VERITAS

Protecting Healthcare and Critical Infrastructure from Modern Malware

A comprehensive guide to combatting the threat of ransomware.

White Paper | October 2021

Contents

Executive Summary 3

Introduction 3

Best Practices 4

Protect, Detect, Recover. 6

- Protect 6
- Detect 8
- Recover 10

Competitive Differentiation. 14

Conclusion 15

References. 15

Executive Summary

Today, ransomware and ransomware attacks are a top concern for industries of all sizes and types, including government institutions, financial companies, and healthcare providers. According to Cybersecurity Ventures, by 2031, a business will fall victim to a ransomware attack every two seconds and that attack will cost its victims more than US$265 billion annually, 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 Internet of Things (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 organizations consider backup and recovery of 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. When a ransomware attack happens to our healthcare systems, it doesn't just impact infrastructure, it also affects every aspect of patient care. When a life is on the line, time is of the essence to act promptly, which is why losing a life because of a ransomware attack that caused a delay in providing quality healthcare is completely unacceptable.

According to a study by Vanderbilt University's Owen Graduate School of Management, cybersecurity remediation at hospitals can slow down doctors, nurses and other health professionals as they offer emergency cardiac care. In fact, according to studies, a data breach or malware infection can cause 36 additional deaths per 10,000 heart attacks that occurred annually at the hundreds of hospitals examined. Given that every year about 805,000 Americans have a heart attack,[1] that can mean an additional 2,800 additional deaths nationwide. Time is of the essence, period.

Veritas solutions are developed with resiliency at top of mind, so we can provide our customers with dependable solutions to ensure their business is 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. The Veritas brand 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

Without question, hospitals are being specifically targeted by bad actors. And unfortunately, the healthcare industry is less prepared than other industries to stop these attacks and successfully retrieve data before it's already been encrypted. Relying solely on backup recovery and defensive strategies focused on the perimeter are no longer enough. We are currently tracking four nation-state actors and many independent hacker groups targeting healthcare by attacking assets with the most valuable data—formularies, vaccines and treatment protocols used for COVID-19.

As an attack evolves, it can move laterally across an environment by attacking multiple endpoints to maximize the infection and compromise credentials. It then finds and encrypts the backup solution to prevent healthcare system administrators from restoring the infected assets. Most recently on May 14, 2021, hackers targeted the systems of Ireland's Health Service Executive (HSE). The hackers claimed they spent two weeks in the HSE's systems before launching the attack and claimed to have encrypted and stolen 700 GB of data. Most hackers today are savvy—they're able to get in undetected, evaluate the weak areas and patiently wait to attack. They are motivated to ensure you have no other choice than to pay the ransom. Our experience has shown that most hackers are inside an organization's network and surveying assets anywhere from 8–18 months before launching an attack. That means you could have a hacker in your environment right now preparing an attack.

Studies have shown that industries under duress from something such as a global pandemic are twice as likely to pay the ransom to get back to critical business. Additionally, hospitals and hospital systems have historically under-invested in information security, spending on average only 3–5 percent of their IT budget on security compared to the 10–15 percent spent by the most highly regulated industries. With the recent work-from-home model, employees have also created many new entry points into the organization and are often untrained in phishing tactics, creating an ideal situation for ransomware attackers.

There is no way to eliminate the threat of ransomware, but you can be prepared with a multilayered approach by reducing your vulnerability, increasing your protection and enhancing your overall resiliency. Ransomware emerged in the late-1980s into the early 1990s and has continued to evolve in effectiveness, damage and speed. There is no longer a question of if you're going to be hit, but when ransomware will strike. Although there is never a good time, many attacks occur at the absolute worst time, by design. Adding insult to injury, ransomware has another implication specifically for all healthcare providers—new forms of ransomware exfiltrate and expose protected data to unauthorized individuals, creating a breach under the Health Insurance Portability and Accountability Act (HIPAA) that must be reported to the Office for Civil Rights (OCR). This new nightmare can lead to fines on top of the cost of recovery.

This guide will empower you to:

- **Protect** your data assets using system hardening and immutable storage.
- **Detect** threats using machine learning and anomaly detection to provide complete visibility into your organization's environment and highlight a possible infection.
- **Recover** quickly with flexibility, focus and at scale from attacks with a broad range of product features and functionality you can customize to meet your unique needs and requirements.

It's important to note that within the healthcare system 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 environment'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. We suggest developing, rehearsing and consistently evaluating your strategy to evolve with the sophistication of threats and their technologies. Let's dive into our recommended best practices for backing up your organization's ecosystem.

