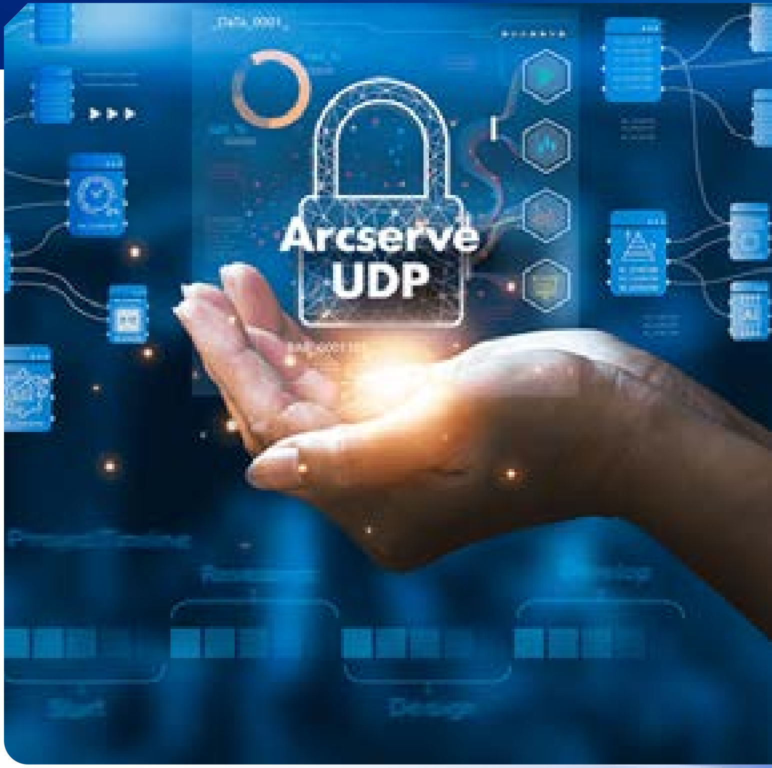
arcserve®

A Deep Dive Into Arcserve Unified Data Protection (UDP): Achieving Data Resilience

Table of Contents

Elevating Excellence: Arcserve UDP Updates Bolster Ransomware Resilience, Availability, and Recovery



We recently shared the highlights of a review by industry analyst DCIG calling Arcserve Unified Data Protection (UDP) "The Obvious Solution to Simplify Data Backup and Defeat Ransomware."

That recognition speaks directly to our focus on offering cost-effective, agile, and massively scalable best-in-class solutions that eliminate the complexities of managing, protecting, and recovering all data workloads across all data environments.

Safeguarded by Sophos Intercept X Advanced cybersecurity, Arcserve UDP uniquely combines deep learning server protection, immutable storage, and scalable onsite and off-site business continuity to support your data resilience strategy.

A critical component of Arcserve's Unified Data Resilience Platform, Arcserve UDP delivers complete ransomware resilience for protected data and multilayered protection for priceless digital assets.

Here's what you can expect from Arcserve UDP, including recent updates and improvements.

Cloud-Based Management Console Adds Flexibility

Based on your needs, you can now manage Arcserve UDP with either the on-premises private management console or the cloud-based management console. Long used on-premises by IT pros, the private management console is a good choice if your environment requires a private setting. The cloud-based management console is perfect if you need more flexible controls, such as multitenancy.

Multitenant management is simplified with the cloud-based management console. You can easily configure sub-organizations and manage them like different tenants as well as separate workloads into different domains for easier management.

Enhanced Security

Cloud Console protects data with a robust authentication system that uses Okta user authentication services. Okta's zero trust implementation employs multifactor authentication (MFA), adding strong restrictions for countering account takeovers during ransomware attacks. Centralized user account management using Arcserve Identity Services also greatly simplifies authentication and access control.

With Google and Microsoft having deprecated and no longer offering support for basic authentication, Arcserve UDP now offers improved security via Open Authorization (OAuth). And Arcserve UDP's email alerts can now secure communications using the recommended authentication type by providing you the option to use OAuth for Microsoft 365 and Google Cloud. Arcserve has also further tightened security with upgrades to newer versions of critical third-party components.

Amplified Availability, Durability, and Scalability

Arcserve UDP delivers availability-oriented protection to support always-on businesses, and a recent update now boosts data availability with support for generation 2 virtual machines (VMs) on Microsoft Azure, which are purported to deliver higher performance with much-improved security. And Virtual Standby support lets you quickly spin up these VMs, offering immediate access to your data and applications.

