VERITAS™

Ransomware Protection with Veritas NetBackup™ Appliances

Using Veritas NetBackup & NetBackup Appliances to protect against and recover from ransomware attacks.

Veritas™ White Paper | August 2020

Contents

INTRODUCTION

Executive Summary

Ransomware and ransomware attacks are a top concern for enterprise customers today. Spear phishing works. Ransomware is big business and attackers are relentless in their pursuit to develop new, creative ways to infiltrate corporate networks and IT environments to seize data and hold it hostage. The key is to be resilient and to be able to restore at scale. Enterprise customers also want to leverage the cloud, using a hybrid approach that combines on-premises infrastructure with multiple cloud storage vendors.

NetBackup Appliances provide a simple, performant and secure backup solution. As a comprehensive data protection solution, you can use NetBackup Appliances to help protect against the potential attack of backup and recovery infrastructure and quickly recover production environments from such attacks. This allows companies to stay focused on their daily business instead of focusing on managing infrastructure. NetBackup Appliances have been designed and optimized to bring you the best data protection and recovery tools available combined with integration with multiple cloud vendors.

Scope

The purpose of this document is to provide an overview of the ransomware and malicious insider problem, the basics of how ransomware works, as well as to provide a detailed description about how businesses can best protect themselves and recover from a ransomware event using Veritas NetBackup Appliances. Some general guidance and best practices are included, though this document should not be considered as a comprehensive best practices or implementation guide.

WHAT IS RANSOMWARE?

Malware is a general classification for a type of malicious computer software that is intended to harm a computer by causing it to malfunction or to delete its data. Malware is broken down into a few different types: viruses, trojan horses, worms, spyware, and adware. These types are, for the most part, beyond the scope of this paper. Ransomware is also a type of malware and what makes this specific type of malware unique is that it is designed to either lock access to a computer system or to encrypt the data on a computer. Ransomware can also take advantage operating system vulnerabilities and spread to other systems. Then, the individual will demand a ransom to relinquish access to and control of the system or to decrypt the data. The cyber-criminals are often many miles away, in other countries, and demand non-refundable, untraceable payments in the form of bitcoins, other online currencies or by asking for the numbers from gift cards such as Apple iTunes, Google Play and other cards which can be converted into cash and merchandise by the perpetrators. There is often no digital evidence and way to trace the criminals, let alone recover any money that might have been paid in ransom. And there is no guarantee that the data will be decrypted in full or in part by the perpetrators once a ransom is paid. As has been reported in the article titled The Untold Story of NotPetya, the Most Devastating Cyberattack in History, the ransomware attack that happened to Maersk cost over $10 billion in total damages.

Ransomware and Encryption

There are two kinds of ransomware encryption. One type will have keys and these keys, required to decrypt the data, will be held for a ransom. With the other kind of encryption used, there are no keys. What makes this type of encryption particularly malicious is that a random key generator is used to generate unique keys for each file and no digital record is kept of the keys. Even if a ransom is paid, the data cannot be decrypted. The data is left essentially inaccessible with no way to decrypt the files, requiring a complete restore from backup.

Ransomware can find its way into an enterprise through many vectors. It could be via spear phishing, a malicious web site or an infected thumb drive.

Malicious Insider

While not malware or even ransomware per se, the malicious insider poses a similar threat to critical company data. This is where a person with access to sensitive data inside of a company deletes data or perhaps even encrypts or moves the data to another location and then demands a ransom. What makes a malicious insider attack particularly heinous is that the insider may not even need to use malicious code or encryption. The malicious insider may just be destructive without demanding a ransom.

Ransomware in the News

The threat of ransomware is constant and ever-growing because the crimes can be committed from a location almost anywhere in the world and the cyber criminals can easily hide their digital and monetary tracks. There is no shortage of news articles revealing the latest victims of these crimes. These articles are specifically on the topic of ransomware that uses encryption.

- The Untold Story of NotPetya, the Most Devastating Cyberattack in History
- Atlanta Spent $2.6M to Recover From a $52,000 Ransomware Scare
- Scottish brewery recovers from ransomware attack

Cryptocurrency and Ransomware Negotiators

Something else to consider is the fact that new companies have come into existence to serve as cryptocurrency ransom negotiators who attempt to negotiate a lower ransom fee. Some companies have even chosen to purchase and maintain a small stockpile of cryptocurrency just in case a ransomware attack occurs. If nothing else, these examples should serve to demonstrate just how large the problem of ransomware really is.

