VERITAS

The Comprehensive Ransomware Guide with Veritas

White Paper | January 2023

VERITAS ALTA™

Contents

Executive Summary . . . 3
Introduction . . . 3
Best Practices . . . 4
- Version Management and Prompt System Updates . . . 4
- Zero Trust Model and Policies . . . 4
- Immutable and Indelible Storage . . . 5
- Data Encryption . . . 5
- Configuration and Network Segmentation . . . 5
- Deployment and the 3-2-1 Backup Strategy . . . 5
- Complete Endpoint Visibility . . . 5
- Optimize for Rapid Recovery . . . 5
- Frequency and Diligent Rehearsals . . . 5
- Educate Employees . . . 6

Our Strategy: Protect, Detect, Recover . . . 6
- Protect . . . 6
  - Identity and Access Management . . . 6
  - Data Encryption . . . 6
  - Immutable/Indelible Image Management and Storage . . . 7
  - Solution Hardening . . . 8
- Detect . . . 8
  - Backup and Storage Infrastructure Awareness . . . 8
  - Anomaly Detection . . . 9
  - Primary Storage Detection . . . 10
  - Malware Detection . . . 10
- Recover . . . 11
  - NetBackup Resiliency . . . 11
  - Other Recovery Methods with NetBackup . . . 12

Competitive Differentiation . . . 14
Conclusion . . . 15
References . . . 16

Executive Summary

Today, cybersecurity and the threat of ransomware attacks are top concerns for every industry throughout the globe. According to the 2022 SonicWall Cyber Threat Report, there were 19 attacks every second, with 623.3 million attacks globally. It's now clear that ransomware is the fastest-growing type of cybercrime. Ransomware as a service (RaaS) has developed into an organized, lucrative business model and 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 as well as software vulnerabilities are gaining popularity. That's why it's critical for IT teams to realize they can't achieve true ransomware resiliency by endpoint security alone. Instead, they need a multi-layered strategy.

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

Veritas solutions were developed with resiliency at top of mind and security at their core, so we could provide our customers with dependable solutions to ensure their business stays up and running with minimal impact. Our solutions protect IT systems and safeguard data integrity with a wide range of Zero Trust security controls, workload support, and industry-leading immutable and indelible storage options to suit varying needs. Our solutions provide complete visibility of your entire environment, including physical, virtual, and cloud workloads and ranging from storage to compute and even across other backup vendors and services, ensuring no system falls through the cracks. Our tools provide you with near-real-time, artificial intelligence (AI)-driven detection of anomalous behaviors or activities associated with both data and user activity across your whole environment. Our automated and on-demand malware scanning also provides clear warning prompts, spot-checking of known high-risk areas, and recovery of clean data. When it comes to recovery, the Veritas brand has been synonymous with resiliency for decades. Dependable Veritas solutions incorporate proven technology, so you can recover quickly with flexible, automated, and orchestrated options that have your business back up and running in minutes.

Introduction

This paper focuses on Veritas solutions that comprise the industry's most comprehensive, compliant, and secure ransomware resiliency platform. Our solutions help provide valuable peace of mind, reduce risk, and ensure you can protect, detect, and recover your data and stay resilient against the ever-evolving threat of ransomware.

This paper is designed for business and technical audiences, including customers, partners, and others who want to learn more about how our solutions help protect against and recover from a malicious attack.

This white paper will help you:

- Learn how to protect your IT systems and safeguard data integrity
- Understand how Veritas solutions help you monitor and mitigate threats and vulnerabilities
- Explore options for rapid and complete cross-system restoration and develop your plan to optimize your environment for recovery

It's important to note that there's no one-size-fits-all solution for ransomware resiliency, 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 multi-layered and comprehensive strategy structured around the National Institute of Standards and Technology (NIST) methodology—identify, protect, detect, respond, and recover. In addition to what we share in this white paper, we recommend you retain traditional security measures as a primary part of your organization's defensive strategy; make sure to add firewalls, email, and spam filters plus anti-malware and point protection software; and introduce segmented network strategies and employee education programs.

Enterprises must develop, rehearse, and consistently evaluate their strategy to evolve with the growing sophistication of threats and their technologies. Practicing regular rehearsals and validation are vital for success to ensure things actually work when you're in crisis mode. Plus, it's always advisable to hire a third-party agency to audit your strategy, check your work, and help you identify vulnerabilities.

Let's dive into our recommended best practices for an organization's backup ecosystem (see Figure 1).

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

Best Practices

Although ransomware can cause serious damage to your business and reputation, it's not invincible. In fact, it's only as strong as your organization's weakest link. The good news is that there are clear steps your organization can take to avoid becoming a cybercrime target and diminish the likelihood an attack could take down your business.

