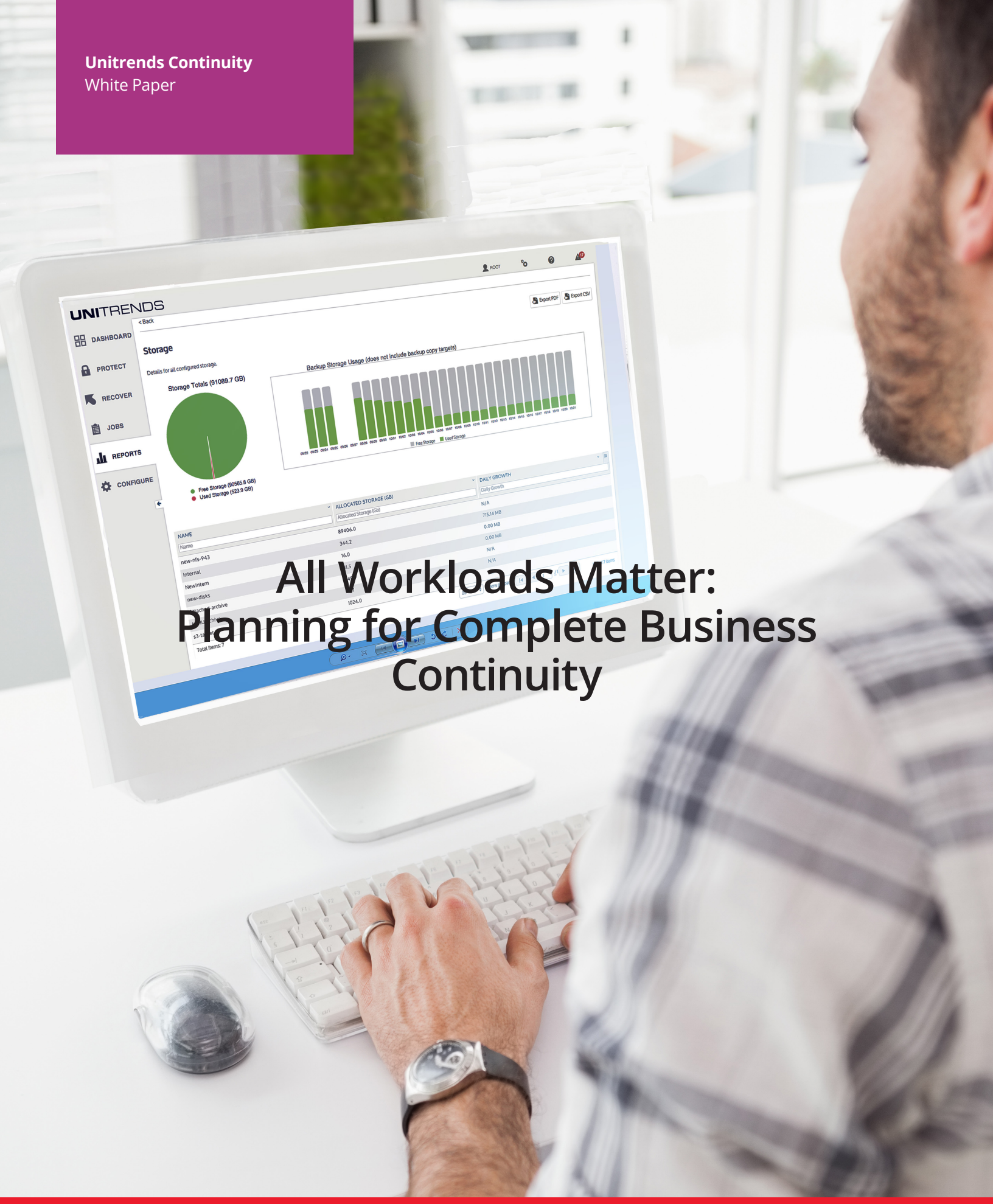
Unitrends Continuity
White Paper



All Workloads Matter: Planning for Complete Business Continuity

All Workloads Matter: Planning for Complete Business Continuity

Business Continuity

It's no longer sufficient to back up data and systems: today, organizations must take a systematic approach to continuity. The goal is clear and simple: to make sure your business stays up and running, whatever happens.

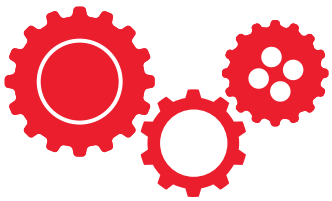
Stay Up and Running

When this is your goal, all workloads matter -- virtual, physical, and cloud. A second observation, tightly linked to the first, is just as important: while all workloads matter, not all are equal. All must be protected, but not all require the same level of protection, and not all are equally difficult to protect.

