VERITAS

Designing for Recovery From a Cyber Attack

Veritas Flex Appliance

White Paper | July 2023

Contents

Executive Summary 3

Know Your Stakeholders 3

Protect Your Backup 3

- Zero Trust Architecture (Never Trust and Always Verify) 3
- Isolated Recovery Environment (IRE) Immutable Storage with Air Gap 4
- Increase Security Posture 5

Design for Recovery 8

- Recovery at Scale 9
- Data Security with Malware Scanning and Anomaly Detection 10
- Dedicated Ransomware Assistance Team 10

Take Action on Day One to Recover 10

NetBackup Ransomware Restore Best Practices 12

Summary 13

Executive Summary

Today, organizations of all types and sizes face similar problems: defending against ransomware attacks. Ransomware attacks are increasing in numbers and sophistication. Cybercriminals have proved themselves adept at finding novel and devious ways to penetrate organizations' systems and bring them to a screeching halt. It is vital that companies prepare themselves now, before it is too late. Security experts from Cybersecurity Ventures are estimating that by 2031, a business will fall victim to a ransomware attack every two seconds and it will cost its victims about US$265 billion annually.[1]

Our response to the community leads us to focus on a multifaceted resiliency framework and make it possible for you to protect all your data regardless of the source, recognize potential ransomware issues, and orchestrate automated retrieval so that your business can be up and running again in no time. Veritas provides an integrated three-pillar approach to safeguarding against ransomware that aligns to the NIST Cybersecurity framework: Protect, Detect, and Recover.

This whitepaper explains who the stakeholders are, what Flex Appliance offers in enhancing the protection of backups, how to design for recovery and actions to take to recover from ransomware and malware attacks utilizing Veritas solutions.

Know Your Stakeholders

It is important for organizations to align internal stakeholders and outside experts in advance of a ransomware attack, and to ensure that all the key personnel are trained and prepared to respond to the attack. External resources include forensics firms; counsel, human resources, communications, business continuity, business application owners, and help desk personnel. Organizations can benefit from a resiliency project manager that can manage tabletop exercises with all key stakeholders.

Below are the roles of the internal teams. They need to get training and work together to understand the priority of data and applications to run the essential business. Understanding the right priority can speed up the restore.

- **Backup administrators**: Responsible for creating and managing protection plans, backup schedules and managing storage. They should work with system administrators to understand the data priority, and what data or applications are essential to keep business operations online.
- **Security administrators**: Monitor networks for security breaches or violations, conduct penetration, report on security breaches, and implement software updates to protect information.
- **System application administrators**: Support the computing environment of a company and ensure the continuous and optimal performance of its IT services and support systems. Security administrators secure systems and provide the backup administrators essential information. They also ensure that applications are protected using immutable storage.

Protect Your Backup

The data that is backed up, and the backup infrastructure, are the last line of defense from an attack and ultimately your organization's key to recovery. Veritas NetBackup™ offers the widest support from edge to core to cloud, with more than 800 data sources, more than 1,400 storage targets, and more than 60 cloud providers, so your environment is always protected and recoverable. Veritas Flex Appliance adds an additional value of immutable storage, air gap strategies, zero trust architecture and features to increase security posture.

Zero Trust Architecture (Never Trust and Always Verify)

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 protected with a universal strategy that is applied intelligently and managed automatically to ensure scalability. Then your backup infrastructure and protected data become the last line of defense from an attack, and ultimately your organization's key to recovery. Using the security features of the data protection system is one key element in this step.

The Flex Appliance uses a Zero Trust security architecture to provide a unified, multi-layered platform approach to seamlessly integrate intelligent protection, comprehensive detection, and industry-leading backup and recovery. As illustrated in Figure 1, it offers hardware security, the secure Veritas VxOS operating system, container service isolation, secure storage services, and data security. It also provides immutable storage, STIG-compliant operating system (OS) hardening, FIPS140-2-compliant data encryption, and comprehensive security access controls. Flex Appliances provide a complete immutable and indelible storage solution to defend an organization's backup data. For more details, please review the NetBackup Appliance Security Guide.

