VERITAS

Ransomware Resiliency with the Veritas Enterprise Data Services Platform

Veritas™ White Paper | November 2020

Contents

EXECUTIVE SUMMARY

Today, ransomware and ransomware attacks are a top concern for enterprises of all sizes and types. By 2021, a business will fall victim to a ransomware attack every 11 seconds, making ransomware the fastest-growing type of cybercrime. Attackers are continually evolving creative techniques to pass even the most vigilant frontline security. Old techniques like phishing are still prominent, but new, sophisticated methods involving social engineering, targeting IoT devices and infrastructure vulnerabilities are gaining popularity. Therefore, it's critical for IT teams to realize that true ransomware resiliency can't be achieved by endpoint security alone.

Many consider backup and recovery of your data to be the last line of defense against ransomware attacks. At Veritas, we recommend prioritizing it as a meaningful and reliable part of a comprehensive, multi-layered cybersecurity strategy. It's not just your data that goes down—it's your business.

Our Enterprise Data Services Platform solutions were developed with resiliency at top of mind, so we could provide our customers with dependable solutions to ensure their business was up and running with minimal impact. Our solutions **protect** IT systems and data integrity with a wide range of security controls to suit your needs. These tools monitor and **detect** threats with a complete view of your user activity and data infrastructure and provide backup monitoring capabilities to ensure your critical data is protected. Veritas and Veritas NetBackup™ software have been synonymous with resiliency for decades. Dependable Veritas solutions incorporate proven technology, so you can **recover** quickly with automation and orchestration at scale.

INTRODUCTION

This paper dives into the Veritas Enterprise Data Services Platform solutions, the industry's most comprehensive, compliant and secure ransomware resiliency platform. Our tools help to provide valuable peace of mind, reduce risk and ensure our customers can protect and recover their data from threats like ransomware today and into the future. This document is designed for business and technical audiences, including customers, partners and others who would like to learn more about NetBackup and other solutions in our Enterprise Data Services Platform to protect against and recover from malicious malware.

This white paper will help you:

- Learn how to **protect** your IT systems and maintain data integrity.
- Understand the Veritas solutions to help you **detect** abnormalities in your system by monitoring and mitigating threats.
- Determine which of our **recover** options best suits your needs, so you can apply the right recovery to your specific environment.

It's important to note that there's no one-size-fits-all solution and this paper is not intended to be all-encompassing. Veritas gives you the freedom to choose from a variety of solutions that best fit each application's specific recovery needs. You should implement a holistic and comprehensive strategy and add firewalls, email and spam filters, anti-malware and point protection software to your organization's defensive strategy. Enterprises must develop, rehearse and consistently evaluate their strategy to evolve with the sophistication of threats and their technologies. Let's dive into our recommended best practices for an organization's backup ecosystem.

Figure 1. Recommended best practices for an organization's backup ecosystem.

BEST PRACTICES

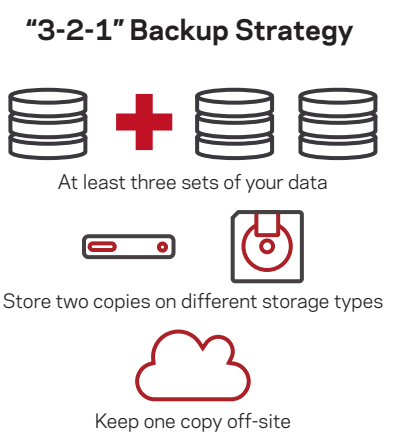
The National Institute of Standards and Technology (NIST) developed a recommended Cybersecurity Framework that helps organizations put a comprehensive, structured methodology around five key functions; identify, protect, detect, respond and recover. Veritas is aligned with this approach and recommends implementing our solutions within the broader NIST framework.

When it comes to an organization's backup ecosystem, Veritas recommends keeping in mind the key best practices shown in Figure 1.

- Version Management
  - Reduce vulnerability exposure by staying current with security patches and releases that contain security updates.
  - Monitor Veritas Technical Alerts by visiting the Veritas Support website or Veritas Services and Operations Readiness Tools (SORT)
- Identity and Access Management
  - Require users to log in with their own credentials.
  - Implement role-based access control (RBAC) and two-factor authentication to limit access to only required functionality for each persona and prevent account takeover from using a single credential.
  - Change built-in generic user IDs and passwords, including the host 'admin', 'maintenance', RMM 'sysadmin' and 'nbasecadmin' accounts.
- Immutable Storage
  - Prevent ransomware from encrypting or deleting backups using immutable and indelible storage technology.
- Data Encryption
  - Implement in-transit encryption to protect your data from being compromised within the network.
  - Implement at-rest encryption to prevent ransomware or bad actors from stealing your data and threatening to make it public or take other malicious actions.
- Configuration
  - Follow security implementation guides.
  - Harden your environment by restricting ports and processes by enabling firewalls.
  - Update the default Master Catalog backup policy.
  - Set up a backup policy for the NetBackup Key Management Server (KMS).

