eBook

datto
A Kaseya COMPANY

The Ultimate Guide to BCDR: Why Backup and Disaster Recovery Matter

The threat landscape for small and midsize businesses (SMBs) is evolving at an alarming rate. Cyberattacks, hardware failures and natural disasters are causing costly disruptions, making downtime more frequent than ever before. **According to The State of BCDR 2025 Report[1],** nearly 60% of IT teams experienced downtime for a day or more in 2024 — a stark reminder that no business is immune anymore. When downtime strikes, it doesn't just impact IT systems; it grinds operations to a halt, erodes customer trust and causes significant financial and reputational loss.

That's why business continuity and disaster recovery (BCDR) has become critical for IT teams. While cybersecurity solutions help prevent attacks, they don't ensure resilience when a breach, failure or disaster occurs. Without a solid BCDR strategy, businesses risk extended downtime, critical data loss and operational paralysis. **Think of BCDR as the missing piece of the cybersecurity puzzle: security helps prevent threats, but BCDR ensures your business survives them.**

[1] *https://www.datto.com/wp-content/uploads/dlm_uploads/DAT-The-State-of-BCDR-2025.pdf*

This eBook is designed to be your practical guide to BCDR, equipping you with the knowledge and strategies to protect your business. We'll explore what BCDR is, its key components, real-world examples of its impact and actionable steps to build a resilient BCDR strategy. Whether you're an SMB owner or an IT pro, this guide will help you take complete control of your business continuity and disaster recovery planning — before disaster strikes.

BCDR simplified: Keep your business running no matter what

Business continuity (BC) and disaster recovery (DR) are two interdependent yet distinct processes that help organizations prepare for, respond to and recover from disruptions while keeping operations running smoothly.

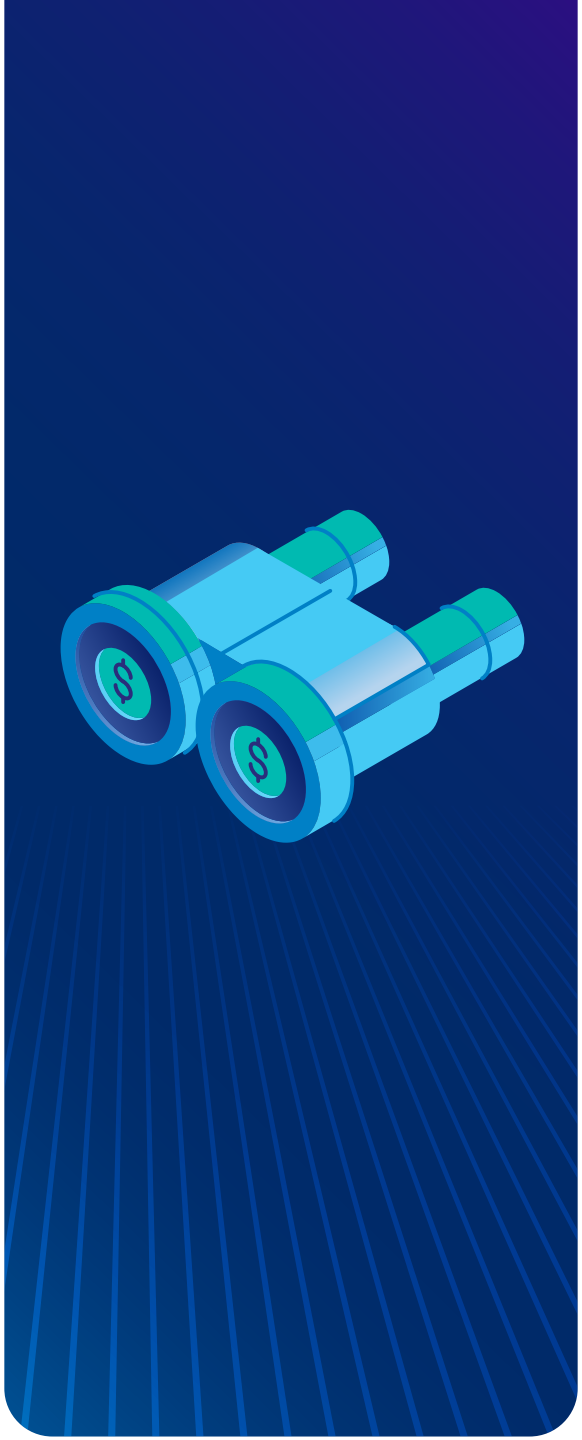
Business continuity: Business continuity focuses on keeping essential operations running during and after a disruption. It involves proactive planning, risk assessment and implementing strategies to maintain productivity, such as redundant systems, alternative work arrangements and operational contingencies.

