arcserve®

Zero Trust, Cyber Resilience, and Cloud Security:

How to Achieve Unmatched Data Protection

Table of Contents

Why Your Zero Trust Security Strategy Needs to Include Data Backup and Disaster Recovery

The security maxim has been "Trust but verify" for a long time. Unfortunately, that doesn't work anymore. In today's borderless, global, mobile, hybrid, cloud-based environment, traditional security approaches aren't enough, and nobody is to be trusted, including employees, customers, and partners.

The idea that you can build a protective moat around your enterprise—where interactions inside the castle are trusted, and all interactions outside the castle are not—is hopelessly outdated. Now there's a better way. Zero trust replaces outdated security strategies because it demands that organizations entirely remove trust from the equation by denying access to everyone. And IT pros are clearly seeing the approach's benefits, with the global zero trust market projected to reach $52 billion by 2026.

Zero Trust: Authenticate and Authorize Every Connection

Zero trust is all about evaluating the security posture of users based on location, device, and behavior to determine if the users are who they claim to be. Zero trust is also about granting just enough privilege, just in time, so that users can perform their needed tasks and operations—and nothing more.

With zero trust, only minimum permissions are granted at just the right time to get a job done. Those permissions are then revoked immediately upon completion of the job or transaction. A zero trust security approach authenticates and authorizes every connection. One example is when a user connects an application or software to a data set via an application programming interface (API).

The U.S. government recently announced that it is moving toward a zero trust approach to cybersecurity to dramatically reduce the risk of cyberattacks against the nation's digital infrastructure. To that end, the Cybersecurity and Infrastructure Security Agency (CISA) offers its zero trust maturity model and recently published Applying Zero Trust Principles to Enterprise Mobility to help you put these protections in place.

The bottom line is that today's security is not secure. You must assume bad actors will inevitably get in. So you need to do everything you can to minimize your attack surface and protect your business-critical data from being damaged or destroyed.

Zero Trust in Data Backup and Disaster Recovery

You also need to be exceptionally vigilant about your data backup and recovery strategies within your zero trust strategy. The concept of constantly verifying, continuously authenticating, and always logging who is going where and doing what should apply to regular operations and application usage. It should also apply to your data backup and recovery processes—it's critical that you know who is initiating that backup and where they are backing up the data.

It's also essential to ensure that, regardless of the applications you're using for your backup and recovery, you have embedded authentication mechanisms like multifactor authentication (MFA), identity access management (IAM), and role-based access controls (RBAC). Say a worker needs to have data recovered from a laptop. What are the credentials that allow this employee to restore the machine? What permissions were granted, and do those permissions need to be changed to reflect a new set of requirements? If your IT team is restoring a laptop set up a year ago, who ensures no one else has access to that machine? A zero trust approach to data backup and recovery can go a long way toward resolving these questions while further securing your organization's data.

The good news is that adopting zero trust for backup and recovery can simply mean extending the security controls you already use within your environment. For example, applying MFA to your backup and recovery processes can go a long way toward ensuring users are whom they say they are, adding stronger protections to your organization.

Immutable storage should also be part of your zero trust initiative. Immutability is when data is converted to a write-once, read many times format. This technology safeguards data from malicious intent by continuously taking snapshots of that data every 90 seconds. Because the object store is immutable, you can quickly restore data even if someone tampers with it.

As data breaches grow in volume and complexity, you need to consider novel approaches to strengthen your protection against cyber threats. Zero trust is not a specific technology or architecture. Instead, it's a new way of thinking that can help you achieve robust threat protection and gain next-level security.

Learn More About Zero Trust

To get help putting your zero trust security strategy in place, find an expert Arcserve technology partner. You can also check out our no-obligation free trial offers or contact us for product details.

How to Choose and Deploy the Right Cyber Resilience Solution

You're at risk from ransomware attacks no matter what size your organization is. In a recent survey, an astonishing 80 percent of 1,100 IT and OT pros said their organizations had already experienced a ransomware attack, with 52 percent paying a ransom of at least $500,000. "Pervasive" is the word DCIG President and Founder Jerome Wendt uses to describe the ransomware epidemic in his recent Technology Report, "Identifying and Deploying the Right Cyber Resilience Solution."

The report also says the inevitability of a ransomware attack and its devastating impacts makes complacency a risky option. The recommended response? Put a combination of cybersecurity and cyber resilience technologies in place that works together to defend against ransomware.

Start With Cybersecurity

The report suggests that a zero trust cybersecurity approach is an excellent first step in bolstering your defenses. Zero trust controls access to your corporate IT systems and digital assets using technologies including multifactor authentication (MFA) and role-based access controls (RBAC) to authenticate system and user access. Cybersecurity technologies like antivirus software and firewalls are also crucial to your defenses.