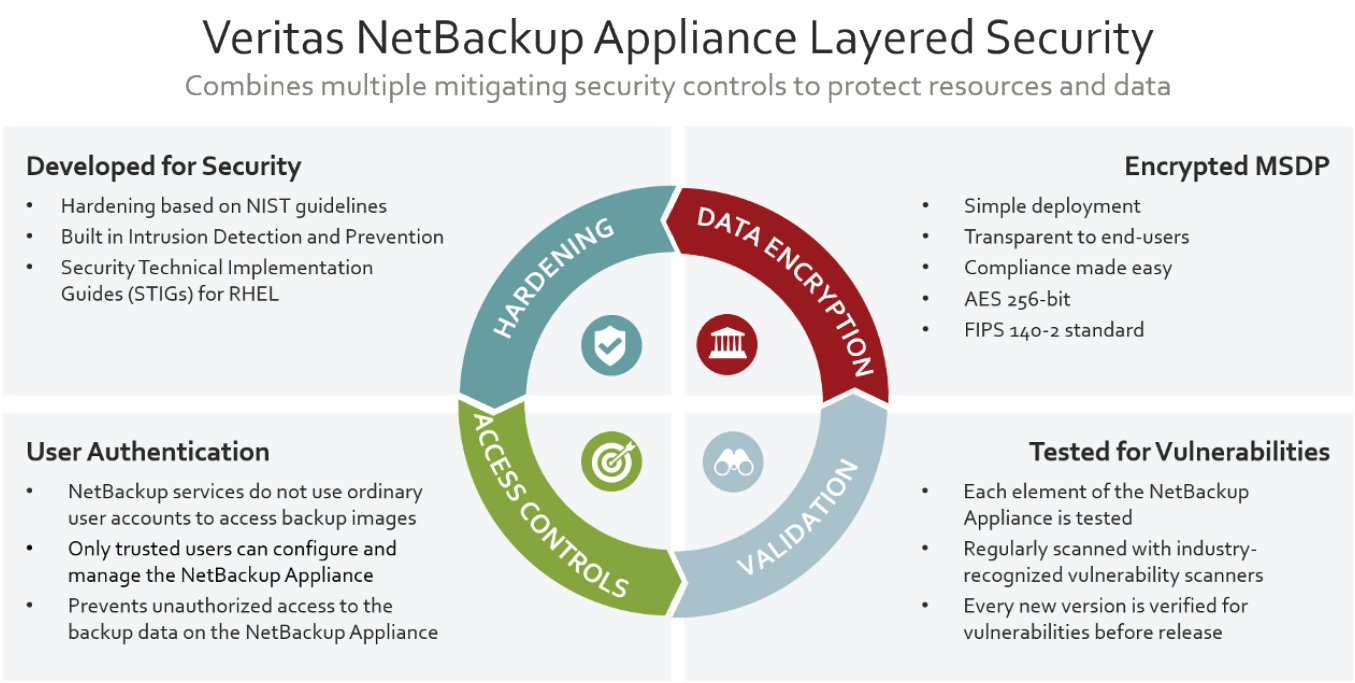
- Negotiating Bitcoin Ransomware With Cyber-Criminals as a Service

How can companies protect themselves against cyberattacks and recover in case of a successful attack?

A CASE FOR NETBACKUP APPLIANCES

Multi-Layered Security

NetBackup Appliances combine an optimized version of NetBackup along with integrated, multi-layered security to help provide maximum protection against ransomware and malicious cyber activity.



Developed from Inception for Security

STIGS, or "The Security Technical Implementation Guides," are based on rules created by the Defense Information Systems Agency (DISA). They provide technical guidance for increasing the security of information systems and software to help prevent malicious computer attacks. Using STIGs for security is also referred to as "hardening." NetBackup Appliances include the OS STIG built-in.

Enabling STIG on the appliances is a requirement by the United States Federal Government for government systems. The STIG support is enabled via the command line interface; once enabled it cannot be disabled.

Please see the Veritas NetBackup Appliance Security Guide for details on how to enable it.

Symantec Data Center Security

Symantec Data Center Security (SDCS) is embedded into every NetBackup Appliance. It is configured to automatically startup with the appliance and requires no management. SDCS provides industry leading, agentless intrusion prevention and intrusion detection built-in and requires no expertise, setup or configuration is needed to get started. Most ransomware attacks may be prevented by SDCS. It offers very strong protection against disk-encryption-type attacks and could potentially stop the general destruction or encryption of backup data files.

