portworx® by Pure Storage

Modernizing Disaster Recovery in Financial Services

Kubernetes Usage In Financial Services

In today's landscape, financial services institutions (FSIs) are under unprecedented pressure to rapidly innovate while maintaining operational resilience. Disruptive technology trends and ever-evolving compliance requirements necessitate a revolutionary approach to both application development and operational frameworks.

FSIs face a challenging dual mandate:

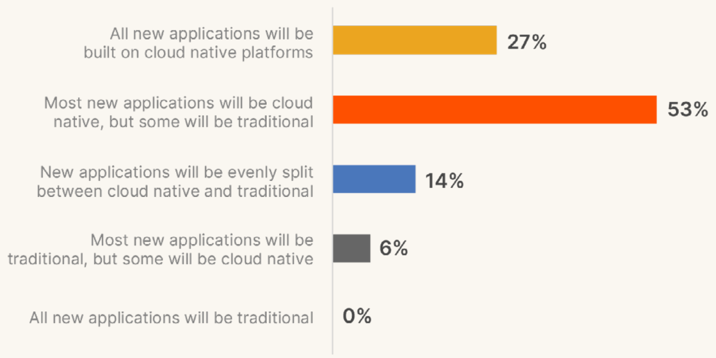
1 An existential need to innovate: Banks, credit issuers, payment processors, and investment managers must innovate quickly in a market disrupted by digital-first fintechs, peer-to-peer payments, buy-now-pay-later (BNPL), mobile-first services, and AI/ML-assisted hyper-personalization in investment, and trading.

2 Meeting stringent resilience requirements: FSIs must address evolving cybersecurity threats, new fraud attacks, ever-changing compliance and regulatory requirements, and meet high customer expectations.

Successfully navigating this dual mandate is crucial for the survival and growth of financial services organizations.

As an IT professional in the financial services industry, you are likely witnessing the increasing adoption of cloud-native technologies to address this dual mandate. A recent survey found 80% of companies plan to build most of their new applications on cloud native platforms over the next 5 years.[1]

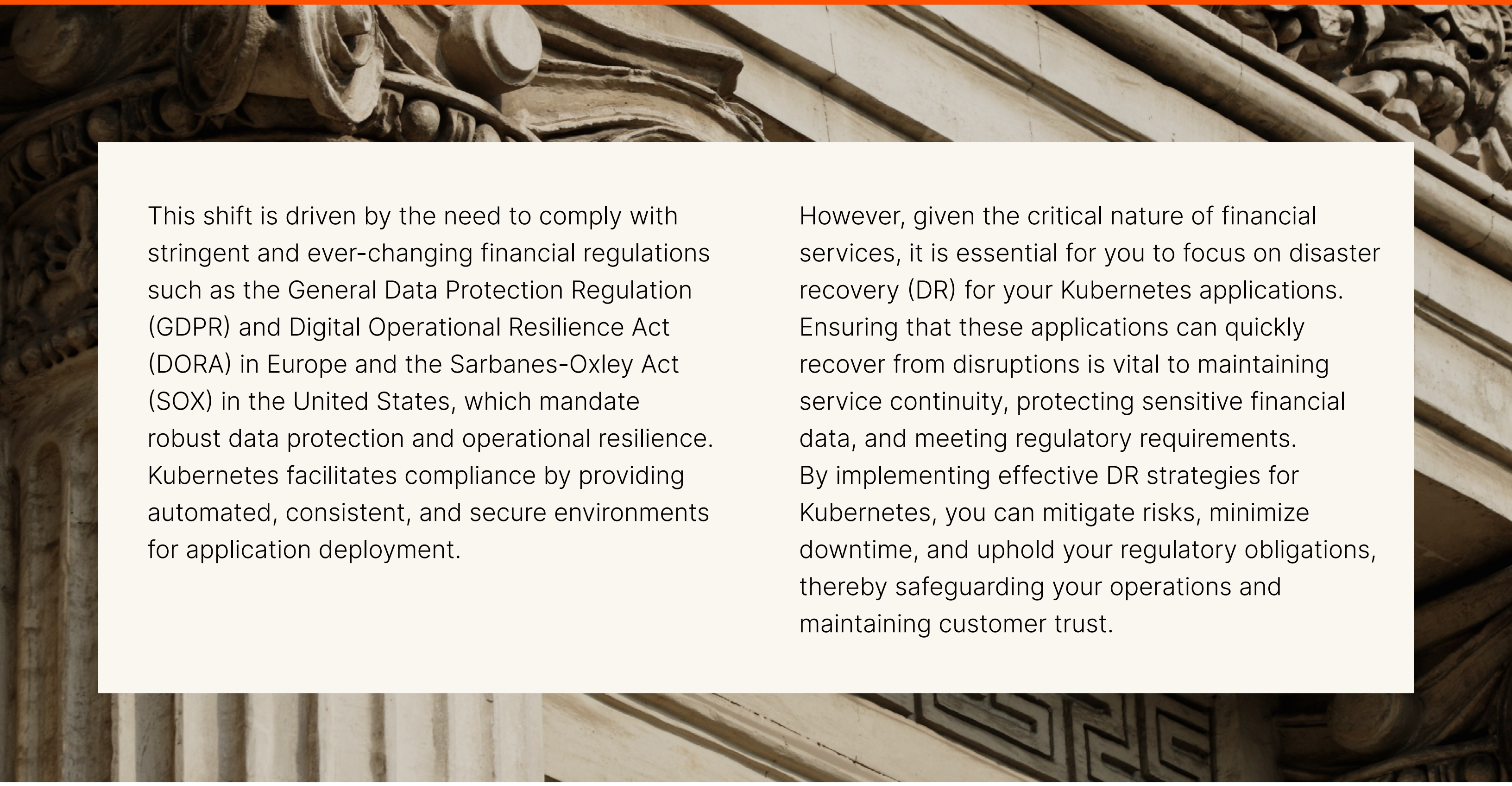
How would you describe your company's investment plans for NEW applications in the next five years?



