CryptoSafeGuard User Guide: Beta

BackupAssist 10.1.0 will introduce CryptoSafeGuard, a new tool that protects your backups from ransomware attack and prevents ransomware-encrypted files from being backed up.

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 by performing two important functions:

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.

CryptoSafeGuard Protector - protects your existing backups from ransomware.

CryptoSafeGuard protects your backups from ransomware by allowing only BackupAssist to move or update data in your backups. This feature runs automatically in the background when CryptoSafeGuard is enabled.

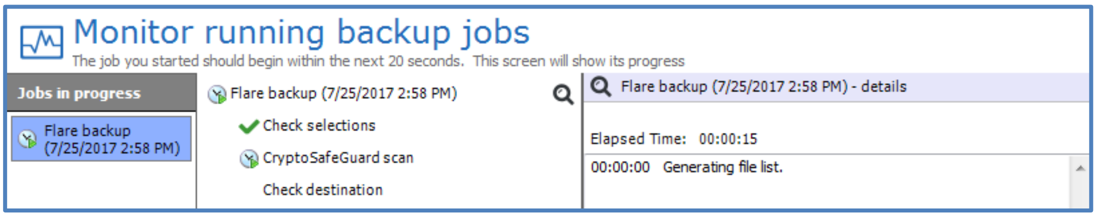
Important: CryptoSafeGuard detects signs of a ransomware infection. It does not protect the actual system from ransomware, or remove ransomware.

Running CryptoSafeGuard

CryptoSafeGuard is available for BackupAssist 10.1 (or newer) users with valid BackupCare. It is permanently enabled in the beta and will run by default with each backup job.

Each job's first CryptoSafeGuard scan may take some time depending on the amount of data being backed up. Subsequent CryptoSafeGuard scans will be a lot faster and have minimal impact on the backup jobs' run times. The first scan may also detect a number of files for review, and whitelisting.

CryptoSafeGuard will appear in the backup monitor screen and show its progress in the right pane.



Monitor running backup jobs

The job you started should begin within the next 20 seconds. This screen will show its progress

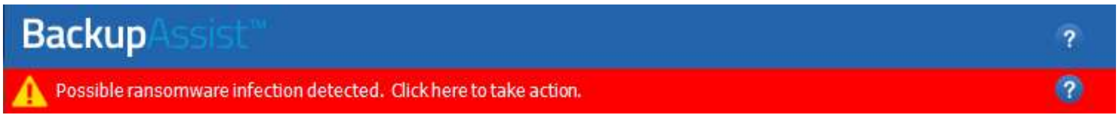
Jobs in progress
Flare backup (7/25/2017 2:58 PM)
Flare backup (7/25/2017 2:58 PM)
Check selections
CryptoSafeGuard scan
Check destination
Flare backup (7/25/2017 2:58 PM) - details

Elapsed Time: 00:00:15

00:00:00 Generating file list.

CryptoSafeGuard alerts

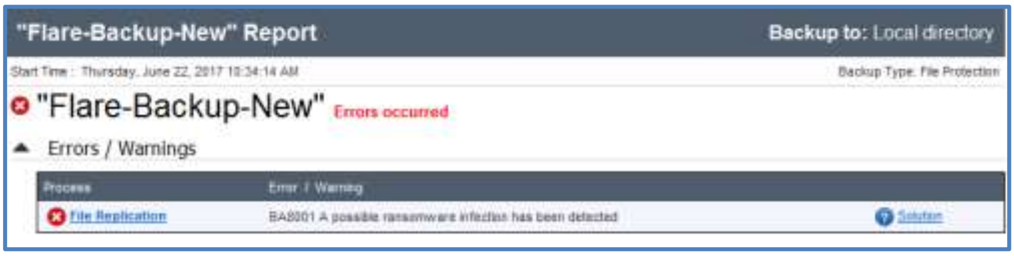
When a backup job's CryptoSafeGuard scan believes there may be ransomware, an alert will show next to the job in the Monitor UI and a red banner will appear at the top of BackupAssist's UI. If you have configured email and SMS notifications, an email and SMS alert will also be sent. BackupAssist's alert banner is clickable and has a help link to the CryptoSafeGuard documentation. You must click the banner and follow the dialogs to respond to a possible ransomware infection.



