DCIG Technology Review Article

Arcserve OneXafe Product Review

The Immutability Attributes of Arcserve OneXafe and Their Role in Recovering from a Ransomware Attack

By
DCIG President & Founder
Jerome Wendt

DCIG, LLC
7511 Madison Street
Omaha NE 68127

O 844.324.455

When, not if, Ransomware Attacks

Headlines lead almost daily with the consequences of another ransomware attack. Enterprises now regularly pay ransoms over $1 million. Further, new research indicates 80 percent of organizations paying a ransom experience a subsequent ransomware attack. Any follow-on incident may result in additional downtime and ransom payments.

To breach corporate networks, hackers primarily target edge devices. Analysts forecast that by 2025 enterprises will generate 75% of their data outside of their data center. This data often gets generated or gathered by laptops, PCs, mobile devices, or edge servers. More susceptible to attacks, they provide a gateway into organizations for hackers to access their data stores.

In response, organizations deploy cybersecurity software to detect, prevent, and remediate from ransomware attacks. However, as Apple, JBS SA, Kaseya, and others can attest, cybersecurity software alone cannot defend against all ransomware attacks.

Immutable Storage: Cybersecurity Software's New Best Friend

These incidents put organizations on notice to safeguard their data for times when ransomware breaks through their cybersecurity defenses. When attacks occur, ransomware attempts to delete, encrypt, or lock any data it accesses. This puts any organizational data within ransomware's reach potentially at risk.

To recover from these attacks, more organizations look to immutable storage solutions. These devices complement cybersecurity software by storing production and/or backup data in an unalterable format. In this way, when a ransomware attack occurs, organizations may recover and restore unaltered copies of their data. Organizations frequently use the Arcserve OneXafe storage system for this purpose.

OneXafe's Ease of Deployment

OneXafe offers a standard file system interface that supports NFS and SMB networked file protocols. The widespread use of these protocols eases OneXafe's deployment and adoption in organizations. OneXafe presents shared network drives using these protocols to applications and clients. They, in turn, use them to discover and store data on OneXafe.

Organizations commonly use OneXafe to perform secure, corporate file sharing and store long-term data archives. OneXafe also serves as a logical storage target for backup solutions.

Unfortunately, the network file system features that facilitate OneXafe's ease of use also exposes it to ransomware attack attempts. Ransomware uses these same protocols to access, modify, and encrypt data stored on networked attached storage (NAS) solutions.

This makes any backup data stored on these solutions potentially susceptible to ransomware attacks. Should ransomware encrypt backups on a NAS solution, an organization may not recover.

arcserve® OneXafe®

Product: OneXafe

Website:
https://www.storagecraft.com/products/onexafe-converged-storage

Company: Arcserve

Location:
8855 Columbine Road, Suite 150,
Eden Prairie, Minnesota 55347

Phone:
+1 844 639 6792

https://www.cybereason.com/hubfs/dam/collateral/ebooks/Cybereason_Ransomware_Research_2021.pdf. Referenced 6/25/2021.
https://www.gartner.com/smarterwithgartner/what-edge-computing-means-for-infrastructure-and-operations-leaders/. Referenced 5/10/2021.

OneXafe's Immutable Object Store

The OneXafe system counters ransomware attacks by running a file system atop its immutable object store. Applications and clients only see and write data to the OneXafe file system. Beneath the file system, OneXafe automatically stores data on its underlying object store.

This differentiates OneXafe's architecture from other NAS offerings. When OneXafe stores file data as objects, its object store preserves file data in its original, unaltered state.

OneXafe also takes the additional steps of compressing and deduplicating the file data stored in each object. These steps reduce the storage capacity requirements for each object plus OneXafe creates a cryptographic integrity check for each object. The cryptographic hash created when each object gets compressed and deduplicated further ensures each object's data integrity. If a ransomware attack attempts to hack a OneXafe system, hashes associated with pre-existing objects remain intact.

If an application or client changes or deletes data residing on its file system, OneXafe's permits these actions. However, OneXafe's object store neither changes nor deletes prior versions of the data.

Rather, it functions as a journal. It chronicles new writes as well as any changes, additions, or deletions of existing data. In this way, OneXafe keeps the new data as well as the prior, original versions of the data.

OneXafe tracks these updates by changing the file system pointers to the data in the object store. The pointers only direct access requests to the most current data version. Applications and clients read and write this version of the data. Previously changed, deleted, or modified versions of data remain unchanged and unmodifiable within the OneXafe object store.

OneXafe Stages Recoveries

OneXafe utilizes its journal to stage recoveries should a ransomware attack occur. OneXafe automatically takes a system-wide snapshot every 90 seconds. Each snapshot references data in the state at which it exists at that moment. Once taken, an organization may perform a system-wide, point-in-time recovery of OneXafe using that snapshot.

OneXafe keeps each snapshot for a predetermined time based on the following retention schedule:

- The snapshot taken every 90 seconds gets retained by OneXafe for a minimum of one hour.
- OneXafe retains an hourly, daily, and weekly snapshot for a minimum of one year. It keeps one snapshot taken every hour as the hourly snapshot. It then designates one hourly snapshots as the daily snapshot and one of the daily snapshots as the weekly snapshot.