- Deployment
  - Adopt the "3-2-1" best practice approach of backing up data recommended by the U.S. Cybersecurity and Infrastructure Security Agency: keep three copies of data on two different media types, with one off-site.
  - Use Auto Image Replication (AIR) technology to replicate to other domains.

Once you have your strategy in place, it's vital to periodically test and rehearse. Not only will this practice help shorten threat response times and minimize the impact of an attack, the enhanced visibility will help you identify problems areas to resolve and improve. Your resiliency plan is only as good as your last test, so rehearsing and constantly revising your resiliency strategy is advantageous.



PROTECT, DETECT, RECOVER

Veritas empowers our customers to protect, detect and recover from attacks with a broad range of product features and functionality you can customize to meet your unique needs and requirements. Let's look at the details that comprise the three strategic pillars of the Veritas ransomware resiliency strategy.

PROTECT

The first line of defense is to ensure your critical and most important asset—data—and your IT infrastructure is protected from the unknown and unexpected. Your backup infrastructure and backed-up data are the last line of defense to recover from an attack. Backups are an organization's key to recovery. NetBackup offers the widest support from edge to core to cloud with 800+ data sources, over 1,400 storage targets and 60+ cloud providers, which means your environment is always protected and always recoverable.

In addition, Intelligent Policies can automatically detect and back up Oracle and VMware instances to ensure the necessary level of protection is applied.

Veritas focuses on data integrity to help ensure backup files remain safe and untouched from malicious invaders. We know how vital it is for our customers to protect their data, which is why we've placed NetBackup and key functionality around data integrity at the heart of our Enterprise Data Services Platform.

To maintain data integrity, we offer a wide range of security controls to help with data protection.

- Identity and Access Management (IAM)
  - Role-based access—Granular access controls you can tailor to meet specific persona needs, specifying who can access data and defining what actions they can or cannot perform (see Figure 2).
  - Single sign-on—Support for Active Directory and LDAP as well as SAML 2.0. Organizations can use their authentication provider to achieve two-factor authentication.
  - Customizable authentication—Veritas Flex Appliances support configurable authentication strength.

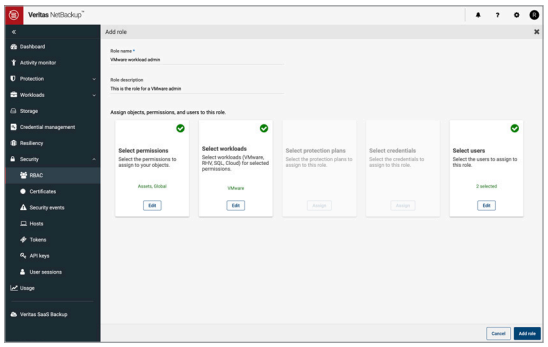


Figure 2. The access permissions dashboard in NetBackup.

- Data Encryption
  - In-transit—Ensure your data is being sent to authenticated environments and is protected while in transit. This solution leverages Veritas or customer-provided TLS 1.2 certificates, with 2048-bit key support to ensure data encryption during transit.
  - At-rest—If hackers are successful in getting to the data, having it encrypted protects it from being exploited. Veritas offers AES 256-bit, FIPS 140-2 cryptography with our own key management while allowing customers to leverage their preferred key management using the Key Management Interoperability Protocol (KMIP).

- Immutable/Indelible Image Management and Storage
  - Image Management Agnostic to Storage
    - NetBackup includes the OpenStorage Technology (OST) API, so you can manage immutable backup images with Veritas or third-party storage solutions.
    - Supports primary, secondary (duplication) and cross-domain replication (with AIR), giving you unlimited configuration options across any backup storage tier.
  - Image Storage
    - The NetBackup Flex Operating Environment provides immutable and indelible storage that reduces the risk of malware or ransomware encrypting or deleting backup data, thereby making it unusable.
    - Within NetBackup Flex, there is a WORM storage server that offers a secure, container-based MSDP solution.
    - NetBackup Flex offers Enterprise and Compliance lock-down modes, so you can choose the right immutability strength (see Figure 3).
    - NetBackup Flex has completed a third-party Immutability Assessment from Cohasset Associates, an industry-recognized assessor of immutability controls, specifically SEC Rule 17a-4(f), FINRA Rule 4511(c) and the principles of Commodity Futures Trading Commission (CFTC) in regulation 17 CFR § 1.31(c)-(d).
    - To read the Cohasset Associates' assessment of NetBackup, visit Veritas.com