Possible ransomware infection detected. Click here to take action.

Email notifications

If you have set up the Email server settings and Email address list, and enabled Notifications in the backup job, a backup report will be sent with a BA8000, BA8001 or BA8002 error message to inform you of the detection.



"Flare-Backup-New" Report

Backup to: Local directory

Start Time : Thursday, June 22, 2017 10:34:14 AM

Backup Type: File Protection

"Flare-Backup-New" Errors occurred

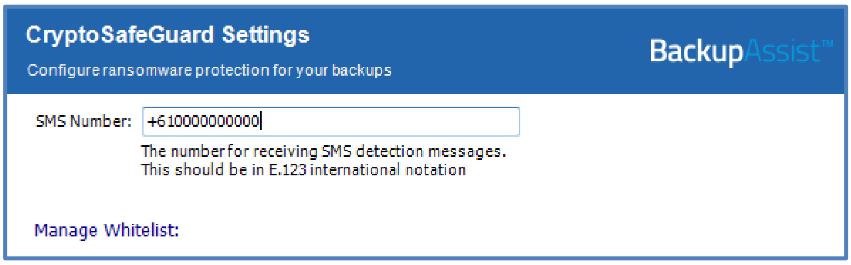
Errors / Warnings

Process	Error / Warning	
File Replication	BA8001 A possible ransomware infection has been detected	Solution

SMS notifications

If you set up SMS notifications, SMS alerts will be sent when CryptoSafeGuard detects a possible ransomware infection. To enable SMS notifications:

- Select BackupAssist's **Settings** tab.
- Select **CryptoSafeGuard**.
- Enter the phone number in the **SMS Number** field using the standard international phone number format "+<country code><mobile phone number>".



CryptoSafeGuard Settings

Configure ransomware protection for your backups

SMS Number: +610000000000

The number for receiving SMS detection messages.
This should be in E.123 international notation

Manage Whitelist:

Figure 1: CryptoSafeGuard SMS setup

Responding to a CryptoSafeGuard alert

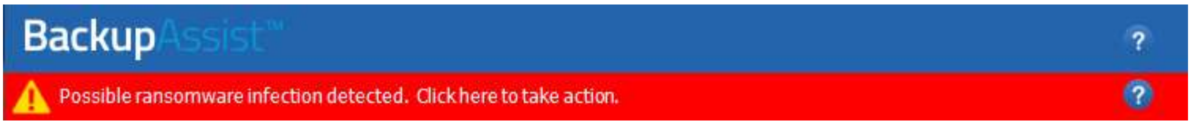
When a possible ransomware infection is detected, all backup jobs will be blocked from running until the CryptoSafeGuard alert has been resolved.

If your IT systems administrator determines that your system has a genuine ransomware infection, you may need to perform a bare-metal recovery from your last successful backup.

If you are not aware of a ransomware infection, BackupAssist will allow your IT systems administrator to review the suspected files. This review should include trying to open the listed files in their relevant applications to see if they still work. Safe files can be whitelisted.

To respond to the alert:

1. Click on the CryptoSafeGuard banner.



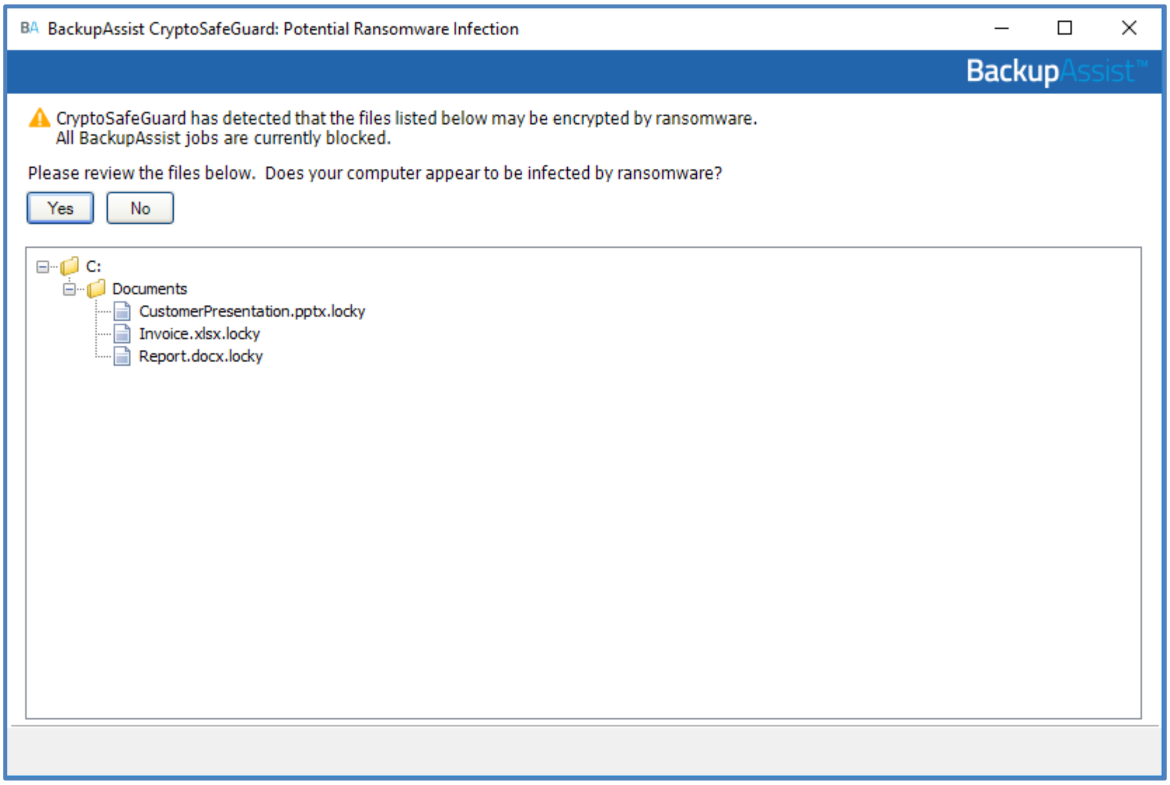
Possible ransomware infection detected. Click here to take action.

This will open the **CryptoSafeGuard** user interface (UI).

2. Decide if there is a ransomware infection.

To help determine if there is an infection, the UI shows all the files that CryptoSafeGuard detected as potentially infected, so they can be reviewed.

Right clicking a folder will allow you to open that folder in Windows. Right clicking a file allows you to open the folder that that file is in.



BackupAssist CryptoSafeGuard: Potential Ransomware Infection

CryptoSafeGuard has detected that the files listed below may be encrypted by ransomware.
All BackupAssist jobs are currently blocked.

Please review the files below. Does your computer appear to be infected by ransomware?

Figure 2: CryptoSafeGuard file review screen

3. Select **Yes** or **No**.

   Your IT systems administrator will determine if you have a ransomware infection or not, and respond accordingly by selecting the **Yes** (have an infection) or **No** (no infection) button.

Determining if there is an infection

Deciding if your system is infected by ransomware will involve checks outside the scope of BackupAssist and involve using anti-malware software and attempting to open important documents and images. A ransomware infection will often display a message on screen.

It is worth noting that the first time you run CryptoSafeGuard, it is possible that safe files will be flagged and need to be whitelisted. Also, in most cases, the first indication of a ransomware infection is a persistent ransomware message on your screen.

