arcserve®

Data Protection and Ransomware Recovery for Your Cloud, Hybrid Cloud, and Critical IT Infrastructure

Table of Contents

How the Cloud Can Simplify Ransomware Recovery

Ransomware is everywhere. Sadly, in a recent survey, 20 percent of companies reported they were attacked. It gets worse. Sophos State of Ransomware 2021 report found that 92 percent of organizations don't get their data back after a ransomware attack, even if they pay the ransom. According to the Sophos report, ransomware can ruin a business—or at least make a severe dent in its success—with the average ransomware recovery costing $1.85 million. If you're an IT pro, you are already well aware of the problem and the consequences.

But preventing ransomware is problematic. The number one ransomware attack vector is phishing, and all it takes is an employee clicking on a malicious link or downloading an infected PDF for hackers to gain entry to your systems and data. Number two on the list of ransomware attack vectors is compromised Remote Desktop Protocol (RDP) credentials. Exploitable vulnerabilities like unpatched systems and software stand at third on the list. Of course, there will always be a new attack vector you'll need to worry about. Today, ransomware even targets internet of things (IoT) devices used throughout numerous industry sectors. Fighting back starts with prevention and ends with recovery.

Take a Proactive, Multi-Layered Prevention Approach

Prevention starts with detection. Arcserve integrates cybersecurity and data protection for on-premises, cloud, and SaaS-based data, serving as your first and last line of defense against cyberattacks and data loss. Arcserve defends your backups with Sophos Intercept X Advanced, cutting-edge cybersecurity that uses a deep learning neural network to detect known and unknown malware—without relying on signatures. Arcserve also lets you quickly respond to and remove threats with CryptoGuard and WipeGuard. These technologies use behavioral analysis to stop zero-day ransomware and boot-record attacks.

Add Immutable Storage

Immutable storage—when your data is converted to a write-once, read many times format. Unlike data encryption, there is no key, so it shouldn't be possible to modify or delete the data. Using immutable storage as a backup target and sound backup practices—including following the new 3-2-1-1 backup rule—you can recover your data even if a ransomware attack is successful. Backups stored/replicated to immutable cloud storage add next-level data protection because your data is still recoverable, even if your entire system is unavailable.

Leverage the Cloud for Fast, Certain Recovery

Arcserve Unified Data Protection (UDP) offers deep cloud integration to prevent downtime and data loss, delivering an all-in-one data and ransomware protection solution to neutralize ransomware attacks. Arcserve UDP lets you quickly and safely spin up copies of your physical and virtual systems onsite and offsite or in private and public clouds. That helps you reduce downtime from days to minutes, meeting the most challenging recovery time and point objectives (RTOs and RPOs).

And Arcserve UDP gives you plenty of fast recovery options, including Virtual Standby—where virtual copies of mission-critical systems are maintained on Nutanix AHV, VMware vSphere, Microsoft Hyper-V, Amazon AWS EC2, or Microsoft Azure—and Instant VM, which makes it easy for you to spin up business-critical system backups as virtual machines on these platforms, on-demand.

Arcserve UDP also offers Assured Recovery—scheduled, automated disaster recovery tests with advanced reporting—so you can be sure recovery from ransomware is possible. You can even use granular recovery to restore individual files, emails, Active Directory objects, and SharePoint documents, and mount backups as virtual drives in Windows and NFS shares in Linux for advanced insights.

Streamline Management

With a web-based, user-friendly management console, Arcserve UDP saves time and simplifies data protection, backup management, and reporting. Role-based administration also tightens security by controlling access, while policy-based management lets you scale disaster recovery and backup effortlessly. Built-in SLA reporting helps you keep business stakeholders informed by comparing your set RTO to your recovery time actual (RTA) so you can adjust as needed.

Focus on What Matters

With Arcserve UDP, you can spend less time on data protection and backup management and more time focusing on strategic initiatives that drive your business forward. Want to learn more about how Arcserve UDP can help you protect and manage your entire infrastructure? Take advantage of our 30-day free trial or contact us to talk to an Arcserve data protection expert.

