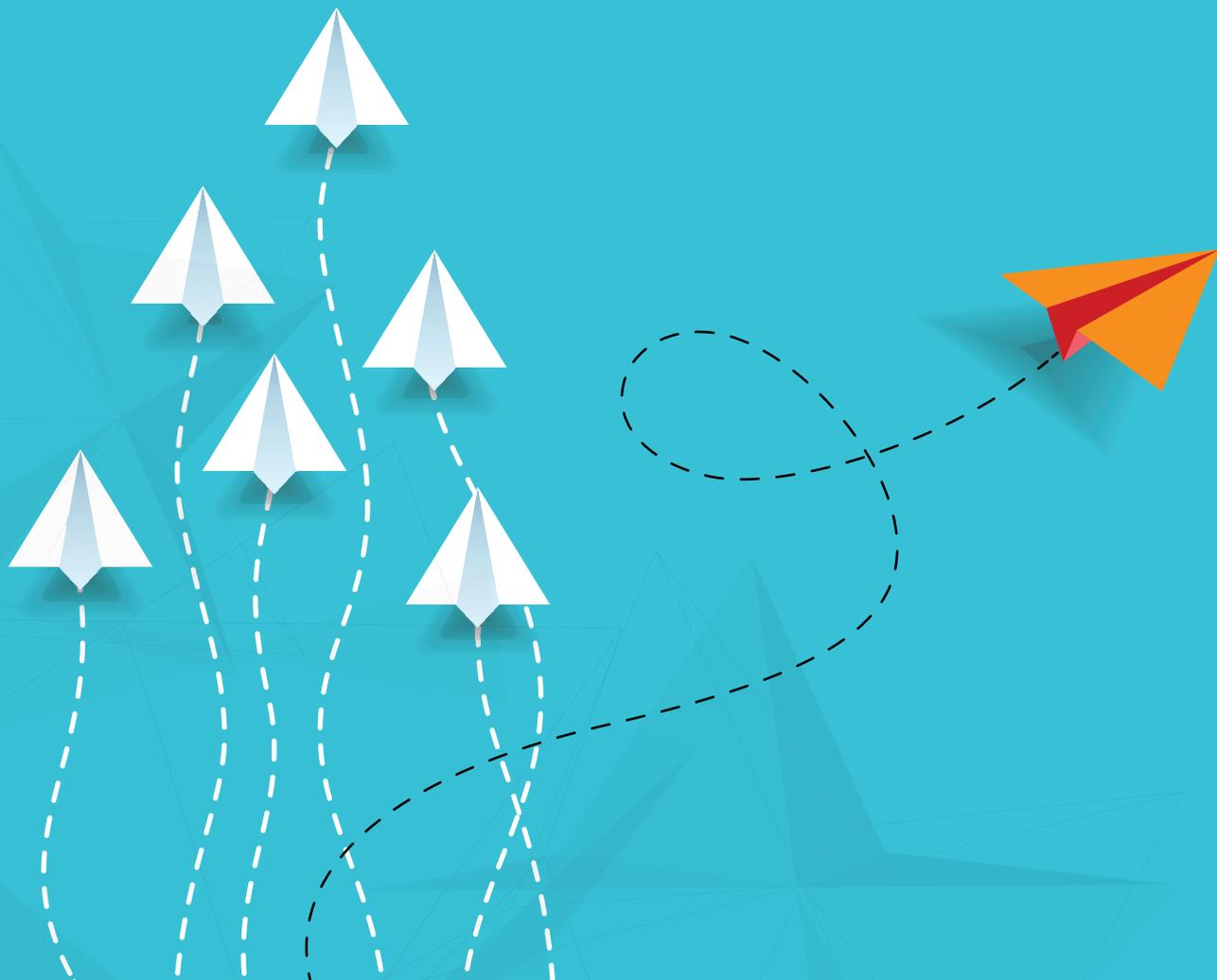


# THE NEW RULES OF RECOVERY



# INTRODUCTION



## 70% of companies either have a digital transformation strategy in place or are working on one.<sup>1</sup>

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

To keep pace with mounting competitive pressure in a 24x7 global economy, companies are forced to adapt or die. 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 of the leaders who thrive today in an at times tumultuous landscape, have been 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.