Disaster recovery: Disaster recovery is the technical side of restoring IT systems, applications and data after a failure or disaster. It includes data backup, system failover and recovery procedures to ensure minimal data loss and a quick return to normal operations.

Business continuity vs. disaster recovery

Aspect	Business continuity	Disaster recovery
Focus	Keeping business operations running during a disruption	Restoring IT systems after a disruption
Scope	Covers people, processes and infrastructure	Primarily focuses on IT systems and data
Objective	Ensuring minimal operational impact and service continuity	Restoring systems and data as quickly as possible
Time frame	Starts before an incident occurs and continues throughout	Begins after a disruption has occurred

While business continuity and disaster recovery serve different functions, they must work together for a business to remain resilient. BC keeps things running while DR restores what's lost. A fragmented approach can leave critical gaps, increasing downtime and risk. By integrating both into a unified BCDR strategy, SMBs and IT teams can mitigate disruptions, recover faster and maintain seamless operations — even in the face of unexpected crises.



BCDR essentials:
Six core components of a winning BCDR strategy

An effective BCDR strategy combines critical processes, technologies and planning to provide seamless continuity and rapid recovery, no matter the disruption. Let's examine each of those six major components.

1. Risk assessment and business impact analysis (BIA)

Every business faces risks, but not all threats carry the same weight. A risk assessment helps identify potential disruptions, evaluate their likelihood and determine their possible impact. However, knowing the risks isn't enough — you need to understand how they affect your business operations.

That's where business impact analysis (BIA) comes in. BIA helps pinpoint which functions are most critical, what resources they depend on and how much financial damage a disruption could cause. By analyzing factors like lost revenue, regulatory penalties and increased operational costs, businesses can prioritize recovery efforts and reduce downtime.

Pro tip: How do you conduct a BIA?

A BIA breaks down how disruptions affect business functions and finances. One effective way to measure impact is through a simple questionnaire:

- How much revenue loss would this cause?
- What penalties or compliance fines might we face?
- How would operational costs increase?

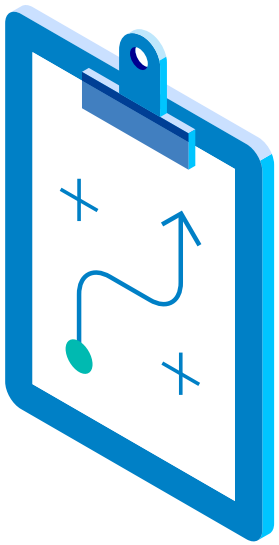
By answering these questions, IT teams can make informed decisions about disaster recovery priorities and response strategies.

2. Data backup and disaster recovery

Data is the backbone of any business, and losing it, even for a short time, can be devastating. Whether it's stored on-premises, in the cloud, or within SaaS applications, every business needs a comprehensive backup and recovery plan.

Key elements of a robust backup and disaster recovery strategy include:

- Automated, frequent backups to protect against data loss.
- Geo-redundant storage to secure against regional disasters.
- Fast, reliable recovery to keep critical systems running.



Pro tip: Achieve faster, more secure recoveries — no matter the threat

We all know the classic 3-2-1 backup rule. However, with evolving cyber threats, experts have enhanced it for even greater protection. Enter the 3-2-1-1-0 rule — a smarter approach that adds extra security and verification.

Here's how it works:

- 3 copies of data: Multiple copies prevent data loss.
- 2 different formats: Store on at least two media types.
- 1 off-site copy: Protect against physical disasters.
- 1 immutable copy: Ensure ransomware-proof backups.
- 0 doubt you can recover: Regular testing guarantees reliability.

3. High availability and redundancy

Disruptions happen, but downtime doesn't have to. High availability (HA) and redundancy ensure that even if a failure occurs, systems stay online and operational. This helps businesses maintain uptime and performance, even during outages or cyber incidents.