Encrypted MSDP

To minimize network bandwidth, infrastructure and the amount of data stored, NetBackup Appliances include data deduplication options built-in. When NetBackup clients backup their data to a NetBackup Appliance, the data is sent a Media Server Deduplication Pool, (MSDP). After the data it is deduplicated, it can also be encrypted for greater levels of security. The encryption ensures the data is encrypted at-rest, so the data cannot be read except by using NetBackup. When enabled, MSDP provides AES 256-bit encryption and meets the Federal Information Processing Standard Publication 140-2 (FIPS PUB 140-2) requirements for the data written to the storage media (FIPS is not enabled by default and needs to be manually enabled, in addition to MSDP). Access to the encrypted data within the MSDP requires a unique key and these internal segment encryption keys are auto-generated.

It should be noted that the encryption used by ransomware is different from the encryption used in the MSDP. The MSDP encryption will not affect deduplication rates like ransomware encryption does. More about this unique scenario is discussed later in the section on NetBackup OpsCenter.

For more detailed information in MSDP and MSDP encryption, please see the Veritas NetBackup Deduplication Guide.

User Authentication

With included role-based access (RBAC), access to resources on the appliance is restricted. Only the users that are assigned the Administrator role are authorized to configure and manage the NetBackup Appliance.

Unlike many other backup products, NetBackup services do not use ordinary user accounts to access backup images. NetBackup services run under non-interactive accounts. These kinds of accounts are not used to check email or access external websites, providing a sandbox from the application layer, and are therefore inherently safer.

Tested for Vulnerabilities

NetBackup Appliances were developed from their inception with security in mind. Each element of the appliance, including its customized Linux operating system and the core NetBackup application, is tested for vulnerabilities using both industry standards and advanced security products. Unnecessary packages have been removed from the appliance to minimize the surface area that allows for a malicious attack. These measures help ensure that that exposure to unauthorized access and resulting data loss or theft is minimized.

Each new version of NetBackup Appliance software and hardware is analyzed for vulnerabilities before release. Depending on the severity of issues found, Veritas releases a patch or provides a fix in a scheduled major release. To reduce the risk of known threats, Veritas periodically updates the third-party packages and modules in the product.

Each version is tested during three different test phases, using a variety of state-of-the-art software development tools.

- **Static Code Analysis**: Software code is analyzed for defects during development cycle using tools like FindBugs™, PMD and Coverity®.
- **Runtime Vulnerability Checks**: Every version of runtime code is tested by multiple vulnerability scanners such as Nessus®, Qualsys®, Trustwave® and OpenSCAP
- **Third Party Penetration Testing**: Penetration testing of the appliance's interfaces is performed by external vendors. Veritas regularly updates the third- party packages and modules in the product as part of regular maintenance release cycles.

Disclaimer: While Veritas employs an array of tools throughout the software development cycle, it does not promote or make specific recommendations for these tools.

DEFENDING AGAINST RANSOMWARE AND MALICIOUS INSIDERS

Prevention, Detection and Recovery

There are three stages of defense against malicious activity, namely: prevention, detection and recovery. Malicious activity will test an organization's defense mechanisms and resiliency at all three stages. The best protection is to employ all available options at all three of the stages and to practice recovery procedures for the best outcomes in case of successful attacks.

Prevention

The intent of the prevention stage is to keep malicious insiders and software out of the systems and network. There are several strategies that IT organizations should use. One of the most important things that administrators should do is to make sure that they stay abreast of new security patches for all network and computer systems and keep them up to date. Ransomware often exploits security vulnerabilities on out of date, un-patched systems. While not a comprehensive list, organizations should implement most of if not all the following additional strategies to minimize threats:

- Securing physical access to production data systems and especially backup and recovery systems
- Securing network access with firewalls and by minimizing port usage
- Implementing user security and role-based access
- URL and email attachment filtering
- Practicing disaster recovery procedures
- Having security awareness training

Organizations should define Service Level Agreements (SLAs), between the IT group and the end user communities, that spell out the services and levels of service that the IT group will provide. Those definitions should include the Recovery Point Objective (RPO) and the Recovery Time Objective (RTO) is defined. Different data types such as databases, virtual machines and user home directories will often have different RPO and RTO requirements. There are numerous backup and recovery options that can be used, and it will be the RPO and RTO that influence the best option to take. A large part of prevention is defining the recovery stage up front and practicing the recovery procedures on a continuing basis. The recover stage is discussed below.