These two simple observations have powerful implications. This white paper considers them, and helps you build a coherent business continuity plan that offers the right protection for every workload, optimally balancing speed and cost.

Taking a closer look at your current workloads

Continuity planning begins with a careful assessment of your current workloads. At many organizations, these workloads have changed dramatically in the past few years. If it's been awhile since you reviewed yours, or if you're relying on intuition, you may be surprised at the current reality.



Physical workloads remain important

According to IDC, roughly 75% of workloads now run virtualized. But many IT decision-makers are surprised to hear that only 21% of bare metal servers are running hypervisors. That's right: roughly 80% of bare metal servers run physical workloads. In fact, according to Unitrends' 2016 Data Protection and Cloud Survey, more than 85% of companies still have significant physical workloads to protect.

We also found that 72% of companies have physical servers running Windows, 32% Linux -- and 18% are still running legacy Unix servers based on Solaris, AIX, or other dialects. Often, these non-virtualized systems can't be virtualized. For example, even though VMware and others have reduced the performance hit associated with virtualization, many non-virtualized applications in transaction-intensive environments can't tolerate any reduction in performance. In other cases, cautious IT organizations have chosen not to concentrate multiple workloads on a single virtualized host, to avoid an unacceptable single point of failure.

Whatever the reason for organizations' continued reliance on non-virtualized workloads, the reality remains: many diverse physical servers must be protected.

Cloud workloads are now fully mainstream

Given the massive investments that have been made in advancing cloud technologies, it's no surprise that nearly 80% of organizations are either deploying or fully embracing cloud workloads. The cloud workloads has clearly "crossed the chasm" to mainstream use.

Unfortunately, 40% of cloud users have already lost data in the cloud. It's easy to imagine that cloud vendors have entirely handled backup, recovery, and business continuity on your behalf. However, as this statistic indicates, this assumption is often false.

There are many ways for data to be lost or business continuity to be compromised in cloud systems. For example, applications running on hyperscale clouds may need advance planning and design if they are to spin up a new instance when a cloud server fails. And, as with locally-run systems, data may be deleted inadvertently by users, or encrypted by ransomware.

Some cloud services may offer basic data protection that falls short of your needs for continuity or compliance. For example, Microsoft's increasingly popular Office 365 cloud productivity solutions offer some basic short-term data protection for email. But they do not currently protect SharePoint Online or OneDrive for Business. Nor do they address long-term retention or inadvertent data deletion by users.

Continuity solutions are fragmented and inefficient

As we've seen, most organizations now operate complex sets of physical, virtualized, and cloud workloads. The need to support new software defined architectures while continuing to protect legacy workloads running on older operating systems adds to the complexity.

Recognizing the need to protect all their workloads, many organizations have turned to tactical or point solutions. Their legacy servers may still be protected by a backup/recovery solution purchased several years ago. Their virtualized workloads may be protected by a solution designed solely or primarily for virtual machines. Cloud workloads may be protected by still other software; via add-on offerings from one or more cloud service providers, or by rudimentary data backup sometimes included with a cloud subscription.

In the real world, this tactical approach is problematic. Companies must manage multiple solutions, pay for multiple support contracts, maintain personnel skilled in each solution, and make sure somebody can operate each system at a moment's notice, notwithstanding vacations or unexpected illnesses. Moving workloads becomes more complex, because backup/recovery arrangements may need to move as well. Interdependent systems may require backup and recovery through multiple solutions which don't work together well, making it uncertain whether recovery will actually succeed.

> "Some cloud services may offer basic data protection that falls short of your needs for continuity or compliance."

In summary, maintaining multiple backup/recovery/continuity solutions increases cost, reduces organizational agility, and undercuts your confidence in your continuity plans.

The Solution: Protect all Workloads Through One Plan and One Platform

The solution consists of two elements: Build a customized plan to protect all your workloads, and deploy a unified platform that can fully support it.

Building your customized plan

Every organization's data protection plan should be unique, because each organization's priorities and workloads are unique. For example, it may be "undesirable" for a manufacturer to temporarily lose its corporate web server -- but for an e-commerce retailer, this would be devastating. On the other hand, if a manufacturer loses a specialized execution or ERP system, manufacturing might be halted, materials scrapped, and multi-million-dollar facilities idled.

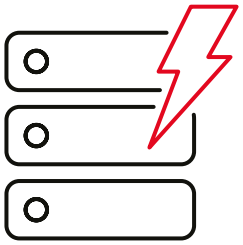
Begin building your plan by listing your current applications. Then, calculate your costs of downtime for each significant application, and how much downtime you can tolerate.

Be sure to consider costs beyond "lost business." For example, downtime costs can include idle resources, scrapped materials, regulatory penalties, damage to reputation, restart costs, and even potential injury or loss of life in some industries.

