Acronis

10 Noble Truths of Modern Backup and Recovery

Business demands evolve – traditional data protection must too

TIMES HAVE CHANGED. IS YOUR BUSINESS KEEPING UP?

Today business is done around the globe and around the clock. To acquire customers, do business, and plan your company's growth, you rely on a wide variety of tools and strategies that generate more complexity, security, and cost concerns than any earlier generation. All of these changes arose because of one thing: an increased reliance on data.

Data is the lifeblood of modern business. It's one of your organization's most valuable assets and requires diligent safekeeping. When data safety, accessibility, privacy, authenticity, and security (SAPAS – or the Five Vectors of Cyber Protection[1]) are at risk, businesses face countless uncertainties. These include everything from how customers and regulatory commissions will respond to the lost data, to how long it will take to get back up and running, how much that process will cost, and how your business will survive the data loss – if it does at all.

Backup and recovery services keep your data protected and available anytime, anywhere so that your business can keep running. Easy, efficient, and secure backup and recovery services do this by beginning with a clear understanding of the 10 noble truths of modern backup and recovery:

- The world is digital
- Computing on the edge
- Threats evolve – endpoints don't
- The best defense is an AI offense
- Tools are easy to use or unused
- Only authentic data is valuable
- Disaster recovery is key to backup
- Partial protection isn't protection
- Security runs from end to end
- Time is of the essence

1. The world is digital

By 2025, there will be 175 zettabytes[2] of data in the world. On our way to that point, the amount of data we create, store, and rely on is going to double every two years[3]. This makes sense given that data now lives in more places than ever before: on-premises servers, off-site storage, personal devices, cloud services, the internet of things (IoT), and more.

You need only look at your own organization to see such change in action: smartphones and tablets[4] are now a central part of the IT landscape for companies and the cloud is on pace to replace traditional data centers[5]. With more data to manage, more sources generating it, and more devices storing it, having a backup and recovery service that protects all your data, applications, and systems is essential.

HOW MODERN BACKUP AND RECOVERY HELPS

Modern backup and recovery services help your business overcome the challenges that come with your expanding IT network while keeping your data comprehensively protected, yet available and accessible. With a quality backup service in place, you're equipped with reliable copies of all the data that keeps your business running. That means uninterrupted business continuity no matter how large your data volume grows, how varied your IT infrastructure becomes, or what the future holds for technological advances.

2. Computing on the edge

As business demands increase, so does the speed your employees and your customers expect. While cloud computing accounted for this need just a few years ago, today the IT industry needs even faster computing.

In response, edge computing is exploding in usage. Gartner estimates that by 2025, 75% of enterprise-generated data[6] will be created and processed outside of central data centers or the cloud – up 65% from today. This shift comes with many benefits including lower latency, better response times, increased availability and connectivity, and more.

Like all technological advancements, however, there are also new challenges: deploying and managing an edge computing environment can be costly, scaling it can be complicated, and securing it from cyberthreats needs to be a top priority – a larger tech footprint provides a larger target for cyberattacks.