NIST developed a recommended Cybersecurity Framework that helps organizations put in place 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 and Prompt System Updates

- Reduce vulnerability exposure by staying up-to-date 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)

Zero Trust Model and Policies

- Develop a mindset where no device or user is trusted by default, even if they are inside the corporate network
- Instead of just requiring a password (yes, even if it's long and complicated), use identity and access management by implementing role-based access control (RBAC) and two-factor authentication (or multi-factor authentication, MFA) to limit access to only required functionality for each persona and prevent account takeover from using a single credential
- Always require users to log in with their own credentials
- Never use factory passwords anywhere. Change built-in generic user IDs and passwords, including the host 'admin,' 'maintenance,' RMM 'sysadmin,' and 'nbasecadmin' accounts
- Limit or lockdown access to backups, which is a common entry method for ransomware and another pair of 10/25 Gb Ethernet ports for client-facing data protection traffic.

Immutable and Indelible Storage

One of the best ways to safeguard your data against ransomware is to implement immutable (can't be changed) and indelible (can't be deleted) storage with an internally managed compliance clock.

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 and Network Segmentation

- Follow security implementation guides
- Harden your environment by enabling firewalls that restrict access to ports and processes
- Update the default Primary Catalog backup policy
- Set up a backup policy for the NetBackup Key Management Server (KMS)

Deployment and the 3-2-1 Backup Strategy

- Adopt the "3-2-1" best practice approach of backing up data recommended by the U.S. Cybersecurity and Infrastructure Security Agency (CISA): keep three copies of data on two different media types, with one off-site. We recommend taking this approach one step further creating a 3-2-1-1 strategy, by keeping at least one copy on immutable and indelible storage (see Figure 2).
- Use Auto Image Replication (AIR) technology to replicate to target domains.

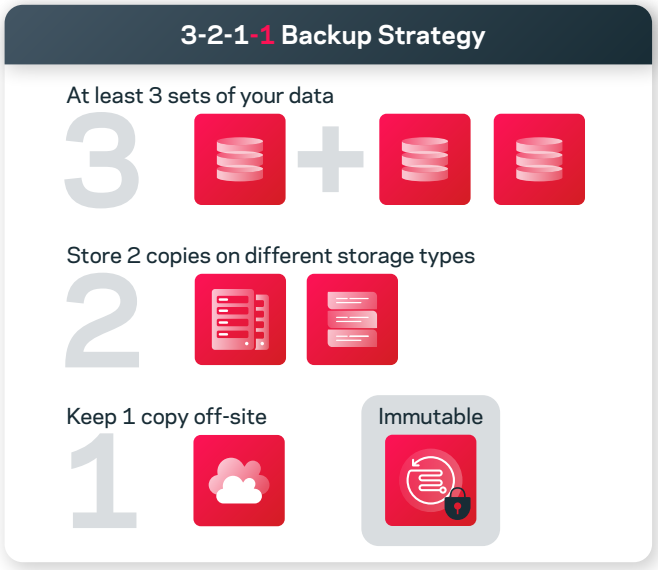


Figure 2. Keep three copies of data on two types of storage, with one copy off-site and one on immutable storage.

Complete Endpoint Visibility

Most organizations have a severe lack of visibility into remote endpoints. It has now become a common practice for bad actors to get past frontline security and hang out, staying dormant long enough to locate weaknesses and find the opportune time to attack. It's vital you implement tools that provide complete visibility across your full environment, detect anomalies, and hunt for and alert you to malicious activity on your network, giving ransomware no place to hide. This approach will help you mitigate threats and vulnerabilities before bad actors have the chance to act.

Optimize for Rapid Recovery

Most ransomware attackers hope for two things: time for the attack to spread and money (from you) to make it stop. Historically, recovery could take weeks or even months when it was a manual, labor-intensive process that extended across multiple stakeholders within an organization. Now, recovery can be orchestrated and automated with flexible and alternative options—like rapidly standing up a data center on a public cloud provider—that can shorten downtime and provide alternatives to paying a ransom. With the right systems in place, your organization's recovery times can be reduced to seconds, if necessary.

Frequent and Diligent Rehearsals

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 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.

Educate Employees

It's common knowledge that employees are often the gateway for an attack. Modern phishing attacks and social engineering are now so advanced they often fool security professionals.

Focus on training employees to identify phishing and social engineering tactics, build strong passwords, browse safely, use MFA, and always use secure VPNs, never public Wi-Fi. Also ensure all employees know what to do and who to alert if they fall victim.

Our Strategy: Protect, Detect, Recover

Veritas empowers our customers to protect, detect, and recover from attacks with a broad range of product features and functionality they can customize to meet their 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 step to ransomware resiliency is to ensure your critical and most important asset—data—and your IT infrastructure is protected from the unknown and unexpected. Make sure all parts of your environment—from physical and virtual to cloud and containers—are backed up with universal protection that is applied intelligently and managed automatically to scale properly. Then your backup infrastructure and backed-up data become the last line of defense from an attack, and ultimately your organization's key to recovery. Veritas offers the widest support from edge to core to cloud, with 800+ data sources, 1,400+ storage , and 60+ cloud providers, so your environment is always protected and always recoverable.

Cloud, database, and virtual machine (VM) administrators save a lot of time using Intelligent Policies that automatically detect and protect an application or compute instances with the appropriate level of protection.

Veritas focuses on safeguarding data integrity to help ensure backup files remain safe and untouched from malicious invaders. To maintain data integrity, we offer a wide range of security controls to help with data protection.