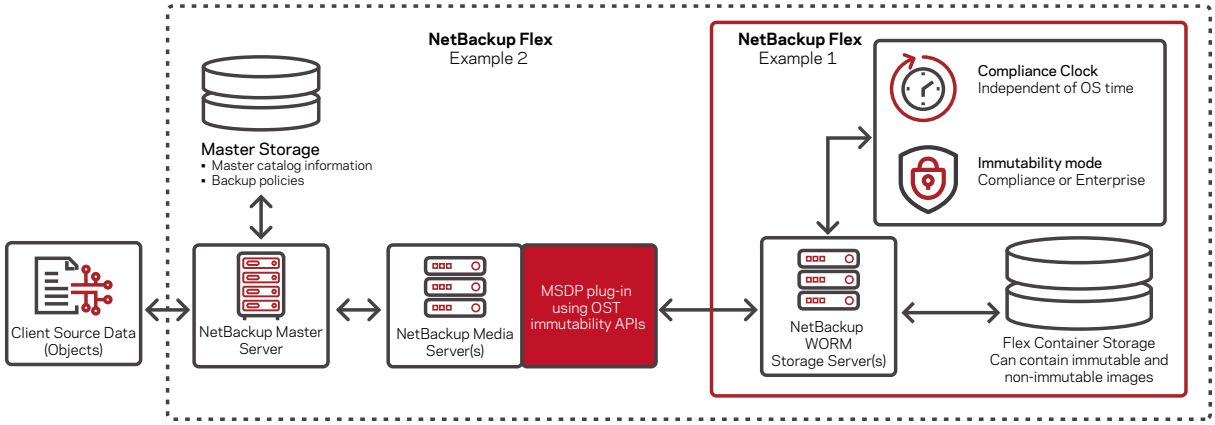


Figure 3. Two of the many NetBackup Flex deployment examples.

- Solution Hardening

  NetBackup Flex has been hardened from a software and hardware perspective to offer a complete secure solution that supports immutable and indelible storage. The solution offers a secure WORM storage sever and hardware security features.
  - Throughout the development cycle, Veritas analyzes NetBackup Flex code for vulnerabilities using recognized third-party detection tools that perform:
    - Static code analysis.
    - Runtime vulnerability checks.
    - Penetration testing.
  - NetBackup Flex comes with a wide variety of security features that includes:
    - OS security hardening, including Security-Enhanced Linux (SELinux).
    - Intrusion Detection System (IDS) / Intrusion Protection System (IPS).
    - Robust role-based authentication.
    - Locked down storage array.
    - A secure, robust and hardened Veritas File System.
  - For details, refer to the Veritas Flex Appliances with NetBackup Security white paper to support secure deployment as well as the Veritas Flex Appliances with NetBackup white paper.

DETECT

Many organizations likely maintain an increasingly complex IT environment they must manage within the constraints of reduced resources. Organizations want assurance their environment is safe, secure and capable of overcoming the threat of ransomware while reducing the day-to-day complexity of monitoring and maintaining backup and storage configurations. Veritas offers solutions that provide backup infrastructure awareness and malware and anomaly detection.

Backup and Storage Infrastructure Awareness

Ensure you're backing up all your critical data with APTARE™ IT Analytics. Empower your organization with APTARE to:

- Discover all hosts or VMs in your infrastructure and compare them with the VMs protected by NetBackup.
- Flag hosts that are missing from the backups as potential risks.

APTARE provides end-to-end backup monitoring that includes:

- Risk Mitigation Analysis (see Figure 4)
- Sources with Consecutive Failures
- Sources with No Recent Backup
- Backup Failures by Application

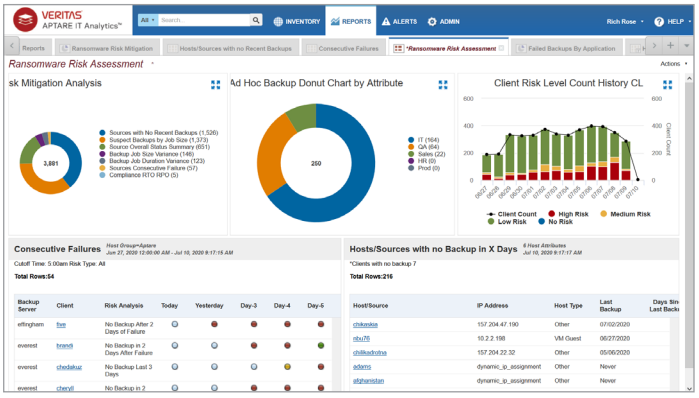


Figure 4. The ransomware risk assessment dashboard in APTARE.

APTARE interrogates successful backups and identifies 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.

