KUBERNETES DATA PROTECTION TRENDS

The Problem with Data Protection for Kubernetes

Table of Contents

01 Introduction

Introduction

The 2022 Kubernetes Adoption Report[1] – commissioned by Portworx by Pure Storage for the fourth year in a row – indicates Kubernetes adoption isn't slowing down. 77% of the enterprise users surveyed reported that their organizations' use of Kubernetes increased over the last two years.

Although containers were once only used for ephemeral workloads, organizations are increasingly using stateful applications with persistent volumes. IONIR found that 60% of organizations are already deploying stateful applications on Kubernetes.[2]

In order to protect their stateful applications, organizations need a solid data protection plan that covers not only backup and restore, but security concerns like ransomware protection and disaster recovery. However, data protection continues to challenge organizations as they move Kubernetes into production. In fact, more than 50% of respondents ranked data protection in their top three challenges.

In this report, Portworx takes a deeper look at the survey data in an effort to uncover why data protection continues to be an issue and what organizations can do to streamline and improve their efforts. Specific topics that are covered include:

- The top data protection challenges associated with Kubernetes
- The prevalence and severity of ransomware attacks
- The impact of service outages

[1] Get your full copy of the report at Portworx.com

[2] IONIR. "The Future of Stateful Applications on Kubernetes: Industry Report."

Survey methodology

The 2022 survey assessed the state of Kubernetes to discover how its adoption and usage has evolved in the last 12 months and what the future may hold. Questions heavily focused on Kubernetes data protection, including ransomware and outages.

The survey gathered online responses from 500 respondents. Respondents worked full-time in IT roles at companies with at least 500 employees and were knowledgeable about their companies' use of IT and Kubernetes technology. The sample was provided by Schlesinger Group, a research panel company.

02 The Kubernetes Landscape

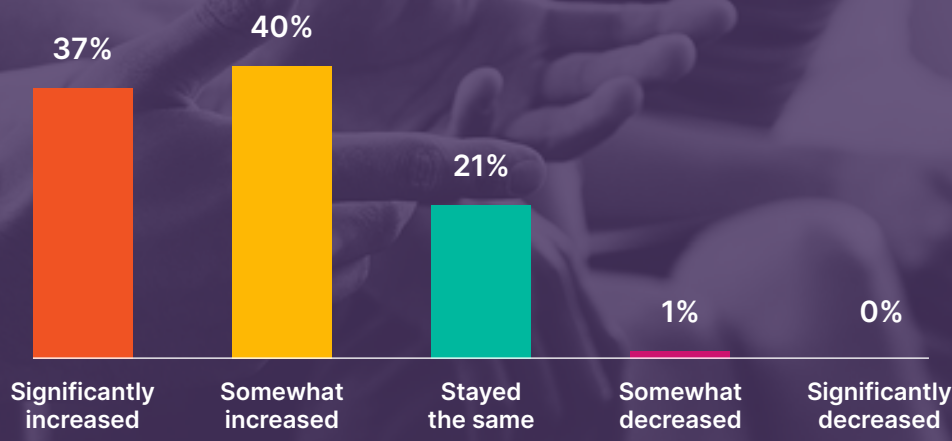
Kubernetes is here to stay

Kubernetes adoption continues to grow. Companies are running an average of 45% of their databases and data services on Kubernetes, and 87% of respondents expect Kubernetes to play an even larger role in their organizations' infrastructure in the next two to three years.

> **90%** of organizations run **more than 20%** of their new apps in containers, and **29%** run more than **60% of their new apps** in containers.

This transformational technology enables faster deployments, cost-effective resource utilization, and support for automated infrastructure scaling and management. These benefits proved useful in 2020 and 2021, as companies accelerated digital transformations by rolling out new apps and services to adapt to remote work, market disruption, and financial pressures.

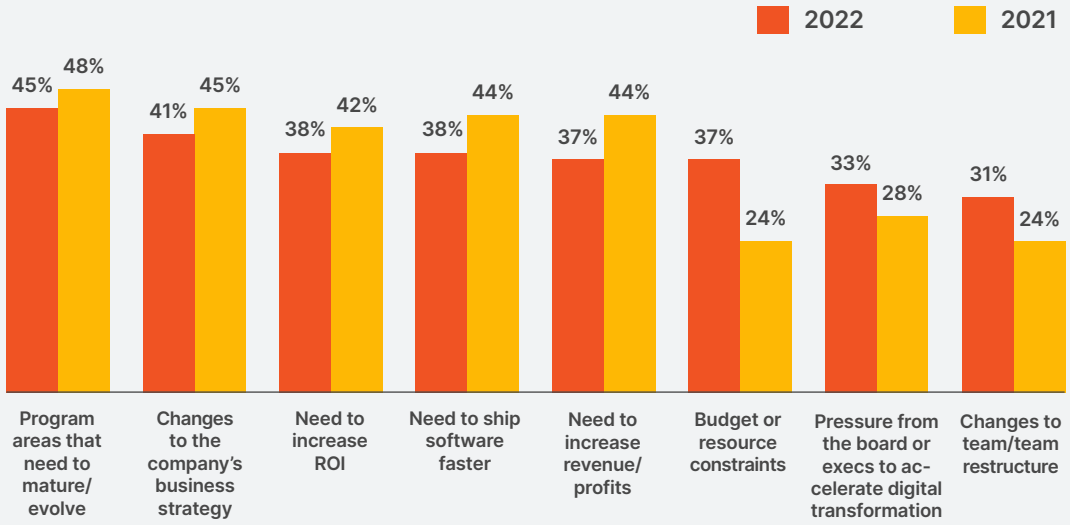
Impact of the pandemic on the use of Kubernetes in 2021 and 2022 as compared to 2020