Identity and Access Management

- **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 3).
- **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.

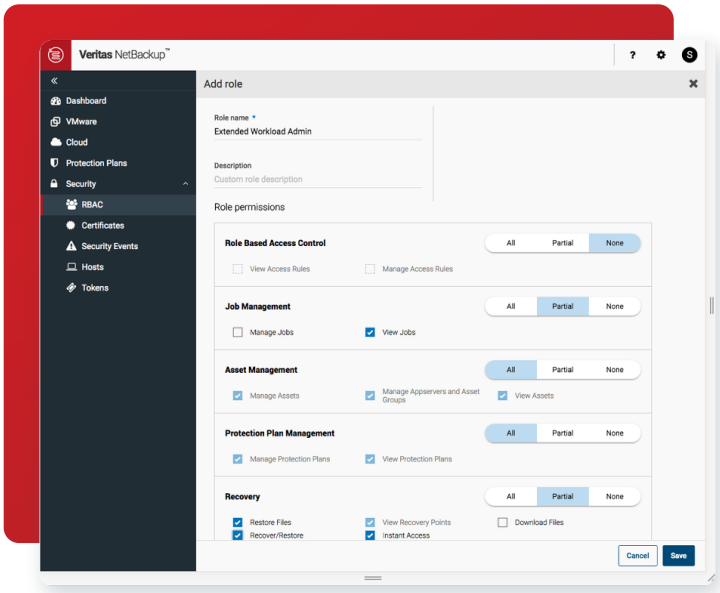


Figure 3. The access permissions dashboard in NetBackup.

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 attackers are successful in getting to your 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 you to leverage your preferred key management using the Key Management Interoperability Protocol (KMIP).

Immutable/Indelible Image Management and Storage

- Flexible, storage-agnostic image management
  - Flexible options, including BYO, Appliance, cloud, and software as a service (SaaS) immutability keep your data secure and compliant, regardless of location.
  - The OpenStorage Technology (OST) API lets you 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.
  - Use cloud immutable storage with Amazon 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.
  - NetBackup Flex Appliance deployment provides both immutable and indelible storage.
- Images stored in WORM (write once, read many) storage
  - NetBackup Flex includes 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 4).

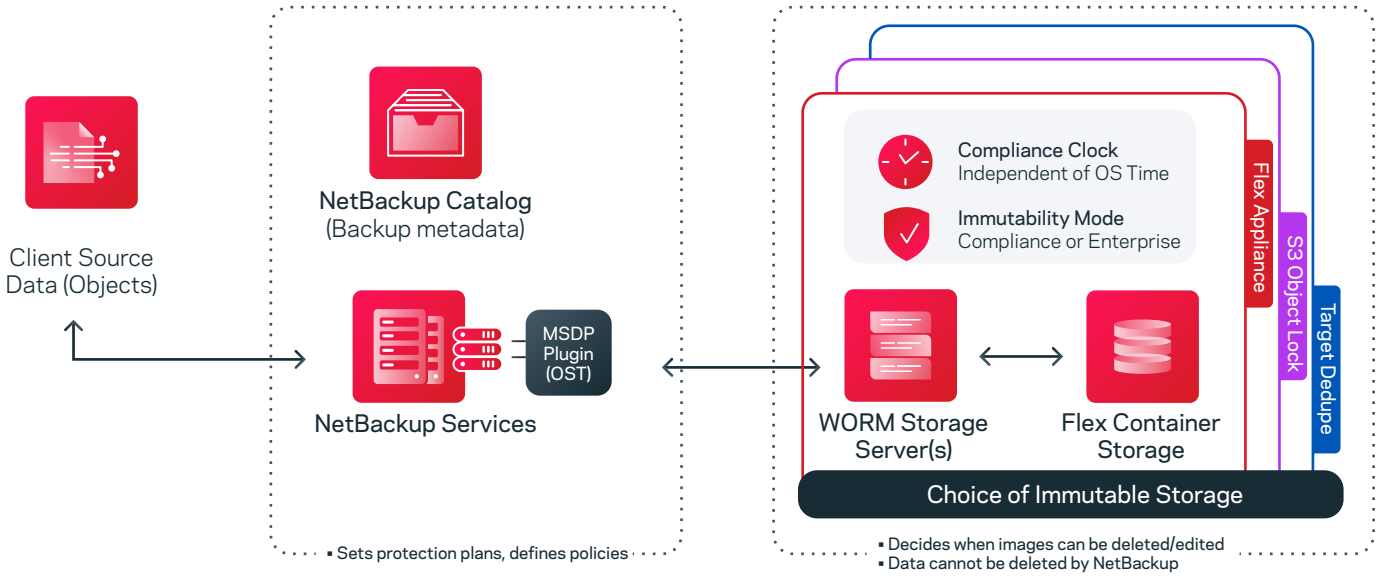


Figure 4. An overview of immutable storage options in NetBackup.

