UNITRENDS

BACKUP AND DRaaS IT BUYER'S GUIDE

FIVE WAYS TO BEAT DATA LOSS & DOWNTIME

WHAT YOU WILL LEARN

When it comes to data protection and business continuity, what is your goal? That's easy – a solution you know will work every time, protecting everything you have in your data center with absolutely zero downtime and zero data loss.

Is that possible? The good news is that we are closer than ever to being able to achieve this lofty goal. However, you will need to make careful choices about the solution you implement as many of today's backup and disaster recovery solutions have large gaps forcing you to compromise or pay high costs to compensate. Additionally, some backup solution vendors are further along in incorporating new and exciting technologies such as artificial intelligence, machine learning and predictive analytics that make IT administrators faster and more productive at their jobs.

5 KEY TOPICS:

1. PROTECT ALL YOUR ASSETS
2. MEET FAST RECOVERY TIME OBJECTIVES
3. ACHIEVE NEAR-ZERO DATA LOSS
4. CLOUD-BASED DISASTER RECOVERY
5. TESTING, REPORTING, & SUPPORT

Backup tools sit in a very strategic location. They touch and manage all corporate data and the majority of applications. With complete access to the lifeblood of a company, backup providers are building ways for corporations to not just protect the data at hand, but to use their reach for capabilities far beyond data protection. Selecting the right solution is increasingly more than just about basic backup.

Before choosing a backup vendor, understand the wide variety of offerings, what to look for and potential gaps in coverage to put your organization in the best position to achieve the lofty goal of total protection all the time.

HOW TO USE THIS GUIDE

This buyer's guide is designed to help you understand the options in the market today and insights into emerging technologies. Why? Because there are hundreds of vendors, new technologies emerging in storage, infrastructure and data management, and broad continuity strategies to consider. After all, you won't be around to guide the future if you can't protect your infrastructure today.

This report is organized around the best practices for data protection and disaster recovery of today's leading enterprises:

1. Protect everything in your data center including virtual, physical, storage, and cloud
2. Gain quick recovery (RTO) from local events, ransomware, enterprise-level failure
3. Achieve near-zero data loss (RPO) and long term data retention
4. Avoid a extended downtime with cloud-based disaster recovery options, and
5. Gain confidence you will recover every time with testing, reporting, and top-rated support

We will provide guidance on each of these topics. In each section, we have created a checklist or you to use to ensure your solution is the best the market can offer. And, finally, on the last page, we've added a convenient chart that can help you create a shortlist of leading features.

SECTION 1: PROTECT EVERYTHING IN YOUR DATACENTER

Your environment is complicated, but protecting it doesn't have to be. You need to protect everything in your data center, whether it be physical or virtual, deployed on premises, at a remote location or in the cloud. In addition, new technologies are emerging, such as hyperconverged infrastructures such as Nutanix and Cisco UCS. A simple, all-in-one approach to backup, recovery automation, and cloud continuity built to deal with all forms of computing styles makes IT administrators more productive as they can do more in less time. Today's leading data protection solutions can protect diverse environments and come pre-integrated and optimized to provide high-speed, error-less performance.

BACKUP AND DRaaS BUYER'S GUIDE

PROTECT EVERYTHING CHECKLIST

	CAPABILITY	DESCRIPTION
☐	Fewer protection solutions	A multi-vendor protection strategy greatly increases IT complexity and costs. Reducing the number of solutions means managing fewer licenses, maintenance and service agreements.
☐	Purpose-built appliance	A purpose-built all-in-one solution is easier to install, upgrade, service, and manage.
☐	Intuitive user Interface	A modern, intuitive user experience is a priority: it should always be possible to operate your backup system without referring to a manual, and substitutes or managers should be able to stand in when primary admins are unavailable.
☐	Wide coverage	Your backup and recovery solution should be able to protect hundreds of versions of operating systems, hypervisors, and applications.
☐	Policy-based management	Administrators should have the choice of how backups are set, either by entering the backup details themselves or using intelligent policy-based scheduling technology.
☐	Deduplication	Deduplication tends to achieve better data reduction efficiency against smaller backup sets (the amount of data being backed up each time), while compression tends to achieve better results against larger data sets.
☐	Compression	Data compression reduces the overall size of files and makes their movement and storage more efficient.
☐	Cloud-enabled	Integrated support for multiple types of clouds including private and hyperscale clouds such as AWS and Azure.
☐	RESTful-API	Can easily integrate with other applications.
☐	AES Encryption	Secures data privacy both at-rest and in-flight.
☐	Near zero Downtime	Supports P2V, V2V, V2P.

