arcserve®

# Cybersecurity, Backup, and Disaster Recovery: Ransomware Defense Best Practices

# Table of Contents

# 3 Backup and Recovery Solutions to Help You Win the Fight Against Ransomware

Our recent global survey of IT decision-makers speaks volumes about today's focus on backup and recovery. As we highlighted in a recent post, 77 percent of those surveyed are not confident they can recover lost data if they get hit by ransomware. The survey's good news is that 92 percent of respondents said they are making additional investments to protect against these attacks.

As TechTarget points out in a recent article, today's evolving threats are a wake-up call for organizations to improve their security postures, especially as sophisticated cybercriminal organizations increasingly target backups with ransomware. So, how do you protect your backups from ransomware? And what should you look for in a backup and recovery solution?

Start by following the 3-2-1-1 backup strategy we've written about frequently in these posts. Then, consider these solutions as you put the strategy into action:

## 1. Cloud-Based Backup and Disaster Recovery

Today's cloud-based solutions can protect your on-premises business systems and your data. That's important because, while local backups can be enough to recover your IT systems if all you've suffered is a server failure or other minor hiccup, a site-wide disaster could destroy your backups and cause some serious downtime. Arcserve Cloud Hybrid is a fully integrated hybrid cloud backup, cybersecurity, and disaster recovery extension to Arcserve backup and recovery products. Together, these products ensure you'll have complete and reliable business continuity.

Arcserve Cloud Hybrid lets you quickly deploy cloud-based backup and disaster recovery to public and private clouds and deep learning system protection to secure backups from cyberattacks. You can also adapt to rapidly changing business requirements while meeting stringent RTOs and RPOs.

## 2. Immutable Network-Attached Storage

Moving to the cloud doesn't mean you won't have any on-premises or secondary offsite infrastructure to protect. And protecting on-premises data isn't easy, no matter how many precautions you take. That's where immutable network-attached storage like Arcserve OneXafe enters the picture by backing up your data to an immutable object store. Every backup object is in a write-once, read-many-times format that can't be modified—even by ransomware.

Any changes you make to the file system always result in the creation of new objects, with OneXafe's continuous data protection (CDP) taking low-overhead snapshots every 90 seconds. These snapshots are a view of your file system at the instant it was taken. Because the underlying objects are immutable, the snapshots inherit this immutability, so they also can't be changed by an outside source. Most importantly, these snapshots let you go back to specific points in time and recover entire file systems in minutes.

OneXafe's scale-out architecture gives you a highly scalable, disk-based backup target for your virtualized and physical server environments. That makes it easy to scale to meet your ever-growing backup data needs and handle storage management tasks with near-zero configuration. And OneXafe helps control growing data storage costs with powerful data reduction technologies, including inline and variable-length deduplication and compression.

## 3. Unified Data Protection Software

Unified data protection software is another enhanced data protection and backup and recovery solution that should be on your list. Arcserve UDP gives you all-in-one data and ransomware protections, neutralizing ransomware attacks and letting you restore your data and perform effective disaster recovery. Arcserve UDP is safeguarded by Sophos Intercept X Advanced cybersecurity, combining deep-learning server protection, immutable storage, and scalable onsite and offsite business continuity.

The solution's multi-layered approach gives you complete IT resiliency, protecting against data loss and extended downtime across your cloud, local, virtual, hyperconverged, and SaaS-based workloads using a unified central management interface. It can reduce downtime from days to minutes and validate your recovery point and recovery time objectives (RTOs/RPOs) and service-level agreements (SLAs) with automated testing and granular reporting. Immutability of your data backups is also assured with support for Amazon AWS S3 Object Lock.

Arcserve UDP lets you restore faster with instant VM and bare metal recovery (BMR), local and remote virtual standby, application-consistent backup and granular restore, hardware snapshot report, and extensions delivering high availability and tape support. The solution also protects Microsoft 365 workloads—Exchange Online, SharePoint Online, and OneDrive for Business—on-premises while offering deep data reduction, granular recovery, and offsite replication.

