Veritas Ransomware Solutions: NetBackup

Adopt a three-prong strategy to successfully protect, detect, and recover critical data.

Introduction

Now you can architect yourself as the hero in your ransomware story. With Veritas NetBackup™, you can build better backup and recovery plans that are optimized at every opportunity. Plus, you can communicate flawlessly with associated teams that have previously set expectations, ensuring you can support their objectives even if an attack occurs. The key: a ransomware strategy based on three components—protect, detect, and recover—already built into NetBackup.

Protect

Today, it's imperative to build your data protection strategy with the intention of recovering your data at scale. That means your infrastructure design needs to meet multiple requirements. Always adopt the latest versions of software to take advantage of new technology and mitigate risks. Then monitor for success in your NetBackup operations to ensure consistent recovery point objectives (RPOs). Take advantage of data encryption options for data in flight and at rest to confirm it's not compromised or exploited within the ecosystem. Conduct tests to ensure your data protection infrastructure maintains resiliency, the team is familiar with procedures, and you can find issues before a real disaster or event.

NetBackup scales to protect enterprise workloads, offering a single-pane-of-glass to help organize backups and orchestrate restores. Its web UI offers streamlined workflows for the most essential applications. And its deduplication technology delivers efficient data protection that integrates with a heterogeneous infrastructure to enable resilient backup strategies incorporating multiple copies, multiple storage types, multiple locations, and immutability. (See Figure 1.)

Figure 1. A best practice is to save at least three copies of your data on at least two types of storage with one off-site and one on immutable/WORM storage.

Implement Zero Trust

Implement a Zero Trust security model that grants access only for a permissible purpose. To do so, you must remove all implied permissions and provide only the level of access users need for specific tasks. This model does not trust any user or device by default, even if it is already inside the corporate network. Instead, it is based on a just-in-time and just-enough access approach. NetBackup's authentication enhancements allow for more robust control to support this model, with improvements to the command-line interface (CLI) that include role-based access control and smartcard authentication.

To build a Zero Trust model:

- Institute identity and access management that includes:
  - Multi-factor authentication (MFA)
  - Role-based access control (RBAC)
- Encrypt data:
  - In flight
  - At rest
- Limit access to backups
- Implement security analytics

Build your IT infrastructure on purpose—not only for backups, but for recovery and security as well. Ensure that for every step in the backup lifecycle, there is a reasonable recovery time objective (RTO) balanced with the capabilities of data movers and recovered systems. NetBackup offers unparalleled data protection management of all your workloads and their recovery points. Architect the design for real-world scenarios, and then rehearse those scenarios, purposefully testing each step in your data protection model. At the same time, build cooperative relationships with your business technology leaders to adjust and enhance the NetBackup protection model as your data needs change.

Secure and harden the rest of your infrastructure by securing all applications and reducing attack surfaces where applications run. Prioritize hardening for edge computing, with deliberate and managed gaps to the internal network. Build system resiliency for operating system (OS) hardening with endpoint threat deterrents and limited-access dedicated network segments using a Zero Trust model.

Detect

Why is detection important? These days, it's a "when-not-if" attack scenario, so it's important to take the right steps to detect anomalies, protect every system, and practice good data hygiene. Bad actors are waiting and watching for mistakes and weaknesses, taking advantage of unvalidated assumptions and exploiting the inherent secrecy and lack of monitoring in the dark corners of an environment.

Detecting anomalies within the backup process gives the backup administrator an important metric to both play a role in the organization's security posture and understand trends and deviations in its heterogeneous data protection footprint. Although backup admins can't be expected to know the norms for all data, anomalies should raise suspicions about events that may require attention.

An anomaly is any significant change in backup image size, number of backup files, data that is transferred in KB, deduplication rate, or backup job completion time. Anomalies indicate potential problems within the data, and thus the IT infrastructure. You don't always know what the next cyberthreat will look like, but anomaly detection will find the aberrations and alert you to potential dangers.