With Arcserve UDP, you can store deduplicated backups directly on cloud object storage, including AWS, S3, Wasabi, or Google Cloud Storage. You'll also realize lower TCO and enhanced disaster recovery support with cloud-based offsite safe stores. New functions include the ability to copy data to another data store and virtual standby, which converts recovery points to virtual machine formats and prepares a snapshot to make data recovery easy. Both are available for use from datastores configured in AWS S3 or other object storage systems. Virtual standby also provides high availability capabilities so the virtual machine can take over immediately when the source machine fails. Both are available for use from datastores configured in AWS S3 or other object storage systems.

Reliable Recovery and Improved Backup Efficiency

Arcserve UDP offers fully automated and nondisruptive disaster recovery (DR) testing that is secure and reliable, so you can be confident you can recover your data. It's simple to schedule automated disaster recovery tests and provide advanced reporting for stakeholders. And you can save backup storage space by removing unnecessary recovery points created for tests or other cases that used manual jobs and are no longer relevant.

You can also count on reliable backup job processing, with jobs marked incomplete if the execution encounters relevant warnings that require your attention but aren't critical enough to cause the job to fail.

Easy-to-Use Interface, Detailed Reporting, and Improved Compliance Support

With Arcserve UDP, no extended configuration is required. The intuitive interface—with an informative dashboard viewable at a super admin or tenant level—also offers multilingual support for Cloud Console so you can provide a localized user experience.

The one-view dashboard offers per-tenant reporting, detailed information, and insightful reports regarding protection status. Retention compliance is supported by the ability to label a manual job as 'Daily,' 'Weekly, or 'Monthly' in case the scheduled job can't create a retention point. And a Backup Success Rate Report offers critical insights, with protection status depicted at a source level or policy level, with more options for daily, weekly, and monthly backups.

Strengthened Enterprise Application Support

Arcserve UDP delivers strong application-aware protection for enterprise applications such as Oracle Databases and Microsoft SQL Server. You may store petabytes of data critical to your business in these applications. Arcserve UDP uses agentless backup methodologies specific to applications, eliminating stress on your production systems and allowing unfettered access to source systems.

Learn More About Arcserve UDP

While Arcserve UDP is "The Obvious Solution to Simplify Data Backup and Defeat Ransomware," expert help can make the difference when improving your organization's data resilience and disaster recovery capabilities. Talking to an Arcserve technology partner is an excellent way to get answers to your most pressing questions.

Find an Arcserve technology partner here. And be sure to check out our Arcserve UDP 30-day free trial offer or learn more by requesting a demo.

5 Ways to Ensure Data Resilience in Cloud Computing

The global cloud computing market is projected to more than double—from $546 billion to $1.2 trillion—between 2022 and 2027. That's a nearly 18 percent CAGR. And Arcserve's annual independent global research found that 82 percent of IT decision-makers expect an increase in hybrid cloud investments, and 70 percent expect an increase in multi-cloud investments.

So, if you're an IT leader, cloud computing probably plays an essential role in how you support your organization. That's no wonder, given that hybrid cloud and multi-cloud infrastructures offer flexibility and agility by letting you mix and match cloud environments based on your needs. That can range from choosing a cloud environment based on performance optimization for different specific workloads to tapping into leading-edge and best-of-breed services, tools, and technologies that cloud providers offer.

Data Resilience and the Shared Responsibility Model

The Arcserve global study also spotlighted a frequent misconception regarding who is responsible for your data, with 43 percent of IT decision-makers saying they believe cloud providers are responsible for data stored in public clouds. That's unfortunate because TechTarget notes that the cloud customer is always responsible for securing their data and workloads under the shared responsibility model.

Meanwhile, a 2022 Sophos report found that those using the cloud for infrastructure as a service (IaaS) experienced a significant increase in cyberattacks in the prior year, with 56 percent experiencing an increase in the volume of attacks on their organization and 67 percent reporting that they had been hit by ransomware.

The numbers make it plain that you need to do more to ensure data resilience in your cloud computing deployment. Here are five ways you can do so.

1. Keep Your Backup and Disaster Recovery Plan Up to Date

Preparation is crucial if your organization is going to survive any hit to your cloud data. Schedule reviews of your backup strategy and processes and your disaster recovery plan. You'll find a step-by-step guide to creating a disaster recovery plan in this blog post. Once your plan is up to date, test it to ensure it will work when needed. And adhere to the 3-2-1-1 backup strategy. That includes keeping one backup in immutable storage, a write-once-read-many-times format that can't be altered or deleted.

A robust incident response plan also bolsters data resilience. So, whether it be a security breach, a hardware failure, or some other unexpected event, you'll have a process in place to quickly detect, respond to, and recover from any disruptions.

