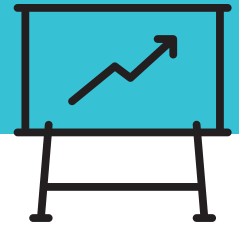


5 STEPS TO BUILDING YOUR **BUSINESS CONTINUITY & DISASTER RECOVERY SOLUTION**

PROTECT, SECURE AND
RECOVERY ANYTHING, ANYWHERE



INTRODUCTION



Data is growing 33 times faster than IT administration.

Data lives in more places than ever before. The proliferation of mobile devices, file retention needs, application enhancements, digital capacity growth and big data has changed how we manage digital assets. Using more technology than ever before, businesses are producing an avalanche of data that must be backed up and stored. While IT tackles explosive growth on the digital front, there's pressure on departments to stabilize or even cut spending. IDG noted that data growth has exceeded staffing growth 33 fold. With IT spending expected to increase by only 9% this year,¹ it's clear that organizations are asking IT to do more with less.

In today's digital world, IT professionals know they're safeguarding more than just data, servers and applications. They are the guardians of their organization's ideas, knowledge and intellectual property, and bear the responsibility of keeping their businesses up and running no matter what.

Today, more than ever, enterprises need a backup and recovery solution that offers a complete platform that requires less management, has the agility to protect all workloads and leverages automation to simplify complex systems, all while securing data from cybercrime and human error.



71% of organizations targeted by ransomware are successfully infected.²

The propagation of **ransomware** has rapidly become one of the most widespread and damaging causes of downtime. A successful attack hampers businesses, vultures valuable IT time, and potentially causes painful damages to data and an organization's reputation.

For enterprises that are not prepared when ransomware attacks, there is little recourse to reclaim your data other than paying the ransom. Ransom payments have increased by 82% in 2021³ and they provide no guarantee you'll recover your data. The Sophos State of Ransomware 2021 report found that only 8% of organizations who paid ransom got all of their data back.⁴

However, for organizations that take the necessary steps, disruptions can be minimized and data loss can be avoided.



One in six (16.667%) data center outages cost more than \$1 million.⁸

About 76% of IT organizations have experienced an IT service outage in the last three years, with nearly one in four (23.5%) outages lasting 12 hours or longer.⁹ Severe outages take days, if not weeks, to resolve. They often involve replacing one or more points of failure. Service disruptions take employees and business assets offline and represent one of your organization's greatest risk exposures. About 93% of businesses that were unable to recover their data within 10 days post-disaster, filed for bankruptcy within a year.¹⁰

21 days — Average downtime experienced after a ransomware attack.⁵

\$170,404 — Average ransomware payout among mid-sized organizations in 2021.⁶

\$20 billion — Global cost of ransomware-related damages in 2021.⁷



Unified BCDR Is the Future

While IT Pros have long experienced success with conventional business continuity and disaster recovery (BCDR) efforts, they understand it's time to modernize their data protection infrastructure. With rising demands for storage, data privacy and government regulations, legacy approaches to BCDR are at odds with today's complex data protection needs.

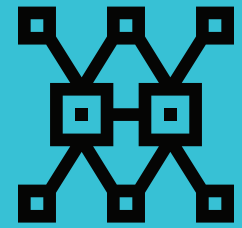
At any given point, businesses store huge volumes of critical data on-premises, in public clouds, in private clouds and SaaS applications. Data fragmentation has become a major obstacle to data protection. A staggering 66% of organizations are projected to be **using three or more unique solutions** in 2021. This leaves IT wasting time managing multiple tools and combating interoperability challenges while jumping from dashboard to dashboard. When third-party "integrations" don't live up to marketing promises, backup and recovery efforts suffer. Nearly **one-third** of all organizations experience problems with backup restoration. Platform incompatibility leaves IT with a time-consuming, inflexible and expensive solution sprawl as a result of more solutions being introduced into the environment to meet the demands of an evolving infrastructure.

A **Unified BCDR** solution simplifies management of a complex backup architecture, enabling modern data protection while **cutting TCO in half**. Centralized management provides visibility across an entire backup infrastructure while the injection of automation combats human error and cybercrime, and validates backups with application-level recovery testing for 100% confidence in any restore to come.



