Detect:

- Veritas offers solutions that provide full infrastructure awareness, shining a light on all the dark data in an organization's environment.
- In addition, Veritas ensures that an organization knows everything in the environment is safe, secure, and capable of overcoming the threat of ransomware.
- Veritas also offers AI-powered anomaly and malware detection on primary and backup data, and event-triggered malware scanning that provides an increased chance to act before cybercriminals or malicious code has the opportunity to do so.

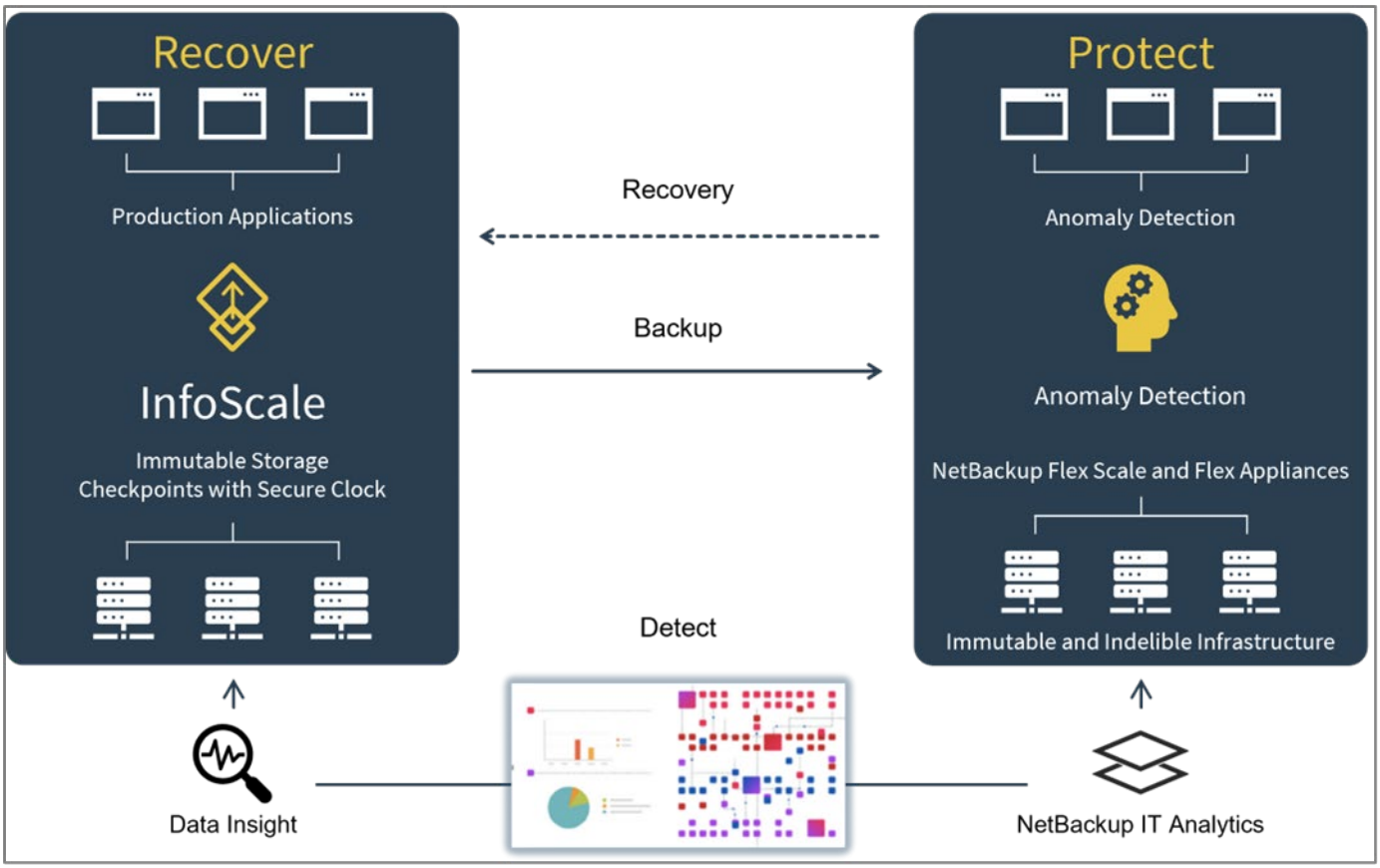
Recover:

- With Veritas solutions as an essential component in resiliency success, environments are optimized for recovery.
- Veritas has built-in security solutions to ensure that clean and ransomware-free data and environments are brought back online.
- Sometimes everything is impacted, so organizations may need to recover an entire data center in the cloud and on demand.
- On the other hand, maybe just a portion of the environment is impacted, so having solutions in place that provide the flexibility to quickly recover individual databases and files to production can be crucial.

- In the case where entire servers become encrypted, organizations may need to quickly recover those servers elsewhere.
- Organizations may just need to recover a large number of application instances back to production.
- Veritas provides solutions to recover at scale, including orchestrated recovery and bulk recovery.

Veritas solutions ensure data is always available and protected, help with application high availability, and provide recovery at scale. Veritas approaches ransomware resiliency through a business value lens, providing a robust resiliency strategy by solving for the protection, detection, and recovery from ransomware (see Figure 2).

Figure 2. Veritas Cyber Resilience Solution Overview



Source: ESG, a division of TechTarget, Inc.

ESG Technical Validation

ESG performed a technical validation of the Veritas cybersecurity solution, including protecting data, detecting threats, and recovering at scale.

