StorageCraft

Best practices for securing backups and mitigating ransomware attacks

A StorageCraft guide

StorageCraft

StorageCraft

Contents

Introduction

Backups and data protection are a must for today's digital businesses. The challenge for many businesses is not only ensuring data is protected, but that it is also secured against inadvertent deletion or malicious attacks.

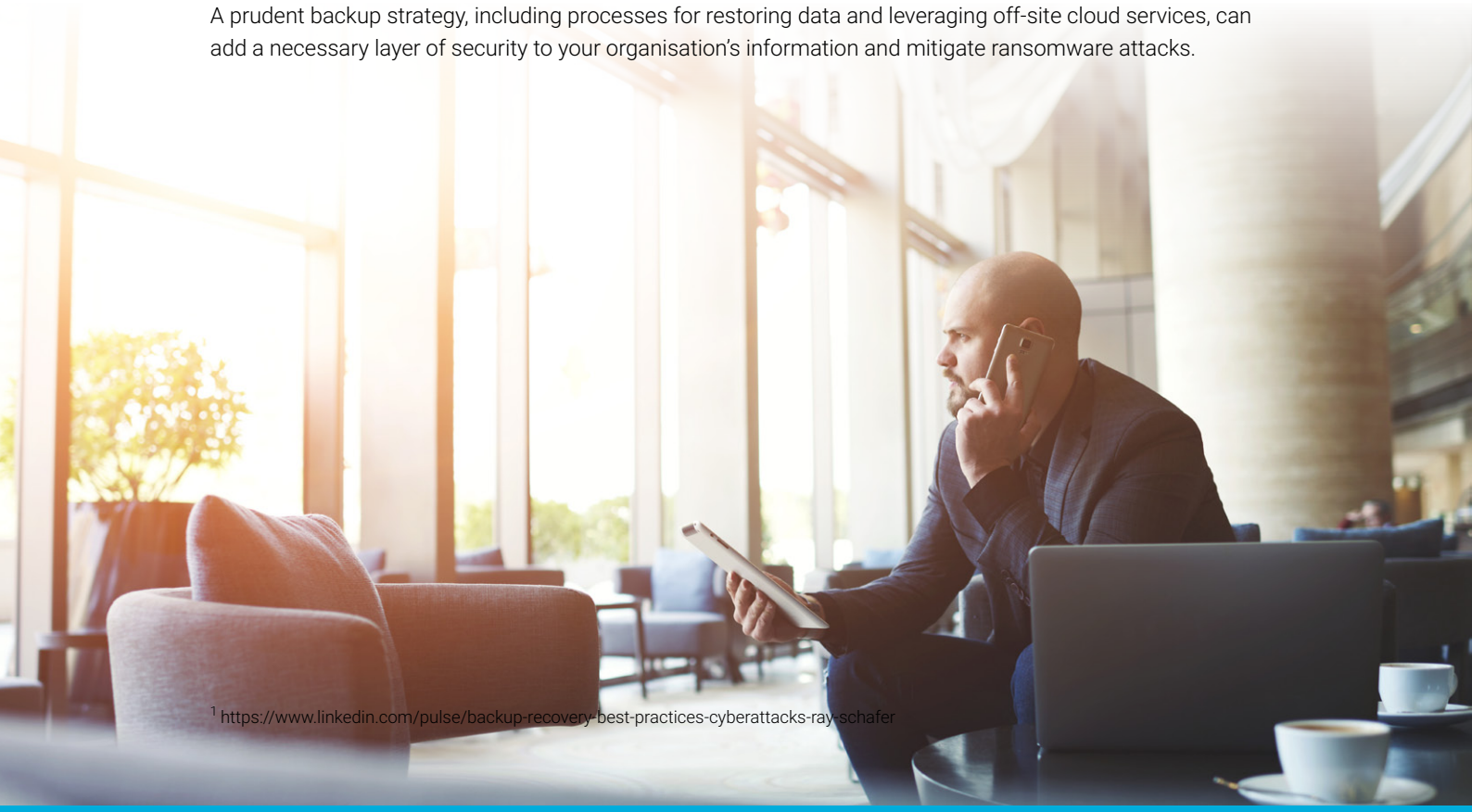
A new wave of malicious code which infects computers and encrypts files is sweeping the Internet and finding its way into company networks. This "ransomware" can interrupt business operations and be very costly if an organisation pays to unlock the data or fails to perform regular backups resulting in data loss.

According to analyst firm Gartner, some 60 per cent of digital businesses will suffer at least one major service failure by 2020 due to the inability of IT security teams to manage digital risk[1]. The company recommends using a structured approach to ensure greater success in recovering from a cyberattack and to avoid a slow, ineffective or failed recovery.