Key HA and redundancy strategies include:

- Failover systems that instantly switch to a backup server if the primary one fails.
- Cloud disaster recovery (Cloud DR) for scalable, on-demand instant virtualization.
- Load balancing to distribute traffic and prevent system overload.

4. Cyber resilience and security

A BCDR plan is incomplete without strong cybersecurity measures. Without proper security, even the best recovery plans can fail.

To strengthen cyber resilience, businesses should prioritize:

- Ransomware protection with immutable, air-gapped backups.
- Endpoint security to protect employee devices from ransomware and phishing attacks.
- User security training to prevent human errors that lead to breaches.

5. Incident response and crisis management

Without a structured incident response plan (IRP), businesses risk costly downtime, financial losses and regulatory penalties. A well-defined IRP ensures that when a disruption occurs, the team knows exactly how to detect, contain and recover efficiently.

A strong IRP includes these five essential phases:

Detection and analysis: Identify security breaches, system failures or cyberattacks early to assess their impact.
Containment: Isolate affected systems to prevent the incident from spreading and causing further damage.

Eradication: Remove the root cause of the issue, whether it's malware, compromised accounts or hardware failures.

Recovery: Restore systems, verify data integrity and resume normal operations as quickly as possible.

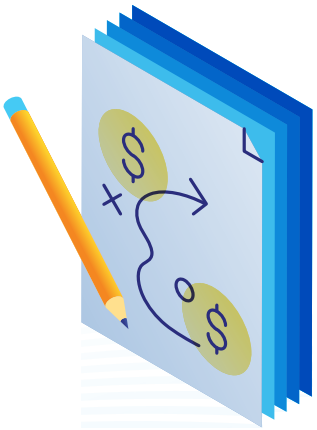
Post-incident review: Analyze the incident, document lessons learned and refine security measures to prevent future disruptions.

6. Testing and continuous improvement

A BCDR plan that isn't tested is a disaster waiting to happen. Even the most well-structured strategies can fail if they aren't regularly evaluated and refined. Testing ensures your business can actually recover when an incident occurs — not just on paper, but in reality.

Three essential ways to test your BCDR plan:

- Walk-throughs: Reviewing step-by-step procedures with your team.
- Tabletop exercises: Simulating different disaster scenarios.
- Live failovers: Testing real-time system recoveries.



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

BCDR lessons: The high cost of breaches and downtime

Outages and downtime are no longer rare incidents; they are a **constant, costly threat for SMBs**. Alarmingly, the **State of BCDR 2025 Report** reveals a troubling reality**:**

- Only about 40% of IT teams feel confident that their backup system can protect critical data during a crisis.
- Close to 30% of IT pros lose sleep over their organization's backup and recovery preparedness.
- The rest (30%) worry their current solution isn't capable of handling a real-world disaster.

And the financial impact is staggering. **Another recent survey[2] found that:**

- Around 50% of businesses experienced IT outages costing more than $100,000.
- Another 16% reported losses exceeding $1 million from their most recent outage.

Now, let's look at two real-world incidents from 2024, where a stronger BCDR strategy could have made all the difference.

The Change Healthcare ransomware attack

The incident: In February 2024, Change Healthcare, a subsidiary of UnitedHealth, fell victim to a ransomware attack by the notorious BlackCat gang. Using stolen credentials, the attackers infiltrated the company's systems, exfiltrated 4 TB of sensitive patient data and deployed ransomware that crippled billing, payments and other critical healthcare operations.

The impact: Change Healthcare processes nearly 40% of all U.S. medical claims, and the attack severely disrupted healthcare services nationwide, delaying patient treatments and financial transactions. The stolen data, including personal, payment and insurance details, was leveraged for a ransom demand of $22 million — which was reportedly paid.

The fallout: Investigations revealed that the breach was preventable. It was caused by a lack of multifactor authentication (MFA) on remote access servers, which is a clear violation of the Health Insurance Portability and Accountability Act (HIPAA) compliance. The Office for Civil Rights (OCR) of the U.S. Department of Health and Human Services (HHS) has since launched investigations into the security failures that led to this catastrophic breach.