Best Practices

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

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

- 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
  - Know where your critical data resides and who has access to it.
  - Require users to log in with their own credentials to prevent account takeover from using a single credential.
  - Implement role-based access control (RBAC) and two-factor authentication (2FA) to limit access to only required functionality for each persona or enforce least-privileged access by ensuring the minimal level of usage or user rights that allow applications and individuals to perform their functions.
  - 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 (WORM storage: write once, read many) and indelible storage technology.
- Perimeter Defense
  - Use virus scanning software to keep your environment secure and conduct tests to validate the safety of your data while continuously monitoring workloads that are not being backed up.
  - Maintain current patches and virus signature files.
  - Create and enforce an accountable security policy by training staff on phishing techniques while also creating a safe environment for employees to report suspicious activity.
  - Monitor data access patterns and respond rapidly when the patterns change.
- 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 by taking other malicious actions.
- Configuration
  - Use security implementation guides to implement best practices with configuration.
  - Harden your environment by restricting ports and processes by enabling firewalls as well as deploying firewall systems with sandboxing to block malware payloads.
  - Update the default Primary 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.
- Incident Response Plan
  - Develop a plan to ensure that in the event of a disaster recovery (DR) or malicious attack you have a strategy in place for business and operational resilience.
  - Understand which applications are strategic and mission-critical to your business so you can prioritize the recovery of those first in the event of a ransomware attack.
  - Keep a 'single source of truth' of your backup data for clinical and critical workstations to ensure you can recover the most critical items to a healthy state first.

"3-2-1" Backup Strategy

At least three sets of your data

Store two copies on different storage types

Keep one copy off-site

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, but the enhanced visibility will also help you identify problem 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.

We at Veritas share your ransomware concerns, which is why we have leveraged the Cybersecurity Framework recommended by The National Institute of Standards and Technology (NIST). As the de facto leader for cybersecurity best practices, NIST 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 solutions within the broader NIST framework.

Protect, Detect, Recover

Organizations must be able to quickly identify a malware attack, where it's coming from and what is being attacked. A short delay in response can mean the difference between a small, contained infection that is easy to remediate versus the entire organization being infected. Organizations should prepare in advance for the "when it happens" scenario so they can respond quickly and effectively.

Protect

Although the first line of defense is often perimeter security, you must also ensure your critical and most important asset—your data—is protected from the unknown and unexpected. Healthcare and NIST rely on the "defense-in-depth" approach to security. You must also consider all aspects of your organization—the people, the processes in place and the technology infrastructure.

When properly trained and empowered, your staff is one the most valuable line of defenses against ransomware attacks. Organizations must develop an accountable security program and train staff on the various types of malware and phishing techniques. Starting in the early 2010s, passive ransomware gave way to targeted attacks that emulated legitimate communication from your organization based on the research attackers had done on individuals and their behavior. Many new attacks take advantage of an employee's fear by demanding, "pay up or we'll inform your organization you violated security policy" as a distraction technique while the malware is spreading. As such, it's equally important to create a safe and open environment for employees to report malicious activity.

Along with making sure your team is equipped with the proper techniques in the event of a ransomware attack, it's vital to have processes in place to cover all possible points of protection. These processes should include actively researching for new exploits, vulnerabilities and malware, continuously scanning your environment with virus protection using the latest signature file and using email security scanning technology to identify and stop malware payloads. With this knowledge and awareness, you can apply patches and fixes for those vulnerabilities or engage with your technology vendors to have those fixes quickly developed. Your backup infrastructure and assets are an essential component in being able to recover from an attack successfully. HIPAA requires that all protected health information (PHI) is backed up and recoverable. Backups are an organization's key to recovery.

Healthcare systems are incredibly diverse, requiring the right technology that prioritizes data integrity with simplicity and flexibility. Veritas NetBackup™ offers the widest support from the edge to the core to the cloud of 800+ data sources, 1,400+ storage targets and 60+ cloud providers, which means your environment is always protected and always recoverable. With a focus on data integrity, Veritas helps ensure your backup files remain safe and untouched from malicious invaders. We know how vital it is for our healthcare customers to protect their data, which is why we've placed NetBackup and its key functionality around data integrity at the heart of our protection strategy.

We offer a wide range of security controls to maintain data integrity 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—NetBackup Flex Appliances support configurable authentication strength.

