A CENTER FOR DIGITAL GOVERNMENT ISSUE BRIEF

CENTER FOR DIGITAL GOVERNMENT

# WHY KUBERNETES AND CONTAINER-NATIVE DATA MANAGEMENT ARE CRITICAL TO MODERNIZING GOVERNMENT TECHNOLOGY

Government IT leaders aiming to modernize with Kubernetes, containers and microservices must keep one point in mind: The storage equation has changed. The Kubernetes platform gives public sector IT development teams the tools to modernize their applications, using containers and microservices to gain speed, agility and scale. At the same time, storing data in modern cloud, hybrid and multi-cloud environments through traditional means poses substantial hurdles for container-native development in Kubernetes.

This brief outlines the opportunities and challenges of container-native data storage and management and explains why Kubernetes requires this new storage management and orchestration layer to reduce complexity and accelerate development timelines.

## ADVANTAGES AND OPPORTUNITIES IN CONTAINER- AND KUBERNETES-BASED APPS

Kubernetes, containers and microservices are taking the development world by storm. According to the Cloud Native Computing Foundation's 2020 Cloud Native Survey, the use of containers in production has jumped 300 percent since 2016. Indeed, 83 percent of the survey's respondents use Kubernetes.[1]

"Kubernetes enables you to automate all of the processes associated with getting applications out into production, and it does that by managing containers," says Michael Ferranti, senior director of product marketing with Portworx by Pure Storage. "This enables you to dramatically speed up the time it takes to deploy and run applications."

Container-native development allows applications to be deployed wherever they make the most sense in cloud, hybrid and multi-cloud architectures. This includes legacy applications government agencies rely upon.

"Because of the interdependencies between government agencies, there's a great impact on the ability to create scale and agility by utilizing a Kubernetes- or containers-based orchestration," adds Eric Simon, director of public sector sales at Pure Storage, a top supplier of software for managing Kubernetes environments.

Kubernetes-native development breaks down into two categories: stateless apps, which are collections of microservices that move data but do not store it, and stateful apps, which store and retrieve data.

"An early trend with Kubernetes was to run stateless components of applications with Kubernetes and run the stateful components on traditional tools," Ferranti says. But thanks to a new generation of container-native orchestration software, "stateful components can run just as easily on Kubernetes as our stateless components," he adds. "And that means the entire application becomes more agile."

All government apps require data that must be stored, managed, protected and recovered. To modernize amid these requirements, governments need the speed and agility of Kubernetes, which is vendor-agnostic. It can run wherever the developer needs it — on premises, in the public cloud and in multi-cloud environments. And thanks to container-native orchestration software, applications can serve multiple agencies, giving governments scale-out capability while improving efficiency and reducing silos. Moreover, backup, disaster recovery and business continuity can have ambitious objectives like near-real-time failover, dramatically reducing downtime risk in critical public sector applications.

## STORAGE AND DATA MANAGEMENT CHALLENGES FOR MODERN GOVERNMENT APPLICATIONS

Government IT leaders, like their counterparts in the private sector, want the agility of container-native architectures, which stitch together microservices and APIs that can be deployed quickly and scaled easily. Data storage challenges can put the brakes on these gains.

"You need to be able to seamlessly manage data in a consistent way, regardless of the environment you happen to be running in at the moment," Ferranti says. "When you have to run across multiple environments, storage becomes the bottleneck that prevents the rest of your application platform from modernizing and becoming more agile."

For all its speed and flexibility, Kubernetes is not a standalone solution for government agencies' non-negotiable requirements: high availability, encryption, data protection and flexible deployment options. And storage is changing dramati-

cally with the growing adoption of hyperscale public cloud and multi-cloud technologies. Kubernetes needs help to handle these kinds of challenges.

"Kubernetes is a completely different way of managing applications," Ferranti says. For instance, the highly distributed structure of Kubernetes reshapes a core storage task like backup and recovery.

"With Kubernetes, a single application may include hundreds of containers on multiple servers," he adds. "We can't take machine-based backups that protect our containerized applications because a snapshot of a machine is only going to capture part of our app and part of our data." Kubernetes environments require sophisticated application configurations that must be backed up correctly to ensure full recovery of all data in an emergency.

Government IT leaders also need to understand that solutions which excel in proof-of-concept (POC) environments may crash in the real world. Software that orchestrates security, storage and backup across complex, sprawling Kubernetes environments is essential to streamlining the transition from POC to live application.

Traditionally, IT departments assigned people to solve these kinds of challenges. But container-native environments have so many tasks, there will never be enough people to handle them all. The solution lies in software that creates an automated data storage and management layer.

## ESSENTIALS FOR DEPLOYING CONTAINER-NATIVE STORAGE MANAGEMENT SOFTWARE

A Kubernetes-native environment will have three specific characteristics:

**Self-service.** Developers manage their environments with little intervention from IT administrators. This requires rigorous, role-based access controls to ensure data protection. "Administrators, application owners and application developers can have permissions consistent with their functions," Ferranti says. If they have no reason to access sensitive data, role-based protections can lock them out of it.

**Programmable.** Provisioning, snapshots and other storage tasks must be available via APIs and automation. "You can't automate people," Ferranti adds. "You have to automate the software."

**Comprehensive.** Kubernetes applications must be compatible with a broad spectrum of data formats and compliance requirements across multiple storage platforms. "You need a platform that covers the most common kinds of data needs of any important application," Ferranti says.

Government IT leaders running mission-critical applications like emergency response have little room for error. Cyberattacks, ransomware and digital fraud ramp up the risk factors for public agencies trying to embrace new technologies while facing public scrutiny.

"The reality of kicking off these big Kubernetes projects is that it's all new to you," Ferranti cautions. The public may have little patience for trial-and-error experiments. "If you architect it the wrong way and then have a major disaster, or if you lose or compromise data, then there's probably no chance to do it again and learn from those mistakes," he adds.

What you can do is learn from a trusted advisor who has guided hundreds or even thousands of IT people through similar rollouts, Ferranti says. Whether working directly with a software vendor or through an intermediary like a system integrator, government IT leaders can take advantage of the hard lessons experts learned while implementing Kubernetes and container-native environments across a broad range of industries and specialties.

## FINDING SUCCESS WITH CONTAINER-NATIVE STORAGE MANAGEMENT

Ferranti and Simon say there are three keys to implementing a container-native solution in public agencies:

**Get it right the first time.** Use the knowledge and experience of trusted vendors to avoid missteps and wrong turns that other agencies have already gone through.

**Don't neglect security and data protection.** Deploy rigorous role-based access policies to give developers the freedom they need while keeping data locked down.

**Ask a lot of questions.** Quiz potential vendors on their ability to deliver aggressive backup and recovery objectives. Make sure they use service-level agreements to create enforceable policies and specific goals.

*This paper was written and produced by the Center for Digital Government, with information and input from Pure Storage.*

[1] cncf.io/wp-content/uploads/2020/11/CNCF_Survey_Report_2020.pdf

Produced by: CENTER FOR DIGITAL GOVERNMENT

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century. **www.centerdigitalgov.com.**

For: PURESTORAGE®

**Portworx® by Pure Storage** provides a fully integrated solution for persistent storage, data protection, disaster recovery, data security, cross-cloud and data migrations, and automated capacity management for applications running on Kubernetes.