arcserve®

Valuable Insights Into Cybersecurity, Data Protection, and Disaster Recovery

Valuable Insights Into Cybersecurity, Data Protection, and Disaster Recovery

New Cybersecurity Incident and Response Playbooks Released by CISA

The orders came straight from the top. The President's May 2021 announcement of the Executive Order on Improving the Nation's Cybersecurity directed the federal government to bring the "full scope of its authorities and resources to protect and secure its computer systems, whether they are cloud-based, on-premises, or hybrid." That includes ensuring federal information systems meet or exceed the cybersecurity standards outlined in the order.

In response, the Cybersecurity & Infrastructure Security Agency (CISA), has just published the Federal Government Cybersecurity Incident and Vulnerability Response Playbooks. While the playbooks were created to provide federal civilian executive branch (FCEB) agencies with cybersecurity incident and vulnerability response procedures, CISA encourages all state, local, territorial, tribal, and private sector organizations to review them to benchmark their own vulnerability and incident response practices.

Standardized Response Processes

The playbooks focus on two primary areas. The Incident Response Playbook provides procedures and processes for:

- Preparation
- Detection and analysis
- Containment
- Eradication and recovery
- Post-incident activities
- Coordination

The Vulnerability Response Playbook offers the same support for:

- Preparation
- Vulnerability response process
- Identification
- Evaluation
- Remediation
- Reporting and notification

Small Lapses Lead to Big Ransomware Vulnerabilities

This week the House Committee on Oversight and Reform also released a memo stating that a series of "small lapses" in cybersecurity led to several recent major breaches and ransomware attacks. The example noted in the memo was that of a single user using a weak password that opened the door to hackers. They may have been referring to Colonial Pipeline being compromised by a single stolen password linked to a profile. That attack led to gas shortages in several states earlier this year after the company was forced to shut down the pipeline. The company eventually paid the attackers around $4.4 million in Bitcoin, the majority of which was later recovered by the Justice Department.

Cybersecurity Education is Your Best Defense Against Ransomware

The House memo also notes that, with seemingly robust security systems falling victim to simple attack vectors, security education and other proactive security measures are critical. In fact, 85 percent of breaches involved the human element, while 36 percent involved phishing. A recent, simple, seven-question cybersecurity assessment quiz resulted in 60 percent of respondents failing. What's even more frightening is that less than 1 percent of respondents got all seven questions right.

So, an effective, ongoing security awareness training program is vital to prevention. The key word here is effective. Look for a training partner that has a proven track record in delivering measurable results in cybersecurity awareness. One study found that employees who receive security awareness training are significantly better at recognizing security threats than those who haven't received training. And the difference is substantial, with 23 percent of IT/security professionals reporting untrained employees as "capable" or "very capable" of recognizing cyberattacks compared to . The percentage spread is much the same for targeted emails, social media, and web scams.

Make Sure You Have a Last Line of Defense

There is no way for you to be 100 percent certain that your data and systems are safe from cyberattacks. That's why you also need a last line of defense, leveraging backup and data recovery processes with well-defined frequency, as well as data storage features like continuous data protection, which takes immutable snapshots of your complete data set. That way, if a ransomware attack is successful in encrypting your data and corrupting your primary file system, the snapshots are completely unaffected—they can't be altered or deleted.

Get Expert Guidance

With so much involved in keeping your data and systems safe and security, it's worth talking to a backup and data recovery professional from Arcserve, an Arcserve company. Or you can dive into your options by watching an on-demand demo.

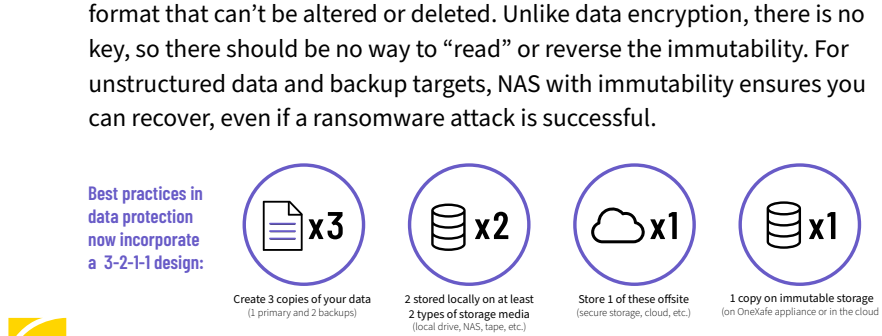
How Immutable NAS Offers Cost-Effective Ransomware-Proof Storage for Unstructured Data and Backup Targets

MarketWatch notes that the global network-attached storage (NAS) market will grow at an impressive compound annual growth rate (CAGR) of nearly 28 percent between 2021 and 2027. Much of that market growth can be attributed to the massive increase in data generated by organizations everywhere. That isn't much different from the global projections for the cloud storage market—pegged at a CAGR of about 26 percent between 2021 and 2028. Each of these two types of storage has its benefits. For this article, let's focus on NAS.