PURPOSE-BUILT APPLIANCES

If you were to build your own backup and recovery solution, you would probably have to integrate dozens of different pieces of software and hardware - servers, storage, deduplication, OS, security, analytics, search, monitoring.... Unfortunately, many vendors ask you to take that approach by partnering with other suppliers rather than building their own total solution. The amount of time you will have to spend on p[protection is directly proportional to the number of servers and components you have to install, manage, and maintain. Time is money.

Newer vendors are taking the integrated approach specifically to reduce time and money spent on continuity. Visionaries in IT are deploying single, complete solutions, purpose-built to perform data and application protection - in other words, an appliance. A purpose-built, all-in-one appliance is easier to install, upgrade, and manage. Today's leading appliances are able to protect all computing platforms, including virtual systems, physical Windows and Linux systems, legacy systems, and cloud workloads deployed in hyperscale clouds such as Amazon AWS and Microsoft Azure. A modern, intuitive user experience is a priority: it should always be possible to operate your backup system without referring to a manual so substitutes or managers can stand in when primary admins are unavailable.

WIDE PROTECTION FOR WORKLOADS

Today's data centers have a wide range of computing styles including on-premises and remote, cloud - including IaaS, SaaS, and PaaS, and new technologies such as hyperconverged infrastructure. Your backup and recovery solution should be able to protect hundreds of versions of operating systems, hypervisors, and applications.

POLICY-BASED MANAGEMENT

Backups should be easy to define and schedule. Administrators should have the choice of how backups are set, either by entering the backup details themselves or using intelligent, policy-based scheduling technology. Policy-based management allows administrators to define their recovery goals (RPO and RTO) with the system calculating and filling in the deployment details. This form of scheduling allows administrators to align data management and availability tactics to business policies, without needing to understand details such as file locations and snapshot schedules.

BACKUP AND DRaaS BUYER'S GUIDE

BUILT-IN WAN OPTIMIZATION

Getting your data to an off site location is critical for disaster recovery, but your WAN may not have the capacity for handling large backup files. Your backup appliance should come with integrated WAN optimization technologies such as adaptive deduplication, deduplication acceleration, compression, and encryption. These technologies provide data protection and reduce the size (and cost) of synchronizing data backups to a remote location or cloud DRaaS.

To ensure you have all aspects of data protection maximized while keeping costs and administrative time commitments to a minimum, here is a list of technologies that should be part of your data protection solution:

PROTECT HYPERSCALE INFRASTRUCTURE

Nutanix created the concept of a hyperconverged infrastructure. No longer do organizations need to purchase, maintain and service server, storage and networking as separate devices. Nutanix and other hyperconverged infrastructure vendors such as Cisco UCS make an integrated enterprise private-cloud infrastructure invisible without sacrificing the security and control of on-premises infrastructure. It is just as important to protect this form of computng as traditional servers. The combination of hyperconverged infrastructure and industry-leading all-in-one backup and continuity helps organizations speed time to value, lower costs, and increase confidence that their applications will be available and ready to run through whatever life throws at them.

SECTION 2: GAIN QUICK RECOVERY TIMES (RTO)

While instant recovery with zero downtime is ideal, putting in place the resources to meet this objective may not be affordable for every application in every organization. Organizations need to inventory their applications and triage them by their importance to the functioning of the business. More backup capabilities should be invested to protect mission-critical applications than those apps that can be off-line for a short while. The following features should be considered to support mission-critical apps.

LOCAL DISASTERS – UTILIZE AN APPLIANCE

Today's backup and recovery appliances are themselves full computing platforms, equipped with CPUs, a large amount of storage, backup software and remote management capabilities. These appliances are the first line of recovery. If a single server or data center rack goes off-line the appliance can run the failed applications with the most recent copy of backed up data. Simple, neat, easy, and fast.

SITE-LEVEL DISASTERS - SUPPORT FOR MULTIPLE LOCATIONS

Backup and recovery tools can now be managed remotely meaning that organizations no longer need to have IT deployed at every site there is a server. A single appliance / user interface should be able to manage all remote devices. Appliances in different locations can act as backups for each other so that site level disasters such as electrical failures or flood do not bring down an entire enterprise. Cross-site monitoring and recovery by backup appliances should also be instantaneous.