This report is a practical guide to securing StorageCraft backups to ensure your organisation can recover its important information in the event of a problem. The recommendations contained in this guide can be applied to Windows Server across the following environments:

- On-premises customer servers
- Partner-hosted environments
- Windows servers in the cloud

A prudent backup strategy, including processes for restoring data and leveraging off-site cloud services, can add a necessary layer of security to your organisation's information and mitigate ransomware attacks.



[1] https://www.linkedin.com/pulse/backup-recovery-best-practices-cyberattacks-ray-schafer

Communicate the need for secure data protection

As businesses digitize more processes the need for data security and protection has increased accordingly. Data can be at risk due to system and software failures, and too often human error is a factor.

Good communication of the importance of secure information protection is imperative for the success of a data backup program. And with ransomware on the rise, it is very important to educate staff on how end-user actions can result in malicious code execution.

Start your secure data protection journey by educating both technical and line-of-business users why it is important for the continuous running of the business. Communicate the need for backups and the need to secure the backups so they are not compromised and the data can be restored.

Figure 1: Start by communicating why backups and security are important to staff.

The business need

Educate staff on the importance of backups and data protection. Relate the importance of data backups to people's day-to-day roles. If the data is not available then their work is likely to be impacted.

Backup security

Backups are only useful if the data in them is secure and not corrupted. Additional measures must be taken to secure backed up data.

Data location

Backups can be performed on direct attached devices, local business networks or with Internet cloud services. Educate on the need for data across different locations to prevent single-site exposure.

Ransomware attacks

Explain to motives for ransomware and how these attacks are proliferated. User actions on email and the Web are still a contributing factor to ransomware effectiveness.

Hold training sessions for staff so they are aware of how ransomware works (including phishing attacks) and what measures are being put in place to prevent data loss.

Encrypt backups before local or offsite storage

Encryption is a method of scrambling data so it can only be read after applying a matching password or decryption key.

Ransomware uses encryption to prevent the owner of the data from reading it without a paid-for way to decipher it. To ensure data cannot be read or tampered with it should be encrypted during the backup process. By configuring encryption on your ShadowProtect SPX backup jobs (or policies) you will prevent malware from mounting or accessing files inside the backup images.

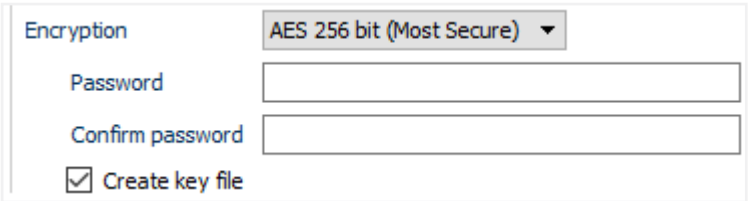
When a backup image is encrypted it can be stored locally (on another server on the network) and then a copy can be replicated to a DR site, cloud or managed service provider data centre. By encrypting the backups before they are transferred to another server you will prevent the data from being "eavesdropped" while in transit.

The ShadowProtect SPX backup schedule and policy defaults to AES 256-bit encryption, and you should specify a strong alphanumeric password.

Encrypted data must also be secured

Encryption is imperative for secure backups, but IT and business staff must be aware any file, even an encrypted backup image, must itself be managed to prevent destruction or malicious corruption. Encrypted backup images do not prevent the image files from deletion, further malicious infection or encryption. This is why additional measures need to be taken secure the end-to-end backup process, as detailed in this guide.

Figure 2: Choose a strong password when setting up SPX backup encryption.



