Commvault®

WHITE PAPER

Anomaly and Threat Detection Primer

THE CHALLENGE

The rise of cyberattacks is forcing organizations to rethink their data protection strategies. While detecting threats remains critical, a more significant challenge has emerged: protecting data from compromise. Attackers are now strategically infiltrating systems and staying undetected for extended periods. Recent copies of protected data will likely contain malicious elements, leaving organizations scrambling to identify safe, uncorrupted data for recovery.

Anomaly and threat detection have emerged as powerful tools to fortify these processes. More than just an early warning system, anomaly and threat detection systems within a data protection solution can increase your confidence that you are storing and recovering clean data. By analyzing anomalies within the data, anomaly and threat detection help with:

Identification of Data Tampering: Attackers may tamper with copies of protected data to manipulate data or cover their tracks. Anomaly detection helps identify unexpected changes in file types, sizes, or access patterns of the data protection solution, potentially revealing hidden threats.

Recovery of Clean Data: By pinpointing clean copies of protected data unaffected by the attack, anomaly detection can minimize downtime and get your systems back in operation faster.

Faster Recovery Times: By identifying threats and anomalies, you can recover uncorrupted data by excluding known threats before recovery begins. This can minimize downtime and get your systems back faster after an attack.

Improved Forensics: Anomaly detection can provide valuable evidence during forensic analysis. By understanding how the attack unfolded and what data was affected, you can determine the scope of the breach and take appropriate measures.

ANOMALY DETECTION

Anomaly detection acts as a data guardian, monitoring activity for unusual patterns. It analyzes metrics like size of the data being protected and access attempts, establishing a normal behavior baseline. Deviations from this norm, such as a sudden surge or decrease in the size of data being protected, unusual deduplication changes, or the number of files created or modified can trigger alerts to prompt investigation.

THREAT DETECTION

Threat detection takes a more aggressive stance by actively searching for known malicious activities. It integrates with security software to scan protected data for malware or ransomware. This proactive defense helps safeguard this data from corruption or encryption. It can also monitor user activity, flagging suspicious attempts to delete copies of protected data or to access sensitive data. A selective approach is recommended. This involves focusing on two key areas:

Critical Business Systems: These are the most important systems for your organization's operations. Prioritizing scans on these systems supports their protection against potential threats.

Alert-Triggered Scans: A system that shows anomalous behavior can trigger a more in-depth scan. This way, you can investigate potentially compromised machines further without using resources on unnecessary scans for low-risk systems.

TYPES OF THREAT DETECTION FOR DATA PROTECTION

1 Signature Scanning

- This method works by comparing files against a database of digital fingerprints known as signatures. These signatures are unique identifiers for specific known malware threats.
- This maps to the following features in Commvault:
  - Threat Scan

2 Cyber Deception

- Cyber deception is a proactive approach that uses strategically placed "canaries" or systems to lure out and identify potential attackers. These canaries can be specific files or fake systems meant to mimic actual production entities. It is inspired by the historical practice of using canaries in coal mines – if the canary stopped singing or died, it signaled danger to the miners.
- This maps to the following features in Commvault:
  - Honeypot file in Commvault Backup and Recovery (trap files are placed and monitored for access triggering the honeypot)
  - Threatwise (setting deception entities to mimic actual production systems trapping malicious activity)

ANOMALY AND THREAT DETECTION AS A COMBINED APPROACH

Some techniques bridge the gap between anomaly and threat detection. One such approach is analyzing user access patterns for anomalies. This could involve flagging sudden spikes in access attempts to data repositories, particularly from unauthorized users or unusual locations. While not definitive proof of a threat, such anomalies could indicate compromised credentials or attempts to tamper with protected data.

Additionally, content inspection techniques can fall into both categories. Scanning protected data for known malicious file types or suspicious patterns can identify established threats. However, these techniques can also uncover unusual file behavior within protected data, which may indicate novel malware or unauthorized data infiltration.

