FUTUREWEI

Container Data Protection Storage Market Analysis

Kubernetes Backup & Recovery for OceanStor®

White Paper

Tariq Nazeer

Ecosystem Development

Intelligent Storage & Computing Lab

Date: August 6, 2024

FUTUREWEI Technologies

Trademarks and Permissions

FUTUREWEI Technologies and other Futurewei® trademarks are trademarks of Futurewei® Technologies. Huawei trademarks are trademarks of Huawei Technologies Co., Ltd. All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services, and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services, and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees, or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

FUTUREWEI® TECHNOLOGIES, INC.

Boston Research Center

Address: 111 Speen Street, Suite 114
Framingham, MA 01701
United States of America

Website: http://www.futurewei.com/

Contents

Executive Summary

Over the past decade, Kubernetes® has become core to how modern computing is orchestrated and executed. Applications that once ran in Virtual Machine (VMs) on servers, data centers and the cloud are now increasing managed and run using containers. Kubernetes is the defacto opensource container orchestration platform, automating many of the manual processes involved in deploying, managing, and scaling containerized applications.

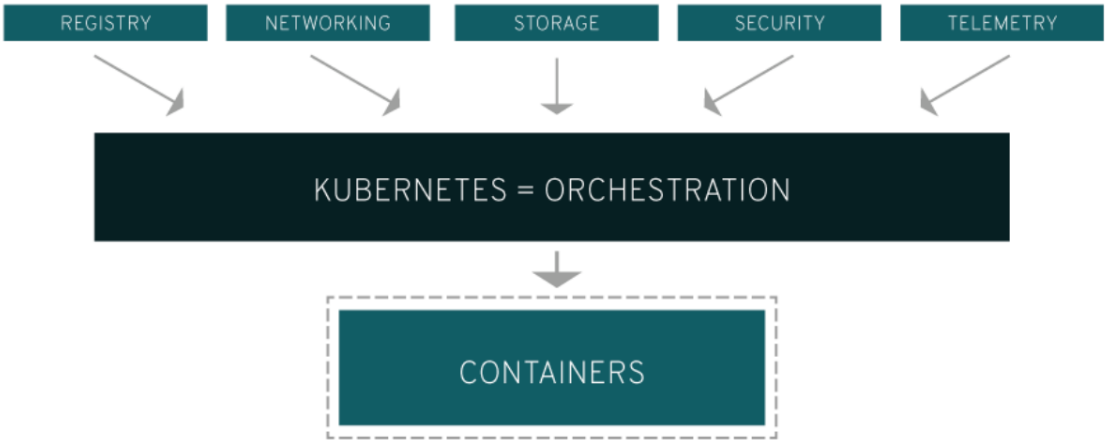
With this meteoric rise of containerized applications there has also been a massive need to handle more container data. Containerized applications bring with it massive amounts of big data - both persistent and non-persistent, and the need to back up and provide disaster recovery for this data. As a result, Container Data Backup & Recovery solutions are fast becoming a critical enterprise need.

This paper briefly examines the growth of Container and Kubernetes usage and evaluates the resulting demands on Data protection and Storage. It explores the market opportunity as well as the primary solution providers in this space; and will share publicly available analyst sources on products available to protect your Kubernetes data.

It will conclude by looking at the Kubernetes backup and recovery solutions available for Huawei's OceanStor® Storage as a specific case-in-point and how these solutions can pull thru more storage infrastructure opportunities.

1. Introduction

Kubernetes is vital for today's business. It is orchestration software that allows building of application services that span multiple containers overseeing infrastructure resources scattered across various servers to ensure that applications get the processing power, memory, storage, and networking facilities to accomplish their tasks efficiently.



Kubernetes has been taking off. This market momentum means that as organizations build more and more containerized applications using Kubernetes as their primary orchestration engine, the amount of data increases exponentially, resulting in a critical need for both storing it and protecting it.

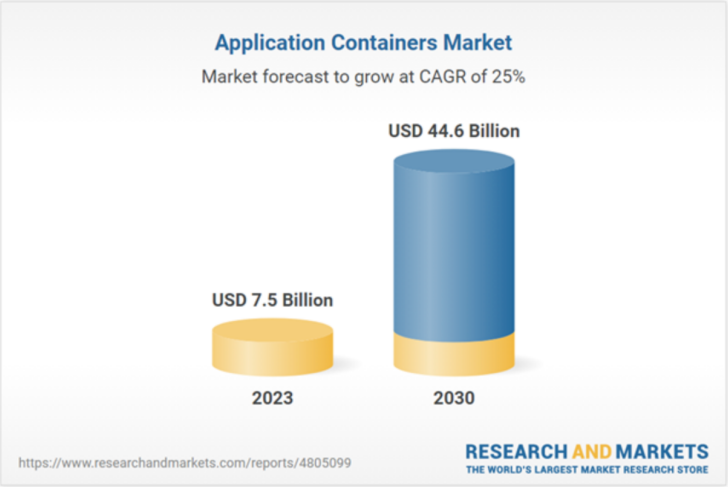
The following 3 general focus areas are becoming increasingly important for Container Data Protection:

- Encrypting Data: Ensure that data at rest and in transit is encrypted. This helps maintain confidentiality and prevents unauthorized access.
- Access Controls: Implement RBAC (Roles Based Access Controls) on data stored in containers. Limit who can read, modify, or delete data to enhance security.
- Regular Backups: Regularly backing up container data. This practice ensures data availability and resilience against failures.

