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

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

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.

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 Critical Role in Responding to a Ransomware Attack

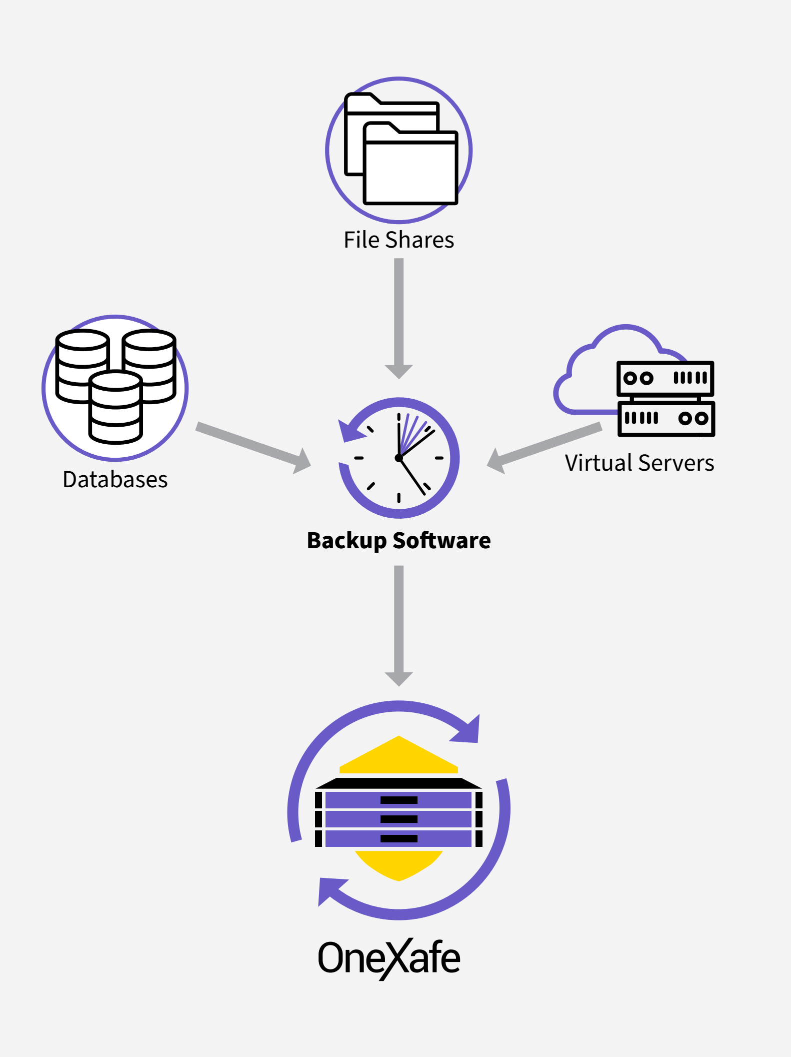
Every organization should use available cybersecurity software as its first line defense against ransomware attacks. Detecting ransomware and stopping an attack still better serves organizations than recovering from an attack. However, cybersecurity software does not provide a foolproof defense against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

The DCIG Technology Review is a product of DCIG, LLC. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. Product information was compiled from both publicly available and vendor-provided resources. While DCIG has attempted to verify that product information is correct and complete, feature support can change and is subject to interpretation. All features represent the opinion of DCIG. No negative inferences should be drawn against any product or vendor not included in this report. DCIG cannot be held responsible for any errors that may appear. This article was commissioned by Arcserve.

Safeguard your data with immutable storage

- Recover file, folder or entire file share rapidly from immutable snapshots that cannot be encrypted or deleted by ransomware attacks. Clone or recover a multiple-TB file share within seconds.
- Protect against a site failure with remote replication in four simple steps

Scale backup data storage

- Drive down the storage capacity requirements with built-in, fast, in-line deduplication of your backups. Efficient block level deduplication can deliver up to 10X data reduction rates, depending on the type of data
- Scale-out storage capacity, one disk at a time. Add an additional OneXafe and have the aggregate capacity immediately available to accommodate your escalating backup and data growth - gone are the days of forklift upgrades

Simplify the management of your backup infrastructure

- Eliminate management complexity, as there is no RAID, LUNs, or volumes to configure. Local ring-level replication protects against multiple disk or appliance failures
- Remove and replace failed disks (or appliances in a cluster) with no disruption to data services and no re-configuration of storage
- Manage OneXafe backup appliances from any browser
- Experience a simplified and intuitive management workflow

Conclusion

When data gets lost, corrupted, or damaged, the time required to restore and resume normal business operations is extremely critical. A reliable and fast recovery solution that does not depend on a time consuming restore can be a good alternative. OneXafe– with its integrated deduplication, immutable snapshots, and ease of management – offers a cost-effective, secure, and non-disruptive storage solution for your backup and unstructured data.

Take the Next Step

Find out more at arcserve.com

About Arcserve

Arcserve is a global top 5 data protection vendor with the broadest range of best-in-class solutions that manage, protect and recover all data workloads, from SMB to enterprise and regardless of location or complexity. Arcserve solutions eliminate complexity while bringing best-in-class, cost-effective, agile, and massively scalable data protection and certainty across all data environments. This includes on-premises, off-premises (including DRaaS, BaaS, and Cloud-to-Cloud), hyperconverged, and edge infrastructures. A 100% channel-centric organization, Arcserve has a presence in over 150 countries, with 19,000 channel partners and 235,000 customers, including MSPs, VARs, LARs, and end-users.