Detection

The detection stage is for rapidly detecting of suspicious activity. Like the prevention stage, the detection stage requires a multifaceted approach. Most, if not all, of the following services should be implemented in a data center for the most compressive protection:

- Endpoint protection for user systems
- Enterprise virus protection for servers
- Intrusion detection
- Known malware detection
- Network port monitoring
- Central logging for event correlation
- Data pattern-detection (see OpsCenter below)

With quick detection of malicious activity, the activity can be contained or stopped before it spreads to other systems and cause further harm. Infected systems should be quarantined immediately, then remediated and restored.

Recovery

When the prevention stage fails to deflect malicious activity and evidence of it is identified in the detection stage, it is the recovery stage that will need to be relied upon as a last resort for rapid and reliable recovery of a wide range of data types. This is the time when administrators rely heavily on their backup and recovery software and recovery procedures. Data will need to be restored quickly. Maintaining offsite copies of data and backups via tape or Veritas Access Appliance, also known as air gaps, is also part of the recovery stage because it may be these off-site copies that are used for recovery.

PREVENTION: TAKING STEPS TO LIMIT AND PREVENT DATA LOSS

Beyond having a highly secure backup and recovery appliance, there are additional implementation options and tools that should be used to maintain the highest levels of backup data protection. This section discusses additional prevention strategies that backup administers can take for configuring their backup environments as well as third party tools that can be used in the prevention and detection stages.

Strengthening the Prevention Stage of Ransomeware Protection

To better protect data from attack, additional backup copies of the data should be created and stored on different media types and at different locations. These steps will help prevent all data from being exposed to loss.

The 3-2-1 Rule

Aimed at a broad range of computer users, from home users to professionals, the United States Computer Emergency Readiness Team (US-CERT) have produced a document titled Data Backup Options. In this document, it is recommended that all computer

users follow the "3-2-1" rule to safeguard their data. Following these simple rules allows administrators to better protect their data by increasing the chances of recovery. The rule is as follows:

3. Keep 3 copies of any important data: 1 primary and 2 backups.
2. Keep the data on 2 different media types to protect against different types of hazards.
1. Store 1 copy offsite (e.g., outside of the business facility).

Veritas NetBackup Appliances enable administrators to follow these recommendations easily with built-in support for multiple media types, off site copies (including cloud and remote site) and of course support for numerous backup copies of the data.

Off-Site Copies and Air Gaps

Ransomware and malicious insider activity can extend beyond the system that was initially exploited and subsequently infected by replicating itself over networks to other systems, potentially including critical backup servers. Even backup data and metadata could be wiped out, leaving no recovery point to restores from if security features are not implemented and used. A malicious insider that could gain access to production and backup systems can accomplish the same thing in person. With enough user access and security holes, an angry, intent insider can perpetrate the most heinous of malicious insider attacks. They could potentially erase every bit of data on every system that he or she can access to beyond the point of recovery. Sometimes, it can be that one last server, appliance or volume that was off line or inaccessible, for any reason, that saves the day with a copy of the data that was unavailable during the attack.

Backup administrators, wanting to maintain as many layers of protection as possible for their backup data, should be keeping off- site copies of the data and implementing air gaps for the most critical data. Malware, ransomware and malicious insiders may not have the required permissions to access remote systems that have copies of the data and will not be able to cross any air gaps that have been implemented.

The practice of maintaining off-site copies of backup data is one of the best ways that backup administrators can keep multiple copies of the data and to meet the recommendations put forth by US-CERN. With NetBackup's built-in replication features, more than three copies of data can be maintained and can be maintained at more than three different locations on different media types. There are two general ways that administrators can use to get copies of data off site. One is to copy or replicate the data to other systems over a wide area network. Another method is to physically carry the data from one location to another. With replication, there is still network access to the replicated data and malicious individuals or software could potentially still access it.

There is another layer of security that NetBackup Appliance and software administrators can take advantage of when configuring replication. When replicating data to other NetBackup Appliances or NetBackup domains, the security on the target devices is different and can be configured differently; thus, preventing access to the replicated data by administrators on the source site.

