

UNITRENDS

UNLOCKING DATA RESILIENCE: A COMPREHENSIVE ROADMAP TO THRIVE IN A RISKY DIGITAL WORLD



In this rapidly evolving digital age, businesses can no longer afford even the slightest amount of downtime. With customer expectations running high and competition as fierce as ever, the impetus to provide services 24/7/365 has become non-negotiable. Whether it's a small e-commerce store, a bustling medical practice or a burgeoning tech startup, the demand for constant availability is universal — a reality modern organizations are forced to embrace.

To meet this ceaseless demand, organizations are increasingly turning to the cloud. The cloud's allure of scalability, flexibility and near-constant availability makes it the go-to solution for organizations to ensure that their business operations continue unfazed. According to Gartner¹, more than 95% of all new digital workloads will be deployed on cloud-native platforms by the year 2025. However, the transition to the cloud is often piecemeal and has given rise to hybrid and multicloud environments, generating a complex web of data dispersed across diverse platforms, providers and locations.

An organization's data now lives in more places than ever before — from on-premises, various clouds and SaaS applications to everything in between. While this diversity offers many benefits, it introduces an array of complex data protection challenges. From the complexities of securing data across these different environments to the ever-evolving and rapidly expanding cyberthreat landscape, organizations must navigate a minefield of risks today to secure their business-critical data.

Cyberattacks remain one of the most prominent data threats organizations face. Cyberthreats, such as phishing attacks, ransomware and malware, are becoming increasingly frequent, targeted and sophisticated, wreaking havoc across the business world. Underlining this growing menace,

Statista² predicts that the global cost of cybercrime could almost triple in the next five years, rising from \$8.44 trillion in 2022 to \$23.84 trillion by 2027.



While also considering other major data threats, like natural disasters and human errors, organizations need to effectively address an ever-growing spectrum of risks today. Failure to do so could result in drastic financial, reputational and operational consequences.

It's against this backdrop of evolving data protection requirements and an exploding threat landscape that data resilience becomes even more critical. Data resilience is a strategic approach that empowers organizations to rise to data protection challenges and keep their data secure and readily available. Techopedia³ defines data resilience as "an organization's ability to ensure business continuity despite any unexpected disruption." Data resilience helps organizations continue their business as usual, even during times of disruption. It is the shield that wards off data loss, the gateway to business continuity and the key to maintaining customer confidence.

We have designed this whitepaper to be your organization's guide in its journey towards data resilience. This whitepaper will provide you with a comprehensive view of the evolving threat landscape and dive into the shifting tides of data protection strategies. We will also highlight some effective backup and recovery solutions, best practices for rapid data recovery and strategies to future-proof your data protection. Unravel the critical significance of data resilience and empower your organization to secure its future in this unpredictable digital world.



¹ <https://www.gartner.com/en/newsroom/press-releases/2021-11-10-gartner-says-cloud-will-be-the-centerpiece-of-new-digital-experiences#:~:text=By%202025%2C%20Gartner%20estimates%20that,to%20be%20aligned%20b y%20products>

² <https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/>

³ <https://www.techopedia.com/definition/34762/data-resilience>

I. Unmasking modern data threats

Today, organizations face a myriad of challenges that test the resilience of their business operations. Understanding these challenges is the first step towards building a robust data resilience strategy. Let's delve into the five key data protection challenges confronting businesses today:

Cybersecurity threats

Cyberattacks are growing in frequency, severity and complexity every day, causing widespread distress across the business community. The rise of the hybrid work model and the exponential increase in the number of employees and systems outside the conventional IT perimeters have expanded the attack surface of organizations, making them more vulnerable than ever to cyberthreats. According to IBM⁴, the global average cost of a data breach in 2023 is \$4.45 million, making cyberattacks a potential existential threat to businesses today.

