Clumio S3 Malware Scan

Malware-Aware Recovery for Amazon S3 Backups

As ransomware and malware incidents increase, organizations are placing greater scrutiny on what data gets restored after an attack – not just what gets backed up. Clumio S3 Malware Scan is an optional security capability integrated into Clumio SecureVault for Amazon S3, designed to help detect malware signatures in backup data and block infected objects from being restored into production environments.

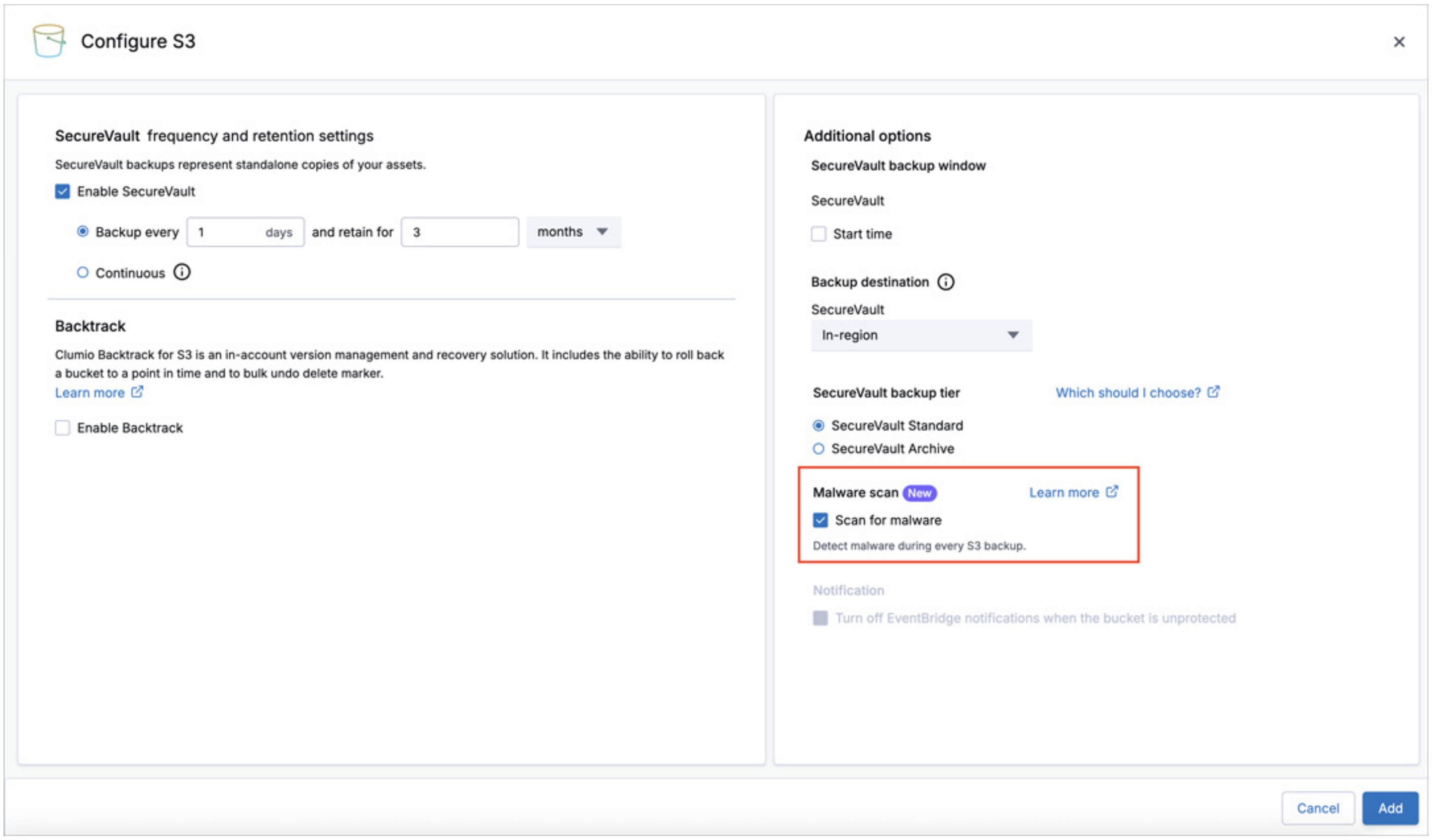
This capability focuses on safe recovery, helping organizations avoid reintroducing malicious content during restore operations.

CLUMIO S3 MALWARE SCAN

- Helps block malware-infected objects from restore workflows, reducing the risk of reinfection after an incident
- Complements immutable, air-gapped backups by adding object-level malware awareness during recovery
- Uses metadata-based scanning to avoid additional data reads or performance impact during backup operations

HOW CLUMIO S3 MALWARE SCAN WORKS

- In-line Backup Scan runs during normal backup operations and scans object metadata as data is ingested
- Continuous Scan periodically rescans the SecureVault to help detect newly published malware signatures
- Hash-based signature matching (MD5)
- When malware is detected, affected objects are automatically blocked from restore operations



Configure S3

SecureVault frequency and retention settings

SecureVault backups represent standalone copies of your assets.

☑ Enable SecureVault

● Backup every 1 days and retain for 3 months

○ Continuous

Backtrack

Clumio Backtrack for S3 is an in-account version management and recovery solution. It includes the ability to roll back a bucket to a point in time and to bulk undo delete marker.

Learn more

□ Enable Backtrack

Additional options

SecureVault backup window

SecureVault

□ Start time

Backup destination

SecureVault

In-region

SecureVault backup tier — Which should I choose?

● SecureVault Standard

○ SecureVault Archive

Malware scan New — Learn more

☑ Scan for malware

Detect malware during every S3 backup.

Notification

□ Turn off EventBridge notifications when the bucket is unprotected

Users can enable malware scanning when configuring S3 backups. Scan results are available as downloadable reports per backup, with consolidated reporting across all backups via the UI and API. Alerts are generated when malware signatures are detected.

SCOPE AND RESPONSIBILITY BOUNDARY

- Scanning applies to objects 4 MB or smaller
- Compressed data is not decompressed or reprocessed
- Designed for detection during recovery, not endpoint or source malware prevention

LEARN MORE

Technical documentation is available at:

https://documentation.commvault.com/clumio/release_notes_for_clumio.html#s3-malware-scan-public-ea

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