Protect local network shares

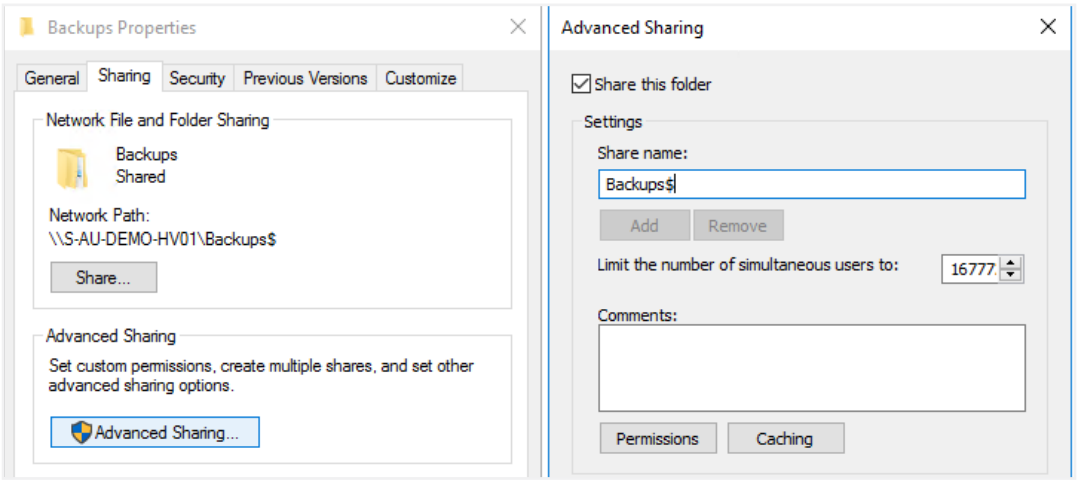
Clients and servers on a local area network (LAN) often have shared folders to facilitate document and general file sharing. If these network “shares” are not protected, ransomware or other malicious code can use them to proliferate through to multiple clients and servers on the LAN.

ShadowProtect SPX performs backups over a local network share which has risks, so partners need to be aware of this and help customers secure them so their backups are not at risk.

To prevent malicious software from finding the backup share it is good practice to isolate backup repositories on the network and only connect to them securely. Never map a network drive (or create a shortcut) to the backup share from any computer on the network.

The "$" appended to the end of the share name means it is a hidden share. Windows will not list such shares among those it defines in typical queries by remote clients to obtain the list of shares. An end-user or application needs to know the name of a hidden share in order to access it as they are not advertised on the network.

Figure 3: Appending a "$" to a share name will keep the share hidden scans.



This setting can be found in “Advanced Sharing” within “Backup Properties”.

Restrict shared folder access

In addition to hiding the share name, enable access-based enumeration on the share where possible. This displays only the files and folders that a user has permission to access. If a user, or application, does not have "read" permissions (or equivalent) for a folder, Windows hides the folder from view.

In the case of a backup share, it should be restricted to a specific user account to prevent unwanted access.

First, create a local account (not a domain user) on the system you are backing up to. Choose a complex password and ensure the new user is not an administrator.

> For the screenshots used in this guide a local user has been created called "SPX".

Assign the new account as the only user with "Full Control" access in the "Share Permissions" and remove the "Everyone" group.

The NTFS (Windows file system) security permissions of the shared folder should only contain the following accounts, each with permissions set to "Full Control":

- CREATOR OWNER
- SYSTEM
- Administrators
- The local user account created (as per above)

If there are any other accounts on the directory you should consider removing them. The new account should only be used by SPX for the destination credentials. Never use these credentials to connect to the share across the network and, importantly, never save the network credentials. Restores from backups can be done directly from the SPX Console with the "Job Timeline" or the "Image Chain Browser".

Figure 4: Assign the local user full control to the share.

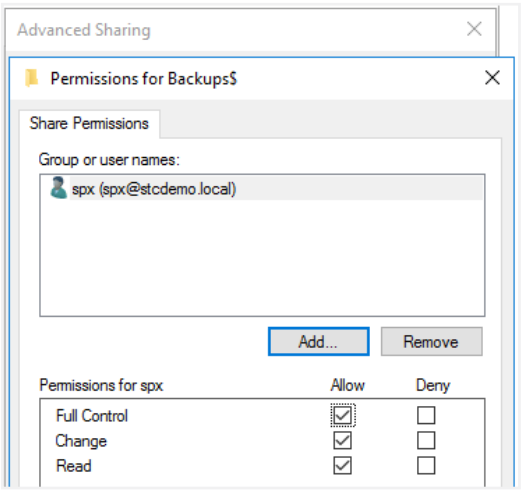
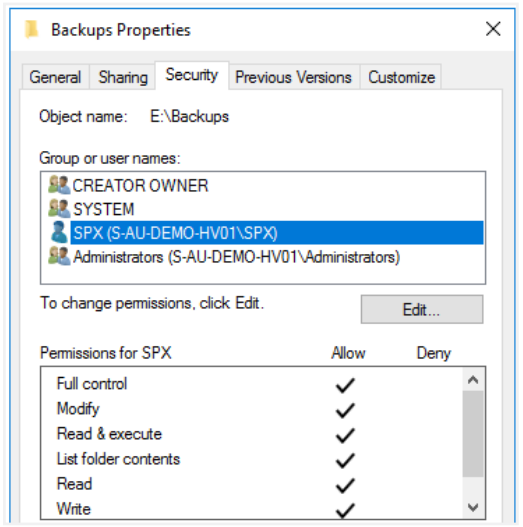


Figure 5: System accounts and their permissions.



