arcserve®

How Unified Data Protection, Immutable Storage, and Tape Backups Ensure Data Loss Prevention and Disaster Recovery

Table of Contents

Sophos Report Finds Hackers Can Breach Active Directory in Hours: Are Your Data Protections Doing Enough?

Arcserve partner Sophos recently posted its midyear Active Adversary report and noted that ransomware hackers took a median time of just 16 hours to gain access to Microsoft Active Directory.

With Active Directory (AD) in use by nearly 75,000 customers and holding a market share of 24 percent, this news should be a call to action for every IT pro whose organization relies on this software.

The report says that hackers try to move laterally to AD servers as soon as possible once they gain access. An AD server is usually a network's core component and can control identity and policies across your organization. Once they gain access, hackers can leverage accounts with admin privileges, create new accounts, and disable legitimate accounts. Even worse, they can use the AD servers' role as a trusted source to deploy malware.

Ransomware Protection Is Priority One, But Not the Only One

The report found that 68 percent of attacks involved ransomware. Network breaches came in a distant second at 18 percent. It also notes that most AD servers are only protected with Microsoft Defender—or not at all. Hacker groups targeting AD with widespread—and highly successful—ransomware families like LockBit 2.0 and BlackMatter spotlight the need for better ways to protect AD from ransomware.

A Cybersecurity and Infrastructure Security Agency (CISA) advisory says that LockBit was the most deployed ransomware variant worldwide in 2022 and is still going strong in 2023. CISA recommends implementing mitigations to improve your organization's defenses against this ransomware operation proactively. Needless to say, those defenses should protect against all ransomware variants.

But there are plenty of other threats—from internal attacks by a disgruntled employee to hardware failures to natural disasters. So, it makes sense to address all of these threats to safeguard your AD environment and your precious data. That's why data resilience matters most.

Data Resilience Delivered

Arcserve's Unified Data Protection (UDP) solution is built on three pillars: prevent, protect, and recover.

Prevent

Arcserve UDP features powerful prevention capabilities with integrated Intercept X Advanced from Arcserve partner and leading cybersecurity solutions provider Sophos. This security solution employs deep learning to predictively prevent attacks, detecting known and never-before-seen threats and unknown malware without relying on signatures.

Sophos Intercept X Advanced also features WipeGuard, which stops malicious processes and protects the master boot record (MBR) from being encrypted. It also prevents the overwriting of critical structures. And it includes CryptoGuard, which monitors your system for processes that begin encrypting files. If CryptoGuard detects behavior like ransomware, it stops the detected running processes and restores the impacted files.

Protect

For your Active Directory deployment, Arcserve UDP delivers protection against data loss and extended downtime. That includes on-premises protection for Microsoft 365 workloads on-premises. Arcserve UDP also supports immutable storage, a write-once-read-many-times format that ensures the stored data can't be altered or deleted, even by admins. So your backups are always protected—whether on-premises or off-premises—using either Arcserve OneXafe immutable network-attached storage or the supported Amazon Web Services (AWS) Object Lock in the cloud.

Arcserve UDP furthers data protection with simplified authentication and access control that relies on centralized user account management. Authentication features include multi-factor authentication (MFA) and role-based access controls (RBAC) that keep unauthorized users out.

Recover

If (or more likely, when) the time comes that you need to recover your data, Arcserve UDP reduces your downtime from days to minutes and validates your recovery time and recovery point objectives (RTOs/RPOs) with included Arcserve Assured Recovery software. Assured Recovery ensures reliable recovery with fully automated and non-disruptive disaster recovery (DR) testing. You can also schedule automated disaster recovery tests, test business-critical systems, applications, and data in a sandbox, and test backups in real time.

Arcserve UDP replicates backup data by saving it as recovery points. Each time Arcserve UDP performs a successful backup, a point-in-time snapshot image of the backup is created, enabling you to locate and specify precisely which backup image you want to restore.

Another vital feature of Arcserve UDP is orchestrated recovery. Orchestrated recovery gives you a systematic, coordinated process for shifting critical IT systems, data, and applications from on-premises infrastructure—such as Active Directory—to other resources.

