eBook

datto
A Kaseya COMPANY

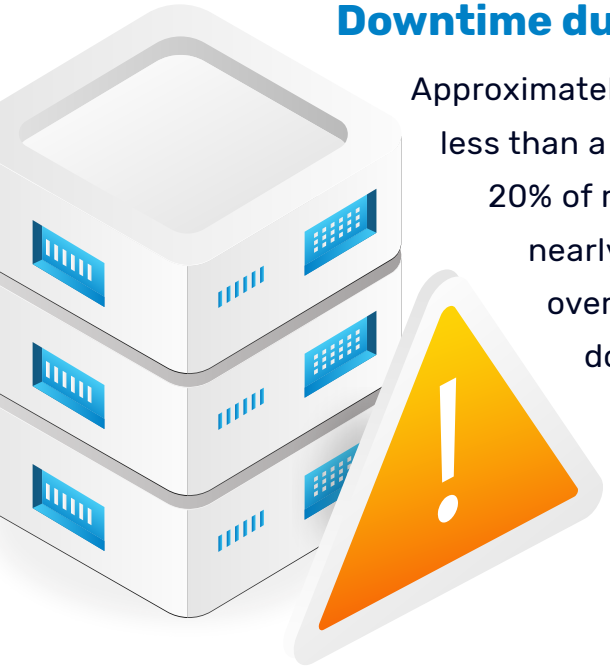
Backup vs Business Continuity

Data protection solutions are essential for businesses of all sizes, regardless of their industry and geographic location. In this white paper, we'll discuss the importance of business continuity rather than simply backup. We'll also explain how to quickly evaluate your internal recovery process and downtime costs to ensure you find the best solution for your needs.

Introduction

Downtime is real and it's costly. Depending on the size of the organization, the cost per minute of unplanned IT downtime ranges from $14,056 to $23,750 for large enterprises. On average, a business will lose around $843,360 per hour of downtime.[1] The numbers speak for themselves.

What causes downtime? According to the *State of Backup and Recovery Report 2025*, server hardware failure accounted for 22% of on-premises outages. Closely behind are service provider outages (e.g., ISP disruptions) and cyberattacks, each causing 19% of outages. Human error was responsible for 18% of disruptions. Meanwhile, natural disasters contributed to 12% of outages.[2]



Downtime due to on-premises outages

Approximately 30% of businesses reported experiencing less than a day of downtime. On the other hand, over 20% of respondents faced 2–3 days of downtime, while nearly 20% endured a full day of disruption. Just over 10% of organizations managed to avoid downtime altogether.

Causes of downtime

Server hardware failure	22%
Service provider outages	19%
Cyberattacks	19%
Human error	18%
Natural disasters	12%

Figure 1. Causes of downtime

What's at stake?

According to Statista's latest forecast, approximately 149 zettabytes of data were generated globally in 2024, including data created, captured, copied and consumed.[3] The majority of the total data in existence was created within the past few years, a significant portion of which has been generated by small businesses. Considering all the servers, desktops and laptops that the typical small and midsize businesses (SMBs) manage, it adds up to a lot of data to protect.

The State of Backup and Recovery Report 2025 reveals a concerning reality — only 40% of respondents feel confident in their backup systems' ability to safeguard critical data during a crisis. Even more striking, 30% admit to losing sleep over their organization's backup and recovery preparedness, while another 30% are anxious that their current solution simply isn't up to the task.

How much does this cost? A recent survey found that over 50% of respondents faced IT outages costing more than $100,000, while 16% reported their latest outage cost over $1 million.[4]

What happens when disaster strikes? Businesses must scramble to retrieve important data. According to the State of Backup and Recovery Report 2025, more than 60% of respondents believed they could recover servers, virtual machines (VMs) and applications in under a day.

WHAT HAPPENS WHEN DISASTER STRIKES? BUSINESSES MUST SCRAMBLE TO RETRIEVE IMPORTANT DATA.

Disaster recovery: Perception vs. reality

When it comes to disaster recovery (DR), the gap between confidence and capability is striking. While over 60% of respondents believed they could recover from downtime in less than a day, only 35% managed to do so. This disconnect highlights the need for organizations to reassess their preparedness and bridge the gap between expectations and real-world outcomes.

