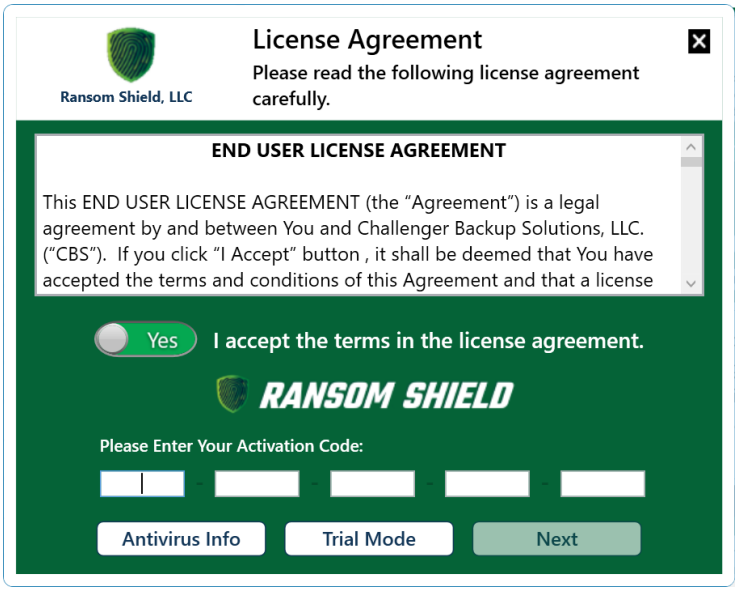
RANSOM SHIELD
Software User Guide

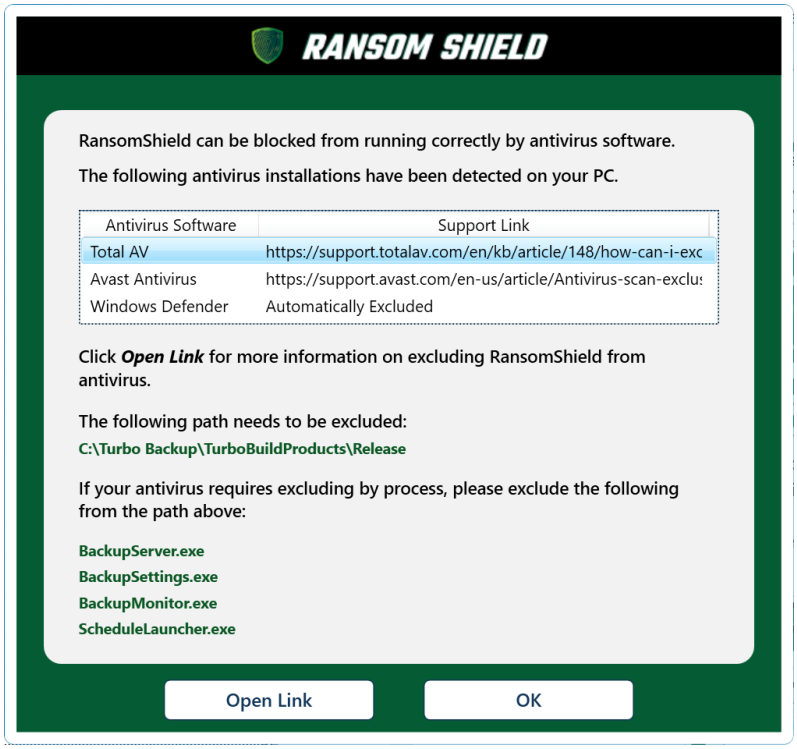
Table of Contents

1- Installation

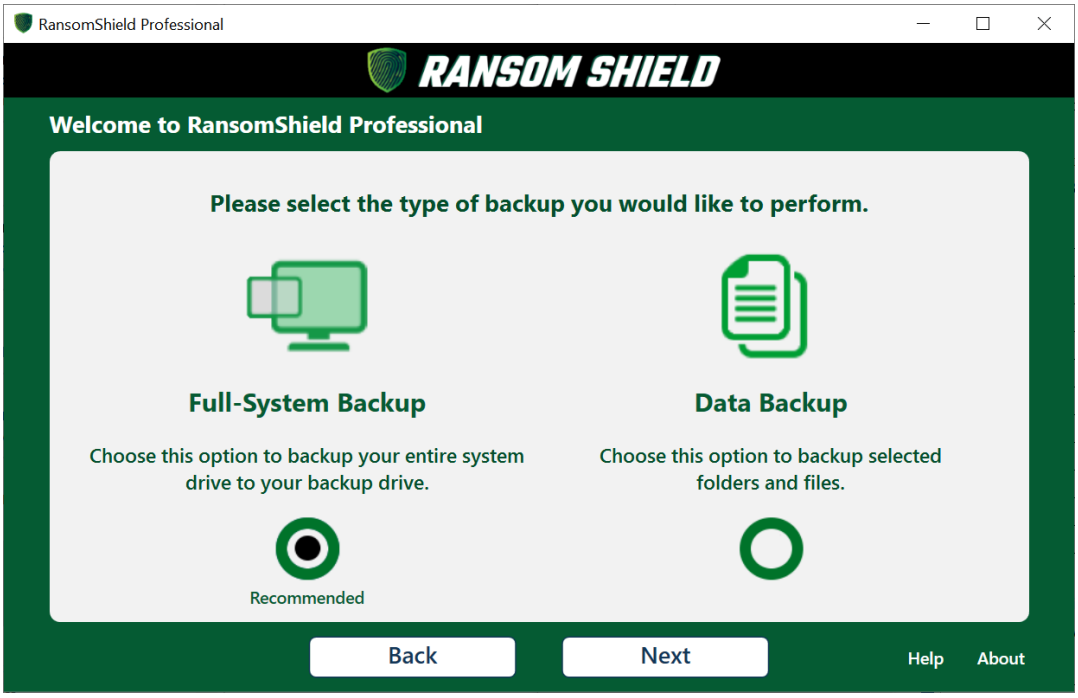
After clicking **Yes** to accept the license agreement, you're prompted to enter your code. You should have received a license key when you purchased the software. You can copy and paste the entire code here. If you want to install Ransom Shield in trial mode, click **Trial Mode**.



Ransom Shield needs low-level access to your backup drive, so some antivirus software may interfere with the backup process. Clicking **Antivirus Info** will display a list of each of your installed antivirus solutions. Clicking **Open Link** will display instructions in your browser for excluding Ransom Shield from your antivirus program. If you're using Microsoft antivirus, exclusions are built automatically.

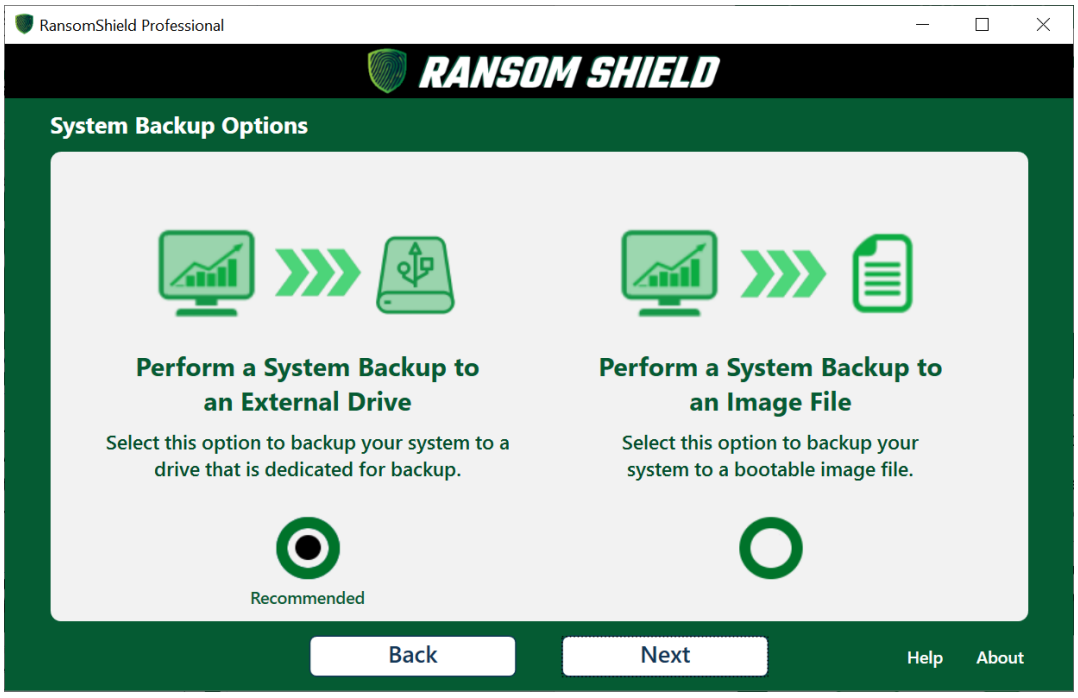


The next step is to select what type of backup you would like to perform. If you want to backup your entire system drive, select **Full-System Backup**. If you would prefer to select specific folders and files to backup, select **Data Backup**. For the Advanced version, this step is skipped, and you move directly to selecting your backup drive.

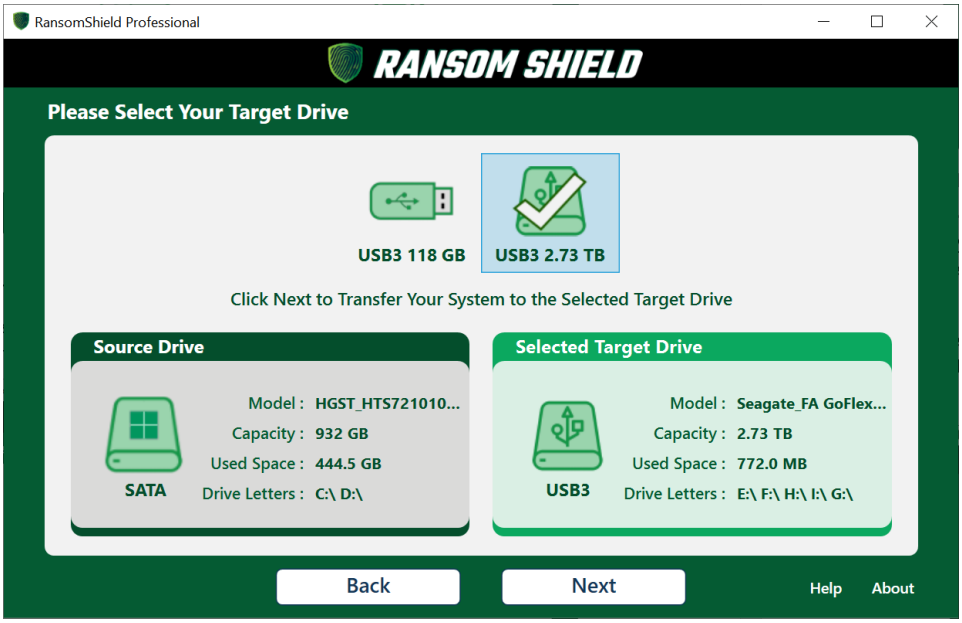


The Full-System Backup option will allow you to create a bootable backup to an external USB drive, and is the recommended method of backing up.

For the professional version, there are two types of full-system backups. For most users, selecting the first option to mirror to a second drive is recommended.



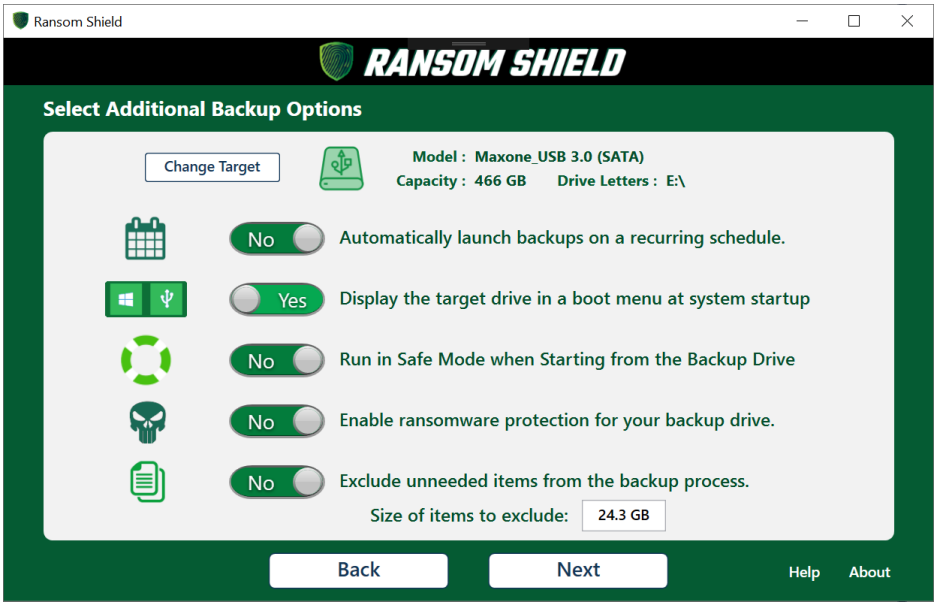
You're next asked to select the backup drive to target for your full-system backup. If there is only one drive available, it is automatically selected. The system drive is also selected automatically.



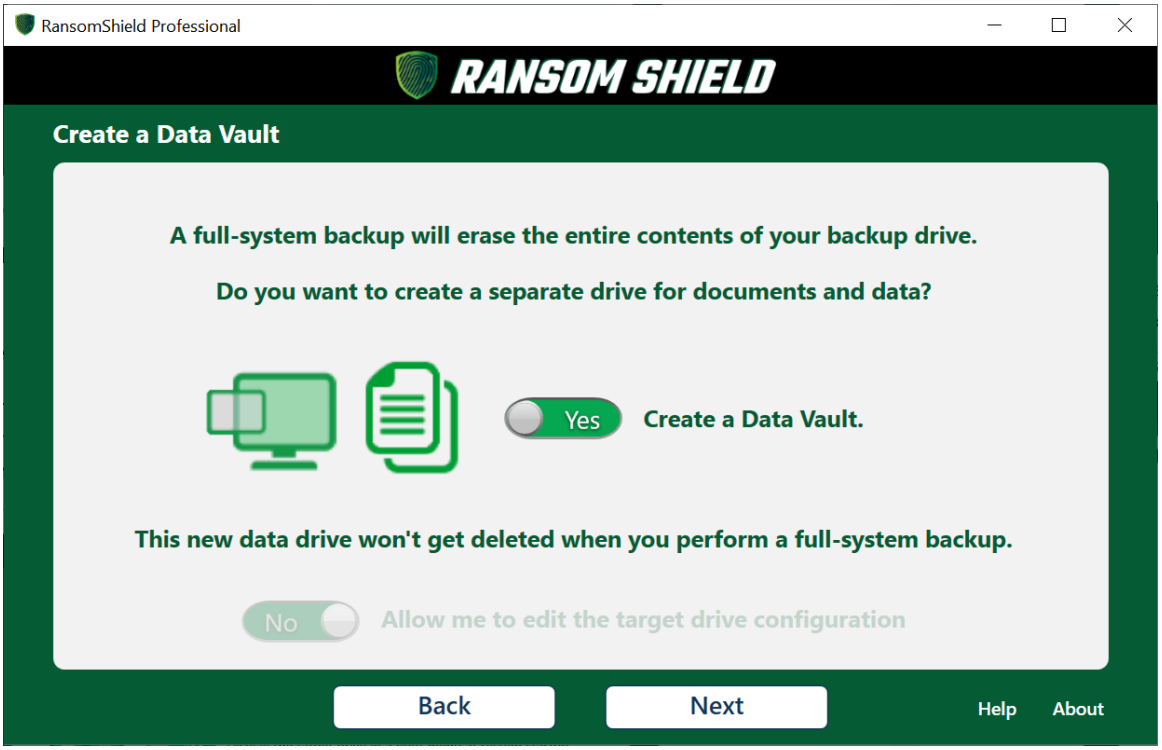
You have 4 options available when creating a bootable backup:

1) Create Backup Schedules (see section 3- Scheduling Backups)
2) Display a Boot Menu at Startup (see section 4- Creating a Startup Boot Menu)
3) Start the Backup Drive in Safe Mode
4) Enable Ransomware Protection (see section 5- Ransomware Protection)
5) Exclude unneeded items from the backup process

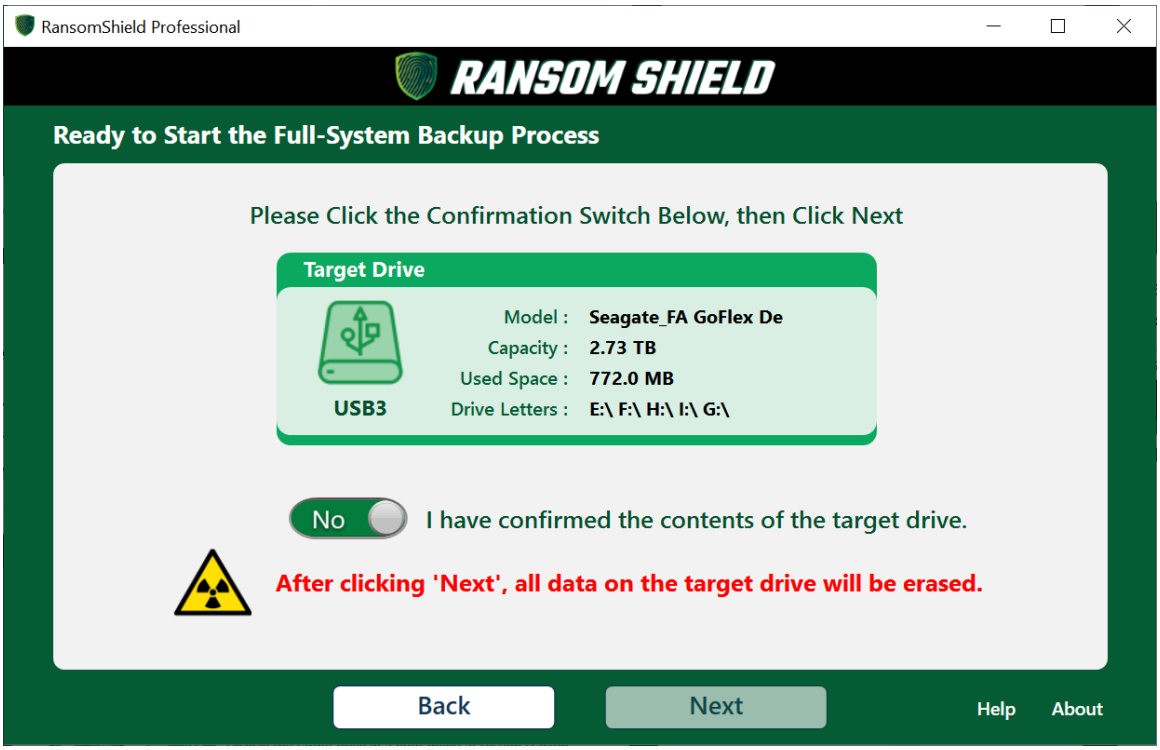
Unneeded items include the Windows temp folder, internet temp folders, plus various cache and log folders. The hibernation file, page file, and crash dump files are also excluded. All items excluded are not needed for backup or the booting process.



