FACTSHEET

CryptoSafeGuard

THE RIGHT BACKUP ™
BackupAssist

Your backups are your last line of defense. But they're useless if corrupted or infected by ransomware.

WHAT'S IN IT FOR YOU ?

- Prevent ransomware from encrypting your backups
- Prevent corrupted files getting into your backups
- Immediate notification alerts for anomaly detection
- Exceptional protection, free with BackupCare

HOW IT WORKS ?

Under the Hood — CryptoSafeGuard uses a two-pronged approach to mitigate the destructive effects of ransomware and protect your backups.

Defense #1

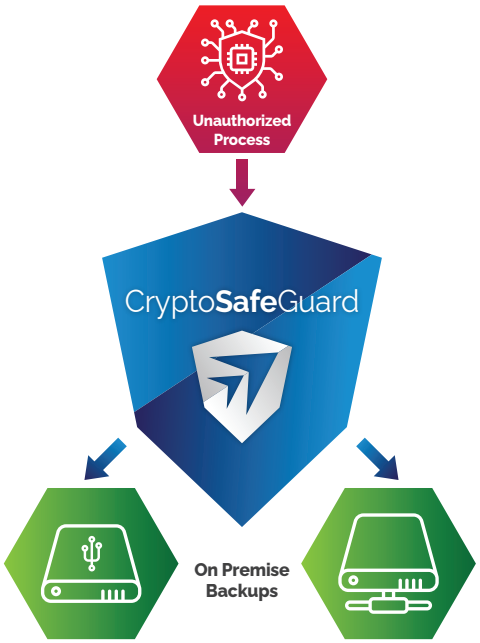
The Shield

The CryptoSafeGuard Shield actively monitors the I/O to your backup files and blocks unauthorized operations.

- Blocks unauthorized processes from accessing a USB or Network connected backup.
- Shields against crypto-infection of on-premise backups.
- Active 24/7.

The Shield protects backup files where ordinary user-based access controls fail. Conventional user-based access controls (such as those offered by NTFS, or NAS that integrate with Active Directory) fail because they restrict access based on the user. Ransomware can bypass these controls as it can run as a regular user or a privileged user.

The Shield restricts based on process, which is a more effective method to preserve the integrity of your backups.



Defense #2

Detect – Preserve – Alert

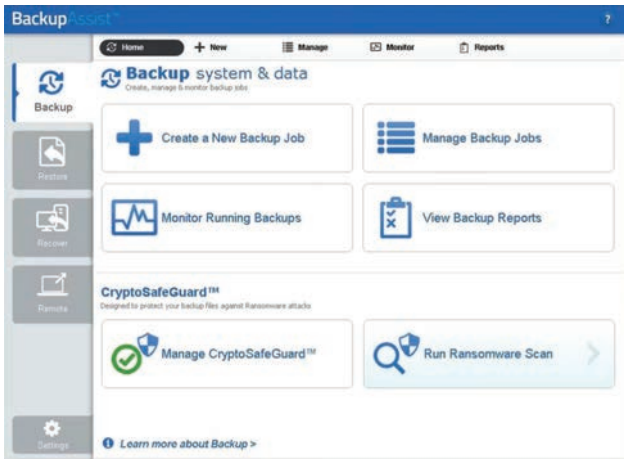
When suspicious activity is detected, CryptoSafeGuard springs into action, preserving the last known-good backup, and sending an SMS alert to the registered administrator.

Finally, system administrators can regain control in the event of a ransomware outbreak.

BackupAssist starts a backup → Detects files encrypted by ransomware attack → Preserves last known good backup → Alerts via email and SMS → Recover from last clean backup

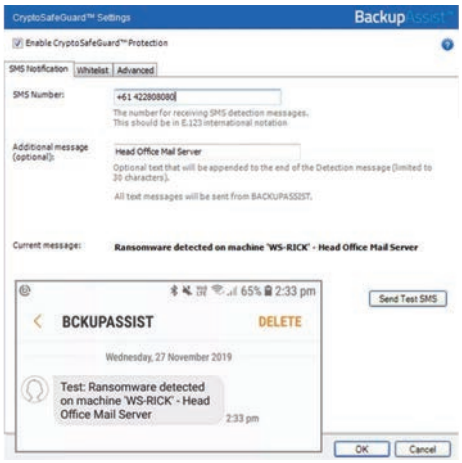
HOW IT WORKS ?