This paper focuses on the Backup and Recovery of Container data and identifies robust backup and recovery storage solutions to safeguard Kubernetes environments.

2. Growth of Containers & Kubernetes

Applications are moving to containers. Research N Markets® forecasts that the application container market will grow from $7.5B in 2023 to $44.6B by 2030 at a CAGR of 25% (Research & Markets®, Container Market Report, 2024).



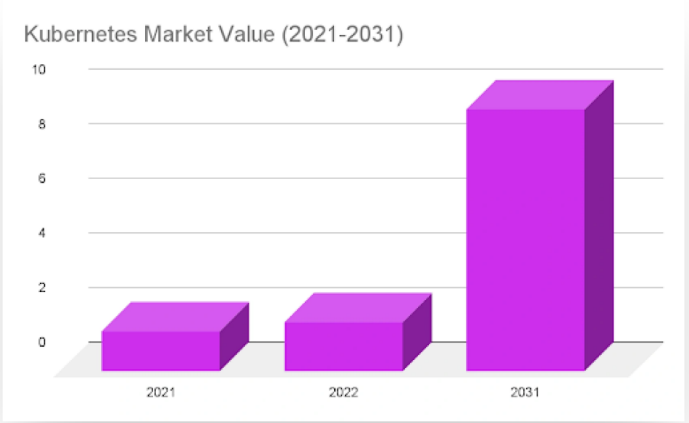
Up until recently, most organizations who were committed moving to Containers in the future, were only experimenting with containers in test, protype mode; or migrating/rebuilding non-critical legacy apps as containers. But this is changing, with Gartner® now estimating that 90%+ of global organizations to be running containerized applications in production by 2027. This is a significant increase from fewer than 40% in 2021. In addition by 2026, 20% of all enterprise production applications will run in containers—up from fewer than 10% in 2020 (CIO Brandpost®, 2021).

This proliferation of Containerized applications has resulted in enterprises needing container management software to orchestrate and manage these applications. This signaled the arrival of Kubernetes (also known as k8s or "kube") as an open-source container orchestration platform to automate many of the manual processes involved in deploying, managing, and scaling containerized applications.

According to Spectro® Cloud's, 2023 State of Production Kubernetes Report where 333 key Kubernetes Enterprise Stakeholders in the industry were surveyed, more than half (56%) of enterprises now have more than 10 Kubernetes clusters, and 69% run Kubernetes in multiple environments (across public, hybrid clouds and enterprise data centers). As many as 80% of companies expect their Kubernetes clusters to scale even further, and 85% of surveyed organizations are migrating existing VM workloads to Kubernetes.

Kubernetes is recognized as the fastest growing project in the history of Open-Source software after Linux. In 2023, Kubernetes worldwide market size was estimated at USD 1.46 billion, and is

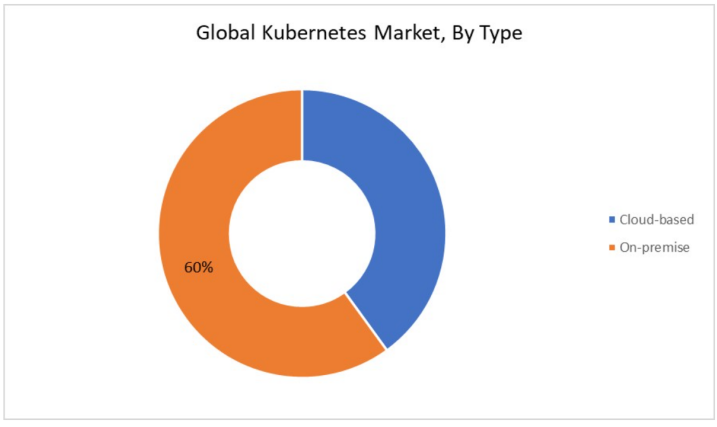
expected to increase at a compound annual growth rate (CAGR) of 23.4% to USD 9.69 billion by 2031 (Skyquestt® Kubernetes market Report, July 2024)



What all of this means, is that Kubernetes has today become the *facto* standard for orchestrating container applications.

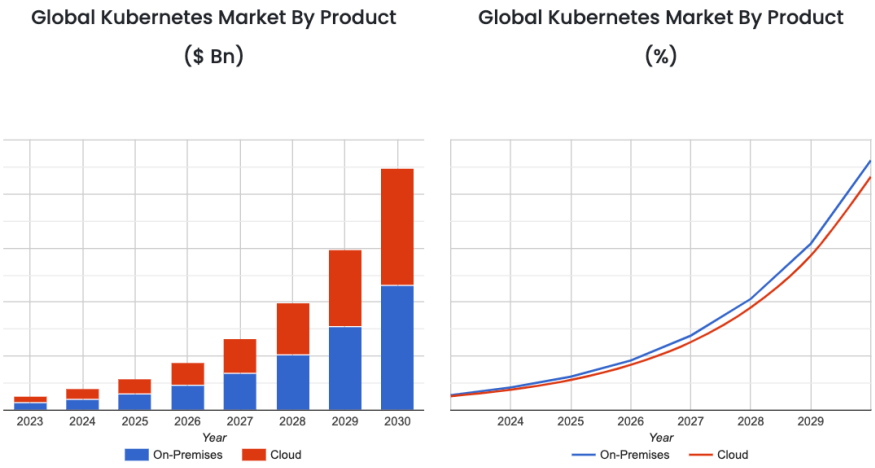
2.1 Kubernetes On-premises Vs Cloud Adoption