For the ultimate protection, access to copies of backup data needs to be completely prevented and with no electronic path. An air gap simply means that there is no path to access backup data or copies of backup data from the production network. As an added layer of protection, the data should be test restored periodically in an isolated environment to ensure that the data has not been damaged and the process is working properly. NetBackup Appliances enable the backup administrator to maintain off-site copies and implement air gaps through support for tape.

NetBackup to tape

The most widely used method to create an air gap is to perform a backup to tape and store the tapes off-site. This leaves no electronic path between ransomware and the backup data, providing an extra layer of defense. NetBackup Appliances have built-in support for fibre channel tape libraries.

Use tape to keep an additional copy of the most critical data. It is also recommended to perform regular tape backups of the NetBackup catalogs to protect those as well. If the NetBackup catalogs become inaccessible because of a ransomware attack, they would need to be reconstructed by reading every backup media back into NetBackup. This extra step at restore time will significantly lengthen the total time that it takes to recover. For this reason; it is important to keep tape backups of the NetBackup catalogs in case they, too, need to be recovered.

Tapes can be stolen or even destroyed if someone has physical access to them. Tapes also need to be secured such that the media itself does not degrade over time. When using tape as a backup media, store the media in secure, environmentally controlled locations that are off-site.

It is important to keep in in mind that when utilizing tape, it takes longer to back up and recover the data and SLAs should reflect the additional recovery time that it takes to restore.

For more information connecting tape libraries to a NetBackup Appliance, please see the Veritas NetBackup Appliance Fibre Channel Guide.

AWS Glacier Vault as WORM

NetBackup Appliances also include support for the cloud through Application Programming Interfaces (APIs) from Amazon Web Services (AWS), Microsoft Azure and OpenStack Swift. Furthermore, NetBackup Appliances provide long- term retention and Write-Once-Read-Many (WORM) support through AWS Glacier and the AWS vault lock policy.

Though originally intended for regulatory compliance, immutable storage is a very useful tool that can be employed at the protection stage as an additional layer of defense against the effects of ransomware. When data is written to an immutable storage system, it cannot be erased and will not change over time. In addition to production systems and data, critical backup systems and backup media can be vulnerable in severe ransomware and malicious insider attacks. Using immutable storage as a backup target for critical data adds a significant layer of protection to the backup data.

Administrators can create vaults in the AWS cloud using Glacier and the amazon lock policy. Once this is done, the NetBackup Appliance can be configured to use the GLACIER_VAULT storage class for backups, thus turning it into a WORM device.

Administrators should be aware of the caveats that come with using AWS Glacier, in general, and when using it for WORM. First, due to the nature of the underlying storage, data recovery will take longer when recovering from AWS Glacier as compared to recovering from other media sources. Also, since data is retained and not often removed, there will likely be higher costs associated with the additional storage overhead.

For more information on configuring and using AWS Glacier Vault, please see the Veritas NetBackup Cloud Administrator's Guide.

Tier to Cloud with a NetBackup Cloud Catalyst Appliance

NetBackup CloudCatalyst uses MSDP deduplication technology to upload deduplicated data to the cloud. The data is uploaded by the CloudCatalyst-enabled MSDP cloud storage server, which first stores data in a local cache before uploading it to cloud storage. When configured for CloudCatalyst, all the appliance's available internal storage is allocated as MSDP cache space. A single NetBackup 5240 CloudCatalyst Appliance supports a cloud storage bucket of up to 1 Petabyte in size.

Using the cloud is an excellent method to maintain copies of data off-premises. At the same time, there is still an electronic path to the data which makes it less protected than with other options such as tape or AWS Glacier Vault.

For more information on CloudCatalyst, please see the Veritas NetBackup Deduplication Guide.

NetBackup AIR

Another method for creating off site copies of data, is to use NetBackup Auto Image Replication (AIR). Backups that are generated on a NetBackup Appliance in one NetBackup domain can be replicated to storage in one or more target NetBackup domains on other NetBackup Appliances.

When using NetBackup AIR, it is important to understand that security configurations can be different between domains/appliances such that an administrator from one NetBackup domain cannot manage backups on an another. Backup administrators who want to use AIR will need to have administrative access on both the source and target systems.

The ability to replicate backups to storage in other NetBackup domains, often across various geographical sites, helps facilitate the following disaster recovery needs:

- **One-to-one model:** A single production datacenter can back up to a disaster recovery site.
- **One-to-many model**: A single production datacenter can back up to multiple disaster recovery sites.
- **Many-to-one model:** Remote offices in multiple domains can back up to a storage device in a single domain.
- **Many-to-many model:** Remote datacenters in multiple domains can back up multiple disaster recovery sites.

