arcserve®

Data Protection Insights Into Cybersecurity, Microsoft Office 365 Data, Containers, and Cloud Downtime Insurance

Table of Contents

How Data Protection Fits Into Every Cybersecurity Strategy

The mass transition to remote and hybrid workforces has opened up new opportunities—and new attack vectors—for cybercriminals. With more and more data being stored in the cloud and employees working in home offices where security is not necessarily a primary concern, ransomware attacks have skyrocketed.

Sophos State of Ransomware 2022 report found that 72 percent of organizations surveyed experienced an increase in the volume, complexity, and impact of cyberattacks, while two-thirds were hit by ransomware last year. Even worse, 65 percent of those attacks resulted in the organization's data being encrypted. That brings us to the only possible conclusion: It's not a matter of if but when your organization will suffer an attack.

Data Protection Depends on a Comprehensive Strategy

Historically, CISOs have focused on building a moat around the castle, relying on firewalls, antivirus solutions, multi-factor authentication (MFA), intrusion detection and prevention systems (IDS/IPS), and other tactics. Sadly, these barriers are no longer up to the task because most organizational data now resides outside the metaphorical castle. Even with layers of defensive measures in place, organizations are still vulnerable to cyberattacks—and their data is still being compromised.

Today, you need a 360-degree view of IT security for effective data protection. That means expanding your focus to include data backup and recovery solutions—and immutable storage. These areas haven't previously been a core part of cybersecurity conversations. But with backups increasingly being targeted by ransomware, they must now be a critical component of every cybersecurity strategy.

In reality, backup, recovery, and immutable storage are the most critical components of your strategy because they are your last line of defense. A solid data protection plan can safeguard your organization's mission-critical data and help secure your company against disruptions and cyberattacks. That minimizes the risks your operation faces.

You also need to look at rebalancing your overall approach to data security. And you likely need a better way to manage risk while optimizing your ability to recover your data in a disaster.

Here are the top three steps you—and every CISO—can take to balance the equation and integrate data protection into your cybersecurity plans.

1. Create or Update Your Recovery Plan

The first step in any cybersecurity strategy should be backing up critical data. But data backup isn't enough. You also need a plan to recover your data quickly and cost-effectively in the event of a cyberattack. Without a well-considered recovery plan, you may be unable to restore the precise version of a file or folder you want if you experience data loss.

Here's another way to think about data backup and recovery. Restoring your data without a solid recovery plan is like putting a jigsaw puzzle together with half the pieces missing. It's a recipe for disaster because once a crisis hits, it's too late. An effective recovery plan helps you locate what you need and quickly begin the recovery process because every minute of downtime is costly.

2. Choose Immutable Storage

A robust backup and recovery plan safeguards your data even if you do fall victim to a cyberattack. A storage solution that continually protects your data by taking snapshots every 90 seconds is a vital component for supporting that plan. These snapshots make it possible for you to go back to specific points in time—before an attack—and recover entire file systems in a matter of minutes. So, even if a ransomware attack is successful, you can quickly and easily recover your data from a very recent point in time.

With immutable backups, your data can't be altered in any way—not even by admins or, more importantly, ransomware. So you can count on having recovery points available when needed. That's the ultimate data protection. Immutability also creates a bridge between security and operational infrastructure teams, removing traditional silos by letting them speak the same language and collaborate in the face of cyber threats.

3. Get One-Click Recovery

You need to do everything you can to minimize downtime after an attack. The first step is choosing a data protection system that's easy to deploy, simple to manage, and steady as a rock under even the most harrowing circumstances. The system should also include orchestrated recovery with a single click. And you should be able to recover confidently by safely spinning up copies of physical and virtual systems onsite and offsite in minutes—not hours or days.

The most effective data protection systems use analytics to identify frequently used data that your business should always back up—and less vital data that doesn't require regular backups. The result is an intelligent, tiered data architecture that gives you fast access to mission-critical information. And it helps you reduce storage costs without sacrificing data protection.

