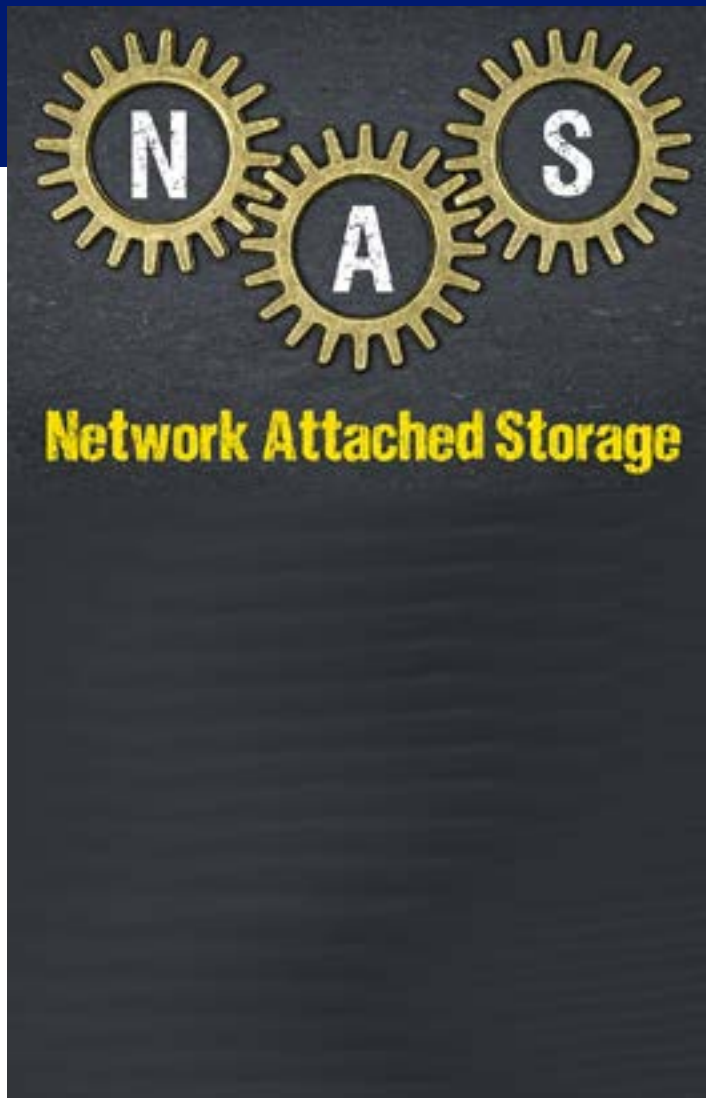
arcserve®

# Ransomware Prevention and Recovery: Data Protection Basics and Network-Attached Storage Benefits

# Table of Contents

# How Network-Attached Storage Can Cut Costs and Protect Your Data




The global network-attached storage (NAS) market is projected to grow at a 20.3 percent CAGR over the next seven years. But, before we look at the drivers behind that growth, here's a quick definition: A NAS system is a type of file-level storage that connects to your network so authorized users can access data and share files from a dedicated central location across a heterogeneous client and server environment.

That's a significant benefit in today's hybrid work environments, where ease of remote access and network performance matter more than ever. But there are plenty of other benefits to NAS. Here are just a few:

## Scale-Out Storage That Grows With You

NAS devices make it easier for you to add more storage to the system as you need it. Arcserve OneXafe is built on a scale-out architecture that lets you seamlessly add one drive at a time or multiple nodes in a cluster. That makes it perfect for unstructured data and backup targets, giving you an affordable option because you don't need to waste money on storage you don't need, as is the case with inflexible scale-up storage architectures.

## Cuts Operational and Storage Costs

Combining the advantages of a distributed, immutable-object store with the accessibility of SMB and NFS protocols, OneXafe's unified architecture makes storage management easy. That reduces IT time spent on storage, also cutting your operational costs. OneXafe goes one step further in keeping your storage costs in line by offering enterprise features like global inline deduplication and compression.

# MFA, Encryption and Immutability: Ransomware, Data Protection, and Recovery

Keeping your data safe is crucial, given that the cost of a data breach was over $4.5 million in 2021. To help you avoid those costs, OneXafe offers multi-factor authentication (MFA) to help prevent breaches and encryption for your data at rest.

Arcserve also strongly recommends that you adopt the 3-2-1-1 ransomware protection update to the old 3-2-1 backup rule. This new approach says to keep three copies of your data (one primary and two backups); store two copies locally on two formats (NAS, tape, or a local drive); and keep one copy offsite in the cloud or secure storage.

