datto
A Kaseya COMPANY

PREPARE, PROTECT & RECOVER

Data Resilience Checklist for IT Teams

Organizations today face significant risks in securing their critical data. The move to hybrid and multicloud environments has resulted in data being dispersed across various platforms and locations, introducing complex protection challenges. At the same time, cybercriminals are leveraging advanced technologies (AI-powered) to launch increasingly sophisticated attacks that can penetrate even the strongest defenses. Over 95% of security professionals worry that their organization may experience an AI-driven cybersecurity incident. In 2023, the global count of malware attacks surged to 6.06 billion, a 10% rise from the previous year. Amid surging cyberattacks, natural disasters and human errors, organizations are at a critical crossroads.

Data resilience is the key to navigating this intricate threat landscape. This strategic approach ensures your business-critical data remains secure and accessible, even during cyberattacks or other unplanned events. To achieve data resilience, we recommend a three-pronged strategy — **Prepare, Protect and Recover**. This checklist will guide you through the challenges and best practices for building a robust backup and recovery plan. Consider these criteria when developing your data protection strategy to achieve complete data resilience.

1. Prepare: Brace for the modern data threats

Modern businesses face various data threats with increased intensity and severity that can disrupt business continuity. Let's explore some of the most prominent threats and the backup and disaster recovery (DR) features that can help you address them.

TYPE OF DATA THREATW	FEATURES TO TACKLE IT	
Cyberthreats, like ransomware, malware and phishing	**Hardened appliance kernel:** Windows is the primary target for threat actors, responsible for nearly 90% of all malicious files detected daily. Leveraging Linux-based backup appliances makes them more difficult to compromise due to their hierarchical architecture. Using Linux-based OS also differentiates your backup environment from production, camouflaging backups from Windows-seeking malware.	☐
	Role-based access control (RBAC): RBAC restricts unfiltered access to your backup environment. Define each user's scope based on the operations they need to perform, and the systems and backups they need to access.	☐
	Immutable storage: Ransomware attacks actively target backup repositories. However, immutable storage enables you to store data in a format that cannot be modified, encrypted or deleted. This secures your backups from ransomware since no external client can read, modify or delete data once it has been ingested and stored immutably. Leverage immutability as part of your off-site backup copy strategy (such as the cloud) to further increase resilience.	☐
	AES encryption: To enhance the security of your data backups, ensure they are adequately encrypted at-rest on the local appliance, in-transit to a secondary recovery target and at-rest on the target.	☐
	Integrated anti-phishing defense: Cyberthreats, like ransomware, are often deployed via spam and phishing emails. Leveraging a solution that alerts employees of external, spoofed or imitated users enables them to quarantine suspicious emails for IT review and investigation via automated workflows and feedback loops.	☐
Hardware failures	**Cloud backup**: Storing up-to-date backup copies in the cloud will enable you to spin up the specific systems or infrastructure in the cloud when there is a hardware malfunction.	☐
	On-appliance Local Virtualization: A dedicated, purpose-built backup appliance should offer you the capabilities and resources to virtualize directly on-appliance for short-term business continuity during a disaster to minimize downtime.	☐
Human errors like accidental deletions and malicious insiders	**Regular backups:** Maintaining up-to-date backups is key to avoiding data loss by accidental deletion. Look for solutions that offer policy-based or predefined, automated backup scheduling (with the ability to run backups on-demand at any time) to easily align the backup cadence to your recovery point objectives (RPOs).	☐
	Cloud Deletion Defense™: Leverage advanced solutions, like Datto BCDR, that come with Cloud Deletion Defense™, adding an extra layer of protection against accidental or malicious deletion of cloud backups.	☐
	Restrict admin privileges: Limit access to systems and applications for users depending on their role. Access control helps you avoid data misuse to an extent.	☐
Natural disasters	**Cloud-based disaster recovery:** Cloud-based disaster recovery is an effective way to protect against data loss caused by natural disasters. If your primary site is damaged, you can recover your workloads in the cloud.	☐
	Geo-redundancy: Geo-redundancy is a key strategy for mitigating the impact of natural disasters. By replicating data across multiple data centers in different geographical regions, your organization can continue operations even in the face of large-scale environmental events.	☐

Sprawling data footprint	**One-stop shop for data backup and recovery:** Your data now resides in more places than ever before — on-premises, cloud, SaaS applications and remote endpoints. Leverage an all-in-one solution that can comprehensively secure your data across all these environments and locations. This eliminates data silos and any existing gaps in coverage. A singular solution also means one set of tools, common processes and a unified user experience.	☐
Data/platform migration	**Future-proof your investment:** Many organizations are undergoing rapid change as data migrates from on-prem to the cloud. Secure your investment by looking for vendors that offer protection for a variety of platforms and offer flexibility to transition from one module to another, without being locked into an underlying infrastructure or platform.	☐

2. Protect: Bolster your defenses to mitigate threats

Adopting a holistic approach that can prevent even the most sophisticated cyberthreats of today and tomorrow is essential to safeguard your business-critical data. Let's look at some features that can help you achieve it.