Ransomware is the most frequently detected cyberattack worldwide⁵, accounting for 68% of all cyberattacks. It has emerged as a highly profitable multibillion-dollar business model for cybercriminals, with annual revenues in the billions and double-digit growth projections. The proliferation of open-source ransomware versions and delivery models like Ransomware-as-a-Service (RaaS) has led to a substantial increase in both the number and complexity of ransomware attacks recently.

According to Statista⁶, over 72% of businesses worldwide have been affected by ransomware in 2023.

Phishing is another common tactic used by cybercriminals currently. With an estimated 3.4 billion⁷ phishing emails sent out each day worldwide, all it takes is a single moment of vulnerability from one of your employees for cybercriminals to spring into action and compromise the entire business network. Other types of cyberattacks, like malware attacks, denial-of-service attacks and zero-day exploits, are also increasing, making it even more challenging for organizations to secure their networks and business-critical data.

An estimated 3.4 billion phishing emails are being sent out each day worldwide.

Hardware failure

Hardware failures are inevitable, even in the most advanced systems. Whether it's a server crash, a hard drive malfunction or a power outage, hardware issues can result in both data loss and downtime. In an environment where the smooth flow of data is crucial, the impact of such failures can be significant.

Human errors/malicious actors

External actors aren't the only ones that pose a threat to your data. Whether through accidental deletion or misconfiguration, your employees' errors can lead to data loss and downtime as well. In fact, the role of insiders in business vulnerability is growing massively. According to a Cybersecurity Insiders report⁸, 74% of companies are at least moderately vulnerable to insider threats. The report also reveals that the average cost of an insider threat incident in 2023 is \$15.38 million. That's why protecting against both inadvertent and deliberate data breaches is paramount for businesses.

⁴ <https://www.ibm.com/reports/data-breach>

⁵ <https://www.statista.com/statistics/1382266/cyber-attacks-worldwide-by-type/>

⁶ <https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/>

⁷ <https://earthweb.com/how-many-phishing-emails-are-sent-daily/>

⁸ <https://www.cybersecurity-insiders.com/portfolio/2023-insider-threat-report-gurukul/>

Natural disasters/environmental factors

It's important to remember that natural disasters can be just as devastating to data as other threats. According to the Federal Emergency Management Agency (FEMA)⁹, 25% of businesses shut shop after a disaster. Earthquakes, floods, fires and hurricanes can all cause significant damage to physical data centers, while environmental factors like power surges and temperature fluctuations can affect hardware performance. With global temperatures on the rise, it's crucial for businesses to prepare for a range of potential natural disasters to protect their data.

Complexities involved in sprawling data footprint

As businesses increasingly adopt cloud solutions, data finds itself distributed across various platforms and environments. Data may reside on local servers, cloud services and employee endpoints, adding layers of complexity to data protection. Data movement to and from these locations poses significant challenges in terms of maintaining its security, availability and recoverability.

II. Crafting resilience: Tailored data protection strategies

In your journey towards data resilience, understanding the challenges is only the beginning. To safeguard your data in the face of these threats, your organization must take concrete steps to fortify defenses and ensure the integrity, availability and recoverability of critical data.

Let's explore some tailored strategies to tackle each of the above-mentioned data protection challenges head-on.

Ransomware and other cyberthreats: Prevention, mitigation and recovery

You need to adopt a multifaceted approach involving prevention, mitigation and recovery to effectively defend against today's sophisticated cyberattacks.

Prevention

Data backups alone cannot help secure your data since ransomware attacks actively target backup repositories. Leverage a backup appliance with a hardened kernel to reduce the risk of ransomware and other cyberattacks. Windows OS is a prime target for threat actors, with over 97% of malware and potentially unwanted applications (PUAs) created targeting the Windows OS¹⁰. As a result, organizations are increasingly transitioning away from malware-susceptible Windows-based backup software to Linux-based.

Linux-based backup solutions camouflage your data from Windows-seeking malware, and the hierarchical architecture of Linux architecture makes it difficult to compromise.