Most Kubernetes installations are still on-premises versus on the cloud. Per the MarketsNResearch® report, the primary reasons for this was governments' concerns over protecting sensitive data related to citizen privacy and national security. On-premises infrastructure continues to be favored as a result and this is expected to accelerate the on-premise segment's growth in the foreseeable years.



(Source: MarketsnResearch® Report, 2023)

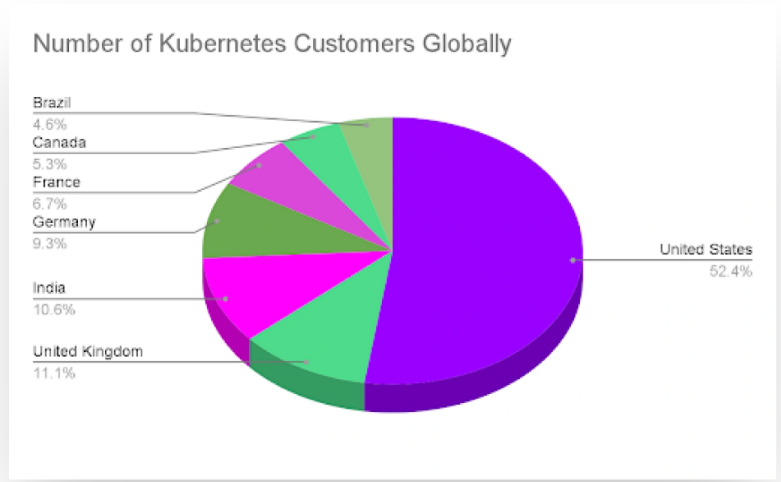
As seen in the figure below Global On-Premises Kubernetes is growing at a slightly faster pace than on the cloud, and it is expected to stay so until 2030. This puts to rest the notion that container application development is largely cloud centric.



(Source: Skyquest®, Kubernetes Market Insights Report 2024)

2.2 Kubernetes regional traction

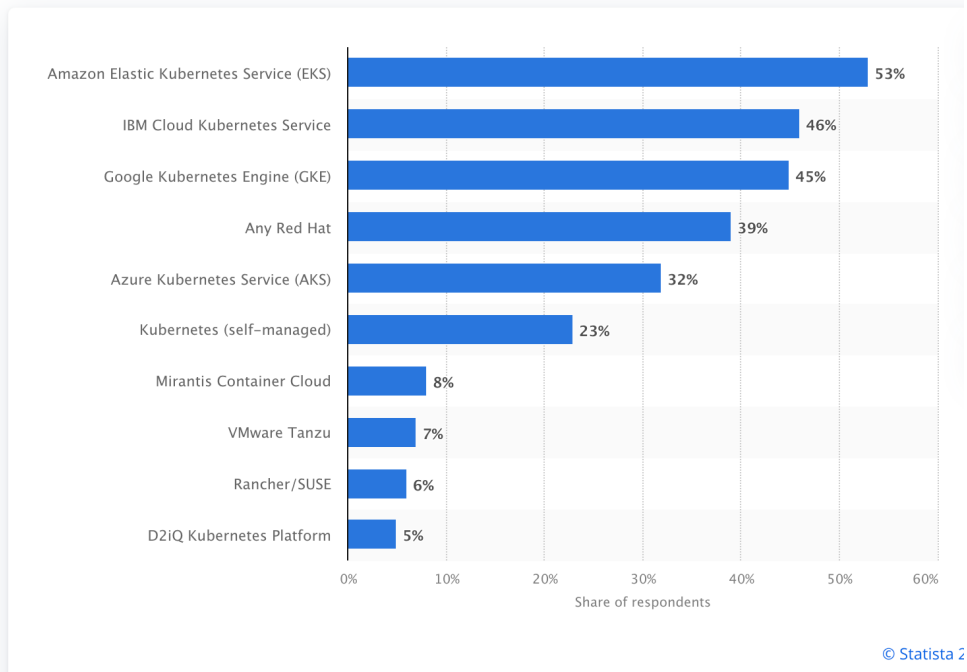
North America is the leading region for Kubernetes adoption (with over 50% of Kubernetes users based in the US). EdgeDelta® May, 2024 report on Kubernetes Adoption Statistics show that Brazil, Canada, France, Germany, India and the UK are not too far behind, with adoption rates ranging from 4.6% - 11.1%, illustrating that Kubernetes usage is quickly catching on globally.