ENTERPRISE-LEVEL DISASTER - RECOVER FROM RANSOMWARE

Ransomware is designed to cripple the entire enterprise to ensure a ransom is paid. The only real defense against ransomware is having solid and frequent backups to replace encrypted files. Cyber criminals look to exploit gaps in your security systems that can come from using multiple backup and recovery tools and complex backup and recovery solutions that make securing the infrastructure too difficult to stave off threats. Look for a backup solution delivered in hardened Linux as ransomware targets Windows applications due to their popularity and the fact that Windows is generally an "open architecture". Linux appliances are written as locked down.

SECTION 3: ACHIEVE NEAR-ZERO DATA LOSS (RPO)

Once you have parsed mission-critical applications from those that don't need near-instantaneous recovery, you are in a position to set recovery point objectives (RPOs) for all classes of apps. A recovery point objective is basically deciding how much data you can afford to lose. Here are features and functions that can help define and deliver on your RPO objectives.

AUTOMATIC RANSOMWARE DETECTION

Nothing can bring an enterprise to its knees more completely than ransomware. Newer variants of the malware will delay notifying you of their presence so it has more time to encrypt additional files. Fortunately leading backup and recovery solutions are now using machine learning, change rate prediction, data entropy and randomness of data creation as measurements to detect in near real-time an active ransomware infection. Once an infection is identified, notifications should be automatically sent to administrators to take action and stop more files from being encrypted, thus avoiding more data loss.

BACKUP AND DRaaS BUYER'S GUIDE

FAST RECOVERY & NEAR-ZERO DATA LOSS CHECKLISTS

	CAPABILITY	DESCRIPTION
☐	Instant recovery from local disasters	If a single server or data center rack goes off-line, a backup appliance will detect the failure and automatically bring up applications running with the most recent copy of backed up data.
☐	Manage protection for multiple sites	A single appliance / user interface should be able to manage all remote devices.
☐	Easy ransomware recovery	Look for a backup solution delivered in hardened Linux as ransomware targets Windows applications due to their popularity and the fact that Windows is an "open architecture".
☐	Bare metal backups	Bare metal restores allow application recovery across servers by different vendors and hardware configurations.
☐	Automatic ransomware detection	Recovery solutions should be using machine learning, change rate prediction, data entropy and randomness of data creation as measurements to detect in near real-time an active ransomware infection. Once an infection is identified, notifications should be automatically sent to administrators to take action and stop more files from being encrypted, thus speeding recovery.
☐	Data loss prediction	Utilize intelligent tools that can simulate different disaster or outage scenarios and predict how and what types of data would be lost in a downtime event to set the right RPO.
☐	Application downtime prediction	Tools can now identify, simulate, and test the many steps and time required to recover complex applications This lets you know if your RPO is achievable.

APPLICATION DOWNTIME PREDICTIONS

An RTO is calculated based on how long it takes to get business up and running again, which means full access to critical applications. Applications today are complex stacks of software, data, databases, and settings frequently spread across disparate hardware. If any one of the components is out of line, a critical application will remain unavailable to business users. You should use newly available, intelligent tools to identify, simulate, and test the many steps required to recover complex applications and get valuable business information flowing again. Only after testing can you know that your RTO is achievable.

DATA LOSS PREDICTION

When calculating desired RPO metrics, one of the most important considerations is understanding the potential loss of data. Data loss can include the corruption of stored or in transit files as well as not capturing business data that would have been produced during a downtime event. Lost sales records, customer contact information, and employee production all have real business value. Intelligent tools are now available that can simulate different disaster or outage scenarios and predict how and what types of data would be lost in a downtime event. Proactive testing helps businesses uncover gaps between strategy/goals and implementation/solutions. Having this knowledge allows IT to conduct an intelligent, business metric-based conversation on what RPO goals to set.

SECTION 4: CLOUD-BASED DISASTER RECOVERY

Cutting edge enterprises as well as organizations doing business at a single location are increasingly using the cloud as their disaster recovery location. Regularly scheduled backups are stored in the cloud at low cost and are isolated from accidental deletion or ransomware attacks. These cloud-based backup files should serve two purposes – first they are preserved to meet data compliance mandates, but they should also be able to be used for disaster recovery.