To help clarify the differences between cybersecurity and cyber resilience, here is the definition of cybersecurity from the Cybersecurity and Infrastructure Security Agency (CISA): Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.

Cyber Resilience Goals: Augmenting Cybersecurity

The DCIG Technology Report explains that cyber resilience technologies differ from cybersecurity solutions in that they reduce and mitigate your organization's risks when a ransomware attack occurs. The critical criterion for cyber resilience solutions is the ability to withstand an attack and let you continue to operate, potentially in a degraded state.

Here's the definition of cyber resilience from the National Institute of Standards and Technology (NIST): The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.

The DCIG report outlines four goals that cyber resilience products should meet to be worth considering.

1. Anticipate a Cyberattack

Since it's clear you're going to be attacked by ransomware at some point, you need to be prepared. The report says that there are three approaches to being so:

- Use third-party cybersecurity providers to monitor and send alerts regarding ransomware attacks
- Monitor your hardware and network resources for unusual or suspicious activity yourself
- Regularly scan and analyze your data for ransomware

Ultimately, monitoring is the linchpin of preparation.

2. Withstand a Cyberattack

Again, given that you'll likely experience a ransomware attack—and understanding that you may not detect an attack for hours, days, weeks, or even months—the report says you need to put software and technologies in place that can withstand both overt and covert attacks.

The report notes that overt attacks are in some ways better than covert attacks in that they cause immediate disruptions to IT and business operations. For these, you need cyber resilience software and technologies that help you survive and continue operations when the incident occurs.

The suggestion is to either take these systems offline or air gap them to keep them secure. Since you may not discover an attack for some time, you also need cyber resilience software and technologies that continually protect themselves, securing and monitoring all activity on your systems.

3. Recover From a Cyberattack

Even if you do everything we've talked about, you may still become a ransomware victim. So you need to configure your cyber resilience solution to place the right data on the right storage media to meet your recovery objectives. Fast recovery media options include cloud, disk, flash, tape, or a combination of these. And you need to test your recovery processes so you know you can respond to both covert and overt ransomware attacks.

4. Continuously Adapt to Change

IT environments are constantly changing, often without considering the impacts on your cyber resilience solution. That's why the report points out that, for your cyber resilience strategy to be viable, you need to

monitor and track changes to your IT environment—and update your cyber resilience solution whenever these changes make it necessary.

Data Protection and Disaster Recovery Plan Viability

The report refers to the NIST cyber resilience definition as your guideline, but it's also worth looking at the NIST publication Developing Cyber-Resilient Systems: A Systems Security Engineering Approach.

The DCIG report suggests you get answers to these questions when considering data protection software and technologies:

- What measures do these products take to anticipate attacks?
- How well do they withstand attacks?
- How quickly can they recover and bring production systems and data back online?
- Does the software and technology meet your disaster recovery (DR) objectives?

Key Data Protection Features

The report adds that these critical data protection features should be included in your chosen solution:

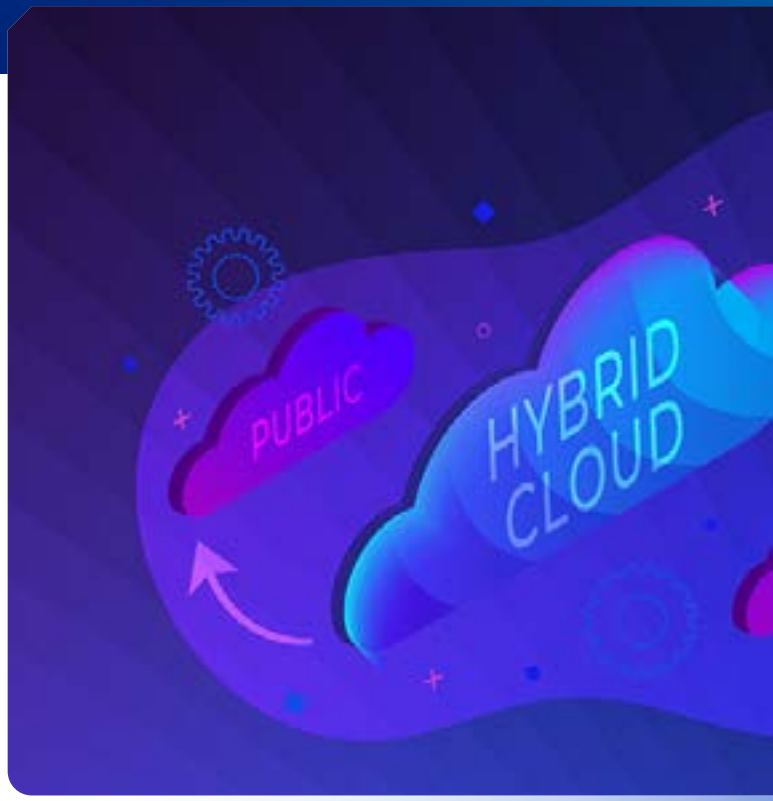
- Restrict and monitor access by authenticating users with RBAC and MFA
- Monitor and log all user actions and validate and authenticate any changes or deletions to backup schedules or data
- Consider requiring a second user to authenticate critical actions like unscheduled deletions of backups
- Forensic analysis of backups with the ability to scan backup data for unusual data change rates and the presence of ransomware
- Store backups in an immutable format so they can't be maliciously deleted or encrypted