2.3 Kubernetes Platform Vendors

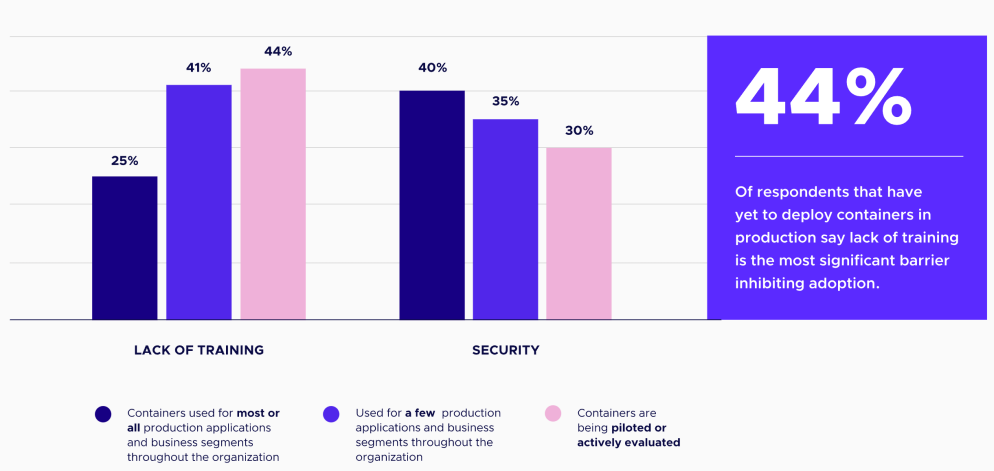
Companies such as Google®, AWS®, Microsoft®, Red Hat®, VMware®, Alibaba® and SUSE® are widely recognized as market leading vendors in this space. (see Garner® Magic Quadrant for Container Management Software, July 2023 below). But it is important to distinguish between Kubernetes vendors who largely have customers in the cloud and those that lean more towards On-premise implementations.

The Statista® June 2024 Report below ranks market share for the top Kubernetes providers. As you would expect, Google®, Amazon®, Microsoft® and IBM® dominate the off premise (cloud) installations of containers. Red Hat®, Rancher® and VMware® dominate the On-Premise installations.



2.4 Kubernetes Adoption Challenges

According to the CNCF® annual Survey Report, 2023 - there are two primary barriers getting in the way of even faster Kubernetes adoption. The primary inhibitors are training, and security/protection concerns for containerized applications (see diagram below).



Kubernetes is complex technology. Therefore, traditional infrastructure engineers who manage conventional storage say, aren't well equipment to manage container storage due to a significant skills gap. In many situations this causes resistance to container adoption and an infusion of newly skilled experts (or upskilling of existing resources) becomes a prerequisite. This

means that when identifying Container storage opportunities, it is important to often, engage with a new contact point at the company to gain access to container storage opportunities early.

The Security and Protection concerns for Containerized application are the second biggest adoption hurdle, and it's an equally big one. The primary container security concern is centered around data, and to address this space, the industry has some up with a series of tools and solutions categorized under Kubernetes Data Protection.

3. Kubernetes Storage & Data Protection

Containers are good for running multiple applications with much less overhead than virtual machines. As the use of Kubernetes grows, it is magnifying the need to address unique data storage considerations resulting from containerized applications. This requires organizations to adopt tools to help manage and maintain their infrastructure (and particularly data) to support containerized applications.

Common data storage rules don't work for containers, which are continuously created and destroyed. Therefore, container data needs to be backed-up and stored to protect against risks, such as system outages and data loss when migrating and deploying new applications.

Here are some key considerations for data protection in containers:

- Data management and protection to ensure the integrity of containerized applications with advanced data recoverability.
- Data Storage and availability management for stateful applications ranging from low-impact to mission-critical.
- A software-defined architecture to improve application performance, reduce costs, and automate key operational processes.

Providing this within a containerized environment is proving to be a challenge for most companies primarily due to a skills gap as touched upon in the earlier section. IT staff that supported applications that ran in a traditional on-premise or VM based environment are now required to become experts in managing data from applications running in a Kubernetes environment because the data tools that worked previously do not work in this new environment.

3.1 Kubernetes Backup & Recovery

Whether it be due to accidental data deletion, an "act-of-god" natural event, or a ransomware attack due to malicious activity, there are many perils threatening your organizational data. The average cost of unplanned application downtime is about half a million dollars an hour

(STCLab®, Inc. 2023 Report). Backup and Recovery is critical to ensure that your data is protected and keeps your organization's critical application running.

While the early days of containers typically meant stateless applications generally being spawned and killed as needed (with high availability built into the container architecture itself), todays container applications are mostly stateful applications.

This has brought about unique data challenges for the data backup and recovery market. To protect stateful applications that are Kubernetes-based, you need a Kubernetes-native data backup solution. You can't just retrofit legacy backup architectures into a containerized ecosystem. That said, the "3-2-1 backup rule" applies to Containers as well to ensure that your data is safe and recoverable in almost any scenario. The rule is to keep at least three (3) Copies of data, store two (2) backup copies on different storage media, and one (1) of them located offsite.