Protecting Data

Veritas offers a wide range of security controls to help with data protection including:

- Identity and Access Management: role-based access, single sign-on, and customizable authentication.
- Data Encryption: in-transit and at-rest.
- Immutable Image Management and Storage: flexible, storage-agnostic image management and images stored in WORM (write once, read many) storage.
- Solution Hardening: NetBackup Flex and NetBackup Flex Scale have been hardened from a software and hardware perspective to offer a complete secure solution that supports immutable storage.

Specifically, ESG validated the following key data protection capabilities.

Cloud Data Immutability

The solution ensures data cannot be changed for a determined length of time to protect data against cybercriminal intrusion and internal threats. To further improve security, the backup storage is on a secure data store that is only visible and accessible to the NetBackup storage service, eliminating users and filesystem services from accessing it.

Hardened Impenetrability

The full NetBackup Appliances stack has been hardened for security, including the Linux operating system, management access, application binaries, and configuration settings. It includes proprietary security policies that conform with STIG guidelines and enforce mandatory access control. It also includes intrusion detection and protection services that restrict access to processes and resources and maintain an audit trail of important user and system actions.

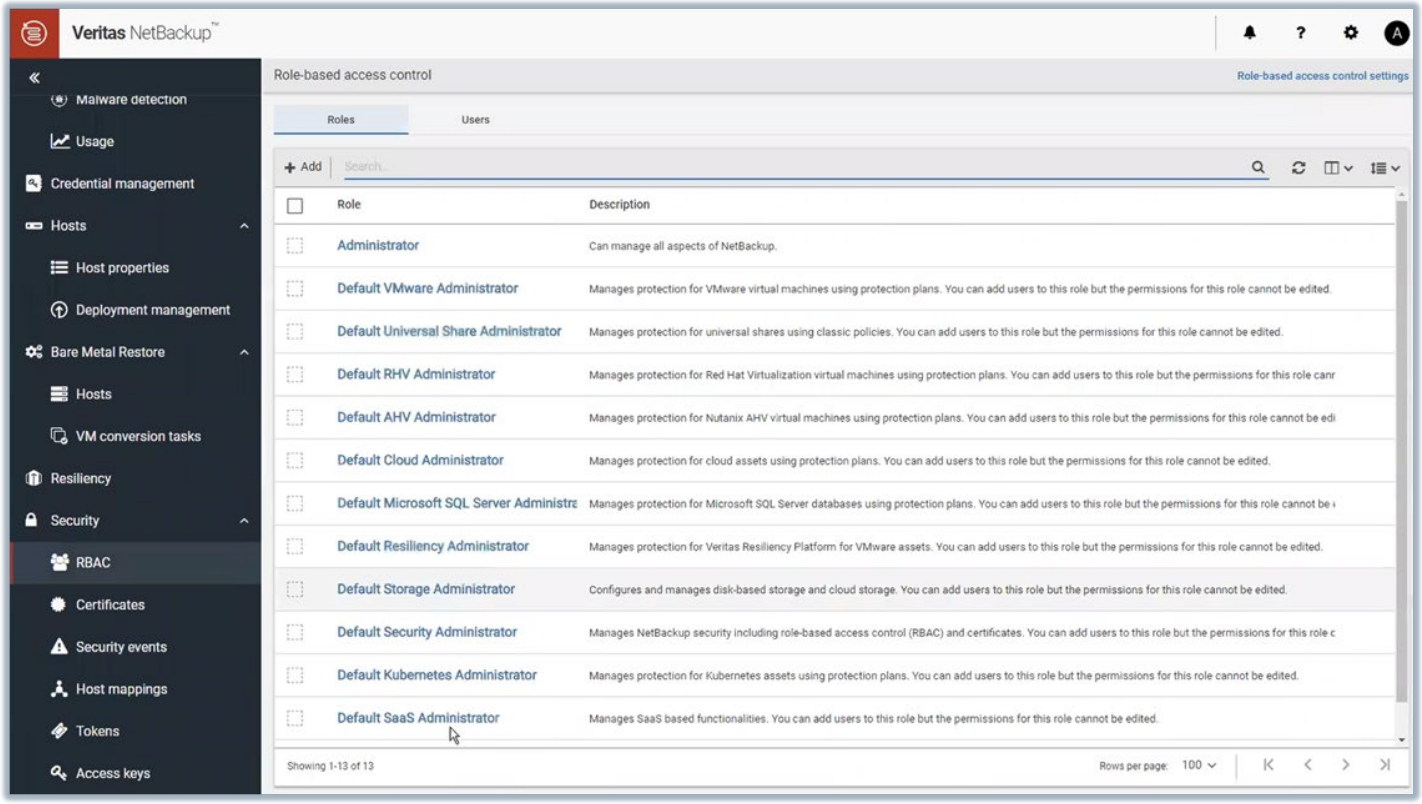
Tamper-resistant Hardware

Appliances hosting immutable storage can move into a heightened level of security to protect both data and infrastructure. Administrators are prevented from making changes to the OS and internal components, all endpoints are secured from unauthorized access, and access to all services is protected and authenticated.

Secured Access Controls

The solution provides role-based access control (RBAC) templates, as shown in Figure 3. This makes it is easy for administrators to provide appropriate access or permissions to users or groups of users. Admins can also drill into each of the templates to see the detailed permissions (e.g., NetBackup Management, Protection, Security, and Storage). Admins can also create custom user or group access or permissions. Based on the custom role, admins can also assign Workloads (i.e., select the workload assets that users can manage), Protection Plans (i.e., select the protection plans that users can manage), and Credentials (i.e., select the credentials that users can manage).