What's driving the continued adoption?

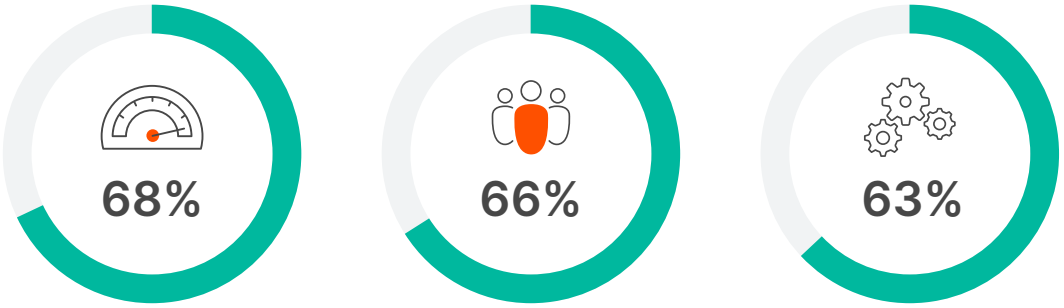
Companies use Kubernetes for numerous reasons, many of which remain somewhat steady from year to year. But in 2022, organizations cited an increasing need to address budget and resource constraints, team changes, and pressure from leadership to accelerate digital transformation initiatives.

Primary reasons for using Kubernetes in 2022 versus 2021



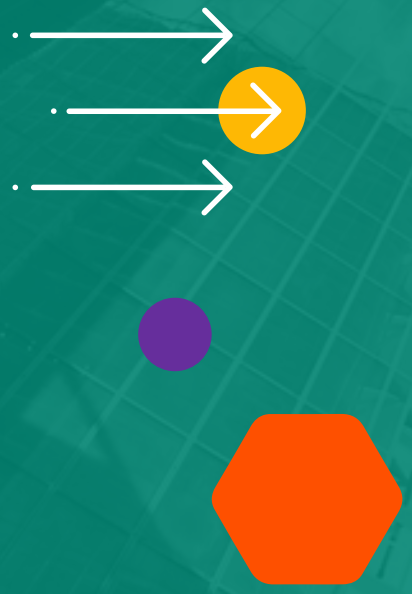
The biggest benefits from adopting Kubernetes have been faster time to deploy new apps and reduced staffing and IT costs. These results demonstrate that companies' are, in fact, being rewarded for investing in Kubernetes as a way to get applications to market faster, increase revenue and ROI, and reduce overhead.

Top benefits of adopting Kubernetes



THE KUBERNETES LANDSCAPE

Key takeaways



Kubernetes adoption shows no signs of slowing down. The value companies receive is immeasurable – they're able to get to market much faster, speeding time to revenue, and realize significant cost savings that directly impact the bottom line.

Managing Kubernetes at scale can be challenging, but it doesn't have to be. When running applications that are going into production faster, all Day 2 operations must be ready to ensure high performance, security, and scalability. If you want to realize the true value of Kubernetes adoption, you need a data management solution that can scale and automate complex manual processes.

