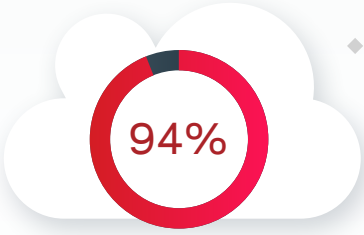
VERITAS

2022 Research Report on Securing Your Enterprise in a Multi-Cloud Environment

Healthcare Outlook

Like their global counterparts, many healthcare organizations rely heavily on standard backup and recovery tools available from their public cloud service provider (CSP). These tools, while functional in scope and cost-effective at the outset, offer little more than a basic level of visibility, support and protection against the volume and complexity of ransomware attacks, data theft and application outages that occur in the cloud. Consequently, organizations are placing their operations – and their customers – at serious risk.

Until these organizations reassess their reliance on CSP backup solutions and pivot to more robust third-party protection, they remain vulnerable to costly assaults on their business that inevitably cause permanent data loss, significant downtime, declines in revenue and compliance issues – all of which result in irreparable damage to their reputation.



Healthcare leaders acknowledged they need to improve their ability to track their entire data footprint

Key Findings

How much is IT complexity increasing from digital transformation and migration to the cloud?

Organizations across the globe have faced myriad challenges in 2022. Economic inflation, labor and supply shortages, and geopolitical uncertainty are nearly eclipsed by increased pressure to implement measures to achieve operational efficiencies, reduce cost and increase sustainability.

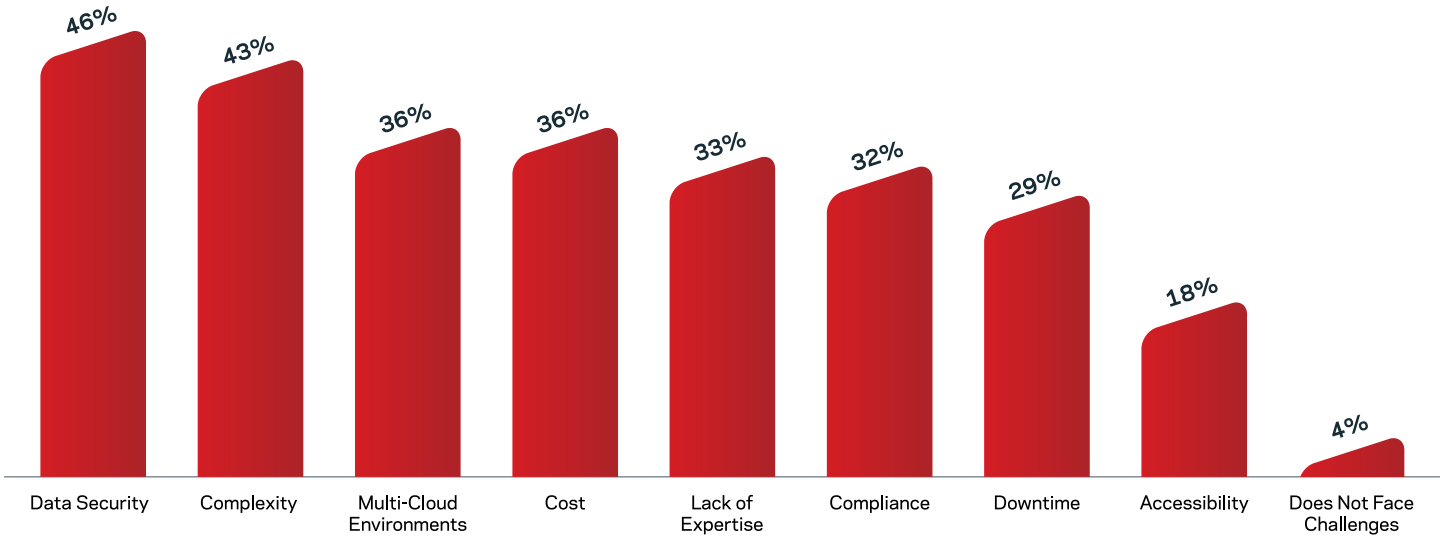
One such measure is the migration of data and software applications from on-premises to the cloud. Turning to built-in tools provided by public CSPs is widely viewed as a logical, cost-effective approach for supporting this migration. In fact, healthcare respondents report that their organizations currently use three public CSPs on average. As more companies push more data to the cloud, however, the opportunity exponentially increases for gaps to form and grow in data security, backup and recovery efforts resulting from improper use of support tools or tools that don't provide adequate air cover.

