IDC MarketScape

IDC MarketScape: Worldwide Container Data and Infrastructure Management Software 2026 Vendor Assessment

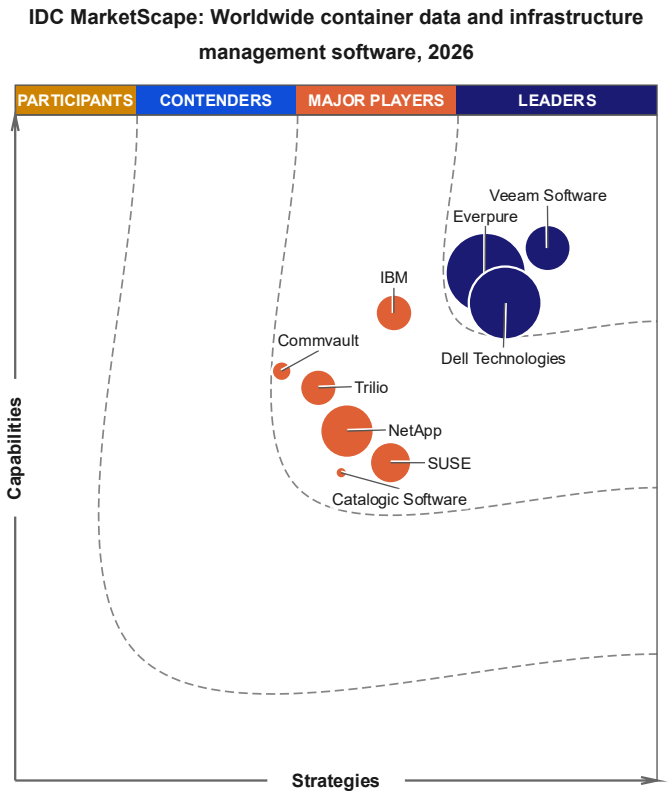
Johnny Yu

THIS EXCERPT FEATURES EVERPURE AS A LEADER

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape: Worldwide container data and infrastructure management software vendor assessment



Source: IDC, 2026

November 2026, IDC #US52039825e

Please see the Appendix for detailed methodology, market definition, and scoring criteria.

ABOUT THIS EXCERPT

The content for this excerpt was taken directly from Worldwide Container Data and Infrastructure Management Software 2026 Vendor Assessment (Doc # US52039825).

IDC OPINION

As organizations increasingly adopt Kubernetes to enable faster application delivery and to support agentic AI workloads, they must also adopt tools that can help them manage and maintain the infrastructure that supports containerized applications.

Container data and infrastructure management software provides this support. These tools are what allow organizations to perform the same support tasks for applications running in containers as they do for applications running on physical storage and virtual machines (VMs). Products in this market include data protection, storage provisioning, disaster recovery (DR), security, and data governance for containers.

However, the challenges customers face have moved beyond simply achieving feature parity between container and non-container environments. Many organizations are migrating VM-based applications to Kubernetes and using KubeVirt to run those applications in Kubernetes environments. They will need tools that can facilitate this migration and ensure their applications are still properly protected, secured, and supported after replatforming.

In addition, IDC research has found that on average, 58% of applications running in containers are considered business critical, mission critical, or life critical. That number is poised to grow as agentic AI becomes more widely adopted. With criticality comes greater demand for preventing application downtime, making cyber-resilience a high priority in this market.

Finally, agentic AI deployment and Kubernetes adoption are closely linked. It is therefore important for customers to find the right software tools that align with their goals and milestones as their Kubernetes estate grows. The ability to scale and address agentic AI data governance challenges will be important customer considerations as this market evolves.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

Vendors qualify for this IDC MarketScape assessment if they can address at least three of the following core capabilities, but container data protection and cyber-resilience must be one of them. In addition, data protection must be integrated with the container orchestration platforms hosting applications — it shouldn't just protect the storage environments hosting containerized applications and data:

- **Container data protection and cyber-resilience.** Solutions can provide application-consistent backup and recovery, immutability, air gapping, anomaly detection, and clean room recovery for containerized workloads and their associated configuration and state.
- **Container-native storage and data services.** Solutions can provide persistent storage, snapshots, clones, replication, encryption, and quality of service delivered through orchestrator-native primitives and addressable at application-level granularity.
- **Application and data mobility.** Solutions can provide cross-cluster, cross-platform, and hybrid movement of applications and their data in support of disaster recovery, workload placement, cloud repatriation, and test and development refresh.
- **Governance, sovereignty, and compliance.** Solutions can provide data residency, encryption key control, audit, and regulatory alignment for containerized environments, including alignment with regional sovereignty and operational resilience frameworks.