Review SMB on Windows and other devices

The Server Message Block (SMB) protocol is the standard way to connect to Windows servers over a LAN. SMB is supported by Windows, Mac OS X and Linux clients to connect to Windows servers. In addition to Windows servers, many NAS appliances use SMB in order to support network shares among Windows clients and servers on the LAN.

SMB is necessary for your backups to be accessible over the network, however, it must be monitored as part of a backup security strategy. There is a known SMB exploit MS17-010[2] affecting most versions of Windows and unpatched machines are at risk. For enhanced security, even Microsoft technical specialists recommend[3] disabling SMB 1.0 altogether.

With SMB 1.0 disabled, additional network measures can be taken to limit the exposure of devices running SMB. The US Computer Emergency Readiness Team (CERT) recommends blocking all versions of SMB at the network boundary[4], including TCP port 445 and NetBIOS (UDP ports 137-138 and TCP port 139).

Backup integrity

StorageCraft ImageManager is an included application with the SPX solution and must be used for managing backups using Continuous Incremental backup schedules. One of the huge benefits of ImageManager is that it performs immediate verification (using MD5 or CRC) on any new backup image, and will, by default, periodically re-verify all images every seven days. This allows for early detection if there is corruption to the image chain. Checking the integrity of a backup is important for a successful restore.

[2] https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
[3] https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/
[4] https://www.us-cert.gov/ncas/current-activity/2017/01/16/SMB-Security-Best-Practices

Use cloud and offsite replication

Another layer of security for backups is obtained by transferring the data to a remote location.

An offsite copy of your backup images is very important to ensure you have a separate isolated copy from local infrastructure. If all the backup data is contained in one location and a disaster, such as a fire or ransomware attack, strikes your organisation could suffer a data loss incident.

Secure the backup chain offsite

ShadowProtect SPX best practice leverages continuous incremental backups which can rely on critical 'shortest path' images in the chain. If certain images are corrupted there is the risk of an unrecoverable situation. Replication to an offsite location is therefore very important.

Replicating a copy of the backups to an offsite location can be easily automated with the StorageCraft ImageManager software, included with ShadowProtect SPX.

ImageManager includes offsite replication technology for a number of protocols including intelligentFTP and Amazon S3. And every image file is verified (MD5 or CRC) to ensure it has not been corrupted before it is replicated offsite. This gives you piece of mind in a worst case scenario that you can still recover.

A lot of replication technology is available to send any file that has changed to a remote location, but this could include a corrupted file so stick with StorageCraft ImageManager.

StorageCraft Cloud Services does not store a second copy of image chain files

StorageCraft Cloud Services is purpose built for disaster recovery, however it is important to understand that it does not store a second copy of the image files. Once replicated, they are converted into unique recovery points in the cloud to facilitate rapid virtualisation. It is best practice to ensure you are also replicating a second copy of your images to another location, including a local drive, network drive, intelligentFTP service or S3-compatible cloud storage.

Another key benefit with ImageManager replication is the ability to significantly reduce bandwidth requirements by leveraging an offsite ImageManager to perform further verification and consolidation processing. Rather than replicating all images, ImageManager can be configured to only send intra-daily, or just the consolidated daily images, using the remote ImageManager to further consolidate weekly and monthly.