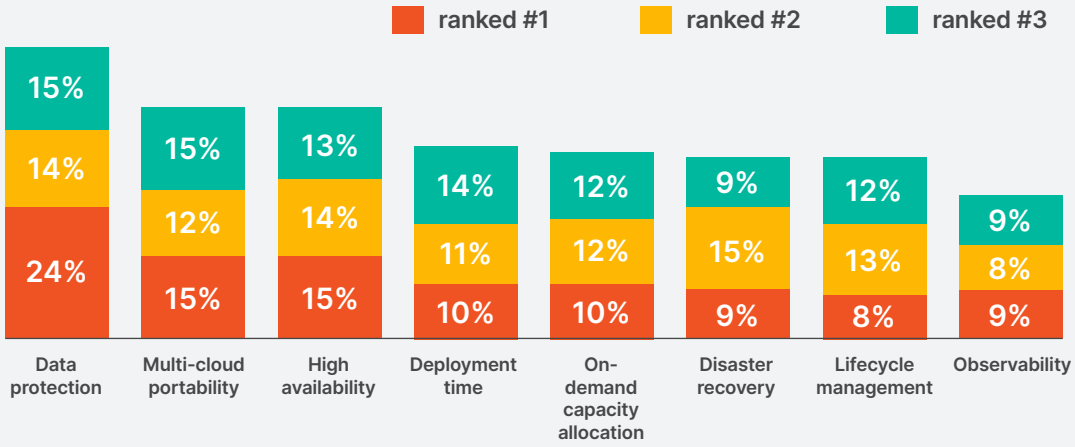
03 Data Protection Challenges

DATA PROTECTION CHALLENGES

Protecting data is an ongoing issue

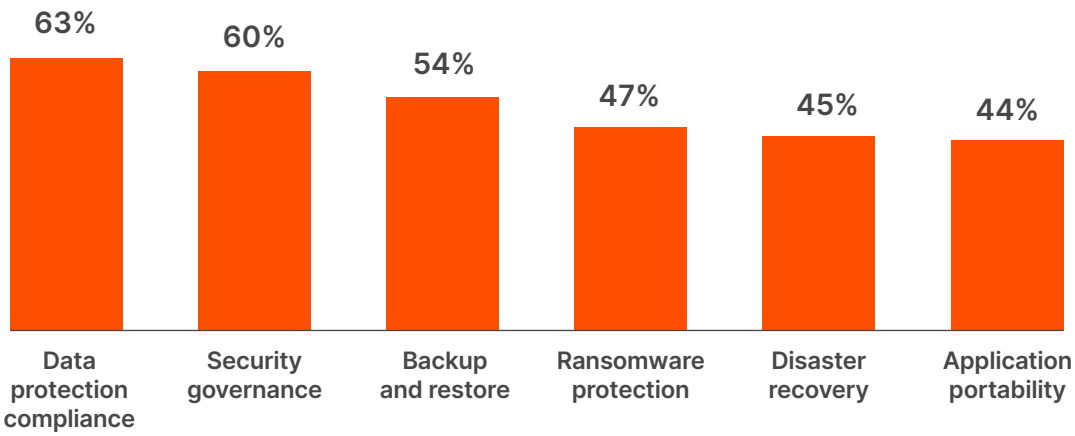
Nearly 25% of respondents cited data protection as their number-one issue when running Kubernetes in production – and 53% place it in their top three.

Challenges running databases on Kubernetes (rank the top three)



What makes data protection so difficult? Compliance and security governance are the most-pressing concerns, with 63% and 60% of respondents, respectively, ranking these challenges in their top three. Within these challenges, respondents indicated that their top struggles were with access control, protecting against malicious attacks, and visibility.

Most challenging elements of data protection



The elements of data protection that organizations are investing in mirror the areas that are their biggest challenges. Data protection and compliance and security governance are the top two areas, with 64% and 63% of respondents, respectively, listing these as in their top three areas for investment.

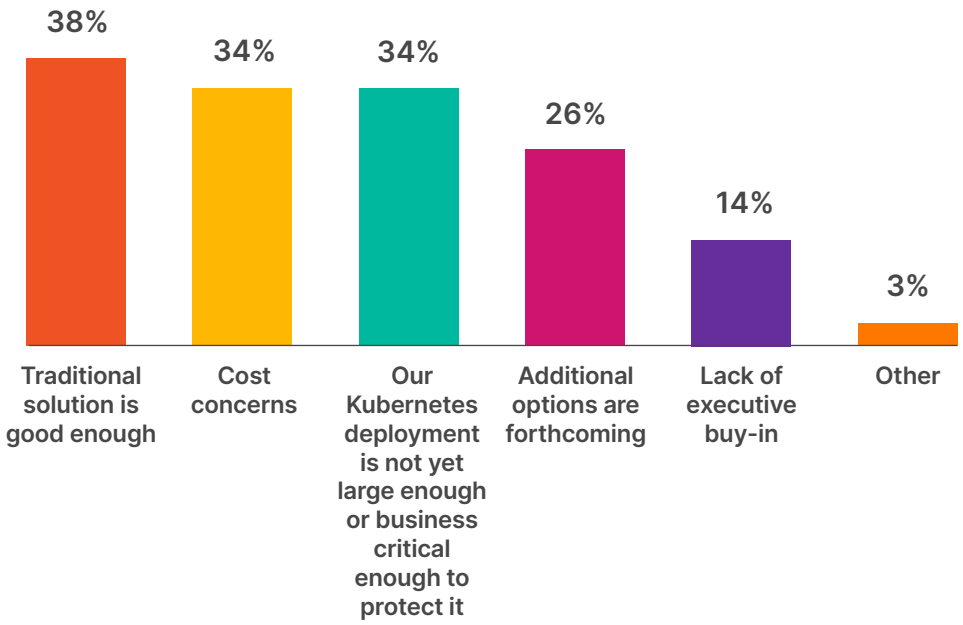
Data protection solutions built for Kubernetes

A majority of organizations recognize that traditional backup solutions don't work for modern applications, and they've chosen purpose-built solutions that can protect and restore the entire application.