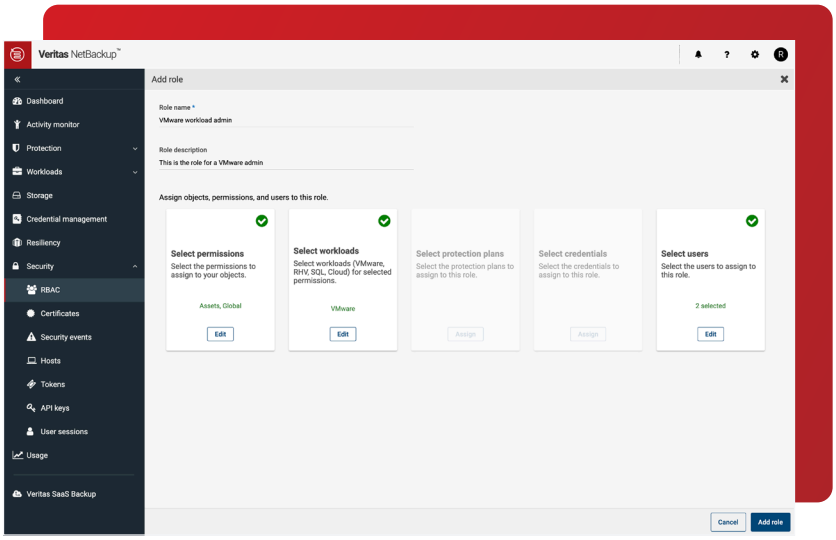


Figure 2. The access permissions dashboard in NetBackup.

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

- Flexible, Storage-Agnostic Image Management
  - 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.
  - To keep your data secure and compliant, use immutable storage on-prem and in the cloud.
  - Use cloud immutable storage with Amazon Web Services (AWS) S3 Object Lock to ensure your cloud data is secure and unable to be compromised. To learn more about NetBackup's cloud immutable storage, see the Object Lock support for AWS technical brief.
  - The NetBackup Flex deployment option provides immutable and indelible storage that reduces the risk of malware or ransomware encrypting or deleting backup data, thereby making it unusable
- Images Stored within WORM (write once, read many) Storage
  - 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).

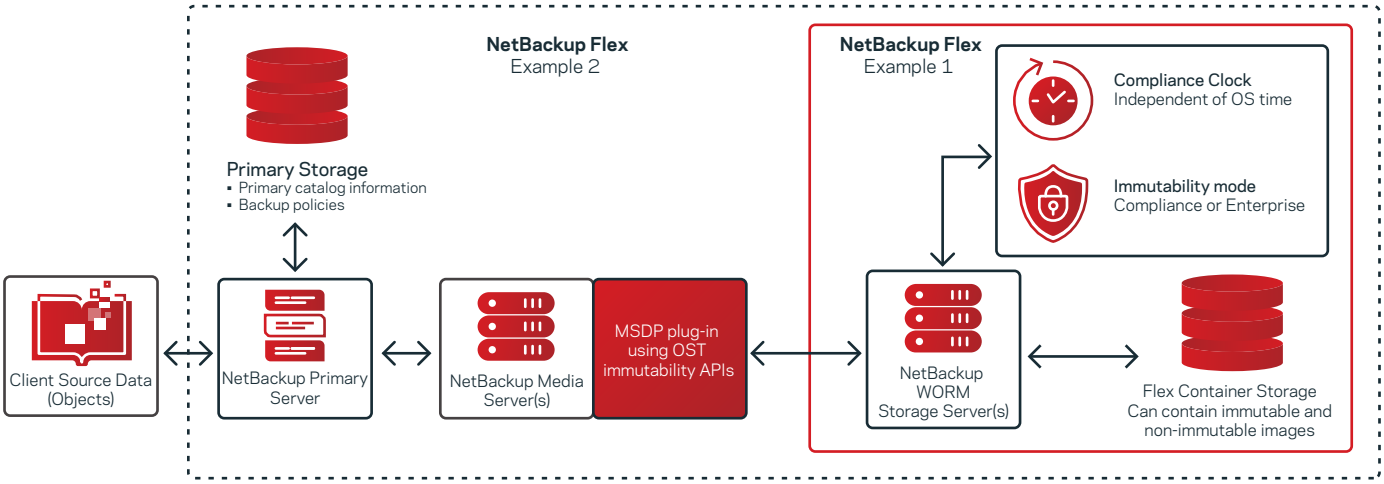


Figure 3. Two of the many NetBackup Flex deployment examples.

- Compliance mode enables immutable storage in which no user, including the root user, can delete the data during a predefined retention period.
- Enterprise mode protects the data from being deleted during a predefined retention period, but only users with special permissions can alter the retention settings or delete the data using dual authorization. Two individuals with different RBAC levels must agree to make any changes to the retention time or modify or delete the data.
- For Enterprise mode, we recommend the roles be placed in separate organizations, such as one role in the infrastructure team and the second role in the information security team. This approach allows user authentication to be separated, so if one authentication mechanism is compromised, then the other cannot be.
- NetBackup and NetBackup Flex prevent the altering and deletion of critical files whether in the data center or in a supported cloud. Few well-known vendors like Veritas have a built-in internal, protected immutability timer for core as well as edge deployment. This feature prevents a relatively new attack vector, where hackers change the system time on storage targets to "expire" and then delete the immutable backup copy.
- 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.