Read the Report

The report also includes a comprehensive list of Arcserve's cyber resilience offerings, concluding, "Arcserve provides organizations with a high level of certainty they can successfully recover in a timely and effective manner." Click here to read the full Technology Report.

To learn more about Arcserve solutions, find an expert Arcserve technology partner or contact us for product details.

3 Crucial Hybrid Cloud Concerns Every Company Needs to Address



By Ivan Pittaluga, Chief Technology Officer, Arcserve

The benefits of the cloud—reduced capital expenditures, more IT flexibility, and business efficiency—are compelling. And it wasn't that long ago that IT experts were predicting organizations would move their entire computing infrastructure to the cloud. That never happened, but Cisco's 2022 Global Hybrid Cloud Trends Report did find that 82 percent of survey respondents have adopted hybrid cloud, calling it "the new normal."

Companies are choosing a hybrid-cloud strategy because of its advantages compared to complete reliance on third-party cloud vendors. And today, many tools make it easy to host an on-premises cloud-like data center. But, while hybrid clouds are appealing because of their flexibility, they are also very complex to manage. The same Cisco survey found that 35 percent of respondents viewed increased operational complexity as their top challenge when using multiple clouds.

At the top of that list of serious challenges you'll find security, backup, and disaster recovery. The Cisco study found that 37 percent of the respondents see security as a significant challenge. With the threat of a data breach or data loss always present, companies that run hybrid cloud environments need to mitigate their risks.

Security: A Shared Responsibility

While there are many misconceptions about cloud security in general, the most common is that the cloud is secure by its very nature. Nothing could be further from the truth—just check out our post listing the seven most infamous cloud security breaches. When organizations transition to the cloud, they must understand that cloud security is a shared responsibility between the cloud provider and the customer. Cloud service providers like Microsoft Azure, Google Cloud, and AWS typically secure the core infrastructure and services as part of their responsibility. But when it comes to securing operating systems, platforms, and data, that responsibility falls to the customer.

Of course, cloud providers don't exactly advertise this fact. You need to read the fine print in their T&Cs to find the legal language that explains who is responsible if anything happens to your data. Whether it's data corruption, a security breach, or even an accidental deletion, you are responsible for recovering your data—not your cloud provider.

Think of it as you would a car. While automakers are required to meet quality and safety standards, it's your responsibility to buckle up and drive safely. The same holds true for your data. It's your data and your responsibility. The fine print protects cloud providers from lawsuits, but it doesn't protect your business from the consequences of a data loss.

Managing Cloud Complexity Isn't Easy

Returning to management complexity, as the saying goes, "more money, more problems"—more clouds can also mean more problems. And the more clouds you try to blend, the more unwieldy your environment becomes.

Some organizations standardize on up to four different public clouds and numerous private clouds and data centers. Those clouds typically operate differently from each other and have very different interfaces. You may be able to manage each cloud environment seamlessly. Still, monitoring and supporting all those disparate cloud platforms and getting them to play nice with each other can be an overwhelming challenge.

Of course, other issues come with hybrid cloud environments, especially compliance and regulatory concerns. Keeping a single cloud compliant is hard enough. With the complexities of hybrid clouds, those challenges ratchet even higher as industries adapt to rule changes and security and certifications requirements.

A Security Solution for Every Cloud

You need to address security and compliance early on in your implementation process. Playing catchup later can be costly—even catastrophic. The optimal backup and recovery solution for your hybrid cloud environment should comprehensively protect and give you complete control over your data. It's worth considering cloud storage that safeguards data by taking continuous snapshots that provide multiple recovery points. That means your data is protected at all times while giving you easy access and visibility.

Some data protection solutions specifically target private, hybrid, and multi-cloud computing environments. The solution you choose should combine security controls, ransomware detection, and data protection across private cloud, public cloud, and SaaS-based environments. It should also include backup and disaster recovery services, including protection for your physical, virtual, and cloud workloads.

