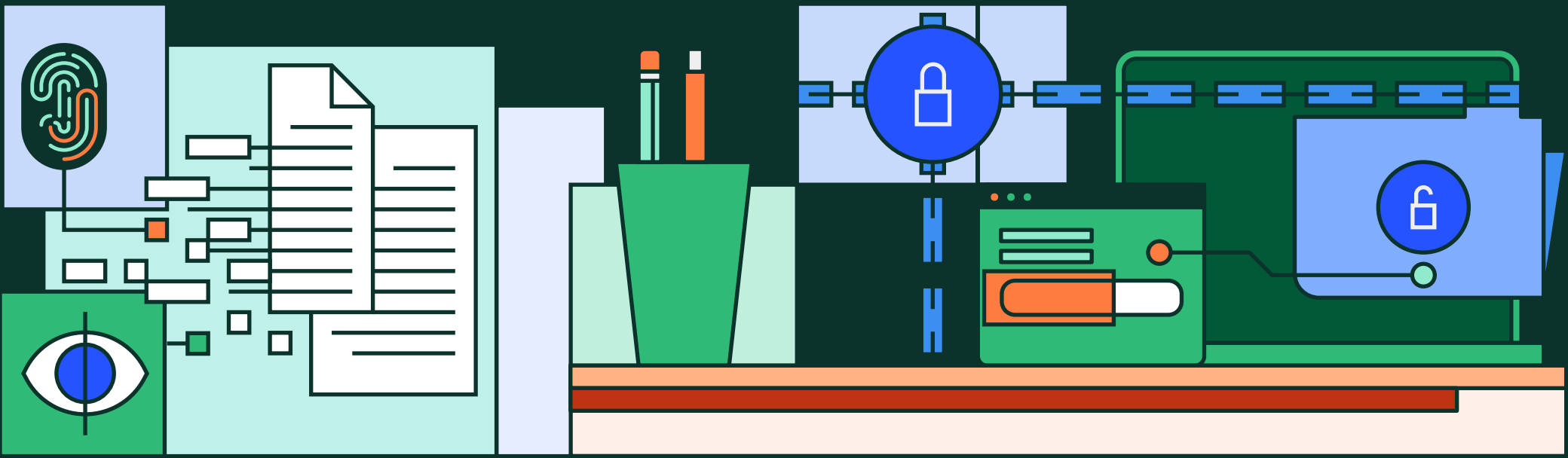
SUSE | portworx by Pure Storage

Building Resilient Kubernetes:

Business Continuity & Data Protection You Can Trust

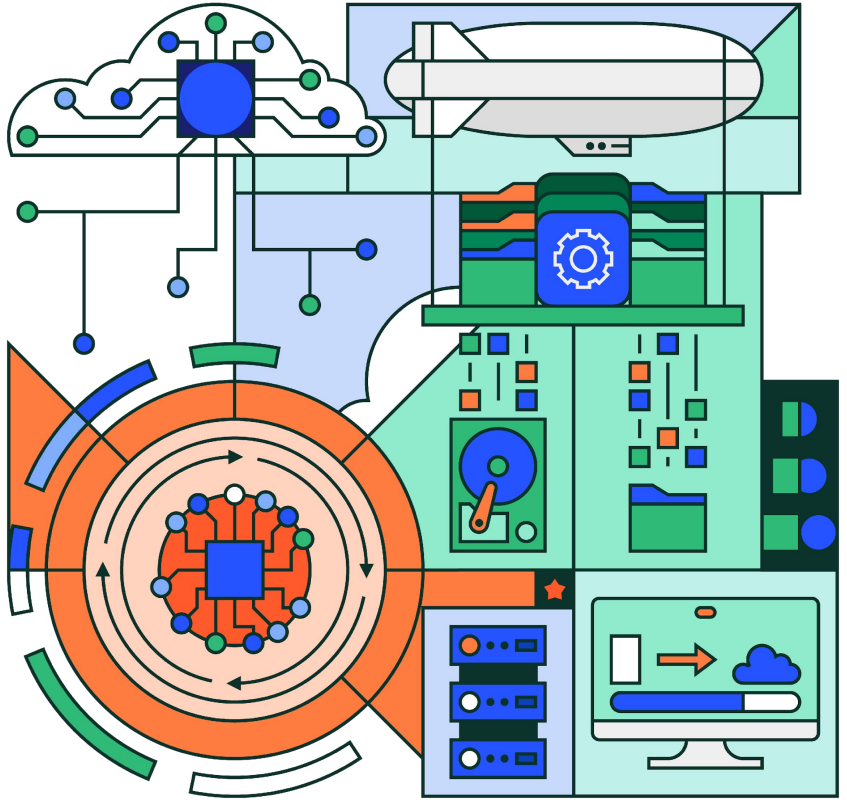


Unlocking Data Resilience and Security for Stateful Applications

Introduction

Kubernetes has rapidly become the standard platform for deploying modern applications. While initially popular for stateless workloads, organizations are increasingly leveraging Kubernetes for mission-critical, stateful applications such as databases, AI/ML, and data analytics. However, running these data-intensive applications at an enterprise scale introduces significant challenges, particularly concerning persistent storage management, data resilience, and security.