Moreover, only around 1% of malware and PUAs target Linux OS.¹¹

You should also secure your backup server or appliance behind company firewalls. It is recommended that you keep your backup appliance completely isolated — preferably in an air-gapped network — so it becomes difficult for potential attackers to access it.

⁹ <https://www.fema.gov/press-release/20230502/stay-business-after-disaster-planning-ahead>

¹⁰ <https://www.av-test.org/en/statistics/malware/>

¹¹ <https://www.av-test.org/en/statistics/malware/>

Besides this environmental security control, you must implement multifactor authentication (MFA) on all systems and platforms where it is available. You can also implement role-based access control (RBAC) to strengthen the security of your backup environment. Define each user's scope based on the operations they need to perform and the systems and backups they need to access. If a particular user or group might benefit from self-service over a subset of your environment, configure user roles to meet those requirements without opening up unfiltered access to the full backup environment. To enhance security, RBAC can be applied at the appliance level, protected asset level and task level for each user.

Mitigation

Should you fall victim to a ransomware attack, focusing on mitigative measures to ensure the attack doesn't spread across the network is vital. It is critical to swiftly respond so you can reduce its impact on your organization. The priority should be identifying all the "patient zeroes" and isolating them from the rest of the network.

Early detection is critical in that regard, and intelligent backup solutions these days leverage leading-edge technologies, like machine learning and predictive analytics, to detect threats in the network early. Predictive analytics and machine learning can help identify anomalies, atypical behavior and conditions typical of ransomware attacks and alert administrators of abnormal fluctuations.

Recovery

The final and most crucial aspect of this three-pronged approach is your ability to make an instant recovery so that you can swiftly roll back your network to a safe restore point and avoid downtime and revenue loss.

Your data backup only has value if you can use it for swift and successful recovery. That's why you need to have the capability to do automated recovery testing regularly in a way that doesn't affect your production workloads. During the disaster recovery (DR) testing, you should be able to restore applications, perform analytics and measure the recovery time objectives (RTO) and recovery point objectives (RPO). That will help you understand whether a recovery could meet your RTO and RPO goals and identify the reasons for any failed recoveries.

Hardware failures: Redundancy and DR

Hardware failures can devastate your business if you do not take regular backups of your business-critical data. You must ensure that your data is backed up regularly and stored at separate off-site locations so that a specific hardware failure doesn't corrupt both your production data and data backup. Cloud-based backup and disaster recovery is an effective way of dealing with this since you can easily spin up your infrastructure in the cloud in case of a hardware malfunction.

A well-thought-out DR plan is equally essential to protect your data. By identifying potential failure points, defining RTOs and conducting regular DR testing, your organization can ensure a swift and effective response to hardware failures, minimizing downtime and data loss.

“The rapid reduction in the ransomware attack timeline is concerning because it adds yet another pressure element for defenders: time. And the bottom line is, if attackers are moving fast, we have to be faster.”

– *John Dwyer, Head of Research at IBM Security X-Force*

Human errors: Employee training, data governance and recovery protocols

Employees are your organization's first line of defense and often its most significant vulnerability. Thorough and ongoing training on data-handling best practices and recognizing potential threats is critical to ensure that their actions do not inadvertently expose your organization to cyberthreats.

Data governance is one way to ensure that your business-critical data doesn't get misused. Create internal data standards and policies that control how data is gathered, stored, processed and disposed of. Effective data governance breaks down data silos in your organization, enhances decision-making with more accurate analytics and empowers you to comply with data privacy laws and other regulations.

Similarly, it is also essential to clearly define data recovery protocols. Clearly define the role of each individual in the DR team, do risk evaluation to determine which disasters are likely to occur, identify assets and data that are most critical for your organization, and create a holistic DR plan that helps you get back up and running swiftly in the aftermath of a disruption.