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 healthcare organizations must maintain an increasingly complex IT environment with reduced resources. Despite these constraints, organizations want assurance their environment is safe, secure and capable of overcoming ransomware threats while reducing the day-to-day complexity of monitoring and maintaining backup and storage configurations. Healthcare IT environments must be empowered with a solution that can identify data points, events and actions that are outside the expected data behavior patterns of a given set of users at the core or in the cloud. Rapid detection of a malware outbreak is critical to containment and recovery. Veritas offers solutions that provide anomaly detection and infrastructure awareness.

Malware and Anomaly Detection

With version 9.1 and higher, NetBackup provides artificial intelligence-powered (AI-powered) anomaly detection that lets you detect and be alerted of behavior at the time of backup.

- This feature ensures your data is always recoverable and enables you to take immediate action when ransomware strikes, isolating backups with malware and limiting its impact.
- NetBackup gives administrators the ability to view data and provides recommendations associated with anomalies at any time by monitoring all your devices, so you can stay on top of issues as they arise.
- NetBackup's AI-powered anomaly detection seamlessly integrates into the NetBackup Primary Server, enabling it to detect anomalous forms of observations—making those that do not fall into the cluster considered as anomalies or outliers. This capability lets a backup architect or security administrator see anomalies and drill down to identify any concerns. It offers the ability to mine large amounts of data and provide actionable intelligence to address ransomware events or simply changes in the environment of which an administrator should be aware (see Figure 4).

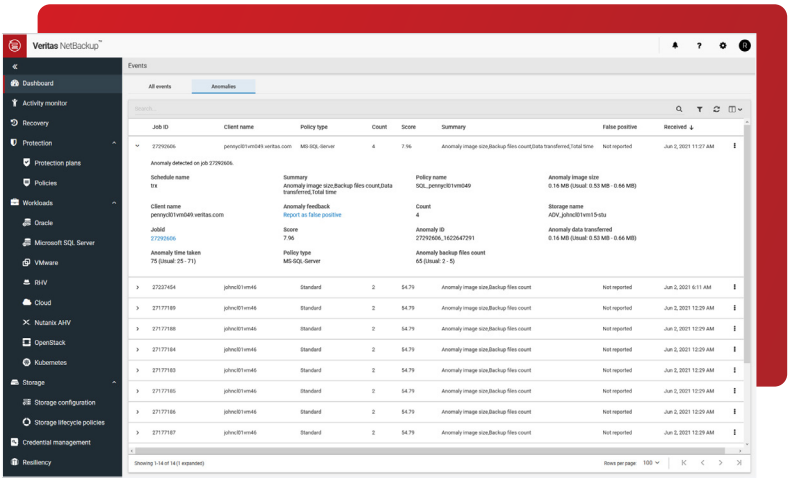


Figure 4. Use NetBackup to detect anomalies and take action accordingly.

- NetBackup trends backup performance and key metrics. For example, if you see a sudden and drastic decrease in your deduplication rate, it's a good indicator that data has changed and is probably encrypted. Identifying that anomaly and responding rapidly will allow you to contain the infection and prevent the spread to other data.

To learn more about NetBackup's anomaly detection capabilities, see the NetBackup Anomaly Detection technical brief.

Veritas not only addresses secondary backup data with NetBackup but also primary storage—where the application lives—with Veritas Data Insight. 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 near-real-time alerting, which helps detect any malicious or anomalous behavior from user accounts.
- It scans the unstructured data systems it monitors and collects audits of all user activities performed on all files—such as read, write, create, delete and rename—while also capturing security and file counts for each user (see Figure 5).
- 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.

Many health systems use this technology today to protect critical formularies and intellectual property. With alerts about unusual activity, customers can respond to concerns in real time. Even if a legitimate user changes expected behavior, such as downloading an unusually high amount of data, the organization is alerted and can take corrective action immediately.

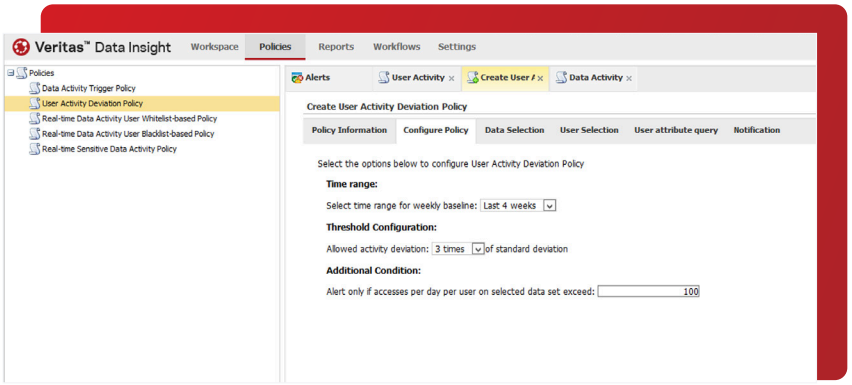


Figure 5. Setting up a User Activity Detection Policy in Data Insight.