Several factors could impede disaster recovery:

Inadequate budget or resources: Limited funding for disaster recovery solutions, tools and staff can slow down recovery efforts.

Lack of a comprehensive DR plan: The absence of a well-documented and tested plan leaves businesses unprepared to respond effectively to disruptions.

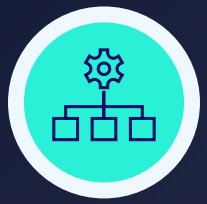
Insufficient data backups: Inadequate or outdated backups make it difficult to recover critical data after a disaster.

Cyberattacks: Ransomware, data breaches and other cyberthreats can compromise critical systems or backups and delay recovery.

Human error: Mistakes like accidental data deletion and not following recovery protocols can increase downtime.

Outdated or unreliable technology: Aging infrastructure or untested recovery solutions may fail to support effective recovery during a crisis.

Lack of employee training: Without proper training, employees may not know how to respond during a disaster, leading to delays and errors.



Lack of redundancy: Failure to implement redundant systems, such as backup servers or network failovers, increases vulnerability.

How SMBs safeguard their data

SMBs are employing a mix of cloud and on-premises solutions to protect their data. The public cloud stands out as the preferred storage option, with 44% of respondents backing up their data to services like Azure Blob. Around 40% utilize a second site or private cloud to ensure the physical separation of backups.

Over 30% of businesses trust vendor-provided cloud solutions for backup storage. While convenient, these integrated options pose risks, such as vendor outages from technical or hardware failures, potentially causing catastrophic data loss without third-party backups.

About 30% of SMBs still use traditional disk storage. Although reliable, it lacks the flexibility and scalability offered by cloud-based alternatives.

Unfortunately, approximately 2% of respondents fail to store backups off-site, leaving their data exposed to localized disasters such as fires, floods or ransomware attacks.

How businesses protect their data

Back up copies to the public cloud	**44%**
Back up copies to the second site (private cloud)	**40%**
Back up copies to the vendor's cloud	**31%**
Back up copies to disk	**30%**

Figure 2. How backup copies are maintained (Respondents selected all that applied)

Some of the most popular data replication strategies businesses adopt include public cloud + private cloud (14%), public cloud + vendor's cloud (14%), and public cloud + hard disk drives (13%). These statistics highlight that multicloud configurations dominate as the prevailing data protection strategy.

Local or cloud backup? The answer lies in between

Using local backup for business continuity works well for quick restores. Because the data is right there, it's fast and easy to restore to its original location and keep the business humming. But what happens if the power goes out? If the device fails? Or if it is stolen or destroyed in a natural or man-made disaster? You might think the cloud looks more attractive for all these reasons. However, cloud-only backup is risky because you can't control the bandwidth. Restores tend to be difficult and time-consuming. After all, the cloud can fail, too.

How does a hybrid-cloud solution work? Your data is first copied and stored on a local device. That way, if something happens, you can quickly and easily restore it from that device. But then your data is also replicated in the cloud. If anything happens to the local device, you've got off-site cloud copies of your data — without having to worry about moving copies of your data off-site physically.

LOCAL OR CLOUD BACKUP? THE ANSWER LIES IN BETWEEN. A HYBRID CLOUD LEVERAGES THE ADVANTAGES OF LOCAL BACKUP AND CLOUD SECURITY.

Data backup vs. business continuity: What's the difference?

Data backup answers the question: Is my data safe? Can I get it back in case of a failure?

Business continuity, on the other hand, involves thinking about the business at a higher level and asking: How quickly can I get my business operating again in case of system failure?

Thinking about data backup is a good first step. Business continuity is equally important to consider as it ensures your organization can get back up and running in a timely manner if disaster strikes. For example, if your server dies, you wouldn't be able to quickly get back to work if you only had file-level backup. Your server would need to be replaced, software and data re-installed, and the whole system would need to be configured with your settings and preferences. This process could take days. Can your business afford to lose that time?

When discussing business continuity, we often refer to recovery time objectives (RTOs) and recovery point objectives (RPOs).

RTO: The recovery time objective is the duration of time within which a business must be restored after a disruption to avoid unacceptable consequences.

RPO: The recovery point objective is the maximum tolerable period in which data might be lost due to a disaster.