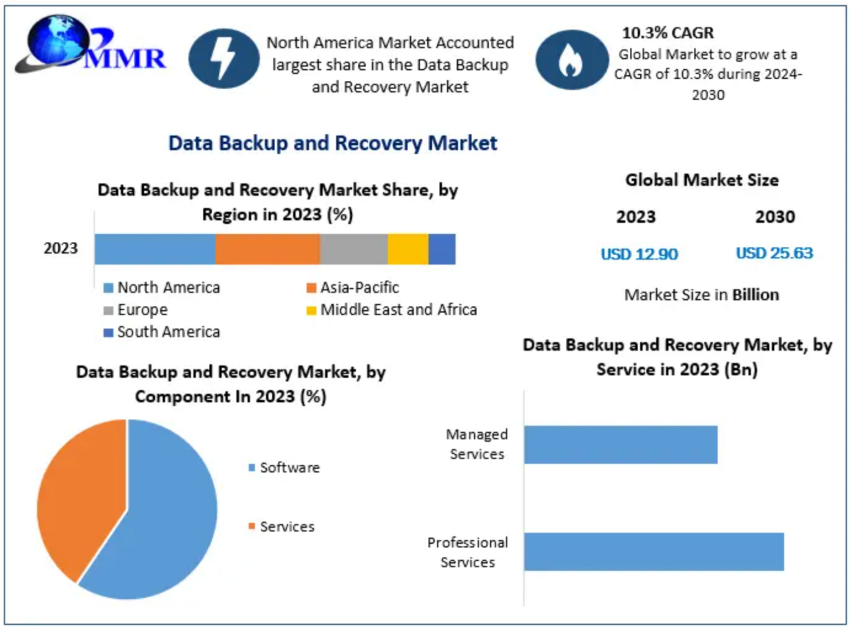
Kubernetes Backup and Recovery solutions take regular, comprehensive copies of your Kubernetes data and store it securely. If, for any reason, your Kubernetes data is lost, you can quickly restore it from the last backup. This allows for your business operations to continue, meaning that a catastrophic data loss can be resolved relatively simply.

Kubernetes backup and storage solutions address the following organizational requirements:

- Data Protection:
    - Safeguard data against accidental deletion, corruption, or cyber-attacks, thereby ensuring data integrity and security.
- Business Continuity:
    - Enables data recovery and disaster recovery capabilities, to ensure business in the face of data loss incidents.
- Optimized Storage Management:
    - Facilitate efficient storage management, for scalability and optimization of storage for a dynamically changing business environment.
- Compliance Adherence:
    - Meet regulatory compliance by protecting data for recovery in accordance with mandated guidelines.

4. Backup & Recovery Market Opportunity

The Backup & Recovery software and services market opportunity was $12.9B in 2023, and expected to grow at 10.3% CAGR to $25.63B by 2030 (source: MaximizeMarketResearch®, 2023 - see figures below). While North America shows up as the largest market, Asia Pacific, Europe, Middle East & Africa and South America all account for significant market opportunity.



Data Backup and Recovery Market			
Report Coverage	Details		
Base Year:	2023	**Forecast Period:**	2024-2030
Historical Data:	2018 to 2023	**Market Size in 2023:**	US $ 12.90 Bn.
Forecast Period 2024 to 2030 CAGR:	10.3%	**Market Size in 2030:**	US $ 25.63 Bn.
Segments Covered:	by Component	Software Services	
	by Service	Professional Services Managed Services	
	by Vertical	BFSI IT and Telecommunications Retail Government and Public Sector Healthcare Media and Entertainment Manufacturing Others	

The Backup & Recovery Software market is large and established, and growing fast as more and more data is created. With Container and Kubernetes applications taking off and generating even more data, the Kubernetes Backup & Recovery market opportunity is also substantial.

4.1 Container Backup & Recovery Storage Market Opportunity

The Kubernetes Backup & Recovery Software Market is estimated by industry analysts (direct sources not publicly available for free) to be about 8% of the overall Backup & Recovery software/services market and expected to grow even more rapidly than the 10.3% CAGR listed for the general Backup & Recovery software market. This approximately, $1B Kubernetes Backup and Recovery software market, opens a promising revenue opportunity for Kubernetes Backup and Recovery Storage both on the cloud as well as on-premises in traditional data centers.

Not every organization doing container data backup is using backup & recovery software. In fact, most don't. That is because traditional backup and recovery software doesn't translate well for container applications. That said, speaking with both vendors, as well as storage industry experts - assuming a storage dedupe rate between 5:1 and 10:1 (based on application use case and storage TB volumes being backed up), the Container Kubernetes Backup & Recovery Storage hardware Market opportunity can be up to a $500M market opportunity today, growing to over a $1B by 2026.

The next section in this white paper, looks at the top Kubernetes Data Protection vendors building backup and recovery software for Kubernetes and captures the top solutions available in the industry today.

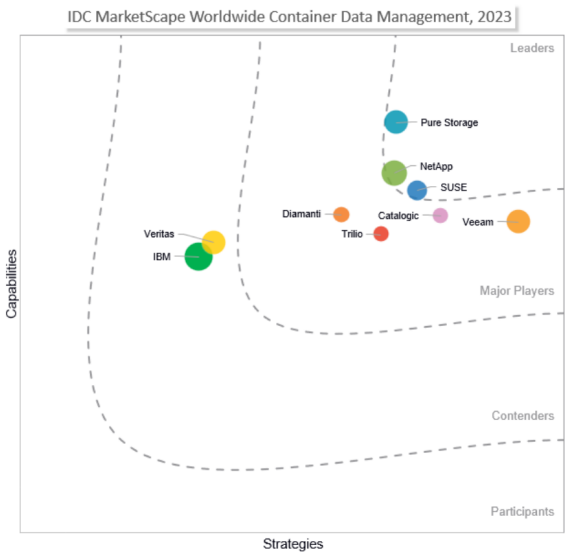
4.2 Top Kubernetes Data Protection and Management Vendors

IDC® published a report last year in 2023 on Container Data Management Market Leaders. These are vendors who provide tools and capabilities for storage and data protection including disaster tolerance, backup & recovery, including Containerized application data protection.

