UNITRENDS

THE NEW RULES OF RECOVERY

INTRODUCTION

FACT

With the seismic shift to a hybrid business model, which introduced remote and cloud workloads, organizations' IT priorities have shifted radically.[1]

IT demands have reached a crescendo. Now more than ever, organizations depend on IT to provide continuous availability of mission-critical workloads, data and applications.

In a 24/7 global economy, businesses must keep pace with mounting competitive pressure or perish. The onset of change has been rapid, with offerings, processes and operations digitized to varying degrees, all with the goal of growing the business. Many leaders who thrive today, even in a tumultuous landscape, were successful in orchestrating these consistent improvements in pursuit of modernizing an ever-evolving tech stack.

More recently, IT professionals have been tasked with juggling the responsibilities of spinning up and empowering a geographically dispersed workforce with, at times, limited access to company facilities and resources. They are also being asked to maintain and secure existing assets, find new ways to boost revenue and minimize costs in the face of forces from within and without.

FACT

41% of cyberattacks leverage phishing techniques to gain initial access to an organizational network.[2]

The transition to a hybrid business model has put the spotlight on the SaaS delivery model. Although the SaaS model was gradually gaining recognition in the pre-COVID era, the rapid shift to the hybrid work culture and the ensuing digital transformation has accelerated its adoption rate among SMBs and large enterprises. Better Cloud projects that 85% of software used by organizations will be SaaS by 2025.[3] While this shift to the SaaS model offers unprecedented speed, scalability and affordability for organizations, it also paved the way for new threat vectors and galvanized others that had fallen out of prominence; IBM's X-Force Intelligence Index revealed that over the last two years, phishing surpassed vulnerability exploits as the leading infection vector.[4]

Various studies suggest that the hastened digital transformation has stirred up a hornet's nest of cybersecurity risks for SMBs and large enterprises. For instance, the Identity Theft Resource Center reports that approximately 92% of the data breaches in the first quarter of 2022 resulted from cyberattacks.[5] This ever-growing threat landscape of SaaS data puts IT security and risk management teams in dire straits today.

Against this backdrop, the significance of a business continuity solution becomes all the more relevant. An ideal business continuity solution creates systems to deal with potential cyberthreats and ensures operational continuity in the wake of a cybersecurity incident. It gives IT the power to proactively drive strategy, control access and visibility into all data streams — whether local, remote or in the cloud — and guarantee systems are recoverable, compliant and will help keep the business running.

From Backup and Recovery to Continuity

At Unitrends, we believe it’s time to reimagine recovery and take advantage of new, available architectures and technology to transform a siloed, legacy approach to backup and recovery into a business continuity solution. For many, the narrow, task-based approach of piecemealed legacy solutions has left gaps in coverage, invited complexity and left organizations bogged down in low-value, manual tasks.

We’ve devised the New Rules of Recovery to help organizations begin the shift from a traditional approach to backup and recovery to a solution-focused approach where success is defined by the outcome and by keeping your business running no matter what. With our solution-focused approach, we empower IT to deliver tangible benefits to your organization and meet the challenges of a digital world today and tomorrow.

In a 24/7 global economy, businesses must keep pace with mounting competitive pressure or perish. The onset of change has been rapid, with offerings, processes and operations digitized to varying degrees, all with the goal of growing the business. Many leaders who thrive today, even in a tumultuous landscape, were successful in orchestrating these consistent improvements in pursuit of modernizing an ever-evolving tech stack.

RULE #01

ROBUST BUSINESS CONTINUITY SOLUTIONS DON'T HAVE TO BE OVERLY CUMBERSOME OR COMPLEX — TODAY'S SOLUTION IS MANAGEABLE, AUTOMATED AND PROACTIVE.

FACT

66% of IT decision-makers see skills gaps in their teams, and 63% have been unable to fill at least three positions in 2022.[6]

We know you're likely wearing many hats. If you're looking for better ways to manage surging workloads, get ahead of the changing demands of the business and work around staffing shortages. Keep in mind that you're not alone. Remember the days when you had a dedicated backup resource? That one IT pro you could always rely on to get things sorted, and who knew what to do and when? Unfortunately, priorities changes, budgets get cut and technology evolves, leaving IT teams wanting.

Your continuity solution shouldn't have you scrambling to identify and fix errors. Being able to respond to an incident quickly, locating the data you need and initiating recovery — whether finding files or recovering multitiered applications — should be intuitive and friendly enough so that even users who infrequently access the solution can navigate with ease and agility.