Backup and Storage Infrastructure Awareness

Veritas realizes that organizations want to understand the risk factors in their environment quickly so they can take remediation actions to clean up the environment. APTARE™ IT Analytics addresses that problem with a ransomware risk assessment dashboard available out of the box. The dashboard houses pre-identified reports that help you gain risk visibility into your backup environment. APTARE allows your organization to:

- Discover all hosts or virtual machines (VMs) in your infrastructure and compare them with the VMs protected by NetBackup.
- Flag hosts that are missing from the backups or have no recent backups as potential risks.
- Detect the potential ransomware-affected files along with their size and where they reside in the environment.
- Use interactive graphs that provide a historical view of the risks generated.

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

- Risk Mitigation Analysis (see Figure 6)
- Sources with Consecutive Failures
- Sources with No Recent Backup
- Backup Failures by Application

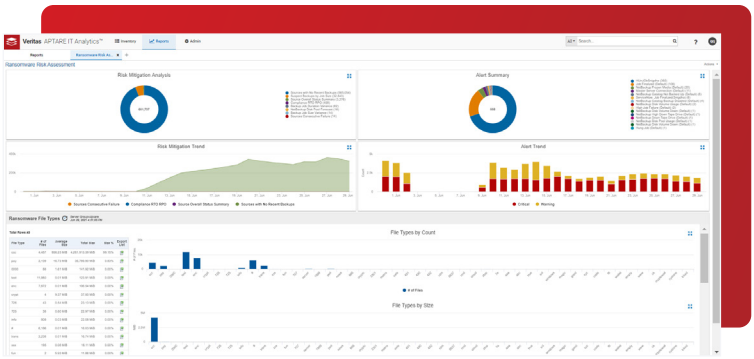


Figure 6. The ransomware risk assessment dashboard in APTARE.

APTARE interrogates successful backups and identifies potential false positives by comparing historical backups against the new backup to identify 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.

Recover

When attacked by ransomware, speed-to-recovery is at stake for all IT environments but especially for healthcare systems. The path to recovery varies, depending on your organization's willingness to pay the ransom.

If your organization has agreed to pay the ransom, then the attackers should provide you with a decryption key. You can use the decryption key to unlock the encrypted data, but that is frequently not enough. As illustrated by the Colonial Pipeline attack in 2021, even though the ransom was paid and the key was received, the decryption was so slow the company had to leverage the backups to recover as well. It appears the hacker community is very concerned with the speed at which they can spread attacks and encrypt data but care very little about the time it takes an organization to recover. And that assumes you actually received the decryption key upon payment. Approximately 20 percent of victims that pay the ransom do not get the decryption codes. In fact, history has shown that victims that pay the ransom are often attacked again by the same or different malicious actors. And why not, given that you've proven you will pay. According to a study conducted by Sophos, even after paying a ransom and attempting to recover data from a backup, more than a third of healthcare providers were still unable to restore their data.

At Veritas, we recommend a comprehensive approach to avoid ever paying the ransom. We provide a variety of solutions that ensure the flexibility required for a speedy recovery, helping healthcare organizations create a strategy to be operational and business resilient. Traditionally, organizations considered 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 7.

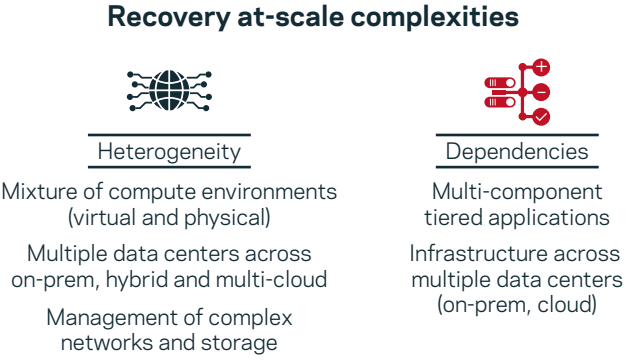


Figure 7. The recovery at-scale complexities Veritas solutions address.

NetBackup Resiliency

NetBackup Resiliency solves these recovery challenges by providing automated orchestration across an organization's entire heterogeneous environment with a consistent user experience and visibility into the best recovery options based on the options available, so organizations can meet their recovery time objective (RTO) and recovery point objective (RPO) (see Figure 8).

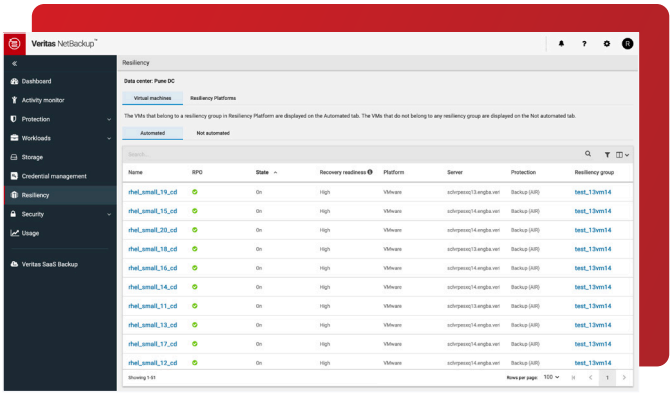


Figure 8. The Resiliency dashboard in NetBackup.

