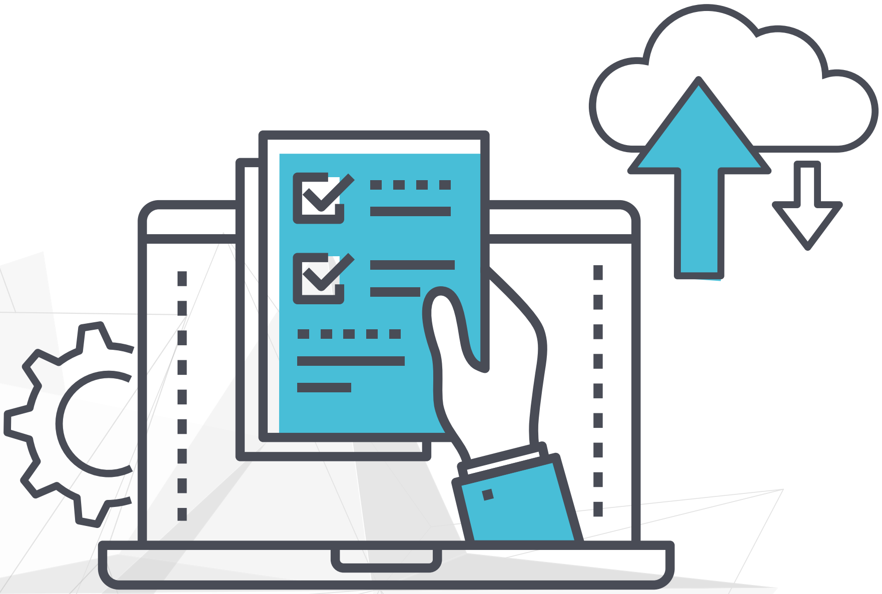
UNITRENDS

BACKUP AND DRaaS IT BUYER'S GUIDE

SOLUTIONS TO OVERCOME DATA LOSS AND DOWNTIME



Introduction

When evaluating solutions for business continuity and disaster recovery (BCDR), what exactly are you looking for?

Is it a solution that is agile and complete to ensure resilience for your unique combination of physical, virtual and cloud workloads?

Is it a solution that leverages automation and artificial intelligence to simplify complex workflows, eliminate manual tasks and provide confidence in recovery?

Is it a solution that future-proofs and secures your investment in today's ever-evolving dynamic data protection landscape?

An effective backup and disaster recovery strategy is imperative in today's always-on digital economy laden with cyberthreats. According to IBM's Cost of a Data Breach Report 2023, organizations with high levels of IR planning and testing saved $1.49 million on average compared to those with low levels. The global average total cost of a data breach was at an astounding figure of $4.45 million in 2023. With cybercrime expected to skyrocket in the coming years according to Statista, backup and disaster recovery play a critical role in empowering organizations to navigate the complex terrain of the digital world.

However, traditional backup and disaster recovery solutions are siloed, leaving large gaps in protection. They force organizations either to compromise on functionality or to pay higher costs and then stitch together disparate components to compensate for the lack of completeness.

A backup solution sits at a vantage point since it touches all corporate data and most of an organization's applications. Choosing the right solution involves more than just investing in a basic backup. Many vendors are bringing new and exciting technologies in the form of artificial intelligence, machine learning and predictive analytics to make IT administrators more efficient and productive at their jobs.

Before choosing a backup solution provider, it's essential to understand the wide variety of offerings, what to look for and where potential gaps in coverage exist to put your organization in the best position to eliminate data loss and downtime risks.

How to Use This Guide

This buyer's guide is designed to help you understand the options in the data backup and disaster recovery market today and provide insights into emerging technologies. Why? With hundreds of vendors and innovations in data storage, infrastructure and data management, there are multiple strategies to consider. By understanding which solution meets the needs of tomorrow, you'll be well-positioned to protect your infrastructure.

