VERITAS

NetBackup™ Malware Detection

Bolster your defenses inside the perimeter.

Technical Brief | September 2023

Malware Detection Bolsters Your Defenses Inside the Perimeter

Anomalies in the data protection landscape are just the beginning of the story. With malware as a serious possibility, you need more security checkpoints inside the perimeter of the IT ecosystem.

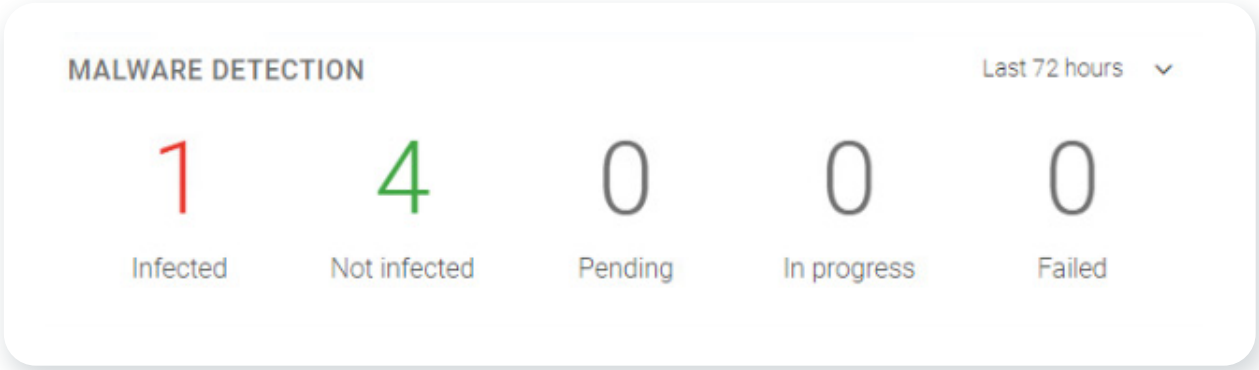

Figure 1. An overview of the malware detection dashboard in the NetBackup web UI

NetBackup malware detection provides another line of defense against undesirable data propagating in the environment. The anomaly detection engine works automatically. While the anomaly detection engine works automatically as of version 10.3, malware detection lets you distinguish between clean or infected recovery points for the following backup data types:

- Standard backup images
- VMware virtual machine backup images
- Windows backup images
- NetBackup Universal Shares
- Cloud-based backup images
- K8s backup images
- Dynamic NAS (DNAS) backup images
- OST device target images

Malware scans during recovery/restore jobs of unstructured data are possible as of NetBackup 10.3. (Scans of structured data such as VMware are not yet supported.) Recovery scans finding malware in backup image(s) to be restored are halted and an alert is posted with options to cancel the restore or proceed. Proper RBAC authorization for the administrator performing the restore is required to proceed. Recovery scans finding no malware proceed without delay.

Rogue administrator detection is also part of the 10.3 malware-handling improvements. The image expiration patterns of each administrator ID is checked for surges in expiration behavior out of norm from their average behavior over the last 90 days. Once a rogue administrator is detected, their ID is temporarily blocked from performing more expirations. An alert is raised to all administrators prompting them to verify that ID's expiration activity is acceptable. They can then reactivate the rogue ID.

Version 10.3 also introduces client health checks. NetBackup clients are checked periodically for encryption on files that shouldn't be and raises an alert if such a client is found. Data protection administrators can then notify the security team to update or check for proper operation of the primary malware-scanning software running on that client.

Universal share scanning is added as well in 10.3 for specific malware filename extensions. A rules engine scans universal share backups for filename extensions associated with malware shortly after these backups complete. An alert is posted if malware-related filename extensions are found.

OST-based flat file storage unit customers at version 10.3 or higher can perform malware scans of non-deduplicated backup images on their OST devices. This feature is available on supported OST devices only. MSDP OST-based storage units are not required to use this feature.

