DATA SHEET

Identify malware and prevent reinfection with Commvault® Cloud Threat Scan

Enable swift and clean data recovery by analyzing backup data to find and quarantine encrypted or corrupted files and virtual machines

OVERVIEW

By leveraging Commvault Cloud Threat Scan, operations and security teams can take control and defend their backup data by proactively identifying malware threats to help avoid reinfection during recovery. Threat Scan analyzes backup data for encryption, corruption, and Cleanpoint™ identification, enabling users recover trusted versions of their data quickly.

CHALLENGE

With the ever-evolving cyber threat landscape, it is a daunting task for organizations to maintain a secure system. Every day, more than 287,000 new malicious programs (malware) and potentially unwanted applications (PUA) are being discovered1, making it challenging to protect against them all. As a result, many organizations fall victim to ransomware attacks and often don't have the tools to analyze file changes over time, preventing them from identifying reliable Cleanpoints and spot when encryption attempts happen and files become corrupted. Failure to detect infected files and quarantine them to prevent the spread can lead to large-scale ransomware attacks, causing damage to systems and reputation, longer recovery times, and possible risk of reinfection when you recover post-attack.

SOLUTION

Threat Scan helps recover your clean data as quickly as possible while minimizing rollback by identifying the last known good copies. Staging your recoveries with Threat Scan enables you to avoid potential reinfections by accidentally restoring malicious files. Threat Scan examines backup content files, backed up VMs, and network share filesystem backups for malware infections and ransomware encryption. With the built-in, signature-based scanning engine that is enhanced by AI techniques and customer-defined indicators of compromise (IOCs), Threat Scan enables accelerated detection, can kick-start responses, and quickly denotes what backup data has potentially become corrupted, encrypted, or heavily changed, giving IT an early warning when attacks occur.

24 hours Malware definitions are updated in the system daily

Zero Additional code or scripting is needed to run Threat Scan.

With Threat Scan, you can:

- Improve recovery initiative by reducing the guesswork required for finding and assembling good versions of data
- Recover infected files into an isolated environment for forensic analysis
- Reduce the risk of reinfection during restore operations
- Defend backup data by monitoring for threats, quarantining malware, and stop aging of backups
- Enable continuous business

1 AV-TEST Institute, May 2025: https://portal.av-atlas.org/malware

Every 24 hours Threat Scan updates its malware definitions

Zero additional code or scripting required to configure and run Threat Scan

SECURE BACKUPS

Threat Scan helps keep data backups pristine and can drive business continuity. By quickly identifying threats within backup content and consolidating security signals, Threat Scan allows operations teams to analyze backups for malware and spot which backup versions have been encrypted, corrupted, and significantly changed.

Benefits

- Reduce RTO
- Improve security posture
- Help ensure pristine backup copies
- Easily identify Cleanpoints and create an assemble for recovery across various points in time
- Enable business continuity

DEFEND AGAINST MALWARE

Operations teams can leverage a detailed visual dashboard to monitor detected threats, take corrective actions, and automate remediation. Once identified, teams can tag VMs, servers, and files with detected threats, cordon off malware with Smart Quarantine, and spot Cleanpoints at a glance.

Threat Scan alerts integrate with operations teams' SIEM and SOAR platforms to jump-start investigative actions by security teams.

RAPID RECOVERY

Threat Scan reduces RTO for files, objects, and VMs after a cyber incident by allowing operations teams to quickly recover the last known good copies, so users can prevent reinfections and recover cleanly to promote continuous business.

Feature	Compatibility
Identify changed files	• Protect and analyze anomalous backups and VMs • Helps operations team flag infected files and VMs so they recover only the last known good versions • Mitigate organizational risk with customer-defied IOCs to hunt for threats • Recover bad versions of files and VMs out-of-place for forensic operations
Smart Quarantine	• Automatically quarantine malware/infected files • Reduces the risk of reinfection during restore operations
Synthetic Recovery	• Identify and retrive the last known good version of data across backup sets for clean recovery initiatives to minimize data rollback • Simplify recovery at scale by restoring a set of Cleanpoints for files and objects automatically assembled across multiple VMs and points in time

ENABLE CONTINUOUS BUSINESS

Threat Scan is easy to deploy, use, and consume, so operations can rapidly identify and respond to security events. Providing comprehensive visibility into latent and silent data threats, Threat Scan improves security posture and protects backup data for rapid recovery.

1 Identify and Investigate Anomalies

Security and IT Operations engineers can monitor security events and take action against anomalies that indicate a cyber incident or malware infection within your data estate. When evidence indicates a compromised asset via an anomalous data change, teams can leverage Threat Scan to automate mitigations and perform an in-line forensic investigation of the backup data to help validate the backup content is not infected.

2 Recover the Last Known Good Version of Data

Security and IT Operations engineers must recover good backup data versions as quickly as possible during a security event. Typically, they must guess which data is not infected, often leading to longer recovery times. Threat Scan automates Cleanpoint identification and allows the teams to orchestrate investigations of backup content for data encryption and corruption with AI-driven engines, so they can quickly locate good and safe versions of your files, thus eliminating guesswork and reducing the overall recovery time initiatives.

Eliminate Guesswork

Reduce RTO

Automate Responses

3 Stage for Forensic Investigations

Security and IT Operations engineers should recover infected versions of backup content into an isolated environment so they can investigate the files and perform root cause analysis. With Threat Scan, engineers can perform thorough investigations and point-in-time recoveries in an isolated environment while limiting risks of human error.

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