Generally, Open Source Velero is the starting point for container data protection in most companies. But when these companies scale beyond the point where Velero can reasonably function, specialized tools become a necessity.

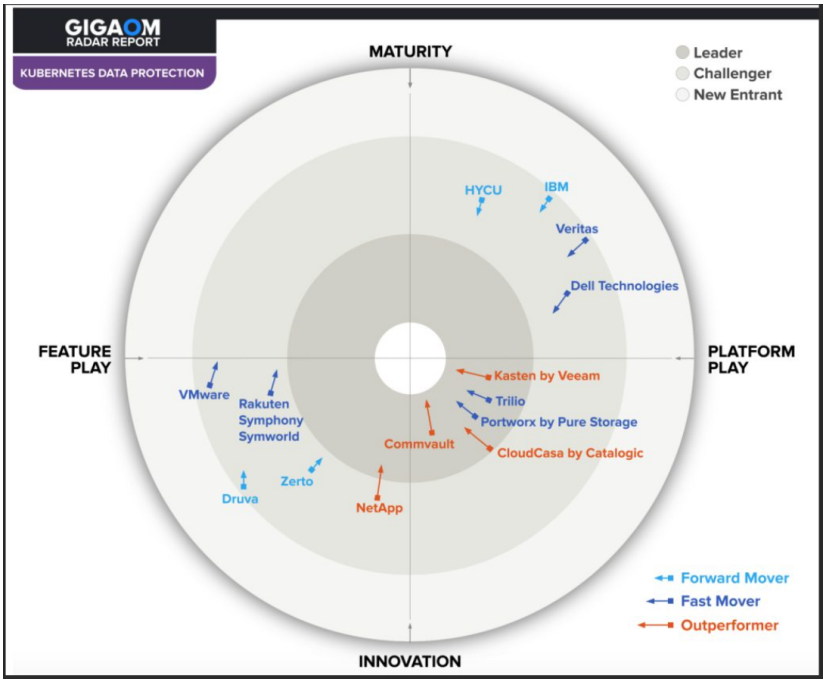
The top 6 vendors with market momentum in this space are Pure Storage® (with Portworx®), SUSE® (with Rancher®), NetApp®, Catalogic®, Veeam® and Trilio®. (IDC Marketscape® Worldwide Container Data Management, 2023)

IDC MarketScape Worldwide Container Data Management Vendor Assessment



Source: IDC, 2023

Outside of IDC, GIGAOM's 2023 Radar Report ranks the top Kubernetes Data protection solutions classified as the industry's outperformers and fast movers. Kasten (by Veeam), Commvault, CloudCasa (by Catalogic) and NetApp®, Trilio® and Portworx® (by Pure Storage®) again show up as the top 6 players.

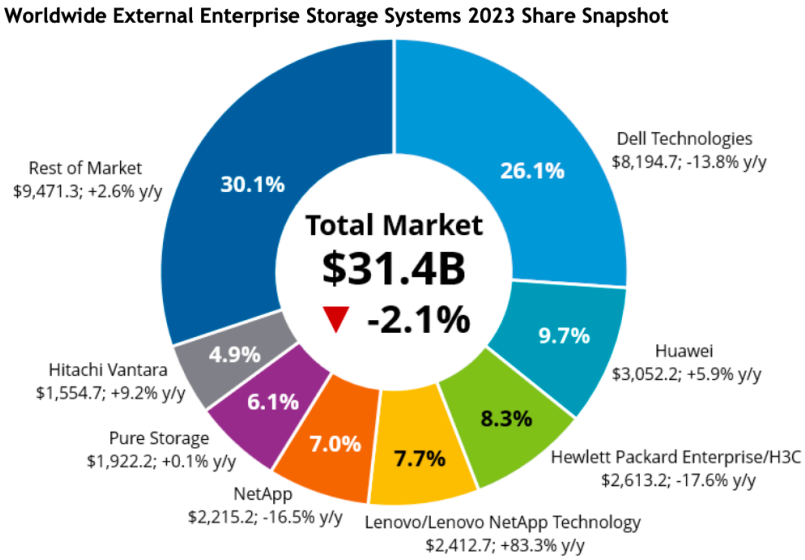


Many of these Data Protection vendors target supporting the major cloud providers as well as Red Hat OpenShift® and SUSE Rancher® as the primary Kubernetes platforms of choice.