Protect Your Active Directory Deployment

Arcserve technology partners can guide you to the best solutions for your needs. That includes your on-premises Active Directory deployment and any other data protection concerns you need to address.

Find an Arcserve technology partner.

To learn more about Arcserve UDP, request a demo or check out our 30-day free trial offer.

How Immutable Backups Safeguard Against Sophisticated AI-Driven Cyberattacks

The use of artificial intelligence is exploding, with Grand View Research projecting the global AI market will expand at an impressive 37.3% CAGR between 2023 and 2030.

While that creates incredible opportunities for improved productivity and innovation, we've all heard about the dark side of AI. A recent CNBC article was headlined, "The generative AI battle between companies and hackers is starting."

Actually, the battle is already well underway. Check Point Research released its 2023 Mid-Year Security Report, noting that "the misuse of AI has escalated, as attackers use generative AI tools for phishing emails, keystroke monitoring malware, and basic ransomware code." The report also revealed an 8 percent "surge" in global weekly cyberattacks during Q2, the most significant increase in two years.

It's important to note that, in addition to all these threats to your primary data, your backups are also a primary target for ransomware attacks. Hackers know that if they can encrypt your backups, they can prevent your organization from recovering. And that means you're much more likely to pay the ransom.

Hackers will find new attack methods as AI—and their skills in using it—become increasingly sophisticated. Your preventive cybersecurity solutions may not be enough to stop these evolving attacks. This means you must protect against ransomware and data loss by ensuring data disaster recovery—whether an attack is AI-driven or just a phishing ploy by a solo hacker.

New Threats Demand Immutability

You're familiar with the 3-2-1 backup strategy, which has been around since 2009. While that was a great start, ensuring data resilience in your organization today requires implementing modern data protection best practices, including the 3-2-1-1 backup strategy. That added "1" in the 3-2-1-1 strategy represents immutability.

When your backups are placed in immutable storage, they are saved in a format that unauthorized users can't change or delete. That includes backups stored in the cloud using Amazon S3 Object Lock.

Employ Unified Cloud Data Protection Against AI

Arcserve UDP, a single platform that simplifies cloud data protection, starts with prevention. The software safeguards your data with Sophos Intercept X Advanced cybersecurity. Sophos Intercept X employs deep learning that predicts and prevents attacks and includes CryptoGuard to prevent unauthorized file encryption, among other unique capabilities. But even if hackers—or a disgruntled employee—find a way around these leading-edge protections, Arcserve UDP software ensures the immutability of your data backups when combined with cloud storage that employs Object Lock or similar means.

Get Help from Data Protection Experts

Arcserve technology partners work with organizations of every size and stripe. They can help you understand your organization's unique requirements and guide you in implementing data protections—including immutable storage—that ensure your data can always be recovered.

Find an Arcserve technology partner.

To learn more about Arcserve UDP, request a demo.

Not Dead Yet: Why Tape Is Still a Valuable Data Loss Prevention Technology (and a Growing Market Segment)

Tape has been around forever, at least in relation to most technologies. TechTarget says that, if you count paper tape, the technology has been around since the 18th century. But the modern era of tape still goes back more than seven decades to 1951, when UNIVAC introduced the UNIVSERVO tape drive.

So you may be surprised to hear that tape is still alive and well. And its use is expanding significantly. How much? The tape market is projected to reach $9.39 billion by 2030, a 7.5 percent CAGR. And some analysts report that up to 80 percent of mid-size and enterprise companies use tape.

There are plenty of reasons for that growth. Here are just a few.

LTO-9 Delivers More Capacity, Faster Data

The Linear Tape Open (LTO)—and LTO-9, the latest format specification for LTO Ultrium tape drive and media—has much to do with that growth. TechTarget says tape continues to set shipment records. And it notes that much of that growth can be attributed to customers looking for secure, cost-effective data backup solutions.

With LTO-9, you can choose an 18 TB tape cartridge, yielding a 50 percent capacity increase over LTO-8 and a 1,400 percent increase over the decade-old LTO-5 technology. And LTO-9 delivers 400 MB/s native transfer speeds and 1,000 MB/s when employing 2.5:1 compression.