Providing a modernized, intuitive user experience is one of our main priorities. The hybrid and multicloud strategies make the organizational infrastructure more convoluted, rendering its management and security more complex, costly and unreliable. On that front, Unitrends UniView empowers organizations with a unique approach to backup data management. Regardless of the platform your data resides in — be it hybrid cloud backup appliances, direct-to-cloud backup or SaaS backup (Microsoft 365 and Google Workspace) — UniView offers a single pane of glass to manage it all.

Moreover, UniView's centralized management hub enables multitenant management with one-screen simplicity so you can manage multiple locations, customers and tenants.

Customizable dashboards give users unique insights into aspects of the solution most important to their scope, making the evaluation of your protection environment to detect and resolve problems quick and seamless without the need to refer to a manual. You will be navigating the same interface regardless of whether you're managing a physical, virtual or mixed environment.

Moreover, you can manage thousands of appliances from one interface with our Distributed Enterprise Manager.

Beyond saving you time through reduced clicks and easy UI navigation, we've augmented our solutions with automation and artificial intelligence (AI) engines to cut down on manual tasks. With supportive activities being performed reliably and seamlessly, you can focus on boosting the business's bottom line with creative projects, product crafting and customer service.

Under the watch of Unitrends Helix, protected assets in your production environment are autonomously kept clean with SaaS-powered remediation of common environmental errors. Helix monitors your backup appliance and production environment to autonomously correct VSS errors and various other software-related issues, ensuring clean, consistent backups and thus saving time for IT teams. Thanks to its self-healing capability, Helix continues to look for new cases and fix them across all customer environments.

Even with a clean environment and successful backups, it is paramount that you periodically test your recovery to identify potential recovery pitfalls and ensure compliance. Unitrends Recovery Assurance powers deep recovery testing for virtual, physical and cloud environments down to the application level. With this deep verification, our users' complete confidence in their ability to recover is second to none. You can have Recovery Assurance run testing as frequently as you need and have detailed compliance and recoverability reports delivered directly to your inbox.

Your continuity solution shouldn't have you scrambling to identify and fix errors. Being able to respond to an incident quickly, locating the data you need and initiating recovery — whether finding files or recovering multitiered applications — should be intuitive and friendly enough so that even users who infrequently access the solution can navigate with ease and agility.

RULE #02

THE RISE OF REMOTE WORKERS MEANS WE NEED TO FINE-TUNE OUR APPROACH TO DATA PROTECTION.

FACT

In the first year of the pandemic alone, Microsoft 365 experienced a staggering 21% rise in usage to 258 million users.[7]

The growth in the user base of Microsoft's SaaS platform — Microsoft 365 — from 60 million (Q3, 2015) to more than 345 million paid seats (Q2, 2022) is a microcosm of our transition to a distributed, remote workforce.[8] Before the events of the COVID-19 pandemic accelerated the adoption of technology-facilitated, socially distanced business practices, the traditional office layout was becoming less and less relevant to the way we do business.

The rise in remote and mobile workers leaves critical data on endpoint devices at risk of deletion, damage, loss and theft. In the past, the geographic distribution of devices made it difficult for IT to have physical control, with the resources available, to meet the backup and recovery needs of these endpoints. However, with every one in 10 laptops being lost or stolen in its lifetime, it is vital to protect the data stored on these machines.

To minimize the cost and productivity impacts of downtime in the event of device loss or damage, Unitrends Endpoint Backup (EPB) offers an easily deployed direct-to-cloud solution to back up and recover data being created and stored on endpoint devices. With on-premises storage or local IT management required, EPB helps simplify your data protection strategy for endpoints and files that don't need to be on a traditional appliance.

A cloud-based UI makes recovery a breeze, enabling point recovery at the same endpoint, or any endpoint with the EPB agent installed, to seamlessly restore files and folders without any fees to access or recover your data.

With EPB securing data saved on the endpoint, the other key factor that ensures continuity for remote workers is safeguarding their SaaS data. Services like Microsoft 365, Google Workspace and Salesforce all operate under a shared model of responsibility, i.e., IT still owns data protection even though the SaaS provider owns the application platform. Providers like Microsoft are worried about providing uptime, redundancy (of workloads, not necessarily your data) and ease of use. Their focus is on maintaining infrastructure and the availability of the applications rather than your data, and typically their SLAs will cover for their mistakes but not yours. Their data centers with advanced disaster recovery capabilities can protect from infrastructure threats like hardware and software failure, power outages and natural disasters. However, they cannot protect your data from the prominent reasons for SaaS data loss, like human errors, external cyberthreats and malicious insider activities.