To learn more, see Increasing Ransomware Resiliency: Gain complete infrastructure awareness with APTARE IT Analytics.

Malware and Anomaly Detection

Veritas Data Insight supplements existing security detection tools by providing anomalous behavior detection, custom ransomware-specific query templates and file extension identification that can be used to detect ransomware. Data Insight includes policy-based monitoring and alerting that is near-real-time, which helps detect any malicious or anomalous behavior from user accounts. It does so by scanning the unstructured data systems it monitors and collecting audits of all user activities performed on all files—such as read, write, create, delete and rename—while also doing security and file counts for each user (see Figure 5).

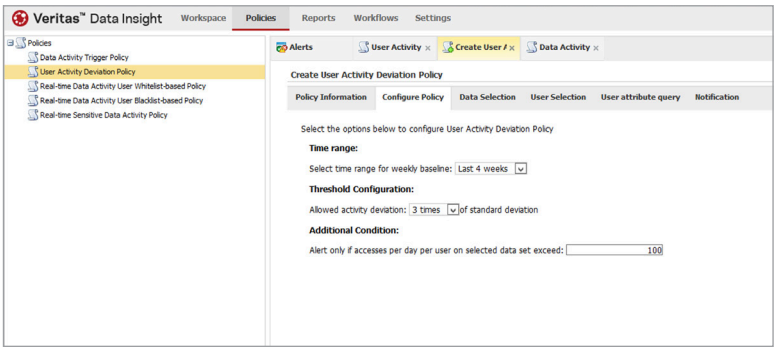


Figure 5. Setting up a User Activity Detection Policy in Data Insight.

This technology compares historical data it has collected and looks for statistical standard deviations to help detect anomalous behavior while identifying accounts that might be compromised due to ransomware. Data Insight can also detect malicious user accounts or ransomware-specific activity and can identify the location of potential ransomware files.

To learn more about Data Insight, see Detect Ransomware Early with Veritas Data Insight.

RECOVER

In the Veritas Enterprise Data Services Platform, we provide a variety of solutions that ensure the flexibility required for a speedy recovery, helping organizations create a strategy to be operational and business resilient. Traditionally, organizations consider backup and recovery the last line of defense, but with Veritas solutions, recovery becomes a vital component in an inclusive strategy, regardless of scale. Veritas provides solutions to the recovery at-scale complexities shown in Figure 6.

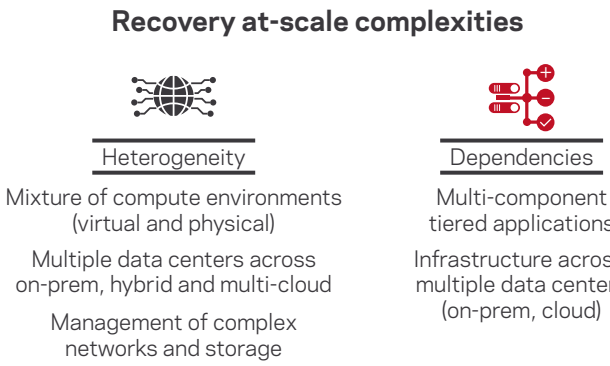


Figure 6. The recovery at-scale complexities Veritas solutions address.

NetBackup Resiliency

NetBackup Resiliency solves these recovery challenges by providing automated orchestration across an organization's entire heterogeneous environment with a consistent user experience, recommending the best recovery options based on the organization's recovery time objective (RTO) and recovery point objective (RPO). (See Figure 7.)

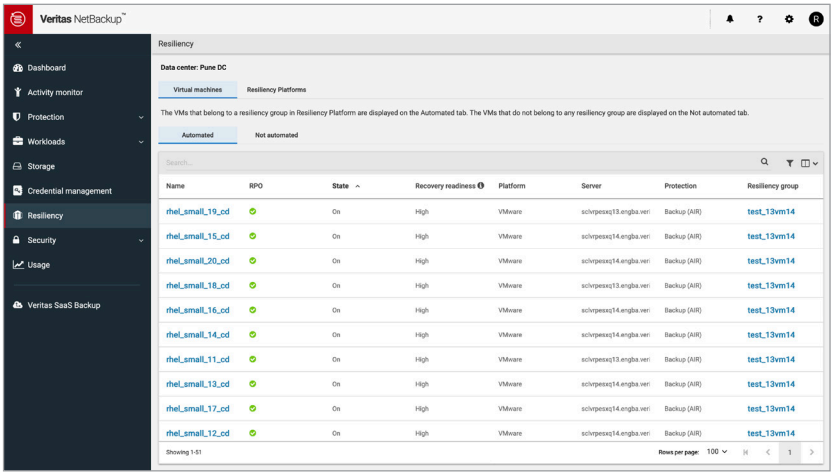


Figure 7. The Resiliency dashboard in NetBackup.