THE 5 Cornerstones

How to Do More With Less



“MUST-HAVES” FOR PROTECTING YOUR DIGITAL ASSETS

It's a challenge for IT professionals to meet the rising demands of stakeholders and end users while struggling with reduced budgets and increasing IT complexity, right from managing heterogeneous environments with physical, virtual and cloud assets as well as an explosion in data volumes, to a range of new software-defined architectures. As a result, backup and disaster recovery, which is an integral part of your infrastructure, often fails to receive the strategic focus it deserves, even as enterprises become more and more reliant on digital assets.

IT visionaries are turning to more complete solutions. They are looking for platforms that offer the agility to protect all workloads while consolidating the number of vendors they need to use. In essence, they are on the lookout for ones that inject artificial intelligence and automation to simplify complex tasks and remediate errors, require less time and effort to manage, and ultimately, solutions they have 100% confidence in.

There's a new frontier in backup and recovery: Unified BCDR. This ideal solution includes:

- One Centralized Platform for all workloads. Consolidating to a Unified BCDR platform enables seamless management of all data, whether protecting data center, remote, cloud or SaaS assets.
- Purposeful Workflow Integrations. Leverage automation and artificial intelligence throughout the platform to reduce risk of errors and failures while cutting management time by as much as 50%.
- Best-in-Class Enterprise capabilities for local and cloud continuity with Recovery Assurance. Eliminate the unknown with orchestrated, application-level DR runbook testing to proactively identify potential compliance or recovery issues.
- Ironclad Security. Purpose-built, hardened Linux architecture camouflages backups from malware and ransomware. WAN-accelerated replication of AES 256-bit encrypted backup copies to immutable cloud storage or air-gapped media secures data in-flight and at-rest, enabling off-site recovery.
- Unified Support. A 100% U.S.-based, customer-obsessed support organization dedicated to our users 24/7/365. Unification of the platform means high confidence and no finger pointing.

ONE CENTRALIZED PLATFORM



Cornerstone #1

HAVING ALL THE FUNCTIONALITY YOU NEED IN ONE PLACE, MANAGED THROUGH ONE INTERFACE, IS PART OF THE SIMPLICITY OF BEING COMPLETE. ACHIEVE FASTER TIME TO RESOLUTION (TTR), LESS JUMPING THROUGH HOOPS AND NO FINGER POINTING BETWEEN DISPARATE VENDORS.

As organizations evaluate their options for a business continuity and disaster recovery (BCDR) solution, more and more IT pros are considering moving towards a single-vendor, all-in-one solution to simplify management and maintenance while minimizing the risks of interoperability and siloed components. This is not always as easy as it would appear since data is fragmented across on-prem, remote and cloud instances. In response, organizations have shown a growing preference towards vendors who can protect all physical, virtual and cloud assets.

IT visionaries aren't just considering the backup and recovery needs of their environment as it exists today. To prepare for future growth, your strategy should provide the agility to adjust backup plans to accommodate changes in services, software and devices as they occur. For instance, an on-prem solution may be the right option for protecting Hosted Exchange, but wouldn't be the best fit for Microsoft 365 once that data moves to the cloud. It's about leveraging the approach that provides the recovery capabilities necessary to meet your organization's SLAs.

Unitrends offers a fully-integrated suite of backup and recovery solutions with varied approaches to protect data, including **hybrid cloud appliances**, **SaaS backup** and **direct-to-cloud endpoint backup**, all managed through a single, **centralized console**. By deploying a Unitrends enterprise backup and continuity solution, you can oversee protection for your entire environment. Purposeful security integrations leverage automation and artificial intelligence to reduce the frequency and severity of data loss events. Unitrends portfolio of all-in-one, cloud-empowered continuity solutions provide IT departments with complete protection for their protected environment, with unmatched flexibility as needs evolve. Automated, application-level DR runbook testing certifies workloads for 100% confidence in recoveries to come.

Unitrends' solution is customizable to support your unique data center and cloud configurations with protection for more than **250 versions of operating systems, applications and hypervisors**. Beyond backup and recovery capabilities for a wide range of assets, the Unitrends platform provides native capabilities for replication, **adaptive deduplication**, compression and encryption, all working in unison to combat the challenges of protecting an organization's digital assets.

A streamlined, single-vendor, turnkey solution that empowers IT to accomplish more with less, validates the transition from multiple, disparate vendors by eliminating management, finger-pointing and hassle.