Previously, you had to use manual analysis of the NetBackup Activity Monitor to detect anomalies. With the new Anomaly Detection engine, however, this activity is now automated. Starting in NetBackup 9.1, anomaly detection uses metadata and machine learning (ML) already available to key into likely indicators of issues.

Using ML, NetBackup can detect anomalies and form an anomaly's score. A higher score is more significant and reflects how different one set of data is compared to previous sets of data for the previous backups.

To access the anomaly detection settings, open the NetBackup web UI and log in as the backup administrator, the account with permissions to all aspects of the web UI. You can find anomaly detection under "Detection and reporting" on the left-hand menu.

You can tune the level of sensitivity to changes under the Anomaly detection settings in the web UI, depending on the needs of your organization. Negative values reduce the deviation tolerance, resulting in more detected anomalies. Conversely, positive values increase the tolerance, allowing for small to medium deviations without alerts and only alerting for significantly large deviations. By default, the sensitivity is set in the exact middle, labeled "Medium" (see Figure 2).

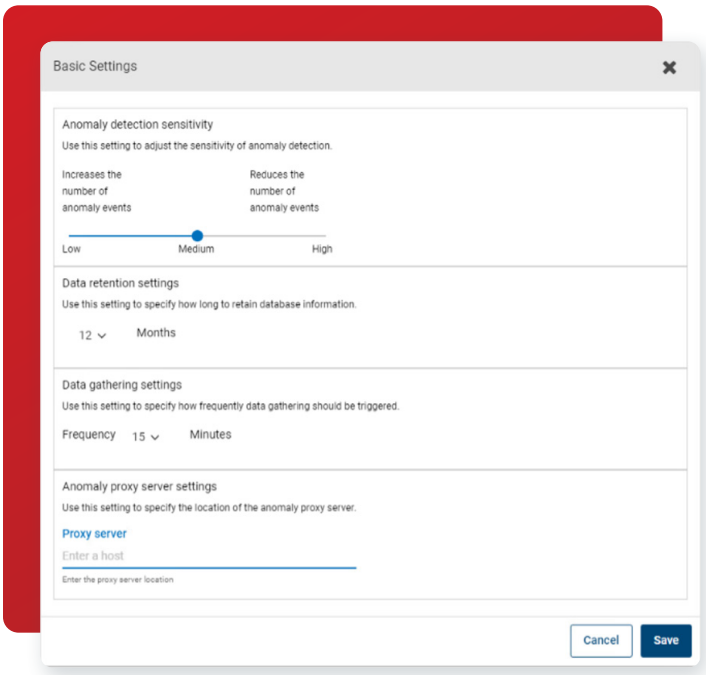

Figure 2. The basic anomaly detection sensitivity settings in the NetBackup web UI.

Anomaly detection can run on NetBackup's primary server or a media server. The optional setting for ANOMALY_PROXY_SERVER allows the anomaly detection service to run on a different host than the primary server, but it must be a host with NetBackup media server software installed. You should also preserve the existing scanning data by copying the NB_Anomaly.db file from the following folder on the primary server to the same folder on the media server:

```
{NB install path}/var/global/anomaly_detection/
```

The proxy anomaly server does not alter the flow of the backup data but only offloads the processing of the metadata. The anomaly detection service, nbanomalymgmt, should be stopped on the primary server and manually restarted on the proxy (media) server after changing this option with nbsetconfig. After the proxy setting has been read at startup, you won't need to take any manual action in the future.

It takes approximately 30 data points to establish a usable baseline from which to detect anomalies. For each of the categories tracked, the backup administrator can leverage anomaly detection in several ways. The admin can allow automation to handle the bulk of the work and isolate and alert on only those tasks that need manual intervention.