  - Compliance mode enables immutable storage, in which no user, including the root user, can delete data during a predefined retention period.
  - Enterprise mode protects 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 data.
  - 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©, and the principles of the 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 and NetBackup Flex Scale have 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 and Flex Scale code for vulnerabilities using recognized third-party detection tools that perform:
  - Static code analysis
  - Runtime vulnerability checks
  - Penetration testing
- NetBackup Flex and Flex Scale come with a wide variety of security features that include:
  - OS security hardening, including Security-Enhanced Linux (SELinux)
  - Intrusion Detection System (IDS)/Intrusion Protection System (IPS)
  - Robust role-based authentication
  - Locked-down storage
  - 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

Bad actors are looking for your weakest links, the dark corners where there may be limited security and/or oversight in your environment. Veritas offers solutions that provide full infrastructure awareness, shining a light on all the dark data in your environment, ensuring you know everything in your environment and it is all safe, secure, and capable of overcoming the threat of ransomware. Veritas also offers anomaly and malware detection that provides a valuable chance to act before cybercriminals or malicious code has the opportunity to do so.

Backup and Storage Infrastructure Awareness

When it comes to ransomware, every second matters. Veritas Alta™ Analytics for cloud and NetBackup IT Analytics for on-premises can help your company understand the breadth and depth of a ransomware attack so you can recover strategically. With the correlated environmental insights of NetBackup IT Analytics—on-prem, in the cloud, data protection, and storage—alerting and reporting is comprehensive and easy to set up. You'll have the insights needed to make informed decisions in the face of an attack with these analytics reporting options that help you gain visibility into your backup environment, enabling your organization 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 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

NetBackup Analytics provides end-to-end backup monitoring that includes:

- Mitigation Analysis (see Figure 5)
- Sources with Consecutive Failures
- Sources with No Recent Backup
- Backup Failures by Application

NetBackup Analytics 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.

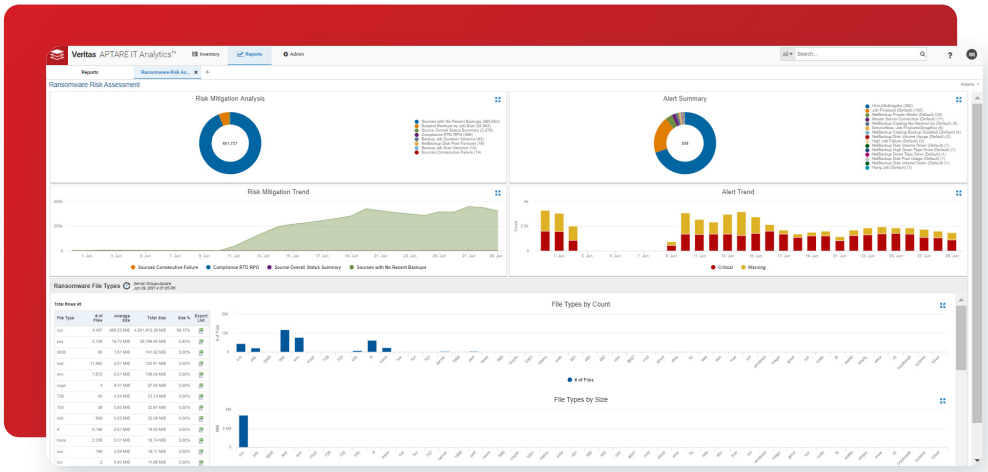


Figure 5. The ransomware risk assessment dashboard in NetBackup IT Analytics.

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

Anomaly Detection

Veritas detects strange data and user activity across your entire environment and alerts you to suspicious anomalies in near real-time using AI-powered anomaly detection with Veritas Alta™ Data Protection for cloud and NetBackup for on-premises. The technology is able to mine an enormous amount of data, automate monitoring and reporting, and provide actionable insights into what is happening in your environment. Alerts could be things like unusual file write activity that could indicate an infiltration, but it could also be detecting known ransomware file extensions, file access patterns, traffic patterns, code downloads, access requests, storage capacity surges, external traffic paths, or even an unexpected jump in activity compared to individuals' typical patterns.

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. Veritas solutions give administrators the ability to view data and provides recommendations associated with anomalies at any time by monitoring all your devices and establishing early warning of any attacks, so you can stay on top of issues as they arise.

AI-powered anomaly detection seamlessly integrates into the NetBackup Primary server, enabling it to detect anomalous forms of observations—considering those that do not fall into the cluster as anomalies or outliers. This capability lets a backup 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 with which an administrator should be aware (see Figure 6).

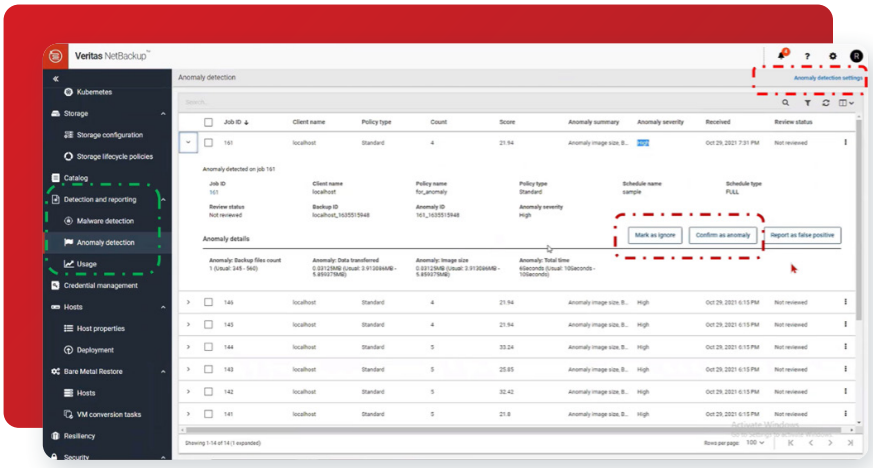


Figure 6. Use NetBackup to detect anomalies and take action accordingly.