## 59% of enterprises expect cloud usage to exceed prior plans due to COVID-19.<sup>2</sup>

Gartner succinctly describes forces of change in the business realm as “turns.”<sup>3</sup> Turns, often occurring in real-time, stem from organizational disruption, the pressure to reduce operating costs, regulatory and compliance intervention, budget shortcomings and shifts in consumer demands.

Turns test the fitness of an organization – the fittest organizations are galvanized, and with IT as a point of leverage, emerge from turns increasing revenue and driving growth. Organizations less adept at navigating turns are likely to fall behind and continue to lag during subsequent turns.

Your Business Continuity solution is one lever. The fittest solutions give IT the power to proactively drive strategy, give control over access and visibility into all data streams whether local, remote or in the cloud, and guarantee that systems are recoverable, compliant and will help keep the business running.

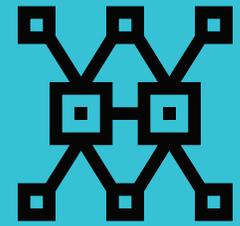
## From Backup and Recovery to Continuity

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’re giving the power to IT to deliver tangible benefits to your organization and meets the challenges of a digital world today and tomorrow.

[A new approach that’s built on the new rules of the day...](#)

# RULE # 01



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



**The number of open IT and computed-related jobs are nearly 8x the graduating computer science students entering the workforce.<sup>4</sup>**

We know you're likely wearing a lot of 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 change, budgets get cut and technology evolves, leaving IT teams wanting.

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

Providing a modernized, intuitive user experience is one of our main priorities. The Unitrends user interface (UI) has coalesced all your local backup and recovery-related tasks within a single pane of glass. 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.

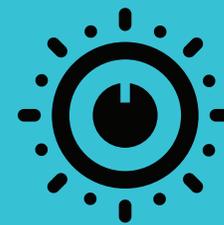
And if you have multiple sites? No problem! You can manage thousands of appliances from one interface with our [Distributed Enterprise Manager](#).

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 the manual tasks you and your team are forced to perform. With supportive activities being performed reliably and seamlessly, you can focus on boosting the business' 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.

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.

# RULE # 02



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



### Microsoft Office 365 grows its 180 million active user pool by 4 million new users per month.<sup>5</sup>

The growth in the user base of Microsoft's SaaS platform, Office 365, from 60 million (Q3, 2015) to more than 180 million (Q34, 2019), is a microcosm of our transition to a distributed, remote workforce.<sup>6</sup> 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 today.

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, or even the resources available, to meet the backup and recovery needs of these endpoints. But, with every 1 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 Cloud Backup](#) (UCB) offers an easily deployed direct-to-cloud solution to backup and recover data being created and stored on endpoint devices. With no-promises storage or local IT management required, UCB 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 with the UCB agent installed, to seamlessly restore files and folders without any fees to access or recover your data.

With UCB securing data saved on the endpoint, the other key factor that ensures continuity for remote workers is safeguarding their SaaS data. Services like Office 365, Google Apps and Salesforce.com all operate 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.

Don't just take it from us! Industry professionals at [Forrester](#) and [Gartner](#) recommend augmenting native tools for "faster, more-flexible" recovery options via the use of third-party tools.<sup>7</sup> To help protect your organization from accidental deletion (leading cause of SaaS data loss), internal and external security threats and more, look no further than [Spanning Backup for O365](#).

An easily deployed SaaS-powered backup solution for O365 (Google Apps and Salesforce.com as well). 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.

# RULE # 03



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



**62% of targeted organizations were compromised by ransomware last year – a 15% increase in successful attacks.<sup>8</sup>**

Ransomware, one of today's greatest cyberthreats, has exploded in both frequency and complexity of attacks in the last few years. 2019 saw thousands of attacks, with costs in excess of billions of dollars. These incidents went beyond expensive inconvenience. With nearly 1,000 public sector entities under siege, including healthcare providers, health, safety and lives were put at risk.<sup>9</sup>

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 towards government entities to exploit security weaknesses in aging infrastructure while others turn towards 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.<sup>10</sup>

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. Being able to rewind the clock to before you were attacked can get your data back – a full disaster recovery plan includes the ability to restore compromised servers near 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 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 to ransom as other applications and workloads. 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. BUT THERE'S MORE THAN ONE WAY TO GET THERE.