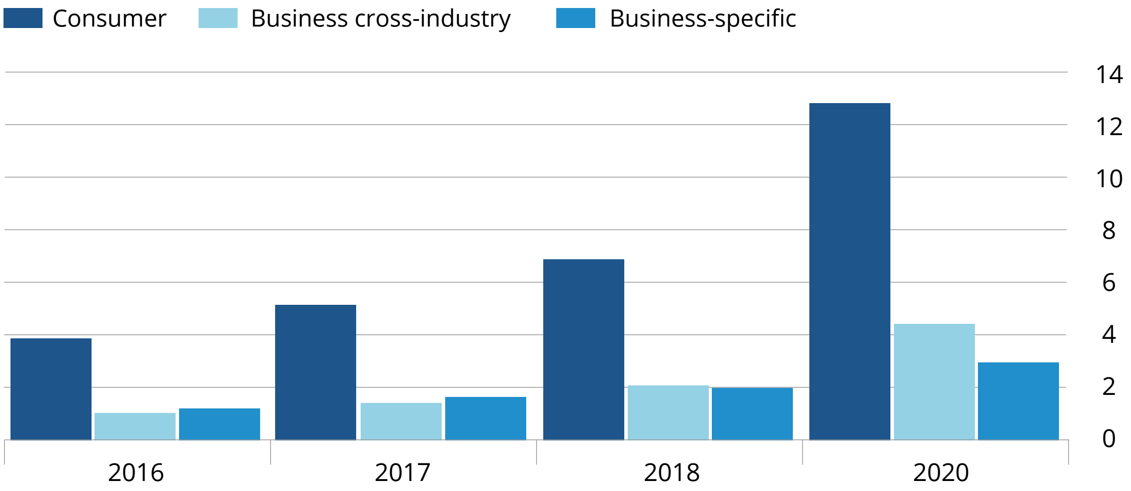
HOW MODERN BACKUP AND RECOVERY HELPS

A diverse IT network comprised of edge devices is subject to an exponentially larger variety of threats – from getting hacked to getting lost. Backups help to ensure that if these issues arise within your organization, your data is safe: A new version of the data, applications, and systems lost can be recovered quickly and completely.

Of course that requires all your endpoint users to consistently perform backups, which any IT professional knows is unlikely. That's why automatic backups are an essential addition to any company migrating their way to the edge. Automatic endpoint data backup solutions allow you to protect your organization's data silently and continuously in the background.

Forecast growth of the internet of things

Number of applications in use by category (bn)



3. Threats evolve - endpoints don't

Unsurprisingly, the growth of data volume on the edge has attracted the attention of cybercriminals. In 2018, the Ponemon Institute revealed that 64% of businesses[7] had experienced one or more "successful" endpoint attacks that compromised their data assets and/or IT infrastructure.

For large organizations, each of these attacks ultimately costs $7.1 million — after productivity loss, asset theft, system downtime, IT infrastructure damages, brand damages, and legal and regulatory fees are added up. What's worse, many businesses rely on anti-virus software to defend against these threats, which are significantly less effective with new and unknown cyberattacks.

Today these zero-day attacks are becoming more prevalent – making up 37% of all endpoint attacks – and proving to be a major challenge for any traditional anti-virus to overcome.

HOW MODERN BACKUP AND RECOVERY HELPS

The best backup and recovery services ensure that all of your data, regardless of whether it's in a data center, the cloud, or on an endpoint device, is protected. What's more, leading backup services now respond to endpoint-targeting and zero-day attacks. They do so through integrated cybersecurity capabilities, like centralized security controls for multiple endpoints and anti-malware defenses that protect every level of your IT infrastructure from known and unknown cyberthreats.

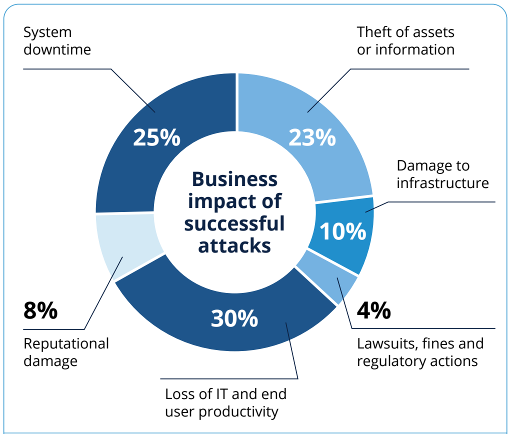
Data Volume on Edge is Growing

Endpoints are not as secure as your datacenter

- **63%** say the frequency of endpoint attacks has increased in 2018
- The average time to patch is **102 days**
- Antiviruses miss **57%** of attacks
- Data is growing **33 times** faster than IT staff
- **50%** of hard drives die within five years
- **60%** of enterprises have been hit by ransomware
- **64%** has experienced successful endpoint attacks in 2018 vs 54% in 2017

Endpoints

- Remote Offices
- Cloud Servers
- Hosted Servers
- Desktops
- Phones
- Tablets



Each successful attack costs $7.1 million for a large organization or an average of $301 per employee or $440 per endpoint

Source: "Trends in SaaS Data Protection", Spanning, 2016; "Understanding the Depth of the Global Ransomware Problem", Osterman Research, 2016; "Hosting and Cloud Study 2017", 451 Research, 2017, The 2018 State of Endpoint Security Risk, Emerson Network Power-sponsored study by the Ponemon Institute (2016), PWC 2016 US CEO Survey

4. The best defense is an AI offense

Traditional backup tools and anti-virus solutions are no longer enough to protect your business. The frequency, scale, and sophistication of cyberattacks you face is evolving just as rapidly as your data reliance.