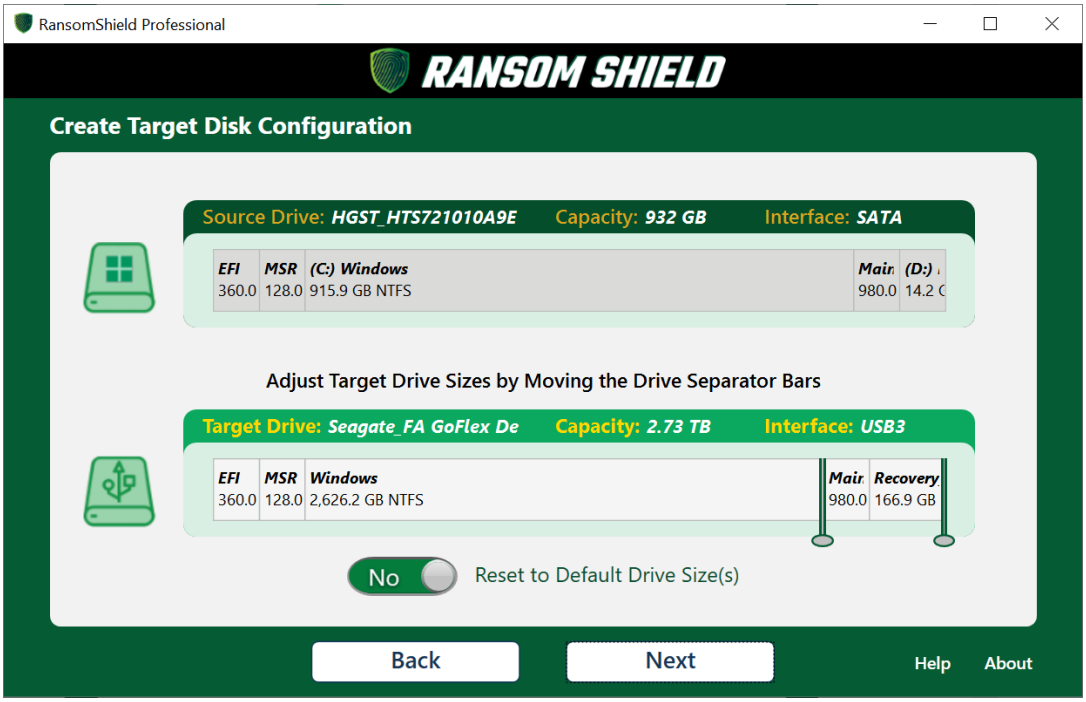
Next, select if you would like to create a Data Vault on your Ransom Shield drive. This will allow you to store items on the backup drive that won't get deleted during your next full-system backup.



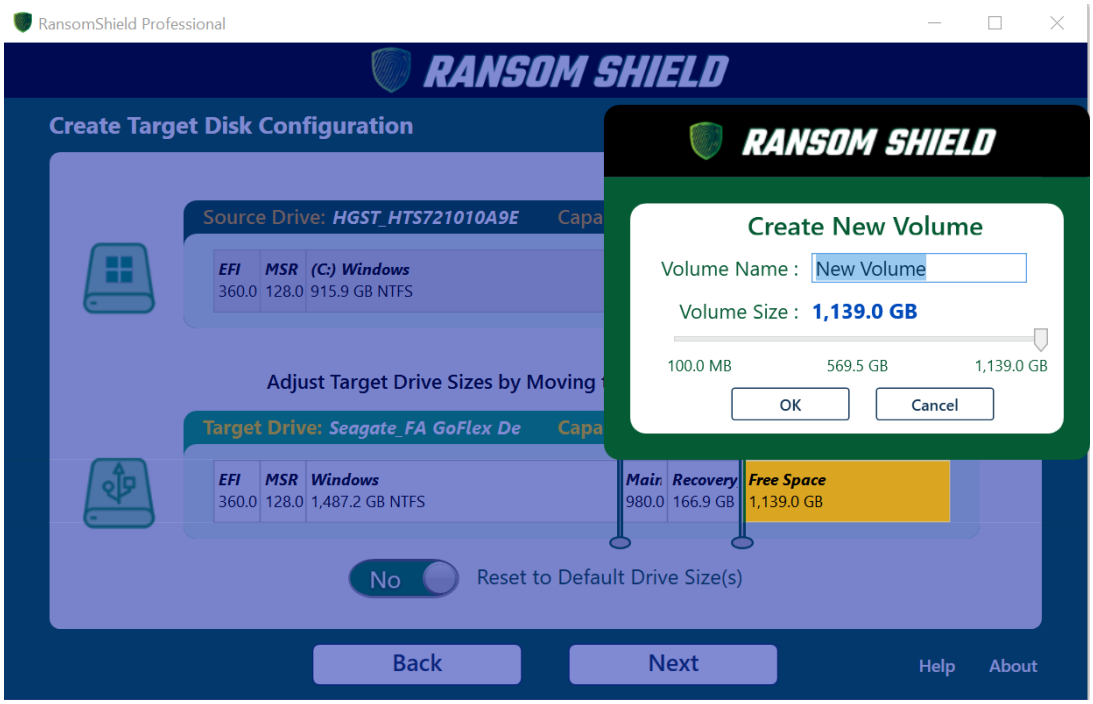
The final installation screen asks you to Click **Yes** to verify that there's no data on the backup drive you want to keep. Clicking **Next** will start the backup process and wipe the drive clean.



NOTE: Advanced users can alter the partition structure of their Ransom Shield drive by clicking the **Back** button from the previous confirmation screen.



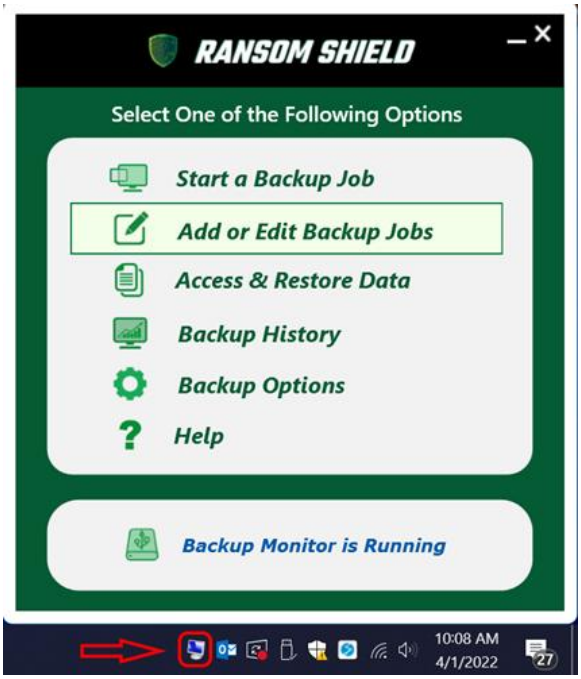
Move the sliders left or right to change the size of a partition. As you move the sliders, the free space of the partition on the left and right will display, along with the new capacity of both partitions. Maintenance partitions created by Windows or the PC OEM cannot be resized.



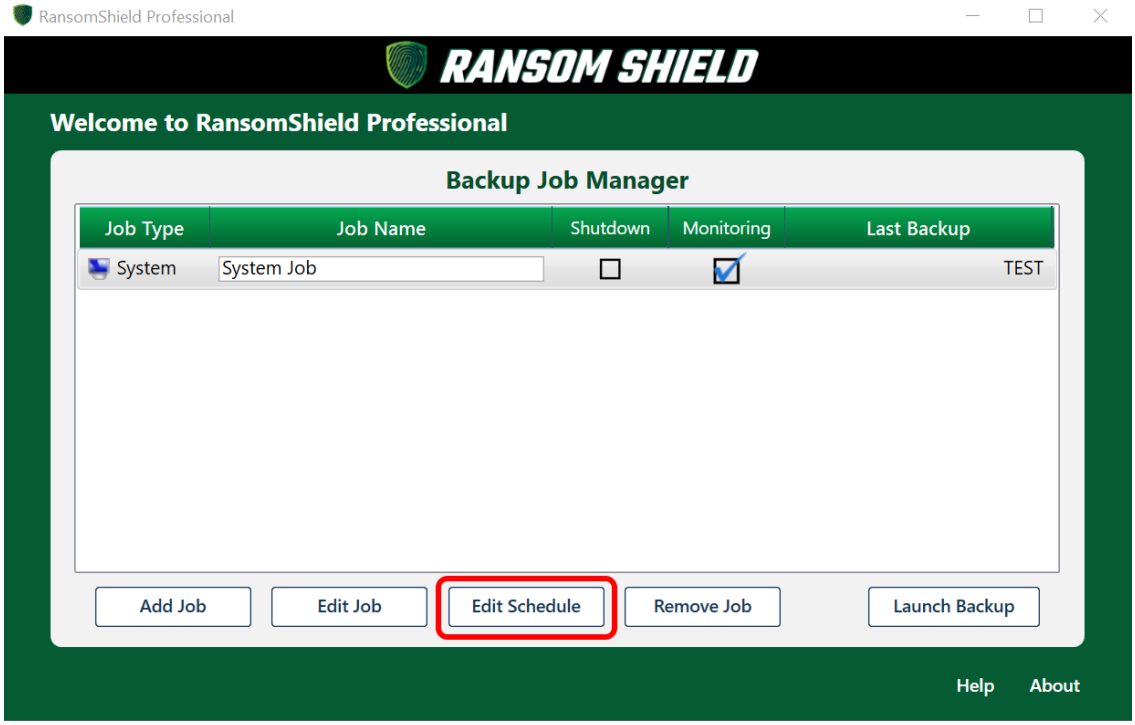
Clicking on free space allows you to create new partitions. Partitions can also be deleted from this view. Click the **Reset** button at any time to restore the default partitions sizes.

2- Scheduling Backups

Ransom Shield can launch backups on a re-occurring schedule. Scheduling is supported for full-system and data-only backups. To create a backup schedule, select **Add or Edit Backup Jobs**.



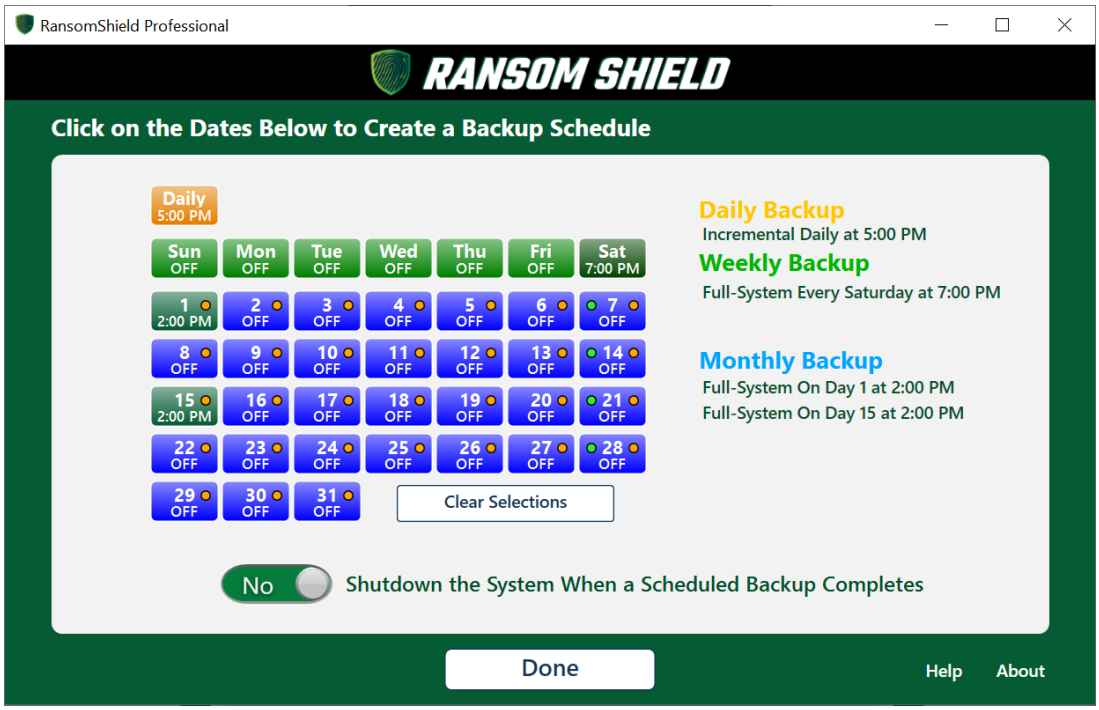
Next, click the Edit Schedule.



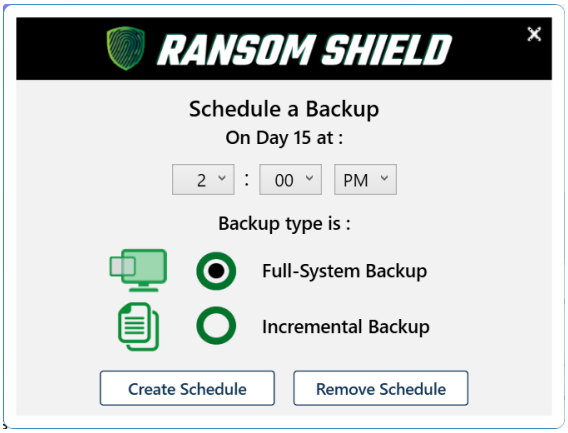
Ransom Shield allows you to create your backup schedules daily, weekly, or monthly. You can create up to 39 different triggers for each backup job.

To create a daily backup, click on the orange button on the upper right of the display. Create weekly schedules by clicking any of the 7 green buttons, and create monthly schedules with the blue numbered buttons. Don't forget that you can create multiple triggers for each schedule.

You can also **shut down your PC** after the scheduled backup completes.



In the example above, the same backup job is scheduled for daily incremental backups at 5PM, full-system backups every Saturday, and a full-system backup on the 1st and 15th of every month.



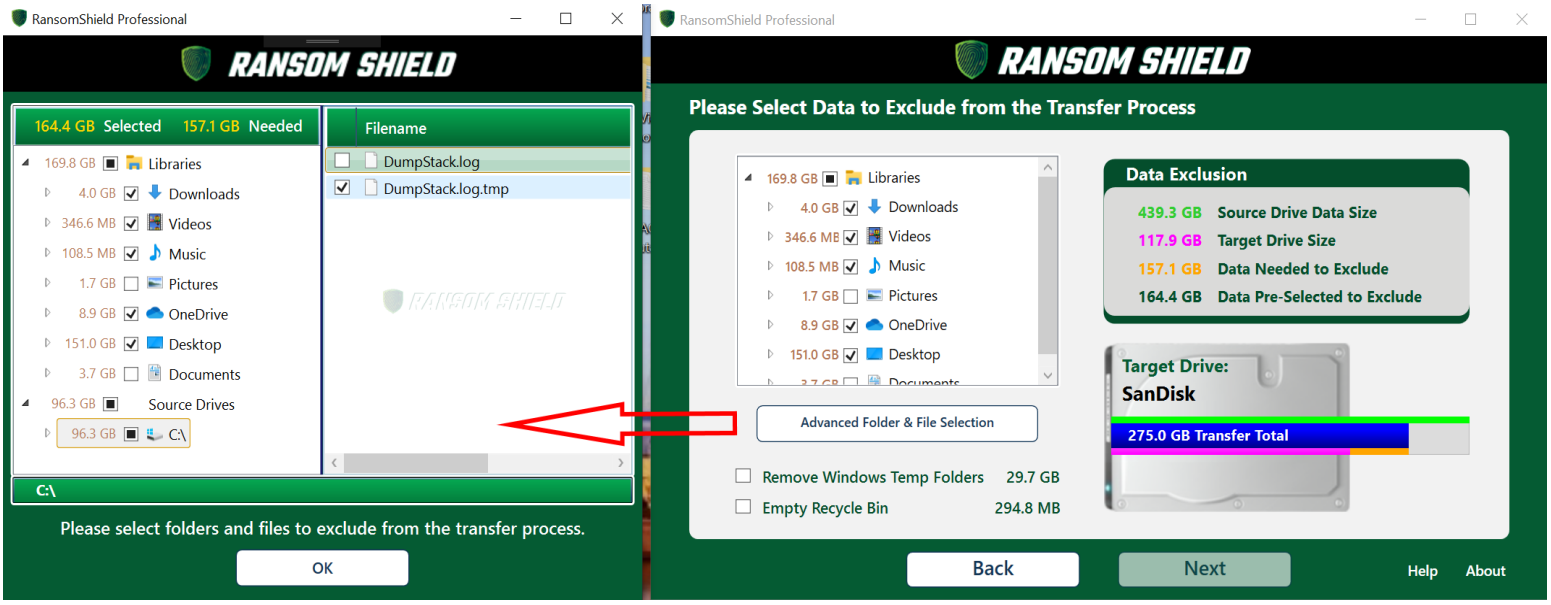
After clicking a schedule button, you're next prompted to select the time the backup will trigger. From here, select a full backup, or only files that have changed since your last backup.

IMPORTANT: Full-system backups will cause Ransom Shield to monitor the entire system for changes. This could cause slower performance of the OS. Ransom Shield does exclude certain cache and temporary folders from this process, but slowness may still occur. If possible, it's recommended to perform daily or weekly full-system backups and not incremental backups.