As you evaluate your next solution, keep the following goals in mind:

1. Protect data center workloads, storage devices, cloud-based workloads, SaaS data and remote endpoints.
2. Achieve near-zero recovery time objectives (RTOs) from outages, malware attacks and other data loss events locally, at remote locations and in the cloud.
3. Optimize near-zero data loss (RPO) and long-term data retention.
4. Leverage cloud technologies to avoid disaster and maintain continuity.
5. Guarantee 100% recovery confidence with automation for environmental self-healing, recovery testing and compliance reporting, all backed by exceptional technical support.

We shed light on each of these goals. At the end of each section, we've created a checklist to use in evaluation to ensure your solution is the best the market offers.

Protecting your evolving data center

IT environments are increasingly complicated, with data living on traditional infrastructure, clouds and SaaS applications, and remote endpoints. The way we think about traditional infrastructure is also changing with the emergence of new technologies in the hyperconverged space, such as Nutanix, Scale and Cisco UCS. Balancing a myriad of technologies can be complex; however, protecting it doesn't have to be. You require agile protection for all workloads with an all-in-one approach to backup, recovery automation and cloud continuity that works with all computing styles. This will help in boosting your productivity and enable IT to accomplish more with less. Today's leading data protection solutions have compatibility to protect a diverse range of infrastructures and are pre-integrated and optimized to provide high-speed, effortless performance.

Purpose-built appliances

If you were to design a homegrown backup and recovery solution, you'd probably have to integrate a half dozen or more different hardware and software components — servers, storage, deduplication, networking, OS, virtualization, security, analytics, search, monitoring and testing. Unfortunately, many vendors ask you to take that approach by partnering with other suppliers to fill in the gaps rather than delivering their own holistic solution. The time spent on data protection and recovery is directly proportional to the number of components you install, manage and maintain. Organizations using multiple data protection vendors are more likely to struggle with data loss and downtime since incorporating different solutions tends to add layers of unnecessary complexity.

In response, many vendors are delivering modernized solutions with an integrated approach — offering IT deployment of a complete, agile solution designed to protect all types of data and applications apart from providing native capabilities. Such capabilities are often supplemental to backup and recovery, including compression, deduplication, WAN acceleration, recovery testing, reporting and more. In other words, a purpose-built backup appliance. A modern, intuitive user experience is a priority. It may be achieved through utilizing a single central console to manage protection across many types of digital assets while offering the customization to design optimal backup approaches for each protected workload.

Protection for all workloads

Modern IT environments have a wide range of computing styles, such as on-premises and cloud-based systems (IaaS, PaaS and SaaS), remote endpoints, and new technologies like hyperconverged infrastructure (e.g., Nutanix). Your backup and recovery solution should offer the agility to easily protect hundreds of versions of operating systems, hypervisors, applications and cloud-native formats from a single pane of glass.

Policy-based management and intelligent alerting

Backups should be easy to define and schedule. Administrators should have a choice in how backup schedules are set — either by entering the specific schedules themselves or by using intelligent, policy-based scheduling technology. Policy-based management enables administrators to define their recovery goals (RTOs and RPOs) for all assets grouped under the policy, with the system calculating and filling in the deployment and scheduling details. This form of scheduling enables admins to align data management and availability tactics with business policies without needing granular details, such as file locations and snapshot schedules. Today's backup environments are increasingly noisy. To ensure compliance with your SLAs (RPOs and RTOs), look for a solution that offers customizable, intelligent alerting based on thresholds you set to cut through alert clutter.

Built-in WAN optimization

Moving backup copies to an off-site location is a critical step in disaster recovery. With organizations demanding near-zero RTOs and RPOs, the cloud has become an increasingly popular choice as a replication target. However, for many organizations, their WAN may not be able to handle large amounts of regular data replication. Your backup appliance should offer integrated WAN optimization technologies, such as global, adaptive deduplication, compression, encryption, deduplication acceleration, source querying, simple rate limits and bandwidth throttling. These technologies augment your data protection schemes by reducing the size (and cost) of synchronizing data backups to remote locations or cloud-based Disaster Recovery-as-a-Service (DRaaS).