What you see — Using CryptoSafeGuard is a piece of cake



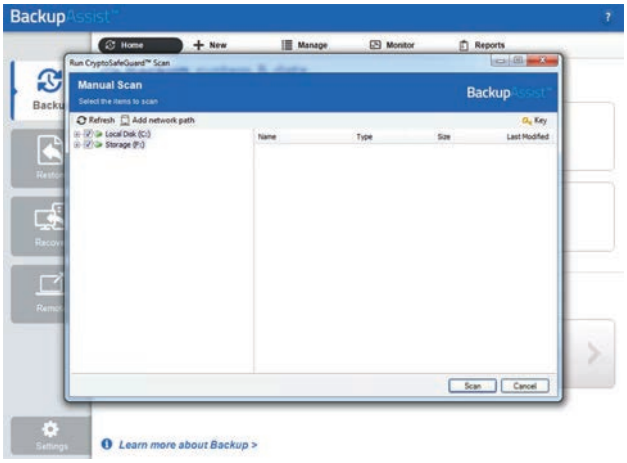
1. Manage your ransomware protection

CryptoSafeGuard is fully integrated into BackupAssist with alert management and notification features.



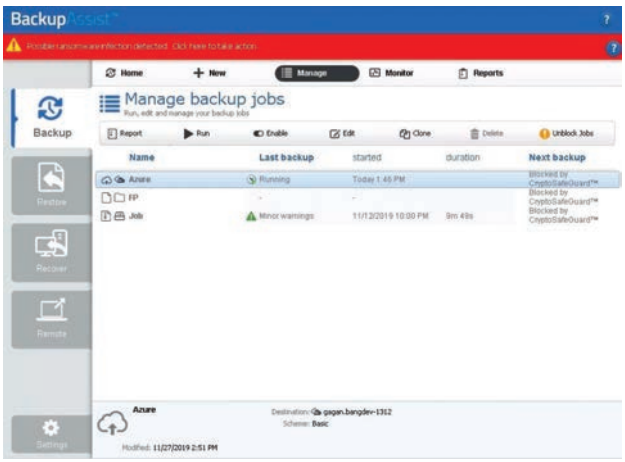
2. Configure SMS alerts

CryptoSafeGuard alerts can be sent to your phone as soon as a possible infection is detected.



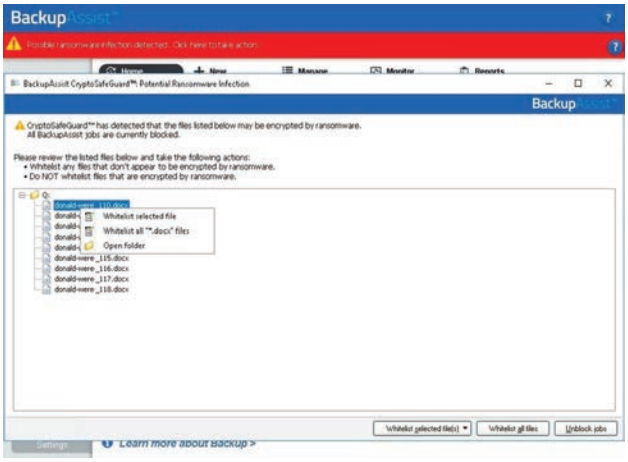
3. Run a manual scan

Running a manual scan checks for any possible false-positive detections so they can be whitelisted before a new job runs.



4. Be protected if infection strikes

If CryptoSafeGuard detects any signs of ransomware, it will display a warning banner and all backup jobs will be blocked from running.



5. Whitelist safe files

If a ransomware scan detects files that are not ransomware, you can whitelist them so they do not trigger further alerts.

