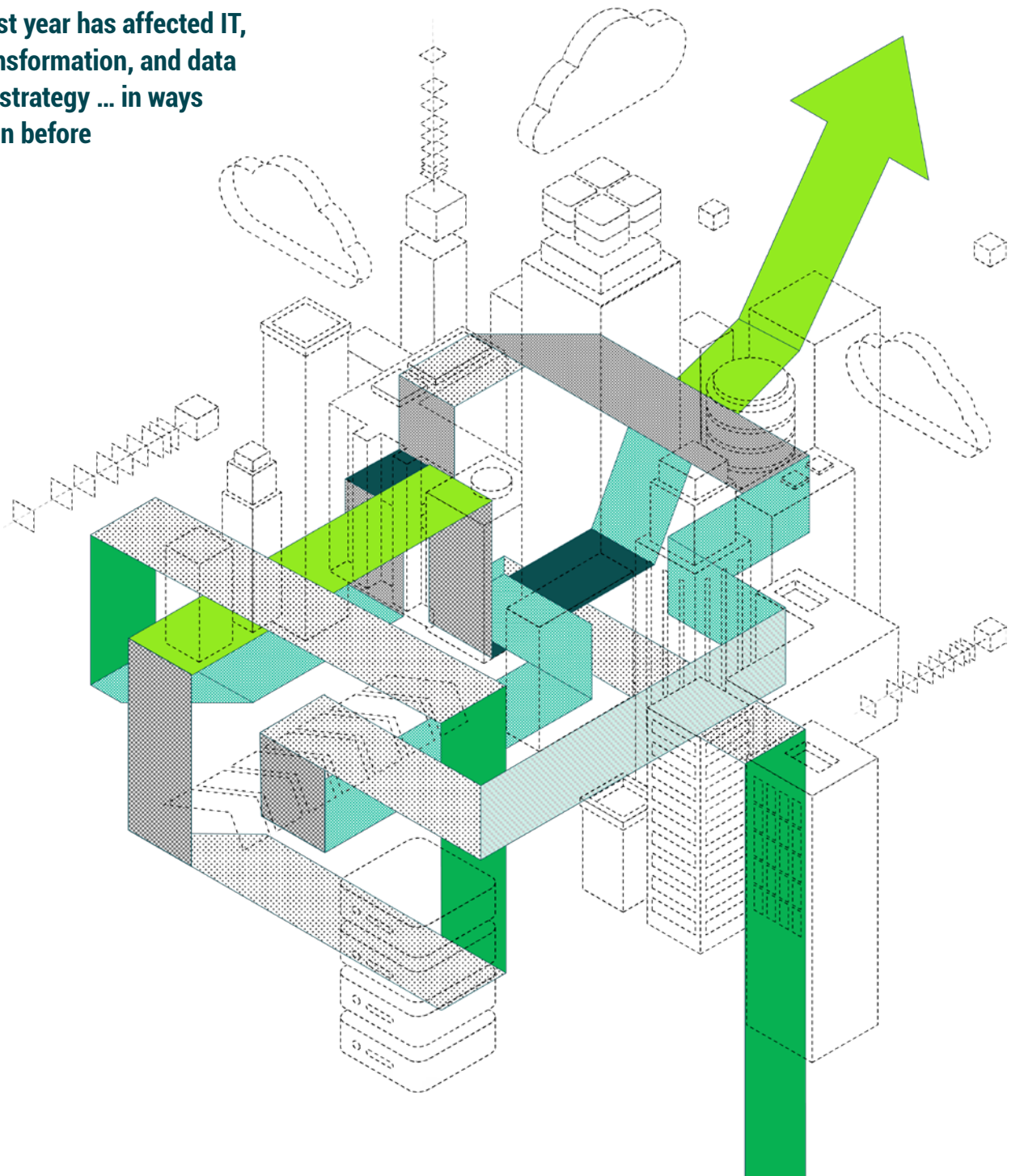


2021 Data Protection Report

How the last year has affected IT,
Digital Transformation, and data
protection strategy ... in ways
NEVER seen before





2020 was a unique year for everyone, and business was no exception. External pressures unknown to our generation have forever changed the IT landscape, creating new challenges for all. Veeam's recent Data Protection Report 2021 looked into a survey of more than **156** unbiased healthcare organizations worldwide to understand how they approached data protection and management today, and future trends. The results provide key insight into how this data can help you with your own IT challenges when tackling modern data protection.

Key findings

Healthcare organizations were among the most "pro-cloud" of any vertical industry represented in the global data. This is likely due to a couple of factors, including the diversion of typical "doing business" budgets from IT to medical service delivery during COVID and the increasingly distributed nature of healthcare providers from individual practitioners, clinics, hospitals, laboratories, and suppliers. Those requirements combined with the highly regulated mandates associated with patient and bio/pharma data drive the aggressive reinvention of core IT systems, which in many cases leads toward cloud-services, where innovation is often more agile.