NAS is defined as dedicated, centralized file storage that enables multiple users and heterogeneous client devices to retrieve data. There are plenty of good reasons that NAS should be a critical part of your storage strategy. First, NAS is easy to access, so it's also easy for users to collaborate and share data. NAS also offers scalable capacity and low costs.

Why Immutable NAS?

Immutability is a crucial feature to look for in a NAS solution. According to IDC, organizations should follow the new 3-2-1-1 backup rule, which says to keep three copies of your data, with two copies stored locally on two formats—NAS, tape, or local drive—and one copy stored offsite in secure storage or the cloud. The "1" at the end stands for immutable storage. Immutability is when data is converted to a write-once, read-many-times format that can't be altered or deleted. Unlike data encryption, there is no key, so there should be no way to "read" or reverse the immutability. For unstructured data and backup targets, NAS with immutability ensures you can recover, even if a ransomware attack is successful.



Why OneXafe Immutable NAS?

OneXafe is an easily managed NAS solution that offers you a scale-out architecture, making it simple to seamlessly add one drive at a time or multiple nodes in a cluster. That means you no longer have to allocate extra storage capacity to compensate for inflexible scale-up legacy storage. OneXafe combines the advantages of a distributed, immutable object-store with the accessibility of SMB and NFS protocols. And OneXafe's unified architecture reduces management complexity and operational costs for storage while enabling enterprise-level features like global inline deduplication, compression, continuous data protection (CDP), and encryption at rest.

How OneXafe Works

OneXafe's file system is based on an immutable object store where every object is written only once and never modified. Any modification you make to the file system always results in the creation of new objects. OneXafe CDP takes low-overhead snapshots—a view of the file system at the instant the snapshot was taken—every 90 seconds.

Since the underlying objects are immutable and can't be changed or modified by an external source, the snapshots inherit this immutability. With the snapshots, you can go back to specific points in time and recover entire file systems in minutes, even if ransomware locks your data down.

Whether you're looking to consolidate file servers, store archival data, or deploy a disk-based backup target, OneXafe is worth a closer look.

Ready to learn more? Watch an on-demand demo or read the solution brief.

How Continuous Image-Based Backups Make Disaster Recovery Fast, Easy, and Reliable in Smaller Environments

Smaller businesses are bearing the brunt of ransomware attacks. That's the headline in a Forbes article summarizing a recent Senate Judiciary Committee meeting. Citing testimony from Justice Department Criminal Division Deputy Attorney General Richard Downing, cybercriminals don't even need to create ransomware anymore now that licensed ransomware-as-a-service (RaaS) has arrived on the (crime) scene. The Department of Homeland Security (DHS) secretary was also recently quoted, saying that about one-half to three-quarters of ransomware victims are small businesses. Combine those two revelations, and it's clear that you need to do more to prevent ransomware attacks and prepare for your small business's recovery. That starts with good backup and recovery practices. And that's where image-based backups enter the picture.

Image-Based Backup vs. Snapshots: What's the difference?

While sometimes referred to as "snapshots," image-based backup technology differs significantly from what we commonly refer to as snapshot technology. Image-based backups are, essentially, a copy of your operating system, files, executable programs, and OS configurations. When people say "snapshots," in this context, they're referring to incremental, image-based backups that only capture the changed blocks for an entire data volume.

True "snapshot" technology, on the other hand, captures a "picture" of a server, including its files, software, and settings, at a specific point in time. Snapshots are taken instantaneously, preserving your data without the need to move or copy it. That gives you a stable point in time from which to take your backup, unlike live backups where open files and active applications are changing during the backup.

While snapshot technology doesn't create true, independent backup copies, image-based backup technology does. Both have tremendous value, depending on your specific needs.

The Case for Image-Based Continuous Data Protection

While snapshot technology can be a valuable element of any backup and disaster recovery strategy, if you're part of a smaller organization, you may find continuous image-based backups to be your best choice. Arcserve ShadowProtect offers image-based backups that deliver comprehensive backup protection and reliable recovery.

Install ShadowProtect on any Windows or Linux server or desktop—physical or virtual—that you want to protect. The software quickly and efficiently captures your entire system, including your operating system, applications, settings, services, and data.

With ShadowProtect, you can take regularly scheduled backups as often as every 15 minutes and create custom full and incremental backup schedules that meet your requirements. You can easily choose where to store your backup files to any internal, removable, or network storage locations, including the Arcserve Disaster Recovery Cloud.

ShadowProtect's image-based backups monitor data at the sector level, tracking only those blocks that have changed in each sector. Application awareness ensures that you get transactionally consistent backups with an image-based snapshot of the database at a point in time. That way, committed transactions in Microsoft Exchange, SQL, and SharePoint are reflected in the database—and uncommitted transactions are not. Add it all up and it means you can count on efficient, reliable, swift backups that will be there when you need them.