Last year, the Center of Strategic and International Studies reported that cybercrime around the world accounted for $600 billion[8], nearly 1% of global GDP. Ransomware, one of the most prevalent and most damaging types of malware is expected to cost $20 billion by 2021, with a business falling victim to an attack every 11 seconds[9]. These attacks have advanced enough to target and eliminate backup files before demanding payment.

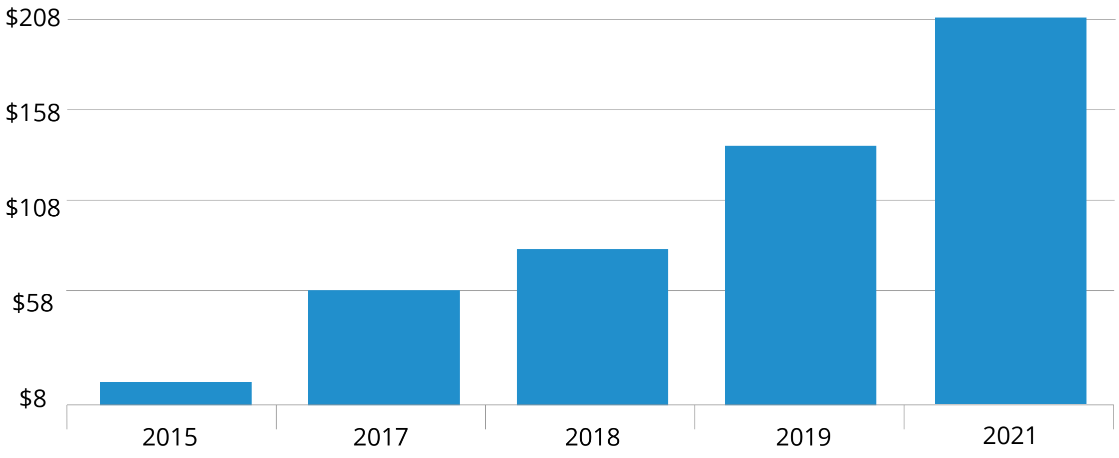
Of course, ransomware is just one form of the malware that threatens your business. Cryptomining malware is another noteworthy emerging cyberthreat that grew by more than 4,000%[10] in 2018.

HOW MODERN BACKUP AND RECOVERY HELPS

Modern backup and recovery services are responding to these evolving threats by rethinking how cybersecurity is done. The most innovative solutions replace the traditional signature-based threat identification model with an active, AI-based approach.

This new technology constantly runs in the background to eliminate security gaps and uses sophisticated system monitoring to quickly detect erratic behavior and stop unexpected, unapproved activities. To thoroughly secure your business from a constantly-evolving cyberthreat landscape, this innovative technology is the modern best practice that all backup services should strive toward.

Global Ransomware Damage Costs



Source: Cybersecurity Ventures

5. Tools are easy to use or unused

The rise of complexity in modern IT has led directly to highly complex software solutions. Unfortunately, this growth in complexity runs parallel with a decline in cybersecurity skills. This year, 53% of organizations[11] reported a problematic shortage of cybersecurity skills – a growth of 10% in just three years.