“

WE USED TO HAVE MULTIPLE PORTALS DO MULTIPLE THINGS. TO GO THROUGH ONE PANE OF GLASS – I LIKE THAT. I CAN GO IN, SEE MY DEVICE, REMOTE IN, LOOK AT BACKUPS, SEE TICKETS... IT'S THAT ONE PORTAL TO LOG IN TO TO GET A GREAT PICTURE OF MY ENVIRONMENT AS A WHOLE.

— Jason Poulin, IT Director, [Bristow Medical Center & Core](#)

”

PURPOSEFUL WORKFLOW INTEGRATIONS



Cornerstone #2

**INJECTING AUTOMATION AND ARTIFICIAL INTELLIGENCE
SIMPLIFIES COMPLEX SYSTEMS, REDUCES MANAGEMENT
OVERHEADS AND STREAMLINES WORKFLOWS, THEREBY
IMPROVING TIME TO RESOLUTION.**

Modern IT environments are complex. They are a combination of physical, virtual and cloud systems that must all work in concert to deliver the services that employees, end users and stakeholders expect. In many ways, production environments are ill-suited for backup and even less so for recovery. By keeping up with environmental changes, backup solutions have grown increasingly complex in turn. Often, IT pros find themselves paying for functionality they aren't using, or being bogged down by features that are difficult and time-consuming to use. At Unitrends, we aim to leverage automation and artificial intelligence to simplify systems and bring our automation technology to solve problems in production before they can impact backups. Backups that are not in lockstep with environment changes will fail more often, requiring remediation and incurring IT expense.

Unitrends Helix is designed to reduce IT investment in backup system management through self-healing technology. Autonomous and SaaS-based, Helix proactively monitors and remediates issues with VSS services and third-party VSS providers that can wreak havoc on backups. It also keeps backup appliances up to date, so you'll always benefit from the latest feature releases and security patches.

We're also leveraging integrations in the security use-case to enable the platform with data loss prevention through automated **phishing defense** and dark web monitoring, purpose-built to complement our **Spanning Backup for Office 365**. Layered phishing defense helps guard against clumsy or careless employees while empowering them to take part in the defense of their organization with actionable banners and click-to-quarantine emails. Dark web monitoring alerts you to potentially compromised credentials, enabling proactive measures to secure accounts at risk from Account Takeover (ATO) attacks and Business Email Compromise (BEC).

BEST-IN-CLASS ENTERPRISE CAPABILITIES



Cornerstone #3

UNITRENDS IS BUILT FOR THE UNEXPECTED, WITH CUTTING-EDGE, SELF-HEALING HARDWARE PAIRED WITH GEOREDUNDANT CLOUD DATA CENTERS. AUTOMATED APPLICATION-LEVEL RECOVERY TESTING AND PROACTIVE MONITORING BY CLOUD EXPERTS KEEPS OUR PLATFORM AT OPTIMAL EFFICIENCY AND RESILIENCY.

For Unitrends, the future is now. Our all-in-one business continuity platform provides organizations with a best-in-class, comprehensive level of integration.

Unified BCDR delivers integrated enterprise backup, replication and disaster recovery. A flexible product suite, including a variety of backup approaches ranging from physical and virtual data center appliances, cloud-to-cloud SaaS protection and direct-to-cloud protection for endpoints, enables users to customize deployment to meet the needs of your unique data center and cloud configurations. Unitrends is the only vendor with a continuity solution that offers backup, instant recovery and 100% Recovery Assurance for physical, virtual and cloud-based workloads.

Our hybrid-cloud appliances form the cornerstone of our platform. Turnkey, all-in-one deployment converges all of the functionality you need in one place. Recovery options range from local capabilities, such as granular file recovery, application recovery and instant recovery of physical and virtual servers, to invisible failover into the Unitrends Cloud. Predictive analytics proactively identifies and resolves threats to recovery before they occur. Self-healing hard drives in Unitrends Recovery Series appliances reduce disk-drive-related downtime by as much as 90% by monitoring and correcting most sources of RAID-level failure, and automatically alerting our 24/7/365 U.S.-based support team if needed.