3- Backup Exclusion Process

If your backup drive is not large enough to fit all the data on the system, then Ransom Shield allows you to select folders and files to exclude from the backup process. If you select all items allowed for exclusion, then a **minimal boot drive** is created. This is a backup that only contains the Windows operating system plus all applications installed on the system. If your Ransom Shield drive is not large enough to contain a minimal boot drive, then the backup process is halted, and you are asked to connect a larger drive.

NOTE: The user interface does not allow selection of data that would render the backup drive unbootable. It also does not allow selecting applications for exclusion.



The bars represented in the UI's hard drive display above are color-coded to correspond with the **Data Exclusion** totals.

Green – Size of data on the source drive

Pink – Size of the target drive

Orange – Amount of data required for exclusion

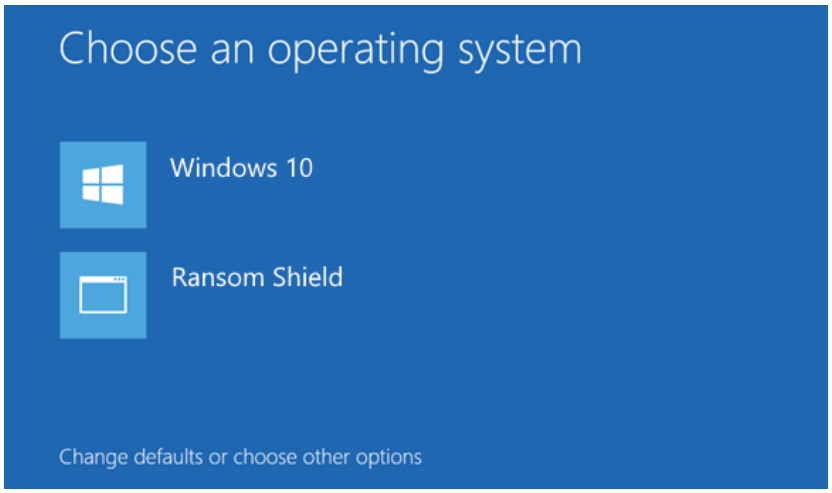
Blue – Amount of data that will be transferred to the target drive

As data is selected for exclusion in the UI, the exclusion amount required before the transfer will fit is updated. The blue bar on the hard drive will then slide to the left. Once this bar is inside the drive display, the **Next** button is enabled, and you're allowed to continue.

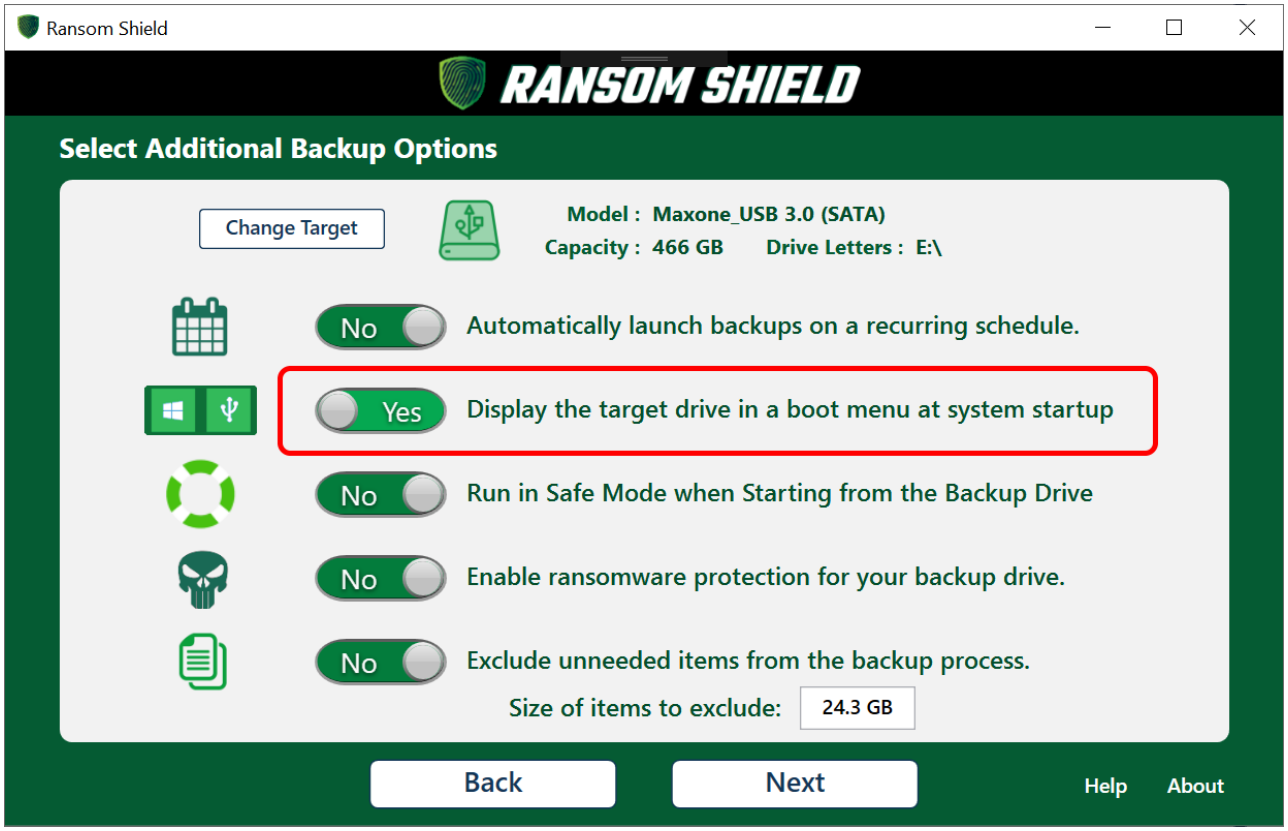
For image backups, you have the option of selecting an image smaller than the recommended size. When this occurs, the backup process will always ask you to exclude data from the image backup process as well.

4- Creating a Startup Boot Menu

Creating a startup boot menu will allow you to select which drive to start your PC from. If you enable this option, the following menu will be displayed each time you start your PC. The default option is to start from your system drive. Select the second option if you would like to start from your Ransom Shield drive. This menu will display for 15 seconds, then continue and start normally.

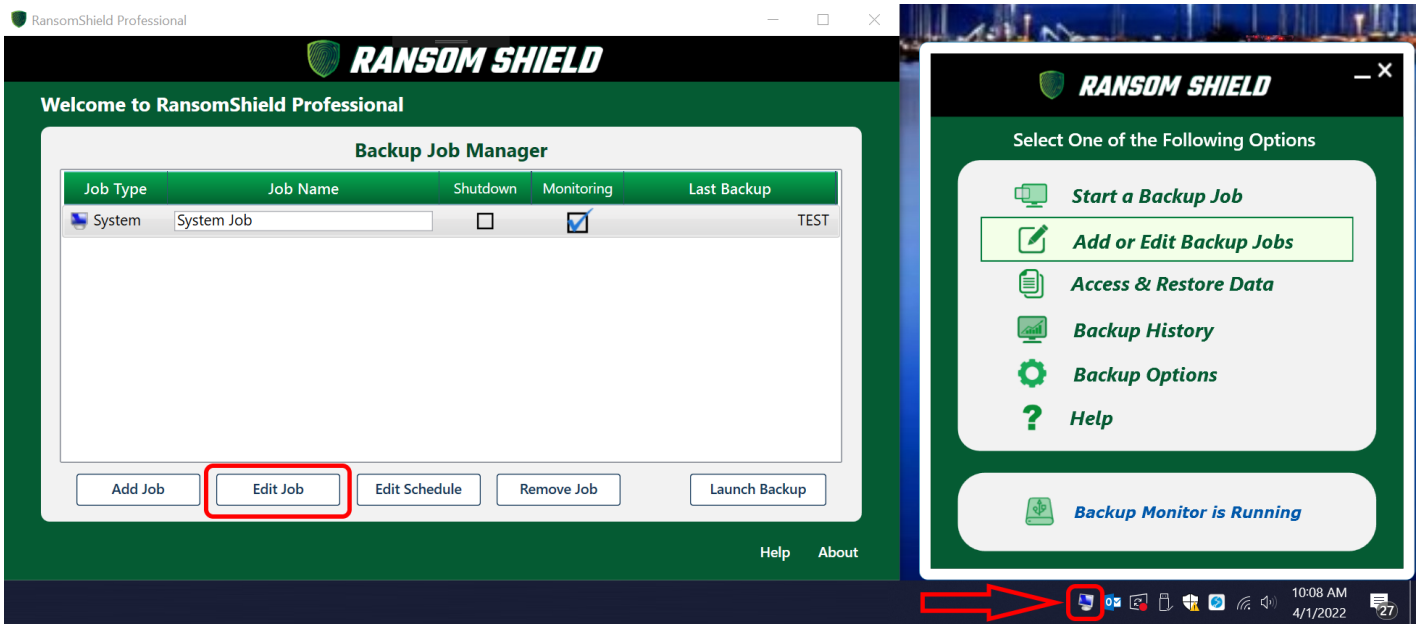


You can select to create a startup boot menu when you initially create a full-system backup.

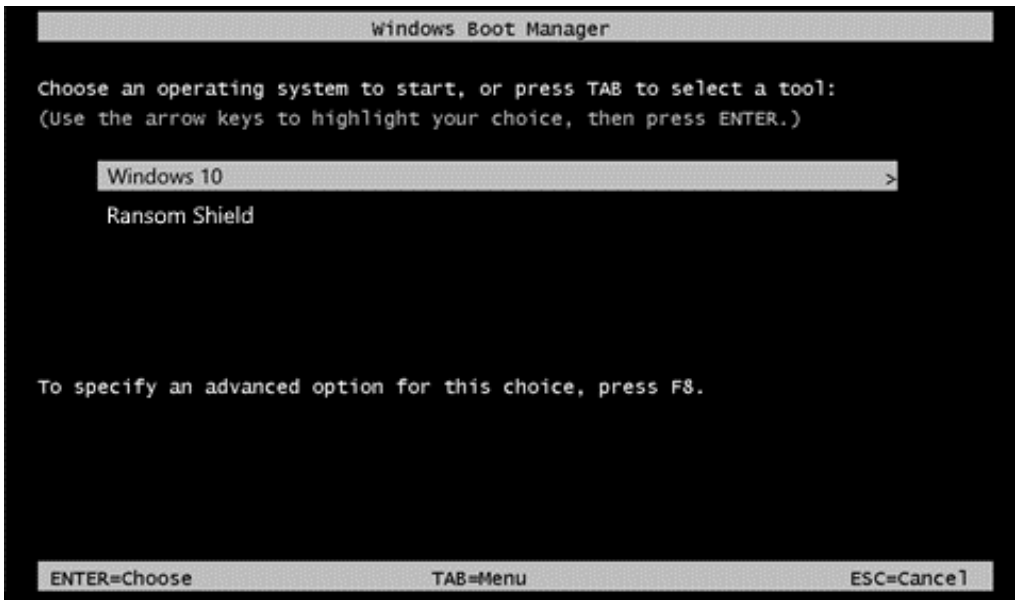


Your Ransom Shield software will create a startup boot menu by default. Change the switch from **Yes** to **No** if you don't want the startup menu to display every time you start your PC.

If you don't create a startup menu then change your mind, you can create it at any time by editing your backup job. To do this, click the Ransom Shield icon in the system tray, then select **Add or Edit Backup Jobs**. Next, select **Edit Job** to turn the startup menu on or off.



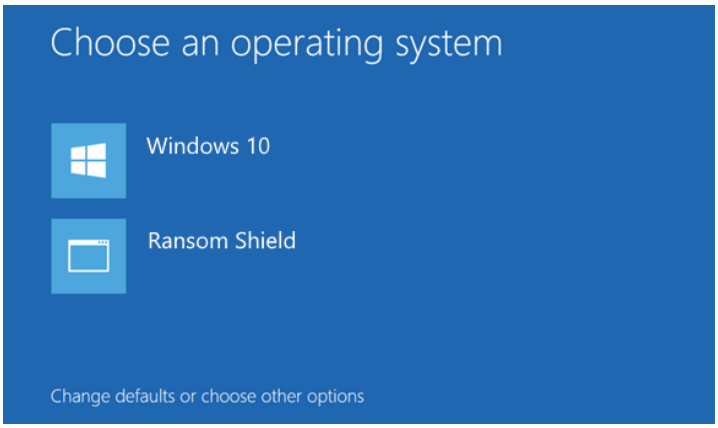
You can start your PC from the Ransom Shield drive at any time by selecting the Ransom Shield option at startup.



5- Starting from Your Ransom Shield Drive

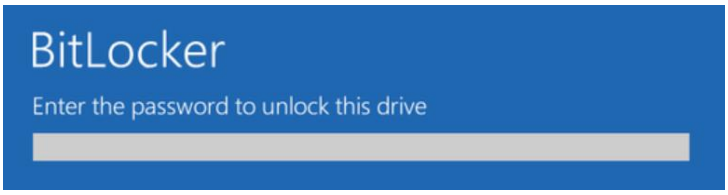
Ransom Shield is unique among PC backup applications in its ability to allow immediate verification that the backup process worked correctly. To do this, start your PC from your Ransom Shield drive! All your applications, Windows settings, internet connectivity, and OneDrive work as if you were running from your internal system drive.

If you chose to create a startup boot menu, you will be prompted each time you reboot if you would like to start from your Ransom Shield drive. After 15 seconds, your PC will automatically start as normal from your system drive.



If you don't create a startup boot menu, you can use your BIOS boot menu to start from your Ransom Shield drive. You do this by tapping the hot key for your PC manufacturer to access the BIOS boot menu. See the troubleshooting section at the end of this guide for a list of BIOS hotkeys.

If you selected to encrypt your Ransom Shield drive, you're prompted to enter the password first.



The type of storage device you select will have a big impact on performance. Many flash drives use older technology that make the booting process painful. An external SSD or a second internal drive are highly recommended and can often boot as fast or faster than your internal system drive.

After your PC has started from your Ransom Shield drive, a popup message displays informing you that your system is running from your Ransom Shield drive.

Gauge Values

Dark blue < 90 seconds

Light blue < 4 minutes

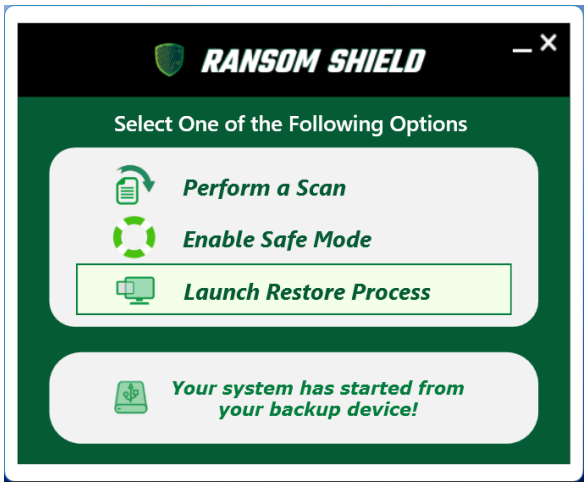
Yellow < 6 minutes

Red > 6 minutes

The **Backup Drive Startup Time** measures the time between PC startup up when the popup is displayed. This won't be accurate if your login screen is left idle.

Full-System Restore from Your Ransom Shield Drive

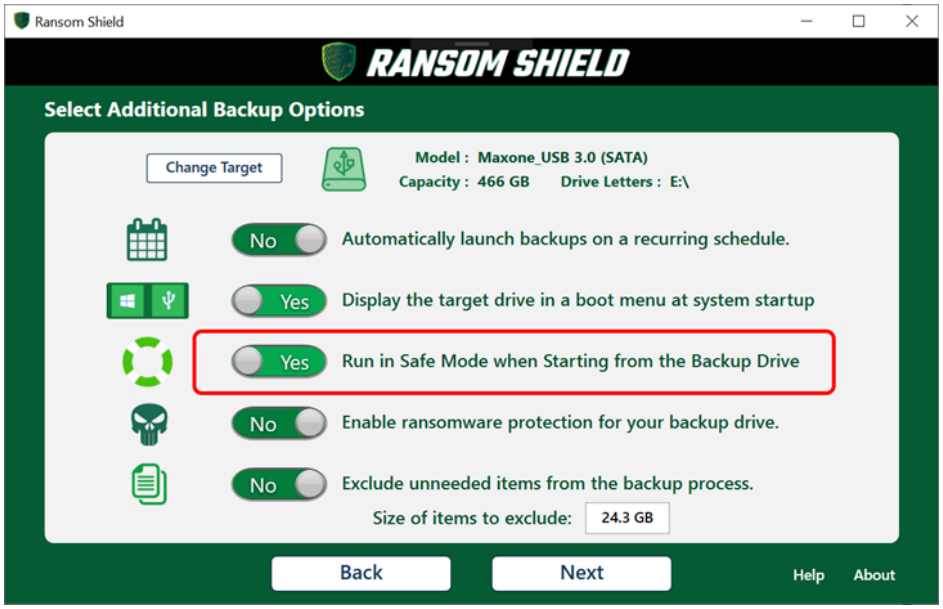
Clicking the Backup Monitor icon in the system tray displays your backup options when running from your Ransom Shield drive. Clicking on the **Launch Restore Process** option will start a full-system restore. This allows you to restore from your booted Ransom Shield drive to your internal drive, or to any connected storage device. Any changes made while running from the booted Ransom Shield drive will be included in the full-system restore process.