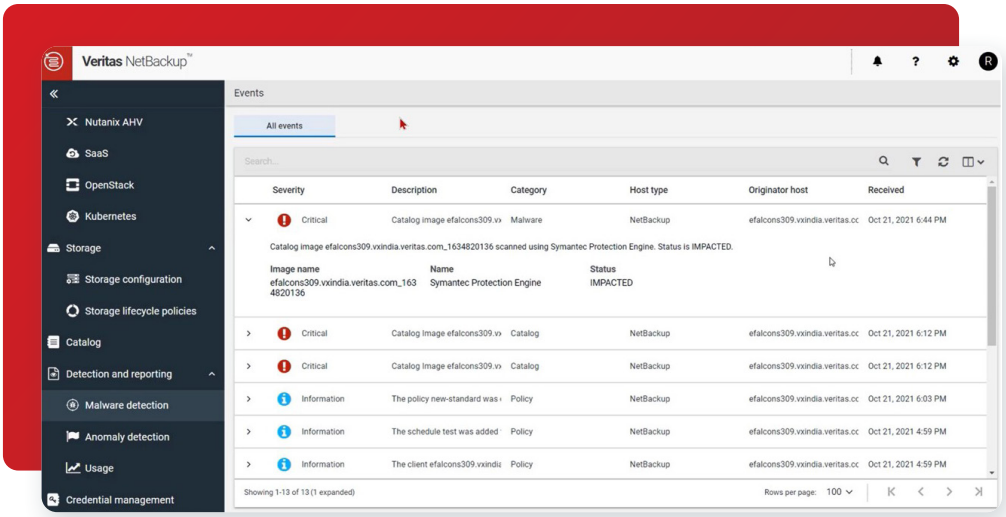

Figure 2. A detail of a malware event selected in the NetBackup web UI

NetBackup easily integrates with leading malware scanners such as Microsoft Defender and Symantec Protection Engine. The NetBackup malware scanner is available for customers to download from the Veritas Download Center, as part of their software entitlement. Malware scanning is achieved without the need to restore data into any sandboxed environment, thus lowering infrastructure costs. Using copy data management capabilities of the Veritas Deduplication Engine, a read-only copy of the backup image is provisioned as a virtual file system; its contents are scanned, and information about infected files are stored in the NetBackup catalog.

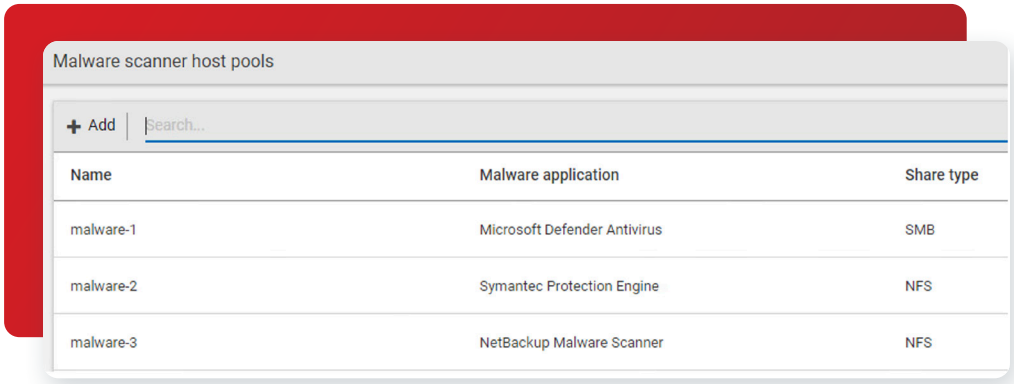

Figure 3. The malware scanners available in the NetBackup web UI

Malware scanners can be deployed on one or more hosts, depending upon concurrent scanning requirements. These scan hosts are grouped together into a scan pool that is capable of scanning backups of VMware and unstructured data on Windows or Linux NetBackup clients, and NAS data protected by DNAS policies. When adding scan hosts in a single scan pool, configure a common malware scanner for the desired protocol type. Avoid mixing different malware scanners or protocols within the same scan pool.

Malware scanning can be initiated on demand using the WebUI, or configured to launch automatically when a high anomaly score is generated from anomaly detection activity. You can also create custom data protection workflows to scan backups using our powerful APIs.

Malware detection leverages the components for Universal Shares—a value-add for media server deduplication pools (MSDPs), without the need to configure a specific share for scanning. Veritas Flex write once, read many (WORM) storage servers and NetBackup Appliances have the prerequisites for malware detection pre-installed. RHEL-based Media MSDP Servers can easily add Nginx, NFS, and Samba, as needed, from Linux repositories. Follow the guidance in the existing documentation on configuring the components to enable your desired protocols, and execute the following command to complete the process:

```
/usr/openv/pdde/vpfs/bin/vpfs_config.sh --configure_byo
```

The MSDP storage server exposes the stored backup image to the scan host as a read-only share, therefore there is no additional risk to reading a potentially impacted image. As an image passes through its storage lifecycle policy (SLP), you can scan images once they reside on MSDP without interrupting the secondary SLP operations.