5. Kubernetes Backup & Recovery Solutions for OceanStor® Storage

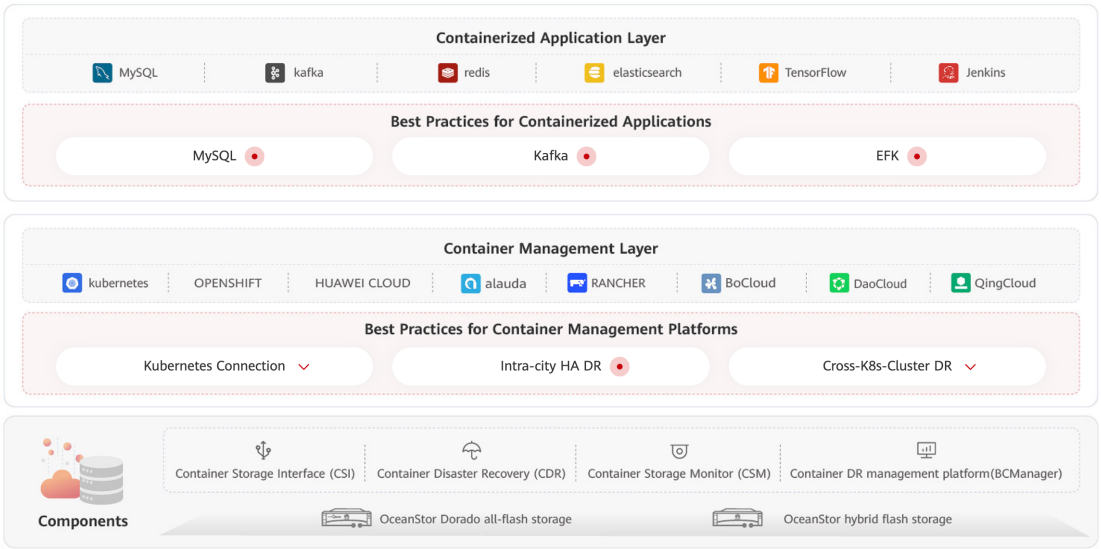
OceanStor® Storage is the 2nd largest external storage brand in the world. IDC's market data from 2023, shows that while Dell Technologies® revenue shrank year-year last year by -13.8% to approximately 26.1% market share, Huawei's OceanStor® storage grew by almost 6% y/y to 9.7% market share globally. (see figure below).

As a leading Storage brand, organizations that are quickly adopting container and Kubernetes technologies are looking to back up their data on OceanStor storage.



5.1 Huawei OceanStor® Kubernetes Data Protection Solutions

Huawei® works with Container Ecosystem Partners to provide state-of-the-art Kubernetes Data Protection Storage solutions, delivering optimal performance, simplified operations and maintenance (O&M), easy sharing, and robust reliability. (Source: [Huawei® Container Solution]). OceanStor® Storage can integrate to the mainstream container management platforms, including Kubernetes, OpenShift®, VMware Tanzu®, Rancher®, Cloud Container Engine (CCE), DaoCloud®, and Alauda® through its standard compliant CSI and CDR driver plugins to provide backup and recovery and robust data protection©.

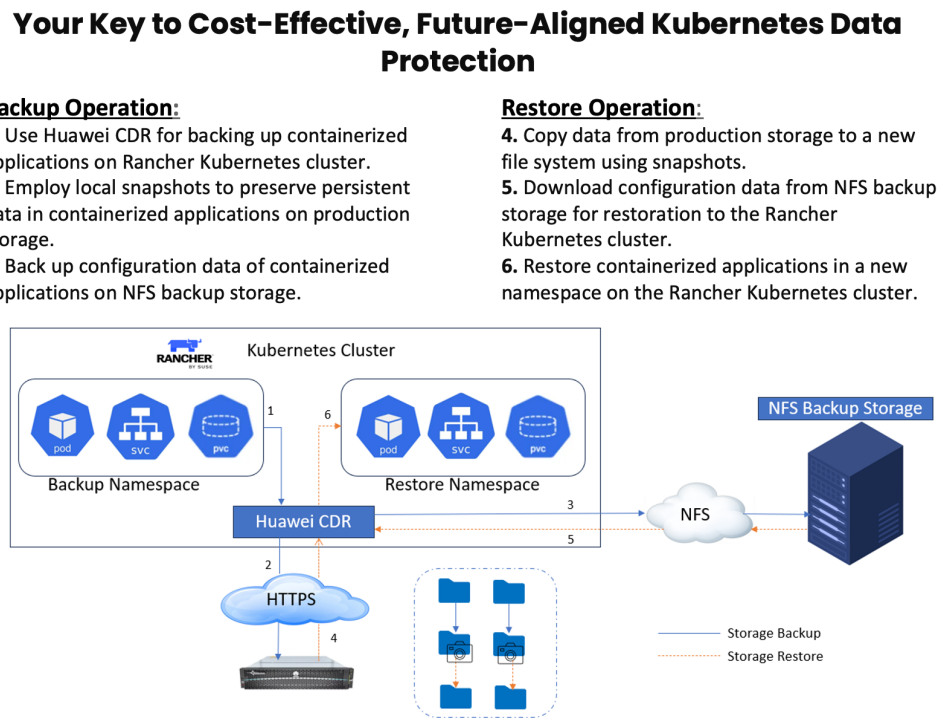


Additionally, the following two partners have conducted additional certification testing and validation to provide a fully end to end supported Kubernetes Data Protection solution on Huawei OceanStor® storage.