**93% of enterprises have a multi-cloud strategy; 87% a hybrid cloud strategy.<sup>11</sup>**

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.<sup>12</sup>

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 aren't prioritized and centralized.<sup>13</sup>

However, the public cloud is far from the only cloud 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](#).

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, you have a solution that 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.<sup>14</sup>

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?

And the list goes on. In response to the rising needs for recovery and helping navigate a growing cloud landscape, Disaster Recovery as a Service (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 Recovery Times (RTO) 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).



### 55% of organizations test recovery once a year, or less.<sup>15</sup>

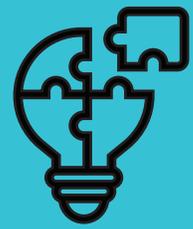
Disaster Recovery testing is critical but also painful. After all, if you don't test, how can you be sure the workload will be recoverable (or free of malware or compliant)? We know you'd rather be doing something more interesting than running a DR test; they eat up time for planning, potentially disrupts 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](#) eliminates the manual hassle of recovery testing by automatically performing the highest levels of application recovery testing with minimal IT intervention. 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, Recovery Assurance 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 out regular intervals for compliance tracking any time changes are made to production or during larger-scale DR exercises.

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

# RULE # 07



## TODAY'S SOLUTION ELIMINATES TOMORROW'S PROBLEMS.



**42% of organizations were hit with downtime last year and 30% lost data as a result of the outage.<sup>16</sup>**

As complexity increases across clouds, downtime risks remain high. The emergence of Artificial Intelligence (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 O365 migration – it might be a little scary, it's a big project with a lot of stakeholders – but immensely rewarding too. You come in to 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 enhancement for future versions to intelligently increase Recovery Point Objectives (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. BUT 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 WITH UNITRENDS OR YOUR UNITRENDS PARTNER.

## Reach Out Today!

Your Unitrends Product Experts:  
 Alan Fink at Prianto Distribution  
 alan.fink@prianto.com  
 01635 225262

Paul Hollow at Unitrends:  
 phollow@unitrends.com  
 0203 608 2749



### SOURCE

- 1 <https://www.forbes.com/sites/blakemorgan/2019/12/16/100-stats-on-digital-transformation-and-customer-experience/#28a841423bf3>
- 2 <https://www.flexera.com/blog/industry-trends/trend-of-cloud-computing-2020/>
- 3 <https://www.ciodive.com/news/the-fit-and-the-fragile-2020-cio-agenda-requires-it-flexibility/565625/>
- 4 <https://www.advsyscon.com/en-us/corporatesite/media/pdf/workload-automation.pdf>
- 5 <https://office365itpros.com/2019/04/25/office-365-reaches-180-million-users/>
- 6 <https://office365itpros.com/2019/04/25/office-365-reaches-180-million-users/>
- 7 <https://www.gartner.com/en/documents/3730718/adopt-microsoft-office-365-backup-for-damage-control-and>
- 8 <https://cyber-edge.com/cdr/>
- 9 <https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/>
- 10 <https://blog.malwarebytes.com/threat-spotlight/2020/02/threat-spotlight-robbinhood-ransomware-takes-the-drivers-seat/>
- 11 <https://www.flexera.com/blog/industry-trends/trend-of-cloud-computing-2020/>
- 12 [https://www.unitrends.com/wp-content/uploads/Cloud\\_Survey\\_Results.pdf](https://www.unitrends.com/wp-content/uploads/Cloud_Survey_Results.pdf)
- 13 <https://www.ciodive.com/news/with-the-cloud-comes-a-side-effect-cost-overrun/557513/>
- 14 <https://www.unitrends.com/wp-content/uploads/Premium-DRaaS-Data-Sheet.pdf>
- 15 [https://www.unitrends.com/wp-content/uploads/Cloud\\_Survey\\_Results.pdf](https://www.unitrends.com/wp-content/uploads/Cloud_Survey_Results.pdf)
- 16 [https://www.unitrends.com/wp-content/uploads/Cloud\\_Survey\\_Results.pdf](https://www.unitrends.com/wp-content/uploads/Cloud_Survey_Results.pdf)

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

**UNITRENDS**  
 A Kaseya COMPANY

