



# PROTECT YOUR CONTAINERS WITH HPE AND COHESITY

Flexible, granular, and hybrid protection for enterprise-scale containers

The global application container market size was valued at USD 1.5 billion in 2018 and is expected to reach USD 8.2 billion by 2025, according to a new report by Grand View Research, Inc. and other analytics firms, registering a 26.5% CAGR during the forecast period.

#### Top reasons to protect containers:

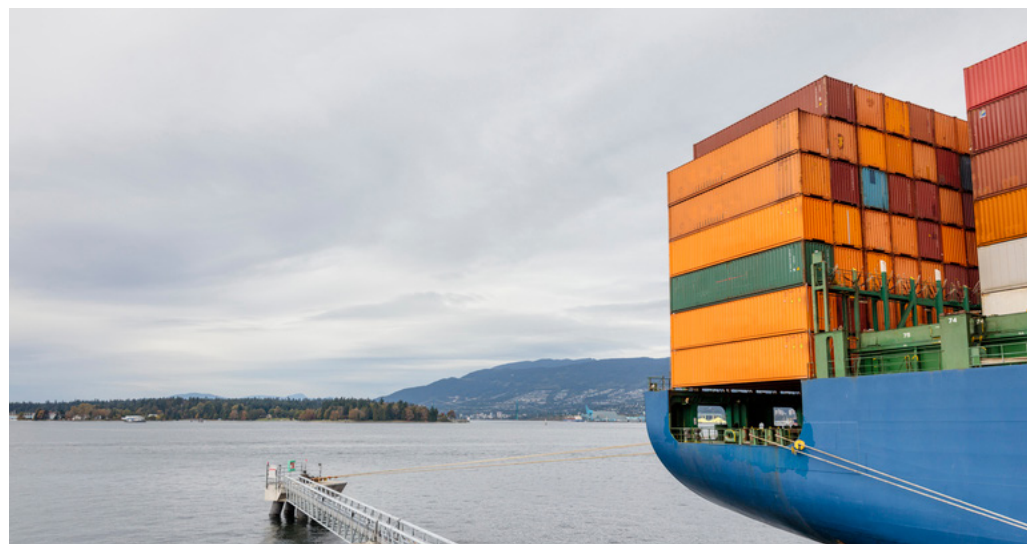
- Recovery of stateful containerized applications from failures and disasters
- Replication of the environment for migrating a test/dev environment to production or from production to staging before an upgrade
- Easy migration of container clusters

#### Top requirements for a container protection solution:

- Public cloud and on-premises coverage
- Application-level protection
- Automatic policies
- High level of security

#### The HPE and Cohesity container protection solution:

- Is fully tested, validated, and optimized
- Provides the maximum level of flexibility and granularity for containers backup and restore
- Can be deployed and managed in hybrid environments (public clouds and on-premises)
- Offers a [step-by-step implementation for containers' protection](#)



## WHAT'S DRIVING GROWTH IN CONTAINER ADOPTION?

### Container technology adoption is increasing at an amazing rate.<sup>1</sup>

This growth is the result of the ease with which containerized applications can be ported and deployed across different environments. Indeed, containers virtually package the applications with everything they need to run (configuration files, dependencies, and so forth) and isolate them for the deployment environment. This enables containerized applications to run easily on a variety of environments such as local desktops, virtual and physical servers, development, testing and production environments, and private or public clouds.

Another benefit of containers is that the number of containers a physical server can host is more than the number of virtual machines it can host. Because each container shares access to the

host's operating system kernel, it requires much less space than an equivalent virtual machine. The average size of a container is within the range of tens of megabytes; virtual machines can be up to gigabytes in size.

Lastly, containers' use cases have extended to artificial intelligence (AI) and analytics applications. Containers are becoming the standard way to build and deploy machine learning (ML) models, creating real-time analytics pipelines and running batch analytics and extract, transform, load (ETL) jobs. Their portability across different environments makes containers the perfect vehicle to manage the full lifecycle of AI/ML models and, for that matter, most any analytics application.

The massive adoption of containers for analytics and AI/ML applications is creating a demand for containers for stateful applications that use and generate a lot of data, and as a result, need persistent storage.

<sup>1</sup> Best Practices for Running Containers and Kubernetes in Production, Gartner, August 2020

## Solution brief

### Why protect containers?

Container adoption will drive the need for similar levels of protection and disaster recovery requirements in place for servers and VMs.