> **84%** of respondents use a data protection solution that's built for Kubernetes.

For companies not using data protection that's purpose built for Kubernetes, their reasons include the belief that the traditional solution is good enough, cost concerns, and non-business-critical deployments. However, a traditional solution doesn't understand modern architectures, leaving production data at risk for potential loss and slow recovery. Perhaps that's why 95% of companies that have experienced a ransomware attack have turned to purpose-built backup solutions – they know firsthand how important it is to fully protect their apps.

Reasons for not using a data protection that's built for Kubernetes



DATA PROTECTION CHALLENGES

Key takeaways

Many organizations need to adhere to strict regulatory or corporate compliance that dictates backup policies. For example, many organizations follow the 3-2-1 backup rule – a gold standard for data protection compliance – and require role-based access control to limit user access to the precise actions required for their role.

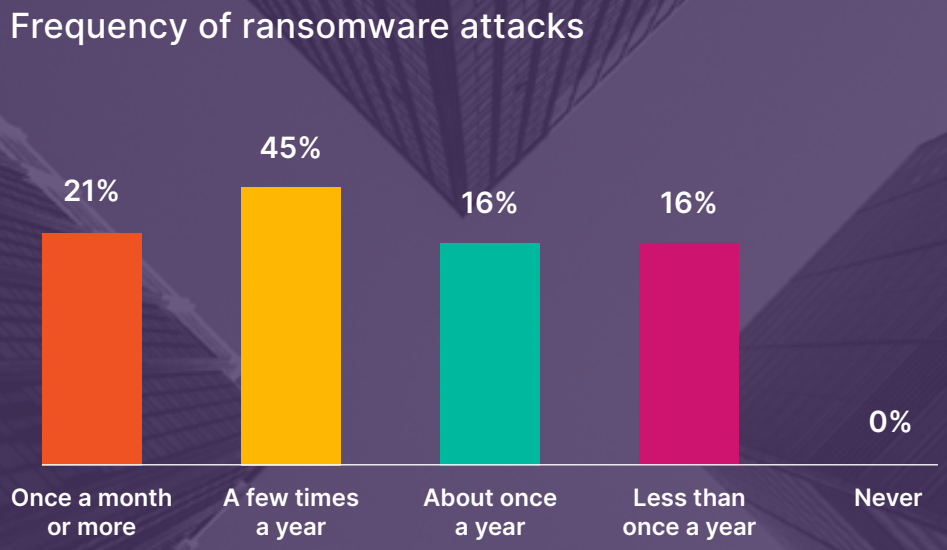
When using a solution that isn't built for Kubernetes, DevOps teams must build manual or do-it-yourself solutions that ultimately create more work or may not be robust enough to protect their mission-critical applications. Instead of relying on traditional backup solutions – which don't work with modern apps – use a built-for-Kubernetes solution that automates routine data protection tasks and access control, protects apps from malicious attacks, and increases overall visibility.

04 Ransomware

Ransomware attacks keep coming

Protecting against ransomware attacks is mission critical. More than 40% of respondents indicate that their organizations have been victims of ransomware attacks, and smaller companies (those with fewer than 1,000 employees) were 11% more likely to be attacked than their larger counterparts. Furthermore, companies that run more than 60% of their new apps on containers saw 24% more attacks than companies that run 40% or fewer apps in containers.

Ransomware attacks are growing in frequency and sophistication. More than one in five respondents get hit with an attack at least monthly. And 75% were targets within the last six months.

