

# How You Can Make VMware Downtime History

Change your expectations about what is acceptable

## THE NEW DOWNTIME PARADIGM

As your VMware environment continues to be critical to your business, uptime is more important than ever. However, VMware backups have their challenges. VMs are getting larger and difficult to meet recovery objectives. Storage technologies are changing quickly and adding more features and performance every few months. That's great, but it's difficult to keep up with it all.

Today, customers expect 100% reliability: faced with downtime, they take their business elsewhere. Many systems are mission-critical. In industries such as healthcare and manufacturing, failures can even cause deaths. This state of affairs might be tolerable if downtime and data loss were rare. They aren't. Unitrends finds that 91% of companies have experienced unplanned downtime within the previous year, and 30% have experienced data loss. You can prevent some downtime-generating events, but not all. And downtime-related costs have risen dramatically: common estimates range from \$90,000 to \$300,000 per hour, depending on the analysis, industry, and size of organization.

Unfortunately, traditional backup/recovery systems haven't changed as fast as the demands placed on them. Meanwhile, systems have become increasingly distributed, networked, interdependent, and complex. The result has been both predictable and troubling: using these legacy solutions, many companies simply can't be confident in their ability to get back up and running as quickly as their business requirements demand.

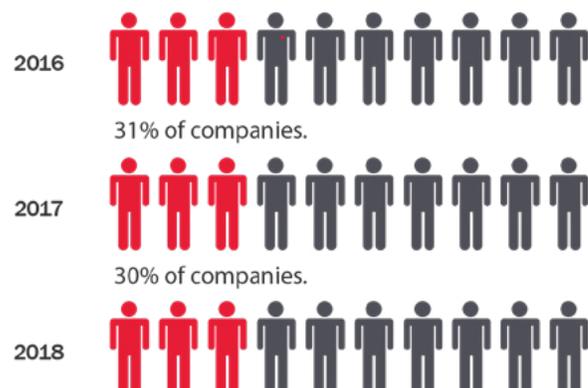
We call it "making downtime history." That's no small achievement, given the ways traditional systems have fallen short. But you can get there in three steps, and this white paper will show you how.

### Step #1: Change your mindset

The first step costs you nothing and requires no advanced technology: *change your mindset*. Move *away* from thinking about "backup and recovery." Move *towards* thinking about "continuity and resiliency."

Your goal is *not* to possess a set of media containing all your

### Percent of Companies That Experience Data Loss over the Last Year 2016, 2017, 2018



applications and data, nor even all your virtualized instances. Your goal isn't to create off-site data centers, nor even to buy cloud subscriptions.

Rather, **your goal is to make sure your business can keep running, whether you encounter a Category 5 hurricane, a ransomware attack, a data center fire, or just simple user error.** That means making sure you can recover and restart whatever you need, as quickly as you need to do so.

## Step #2: Plan and prioritize

Since you know downtime events are inevitable, you now focus on what your IT team can control: the impact of those events. This involves implementing the right plans, systems, and tests for each application and dataset. Start by understanding the costs of downtime and data loss in your unique organization: both at the macro business level, and for each significant application or system.

Tally the direct monetary costs that roll up to your P&L: lost transactions, potential regulatory penalties, and so forth. But don't forget about other costs -- some of which can be partly quantified, others equally important but not as quantifiable. For example, what is the impact to your company's reputation and brand when customers can't reach your sales team, or -- more likely -- when your sales team serves them poorly because accurate account or product information is unavailable?

At Unitrends, we often say that "all workloads matter, but they're not all equal." Control systems in a high-risk manufacturing or process-oriented business have radically higher downtime costs than low-risk reporting systems, run quarterly on a flexible schedule. Knowing each application's downtime costs helps you customize their continuity plans to balance cost and benefit.