LTO-9: Immutable Storage, Backward Compatibility

This latest iteration of the LTO technology includes multilayer security support with hardware-based encryption. LTO-9 also supports immutable storage, a write-once-read-many times (WORM) format that unauthorized users can't alter or delete. That means your backups are protected from ransomware, even if hackers get past your defenses.

LTO-9 offers full backward read and write compatibility with LTO generation 8 cartridges. It also provides a scalable, adaptable open tape storage format. That makes tape an attractive investment when considering primary archival and data protection solutions.

Tape Delivers Air-Gapping and a Much Lower TCO

Ransomware attacks are now so frequent and sophisticated that it's not a matter of if but when your company will be hit. That's why Arcserve recommends tape as a cost-effective option for air-gapping your backups. You can learn more about physical and virtual air-gapping in this recent post.

Fujifilm offers a total cost of ownership (TCO) calculator illustrating how cost-effective tape can be. The default example shows how an organization that

- loads 20 petabytes (PB) in year one

- projects 30 percent annual growth in stored data

- and 12 percent of its data each year will need to be retrieved

will save 79 percent versus disk storage and 72 percent versus cloud storage. That is some serious savings.

Tape Is Incredibly Reliable

Ultrium LTO says that LTO-9 delivers better than one uncorrectable error event in 1020 user bits in the data reliability category. Typically referred to as uncorrectable error rate, or UBER, that translates into at least 17 nines of durability.

UBER is a crucial data reliability metric for all data storage devices—hard disk drives (HDDs), solid-state drives (SSDs), and tape. An LTO-9 analysis of user data reliability noted that "due to LTO's unique format, which is based on orthogonal interleaved 2-dimensional 32 channel Reed Solomon error correction codes, the probability of an UBER event is orders of magnitude lower than HDD."

Here's another way to look at HDDs vs. tape. In the LTO-9 analysis example, the HDD would experience an UBER about every 125 terabytes or every 7 HDDs. LTO-9 technology would only experience an UBER every 12.5 zettabytes, which is 12.5 billion terabytes or almost 700 million LTO-9 cartridges. That's a lot of storage with little risk of errors.

Powerful, Proven Tape Backup Software Closes the Deal

Given how long tape has been around, many IT pros assume the technology hasn't kept pace with our evolving digital environment. That isn't so. Arcserve Backup software can greatly enhance your tape data protection strategy. Here's how:

Centralized Data Management, Sophisticated Functionality

Arcserve Backup offers centralized data management and storage resource manager (SRM) reporting. The software monitors the status of all backup activities, finds the nodes that are taking the longest, locates backed-up data, and tracks volume, disk, and memory usage on every production server.

Arcserve Backup lets you incorporate sophisticated functionality into your VMware, Microsoft Hyper-V, and Citrix XenServer platforms. That includes simplified system management with a view of your entire environment to mitigate the risk of data loss on virtualized servers.

Fast, Efficient Backups and Restores

The software further increases reliability with smart restore capabilities that redirect restore jobs to other media containing the same data without manual intervention. You can also quickly restore individual application objects from Active Directory, Microsoft Exchange, Microsoft SQL Server, and Microsoft SharePoint.

With Arcserve Backup, you'll realize faster, more efficient backups and restores by leveraging UNIX and Linux data movers for SAN-based backups. You'll also be able to meet application-specific requirements including:

- Backup to disk
- Backup to tape
- Disk-to-disk-to-tape (D2D2T)
- Disk-to-disk-to-cloud (D2D2C)
- Virtual tape library (VTL)
- Hardware snapshot support
- Multiplexing
- Multi-streaming

Take a Closer Look at Tape

Working with an Arcserve technology partner, you can evaluate how tape fits into your backup and disaster recovery strategy. They have the expertise to guide you to the optimal solutions to meet your requirements.

Find an Arcserve technology partner.

Need Answers?

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

arcserve®

+1 844 639-6792

arcserve.com