Natural disasters: Off-site backups, cloud solutions and geo-redundancy

In the face of natural disasters, the name of the game is redundancy. Maintain off-site backups in secure locations to protect data even if your primary site is compromised. Cloud backup is a potent solution on that front. You can back up a single server, workstation or even an entire IT environment in the cloud and rest easy knowing that your data remains accessible anytime, anywhere, no matter the circumstances.

Geo-redundancy is also a key strategy for mitigating the impact of natural disasters. By replicating data in data centers across multiple geographical regions, your organization can continue operations even in the face of large-scale environmental events.

Protecting data no matter where it lives

An organization's data now resides in many places — on-premises and virtual data centers, various clouds, SaaS applications like Microsoft 365 and Google Workspace, and laptops of the on-the-go workforce. It is critical that your data protection strategy considers this multitude of environments and locations and comprehensively protects data wherever it resides.

Cloud-native does not equal resilience

Finally, let's debunk a common misconception. Storing data backup in the cloud is not synonymous with resilience. While cloud solutions offer flexibility and accessibility, **data residing in the cloud is still vulnerable to a wide range of data threats, such as scripting and sync errors, cyberattacks, and human errors like accidental deletions.** When it comes to ransomware, many sync tools can actually further the damage by replicating encrypted files from the local device and syncing them to the cloud. Cloud data is also susceptible to single cloud vulnerabilities, meaning your data in the cloud will not be accessible if there is an outage in the cloud you are leveraging. For instance, it's only very recently that a networking outage¹² took down the entire Microsoft Azure platform along with its services like Teams and Outlook. The key to true data resilience thus lies in a comprehensive strategy that transcends a single cloud environment.

¹²<https://www.reuters.com/technology/microsoft-teams-down-thousands-users-india-downdetector-2023-01-25/>

III. Resilience in action: Effective backup and recovery solutions

In your quest for data resilience, understanding the challenges and tailoring strategies is pivotal, but the execution is where the rubber meets the road. This section takes a closer look at implementing effective backup and recovery solutions, shedding light on the critical decisions that can make or break your data protection strategy.

On-site vs. off-site (cloud) backups

When it comes to data protection, one of the key decisions to make is where to store your backups. There are two primary options to choose from: on-site and cloud backups. Each approach has its own unique advantages and considerations. It is crucial to evaluate the organizational needs carefully before selecting one over the other.

On-site backups: This conventional approach involves setting up your own data centers, where you store data backups in the servers you control. In this case, you are in charge of access and privacy to the data center and can manage the server hardware accordingly. On-site backups provide quick access to data and can be cost-effective for small-scale operations.

However, this approach's downside is that your hardware's capacity limits you. You will have to upgrade your servers whenever you need to increase the backup storage and the workload it can handle. They are also vulnerable to on-site disasters like natural disasters and theft.

Cloud backups: Cloud backup backs up your data and sends it to a remote server over a proprietary or public network. Cloud-based backup has been soaring in popularity recently thanks to its unprecedented flexibility, scalability and cost-efficiency. Unlike the on-site backup options, cloud backup does not come with hefty data center footprint and maintenance costs. These services are available over the WAN and can often be accessed from anywhere remotely. However, if not appropriately managed, cloud backups can face security and latency issues.

Wondering which backup method best suits your organization? With the increasing popularity of the new hybrid work model and the advent of remote and cloud workloads, cloud backup has become an indispensable part of modern organizations' backup and recovery strategies. The flexibility, cost-effectiveness and ease of use make cloud backup an ideal choice for organizations, especially when the data footprint is expanding rapidly.

However, as they say, don't put all your eggs (i.e., backups) in one basket. What if your internet connectivity fails while accessing your online backup? Since the cloud relies on internet connectivity, it can drastically affect your RTO. So, leverage a combination of on-site and off-site backups to get unparalleled accessibility and seamless continuity.



Automating backup processes

Your data gets generated around the clock, and cumbersome and error-prone manual backups are not the way to go. Automating your backup processes will streamline data protection, ensuring critical data is consistently backed up at specified intervals. The risk of human error is significantly reduced with automated backups. Look for solutions that offer a policy-based approach to backup and replication to automate scheduling against your desired RPO(s). This approach not only enhances data resilience but also frees up your valuable resources for other critical tasks.