## Step #3: Align protection levels to downtime costs

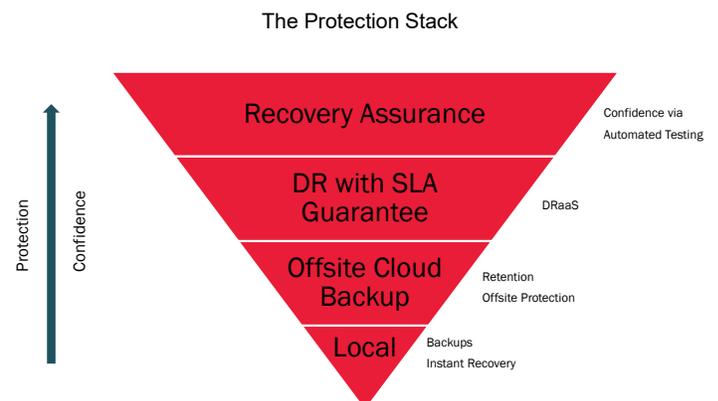
Obviously, the higher an application's downtime costs -- and the greater its importance to your business -- the more protection it needs. The pyramid in Figure 1 shows a modern "Protection Stack," rising from basic to maximum protection. As you move

up the stack, costs rise -- but so does your confidence that recovery targets will be met, even in extreme circumstances.

## Level 1 Protection: Local backups with instant recovery

Virtually all applications and data need at least basic local protection. Even at this level, a modern backup system should provide some form of "instant recovery" technology. This allows extremely rapid local recovery of a virtual machine or physical server, from backups on a local appliance. If one of your virtualized hosts or an individual guest fails, you can quickly switch to a virtualized backup running on the appliance or on another host system and keep running there while you're fixing your production device.

Strikingly, many IT organizations don't realize that instant recovery is now available with local backup appliances. Sometimes, even organizations that have purchased such appliances don't realize they have this capability, or haven't configured it. We encourage them to do so.



**Unitrends helps VMware users meet their RTOs, RPOs, and retention requirements with both hypervisor-level and guest-level protection.** You protect just what's needed, whether it's a full VM, a file, or just a single database. All VMware backup options provide application-level awareness to ensure data consistency, as well as instant recovery and global deduplication for fast recovery and maximum retention.

Unitrends also offers VMware replicas and application-aware backups for VMware VMs running Microsoft applications such as Microsoft Exchange, Active Directory, SharePoint and SQL without requiring agents in each and every VM.

---

## Level 2 Protection: Offsite cloud backup

For some applications, Level 1 protection is sufficient. But it is fully local: if your site becomes inaccessible -- for example, due to a network outage, natural disaster, or data center fire -- your backups will likely become inaccessible, too. This is one key reason many applications and databases require offsite backup. (A second reason: long-term records retention.)

Today, offsite backup is increasingly cloud-based -- sometimes, via purpose-built clouds designed specifically for the task; other times, via hyperscale public clouds such as Amazon Web Service or Microsoft Azure.

Cloud-based solutions and high-speed WANs have made offsite backup practical for many more organizations. But offsite data backup still doesn't guarantee that your mission-critical apps will be up-and-running as fast as you need them to be. For that, you must move further up the protection stack.

VMware backups can be used as part of a cloud-empowered disaster recovery and business continuity program. All Unitrends Recovery Series hardware and Unitrends Backup virtual appliances include cloud integration so you can easily benefit from Cloud-based Disaster Recovery as a Service that reduces downtime in the event of a major outage. Recover your VMware backups with Unitrends Cloud and our DRaaS services, or migrate, failover, and failback to 3rd party clouds including Amazon Web Services (AWS) and Microsoft Azure. Unitrends Boomerang easily and inexpensively replicates your VMware VMs to low cost AWS S3 or Azure Blob storage, until needed.

## Level 3 Protection: Cloud-based disaster recovery with SLA guarantees

As already discussed, Level 2 protection placed copies of your data offsite. If this data is stored in cloud environments, you already have the foundation in place for a modern DRaaS solution -- preferably with an SLA guarantee.