Application-level recovery testing through [Recovery Assurance](#) automates DR testing against your customized DR runbook, proactively detects recovery issues and orchestrates failover in the event of disaster. Test as often as you need, directly on your Recovery Series appliance or on a designated virtual host. Results, including SLA compliance reports, are delivered directly to your inbox.

Beyond backup and recovery procedures, the platform offers native **adaptive deduplication**, compression and encryption for backups at-rest locally as well as in-flight. Built-in **WAN acceleration** optimizes data transfer to a variety of private and public cloud targets. Unitrends offers connectivity to multiple public and private cloud providers. IT Pros can also tap into our proprietary cloud service for long-term, off-site retention and Disaster-Recovery-as-a-Service (DRaaS).

Beyond utilizing public clouds, such as AWS for off-site retention and disaster recovery, Unitrends appliances can be deployed to protect native AWS instances. **DCIG** named Unitrends a Top 5 AWS Cloud Backup Solution in 2020-2021. Unitrends was distinguished as a Top 5 solution in part due to Recovery Assurance. “Unitrends stands apart as one of the only providers to formally offer backup testing and verification. This grants enterprises the flexibility to regularly test and verify they can successfully recover from their backups.”

“

THE INTERFACE IS REALLY EASY TO USE. I IMPORTED DATA FROM [OUR] REMOTE [ARCHIVE] LOCATION AND BROWSED. I WAS ABLE TO GO BACK OVER A YEAR AND GET THE FILE. IT WAS REASSURING THAT EVERYTHING WAS THERE IN THE ARCHIVES AND WORKING AS WE'D HOPED.

— Greg Lanz, Sr. Systems Admin, [Canada Diagnostic Centers](#)

”

This testing may be performed in the Unitrends Cloud as part of our proprietary DRaaS offering. By doing so, this approach “mitigates the additional compute and storage costs as well as configuration overheads that performing these tasks in the AWS cloud would incur. It also gives enterprises confidence they can recover outside the AWS cloud should it become unavailable, which does occur.”

Additionally, Unitrends provides these enterprise capabilities:

- Proactive discovery of recovery issues for physical and virtual appliances
- SLA Policy scheduling scheme
- Seamless long-term retention with self-service recovery
- Business-level DR compliance report automation
- Functionality for local, DR site and Unitrends Cloud

Unitrends portfolio of all-in-one, cloud-empowered backup and continuity solutions delivers a best-in-class enterprise solution for supporting physical, virtual and application workloads both locally as well as across public and private clouds.



Cornerstone #4

PURPOSE-BUILT BACKUP APPLIANCES OFFER MULTIPLE LAYERS OF SECURITY FROM A HARDENED LINUX OS KERNEL, IMMUTABLE STORAGE AND PROACTIVE MALWARE DETECTION.

AV Test's 2020 Security Report revealed more than 78% of malware developed in the last two years is designed to target and penetrate the Windows operating system, peaking at 83% of malware code developed in Q1 of 2020.¹¹ With the CVE database attributing more than 660 "dangerous" vulnerabilities to Windows (357 specifically to Windows 10), ransomware security has become a major concern for enterprises running Windows operating systems. The newest innovations in malware extend beyond targeting the Windows OS.

“

OUR ENTIRE NETWORK WAS COMPROMISED. A MASSIVE RANSOMWARE ATTACK HAD HIT EVERYTHING. I WAS IN THE DOOR AT 3 A.M. PULLING NETWORK CORDS TO ISOLATE WHAT WAS LEFT. ALL TOLD, I WAS ABLE TO GET THE COMPANY BACK UP BY MONDAY MORNING. I DON'T KNOW WHAT WOULD'VE HAPPENED TO THE COMPANY IF WE DIDN'T HAVE UNITRENDS.

— Chris Rolke, IT Manager, [Dualite, Inc.](#)

”

New ransomware variants have mechanisms designed to overcome the backup defense, including targeting backups on network-accessible locations and using publicly available APIs to delete backups autonomously. Modern ransomware doesn't encrypt data immediately. It has a period of gestation to avoid detection before detonation. When dormant malware is backed up along with legitimate data, an attack loop is created since the backups used to recover after an attack contain the malware, which detonates again.¹²

In response to the widespread attacks on Windows machines, many organizations are transitioning away from Windows-based backup software. By contrast, Linux operating systems are far less common. In addition to a small market share, the hierarchical architecture of Linux systems makes them more difficult to compromise.