To achieve the most efficient RTO, NetBackup Resiliency provides insight into recovery operations that help determine the best method of recovery based on your RTOs, workload(s) and application(s) throughout your entire data center. NetBackup Resiliency enables orchestration across heterogeneous environments that include the workload and application as well as corresponding data. By using NetBackup's automated replication, storage-based replication or Resiliency's built-in data mover, you can choose the RTO and RPO that meet your application's business requirements.

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

From an RPO perspective, NetBackup's continuous data protection (CDP) ensures recovery capability for applications across your heterogenous environment using granular recovery points in NetBackup Resiliency's near-real-time data replication (see Figure 9). This capability supports recovery from malware or corruption when it's already been replicated.

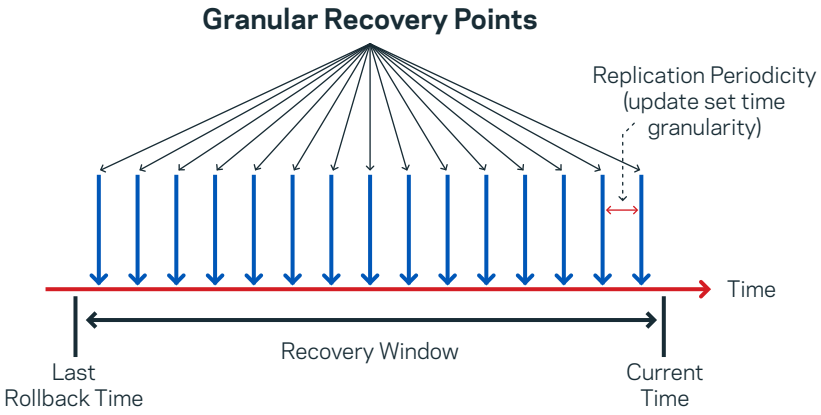
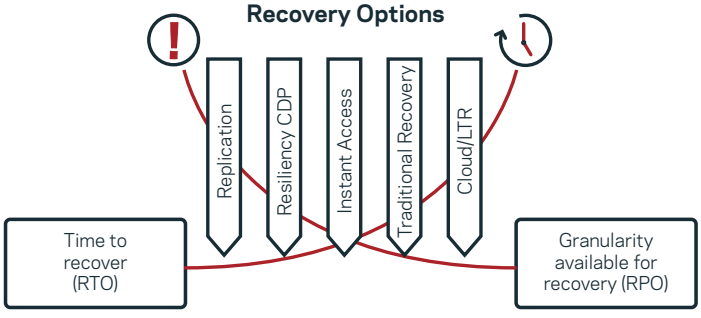


Figure 9. An overview of how NetBackup's continuous data protection works.

Learn more about Continuous Data Protection for VMware and advanced resiliency options for VMware application protection with NetBackup by reviewing their respective blogs.

Other Recovery Methods with NetBackup

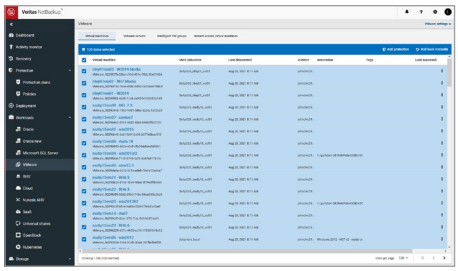
Veritas provides a variety of other recovery methods to meet your RTOs and RPOs, giving you the flexibility to choose the best method of recovery for your organization. Figure 10 illustrates the optimal recovery option based on RPOs and RTOs .



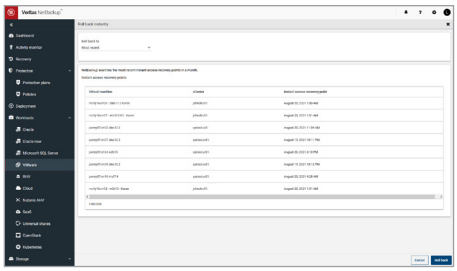
RTO & RPO objectives determine optimal option

Figure 10. An overview of how NetBackup's continuous data protection works.

