VERITAS

Cross-Cloud AI-Powered Anomaly Detection

A powerful tool for monitoring your cloud data and user activity.

Anomaly detection is a powerful early warning system that tracks and alerts for out-of-the-ordinary activity or strange behaviors of your cloud data and user activity. Essentially, it helps to see problems before they occur. Detecting these anomalies is now a critical practice for data security, as anomalies can be indicators of a security breach, a hardware or software problem, shifting customer demands, or any number of challenges that require immediate attention. It works by using a process of locating unusual points or patterns in a set of data. Anything that deviates from an established baseline (within a predefined tolerance) is considered an anomaly. With an established set of parameters and intelligent indicators, customers are alerted for anomalies requiring immediate attention and can easily view a dashboard that is updated in real time with activity monitoring. Examples of anomalies include unusual file write activity that could indicate infiltration (but could also be detecting known ransomware file extensions), file access patterns, traffic paths, or even an unusual jump in activity compared to typical patterns. Being notified immediately of anything out of the ordinary provides a valuable advantage to act or mitigate quickly. It is so valuable to be able to stay on top of any issue as it arises, or mitigate a risk and isolate it quickly to prevent anything destructive, downtime, or other issues related to a breach.

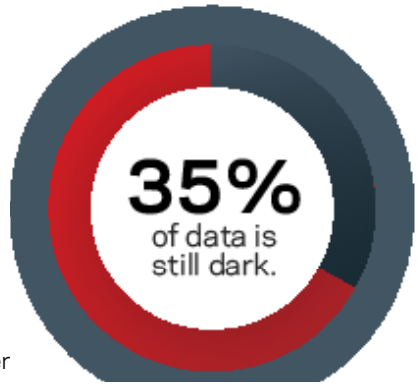
The Power of a Data Watchtower

With cloud data exploding in size and sprawl, there is increasing need for anomaly detection, to serve like a watchtower over all your cloud data, especially in the face of cyber threats and ransomware. Historically, cyber criminals have gained access to systems and data in a variety of creative avenues. They get into a system, start encrypting, and download as much as they can, only to escape before detection. In this scenario, anomaly detection would alert you about the issue, and help you take action.

Cloud is the number one ransomware attack vector for cyber criminals in 2022[1], and now cyber criminals often play the long strategic game, taking a few plays from the organized crime playbook. They have perfected the art of cyber-reconnaissance. A practice often called dormant ransomware or sleeper ransomware, is now a regular occurrence in the digital world. What this means is that once access is gained, criminals will strategically lay low and remain hidden. Why? Because their top priority is to observe, learn, and move across your cloud environments trying to find your weaknesses and exploit your vulnerabilities—all while waiting for the optimal time to strike. In this situation, detecting them before they have the chance to take action provides a powerful opportunity to know about problems before they occur, and take action to prevent a devastating impact.

Bad actors are highly motivated to cause as much destruction as possible to make more money and maximize their efforts—just as with any business, it's all about ROI. Some reports suggest that ransomware may lay dormant for up to 18 months. The bad actors know that optimal destruction depends on multiple factors such as timing and scope. They want you to have zero choice but to pay their ransom. The old days of a breach and attack happening at the same time are long gone. This added complexity means that they can often know your systems better than you do, therefore the chance that they launch a series of events designed to disrupt and disable critical systems to net larger payouts is rising drastically.

Cross-Cloud Data Visibility



Before an organization can implement successful anomaly detection, it is important to first take a step back to ensure that you know where all your data resides, and make sure that you don't have any dark data lurking in your environment. According to Veritas Vulnerability Lag Research[2], 35 percent of data is still dark. That is alarmingly high. We recommend you get to work discovering what data you have, and where it is—immediately.

Veritas solutions provide a comprehensive view of all your data across all your cloud providers, physical, and virtual environments. You also have a view of your storage, to compute capacity, to ever major data protection solution and cross reporting, which ensures no system falls through the cracks. This is especially crucial in today's threat landscape, as cyber criminals are hoping that you are not keeping an accurate inventory of all your applications and data, or that there may be areas where you have limited security and/or oversight to your data.