Additional inclusion criteria include the following:

- Qualifying vendor's products must be built from the ground up to be focused on container environments. Products that are primarily built and used for virtual or physical environments that have been updated to extend their capabilities to containers or require a plug-in or add-on to work with containers are excluded from this study.
- Qualifying vendor's products are available standalone and not offered solely as a feature or component of another product.
- Qualifying vendor's products have been generally available for the past 12 months.

ADVICE FOR TECHNOLOGY BUYERS

IDC does not expect any one of the vendors' products to be the perfect solution for every organization. Container data and infrastructure management software vendors differentiate themselves in a variety of ways, and a solution that is perfect for one organization could be suboptimal for another.

The following are some key points to consider when evaluating the right vendor for your organization:

- Consider your own organization's level of container and Kubernetes expertise. Some vendors have extremely robust and highly configurable products, but IT teams need enough technical knowledge and infrastructure familiarity to take advantage of these advanced features. Some vendors provide container and Kubernetes help beyond product support, such as by offering consulting services or fostering a user community via forums and official Discord and Slack channels.
- Note that for many organizations, moving to VMs-on-Kubernetes architecture is a multiyear migration. This platform transition typically involves adopting new data protection, security, and governance tools as well as reskilling IT team members. Some vendors in this market offer features and capabilities specifically to aid this transition and are highly worth considering for organizations that are trying to reduce their dependency on virtualization platforms they are deeply embedded in.
- Plan for your Kubernetes environment to scale, especially if your container adoption is driven by agentic AI deployment. When evaluating any container data and infrastructure management solution, it is therefore important to pay attention to how its performance and cost will change after two or three years of growth.
- Consider cyber-resilience and AI data governance for applications running in Kubernetes. As the criticality of these applications increases, the risk of sensitive data being exfiltrated by malicious attackers or exposed by poorly configured AI agents grows with it.

This IDC MarketScape highlights what we believe are the most important criteria when evaluating a container data and infrastructure management software product, but it is not intended to be a buyer's guide. Instead, readers should use this study to identify strengths, weaknesses, and key points of differentiation between products in this market in order to narrow down the list of vendors that work best for them.

VENDOR SUMMARY PROFILES

This section briefly explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of each vendor's strengths and challenges.

Everpure

IDC has positioned Everpure in the Leaders category in this 2026 IDC MarketScape for container data and infrastructure management software.

Everpure Inc., headquartered in Santa Clara, California, was founded in 2009 as Pure Storage and adopted the Everpure name on February 23, 2026. It acquired Portworx, a software-defined data management and storage platform built specifically for containerized applications and Kubernetes, in 2020.

Portworx is Kubernetes-native software that runs as containers on the customer's cluster and aggregates node-local disks, cloud block storage, and external arrays into shared storage pools. Product packages include Portworx Enterprise for mixed container and VM estates, Portworx Modern Virtualization for VM-only KubeVirt deployments, and Portworx Edge for clusters of up to five nodes. Backup and Disaster Recovery are included in select packages and can also be purchased standalone. Licensing is per node on subscription or per node-hour on pay-as-you-go terms, and the product is listed in the AWS, Azure, and Google Cloud marketplaces.

Management runs through Kubernetes constructs as well as a UI, API, and the pxctl command line. The Portworx Operator reconciles a StorageCluster custom resource for installation and upgrades; StorageClass parameters set replication, encryption, I/O priority, and placement; and Stork-managed custom resources handle snapshots, schedules, migration, and backup, so policies can be reviewed in Git and applied through Argo CD or Flux. Autopilot adds rule-driven automation such as growing volumes and rebalancing pools.