Testing and validating recovery plans

Imagine finding out during a disaster that your recovery plan doesn't work. The efficacy of your data recovery plan is only as good as its testing. Many things can go wrong during a recovery — network configurations might not get replicated properly, application dependencies might not be in sync across sites or DR resources might become insufficient over time. The worst time to identify such an issue is during an actual emergency. Regular testing and validation of recovery plans are thus imperative to ensure your organization can recover swiftly and effectively when disaster strikes.

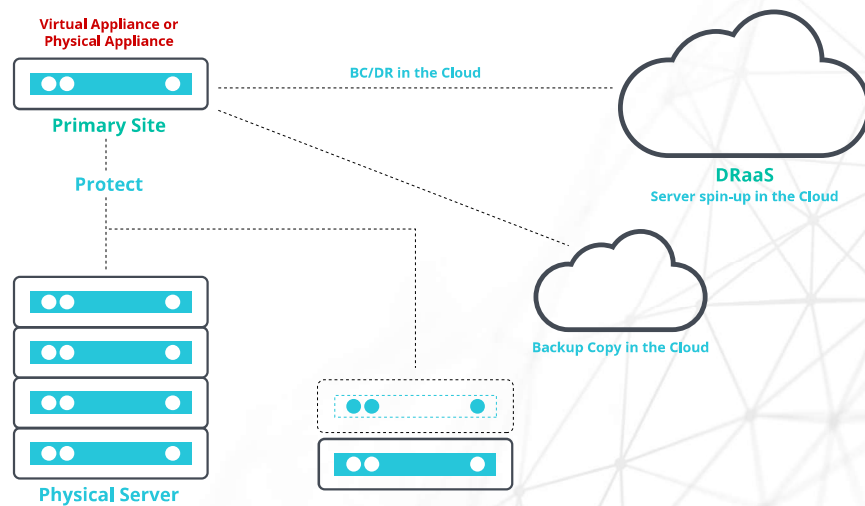
Today, organizations can perform the highest level of application recovery testing with no IT time or effort and without affecting production workloads. In a test environment, you can fully restore applications, perform analytics, measure RTO and RPO, and identify reasons for failed recoveries. This allows you to fine-tune your DR plan, bolstering your organization's readiness for any data protection challenge.



What is DRaaS, and why it could be the best option for you?

Disaster Recovery-as-a-Service (DRaaS) empowers businesses to offload the maintenance and management of DR functions to a third-party provider. TechTarget¹³ defines DRaaS as “a cloud computing service model offered by third-party vendors that provides failover in the event of a natural catastrophe, power outage or other type of business disruption.” DRaaS allows an organization to back up its data (along with IT infrastructure configurations and DR runbook) in a third-party cloud computing environment. When a disaster strikes, the cloud service provider will provide the business with the DR orchestration necessary to regain access and functionality to the IT infrastructure.

If your organization doesn't have the budget or resources to research, implement and test DR plans, then DRaaS is the best option for you. As DRaaS mirrors your complete IT infrastructure on virtual servers in fail-safe mode, you can rest assured that your recovery will be much faster or near instantaneous. Since the third-party facility provides the infrastructure, maintenance and management, you can also reduce CapEx costs and free up your workforce for more strategic initiatives.



¹³ [https://www.techtarget.com/searchdisasterrecovery/definition/disaster-recovery-as-a-service-DRaaS#:~:text=Disaster%20recovery%20as%20a%20service%20\(DRaaS\)%20is%20the%20Replication%20and,another%20type%20of%20business%20disruption.](https://www.techtarget.com/searchdisasterrecovery/definition/disaster-recovery-as-a-service-DRaaS#:~:text=Disaster%20recovery%20as%20a%20service%20(DRaaS)%20is%20the%20Replication%20and,another%20type%20of%20business%20disruption.)