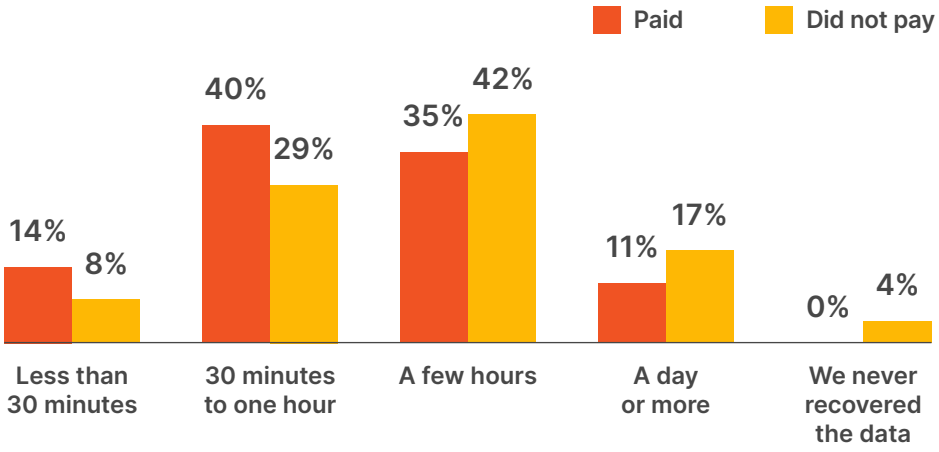


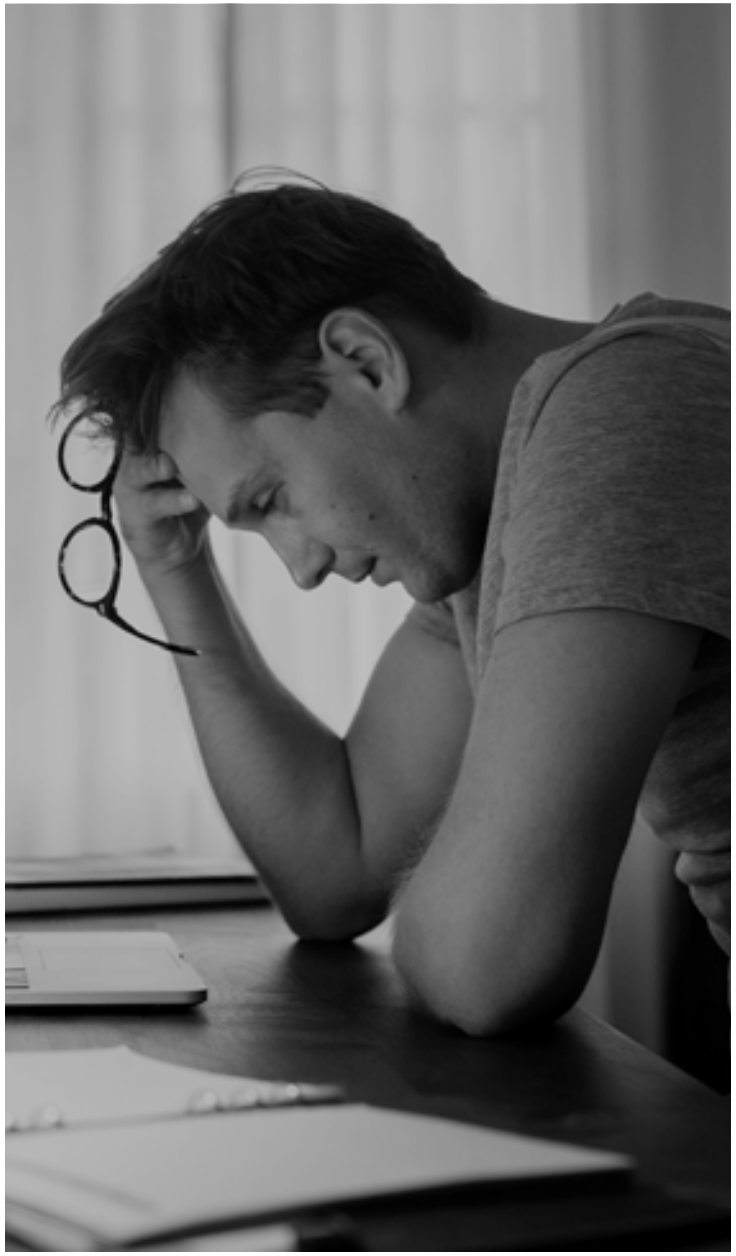
The cost of recovery

There are many hidden costs to getting hit by a successful ransomware attack. Along with harder to quantify lost opportunities, organizations must pay for downtime, people hours, server and device costs. According to Sophos, the average cost of remediation following an attack is $1.4 million.[2] These costs are in addition to paying the ransom, should the organization decide to do so. 60% of attacked companies in our survey paid the ransom. While this is no guarantee that data will be released or that they will never be targeted again, 54% of paying companies were able to recover in an hour or less.

[2] Sophos. "The State of Ransomware 2022."