Figure 3. Secured Access Controls

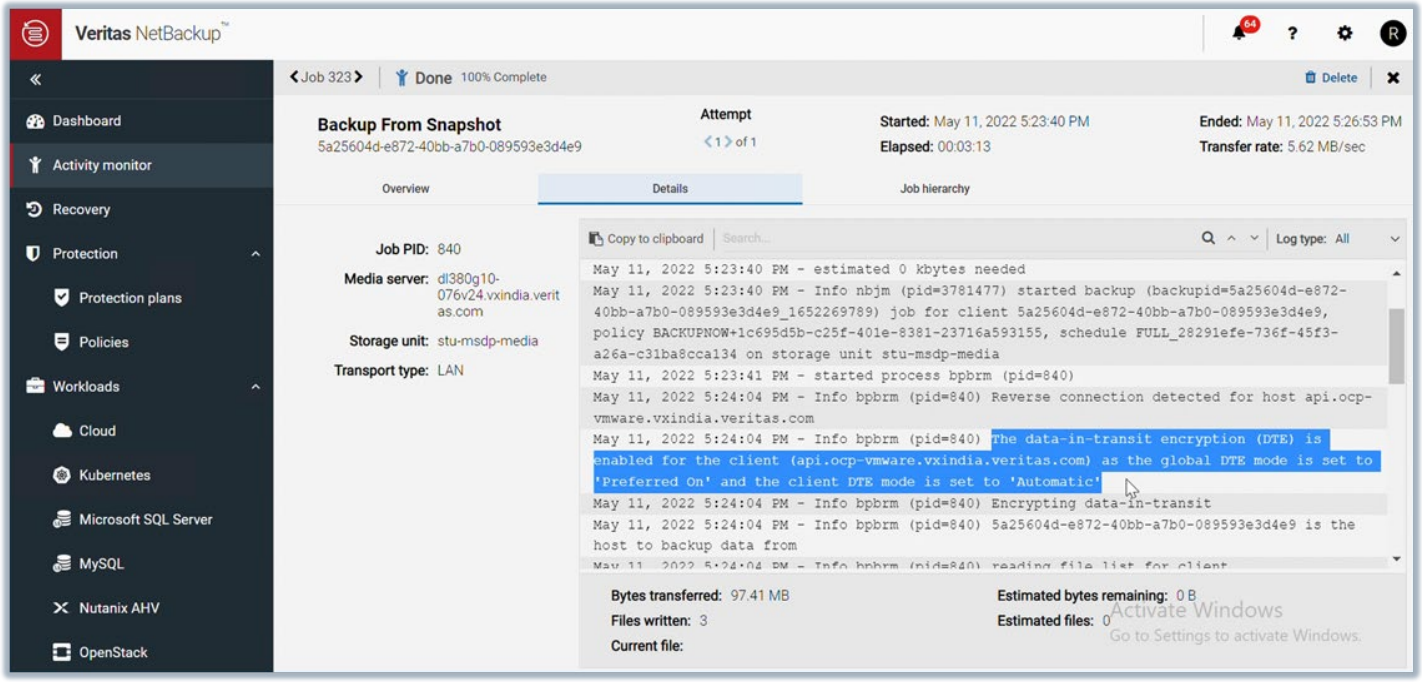


Source: ESG, a division of TechTarget, Inc.

Protection for Modern Infrastructures

The solution provides next-generation data protection technologies for modern infrastructures, including big data, hyperconverged, or open source MySQL/NoSQL databases. NetBackup enables organizations to protect multi-cloud, virtual, physical, and modern workloads, no matter where they reside, all from one console. Figure 4 shows a backup from a snapshot. The backup had data-in-transit encryption (DTE) enabled for the client as the global DTE mode is set to "Preferred On" and the client DTE mode is set to "Automatic." Users can restore, if needed, from this backup, which has DTE enabled, as the DTE mode of the backup image is set to "On."

Figure 4. Protection for Modern Infrastructures



Source: ESG, a division of TechTarget, Inc.

Why This Matters

As ransomware attacks evolve and become more sophisticated, it is important for enterprises to easily adapt to rapidly changing threat vectors to avoid service downtime and data loss. Veritas advanced data protection and secure appliances provide several features to combat ransomware, such as integrated anomaly detection, malware scanning, a zero trust architecture, and immutable and indelible storage.

Detecting Threats

Veritas offers a wide range of security controls to help with detecting threats, including:

- Backup and Storage Infrastructure Awareness: NetBackup IT Analytics provides end-to-end backup monitoring that includes mitigation analysis, sources with consecutive failures, sources with no recent backup, and backup failures by application.
- Anomaly Detection: NetBackup provides AI-powered anomaly detection that detects unusual data across the entire environment and provides alerts to suspicious anomalies in near-real-time.
- Primary Storage Detection: Veritas addresses secondary backup data with NetBackup and primary storage data with Veritas Data Insight, which supplements existing security detection tools by providing anomalous behavior detection in user and data context in near real-time, custom ransomware-specific query templates, and file extension identification useful for detecting ransomware.

- Malware Detection: Veritas provides both automated and on-demand scans for protected backups. The automated malware scanning feature removes human dependencies and allows artificial intelligence/machine learning (AI/ML) technology to jump in and scan for malware.