80%

are building most of their new applications on cloud native platforms

[1] The Voice of Kubernetes Experts Report 2024



This shift is driven by the need to comply with stringent and ever-changing financial regulations such as the General Data Protection Regulation (GDPR) and Digital Operational Resilience Act (DORA) in Europe and the Sarbanes-Oxley Act (SOX) in the United States, which mandate robust data protection and operational resilience. Kubernetes facilitates compliance by providing automated, consistent, and secure environments for application deployment.

However, given the critical nature of financial services, it is essential for you to focus on disaster recovery (DR) for your Kubernetes applications. Ensuring that these applications can quickly recover from disruptions is vital to maintaining service continuity, protecting sensitive financial data, and meeting regulatory requirements. By implementing effective DR strategies for Kubernetes, you can mitigate risks, minimize downtime, and uphold your regulatory obligations, thereby safeguarding your operations and maintaining customer trust.

Introduction To Kubernetes Disaster Recovery

These new applications built and run on Kubernetes are crucial to your organization’s success in maintaining or expanding your industry differentiation. But with the adoption of any new technology, there are many factors to pay attention to: new development methodologies, new teams, new staff, new technologies, new partners, new vendors, and new challenges.

As mission-critical applications increasingly move to Kubernetes, disaster recovery tops the list of concerns for enterprise IT leaders.

After making significant investments in Kubernetes, the last thing you want to happen is for applications to be unavailable, or data to be lost because of some disaster out of your control—cloud providers go down, data centers lose power, services are unavailable, connectivity is disrupted, and customers are unhappy.

The Uptime Institute reports[2] that 60% of companies experienced an outage in the last 3 years, and those outages are costly: with more than two-thirds of all outages costing more than $100,000. Power issues are consistently the most common cause of serious and severe data center outages and cloud, colocation, telecommunications and hosting companies — account for a growing proportion of outages.

[2] Uptime Instituite Annual Outage Analysis 2023

Key Takeaways

Portworx solves the three major challenges to ensuring an enterprise-grade disaster recovery solution for your cloud-native Kubernetes applications. Built from the ground up specifically for Kubernetes, Portworx PX-DR is:

1 **Container granular and application aware:** Kubernetes applications are container based, not virtual machine or server based. To effectively run Kubernetes backup and disaster recovery, replication needs to happen at the container level.

2 **Automated disaster recovery:** Relying on a manual process for Kubernetes application recovery is unreliable—it takes time you can't risk and leaves room for error. You need to know that you are meeting SLAs without intervention, not implementing complex scripts once a server has already gone down.

3 **Mission Critical: Zero RPO & low RTO** Flexible, synchronous and async DR capabilities enable a range of application uptime and recovery SLAs. For data centers in a metro area, a single Portworx cluster can span two distinct Kubernetes clusters, enabling Zero RPO failover for mission-critical apps.

Financial services IT teams must deliver robust disaster recovery solutions for many enterprise applications.