## Find the Right Backup and Recovery Solution for Your Organization

Every organization has different requirements. Get expert guidance for putting a proper backup and recovery solution in place by choosing an Arcserve technology partner. To learn more about Arcserve products, check out our product demos and free trial offers.

# How to Protect Your Backups From Ransomware Now

You're likely already doing everything you can to protect your organization's data from all the cyber threats out there. But ransomware is the threat that's undoubtedly making most of the headlines. And it's one of the costliest threats we see, with the FBI's Internet Crime Complaint Center (IC3) having 3,729 complaints identified as ransomware in 2021 with adjusted losses of nearly $50 million. Another report found a 13 percent increase in ransomware attacks over the year the report covers. That increase equals the growth in attacks seen over the last five years combined.

Most companies—73 percent, according to the Sophos State of Ransomware 2022 report—rely on their backups as their primary defense against ransomware. But backups aren't always safe from attacks. CSO Online recently reported how Conti ransomware encrypts files and deletes backups. So just taking regular backups isn't enough.

## The 3-2-1-1 Rule: Protect Your Backups From Ransomware With Immutability

You can expect a unanimous "yes" when you ask anyone in IT if backups are essential. But how you back up your data is crucial if your efforts will be of any use. That's why firmly recommend that you employ a 3-2-1-1 backup strategy. The strategy is simple:

- Keep three copies of your data (one primary and two backups)
- Store two copies locally on two formats (network-attached storage, tape, or local drive)
- Store one copy offsite in the cloud or secure storage
- Ensure one copy is immutable

Immutable storage is a write-once, read-many-times format that can't be altered or deleted, even if a ransomware attack successfully gets to your backups. Arcserve OneXafe's file system is based on an immutable object store, delivering that extra level of protection. Any modification to the file system always results in the creation of new objects, with OneXafe continuous data protection taking low-overhead snapshots every 90 seconds, capturing a view of the file system at the instant the snapshot is taken.

Because the underlying objects are immutable and can't be changed, the snapshots inherit this immutability, rendering ransomware ineffective at destroying your backups. And you can go back to any snapshot at any specific point in time and recover your entire file system in minutes.

## Air-Gapping and Tape Backup Software: No Path In, No Damage Done

We recently posted about how air-gap cyber security technologies help stop ransomware attacks. Put simply, air-gapping means physically disconnecting your backups from all your systems. While an air-gap strategy may take a bit of IT time and effort, it is a highly effective means of ensuring access to your backups is controlled and online access is impossible.

Tape backup is a tried and true strategy for air-gapped backups because you simply remove and store each tape cartridge securely offline on a predetermined schedule. Arcserve Tape Backup software lets you leverage the benefits of tape with a modern approach that includes a centralized management and storage resource manager (SRM) and the ability to monitor the status of all backup activities.

Arcserve Tape Backup lets you incorporate sophisticated functionality into your VMware, Microsoft Hyper-V, and Citrix XenServer platforms, too. You even get smart restore capabilities that let you redirect restore jobs to other media containing the same data without manual intervention and quickly restore individual application objects from Active Directory, Microsoft Exchange, Microsoft SQL Server, and Microsoft SharePoint. And you can count on faster, more efficient backups and restores with UNIX and Linux data movers for SAN-based backups.

## Understand Your Options

Talk to an expert Arcserve technology partner for help putting solutions in place that protect your backups from ransomware—and all the other threats you face. To learn more about Arcserve data protection, backup, and disaster recovery solutions, check out our free product demos.

# The 5-Step Ransomware Disaster Recovery Plan Template


*By Ahsan Siddiqui, Director of Product Management, Arcserve*

Ransomware attacks continue to impact organizations worldwide—and the costs are staggering. A new global survey of over 1,100 IT decision-makers at small and midsize companies found that 50 percent had been targeted by a ransomware attack, with 35 percent asked to pay over $100,000 in ransom and 20 percent asked to pay between $1 million and $10 million.

