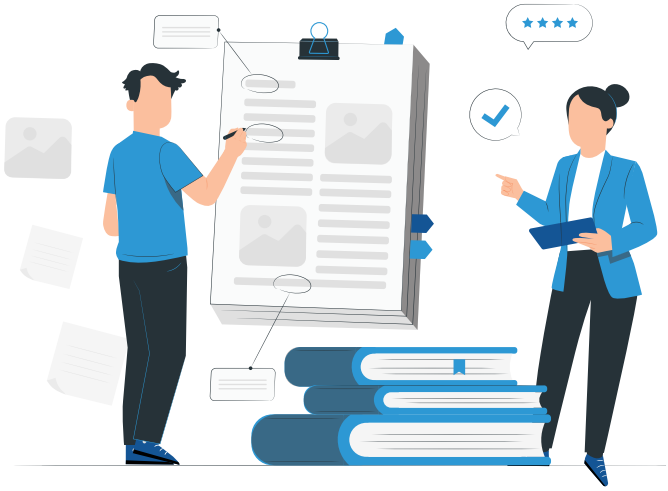


The MSP Buyer's Guide to Backup and DR

UNITRENDS MSP

msp.unitrends.com

Introduction

When evaluating solutions for business continuity and disaster recovery (BCDR):

What exactly are *you* looking for?

Perhaps it's a solution that's complete and agile enough to protect a unique combination of customer workloads, from physical and virtual to SaaS and cloud-based.

Maybe you're looking to optimize your technicians' time by injecting automation and artificial intelligence to simplify complex workloads and streamline tasks.

In today's threat landscape, data loss prevention and reducing the severity of incidents such as cyberattacks is paramount. You should look for a solution with the resilience to protect your digital assets with absolutely zero downtime. Customer environments are heavily fragmented. That combined with global, dispersed workforces makes achieving the recovery time objectives (RTO) and recovery point objectives (RPO) demanded by modern SLAs a huge challenge.

Many of today's siloed backup and disaster recovery solutions leave large gaps in protection, forcing MSPs to compromise on functionality or pay higher costs and rely on stitching together disparate components to compensate for the lack of completeness.

A backup solution sits in a strategic location since it touches all corporate data and the majority of an organization's applications. With access to the lifeblood of your clients, backup solution providers are extending their reach beyond simply backup and recovery. Selecting the right solution is increasingly about more than just basic backup. Many vendors are bringing new and exciting technologies in the form of artificial intelligence, machine learning and predictive analytics to make technicians more efficient and productive at their jobs.

Before choosing a backup solution provider, it's important 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 the risks of data loss and downtime.

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, innovations in data storage, infrastructure and data management, there are a number of strategies to consider. By understanding what solution in the market meets the needs of tomorrow, you'll be well positioned to protect your clients now and in the future.

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

1] Protect everything: 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] Guaranteed 100% recovery confidence with automation in the infrastructure use-case, recovery testing, reporting and exceptional technical support.

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

Protecting your evolving data center

IT environments are increasingly complicated, with client data living on traditional infrastructure, in clouds and SaaS applications and on remote endpoints. Balancing a myriad of technologies can be complex but protecting it doesn't have to be. You need the agility to protect all workloads with a streamlined, all-in-one approach to backup, recovery automation and cloud continuity. It should be designed to work with all forms of computing styles to enable technicians to be productive and 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 dozens of 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. MSPs using multiple data protection vendors are more likely to struggle with data loss and downtime since incorporating multiple solutions tends to add an extra layer of unnecessary complexity.

In response, vendors are delivering modernized solutions with an integrated approach to reduce the time and money spent managing continuity. It enables MSPs to deploy a complete, agile solution designed to protect all types of data and applications. In other words, a purpose-built appliance. Industry-leading purpose-built backup appliances protect all computing platforms, from physical Windows and Linux systems, virtual machine infrastructure, hyperconverged infrastructure, legacy systems and cloud workloads deployed in hyperscale public clouds such as Amazon AWS and Microsoft Azure. A modern, intuitive user experience is a priority. That means the solution should be presented in a way that makes it easy to manage and operate without needing to refer to an administrative guide. This is achieved through utilizing a single, central console enabling you to manage protection across a myriad of digital assets while offering the customization to design optimal backup approaches for each protected workload.

Protection for all workloads

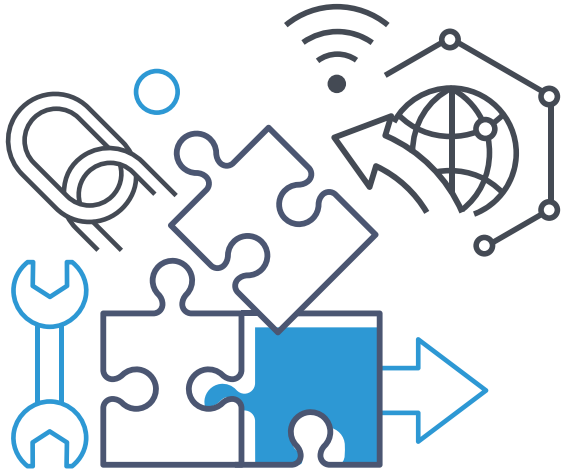
Customer environments have a wide range of computing styles such as on-premises systems, cloud-based systems (IaaS, PaaS and SaaS) and remote endpoints. Your backup and recovery solution should offer the agility to easily protect hundreds of versions of operating systems, hypervisors, applications and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

Policy-based management

Backups should be easy to define and schedule. Technicians 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 you to define recovery goals (RTO and RPO) for all assets grouped under the policy, with the backup system calculating and filling in the deployment and scheduling details. This form of scheduling enables MSPs to align data management and availability tactics with client business policies without the need for granular details such as file locations and snapshot schedules.