Recovery Made Easy

If disaster does strike, ShadowProtect lets you restore failed servers and recover complete systems in minutes and individual files and folders in seconds from your image-based backups. All without having to restore the entire system. You can also use patented VirtualBoot technology to boot a backup image into a virtual machine instantly. With frequent, regularly scheduled backups, you'll never risk losing more than a few minutes of data so you can meet tight recovery point objectives (RPOs). ShadowProtect also lets you run automated, easy-to-execute verification of your backup images, so you can be sure your backups will work when a disaster strikes.

Image-Based Backups Are Just the Beginning

Image-based backups that offer continuous data protection may be the best option for your small business. But every business—large or small—is different and has different needs. Watch this on-demand demo to learn more about your options for recovering quickly, easily, and reliably.

Why You Need Unified Data Protection and How to Get It

The frequency of ransomware attacks continues to soar. Global attack volume jumped up 151 percent, year over year, in the first six months of 2021. In absolute numbers, SonicWall's 2021 Global Cyberattack Trends report says there were 304.7 million ransomware attacks over the same period. In the past, data protection, recovery, and security have been treated as separate IT security efforts. But this intense battle demands that IT pros start looking at IT security from a new perspective.

That transformation is already underway. An IDC white paper, "Increase Data Resilience and Improve Ransomware Defense by Integrating Data Protection and Security," cites a recent study where 78 percent of IT leaders indicated digital resilience would be a top investment priority over the next two years. IDC's research also shows that 90 percent of organizations operate in a hybrid cloud or multi-cloud environment, with their data spread across multiple private and public cloud locations. Protecting data that is now everywhere requires comprehensive data protection solutions.

Key Data Protection Capabilities?

The IDC white paper says that IT leaders should no longer consider data security and data protection as separate tasks. That means you need a multi-cloud data management platform that covers data protection, cyber-recovery, and disaster recovery. The best platforms often extend beyond data protection and recovery to include data capture, movement, and governance across the core, cloud, and edge.

These platforms include a policy engine that ensures consistent data treatment—regardless of the repository—while slashing the time it takes IT to manage data. IDC also says that any solution you choose should be extensible to integrate with other solutions, like intrusion detection and the ability to scale as your organization grows.

When evaluating the right data protection platform for your situation, IDC recommends that it include these key capabilities:

Ensure Encryption Everywhere

The solution you choose should encrypt data at rest, in flight, and in backup sets to prevent data exfiltration and theft by external and internal threats

Include Immutable Data Backups

Encrypted, immutable data copies can't be corrupted, changed, or deleted by anyone, whether internal or external, except those using unique processes. That ensures your data will survive an attack. So look for immutability as a highly critical feature for your backups.

Keep An Air-Gapped Backup Data Copy

An air gap that physically isolates an immutable backup copy of your data keeps it safe from unsecured networks, like the internet, preventing bad actors from gaining access. And make sure that you separately manage your control path and data path to reduce the chances that your data will be compromised. Many organizations are turning to tape backups—where the tapes are physically removed from the tape library, onsite or offsite, to provide this air gap.

Find An Integrated Solution

Look for a solution that seamlessly integrates hardware, software, and cloud capabilities. That gives you a layered approach to data protection and cyber security. And it gives you your best chance of surviving a cyberattack.

Insist On MFA

Many breaches are the result of stolen credentials. IBM's Cost of a Data Breach Report 2021 says today's most frequent initial attack vectors are compromised credentials, at 20 percent of breaches, followed by phishing, at 17 percent of breaches. Multi-factor authentication (MFA) can help prevent breaches, even if someone's credentials are compromised.

Unified Data Protection: Backup and Recovery Across Platform

Arcserve and Arcserve, an Arcserve company, offer Arcserve Unified Data Protection (UDP) software to give you an all-in-one data and ransomware protection solution. This solution neutralizes ransomware attacks, restores your data, and performs effective disaster recovery (DR). Safeguarded by Sophos Intercept X Advanced cybersecurity, Arcserve UDP uniquely combines deep-learning server protection, immutable storage, and scalable onsite and offsite business continuity. That gives you a multi-layered approach that delivers complete IT resiliency for your virtual, physical, and cloud infrastructures.

arcserve® UDP

Get the Scoop on UDP

Contact us today if you're ready to learn more about Arcserve UDP and other Arcserve data protection solutions. Arcserve is always here—standing by and ready to help.

arcserve®

+1 844 639-6792
arcserve.com

About Arcserve

Arcserve, a global top 5 data protection vendor, provides the broadest set of best-in-class solutions to 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, cloud (including DRaaS, BaaS, and Cloud-to-Cloud), hyperconverged, and edge infrastructures. The company's nearly three decades of award-winning IP, plus a continuous focus on innovation, means that partners and customers, including MSPs, VARs, LARs, and end-users are assured of the fastest route to next-generation data workloads and infrastructures. A 100% channel-centric organization, Arcserve has a presence in over 150 countries, with 19,000 channel partners helping to protect 235,000 customers' critical data assets. Explore more at arcserve.com and follow @Arcserve on Twitter.