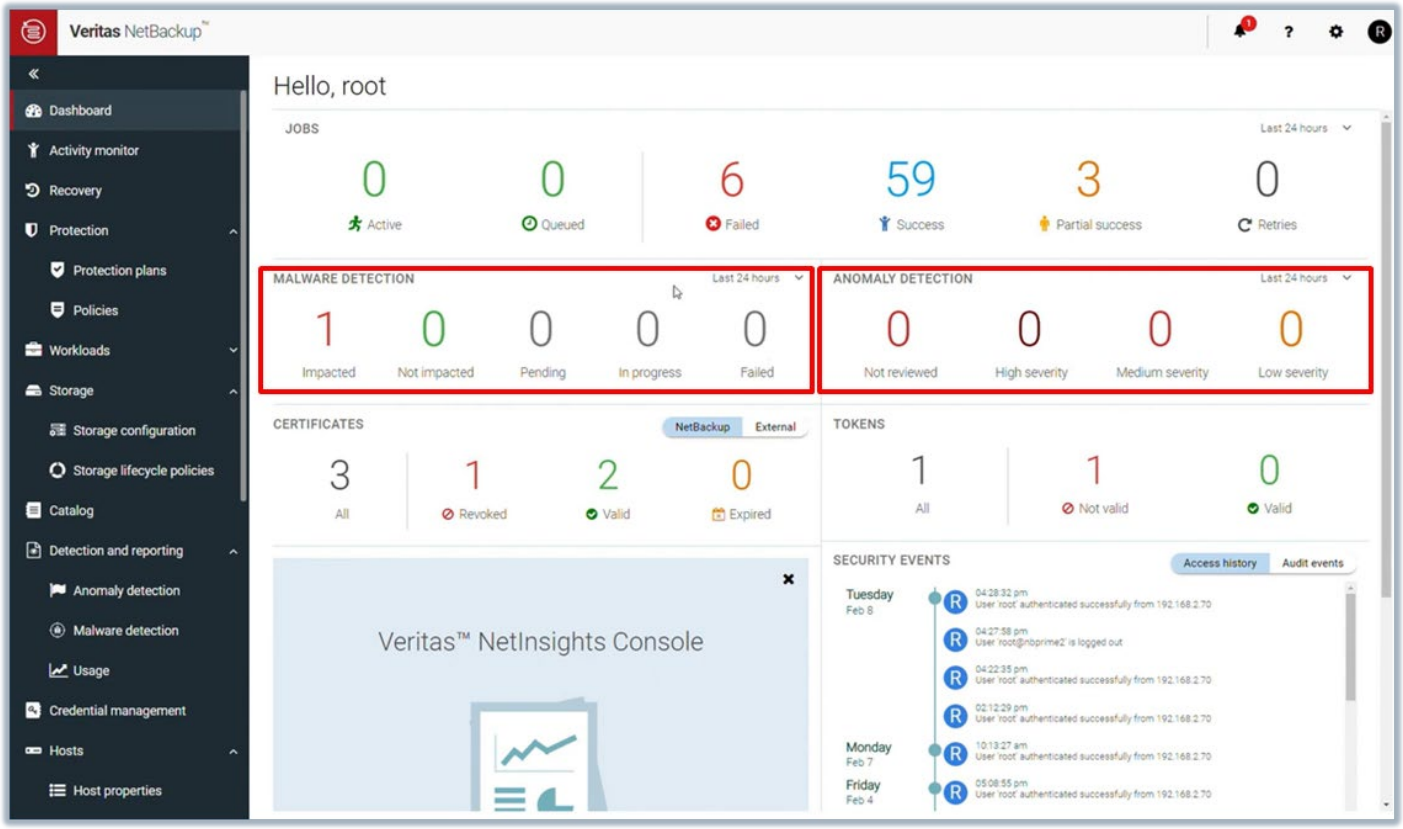
Specifically, ESG validated the following key threat detection capabilities.

Integrated Malware Scanning and Anomaly Detection

Anomaly detection tracks image metadata separately from malware detection, but malware detection can leverage anomaly detection scores. Malware detection events are sorted into Impacted, Not Impacted, Pending, In Progress, and Failed, according to the "last 24 hours," as shown in Figure 5. The timeframe is also configurable to the "last 48 hours" or the "last 72 hours." Users can drill into each area (e.g., Impacted) to view more details. For each impacted backup image, users can take action, including expiring all copies or viewing infected files. The malware detection dashboard provides the following information: Client, Backup Time, Scan Result, Backup Type, Date of Scan, Malware Application Scanner, Number of Files Impacted, Scan Host Name, and Backup ID. Malware scanning time will vary depending on several factors, including the size of the image and the number of files.

Anomaly detection events are sorted into Not Reviewed, High Severity, Medium Severity, and Low Severity, according to the "last 24 hours," as shown in Figure 5. The timeframe is also configurable to the "last 48 hours," the "last 72 hours," or "the last 7 days." Users can also filter on the Review Status (Not Reviewed, False Positive, Anomaly, Ignore) and the Anomaly Severity (High, Medium, Low). The anomaly detection dashboard provides the following information: Job ID, Client Name, Policy Type, Count, Score, Anomaly Severity, Anomaly Summary, Received, Review Status, Policy Name, Schedule Name, and Schedule Type. Users can take the following actions regarding anomalies: Mark as Ignore, Confirm as Anomaly, and Report as False Positive.

Figure 5. Integrated Malware Scanning and Anomaly Detection



Source: ESG, a division of TechTarget, Inc.