According to Verizon's 2021 Data Breach Investigations Report, 44% of data breaches in small and midsize businesses (SMBs; <1000 employees) and 36% of data breaches in mid-market enterprises (MMEs; >1000 employees) are caused by insider threats.[9] To help protect your organization from accidental deletion (the leading cause of SaaS data loss), such internal and external security threats and more, look no further than Spanning Backup for Microsoft 365.

An easily deployed SaaS-powered backup solution for Microsoft 365, Google Workspace and Salesforce, Spanning gives you the power to readily recover deleted data and meet long-term retention and compliance requirements with unlimited retention, with a backup environment that is fully managed. Self-service recovery means you can initiate restores from anywhere you can access the web interface and recover to any user on your tenant.

The growth in the user base of Microsoft's SaaS platform — Microsoft 365 — from 60 million (Q3, 2015) to more than 345 million paid seats (Q2, 2022) is a microcosm of our transition to a distributed, remote workforce.8 Before the events of the COVID-19 pandemic accelerated the adoption of technology-facilitated, socially distanced business practices, the traditional office layout was becoming less and less relevant to the way we do business.

RULE #03

BLACK HATS ARE SAVVIER THAN EVER. TO GUARANTEE RECOVERY, YOUR BACKUPS *MUST* BE SECURED.

The annual share of ransomware attacks experienced by organizations worldwide has been on the rise since 2018, peaking at a whopping 71% in 2022.[10]

Ransomware, one of today's greatest cyberthreats, has exploded in both frequency and complexity of attacks in the last few years. The worst year on record for ransomware attacks is set to be taken by 2022 from last year. During the first half of 2022 alone, there were a total of 236.1 million ransomware attacks worldwide.[11]

It's become clear that ransomware is not a fad spyware or a "flavor of the month" sort of prank but rather a sophisticated business model with specific targets, delivery vectors and robust ROI in many cases for the attackers. Many programs are targeted toward government entities to exploit security weaknesses in aging infrastructure, while others turn toward enterprises where the stakes are high regarding the loss of sensitive corporate data.

For either target, successful intrusion can wreak tremendous damage in terms of operations and reputation. Furthermore, recent ransomware variants are rapidly becoming masters at deception — refining functions to minimize their chance of detection while a slow-burning infection begins to encrypt and lock access to data and in some cases even disable protective programs, Windows utilities and backup software.[12]

Up-to-date security, user education, consistent patch management and a strong backup strategy have proven to be an effective layered approach to combating ransomware since thorough disaster recovery planning can dramatically reduce the impacts of a ransomware attack. A full disaster recovery plan includes the ability to restore compromised servers nearly instantaneously.

Unitrends Instant Recovery restores any compromised machines in minutes while you work to rebuild the production server. In addition to fast recoveries, we've taken steps to harden the backup environment as well. Unitrends cloud-empowered appliances provide an immutable backup copy by storing a copy of your backups in the cloud or on detached media (such as a disk) that is separate and isolated from your production environment and network. Our appliances operate on a hardened Linux kernel — less targeted and less vulnerable than Windows-based counterparts since those appliances and network shares are as equally vulnerable to being encrypted and held ransom. We've also augmented our appliances with machine learning — analyzing change rates, entropy (randomness) to identify anomalies, and encryption with automated emails and alerting — enabling you to catch hackers in the act before the damage is done.

RULE #04

THE WORLD IS MOVING TO THE CLOUD, AND YOU SHOULD TOO. HOWEVER, THERE'S MORE THAN ONE WAY TO GET THERE.

FACT

89% of enterprises have a multicloud strategy, while 80% have a hybrid approach.[13]

The cloud has become an integral part of our technology stack. Yet, as more and more organizations embrace cloud technologies, we've learned cloud adoption is not a case of one size fits all. For some, the cloud is an inexpensive, scalable storage resource while others see the cloud as their final destination and are redesigning their entire business model around it. What's become clear is that there is no single journey to the cloud.