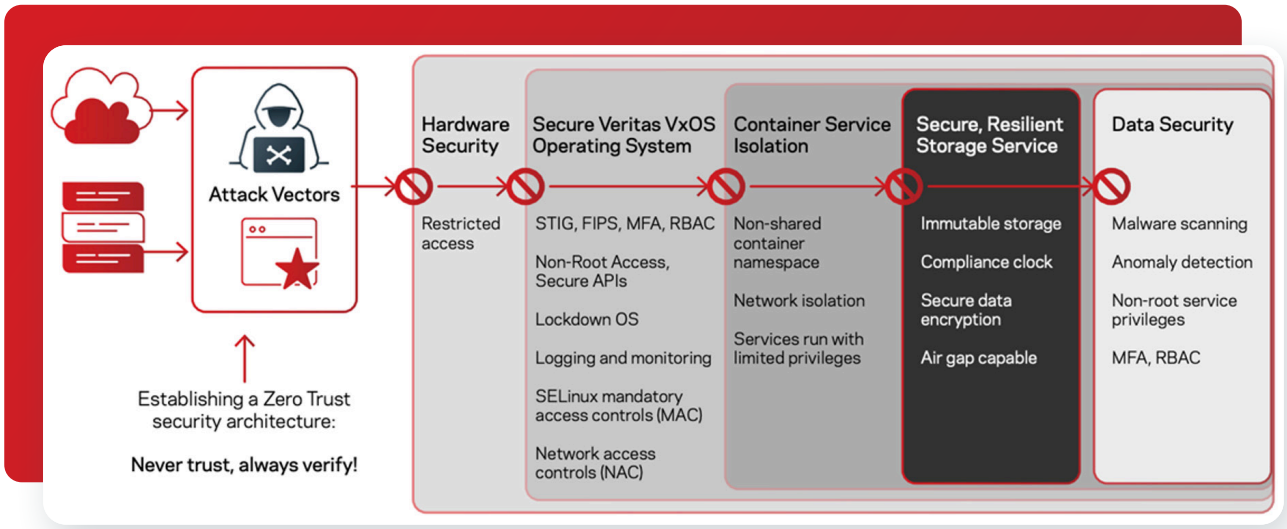

Figure1: Flex Appliance Zero Trust Security Architecture

Isolated Recovery Environment (IRE) Immutable Storage with Air Gap

For enhanced ransomware resiliency, it is important to secure your backup data on immutable storage and maintain an isolated copy of your backup data. This is often referred to as an air-gapped copy. An IRE enables air-gapped backup copies by disabling network connectivity to a secure copy of your critical data, providing administrators a clean set of files on demand to neutralize the impact from a ransomware attack.

The Veritas IRE solution:

- Ensures data is immutable and indelible, minimizing threats from ransomware and rogue users
- Detects ransomware infections within the protected data to prevent reinfection when restoring data
- Enables recovery operations at scale so business services can meet service level objectives
- Enables predictable recovery processes that can be rehearsed to on-premises or cloud infrastructure

Unlike traditional IRE solutions, the Veritas IRE solution is based on the Flex Appliances' container-based multi-tenant WORM storage with OS hardening and a Zero Trust security architecture. It offers a unified, scalable solution with immutability and indelibility. In addition, there is anomaly and malware detection which provides another line of defense against malware propagation in the environment. Starting with NetBackup 10.1, the air gap restricts network access to the IRE all the time and works for Flex Appliances and BYO deployments. For more detail, please review the Veritas Isolated Recovery Environment white paper.

Increase Security Posture

The Flex Appliance has security features to strengthen your cybersecurity stance and prevent attacks to backup and data protection systems. Illustrated in Figure 2 are actions to take and/or enable on the Flex Appliance to increase the security posture of your backup data. For more details on how to enable these features, check the NetBackup and Veritas Appliances Hardening Guide.

Figure 2 - Flex Appliance Features to Increase Security Posture

Highlights of each of these features and actions to take are described as follows:

1. **Enable multi-factor authentication (MFA) and elevate Veritas appliance security level with lockdown mode**

   The administrative credentials hold the keys to the kingdom. When the credentials are compromised, the attacker gets into backup systems and deletes your backups. Veritas Appliances offer unique protection from compromised credentials with lockdown modes and built-in OTP mechanisms to prevent unauthorized access to the operating system. Additionally, to protect the Appliance WEB UI from unauthorized access, don't forget to enable SAML SSO-based MFA or smart card authentication.

2. **Keep all systems and software updated**

   Don't fight today's ransomware with yesterday's technology. Upgrade NetBackup and Appliance software to the latest releases to gain advantages from enhanced security features. Running out-of-date software can allow attackers to exploit security vulnerabilities. Veritas delivers monthly security patches to address critical vulnerabilities.