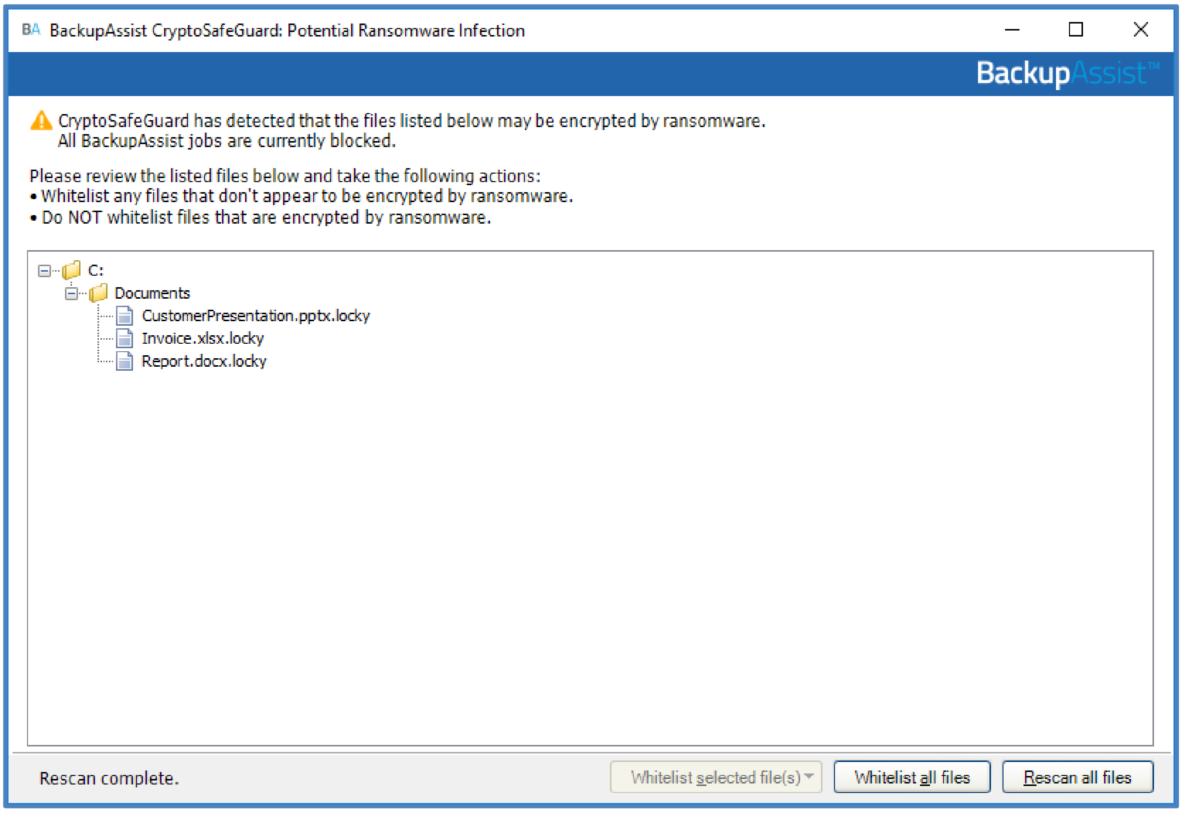
Selecting Yes

If you select **Yes**, a dialog will open and advise you to that all backup jobs have been blocked and will not run until the infection has been resolved. This resolution may involve performing a full system recovery using RecoverAssist. In this case, BackupAssist will be recovered with your system to an earlier functioning state.

If you resolve the ransomware infection without a recovery, the alert banner will still appear in BackupAssist. Clicking the banner again will re-scan all of the previously listed files. If the rescan detects that all the files have been cleaned up, all backup jobs will be automatically unblocked.

Selecting No.

If there is no infection, select **No**. A dialog will advise that you need to remove or whitelist the detected files. To help you do this, new buttons will appear in the CryptoSafeGuard UI.


BackupAssist CryptoSafeGuard: Potential Ransomware Infection
BackupAssist™

CryptoSafeGuard has detected that the files listed below may be encrypted by ransomware.
All BackupAssist jobs are currently blocked.

Please review the listed files below and take the following actions:
- Whitelist any files that don't appear to be encrypted by ransomware.
- Do NOT whitelist files that are encrypted by ransomware.

```
C:
  Documents
    CustomerPresentation.pptx.locky
    Invoice.xlsx.locky
    Report.docx.locky
```

Rescan complete.

Figure 3: CryptoSafeGuard whitelisting

Removing files

You cannot delete files using the CryptoSafeGuard UI, but you can access the files by right clicking their folder and selecting open folder. This will open the folder in Windows explorer. If you delete any files, use the **Rescan all files** button to update the list of files shown.

The list of suspicious files will include:

- Potentially encrypted user files (If safe, they should be whitelisted)
- Ransom notes created by ransomware itself (If present, they should be deleted, not whitelisted)

> Note: You should not delete files just because they are in this list as they may be files you need to run your system or applications.