How a robust BCDR strategy could have prevented this:

- Enforcing MFA on all remote access points would have blocked attackers from using stolen credentials.
- Immutable backups would have protected critical data from encryption and ransom demands.
- Incident response drills could have prepared IT teams for faster threat detection and containment.

The Ticketmaster data breach

The incident: In May 2024, Ticketmaster Entertainment LLC suffered a massive data breach at the hands of ShinyHunters, a well-known cybercriminal group. The attackers infiltrated a third-party cloud storage platform, stealing 1.3 TB of customer data, and demanded a $500,000 ransom.

The impact: The breach exposed the sensitive information of over 40 million users, including order history, payment details, names, addresses and email accounts. The incident caused widespread panic as customers scrambled to secure their accounts and prevent fraud.

The fallout: Beyond reputational damage, the attack led to legal consequences. The Justice Department filed a civil antitrust lawsuit against Ticketmaster and its parent company, Live Nation, compounding their financial and operational strain.

How a robust BCDR strategy could have prevented this:

- Zero trust security and stronger access controls could have prevented unauthorized access to cloud storage.
- Encryption and tokenization of customer data would have minimized the impact of the breach.
- A rapid IRP could have contained the attack before massive data exposure.

What's downtime really costing you? Find out now! Use our Recovery Time and Downtime Cost Calculator to get a real-time estimate of your financial risks based on key business metrics. The numbers might surprise you!

Calculate your downtime cost now.

BCDR strategies: Basic four foundations for a resilient recovery plan

To build a resilient, disaster-proof business, SMBs need the right mix of technology, automation, security and compliance. **Here's how to get it right:**

Choose the ideal backup solution

Your recovery time objective (RTO) and recovery point objective (RPO) determine how quickly and how much data you can restore after an outage. Before choosing a backup solution, ask:

- How fast do we need to recover? (RTO)
- How much data can we afford to lose? (RPO)
- Where and how will we recover data — on-prem, cloud or hybrid?

A workload-based approach is crucial here: mission-critical applications require low RTO and RPO, while less critical workloads can have longer recovery windows.

Pro tip: Finding the balance between local and cloud backup

Local backup ensures faster restores when everything is operational, but what if the power goes out, hardware fails or a disaster strikes? Cloud backups provide off-site protection, but restore speeds depend on bandwidth — and cloud services can fail, too.

The best strategy? A hybrid-cloud solution. It stores data locally for quick recovery while also replicating it to the cloud for off-site protection, offering the best of both worlds.

Automate backup and failover processes

Manual backup processes invite errors, delays and data gaps. Automating backup and failover ensures continuous protection and instant system recovery when disaster strikes.

Key elements of automation:

- Scheduled, real-time backups to prevent data loss.
- Automated failover to minimize downtime.
- Backup verification to ensure recoverability.

Automating backups is crucial, but automating testing is just as important. It ensures that recovery plans work flawlessly and identifies gaps before a real disaster exposes them.

Strengthen cloud and SaaS resilience

SaaS applications like Microsoft 365, Google Workspace and Salesforce store critical business data. However, they don't offer full protection against accidental deletion, cyberattacks or service outages.

Key strategies for cloud and SaaS resilience:

- Third-party backup solutions to prevent data loss from SaaS apps.
- Geo-redundancy to ensure availability even if a cloud region fails.
- Strong access controls and encryption to protect against insider threats.

It would be a grave mistake to assume that your cloud provider fully protects your SaaS data. Shared responsibility models mean you are responsible for backing up and recovering your critical data, not them.

Stay compliant with industry regulations

Regulations like the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA) and the HIPAA require businesses to secure, back up and recover data efficiently.

Here's what's at stake for some common compliance violations:

Compliance legislation	Potential penalties
HIPAA	Fines up to $250,000 and 10 years imprisonment
GDPR	Fines up to $21 million or 4% of global annual revenue, whichever is higher
CCPA	Civil penalties up to $7,500 per violation, with other violations capped at $2,500 per violation

It isn't just about avoiding fines, though; it's also about protecting customer data and maintaining trust.

