CHECKLIST

Achieving Data Resilience With Unitrends: Prepare, Protect & Recover

Organizations navigate a minefield of risks in today's digital world to secure their business-critical data. Ongoing cloud adoption has given rise to hybrid and multicloud environments, where data is dispersed across diverse platforms, providers and locations, introducing complex data protection challenges. Meanwhile, cybercriminals are leveraging cutting-edge technologies and innovative tactics to launch increasingly sophisticated attacks that could leave even the most advanced defenses vulnerable. While also considering the other familiar data threats, like natural disasters and human errors, organizations currently find themselves at a crossroads.

Achieving data resilience is the key to successfully navigating this increasingly intricate threat landscape. Data resilience is a strategic approach that will help you rise to today's complex data protection challenges and keep your business-critical data completely secure and readily available. It will empower you to continue your business as usual, even during cyberattacks and other data threats.

But how do you achieve data resilience? This checklist is designed to help you answer that exact question. We suggest adopting a three-pronged approach of prepare, protect and recover to comprehensively protect your business-critical data and achieve data resilience. While exploring this strategy, we will look in-depth at the various data protection challenges you could face and the best practices to overcome them efficiently. Consider these criteria while evaluating your data backup and recovery strategy to achieve complete data resilience.

1) Prepare: Brace for the modern data threats

Organizations today face an array of data threats that can impact their business continuity. Let's examine some of the most prominent data threats and the features that could help you tackle them.

TYPE OF DATA THREAT	FEATURES TO TACKLE IT	
Cyberthreats like ransomware, malware and phishing	**Hardened appliance kernel:** Windows OS is a prime target for threat actors, with over 97% of malware and potentially unwanted applications (PUAs) created targeting the Windows OS. Leverage Linux-based backup appliances since their hierarchical architecture makes them more difficult to compromise. 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 changes since no external client can read, modify or delete data once it has been ingested and stored immutably. Leverage immutability as part of your offsite (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 very often deployed via spam and phishing emails. Leverage a solution that alerts employees of external, spoofed or imitated users and 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.	☐
Human errors like accidental deletions and malicious insiders	**Regular backups:** Maintaining up-to-date backup is key to avoiding data loss by accidental deletions. Look for solutions that offer policy-based scheduling to easily align the backup cadence to your RPOs.	☐
	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 infrastructure 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 daily backups	Automated daily backups are pivotal in ensuring your business-critical data is regularly backed up without hiccups. It significantly reduces your organization's recovery point objectives (RPO), reducing the amount of data loss should an incident occur. Also, look for more frequent backups by default, for example, hourly, to ensure the ready availability of your most critical data.	☐
Wide coverage and policy-based management	Your backup solution should be able to natively support the hundreds of versions of operating systems, hypervisors and applications. Furthermore, administrators should have the flexibility to choose how backups are scheduled, either by defining a specific schedule or through intelligent policy-based scheduling technology.	☐
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 + dark web monitoring	Multifactor authentication (MFA) helps in authenticating users, devices and other assets by the transactional risks (security and privacy risks of individuals and the organization), which can prevent account takeover (ATO) attacks. Combining that with dark web monitoring helps identify potentially vulnerable accounts before any malicious incident occurs. This is very effective against today's sophisticated ransomware attacks.	☐
Purpose-built cloud	Leverage a dedicated cloud that can offer turnkey solutions specifically tuned to meet the needs of your immutable off-site storage, long-term retention and disaster recovery (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 in that endeavor.

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	However, screenshot verifications don't provide any means of identifying data corruption within backups or whether applications and services are functional upon recovery. Look for a solution that certifies backups at the application level, often through automated scripting, to verify workloads will perform as expected upon restoration.	☐
Automated DR testing	Regular DR plan testing and validation is the only way to ensure you can recover swiftly and effectively when a 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 automates testing in a pre-determined, isolated environment on a set schedule according to predefined parameters such as boot orders, machine reconfiguration and application verification — all without affecting the production environment.	☐
Compliance tracking	To ensure that your organization's backup and recovery strategy meets the demanded 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 to ensure that set goals are being met and any deviations can be identified and addressed promptly.	☐
Audit-mode restore	Audit mode is a method of recovery that enables you to selectively verify that particular machines can be recreated from any given recovery point. Isolated from production (no network connectivity), audit-mode restores verify that machines are booting correctly and that data is accessible. Upon verification, the audit-mode instance can be safely torn down. This is really helpful in constantly verifying the recoverability of your mission-critical applications following a ransomware or other cyberattack.	☐
Exportable reports	Your solution should provide exportable reporting 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 role-based access control 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 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, remember it's an ongoing journey filled with complexities. 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 Unitrends Unified Backup

Now that you know what to look for in a data backup and recovery solution, take a look at Unitrends Unified Backup, the one-stop shop for all your business continuity and disaster recovery (BCDR) needs. No matter where your data lives, Unitrends Unified Backup can comprehensively protect it, all while significantly cutting down your management time and expenditure. The Unitrends platform 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 UNITRENDS?

REQUEST A DEMO TODAY!

ABOUT UNITRENDS

Unitrends makes efficient, reliable backup and recovery as effortless and hassle-free as possible. We combine deep expertise gained over 30 years of focussing on backup and recovery with next-generation backup appliances and cloud purpose-built to make data protection simpler, more automated and more resilient than any other solution in the industry.

UNITRENDS
A Kaseya COMPANY