Whitelisting all files

You can select *Whitelist all files* to whitelist and clear all of the files shown. You should not do this unless you have reviewed the files and know they are safe. A confirmation dialog will appear, then another to advise that the backup jobs will be unblocked.

Whitelisting some files

You can work through the flagged files whitelisting as you go, as follows:

a. Right-click the file and select that file or all files of that type.

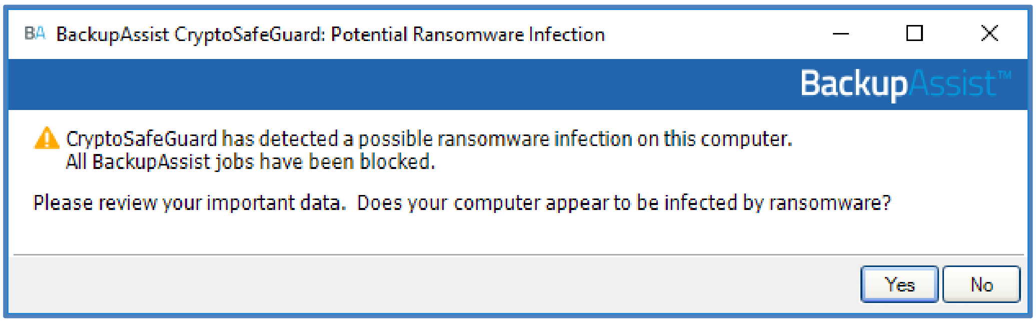
b. Select the **Whitelist selected files** button.

When all files have been cleared from the CryptoSafeGuard UI, a dialog will confirm that your backup jobs will be unblocked.

The backup job that was stopped by CryptoSafeGuard will not automatically rerun. You can manually run the job or allow it to run at its next scheduled run-time.

Infection detection

CryptoSafeGuard may generate a possible ransomware alert and display the banner without detecting an infection in the files you are backing up. This could happen if CryptoSafeGuard detects certain patterns of behavior consistent with a ransomware infection. If this happens, clicking the alert banner will open the following dialog.



BackupAssist CryptoSafeGuard: Potential Ransomware Infection

CryptoSafeGuard has detected a possible ransomware infection on this computer.
All BackupAssist jobs have been blocked.

Please review your important data. Does your computer appear to be infected by ransomware?

There are no files to whitelist or delete. You must check your system for signs of an infection, and then select **Yes** or **No**. The workflow is similar to the process above, but selecting **No** will proceed to unblock your jobs without the need to remove or whitelist files.

Managing the whitelist

If you respond to a CryptoSafeGuard alert by whitelisting files, you can review and change your whitelist using the **Manage Whitelist** section of the **CryptoSafeGuard Settings** dialog. You can also use this dialog to add to your whitelist without an alert, but it is recommended that you use the alert list to inform your whitelisting decisions.

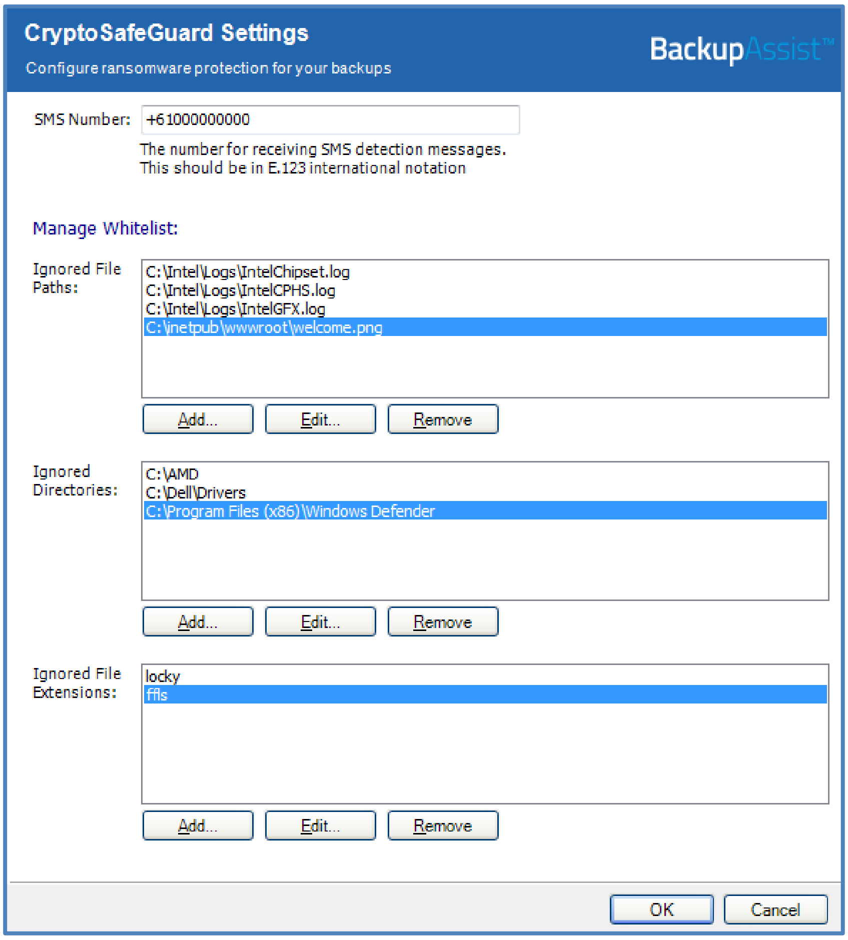
How to access the Manage Whitelist fields