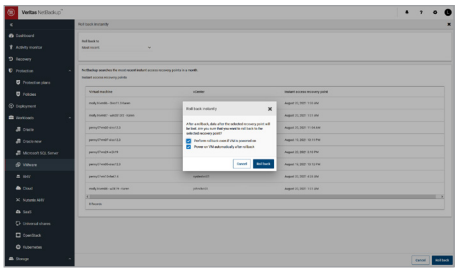
NetBackup Instant Rollback for VMware—Provides high-speed VM recovery by using Change Block Tracking to identify which unique blocks need to be recovered and applying just those changes to bring your VM back to a healthy state—from a disaster or ransomware attack—in seconds instead of minutes or hours. This process effortlessly recovers 1 or 100 machines, providing quick bulk recovery regardless of where your infrastructure lives (see Figure 11).



Select all of the VMs that you would like to roll back.



Select the recovery point that you would like to use.



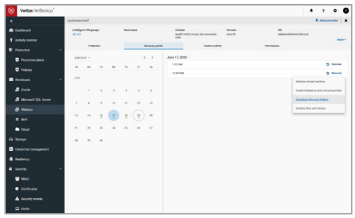
Confirm your choice to roll back.

Figure 11. Using Instant Rollback for VMware to seamlessly revert back to any time.

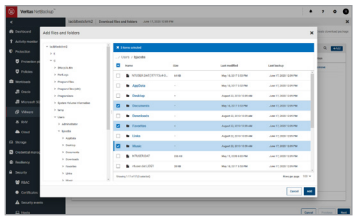
For more information on Instant Rollback for VMware, read this VOX blog.

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.

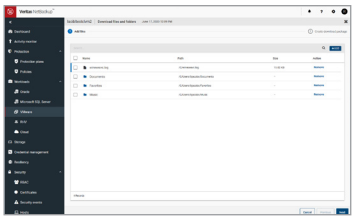
Instant Access for MSSQL and VMware—With Instant Access for VMware, you can recover any machine almost instantly, without waiting to transfer the VM's data from the backup (see Figure 12). You can also use a backup to test or recover VMs directly from backup storage. These VMs will automatically show 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 .



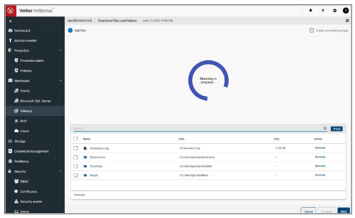
Browse available recovery points for a protected VMware Virtual Machine



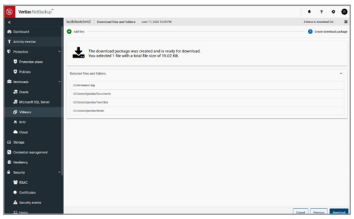
Select the files or folders to recover



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 12. 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.

Instant Access for MSSQL provides instantaneous availability of databases and granular recovery of database elements using the backup storage (see Figure 13). Self-service capabilities enable database administrators to quickly provision MSSQL databases for their dev/test needs. If some copies of data are impacted by ransomware, NetBackup gives you the flexibility to recover from any available backup copy using both our interface and APIs (see Figure 14).

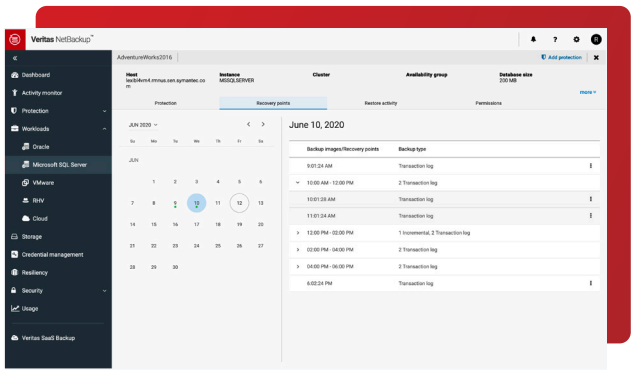


Figure 13. NetBackup provides granular point-in-time recovery options for MSSQL.

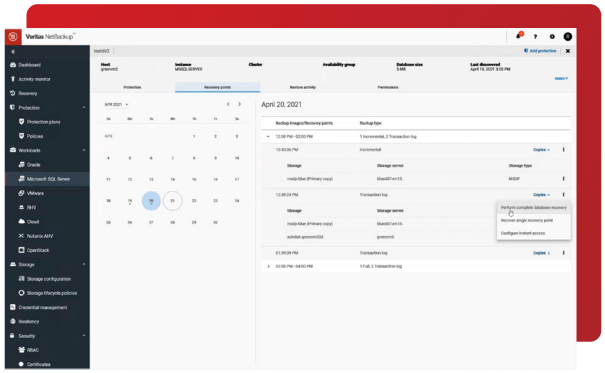


Figure 14. Recovery databases from any copy a MSSQL backup.

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

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

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 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 that 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 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.