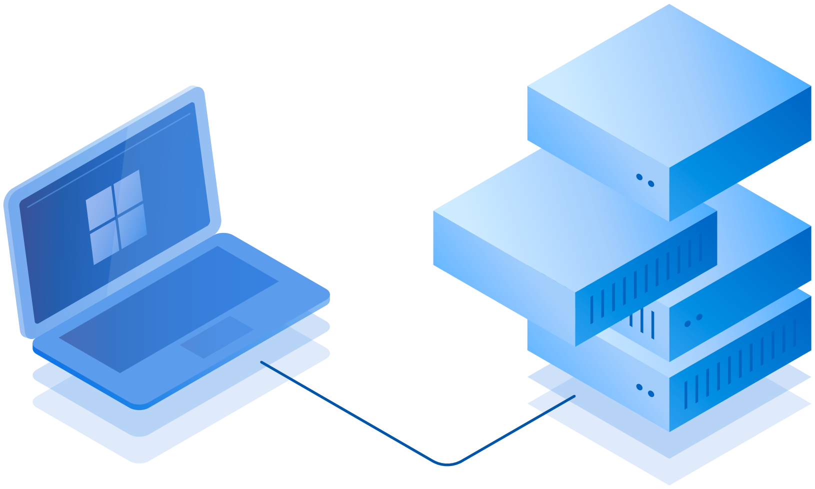
This means many businesses need to decide between investing in solutions that require special expertise, or spending valuable time and money on IT training. In both cases, overly complex solutions lead to high operational expenses, reduced business productivity, and the risk of inadequate or improper use.

HOW MODERN BACKUP AND RECOVERY HELPS

The best backup and recovery services deliver protection that balances complete security, cost-efficiency, and ease of use. This helps to ensure that even IT generalists can perform successful backup and recovery processes – reducing the time your organization needs to spend learning and executing important steps and helping to increase overall productivity.

Also facilitating greater ease-of-use, some services now centralize all backup and recovery management resources into a single console. This approach establishes a centralized work "hub" instead of disparate dashboards.

When comparing backup and recovery solutions, use demo and trial periods to review how intuitive each tool is. This information is important to your final decision.



6. Only authentic data is valuable

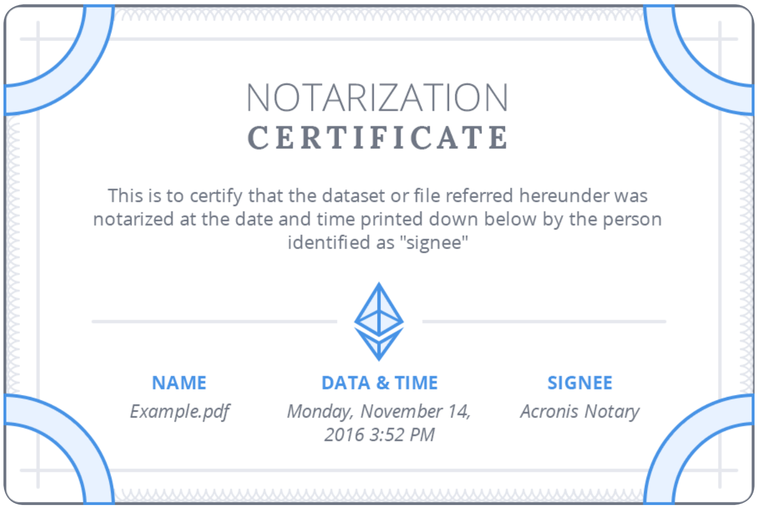
The Big Data industry will be worth $77 billion by 2023[12]. With data volumes that large, data authenticity has become a top priority for businesses. Between exponentially growing unstructured data and unprecedented levels of cyberthreats aimed at compromising your data, inauthenticity has become more of a threat overtime.

Given how valuable your data is to your business' success, this inauthentic data is just as serious as data loss. When business data is unexpectedly modified, regardless of whether it was done accidentally or maliciously, it throws the authenticity of all of your organization's data into question. This can bring your business to a halt, particularly if you host customer data.

HOW MODERN BACKUP AND RECOVERY HELPS

Today, backup and recovery services ensure data authenticity through careful tracking of files throughout the lengthy chain of data transaction events – from creation, to revision, to storage, to access by users around the globe. This helps ensure that the data recovered through modern backup and recovery services is certifiably authentic and of value once it's restored.

The most innovative backup and recovery services on the market today are using blockchain technology to accomplish this[13]: applying a unique cryptographic hash to each backed up file. These hashes are recorded, time-stamped, and independently verifiable, meaning that any file alteration can be identified and an unaltered, earlier version can be used instead.