FEATURE	DESCRIPTION	
Automated backups	Automated backups are pivotal in ensuring your business-critical data is backed up without hiccups. It significantly reduces your organization's RPOs, minimizing data loss should an incident occur. Also, look for more frequent backups by default, for example, hourly, to ensure your most critical data is readily available.	☐
Flexible options for data protection	Your backup and recovery solution should offer flexible options to protect data at the file, image or application level. Look for a solution that provides the following benefits: • Ability to restore files, folders or the entire base image. • Options to virtualize locally on the backup appliance in the event of a local disaster. • Ability to restore at the virtual machine and hypervisor level (i.e., OS drive). • Flexibility to migrate machines to other hypervisors or physical hardware as needed.	☐
Predictive threat detection	You can detect an intrusion in near real-time by leveraging artificial intelligence (AI) and machine learning. AI helps identify anomalies in data and automatically alerts admins, enabling them to take immediate action to slow the spread of the threat and speed up recovery efforts.	☐
Internal anomalous monitoring and detection	AI-powered solutions can also help identify threats that conventional security tools can't, such as misconfigurations, unauthorized logins, new devices being added to the network, gaps in backups, admin rights being granted and more.	☐
MFA	Multifactor authentication (MFA) helps authenticate users, devices and other assets based on transactional risks (security and privacy risks of individuals and the organization), reducing the chances of account takeover (ATO) attacks.	☐
Purpose-built cloud	Leverage a dedicated cloud that can offer turnkey solutions specifically optimized to meet the needs of your immutable off-site storage, long-term retention and DR. This also helps you utilize functions delivered "as-a-Service," like Disaster Recovery-as-a-Service (DRaaS), reducing your CapEx costs and the reliance on your internal IT.	☐

3. Recover: Be ever ready for instant recovery

In the realm of data protection, preparing for the worst is imperative. Should you fall victim to a data disaster, you should be prepared to restore your most critical systems and recover essential information swiftly. The following attributes will significantly help you do that.

FEATURE	DESCRIPTION	
Screenshot verification	Screenshot verification ensures your virtual machines (VMs) boot correctly from backups and are recoverable. Look for a solution that offers automated verification to save you the time and cost it takes to perform manual spin-up.	☐
Application-level certification	Screenshot verifications, however, don't provide any means of identifying data corruption within backups or whether applications and services are functional upon recovery. Look for a solution offering the ability to certify backups at the application level to verify that workloads will perform as expected upon restoration.	☐
On-demand DR testing	Regular DR plan testing and validation is the only way to ensure you can recover swiftly and effectively when disaster strikes. However, many organizations do not test their DR plans often, citing the time, resources and money needed to invest. Fortunately, cost-effective, intelligent technologies available today can automate and orchestrate DR testing. Look for a solution that facilitates testing in a predetermined, isolated environment on a set schedule according to predefined parameters, such as boot orders, networking and more — all without affecting the production environment.	☐
Compliance tracking	To ensure your organization's backup and recovery strategy meets the demanded recovery time objectives (RTOs) and RPOs under the SLAs, it is important to have a solution that allows tracking and reporting of actual recovery point and recovery time. This helps ensure that set goals are being met and any deviations can be identified and addressed promptly.	☐
Local verification	Look for a backup solution with the Local Verification feature, which checks the health of a backup snapshot at the file level to ensure data integrity. This helps you choose the best recovery points for restoration in case of a disaster.	☐
Exportable reports	Your solution should provide exportable reporting, such as backup dates/times, screenshot verification status, recovery point integrity and retention settings, on all testing outcomes to support compliance with your DR plan.	☐
Quick file recovery	Removing the malware and recovering any infected files may prove sufficient if the infection is caught early and contained to specific systems. To achieve this, your solution should make finding and restoring individual files from backups easy, with only a few clicks. Indexed search capabilities and self-service features with RBAC can help. These features will not only save time but also ensure that the recovery process is intuitive and secure.	☐
Flexible recovery options	Your solution must support a variety of recovery modes, including physical-to-virtual (P2V), virtual-to-virtual (V2V), virtual-to-physical (V2P) and bare metal replicas, while also allowing for flexible asset and data recovery locations.	☐
Instant recovery	When a cyberattack occurs, it is crucial to act promptly to prevent the spread of the infection, investigate the incident, eliminate the threat and restore normal operations. Suppose a server or virtual machine is compromised. In that case, your appliance should be capable of orchestrating a failover process to quickly bring applications back up from your most recent verified backup with a near-zero RTO.	☐
Bare metal recovery	Bare metal recovery (BMR) technology facilitates disaster recovery of protected assets, enabling system and application recovery across servers with different hardware configurations and from various vendors.	☐
DRaaS	DRaaS can help you reduce cost, complexity and time to recovery in the event of an attack. DRaaS providers offer a secure cloud environment that allows for rapid spin-up of critical systems and applications and assists in redirecting user traffic until the on-premises site is fully operational.	☐

In your pursuit of data resilience, it is important to keep in mind that it is an ongoing and complex journey. These features and attributes will help you confidently navigate the multifaceted landscape of data protection challenges and attain complete data resilience.

Achieve data resilience with Datto Unified Backup

Now that you know what to look for in a data backup and recovery solution, take a look at Datto Unified Backup, the one-stop shop for all your business continuity and disaster recovery (BCDR) needs. No matter where your data lives, Datto Unified Backup can comprehensively protect it, all while significantly cutting down your management time and expenditure. Datto offers comprehensive backup and recovery for on-premises workloads, SaaS applications, cloud workloads and endpoints, all managed from a single, elegant portal.

READY TO EMBRACE SIMPLER, BETTER BACKUP WITH DATTO?

REQUEST YOUR DEMO TODAY