Data reduction techniques, such as deduplication and compression, reduce the overall size of backup files by eliminating redundancy, saving on storage requirements and making replication more efficient. Deduplication tends to achieve better data reduction efficacy against smaller backup sets, while compression tends to achieve better results against larger data sets.

To ensure you're maximizing all aspects of data protection while keeping administrative time and cost commitments to a minimum, the following technologies should be a part of your data protection solution:

Checklist:
Optimizing Protection for Everything in Your Evolving Data Center

Capability To Look For	Description	
Holistic data protection platform	Multivendor protection strategy greatly increases IT complexity, cost and risk. Reducing the number of unique backup solutions means managing fewer licenses, maintenance and service agreements.	□
Purpose-built appliance	A purpose-built, all-in-one solution is easier to deploy, upgrade, manage and service.	□
Intuitive global user interface (UI)	Modern, simple yet intuitive user experience is a priority. Operating your backup system without referring to a manual should be possible, so substitutes can stand in when primary admins are unavailable.	□
Wide range of compatibility	Your backup and recovery solution should be able to protect hundreds of versions of operating systems, hypervisors, applications and cloud-native formats with different approaches (file-level, image-level, host-level, etc.) depending on your recovery requirements.	□
Policy-based management	Admins should have the choice of how backups are set — either by entering the specific schedules themselves or utilizing intelligent, policy-based scheduling technology.	□
Native data reduction techniques	Data reduction techniques, such as deduplication and compression, reduce the overall size of backup files by eliminating redundancy, saving on storage requirements and making replication more efficient.	□
Cloud-enabled	Integrated support for multiple types of clouds, including private and hyperscale clouds and cloud storage platforms — AWS, Azure and Google Cloud Platform (GCP), Rackspace and Wasabi.	□
RESTful API	RESTful API is an architectural style for an application program interface (API) that uses HTTP requests to access and use data. REST tends to use less bandwidth than similar technologies and can easily integrate with other applications.	□
AES encryption	Military-grade encryption should be utilized to secure all in-flight and at-rest data.	□
Intelligent alerts	You should be able to customize thresholds for alerts to cut through the clutter. This enables you to prioritize alerts for issues that directly impact your recovery SLAs, like skipped backups or replication.	□

Strategies to beat downtime

While being able to instantly recover workloads with zero downtime is ideal, putting in place the resources to achieve that objective may not be affordable for every application. Organizations need to inventory their applications and workloads and triage them by their importance to keep their business functioning. The most robust backup and recovery capabilities are suitable to protect mission-critical applications compared to applications that can be temporarily offline. With a well-crafted disaster recovery (DR) plan, you can set priorities for workloads. DR planning can involve structuring recovery in a tiered format to cut downtime and protect high-priority data.

The following features should be considered to support mission-critical applications:

Local disasters — utilize an appliance

Today's purpose-built backup appliances are equipped with full computing platforms, boasting robust CPU and memory resources, large storage volumes, backup software and remote management capabilities. These appliances are your first line of recovery. If a server, virtual host or data center rack goes offline, you can spin up and run any failed applications directly on the appliance from a recent backup data copy. The appliance may also support the recovery of virtual environments by acting as a temporary data store in an instant recovery process. With this method, backup data is injected into a share mounted to the appliance to spin up virtual machines (VMs) much more quickly than rebuilding the backup chain on the VM's attached storage. Appliances may also create and act as a storage location for replicas and standby copies of production machines, kept updated with every backup and stored in a warm state ready for immediate failover into production.

Site-level disasters — support for multiple locations

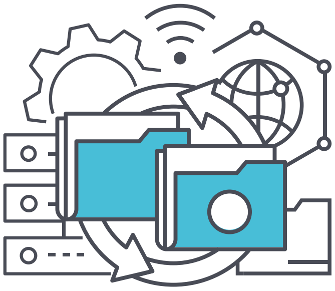
Backup and recovery solutions can be managed remotely, meaning organizations no longer need IT staff present at every server location. A singular appliance UI should enable you to manage all remote devices. Appliances in different locations may serve as replication targets for other appliances so that a site-level disaster, such as electrical failure or flood, does not bring down an entire enterprise. Should an organization not have multiple locations or the resources to support a colocation, cloud-based DRaaS providers enable rapid spin-up of mission-critical applications and redirect user traffic to hosted workloads, minimizing the impact of a site-wide outage.