Reporting and Alerting

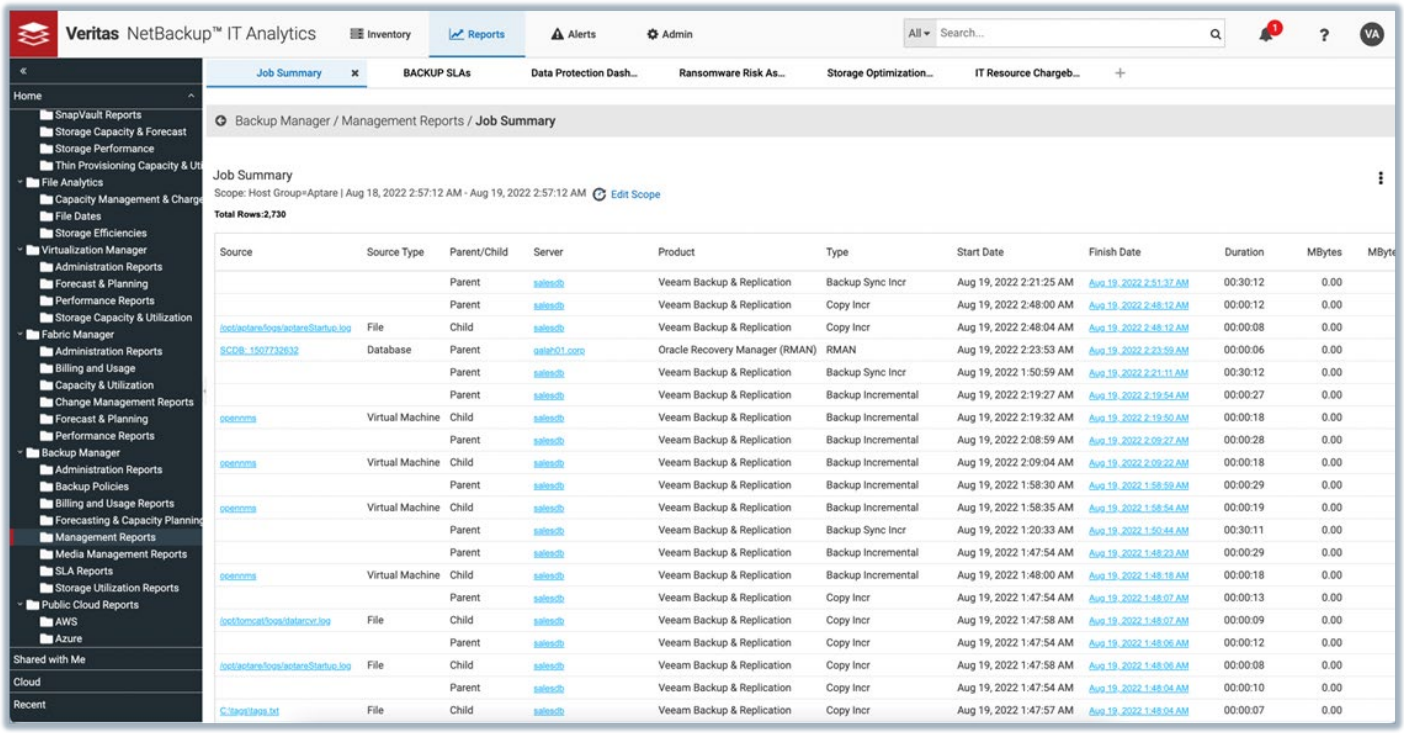
Veritas NetBackup IT Analytics provides a ransomware risk assessment dashboard out of the box. The dashboard gives users a quick view of the pre-identified reports that use predictive analytics to understand potential risks within a backup environment (see Figure 6). The analytics help users ensure that the backup environment is both optimized and secure by providing comprehensive reporting on several data points including:

- Discovery – Users can track all changes within the backup environment to help detect ransomware and quickly respond, including support for over 850 known ransomware extensions.
- Visualizing risks – Intuitive graphs give users a historical view of all the risks generated within the environment, flag hosts that are missing from the backup schedule, and visualize applications with failed backups.
- Backup monitoring – Users can monitor and identify changes within the backup environment with summary graphs that provide actionable insights. Users can also mitigate risk by identifying anomalies using a baseline of known successful backups.

In addition to detecting files with known ransomware extensions, NetBackup IT Analytics allows users to organize this information in a meaningful way so users can execute on a quick plan of action. Users can organize the ransomware files detected by hosts, locations with the most ransomware files, types of ransomware extensions, and owners of files.

NetBackup IT Analytics also probes successful backups to identify potential false positives by comparing historical backups against the new backup and identifying anomalies, such as significant changes in job durations, image size variations, and/or policy configuration changes. This gives users the assurance that critical IT services are being protected.

Figure 6. Reporting and Alerting



Source: ESG, a division of TechTarget, Inc.

Why This Matters

As stated earlier, ransomware attacks have evolved and become more sophisticated, so Veritas provides holistic real-time visibility into the status of applications and data with anomaly detection and tailored insights that help identify malware infiltration in both primary and backup data.

Recovering at Scale

Veritas offers a wide range of capabilities to help recover at scale, including:

- NetBackup Resiliency: NetBackup Resiliency provides automated orchestration across an organization's entire heterogeneous environment with a consistent user experience and visibility into the best recovery options based on the options available.
- NetBackup Instant Rollback for VMware: Provides high-speed VM recovery by using Reverse Change Block Tracking to identify which unique blocks need to be recovered and applying just those changes to bring VMs back to a healthy state in seconds.