Protect Your Most Important Asset

Your data is your organization's most important asset. If it's compromised by ransomware, your operations are dead in the water. That's why you need to make data protection a crucial part of your cybersecurity strategy. With the right approach, your data will be quickly and easily recoverable, even after an attack.

Get expert data protection guidance and advice by choosing an Arcserve technology partner. To learn more about Arcserve data protection products, request a free demo.

How to Protect, Back Up, and Recover Your Microsoft Office 365 Data in the Face of Ransomware, Malware, and More

One recent headline alerted users about a Microsoft 365 config loophole that opens OneDrive and SharePoint data to a ransomware attack. Another explained how malicious actors are mounting cyberattacks that target supply chains using Office 365. But human error is still the number one reason behind data disasters.

Regardless of what could cause data loss, your Microsoft 365 data is precious. That's why it's essential to understand and implement effective backup and recovery methods and solutions for that data.

More than likely, virtually everyone in your organization relies on Microsoft 365 for their core productivity apps. If those apps—or the data they depend on—aren't available, your organization could come to a screeching halt.

While Microsoft takes full responsibility for critical components of the stack—like physical and IT security, application-level controls, and more—you are responsible for your data that's stored in its cloud. Even Microsoft recommends regularly backing up the content and data you keep on its Services using Third-Party Apps and Services.

But not every backup solution completely protects your Microsoft Office 365 data from the ravages of ransomware. Arcserve UDP and Arcserve SaaS Backup are two options that do.

Arcserve UDP: Backup for Microsoft 365 Data

Arcserve UDP offers comprehensive ransomware protection for your Microsoft 365 data with on-premises backup and granular and instant recovery capabilities.

Arcserve UDP protects Microsoft 365 workloads—Exchange Online, Teams, SharePoint Online, and OneDrive for Business—with multilayered data security and protection on-premises. With Arcserve UDP, you can back up easily using simple configuration tools to set up your backup strategies. You also gain enhanced security and compliance with AES encryption and role-based access control (RBAC).

Simplify Data Protection and Recovery, and Scale Easily Across Topologies

IT teams can reduce the time required to implement and maintain complete Microsoft 365 data security and protection—as well as other physical, virtual, and cloud workloads—by as much as 50 percent, thanks to Arcserve UDP's single, simple UI.

You can also quickly scale hybrid business continuity topologies, locally or over long distances, to multiple sites—including service and cloud providers. Installation takes a few clicks. Then create data stores on your recovery point server (RPS), add the nodes you want to protect, a storage destination, and a plan. Arcserve UDP also makes it easy to perform jobs like backup, virtual standby, replication, and execution of a simple restore or a bare metal recovery.

Reduce Storage, Get More Options, Enhance Security

With Arcserve UDP's global source-side deduplication, i2 technology, and compression, you can achieve substantial data reduction rates and cut your storage requirements. Back up to a local machine or a central destination—RPS, local folder, or remote shared folder—and easily add network CIFS/NFS shares, Office 365 Exchange, or SharePoint online nodes. And your data is protected from ransomware because Arcserve UDP is fully integrated with Sophos Intercept X Advanced, award-winning protection that uses artificial intelligence (AI) and deep learning to stop attacks.

Arcserve SaaS Backup: Cloud-Native SaaS Application Data Protection

Arcserve SaaS Backup is another option that offers complete protection for your SaaS application data stored in Microsoft 365, Microsoft 365 Azure AD, and Microsoft Dynamics 365, as well as Salesforce and Google Workspace. The solution is simple to set up—it takes less than five minutes—using a single pane of glass with multi-tenant capabilities and RBAC.

Arcserve SaaS Backup keeps your data secure and encrypted in transit and at rest. Your data sovereignty is guaranteed, too, with four copies of backups stored in two different data centers within the same region. The solution also features immutable backups, using a blockchain-based algorithm for ransomware resilience. It also provides 30-day delete retention to protect against inadvertent deletions—or ransomware attacks. And it automatically updates applications without stopping active jobs.