- As healthcare continues to hyper-accelerate to the cloud, data protection is still paramount (**14%** for healthcare vs. **9%** globally).
- The most important thing is moving to a cloud. They are moving fast towards O365, and Epic and Caché are increasingly moving to deliver healthcare capabilities as a service.
- Adherence to regulations is a crucial area of downtime/data-loss concern for healthcare, with "Revocation of licenses and accreditation" for health care being the 3rd highest concern (**37%** of orgs) compared to 6th place for all other verticals and globally (at **25%**). This makes sense due to HIPAA or JCAHO.
- Healthcare is most interested in achieving DR between their multiple self-managed sites, making sense with so many hospital networks having numerous buildings with IT facilities replicated. HC has little interest in traditional third-party DR hot-site facilities (**8%** for Healthcare vs. **15%** globally), likely to ensure access control of the data.
- Overall, HC is "going cloud and knows that they have to back it up" significantly as it's regulated. It's critical data, and they're already further along than several of the other sectors (**55%** for healthcare vs. **47%** globally).

Challenges for the year ahead

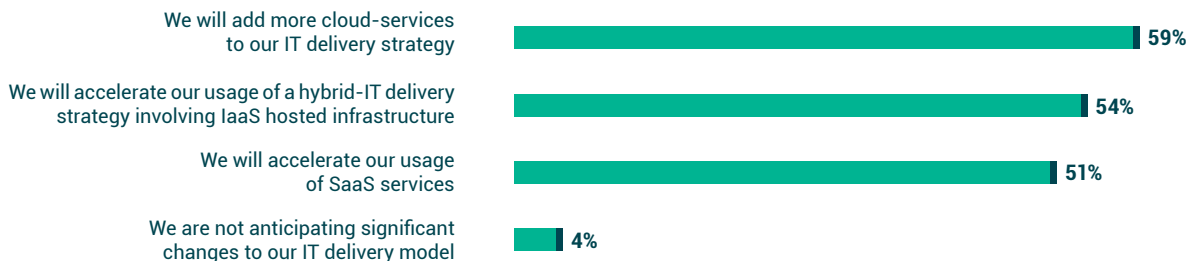
2020 changed the landscape of IT. Economic uncertainty is undoubtedly topping the list of anticipated challenges in 2021 as reported by **39%** of healthcare organizations worldwide, which is up from **11%** globally from the previous year. Including growth in meeting changing customer needs, it confirms much of what we expect. Businesses are laser-focused on driving growth while ensuring they exceed customer expectations. This is putting more pressure on data protection, as in times of business stress, business continuity becomes hyper-important, and that rests on having a strong data protection solution.

The effect of COVID

COVID-19 also had an extraordinary effect on Digital Transformation (DX) efforts. In many cases, you would expect DX plans to slow down due to the reallocation of efforts, and in **28%** of organizations, that is precisely what happened. But there was also a massive increase in DX speed, with **54%** of organizations accelerating their DX initiatives. Organizations with mature DX plans accelerated their investments, however, the companies that have less mature efforts tended to pause to focus on sustainability.

What will 2021 bring to IT strategy? The results show a massive investment change in IT delivery. In fact, only **4%** of organizations surveyed were not anticipating any significant changes in 2021.

In the first months of the pandemic, **92%** of organizations increased their cloud services usage (**35%**) significantly. This came from remote workers using SaaS-based collaboration services and the increased challenge for IT to maintain on-prem, physical operations. This trend will continue through 2021, with most organizations planning to add more cloud services and cloud usage to IT delivery strategy.



The reality gap

The increased focus on modern and cloud-based services has a major impact on data protection trends for IT delivery practices. Inadequate backup or failure to meet SLAs topped the global data protection challenges for 2021 at **40%** (up from **31%** in 2019), beating out all other metrics. As systems are aggressively turning to cloud and modern services, backup failure rates due to legacy systems increase IT's pressure to resolve.

To understand this impact even more, we asked customers a simple question: Does your organization have a gap between how fast you can recover applications versus how quickly you need applications to be recovered. **78%** of all organizations recognized that they have an **"Availability Gap"** between how fast they can recover applications versus how fast they need applications to be recovered. As a follow-up, **79%** of those same organizations said they have a **"Protection Gap"** between how frequently data is backed up versus how much data they can afford to lose.

Those results tell us one simple thing; there is a reality gap in most organizations between business and IT. Today's legacy data protection systems are letting down the company, and something needs to change. When asked about the catalyst for change, **28%** of respondents said to improve RPO/RTO SLAs, **33%** to improve backup reliability, and **31%** to reduce costs.



What is the reason behind the need to improve RPO/RTO SLAs and backup reliability? On average, **25%** of servers had at least one expected outage in the last 12 months (with **41%** of organizations stating up to **50%** of their servers had at least one outage). Any unexpected downtime means potential data loss, and if adequate backup processes are not in place, data loss could be permanent.

But I can still protect my data, even with legacy backup, right?

There continues to be a misperception that even with legacy data protection, the basics are still covered – the backup and recovery of essential data and applications. This could not be further from the truth. With current legacy backup, there remains a lack of core functionality to provide backup and recovery capabilities.

On average, **28%** of the time, organizations showed that their backup jobs ended up with errors or could not complete in their allocated backup window. **That means potentially over one-third of all backups may not be restorable.** The research also showed that **one-third (27%) of all restorations fail to restore** within the expected SLA.