These numbers are not expected to improve soon. The sad truth is that, despite spending billions on cybersecurity tools, businesses are still poorly prepared for ransomware attacks. Less than a quarter (23 percent) of all respondents to the survey said they're very confident in their ability to recover lost data in the event of a ransomware attack. Smaller businesses are even less well prepared. Under 20 percent are very confident in their ability to recover lost data in the event of a ransomware attack.

Meanwhile, the attack surface continues to expand as organizations using technologies like IoT, artificial intelligence, and 5G generate even more data—data that can be compromised and held captive by ransomware attackers.

For this reason, companies must take a new approach to data resilience. They must strengthen their disaster-recovery strategies, backup systems, and immutable storage solutions to prevent the loss of mission-critical data.

Many are. The survey found that 92 percent of organizations are making additional investments to protect against ransomware attacks, with the top areas of investment being security software (64 percent), training and certification (50 percent), and managed services (43 percent).

While these investments are encouraging, more should be done. Because, for most companies, it's not a matter of if their data will be compromised; it's a matter of when. With ransomware attacks increasing yearly, data backup and recovery should be at the very top of every organization's priority list.

Here are five steps businesses can take now to reduce their exposure to ransomware and avoid staggering losses.

# 1. Educate Employees

It's essential to invest in training for staff so that they're aware of how ransomware works. From there, employees will be better prepared to recognize and prevent it. They should know that ransomware can sneak in from anywhere. The training should remind them to scrutinize every link in emails and not open attachments in unsolicited emails.

Employees should be reminded to only download free software from websites they know and trust. When possible, employees should verify the integrity of downloaded software through a digital signature before execution.

# 2. Focus on Remediation and Prevention

Companies continue to invest loads of money in cybersecurity solutions like next-generation firewalls and extended detection and response (XDR) systems designed to prevent attacks. Yet these same companies are still falling prey to ransomware and being forced to pay a hefty price.

It's time for companies to stop focusing entirely on prevention. They should also invest in remediation measures like backup and disaster recovery and immutable storage that allow them to quickly restore their data and avoid paying the ransom when attackers break in.

Regular data backups and encryption play a key role in protecting an organization's data. A consistent backup schedule will enable you to restore any compromised systems or data seamlessly. Encrypting your sensitive data is also highly recommended. After all, if ransomware attackers gain access to your critical assets, encryption has the benefit of keeping data from being read and further exploited by the bad guys.

# 3. Place a Premium on Data Resilience

Your data resilience is only as strong as your weakest link. Monitor your weaknesses, fix them when you find them, and you can bounce back quickly from disruption and return to normal operation. To do this, you must have the technologies required to back up your data and recover it if necessary, along with the proper mindset. That means a defensive posture is regularly maintained with drills that simulate an intrusion to measure your resiliency and bolster it where necessary.

Many companies develop a strategy and then neglect to test it. That's like a basketball team devising a sophisticated defense and never bothering to practice it. All companies should regularly test their data backup and recovery plans to ensure they can effectively restore their data and systems if an attack or natural disaster occurs.

# 4. Know Which Data is Most Critical

Data varies in value. If you're concerned about costs, as most organizations are these days, you don't have to store or back up all your data in the same place. Look into storage solutions that provide options like data tiering. These enable you to place less-important data in less-expensive levels of storage or "tiers."

Another upside of data tiering is lower energy costs. You'll use less compute power if you're not storing every last byte of your data at the highest security level.

# 5. Put a Disaster Recovery Plan In Place

Despite all the preventive measures you take, you need to prepare for the possibility that you will get hit. So, it would be best if you had a disaster recovery plan. You need to be able to back up data as often as is appropriate—ideally every 15 minutes for critical data. You also need to easily verify that your whole environment is backed up, including your remote workers and any SaaS applications you use, such as Microsoft 365.

A good disaster-recovery solution will back up your data to a location of your choice and on a schedule that suits you. It will also be easy to test, which is crucial because testing is the only way you can validate that your recovery-time goals can be met. It may seem obvious, but this is where many solutions fall short. Your disaster recovery solution must be able to recover your data every time and on time. When ransomware hits, you want to be confident you can recover your data and get on with business as soon as possible.

Check out this post for a step-by-step guide to creating a disaster recovery plan.