The extra "1" in 3-2-1-1 is probably the most essential feature in terms of your ability to recover from a ransomware attack or other data disaster. It stands for immutable storage. OneXafe uses an immutable object store, with every object written only once and never modified. Any changes you make to the file system always result in the creation of new objects, with OneXafe CDP taking low-overhead snapshots—a view of the file system at the instant it is taken—every 90 seconds.

Because underlying objects are immutable and can't be changed, the snapshots are also immutable, so an external source can't alter them. These snapshots let you roll back to a specific point in time and recover entire file systems in minutes.

# NAS Use Cases

OneXafe offers you a cost-effective option for various uses within your infrastructure. For file server consolidation, OneXafe is highly scalable and available and makes it easy to manage the storage of your unstructured data while adding a new level of resilience to your organization. Because it can scale capacity granularly, OneXafe helps you cost-effectively manage the ever-growing amount of data your organization generates.

Finally, OneXafe is the perfect disk-based target for both virtualized and physical server environments. That gives you the scalability you need for your backup data with almost effortless storage management. And don't forget about OneXafe's other cost controls like inline and variable-length deduplication and compression technologies.

# Get the NAS You Need

Get the details and learn how Arcserve OneXafe can help protect your data and reduce your data storage costs by watching an on-demand demo. Or choose an Arcserve technology partner for expert answers to your storage and security questions.

# Scale-Out NAS Delivers ROI for Bunduq's HCI Infrastructure Data Backups

Bunduq Company Limited has been developing the El Bunduq offshore oil field since 1975. Recognized by the industry for its operational efficiency, the company has adopted digital technologies that are indispensable for its day-to-day operations and management. For Bunduq, having an agile, resilient, dependable, and scalable IT infrastructure is crucial to its success.

That is among the reasons the company embraced a hyper-converged infrastructure (HCI) several years ago. It also chose HCI to maintain stability and increase performance across its many digital processes. Scale-up network-attached storage was another important consideration because of the massive amount of data the company needs to back up.

Bunduq used a scale-up storage environment for those data backups, built with solutions from QNAP and Netgear. But the Bunduq IT team soon realized that this storage architecture's scale-up technology had significant limitations—it only allowed them to add data storage within a fixed upper limit, at which point they would have to add more storage controllers or upgrade their system with newer models with higher capacities.

## More Data Requires More Backup Storage

"We needed a solution that would not only be compatible with our hyper-converged setup but one that would also be able to manage the sheer volume of data we were generating and needed to back up," said Bunduq IT Supervisor Muayad Fahmawi. "Our data growth is exponential, and we had to have multiple backups in place to cover our disaster recovery site. But this was becoming complex and inefficient. We wanted to consolidate everything in one place."

Bunduq recognized that its current solution wasn't cost-effective and was concerned that it would become ever more complex to manage. It also had severe inefficiencies in data migration and workload resource allocation. Led by Muayad, Bunduq started searching for a better storage solution.

## Arcserve Partner Recommends OneXafe

Arcserve technology partner and IT and cybersecurity solution provider Unicorp Technologies, LLC, recommended the Arcserve OneXafe platform. Unicorp showed the Bunduq IT team how OneXafe would easily integrate into their setup, secure their data, and, most importantly, meet their mounting capacity needs. It was also more powerful and offered a more comprehensive range of features than alternative offerings.

## Scalable Capacity for Primary and Secondary Workloads

"Arcserve OneXafe not only provided scale-out architecture. It also offered ransomware protection to backup files thanks to the immutable snapshots it takes every 90 seconds, which made it unique when compared to other storage solutions. It also had replication features built into the same license, making it much more cost-effective. And the OneSystem management console made it much easier to manage—with all these advanced features, we felt that OneXafe met our needs and then some," said Muayad.

OneXafe is designed to offer scalable, immutable network-attached storage (NAS) capacity for either primary or secondary workloads. It expands storage seamlessly—by either adding one drive at a time or multiple nodes within a cluster—without any configuration changes to the application. OneXafe also minimizes storage requirements with powerful data reduction technologies such as inline deduplication and compression, further reducing storage and operational expenses.

## OneXafe: Cost-Effective and Easy

Bunduq realized OneXafe's benefits as soon as it was introduced into its infrastructure. "It is an incredibly user-friendly solution; it's just plug-and-play. The implementation was quick, it fits in seamlessly, and we didn't need any training. It requires limited monitoring and maintenance. It has been so effective that within a year, we were adding a second box to the cluster to increase our backup coverage," said Muayad.

Bunduq now uses OneXafe NAS storage for more than 80 TB of its business-critical data. The company's IT team has been impressed by OneXafe's advanced deduplication and compression features which have helped it realize a data reduction ratio of just under 8:1.