NOTARIZATION
CERTIFICATE

This is to certify that the dataset or file referred hereunder was notarized at the date and time printed down below by the person identified as "signee"

NAME	DATA & TIME	SIGNEE
Example.pdf	*Monday, November 14, 2016 3:52 PM*	*Acronis Notary*

7. Disaster recovery is key to backup

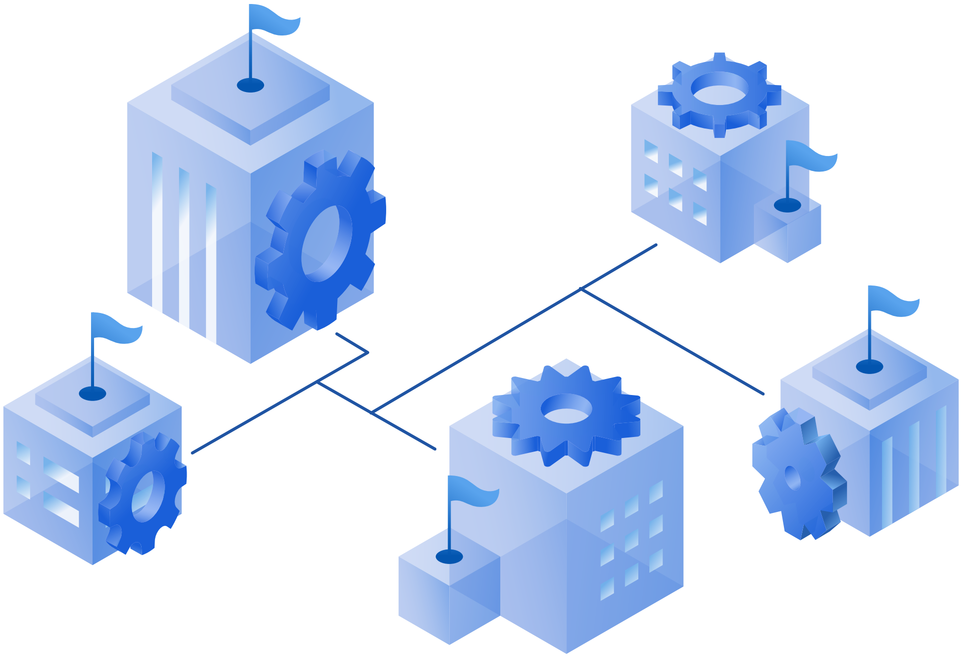
Despite 29% of businesses having suffered data loss events[14], 68% of businesses don't have a written disaster recovery plan to enable rapid recovery from natural and human-caused disasters[15]. This opens organizations to significant downtime – and expenses – as they recover from disasters with whatever portion of their backups that survived.

Given that a single hour of downtime can now cost a business well over $300,000[16], this is a costly mistake for a modern business to make. Put simply, in today's always-on digital world, businesses can't afford downtime. And while you can't plan for all disasters, you can plan for how you'll recover from them should they happen.

HOW MODERN BACKUP AND RECOVERY HELPS

Fortunately, modern backup and recovery services are now making it easier than ever to develop these plans by integrating disaster recovery directly into the backup and recovery process. In fact, IDC predicts that by 2025, backup, high availability, and disaster recovery capabilities will all blend into a continuum of application availability[17].

Such a process is already underway with modern backup services featuring disaster recovery add-ons and capabilities that offer business critical data recovery to virtual machines in minutes[18]. This approach enables you to keep your business moving following a disaster scenario, even while a full system recovery is in-progress.



8. Partial protection isn't protection

Increased data reliance has led to increased infrastructure sophistication[19]. Today, as your business scales up, a variety of new data sources need to be integrated – ranging from virtual and physical to cloud and mobile platforms. This growth in complexity enables a number of benefits: expanded productivity, more robust data management, and expanded data accessibility.

Of course, such growth also causes many unique challenges. In fact, 58% of businesses cite security for their workloads as their biggest issue[20]. With more devices, more locations, and more interconnection, you can no longer automatically count on backup and recovery services to deliver the universal protection you need today or the scalability you'll need tomorrow.

HOW MODERN BACKUP AND RECOVERY HELPS

Modern backup and recovery services are built with scalability and flexibility in mind, extending to a wide variety of workloads, hypervisors, and cloud applications to help ensure complete backups and remove data security gaps. Today, the leading backup and recovery services offer this unified approach to backup with complete protection for more than 20 different platforms[21], defending your business data wherever it rests with a single pane of glass solution.

