Enhancing HPE NonStop Backup Security with Intelligent Anomaly Detection

Written by Mike Mitsch

Backup Targets: Next Up in Malicious Defense

As cyber threats continue to evolve, HPE NonStop clients must expand their security frameworks to include robust protections for backup data. With cybercriminals adopting increasingly sophisticated tactics, particularly through the use of Artificial Intelligence (AI) backup environments are becoming high-value targets for ransomware and other malicious attacks.

AI-enhanced ransomware techniques add complexity to threat detection, allowing malicious actors to penetrate security layers and infect both production and backup environments, often undetected.

In response, many backup solutions now include basic ransomware detection features. However, with AI-driven threats on the rise, it is no longer sufficient to rely solely on cybersecurity software. Backup targets themselves must actively participate in threat detection and mitigation.

ETI-NET BackBox and QoreStor are Uniquely Positioned for Anomaly Detection

With the introduction of anomaly detection[1] in QoreStor 7.4, the role of the VTC has evolved to include malicious detection. The VTC is now positioned not just as a passive data repository but as an intelligent sensor capable of identifying unusual activity within NonStop backup data.

While the introduction of anomaly detection for NonStop backup data does not replace traditional cybersecurity software, it provides a valuable complementary layer of insight—especially crucial for NonStop environments that handle high volumes of transactional data.

Together, BackBox and QoreStor offer a uniquely strategic vantage point for identifying anomalous behavior. While not a direct replacement for cybersecurity solutions, it serves as an ideal way to complement these security solutions. It provides additional very valuable information that can help identify active or even previously undetected ransomware. Given that NonStop Backup targets often aggregate and store large amounts critical transaction data the BackBox VTC with QoreStor is uniquely positioned to detect anomalies in organizational data.

Understanding NonStop-Related Anomalies

NonStop environments regularly experience fluctuations in data activity that may be misinterpreted as threats. Examples of legitimate business-driven anomalies include:

- **DSM/TC** cleanup of backup files

[1] https://www.quest.com/learn/what-is-anomaly-detection.aspx

- **Increased transaction workloads** leading to more frequent writes of TMF Audit Trails, Enscribe files, and third-party applications logs written to backup storage.
- **NonStop Infrastructure modernization** resulting in migration of backup data from one physical storage location to another
- **End of life for** data, application, or project. Organizations may terminate an application or project and archive or delete all data associated with it.

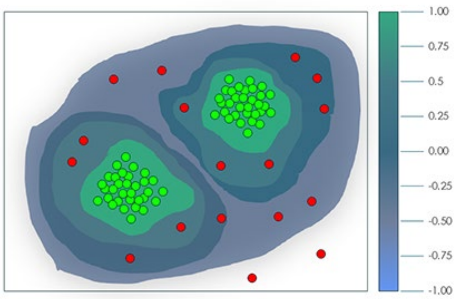
These and other events, while non-malicious, deviate from a NonStop organization's normal backup data access and usage patterns. As a result, these deviations may be classified as an anomalous event. However, these anomalous events do not automatically equate to malicious activity. Rather, they represent business-related anomalous events that should not internally raise security concerns.

Monitoring NonStop backup data by BackBox QoreStor can assist organizations identifying events that may be undetected by cybersecurity software. Malicious activity may begin with data exfiltration, deleting or encrypting production data, and/or changes to backup processes. Should any of these events occur, the primary backup target may be detected through independent monitoring.

Informed AI2 Provides Intelligent Anomaly Detection

BackBox 5.0 with QoreStor 7.4 represents a generation of primary backup targets that incorporates generative AI to perform anomaly detection. This enables the VTC w/QoreStor to use artificial intelligence and machine learning to examine NonStop backup content stored in the respective VTC data stores and build a abstracted representative model. This enables QoreStor to effectively learn the ways that NonStop backup data comes and changes over time. Using this process QoreStor builds a model to study the ingest, access, and usage patterns.

Through isolation forest technology[3] QoreStor starts to identify clusters forming from various data sets (Figure 1). identify unusual patterns in data to isolate anomalies quickly and ensure rapid detection of potential threats. With low linear time complexity, this method is highly efficient for large datasets. For NonStop customers, this means improved data protection and quick identification of threats. Data sets that lie outside of these identified clusters may deem as anomalies.



The challenge for NonStop backup data analysis is twofold:

1. Determine when these outlying data sets "officially" become anomalies.

2. If deemed as an anomaly, classify it as business related, suspicious or a malicious anomaly.

To help make this determination, QoreStor uses machine learning to build a normalized model using isolation forest technology to get trained on the operational state of NonStop backup and restoration systems. To do so, it must first complete a minimum training period of 90 days (which can be adjusted) for QoreStor to begin making informed predictions.

[2] https://www.sciencedirect.com/science/article/abs/pii/S026840122200010X
[3] https://www.researchgate.net/publication/224384174_Isolation_Forest

Once enabled, QoreStor can determine if anomaly is business-related or suspicious. By default, every 30 minutes QoreStor checks on items such as:

- I/O operations / wait times
- Increases or decreases in data backup sizes
- Reduction in storage savings (less effective deduplication and compression)
- Unexpected amounts of data removal and overwrites
- Unexpected attempts at logging in to a protocol, to the OS, or its user interface (UI)
- Stopped/paused logging of audit processes

Business Value

When properly configured, anomaly detection becomes more than a security feature, it becomes a business intelligence asset. Organizations that proactively account for known operational events (e.g., data migrations or decommissions) can leverage anomaly detection to:

- Accurately classify business-related deviations
- Prevent false positives
- Improve incident response

Summary

The introduction of Informed Anomaly detection into BackBox with QoreStor provides a powerful tool to not only assist in first response to malicious activity, but it also provides quantifiable business value. Organizations that embrace and configure QoreStor to account for upcoming business events such as data migrations, mass data archiving or deletions, or large influxes of data can benefit by the detection of these business-related anomalous events and accurately classify them.

In summary, NonStop backup anomaly detection can be mainly used for:

- **Malicious Protection**
  Anomalous behavior detection plays a crucial role in ransomware protection for backup data by continuously monitoring unusual patterns or deviations from normal behavior. It helps identify potential ransomware activities early, often before significant damage occurs, protecting your last line of defense and maintaining your ability to recover data.
- **Capacity Planning and Storage Optimization**
  Anomaly detection can identify unexpected increases in storage consumption, which might indicate data growth patterns that need attention or cleanup.
- **Backup Policy Compliance**
  Anomalous backup behaviors, such as incomplete backups, backups happening at unusual times, or missing files, may indicate deviations from established backup policies. This helps ensure that backups are compliant with organizational standards and regulatory requirements.

To know more about how ETI-NET can assist you with your HPE NonStop needs, get in touch with us today at **https://etinet.com/contact-us/**