In response to the widespread attacks on Windows machines, many organizations are transitioning away from Windows-based backup software. By contrast, Linux operating systems are far less common. In addition to a small market share, the hierarchical architecture of Linux systems makes them more difficult to compromise.

Unitrends understands the advantages of differentiating the backup environment from production environments and offers the ability to deploy a Linux-based virtual appliance for VMware ESXI, Microsoft Hyper-V and Nutanix Acropolis (AHV), or as a purpose-built turnkey hardware appliance. Hardening of the appliance kernel helps in creating a more secure system, and additional security measures are implemented upon installation, such as forcing the user to change the appliance root password and limiting the ports used by the appliance. Many users will deploy and operate their solution on air-gapped networks to keep the backup appliance completely isolated. This can be achieved without any loss of functionality. Beyond hardening of the appliance kernel and environmental security controls, Role Based Access Control (RBAC) enables individual self-service while also securing the system from unwanted access.

Beyond your local appliance, you can leverage Unitrends WAN-accelerated replication to replicate backup copies to alternative target(s). By replicating data to removable media such as disk or tape, users can create an airgap from the production network for their backup copies by storing them offline in a secure, secondary location. Data replicated to the **Unitrends Cloud** lands on immutable storage. Once written to the cloud target, no source can modify, change or delete backup copies. Backups stored in the Unitrends Cloud are in a ready-for-recovery state and are accessible right from your local appliance interface. All data is AES 256-bit encrypted in-flight and at-rest.

Through a combination of local protection and off-site, air-gapped targets, Unitrends provides you with ironclad security to ensure maximum protection of digital assets.

UNIFIED SUPPORT



Cornerstone #5

CUSTOMER-OBSESSED SUPPORT WITH A 98% CUSTOMER-SATISFACTION RATING

At Unitrends, customer service and support is a priority. As providers of Business Continuity Disaster Recovery solutions, including hardware, software and a full-service, proprietary cloud offering, we know you have to keep your business up and running no matter what.

“

[UNITRENDS IS] THE MOST COMPREHENSIVE AND BEST SUPPORTED SOLUTION AVAILABLE. WE WERE SADLY A VICTIM OF RANSOMWARE. TO PUT IT BLUNTLY, YOU SAVED OUR BACON.

— Christopher Frake, [Frontier Distributing](#)

GREAT PRODUCT WITH GREAT SUPPORT. THEY ARE EFFICIENT AND VERY GOOD AT FOLLOWING UP WHEN NECESSARY... EXTREMELY HELPFUL AND KNOWLEDGEABLE.

— Lauren Benson, [Advanced Invasive Pain Management of Houston](#)

”

Our award-winning customer support and service team strive to provide our customers with the fastest and most comprehensive support possible. Recently, we've achieved a 16% reduction in phone and chat response time and maintained a 98% customer satisfaction rating year-over-year. Unitrends offers full support for the entire business continuity stack, from local hardware and software to our dedicated cloud services. The platform encompasses data protection for all workloads, including data center workloads, SaaS applications, and remote endpoints and devices.

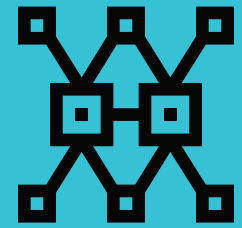
Often, when IT pros combine multiple vendors, they expose themselves to fragmented support as disparate products are stitched together with the goal of achieving business continuity. This siloed approach opens the floodgates to a downward spiral of interoperability, misconfigurations and finger pointing, ultimately decreasing satisfaction and increasing time to resolution. By utilizing a Unified BCDR platform, the risks that come along with multiple vendors are eliminated, disjointed support experiences become a thing of the past, and you benefit from a comprehensive support and service organization.