NetBackup supports AIR from a Media Server Deduplication Pool in one NetBackup domain to a Media Server Deduplication Pool in another domain.

For more information, please see the Veritas NetBackup Deduplication Guide.

DETECTION: USING BUILT-IN AND OPTIONAL TOOLS FOR RANSOMWARE DETECTION

Evidence of a successful ransomware attack may not be discovered until it is too late, and an attempt is made by the unsuspecting user to access the newly-encrypted data. Data encrypted by a ransomware attack can also find its way into scheduled backups if not caught early enough, rendering the data that is recovered from these backups useless. For this reason, administrators should be extra vigilant at the detection stage of ransomware protection. Proactive monitoring should be used to give administrators an early warning so that they can get to work containing and stopping the attack as soon as possible as well as begin the process of restoring any data that had been encrypted or deleted.

There are several Veritas and third-party tools that can be used to potentially detect intruders and attacks ahead of time, giving administrators the advanced warning that they need to neutralize the threat. NetBackup OpsCenter and Veritas Data Insight are examples of such tools.

Netbackup OpsCenter

OpsCenter is a web-based software application that helps organizations gain visibility into their NetBackup data protection environment. By using OpsCenter, administrators can track the effectiveness of backup operations by generating comprehensive reports. OpsCenter is available in two versions. There is a free version called, simply "OpsCenter" and there is an enhanced version available at additional cost called "OpsCenter Analytics."

A unique scenario exists for NetBackup customers that use the Media Server Deduplication Pool (MSDP) for their backups. The encryption used in the MSDP works differently from the encryption commonly used in ransomware. MSDP encryption does not impact deduplication rates because MSDP encryption is applied after the segment data is hashed versus before. As a result, MSDP encryption will not affect deduplication rates like ransomware encryption does.

Proactive backup administrators can use OpsCenter to monitor the dedupe rates of their backups. A sharp and sudden decrease in dedupe rates can indicate that the files being backed up have been newly encrypted, indicating that backup administrators should investigate further whether the decrease is due to normal user activity or ransomware activity.

Another method that can be used for possible early detection of malicious activity is to monitor for a large data change rate. This works for encrypted or non-encrypted data. A data change rate of 50% or greater could indicate that data has been encrypted. Keep in mind that data that has been encrypted already can be encrypted further with additional encryption attempts.

To learn more about NetBackup OpsCenter, please see the Veritas NetBackup OpsCenter Administrator's Guide.

Veritas Data Insight

Data Insight provides the analytics, tracking, and reporting necessary to deliver organizational accountability for file use and security. Designed to manage the needs of organizations with petabytes of data and billions of files, Data Insight integrates with archiving and security solutions to prevent data loss and ensure policy-based data retention.

- Automate governance through workflows and customization
- Drive efficiencies and cost savings in your unstructured data environment
- Maintain regulatory compliance for information access, use, and retention
- Protect confidential information from unauthorized use and exposure

With Veritas Data Insight software, users can monitor file access to automatically identify the data user of a file based on the access history. It also includes custom report templates that can be used to detect ransomware.

Data Insight scans the unstructured data systems and collects a history of access by all users across all of the data. It helps organizations monitor and report on access to sensitive information.

Veritas Data Insight periodically collects audits of the read, write, and rename activities performed on the files in the monitored storage environment. With the ransomware reports, count of write and rename activities performed on the files by each user can be captured. If the count is higher than the specified threshold value, then the files on which the activities occurred could be exploited.

Insider Threat 101

Veritas Data Insight is an excellent tool that allows administrators in an organization to discover which users might be a risk to for obtaining and exposing sensitive data and to take steps to protect the data.
https://www.veritas.com/product/information-governance/data-insight/insider-threat

To read more about Veritas Data Insight, please see the Veritas Data Insight Administrator's Guide.

To read more about the ransomware report templates, see these sections: About Data Insight custom reports About DQL query templates

Additional Third-Party Tools

Protecting the backup appliance itself is important but the rest of the user systems and production data need to be protected as well. Third-party malware and ransomware detection tools can also be used to help detect and protect against ransomware attacks on systems other than NetBackup Appliances. Please visit the web sites of these third-party vendors for further information.