OneXafe only deletes any snapshot after the snapshot's retention period expires. Organizations may extend the retention period associated with hourly, daily, and weekly snapshot for longer than a year. However, they may not change a retention period associated with any pre-existing snapshots. They may only change the retention period for future snapshots.

Using this configuration, should a ransomware attack occur, organizations may select any retained snapshots as a recovery point. In this way, organizations may select a recovery point prior to the time when they detected ransomware in their environment.

Responding to a Prolonged, Undetected Ransomware Attack

OneXafe's method of journaling changes still allows for the possibility of a rare type of ransomware attack. Ransomware could encrypt an extensive amount of data for an extended period. Should this occur, OneXafe may not have any usable snapshots that organizations may use for recovery.

This scenario only plays out if ransomware runs undetected for a prolonged time (minimally days and more likely weeks or months.) Should this occur, OneXafe by default ages off older snapshots and makes them unavailable for use in a recovery. At the same, OneXafe continues taking snapshots every 90 seconds. These snapshots would contain data encrypted by ransomware. This scenario applies equally to similar storage entities that claim immutable storage and rely on snapshots to recover from ransomware attacks.

This hypothetical scenario may occur if ransomware runs undetected for too long. While OneXafe scales to over a petabyte of storage capacity, ransomware could change sufficient data to fill OneXafe up.

Arcserve acknowledges this rare type of ransomware attack could take place. To prevent it, it recommends organizations set alerts on OneXafe. This feature monitors specific thresholds on OneXafe.

For instance, it can monitor OneXafe's storage utilization. Should OneXafe breach this threshold, OneXafe generates an alert. The alert does not automatically mean ransomware exists in the environment. It only indicates the possibility of its presence.

OneXafe's Critical Role in Responding to a Ransomware Attack

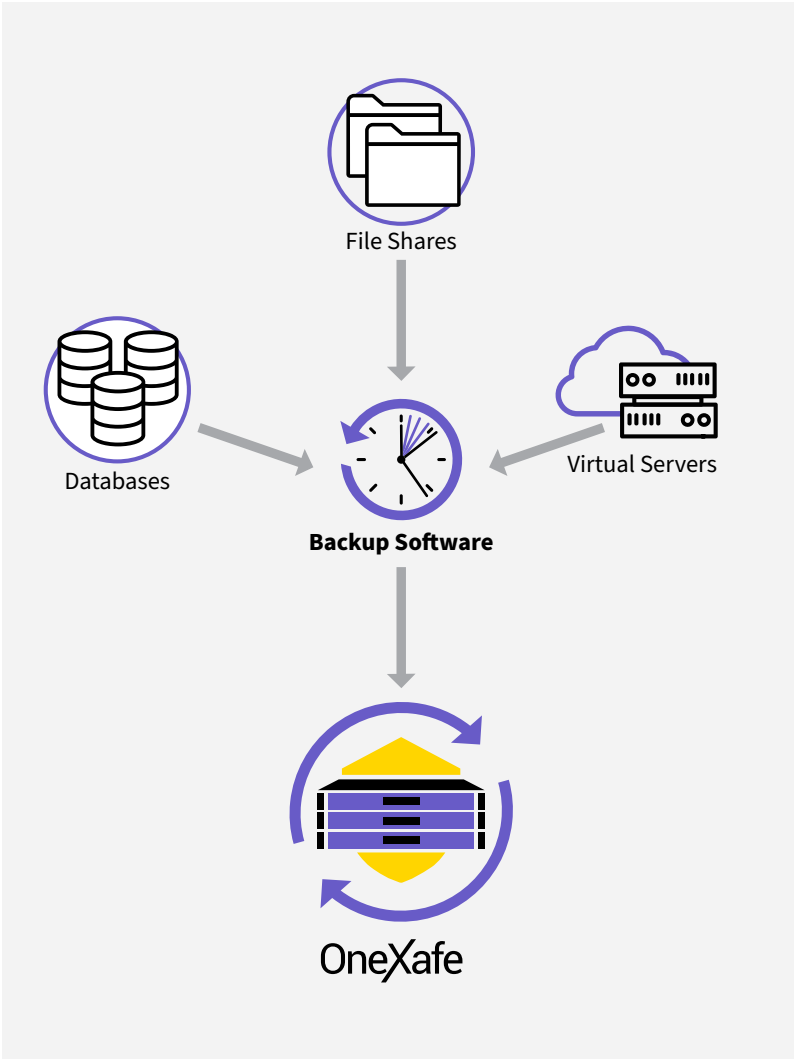
Every organization should use available cybersecurity software as its first line defense against ransomware attacks. Detecting ransomware and stopping an attack still better serves organizations than recovering from an attack. However, cybersecurity software does not provide a foolproof defense against ransomware attacks.

This data protection gap dictates organizations have a recovery plan in place. Placing backups on an immutable storage solution such as OneXafe plays a critical role in recovering from a ransomware attack.

OneXafe's simplicity of deployment and use belies its underlying sophistication that defends backup data from ransomware attacks. Using OneXafe, should a ransomware attack occur and encrypt backups stored on OneXafe, organizations can still recover.

Its immutable object store preserves all data, to include backup data, in an unaltered stated. Its underlying snapshot capabilities then ensures organizations have multiple, viable recovery points. These may go back days, weeks, months, and even years. These features used in conjunction with OneXafe's threshold alerting features ensure all backup data remains secure and recoverable.

arcserve® OneXafe®



About DCIG