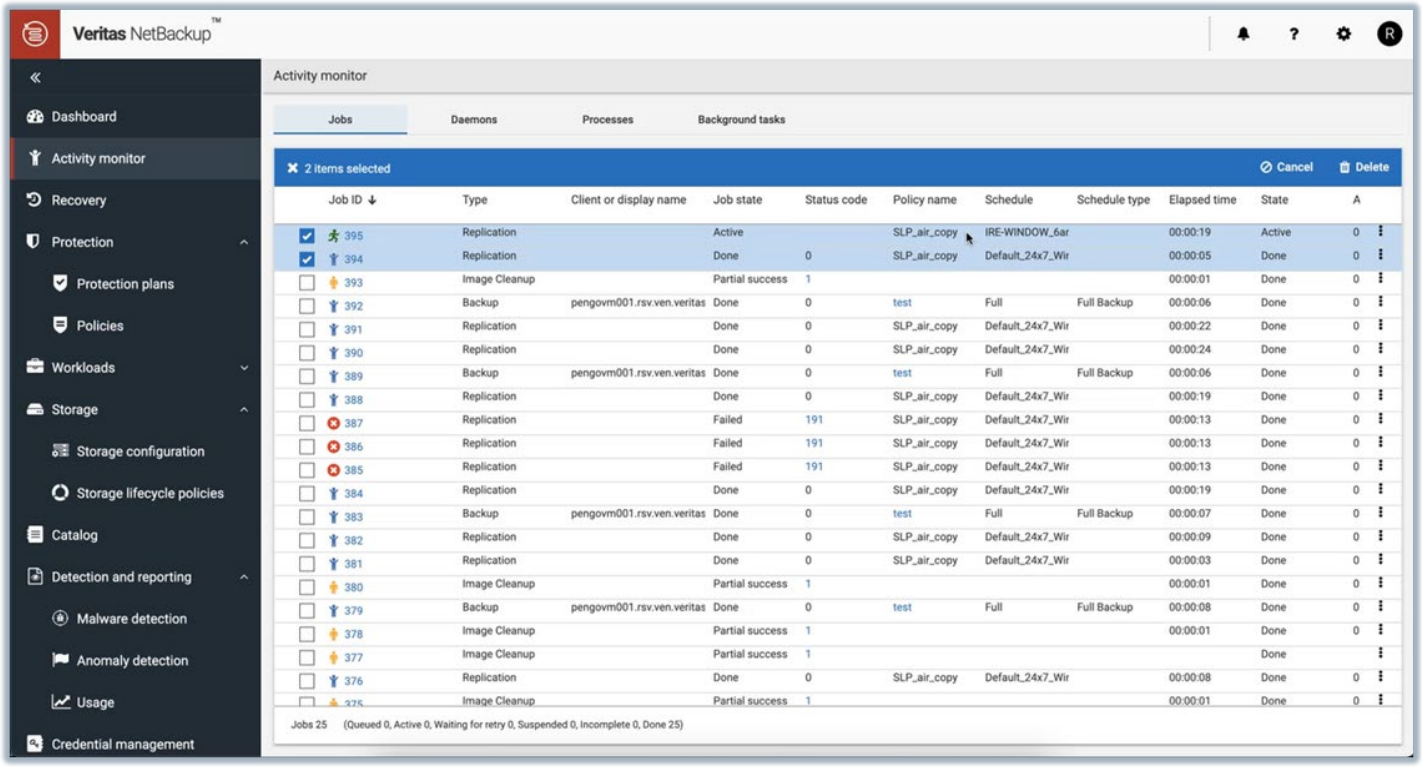
- VM Recovery: Provides eight types of recovery for one backup of VMware VMs, including full VM, individual VMDK, file and folder, full application, Instant Access, file download, application GRT, and AMI conversion.
- Instant Access for MSSQL and VMware: Provides almost instant machine recovery (e.g., 1,600 VMs) without waiting to transfer the VM's data from the backup. Also provides the ability to test or recover VMs directly from backup storage.
- NetBackup CloudPoint: NetBackup CloudPoint uses cloud-native snapshot technology in a cloud vendor–agnostic way that allows easy protection of hybrid and multi-cloud infrastructures.
- Universal Share and Protection Points: Allows organizations to provision deduplication-backed storage on the NetBackup server as secure shares, thereby protecting databases or other workloads where no agent or backup API exists.
- NetBackup Universal Shares for Oracle: Allows Oracle database admins to start up databases directly from a NetBackup Appliance's storage.
- Long-term Retention Archive: Provides a cost-effective and durable solution that features deduplication and compression of data, including the use of object storage and private or public clouds with this method. Traditional Recovery includes granular restore of a specific file, full server/application restore, and disaster recovery (DR) restore to a different site location or the cloud. Using Veritas Resiliency Platform, organizations can automate and orchestrate traditional recovery with the push of a button, streamlining the DR process.
- Bare Metal Restore: Automates the server recovery process, making it unnecessary to reinstall operating systems or configure hardware manually. Allows organizations to rebuild systems quickly from scratch, restoring the OS and the application data with a single operation.

Specifically, ESG validated the following key recovery-at-scale capabilities.

Isolated Recovery Environment

The Veritas NetBackup Isolated Recovery Environment allows recovery plans for thousands of VMs that may be part of complex, multi-tier environments and the ability to run rehearsals of the same in an isolated environment (see Figure 7). This capability can provide support for built-in immutability and indelibility, third-party hardware immutability, cloud-based locked object storage immutability, and immutability for SaaS workload backups. Also, NetBackup can directly send and efficiently store deduplicated data on AWS S3 Object Lock.