What does this all mean? It means that with current legacy data protection, **only 72% of backups will be successful AND 73% of restores will be successful**, and ultimately, you'll be able to recover **less than half of the time (53%)**.





Modern data protection to the rescue

The need for modern data protection now feels more pressing than ever. With the acceleration of cloud and modern delivery practices and the reality of backup and restoration issues with legacy backup, modern data protection is now necessary. But what is it, according to the organizations needing it?

According to the **156** participants who took part in the research, integrated data protection and security (**33%**), cloud workload migration (**35%**), and the ability to automate recovery (**34%**) top the list.



Clearly, modern data protection needs to support the vast diversity of organizations' IT platforms (cloud, SaaS, virtual, physical), make data safe, accessible, and usable for purposes such as DevOps and analytics, and ultimately enable consistent and unified data protection.

The future of backup and DR is cloudy

Cloud is having a significant impact on modern backup. As organizations modernize their IT services, we also see steady growth in cloud-based data protection. The results also show growth of BaaS (Backup-protection-as-a-Service) with an **17%** estimated increase through 2021. In comparison, self-managed backup using cloud services will see growth stagnation, with an average of **1%** increase per year globally. The noteworthy result here is the decline of on-prem tool usage, expected to be down **16%** from current actuals within two years.

Typically, DR follows backup modernization trends, being tightly tied to the platforms, which remains the case here. With the growth of cloud-based modern data protection, the results also show a swing of **16%** through 2023 to DRaaS first approaches.





The pressure is mounting

The facts are clear; legacy data protection costs you time and money while putting your data at risk. It's holding you back from unleashing your data's full potential and ensuring its **100%** protection and recovery. Modern data protection can provide new levels of confidence and operational excellence, ensuring your data is always protected and available, as well as many other economic and productivity benefits. Recently, Veeam sponsored IDC Research to develop a white paper targeting economic outcomes ([IDC Research, The Economic Impact of Veeam Cloud Data Management Platform, April 2020](#)). Some of those results, as with other research findings, are included below to showcase measurable benefits.

Digital resiliency

Data protection costs and efforts increase as legacy systems continue to struggle to support modern services and innovation. Customers today don't have confidence that their data across all their platforms are fully protected and recoverable.

Enterprises that deploy modern data protection solutions are experiencing **50%** lower five-year cost of data backup and recovery, and **55%** more efficient data backup and recovery teams¹. They also see operational improvements through **55%** more RPO and **58%** more RTO objectives met¹ – all while ensuring their data is fully portable across clouds.

Data accessibility and management

Intelligent data management increases availability through automated and instant recovery, keeping data platforms healthy without manual intervention, and reducing compliance risks. Managing data without process reduces efficiency and can increase the time of recovery. Systems need automated processes to simplify management and recovery while reducing risk.

Data accessibility is a result of well-managed systems and defined data practice processes. Well-managed data provides nearly perfect availability and uninterrupted accessibility, driving data trust and integrity. Enterprises that have adopted a strong data management platform experience **30%** more efficient IT infrastructure teams, **72%** faster time to respond to problems, and **33%** fewer instances of data loss¹.

More than just backup – driving innovation

Innovation accelerates when data is readily accessible. Legacy backup traps data, not allowing it to be reused. Modern data management can help unleash this data, driving business goals faster. Backup can no longer be just backup. That powerful central repository of data needs to be used for more.

By reusing the trapped data in backups, institutes can drive business analysis, decision making, development and richer customer experiences faster. Enterprises doing this today experience an **11%** higher developer productivity¹, reduce risk of compliance and audit failure (**17%**)² and **82%** less lost employee productive time due to data loss¹.



Conclusion

With the rapid change of IT strategy and faster adoption of modern services, data protection is more than ever under pressure to support and help business grow. No longer can backup be enough; organizations are looking for more from their data protection systems — lower costs, higher automation, and intelligence and data reuse, to name just a few.

With the accelerated adoption of cloud-based services, mainly from the COVID-19 impact, legacy data protection harms organizations' ability to keep critical data available. As healthcare organizations look to modernize their business practices, data protection must remain a key component of this plan.

About Veeam

With more than a decade of innovation, Veeam® continues to distinguish itself as the industry leader for backup and data protection. While we started our company focused on protecting virtualized workloads, our breadth of capabilities now spans physical infrastructure to public clouds like AWS, Azure and GCP, Kubernetes, and SaaS workloads.

Our complete data management platform extends beyond core backup and recovery with monitoring, disaster recovery, data mobility across cloud and data centers, security focusing on ransomware protection, and data reuse capabilities. These key components take backup to the next level. Veeam's platform growth has resulted in a leadership position in every top tier analyst ranking, peer review platform, and growth that far outpaces any leading vendor in the market.

Learn more about [Veeam Cloud Data Management™](#).

¹ IDC Research, The Economic Impact of Veeam Cloud Data Management Platform, April 2020

² IDC Research, IDC Race to Zero Survey 2018, October 2018



[veeam.com](https://www.veeam.com)