3. **Reduce network exposure by implementing network access controls**

   Once ransomware enters an infrastructure, it spreads fast and purposefully to increase the attack's blast radius. One way to prevent such infection is to implement network access controls for your data and control plane. Network access controls mitigate the risk of accessing information without the appropriate authorization. You can control which IP address or subnet can access Veritas Appliances via SSH and HTTPs with an allow list. All IP addresses not on the allow list are blocked by default. Should your credentials be compromised, attackers will not find a way to enter your backup infrastructure due to network access controls.

4. Secure credentials with privileged access management

   IT administrators commonly share root, built-in accounts, and many other privileged credentials for convenience so workloads and duties can be seamlessly shared as needed. However, with multiple people sharing an account password, it may be impossible to tie actions performed with an account to a single individual. This creates security, auditability, and compliance issues. External hackers covet privileged accounts and credentials, knowing that once obtained, they provide a fast track to an organization's most critical systems and sensitive data. Don't share or reuse credentials.

   Veritas NetBackup and Veritas Appliance supports external password management solutions. You can deploy CyberArk Privileged Access Manager (PAM) to keep unauthorized users out and detect and stop threats in real time. You can download the Veritas Flex Appliance API (availability, protection, and insights) CPM plug-in. Don't forget to set unique passwords for built-in accounts to provide additional protection from stolen credentials.

5. Immutable and isolated data vault is not a choice and should be part of your core backup strategy

   Imagine that a few of your critical systems are unavailable due to ransomware or sabotage from a disgruntled employee. During the investigation, you found that data was encrypted or deleted, and you think about how to gain protection from such attacks. Veritas NetBackup Appliances provides immutable storage options with secure and encryption-resilient storage, so backup copies are tamper proof. Once immutability is enabled, data no longer can be deleted or encrypted during ransomware attacks, and that's the key to recovery. It's time to revisit the 3-2-1 model—redundancy, geographic distance, and access. Three copies of your data, two on-site but on different media, and one copy off-site. Leverage Veritas Recovery Vault for immutable and indelible off-site copy. 3-2-1 provides the protection you need from natural disasters. The rise in ransomware attacks calls for an extra 1 in 3-2-1 model. The extra 1 represents immutable storage.

6. Enable encryption

   It is a best practice to enable encryption at rest and in transit. Encryption is specifically suited to thwarting data theft (leakage) and internal threats. If data is encrypted using robust industry standards, then even if data is stolen, it significantly reduces the attack exposure so that you can safely ignore ransom demands. NetBackup provides various options to configure encryption. To ensure optimal security, NetBackup includes encryption features for data at rest and data in transit. You can encrypt your data before you send it to the cloud. You can configure the KMS service from the NetBackup administration console or the NetBackup command line during storage server configuration.

7. Enable malware scanning and anomaly detection

   Malware and ransomware programs may go undetected on the target system for days, weeks, or months. These long durations make it quite likely that the malware will be backed up along with the regular backups. It is critical that organizations have malware scanning software to scan backups prior to recovery to find and eliminate malware before it is restored. Veritas NetBackup provides unique built-in anomaly detection and malware scanning to help detect ransomware early. Once malware scanning is enabled, please make sure critical events are fed to SIEM for alerts and security incident orchestration through platforms such as Service Now.

8. Enable NetBackup catalog protection for Primary and Media servers

   Veritas strongly recommends protecting NetBackup catalogs by configuring dedicated policies during disaster recovery. Failure to back up the NetBackup catalog may result in data loss if a catastrophic failure occurs to the file systems housing the various parts of the catalog. You can configure a dedicated catalog policy from the NetBackup console to protect the Primary and Media server catalog.

   For immutable storage, you can create shadow copies of a catalog using CLI options available from the MSDP shell interface: *cacontrol –catalog addshadowcopy /mnt/msdp/vol1*

9. **Refresh your old generation of NetBackup Appliances with a next-generation cyber-resilient containerized, microservices-based architecture such as Flex or Flex Scale**

   Older servers and appliances that have seen five or more years of operation have a three times greater chance of failure and unplanned downtime that might prevent your ability to quickly recover during ransomware attacks. Next-generation appliances provide cyber-resilient containerized microservices architectures with isolation capabilities for air gap or isolated recovery.

10. **Enable security observability through SIEM, XDR, and SOAR integrations**

    To detect and prevent threats, organizations need to promptly spot malicious insiders, compromised accounts, malware infections, and other problems. With Flex Appliances, you can view the events at the Web UI, or forward syslog and audit logs—including elevated shell commands—to a syslog server or security information and event management (SIEM). The logs have consistent timestamp formats which are necessary for accurate and efficient event correlations and log analysis.