Figure 7. Isolated Recovery Environment

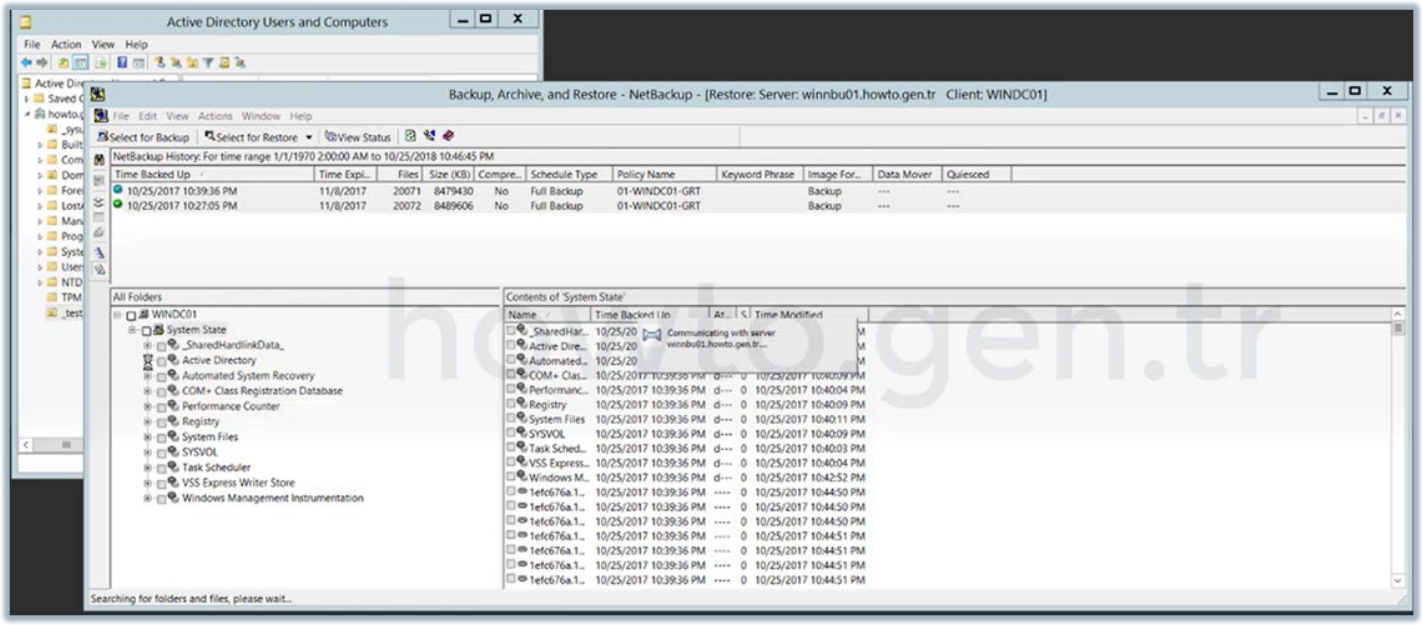


Source: ESG, a division of TechTarget, Inc.

Lost Active Directory Recovery

The Veritas NetBackup solution provides the capability to recover a lost Active Directory by browsing the Active Directory backups (see Figure 8). Then, the user simply initiates the proper Active Directory backup. The user can also view the progress of the restore until it shows that the requested operation was successfully completed.

Figure 8. Lost Active Directory Recovery

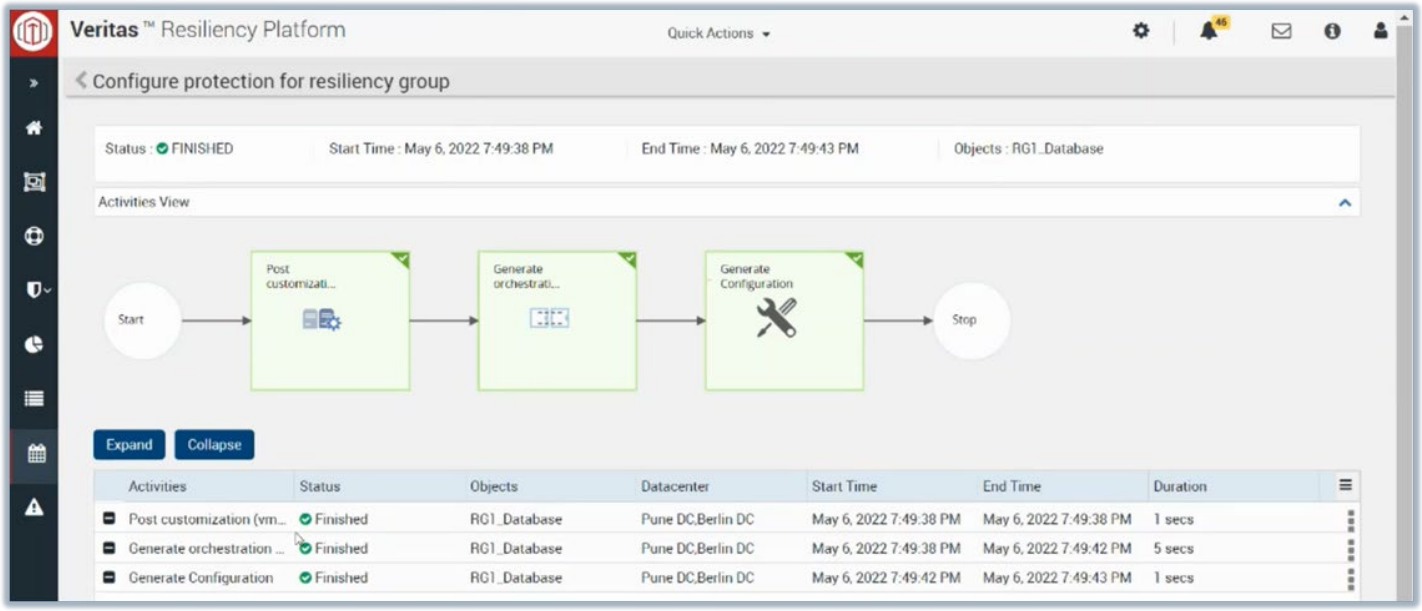


Source: ESG, a division of TechTarget, Inc.