Traditional IT solutions, often designed for virtual machines (VMs) or physical servers, are ill-suited to the dynamic, distributed nature of containerized applications. This ebook explores how the joint solution from SUSE Rancher Prime and Portworx by Pure Storage addresses these critical challenges, enabling enterprises to achieve enterprise-grade business continuity and data protection for their stateful applications.



The Need for Data Resilience in Kubernetes

Running critical applications on Kubernetes demands robust data platforms that limit application downtime and data loss. Without adequate data protection and a robust disaster recovery (DR) solution, businesses face significant risks, including prolonged downtime, data loss, potential compliance violations, and severe impacts on revenue and customer trust.

Why Traditional Tools Fail Kubernetes

- **Traditional backup and disaster recovery tools were not built for Kubernetes environments.**
- Kubernetes applications are **container-based**, with components distributed across nodes, unlike traditional VM or server-based applications.
- A VM-based approach for Kubernetes clusters **slows down the recovery process** because a single VM may contain components of multiple applications but not all components for any single application.
- Simply backing up the container itself may **not capture the externally stored persistent data**, leading to inconsistent restores.

The Need for Kubernetes-Native Solutions

- A **built-for-Kubernetes solution is essential** because it is designed to inherently recognize and restore all components of an application, including persistent data and any necessary configurations.
- Effective Kubernetes data protection requires solutions that are **container-granular and application-aware**, and capable of capturing the full application, including persistent data stored externally on a volume.

Robust Data Protection and Security Features

The Portworx and SUSE Rancher Prime solution provides **comprehensive data protection and security features built specifically for Kubernetes.**

Application-Aware Backup and Restore:

- Portworx delivers **enterprise-grade, self-service Kubernetes data protection** through a point-and-click UI.
- **All data is captured**, including any pending write activity, for **consistent backups and speedy restores.**
- Protects not only your data but also **application configuration and Kubernetes objects.**
- **Container granularity** allows users to target specific applications or containers for restoration.