BCDR planning: Laying the groundwork for resilience

As Abraham Lincoln famously said, "Give me six hours to chop down a tree, and I will spend the first four sharpening the axe." The same applies to BCDR — the better you prepare, the faster you recover. Here's how to plan an effective BCDR strategy:

Step 1: **Build a BCDR team and define roles**

BCDR success starts with a dedicated team. Assign clear roles and responsibilities, ensuring key personnel know who takes charge of what during a crisis. Your team should include:

- Incident coordinators to oversee response and recovery efforts.
- IT and security teams to manage data protection, failovers and system restoration.
- Communication leads to inform employees, customers and stakeholders.

Step 2: **Develop a comprehensive disaster recovery plan (DRP)**

A disaster recovery plan (DRP) outlines how to restore critical systems after a disruption. It should include:

- Step-by-step recovery procedures for different disaster scenarios.
- Data backup locations and recovery methods.
- Emergency contacts and escalation processes.

Step 3: **Define RTOs and RPOs based on business impact**

Not all systems are equally critical. Conduct a business impact analysis (BIA) to classify systems and define your optimal RPOs and RTOs. Critical systems require near-instant recovery, while others may have longer recovery windows.

Step 4: **Test and update your plan regularly**

A BCDR plan that isn't tested is as good as no plan at all. Periodic testing and plan updates ensure your recovery strategy works when it matters most.

- Tabletop exercises to simulate real-world disaster scenarios.
- Live failover tests to verify backup integrity.
- Annual plan reviews to update roles, technologies and compliance requirements.

The Datto advantage: Unmatched BCDR for total resilience

Not all BCDR solutions are created equal. Datto's comprehensive BCDR platform ensures seamless, instant recovery — no matter where your data resides, whether it's on-premises, in the cloud or anywhere in between. Designed for SMBs, Datto delivers end-to-end protection with fast recovery, ransomware-resistant backups and a hybrid-cloud approach for ultimate resilience.

Here's what sets Datto apart:

Instant virtualization:
Spin up systems locally or in the cloud within seconds, keeping operations running while full recovery takes place. Traditional backups can take hours or days to restore, but Datto eliminates the wait.

Immutable backups and ransomware protection:
Datto Cloud backups cannot be altered, deleted or encrypted, even by ransomware.

- Hardened Linux architecture that prevents unauthorized changes.
- Built-in ransomware detection that scans for malware before recovery.
- Immutable cloud snapshots that keep your data untouchable.

Hybrid-cloud resilience: Unlike local-only backups that fail in disasters or cloud-only backups that can be slow to restore, Datto's hybrid-cloud model provides:

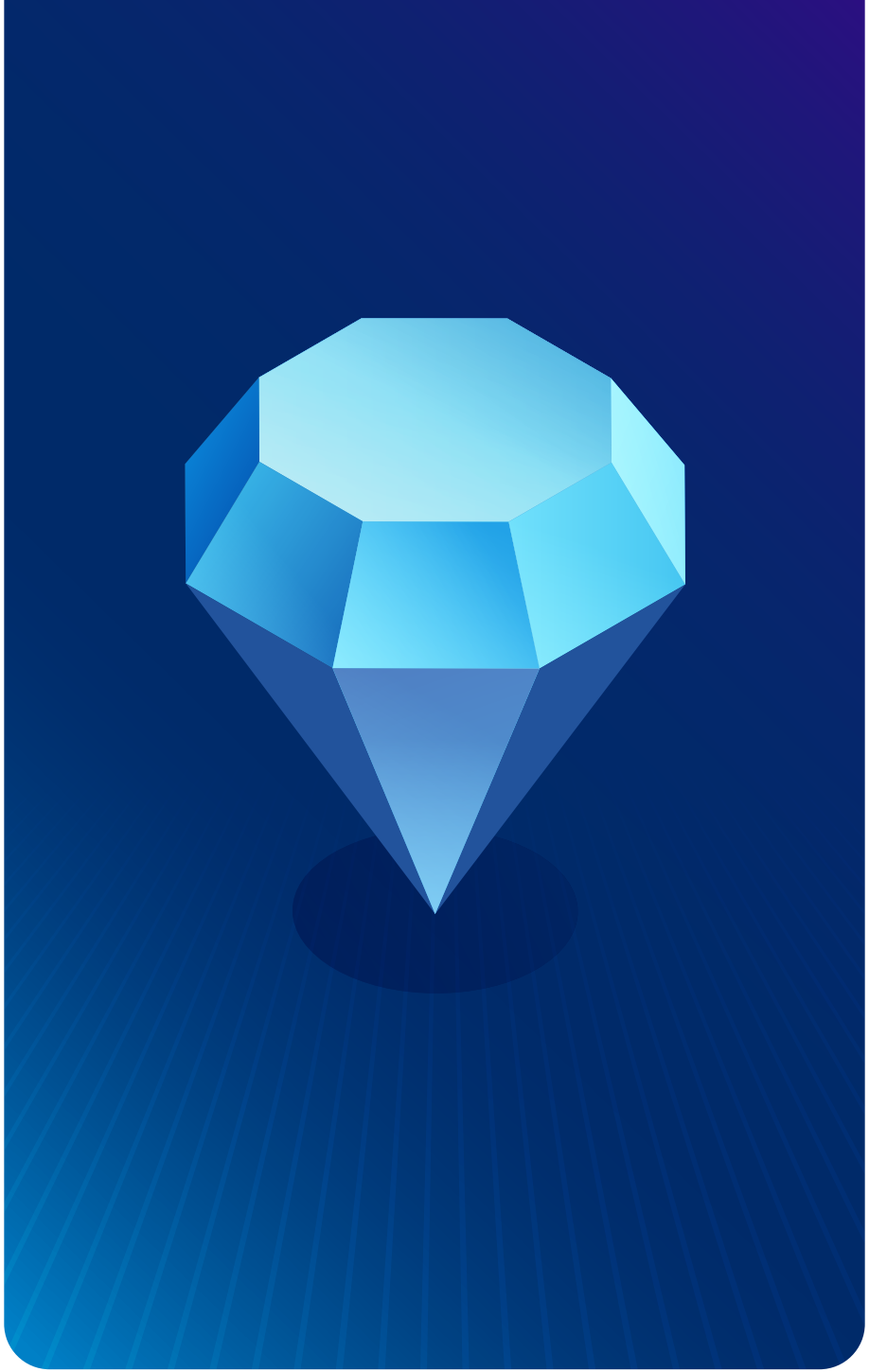
- Local backups for ultra-fast recovery.
- Cloud replication for off-site protection.
- Seamless failover between local and cloud environments for uninterrupted business continuity.

With Datto BCDR, businesses don't just back up data — they ensure continuous operations, minimal downtime, and fast, reliable recovery when it matters most.

Datto in action: Keeping a luxury resort running after a ransomware attack

For a high-end resort, downtime isn't an option, especially on one of its busiest days of the year. However, when ransomware struck, operations across a 180-room luxury hotel froze — from restaurant transactions to guest check-ins and check-outs. With nine out of ten servers and 30 workstations infected, the resort faced a devastating loss of revenue and customer trust.

Thankfully, the resort had a Datto-powered BCDR strategy in place. By 10 AM, IT teams identified the last clean backup, which was a snapshot taken just hours before the attack. Using Datto's instant virtualization, they quickly spun up critical servers both locally and in the cloud, restoring key systems in just 10 hours. Within 13 hours, the resort was fully operational, avoiding days of costly downtime and a massive ransom payment.



"The client was skeptical that recovery could be achieved without paying the considerable ransom. We stated we were confident it would take nowhere near that time,"

says Linda Kuppersmith, President and CEO, CMIT Solutions Stamford.

The rapid recovery reinforces why having the right BCDR solution is crucial. With immutable backups, hybrid-cloud resilience and instant failover, businesses can recover quickly and come out stronger after an attack — just like this resort did with Datto.

Identify gaps in your disaster recovery plan and ensure your business is fully prepared for any disruption. ***Download the BCDR readiness checklist now.***

Unexpected disruptions can bring businesses to a standstill. However, with the right BCDR solution, recovery doesn't have to be uncertain or slow. Datto's BCDR solutions go beyond traditional backup, offering instant failover, immutable security and hybrid-cloud flexibility to keep businesses running smoothly, no matter the challenge. Don't just react to disasters — be ready for them. Ensure fast, seamless recovery when every second counts.

See how effortless, reliable recovery works in action.

GET A DATTO BCDR DEMO TODAY

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