# Delivering Beyond Expectations

“OneXafe’s performance has exceeded our expectations—its return-on-investment is quite substantial. Its scalability, compression, and deduplication technology have boosted our efficiency and reduced our cost of operations. And its protection from ransomware attacks ensures that our business-critical data is secure. It supports any expansion plans we might undertake now or in the future,” said Muayad.

If you’re looking for a better scale-out storage solution, Arcserve has the answers. To get started, find an expert Arcserve technology partner, or check out our OneXafe on-demand demo to see for yourself what OneXafe can do.

# 5 Ways to Prevent and Recover From Ransomware

Maybe you're one of the 77 percent of respondents to a recent ExtraHop survey of security and IT decision-makers (ITDMs) in the US, UK, France, and Germany who feels highly confident in your organization's IT security readiness.

But the same survey found that 64 percent of those same ITDMs acknowledge that at least half of their cybersecurity incidents resulted from their own outdated IT security solutions. Even worse, 85 percent of respondents had suffered at least one ransomware attack in the past five years, 74 percent have experienced multiple attacks, and 42 percent of those attacked paid the ransom.

Those are staggering numbers. And if you're a security pro or ITDM, it should be a glaring sign that it's time to take a closer look at your disaster recovery strategy and backup system to make sure everything is up to date and able to prevent the loss of mission-critical data.

## 1. Keep Software Patched to Prevent Known Vulnerabilities

One of the more exasperating reasons ransomware attacks succeed is the failure to keep software patched and updated. The ExtraHop survey noted that 68 percent of ITDMs admit to running SMBv1. First introduced by Microsoft in 1996, this file-sharing protocol lacks modern security protocols. Hackers consider this vulnerability to be an open invitation to attack, leading to more than $1 billion in cyberattack damages.

A more recent example is the Log4j vulnerability found in the Apache logging framework. Web and server application developers commonly use Log4j, so the threat is widespread and extremely dangerous. But that's just one vulnerability among hundreds. The Cybersecurity & Infrastructure Security Agency (CISA),

part of the Department of Homeland Security (DHS), offers a list of 478 exploited known vulnerabilities in its online catalog, adding 95 more to this list just this week.

In a recent blog post, Security Week says 2022 will most likely be a record year for the number of common vulnerabilities and exposures (CVEs) reported—likely more than 22,000. As the post notes, many organizations are finally dedicating time to basic cyber hygiene. The point is clear: It's time to audit all of your software and hardware to confirm everything is patched and up to date.

## 2. Update and Test Your Disaster Recovery Plan

Forrester's 2022 State of Disaster Recovery Preparedness just released a new study with some good news and some bad news. The good news is that more than 80 percent of respondents said they have some form of disaster recovery (DR) program, and 48 percent of respondents update DR plans annually. The bad news is that nearly a quarter of respondents that do have a plan only review those DR plans every two years or less. Now is the time to dust off your DR plan and make sure you're prepared for evolving ransomware threats.

Of course, your plan will have little value if it doesn't work properly when you need it. That's why you need to schedule regular tests of every aspect of your disaster recovery plan, from your backup and recovery capabilities to your physical recovery procedures.

## 3. Follow the 3-2-1-1 Rule

We frequently mention this update to the old 3-2-1 rule in our posts because we believe it is crucial for data recovery. Hackers are now targeting backups more often, preventing you from getting your systems back up and running from restored, uncompromised data. The new 3-2-1-1 rule eliminates that problem with a layered strategy. Keep three copies of your data (one primary, two backups), with two copies stored locally on two formats (network-attached storage or local drive), and one copy stored offsite in the cloud or secure storage. The final "1" is what makes all the difference in the world when it comes to backups because it states that one copy should be immutable. Immutable backups can't be altered or deleted.

## 4. Put a Multi-Layered Backup Data Protection Approach in Place

A proactive, multi-layered approach to data protection that includes immutable backups protects and immunizes your backup data from ransomware and other cyberattacks. Arcserve solutions do just that. Here's how:

### Detect, Prevent, Protect, and Neutralize

Arcserve ransomware recovery solutions integrate Sophos Intercept X Advanced to secure your on-premises, cloud, and SaaS-based backups. By detecting signature-based and signatureless malware using a deep learning neural network, anti-exploit technology, CryptoGuard anti-ransomware, and WipeGuard technologies, Sophos Intercept X Advanced ensures you can count on continuous detection and prevention.

Arcserve's heterogeneous, image-based technology protects your data in transit to and from any target. By combining enterprise-ready features with ease of use, data protection is simpler. And you can easily scale up or down based on demand and turn features on and off without forklift upgrades while threats are neutralized.

## 5. Consider Disaster Recovery as a Service

A cloud-based backup and disaster recovery as a service (DRaaS) solution should be a leading contender for protecting your on-premises business systems and data. While local backups may make it possible for you to recover IT systems from server failure or other common problems, a sitewide disaster—like ransomware or an earthquake—could destroy those backups. The result is likely to be too much costly downtime.