Tiered Recovery Orchestration

Veritas NetBackup Resiliency's Virtual Business Services allow users to manage recovery for multi-tiered applications as a single consolidated entity. With Virtual Business Services, users can completely automate the recovery of a complex, multi-tier application that spans multiple systems. In the event of a ransomware attack, this provides easier, faster recovery and minimal application downtime. Specifically, the Veritas Resiliency Platform provides tiered recovery orchestration by, for example, configuring virtualization and private clouds (e.g., adding VMware vCenter), NetBackup Primary Servers, networks (e.g., Network Pairing), physical servers, databases, etc. See Figure 9 for the completed resiliency group protection configuration.

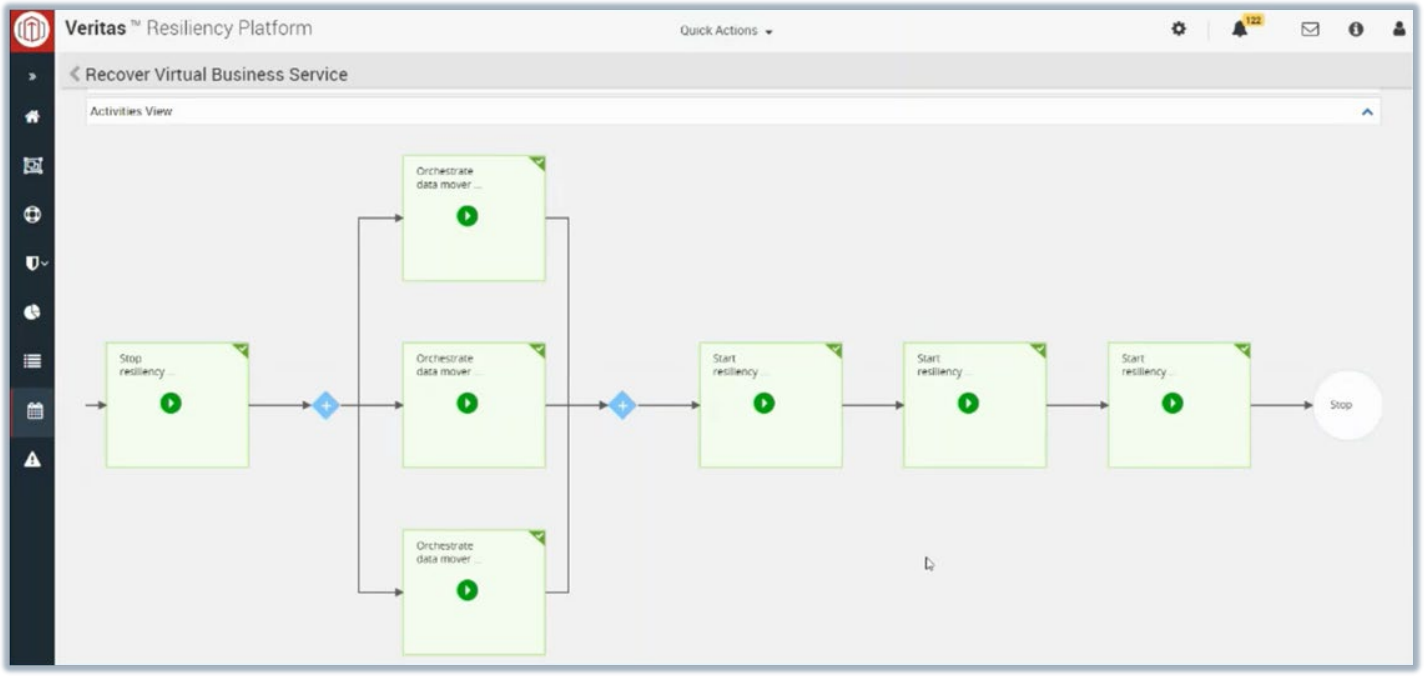
Figure 9. Tiered Recovery Configuration



Source: ESG, a division of TechTarget, Inc.

After the resiliency group protection configuration has been completed, the user needs to set up the tiered Virtual Business Service. Next, the user can orchestrate the tiered recovery of the Virtual Business Service (see Figure 10).

Figure 10. Tiered Recovery Orchestration



Source: ESG, a division of TechTarget, Inc.

Why This Matters

As ransomware attacks increase, it is important for enterprises to have a comprehensive ransomware resiliency and recovery strategy. Veritas provides advanced storage and fast recovery capabilities for primary data with integrated storage resiliency, immutability, and data isolation capabilities that ensure the availability of applications, as well as the security and integrity of data.

The Bigger Truth

Ransomware and malicious insiders pose serious threats. New operating system vulnerabilities are continually being discovered and variants of known malware and ransomware are regularly being developed. Ransomware is big business, which means bad actors are motivated to continue to innovate in new ways to penetrate an organization's infrastructure and halt its business.

ESG validated 12 test scenarios covering the Veritas solution for cybersecurity, including protecting data, detecting threats, and recovering at scale. A holistic, multi-layered, and comprehensive cybersecurity strategy is always the best defense against downtime and data loss due to malware infiltration. Veritas understands that this can be a complex challenge and has delivered an enterprise foundation to help organizations protect IT services as part of an overall cybersecurity strategy. The Veritas cybersecurity strategy provides organizations with the tools, functionality, and confidence that IT services will be highly available, resilient, and protected from ransomware.

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188

© 2022 TechTarget, Inc. All Rights Reserved.