    SIEM, SOAR, and XDR platforms are popular tools for combating unwanted trends and unsanctioned actions in IT ecosystems. NetBackup audit messages can now be custom filtered and consumed by SIEM platforms by scanning the system log of the primary server and digesting that information to provide reports, insights, and alerts. Automated response integration within NetBackup can pause clients to stop any spread of undesired data, and SOAR integrations allow further customized actions based on triggers in the various categories of messages. NetBackup adds more capability to your ransomware response plans, with audit messaging insight and control.

    To help you fully utilize the Veritas Appliance Zero Trust architecture, a security meter provides you with one glance to view, and one click to configure the security settings. As shown in Figure 3, the security meter can keep track of security settings and show you a list of available security features with quick links to configure them. The security meter can be found at Flex Appliance web console and only the administrator user can view this feature. To learn more about this feature, review the NetBackup Flex Appliance Security white paper.

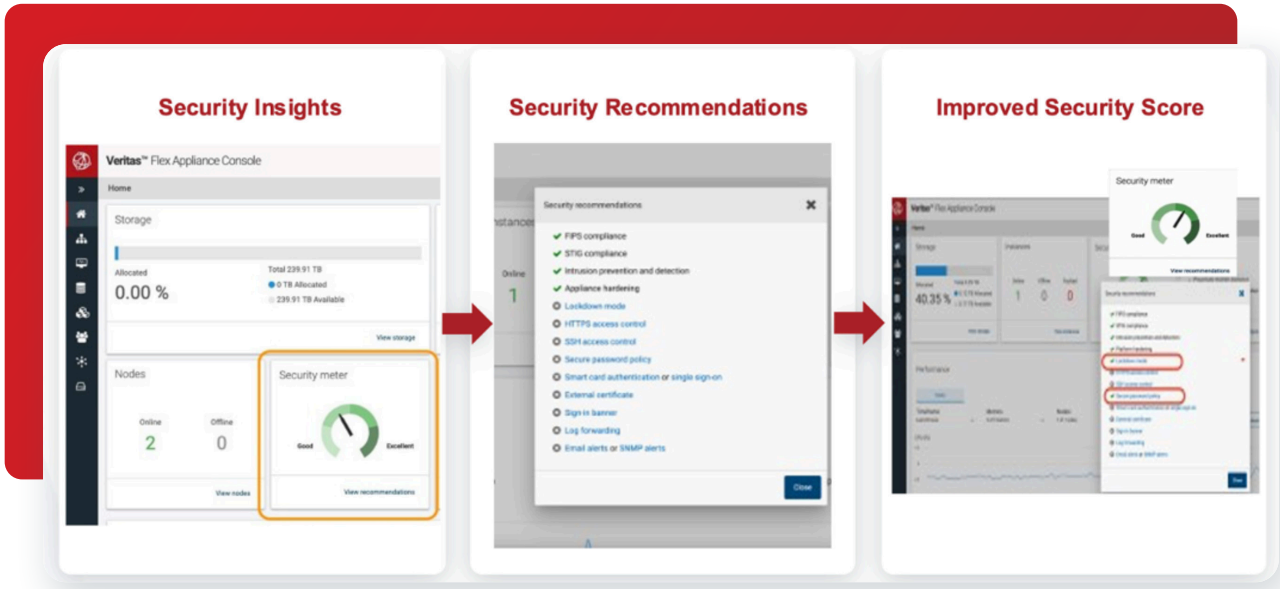

Figure 3 - Flex Appliance Security Controls and Introspection with Security Meter

Design for Recovery

Cyber incident response teams must be well-equipped with the right tools and knowledge to manage a ransomware attack and ensure the recovery of the services to meet the expectations of the business, its customers, and its regulators. Figure 4 depicts how to design for recovery.