Enterprise-level disasters — mitigate ransomware and cyberthreats

Ransomware cripples IT environments by disabling security services and backup utilities and destroying backups. Cybercriminals look to exploit gaps in environments that may arise from utilizing multiple solutions since the increased complexity of the environment makes securing infrastructure a challenge. Secure, well-tested backups are your last line of defense against such an attack. Look for a backup solution that is delivered in hardened Linux. It helps differentiate and camouflage the backup environment from ransomware attacks as it lies outside the attack surface that predominantly targets Windows-based systems. The popularity of the Windows OS and its "open architecture" makes it a prime target for threat actors. In contrast, the hierarchical nature of the Linux operating system and additional hardening of the appliance kernel help further secure the backup environment.

You must also implement multifactor authentication (MFA) and role-based access control (RBAC) to strengthen the security of your backup environment further. This allows you to restrict unauthorized and unwarranted access to your full backup environment. Similarly, look for a solution that leverages immutable cloud storage to secure your offsite backups. Immutable storage enables you to store data in a format that cannot be modified, encrypted or deleted, protecting your backups from ransomware changes. Artificial intelligence (AI) is another close ally for you in your defense against ransomware. You can detect an intrusion in near real-time by leveraging AI and machine learning. It 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.

Avoid data loss



Once you've classified and tiered mission-critical applications from those that don't require aggressive RTOs, you can determine the RPOs for all applications. Do it by understanding how much data you can afford to lose in the event of an incident or outage. In other words, they inform the frequency required of your backup schedules or policies.

When evaluating a solution, consider the following capabilities to help you define and deliver on your RPOs:

AI-based ransomware detection

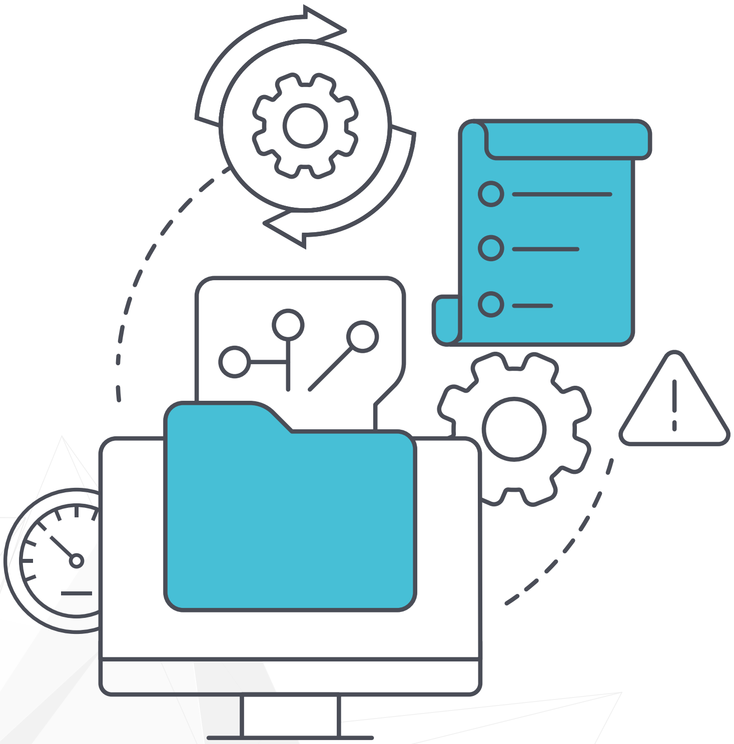
Data is becoming more lucrative for attackers, and ransomware remains the most prominent cyberthreat today. Modern variants are designed to overcome security and backup defenses by staging phased attacks to defeat backups in multiple ways. These are typically done by building in periods of gestation and dormancy before the detonation of the payload. Early detection means faster recovery. Vendors are increasingly leveraging artificial intelligence and machine learning to identify attacks and alert admins of abnormal data fluctuations as backups are ingested. Heuristics such as change rate prediction, data entropy, variance in compression and deduplication rates, and randomness of data creation are some of the metrics that help detect an active ransomware infection in near real-time. Post identification of the infection, notifications should be automatically sent to admins, and any potentially infected files should be flagged to prevent their use in recovery.