Competitive Differentiation

Veritas solutions ensure your data is always available and protected, help with application high availability and provide proven recovery at scale—all while maintaining business continuity in the event of attacks on data and infrastructure. Traditional data protection technologies, whether primary storage giants or scale-out vendors, do not approach ransomware resiliency comprehensively like Veritas. Compared to the competition, Veritas approaches ransomware resiliency through a business value lens, providing a robust resiliency strategy by solving for the protection, detection and recovery from ransomware.

What to consider when selecting a data protection vendor:

- Does the solution provide ransomware resiliency at the core and the edge and in the cloud?
- Does it offer immutable storage whether deployed as BYO, appliance, cloud or SaaS?
- Does the solution support the 3-2-1 backup copy rule in every scenario?
- Does the solution have an internal and protected immutability timer? Or does it rely on the system date/time for the storage target?

Veritas solves for all of the above and more:

- Offers multiple deployment options and ransomware resiliency for any enterprise deployment scenario.
- Takes a multilayer security approach for protecting backup data, closing back doors such as cluster resets, external clocks or BIOS.
- NetBackup and NetBackup Flex prevent the altering and deletion of critical files whether in the data center or in a supported cloud with a built-in internal, protected immutability timer for core as well as edge deployment.
- Uses a hardened OS to reduce the attack surface of ransomware.
- Designs solutions based on the 3-2-1 best practice, providing copy standards for tape support, immutable storage and air gap.
- Creates appliances with hardened containerized deployments, making it even harder to get into than traditional physical or VM form factors.
- Includes built-in intrusion detection and protection in appliances that eliminates overhead on IT and security teams.
- Offers detection not only at the backup monitoring level, but also expands it into infrastructure and the primary data access pattern level, providing the ability to delete known ransomware as well as disable a potential breached account to minimize the impact of ransomware.
- Provides the ability in NetBackup to rollback only changes to VMs from ransomware attacks, making recovery from ransomware efficient and quick.

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 create new ways to penetrate an organization's infrastructure that will halt business while impacting the lives of all those involved. When it comes to healthcare systems, time is even more critical because lives are at stake as well as your ability to deliver quality care to the people who need it the most. Even with significant effort by system and backup administrators to protect corporate data, ransomware and malicious insiders can still occasionally get through and impact your most critical data. That's why having a holistic, multilayered, comprehensive strategy is essential—and the best defense.

Veritas enables healthcare IT administrators with the tools they need to protect, detect and recover critical assets in the face of ransomware attacks. Remember prevention, tertiary care and restorative care are the essence of critical patient care, and with Veritas solutions, the ability to protect, detect and recover are the essence of critical IT systems care. Our solutions reduce vulnerability, eliminate islands or potential attack surfaces and are easy to scale, upgrade and maintain by leveraging automation and orchestration. No data is left unprotected—from the edge to the core to the 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, multilayered 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), has 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/140216462-147580071-0/v109979856-147580071
  - About DQL query templates
    https://www.veritas.com/content/support/en_US/doc/140216462-147580071-0/v109979871-147580071

- 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/content/support/en_US/doc/140216468-147568119-0/index
- Veritas Data Insight User's Guide:
  https://www.veritas.com/content/support/en_US/doc/140216462-147580071-0/v109977986-147580071
- Veritas NetBackup Administrator's Guide, Volume I:
  https://www.veritas.com/content/support/en_US/doc/18716246-145636479-0/v41803467-145636479
- Veritas NetBackup Appliance Administrator's Guide:
  https://www.veritas.com/content/support/en_US/doc/75895731-145526127-0/v36825596-145526127
- Veritas NetBackup Appliance Fibre Channel Guide:
  https://www.veritas.com/content/support/en_US/doc/99943943-147509185-0/v120257742-147509185
- Veritas NetBackup Appliance Security Guide:
  https://www.veritas.com/content/support/en_US/doc/96220900-145526125-0/v96220920-145526125
- Veritas NetBackup Cloud Administrator's Guide:
  https://www.veritas.com/content/support/en_US/doc/58500769-150013608-0/v95640390-150013608
- Veritas NetBackup Deduplication Guide:
  https://www.veritas.com/content/support/en_US/doc/25074086-149019166-0/v95646212-149019166
- Veritas NetBackup Security and Encryption Guide
  https://www.veritas.com/content/support/en_US/doc/21733320-146139160-0/v127786676-146139160
- Veritas NetBackup for Oracle Administrator's Guide:
  https://www.veritas.com/content/support/en_US/doc/16226115-145903096-0/v78442622-145903096
- Veritas NetBackup for VMware Administrator's Guide:
  https://www.veritas.com/content/support/en_US/doc/21902280-148036804-0/v19545336-148036804

1 https://onlinelibrary.wiley.com/doi/pdf/10.1111/1475-6773.13203

About Veritas

Veritas Technologies is a global leader in data protection and availability. Over 80,000 customers—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.

VERITAS

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

For global contact information visit:
veritas.com/company/contact

V1398 10/21