VERITAS

NetBackup Malware Detection

Bolster your defenses inside the perimeter.

Technical Brief | September 2022

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.

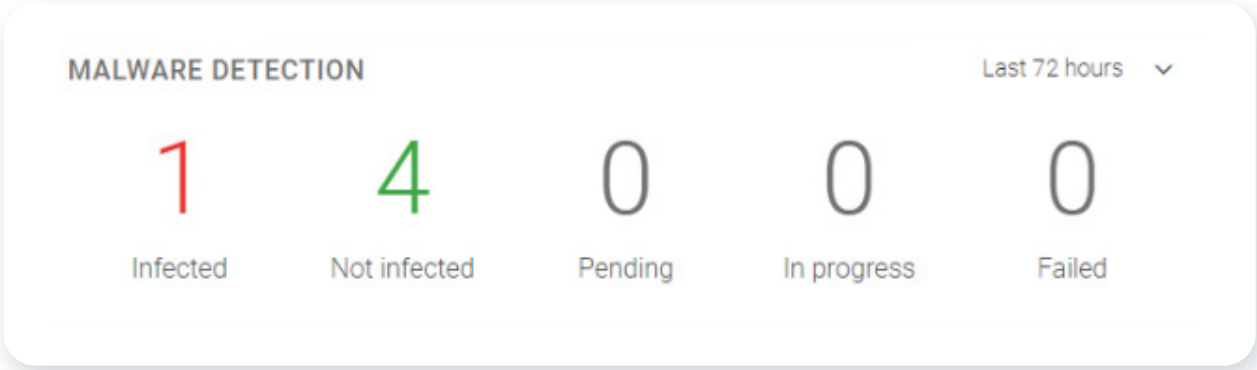

Figure 1. An overview of the malware detection dashboard in the NetBackup web UI.

NetBackup malware detection provides another line of defense against undesirable data propagating in the environment. While the anomaly detection engine works automatically, malware detection lets you distinguish between clean or infected recovery points for VMware virtual machines, Standard backups, and Windows backups. Malware detection offers a powerful point of insight into the backup images as a response to an alert or an on demand scan.

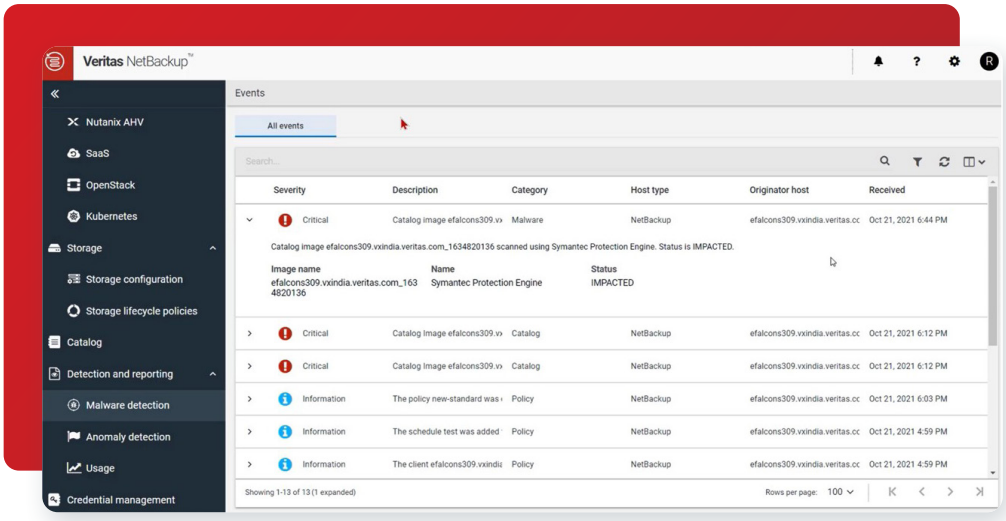

Figure 2. A detail of a malware event selected in the NetBackup web UI.

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.

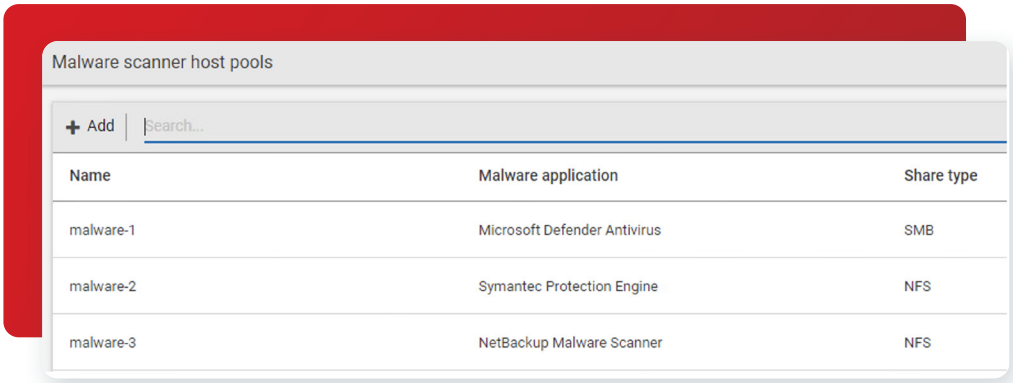

Figure 3. The malware scanners available in the NetBackup web UI.

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. 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 launched 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.

