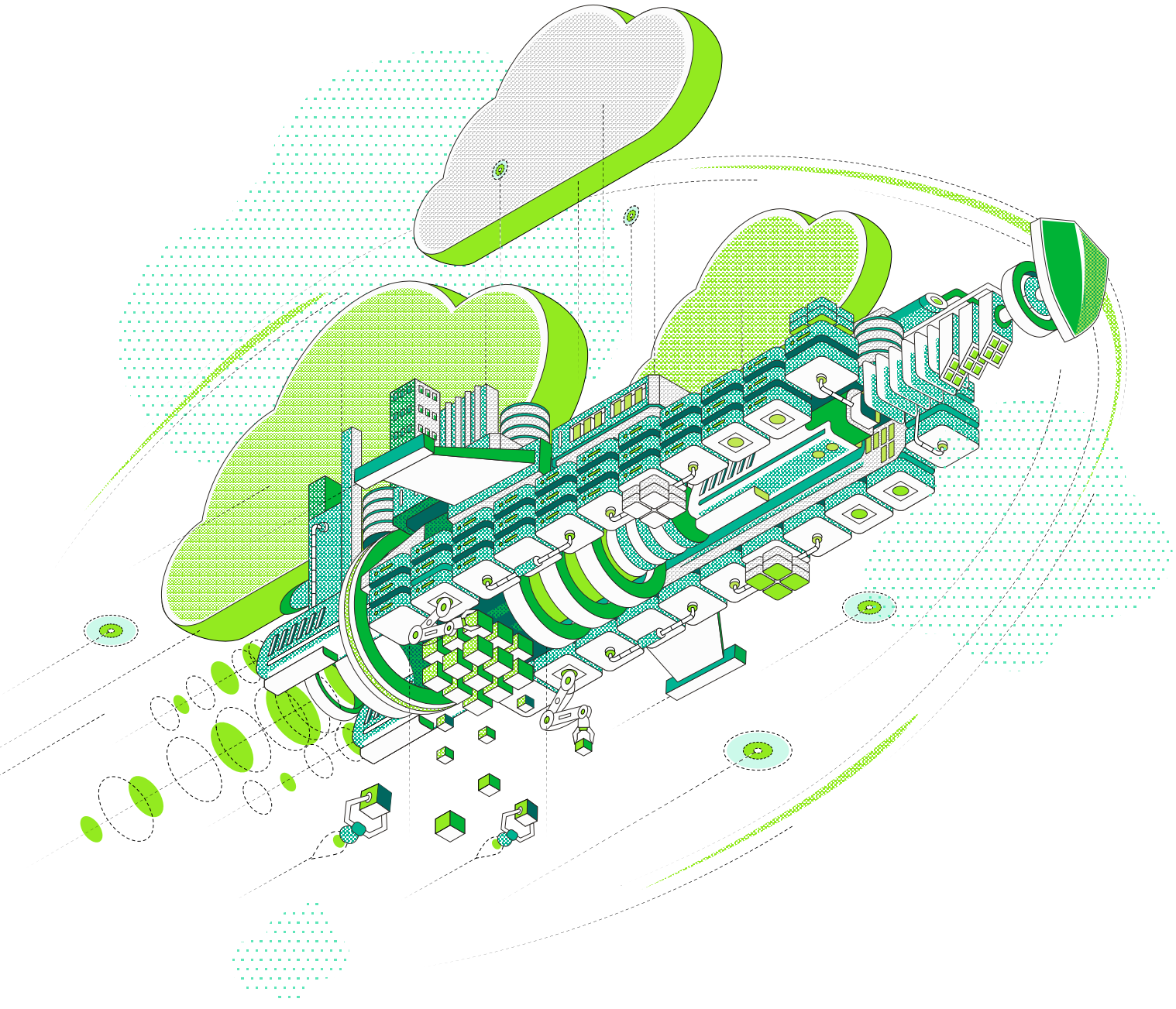
EXECUTIVE BRIEF

2022

Top Trends in Data Protection

Healthcare Edition



The pace for change in IT continues to rise, but how exactly are companies adapting for Modern Data Protection? Between October and December 2021, an independent research firm surveyed over 3,000 IT decision makers and IT professionals about their IT and data protection drivers and strategies heading into 2022. Almost all respondents were from organizations with more than 1,000 employees — from 28 different countries, including 399 from the healthcare industry.

This executive brief focuses on data from healthcare market participants and will help you better understand what your market peers are experiencing and how they're planning for 2022's IT demands. You can also download the complete global report which covers all industries at http://vee.am/DPR22.

On average, healthcare respondents expected their organization's budget for data protection, including both backup and BC/DR, to increase by **4.9%** globally in 2022. The unique circumstances of healthcare IT over the last two pandemic years were unprecedented. With the new dynamics that come with telehealth adoption, staffing shortfalls, supply chain disruptions and increasing cybersecurity threats, it's understandable that 2022 could see a myriad of investments in innovation and data protection as organizations strive to improve the quality, and their capacity, for patient care.