The platform is delivered across more than 20 orchestration platforms, including upstream Kubernetes, Red Hat OpenShift and OpenShift Virtualization, SUSE Rancher and SUSE Virtualization, VMware Tanzu and vSphere Kubernetes Service, Spectro Cloud, Mirantis, and the managed services EKS, AKS, GKE, IKS, and OKE. Everpure FlashArray and FlashBlade integrate natively, and third-party arrays, direct-attached disks, and cloud block storage are supported as back ends.

Data protection is offered at application and namespace levels through Portworx Backup. Portworx Backup captures persistent data along with Kubernetes objects, custom resources, and configuration; uses pre- and post-execution rules for application consistency; and protects KubeVirt VMs with file system–consistent backups and file-level restore. It supports immutable targets through Object Lock to enable ransomware protection.

Portworx DR provides synchronous zero-RPO replication for clusters in the same metro region with latency below roughly 10ms, and asynchronous replication with RPOs of 15+ minutes for distant clusters. Failover and failback are driven from a graphical interface or through Kubernetes manifests and pipelines. Security features include token-based RBAC, per-cluster and per-volume encryption with customer-held keys in HashiCorp Vault, cloud key services, or Kubernetes Secrets.

Everpure serves platform engineering teams, VM administrators moving from VMware to Kubernetes-based virtualization, and organizations running AI workloads on Kubernetes. For VMs, the company offers live migration, ReadWriteMany (RWX) block storage tuned for virtual machines, and a console-embedded experience through OpenShift, SUSE, and Spectro Cloud plug-ins that manage VMs, containers, or both. For AI, KV cache offload extends GPU memory for inference workloads, and Pure1 AI Copilot supports natural language queries of cluster health and capacity.

Everpure's partnerships include joint reference architectures with Red Hat, SUSE, and Spectro Cloud, a turnkey edge appliance announced with Red Hat, cloud marketplace listings, and integrations with Prometheus, Grafana, Datadog, and Red Hat Advanced Cluster Management. Security and cyber-recovery integrations include CrowdStrike, Varonis, Superna, Rubrik, and Commvault. Portworx is sold by a cloud-native specialist team working with Everpure account teams, resellers, global systems integrators, managed service providers, and cloud marketplaces.

Strengths

- **Storage-agnostic portability:** Portworx pools local disks, cloud storage, and storage arrays across more than 20 orchestration platforms. StorageClass parameters, operator-reconciled resources, and Stork custom resources keep policy in Git, while migration and restore allow for movement of applications between clusters, clouds, and storage vendors without rebuilding data services. This lets platform teams standardize on one data layer even when clusters, clouds, and arrays differ.
- **Unified resilience:** Application-aware backup, asynchronous DR, and synchronous zero-RPO metro replication operate on a single platform. Backups capture custom resources and KubeVirt VMs, support Object Lock immutability, and allow file-level restore, while volume placement strategies and customer-held encryption keys support residency requirements. Application-consistent restores to alternate clusters also support recovery testing without impacting production.
- **VM and AI readiness:** Portworx reduces the Kubernetes expertise needed with one data platform for VM and AI workloads. For VMs, live migration via RWX shared block volumes, console plug-ins, and dedicated guides help VM administrators move applications to KubeVirt from virtualization platforms. For AI, KV cache offload extends GPU memory, and Pure1 AI Copilot gives AI operators natural language visibility into fleet health and capacity.

Challenges

- **BC/DR considerations:** Failover is operator initiated through the interface or manifests, and policy-based automatic failover is not yet a feature. In addition, asynchronous RPOs start at 15 minutes, which may not fit buyers with strict

availability targets. Buyers can still use synchronous metro replication within latency limits and script pipeline-driven failover.

- **Operational complexity:** Managing and troubleshooting Portworx benefits from a deep understanding of distributed storage mechanics as well as Kubernetes expertise. Organizations that are deeply embedded in virtualization platforms or have little Kubernetes skill may struggle to use Portworx's features to their full potential. Everpure offers professional services and free training to help address Kubernetes maturity issues.