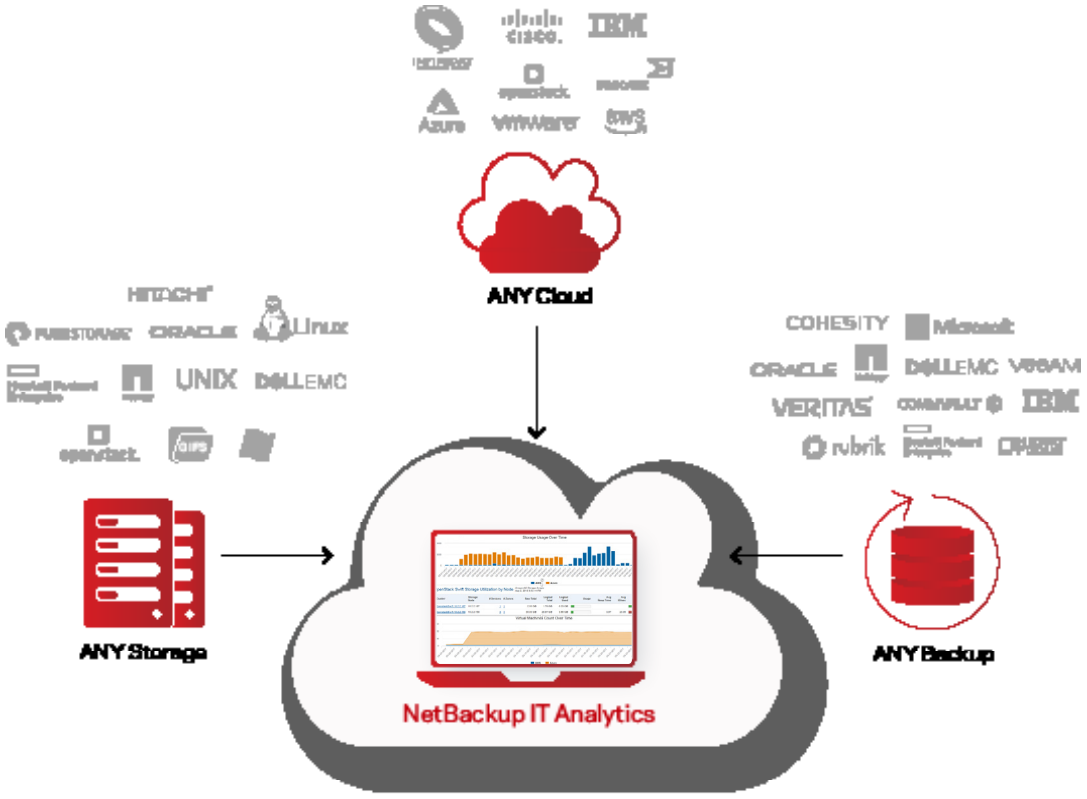


Figure 1: Unified IT infrastructure across all your data, regardless of where it is

In addition to shining a light on the dark areas of your environment, Veritas solutions provide comprehensive insights, alerting and reporting across on-prem, cloud, data protection, and storage. You'll have the insights needed to make informed decisions in the face of a cyberattack with reporting options that help you gain visibility into your backup environment, enabling your organization to:

- Discover all hosts or virtual machines (VMs) in your infrastructure and compare them with the VMs protected by NetBackup™
- Flag hosts that are missing from the backups, or have no recent backups, as potential risks
- Detect the potential ransomware-affected files, along with their size and where they reside in the environment
- Access interactive graphs that provide a historical view of the risks generated

Cross-Cloud AI-Powered Anomaly Detection

Once your data visibility is in place, the next step is to implement AI-powered anomaly detection. Veritas NetBackup detects anomalous data and user activity across your entire environment and alerts you to suspicious anomalies, in near-real-time. The technology is designed to mine an enormous amount of data, automate monitoring and reporting, and provide actionable insights into what is happening in your environment.

A great way to visualize Anomaly Detection is to envision a polygraph test. When you take a polygraph test, the examiner will begin with pre-screening where they ask a series of questions to establish parameters that will constitute normal as a baseline. When you lie, the physiological indicators of **blood pressure, pulse, respiration, and skin conductivity** will fluctuate, expectedly, outside of the normal parameters established. Similarly, NetBackup will leverage an AI-powered detection engine to calculate parameters of what constitutes normal based on backup job metadata patterns over time, and auto-adjusts for custom backup policies.

Events that occur outside of the established normal are captured, and notifications happen in near-real-time. Anomalies observed are assigned a score based on severity, which is calculated based on the observed distance from the cluster. The farther the distance, the more severe the score. This is designed to help administrators identify which insights are actionable, and to reduce false positives.