Choosing the Right Microsoft 365 Backup and Recovery Solution

With so many options to choose from, it's worth talking to an Arcserve technology partner to help guide you along. Our partners offer the deep expertise and hands-on experience that smooths your IT transitions. If you'd like to dive deeper, check out our 30-day free trial offers for Arcserve UDP and Arcserve SaaS Backup.

Containers Are Temporary, Your Data Isn't: How Data Protection and Storage Factor Into Containerized Environments

As organizations implement application-modernization strategies, containers are becoming an increasingly essential technology. The numbers bear this out, with the global application container market expected to grow from $1.5 billion in 2020 to $9.7 billion by 2027—a CAGR of 30 percent. In the Asia Pacific alone, the containerized data center market is predicted to reach nearly $1 billion by 2028.

The technology continues to mature, but its benefits are evident as containers let you consolidate all your code into a single package that can be spun up quickly and seamlessly moved from one computing environment to another. Containers can also be spun down when their work is finished, so they don't consume resources while sitting idle.

That's a tremendous bonus for developers because containers now make it feasible to move an application from a testing environment to a live production environment—or migrate from a physical machine to a virtual machine (VM) in the cloud. Containers also let developers reuse code as they focus on building high-value software.

These benefits are just some drivers behind IDC's projection that 80 percent of workloads will shift to containers by 2023. But containers bring two significant challenges: data storage and data protection. Containers are, by nature, temporary. Storage is typically permanent. As you quickly spin up and take down containers, you'll likely find that the data lives on long after the container is gone.

Containers vs. Data Storage: Different Technologies, Different Rules

Data storage rules don't work for containers, which are continuously created and destroyed. Instead, container data must be backed up and stored to protect against risks like system outages and data loss that can occur when migrating and deploying new applications.

As you look to ramp up your container strategy, you need to understand that a robust and reliable data backup and recovery plan is a crucial part of that strategy. That's common sense, given that any loss

of mission-critical data—at any stage of a container's development—can put your IT investments and more at risk. Active containers and containerized applications need a place to store and secure their current and historical data. Compliance and other requirements also mean container data must be stored and protected long after the container has been spun down.

The Shared Responsibility Model: Data Protection Is on You

It's a common misunderstanding that if containers are stored in a cloud service, your data is automatically protected, and a recovery plan is in place. Not true.

Cloud providers only take responsibility for their stack. Under the shared responsibility model, as Microsoft notes regarding Azure, "you are responsible for protecting the security of your data and identities, on-premises resources, and the cloud components you control." Since it's your data, you need internal policies to protect that data—and recover it with minimal loss in the event of an incident.

It's important to remember that storing containerized data isn't a time-based process, with backups scheduled every few minutes or hours. Container backups are event-driven. For example, you modify a container but don't get the expected results. You'll likely want to revert that container to its previous state, which requires a proper backup of that earlier state. That makes data storage a front-burner issue for your developer teams.

Don't assume containers are immune to disasters or cyber threats. In 2021 Siloscape made it clear that containers are at risk, as the first known threat targeting Kubernetes environments arrived on the scene. So, how can you ensure that your data is securely stored and backed up when using containers? All container applications and data should be part of your overall data resilience and data protection strategy. It simply boils down to the fact that you need to secure every container in your environment.

You also need to protect the location where your data is stored, including the systems, storage devices, and databases housing copies of your data. As you expand your containerization efforts, you must ensure that your overall disaster recovery strategy can adapt to accommodate new data generated by emerging technologies and next-generation appliances.

It's Time to Choose Better Backup Technologies

Add it all up, and it's clear that backing up your data is critical and will only become more so over time. As your organization creates more containers, you'll also generate more data that needs to be backed up, stored, and protected.

While containerization brings many benefits to application development, it also adds new challenges for backup and recovery. That's why it's worth talking to an expert Arcserve technology partner to understand your options and determine the optimal solution for your situation. Request a demo to learn more about Arcserve data protection, backup, and recovery solutions.