Recovery time for paying versus not paying the ransom

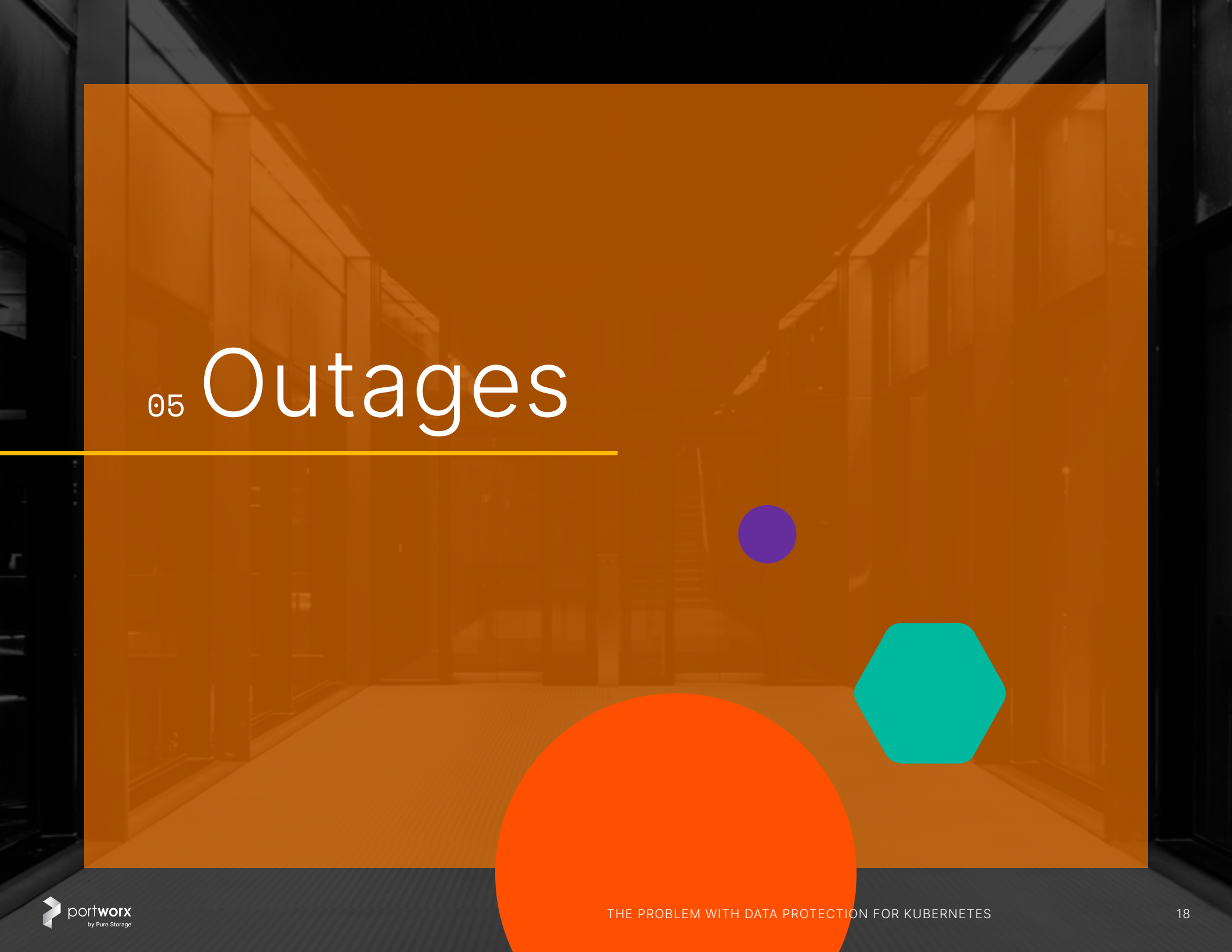




RANSOMWARE

Key takeaways

Having restorable copies that cannot be accessed by malicious actors is the best way to protect your organization from ransomware attacks. You need a solution that supports air-gapped environments or object-locked buckets, so any ransomware threat won't risk production data. This barrier safeguards data and gives your team peace of mind that your apps are protected from the growing threat of ransomware.