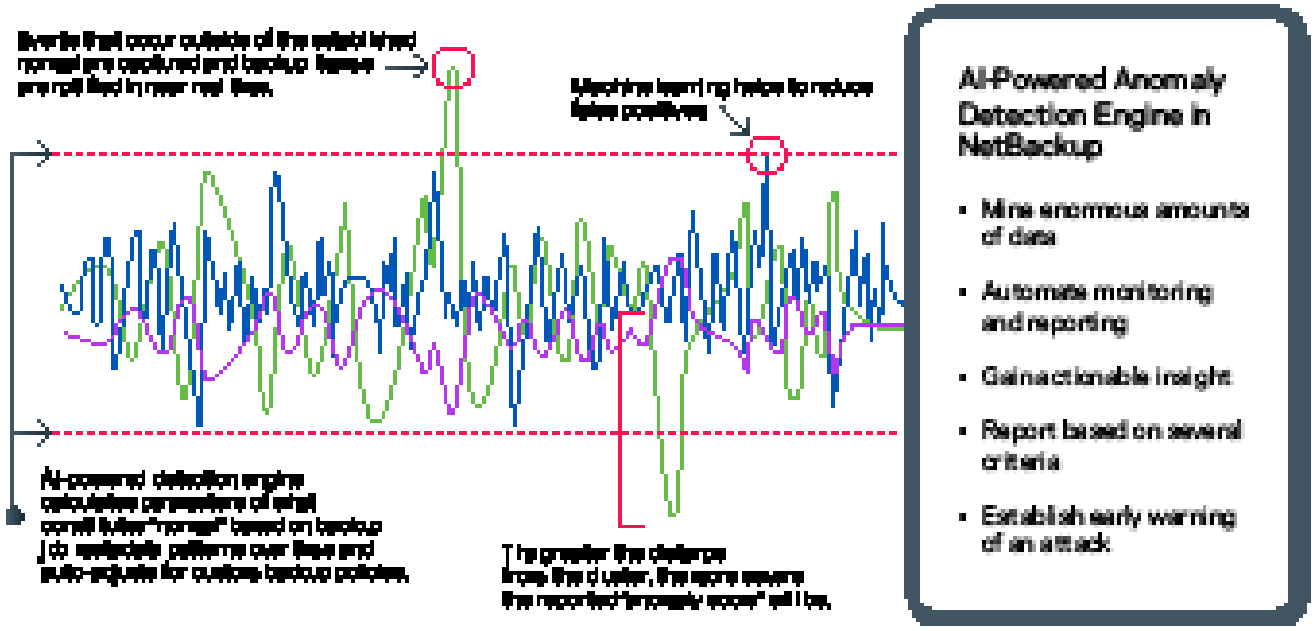


Figure 2. Understanding anomaly detection.

Overall, the AI-powered anomaly detection engine in NetBackup helps you mine enormous amounts of data, automate monitoring and reporting, gain actionable insights, report based on several criteria, and more importantly, establish early warning of an attack. Administrators have the ability to view data and provide recommendations associated with anomalies at any time by monitoring all devices and establishing early warning of any attacks, to stay on top of issues as they arise. For example, NetBackup's AI-powered anomaly detection seamlessly integrates into the NetBackup primary server, enabling it to detect anomalous forms of observations—considering those that do not fall into the cluster as anomalies or outliers. This capability lets an administrator see anomalies and drill down to identify any concern. It offers the ability to mine large amounts of data and provide actionable intelligence to address ransomware events, as well as simple changes in the environment that an administrator should be aware of. These solutions can help recognize indicators that an attack is underway, or potentially about to begin, which enables you to take immediate action and limit the impact.

The tool is also intelligent, with the ability to identify potential false positives by comparing historical backups against the new backup, and identifying anomalies such as significant changes in job durations, image size variations, and/or policy configuration changes. The AI engine monitors files or groups of files, and understands when file characters are changing (down to the metadata level) regardless of whether it is in block disk or object storage in the cloud—all with no post processing. Only Veritas can scan and monitor all systems, is agnostic, and can cover all cloud platforms including third-party backup products. Our artificial intelligence/machine learning (AI/ML) engine can run on any server. This level of coverage ensures the elimination of blind spots.