As the third annual study of Data Protection Trends, this year's survey was designed to quantify the shifts in overall concerns/goals and strategies for data protection, as well as gain an understanding of the current market landscape on data protection, disaster recovery, cybersecurity/ransomware and containers.

"Hybrid" and "Multi" are mainstream and here to stay

With over **8,000** global data points from three consecutive years of this survey, it is clear that "the new normal" for modern IT is approximately 50/50 between on-premises servers and cloud-hosted servers. Within healthcare organizations' data centers, there is a consistent expectation for both physical and virtual platforms. However, when compared to other industries, and the global trend, healthcare moved more quickly from physical to virtual infrastructure, and jumped more quickly to the cloud.

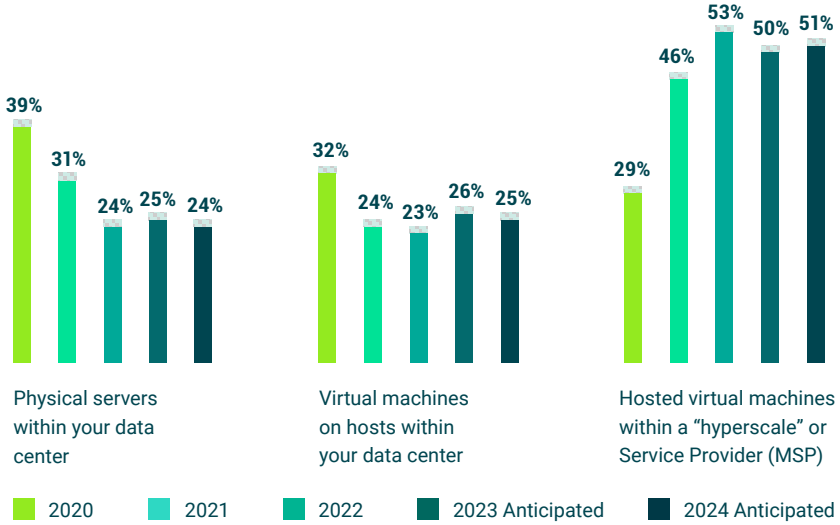


Figure 1.1

What do you estimate is your organization's percentage of servers in each format currently and what do you anticipate the percentage will be in two years' time?

25%

of organizations' primary driver to change backup solutions was for better economics, while 14% were looking to increase reliability while reducing RPO/RTO

68%

of organizations use cloud-service as part of their DP strategy

76%

of organizations had at least one ransomware attack in the last year

In 2022, healthcare infrastructures (on average) consist of 26% physical servers, 24% virtual and 50% cloud-hosted infrastructure. There are two key takeaways from these trends:

- The data center is neither dead nor dying. There are as many good reasons to run a workload on premises as cloud hosted, even for those with a "cloud-first" strategy
- Your data protection strategy needs to include physical, virtual and multiple cloud-hosted workloads

The "Gap" between business expectations and IT delivery has never been worse

The gap between what healthcare organizations expect and what their IT can deliver continues to widen, as tracked for the past five years in this project. For 2022, in healthcare:

- **96%** of IT leaders believe their organizations have an "availability gap" between the SLAs expected and how quickly IT can return to productivity. This is higher than all other industries included in the report and is a full six percent higher than the global figure.
- **93%** of IT leaders believe their organizations have a "protection gap" between how much data they can afford to lose and how often data is protected.

The rationale for these higher gaps is most likely due to the extreme criticality of patient data and healthcare-specific workloads. But there is an obvious corollary between the top change drivers of improving RTO (availability), RPO (protection) and reliability — versus these perceived "gaps." The perception gaps by IT leaders and the change drivers for IT implementers around reduced data loss and downtime is even more justified when considering that **52%** of healthcare servers suffer at least one outage per year — a full **12%** higher compared to the global, all-industry number.

52%

of servers have at least one unexpected outage

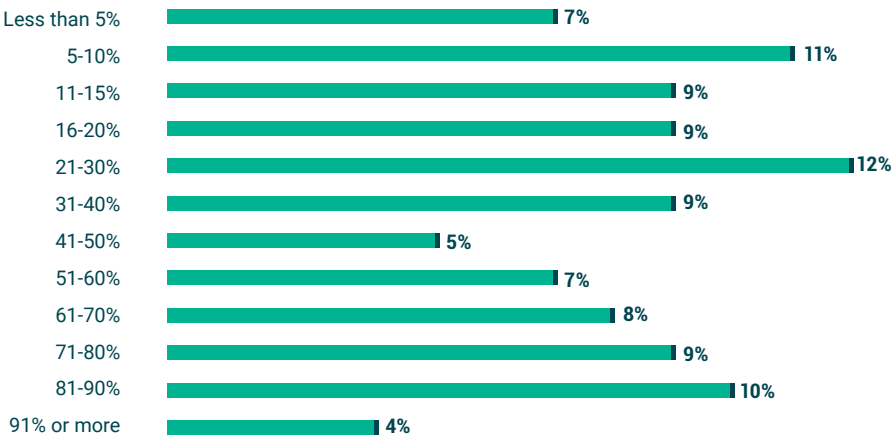
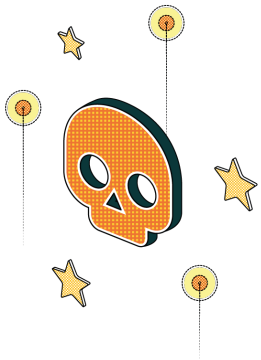