Your disaster recovery solution not only needs to be portable and easy to use, but it also must be aware of the specific containerized applications and their individual technology components.

As a result, an easy-to-use and portable disaster recovery solution built specifically for Kubernetes is more important than ever.

High availability/disaster recovery is the

#1

data management capability that would benefit organizations working with data and applications on K8s[3]

[3] The Voice of Kubernetes Experts Report 2024

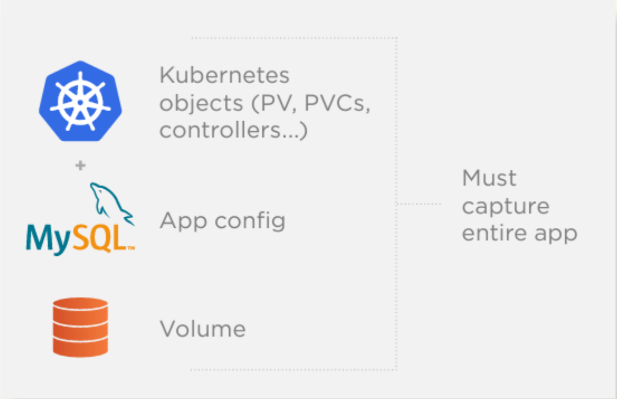
Unique Challenges of Protecting Kubernetes Applications

Containers Are Fundamentally Different From Virtual Machines

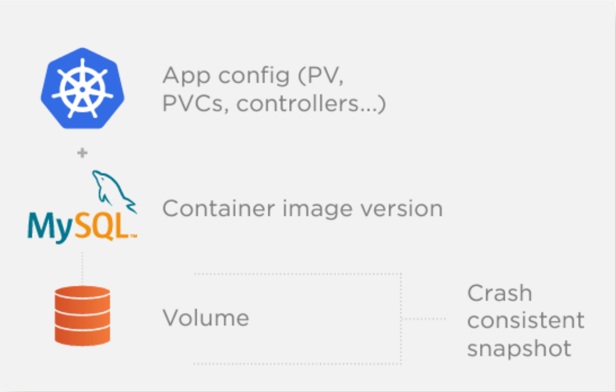
Containerized applications are different from applications running in virtual machines. To successfully protect and then restore a containerized application, you must orchestrate a complex series of synchronized actions across a distributed system. This is because the application is likely running in multiple containers, and those containers are on different nodes within a Kubernetes cluster.

This is a vastly different architecture than the traditional single application in a virtual machine paradigm we've seen for the past 15+ years in financial services.

Your existing backup and disaster recovery solution may work very well for your current virtual machine based applications, but it won't work with containers or Kubernetes. Trying to use a traditional enterprise backup and DR system that understands virtual machines will, at best, leave you with a false sense of security and, at worst, unavailable applications with corrupted data. The first rule of data protection is never to lose data. With a virtual machine-based solution, you're at risk.



Seamless migrations, faster recovery


App config (PV, PVCs, controllers...)
+
MySQL
Container image version
Volume
Crash consistent snapshot

Other recovery solutions

Applications Require Automated Intelligence For Recovery

Recovering a Kubernetes application after a disaster is not as simple as starting a new container in another location. Simple snapshots are no longer sufficient to ensure data consistency.

Containerized application components are deployed and scaled individually, each with their own container image, deployment configuration, state rules, extensions, life cycle operations, dependencies, and data. The additional configuration data and application business rules are often stored as metadata in your Kubernetes cluster and need to be protected and recovered to allow for application failover to work properly.

Furthermore, today's containerized applications are more than just a single component with their container image and data. Applications in a microservices architecture are comprised of front-end services combined with numerous middleware layers implementing business logic that is, most importantly, connected to persistent data services. This entire application stack must be backed up and recovered as a group.

54%

of respondents say their most recent significant, serious or severe outage cost more than $100,000, with 16% saying that their most recent outage cost more than $1 million.[4]

> The unparallelled performance and reliability of Pure's platform was convincing, and how it supported our sustainability initiatives **really won over our team.**
>
> **Steve Allgeier**
> Vice President of the Distributed Infrastructure Group, Fiserv

Finally, the most popular data services (Kafka, Cassandra, Elastic, MySQL, and MongoDB) are all built by different communities with very little in common with respect to their operational life cycle and the skills required to operate them.

The increasing popularity of distributed data services demands a rethink of application protection, one that takes into account both the data and declarative operational metadata.