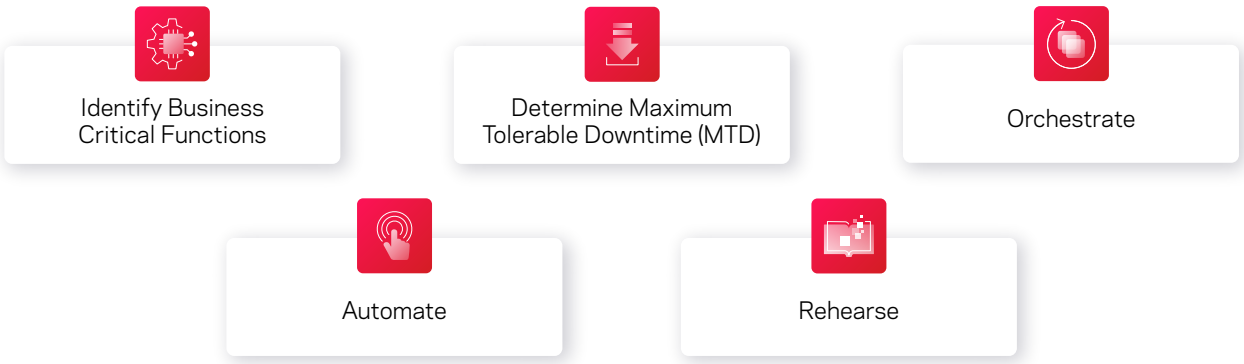

Figure 4 - Strategies to Design for Recovery

The details of the strategies illustrated above include:

1. **Identify Critical Business Functions**—Identifying critical business functions will help you to restore your business quickly and efficiently in the event of a ransomware attack. This involves:
   - Identifying the critical infrastructure and business services, and determining the criticality of the data that is stored or processed by these services
   - Prioritizing systems and data in order of importance, and determining which systems and data need to be restored first in the event of a disruption
   - Planning the system recovery order timeline with the prioritized list; the timeline should take into account factors such as dependencies between systems, recovery time objectives (RTOs), and recovery point objectives (RPOs)
2. **Identify Business Critical Functions with Maximum Tolerable Downtime (MTD)**
   RTOs and RPOs are traditionally used as goals to frame a conversation for overall recovery. MTD is simply how long the key revenue-flow applications can be offline. MTD brings focus to the critical functions an organization needs to get up and running to avoid a business disaster. Business function downtime is based on two elements: the systems or technology recovery time objective (RTO), and the people-based work recovery time (WRT). As such, the formula for maximum allowable downtime is the following: *Maximum allowable downtime = RTO + WRT*
3. **Orchestration**—Orchestrate restore technologies based on the MTD and business-critical functions, choose the appropriate restore technologies and orchestrate a flexible recovery strategy.
4. **Automation**—use automation solutions with resiliency and evacuation plans (runbooks) which allows for automation recovery at scale between data centers, or to cloud infrastructures. 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.
5. **Rehearse a Plan**—A detailed resiliency plan and rehearsal are two key elements in ensuring ransomware resiliency. During a stressful ransomware attack, the key stakeholders should know what to do and when to do it. The test plan will reduce the potential damage and help quickly restore operations. A rehearsal is essential to test the success of data recovery and calculate recovery times. It is essential to periodically test all backup and recovery plans

Veritas products has numerous features to assist in your recovery strategies. It provides recovery at scale, malware scanning and detection prior to recovery, and a dedicated ransomware team which has the knowledge to assist and support in the recovery. The next sub-sections highlight these offerings.

Recovery at Scale

The key to a successful recovery strategy is flexibility to orchestrate the appropriate solutions to ensure operational and business resiliency for rapid recovery. Sometimes everything is impacted, and you may need to recover an entire data center in the cloud and on demand. On the other hand, perhaps 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 perhaps you just need to recover many VMs back to production. Veritas provides a wide range of technologies and capabilities to orchestrate, automate, and rehearse a robust recovery strategy, including:

- NetBackup Resiliency: NetBackup Resiliency provides automated orchestration across an organization's entire heterogeneous environment, with a consistent user experience and visibility into the best recovery options based on the options available
- NetBackup Instant Rollback for VMware: Provides high-speed VM recovery by using Reverse Change Block Tracking to identify which unique blocks need to be recovered, and applying just those changes to bring VMs back to a healthy state in seconds
- NetBackup Resiliency's Continuous Data Protection (CDP): Provides advanced resiliency for your applications by offering checkpoints derived from real-time replication of your production data that can be used for recovery purposes; CDP augments primary data replication by providing granular recovery for your VM's with a near-zero RPO to ensure recovery capability for your applications across heterogeneous environments, using granular recovery points in addition to near-real-time data replication; with this functionality, CDP provides an additional layer of recoverability from malware or data corruption with a much lower RPO than recovering from a backup copy; NetBackup Resiliency also provides a single interface to manage recovery from CDP checkpoints and backups, which simplifies the recovery process
- VM Recovery: Provides eight types of recovery for one backup of VMware VMs, including full VM, individual VMDK, file and folder, full application, Instant Access, file download, application GRT, and AMI conversion
- Instant Access for MSSQL and VMware: Provides almost instant machine recovery (such as 1,600 VMs) without waiting to transfer the VM's data from the backup; also provides the ability to test or recover VMs directly from backup storage
- NetBackup Snapshot Manager: Uses cloud-native snapshot technology in a cloud vendor-agnostic way that allows easy protection of hybrid and multi-cloud infrastructures
- Universal Share and Protection Points: Allows organizations to provision deduplication-backed storage on the NetBackup server as secure shares, thereby protecting databases or other workloads where no agent or backup API exists
- NetBackup Universal Shares for Oracle: Allows Oracle database admins to start up databases directly from a NetBackup Appliance's storage
- Long-Term Retention Archive: Provides a cost-effective and durable solution that features deduplication and compression of data, including the use of object storage and private or public clouds; traditional recovery includes granular restore of a specific file, full server/application restore, and disaster recovery (DR) restore to a different site location or the cloud—using Veritas Resiliency Platform, organizations can automate and orchestrate traditional recovery with the push of a button, streamlining the DR process
- Bare Metal Restore: Automates the server recovery process, making it unnecessary to reinstall operating systems.
- Veritas Alta™ Recovery Vault: Seamlessly integrated with NetBackup to provide secure cloud storage as a service, managed by Veritas and optimized for data protection. Recovery Vault provides secure air-gapped storage to reduce the threat of data loss from ransomware attacks; flexibility to choose whether to recover workloads in your data center or in the cloud and storage management provided by Veritas to delivering low-cost long-term data retention in the cloud that can complement tape as an additional option for air-gapped storage.

Data Security with Malware Scanning and Anomaly Detection

NetBackup Malware Scanning and Anomaly Detection provides greater control for detection and recovery workflows. NetBackup offers two malware scanning methods to protect your data's integrity and the backup image: on-demand scans, and scans automatically triggered by high anomaly scores. The last-known-good image will be clearly visible in the recovery workflow. Selecting an impacted image will present several warnings to the user. If we find something infected in the immutable storage, the image cannot be expired before the minimum retention period. But in this situation, administrators will know there is an infection, so they can plan accordingly. You can also scan the image before the recovery. NetBackup will give warnings on detection before the restore. NetBackup Malware Scanning and Anomaly Detection as shown in Figure 5 offers a powerful point of insight into the backup images as a response to an alert or on-demand scan of a backup image.

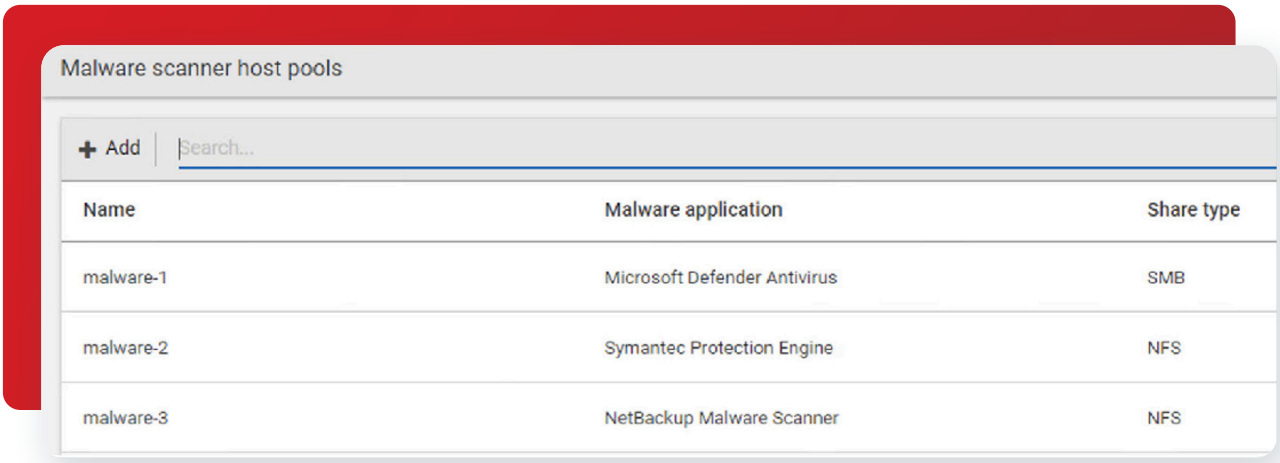

Figure 5 - NetBackup Malware Scanning and Anomaly Detection

Dedicated Ransomware Assistance Team

Veritas Support offers a dedicated ransomware assistance team with 24x7 support to help you recover from an attack. As the leader in data protection, Veritas offers a ransomware resiliency assessment program—a comprehensive approach to data protection. The program provides practical advice for data protection, detection, and recovery, based on real-world experiences; and identifies the current gaps between security and data protection.