To summarize, anomaly detection identifies novel threats, while threat detection guards against established ones. Early anomaly detection prevents potential threats from escalating, while threat detection helps safeguard protected data from known threats. By combining anomaly detection flags with threat detection techniques, you can gain a more comprehensive view of potential threats and investigate suspicious activity to determine if it is a benign anomaly or a genuine security risk. This can strengthen your security posture by increasing the probability of securing reliable copies of protected data for swift recovery when needed. Together, they can minimize damage and help maintain your protected data's integrity, fortifying your defense against evolving cyber threats.

CHALLENGES WITH ANOMALY AND THREAT DETECTION AS AN EARLY WARNING

Relying on anomaly and threat detection in your data protection solution as an early warning system is challenging in today's threat landscape. Today 68% of attacks are achieved via exploiting users allowing attackers to login, mimicking a normal user (Verizon Business 2024[1]). Once attackers are in, they learn your environment moving laterally within as few as 62 minutes, setting up back doors and more compromised accounts (Crowdstrike 2024[2]). This is all done without tripping alarms. It is not until the attacker has done damage and is prepared to be found that they initiate the encryption attack.

The other prevalent attack method is the “smash and grab” approach. This is a rapid assault that overwhelms defenses before they can react. Even if the attack is noticed, its speed makes stopping it incredibly difficult.

In these types of scenarios, anomaly and threat detection in the data protection solution would likely not have detected the attack or would have detected it after the attack was issued. This is because most detection in data protection happens during or after the copy of protected data. Even if copies run every four hours, by the time the copy runs and is analyzed, the damage is done.

To enhance the success of preventing such attacks, organizations can also use a cyber deception system within the environment, such as Commvault Threatwise. With a cyber deception system, threats like ransomware and zero-day attacks can be identified in their earliest stages, even when they try to operate silently. This allows security teams to intervene before data encryption, exfiltration, or damage occurs, minimizing potential disruptions and data loss.

COMMVAULT SOLUTIONS

Commvault has the most comprehensive anomaly and threat detection in the data protection industry. Commvault will check for threats and anomalies on live systems prior to copy, during the copy, post-copy, and during recovery. These are the types of detection Commvault performs per product.

Commvault Data Protection

(All Commvault Data Protection features are enabled by default with new installations.)

Feature	Phase	Description
File activity anomaly detection	pre-copy/post-copy	Monitors for anomalies in file creation, modification, deletion, and renaming
Honeypot file	Live monitoring	Trap files are placed and monitored for access triggering the honeypot
File MIME type anomaly detection	during copy	Monitors for anomalies in file MIME type vs file extensions
Copy size anomaly detection	during copy	Monitors for anomalies in copy size growth or reduction by a larger than normal amount
File extension anomaly detection	during copy	Monitors for anomalies in file extensions increases or decreases
Data verification	post-copy	Internal processes to check the integrity of data backed up on storage

Cyber Deception and Threat Analysis

Feature	Phase	Description
Threatwise	live monitoring	A cyber detection system that sets canary entities to mimic actual production systems trapping malicious activity
Threat Scan	post-copy	Inspects and analyzes protected data copy content for malware threats using a built-in malware scanning engine

File Data Analysis

Feature	Phase	Description
Risk Analysis	post-copy	File system optimization and sensitive data discovery tools that scan data for sensitive information to determine where sensitive data sits or has been exposed to determine your risk

Threat Indicators

Feature	Phase	Description
Threat Indicator Dashboard	N/A	Framework that encompasses Commvault's anomaly and threat detection features and security ecosystem insights to provide proactive, reactive, and post-analysis reports

[1] Verizon Buisness, "2024 Data Breach Investigations Report", May 2024.

[2] CROWDSTRIKE, "CrowdStrike 2024 Global Threat Report", MAY 9, 2024.

To learn more, visit **commvault.com**