Consider Everpure when

Everpure's Portworx offering is a good fit for enterprises running mission-critical VMs, containerized applications, or AI workloads on Kubernetes across multiple distributions or mixed storage that want integrated backup and DR. Everpure is actively developing virtualization platform feature parity into Portworx. Organizations interested in a seamless transition from VMs to containers should consider Portworx.

APPENDIX

Reading an IDC MarketScape graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under this category, IDC analysts will look at how well a vendor is building and delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis, or strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the market share of each individual vendor within the specific market segment being assessed. For this IDC MarketScape, IDC determined the vendor market size using IDC's Worldwide Semiannual Software Tracker, which represents an estimate of each vendor's 2025 container data and infrastructure management software revenue.

IDC MarketScape methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

Market definition

The container data and infrastructure management software market comprises the products and services that provide persistent storage, data protection, cyber-resilience, mobility, and governance for stateful applications running on container orchestration platforms. In 2026, these platforms are overwhelmingly based on or derived from Kubernetes, spanning upstream distributions, commercial enterprise distributions, managed cloud services, and edge-optimized variants. Offerings in this market deliver their data management control plane through orchestrator-native constructs and operate at the application, namespace, and orchestrator-native grouping level rather than solely at the volume level.

The market draws suppliers from three archetypes: infrastructure incumbents extending established portfolios into containerized environments, data protection and management specialists adapting their offerings to orchestrator-native contexts, and pure-play vendors built from inception around containerized workloads. Vendors with adjacent capabilities such as enterprise data protection without orchestrator-native integration, software-defined storage without orchestrator-native data services, container security posture management, and general-purpose data governance platforms fall outside this scope.

Vendors' products within this market consist of four core capabilities:

- **Container data protection and cyber-resilience.** Solutions can provide application-consistent backup and recovery, immutability, air gapping, anomaly detection, and clean room recovery for containerized workloads and their associated configuration and state.
- **Container-native storage and data services.** Solutions can provide persistent storage, snapshots, clones, replication, encryption, and quality of service delivered through orchestrator-native primitives and addressable at application-level granularity.

- **Application and data mobility.** Solutions can provide cross-cluster, cross-platform, and hybrid movement of applications and their data in support of disaster recovery, workload placement, cloud repatriation, and test and development refresh.
- **Governance, sovereignty, and compliance.** Solutions can provide data residency, encryption key control, audit, and regulatory alignment for containerized environments, including alignment with regional sovereignty and operational resilience frameworks.

LEARN MORE

Related research

- *Agentic AI Poses New Data Resilience Risks* (IDC #US54594526, June 2026)
- *IDC Survey Spotlight: Where Is IT Spending Increasing the Most?* (IDC #US54298926, March 2026)
- *IDC PeerScape: Peer Insights for Transitioning to Modern Virtualization* (IDC #US53148625, December 2025)

Synopsis

This IDC study is an evaluation of prominent container data and infrastructure management software vendors on a worldwide basis. While it offers details on each vendor's capabilities and offerings, it is not meant to be a buyer's guide. Instead, this evaluation is intended to help IT leaders differentiate between vendor solutions and narrow down candidates that align with their stage of Kubernetes adoption, level of Kubernetes expertise, agentic AI workload deployment, and long-term goals of their application infrastructure.

"Many organizations are accelerating their agentic AI deployment, which is also driving them toward container and Kubernetes infrastructure," said Johnny Yu, research manager, Infrastructure Software Platforms at IDC. "The result is greater demand for container data and infrastructure management software to not only protect Kubernetes application data but also bring in elements of AI data governance and control."

ABOUT IDC

International Data Corporation (IDC) is the premier global market intelligence, data, and events provider for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight help IT professionals, business executives, and the investment community make fact-based technology decisions and achieve their key business objectives.

Global headquarters

One Beacon Street
Suite 33100
Boston, MA 02108
USA
508.872.8200
X: @IDC
blogs.idc.com
www.idc.com

Copyright and trademark notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, and web conference and conference event proceedings. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit idc.com/about/offices. Please contact IDC at customerservice@idc.com for information on additional copies, web rights, or applying the price of this document toward the purchase of an IDC service.

Copyright 2026 IDC. Reproduction is forbidden unless authorized. All rights reserved.