IV. Fine-tuning resilience: The art of testing and recovery assurance

In the realm of data protection, preparing for the worst is imperative. Regular testing and recovery assurance are the cornerstones of data resilience that ensure your organization can weather any storm.

How to perform regular testing

As we discussed earlier, many things can go wrong during a DR process, and regular DR testing is necessary to ensure that businesses can recover swiftly in the event of a disruption. If testing is that important, why don't organizations test their DR plans more often? The reason is simple. DR testing is costly, difficult to carry out and risks interrupting the production workloads.

However, these old excuses for not testing are no longer valid today.



Fortunately, there are cost-effective, intelligent technologies available today that can automate, orchestrate and analyze application recoverability to ensure entire workloads are functional and, if not, report what is broken — all without affecting the production environment. You can execute security tests and automate reports and alerts so your DR plan stays fail-proof.

Creating a robust testing framework

A well-defined testing framework ensures clarity, control, accountability and reliability during data recovery. It is important to acknowledge that not all data is equally important to an organization, and the resources available for backup and recovery procedures are finite. Therefore, mission-critical data and applications should be backed up more frequently and with an approach that enables quick recovery. On the other hand, less critical data may be backed up at less frequent intervals. Based on these factors, it is necessary to define the two critical recovery objectives — RPO and RTO.

In an outage, RTO is the timeframe within which applications and systems must be restored. On the other hand, RPO is the acceptable amount of data loss that a business can withstand and still function effectively. These metrics provide a realistic backdrop against which you can plan and execute DR testing. Measuring RPOs and RTOs during testing allows you to determine whether your data recovery plan aligns with your goals.

Periodic review and adjustment

Running automated DR tests will reveal how an outage would impact your business continuity. If the DR tests show that you can't meet your RTO and RPO goals and SLAs, make adjustments in your backup process and rerun the tests to track the changes. Regularly scheduled reviews of your recovery plan can uncover vulnerabilities and identify opportunities for improvement.

V. Future-proofing resilience: Staying ahead of the curve

Yesterday's solutions may no longer suffice for tomorrow's challenges in this ever-evolving data threat landscape. Your organization must adopt a forward-looking strategy to maintain data resilience in the face of emerging risks.

How can you secure your investment in today's ever-evolving dynamic data protection landscape?

That's another important question you need to ask yourself. Let's say you are migrating your on-premises workloads to the cloud; your investment in backup appliances will sink. That's why it's critical to future-proof your investment. Look for vendors that offer protection for the whole range of environments and offer flexibility to transition from one solution to another. That way, you can flexibly adapt to your evolving data protection requirements without the fear of sunk costs or your contract being locked into an underlying infrastructure or platform.

The ever-evolving threat landscape

Today, cybercriminals leverage cutting-edge technologies and innovative tactics to launch increasingly sophisticated attacks. The recent proliferation of ransomware attacks presents a stark example of this burgeoning threat landscape. The open-source versions and as-a-Service delivery model are democratizing this malevolent trade, significantly lowering the barrier to entry for carrying out ransomware attacks.

In 2022 alone, organizations worldwide detected 493.33 million ransomware attempts, according to [Statista](#).

Similarly, phishing campaigns leverage advanced social engineering tactics that make it challenging to discern malicious emails from legitimate ones. Threat actors exploit human psychology, using personalized messages and seemingly trustworthy sources to lure victims. The result, again, is an increased risk of data breaches. The future of data resilience lies in anticipating, adapting to and neutralizing these sophisticated threats, ensuring the safety of your organization's data.

Harnessing AI and predictive analytics

AI and predictive analytics are powerful technologies that could help you bolster your defenses against cyberattacks. For instance, AI's ability to analyze vast amounts of data in real-time enables the swift identification of anomalous patterns and behaviors. It can detect irregularities that may indicate a potential attack. AI can also autonomously initiate response measures, such as isolating affected systems or mitigating the impact.