Boosting enterprise visibility goes hand in hand with thwarting vulnerability in the cloud. Alongside global peers, healthcare IT leaders are deeply concerned about maintaining insight into their enterprise data footprint.

When asked to what extent their organization could improve its ability to track its entire data footprint, a staggering 94% acknowledged that some improvements are needed. Just 56% of healthcare respondents said they have "complete visibility" into data stored within cloud environments, compared to 59% of their global counterparts.

QUESTION

What challenges, if any, does your organization face when accessing/maintaining data in cloud environments?



To what extent do enterprises understand their cloud data protection responsibilities?

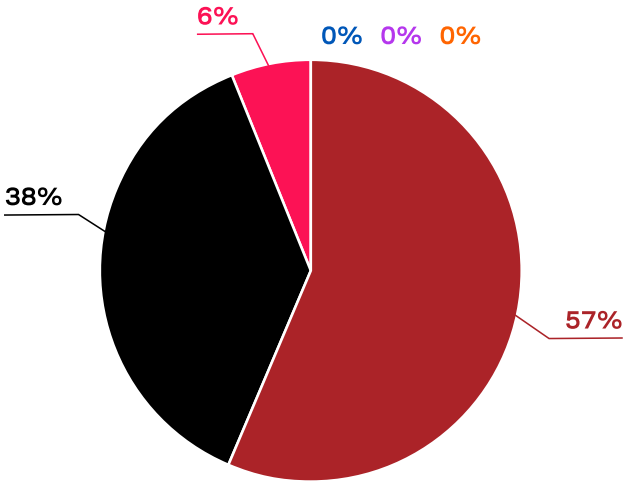
Coupled with this visibility/vulnerability scenario is a staggering disconnect between actual and perceived responsibility for data protection when enterprises move data to the cloud.

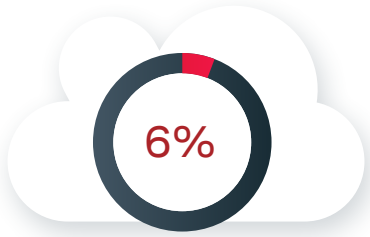
Every CSP requires customers to sign an end-user licensing agreement, which typically includes language buried deep within stating that the CSP is only responsible for protecting the infrastructure; i.e., the customer is responsible for protecting their own data and workloads within that cloud environment.

Key findings point to an astounding percentage of respondents who do not understand this division of responsibility: 94% of healthcare respondents, equal to 94% of global respondents. These organizations face an urgent need to understand their data protection responsibilities more clearly – before it's too late.

QUESTION

Which of the following statements most closely aligns with your understanding of the cloud shared responsibility model?





of healthcare respondents correctly answered that the customer is responsible for protecting their own data and workloads, compared to **6% globally**

- The CSP protects the infrastructure, applications, and data within the cloud
- The CSP protects the infrastructure and the applications within the cloud; the customer is responsible for data backup and recovery
- The CSP protects the infrastructure only; the customer is responsible for protecting their applications, and data
- The CSP provides the infrastructure; the customer is responsible for protecting everything
- I have not heard of the cloud shared responsibility model
- Don't know

What are the consequences of using CSP backup and recovery tools?

