

Identify malware and prevent reinfection with Commvault Threat Scan

Enable swift and trusted data recovery by analyzing backup data to find encrypted and corrupted files

OVERVIEW

By leveraging Commvault Threat Scan, Operations 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 to find encrypted or corrupted files, ensuring users recover trusted versions of their data quickly.

CHALLENGE

Today, Security Operations and IT Operations teams lack insight into malware and ransomware attacks at the early stages of data backup. Teams often lack tools to analyze file changes over time and thus fail to see when encryption efforts fail and files become corrupted. Failure to identify infected files and prevent their dissemination grants bad actors even more access to, and time in, your environments. This encourages more pervasive ransomware attacks, which inflict greater damage to your systems and reputation. This also results in longer recovery times due to larger volumes of affected data sets and difficulty in determining which files are safe to recover.

SOLUTION

Commvault Threat Scan helps ensure that you can securely recover your data as quickly as possible by identifying the last known clean copies and help avoid any potential reinfection by accidentally restoring malicious files. Threat Scan examines backup content files and network share filesystem backups for malware infection using a built-in, signature-based scanning engine. Threat scan quickly denotes what backup data has 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 Commvault Threat Scan, you can:

- Improve recovery initiative by reducing the guesswork required for finding 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 threats



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 to keep data backups pristine and help ensure business continuity. By quickly identifying threats within backup content, Threat Scan allows operation teams to analyze backups for malware and de-note which files have been encrypted, corrupted, and significantly changed.

Benefits

- Reduce RTO
- Increase security posture
- Help ensure pristine backup copies
- Enable business continuity

DEFEND AGAINST MALWARE

Operations teams can leverage a detailed visual dashboard to monitor detected threats and take corrective actions. Once identified, teams can tag servers with detected threats, cordon off malware with Smart Quarantine, and mark suspicious files as infected.

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 after an attack by allowing Operations teams to quickly recover the last known good and safe versions of files, preventing reinfections and promoting business continuity.

Feature	Integration	Capabilities and Benefits
Identify changed files	✓ Commvault Platform	<ul style="list-style-type: none">• Protect and analyze anomalous backups• Help ensure operations teams can flag infected files so they recover only the last known good versions• Improve recovery initiatives by reducing guesswork needed to find good and usable recovery data• Recover bad versions of files out-of-place for forensic operations
Smart Quarantine	✓ Commvault Platform	<ul style="list-style-type: none">• Automatically quarantine malware/infected files• Reduces the risk of reinfection during restore operations

ENABLE BUSINESS CONTINUITY

Natively integrated with the Commvault platform, Threat Scan is easy to deploy, use, and consume, help ensure operations teams can rapidly identify and respond to security events. Providing comprehensive visibility into latent and silent data threats, Threat Scan improves security posture and protects pristine backup data for rapid recovery.

1 Analyze 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 investigate the backup data to help ensure 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 allows them to orchestrate investigations of backup content for data encryption and corruption, 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



Automatically
Quarantine

3 Recover 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.

To learn more, visit commvault.com >