Figure 6: Select your offsite target in ImageManager

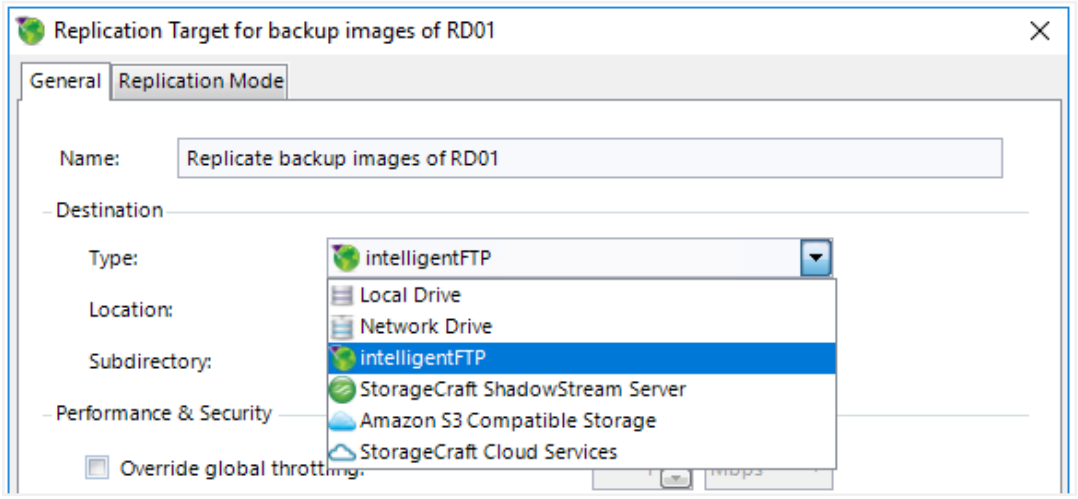
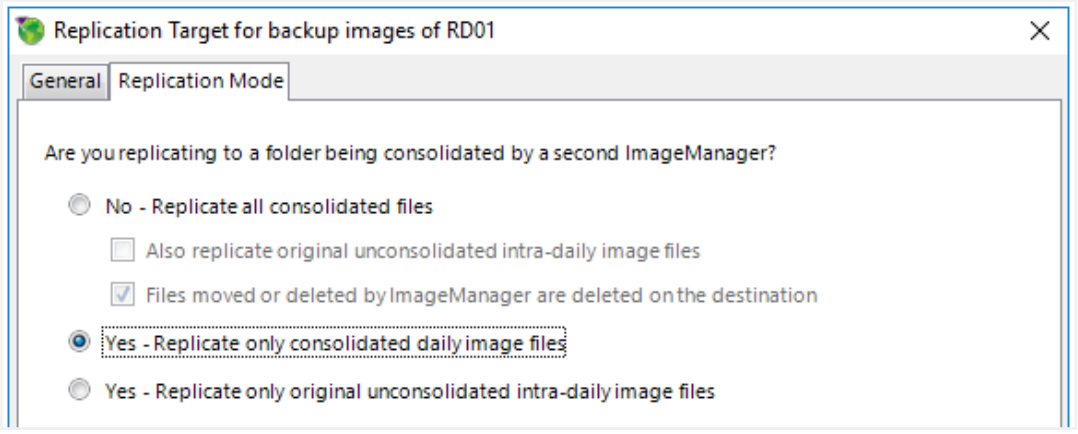


Figure 7: Select the frequency of image file replication.



Further recommendations

ShadowProtect SPX for Windows Server can be secured to remove the exposure to a ransomware or other malware attack.

The steps in this guide should be combined with other best practices for security for the highest level of protection possible. Here are a number of further recommendations partners and customers can take to improve the security of their digital assets.

- **Endpoint protection.** Look for a security product to protect endpoint devices not only against malware and ransomware, and other advanced online threats. Ensure anti-virus and anti-malware solutions are set to automatically update and regular scans are conducted.
- **Patch your systems.** As we have indicated in this guide patching closes known vulnerabilities that ransomware takes advantage of. Ensure all patches for the operating system, software and firmware are up to date, including popular apps like Adobe Flash, Java, and Web browsers. This precaution can be made easier through a centralized patch management system.
- **Implement software restrictions.** Implement software restrictions or other controls to prevent the execution of programs in common ransomware locations. These include temporary folders supporting popular Internet browsers, or compression and decompression programs, such as those located in the AppData/LocalAppData folder on Windows. The Windows Group or Local Policy Editor can be used to create Software Restriction Policies that block executables from running when they are located in specific paths.
- **Review administrative access.** Configure access controls with least privilege in mind. If a user only needs to read specific files, they should not have write access to those files, directories or shares. No users should be assigned administrative access unless absolutely needed. Those with a need for administrator accounts should only use them when necessary and should operate with standard user accounts at all other times.
- **Test your recovery plan.** Testing your Disaster Recovery plan is a must for security. Do not let a disaster be your first test. A good DR plan will be easy to test (and test often). This is the only way that you can validate that your recovery time objectives can be met. The ShadowProtect solution includes StorageCraft VirtualBoot™ technology for easy DR and testing. The included ImageManager software can also be configured with Advanced Verification to automatically boot via integrated VirtualBoot, providing an email with attached screenshot of the System Login Screen. Partners might be selling DRaaS to a customer and experience a change in the environment. Testing is also process of training someone to become familiar with recovery so should something go wrong, people in the business know what to do.

StorageCraft

StorageCraft

About StorageCraft

The StorageCraft family of companies, founded in 2003, provides award-winning backup, disaster recovery, system migration and data protection solutions for servers, desktops and laptops in addition to powerful data analytics, and scale-out storage by Exablox. StorageCraft delivers software products that reduce downtime, improve security and stability for systems and data, and lower the total cost of ownership.

For more information, visit
www.storagecraft.com/au