Data loss prediction

When calculating desired RPO goals, one of the most important things to consider is the potential for data loss due to corruption of stored or in-flight files or failure to capture business data produced during a downtime event. Lost sales records, customer contact information and employee production — all have significant business value. Today, intelligent tools are available that can simulate different outage scenarios to predict how and what types of data can get lost in a downtime event. Proactive testing helps businesses uncover gaps between strategy and goals and the ability to meet them with the current solution as implemented. The visibility enables IT to have metric-based conversations on the RPO goals (that must be set) to achieve the optimal protection strategy for the business.

Application downtime prediction

RTO measures how long it takes to get an organization up and running after a disaster, including full access to critical applications. As environments grow in complexity, applications today are often N-tier or multitiered. This means processing, data management and presentation functions are physically and logically separated across several machines or clusters to ensure services are provided at maximum capacity with dedicated resources for each function. If any of these dependencies is out of line, a critical application remains unavailable to business users. Look for a solution that enables you to identify, simulate and test the multiple steps required to recover complex applications. Testing will identify potential misconfigurations, corruption or other pitfalls that you can remediate before needing to recover in an actual downtime event. Tools that go a step further by tracking RTO will help you understand whether your backup approaches and the recovery methods available are sufficient to meet your objectives. By validating testing down to the application and services level, you will confidently know that your RTOs are achievable.

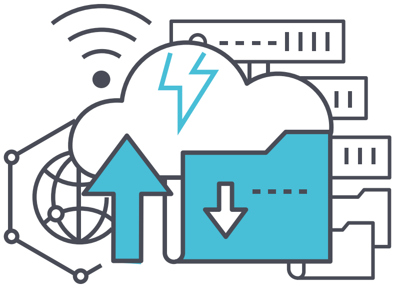


To ensure you can meet the most aggressive RTOs and RPOs, look for the following in your data protection solution:

Checklist:
Avoiding Data Loss and Downtime

Capability To Look For	Description	
Instant recovery from local outages	If a server, virtual host or data center rack goes offline, your backup appliance offers a variety of methods to immediately recover failed applications, whether on the appliance itself or on a secondary host.	□
Management for multiple sites	A single, seamless appliance UI enables you to manage backup and recovery operations across all devices — both on-premises and at any remote location(s).	□
Hardening against ransomware	Backup solution is delivered in hardened Linux to combat ransomware, which predominantly targets Windows-based systems and applications due to their popularity and the security vulnerabilities of their "open architecture."	□
Support for bare metal recovery	Bare metal recovery enables consistent application recovery across servers from varying OEMs and dissimilar hardware configurations.	□
AI-based ransomware detection	The solution leverages AI to measure several heuristics in data to detect an active ransomware infection in near real-time. Once identified, alerts are automatically sent to administrators, and suspected files are flagged.	□
Data loss prediction	Simulates different disasters or outage scenarios to predict what types of data are at risk in an outage and the potential impact of the outage, defining appropriate scheduling approaches to meet RPO goals.	□
Application downtime prediction	Use automation to simulate the recovery process for more complex applications requiring multiple component dependencies.	□
Immutable cloud storage	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 party can read, modify or delete data once it has been ingested and stored immutably.	□
Multi-factor authentication (MFA)	MFA helps authorize users, devices, and other assets by the transactional risks (security and privacy risks of individuals as well as the organization), thereby preventing account takeover (ATO) attacks.	□
Role-based access control (RBAC)	RBAC restricts unwarranted access to your backup environment. You can define each user's scope based on the operations they need to perform and the systems and backups they need to access.	□

Keeping cloud DR from becoming its own disaster



Organizations of all sizes, from large enterprises to one-shop SMBs, are increasingly using the cloud as their DR site. Regularly scheduled backups are replicated and stored securely in the cloud at a low cost, isolated from accidental deletion or ransomware attacks. Cloud-based backup files should serve two purposes — they are preserved to meet data compliance and retention mandates, and they are readily available for disaster recovery.