2. Build Redundancy and High Availability Into Your Infrastructure

Building data resilience in cloud environments demands redundancy. That goes back to the 3-2-1-1 rule, which is all about ensuring your data and applications are backed up in multiple locations—with one of those backups saved in immutable format. Hence, it's always accessible, even if a hardware failure, natural disaster, or cyberattack strikes you. By distributing workloads and backups across multiple locations, you mitigate those risks, ensuring high availability.

3. Strengthen Your Cybersecurity and Data Protection Defenses

Achieving data resilience can be simplified by combining cybersecurity and data protection into a single, integrated solution. That's precisely what Arcserve Unified Data Protection (UDP) and Arcserve Cloud Hybrid deliver. These Arcserve solutions include Sophos Intercept X Advanced for Server, which protects your backup infrastructure by effectively neutralizing malware, exploits, and ransomware with AI-based endpoint protection.

It's also essential to regularly assess your cybersecurity and data protection efforts to identify vulnerabilities and ensure you can combat the latest threats. Because cybercriminals are always looking for the most accessible entry points to hack into your systems, ensure all your software and hardware are patched as soon as updates are released.

4. Employ Monitoring and Analytics to Identify Threats, Anomalies, and Performance Problems

Consistent monitoring is essential for maintaining data resilience in highly available architectures. It's worth investing in effective monitoring tools that give you insights into how your systems perform and inform you of security threats and potential anomalies. Here again, leveraging AI and machine learning can help you identify patterns and detect potential issues before they become big problems. And consistent monitoring ensures your IT team can quickly respond to any incident, reducing downtime and preventing data loss.

5. Talk to the Data Resilience Experts

Most IT teams are kept busy today, just running operations smoothly and putting out fires. But, given the high probability that some cloud data disaster will hit your organization, no matter the cause, it's worth talking to people who are laser-focused on delivering data resilience to their customers. That's precisely what Arcserve does. To talk to a data resilience expert, contact us.

And get expert IT guidance by choosing an Arcserve technology partner here. Or request a demo to find out how Arcserve solutions deliver data resilience across your hybrid cloud, multi-cloud, private cloud, on-premises, and off-premises infrastructures.

5 Steps Every Organization Should Take to Bolster Data Resilience (and Why #5 May Matter Most)

In a recent Solutions Review *Expert Insights* interview with Arcserve Vice President, Sales Engineering, North America, Shawn Massey shared his perspectives on the data risks that organizations everywhere face today and the five steps they should take to ensure data resilience.

The conversation shed light on two major concerns: the growing sophistication of cyber threats and the failure of organizations to prioritize data resilience.

Let's look at these two issues and the five steps you should take to ensure your data is safeguarded, and your organization can recover from any disaster.

1. Know Your Data

Your data is precious. Without access to it, your operations likely come to a screeching halt. That's why it's vital that you understand the value of all your data, where it is stored, and where and how it is backed up. Failure to do so can leave your organization vulnerable to ransomware, data loss, and the inability to recover.

Massey says to start with an inventory and classification of your data. That includes on-premises, off-premises, remote locations, and the cloud. Then use data tiering, as we describe In this post, to help you cost-effectively store and manage the flood of data being generated. That includes data generated by SaaS applications—the lifeblood of many businesses today. With visibility into its sensitivity and importance, you can prioritize data protection efforts based on your data's value and risks.

2. Protect Against Sophisticated Cyber Threats

Cybercriminals keep getting craftier as they seek new ways to find vulnerabilities and penetrate your defenses. The 2023 Verizon Data Breach Investigations Report found that 74 percent of all breaches involve the human element—errors, stolen credentials, and clicking on suspicious links, for example. And the same report found that 24 percent of breaches were ransomware.

In the interview, Massey points out that bad actors now leverage advanced techniques targeting specific organizations rather than casting a wide net. He notes that ransomware attacks, in particular, have become more targeted, focusing on sectors that include manufacturing, education, government, and healthcare, adding that when attackers infiltrate networks, they try to time their attacks for maximum impact. That translates into grave risks for organizations that haven't kept their data protections up to date.

Massey recommends that you implement a comprehensive approach to data resilience. That includes conducting regular risk assessments that identify potential threats and vulnerabilities, putting proper mitigations in place, adding or updating firewalls, and implementing identity access management (IAM) controls, intrusion detection systems (IDS), and other security technologies.

3. Train Your Team

With such a large percentage of breaches involving humans, it's common sense that you enlist your team's help with data protection. Educate your people regarding cybersecurity best practices, how to recognize and respond to potential threats, and the importance of using strong passwords. Regular training sessions, awareness campaigns, and ongoing testing can go a long way toward ensuring your organization is protected from ransomware, phishing, and other attack vectors.

4. Implement Continuous Monitoring and Response

Constant monitoring and a proactive response to emerging threats help stop attacks before they become disasters. Massey says that organizations should implement robust monitoring tools and technologies that provide real-time visibility into their IT infrastructure, network traffic, and user activity.

