NetBackup 10 Anomaly Detection and Malware Scanning

Leverage the advanced capabilities of a unified resiliency platform to deliver ransomware anomaly detection and malware scanning.

Introduction

IT organizations are beginning to understand the importance of interconnected operations to get a complete picture of their environments in the face of security threats such as security breaches and bad actors. Enterprises are being forced to respond promptly to fast-moving changes in data, especially in the case of ransomware threats. Anomaly detection can be key in solving such intrusions while detecting anomalies, disruptions of normal behavior that indicate the presence of intended or unintended attacks

Given the amount of data handled by Veritas NetBackup™ on an hourly and daily basis, there is no effective way to manage and analyze constantly growing datasets manually. Because NetBackup has numerous components in perpetual motion where "normal" behavior is redefined continuously, NetBackup 10 includes anomaly and malware detection to process data faster and more efficiently to detect abnormal events, changes or shifts in NetBackup datasets. This anomaly detection relies on artificial intelligence (AI) to identify abnormal behavior within the pool of collected NetBackup data, with the objective of providing advanced warning of a ransomware event. Malware Detection relies on industry-leading scanners integrated with NetBackup for on-demand scanning.

The Challenge

Enterprises need to be empowered with a solution that can identify data points, events and actions that are outside the expected data behavior patterns of a given set of users, whether at the edge, the core or the cloud. NetBackup 10 provides anomalous insights into activities and can provide indicators of ransomware and bad-actor behavior. The NetBackup 10 anomaly detection solution can serve as an early indicator of infrequent but anomalous activities and can help address these issues when used in conjunction with security products.

Many organizations do not have the automated capabilities to identify data growth, kilobytes transferred, dedupe ratios and image size across their backup environments, which makes it harder to manage the security and lifecycle of their data. Backup and cloud architects often need to work with security teams to provide information that exposes early insights and allows these teams to proactively take steps to remediate and prevent security breaches and data loss.

The Veritas products are developed with resiliency at top of mind, so we could provide organizations with dependable solutions to ensure their business remained up and running with minimal impact. Our solutions protect IT systems and data integrity with a wide range of security controls. These tools monitor and detect threats with a complete view of your user activity and data infrastructure and provide backup monitoring capabilities to ensure your critical data is protected and also provide early warning of threats that have infiltrated your environment. Veritas and NetBackup™ software have been synonymous with resiliency for decades. Dependable Veritas solutions incorporate proven technology, so you can protect, detect and recover quickly with automation and orchestration at scale.

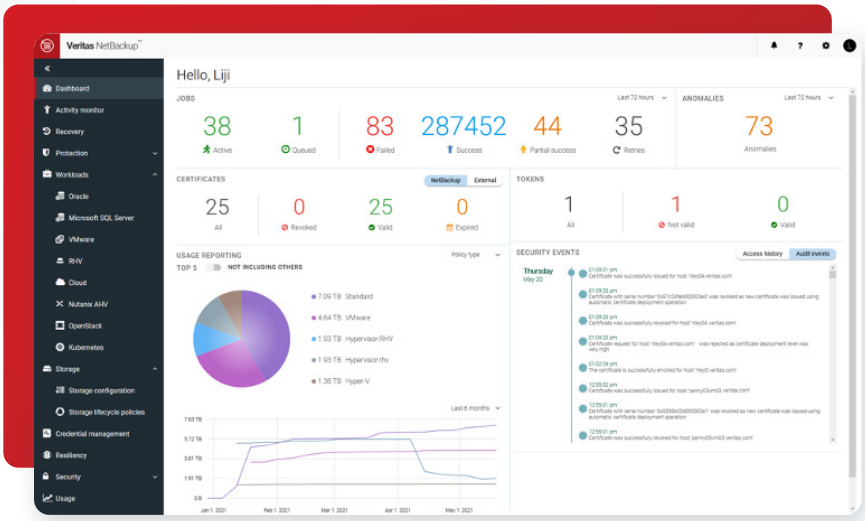

Figure 1. The NetBackup 10 user interface provides insight into the number of anomalies and security events detected.