[4] Uptime Institute Annual Outage Analysis 2024

Fast Recovery with Zero Data Loss Across Every Cloud

Backup and disaster recovery have always been the worst mix of the mundane and critically important. You want it to be boring because when it's exciting, it means something has gone wrong. You want it to "just work" and be part of your operational procedures as you scale your applications and environments.

Most critically, recovering your mission critical applications with zero data loss in a timely fashion is the most important aspect of your disaster recovery strategy.

Over 80% of the respondents to a recent Uptime Institute data center survey say that their most recent serious outage could have been prevented with better management, processes and configuration.[5] There is still a long way to go for most organizations to achieve their availability requirements.

Finally, the need for your protection and recovery strategy to "just work" across all of your environments is more crucial than ever before. With over 94% of large enterprises having already implemented a hybrid, multi-cloud approach[6], and on average using over 10 different public cloud and SaaS solutions, you can't afford to have bespoke solutions for each provider.[7]

Kubernetes is rapidly becoming the platofrm of choice for strategic high-value workloads.

72%

of organizations are running **databases** on K8s

67%

of organizations are running **analytics applications** on K8s

54%

of organizations are running **AI/ML workloads** on K8s

[5] Uptime Institute Annual Outage Analysis 2024

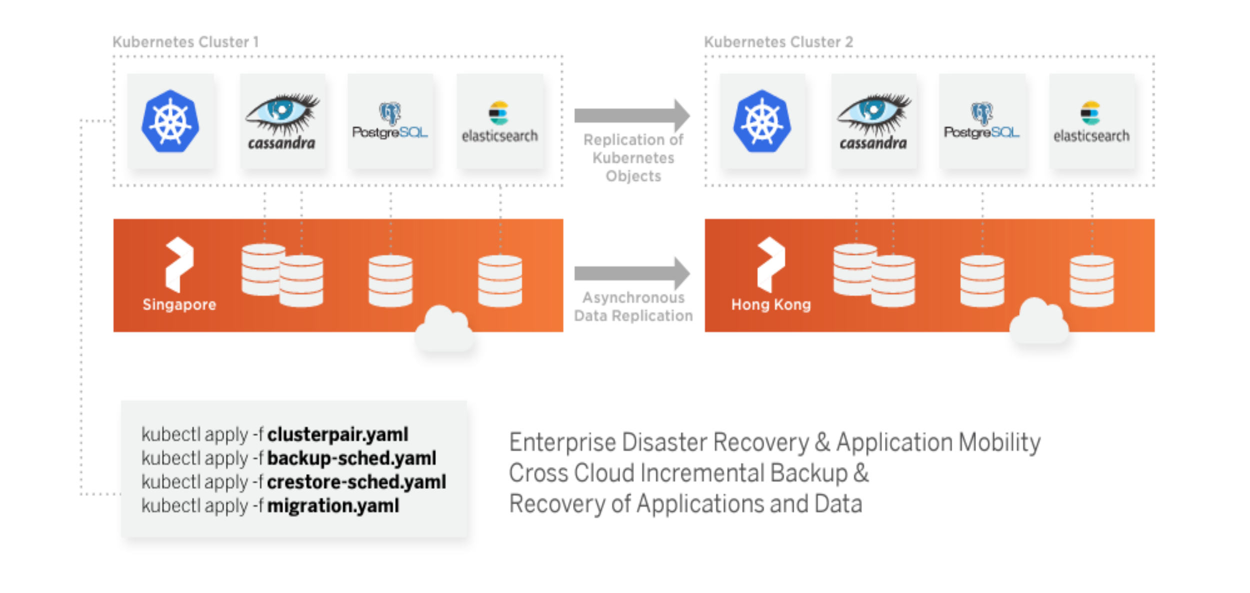
[6] Statista: Multi cloud adoption worldwide in 2021 and 2023, by organization size

[7] Statista: Forecast of use number of clouds in multicloud environment from 2020 to 2023*, by industry

Portworx Delivers Disaster Recovery For Kubernetes

Portworx understands Kubernetes and containerized applications. We built a series of storage and data management solutions specifically to solve the challenges faced by financial service organizations as you modernize your IT.