Every business needs to step up and take responsibility for managing its data storage and backup requirements, no matter where that data resides. You can't place your trust solely in your cloud providers. You need to implement a data protection and recovery strategy that adds an extra layer of protection so you are confident of recovery in the event of a disaster.

To learn more about Arcserve hybrid cloud data protection, backup, and disaster recovery solutions, find an Arcserve expert technology partner, or contact us for product details.

The Rise of Cloud Downtime Insurance and the Role of Proven Data Backup and Recovery Solutions

The Uptime Institute's 2022 Outage Analysis found that 80 percent of data center managers and operators have experienced some type of outage in the past three years. The same study found that cloud, hosting, colocation, and other IT providers accounted for 63 percent of all significant public outages. But here's what really hurts. ITIC's 2021 Hourly Cost of Downtime survey found that a single hour of unplanned downtime costs $300,000 or more for 91 percent of mid-sized enterprises.

Another recent article lists the seven biggest cloud outages of the past year. At the top of the list is the AWS cloud outage that caused digital traffic delays or site shutdowns worldwide for about seven hours. Google Cloud wasn't immune either, going down in mid-November and taking Home Depot, Snapchat, Etsy, Discord, and Spotify with it.

The Rise of Cloud Downtime Insurance

These statistics are why we found a recent Insurancejournal.com article titled How Cloud Downtime Insurance Became a Thing of great interest. The article credits the founders of Parametrix Insurance for coming up with the idea to provide coverage for clients for short-term outages, network crashes, and platform failures that last up to 12 to 24 hours.

A Parametrix co-founder is quoted as saying that the product was conceived with the understanding that everything was moving to the cloud. The company was surprised that this risk wasn't covered before it started operating in the space. They also saw that this transition created a vast coverage gap because downtime and other risks were excluded and restricted from most insurance policies.

Parametrix recognized that it needed reliable data on outages to develop models to assess downtime risks. Before offering the coverage, the company's first order of business was to create monitoring systems that independently verify uptime and downtime for cloud and other enterprise technologies. These include software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) systems.

Here's where it gets interesting. According to the Insurancejournal.com article, cloud downtime coverage is usually $100,000 to $5 million for an annual policy. Coverage can start as soon as an hour after a downtime event's onset, and lasts up to 12 to 24 hours. That could add up to a significant amount of money still well spent when you consider that typical cybersecurity insurance policies have a waiting period of 12 hours or more and only cover specific losses.

We still believe cybersecurity insurance may be worth considering as a hedge against data loss and downtime's financial impacts. But the best way to avoid downtime costs is to reduce downtime as much as possible. That's where proven data backup and recovery solutions come in.

Unified Data Protection: Fast Recovery Equals Less Downtime

Arcserve UDP delivers on the promise of reduced downtime with comprehensive data protection and cybersecurity for your critical backup infrastructure. Safeguarded by Sophos Intercept X Advanced cybersecurity, it is the only product that combines deep-learning server protection, immutable storage, and scalable onsite and offsite business continuity. The result is complete resiliency for your virtual, physical, and cloud infrastructures.

Thanks to Arcserve UDP's orchestrated recovery capabilities, you can reduce your recovery time and recovery point objectives (RTOs/RPOs) to minutes while validating service level agreements (SLAs) with Assured Recovery™. Recover your data faster, too, with instant virtual machine (VM) and bare metal recovery (BMR) and local and remote virtual standby.

You can also count on application-consistent backup and granular restore, hardware snapshot support, and extensions that deliver high availability and support tape backups. It's easy to use, managed from a single console, and simplifies running hybrid environments with on-premises, virtual, and SaaS-based applications and systems.

Protection Across Platforms

Arcserve UDP offers data protection across a broad range of platforms, including:

- Amazon EC2
- Microsoft Azure
- Windows
- Linux
- Office 365 (Exchange Online, Teams, SharePoint Online, and OneDrive for Business)
- Microsoft Exchange
- Microsoft SQL

- File servers,
- Microsoft IIS
- Microsoft Active Directory
- Oracle Database with native RMAN support
- VMware vSphere (agentless)
- Microsoft Hyper-V (agentless)
- Supports Nutanix Objects and Nutanix Files for protection of Nutanix HCI

Insurance Doesn't Ensure Your Data Is Protected

While every organization is different, it's worth taking a closer look at cybersecurity insurance and even the new cloud downtime insurance policies. Regardless of your decision, better data protection and recovery capabilities can keep downtime to a minimum and possibly result in lower premiums if you choose to buy any insurance. That makes it an investment that will likely pay for itself in a single incident. Of course, the peace of mind it gives you is priceless.

See the difference Arcserve UDP can make by checking out our free 30-day trial. If you'd like expert help in putting a data protection and downtime deterring solution in place, 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