How Hybrid Cloud Data Protection Makes a Difference When Disaster Strikes

All kinds of challenges come with a hybrid cloud computing strategy. But that isn't stopping its adoption. That's because a hybrid approach gives you the flexibility to take advantage of the specific benefits private clouds, public clouds, and on-premises resources deliver for your enterprise. And you can adapt as your needs change. It's no wonder then that the hybrid cloud market is expected to grow at a robust 17.6% CAGR from 2021 through 2026.

Cybersecurity Is Still a Big Concern

First, the good news. The Cost of a Data Breach Report 2021 says hybrid cloud had the lowest average total cost of a data breach compared to public, private, and on-premises cloud models. The bad news? The average cost of a breach in a hybrid cloud environment is a whopping $3.61 million. But the really bad news is that 85 percent of breaches involved the human element, and 40 percent of organizations have suffered a cloud-based data breach. Preventing humans from being, well, human, simply isn't possible, and that includes cybercriminals. So, how can you protect your data and ensure business continuity across your hybrid infrastructure?

An Integrated Solution Is the Answer

Arcserve Unified Data Protection (UDP) Cloud Hybrid secured by Sophos gives you a fully integrated cloud backup, cybersecurity, and disaster recovery extension to Arcserve data protection software and appliances. UDP lets you create a cohesive data security, protection, and retention strategy. And if the worst does happen—whether it's a ransomware attack or natural disaster—UDP lets you quickly deploy cloud-based backup and disaster recovery (DR) to public and private clouds.

Combined with Arcserve UDP software and appliances, Arcserve UDP Cloud Hybrid automatically replicates your data and backups from an on-premises Arcserve UDP recovery point server (RPS) to a corresponding RPS in the cloud. Integrated Sophos Intercept X Advanced cybersecurity protects cloud workloads from threats using a deep

learning neural network to identify known and unknown threats. This artificial intelligence (AI) effectively neutralizes malware, exploits, and ransomware. Included signature-based protection defends against common threats, and ransomware attacks on backup data are blocked with CryptoGuard while boot record attacks are prevented with WipeGuard.

You chose a hybrid cloud strategy because of the flexibility it offers. Arcserve lets you retain that flexibility while making it possible for you to keep your business running in the face of almost any disaster.

Look for Comprehensive Cloud-Based Protection

Arcserve UDP Cloud Hybrid gives you added peace of mind by protecting your data in SSAE 18-, SSAE 16-, and ISAE 3402-certified data centers with full 256-bit AES encryption of data at the source, in flight, and in the cloud. SOC 1 Type 2 and SOC 2 Type 2 reports for Arcserve Cloud data centers are available on request. You also get remote virtual standby for emergency application failover, and failback to the cloud with manually triggered failover to remote resources and instant VM recovery.

You can even restore files, folders, and workloads with ease and manage the entire backup process from the UDP console, specifying the backup source, destination, and retention policies. And you can be confident in your recovery capabilities because Arcserve UDP Cloud Hybrid lets you confirm your RTOs, RPOs, and SLAs with fully automated DR testing and application-level recovery, and RPO and SLA validation.

Software That Keeps Things Simple

You can count on Arcserve UDP software because it has been battle-tested in the most challenging IT environments. It supports cloud, physical servers, and VMs running Windows and Linux-based applications, Office 365, vSphere and Hyper-V, and Nutanix AHV hypervisors in the cloud. The software lets you quickly adapt to changing business requirements with heterogeneous protection for workloads on-premises or in private and public clouds, including AWS, Microsoft Azure, and Google Cloud. And simple, cost-effective subscription-based licensing helps you keep your budget under control.

Protect Your Hybrid Cloud Environment

Take the next step and find out how Arcserve UDP Cloud Hybrid can make a difference for your enterprise. To learn more, read the datasheet or contact us.