- Expert, comprehensive advice on ransomware resiliency strategies and issues
- Developed to facilitate wide-ranging discussions with IT leadership teams about their ransomware resiliency strategy
- Designed to identify the potential risks of ransomware attacks that exist in the data protection infrastructure and recovery process

Take Action on Day One to Recover

Time is of the essence when it comes to ransomware infections. The sooner you can contain the infection, identify the source, and notify the appropriate stakeholders, the better your chances of minimizing the damage and recovering your data. Figure 6 shows the actions on what to do when a ransomware attack occurs.

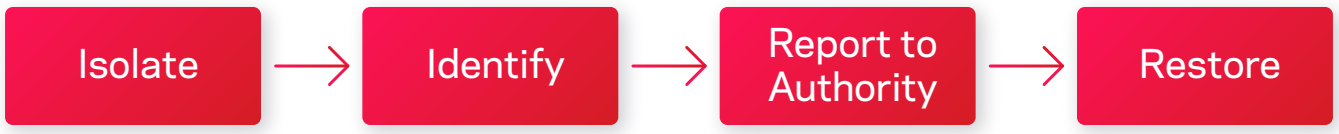

Figure 6 - Actions to Recover

Description of the steps illustrated above to conduct on day one to recover are as follows:

1. Isolate the Infection

   Most ransomware will scan the target network, delete, or encrypt files stored on network shares, and propagate to other systems. Isolation of the infection is the top priority to contain and prevent ransomware from spreading. The infected systems must be removed from the network as soon as possible.

   Backups are your defense to ransomware, but they are not immune. Many ransomware strains specifically target your backups and encrypt, override, or delete them. You must secure the backups by disconnecting backup storage from the network, or by locking down access to backup systems until the infection is resolved.

2. Identify the Source and Assess the Damage

   Identifying the source and timeline of the infection is crucial for understanding how attackers gained access to the system, what other actions they took while they were on the network, and the extent of the infection. Detecting the source of the infection is useful to not only resolve the current incident, but to help organizations address vulnerabilities and reduce the risk of future compromise.

   With Veritas Appliances, you can view the events at the Web UI, or forward syslog and audit logs including elevated shell commands to a syslog server or SIEM. The log has consistent timestamp formats across all event logs, which are necessary for accurate and efficient event correlations and log analysis. Veritas Appliances have integrated data collection including application instance logs, OS logs, and shell commands. Veritas Appliance platform auditing logs can help you establish the timeline of the attack.

   Veritas Data Insight creates a baseline of user activity over a period of time and looks for any statistical standard deviation in the user account behavior resembling a malware attack on zeroth day. Once detected, it alerts the administrator directly or via a SIEM event and provides report templates to analyze the list of impacted files (based on activity monitoring), highlights the compromised account, helps find instances of malicious executables, and stops further damage by automatically locking the account down through automation and integration with the organization's remediation processes.

   Post attack, Data Insight can help review the extensions of each of the files that were renamed or modified. It compares the files with more than 880 known ransomware file extensions, to further support the assessment, and to ensure that the downstream recovery processes incorporate that knowledge to restore uninfected data. As part of the automatic content classification capability, Data Insight can also detect and alert if ransomware notes are found in the unstructured environment to help prevent schedule-based malware attacks.

