Acronis

WHITEPAPER

Acronis Backup scan for malware

Non-disruptive performance with no trade-offs to security or usability

Backup and anti-malware are two essential parts of a modern endpoint security posture. While scanning for malware is usually performed before doing a backup, there are many cases when malware makes its way into backup images. This can happen because of the limited detection capabilities of an average anti-malware solution or because a backup was done before the anti-malware scan.

Full scans of large archives (including backups) to detect malware require considerable time and computational resources. As a result, they're often not an efficient use of time and resources. That said, scanning archives becomes especially critical if the archives are not stored locally, but in cloud storage, because the speed of access to an archive in the cloud may be significantly slower than accessing a local storage device (depending on the speed of the network or communication channel being used, and/or how heavily-loaded the channel is). Additionally, if any viruses and/or malicious files are found in the archive, the archive is considered damaged or infected, and may not be suitable for use in a system recovery or for file and data extraction.

Historically, to avoid restoring data that's infected, archives were periodically scanned with anti-virus scanners during storage, when new slices are added to the archive, and/or before restoring the data. However, today there is no solution that allows for custom archive scans in terms of timing or scope. Instead, solutions are forced to scan the entire archive. Furthermore, damaged or infected data in archives cannot be repaired.

Acronis technology solves all of these issues

A typical systems administrator has to deal with a lot of machines and their corresponding backups. As part of that work, they need to deal with all of the issues mentioned above and be prepared for other challenges. For example, backed up system drives aren't the only components susceptible to malware. A device's OS and third-party apps can also become gateways of infection.

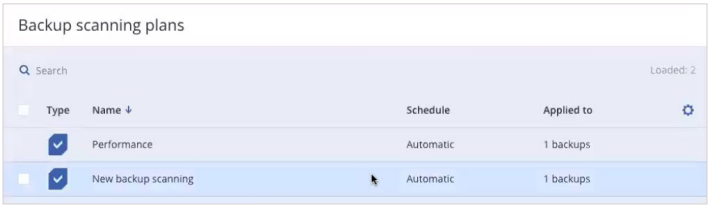
Patching machines and applying the latest anti-malware definitions allows sysadmins to restore an OS image that's ready to withstand a reoccurring infection. To scan backups for malware effectively and properly in a centralized location is another necessary step to ensure safe restores and safe data storage. This is what Acronis Cyber Protect provides.

Through Acronis Cyber Protect, users can scan full disk backups at a centralized location (Acronis Cloud or on-premises server with the ability to expand support for Amazon, Google, Microsoft, or any other popular cloud storage environment in the future) to find potential vulnerabilities and malware infections, thus ensuring a malware-free backup for a malware-free restore, should it become necessary.

Acronis engineers made it possible to inspect not only one big backup but also archived slices for malware. We can mount the first slice of a plurality of slices in a backup archive to a disk, wherein the first slice is an image of user data for the first time. Acronis technology can detect a modified block of the mounted slice, identify files in the mounted first slice that correspond to the detected modified block, and scan specific files for viruses and other malicious software. This approach also allows Acronis to generate a cured slice that comprises the user data of the mounted first slice without the inclusion of malicious files. By scanning in centralized locations, Acronis Cyber Protect allows users to:

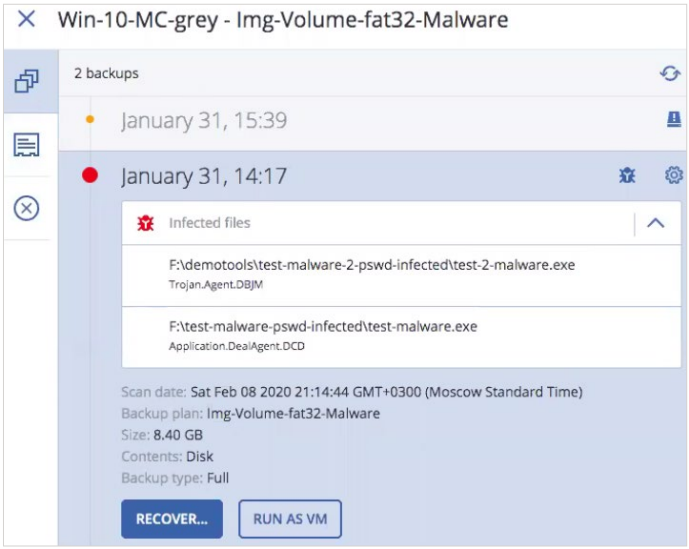
- **Reduce loads on client endpoints**
- **Restore only clean data**
- **Increase the potential of rootkit and bootkit detections (which are not easily detected during the first on-access or on-demand scans)**

That means admins can perform a regular backup scan and each of their clients' backup increments can be scanned for malware in a centralized location. For the first release of Acronis Cyber Protect only Acronis Cloud storage is supported as a centralized location. In future iterations, support will expand to Amazon, Google, Microsoft, and other popular cloud storage environments.