6- Starting Your Backup in Safe Mode

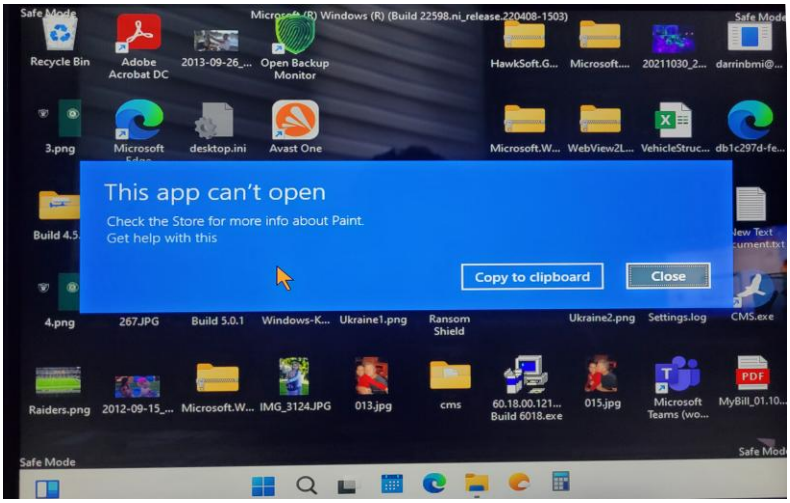
Ransom Shield provides a safe environment to run your system if a ransomware strike or other malware infects your PC. In the safe mode environment, all startup apps, most services, and most drivers are disabled. In this locked down environment, ransomware and malware should be disabled and should not be allowed to install or execute, even if backed up to the Ransom Shield drive. Ransom Shield allows you to scan the PC and remove malware in this environment.

To turn on the Safe Mode booting environment for your Ransom Shield drive prior to your first full-system backup, select ***Yes*** for the Safe Mode option in the screen below.



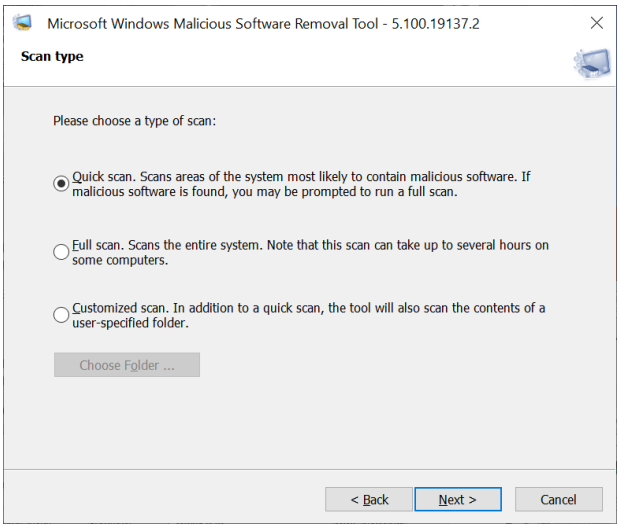
After your first full-system backup has completed, you can change this option at any time by selecting ***Add or Edit Backup Jobs*** in the system tray app. Toggling this option on or off will immediately turn safe mode on or off on your Ransom Shield drive.

When booted in safe mode, basic applications like notepad and paint won't run.



Running in safe mode may provide a lower screen resolution but scaling from your display settings can usually be accessed to make your screen more readable. Ransom Shield's patent-pending technology allows you to run Ransom Shield from within the safe mode environment, but you do need to double click the Ransom Shield icon on the desktop.

Performing a scan of your PC is recommended when running in safe mode. This will allow you to verify and clean any malware or viruses from your PC with the Windows Malicious Software Removal Tool. To scan your internal drive, use the ***Customized scan*** option.



Once you've scanned and cleaned your system, select the ***Disable Safe Mode*** option to turn safe mode off. The next time you restart and run from the Ransom Shield drive, you'll run in your normal environment and have full access to your PC.

7- View Backup History

To get a detailed report of previous backups, please do the following:

1) Right-click the Ransom Shield icon in the system tray
2) Select **Backup History**

Your backup report includes all your previous incremental and full backups, the time and duration of the backup, file and byte totals, plus the result and any errors if applicable.

You can also view previous files backed up during incremental backups and view a list of files that are scheduled for your next incremental backup.

8- Creating a Data Vault

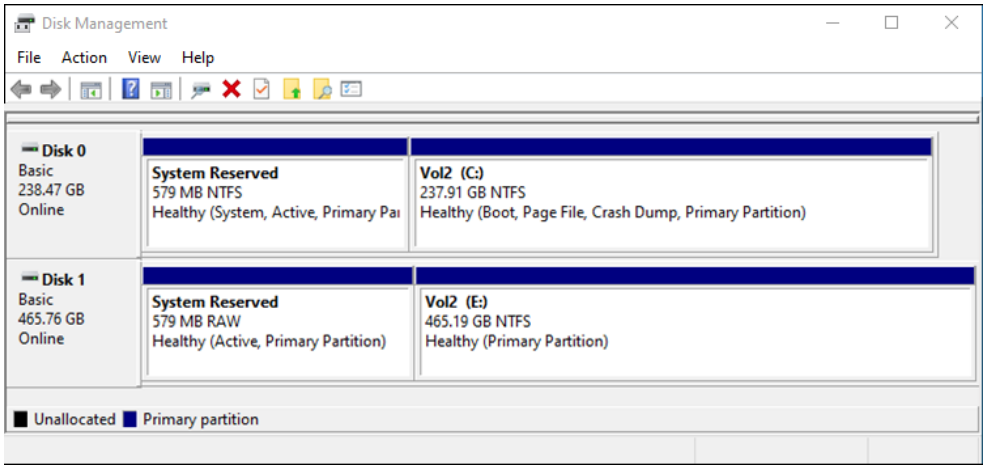
Many users will want to create both full-system and data-only backups, and schedule both backup types on a reoccurring basis. For both backup types, you have the option of performing a full backup, or an incremental backup (backup of changed files only). Data backup jobs will maintain previous versions of all your files backed up.

IMPORTANT: If you target your Ransom Shield drive for data backups, a full-system backup will erase your Ransom Shield drive, including all backup versions and history.

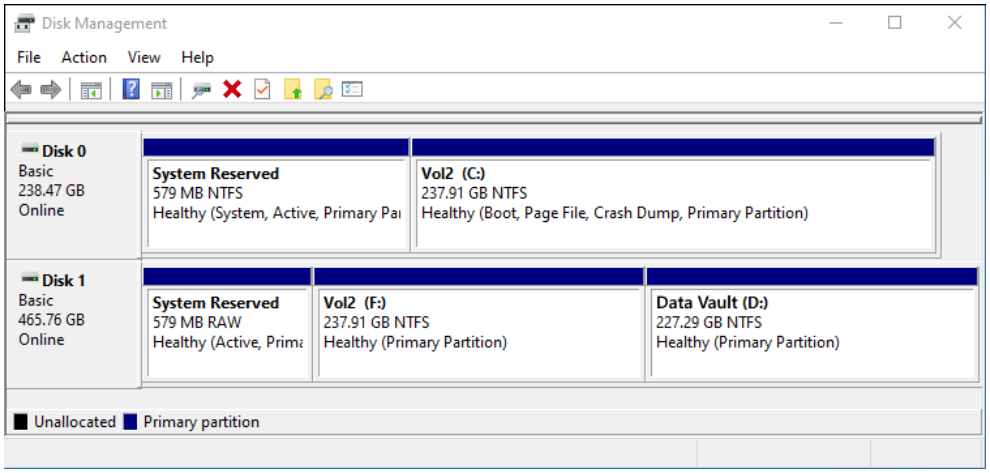
How can you solve this problem? Create a Data Vault!

Ransom Shield allows you to create an extra data drive on your backup drive called a Data Vault. This additional drive is created after the mirror created by a full-system backup. Whenever subsequent full-system backups are performed, the Data Vault is left intact and not deleted. This allows for storing data that only exists in the Data Vault and not on the system drive. Ransom Shield no longer requires separate backup drives for both full-system and data-only backups.

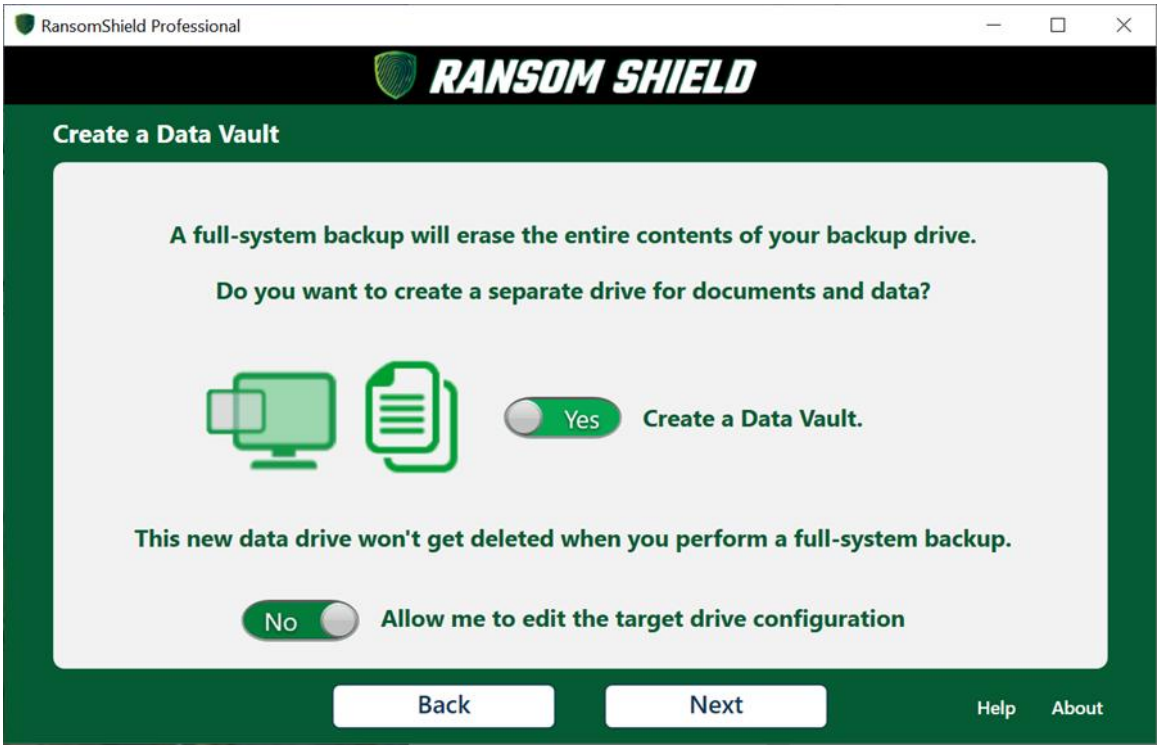
Backup Drive Configuration Without a Data Vault



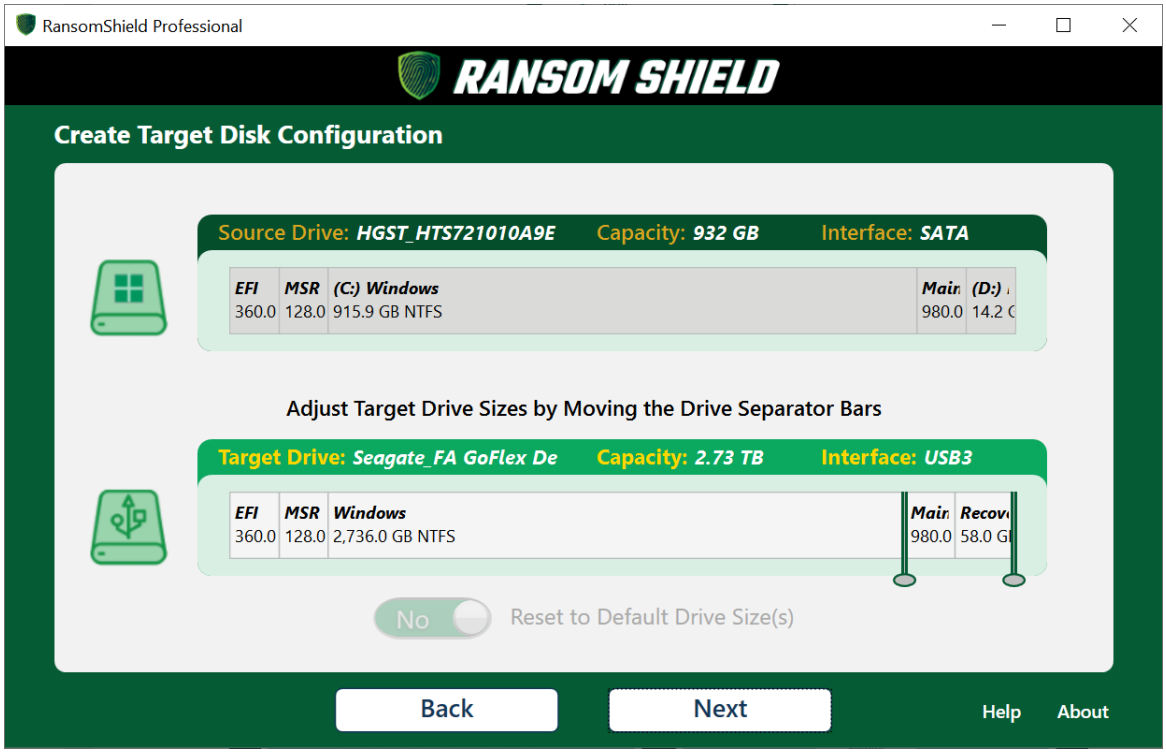
Backup Drive Configuration with a Data Vault



Selection Process in the Ransom Shield UI



The default size of the Data Vault can be changed by the user by clicking the toggle on the bottom of the screen to **Yes**. This feature is especially useful for large capacity backup drives.

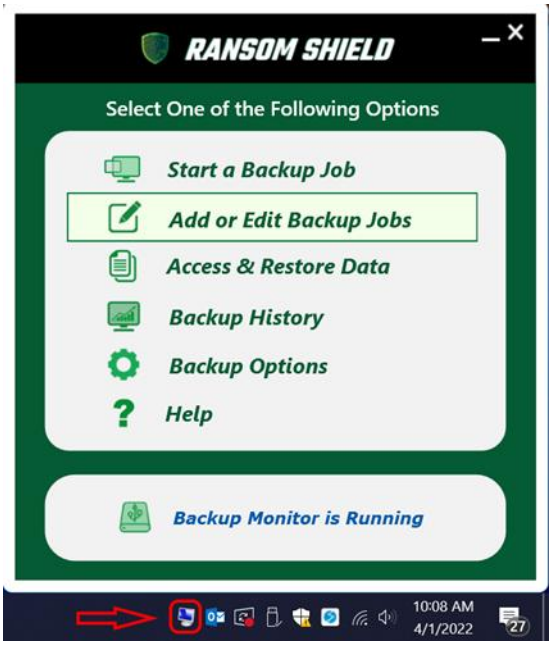


WARNING: Turning Data Vault **OFF** will result in the extra drive getting deleted during the next full-system backup, along with any data stored in the extra drive.

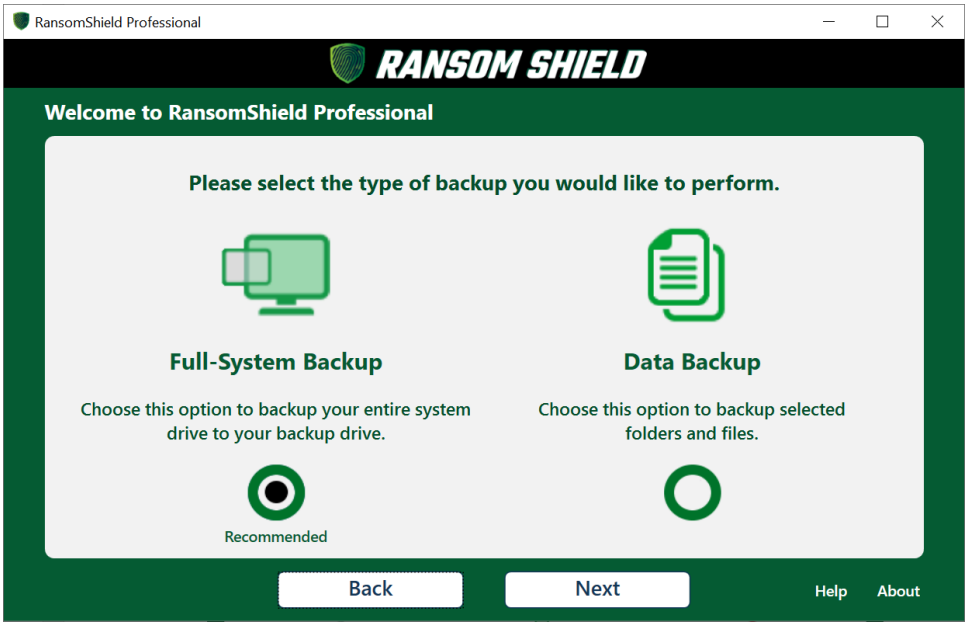
9- Data-Only Backup

In addition to full-system backups, Ransom Shield also allows selecting folders and files for backup. The resulting backup job can be scheduled for both full and incremental backups, supports ransomware protection, and backing up your data in real-time. To create a data-only backup, please do the following:

1) Right-click the Ransom Shield icon in the system tray
2) Select **Add or Edit Backup Jobs**

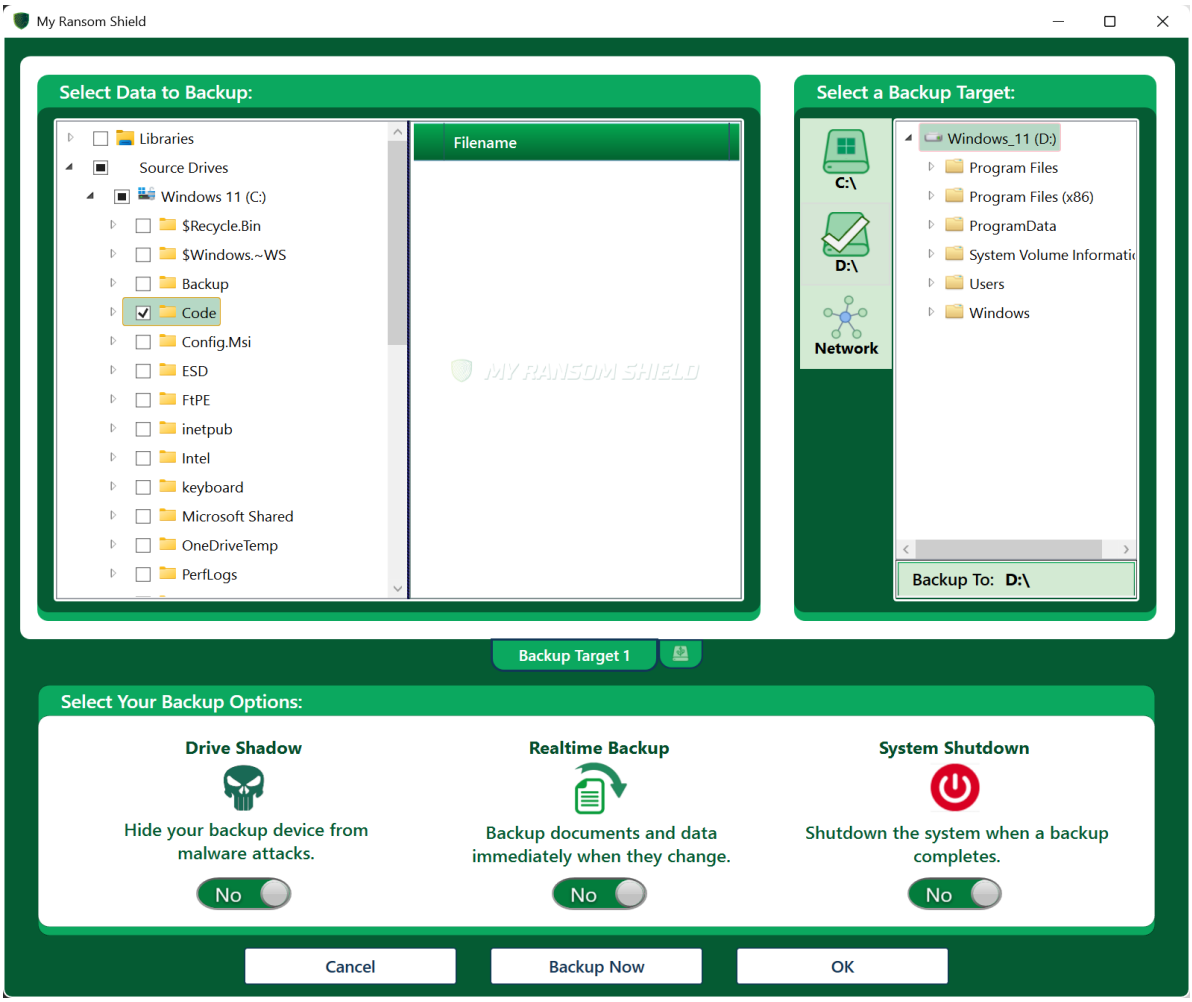


1) Click the **Add Job** button
2) Select **Data Backup**



The next step is to select the folders and files that you want to backup under the section titled, **Select Data to Backup**. This can be a drive or folders, including the selection of individual files. Once your data is selected, choose where to backup to in the **Select a Backup Target** section.