By calculating your desired RTO, you have determined the maximum time that you can be without your data before your business is at risk. Alternatively, by specifying the RPO, you know how often you need to perform backups. You may have an RTO of a day and an RPO of an hour, depending on what your business requires. But calculating these numbers will help you understand what type of data backup solution you need.

Figure 3. Difference between RPO and RTO

Once you determine your RPO and RTO, it's time to calculate how much downtime and lost data will actually cost you. Simply add up the average per-hour wage, the per-hour overhead and the per-hour revenue numbers, and you have how much a data loss will cost you.

Alternatively, check out this free, easy-to-use *online RTO Calculator* for instant RPO, RTO and downtime costs.

Given that budget constraints can be a challenge for many businesses, obtaining these costs provides a financial validation to justify the purchase and maintenance of a business continuity solution.

Calculating the real costs of data loss will provide you with the financial validation needed to justify a business continuity purchase.

Image vs. file-only backup

There are two well-known types of backup solutions: file- and image-based.

A **file-based backup** does exactly what it sounds like: you choose which files you want to back up, and those files are saved to an on-site device or to the cloud, whichever type of solution you have chosen. But only the files you choose are saved. What if you forget to save a key file?

Image-based backup, on the other hand, captures an image of your data in its environment. Thus, you have exact replications of what is stored on a server — including the operating system, configurations, settings and preferences. If a server goes down, you can restore it in minutes, rather than the hours or days it would take to requisition a new server and install and configure the operating system.

What to look for in a business continuity solution

To sum up what we've learned today, here are some key things to look for when seeking a business continuity solution:

- **Hybrid cloud backup:** A hybrid approach fixes the vulnerabilities that a cloud-only or local-only possesses.
- **Superior RTO and RPO:** Think in terms of business continuity rather than simply backup and calculate how much downtime your business can endure and still survive (RTO) as well as how much data you can afford to lose (RPO).
- **Image-based backup:** Ensure that the backup solution takes images of all data and systems rather than simply copying the files.

ENSURING YOUR BUSINESS CAN OPERATE IN CASE DISASTER STRIKES IS CRITICAL, REGARDLESS OF THE SIZE OF YOUR ORGANIZATION.

Make data backup and business continuity your top priority

With the increasing risks of cyberattacks, data loss and downtime, a robust business continuity strategy is critical to protecting your operations and reputation. By leveraging reliable solutions like Datto's all-in-one business continuity, you can ensure your data is secure, accessible and recoverable when you need it the most. Don't wait until disaster strikes — take control of your data and business with Datto today.

Request a personalized demo and discover how our industry-leading solutions can fortify your data protection strategy and keep your business running seamlessly.

REQUEST A DEMO

Sources:

1 https://www.bigpanda.io/ar-ema-outage-cost-2024/

2 https://www.unitrends.com/resources/the-state-of-backup-and-recovery-report-2025/

3 https://www.statista.com/statistics/871513/worldwide-data-created/#:~:text=The%20total%20amount%20of%20data,replicated%20reached%20a%20new%20high.

4 https://uptimeinstitute.com/uptime_assets/2564c126499732e5fb721dd333bc7daade3c4f6dff9875b2763a3051578518bf-GA-2024-03-annual-outage-analysis-2024.pdf

About Datto

As a leading global provider of security and cloud-based software solutions purpose-built for managed service providers (MSPs), Datto, a Kaseya Company, believes there is no limit to what small and medium-sized businesses (SMBs) can achieve with the right technology. Datto's proven Unified Continuity, Networking, Endpoint Management and Business Management solutions drive cyber resilience, efficiency and growth for MSPs. Delivered via an integrated platform, Datto's solutions help its global ecosystem of MSP partners serve over one million businesses around the world. From proactive dynamic detection and prevention to fast, flexible recovery from cyber incidents, Datto's solutions defend against costly downtime and data loss in servers, virtual machines, cloud applications or anywhere data resides. Since its founding in 2007, Datto has won numerous awards for its product excellence, superior technical support and rapid growth, and for fostering an outstanding workplace. With headquarters in Miami, Florida, Datto has global offices in Norwalk, Connecticut as well as Australia, Canada, Denmark, Germany, the Netherlands and the United Kingdom.

datto
A Kaseya COMPANY