To learn more about anomaly detection capabilities, see the Veritas Anomaly Detection technical brief.

Primary Storage Detection

Veritas not only addresses secondary backup data with NetBackup, but also primary storage—where the application lives—with Veritas Alta™ Data Insight for cloud and NetBackup Data Insight for on-premises. Data Insight supplements existing security detection tools by providing anomalous behavior detection, custom ransomware-specific query templates, and file extension identification useful for detecting 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 7).

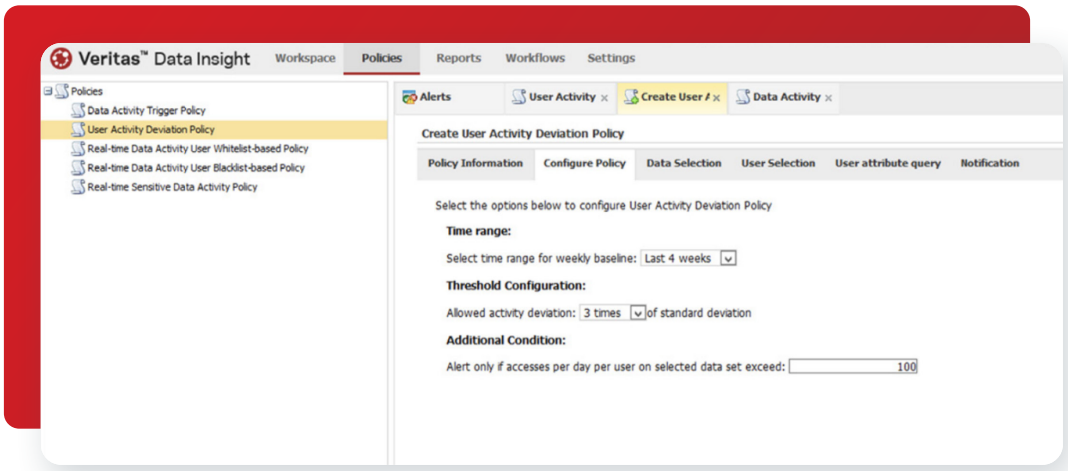


Figure 7. Setting up a User Activity Detection Policy in Data Insight.

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.

Malware Detection

Veritas provides both automated and on-demand scans for protected backups. The automated malware scanning feature will remove human dependencies and allow artificial intelligence/machine learning (AI/ML) technology to jump in and scan for malware. The malware scan is automatically triggered by a high anomaly score. Scanning includes unstructured data, both Windows and Linux. This inclusion is vital because malware often enters your environment in a home directory because these are typically the locations where large sets of unstructured data exist.

When recovery is necessary, the backup data is scanned. Clear visuals and warning prompts provide awareness of impacted backups, ensuring all data restored is clean and unimpacted. This practice is often referred to as restoring to the "last-known-good" copy. (See Figure 8.)

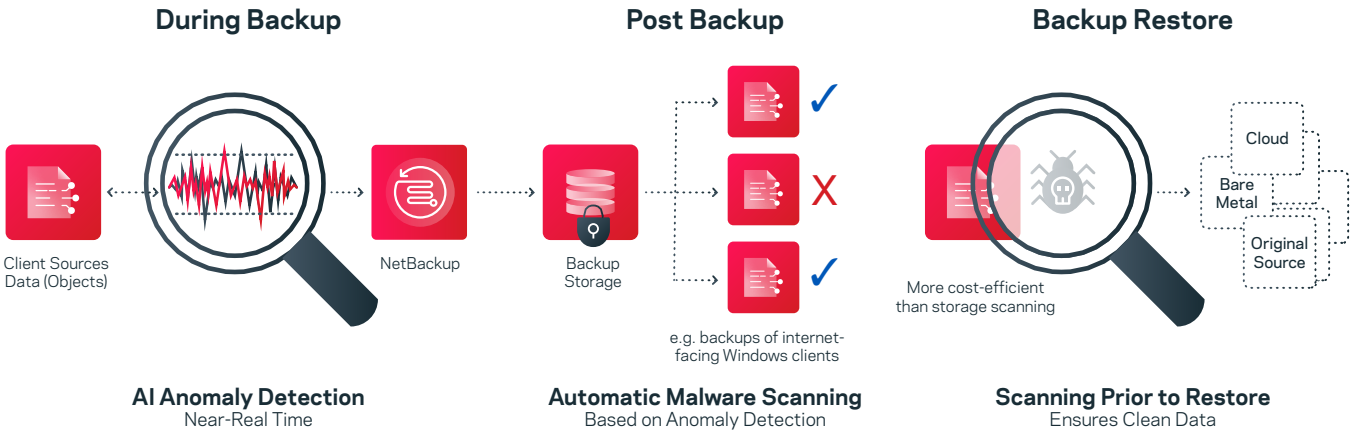


Figure 8. A high-level overview of malware detection in NetBackup.