Early adopters prioritized functions like web hosting, web-based applications and Unified Communication (UC) migration to a cloud service. Recently, organizations have been increasingly turning to cloud platforms for backup and recovery-related tasks. Storage, archiving and backup are some of the services most likely to have been migrated to cloud platforms. In fact, a majority (60%) of organizations report using the cloud as a tool in their data protection strategy.[14]

So, how do you determine which cloud is the right one for your backup, recovery and business continuity needs? Some vendors build their offerings based on hyper-scale public clouds from Amazon, Microsoft and Google. With generally low upfront costs, near-unlimited scalability and high reliability, public clouds are one option you may consider. Yet, despite their many advantages, public clouds aren't without risk. Without the right plan and expertise in place, you may find your resources (and costs) running wild — an estimated 25–35% of cloud spend is "wasted," especially in cases where visibility and governance are not prioritized and centralized.[15]

However, the public cloud is far from the only option, and some vendors prefer to focus on the benefits of private or purpose-built cloud offerings. A purpose-built cloud is one designed solely for a specific purpose. In the case of the Unitrends Forever Cloud, that purpose is cloud-enabled continuity. In tune with, and developed alongside our backup software, Unitrends integrated cloud data centers are equipped with resources focused on receiving inbound backup jobs, initiating recovery requests and running the workloads and applications enrolled in our white-glove Disaster Recovery-as-a-Service (DRaaS).

Our dedicated Cloud Services teams help shorten the learning curve for organizations looking to use the cloud for the first time and help take the risk out of cloud adoption with a turnkey approach to cloud backup and recovery. Our cloud storage is based on the amount of data you want to protect, not the amount of storage that's consumed, and our DRaaS enables you to spin-up critical applications and infrastructure to keep your business running.

Unitrends gives you the choice of all cloud options to build a continuity solution that fits your organization's recovery needs. Supporting Public Cloud Integrations (AWS, Google, Azure), Unitrends Forever Cloud, or private cloud deployments, the solution integrates with the cloud of your choosing to orchestrate off-site recovery, long-term data retention and Disaster Recovery capabilities.

RULE #05

DISASTER RECOVERY WITHOUT AN SLA IS NOTHING MORE THAN A BROKEN PROMISE.

Unitrends DRaaS provides a contractually guaranteed, 1-hour recovery time SLA.[16]

You wouldn't buy a car without knowing the specifications, features, mileage and accident history, would you? It's unlikely you'd enter into many contracts, personally or professionally, without knowing what you're going to get for your money. Your disaster recovery is no different. SLAs are particularly important for backup and recovery. To ensure compliance with objectives, it's critical to understand what the vendor or service provider responsibilities and guarantees are, if any. Less thorough consumers may find themselves signed up with cloud-based services with SLAs so soft, or even non-existent, that all they've really purchased is cheap off-site storage.

"Cloud" can mean so many different things today. With offerings of varying scope and quality, it's important to define your requirements so you know what to look for. Does the provider guarantee or offer a specific recovery time (RTO)? What about resiliency or guarantees for uptime with the service? If you're subject to maintaining data compliance, the sovereignty of data may be important. Are you certain of where your data is being stored? How many cloud data centers in how many regions? What sort of native tools or services does the provider offer? Are they available to you 24/7 by phone, web or email? If you're marrying multiple vendors as part of the solution, are they all subject to the same SLA?

The list goes on. In response to the rising needs for recovery and helping navigate a growing cloud landscape, DRaaS solutions have emerged. DRaaS equips organizations to simultaneously automate, accelerate and simplify cloud adoption and recovery of applications individually or at scale.

At Unitrends, we believe the consumer deserves total transparency and confidence in your ability to recover mission-critical applications in the time their business demands. We understand that recovery presents a new set of challenges for many — you're tasked with achieving specific RTOs measured in seconds/minutes/hours for each application, and the recovery point (RPO) to determine how much, if any, data loss an application can sustain prior to recovery. However, we are here to help you every step of the way.

Think of Unitrends DRaaS as an extension of your team. We'll work closely with you to ensure applications and data are made available within your defined RTO/RPOs and perform the spin-up of critical systems in the Unitrends Cloud for complete disaster protection.

Unlike other providers, we offer physical seeding options to accelerate initial cloud setup to be prepared should disaster strike. You can spin-up and maintain key applications and data in the Unitrends Cloud in the event of a local disaster. When you're ready to failback to your primary site, we also provide a Data Shipment SLA in which we'll have your data back to you on disks or a new backup appliance within 24 hours.