Built-in WAN optimization

Moving backup copies to an off-site location is a critical step in preparing for disaster recovery. With clients demanding near-zero RTOs and RPOs, the cloud has become an increasingly popular choice as a target for replication. However, for many MSPs, their WAN may not have the capacity to handle large amounts of data being replicated regularly. 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).



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:

Optimizing Protection for Everything in Your Evolving Datacenter

Capability To Look For	Description	
Fewer Point Products	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. It should be possible to operate your backup system without referring to a manual so substitutes can stand in when primary technicians are unavailable.	☐
Wide Range of Compatibility	Your backup and recovery solution should be able to natively protect hundreds of versions of operating systems, hypervisors, applications and cloud-native formats.	☐
Policy-Based Management	Technicians 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. Deduplication tends to achieve better data reduction efficacy against smaller backup sets while compression tends to achieve better results against larger data sets.	☐
Cloud-Enabled	Integrated support for multiple types of clouds, including private and hyperscale clouds such as AWS, Azure and Google Cloud Platform (GCP).	☐
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 compared to similar technologies and can easily integrate with other applications.	☐
AES 256 Bit-Encryption	Military-grade encryption should be utilized to secure all data both in-flight and at-rest.	☐

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. MSPs need to inventory clients protected assets and workloads and triage them by their importance to keep each clients functioning. Robust backup and recovery capabilities should be deployed to protect mission-critical applications compared to applications that can be temporarily offline.

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 compute 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 with your most recent copy of backup data. The appliance may also support the recovery of virtual environments by acting as a temporary datastore in an instant recovery process. The backup data is injected into a share mounted to the appliance in order to spin up virtual machines (VMs) much more quickly in comparison to rebuilding the backup chain on the VM's attached storage. By leveraging VMware's Storage vMotion or Hyper-V's Live Migration, the location of the virtual disk is moved off the appliance to the target datastore as a passive background operation after the VMs are brought back online. Appliances may also create and act as a storage location for replicas, standby copies of production machines, kept updated with every backup and stored in a warm state ready for immediate failover into production.

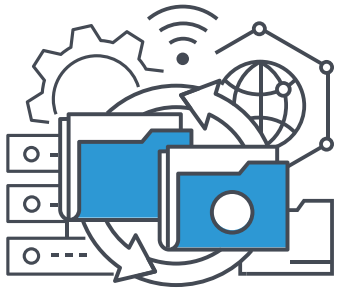
Site-level disasters – Support for multiple locations

Backup and recovery solutions can be managed remotely our technicians can be on-site for every client at any time. A singular appliance user interface should enable you to manage all protected sites from a single console. 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 a client. Should a client not have multiple locations, or the resources to support a co-location, 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 an IT environment by disabling security services, backup utilities and destroying the backups themselves. Cybercriminals look to exploit gaps in environments that may arise from utilizing multiple solutions since the increased complexity of the environment makes securing infrastructure to stave off threats 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 surface of attacks that are predominantly targeting 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 secure the backup environment.

Avoid data loss



Once you've classified and tiered mission-critical applications from those that don't require aggressive RTOs, you're in a position to determine the Recovery Point Objective (RPO) for all classes of applications. RPOs are determined by understanding how much data a client can afford to lose in the event of an incident or outage. In other words, they inform the frequency required of backup schedules and 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 aimed at defeating 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 fluctuations of data 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 may be measured and evaluated to detect in near real-time an active ransomware infection. Once the infection is identified, notifications should be automatically sent to technicians, flagging any potentially infected files 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. Data loss may occur due to corruption of stored or in-flight files as well as 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 would be lost in a downtime event. Proactive testing helps MSPs uncover gaps between strategy and goals and the ability to meet them with the current solution as implemented. The visibility enables MSPs to have metric-based conversations on the RPO goals (that must be set) to achieve the optimal protection strategy for each client.

Application downtime prediction

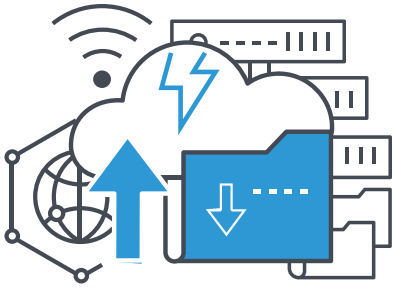
Recovery time objective (RTO) is the measure of how long it takes to get a client up and running after a disaster, including full access to critical applications. As environments grow in complexity, applications today are often N-tier or multi-tiered. This means processing, data management and presentation 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 one 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 client objectives. By validating testing down to the application and services level, you will know with confidence that RTOs are achievable.