Protecting Your Critical IT Infrastructure Against Downtime, Data Loss, and Ransomware

The Uptime Institute's Annual Outage Analysis found that three-quarters of data center operators and enterprise IT managers say they have experienced an IT service outage in the past three years. Unfortunately, 42 percent of those outages were caused by human error. The human element was also involved in 85 percent of breaches. Humans aren't perfect, so there is no way to eliminate these vulnerabilities. At the same time, the Department of Homeland Security lists six natural disasters that threaten critical infrastructure. Whether it's headline-grabbing floods, tornadoes, and wildfires, or human error, threats to your IT infrastructure are everywhere.

Regardless of the cause—ransomware, malware, hardware failure, or a natural disaster—all that matters for IT pros is that you are doing everything you can to protect your infrastructure. That includes keeping downtime to a minimum and ensuring your data is protected.

Start with a Plan

Because, whatever the cause—odds are you will face downtime, data loss, cyberattacks, and ransomware attacks—the only way you can be confident your data is protected is to be sure it can be recovered. That starts with a plan. We've put together a quick guide, *How to Build a Disaster Recovery Plan*, to help you get started with disaster recovery (DR) planning best practices.

Your plan needs to cover business impacts analysis, risk assessment, and risk management. But the most essential part of your plan is DR testing. That's just commonsense. You don't want to wait for a disaster to strike to find out your plan will or won't work. Want a better reason? Organizations that have formed incident response teams and tested their incident response plans saw an average total cost of a data breach that was $2.46 million less than organizations that didn't have a team and test their plan.

Simplify and Secure Your IT Environment

One of the biggest challenges facing IT teams today—as they work to prevent downtime, stop data loss, and prevent ransomware attacks—is infrastructure complexity. Seventy-five percent of PWC's 2022 Global Digital Trust Insights survey respondents say their organizations are too complex. But those that had the best cybersecurity outcomes over the past two years are five times more likely to have streamlined operations enterprise-wide.

You can start to tame the complexity of your IT environment and secure your data with Arcserve N Series, an all-in-one backup and recovery appliance combining ransomware prevention and hyperscale design. Arcserve N Series appliances protect any type and number of workloads while reducing your RTOs and RPOs to just minutes or seconds with Arcserve's Virtual Standby and Instant VM.

Scalable HCI Made Simple

Arcserve N Series appliances combine the recovery of Arcserve Unified Data Protection (UDP) with the flexible scale-out design of Nutanix. Hyperconverged infrastructure (HCI) from Nutanix delivers high performance and flexibility, with a scale-out architecture that lets you add storage without disruption and compute capacity on the fly. Overprovisioning unnecessary storage capacity "just in case" is a thing of the past. Arcserve N Series appliances take "simple" one step further, giving you a hyperconverged secure solution from a single vendor.

Unified HCI, Backup, and DR Management

With a unified management console available via Nutanix Mine, Arcserve N Series appliances let you manage your HCI from a single pane of glass, monitor all of your backup and DR services, including physical, virtual, and cloud workloads, and quickly recover your systems and data.

AI-Powered Cybersecurity Protection

Arcserve N Series features market-leading Sophos cybersecurity for protecting the appliance. With signature-based and signatureless malware detection, an AI-powered deep learning network, anti-exploit technology, Cryptoguard anti-ransomware, and WipeGuard technologies, Arcserve N Series stops the broadest range of endpoint threats, including never-before-seen ransomware and boot-record attacks.

Take the Next Step

You need to protect your critical IT infrastructure. Considers Arcserve's integrated hardware and software solutions that simplify deployment, management, and support. Scale-out capacity lets you adjust storage to meet your evolving needs—without disruptions—and high availability with powerful data protection and security software ensures your data is safe *and* you can recover from any data disaster. Contact us to learn more.

How to Securely Manage and Protect Cloud Workloads

Gartner says end-user spending on public cloud services will exceed $480 billion in 2022. This fast growth shouldn't surprise you if you're an IT pro. With businesses being forced to evolve and adapt quickly in today's changing markets—while containing IT costs—the cloud makes much sense. First, cloud capacity is essentially limitless, offering on-demand scale that's available in an instant. Additional servers can be added to a cloud network whenever extra computing power is needed—unexpectedly high user traffic, for example—and taken down just as quickly. Data storage can be expanded or reduced on demand, too.