Ransom Shield supports backing up to more than one backup target in the same backup job. To do this, click the tab next to **Backup Target 1** below.



Three options are supported for data-only backups to your Ransom Shield drive:

1) **Drive Shadow**
2) **Shutdown System**
3) **Realtime Backup**

Realtime Backup backs up the selected documents or files immediately when they change. This option is best suited for desktop PCs where your Ransom Shield drive is always connected. This may also come in handy for laptops that need to backup to network paths. Ransom Shield fully supports backing up to network paths, including NAS drives.

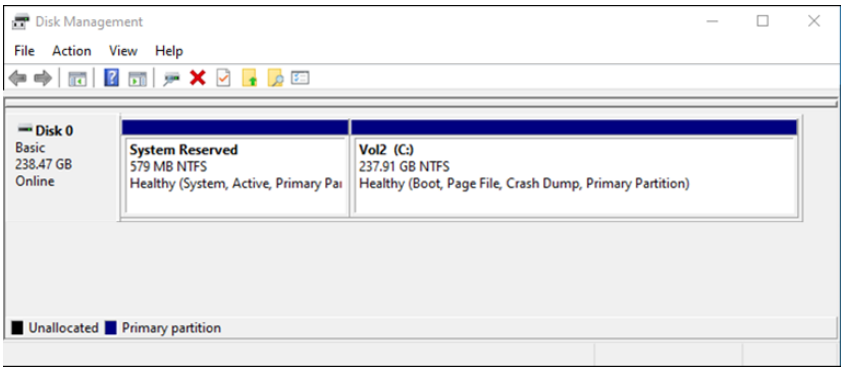
If you prefer not to utilize the real-time backup option, Ransom Shield can schedule data-only backups on a daily, weekly, or monthly basis. Both full data and incremental backups can be scheduled. To access and restore your data, please see the **Restoring Folders & Files** section of this guide.

10- Drive Shadow

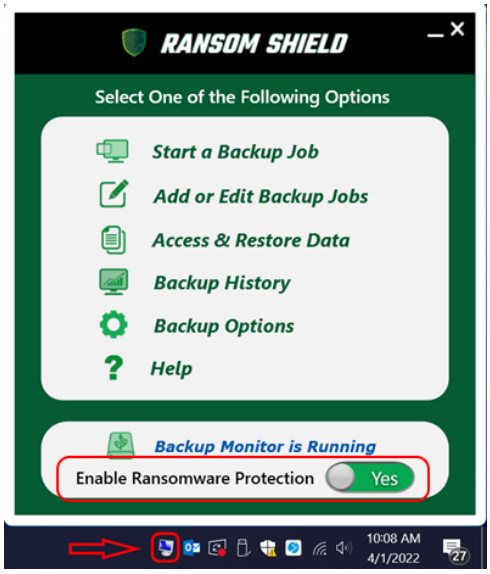
Ransom Shield has patent-pending technology that allows you to protect your Ransom Shield drive from ransomware attacks. By disabling the drive after a backup completes, ransomware cannot access the drive or your data. Your Ransom Shield drive is only visible while a backup is in progress. If ransomware infects your system at any point, you can reboot and start directly from your Ransom Shield drive. Drive Shadow is supported for both full-system and data-only backup and can be enabled when creating a new backup job, or when editing an existing job.

WARNING: This feature disables access to your Ransom Shield drive except when a backup is in progress. You may not want to use this feature if you need to access your Ransom Shield drive.

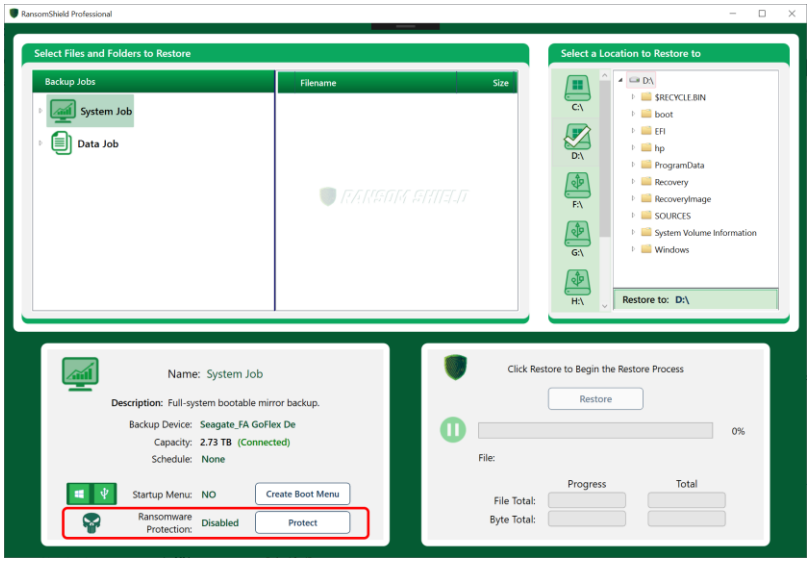
You can verify that Drive Shadow is working correctly in the Windows Disk Manager program. When enabled, your Ransom Shield drive will not be visible.



You can toggle Drive Shadow on or off from the Backup Monitor in your system tray. This will **temporarily** enable or disable protection. After your next backup completes, Drive Shadow will be disabled, and your Ransom Shield drive will be hidden from the system.

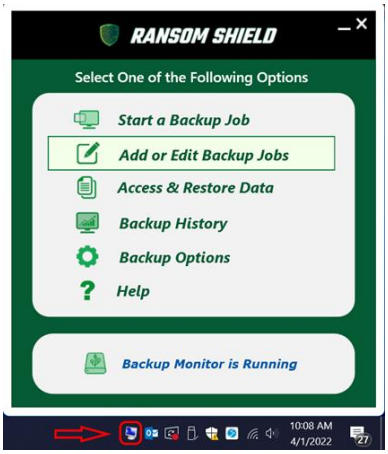


You can also toggle Drive Shadow on or off from the **Access & Restore Data** application.

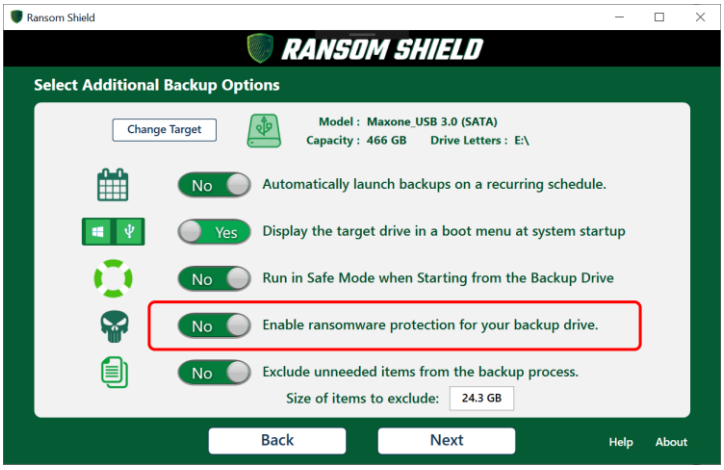


If you want to **permanently** turn Drive Shadow on or off, perform the following steps:

1) Right-click the Ransom Shield icon in the system tray
2) Select **Add or Edit Backup Jobs**



3) Click the **Edit Job** button
4) Toggle the switch for **Enable Drive Shadow for your backup drive**



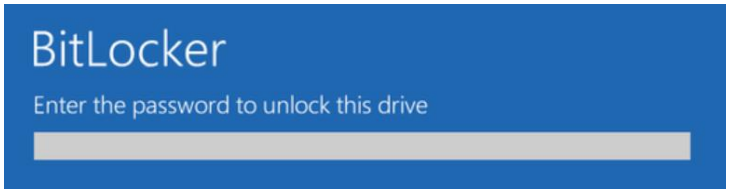
NOTE: Drive Shadow is not compatible with the real-time backup feature for data-only backups.

11- BitLocker Full-Disk Encryption

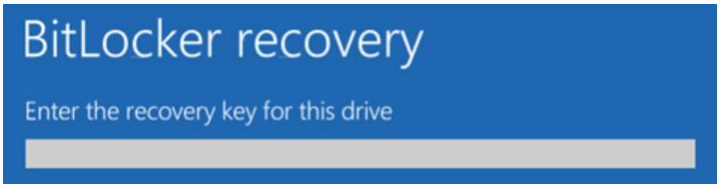
Ransom Shield allows you to create a full-system backup using BitLocker encryption. If your Ransom Shield drive is lost or stolen, the contents cannot be accessed without the correct password. BitLocker can be utilized on your Ransom Shield drive even if the internal drive is unencrypted or is encrypted with third party encryption. When creating a full-system backup, you're given the option to enable BitLocker encryption.

NOTE: Image backups do not support BitLocker.

The password will be required to unlock the drive when starting from your Ransom Shield drive:



In addition to a password, Ransom Shield supports setting a recovery key. This allows you to unlock the drive from the key in case you forget the password. You can enter your recovery key at startup by clicking **ESC** from the password prompt. The recovery key is saved to a file and can be stored on the local PC, or to a remote location.



Other encryption options include:

Auto Unlock	The Ransom Shield drive is unlocked whenever the drive is connected
Lock on Completion	Your Ransom Shield drive will lock after a backup completes
Store Password	If you schedule your backups, your BitLocker password will be encrypted and stored locally.

NOTE: You cannot launch scheduled backups to encrypted drives without storing the password.

You can change your BitLocker password, or lock and unlock the drive at any time by selecting to **Add or Edit Backup jobs** from the Backup Monitor app in the system tray.

1) Right-click the Ransom Shield icon in the system tray
2) Select **Add or Edit Backup Jobs**

5) Click the **Edit Job** button, then click **Next**

BitLocker for Enterprises

For enterprise customers, Ransom Shield supports backing up systems with **McAfee Endpoint Encryption** and converting your Ransom Shield drive to BitLocker. If a disaster strikes such as a ransomware attack, the internal drive can be restored from the booted BitLocker backup drive. After rebooting the PC to the newly restored internal drive, all the McAfee tools are in place and ready to re-encrypt with Endpoint Encryption.

Trusted Platform Module

BitLocker normally requires a Trusted Platform Module, or TPM on your computer's motherboard. This chip generates and stores the actual encryption keys. It can automatically unlock your backup drive when connected, or prompt you for the password. Ransom Shield lets you select which behavior is best for you. When booting the backup drive, you are always asked to type your password at boot time.

If someone tampers with the PC and removes the internal drive in an attempt to decrypt and access data, it won't be accessible without the key stored in the TPM. The TPM also won't work if moved to another PC's motherboard. Ransom Shield also supports BitLocker encryption on PCs that don't have a TPM module.

Ransom Shield Admin Console

Administrators can control which Ransom Shield features are exposed to the user with the Ransom Shield Admin Console. For instance, if it's determined that the enterprise does not want their users to create a Data Vault or a startup boot menu, these features can be disabled and hidden from view during installation. Admins can also control how BitLocker passwords are created and stored. This includes automatically encrypting drives without their knowledge and storing the passwords in encrypted form at a remote location. Please contact us for more details.

Group Policy Management of BitLocker and Ransom Shield Drives

Microsoft Azure Active Directory (Azure AD) and Microsoft Intune bring the power of the intelligent cloud to Windows 10 device management, including management capabilities for Ransom Shield with BitLocker. Some of these capabilities work on Windows 10/11 Pro, while other capabilities require Windows 10/11 Enterprise or Education editions. For more information please see the following:

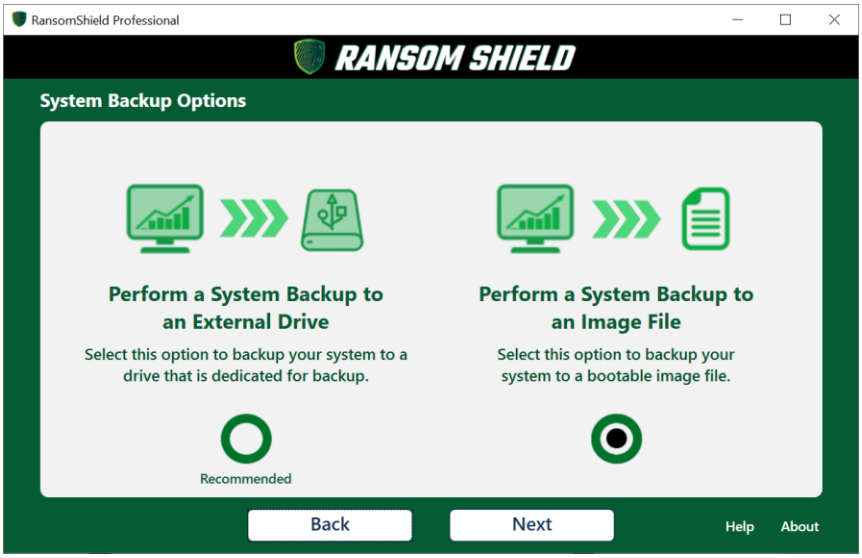
https://techcommunity.microsoft.com/t5/microsoft-endpoint-manager-blog/managing-bitlocker-with-microsoft-endpoint-manager/ba-p/1582523

12- Image Backup with VHDs

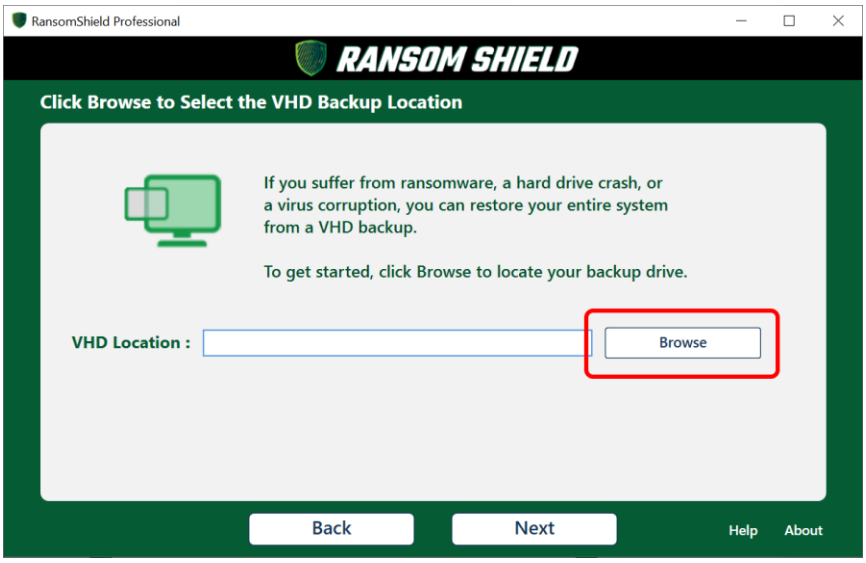
Ransom Shield supports VHD image backup, which allows full-system backups of multiple PCs to the same backup drive. In most instances, these backups can be made bootable on PCs that were not the original backup target. If Ransom Shield is installed on multiple PCs, each PC can be started from the same backup drive!

VHD backups are a snapshot of your entire system at the time a backup is performed, which allows you to boot and rollback your system to a previous backup date. Multiple VHD backups can also be mounted at the same time to allow access to previous file versions.

To create a VHD backup, click the Ransom Shield icon in the system tray, then select **Add or Edit Backup Jobs**. Select **Full-System Backup**, then **Perform a System Backup to an Image File**.