The speed and precision of AI in threat detection and response is a game-changer, reducing the window of vulnerability and safeguarding organizations from data breaches.

Similarly, by analyzing historical data, predictive analytics identifies trends and patterns that may signify a potential attack. This allows organizations to proactively strengthen their defenses before a threat materializes. By incorporating AI and predictive analytics into their data protection strategies, businesses not only bolster their resilience but also enhance their ability to anticipate, adapt and respond to the ever-evolving threat landscape.

Prepare for emerging challenges

The cybersecurity landscape is in a perpetual state of flux, presenting organizations with a slew of emerging challenges. New data protection challenges are already on the horizon, from the increasing use of the Internet of Things (IoT) devices to the complexities of managing data in decentralized and hybrid cloud environments. Preparing for these emerging challenges means staying abreast of technological advancements, regulatory changes and the shifting threat landscape. It also entails embracing new technologies and solutions to enhance data resilience.

VI. Your resilience blueprint: Key takeaways and insights

As we conclude our journey through the world of data resilience, let's extract the core insights from this whitepaper. These key takeaways will help you guide your organization toward a data-resilient future, where your business-critical data stays impervious to any kind of threats.



Acknowledge the ever-evolving threat landscape

In this digital world, change is the only constant. Stay informed about evolving data threats to remain proactive in your defense.



Leverage a comprehensive data protection strategy

Your data now lives in more places than ever before and is constantly under attack. You must implement a data protection strategy that comprehensively secures your data, no matter where it resides.



Strengthen your backup and recovery plan

Ensure that your organization has a robust backup and recovery plan in place. Utilize a combination of on-site and cloud backups, implement automation for efficient data protection, rigorously test recovery plans and consider the advantages of DRaaS to ensure swift data restoration.



The crucial role of rigorous DR testing

Regular testing and validation of recovery plans are vital. Regularly verify that your DR process meets your RPO and RTO goals and SLAs.



Future-proof your resilience strategy

Embrace leading-edge technologies, such as AI and predictive analytics, to identify and mitigate evolving threats. Be prepared for the challenges of tomorrow, including the complexities of decentralized cloud environments and evolving data protection requirements.

The path to data resilience may be winding, but it's a road to total security and lasting success. By following these guidelines and remaining vigilant, proactive and adaptive, your organization can confidently navigate the complex landscape of data protection challenges.

Unlock Data Resilience With Unitrends Unified Backup

Now that you know how to achieve data resilience, take a look at Unitrends Unified Backup. The solution comprehensively protects your data wherever it resides, whether on-premises, cloud, SaaS applications or employee endpoints. It empowers you to seamlessly manage all your data backups from one place. Moreover, it leverages leading-edge technologies like AI and predictive analytics to help you confidently protect your data from today's advanced cyberthreats — all while significantly cutting down your management time and expenditure on backup and recovery.

CONTACT ME TODAY FOR A DEMO!

Christina Baer | Vendor Manager | ChristinaB@climbcs.com
732-276-2697

"Unitrends isn't just reactive — it's downright prophetic. With its predictive analytics, it can foresee potential data catastrophes and prevent them before they even happen. It's like having a crystal ball that whispers tech secrets to you!"

– [Jonathan A.](#)



"Easy to use. Their support was top of the line when in a pickle. There were one or two times that I ran into big issues, and after calling their support, they helped me get those servers back to working condition. Support for me has become huge since our IT department is small, and we have to deal with IT issues all over the place."

– [Cesar T.](#),
Network Administrator



"We had an incident last year with Ransomware. Unitrends was instrumental in getting our services back online."

– [Jason D.](#)



"Unitrends backup and recovery is the best total backup solution I have worked with in over 20 years of IT management. The ability to use the recovery system to restore a file or a server is simple, effective and easy to use. Great support staff, among the best I have had the pleasure of working with."

– [Bill C.](#),
IT Manager



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