Figure 1.2

What percentage of your servers had at least one unexpected outage (even an unplanned reboot) within the last 12 months?

There is not as much difference between “high-priority” and “normal” data



While there will always be some workloads or data that is deemed of higher importance, the expectations between those significant workloads and the rest of IT are not that wide.

Data loss — **Globally, 56% of “high-priority” data and 49% of “normal” data have a data loss tolerance of no more than one hour. Organizations in healthcare cite 51% of “high-priority” and 43% of “normal” data having that “hour or less” tolerance. This means:**

- There is some difference between “high-priority” data and everything else. While all data matters in healthcare, the operational data that directly effects patient care and treatment outcomes must be more available than other data categories.
- Backup alone is not enough because it doesn't run hourly. Instead, backups must be combined with snapshots and/or replication.

These statistics are more interesting when considering the three-year trend from the respective global Data Protection Trends research reports. Here's a look at the average frequency of protecting data (in minutes) to mitigate the data loss of “high-priority” and “normal” data:

	2019	2020	2021
“High-Priority” protection frequency	205 minutes	198 minutes	121 minutes
“Normal” protection frequency	663 minutes	423 minutes	171 minutes

It is reasonable that organizations would continue to incrementally improve their protection of “high-priority” data over time; from every **205** minutes in 2019 to **121** minutes in 2021. It is very revealing that over the same two years, organizations have radically improved the frequency for protecting the rest of their data from every **663** minutes (roughly **8** hours or “nightly”) to **171** minutes (every **3** hours, meaning recurring during the day). That is nearly on par with “high-priority” protection, thus supporting the hypothesis that “all data matters” and the universal appeal of combining (typically nightly) backups with snapshots, replication or both.

Downtime — Similar to the data loss trend, in healthcare there is only a **8%** variance between the tolerable downtime of “high-priority” and “normal” applications for up to one hour — revealing the same realities that all data matters and the need for better than traditional once-per-day backups.

55%

of organizations had outages caused by ransomware. And for the second year in a row, cyberattacks caused the most outages

36%

of data on average was unrecoverable after a ransomware attack

What does this mean for 2022?

The last two years have seen significant IT modernization, particularly where cloud-hosted services could be leveraged. This is due to ongoing Digital Transformation initiatives, as well as accelerated cloud adoption during the global pandemic. **The rapid modernization of production has forced many organizations to recognize that their protection has not modernized at the same rate, even though their dependency on data and their dissatisfaction with the status quo are both at an all-time high, revealing three major trends leading into 2022:**

- Data protection will be an area of increased investment to protect the modern, and often cloud-hosted, workloads that are already in production
- Drivers for change will be based predominantly around qualitative improvement in reliability, protection frequency and agile recoveries — to improve RPO and RTO. In addition, better economic value and consumption, along with protecting IaaS/SaaS/containers and leveraging cloud for operational backups and disaster recovery, will be key initiatives.
- Improving data protection is in large part being driven by the recognition that cyberattacks, most notably ransomware, is a "when" not an "if" for most organizations — with reliable recovery being the remediation part of one's cyber-preparedness strategy. In that way, it is universally understood that "ransomware is a disaster," and that orchestrated recovery from backups is a critical component of every cyber- and BC/DR plan.

42%

of IT leaders consider the most important aspect of any "enterprise" backup solution to be the breadth of the workloads they protect

The Veeam perspective

Veeam's Backup and Data Management Platform

Now more than ever, it's critical for businesses to remain confident their data is protected and always available, whether it's on premises, at the edge or in the cloud. Veeam provides a single platform for Cloud, Virtual, Physical, SaaS and Kubernetes environments. Our customers are confident their apps and data are protected from ransomware, disaster and harmful actors, and are always available with the most simple, flexible, reliable and powerful platform in the industry.

Veeam gives clients the confidence to accelerate Digital Transformation, protect against cybercrime and drive business resiliency, ensuring that your data is always protected and always available. Reduce cost and complexity and achieve your business objectives with Veeam: the #1 Backup and Recovery.

To learn more, visit **https://www.veeam.com**.

Click here to view the Global complete research report

Questions related to this research data and insights can be directed to StrategicResearch@veeam.com