Symantec Endpoint Protection

Symantec Endpoint Protection provides malware and ransomware detection as well as antivirus protection for all physical and virtual servers. Intrusion detection and prevention is also included. Please see the Symantec Endpoint protection web site.

Tripwire

Trip wire is used to monitor for specific types of file change and can be integrated with Symantec Endpoint Protection. Please see the Tripwire/Symantec Solution Brief.

RECOVERY: THE LAST STAGE, AFTER A SUCCESSFUL RANSOMWARE ATTACK

NetBackup

There are no silver bullets that can provide 100% protection against all threats. Unfortunately, no matter how well prepared at the detection and prevention stages an organization is, successful attacks do occasionally happen and force organizations into the recovery stage. Depending on how widespread the attack is, the impact could range from a few files on a single volume on one system that have been encrypted by ransomware to data for an entire site being erased thoroughly with multiple passes. When this happens, and regardless of scale, it will be a company's most critical data that is attacked. Disaster recovery tools and procedures will be used for recovery and fully tested in the process.

NetBackup Appliances feature the entire NetBackup suite on performance-optimized hardware—a secure turnkey solution for backup, storage, and deduplication. Using the optimized version of NetBackup included in every NetBackup Appliance, administrators can recover data more quickly and efficiently than ever.

NetBackup Appliances enables backup administrators to recover part or all their data in the event of loss due to malicious activity. The newest versions of the software include features that enable administrators to restore faster than ever before.

For detailed information on using NetBackup and NetBackup Appliances, please see the Veritas NetBackup Administrator's Guide and the NetBackup Appliance Administrator's Guide.

NetBackup Instant Access

NetBackup Appliances are designed to backup and recover a virtual machine almost instantly, without waiting to transfer the virtual machine's data from the backup. NetBackup starts the virtual machine directly from the backup image and makes it accessible to users on the target ESX host immediately. Files can be copied (including vmdk files) without restoring the entire virtual machine. To restore the virtual machine, use VMware Storage vMotion to migrate the virtual machine data files from the backup image to the ESX host.

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

NetBackup Universal Share

One of the newest features found on NetBackup Appliances is called Universal Share. It provides the ability to mount a NetBackup Appliance's storage as secure NFS or CIFS shares and enables the protection of databases where no agent or backup API exists. Universal Share can be used to store data using compression and deduplication. It can also be extremely useful when used as a recovery tool, enabling fast access to backed-up data.

NetBackup Copilot for Oracle Instant Recovery

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

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

BEST PRACTICES

Beyond the built-in security features and configuration options for maintaining security and using off-site copies and air gaps that have already been mentioned above, businesses should consider taking additional steps to defend their backup infrastructure against cyberattack.

It is very important to protect both production data as well as the backup data within a data center. At the same time, it is the backup and recovery infrastructure that could be relied upon to bring an entire enterprise back online after experiencing massive data loss. Businesses need to take every possible step to protect their backup data. A lax approach to following best practices and implementing available security options can be an organizations biggest vulnerability. While not a comprehensive list of best practices, these additional steps can help prevent an attack in the first place and minimize impact if there is a successful attack.

- The administrators tasked with performing disaster recovery operations may not be the same administrators who ultimately carry out the disaster recovery procedures. Disaster recovery procedures for all of a businesses' important data should be fully documented and accessible, even during a disaster. Furthermore, the procedures should be practiced at regular intervals. Disaster recovery procedures will be tested in real time when a critical restore procedure is attempted during an actual disaster or cybersecurity event. The worst time to find out that backup software, backup hardware or recovery procedures do not work is in the middle of the post-event recovery procedures. The best time to practice these procedures is before the event, affording administrators the time to remediate hardware, software and restore procedures that do not work. It is also good to practice procedures for flawless execution of security audits. Backup and restore procedures should be practiced even more frequently for critical data. A malicious insider with enough security clearance can start encrypting data well in advance so that the encrypted files are silently backed up over time to the point that all of the good (non-encrypted) data has been cycled out of retention policies leaving backup administrators with useless restore points.
- Backup administrators should be familiar with last known recovery points and how long recovery procedures take for all types of data. Backup sets could potentially be off site and on tape or in long term cloud storage and will take time to recover. Backup administrators need to understand the recovery times so that expectations can be set with end users.
- New operating system vulnerabilities are always being discovered and then patches and security updates are subsequently released by the OS vendors. It is often these known operating system vulnerabilities that are exploited by malware and ransomware programs, enabling them to spread to other systems. Individual users and companies can be less than up to date with performing the operating system updates; thus, leaving open security holes for the malicious software to spread. Staying up to date with system updates is a critically important to minimizing the impact of a successful attack.
- User credentials should be limited to provide the least amount of access that individuals need to perform their job. Even administrative accounts should be restricted to only the minimum privilege level required for the administrative tasks that need to be performed.
- Conduct background checks on the administrators who will be working closely with and who have access to a company's data. The more access an individual user or administrator has, the greater potential impact of malicious activities. A malicious insider can have easy access to and free reign over a company's data once inside the company and a background check is one of the only ways to protect against this type of threat.
- Change all built-in account passwords including the NetBackup Appliances regularly for the host 'admin', 'maintenance', RMM 'sysadmin' and 'nbasecadmin' accounts.