This gives you the ability to detect suspicious activities early on and respond quickly to contain and mitigate potential breaches. Regular security audits and vulnerability assessments can also help you identify and address weaknesses in your organization's security posture.

5. Invest In Effective Backup and Disaster Recovery Solutions

Massey points out that, first and foremost, your organization needs to update its disaster recovery plan to align with your data protection strategy, including your RTOs and RPOs.

But you need more than a disaster recovery plan. You also need a robust backup and recovery solution that ensures your data is always available and can be rapidly recovered if you suffer a ransomware attack, system failure, or other data loss. Solutions like Arcserve Unified Data Protection (UDP) deliver all-in-one data protection for on- and off-premises workloads, with your data safeguarded by Sophos Intercept X Advanced cybersecurity.

The software uniquely combines deep-learning server protection, immutable storage, and scalable onsite and offsite business continuity for a multilayered approach that delivers complete IT resiliency for virtual, physical, and cloud infrastructures.

And Arcserve UDP protects SaaS workloads like Microsoft 365 and a broad range of platforms, from Windows to Amazon EC2, Oracle Database to VMware.

It All Adds Up to Data Resilience

While all five steps Massy lists are crucial to ensuring your data is protected and available, number five may matter most. Because if your defenses are breached—and you can't recover your data—you may not even have a business.

Watch the full Solutions Review interview with Shawn Massey here.

For expert help with choosing and implementing the best data resilience strategy for your organization, choose an Arcserve technology partner. To learn more about Arcserve UDP, schedule a free demo.

Industry Analyst DCIG's Arcserve UDP 9 Review: The Obvious Solution to Simplify Data Backup and Defeat Ransomware

Like most, your organization is probably challenged by the IT complexities and threats that are pervasive today. That's especially true regarding protecting against ransomware, managing backups, and ensuring disaster recovery.

Now, a comprehensive review of the Arcserve Unified Data Protection (UDP) 9 backup solution—conducted by independent research firm DCIG—confirms what we already firmly believed: Arcserve UDP 9 offers your organization a clear edge in protecting against ransomware while tackling the persistent challenges of managing backup and recovery complexities.

The product review notes that four core challenges and threats facing organizations today:

- Lack of a centralized backup console
- Need for multiple backup administrator roles
- Vulnerable Identities of IT personnel
- Lack of sophisticated backup and recovery features

Arcserve UDP 9 answers these challenges simply and effectively. "Arcserve UDP has for some time delivered advanced data protection features at its core that organizations routinely use," said Jerome Wendt, CEO and lead data protection analyst at DCIG, regarding Arcserve UDP's multiple backup and disaster recovery capabilities. "Arcserve offers both agent-based and agentless backup options, which give organizations the flexibility to use the best backup approach to meet specific application data protection requirements."

Powerful Ransomware Prevention and Strengthened Data Resilience

Arcserve UDP 9 delivers a cloud-based, multi-tenant Cloud Console that enhances protection of enterprise applications such as Oracle and Microsoft SQL Servers by centrally managing UDP and Cloud Direct. The solution includes architectural and user interface enhancements to improve performance and simplify management.

UDP also enhances data resilience, availability, and durability through its support for multiple cloud object storage providers. These features, combined with Arcserve's existing integration with Sophos, provide you with a reinforced beachhead against ransomware threats.

Arcserve UDP offers multiple disaster recovery options, including DRaaS, Instant Restores, and Virtual Standby (VSB). DRaaS is available via its fully managed cloud services extension, Cloud Hybrid. This DRaaS service keeps critical data and workloads protected offsite and available and positions organizations to continue operations during or after unplanned on-premises outages.

The Instant Restore feature allows IT personnel to spin up a VM directly from a backup quickly. At the same time, VSB offers a highly available configuration for data and applications for even faster recoveries than its Instant Restore feature.

A Strong Backup Solution Is a Must-Have

“As ransomware attacks become more sophisticated and frequent, a weak backup solution is no longer an option. With Arcserve UDP 9, organizations empower themselves to defend against the latest ransomware threats and overcome the complexity inherent in IT environments,” said Patrick Tournoy, executive vice president of operations at Arcserve. “DCIG's review confirms that Arcserve UDP 9 is a robust backup solution that can effectively protect organizations against these threats.”

Take Arcserve UDP Out For a Spin

Learn how Arcserve UDP 9 can simplify your backup and disaster recovery efforts by requesting a demo. If you're ready to take it out for a test drive, check out our 30-day free trial. For expert help with implementing proper backup and disaster recovery solutions and processes, talk to an Arcserve technology partner.

Need Answers?

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

arcserve®

+1 844 639-6792
arcserve.com