Such modern backup and recovery services reduce storage and service costs, process complexity, and stress for your entire IT team. All it takes is one solution with unified backup and recovery processes, regardless of data volumes, platforms, or location.

9. Security runs from end to end

As of 2018, 96% of organizations use cloud computing for some portion of the IT infrastructure[22]. With so much business taking place in the cloud, complete security can be difficult to achieve and maintain. In fact, only 9.4% of cloud providers encrypt data once it's stored and at rest[23].

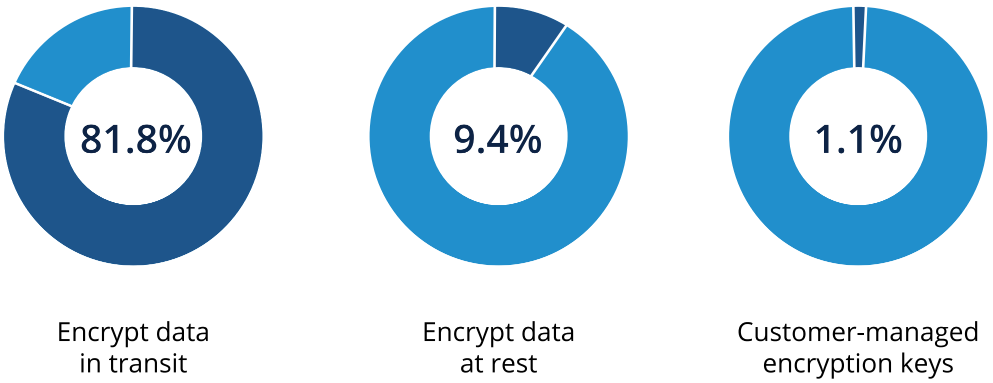
This failing leaves a major gap in your data protection for both original and backup files stored in the cloud. It can also lead to data loss or data corruption that makes rapid, reliable backup restoration difficult. For backup and recovery services to be as valuable as possible, they need to offer encryption that protects both on-premises and cloud-based data while it's in transit and at rest.

HOW MODERN BACKUP AND RECOVERY HELPS

Leading backup and recovery services understand this need – they deliver top-quality data encryption from end to end. The very best backup vendors, particularly those that offer cloud platforms and cloud storage, will feature military-grade encryption for files such as AES-256.

For added security, modern backup and recovery services will place the key to decrypt these files exclusively with the user, eliminating any possibility of interference from outside actors. As computing moves further away from data centers and further toward the cloud and edge devices, this level of security becomes more and more essential.

Encryption controls vary widely among cloud providers



Source: Skyhigh Networks

10. Time is of the essence

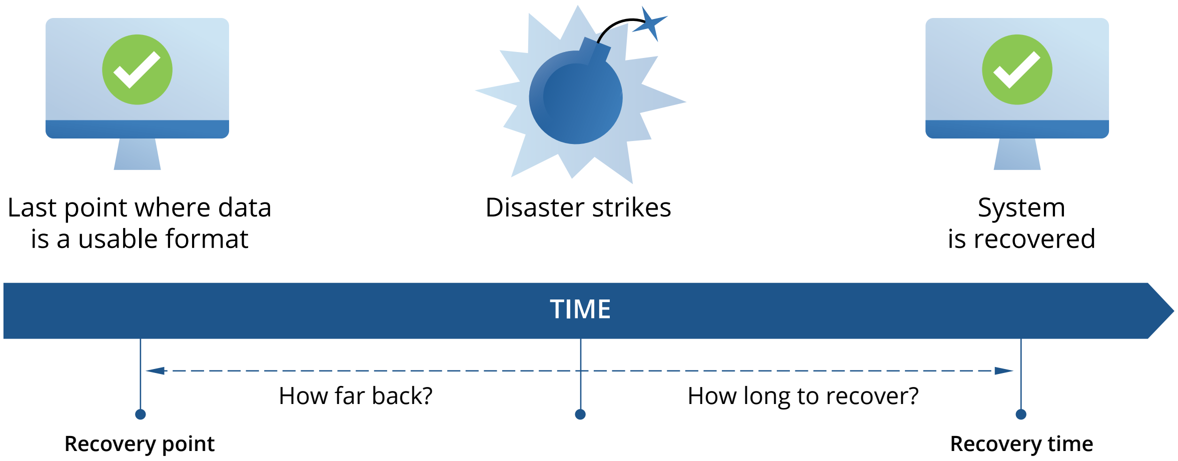
Between your expanding IT infrastructure, the sophisticated cyberthreat landscape, and the ever-present risk of human error, data loss is increasingly a matter of when, not if. When business-critical data loss strikes your business, your backup and recovery plan will be your first line of defense, helping you get back up and running as quickly and easily as possible.