Portworx PX-DR is purpose-built to protect your Kubernetes applications, enable fast recovery with up to zero loss of data, and ensure your teams scale without requiring specialist skills for each new containerized technology you rely on.



```
kubectl apply -f clusterpair.yaml
kubectl apply -f backup-sched.yaml
kubectl apply -f crestore-sched.yaml
kubectl apply -f migration.yaml
```

Enterprise Disaster Recovery & Application Mobility
Cross Cloud Incremental Backup &
Recovery of Applications and Data

Built for Kubernetes

Containerized applications typically run in multiple containers across multiple hosts. The delineators are Pods and Namespaces (or Project by some Kubernetes distributions). Portworx PX-DR understands both the Pod and Namespace constructs, enabling you to protect an entire application at the container-granular or Namespace level.

By protecting the Pod or entire Namespace, you get peace of mind that, regardless of your application configuration or the placement across machines in your cluster, you can simply and easily select applications to protect.

Protecting your application is more than orchestrating snapshots, although that is complex enough. Portworx's disaster recovery solutions also make it simple to restart your application quickly in another Kubernetes cluster—regardless of cloud provider or location.

By ensuring the protection of your application, its configuration, and, most importantly, its data, Portworx delivers true Kubernetes native disaster recovery.

Portworx PX-DR speaks to Kubernetes natively and has pre-built integrations with many of the leading data services **used by many Global 2000 today.**

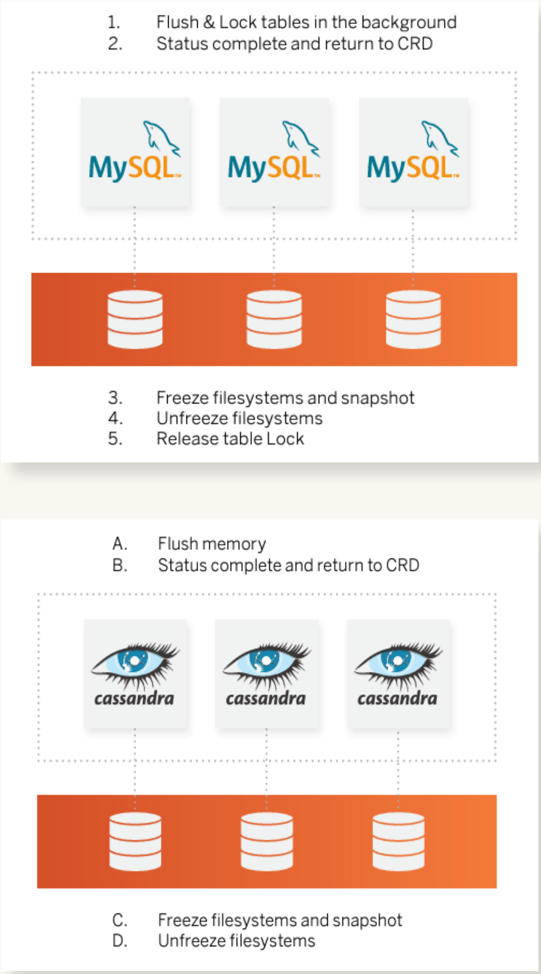
Application Aware

Today's containerized applications are increasingly built with a diverse set of technologies—presentation, message streaming, analysis, and data storage—that have vastly different operational models and communities.

To effectively scale your application and data protection strategy, you typically have two options: either restrict yourself to a limited set of technologies, which may curb your agility, or adopt a solution that inherently manages these complexities.

This approach can significantly speed up your transformation by integrating seamlessly with a wide range of technologies and automating protection measures. This means that you can continue to innovate and deploy new and transformative applications, safe in the knowledge that you don't need individual specialists for every technology. Portworx takes care of the underlying integration for you.

Apps-consistent backups means understanding apps



1. Flush & Lock tables in the background
2. Status complete and return to CRD
3. Freeze filesystems and snapshot
4. Unfreeze filesystems
5. Release table Lock