Leverage the Benefits of Anomaly Detection

NetBackup's anomaly detection service can help the backup administrator contribute to the overall health of the infrastructure by identifying unforeseen impacts, system performance issues, forecasting future storage needs, and detecting possible compromised systems. These indicators reveal important changes in the environment sooner. Any anomaly should prompt investigative questions and adoption of the Zero Trust model to address malignant issues as quickly as possible. Keep in mind that changes in the environment do not always indicate a bad actor or malware infection but should always elicit a response to maintain confidence by asking:

- Is this a predictable change from standard events or an unknown event suggesting unscrupulous action?
- When did this change happen?
- What is driving this anomaly?
- How could this change be explained? Is it a patch, an upgrade, or a breach?

Look for symptoms of unhealthy changes. Leveraging anomaly detection from deduplication rates can highlight fundamental changes to data that require prompt attention. If the normal deduplication rate is dropping, it indicates that more unique data is entering the backup stream, which becomes useful information for the backup administrator. Identifying reasonable and unreasonable causes for this kind of anomaly can elicit a more thorough investigation of that data. Significantly lower deduplication rates will use more backup storage, which can have ramifications for other NetBackup operations as well as indicating an unhealthy change. When the data protection footprint increases in size, number of files, or time, you need to eliminate the possibility the anomaly is caused by harmful data, malicious insiders, or harmful activities on the system manifesting as performance issues. The integration of several malware scanners in NetBackup 10, provides a more purposeful malware scan of a backup image that can be another defense against malicious software breaching your servers.

Answering "Why did this happen?" will help optimize other workloads. Understanding anomalies helps avoid detecting events that are simply reflecting how an organization's data lives and works. Taking action in the NetBackup web UI helps improve the artificial intelligence (AI/ML) for the anomaly detection. As a backup administrator, you can also flag the anomaly as a false positive to remove it from the baseline data or confirm the anomaly to reinforce the detection logic.

Alternatively, an admin can opt to ignore an anomaly, treat it as a statistical outlier, and use the event as an opportunity for tuning more strict or lenient detection settings. Combine this front-line detection with the powerful Risk Mitigation dashboard in NetBackup™ IT Analytics for a comprehensive view of your IT infrastructure.

Implement Malware Scanning

With anomaly detection, a backup administrator can play an important role in maintaining an organization's security posture. We all know security is everyone's responsibility, and bad actors and attackers will take advantage of the smallest mistakes and oversights. That's the source of the saying, "If you see something, say something." NetBackup's malware detection and anomaly detection provide powerful tools for the backup administrator on the front lines of an organization's data protection.

Integrating your malware scanner into the backup cycle allows your organization to reinforce its security posture and use appropriate detection settings to highlight issues, streamline the workflow, and leverage automation.

With malware scanning, NetBackup can use Microsoft Defender or Symantec Protection Engine (SPE) to cold scan the backup image to ensure a last-known-good image is available for restores. This powerful feature combines NetBackup deduplication and Instant Access with an organization's endpoint security to bolster business continuity plans. (See Figure 3.)