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

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 onto a secondary host.	☐
Management for Multiple Sites	A single, seamless appliance user interface (UI) enables you to manage backup and recovery operations across all devices, both on-premise 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 artificial intelligence to measure a number of heuristics in data to detect in near real-time an active ransomware infection. Once identified, alerts are automatically sent to technicians and suspected files 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 that require multiple component dependencies for recovery.	☐

Keeping cloud DR from becoming its own disaster



Organizations of all sizes are increasingly using the cloud as their disaster recovery site. Regularly scheduled backups are replicated and stored securely in the cloud at low cost where they're isolated from accidental deletion or ransomware attacks. Cloud-based backup files should serve two purposes – firstly, they are preserved to meet data compliance mandates and secondly, they are readily available to be used for disaster recovery.

Long-term cloud retention

With a variety of 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. It means as client data grows, or as they 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 provides predictable, forecastable total cost of ownership (TCO) for cloud storage without unpredictable access fees or paying for unwanted storage space. You should be able to select the exact volume of storage and the specific retention period required for each client's data set. This removes the burden of retention management and operational spending as 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 having to retrieve, rehydrate and restore data stored on cold media at an off-site location.

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

Data backup is a challenge and successful recovery can be even more difficult. With MSPs facing increased demands for recovery, evaluating available technologies to determine the best fit to meet a client's unique needs is vital. In response to burgeoning demands, vendors and service providers are now offering Disaster Recovery-as-a-Service aka DRaaS. It is designed to equip organizations with the resources and expertise to automate, accelerate and simplify the recovery of mission-critical applications individually or at scale.

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

The main advantages of a DRaaS model are cost-effectiveness and flexibility. For MSPs, DRaaS offers an affordable alternative to hosting a private disaster recovery site and deploying additional IT staff for emergencies. If disasters don't happen, the secondary infrastructure and staffing may never be utilized. By using DRaaS, MSPs don't have to worry about owning resources or managing DR since service providers take care of them. With DRaaS, you only pay for the services you use, which cuts down costs significantly. DRaaS also allows you to mix and match SLAs (typically tied to an RTO) to meet each client's unique objectives. For instance, combining mission-critical systems, such as financial and point-of-sale 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 model of shared responsibility. It means the users, data and applications are the responsibility of the organization subscribing to the service, while the service provider manages the resiliency and availability of the infrastructure.

While SaaS applications come with basic recovery capabilities, they are ill-suited to the backup and recovery demands of today since they come with significant limitations regarding what you can recover, where you can recover and how long the data is available for recovery. Deleted emails, files, folders and contacts are permanently deleted and are unrecoverable by even the service provider if not caught in time.

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 your team 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.

Endpoint backup and recovery - Remote employee protection

In hybrid environments, end users are increasingly creating critical data and IP on the edge, stored on 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 at the same time can lead to expensive help desk costs. Consider a solution that offers a range of self-service options. By empowering users in this manner, restores are accomplished quickly and maximum productivity is ensured. 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.

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 storage for a variety of different retention schedules (whether measured in days, months, years or indefinitely) while keeping backups readily available and easily recoverable.	☐
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	The cloud provider should offer a seeding service, generally by overnight shipment of hard copy media, to establish your library of encrypted backups with the ability to upload data to the cloud target quickly to prepare the environment for a disaster event.	☐
Purpose-Built Cloud	Backup cloud providers 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 datacenter) and apply 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 minimize data loss with a solution that supports reliable WAN-based backup for PCs and other remote endpoint devices.	☐

Proof, confidence and productivity

With RTO, RPO goals and protection schedules set, you need to be completely confident that your client 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 disaster recovery plan. You need proof that your strategies will work in an emergency and the ability to provide proof to clients 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 and 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, essentially ensuring all success criteria in the environment is being 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 for sure you can restore in an emergency is to test recovery regularly, including any time a change is made to production infrastructure. New intelligent tools simplify the testing process by automatically testing multiple systems down to the application and services level. It ensures all components are in place and capable of recovering an application. It also identifies potential failures and pitfalls, enabling you to proactively address issues before a true recovery is required. Beyond testing, the solution should provide easily readable, formal reports certifying the DR test and recording the results. Automated testing provides you with visibility into recoverability, so you know exactly how fast (RTO) and from what point (RPO) client 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. MSPs and their clients need to 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 the production environment as they're created from your most recent backups. Any problems that are found in the lab can be pinpointed and addressed prior to pushing into production. Once testing is completed, the entire test environment can be easily torn down freeing up resources.

Customer support – 24/7/365

Disasters don't give advance warning, and they 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 that are available on phone, chat and email 24/7/365. Ideally, support engineers are located at the same location as product development and qualify control engineers 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 provider's support service.

to

Proof, Confidence and Productivity

Capability To Look For	Description	
Self-Healing Backups	Self-healing backups ensure environmental success criteria is met prior to backups being run, improving the chances of each backup being successfully completed 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 that leading business continuity and disaster recovery 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 MSP

Unified BCDR solutions for yourself.