To achieve the most efficient RTO, NetBackup Resiliency determines the best method of recovery by understanding your RTOs, workload(s) and application(s) through your entire data center.

NetBackup Resiliency enables orchestration across heterogeneous environments that include the workload and application as well as the corresponding data. Using NetBackup's automated replication, storage-based replication or Resiliency's built-in data mover lets you choose the RTO and RPO that meets your application's requirements.

Specifically, the solution supports automation by leveraging Virtual Business Services (disaster recovery protection for a multitier application) with Resiliency and Evacuation Plans (the runbook), allowing you to automate recovery at-scale between data centers or to cloud infrastructures.

The solution also allows for push-button rehearsed validation in isolated networks. In ransomware recovery scenarios, organizations can leverage custom scripts to integrate with third-party virus scanning solutions within the workflow to validate against malware prior to returning to production.

From an RPO perspective, NetBackup's continuous data protection (CDP) provides added resiliency through granular recovery of VMware virtual machines (VMs) with near-zero RPO. CDP ensures recovery capability for applications across your heterogeneous environment using granular recovery points in Resiliency's near-real-time data replication (see Figure 8). This capability supports recovery from malware or corruption when it's already been replicated.

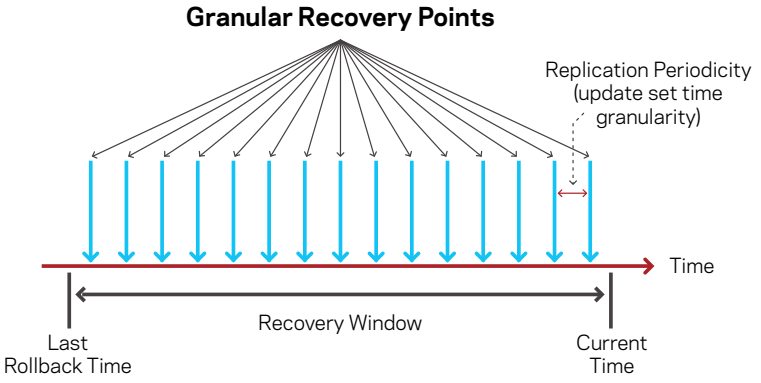


Figure 8. An overview of how NetBackup's continuous data protection works.

Other Recovery Methods with NetBackup

Veritas provides a variety of other recovery methods to meet your RTOs and RPOs, giving you the flexibility to choose the best method of recovery for your organization. Figure 9 illustrates the optimal recovery option based on RPOs and RTOs.

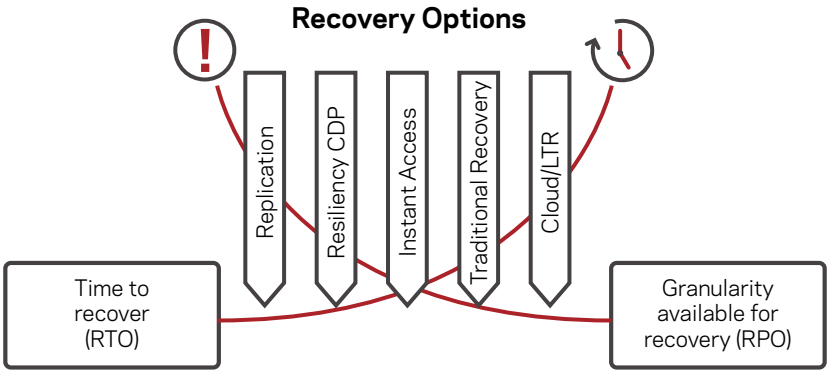
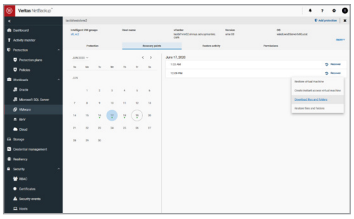


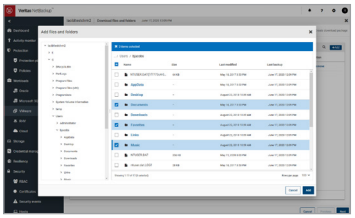
Figure 9. Choosing an optimal recovery option based on RTOs and RPOs.

VM recovery—There are eight types of recovery available for one backup of VMware VMs: full VM, individual VMDK, file and folder, full application, Instant Access, file download, application GRT and AMI conversion. Added support for vTPM ensures backup and restore for high-security environments.