Malware Scanning

Veritas can help you detect multiple types of malware such as encrypting and exfiltration, providing automated and on-demand scans. The automated malware scanning feature will remove human dependencies and allow AI/ML technology to jump in and scan for malware. The AI/ML malware scan is automatically triggered by a high anomaly score. Scanning includes unstructured data, Windows, Linux, and VMware. This inclusion is vital because malware often enters your environment in a home directory, as these are typically the locations where large sets of unstructured data exist.

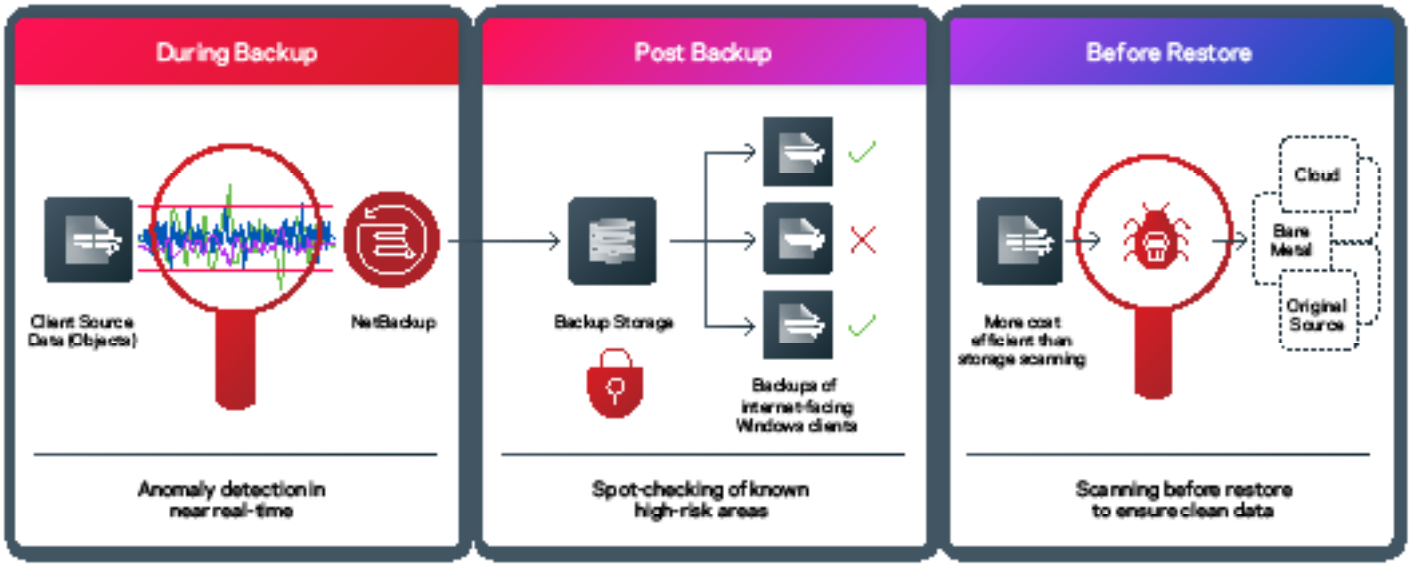


Figure 3: Malware scanning overview

Additionally, when recovery is necessary, the backup data can be scanned, ensuring the latest malware signatures are leveraged. Clear visuals and warning prompts provide awareness of infected backups, ensuring all data restored is clean and unimpacted. This practice is often referred to as restoring to the last-known-good copy.

Veritas is Secure by Design

Veritas delivers all of this unified data visibility, anomaly detection, and malware scanning through NetBackup IT Analytics.
A sample dashboard is pictured below.