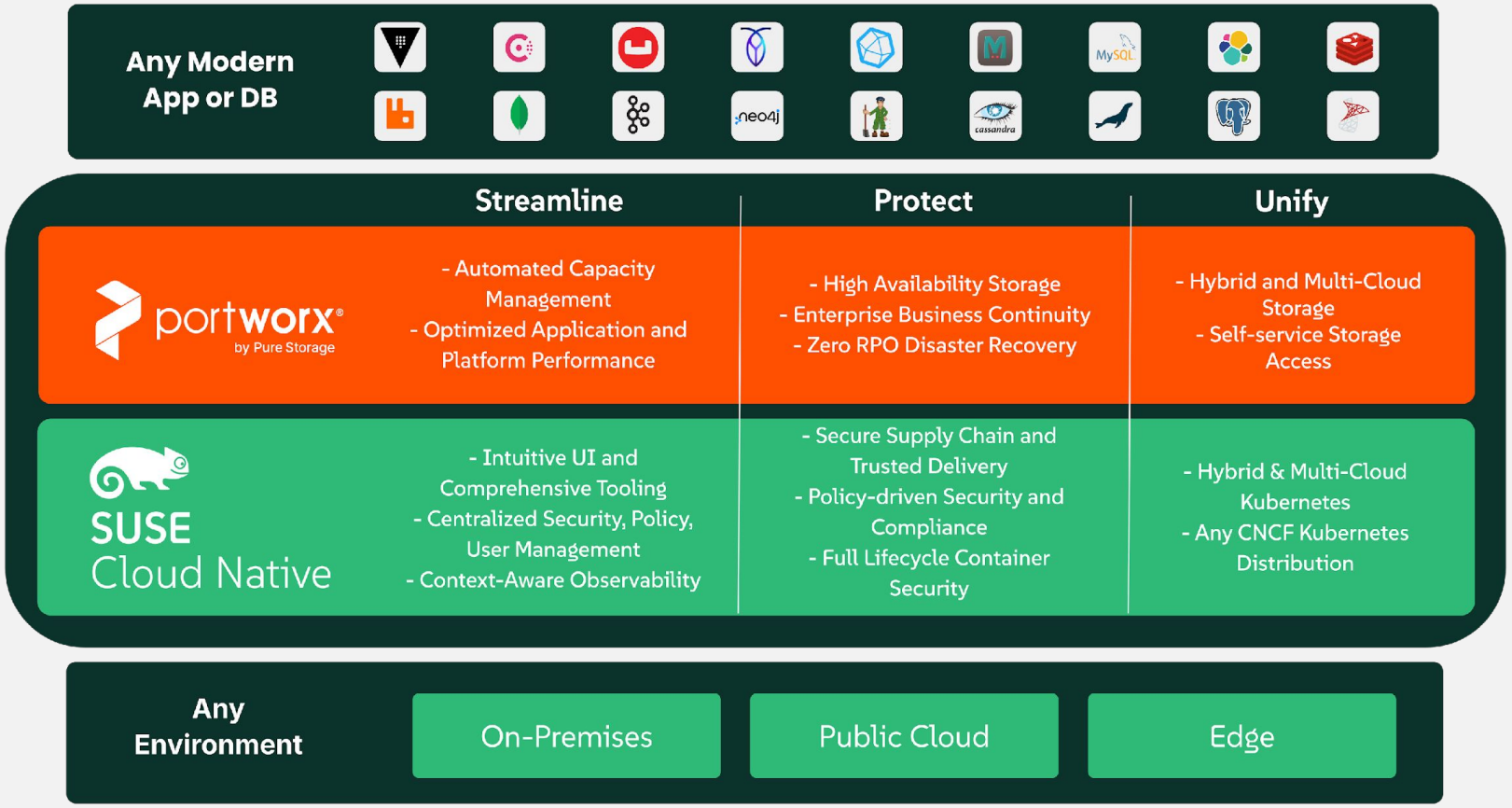
Ransomware Protection:

- Portworx provides **ransomware protection through immutability and delete protection**, preventing malware and malicious actors from altering or deleting backup data.

Enterprise-Grade Security:

- Portworx offers **enterprise-grade encryption** for secure data storage and movement, along with **data isolation and compliance features**, being SOC3 and ISO 27001 compliant.
- SUSE Rancher Prime integrates **security policies across the Kubernetes infrastructure** to prevent unauthorized access and breaches. It offers features like SLSA Level 3 compliance, on-demand SBOMs, a trusted registry, and advanced policy management.

Robust Data Protection and Security Features



Achieving High Availability and Disaster Recovery with Portworx and SUSE Rancher Prime

The joint solution is designed to deliver **enterprise-grade availability and business continuity** for containerized applications. SUSE Rancher Prime minimizes downtime risk through trusted delivery and policy-driven security, while Portworx ensures business continuity through disaster recovery that limits downtime for critical applications.

Backup vs. Disaster Recovery:

- Portworx provides **flexible disaster recovery policies that are separate from data protection capabilities.**
- While backup is a component of a holistic DR plan, **it is not the same as disaster recovery.**
- Backup and restore might suffice for lower-tier applications where some data loss is acceptable, **but mission-critical applications requiring limited downtime and no data loss must be protected by disaster recovery that replicates data at the storage level.**

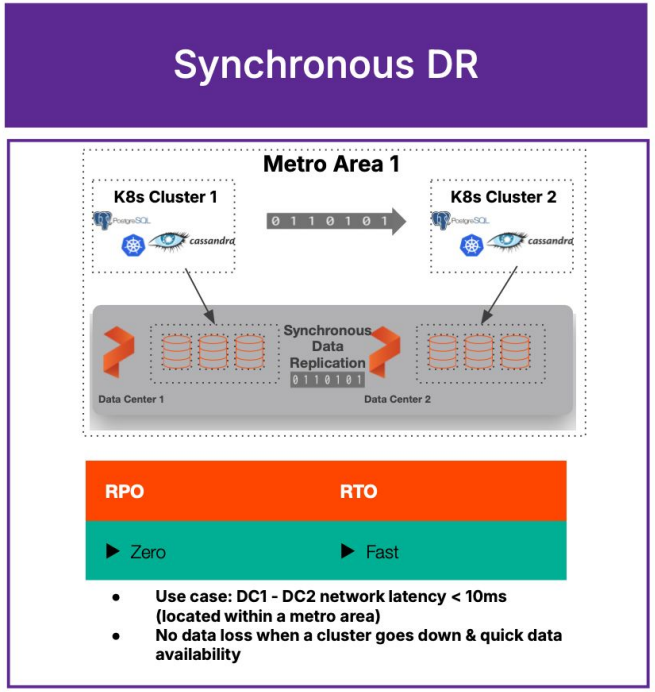
Disaster Recovery Policies: Sync DR and Async DR