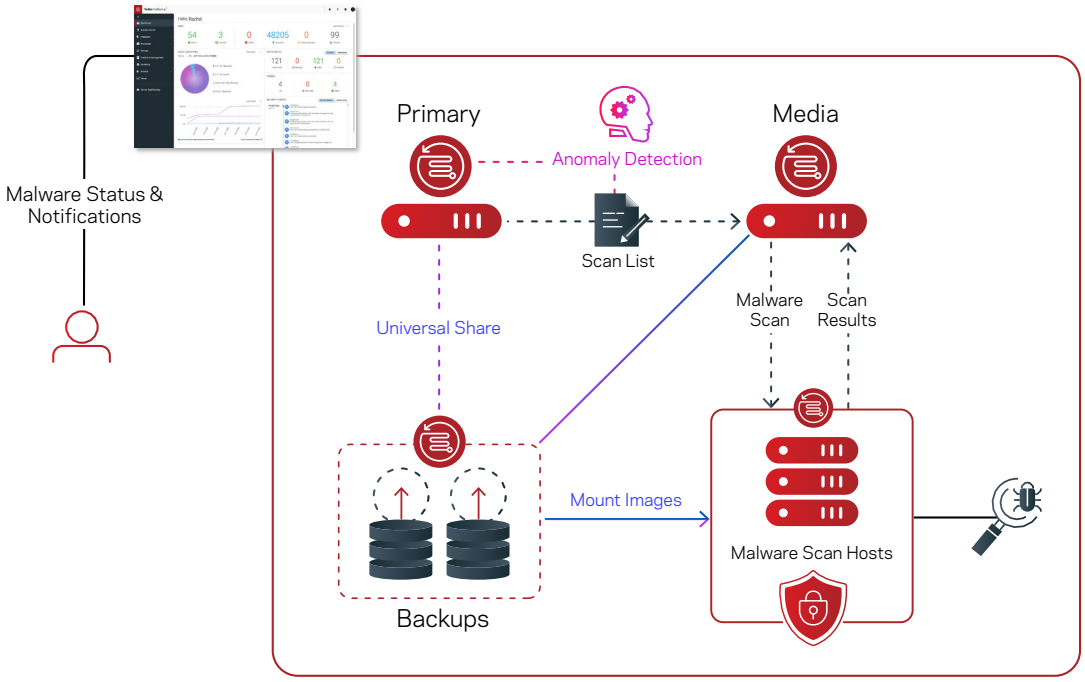

Figure 4. An overview of malware scanning and anomaly detection using NetBackup.

An on demand scan model in the NetBackup WebUI is focused on periodic inspection of images, with the option of enabling automatic scanning for images with high anomaly detection scores. Focus your on demand scans against the critical data and high-risk machines—hosts interfacing with the public internet, Internet-of-Things (IoT) devices, and other edge machines. NetBackup supports malware detection for unstructured data for Windows, Standard, and VMware policy types. 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 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.

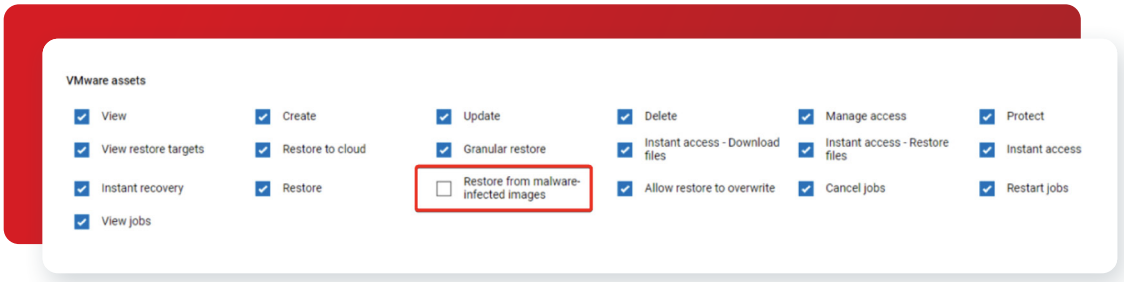

Figure 5. RBAC permissions preventing malware-infected restores.

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 WebUI.

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.

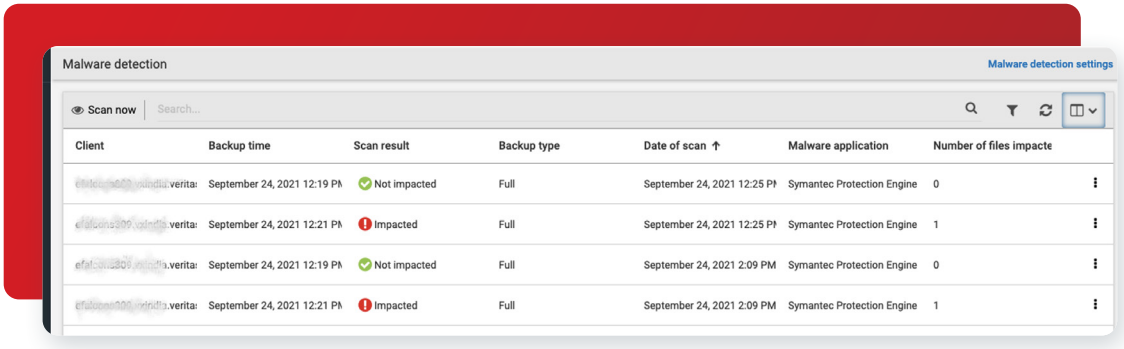

Figure 6. An overview of malware scanning results in the NetBackup web UI.

For unstructured data protected by Windows or Standard policy types, NetBackup offers the bpcleanrestore command that ensures only clean versions of files are recovered. If a file selected for restore is marked as infected, the clean restore will restore a previous clean version of the file from an uninfected backup. If a clean version of the file does not exist within the selected date range for recovery, that file is skipped during recovery. This avoids re-infecting the target machine. This command should be familiar since it parallels the often-used bprestore command.

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 cyber-terror threat landscape.

About Veritas

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

VERITAS

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

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

V1507 09/22