Recover

Cyberattacks are never one-size-fits-all. In today's ever-evolving threat landscape, it is vital to set up an optimized strategy that extends far beyond restore points and single backup copies. Architecting an optimized and simplified recovery experience will help you get back up and running in minutes instead of hours and days, regardless of scale.

Traditionally, organizations have considered backup and recovery to be the last line of defense, but with Veritas solutions, environments are optimized for recovery and it becomes an essential component in resiliency success. Veritas provides a variety of solutions that ensure operational and business resiliency by providing the flexibility and choice necessary for rapid recovery. Why is that flexibility important? Sometimes everything is impacted and you may need to recover an entire data center in the cloud and on demand. On the other hand, maybe just a portion of your environment is impacted, so having solutions in place that let you grab individual databases and files to recover quickly to production can be crucial. In the case where entire servers become encrypted, you may need to quickly recover those servers elsewhere. Or maybe you just need to recover a large number of VMs back to production.

Veritas provides solutions to the recovery at-scale complexities shown in Figure 9.

Recovery at-scale complexities

Heterogeneity

Mixture of compute environments across data centers from edge to core to cloud. (Physical, Virtual, Cloud, Hybrid, Tape)

Flexible, hybrid and rapid recovery. Recovery not always possible back to original or scaling from object level to data center recovery.

Cost effective, non-disruptive recovery rehearsals Increased productivity and reduced downtime.

Dependencies

Management of complex infrastructure, networks, storage and cross-functional teams. (on-prem, hybrid, cloud)

Multi-component tiered applications. Recover from clean data, anywhere to anywhere. (edge to core to cloud)

Can be a time-consuming, laborious, manual process. Education and skills gaps.

Figure 9. The recovery at-scale complexities Veritas solutions address.

Veritas Resiliency Platform

Veritas Resiliency Platform solves these recovery challenges by providing automated orchestration across your organization's entire heterogeneous environment with a consistent user experience and visibility into the best recovery options based on the options available, so you can meet your recovery time objective (RTO) and recovery point objective (RPO). (See Figure 10)

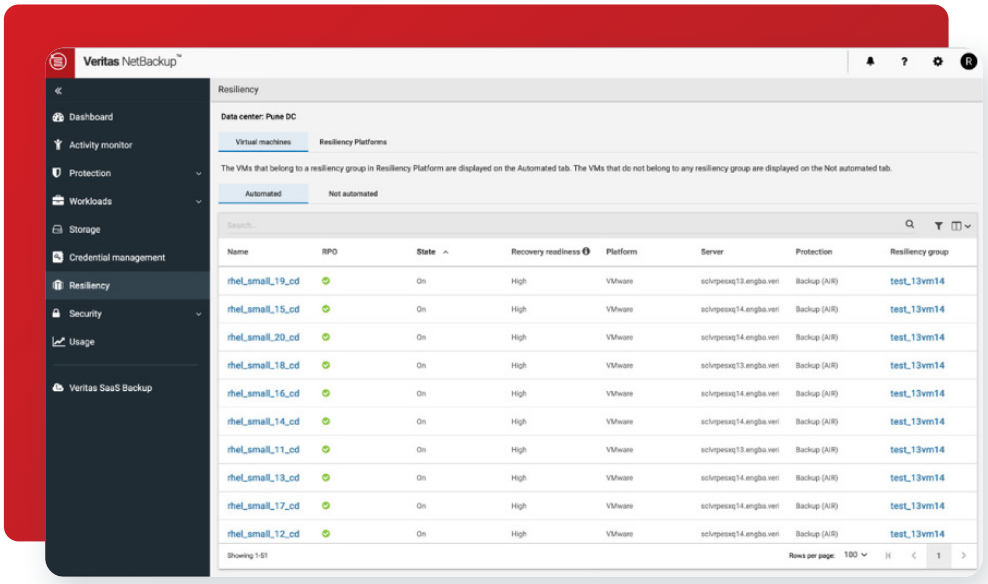


Figure 10. The Resiliency dashboard in the NetBackup web UI.

To achieve the most efficient RTO, Veritas provides insight into recovery operations that helps determine the best method of recovery by understanding your RTOs, workload(s), and application(s) throughout your entire data center.

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

Specifically, the solution supports automation by leveraging Virtual Business Services (disaster recovery protection for a multi-tier 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 for on-premises and Veritas Alta™ Data Protection for cloud continuous data protection (CDP) provides added resiliency through granular recovery of 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 11). This capability supports recovery from malware or corruption when it's already been replicated.