CLOUD DISASTER RECOVERY-AS-A-SERVICE

Disaster Recovery-as-a-Service (DRaaS) allows organizations to spin up their applications in the cloud if their datacenter goes down for any reason. Pay for DRaaS protection only for the apps you determine to be important and you should add optional 1-hour or 24-hour SLAs (Service Level Agreements) for your most mission critical applications to ensure you have your cloud provider's undivided attention. Charges for DRaaS can vary widely across cloud

BACKUP AND DRaaS BUYER'S GUIDE

CLOUD CHECKLIST

	CAPABILITY	DESCRIPTION
☐	Disaster Recovery-as-a-Service	Pay for DRaaS protection for the apps you determine to be important and add optional 1-hour SLAs for your most mission critical applications.
☐	Protect SaaS applications	Protect Exchange mail, SharePoint and OneDrive business applications running in Microsoft Azure.
☐	Service Level Agreements	1-hour and 24-hour DRaaS services for mission critical VMs.
☐	Purpose-built cloud	A backup cloud provider can provide better performance by designing services specifically for the backup needs of the customers.
☐	Support for hyperscale clouds	Allow easy integration with hyperscale clouds such as AWS and Azure.
☐	Long-term Cloud Retention	An integrated cloud solution can provide safe, trustworthy and easily-recoverable storage for different retention schedules – 1 year, 3 years, 7 years or infinite.
☐	Tiered retention pricing	Pay only for the storage volumes and time periods you require. Long term data retention is not one-size-fits-all.
☐	Cloud seeding services	Sending large amounts of data to the cloud via a WAN can take weeks. Your DRaaS provider should be able to accept hard-copy media to establish your library and create media to quickly repopulate your local files after a disaster.
☐	Microsoft 0365	Microsoft does basic backups but enterprise class recovery requires advanced 0365 protection

vendors so be sure to ask about all fees for both storage as well as recovery services.

LONG TERM CLOUD RETENTION

The cloud can provide safe, trustworthy and easily-recoverable storage. Different types of data have different retention schedules – 1 year, 3 years, 7 years or infinite. Look for tiered retention pricing so you don't pay for more than you need. You should be able to select the number of years that data must be retained with cloud pricing to match. Remove the burden of retention management and operating spending as remote cloud storage may be cheaper than managing your own physical backup media.

SAAS – RECOVER YOUR APPLICATIONS RUNNING IN THE CLOUD

More enterprises are deploying office productivity applications such as Exchange Online, SharePoint Online and OneDrive. While they do come with very basic backup and recovery capabilities, they do not allow you to recover anything at any time. Deleted emails, files, folders and contacts will be permanently deleted if not caught in time. There are services available with self-service recovery as standard recovery times can be longer than you want. For cloud-based applications you can do cloud-to-cloud backups with virtual appliances that completely free you from burden of backup and storage management.

OFFICE 365

Running Microsoft 0365 in the cloud has become a common practice to reduce the overhead and cost of Exchange email, SharePoint and OneDrive. Microsoft 0365 offers robust disaster recovery, but limited native backup and recovery. Office 365 and the cloud do not prevent data loss caused by users. 75% of data loss is due to people deleting content accidentally or intentionally, and that's not the only threat. Ransomware can also infect 0365. IT leaders using or evaluating 0365 should consider investing in third-party backup and recovery tools for faster, more-flexible recovery options, as well as reputation damage control after a malicious attack.

BACKUP AND DRaaS BUYER'S GUIDE

SECTION 5: TESTING, REPORTING AND SUPPORT

Now that you have set your RPO and RTO goals you need to be confident that they can be met. You also need to prove to others, including senior management, auditors and regulatory agencies to name a few, that you have verifiable plans in place to execute your recovery program. You need confidence that your programs will work in an emergency and reports that back you up.

TEST, TEST AND TEST AGAIN

The only way to know if you can recover in an emergency is to test regularly and each time you make a change to your infrastructure. New, intelligent tools are now available that can greatly ease your concerns by automatically testing to ensure all components are in place and capable of recovering or telling you what is broken so it can be fixed. Additionally, you get an easy to read, formal report certifying that your disaster recovery solutions have been tested and showing the results. These tools automate testing so you know exactly how fast and to what point your data and applications are protected without requiring manual work on your part.