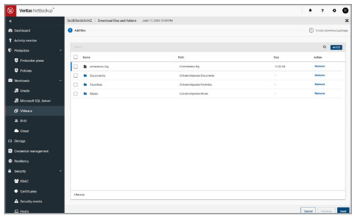
Instant Access—With Instant Access for VMware, you can recover any machine almost instantly, without waiting to transfer the VM's data from the backup. You can also use a backup to test or recover VMs directly from backup storage. These VMs will automatically show up as a regular guest in the VMware infrastructure. In addition, you can browse and recover individual files right in the Web UI. For quick recovery scenarios, you can use VMware Storage vMotion to migrate the VM from backup storage to production while in use.



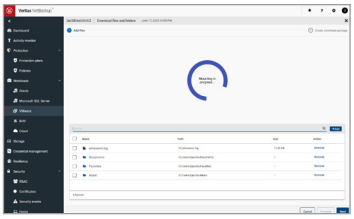
Browse available recovery points for a protected VMware Virtual Machine



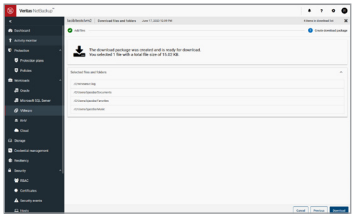
Select the files or folders to recover



Verify the list of files or folders for download



NetBackup Instant Access mounts the backup image to extract files into a package



The packaged files or folders are available for download

Figure 10. Using VMware Instant Access to back up VMs across your infrastructure.

For complete configuration and details, please see the Veritas NetBackup for VMware Administrator's Guide.

Using the same technology, Instant Access for MSSQL provides instantaneous availability of databases and granular recovery of database elements using the backup storage (see Figure 11). Much like Instant Access for VMware, this feature gives you the ability to quickly recover or easy dev/test resources that can be provisioned on demand by or for users and easily cleaned up with a single click later. (See Figure 12.)

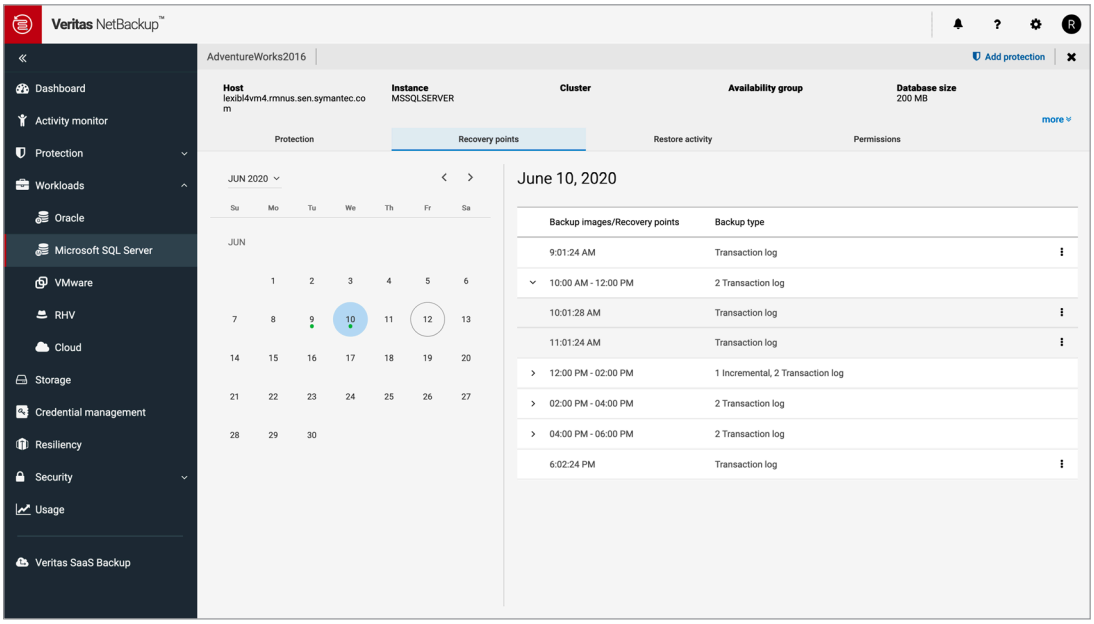


Figure 11. Using VMware Instant Access to back up VMs across your infrastructure.