Long-term cloud retention

With various options for "cheap and deep" storage, the cloud has become a popular option to provide safe, easily recoverable long-term storage. Different types of data across different industries require different retention schedules — whether measured in days, years or indefinitely. The challenge with many public cloud storage providers is that they charge per consumption and for retrieval events. So, as your data grows, or should you require access for litigation, discovery or disaster recovery charges continue to pile up. For long-term retention and DR use cases, look for providers that offer tiered retention-based pricing. This model offers predictable, forecastable total cost of ownership (TCO) for cloud storage without unpredictable access fees or paying for unused storage space. You should be able to select the exact volume of storage and the specific retention period required for each data set to remove the burden of retention management and operational spending. Remote cloud storage may be less labor-intensive and more cost-effective than managing your own physical backup media. Cloud technologies also help achieve more aggressive RTOs when compared to retrieving, rehydrating and restoring data stored on cold media at an off-site location.

Cloud Disaster Recovery-as-a-Service (DRaaS)

With businesses facing increased demands for recovery, evaluating available technologies to determine the best fit to meet a company's unique needs is vital. In response to growing demands, vendors and service providers are now offering DRaaS, designed to supplement an organization's IT team with resources and expertise to automate, accelerate and simplify the recovery of mission-critical applications, whether individually or at scale.

DRaaS is cost-effective and easy to implement and manage compared to maintaining a colocation. Many service providers do the heavy lifting — from installation and implementation to failover and recovery of service, as well as assisting with failback to your primary data center when ready. With DRaaS, organizations not only get a comprehensive disaster recovery plan in place but also benefit from the rich experience of the service providers. This expertise in BCDR helps businesses quickly get back up and running with minimal or no downtime when the unexpected happens.

With DRaaS, companies only pay for the services they use, cutting down costs significantly. DRaaS also allows businesses to mix and match SLAs (typically tied to an RTO) to meet their company's unique objectives. For instance, combining mission-critical systems, such as financial and POS systems, with a one-hour RTO SLA and file shares for the marketing/design department with a 24-hour RTO SLA.

SaaS — protect and recover data for applications running in the cloud

More organizations are deploying cloud-based productivity applications, such as Microsoft 365, Google Workspace and Salesforce. These Software-as-a-Service (SaaS) providers operate under a shared responsibility model, meaning the users, data and application administration are the responsibilities of the organization subscribing to the service, while the service provider manages the resiliency and availability of the application and infrastructure components.

While SaaS applications offer some basic recovery capabilities, they are ill-suited to today's backup and recovery demands since they come with significant limitations regarding what you can recover, where you can recover and how long the data is available for recovery.

There are tools available today that boast complete backup and recovery for SaaS applications, including admin and end-user self-service recovery. For cloud-based applications, leverage a cloud-to-cloud backup solution that frees you from the burden of managing backup and storage infrastructure on-premises. A cloud-based backup and recovery solution helps improve costs and time to recovery without requiring your networking resources for data transfer, unlike a solution that stores SaaS data locally.

IaaS — Don't put all your eggs (backups) in one basket (cloud)!

Organizations of all shapes and sizes are increasingly leveraging public clouds like Microsoft Azure and Amazon Web Services (AWS) to modernize their IT operations. While migrating your data and workloads to these public clouds presents a whole range of opportunities, they also have their fair share of risks. With cyberattacks against public clouds growing at an exponential rate, you should be wary of storing your backups along with the production data in the public clouds.