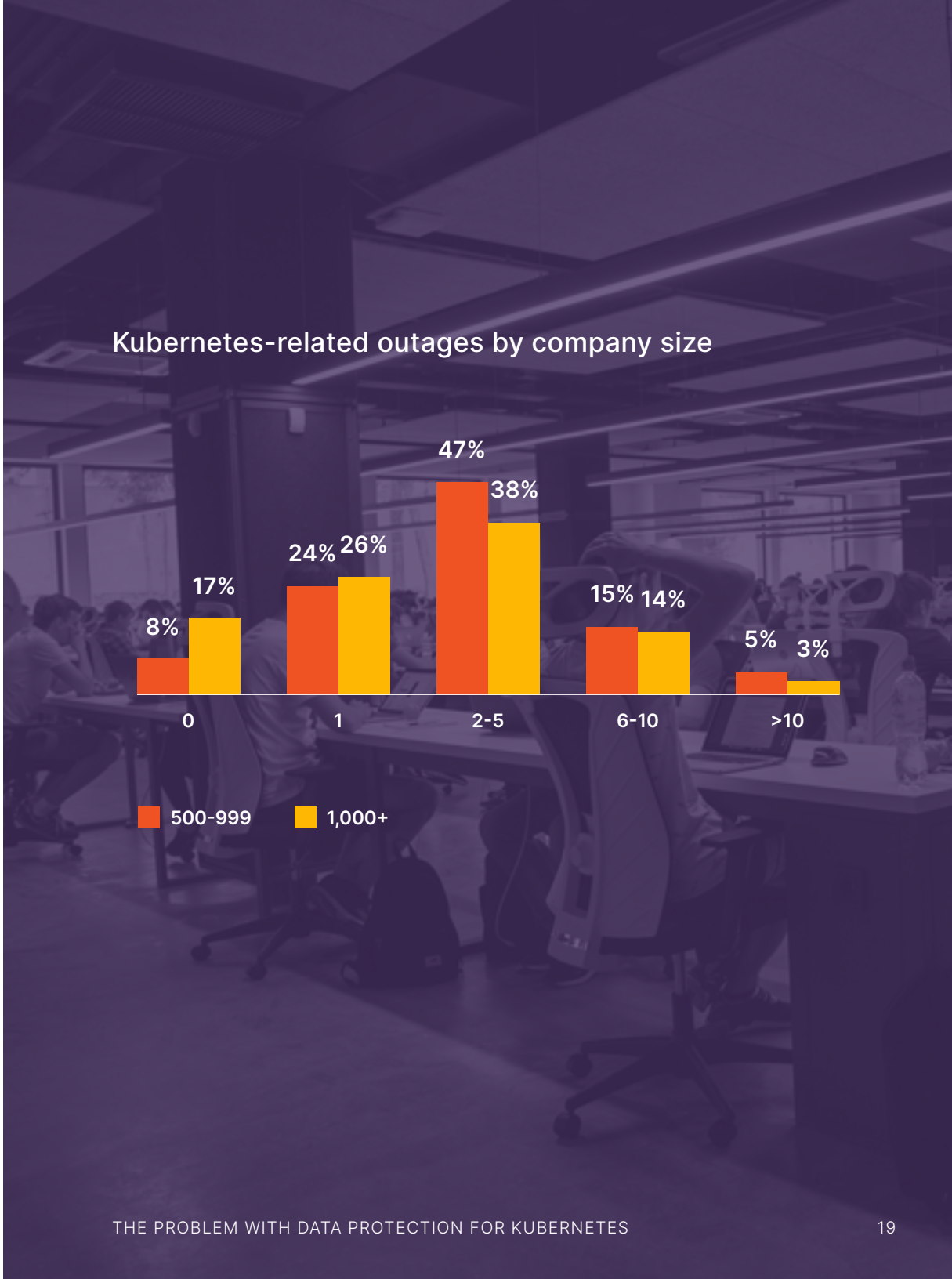
05 Outages

OUTAGES

A server, disk or node failure can happen at any time

Ensuring business continuity is a key part of running anything in production. Anyone can have a server, disk, or node fail – but if this failure leads to a service outage, it can have huge ramifications in terms of lost data, revenue, and customer loyalty.

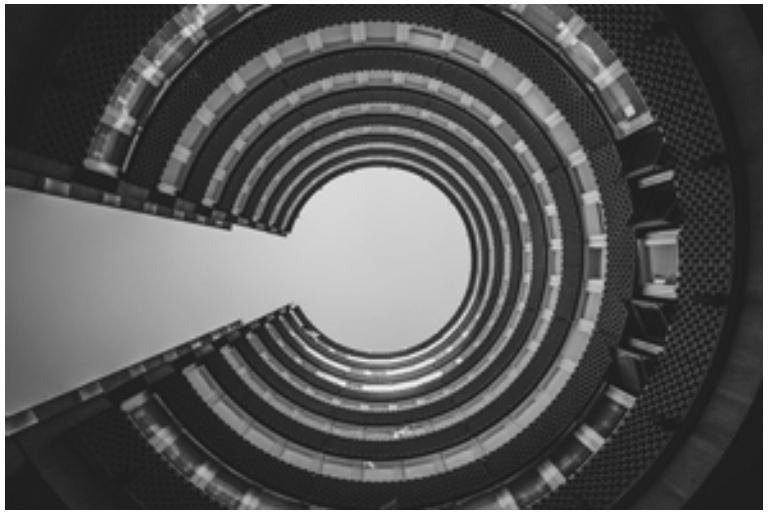
In the last 12 months, 87% of respondents experienced an outage – and 83% were Kubernetes related. Companies with fewer than 1,000 employees were more likely to report a higher number of outages overall and more Kubernetes-related outages than their larger counterparts.