- Stay informed of Veritas Technical Alerts by visiting the Veritas Support web site at: https://www.veritas.com/content/support/en_US.html
- Take additional steps to protect critical NetBackup meta-data:
  - Update the default Master Catalog backup policy
  - Setup a backup policy for the NetBackup Key Management Server (KMS):

Appliance Security Guide

Veritas provides an in-depth security guide that explains the security features that are included with every NetBackup Appliance running software version 3.1 and above. It should be considered an additional best practice to go through this guide when deploying NetBackup Appliances. General security is enabled by default on NetBackup Appliances and the more advanced features are left for users to enable. To achieve maximum protection, all security features should be configured and used.

These features include:

- User authentication/authorization
- Intrusion Prevention and Intrusion Detection
- Operating system security
- Data Integrity and security
- Web UI, network, Call home, and IPMI security
- Firewall

It is strongly recommended that this guide be consulted, and all security features be taken advantage of for every NetBackup Appliance. Please consult the on-line Veritas NetBackup™ Appliance Security Guide.

CONCLUSION

Ransomware and malicious insiders pose serious threats and new operating system vulnerabilities are discovered all the time. Variants of known malware and ransomware are developed often. The threat of clicking the wrong hyperlink or opening a malicious email is constant. Even with significant effort by system and backup administrators to protect their data; ransomware and malicious insiders can still occasionally get through to impact businesses' most critical data.

Veritas NetBackup software has been synonymous with disaster recovery for decades. Every NetBackup Appliance includes a customized Linux operating system, an optimized version of NetBackup and an embedded version of Symantec Data Center Security.

Combined with on-premises and cloud storage, NetBackup Appliances provide excellent protection against ransomware and malicious insiders. NetBackup Appliances allow backup administrators to reduce exposure and recover quickly in the event of an attack, no matter how severe.

REFERENCES

- The National Cybersecurity Center of Excellence (NCCoE) , a part of the National Institute of Standards and Technology (NIST) have produced a special publication titled: Data Integrity, Recovering from Ransomware and Other Destructive Events. This is a comprehensive, three-part document that details strategies that should be taken to protect against malicious activity as well as the recovery steps that should be taken 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
- Veritas NetBackup Appliance Security Guide
- United States Computer Emergency Readiness Team: Data Backup Options
- Veritas NetBackup Cloud Administrator's Guide
- Veritas NetBackup Deduplication Guide
- Veritas NetBackup Appliance Fibre Channel Guide
- Veritas NetBackup OpsCenter Administrator's Guide
- Veritas Data Insight Administrator's Guide
- Veritas Data Insight User's Guide
- Insider Threat 101: Detect and Protect with Veritas Data Insight
- To read more about the ransomware report templates, see these sections in the User's Guide:
  - About Data Insight custom reports
  - About DQL query templates
- Symantec Endpoint Protection web site
- Tripwire/Symantec Solution Brief
- Veritas NetBackup Appliance Administrator's Guide
- Veritas NetBackup Administrator's Guide, Volume I
- Veritas NetBackup for VMware Administrator's Guide
- Veritas NetBackup for Oracle Administrator's Guide
- The Untold Story of NotPetya, the Most Devastating Cyberattack in History
- Atlanta Spent $2.6M to Recover From a $52,000 Ransomware Scare
- Scottish brewery recovers from ransomware attack
- Negotiating Bitcoin Ransomware With Cyber-Criminals as a Service

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.

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

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

VERITAS

V0827 08/20