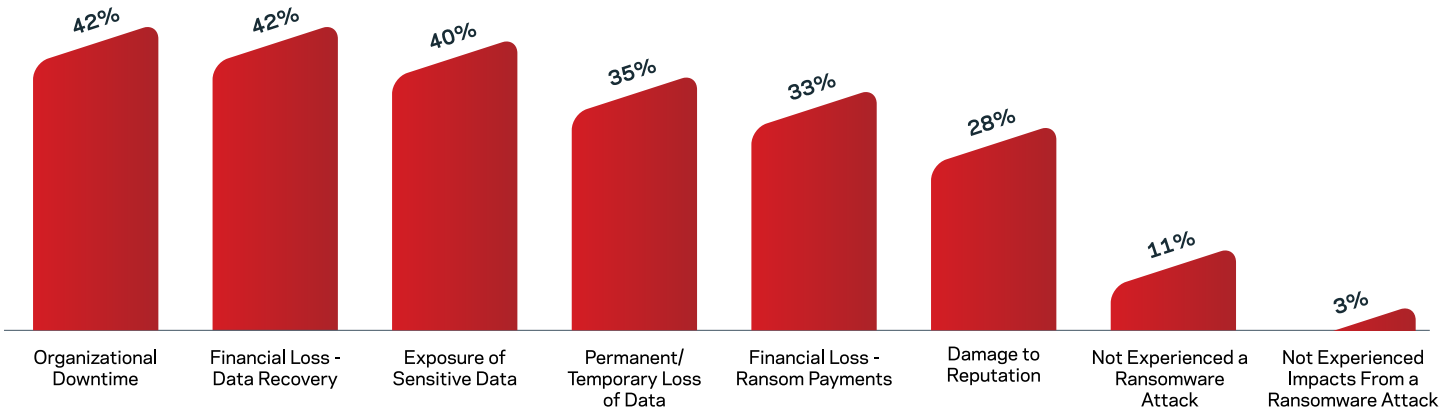
When an enterprise experiences a ransomware attack, they are better positioned to prevent or mitigate data loss, avoid paying ransoms and minimize downtime and business disruption if they are following best practices for backup, data protection and disaster recovery. This includes measures such as having a "3-2-1" backup strategy – one primary backup and two additional copies of their data, using at least two different storage mediums, with at least one copy offsite. Other measures include frequent disaster recovery rehearsals and comprehensive data protection for containers and even for SaaS applications like Microsoft 365, Slack and Box.

But organizations that base their data protection strategy around the CSP tools from their provider appear to be paying a heavy price. Among healthcare respondents, 44% use CSP tools "all of the time" compared to 48% globally. More frequent use of CSP tools is also associated with more operational downtime related to outages, application failures, human error, and even natural disasters.

Areas where healthcare organizations were adversely impacted by ransomware attacks on data it holds in cloud environments include exposure of sensitive data/information (40%), permanent/temporary loss of data (35%), financial loss-ransom payments (33%) and damage to reputation (28%).

QUESTION

What impacts, if any, has your organization experienced as a result of a ransomware attack on the data it holds within cloud environments?



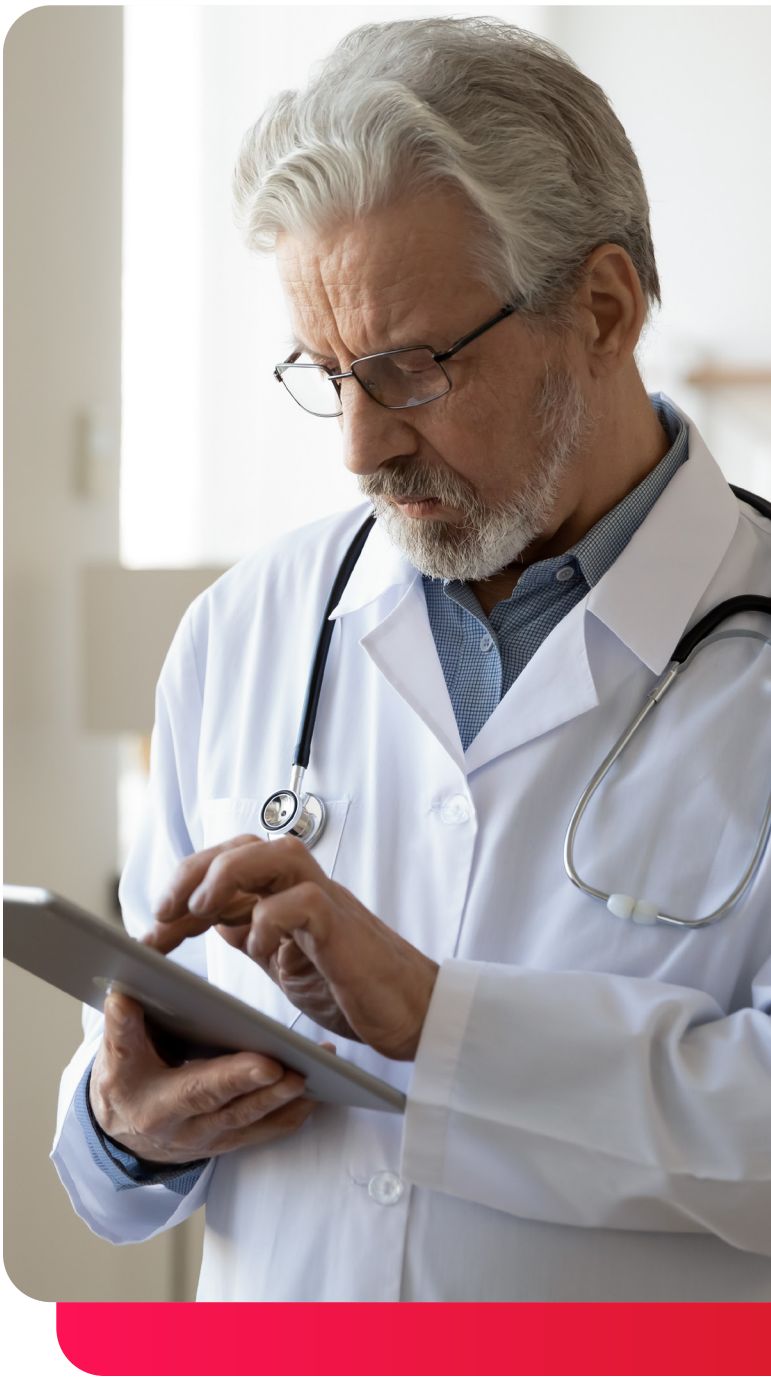
*Among healthcare respondents, **44%** use CSP tools "all of the time" compared to **48%** globally.*