Customer service and support is often overlooked but is something we take immensely seriously here at Unitrends. We're extremely committed to our customers' success and are proud to offer the very best, award-winning, white-glove cloud services.

RULE #06

DR TESTING DOESN'T HAVE TO EAT INTO YOUR FTE HOURS (OR WEEKENDS).

FACT

While 29% of SMBs and 31% of MMEs perform DR testing once a year, 17% of SMBs and 11% of MMEs do not perform it at all.[17]

Disaster Recovery (DR) testing is critical but also painful. After all, if you don't test, how can you be sure the workload will be recoverable (or free of malware or compliant)? We know you'd rather be doing something more interesting than running a DR test; they eat up time for planning, potentially disrupt the business while running and can cost more than just employee time. Yet, with the growing strategic importance of digital information, a shrinking tolerance of downtime across industries and the increasing operational dependence on IT, testing once a year just isn't enough. With so much changing so rapidly, are you confident you can rely on results of a March test for a disaster scenario in November?

Unitrends Recovery Assurance (RA) eliminates the manual hassle of recovery testing by automatically performing the highest levels of application recovery testing with minimal IT intervention. RA accesses production data as fully functional VMs contained within isolated testing labs. These Instant Labs allow for testing, data analysis and dev sandboxes without impacting your production environment. RA fully restores applications, performs analytics measuring RTO and RPO, and identifies reasons why any recoveries have failed. Testing occurs on the backup appliance or within the Unitrends Cloud, so there is no impact on your product systems.

Simply schedule the time and systems you want tested, customize and define aspects such as boot order, machine resource allocation and application-level tests, and the appliance does the rest. Using your latest backups, RA installs the full software stack, boots it in a test environment and orchestrates the sequences you've defined.

Once completed, RA tears down the isolated testing environment and automatically creates and emails complete, graphical reports of results to your designated recipients. Run tests on demand or as required by scheduling regular intervals for compliance tracking any time changes are made to production or during larger-scale DR exercises.

Unitrends RA works at the application level to validate that applications boot and are running correctly, exercising APIs, and RTO and RPO goals are being met. The confidence you'll feel reading regular proof of recoverability reports is second to none.

In the event of a disaster, RA orchestrates failover from certified recovery points. In spite of a disaster, it spins up n-tier applications or entire sites within the cloud for business continuity. It means production data becomes accessible to users in the aftermath of an incident so that users can continue working swiftly.

RULE #07

TODAY’S SOLUTION ELIMINATES TOMORROW’S PROBLEMS.

FACT

One in five organizations experienced a serious or severe outage (involving significant financial losses, reputational damage, compliance breaches and in some cases, loss of life) in the past three years.[18]

As complexity increases across clouds, downtime risks remain high. The emergence of AI, however, is growing in its use to solve errors before they even occur and can be taught to catch new ones too. Imagine planning to come in to work to finally kick off your company’s Microsoft 365 migration — it might be a little scary, it’s a big project with a lot of stakeholders — but immensely rewarding too. You come into the office and notice you’ve got a bunch of alerts saying backups failed yesterday. You look at the logs but aren’t quite sure what to make of them.

Now you’re combing through error logs and calling up support. Dreams of kicking off the migration today are fading fast. L1 wasn’t sure of the issue so they’ve escalated you to L2. L2 has you run some tests, but nothing’s working. Half a day of troubleshooting later, you finally identified a failed VSS writer on the host that was the root of the issue. When it’s time to report on the status of your migration project, it’s a huge bummer — “No progress today. Worked with our backup vendor to get backups working.”

It’s all too common to go off track when something goes awry. Although no solution is without error, we want our users dedicated to more interesting and fulfilling work than babysitting backups. A key piece is how Unitrends helps keep the production environment clean of nagging service errors and potential utility failures with Unitrends Helix Self-Healing.

Helix is designed to identify and fix some of the most common backup problems without you having to lift a finger. In addition, there’s minimal overhead with Helix — no servers to manage and the agents are updated without any user interaction.

Always on alert, Helix is a SaaS-powered platform that’s constantly looking for any issues within the OS of protected systems — VSS writer state, disk space checks, network connectivity and more will be remediated proactively upon detecting an issue to save you time pouring over logs and calling up support. Instead of failed backups, warning lights flashing and a mess of alerts, you come in to see successful backups and, when performed, an email from Helix so you’re aware of any remediation actions that were taken. With Helix monitoring and solving errors without manual intervention, you’re free to tackle those more fulfilling and interesting projects.