In an ideal world, your backup services will provide short recovery time objectives (RTOs) and recent recovery point objectives (RPOs). Unfortunately, with the speed of business constantly accelerating, businesses are having a harder time finding backup and recovery services that can reliably meet these needs.

HOW MODERN BACKUP AND RECOVERY HELPS

Modern backup and recovery services streamline backup and recovery processes to keep RTOs low and backup points frequent to keep RPOs close. These services achieve this by allowing businesses to customize their own backup schedule frequency, establishing RPOs for data that ensure your business doesn't lose data following a data loss recovery.

Through rapid backups and custom backup scheduling, these services are able to deliver complete recovery in a matter of hours. Moreover, leading backup and recovery services utilize virtual machines as a potential recovery destination.[24] This method reduces essential file recovery times to a matter of minutes and ensures that your business can bounce back from data loss events with close to zero downtime.



Source: Enterprise Storage Forum

Final Thoughts

In the modern digital world, backup and recovery services are an essential part of any business IT environment. Despite all the changes that have brought IT services to where they are today – and all those that are sure to come – ensuring data safety, accessibility, privacy, authenticity, and security will always be a top priority for your business. Modern backup and recovery services provide you with the protection and support you need to stay productive and grow. Learn more and protect your business data with the industry's top backup and recovery service.

Sources

1. https://www.acronis.com/en-us/cyber-protection/
2. https://www.seagate.com/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf
3. https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm
4. https://www.acronis.com/en-us/resource-center/resource/116/
5. https://www.zdnet.com/article/cloud-computing-will-virtually-replace-traditional-data-centers-within-three-years/
6. https://www.gartner.com/smarterwithgartner/what-edge-computing-means-for-infrastructure-and-operations-leaders/
7. https://cdn2.hubspot.net/hubfs/468115/whitepapers/state-of-endpoint-security-2018.pdf
8. https://www.csis.org/analysis/economic-impact-cybercrime?wpisrc=nl_cybersecurity202&wpmm=1
9. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/
10. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2018.pdf
11. https://www.csoonline.com/article/3331983/the-cybersecurity-skills-shortage-is-getting-worse.html
12. https://www.entrepreneur.com/article/325923
13. https://www.acronis.com/en-us/blockchain-data-authentication/
14. https://www.acronis.com/en-us/blog/posts/world-backup-day-2019-survey-results
15. https://biztechmagazine.com/article/2019/01/disaster-recovery-does-your-small-business-have-plan
16. https://blogs.gartner.com/andrew-lerner/2014/07/16/the-cost-of-downtime/
17. https://www.idc.com/getdoc.jsp?containerId=US44058018
18. https://www.acronis.com/en-us/business/backup/disaster-recovery-software/
19. https://hbr.org/2011/08/the-world-really-is-more-compl.html
20. https://www.cloudcomputing-news.net/news/2018/jan/11/cloud-infrastructure-becomes-more-complex-security-struggles-it/
21. https://www.acronis.com/en-us/business/backup/complete-protection/
22. https://www.cio.com/article/3267571/it-governance-critical-as-cloud-adoption-soars-to-96-percent-in-2018.html
23. https://www.skyhighnetworks.com/cloud-security-blog/only-9-4-of-cloud-providers-are-encrypting-data-at-rest/
24. https://www.acronis.com/en-us/business/backup/no-downtime/

For additional information, please visit www.acronis.com

Acronis