How aware are IT leaders of the dangers of using CSP cloud security, backup and recovery offerings?

A strong majority of healthcare IT leader respondents (68%) said they "strongly agree" or "somewhat agree" with the statement that "the current offerings from public cloud service providers fall short of my organization's security needs."

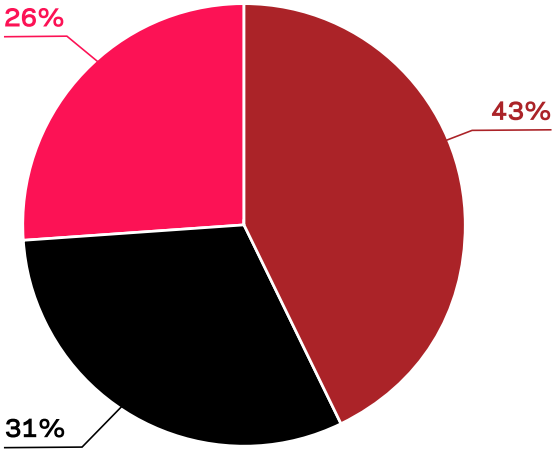
Additionally, in a separate question, 58% of healthcare respondents agreed that relying solely on CSP backup and recovery tools puts their organization at risk.

Despite this awareness, built-in backup and recovery offerings remain the top option for backing up public cloud data.



QUESTION

Approximately what percentage of your organization's public cloud data is backed up using the following tools?



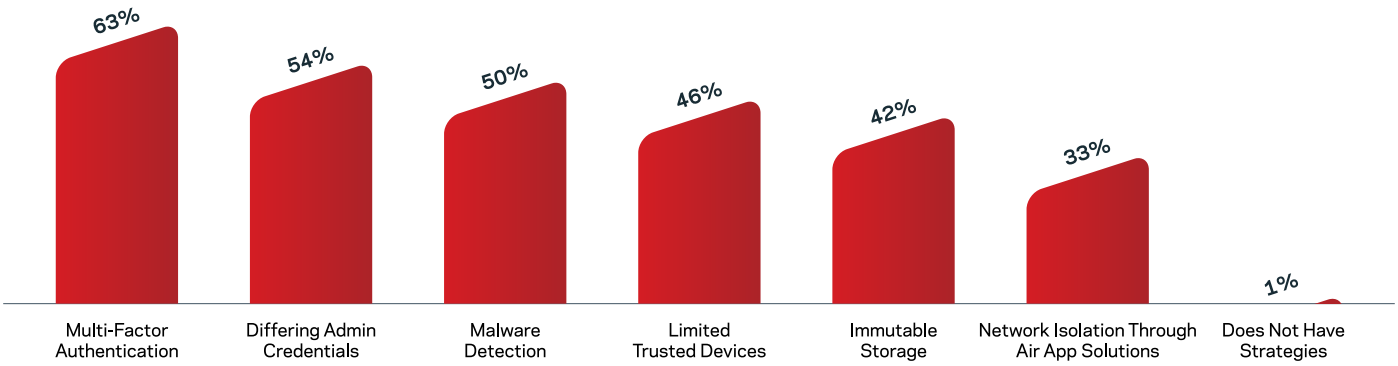
- CSP security tools
- In-house tools
- Third-party tools

In what ways are healthcare enterprises ensuring data protection and disaster recovery?