Follow these steps:

- Select BackupAssist's **Settings** tab
- Select **CryptoSafeGuard**
- A dialog will open with **Manage Whitelist** and the three sections.

How to modify the whitelist sections

The Manage Whitelist sections allow you to add, modify and delete whitelisted files, directories, and file extensions. Any files whitelisted in the CryptoSafeGuard alert dialog will automatically appear here.



CryptoSafeGuard Settings

Configure ransomware protection for your backups

SMS Number: +61000000000

The number for receiving SMS detection messages.
This should be in E.123 international notation

Manage Whitelist:

Ignored File Paths:
C:\Intel\Logs\IntelChipset.log
C:\Intel\Logs\IntelCPHS.log
C:\Intel\Logs\IntelGFX.log
C:\inetpub\wwwroot\welcome.png

Ignored Directories:
C:\AMD
C:\Dell\Drivers
C:\Program Files (x86)\Windows Defender

Ignored File Extensions:
locky
ffls

Figure 4: CryptoSafeGuard Settings dialog

Ignored File Paths

This field is used to manage whitelisted files. Use the **Add** button to browse to the file and add it, and the **Remove** button to remove the selected file from the list. Selecting **Edit** will allow you to manually edit the entry, or browse from the entries location. Select **Save** after making manual changes.

Ignored Directories

This field is used to manage whitelisted directories, which excludes all files inside the directory from the CryptoSafeGuard scan. Use the **Add** button to browse to the directory and add it, and the **Remove** button to remove the selected directory from the list. Selecting **Edit** will allow you to manually edit the entry, or browse from the entries location. Select **Save** after making manual changes.

Ignored File Extensions

This field is used to manage whitelisted file extensions, which excludes all files with that extension from the CryptoSafeGuard scan.

To add a file extension:

1. Select **Add**
2. Enter the file extension. Do NOT include periods or wildcard symbols. E.g. enter txt. Not .txt or *.txt.
3. Select **Add**.
4. Repeat this process for each file extension. Do not enter multiple extensions as a single entry.

Use the **Remove** button to remove the selected file extension from the list and the **Edit** option to edit an existing entry. Select **Save** after making manual changes.

Note: Adding files and folders to the whitelist means they are excluded from CryptoSafeGuard's scan when a backup job starts. It is important to only whitelist files that create, or are expected to create, false positive responses when the scan runs.

CryptoSafeGuard's current limitations

Hyper-V Server

When BackupAssist is installed on a Hyper-V host to back up the guests (VMs), CryptoSafeGuard will scan the guests' contents before backing them up. However, only basic partitioned volumes are scanned. Dynamic partitioned volumes (e.g. striping, spanning) are not scanned.

Only locally supported file systems are supported when scanning guests. This means that Linux file systems like ext3 are not scanned inside guests unless there is a driver supporting that file system on the host.

SQL Server

SQL Protection jobs do not currently run with CryptoSafeGuard detection.