With Unitrends you get:

- **24/7/365 Support:** Disasters can strike when you least expect, and they certainly don't take evenings or weekends off. Our tireless Customer Support team is available to our community all year round by phone, chat and email. In fact, 24/7/365 is our support standard. Regardless of whether you're running a single instance of our virtual appliance or have deployed dozens of Recovery Series appliances across your several locations, our support team has your back 24 hours per day, 7 days a week, 365 days a year.
- **Technical Expertise:** Unitrends backup approaches encompass protection for on-prem physical and virtual workloads, applications, SaaS apps such as Microsoft 365 and Google Workspace, as well as cloud infrastructure. As such, it's paramount our support engineers are knowledgeable and educated on supporting the wide range of IT systems used by our customers and protected by our products. With decades of experience in the backup and recovery space and a shared passion for BCDR, our support engineers are well-versed and keep pace with the ever-changing landscape of data protection.
- **Customer Onboarding & Education:** All of our customers receive onboarding training and education. As part of the onboarding process, our team takes time to understand each customer's unique environment and needs, helps set up the backup appliance, implements backup strategies (agent and agentless), and shares best practices to manage backups and optimize your experience going forward.
- **Proactive Monitoring and Outreach:** Our purpose-built physical appliances are equipped with hardware proactively monitored by a predictive analytics engine. This self-healing technology is built to correct most sources of RAID-level failure and has reduced drive-related component failures by 90%. In the event a drive cannot fix itself, it phones home to our support team who proactively get a replacement overnighted to your appliance site the next day. This way, our support team is able to connect with customers before hardware issues negatively impact backups.
- **Customer Portal, Knowledgebase and Community:** Customers get access to Unitrends [Customer Portal](#) with an in-depth Knowledgebase and Technical Library, Live Chat expertise, Video Tutorials and Downloads (agents, trials, updates). They're also invited to take part in the [ConnectIT Community](#), a global, homegrown community for IT professionals utilizing any of Kaseya's brands, where you can engage with special interest groups, get answers and provide suggestions and feedback to key stakeholders, and even share, buy and sell your own scripts and templates as part of the Automation Exchange.

Unitrends offers our customers round-the-clock access to continuity experts who are laser-focused on successful outcomes for our customers. Beyond addressing your concerns when they arise, our team strives to empower and teach customers as we work with them along the way. The Unitrends team is always there to lend a guiding hand.

THE **5** Cornerstones of **BUILDING A BUSINESS CONTINUITY AND DISASTER RECOVERY SOLUTION**



Innovators set the standards, not stick to them. Unitrends is transforming the traditional approach to backup and disaster recovery by eliminating siloes and injecting automation and artificial intelligence to enable our customers to do more with less and meet the challenges of the digital world today and tomorrow.

Unitrends Unified BCDR is built on these five cornerstones:



Cornerstone 1:

- One Centralized Platform for protection of all workloads



Cornerstone 2:

- Purposeful Workflow Integrations simplify complex systems



Cornerstone 3:

- Best-in-Class Enterprise Capabilities for local and cloud continuity



Cornerstone 4:

- Ironclad Security secures data locally and in the cloud from today's advanced cyberthreats



Cornerstone 5:

- Unified Support; award-winning support available 24/7/365



YOUR NEXT STEPS:

TO DISCOVER HOW UNITRENDS CAN HELP YOU REIMAGINE BACKUP AND RECOVERY FOR YOUR DIGITAL WORLD, [GET IN TOUCH WITH US TODAY.](#)

DOWNLOAD

A FREE 30-DAY TRIAL

- SIGN UP NOW FOR A FREE, 30-DAY, NO-RISK TRIAL OF UNITRENDS ENTERPRISE BACKUP SOFTWARE. EVALUATIONS OF OUR RECOVERY SERIES PHYSICAL APPLIANCES ARE ALSO AVAILABLE.

REGISTER

FOR A LIVE DEMO WITH ONE OF OUR CONTINUITY EXPERTS

- SEE FIRSTHAND THE #1 UNIFIED BCDR SOLUTION IN ACTION.

EXPLORE

UNITRENDS PRODUCTS

LEARN MORE ABOUT OUR INDUSTRY-LEADING PRODUCTS AND SERVICES ONLINE AT WWW.UNITRENDS.COM

SOURCE

- | | |
|-------------|--|
| 1 Gartner | 8 Uptime Institute |
| 2 Varonis | 9 Uptime Institute |
| 3 PurpleSec | 10 invenioIT |
| 4 Forbes | 11 https://www.av-test.org/en/news/facts-analyses-on-the-threat-scenario-the-av-test-security-report-2019-2020/ |
| 5 Varonis | 12 https://securityboulevard.com/2020/10/ransomwares-next-target-backup-data/ |
| 6 Sophos | |
| 7 ZDNet | |

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