Cloud Downtime Insurance and Disaster Recovery: Weighing the Costs and Benefits

Gartner forecasts worldwide end-user spending on public cloud services will grow more than 20 percent in 2022 to $494.7 billion. Gartner also projects that number will increase to $600 billion by 2023. As more and more companies adopt cloud computing, their downtime risks also increase.

For those reasons, among others, we've seen a rise in cloud downtime insurance in recent years. Downtime insurance covers you for short-term cloud outages, network crashes, and platform failures that last up to 24 hours.

Cloud Downtime Happens More Often Than You Think

You may think your data is safe when you move it to a cloud provider, but that isn't always the case. Last year, a fire in the data center of French web hosting service OVHcloud, Europe's largest cloud provider, caused the loss of massive amounts of customer data. The impacts were felt by government agencies, e-commerce companies, banks, and many other sectors.

While you should consider the cloud as a reliable resource, the reality is that cloud downtime isn't unusual. Cloud insurance provider Parametrix says that, on average, one of the three major cloud providers—Microsoft Azure, AWS, and Google Cloud—has an outage lasting at least 30 minutes every three weeks. Cloud downtime insurance can be a helpful safety net for your business. Still, it doesn't eliminate all your risks, including ensuring your business can get back up and running quickly when disaster strikes.

While insurance may cover you for any short-term losses you incur, it won't cover the damage to your brand and customer loyalty that downtime can cause. Rather than rely entirely on cloud downtime insurance, we recommend three strategies to help weather cloud downtime and other unexpected events.

Data Resilience: A Proactive Approach

A proactive approach starts with ensuring your disaster recovery plan is up to date and regularly tested. Your plan should include a data resilience strategy that ensures business continuity in the event of an incident.

Critical metrics for your plan include your recovery point and recovery time objectives (RPOs, RTOs). RPO determines how much data your business can afford to lose in a disaster and is the basis for how frequently you back up your data. For some organizations, backing up 24 hours is enough. For others, such as finance and healthcare, RPOs may be measured in milliseconds.

RTO determines the acceptable amount of time your operations can be offline in a disaster and is the basis for your disaster recovery solution investment. If your RTO is one hour, you need to invest in solutions that can get your business running again within that timeframe. Establishing your RPO and RTO—then implementing the solutions you need to achieve them—are the keys to data resilience.

Make Your Backup and Recovery Solution a Priority

Your cloud data is secured under the shared responsibility model. While cloud providers may promise to secure their infrastructure and services, securing operating systems, platforms, and data is your responsibility. Ultimately, you are responsible for protecting your data if anything goes wrong. That's why many cloud providers recommend that their customers use third-party software to protect their data.

A reliable cloud backup and recovery solution will help you secure and gain better control over all your data. Look for a data protection solution that automatically backs up your data every 15 minutes and gives you multiple recovery points. That guarantees your data is continuously protected while giving you fast access and visibility 24/7.

Test Your Disaster Recovery Plan

Backing up your data on-premises or in the cloud is a crucial and cost-effective first step in any disaster recovery plan. But it's only the first step. You also need a plan to recover your data quickly in an emergency. Think of your business journey as a trip on a cruise ship (although probably not as relaxing). Just like a cruise ship regularly tests its lifeboats (weekly, in case you're wondering), you should test your recovery plan often. You should simulate disruptions to see how well your plan works and regularly test your backup images to ensure they will be available when needed. Your recovery plan is your lifeboat. And it will serve you best if it's built based on the 3-2-1-1 backup strategy,

Be Ready

More threats are coming your way every day. That's why it's worth considering cloud downtime insurance. But insurance alone isn't nearly enough. Learn how Arcserve solutions can help you meet your RPOs and RTOs—and be confident of recovery no matter what—by choosing an expert Arcserve technology partner. Check out our free demos to see how Arcserve products perform for yourself.

Need Answers?

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

arcserve®

+1 844 639-6792

arcserve.com