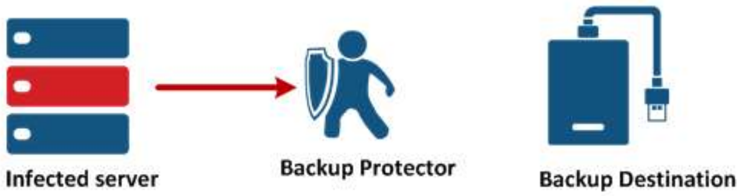
CryptoSafeGuard Product Overview

The advent of ransomware has exposed computer systems to a new threat and expanded the role of backup software. This is because a system recovery is usually the only safe solution to a ransomware infection, so it's critical that your backups are ready for this new role. BackupAssist has always had a robust and reliable recovery solution because we match flexible image backups with our custom recovery environment. CryptoSafeGuard now steps in to protect your backups so you can perform a data recovery if your business is hit with a ransomware infection.

The CryptoSafeGuard Protector

CryptoSafeGuard's Protector prevents unauthorized processes from accessing, editing, deleting and adding data to your backups. This layer of protection is switched on when the backup job first runs, to keep the backups safe.



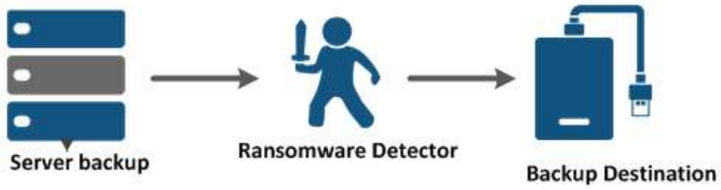
The Protector will not put any noticeable overhead on BackupAssist or your system because it runs at the driver level, a low-level interface between your system and backups. This means the CryptoSafeGuard Protector supports backups on destinations that could be reached by ransomware, including NAS and iSCSI.

The CryptoSafeGuard Protector only works on the machine that BackupAssist is installed on, so if a user connects the backup media to another machine, the backups on that media will not be protected.

When BackupAssist is uninstalled, CryptoSafeGuard is removed and the Protector can no longer protect the data in your backups. However, if you delete or disable the backup job, the Protector will continue to run and provide ransomware protection.

The CryptoSafeGuard Detector

CryptoSafeGuard's Detector runs when a backup jobs starts and scans the data to be backed up. The first time the job runs, all of the selected data is scanned. After that, only data that has changed will be scanned.



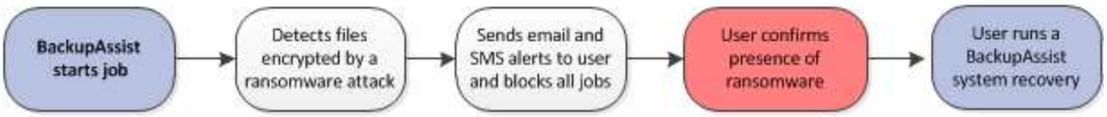
The Detector's scan applies different rules to look for indicators of known ransomware families. It also uses detection strategies that ensure the scan is looking for both known signatures and new variants.

CryptoSafeGuard will be updated with new rules as new families of ransomware are discovered, and the scanning process will evolve to stay ahead of the threats posed by ransomware.

By applying multiple checks to the same data, CryptoSafeGuard reduces the incidence of false positive detections, minimising the need for file reviews and whitelisting by the user. If the user does need to whitelist data, they can include folders and file extensions to make this process easier to administer.

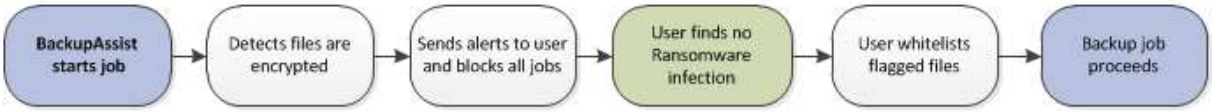
The infection detection process

This diagram shows how CryptoSafeGuard's Detector responds to a ransomware infections and how BackupAssist can play a part in the resolution by recovering the infected data. The key is the protection of the backups that are needed to perform a recovery, and that all jobs are blocked from infection when any job detects one.


BackupAssist starts job
Detects files encrypted by a ransomware attack
Sends email and SMS alerts to user and blocks all jobs
User confirms presence of ransomware
User runs a BackupAssist system recovery

The whitelisting process

This diagram shows how CryptoSafeGuard's Detector steps in after a system has been compromised to make sure the infection does not spread to your backups. The final recovery step demonstrates the importance of having a protected 'clean' backup, which are key to recovering from the damage caused by a ransomware attack.


BackupAssist starts job
Detects files are encrypted
Sends alerts to user and blocks all jobs
User finds no Ransomware infection
User whitelists flagged files
Backup job proceeds

The CryptoSafeGuard Detector performs a **hierarchical threat scan** when a backup job starts to make sure that the data being backed up is clean. It uses simple criteria to initially flag a file as suspicious, and then applies increasingly complex sensors and analysis to confirm a possible threat. This results in faster and less intrusive ransomware scans while reducing incidences of false positive detection.

How to get CryptoSafeGuard

CryptoSafeGuard is available for BackupAssist 10.1 (or newer) users with valid BackupCare.

BackupCare is an annual subscription that provides access to all BackupAssist updates and new BackupAssist versions, as well a CryptoSafeGuard.