5.2 SUSE Rancher® for OceanStor®

The Kubernetes Benchmark Report®, 2024 lists SUSE's Rancher® as a market leading Kubernetes platform that is 2nd only to Red Hat OpenShift® in market share (when removing the Kubernetes cloud platform vendors from consideration). It is well regarded for its ease of use, and in addressing both operational and security challenges when managing multiple Kubernetes clusters, and for providing an extensive tool set for executing container workloads.

SUSE's Rancher® platform supports OceanStor® storage for Container Data Protection, Backup & Recovery by using Huawei's® Container Storage Interface (CSI) plugin to ensure secure storage. It also leverages the Container Disaster Recovery (CDR) plugin to protect against data loss due to backup processes, node failures, storage failures, and cluster failures. Rancher® with Huawei's® CDR plugin creates a robust solution for container backup and disaster recovery (source: SUSE® Partner Certification & Solutions Catalog).

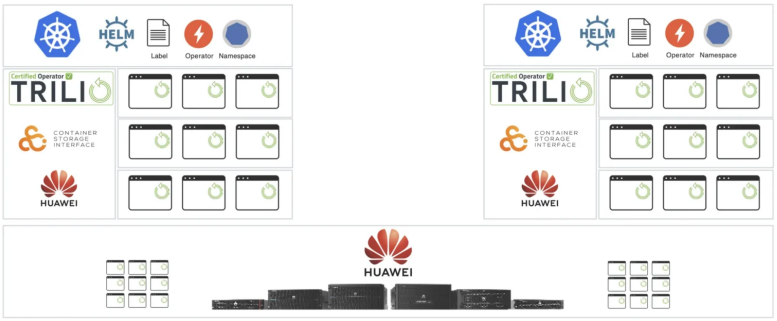


5.3 Trilio® for OceanStor®

Trilio®, provides for reliable, cost- effective, protection and recovery for Kubernetes environments for Huawei's® market leading OceanStor® storage products. It allows applications and data to move between siloed environments easily and seamlessly. The Trilio® Intelligent Recovery platform is specifically designed to provide a consistent experience across private, public, and hybrid clouds. Trilio® protects and intelligently recovers thousands of applications spanning multiple clouds, clusters and containers while capturing and restoring variations of network and storage configurations (Source: [Trilio® for OceanStor® offering])

Huawei OceanStor Dorado with Trilio

Trilio is the exclusive certified Kubernetes partner for backup and recovery using Huawei OceanStor Dorado storage. With Trilio and Huawei, users can deploy any distribution of Kubernetes, including OpenShift, Tanzu and Rancher, and provide ransomware recovery on Huawei's award winning scale-out storage platform.



Key Benefits

- **Reliable:** Certified for Huawei's Award Winning Storage
- **Performance & Value:** Protect and store Cloud Native workloads in any OceanStor Dorado environment
- **Secure:** 99.9% Ransomware Detection Accuracy
- **Scale Economically:** 56% Space Saving, 1.09 W/TB Power Consumption
- **Flexible:** Airgap, Production, Backup and Archive

6. Conclusion

Most enterprise application today are being built using Containers, and Kubernetes is the defacto orchestration engine for these applications. Kubernetes managed applications are generating massive new amounts of organizational data that needs to be protected. This requires new tools and capabilities that are different from those used for protecting traditional applications.

Kubernetes Data Protection software and services is about a $1B market that is growing at double digit CAGR. This is creating a growing demand for Backup and Recovery Data protection storage hardware, that is an attractive growth opportunity for Data Storage companies. Even with efficient storage dedupe technology, experts predict that consumers are spending between $500m and $1B to on Kubernetes Backup and Recovery storage.

The primary storage hardware vendors are addressing this market opportunity by bringing to market, solutions of their own or partnering with the world's leading Kubernetes data protection software vendors to sell and integrated joint solution.

Huawei's OceanStor® storage addresses this space by having its storage integrate to all of the mainstream container management platforms, including Kubernetes®, OpenShift®, VMware Tanzu®, Rancher®, Cloud Container Engine® (CCE), DaoCloud®, and Alauda® through its standards compliant CSI and CDR driver plugins for Container Data Protection. Additionally, both SUSE Rancher® and Trilio® provide an end-to-end, tested, validated, supported Kubernetes Backup and Recovery offerings for OceanStor storage.

7. References

[1] Research & Markets®, Container Market Report, 2024

[2] CIO Brandpost®, 2021

[3] 2023 State of Production Kubernetes Report®

[4] Skyquestt Kubernetes market Report®, July 2024

[5] MarketsNResearch Report®, 2023

[6] Skyquest®, Kubernetes Market Insights Report, 2024

[7] EdgeDelta® Report, May, 2024

[8] Garner® Magic Quadrant for Container Management Software, July 2023

[9] Statista Report®, June 2024

[10] CNCF® annual Survey Report, 2023

[11] STCLab, Inc®. Report, 2023

[12] MaximizeMarketResearch® Report, 2023

[13] IDC Marketscape® Worldwide Container Data Management, 2023

[14] GIGAOM® Radar Report on Kubernetes Data Protection, 2023

[15] IDC® Worldwide External Enterprise Storage Report, 2023

[16] Huawei® Container Solution

[17] Kubernetes Benchmark Report®, 2024

[18] SUSE® Partner Certification & Solutions Catalog

[19] Trilio® for OceanStor® offering