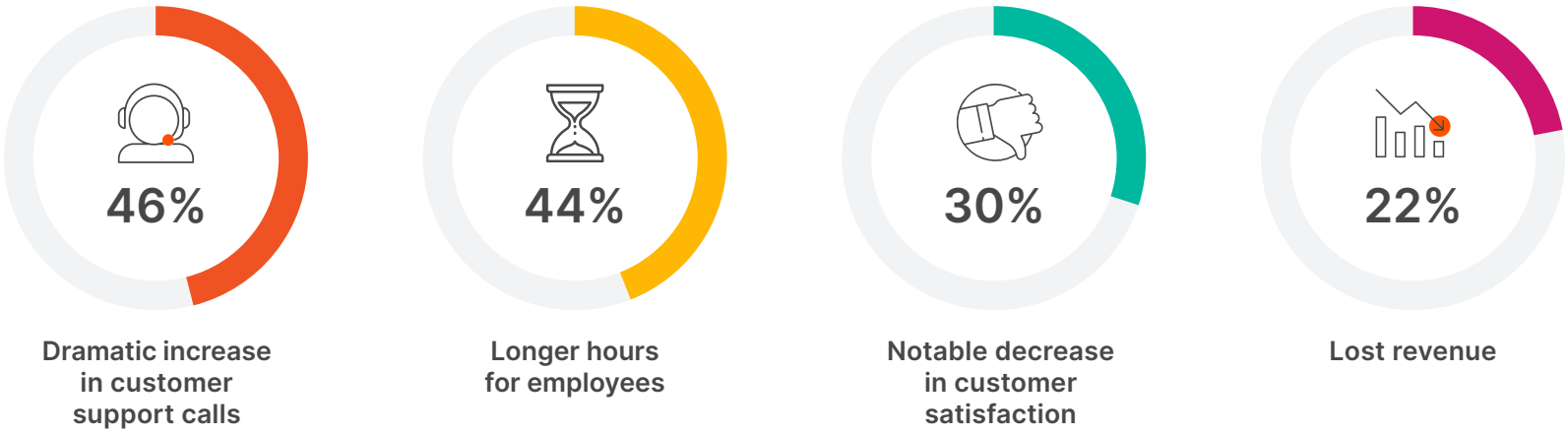
Results of outages

For 63% of respondents, outages were resolved in less than an hour; however, 10% reported outages lasted one day or longer. Only 8% of respondents indicated that these outages did not have a negative impact on their business; the remaining 92% experienced hits to their reputation, workloads, and revenue. A recent survey by 451 Research further drives home just how significant these impacts can be: 30% of outages cost organizations more than $1 million in damages.[3]

[3] 451 Research. "Storage, Data Management & Disaster Recovery 2022." July 2022.

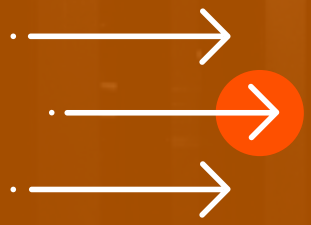


Negative impacts experienced from outages



OUTAGES

Key takeaways



As the data shows, service outages are common. To minimize negative impacts, having a comprehensive disaster recovery plan is essential. But disaster recovery for Kubernetes is often misunderstood. Many solutions claim their disaster recovery capabilities are a simple restore from backups – but that does not offer the true synchronous disaster protection required for mission-critical applications.

If your organization cannot tolerate any loss of your mission-critical application data, you need a solution that can offer zero RPO disaster recovery. This means that mission-critical data from the primary location is automatically copied to a secondary location, ensuring no data loss in the recovery copy and no downtime.

06 Conclusion

CONCLUSION

Get fast, easy, and secure data protection for Kubernetes apps

The growing adoption of Kubernetes proves the attention this technology has received is warranted. It promises incredible benefits – faster time to market, reduced staffing costs, and easier updates – and it's delivering on those promises. But Kubernetes comes with its fair share of challenges, perhaps none more pressing than data protection.

As ransomware and outages continue to pose real threats to data in your mission-critical apps, ensuring data protection, security, and compliance is more critical than ever. You need a backup solution that's purpose-built for Kubernetes – one that delivers enterprise-grade data protection with fast recovery and no data loss.

Portworx Backup is the solution that puts an end to the data protection challenge by enabling you to:

Recover data in a single click with application-aware backup.

Migrate apps across environments and regions within minutes.

Simplify compliance with sophisticated role-based access control and 3-2-1 rule support.

Protect data from loss or attack with fast failovers and zero RPO disaster recovery.

Wherever you are in the cloud-native journey, it's imperative that you have a data protection strategy with backup capabilities that are scalable, flexible, and purpose-built for Kubernetes. Experience how Portworx Backup makes data protection fast, easy, and secure. Visit **portworx.com/backup.**

About Portworx by Pure Storage

Portworx, acquired by Pure Storage in October 2020, is the container storage company enterprises rely on to manage mission-critical data services in containers. By enabling data availability, data security, and backup and disaster recovery for Kubernetes-based applications running on-premises or across clouds, Portworx has helped dozens of Global 2000 companies such as Carrefour, Comcast, GE Digital, Lufthansa, T-Mobile, and SAIC run containerized data services in production. Portworx partners with Amazon, Google, IBM, VMware, and other leading enterprise software companies to accelerate container adoption. For more information, visit **portworx.com** or follow **@portwx.**