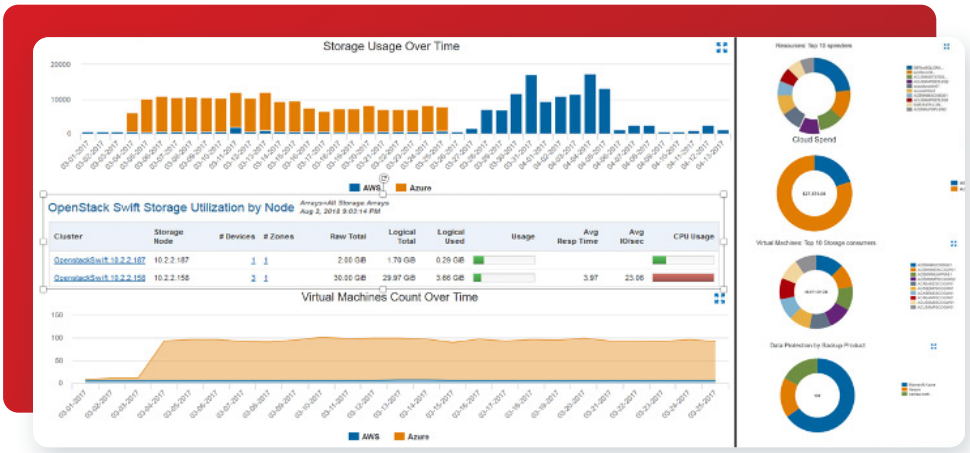


Figure 4. A sample NetBackup IT Analytics dashboard showing storage usage over time.

NetBackup IT Analytics Attributes:

- **Comprehensive**—A single solution from an integrated console to identify data assets, NetBackup IT Analytics provides support for every popular server, storage, hypervisor, database, and application platform used by enterprises today.
- **Scalable**—Centralized management provides an agentless data collector gathering approximately 30,000 unique data points from all aspects of on-premise and cloud environments, including applications, cloud, data protection, hosts, network, storage, virtualization, and unstructured data.
- **Innovative**—NetBackup IT Analytics' proprietary algorithms—driven by five patents for autonomous design, and updates from the cloud—analyze data points and make recommendations that improve performance, resiliency, and utilization. The analysis is machine-led, but governed by human policies, with data used to present actionable solutions to help improve efficiency measures and minimize risk, predict failures, and streamline audits and compliance.
- **Proven**—For more than a decade, NetBackup IT Analytics has led the industry with customer-proven scalability and reliability, bringing together and analyzing data from across the organization.

NetBackup IT Analytics Key Features:

- An integrated console providing insight into:
  - Local and cloud backup, compute, and storage
  - Cloud and on-premises capacity, cost, and usage
- Chargeback:
  - By any user-defined group, such as application, department, and cost center
  - Usage across backup and cloud, compute, and storage
- Capacity planning:
  - Budget based on cloud costs and use rates
  - Media/storage planning based on consumption usage

Maximize Cloud Business Value with NetBackup IT Analytics

At Veritas, we've found that organizations are moving to the cloud for several reasons: smaller organizations benefit from reducing the draw of maintaining a data center and/or disaster recovery site; midsize organizations appreciate accessible off-site data storage built on highly scalable hardware, leveraging just-in-time cloud recovery; and large organizations are identifying workloads capable of taking advantage of cloud availability and cost, while freeing up expensive data center space for mission-critical workloads. Sometimes an organization requires temporary space for a workload. Instead of ramping up a new rack of disks in a data center, it can leverage space at a cloud provider to avoid the additional cost of purchased data center hardware. Cloud subscription models work well for these projects, offering scalable, simple-to-use models.

The current mega-trend of moving data to the cloud revolves around driving costs down for businesses. The cloud model is agile when it comes to requirements, enabling organizations to add a disk to a server easily and quickly, versus sourcing hardware and the rack and stack that comes along with it. The cloud also allows organizations to avoid the cost and time associated with replacing or upgrading hardware and software in the data center. Instead, these requirements are fulfilled by the cloud service provider and are invisible to the business itself. Regardless of what reason drives an organization to decide to transition to the cloud, NetBackup IT Analytics can ensure the experience is compliant and cost-effective, versus an on-premises environment.

Veritas provides you with an AI-powered watchtower, so you can take control of your expanding cloud data. With Veritas you can confidently know where all your data is, in a single-pane of glass for all enterprise data, wherever it resides. 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. Veritas eliminates uncertainty with complete data visibility technology, intelligent anomaly detection, and malware scanning—all delivered through NetBackup IT Analytics.

Think beyond cloud-native utilities and point products, and architect a unified strategy for data management with cyber security and data safeguards paramount.

Veritas provides you with cloud control.

1. https://www.esg-global.com/ransomware
2. https://www.veritas.com/content/dam/Veritas/docs/reports/GA_ENT_AR_Veritas-Vulnerability-Gap-Report-Global_V1414.pdf

About Veritas

Veritas Technologies is a global leader in data protection and availability. Over 80,000 customers—including 95 percent of the Fortune 100—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

V1627 09/22