The future of Helix is bright. As it evolves with your needs, we are building enhancements for future versions to intelligently increase RPOs and initiate automated recoveries after certain failure conditions.

THE 7 NEW RULES OF RECOVERY:

History is written by the victors. We feel true leaders set the rules, not stick to them. Are you ready to reimagine your approach to DR and business continuity? We're transforming the traditional approach to backup and recovery to keep your business running as we meet the demands of tomorrow's digital world.

An approach built on the New Rules of Recovery:

RULE 1:

ROBUST BUSINESS CONTINUITY SOLUTIONS DON'T HAVE TO BE OVERLY CUMBERSOME OR COMPLEX — TODAY'S SOLUTION IS MANAGEABLE, AUTOMATED AND PROACTIVE.

RULE 2:

THE RISE OF REMOTE WORKERS MEANS WE NEED TO FINE-TUNE OUR APPROACH TO DATA PROTECTION.

RULE 3:

BLACK HATS ARE SAVVIER THAN EVER. TO GUARANTEE RECOVERY, YOUR BACKUPS MUST BE SECURED.

RULE 4:

THE WORLD IS MOVING TO THE CLOUD, AND YOU SHOULD TOO. HOWEVER, THERE'S MORE THAN ONE WAY TO GET THERE.

RULE 5:

DISASTER RECOVERY WITHOUT AN SLA IS NOTHING MORE THAN A BROKEN PROMISE.

RULE 6:

DR TESTING DOESN'T HAVE TO EAT INTO YOUR FTE HOURS (OR WEEKENDS).

RULE 7:

TODAY'S SOLUTION ELIMINATES TOMORROW'S PROBLEMS.

YOUR NEXT STEPS:

TO DISCOVER HOW UNITRENDS CAN HELP YOU REIMAGINE BACKUP AND RECOVERY,

GET IN TOUCH NOW:

EXPLORE UNITRENDS SOLUTIONS

— DISCOVER OUR INDUSTRY-LEADING PRODUCTS AND SERVICES.

DOWNLOAD A FREE 30-DAY TRIAL

— SIGN UP AND CLAIM YOUR FREE, 30-DAY,
RISK-FREE TRIAL OF UNITRENDS ENTERPRISE BACKUP SOFTWARE,
UNITRENDS CLOUD BACKUP OR SPANNING BACKUP FOR MICROSOFT 365.

CONTACT UNITRENDS

— SPEAK DIRECTLY WITH ONE OF OUR CONTINUITY EXPERTS.

Source:

[1] Tech Trends & Insights Survey Report - Unitrends

[2, 4] IBM Security X-Force Threat Intelligence Index 2022 Full Report

[3] 2020_StateofSaaSOpsReport.pdf (bettercloud.com)

[5] Q1 Data Breach Analysis - ITRC (idtheftcenter.org)

[6] Skillsoft Research Reveals More Than Half of IT Professionals Likely to Pursue a New Position Within the Next Year - Skillsoft

[7] https://www.statista.com/statistics/545520/market-share-of-internet-browsers-usa/

[8] https://office365itpros.com/2019/04/25/office-365-reaches-180-million-users/

[9] 2021-data-breach-investigations-report.pdf (verizon.com)

[10] https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/

[11] Number of ransomware attacks per year 2022 | Statista

[12] https://blog.malwarebytes.com/threat-spotlight/2020/02/threat-spotlight-robbinhood-ransomware-takes-the-drivers-seat/

[13] Trends in Cloud Computing: 2022 State of the Cloud Report | Flexera Blog

[14] https://www.unitrends.com/wp-content/uploads/Cloud_Survey_Results.pdf

[15] https://www.ciodive.com/news/with-the-cloud-comes-a-side-effect-cost-overrun/557513/

[16] https://www.unitrends.com/wp-content/uploads/Premium-DRaaS-Data-Sheet.pdf

[17] Tech Trends & Insights Survey Report - Unitrends

[18] Uptime Institute’s 2022 Outage Analysis Finds Downtime Costs and Consequences Worsening as Industry Efforts to Curb Outage Frequency Fall Short - Uptime Institute

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 focusing 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