## Final Thoughts

There is no perfect defense against ransomware. The best approach is a multilayered one that includes educating your staff, investing in reliable data backup and recovery and immutable storage solutions, and having a robust disaster recovery plan. That's how organizations can stay ahead of this growing threat and protect their data and bottom line.

To learn how Arcserve can help you prevent the consequences of ransomware, talk to an expert Arcserve technology partner.

# How to Upgrade SLED Backup and Recovery Methods

A recent article in CPO Magazine says that funding is flowing for cybersecurity efforts in every government jurisdiction. One source of that funding is the Infrastructure Investment and Jobs Act (IIJA), signed by the President in 2021, which allocates $195.3 billion to the states and an additional $130.2 billion to local governments and authorities.

The law lets state, local, and education (SLED) organizations use the IIJA funding for cybersecurity modernization and resilience programs, with 80 percent of those funds required to go directly to local governments and 25 percent directed to rural areas. The states stepped up, too, with more than 300 pieces of legislation related to cybersecurity introduced at the state level in 2022.

If you're an IT pro responsible for data protection for a SLED organization, it's clear you need to invest whatever you can in cybersecurity prevention solutions—regardless of where you find the funding. Backup and recovery solutions and software are just as important, given that, when it comes to ransomware attacks, the local government sector is most likely to have its data encrypted, and education is the sector most likely to suffer an attack.

## Backup and Recovery Methods: Follow the 3-2-1-1 Rule

Regardless of the technology you choose, the backup and recovery methods you put in place can be the difference between a devastating data loss and full, fast recovery. The 3-2-1-1 strategy is the foundation of a sound solution because it gives you multiple ways to recover, including a last line of defense that ensures your data is always protected.

The strategy is simple. Keep three copies of your data—one primary and two backups—with two copies stored locally in two formats. These can be network-attached storage, tape, or drives. One copy should be stored offsite in the cloud or secure storage. And one copy should be in immutable storage. Stored immutable backups are in a write-once, read-many-times format that can't be altered or deleted. Since there is no key, as with encryption, there should be no way to "read" or reverse the immutability. So your data can always be recovered.

# Immutable Storage: Built for Backups

Arcserve OneXafe was designed to deliver immutable network-attached storage for your unstructured data and backup targets. This scale-out storage solution eliminates the need for forklift upgrades while giving you an immutable object store. OneXafe features continuous data protection (CDP), taking low-overhead snapshots every 90 seconds. Each snapshot is a restorable view of the file system at the moment the snapshot was taken. And it's easy to go back to any snapshot at a specific point in time and recover entire file systems in minutes.

OneXafe's scale-out approach lets you add one drive at a time or multiple nodes in a cluster, so you don't have to allocate storage capacity that you don't need "just in case." OneXafe also features the accessibility of SMB and NFS protocols, while its unified architecture keeps management simple and reduces operational costs for storage. It also enables enterprise features like global inline deduplication, compression, and encryption at rest.

# Data Protection for Simpler SLED Environments

Your data is precious, regardless of the size of your SLED organization. Arcserve OneXafe Solo is a plug-and-play data protection appliance that streams data directly to Arcserve Cloud Services to ensure operational continuity. Extremely easy to deploy, with cloud-based management from anywhere via a web browser, OneXafe Solo is perfect for smaller institutions and governmental agencies, especially those with remote and branch offices that also need data protection.

OneXafe Solo also delivers cost-effective, enterprise-class features, including the ability to quickly boot up backup images as virtual machines (VMs) using patented VirtualBoot technology. You can recover files and folders in seconds and entire systems in minutes. And OneXafe Solo offers both host-based and agent-based data protection, complete with physical and virtual system recovery and set-and-forget, SLA-based policy management.

# Upgrade Your Backup and Recovery Capabilities

Whether you work in local government, education, or any public institution, learn how Arcserve solutions can support your data protection, backup, and disaster recovery strategy by talking to an Arcserve technology partner. To learn more about Arcserve OneXafe, check out our free demo.

# Need Answers?

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

arcserve®

**+1 844 639-6792**

**arcserve.com**