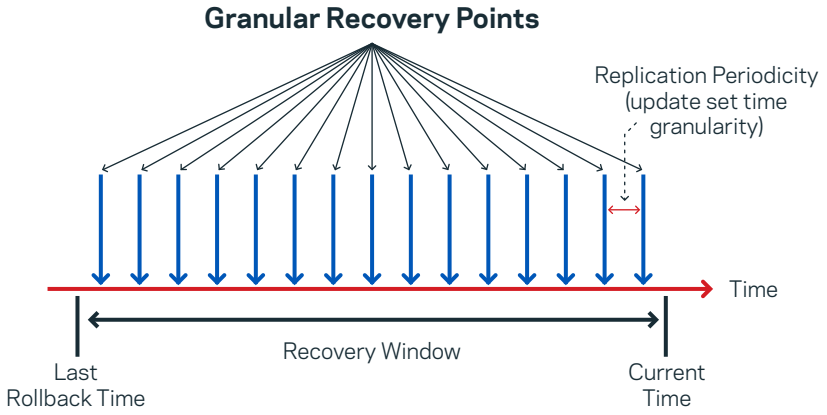


Figure 11. An overview of NetBackup's continuous data protection.

Learn about more about Continuous Data Protection for VMware and advanced resiliency options for VMware application protection by reviewing the 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 12 illustrates the optimal recovery option based on RPOs and RTOs.

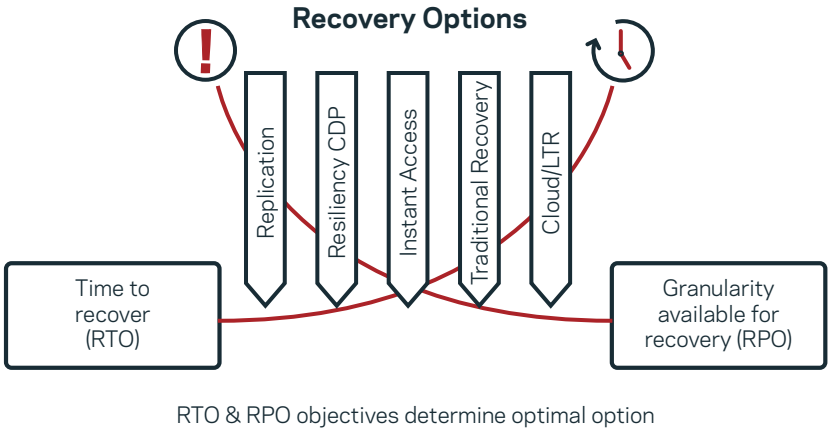


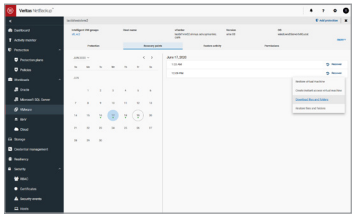
Figure 12. Choosing an optimal recovery option based on RTOs and RPOs.

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.

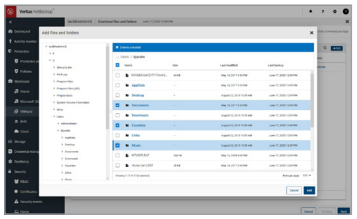
For more information on Instant Rollback for VMware, read this blog.

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.

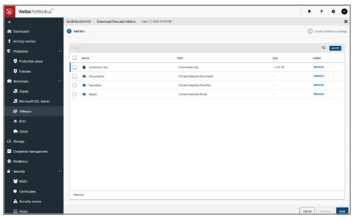
Instant Access for MSSQL and VMware—With Instant Access for VMware, you can recover any machine almost instantly, without waiting to transfer the VM's data from the backup (see Figure 13). You can also use a backup to test or recover VMs directly from backup storage. These VMs will automatically show up as regular guests in the VMware infrastructure. In addition, you can browse and recover individual files right in the NetBackup web UI. For quick recovery scenarios, you can use VMware Storage vMotion to migrate the VM from backup storage to production while in use.



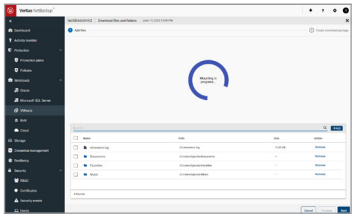
Browse available recovery points for a protected VMware Virtual Machine



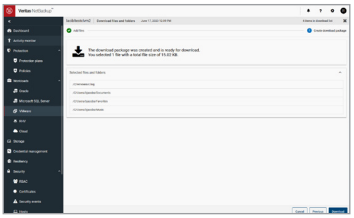
Select the files or folders to recover



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 13. 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 backup storage (see Figure 14). 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 15).

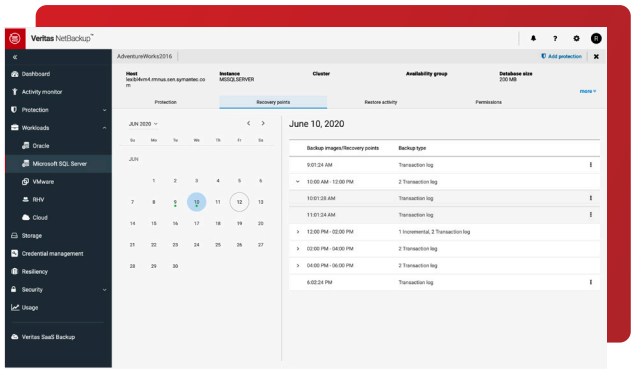


Figure 14. NetBackup provides granular point-in-time recovery options for MSSQL.