Innovation Through Virtualization

But the ultimate driver behind cloud adoption is the ability to leverage a fast-growing list of cloud-native technologies like containers, virtual machines (VMs), machine learning, and artificial intelligence (AI). The cloud also lets you invest in innovation instead of spending your IT time and budget maintaining and managing your infrastructure and data centers.

It's no wonder then that Gartner also predicts that by 2025 more than 90 percent of enterprises will pursue a multi-cloud infrastructure and platform strategy. And almost half of the respondents to the 2021 Cloud Adoption Survey said they plan to migrate 50 percent or more of their applications to the cloud in the coming year. The cloud will likely be part of every enterprise IT strategy at some point. But the cloud isn't perfect.

Cloud SLAs Don't Eliminate Downtime Completely

Public cloud service providers offer robust security measures, and most provide service level agreements (SLAs) that ensure 99.99 percent uptime. While that sounds great, that .01 percent translates to almost an hour of downtime per year. And 44 percent of firms that responded to ITIC's 12th Annual 2021 Hourly Cost of Downtime Survey indicated that hourly downtime costs can exceed $1 million to $5 million. Recent

headlines confirm the problem is real. Amazon Web Services (AWS) recovered from its third major outage just last week. That reality combined with those high costs makes a case for adding another level of data protection for cloud workloads.

Cloud-Enabled Data Protection Makes the Difference

What's needed is a way for you to take advantage of all the benefits of the cloud while limiting your risks. That means taking data protection to the next level with multi-cloud and cross-cloud backup, disaster recovery, and high availability. And that's precisely what Arcserve's Business Continuity Cloud delivers. Powered by a unified, cloud-based management interface, Arcserve Business Continuity Cloud lets you protect your entire IT ecosystem—on-premises and in the cloud. Here are some of Arcserve Business Continuity Cloud's key benefits:

Prevent Downtime

Even complex, multi-generational IT infrastructures are protected from data loss and downtime with the only integrated cloud-native, cloud-based, and cloud-ready business continuity data solution.

Meet Stringent SLAs

With Arcserve Business Continuity Cloud, you can reduce your recovery time and recovery point objectives (RPOs, RTOs) to seconds and meet your SLA commitments.

Automate Testing

The best way to be confident of recovery after a data disaster is to test and validate your ability to recover ahead of time. Arcserve Business Continuity Cloud automates testing and provides granular reports to key data protection stakeholders.

Securely Migrate Data and Scale

Safely move large volumes of data to and from the cloud—without draining bandwidth. And you can quickly scale and pay-as-you-grow without adding more tools or management interfaces.

Restore Data Immediately

Arcserve Business Continuity Cloud lets you immediately restore access to critical systems and applications after an outage or disaster—including after a successful ransomware attack.

Ensure Corporate Compliance

With Arcserve Business Continuity Cloud's built-in compliance capabilities, legal discovery and audits are simplified.

The Right Cloud Workload Solution for Your Enterprise

Arcserve Business Continuity Cloud gives you a range of data protection solutions to choose from, including:

Arcserve UDP Cloud Direct is the only direct-to-cloud backup and disaster recovery as a service (BaaS/DRaaS) that offers complete data protection with ease of usability—and without any on-premises hardware required. Scalable and flexible, it provides always-on continuity for industry-best RTOs and RPOs.

Arcserve UDP, secured by Sophos, provides ransomware-free IT, protecting your critical data from cyberattacks, detecting and reversing ransomware encryption, and ensuring you can safely recover all of your systems and data.

Arcserve Email Archiving Cloud makes configuration easy with quick transfer of existing and historic emails enabled by deep API-based integration with your on-premises Microsoft Exchange or online Microsoft 365.

Backup and Recovery That Eliminates Downtime

Arcserve Business Continuity Cloud’s hosted business continuity and disaster recovery solution combines powerful backup, high availability, and email archiving technologies. With these technologies, you can rest assured that your systems and applications—on-premises or in your clouds—are protected. To learn more about Arcserve solutions, check out our free trial offer, or contact us to speak to a data protection expert.

Need Answers?

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

arcserve®

+1 844 639-6792
arcserve.com