For instance, it's only recently that a networking outage took down the entire Azure platform along with its services, such as Teams and Outlook. If you do not store your backup data in a redundant location away from your production Azure stack, you would likely fall victim to such a single-cloud vulnerability, significantly affecting your business continuity. Moreover, suppose you are using native backup and recovery solutions offered by your provider. In that case, your data backups will be stored behind the same login credentials as your production, exposing your backups to a wide range of threats like cyberattacks and malicious insiders.

It is thus critical to store your data backups in a third-party recovery site outside of your primary cloud. That way, you can easily spin up your infrastructure in the redundant cloud in the event of an incident affecting your primary site and failback to your primary cloud after recovery.

Endpoint backup and recovery — remote employee protection

In hybrid environments, employees are increasingly creating critical data and IP on edge devices that aren't consistently connected to corporate networks for backup and recovery by local solutions. Endpoint backup solutions protect critical data by copying data from endpoints — whether Android and iOS phones/tablets, Windows and Mac desktops/laptops or even Windows servers — to data centers. However, the value of an endpoint backup solution lies in how well it performs data restoration in the wake of a data loss incident caused by malicious or accidental deletion, ransomware or any other cyberthreats.

Backup and restoration deployment needs to be flexible for effective endpoint protection. Resolving tickets for endpoint issues for everyone simultaneously can lead to expensive IT help desk costs. Consider a solution that offers a range of self-service options. Restores are accomplished quickly, and maximum productivity is ensured by empowering users in this manner. As endpoint backup solutions deal with remote devices, they should be optimized to replicate data over the WAN. Look for a solution that offers deduplication, compression and encryption (for security), as well as options for incremental backups or incremental forever backups to minimize the amount of data transferred over the WAN.

Protects Microsoft 365, Google Workspace and Salesforce applications from accidental deletion, corruption, malicious threats and other causes of data loss not covered by provider SLAs.

Checklist:
Finding the Best Cloud Solutions for Backup and Recovery

Capability To Look For	Description	
Long-term cloud retention	An integrated cloud solution provides safe, trustworthy and easy recovery storage for various retention schedules, whether measured in days, months or indefinitely.	□
Tiered retention pricing	A solution that licenses against the volume of data being protected and the time periods required, without ingress and egress fees.	□
Cloud seeding services	It would be advantageous if the cloud provider offers a seeding service, which usually involves shipping hard copy media overnight. This service will enable you to create an encrypted backup library, and also allow you to quickly upload data to the cloud target, thus preparing the environment for a disaster event.	□
Purpose-built cloud	Backup cloud providers that have tuned their environments specifically for retention and disaster recovery use cases to meet your BCDR needs with easily understandable licensing models.	□
Support for hyperscale clouds	The backup provider should enable easy integration with hyperscale cloud providers such as AWS and Azure.	□
Disaster Recovery-as-a-Service with RTO SLAs	DRaaS offers protection for specific applications enrolled in the service (or even your entire data center) and applies RTOs to support one-hour, 24-hour or bulk SLAs for critical applications.	□
Protection for SaaS applications	Protects Microsoft 365, Google Workspace and Salesforce applications from accidental deletion, corruption, malicious threats and other causes of data loss not covered by provider SLAs.	□
Protection for remote endpoints	Maximizes end-user productivity and minimizes data loss with a solution that supports reliable WAN-based backup for PCs and other remote endpoint devices.	□
Protection for IaaS	Your data and workloads in the public cloud are subject to different threats, including single-cloud vulnerabilities. Your backup provider should be able to secure these workloads in a — preferably purpose-built — redundant cloud.	□

Proof, confidence and productivity

With RTO and RPO goals and protection schedules set, you need to be completely confident that your objectives can be met. You also need to prove to senior management, line-of-business leaders, auditors, regulatory agencies and other stakeholders that you have verifiable plans in place to execute your DR plan. You need proof that your strategies will work in an emergency and the ability to provide evidence in the form of enterprise-level reporting. High levels of confidence are achieved through regular, in-depth automated recovery testing.