INDEPENDENT SECURITY ANALYSIS

MRG Effitas

"BackupAssist's CryptoSafeGuard Detector and Shield had a 100% success rate against every ransomware strain we tested it against, including highly destructive strains of Locky, CryptoLocker, and TeslaCrypt. In every case, CryptoSafeGuard successfully identified the ransomware infection and ensured no backups were overwritten with encrypted files."

FREQUENTLY ASKED QUESTIONS

Q1. Tell me more about the problem you're solving.

Unfortunately, ransomware can infect and corrupt your backups. There are two essential problems:

1. The entire backup can be corrupted by ransomware, which tries to delete or encrypt your backup.
2. If you suffer an infection, encrypted files can sneak into your backup, if left unchecked.

A full description of the problem is provided in our blog post: **Can ransomware infect your backups? That's like a leaking life raft!** Therefore it is important to protect your backups from ransomware. You can do that easily in the BackupAssist solution in two ways:

1. Take your backup offline. For example, if you back up to rotating hard drives, the hard drives that you disconnect from the server cannot be corrupted because they are not physically connected to the machine.
2. For all online backups, CryptoSafeGuard will protect them from ransomware as we explain above.

Q2. Does the CryptoSafeGuard Shield protect against other forms of sabotage?

Yes, it blocks unauthorized forms of access, such as a malicious user deleting or otherwise attempting to overwrite or alter the backup files.

Q3. Does CryptoSafeGuard work with other backup software?

No. CryptoSafeGuard is exclusive to BackupAssist products.

Q4. If I airgap my backups, do I still need CryptoSafeGuard?

Even if you air gap your backups, we still recommend running CryptoSafeGuard. A normal hard drive rotation scheme will still expose a backup to possible ransomware corruption when it is connected to the computer. Therefore, CryptoSafeGuard will reduce your potential data loss from the time of your 2nd last backup to your last backup.

The second benefit of CryptoSafeGuard is the Detector. This will prevent encrypted files from sneaking into your backup, while also giving control back to the administrator by alerting about the suspicious activity.

Q5. Does CryptoSafeGuard guarantee that my backups will never be corrupted by ransomware?

The goal of CryptoSafeGuard is to provide the best security possible within the context of an SME backup solution. It does a remarkable job at shielding backups from ransomware, and has been independently verified by a leading security testing firm.

That being said, the general consensus among security experts is that any attacker, sufficiently well funded and motivated, is exceptionally difficult to defend against. By way of example, nation state hacking is a problem that is almost impossible to address. CryptoSafeGuard is designed to protect against ransomware, not necessarily teams of sophisticated hackers. However, these should not be the concerns of the average SME!

As mentioned previously, taking the backup offline (completely disconnected from a running machine) or writing it to write-once media are the only 100% sure ways of ensuring that the backup will not be destroyed via electronic sabotage.

Realistically, no security vendor – including anti-virus and anti-malware vendors – can guarantee 100% security, 100% of the time. Security is an ongoing pursuit as what is considered safe today may not be considered safe tomorrow.

Q6. How exactly does your Detector work?

Just as a hurricane leaves identifiable signs of destruction, so too does ransomware.

The role of CryptoSafeGuard is to protect against the threat in the most generic way possible.

CryptoSafeGuard's detector looks at patterns of behaviour. We have multiple techniques for detecting suspicious behaviour, and if anomalies are found, the detector will progressively scan further to more accurately assess and diagnose the issue. While we do not publish our exact methods, at a broad level, things that our detector looks for include:

- Changes to the file and directory structure
- Deep content inspection
- Ransom messages

Q7. How do I get CryptoSafeGuard?

The only way to get CryptoSafeGuard is to have a valid subscription to BackupCare, our assurance program for BackupAssist.

For more information, visit www.backupassist.com

CLIENT SUCCESS

+1-855-314-1458
sales@backupassist.com

TECHNICAL SUPPORT

+1-812-206-4265
support@backupassist.com

PARTNER SERVICES

+1-855-314-1458
resellersupport@backupassist.com