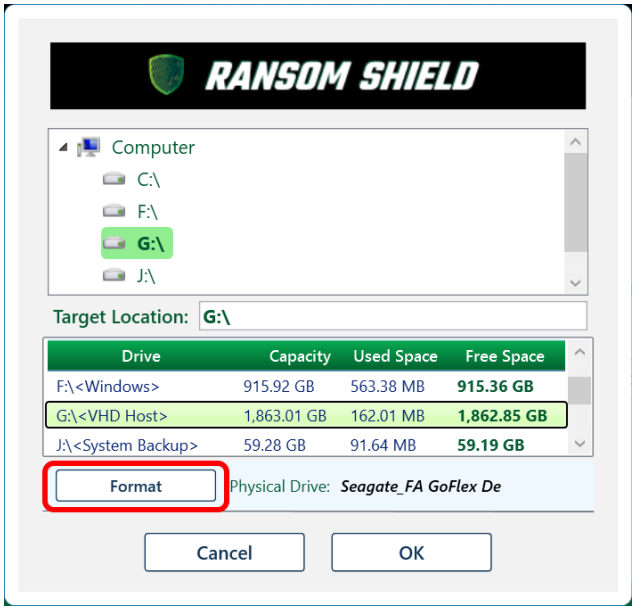


When prompted, click the **Browse** button to select a path to target for your VHD image backup.

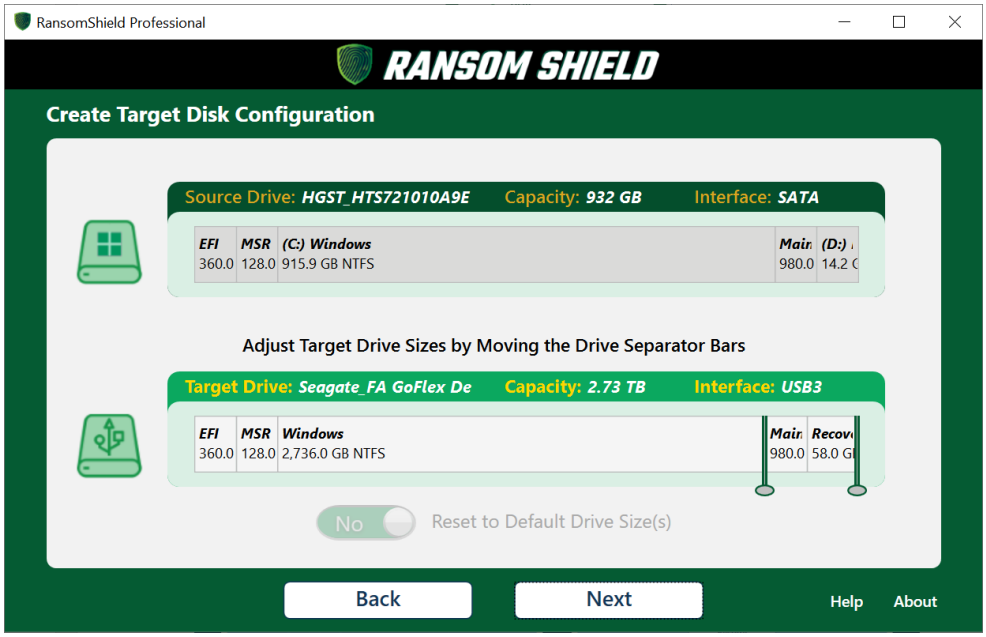


A popup will display allowing you to select the VHD host drive. You can backup your VHDs to the root of the selected drive, or to a subfolder. Backing up to your system drive is not recommended. If the system crashes, you won't be able to boot from your backups!

IMPORTANT: Prior to creating your first VHD backup, click the format button. This will configure the Ransom Shield drive to allow booting from your image backups. You only need to perform this step once. **Formatting the drive will erase everything on the drive.**



Ransom Shield will automatically determine the capacity required to backup your system. You can optionally create the VHD image larger or smaller than the recommended capacity. If you select a larger capacity, you can change partition sizes or create new ones.



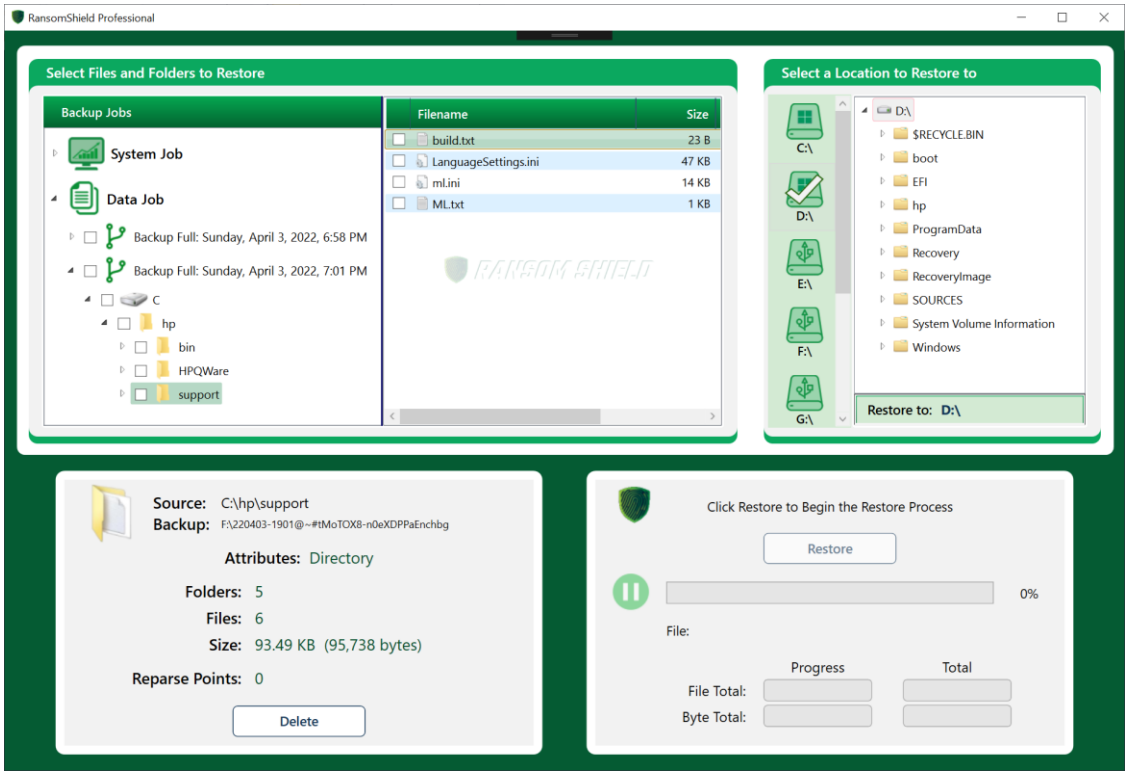
Selecting a smaller capacity will require selecting folders and files to exclude from the backup process. This is documented in the next section.

13- Restoring Folders & Files

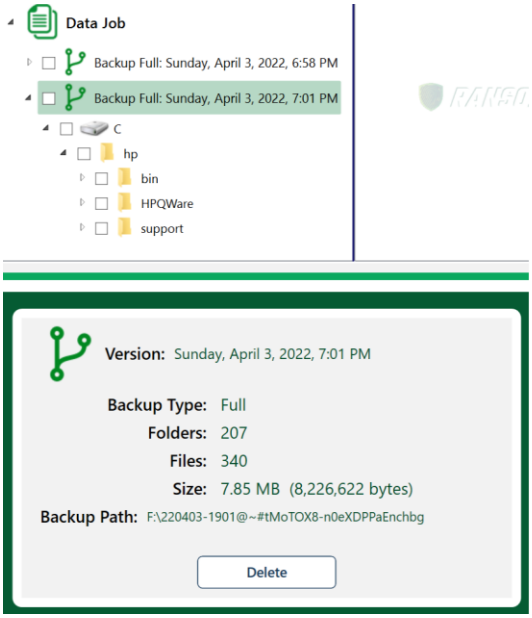
You can access or restore the data from any of your backup jobs by selecting **Access & Restore Data** from the Backup Monitor app in the system tray.

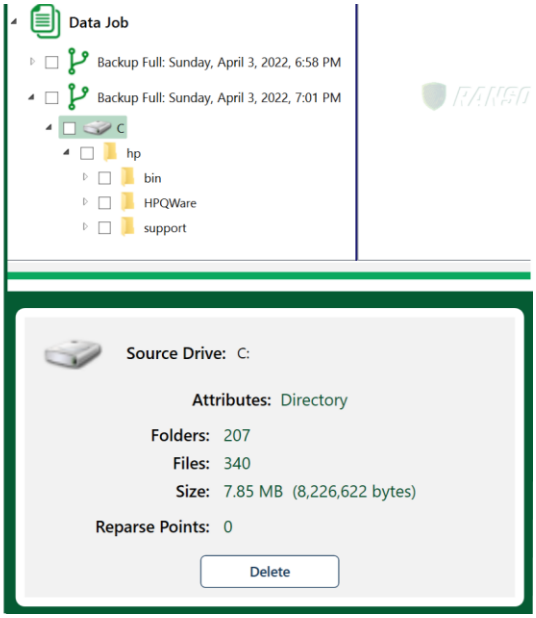
Restore from a Data-Only Backup

Each time you launch a data backup, Ransom Shield will create a version for the backup. Each version is accessible in the restore app, including both full and incremental backups. You can view or restore any file from any backup. Folders can also be restored. Clicking on the data Job node in the upper left will display information about your backup drive, plus allow you to toggle ransomware protection for the drive (if enabled).

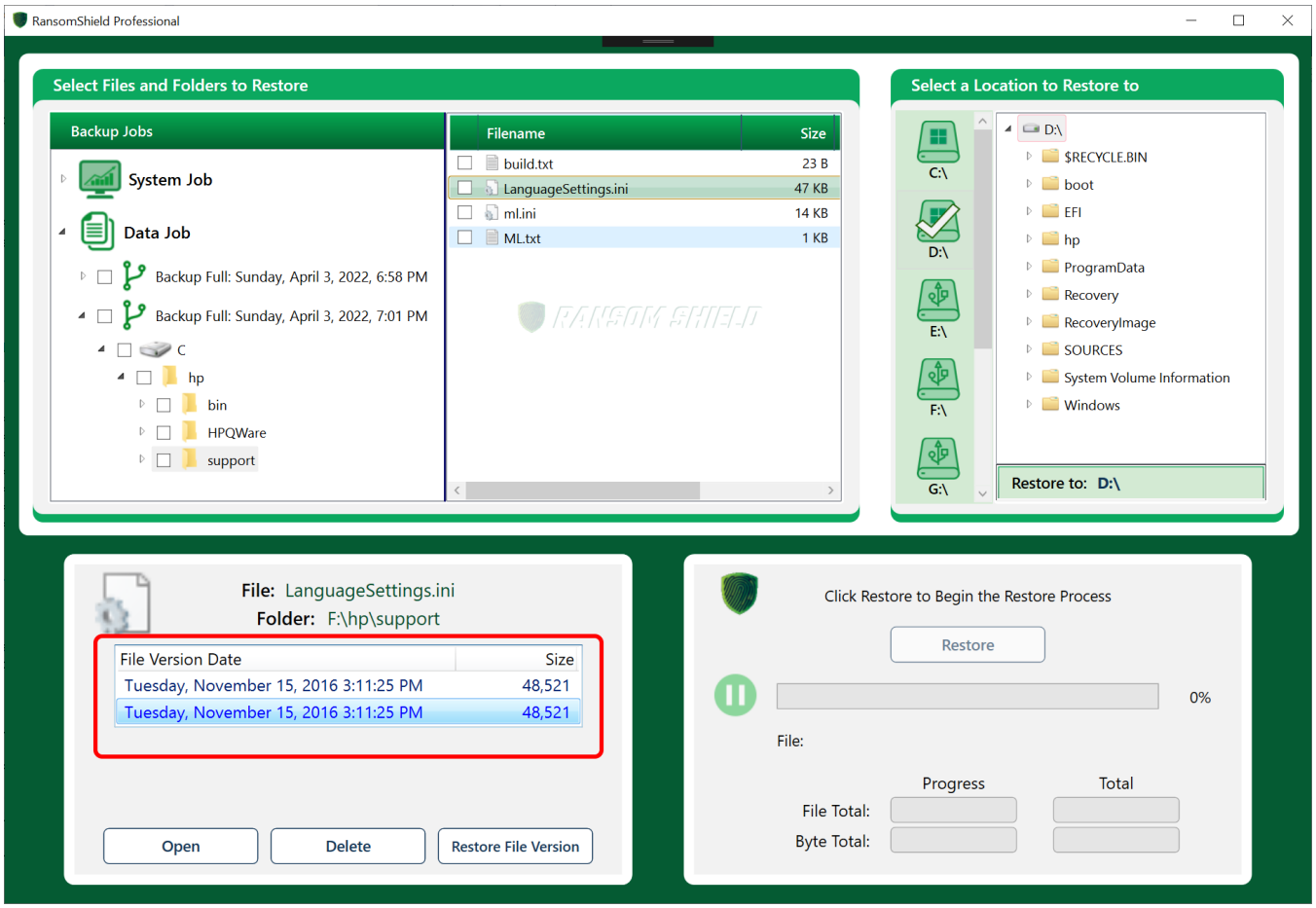


Clicking on the version node displays version info, clicking a drive or folder node displays file totals.





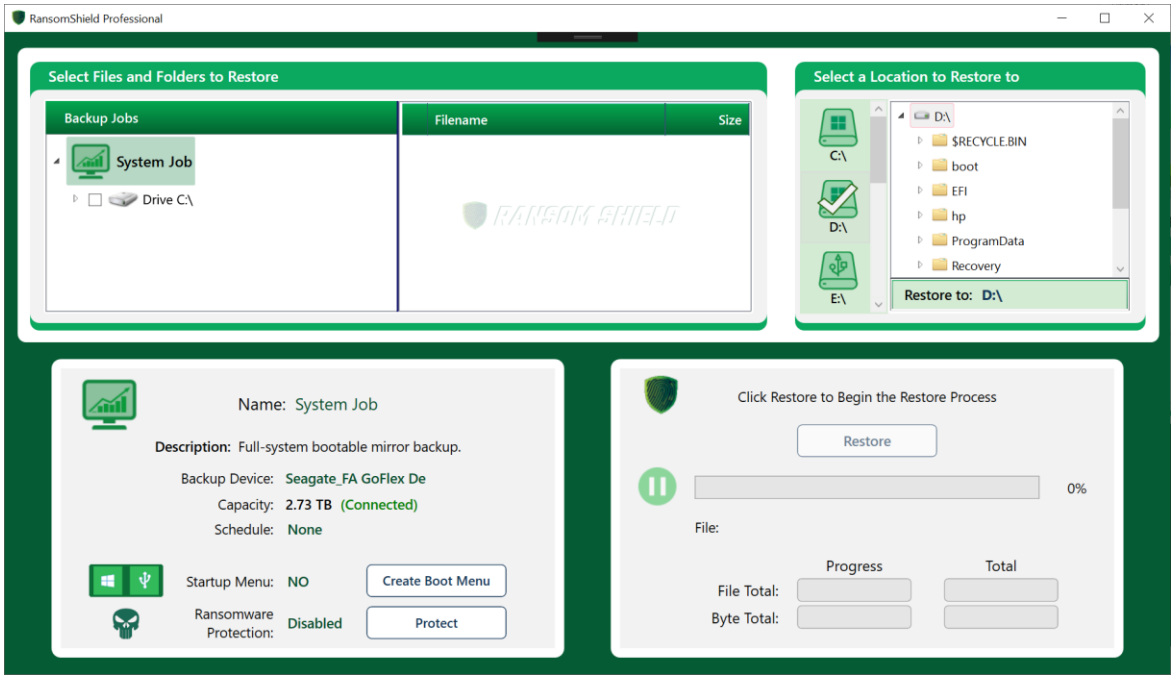
Clicking on a file displays all file versions with their backup dates in the lower left pane. Double-clicking any a version will open the file in the default app for that file type. You can also select an individual file version for restore.



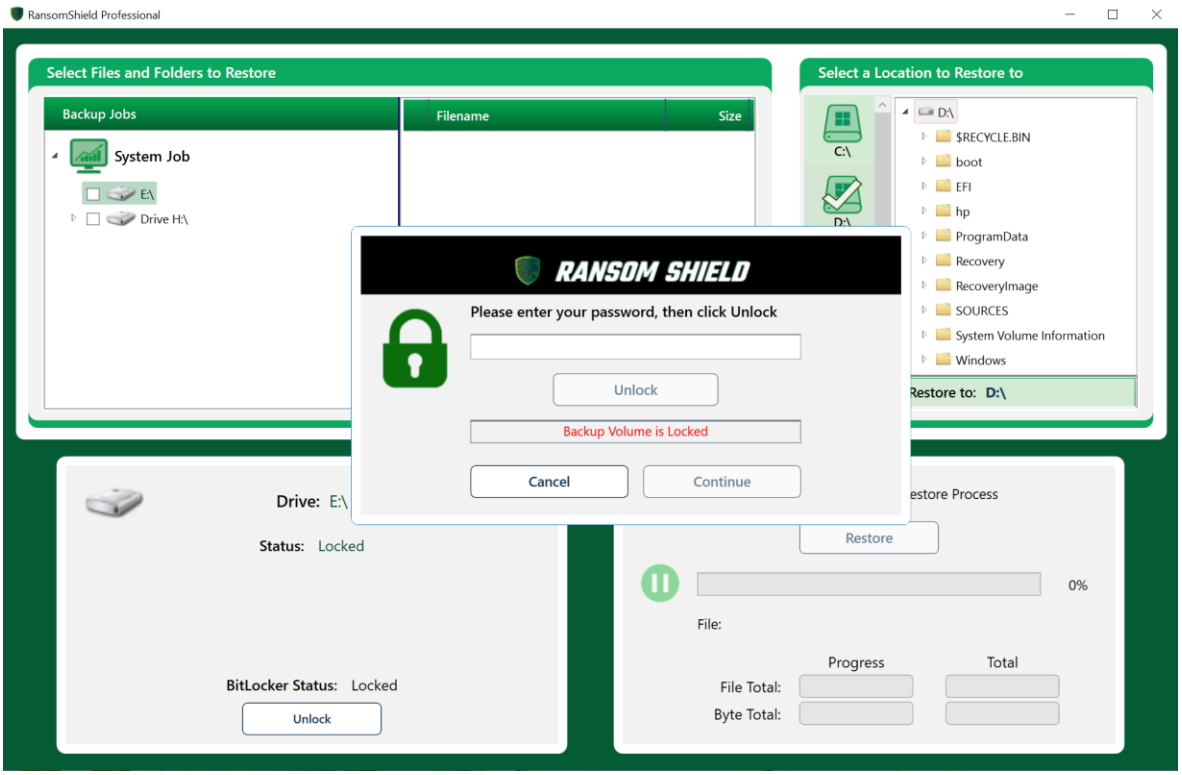
After both source and target are selected, click the **Restore** button to launch the restore process.