For the impact to be fully understood, calculate cost in the language your business owner will understand. For example, in finance or retail, how many transactions will be lost per minute of downtime? In manufacturing, how many widgets won't be manufactured? In healthcare, how many patients would miss critical treatments or appointments? What regulatory or compliance faults would be triggered?

Once you know the business impact of downtime, you can determine how much protection each application needs. For non-critical workloads, traditional local and off-site cloud backup may be sufficient. For more important workloads, consider incorporating a Disaster Recovery (DR) component. Disaster Recovery as a Service (DRaaS) solutions have made this easier, eliminating the requirement to maintain a backup data center.

When selecting a DRaaS solution for critical workloads, determine how quickly you need to be back online, and require a true SLA that guarantees to meet your RTO/RPO objectives. Consider, also, implementing recovery assurance technology. This technology guarantees that your application will recover to a certified recovery point, no matter what.



Traditionally, testing backups and DR required manual testing that was both disruptive and expensive. This explains why, of the companies that use DR, at least half test only annually or not at all. You obviously can't be confident about business continuity systems that you can't or don't test.

Recovery assurance solves this problem by automating DR testing on whatever schedule you specify: monthly, weekly, daily, or even more frequently. With recovery assurance, a complete new instance of your system's environment is spun up in a sandbox. Recovery assurance doesn't just test whether your application will boot: it tests all interdependencies and interconnections, even in complex n-tier systems. Not every workload requires this, but for those that do, there's no substitute.

Choosing your unified platform

Choosing a unified platform can significantly reduce complexity, because:

- You only pay for and support one tool, with one maintenance contract
- Your people must only master one system and interface; when some team members are unavailable, others can fill in to protect or recover any workload
- You can move workloads without swapping out recovery solutions
- You can test recovery of complex interdependent systems without involving multiple backup/recovery solutions or their operators

However, your unified platform must fully support your continuity plan, both now and in the future. This means it must:

- Protect all your physical, virtual, cloud, and software-as-a-service workloads, current and emerging
- Support all levels of protection, including local backup, offsite cloud backup, DR with SLA guarantees, and recovery assurance

- Protect against disruptions ranging from equipment failure to ransomware attack to major natural disasters
- Be fully integrated and intuitive

> "Unitrends' platform protects 250+ versions of operating systems, hypervisors, and applications."

Unitrends Connected Continuity Platform™

Protecting all workloads and your entire business

Unitrends responds to these challenges with the industry's broadest portfolio of cloud-empowered continuity solutions for backup, cloud continuity, disaster recovery, and recovery assurance.

Unitrends' Connected Continuity Platform redefines recovery around the goal of ensuring continuity for your entire business. It can protect all your workloads, offer continuity wherever you need it, guarantee full recovery without a doubt, and do all this through a highly-intuitive interface, so it's easy to protect even the most complex hybrid environment.

Unitrends' platform protects 250+ versions of operating systems, hypervisors, and applications. These include everything from the newest versions of Windows and Linux back to Windows NT 3.1 and IBM AIX; VMware and Hyper-V as well as alternative virtualization solutions such as KVM; and major applications such as Microsoft Exchange, SQL Server, Oracle, and Office 365 in the cloud.

Unitrends' Connected Continuity Platform solutions include:

- Continuity planning resources, including our BC/DR Link website which walks you through building your own DR plan
- Advanced appliances: both physical appliances as well as software-based appliances running within your virtualized infrastructure
- Multiple cloud-based continuity solutions, including Unitrends' purpose-built Forever Cloud for offsite backup storage and long term data retention; our comprehensive DRaaS solution; and multiple options for utilizing public hyperscale clouds such as Amazon Web Services (AWS) or Microsoft Azure for storing backup copies or Disaster Recovery.
- Guaranteed recovery to your RPO and RTO requirements, via recovery assurance technology that can integrate with any Unitrends continuity solution, on your premises, a second site, Unitrends' cloud or your own private cloud
- Comprehensive service and support with a customer satisfaction rating exceeding 98 percent

Learn more about how the Unitrends' Connected Continuity Platform can help you achieve complete business continuity with total confidence and minimal complexity.

Visit unitrends.com to get free trial software, schedule a demo, or test drive an appliance.

About Unitrends

Unitrends is trusted by business visionaries, IT leaders and Pro's who know that in today's digital world protecting their ideas and keeping their business running is non-negotiable. The Connected Continuity Platform™ enables organizations of all sizes to protect their data and assure business continuity for their physical, virtual and cloud based environments.

Unitrends offers the industry's broadest portfolio of cloud empowered continuity solutions in a single super intuitive platform delivering unmatched flexibility as needs evolve, providing 100 percent confidence in recovery and business continuity.

Unitrends' Continuity Solutions are backed by a global support team that consistently achieves a 98% satisfaction rating and are sold through a community of thousands of expert technology partners, service providers and resellers worldwide.