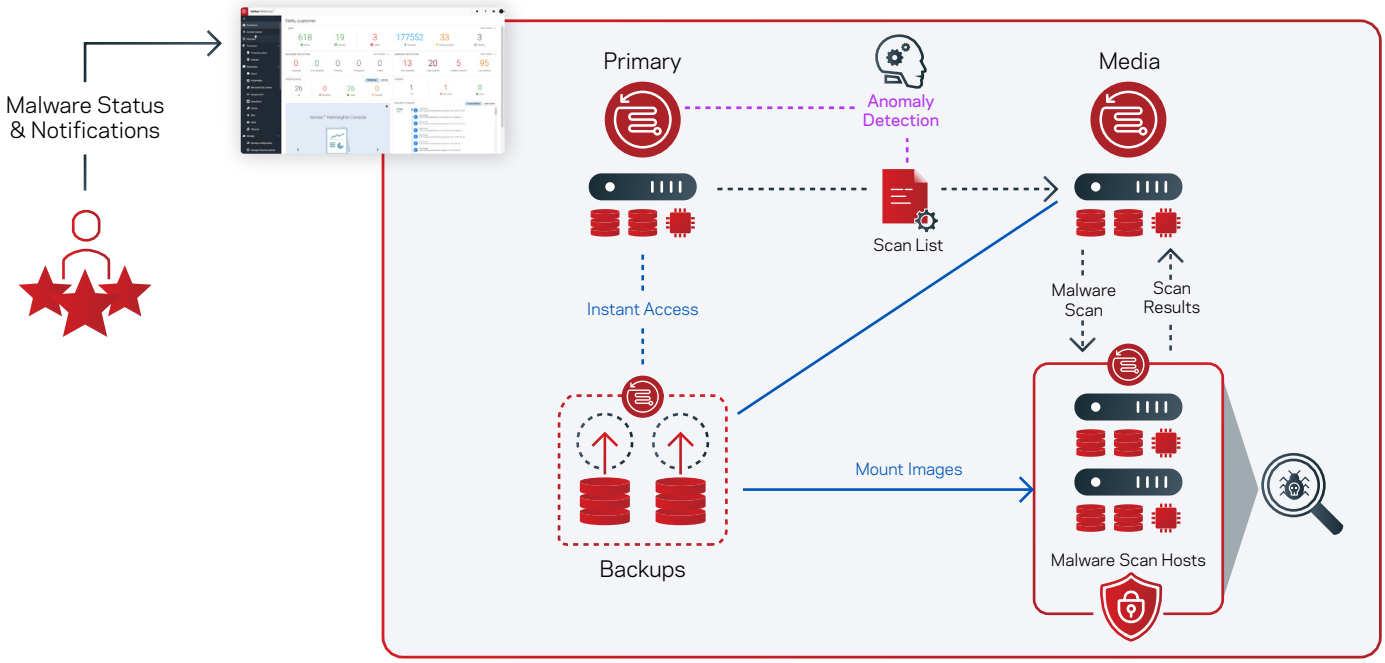

Figure 3. An overview of how to use NetBackup to create a last-known-good image for restores.

NetBackup Appliances will immediately support this feature as will NetBackup media servers using MSDP with the required components for Universal Shares.

The Network File System (NFS) and Samba components of Universal Shares will control how the scanner will attempt to mount the image for scanning. Different scan hosts may have different OS permissions and networking requirements, depending on their malware detection engine. Using Samba will always have a prerequisite of Active Directory information for authentication purposes.

Scan hosts are a new entity in the backup infrastructure that allows the scan to be offloaded to a location where the anti-malware engine resides and then filters the results back to the NetBackup web interface. Taking further advantage of NetBackup deduplication beyond the storage savings and using Instant Access, the Scan Host temporarily mounts the image and performs the scan.

With on-demand malware scanning, backup administrators can target high-risk hosts like those connected to the external web or interfacing with susceptible Internet of Things (IoT) devices. Ransomware is notorious for staying dormant and mining information about an environment to further weaken its defenses and mitigations. Position high-risk clients for more intense scrutiny and bolster data protection confidence with on-demand scanning.

You can also automate this process for situations where anomaly detection scores "High," thus reducing the need for administrative manual workflows.

Malware detection helps build business continuity confidence with last-known-good backup images. Malware detection uses the same configuration file as anomaly detection:

```
# /usr/openv/var/global/anomaly_detection/anomaly_config.conf
```

Once a scan pool is configured, enable automatic malware scanning of high-anomaly images by including the following line in the configuration file:

```
ENABLE_AUTOMATED_SCAN=1
```

For organizations that do not have a malware scanning engine immediately available to their backup environment, Veritas has an option for malware scanning in the Veritas Download Center, with installation files for SUSE Linux, Red Hat Enterprise Linux, and Windows x64. The installation files provided by Veritas do not require additional licenses. This is an optional, separate setup process. In a recovery scenario, a user will be able to see an image's scan status in the NetBackup web UI. (See Figure 4.)