Restore Folders & Files from a Full-System Backup

For full-system backups, you have access to all the drive letters, folders, and files on the system. You can control if the startup boot menu is enabled for the backup job. You can also manually turn ransomware protection on and off. As with data backups, folders and files can be opened for viewing, deleted, or selected for restore.

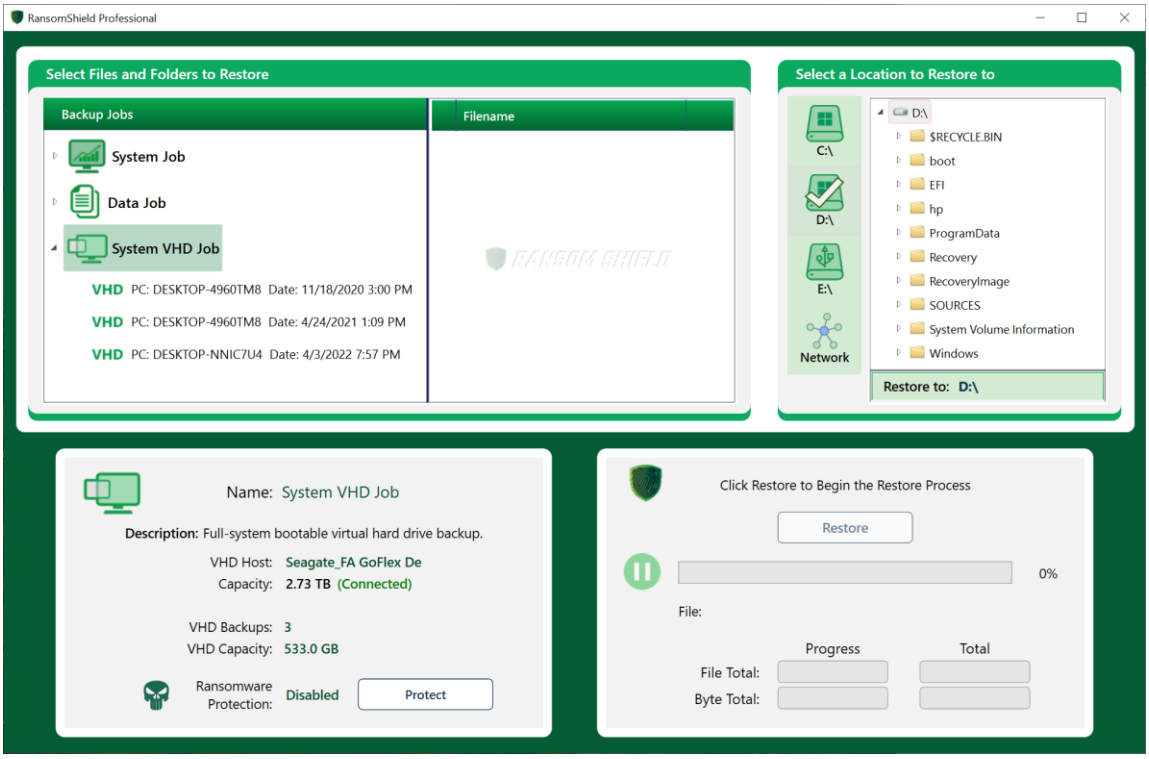


If you're using BitLocker, entering the password is required before you can access the drive.

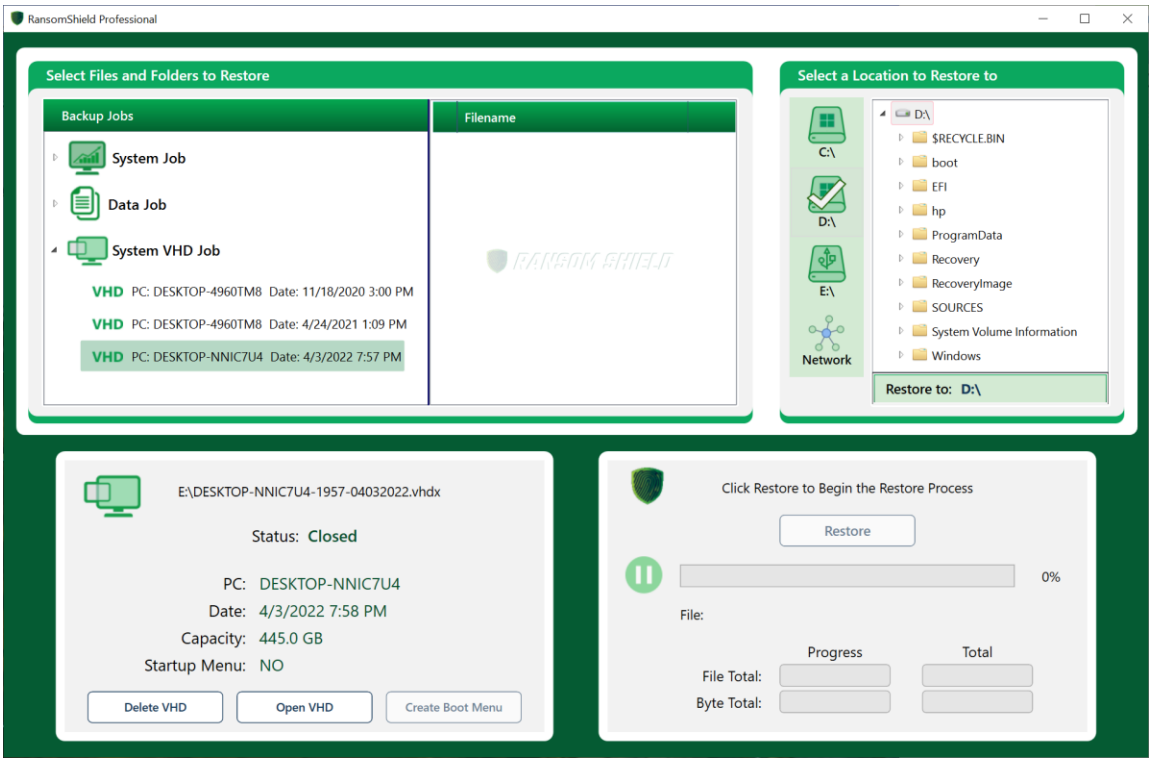


Restore from an Image Backup

The Ransom Shield restore app gives you access to all your images backups. The connection status and capacity of the host drive is displayed, along with the number and capacity of images. This is where you can manually turn ransomware protection on or off for the host drive.



Clicking a VHD displays the status, plus allows opening or deleting that VHD.



Clicking the **Open VHD** button will mount the image and assign drive letters to each volume in the full-system backup. As with data backups, folders and files can be accessed, opened for viewing, or can be selected for restore.

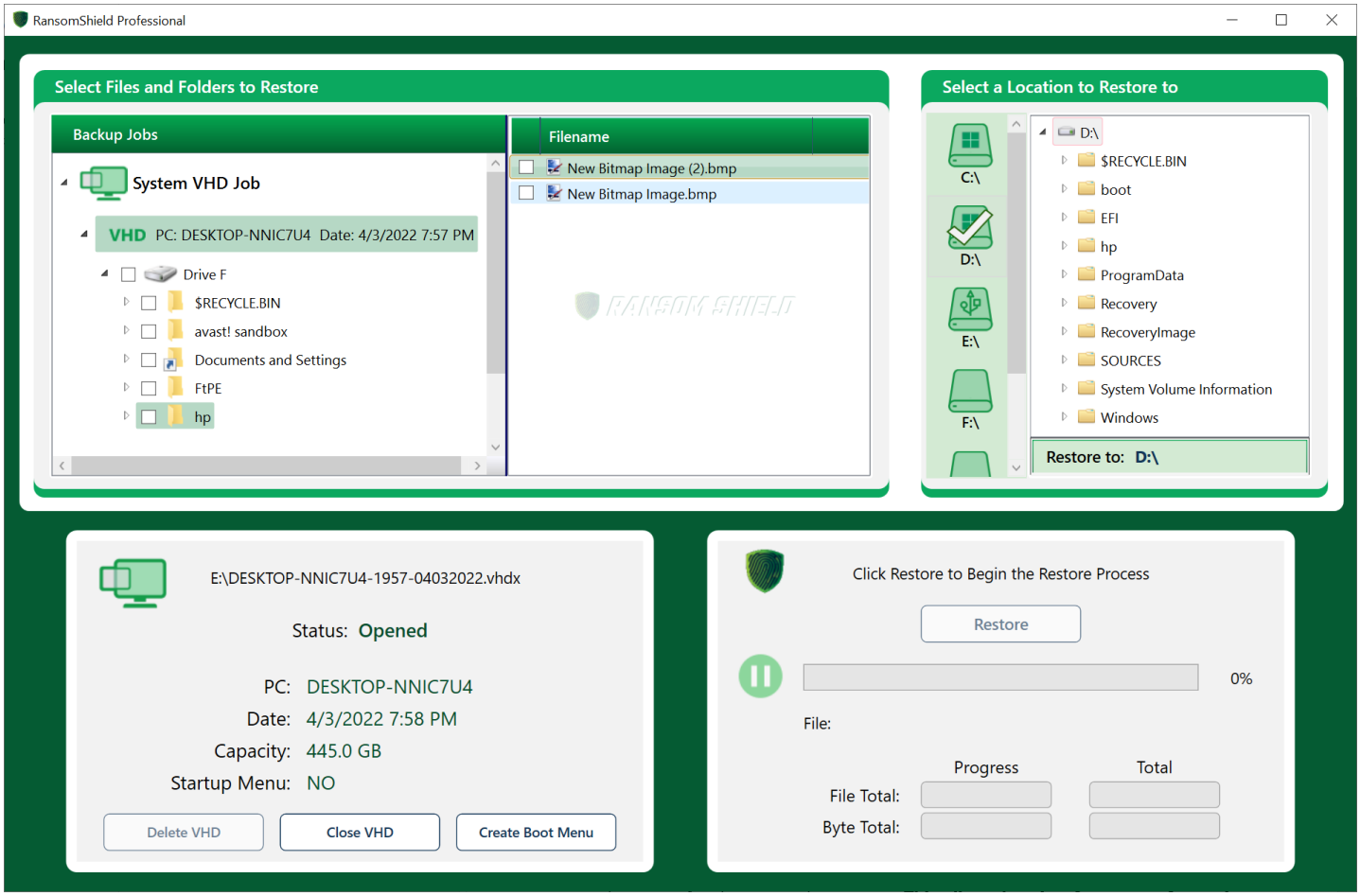


Image backups are basically a snapshot of your entire system at a particular date and time. Multiple images can be opened at the same time, allowing you to compare folders and files from different image backups, and from anywhere in your system.

NOTE: You'll notice there's a star preceding the image name in the display above. This indicates that this image is set in the startup boot menu. Ransom Shield allows you to select any image to set as the target for the startup boot menu. **This allows booting from any of your image backups!** You can run indefinitely from your Ransom Shield drive as all your applications and internet connectivity are available. When booted, you're given the option of restoring your system from the booted image to your internal drive, or to other drives attached to the system. Any changes you made while running from your image are also included in the restore process. This unique feature is exclusive to Ransom Shield!

14- Portable Ransom Shield Drives

Ransom Shield lets you take your personal system with you wherever you go.

When your Ransom Shield drive is first booted on another PC, it will detect all hardware on that PC and install any needed drivers. Unlike ***Windows To Go***, Ransom Shield can backup to any storage device. The Ransom Shield environment is not virtualized, which allows you to perform full-system restores from your booted Ransom Shield drive to either the internal drive or connected USB drives.

Using high speed devices like SSDs will drastically improve performance. Some external SSD drives are capable of booting as quickly as many internal drives.

Frequently Asked Questions

Is Ransom Shield supported on the Windows Home Version?

Ransom Shield can run from Windows Home, Professional, and Enterprise.

Is Ransom Shield supported on both USB 2.0 and 3.x drives?

Yes, but USB 3.0 and above is highly recommended.

Are Windows Updates supported on the booted Ransom Shield Drive?

Yes, if you need to run from your Ransom Shield drive for an extended period of time, Windows updates will occur normally. When you restore back to another drive, the restore process will include any Windows Updates that occurred when running from the Ransom Shield drive.

Can I put my PC to sleep when running from my Ransom Shield Drive?

Yes, sleep is supported. Hibernation is not supported.

What happens if I remove my Ransom Shield Drive while it's running?

If your Ransom Shield drive is removed, your PC will freeze and allow you up to 60 seconds to reconnect the drive. After 60 seconds, the PC will shut down.

Can I see my internal drive when running from my Ransom Shield drive?

Yes, drive letters normally assigned to the backup drive will be assigned to the internal drive.

Does Ransom Shield break my Windows license agreement?

No, Windows allows you to make a single full-system backup of your PC.

15- Mirror Versus Image Backup

Choosing image backups will generally require a larger capacity backup drive. A 4TB drive can contain at least 15 full-system image backups on the average PC. Ransom Shield will optionally delete the oldest if there's no space available when a new backup is launched.

		
Ransom Shield Drive is Bootable	✓	✓
Supports All Windows Versions	✓	✗
BitLocker Full-Disk Encryption	✓	✗
Supports Multiple Bootable Backups	✗	✓
Supports Bootable Backups of Other PCs	✗	✓
Supports Scheduling Full-System Backups	✓	✓
Supports Scheduling Incremental Backups	✓	✗
Drive Can Contain Other Non-Backup Data	✗	✓
Backup Drive Can Replace the Internal Drive	✓	✗

Notes: Image backup is only supported on Windows Professional and Enterprise versions, while mirror backups support the Windows Home version. BitLocker does not support Windows Home. Image backups do not currently support incremental backups. An image host drive can replace your internal drive, but the format is converted to the virtual drive structure supported by VHDs.

16- Troubleshooting

My Ransom Shield Drive Won't Boot

Two Methods for Starting from your Backup Drive

1. **The Startup Boot Menu** You can select to create a startup menu that displays each time you restart your PC To do this, you need to select the boot menu option prior to creating your first full-system backup. The default for this option is ON when creating your first full-system backup.
2. **The BIOS Boot Menu –** All PCs have a hot-key to access BIOS options. By pressing the BIOS hot-key before your system starts, you can select to start from your backup drive. See below for the hot-keys for various PC manufacturers. If you see two items in the BIOS drive list for your backup drive, the UEFI option is usually correct for newer PCs.

Both mirror and VHD backups can start with either method. For VHDs, you can select which VHD you would like to start from.

What should I do if the backup drive won't boot?

1. Try both booting methods. If the drive fails to startup correctly when using the startup boot menu, try again from the BIOS boot menu.

2. Check your BIOS settings to ensure booting from USB drives is not blocked. Windows 7 PCs will often require additional changes to BIOS settings.

3. It's possible that the backup process failed. Perform another full-system backup, then try again to boot the backup drive.

BIOS Settings

When starting some PCs, it may be necessary to press CTL-ALT-DEL if the boot menu does not initially display your backup drive.

A small percentage of PCs may require a BIOS setting change to enable USB boot, especially on Windows 7. These BIOS changes could include:

BIOS Values

Post Settings:	**Thorough**
Enabled External Device Boot:	**Enabled**
Quick Boot:	**Disabled**
Diagnostic Mode:	**Enabled**

Computer Manufacturer	Type	Model	Boot Menu Key	BIOS Key
ACER			Esc, F12, F9	Del, F2
ACER	netbook	AspireOne, Aspire Timeline	F12	F2
ACER	netbook	Aspire v3, v5, v7	F12	F2
APPLE		After 2006	Option	
ASUS	desktop		F8	F9
ASUS	laptop		Esc	F9
ASUS	laptop	R503C	F8	DEL
ASUS	netbook	Eee PC 1025c	Esc	F2
COMPAQ		Presario	Esc, F9	F10
DELL	desktop	Dimension, Inspiron, Latitude	F12	F2
DELL	desktop	Inspiron One 2020, 2305, 2320, 2330 All-In-One	F12	F2
DELL	laptop	Inspiron	F12	F2
DELL	laptop	Precision	F12	F12
EMACHINES			F12	Tab, Del
GATEWAY			F11, Esc, F10	F2, Del
HP	generic		Esc, F9	Esc, F10, F1
HP	desktop	Media Center	Esc	F10
HP	desktop	Pavilion 23 All In One	Esc	F10
HP	desktop	Pavilion g6 and g7	Esc	F10
HP	desktop	Pavilion HPE PC, h8-1287c	Esc	Esc F10
HP	desktop	Pavilion PC, p6 2317c	Esc	Esc F10
HP	desktop	Pavilion PC, p7 1297cb	Esc	Esc F10
HP	desktop	TouchSmart 520 PC	Esc	Esc F10
HP	laptop	2000	Esc	Esc
HP	notebook	Pavilion	Esc	F10
HP	notebook	ENVY dv6 and dv7 PC	Esc	Esc
INTEL			F10	
LENOVO	desktop		F12, F8, F10	F1, F2
LENOVO	laptop		F12	F1, F2
LENOVO	laptop	IdeaPad P500	F12 or Fn + F11	F2
NEC			F5	F2
PACKARD BELL			F8	F1, Del
SAMSUNG			F12, Esc	
SAMSUNG	netbook	NC10	Esc	F2
SAMSUNG	ultrabook	Series 5 Ultra and Series 7 Chronos	Esc	F2
SHARP				F2
SONY		VAIO, PCG, VGN	F11	F1, F2, F3
SONY		VGN Esc	F10	F2
TOSHIBA		Protege, Satellite, Tecra	F12	F1, Esc
TOSHIBA		Equium F12	F12	F12

My Virus Protection is Interfering with Ransom Shield

Your virus protection can block or interfere with the operation of the Ransom Shield software. This can result in slow backups or the software crashing. It's a good idea to create antivirus exclusions for Ransom Shield even if you don't have these issues. Ransom Shield will automatically create an exclusion for Windows Defender. The following folders need to be excluded for Ransom Shield.