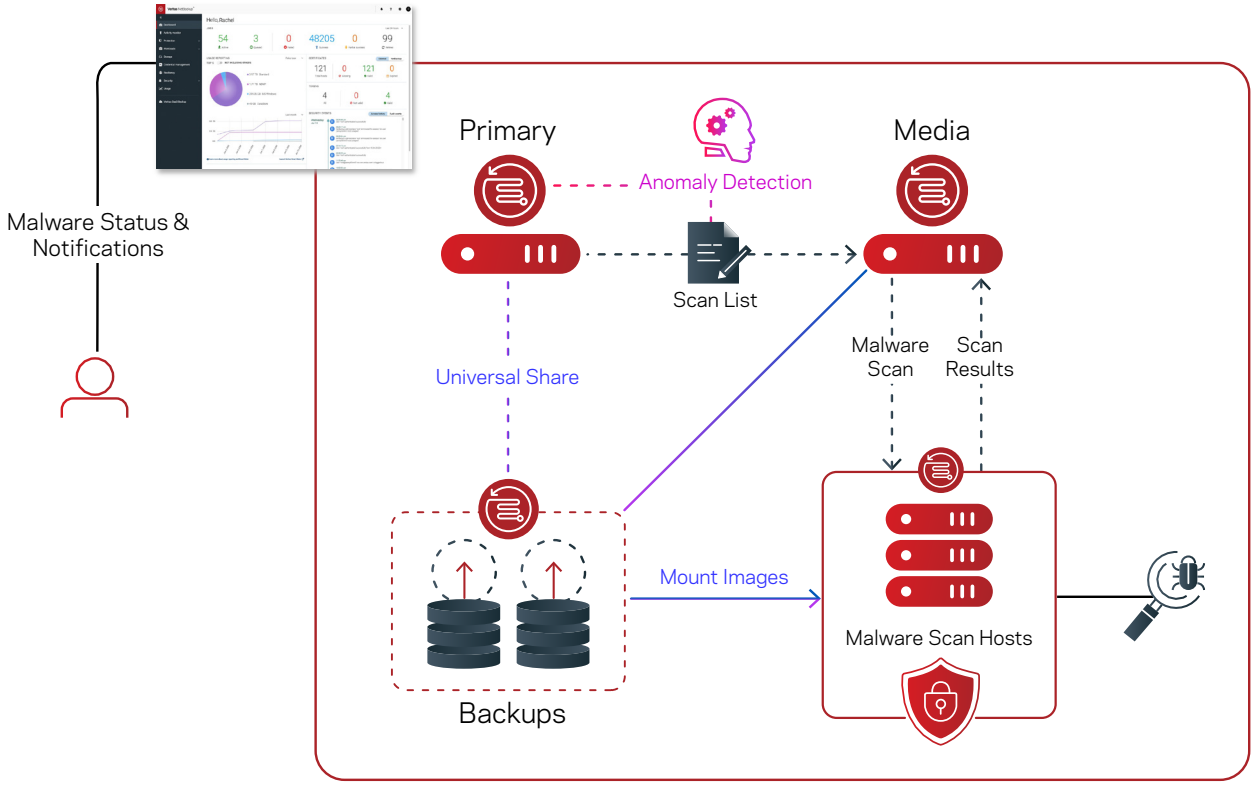

Figure 4. An overview of malware scanning and anomaly detection using NetBackup

NetBackup includes an on-demand scan model in the WebUI that performs periodic image inspections. You can configure automatic scanning to occur when images reach the anomaly score you select. On-demand scans should be used primarily on critical data and high-risk machines. These are hosts interfacing with the public Internet, Internet-of-Things (IoT) devices, and other edge machines. NetBackup supports malware detection for unstructured data for policy-protected Windows, Standard, VMware, and NAS data. Because of the nature of incremental schedules for virtual machines, we cannot perform malware scans for incremental backups of VMs that did not use the NetBackup Accelerator feature. VMware block-level incremental backup (BLIB) images are not always made up of complete files, but rather changed blocks of those files. When Accelerator is used with VMware policies, file boundaries are stable since a full image is synthesized behind the incremental image on the deduplication storage, and a virtual file system can be created for malware scanning. Attempts to scan an incompatible VMware policy schedule or an encrypted file system will result in an error.

VMware recovery points provide visibility into the malware scan status. For an infected image, the VMware Administrator RBAC role prevents the user from initiating the Instant Rollback feature, in order to limit the spread of malware. For an image that is not scanned, a cautionary dialog is presented but the action can continue.

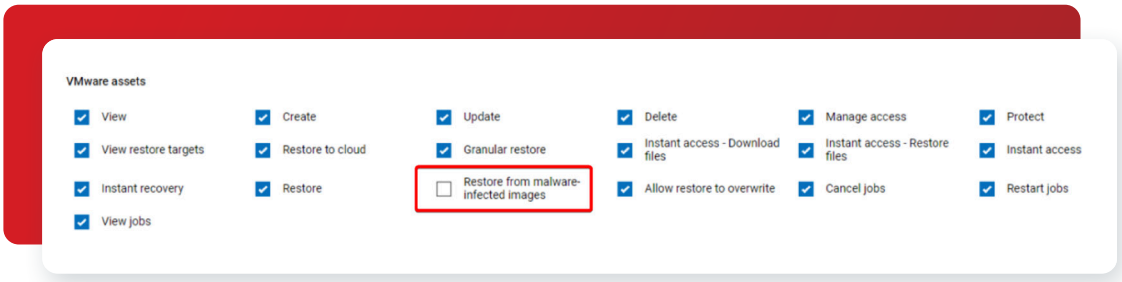

Figure 5. RBAC permissions preventing malware-infected restores

On demand scanning targets images within a specific range according to your selection, and each image will be scanned in a single task. The scan status is stored in the catalog and offers common remediation actions. This also triggers an alert in the top-right notification section of the Web UI.