True "disaster recovery" either required building a complete backup datacenter, or contracting for access to one. Either way, it was too expensive and complex for all but very large companies. DRaaS democratizes disaster recovery, enabling nearly any organization to rapidly spin up critical workloads in the cloud, without building or staffing an additional datacenter.

---

*If you rarely or never test, you have no idea whether disaster recovery will work when needed.*

---

If you choose a DRaaS solution that a service provider can manage end-to-end (including cloud and local components), you can demand an SLA aligned to your application's business requirements. So, if an application must be online within four hours (or even one hour) you can hold your provider accountable for this. Given that (as discussed earlier) most organizations failed to meet Recovery Time Objectives during their most recent downtime event, this might be a higher standard than you can achieve on your own.

## Level 4 Protection: Recovery Assurance

Recent Unitrends research found that 60% of organizations that have invested in disaster recovery test it no more than once per year. Some never test it at all. It's easy to understand why. Testing disaster recovery systems has traditionally been time-consuming, disruptive, and expensive.

But let's be blunt: if you rarely or never test, you have no idea whether disaster recovery will work when needed. Today, production environments change rapidly. Complex dependencies between applications can shift overnight. For IT professionals, few experiences are worse than troubleshooting a disaster recovery failure during a disaster.

Recovery Assurance solves this problem by providing systematic automated testing to validate that your DR environments are working properly -- and notifying you of potential problems in advance, so you can resolve them in an orderly way, before disaster strikes.

Some IT professionals are surprised at just how effective Recovery Assurance can be. Using virtualized sandbox environments, you can test individual applications as often as you need to: monthly, weekly, daily, or even more often. You can spin up and validate even complex multi-tier/n-tier applications, check dependencies, and stress-test performance. The outcome should be a remote "Certified Recovery Point" that gives you absolute confidence you can meet your RPO/RT0 objectives.

# WHERE UNITRENDS FITS: ONE PLATFORM, EVERY SOLUTION

Aligning protection levels to specific needs works best when all your protection works together, and it's easy to move between protection levels as your business evolves. That's most practical if you can choose a single unified platform. Unitrends offers just such a platform. Unitrends' purpose-built all-in-one backup appliances with support for Unitrends Cloud deliver a complete disaster recovery platform. Unitrends' solution provides best-in-class backup and business continuity at all four levels of the protection stack -- all through one unified interface, one contractual relationship, and one world-class support organization. This gives you unmatched flexibility to choose the right continuity solution for every app, system, and business process.

For **Level 1** requirements, Unitrends offers the Unitrends Recovery Series: a scalable family of high-performance, cloud-empowered appliances that integrate purpose-built hardware, enterprise-class backup and recovery software, and instant recovery technology to support both virtualized and physical Windows workloads.

For **Level 2** applications, it's easy to build on your Recovery Series appliance, enabling its built-in support for replicating backup copies to the Unitrends Cloud for long term retention. If you prefer, you can replicate backup copies to public hyperscale clouds, use other service provider clouds, or use your own offsite private cloud.

At **Level 3**, we offer full cloud-based Unitrends Disaster Recovery as a Service (DRaaS) with the industry's only 1 hour SLA guarantee for your entire environment. Through this "white glove experience," we help you copy data into the cloud, set up your environment for recovery, and get everything tested. Since we can control the entire process, we can offer SLAs as rigorous as one hour for recovering your environment and restarting any essential workload in the cloud.

Finally, at **Level 4**, we offer state-of-the-art Recovery Assurance testing for backups at any level, whether stored on a Unitrends backup appliance or in the cloud. You can test continuity on whatever schedule you find appropriate, establish Certified Recovery Points where you can be sure of performance, and receive regular reports of anomalies -- so you can resolve them as part of routine IT administration.

Learn more about how Unitrends backup and continuity solutions can help you *make downtime history*. Visit [unitrends.com](https://unitrends.com) to get [free trial software](#), [schedule a demo](#), or test drive an appliance.

## BACKUP & DRaaS BUYER GUIDE

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](https://unitrends.com) or follow us on LinkedIn and Twitter @Unitrends.