TEST AND DEV ENVIRONMENTS

Using advanced automated provisioning tools you can test beyond just application recovery. Organizations need to know that new software versions and patches will not cause performance interruptions by testing them prior to deployment on production servers. Automated provisioning tools can now spin up and create test sand boxes that are exactly the same as your production environment because they are created from your most recent backups. If problems are found, they can be pinpointed and solved. Once all testing is finished the entire test environment can easily be torn down.

CUSTOMER SUPPORT

Since disaster can strike at any time, you need to have your backup and recovery solution supported by a team available by phone, chat, and email—24 hours a day, 7 days a week, 365 days a year. Ideally the support engineers should be located at the same site as development and quality control engineers to ensure easy access for advanced questions. Ask your vendor to document their satisfaction rating to see how satisfied their existing customers are with their support.

TESTING, REPORTING AND SUPPORT CHECKLIST

	CAPABILITY	DESCRIPTION
☐	Automated Testing	Utilize automatic testing so you know exactly how fast and to what point your data and applications are protected without requiring manual work on your part.
☐	Spin up test / dev environments	Ensure that you can automatically spin up test and dev sand boxes from your backups that are exactly the same as your production environment.
☐	Highly rated customer support	Ask your prospective vendor to document their customer satisfaction rating to see how satisfied their existing customers are with their support.
☐	Failure predictive analysis	Can the vendor identify and fix hardware and software issues before you even know there is a problem?
☐	Compliance Reporting	Ensure that your testing tools will automatically generate reports that IT can use to satisfy auditors and senior management that recovery can take place in mandated times.
☐	Self-healing, Resilient Hardware	Your backup systems should be able to monitor the RAID and correct most RAID level failure scenarios.

BACKUP AND DRaaS BUYER'S GUIDE

SELF-HEALING, RESILIENT HARDWARE

Hardware reliability has come a long ways. Self-healing disks continuously monitor hard drives for anomalies that indicate a mechanical failure. Your backup systems should be able to monitor the RAID and correct most RAID level failure scenarios. If a drive failure is identified, the appliance should automatically open a support ticket and notifiy the administrators that a drive replacement is needed. The system should also perform regular scheduled maintenance to maintain optimal RAID efficiency. This technology eliminates time, complexity and the risk of human error associated with repairing the RAID array by automatically rebuilding the replacement drive into the array without manual intervention.

HARDWARE FAILURE PREDICTIONS

Solution providers should proactively monitor their systems at customer locations to predict hardware and software malfunctions before they happen. Predictive analytic technology enables customer support to understand what is inside the range of normal performance. With remote monitoring, slight performance anomalies can predict future issues. Solution vendors should fix issues before you even know there is a problem.

PRODUCT COMPARISONS

DCIG 2018 HYBRID CLOUD BACKUP APPLIANCE BUYER'S GUIDE

More models from Unitrends received the top Recommended and Excellent honors than all other vendors combined. See DCIG's backup appliance ratings. Click Here

COMPETITIVE COMPARISONS

See how vendors stack up against the features in the Checklists. Click Here

CONCLUSION

We have outlined the features and functions that leading backup and business continuity solutions offer to protect your company's computing assets. These will protect you from all sorts of downtime events, malicious attacks, employee sabotage, accidental deletions and other now unforeseen potentially destructive events. Use our product checklist to ensure your data protection solution delivers the best cutting-edge features:

- FULLY INTEGRATED SOLUTION WITH CLOUD STORAGE AND DRAAS
- LINUX APPLIANCE HARDENED AGAINST RANSOMWARE
- ALL-IN-ONE SOLUTION WITH OPTIMIZED OS AND SW
- INTEGRATED, AUTOMATED TESTING TOOLS
- PREDICT HARDWARE FAILURES
- PREMIUM DRAAS WITH 1-HOUR & 24-HOUR SLAS

GET YOUR UNITRENDS FREE TRIAL

Unitrends increases uptime and confidence in a world in which IT professionals must do more with less. Unitrends leverages high-availability hardware and software engineering, cloud economics, enterprise power with consumer-grade design, and customer-obsessed support to natively provide all-in-one enterprise backup and continuity. The result is a "one throat to choke" set of offerings that allow customers to focus on their business rather than backup. Learn more by visiting unitrends.com or follow us on LinkedIn and Twitter @Unitrends.