NetBackup media servers running versions 10.2 and above can use batching to increase malware scanning performance. Images with over 500,000 files are scanned in batches of 500,000 files. For example, if a backup image consists of more than one million files, it will be processed as two 500,000 file batches. Each batch is created and scanned seperately on a different scan host (in parallel) if multiple scan hosts are configured/available. Note that the Malware Detection UI *will not* show the individual batches, and only a single backup image entry is shown in the WebUI. Instead of individual batches, the WebUI shows scanning progress as percentage of the number of files scanned instead of the total number of files. This feature avoids a confusing display that doesn't match the catalogs. It also shows the true scanning progress despite various scan hosts finishing their batches at different times.

Parallel scan host limits can be set globally, or on individual scan hosts. This allows you to limit the number of simultaneous scans on any scan host with one global setting, or on each scan host with a custom local setting. How you use these settings depends on how often you add/delete/change scan hosts, and the similarity of their capabilities such as available RAM, CPU, disk speeds, and networking. If no specific value is configured on a scan host, the global default setting is used. The default global limit is three simultaneous scans per scan host. The minimum configurable value is one and the maximum is ten.

Key metrics are included in uploaded telemetry data collection to enhance this feature. These metrics benchmark existing performance and performance changes over time. They establish what "normal" scanninng performance is in any given NetBackup domain:

- Number of scan operations performed
- Size of backup data scanned
- Number of infected images found
- Number of infected files found

If a scan operation fails, users can copy the failure message from the Web UI. Failure messages include information requred to search logs for more details. For example, this error shows which backupId and worklistId to search for in the nbwebservice and other logs for more details about this failure:

```
backupId: filer-1.hyperconverged.yourorganization.com_1673869734: worklistId: 174: Failed to connect to the scan host.
```

Once a malware-infected image is detected, you can view or export the list of infected files, expire all copies, view or export infected file lists, or leave the image in place where the scan status tag will alert when the backup image is selected in a recovery workflow. The last-known-good image will be clearly visible in the recovery workflow as the most recent image that is not infected. Selecting an infected image will present several warnings.

Each malware detection notification in the Web UI contains a URL so users can download list of infected files in the scanned image. Audit events are generated when anomaly detection triggers a manual or automated malware scan. These events create messages containing accessible lists of Infected file names associated with the backup image(s) that triggered the scan(s). These messages can also be sent to a SIEM security monitoring platform.

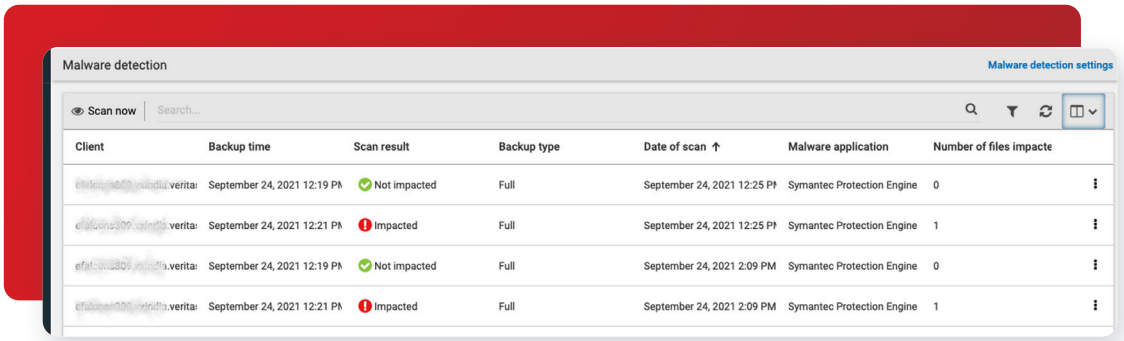

Figure 6. An overview of malware scanning results in the NetBackup web UI

For unstructured data protected by Windows or Standard policy types, NetBackup offers CLI commands to ensure only clean versions of files are recovered.

Conclusion

In conclusion, NetBackup malware detection provides more control in the detection and recovery portions of the workflow. On demand malware scans and scans triggered from high anomaly scores ensure confidence in the data integrity of the backup image. Storing the scan's status in the NetBackup catalog empowers you to restore confidently, with visibility into the malware scan status. Add malware scanning to NetBackup for added resistance to the growing cyberthreat landscape.

VERITAS

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

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

V1587 09/23