The NetBackup Approach to Ransomware Anomaly Detection

The Veritas approach to anomaly detection reliability recognizes that the goal is to ensure security for mission-critical data, provide insights that ensure they are not compromised by ransomware and deliver actionable information for backup administrators to address changes in their environment. NetBackup 10 anomaly detection also recognizes that reliability and insights should be simple, easy to use and extensible to derive the greatest value.
(See Figure 1.).

The Benefits

NetBackup 10 anomaly detection derives its unique value from an extensible and robust architecture that offers numerous advancements. Our machine-learning approach seamlessly integrates into the NetBackup primary server and requires minimal configuration. This process allows NetBackup to detect anomalous forms of observations—those not falling into the cluster can then be considered as anomalies or outliers. The detection engine calculates a parameter based on the historical data available after a certain frequency and adjusts to custom backup policies to reduce false positives
(see Figure 2).

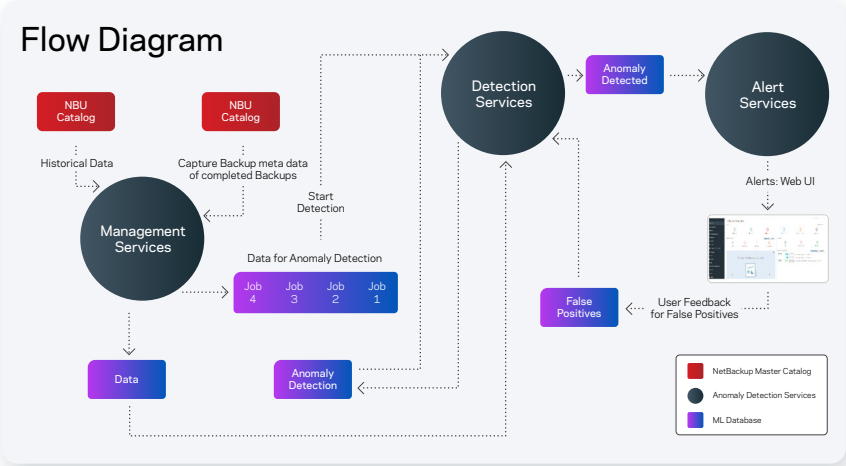

Figure 2. A high-level flow diagram showing the relationship between the NetBackup primary server and the detection services to the alert services.

As shown in Figure 3, the NetBackup user interface (UI) provides the ability to reliably report on anomalies based on a variety of criteria:

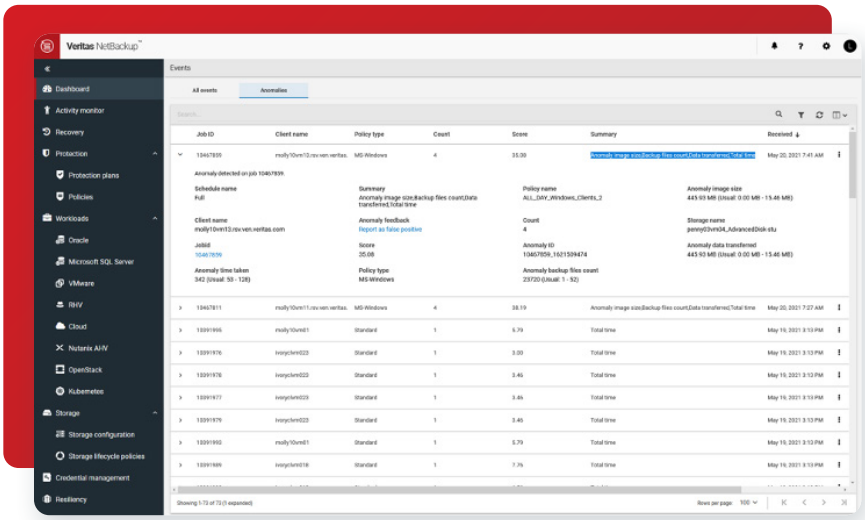

Figure 3. A drill-down from the NetBackup UI shows the details of the anomalies detected.