For 32-bit systems:
C:\Program Files\Ransom Shield\Ransom Shield

For 64-bit systems:
C:\Program Files\ Ransom Shield\Ransom Shield\x64

If your unsure if you have a 32 or 64-bit system, exclude both. Some antivirus may require you to exclude individual processes. If so, these files should be excluded in the folders above:

BackupServer.exe
BackupSettings.exe
BackupMonitor.exe
ScheduleLauncher.exe
PasswordPrompt.exe (if you are using BitLocker)

Here are links to popular antivirus websites with instructions on creating exclusions:

Bitdefender
https://www.bitdefender.com/consumer/support/answer/13427/

NortonLifeLock
https://support.norton.com/sp/en/us/home/current/solutions/v36687854

PCMatic
https://forums.pcmatic.com/topic/203530-manually-adding-a-programservice-to-whitelist/

Avast
https://support.avast.com/en-us/article/Antivirus-scan-exclusions/

AVG
https://support.avg.com/answers?id=906b00000008tbFAAQ

Kasperski
https://support.kaspersky.com/11481#block2

Total AV
https://support.totalav.com/en/kb/article/148/how-can-i-exclude-certain-files-or-folder-paths-from-scanning

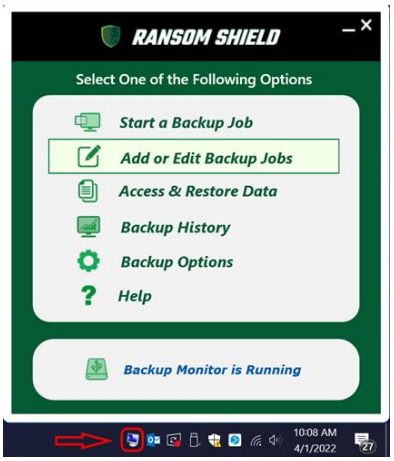
McAfee
https://service.mcafee.com/webcenter/portal/cp/home/articleview?locale=en-US&articleId=TS102056

For other antivirus solutions, see here:
https://www.scrapersnbots.com/software/troubleshooting/how-to-whitelist-software-in-antivirus-anti-virus-deletes-files-false-flagging.php

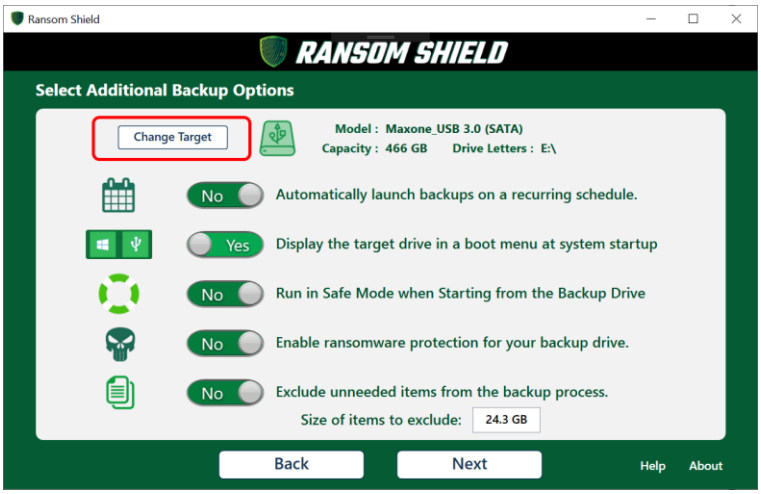
Can I Change the Target Drive for a Full-System Backup?

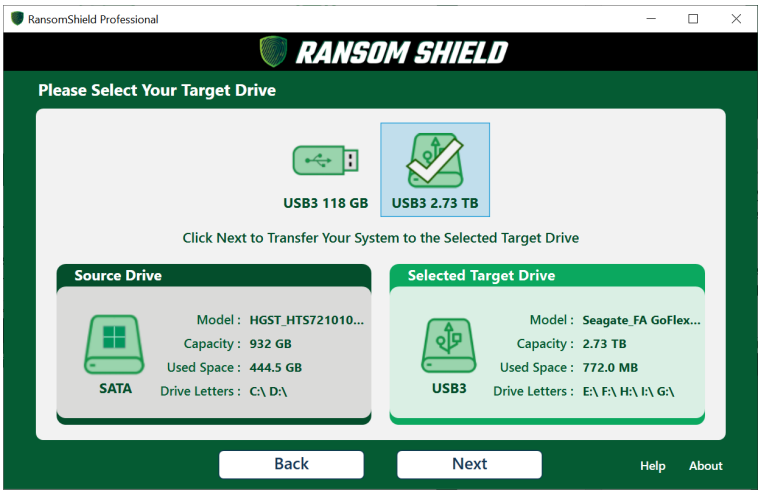
Yes, you can change the target drive with the following steps:

1) Right-click the Ransom Shield icon in the system tray
2) Select **Add or Edit Backup Jobs**



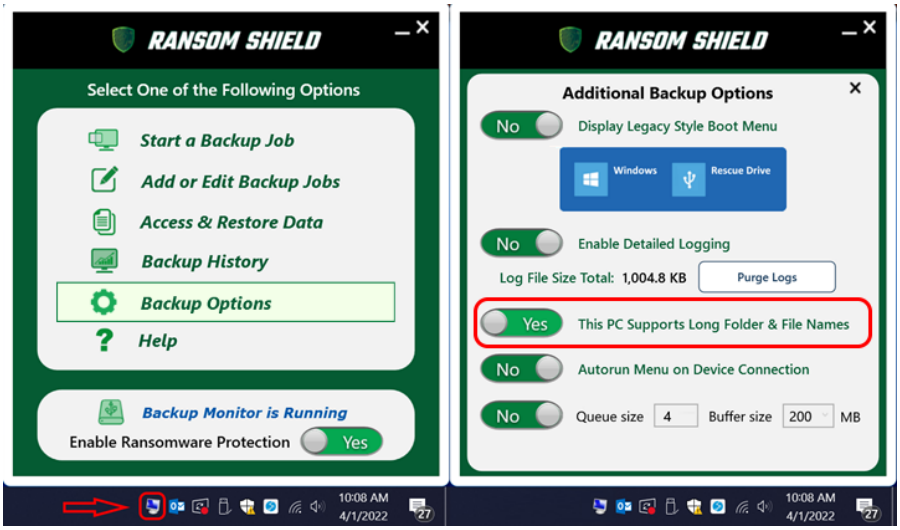
6) Click the **Edit Job** button
7) Click the **Change Target** button





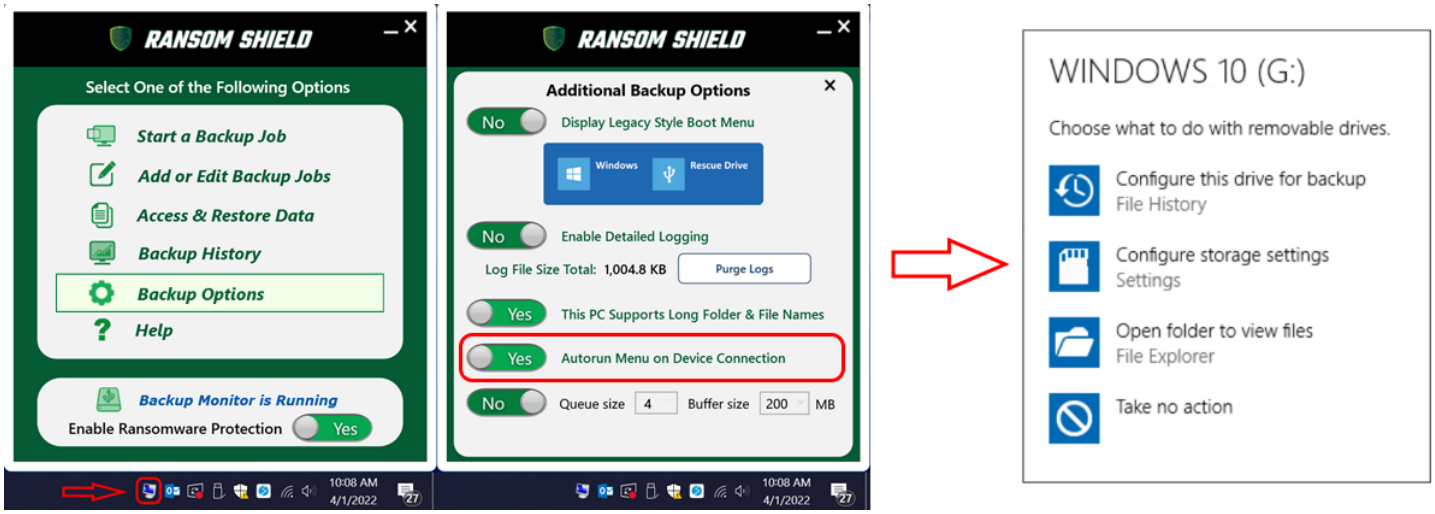
Some Applications Won't Run Properly when I'm Running from the Ransom Shield Drive

Some applications like MS Office have numerous long folder and file names associated with their installation paths. Your PC may have support for these paths disabled to enable support for older legacy software. Microsoft ensures these long paths work correctly when installed on your system, but backing them up to your Ransom Shield drive can cause problems. To resolve this issue, you can verify if long name support is enabled for your system in Ransom Shield. If turned off, applications like Office may not function properly on the booted Ransom Shield drive.



How Do I Disable Windows AutoPlay When Connecting the Ransom Shield Drive?

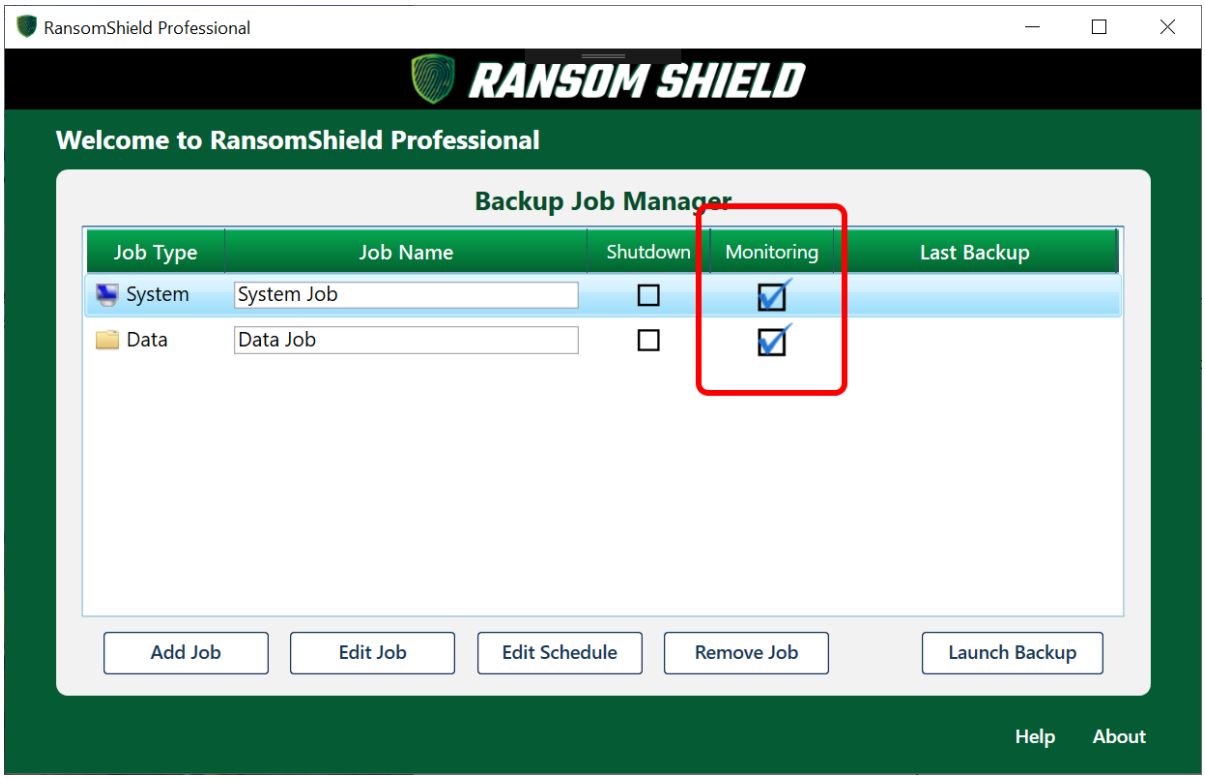
You can turn the Windows autoplay menu for your Ransom Shield drive on or off with the following setting in the Ransom Shield software



My PC is Running Slow

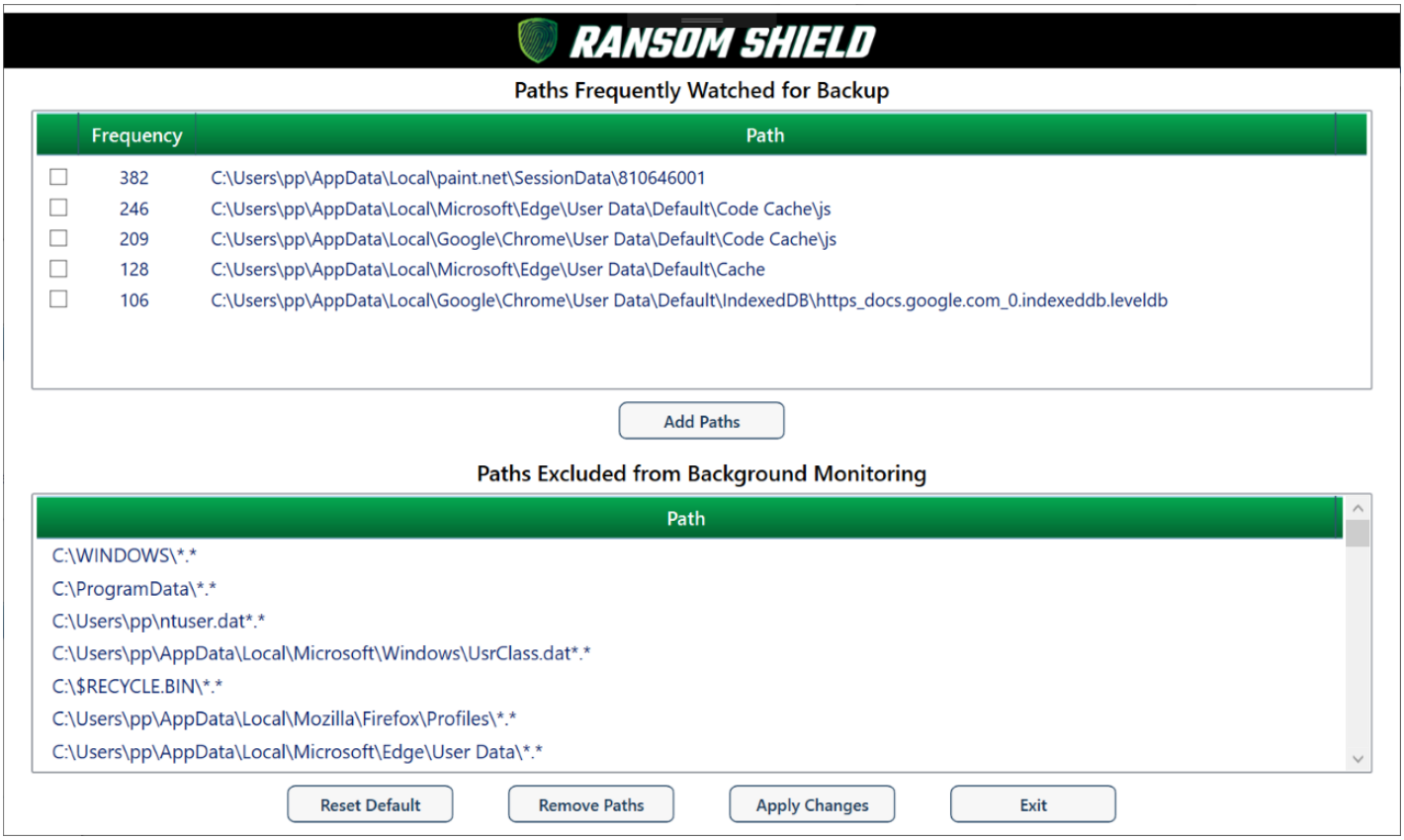
When you create a full-system mirror backup, the Ransom Shield backup monitor will run continuously. This allows the software to track any changed files in the background. Since it's monitoring your entire system including the OS, this can become quite a busy task. This is complicated when antivirus or other applications continuously change log or temporary files in the background. Ransom Shield has identified and excluded many of these paths by default. It's possible that some of your applications are making these types of changes, which in turn causes your system to slowdown during the monitoring process. There are two methods to resolve this issue.

1. **Disable Backup Monitoring –** Choosing this option will cause Ransom Shield to not track file changes for a backup job. This results in losing the ability to perform incremental backups for that job. Many users may not need this option if they always perform full-system or full-data backups.



2. **Add Offending Paths to the Watcher Exclusion List –** For advanced users, Ransom Shield maintains a list of paths excluded from monitoring for incremental backups. This applies only to full-system backups. Paths to frequently changing folders such as browser temp and system cache folders are automatically excluded from incremental backups. You can determine which files and folders are causing issues by launching the following application:

   C:\Program Files\Ransom Shield\Ransom Shield\x64\WatcherExcluder.exe



The items in the top panel are items that are frequently changing and being flagged for backup on your system. The items in the lower panel have been previously identified for exclusion from the background watcher and from your incremental backups. You can see the frequency of changed items in the upper panel, so you can add the worst offending items for exclusion below by clicking the checkbox, then clicking **Add Paths**. Make sure these are items that you do not want included during incremental backups. Also keep in mind that these items are not excluded during your full-system backups.

You can remove paths from the excluded list by selecting them, then clicking the **Remove Paths** button. Clicking the **Reset Default** button will reset to the original defaults created during the Ransom Shield installation.

NOTE: The preceding does not apply to image backups since incremental backups are not supported with image backups.

NOTE: If you find this process to be too complicated, please don't hesitate to contact Ransom Shield support. We will guide you through making the needed changes. Suffering from a slowdown to your system is unacceptable, so we're here to help! 😊

https://rescue-drive.com/contact/