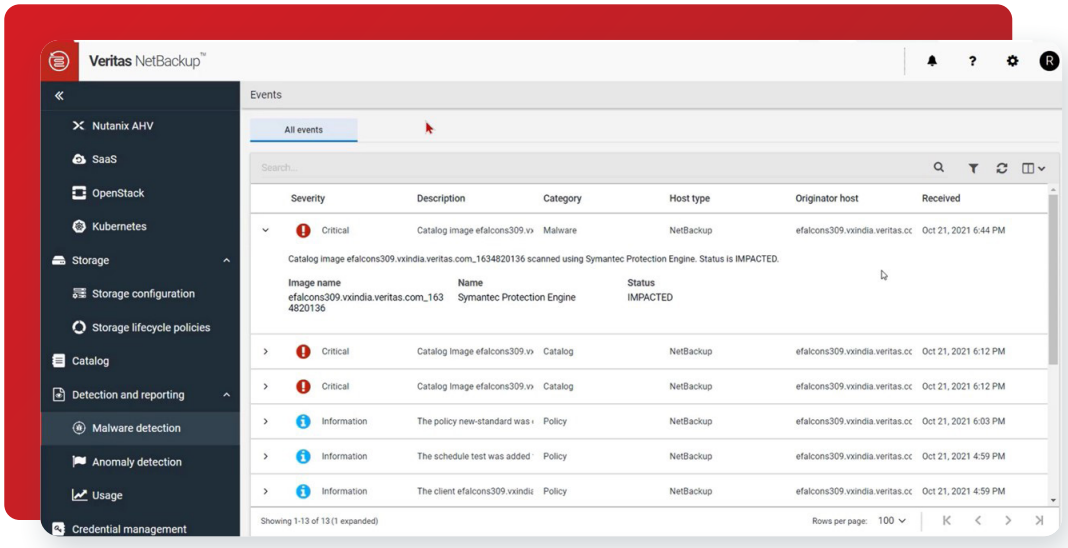

Figure 4. An overview of events detected by malware scanning in the NetBackup web UI.

The backup administrator can also use another NetBackup feature to restore only clean files. If a file selected for restore is marked as impacted, the clean restore will restore that file from an uninfected backup, allowing a safe and effective way to recover from that point in time without re-infecting the target machine. The CLI option for this newly added feature is bpcleanrestore. This command's options will be familiar because it parallels the often-used bprestore command. For recovery at scale, using the CLI is also popular because it lends itself to scripts and reduces clicks in the graphical user interface (GUI).

Anomaly detection will alert the backup administrator to deviations, giving the organization the warning needed to close the gaps and assume a recovery posture before the infection has the opportunity to spread and cause debilitating damage to the infrastructure. Malware detection augments this functionality with on-demand scanning of images and automatic scanning for images considered high risk. Use NetBackup's detection options to reduce your risks and spot suspicious activity. Remember to secure your network and operating system with a Zero Trust posture to reduce attack surfaces. Upgrading NetBackup takes advantage of the latest enhancements to these features as well as the latest security updates in Veritas products such as Log4j.

Recover

Your recovery plan is only as good as your last test. Ensure that you have tested a rapid recovery plan and fine-tuned it for success. Learn from previous testing experience where challenges may arise and document those procedures. Test your plan regularly to confirm procedures are updated and in compliance with improvements to your disaster recovery objectives. Olympic athletes train for years to prove themselves in an event that may last only minutes. Flawless implementation comes from practice.

NetBackup RBAC roles and NetBackup client-side software enable ease-of-use by data owners to self-serve their restore requirements. With backup administrators instilling high confidence in data integrity, the tested threat remediation procedures will work at any scale and minimize downtime.

Conclusion

Your backup solution needs to protect your data from the edge to the cloud to the core. Replace assumptions about data protection with purposeful tests and use the most appropriate features of NetBackup to protect and recover your organization's important data. Codify these plans in an accessible document and rehearse until you get it right. Implement both immutability and off-site backup copies for the most robust resiliency. Combine anomaly detection with malware scanning to create confidence in this model and identify threats before they're a problem. Recover quickly by planning ahead. And when the worst happens, be the author of your own story where collaborative and purposeful planning and execution avert a potential disaster.

VERITAS

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

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

V1506 02/22