- JobID—The ID number of jobs for which the anomaly was detected
- Client name—The name of the client on which this anomaly was detected
- Policy type—The type of policy for which the anomaly was detected
- Count—The number of anomalies in this job
- A score—An anomaly score. The higher the number, the higher the severity of the anomaly. This score is the distance to the nearest cluster from the anomaly observation in a standard deviation scale
- Summary—The anomalies reported under this job

- Received—The date at which the anomaly was received
- False positive—Whether the false positive has been reported or not

Primary Server Overhead

A requirement of any good anomaly detection solution is a large dataset. The larger the dataset, the greater the accuracy of identifying an outlier. With a large dataset comes the challenges of performance and the impact on the NetBackup primary server. Using an innovative approach that leverages the Nbdeployutil on the NetBackup primary server helps to gather anomaly data much faster. This data is by default available on all primary servers. As a result of this approach, we see low memory and CPU utilization during data gathering, reducing the need to increase server resources.

Malware Detection Bolsters Your Defenses Inside the Perimeter

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

NetBackup Malware Detection provides another line of defense against undesirable data propagating in the environment. With the Anomaly Detection engine working automatically, you can now add Malware Detection workflows. Malware Detection offers a powerful point of insight into the backup images as a response to an alert or on-demand scan of a backup image, (see Figure 4).

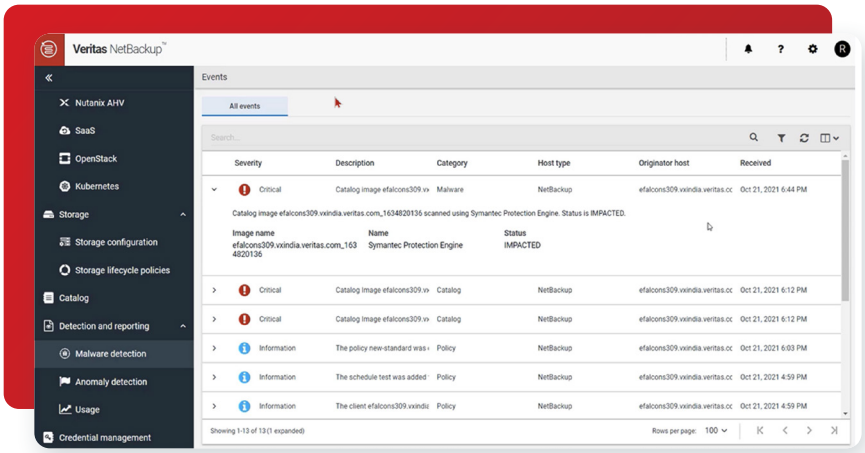

Figure 4. A drill-down from the NetBackup UI shows the details of the malware identified.

NetBackup 10 Anomaly and Malware Detection Value

The included NetBackup 10 anomaly detection engine seamlessly integrates with the NetBackup primary server and requires minimal configuration. This capability lets a backup architect or security administrator see anomalies and drill down to identify any concerns. It offers the ability to mine large amounts of data and provide actionable intelligence to address ransomware events or simply changes in the environment with which an administrator should be aware. Fully automated with the ability to reduce false positives that will learn over time, NetBackup 10 anomaly detection allows enterprises to feel confident in their environment. Paired with Malware Detection, high-scoring anomalies can alert on real threats in close proximity to infection events.

NetBackup 10 reduces the staggering complexity of enterprise data protection with a unified solution built on converged infrastructure. It easily scales while providing best-in-class performance for petabyte-level capacity and paves the way to IT as a service through convenient self-service operation and a ransomware-protected environment.

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.

VERITAS

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

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

Copyright © 2022 Veritas Technologies LLC. All rights reserved. Veritas, the Veritas Logo, and NetBackup are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

V1351 02/22