Examining more closely how enterprises are protecting their data offers a worrisome picture. Too many organizations are not using data protection best practices, such as immutable storage, in which data is completely static and unchangeable during its entire lifecycle, as well as limiting trusted devices on the network.

QUESTION

What strategies does your organization have in place to protect its data within cloud environments?



*Just **7%** of healthcare respondents said their organization backs up its data continuously, while **53%** said their organization backs up their data less frequently than every 12 hours.*

Mission-critical data not backed up for 12 hours or more is at risk of permanently being lost if there is a ransomeware attack or server failure

Continuous backups offer more comprehensive protection against data loss, as well as the ability to restore data from any point in time. Just 7% of healthcare respondents said their organization backs up its data continuously, while 53% said their organization backs up their data less frequently than every 12 hours.

This presents serious concerns. If mission-critical data is not backed up for 12 hours or more, the organization runs the risk of permanently losing that data if there is a ransomware attack, server failure, or power outage.

Twenty-nine percent (29%) of healthcare respondents said their organizations experienced a natural disaster that caused downtime over the past two years.

Conclusion

Technology and IT leaders deserve credit for helping their organizations pull through the pandemic while minimizing risks wherever possible. As organizations have supported remote and hybrid workforces, it has led to a proliferation of additional endpoints, cloud services, containerization, mobile devices, server and network sprawl, SaaS usage, and most of all, data growth across many platforms and devices.

Technology and IT leaders have often had to cobble together the best data protection and backup solutions on the fly, using their expertise and experience. Often, the best data protection solution seemed to be built-in backup and recovery offerings from each provider. But most organizations now recognize that these CSP backup and recovery offerings can neither scale, fully protect, nor provide a unified view of their data across all of their environments on-premises, in the cloud or virtualized.

Here are Veritas' recommended checkpoints and solutions for enterprises given these research findings:

- Determine how much your organization is relying on CSP data protection offerings. Senior executives (C-suite executives and VPs) should align with practitioner-level staff, such as cloud architects, to understand the extent to which their company is relying on CSP backup and recovery tools, and whether a robust, third-party data protection solution is needed.
- Determine how much of your business-critical data is in the cloud, and can you recover it following an attack or outage.
- If using the default security configuration from the cloud providers, determine if your cloud data and applications are protected against the latest cyber risks.
- Determine whether the CSP backup and recovery tools you're using offer any of the following data protection measures:
  - Continuous data backup and "3-2-1" backup practices (at least three copies of your data, spread across at least two storage mediums, with at least one offsite copy, away from your data center)
  - Zero trust, multi-factor authentication and role-based access control
  - Complete endpoint visibility
  - Immutable and/or indelible storage
  - Automated, orchestrated recovery processes
  - Regular and automated recovery testing and rehearsals
- In addition to these measures, organizations should educate employees further on phishing and social engineering tactics, reducing the chances they'll be a gateway for an attack.
- Ensure your organization understands its data protection responsibilities for cloud data, as established in your cloud provider's EULA. As the customer, you are responsible for protecting your own data and applications. The cloud provider is only responsible for protecting the infrastructure.
- There is a clear advantage to streamlining your data protection and application availability with a single solution that can reduce costs and complexity as well as provide enhanced and multiple layers of cloud data and application security.

By addressing these checkpoints, enterprises will ensure they are strongly positioned to mitigate the effects of ransomware, human error, cloud and data center outages, natural disasters and other unforeseen challenges.

At Veritas, we recognize these challenges around data protection and are uniquely positioned to help customers overcome them. Our Enterprise Data Services offer an integrated set of capabilities that deliver unmatched data management versatility and control to IT and compliance professionals across every industry and geography. Learn more at veritas.com

About Veritas

Veritas Technologies is a leader in multi-cloud data management. Over 80,000 customers—including 95 percent of the Fortune 100—rely on Veritas to help ensure the protection, recoverability, and compliance of their data. Veritas has a reputation for reliability at scale, which delivers the resilience its customers need against the disruptions threatened by cyberattacks, like ransomware. No other vendor is able to match the ability of Veritas to execute, with support for 800+ data sources, 100+ operating systems, 1,400+ storage targets, and 60+ clouds through a single, unified approach. Powered by Cloud Scale Technology, Veritas is delivering today on its strategy for Autonomous Data Management that reduces operational overhead while delivering greater value. Learn more at veritas.com. Follow us on Twitter at @veritastechllc.

VERITAS

2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For more information visit:
veritas.com

V1715 11/22