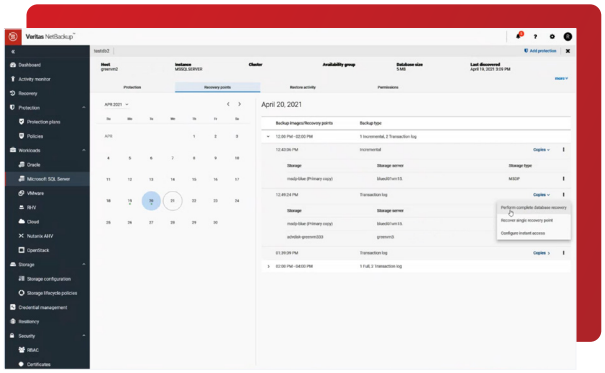


Figure 15. Recover databases from any copy of an MSSQL backup.

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

Universal Share and Protection Points—An MSDP feature, Universal Share 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 network-attached storage (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 that let you 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.

NetBackup Universal Shares for Oracle—Building on the features of Oracle, the latest version of NetBackup Universal Shares for Oracle 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 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 long-term retention (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 way 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—If a ransomware recovery needs to leverage impacted hardware, bare metal restore (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

Our 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 competitors, 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.

Here are some key questions 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 3-2-1-1 backup copy rule in every scenario?

Veritas can do all the above and more:

- Offers multiple deployment options and the ransomware resiliency remains available for any enterprise deployment scenario
- Takes a multi-layer security approach for protecting backup data, closing back doors such as cluster resets, external clocks, or BIOS
- Uses a hardened OS to reduce the attack surface of ransomware
- Designs solutions from the 3-2-1-1 best practices, providing copy standard for tape support, immutable storage, and air gap
- Creates appliances with hardened containerized deployments, making it even tougher 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 to rollback only changes to VMs from ransomware attacks, making recovery from ransomware efficient and quick

At Veritas, we understand the vital nature of resiliency. Consider two types of security systems monitoring a facility: one only looks at the history of security footage to identify intrusion, and the other looks at the live feeds from the monitoring as well as the historical footage. The system that looks at the live feeds also can disable access to the facility if it finds signs of intrusion. Which system do you think is better? Veritas offers ransomware detection by monitoring production systems. This monitoring goes beyond size and extensions while covering data and infrastructure. It can detect deviations in data access patterns and can lock down accounts that might be used to run any ransomware/malware. By analyzing changes in backup attributes using AI/ML, Veritas Alta™ Data Protection for cloud and NetBackup for on-premises can alert organizations about possible ransomware intrusions.

We recognize the need for data to be recovered in the most efficient and fastest way possible. NetBackup offers features such as instant rollback recovery, providing the ability to negate any damage done by ransomware without needing full VM restores and shutdowns. Veritas Alta™ Data Protection for cloud and NetBackup for on-premises 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. NetBackup Flex and Flex Scale Appliances show some of the best-in-class numbers of optimized instant access and restores of key workloads. Veritas Alta™ SaaS Protection (formerly known as Netbackup Saas Protection) is also proven to handle petabyte-scale recoveries. All of these are key research points when comparing the completeness of Veritas ransomware resiliency to that of any competitor.

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 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), 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"

Veritas

- "Insider Threat 101: Detect and Protect with Veritas Data Insight"

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

- About Data Insight custom reports
- About DQL query templates

- Veritas Flex Appliances with NetBackup Security
- Veritas Flex Appliances with NetBackup
- Veritas Data Insight Administrator's Guide
- Veritas Data Insight User's Guide
- Veritas NetBackup Administrator's Guide, Volume I
- Veritas NetBackup Appliance Administrator's Guide
- Veritas NetBackup Appliance Fibre Channel Guide
- Veritas NetBackup Appliance Security Guide
- Veritas NetBackup Cloud Administrator's Guide
- Veritas NetBackup Deduplication Guide
- Veritas NetBackup Security and Encryption Guide
- Veritas NetBackup for Oracle Administrator's Guide
- Veritas NetBackup for VMware Administrator's Guide

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

About Veritas

Veritas Technologies is a leader in multi-cloud data management. Over 80,000 customers—including 95 percent of the Fortune 100—rely on Veritas to help ensure the protection, recoverability, and compliance of their data. Veritas has a reputation for reliability at scale, which delivers the resilience its customers need against the disruptions threatened by cyberattacks, like ransomware. No other vendor is able to match the ability of Veritas to execute, with support for 800+ data sources, 100+ operating systems, 1,400+ storage targets, and 60+ clouds through a single, unified approach. Powered by Cloud Scale Technology, Veritas is delivering today on its strategy for Autonomous Data Management that reduces operational overhead while delivering greater value. 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

Copyright © 2022 Veritas Technologies LLC. All rights reserved. Veritas, the Veritas Logo, and NetBackup are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

V1726 01/23