A. Flush memory
B. Status complete and return to CRD
C. Freeze filesystems and snapshot
D. Unfreeze filesystems

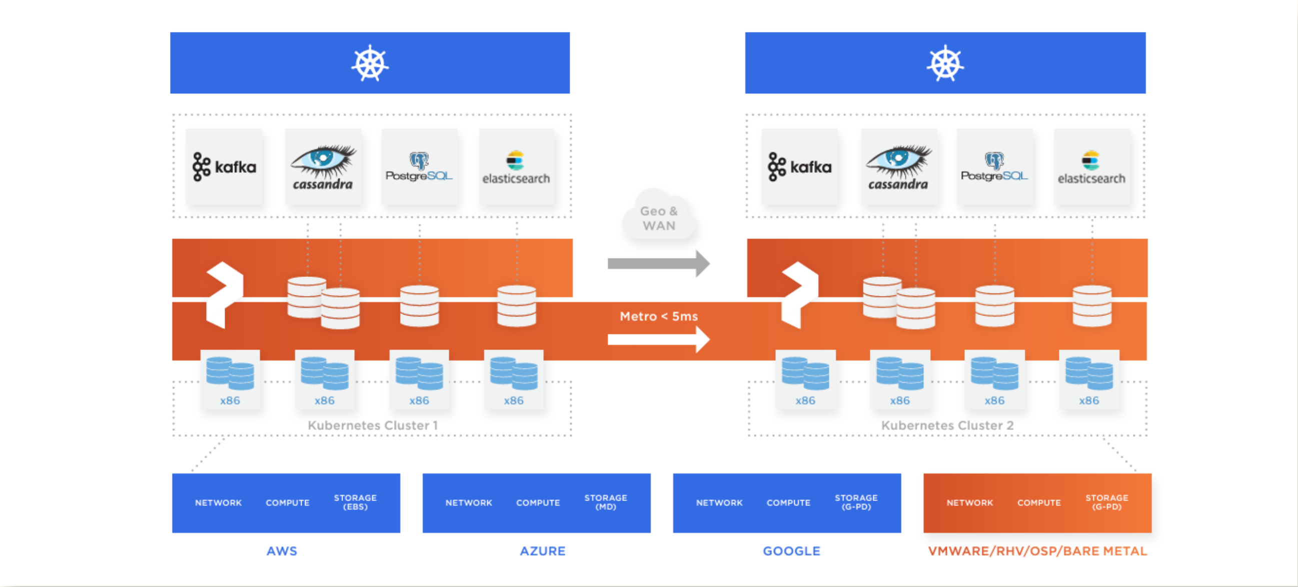
Consistently Reliable DR in a Multi/Hybrid-Cloud World

Your applications don't live in a single controlled environment. Even if you're only using a single cloud vendor, you've deployed applications across multiple regions. As you continue to adopt a multi/hybrid-cloud approach, this complexity will increase.

Portworx PX-DR is built specifically with multiple and heterogeneous environments in mind. Delivering zero data loss (Zero RPO) and fast recovery times (Low RTO) is a key requirement for application resilience—and Portworx's solutions deliver this.

When replicating your applications within the same metro region— Portworx enables you to achieve Zero RPO and Zero RTO. This means no data loss and near instant recovery in the event of a site failure. In more traditional configurations where your applications are deployed across diverse geographic locations, with Portworx, you can experience fast recovery in seconds to minutes without any data loss. **When your applications work even when your clouds don't, your customers keep coming back.**

Push-button easy DR that just works, based on automation across all clouds delivering zero data loss and fast recovery.



Achieving Zero Data Loss for a Global Bank

A global bank based in Canada wanted to take advantage of the benefits they saw in Kubernetes with Red Hat OpenShift©. However, they were not able to meet strict availability requirements with just Kubernetes. With Portworx Container Data Management, and PX-DR, they were able to achieve zero data loss (Zero RPO) and an RTO of less than two minutes. That means they are able to recover their application in another data center in under two minutes with no data loss.

Without Portworx's disaster recovery capabilities, this global bank would not have been able to ensure availability and thus would not have been able to deploy their application on OpenShift©.

Conclusion

Your financial institution is moving fast; your competitors are, too. In this highly-connected world where customer experience is king, failing your customers is not an option.

Mistakes occur, outages happen, and clouds fail—don't get caught without a robust, agile, and fast recovery solution that ensures your applications are up and running again quickly and that you don't lose any customer transactions.

The containerized applications you are deploying on Kubernetes are your growth engine, but they are also built differently than your traditional applications. You need to protect them differently with a solution built specifically for Kubernetes that understands containers.

To truly scale and take advantage of DevOps and Platform Engineering, requiring specialized staff for each technology is a limiting factor you can't afford. Your disaster recovery solution needs to be application-aware and to enable your highly-skilled generalists to scale without limits.

Hybrid multi-cloud is the new normal, which means constraints that limit functionality across providers is untenable. Your applications need to use whatever services they require in whichever cloud you choose.

Portworx PX-DR solves these challenges and enables you to **build a platform for success.**

What’s Next?

Portworx has been helping Global 2000 organizations build Kubernetes data platforms for over 10 years. We understand what you’re trying to achieve and where most of the challenges are. We are ready to help you.

As a next step, we recommend a **Hands-on-Lab** or to **speak directly with a specialist.**

portworx.com

800.379.PURE