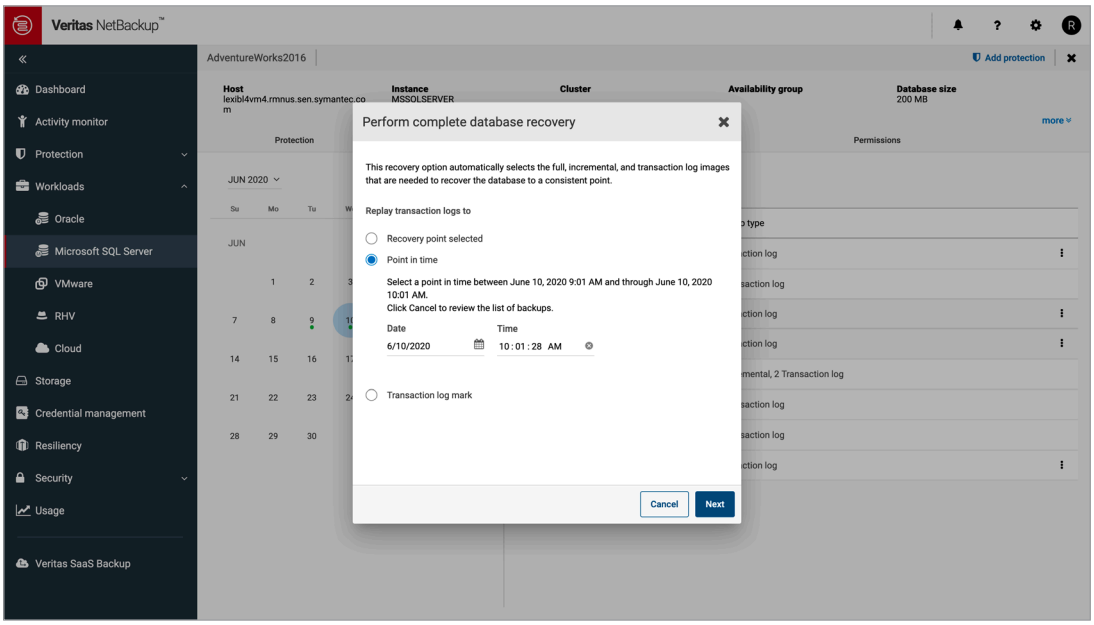


Figure 12. Performing a complete database recovery using Instant Access for MYSSQL.

NetBackup CloudPoint—Using container technology and cloud service providers. Independent of the storage platform, CloudPoint uses cloud-native snapshot technology in a cloud vendor–agnostic way that allows easy protection of hybrid and multicloud infrastructures. In addition, CloudPoint delivers functionally beyond the basic features in a public cloud, enabling application-aware snapshots, single file recovery and multi-region snapshot migration. CloudPoint's multiple account support can securely store backups in a different account, reducing the impact in the event of a compromised account.

Universal Share—An MSDP feature that allows you 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. You can use Universal Share as NAS to store data using compression and deduplication. With full API support and centralized management of shares and protection points in the NetBackup web UI plus user quota support and Active Directory integration, NetBackup HA Appliances provide enhanced management.

For more information, see the Universal Shares section in the Veritas NetBackup Administrator's Guide.

Protection Points for Universal Shares—Allow you to take a point-in-time copy of the data on the share, instantly create a backup image and then use it like any other backup.

CoPilot for Oracle—Building on the features of Oracle CoPilot, the latest version allows Oracle database admins to start up databases directly from a NetBackup Appliance's storage.

For more information, see the Veritas NetBackup™ for Oracle Administrator's Guide.

Long-Term Retention (LTR) Archive—If you need to keep data for an extensive period of time, this option provides a cost-effective and durable solution that features deduplication and compression of data. You can also use object storage and private or public clouds with this method. For private cloud use cases, the Veritas Access Appliance in our Enterprise Data Services Platform provides LTR. When you're deciding on a recovery method, keep in mind that LTR solutions are cost-effective and optimal for healthcare systems and other organizations that need to keep data for a long time.

For organizations that prefer to continue to use tape technologies, we have the most comprehensive, tape-based solution which offers a reliable, air-gapped solution to recover from ransomware.

Traditional recovery—This method 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, you can automate and orchestrate traditional recovery with the push of a button, streamlining the DR process.

Bare Metal Restore (BMR)—If a ransomware recovery needs to leverage infected hardware, BMR can be a valuable solution when you have limited resources. BMR automates the server recovery process, making it unnecessary to reinstall operating systems or configure hardware manually. When systems are corrupted and must be completely overwritten, BMR allows you to rebuild systems quickly from scratch, restoring the OS and the application data with a single operation.

CONCLUSION

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 new ways to penetrate an organization's infrastructure and halt its business. Even with significant effort by system and backup administrators to protect corporate data, ransomware and malicious insiders can still occasionally get through and impact a company's most critical data. That's why having a holistic, multi-layered, comprehensive strategy is essential—and the best defense.

Veritas has simplified the process for you. Our Enterprise Data Services Platform solutions were developed with resiliency at top of mind, providing a single, unified platform to help you protect IT systems and data integrity, detect by monitoring and mitigating and recover quickly with automation and orchestration. Our solutions reduce vulnerability, eliminate islands or potential attack surfaces and are easy to scale, upgrade and maintain. No data is left unprotected, from edge to core to cloud. Although many consider backup and recovery to be the last line of defense against ransomware attacks, we recommend considering it a meaningful and reliable part of your comprehensive, multi-layered protect, detect and recover cybersecurity strategy.