Preventing environmental backup failures — self-healing backups

Vendors building automated solutions on the cutting edge are bringing automation into the infrastructure use case. IT environments are complex, often ill-suited for backup and even less so for recovery. Dependencies within the environment, such as VSS writers in a Windows environment, are critical for the success of backups. Self-healing backup solutions automatically identify and fix production issues within the environment before they can negatively impact backups, ensuring all success criteria in the environment are met before a backup even runs. The result is less management, fewer errors, greater resilience and more successful backups.

Predictive hardware analytics

Solution providers should have proactive monitoring in place to predict hardware and software malfunctions. Predictive analytic technology enables a provider's support organization to understand what is inside the range of normal performance for each component. With remote monitoring, slight performance anomalies can predict future issues, such as an impending hard drive failure. They should be monitoring and fixing issues before they have the chance to impact backup operations.

Recovery testing — proof and confidence in recoverability

The only way to know you can restore in an emergency is to regularly test recovery, including any time you change your infrastructure. New intelligent tools simplify the testing process by automatically testing multiple systems down to the application and services level. This ensures all components are in place and capable of recovering an application and identifies potential failures and recovery roadblocks, enabling you to proactively address issues before an actual recovery is required. Beyond testing, the solution should provide easily readable, formal reports certifying the DR test and recording the results. Automated testing provides visibility into recoverability, so you know exactly how fast (RTO) and from what point (RPO) your data and applications are protected without the cumbersome lifts required for manual testing.

Isolated test, dev and QA environments

By using advanced, automated provisioning tools, you can test beyond just application recovery. Organizations must know that new software versions and patches won't cause performance issues. This is achieved by testing before deploying them on production servers. These tools enable you to spin-up and create isolated testing sandboxes that mirror your production environment as they're created from your recent backups. Any problems found in the lab can be pinpointed and addressed. Isolated labs may also be used in conjunction with dedicated security tools to ensure backups are free of malware or ransomware before restoring systems into production following an attack. Post completion, the entire test environment can be easily torn down, freeing up resources.

Customer support — 24/7/365

Disasters don't give warning, and don't wait to strike between your regular eight to five business hours. You need a backup and recovery solution supported by a team of expert engineers available on phone, chat and email 24/7/365. Ideally, support engineers are located at the same location as product development and quality control engineers to ensure easy access and timely resolutions for more advanced questions and issues. Ask your vendor about documented satisfaction ratings to see how existing customers have rated the provider's support service.

Checklist:

Proof, Confidence and Productivity

Capability To Look For	Description	
Self-healing backups	Self-healing backups ensure environmental success criteria are met before running backups, improving the chances of completing each backup successfully without errors.	□
Predictive hardware analytics	Does the vendor have in place the tools to monitor, identify and fix hardware or software issues before they cause an issue with backup and recovery systems?	□
Automated recovery testing	Offers automated recovery testing for full visibility into the recovery processes for both simple and complex applications, ensuring 100% recovery confidence for all workloads within the metrics defined by your organization.	□
Compliance and recoverability reporting	Does the solution allow for documenting testing results in exportable reports detailing performance against pre-established compliance metrics and criteria for a successful recovery of each system?	□
Support for spin-up of test/dev environments	Automatically spins up test and dev sandboxes from your backups to create an isolated lab environment for patch testing, DevOps and QA purposes.	□
Highly rated customer support organization	Offers documentation regarding customer satisfaction ratings, helping understand current customer satisfaction.	□

Conclusion

We've outlined the features and functions leading BCDR vendors offer to protect your organization's digital assets. Consider these as part of your evaluation criteria, and you'll be well prepared to overcome a variety of system outages, malicious attacks and other unforeseen destructive events.

Now that you know what to look for in a BCDR solution, **take a look at Unitrends Unified BCDR solutions for yourself.**

ABOUT UNITRENDS

Unitrends makes efficient, reliable backup and recovery as effortless and hassle-free as possible. We combine deep expertise gained over thirty 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.

Learn more by visiting unitrends.com or follow us on LinkedIn and Twitter @Unitrends.

UNITRENDS
A Kaseya COMPANY