BackupAssists' CryptoSafeGuard

CryptoSafeGuard is a BackupAssist tool that protects backups from ransomware attack and prevents ransomware-encrypted files from being backed up. CryptoSafeGuard is available for BackupAssist 10.1 (or newer) users with valid BackupCare.

What is ransomware?

Ransomware is malware that encrypts files and demands payment to provide the decryption key so you can access those files again. Some ransomware can spread across connected machines and some can disable your system completely, so infected machines will often need to be recovered from a backup. It is therefore important that your backups are not infected, which is why CryptoSafeGuard is such an invaluable feature.

What does CryptoSafeGuard do?

To protect your systems against ransomware attacks, it's critical that you have reliable backups so you can restore data or recover your entire system to ensure business continuity. However, when ransomware attacks your systems, it can also infect your backups, leaving them unusable. CryptoSafeGuard protects your backups from ransomware using two important features: the CryptoSafeGuard Detector and the CryptoSafeGuard Shield.

CryptoSafeGuard Detector - prevents infected files from being backed up

When a backup job starts, BackupAssist scans the data being backed up. If there is any sign of a possible ransomware infection, all backup jobs will be blocked from running, and email and SMS alerts will be sent if configured. If your job backs up Hyper-V guests, the CryptoSafeGuard Detector will also scan the contents of those Hyper-V guests in one pass.

This scan errs on the side of caution so it may flag files as possibly infected when they are not infected. If this happens, you will be able to whitelist these files so that BackupAssist knows they are safe, and will not flag them again.

Note: CryptoSafeGuard detects signs of a ransomware infection. It does not protect the actual system from ransomware or remove ransomware.

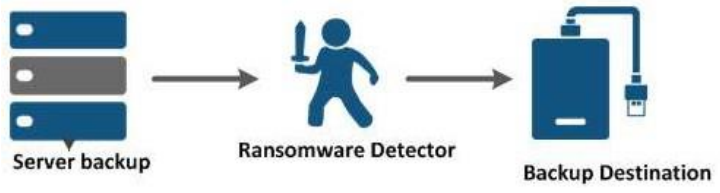
CryptoSafeGuard Shield - protects your existing backups from ransomware

CryptoSafeGuard Shield prevents unauthorized processes from creating, deleting or updating data in your backups. This feature runs automatically in the background when CryptoSafeGuard is enabled.

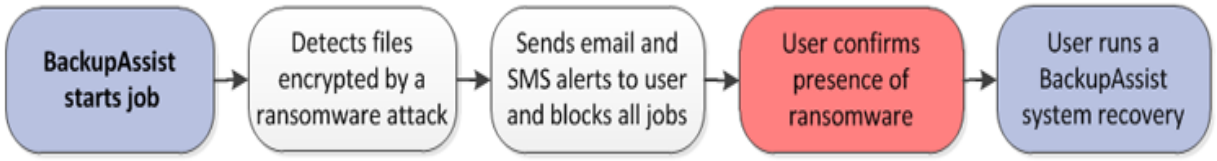
Note: CryptoSafeGuard Shield will prevent you from manually deleting backups. If you need to manually delete backups, disable CryptoSafeGuard, make the deletion, and then re-enable CryptoSafeGuard again.

The 'Detector'

CryptoSafeGuard executes a detection scan before running each backup, using a combination of complementary scan algorithms and signature-based checks to detect infection.



It scans the system, and the specific backup job's selections, using a hierarchical approach so that the slower in-depth checks only happen on the smallest number of files possible.



If an infection is detected, **immediate action** is taken:

1. Sets BackupAssist UI status to "blocked"
2. Stops the backup, sends usual backup error notifications (if configured)
3. Sends SMS notification if configured - recommended!
4. Stops further backups from running

The 'Protector'

When a backup is executed, CryptoSafeGuard initiates write locking on each specific backup job's backup location (path).

The CryptoSafeGuard protector prevents unauthorized processes on the BackupAssist machine from writing to the backup.

It does not prevent other machines from writing to the backup - CryptoSafeGuard is not a replacement for good security practices.

The protection means that only BackupAssist processes can create, modify, or delete files at the backup location.

Please Note:

CryptoSafeGuard is NOT a replacement for your traditional antivirus and/or anti-malware applications - it's to be treated as an extra layer of protection.

Anti-virus and anti-malware	BackupAssist + CryptoSafeGuard
Focused on detecting viruses and threats, and cleaning up infections.	Focused on providing and protecting a time machine to go back in time and restore data before the infection.
Like a bouncer at a nightclub - trying to stop threats from getting in, and cleaning up (evicting) any threats that managed to sneak in.	Protection against damage caused by threats that have managed to infiltrate and circumvent the perimeter security. **"Undo" the damage caused.**
PERIMETER SECURITY	**INSURANCE POLICY IN A SECURE VAULT**