To learn more about our solutions, visit https://www.veritas.com/ransomware or contact us at https://www.veritas.com/form/requestacall/requestacall.

REFERENCES

Government:

- The National Cybersecurity Center of Excellence (NCCoE), part of the National Institute of Standards and Technology (NIST), have produced a special publication titled Data Integrity, Recovering from Ransomware and Other Destructive Events. This is a comprehensive, three-part document that details strategies organization should take to protect against malicious activity as well as the recovery steps to take after a cybersecurity event.

  NIST Special Publication 1800-11
  Data Integrity: Recovering from Ransomware and other Destructive Events (main page)

  - NIST SP 1800-11a: Executive Summary
  - NIST SP 1800-11b: Approach, Architecture, and Security Characteristics – what we built and why
  - NIST SP 1800-11c: How-To Guides – instructions for building the example solution

- United States Computer Emergency Readiness Team: Data Backup Options
  https://www.us-cert.gov/sites/default/files/publications/data_backup_options.pdf

Veritas:

- Insider Threat 101: Detect and Protect with Veritas Data Insight
  https://www.veritas.com/product/information-governance/data-insight/insider-threat

  To read more about the ransomware report templates, see these sections in the User's Guide:

  - About Data Insight custom reports
    https://www.veritas.com/content/support/en_US/doc/133376979-133376982-0/DI_6_1_2_v109979856-133376982
  - About DQL query templates
    https://www.veritas.com/content/support/en_US/doc/133376979-133376982-0/DI_6_1_2_v109979871-133376982

- Veritas Flex Appliances with NetBackup Security:
  https://www.veritas.com/content/dam/Veritas/docs/white-papers/v1108-ga-ent-wp-flex-security-en.pdf
- Veritas Flex Appliances with NetBackup
  https://www.veritas.com/content/dam/Veritas/docs/white-papers/v1111-ga-ent-wp-flex-design-guide-2020-en.pdf
- Veritas Data Insight Administrator's Guide:
  https://www.veritas.com/support/en_US/doc/133377453-133377456-0/
- Veritas Data Insight User's Guide:
  https://www.veritas.com/support/en_US/doc/133376979-133376982-0/
- Veritas NetBackup Administrator's Guide, Volume I:
  https://www.veritas.com/support/en_US/doc/18716246-132504715-0/
- Veritas NetBackup Appliance Administrator's Guide:
  https://www.veritas.com/support/en_US/doc/75895731-133007275-0/
- Veritas NetBackup Appliance Fibre Channel Guide:
  https://www.veritas.com/support/en_US/doc/99943943-132539628-0/
- Veritas NetBackup Appliance Security Guide:
  https://www.veritas.com/support/en_US/doc/96220900-132543872-0/
- Veritas NetBackup Cloud Administrator's Guide:
  https://www.veritas.com/support/en_US/doc/58500769-132715871-0/
- Veritas NetBackup Deduplication Guide:
  https://www.veritas.com/support/en_US/doc/25074086-131900563-0/

- Veritas NetBackup Security and Encryption Guide
  https://www.veritas.com/support/en_US/doc/21733320-139202231-0/index
- Veritas NetBackup for Oracle Administrator's Guide:
  https://www.veritas.com/support/en_US/doc/16226115-133434979-0/
- Veritas NetBackup for VMware Administrator's Guide:
  https://www.veritas.com/support/en_US/doc/21902280-133434834-0/

1. https://www.crn.com/slide-shows/security/the-11-biggest-ransomware-attacks-of-2020-so-far-

ABOUT VERITAS

Veritas Technologies is a global leader in data protection and availability. Over 50,000 enterprises—including 87 percent of the Fortune Global 500—rely on us to abstract IT complexity and simplify data management. The Veritas Enterprise Data Services Platform automates the protection and orchestrates the recovery of data everywhere it lives, ensures 24/7 availability of business-critical applications, and provides enterprises with the insights they need to comply with evolving data regulations. With a reputation for reliability at scale and a deployment model to fit any need, Veritas Enterprise Data Services Platform supports more than 800 different data sources, over 100 different operating systems, more than 1,400 storage targets, and more than 60 different cloud platforms. Learn more at www.veritas.com. Follow us on Twitter at @veritastechllc.

2625 Augustine Drive, Santa Clara, CA 95054
+1 (866) 837 4827
www.veritas.com

For specific country offices and contact numbers, please visit our website.
www.veritas.com/company/contact

VERITAS

V0827 11/20