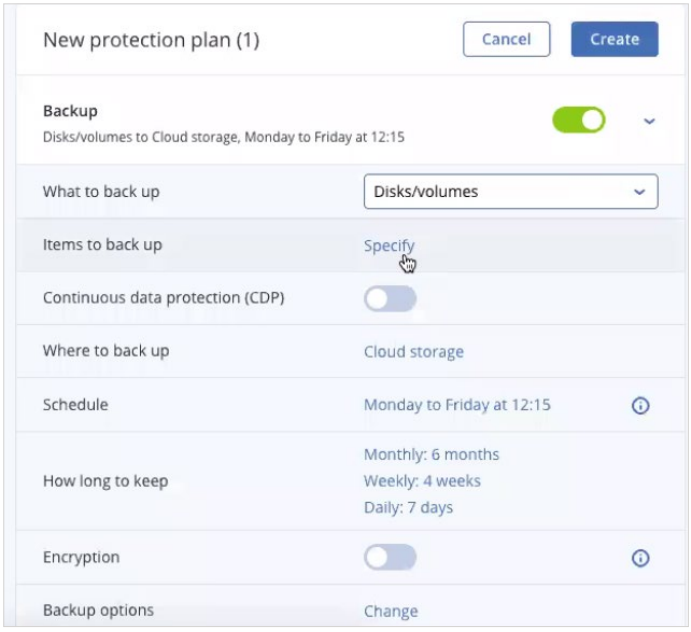
This done, an admin not only has points of recovery but indicated "safe recovery points" where no malware was detected.

An admin can use the Acronis Cyber Protect management console to see in detail what infected files were found and when they appeared. From there they can eliminate the malware from backup slices and restore a clean copy of their data. All backup scans performed through Acronis Cyber Protect use the latest malware definitions, so even if unknown malware wasn't detected initially, it will be identified during the next full backup scan.



Currently, Acronis technology supports full disk or volume backups with incremental options but not file backups.

While other products can only mount and scan a whole image, Acronis offers flexibility and efficiency by quickly scanning new slices after a scan of the initial slice. That means it scans several times faster than the competition (actual results depend on the size of the volume image and competitor scan engine performance). Acronis technology uses advances of its Archive 3 storage format API and NTFS file system capabilities, another reason why operations deliver very high performance.



Backups can also be scanned locally if needed. For example, when a network share is used for backup volume storage in a small company. File storage can be covered without an Acronis Cyber Protect agent. In this case, it can be scanned from any machine in the network that has access to the storage and has an Acronis Cyber Protect agent installed.

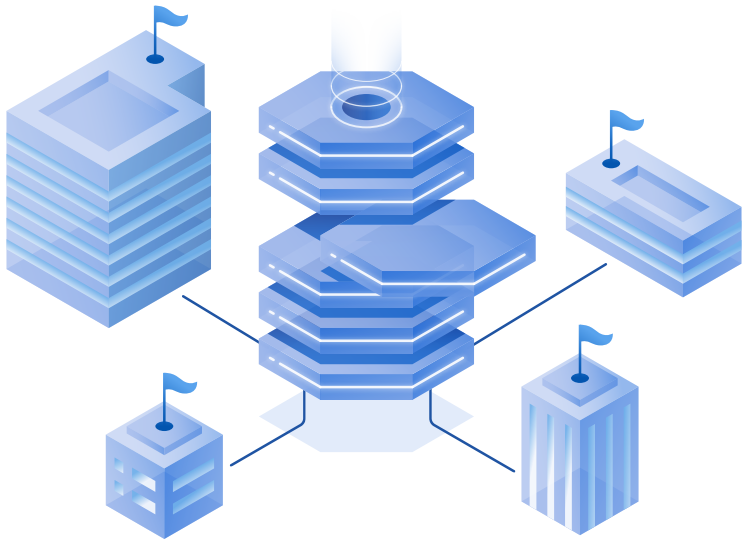
The next step is to get rid of potential vulnerabilities inside the software in the full disk/volume backup. There are many real cases when malware spread over a local network and infected machines through a single unpatched vulnerability. Machines were reinfected after restoration simply because malware quickly infected again as soon as the OS working environment was back online. To avoid such dangerous situations software can be patched during the full machine restore operation, thus eliminating the opportunity for malware to exploit the vulnerability. Acronis Cyber Protect will be able to do so soon, the functionality is now in development, going through testing and quality assurance.

Stop compromising. Trust in top-level anti-malware protection

Malware infects backups quite often. Some companies can scan backups in a centralized location but it takes a lot of time to perform consecutive regular scans. Active malware can also infect unpatched disk images all over again. Daily or even weekly full disk on-demand scans take a lot of time and often can't be done in non-working time, meaning employees are constantly disturbed by scans and can lose productivity.

But there is a better way to provide anti-malware protection: do quick scans of endpoints and the remaining scan in the centralized location after backup. This ensures you don't need to compromise between performance and security with Acronis Cyber Protect.

In this new innovative product from Acronis, cybersecurity and top backup technologies are integrated into one agent. As a result, we can cover both of these essential aspects of cyber protection and eliminate modern threats. Admins gain the ability to scan backups much faster than with other solutions and the confidence that their system can be restored without any malware or reported vulnerabilities.



Acronis

Learn more at
www.acronis.com