Backup and recovery of container environments such as Kubernetes or Docker and their associated applications are needed for:

- Recovery of stateful containerized applications from failures and disasters
- Replication to seed a new development initiative or migration between test/dev and production
- Protection prior to container lifecycle activities
- Easy consolidation of container clusters to reduce cluster sprawl

### Top requirements for container protection

The key challenge for protecting containerized applications in AI/ML environments is managing their dynamic deployment. A complete solution must meet the following key requirements:

- **Implement seamless operations and policies across on-premises and clouds:** Container deployment can span on-premises, cloud, or even multicloud. This “ubiquitous” flexibility must be reflected in the backup and restore approach.
- **Back up and restore at the application level, not at VM/server level:** By their nature, containers are not bundled with physical servers or virtual machines. Protection must be application-centric and collect all application sub-components (data and metadata) to permit recovery.
- **Protection granularity:** A Kubernetes cluster must be able to be backed up with different levels of granularity: Cluster, namespace, label selector, application, or persistent volume levels.
- **Automation:** Fully automatic application restore is among the key criteria of the solution in order to manage large container environments.

Make the right purchase decision.  
Contact our presales specialists.



Chat



Email



Call

- **Data Centric:** Leverage industry standard Container Storage Interface (CSI) drivers to perform dynamic provisioning, snapshots, clones and restores, such as the HPE CSI Driver for Kubernetes.

## HPE/COHESITY SOLUTION

Cohesity offers a solution to modernize and simplify data and application management with a single platform for multiple workloads, eliminating data silos across backup, files/object, and archive.

The combination of HPE and Cohesity provides end-to-end enterprise-grade container protection, safeguarding containers wherever they live (on-premises or in the cloud or hybrid) and restoring them wherever they are needed. Through the HPE Complete program, HPE provides a one-stop shop, where you can purchase validated turnkey backup and recovery solutions, reducing risk and improving recovery readiness while protecting your data.

The solution for protecting containerized applications includes the HPE hardware and Cohesity software components.

### HPE server families

The container protection software is available on two HPE server families:

#### • HPE Apollo Gen10

HPE Apollo systems serve as purpose-built, density optimized compute for demanding High Performance Computing and Artificial Intelligence applications.

HPE Apollo 4200 Gen10 servers offer an architecture optimized for Big Data analytics, software-defined storage, backup and archive, and other data storage intensive workloads. Its unique, easily serviceable 2U design saves data center space with up to 28 large form factor (LFF) or 54 small form factor (SFF) hot-plug drives. HPE Apollo delivers accelerated performance with a superior bandwidth and balanced architecture, Intel® Xeon® Scalable processor family CPUs, and non-volatile memory express (NVMe) connected solid state drives (SSDs).

#### • HPE ProLiant DL380 Gen10

HPE ProLiant DL380 servers are designed to simplify hybrid cloud by providing the agility of a modernized infrastructure with 10th generation servers, improving their existing extensive portfolio of modern solutions.

### Cohesity software

Cohesity protects data and application state for Kubernetes namespace. The web-scale platform backs up the namespace including all its operational state—not just its data.

Cohesity simplifies and strengthens Kubernetes backup and recovery by eliminating data silos caused by mass data fragmentation and replacing them with a hyperconverged solution that effectively consolidates the persistent state of applications, including PVs and operational metadata. Cohesity’s native integration with Kubernetes ensures protection and orchestration for stateful and stateless applications while supporting application-consistent snapshots so code and processes remain connected.

Cohesity software can be deployed on HPE Apollo systems and HPE ProLiant servers, with scale-up and scale-out options to suit your architecture requirements, allowing you to easily scale your infrastructure. Using this approach, the platform grows incrementally with compute, memory, storage, and networking. You can build a unified, modern data protection and management platform that delivers cloud-like services on-premises.

## CONCLUSION

Enterprise-grade container platforms are here to stay. HPE and Cohesity offer a joint solution for protecting containerized applications that:

- Is fully tested, validated, and optimized
- Provides the maximum level of flexibility and granularity for container backup and restore
- Can be deployed and managed in hybrid environments (public clouds and on-premises)
- Is fully documented with supporting technical white papers describing step-by-step implementation of container protection as well as detailed FlexBOMs and predefined configurations to make building and configuring your infrastructure easy

## LEARN MORE AT

[Data Protection for Kubernetes Using Cohesity DataPlatform and HPE Apollo Servers](#)



Get updates

**Hewlett Packard  
Enterprise**

© Copyright 2021 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Docker is a trademark or registered trademark of Docker, Inc. in the United States and/or other countries. Intel Xeon is a trademark of Intel Corporation or its subsidiaries in the U.S. and/or other countries. All third-party marks are property of their respective owners. a50004048ENW, April 2021