When you combine Arcserve's backup and recovery solutions with Arcserve UDP Cloud Hybrid you can count on complete and reliable business continuity. Besides streamlining data backup and recovery management, Arcserve DRaaS lets you get critical systems back up and running quickly and easily.

## Fight Back Against Ransomware Now

Get expert help in finding the right data recovery and ransomware protection solution for your business by finding an Arcserve technology partner. To see for yourself how Arcserve DRaaS can help you sleep better at night, check out our on-demand demos.

# How Going Back to Basics Strengthens Your Data Storage Security

*By Byron Horn-Botha, Lead, Arcserve Southern Africa channel and partnerships*

I think we all share a fairly large degree of optimism and trepidation as we attempt to change how we do things in IT.

Criminals engaged in ransomware are no different. It is increasingly apparent that they dedicate their efforts to causing the most significant damage in the shortest possible time.

IDC has identified this trend with the observation that ransomware attackers have learned that eliminating the possibility of data recovery by attacking the data backups can maximise the attack's impact on primary data.

Just to put it into perspective, as far back as 2014 and based on industry surveys at the time, Gartner estimated the cost of network downtime was typically around US$5,600 per minute, which extrapolates to well over US$300,000 per hour. I'm sure I now have your attention!

Forbes reports that the recent six-hour-long outage of the Facebook family of apps cost the company nearly US$100 million in revenue. Worse, it drove millions of social media users to Twitter as people couldn't view their Facebook feeds, exchange WhatsApp messages, or post Instagram reels. To add insult to injury, it sparked a derisive meme feast that didn't do much for the brand.

None of us need to be reminded that the damage from ransomware can have a profound and lasting impact on organisations. If it is to be defeated, the solution should appear obvious: IT organisations need to architect a system that assures data recovery without paying a ransom. This may appear to be a tall order, but the good news is that it has been achieved.

Many CIOs are familiar with the old '3-2-1' rule when it comes to data protection, namely: three copies of data (primary and two backups); two copies stored locally on two formats (NAS, tape, or local drive); and one copy stored offsite (cloud or secure storage).

But this is now somewhat outdated due to the importance of protecting the backup. Today, the 3-2-1-1 strategy is recommended to safeguard data, with the extra '1' being immutable storage.

Immutability is a critical element of successful ransomware protection. It is when data is converted to a write-once, read-many-times format, which cannot be altered. Unlike data encryption, there is no key, so there should be no way to 'read' or reverse the immutability.

**If ransomware gets into an admin system, it can spread like wildfire and even infect secondary storage.**

The latter is also crucial when paired with other data protection elements, such as continuous data protection, which can capture data on each write at rapid intervals measured in seconds. If that data is stored in immutable form, the customer can then have a 'snapshot' of data that cannot be altered.

Having the right technology in place, augmented by sound and well-rehearsed recovery practices, is essential. But adding immutability means you can access and restore data to its unaltered state and get back into operation within minutes of a breach. What CIOs and CTOs do not want to keep the lights on and be up and running within minutes of an attack?

## Breaking Down 3-2-1-1 vs. Traditional 3-2-1

Let's take a look at what the traditional 3-2-1 rule entails. In essence, as noted, it recommends that you keep at least three copies, store two of them on different media and store at least one additional copy at an offsite location.

While it sounds like having two copies onsite means the business automatically has quick access to its backup if its primary storage fails, that may not always be the case. What happens when disaster strikes and takes both of the onsite devices down?

If ransomware gets into an admin system, it can spread like wildfire and even infect secondary storage. These scenarios are played out every day in businesses across the world.

For example, what if both data copies are compromised? The first thing the company does is shut its systems down and put its backup and disaster recovery plan into motion. That's when it turns to offsite backups. This is precisely when the problems commence.

With secondary storage primarily built for backup security and scale at a relatively low cost, these systems can impair recovery if they can't quickly transfer the vast amount of data that typically needs to be recovered. That could add a considerable amount of time for applications and data to come back online after a disaster, which is, of course, very costly.

In a nutshell, the 3-2-1-1 rule comes into its own in this last example, with at least three backup copies of data and two stored on different storage media while placing one of them offsite.

Immutable storage is the key to successful ransomware protection because the company's data is converted to a write-once, read-many-times format that can't be altered. Essentially, the data cannot be changed or deleted once it is written.

Learn More

Find out how going back to data protection basics and adding immutable storage strengthens your data storage security by talking to an Arcserve expert technology partner or contact us for more details.

# Need Answers?

## Arcserve is always here—standing by and ready to help.

arcserve®

**+1 844 639-6792**

**arcserve.com**