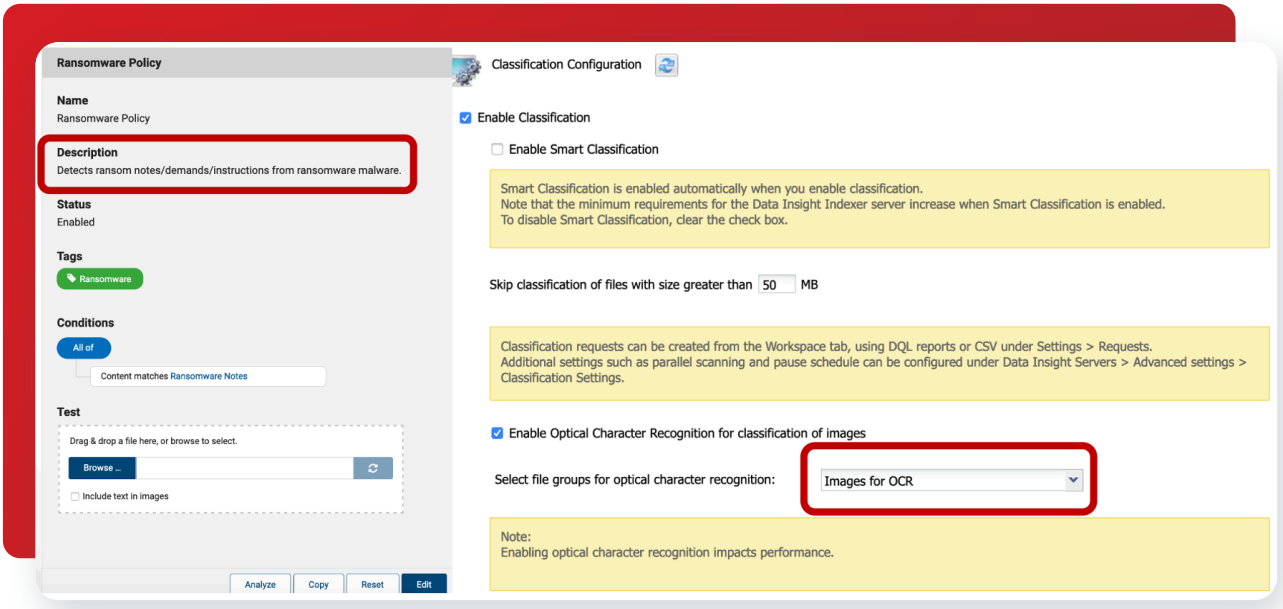

Figure 7 - Veritas Data Insight Detection and Alerting Feature

3. Notify Stakeholders and Report to Authorities

   If you suspect that your organization has been infected with ransomware, it is important to act quickly and notify the relevant stakeholders as soon as possible. Here are some steps you can take:

   a. Inform your IT team immediately about the ransomware infection; they will be able to assess the situation, contain the infection, and initiate the necessary response

   b. Alert management about the ransomware infection and provide them with the details of the situation; they will need to be informed of the potential impact on business operations and any risks to sensitive data

   c. Notify law enforcement: For legislation and compliance standards, it is a requirement to report incidents to the relative authorities; in many countries, ransomware attacks may be considered a crime and should be reported to law enforcement authorities; you can report a ransomware incident to the FBI or use CISA's reporting tool; the FBI's Internet Crime Complaint Center provides a reliable and convenient reporting mechanism to submit information to the FBI concerning suspected internet-facilitated criminal activity; CISA is a US cyber defense center to respond to cyber incidents

   d. Notify affected stakeholders: If the ransomware has impacted any external parties, such as customers or partners, it may be necessary to notify them; this will depend on the severity of the attack and the potential impact on their data

4. Restore

   The final step is the restore of data. Utilizing the recovery strategies described in the previous section, making use of the NetBackup recovery features and/or getting assistance from Veritas ransomware support team can make the restore go smoothly.

NetBackup Ransomware Restore Best Practices

The NetBackup instances in the Flex Appliance can also get infected or attacked. In these scenarios, there are some best practices that can help organizations effectively restore their NetBackup environment in the event of a ransomware attack.

- Rebuild the Primary Server: If the NetBackup Primary server has been infected with ransomware and/or the catalog has been corrupted, it is recommended to rebuild the primary server.
- Full Catalog Recovery: Full catalog recovery is the simplest option to recover the complete catalog when the DR site has the same layout as the production site—the same number and name of media servers. In this case, all device records are removed because the device configuration at the DR site can be different from the production site. It is also recommended to deactivate media servers that do not exist in the DR environment to avoid unnecessary pooling. Device discovery should be run to update the EMM database.
- Partial Catalog Recovery: Partial catalog recovery is recommended for multi-domain configurations and DR sites where the server layout is different from the production site—for example, different numbers of media servers or different library types.
- MSDP Catalog Shadow Copy: By default, MSDP Catalog Shadow Copy is in the same partition as the original, which can prevent recovery from deletion of the filesystem. To avoid this, it is recommended to have the shadow copy on an alternate file system.

Summary

A ransomware attack can halt an organization's operation, disrupt business, and negatively affect your confidence. Veritas purpose-built data protection Flex Appliances offer tamper-proof cyber resiliency, zero trust architecture, scalability, and a simple way to perform mass recovery. With the NetBackup and a Flex-enabled isolated recovery environment, you get an isolated, air-gapped solution as well as confidence in your recovery capability, knowing that your data will be safe and protected with advanced malware scanning. Recover instantly from anywhere, whether it's in the same environment, a different data center, or in the cloud.

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 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

V1923 07/23