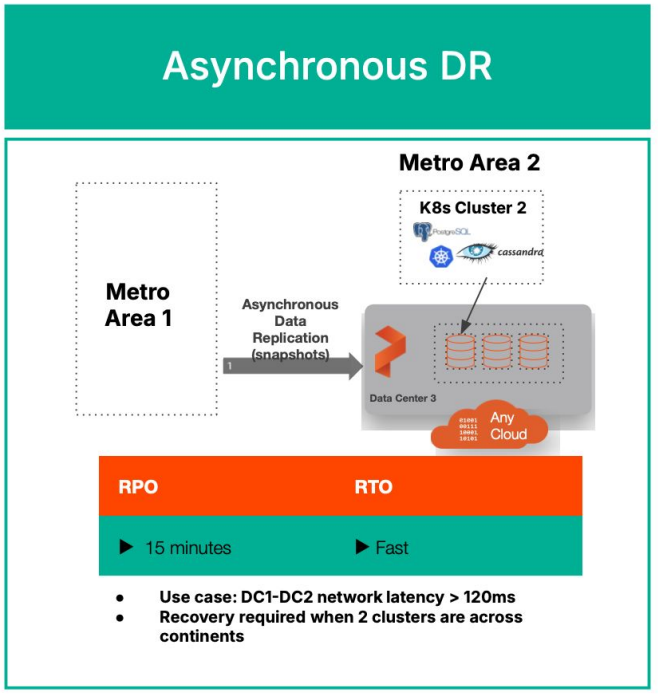
- **Synchronous DR (Sync DR):**
  - Required for **mission-critical applications where zero Recovery Point Objective (RPO) or zero data loss is required.**
  - Data and application configurations from the primary cluster are **automatically and continuously copied to a secondary cluster,** ensuring no delta between copies at any given time.
- **Asynchronous DR (Async DR):**
  - For Tier 2 or 3 applications where **some data loss is acceptable.**
  - Provides an RPO as **low as 15 minutes.**
  - Async DR, like backup/restore, will have a delta between the primary and restore copy, suitable for less stringent requirements.

Achieving High Availability and Disaster Recovery with Portworx and SUSE Rancher Prime

Effective DR Strategy:

- Defining SLAs for different application tiers and implementing appropriate DR strategies (Sync DR, Async DR, or backup/restore for lower tiers) is a **crucial part of an effective DR plan.**
- A good DR strategy must be **repeatable** and work flawlessly every time.
- **Leveraging automation for disaster recovery** helps minimize errors and streamline the process during disaster events, preventing reliance on complex manual scripts.





Conclusion

As enterprises increasingly rely on Kubernetes for their mission-critical, stateful applications, providing a stable, reliable data platform remains key. The joint solution from SUSE Rancher Prime and Portworx provides the necessary **enterprise-grade capabilities to confidently run stateful applications at scale**.

By integrating SUSE Rancher Prime for seamless Kubernetes management and Portworx for advanced container data management, organizations gain the enterprise-grade business continuity they need for their critical applications.

The solution delivers:

Flexible Disaster Recovery Policies

Synchronous DR for mission-critical applications and asynchronous DR, ensuring resilience with flexible DR policies.

Comprehensive Data Protection

Kubernetes-native application-aware and container-granular backup and restore, protecting entire applications (data, configuration, and objects).

Enterprise-Grade Security

Encryption, compliance features, Role-Based Access Control (RBAC), and robust ransomware protection with immutability, and delete protection.

Together, SUSE Rancher Prime and Portworx empower enterprises to accelerate Kubernetes application development while simplifying operations and **safeguarding their valuable data, unlocking the value of Kubernetes at an enterprise scale**.

To learn more, download the IDC Spotlight: Bridging the Kubernetes Management Gap.

SUSE Software Solutions Germany GmbH

Frankenstraße 146 90461 Nürnberg Germany

www.suse.com

For more information, contact SUSE at:

+1 800 796 3700 (U.S./Canada)

+49 (0)911-740 53-0 (Worldwide)

Thank you

© 2025 SUSE LLC. All Rights Reserved. SUSE and the SUSE logo are registered trade-marks of SUSE LLC in the United States and other countries. All third-party trademarks are the property of their respective owners.