ESG WHITE PAPER

Streamlining DevOps in Hybrid, Multi-cloud, On-premises, and Edge Environments

Red Hat OpenShift on IBM Cloud Simplifies the User Experience and Delivers As-a-service Benefits

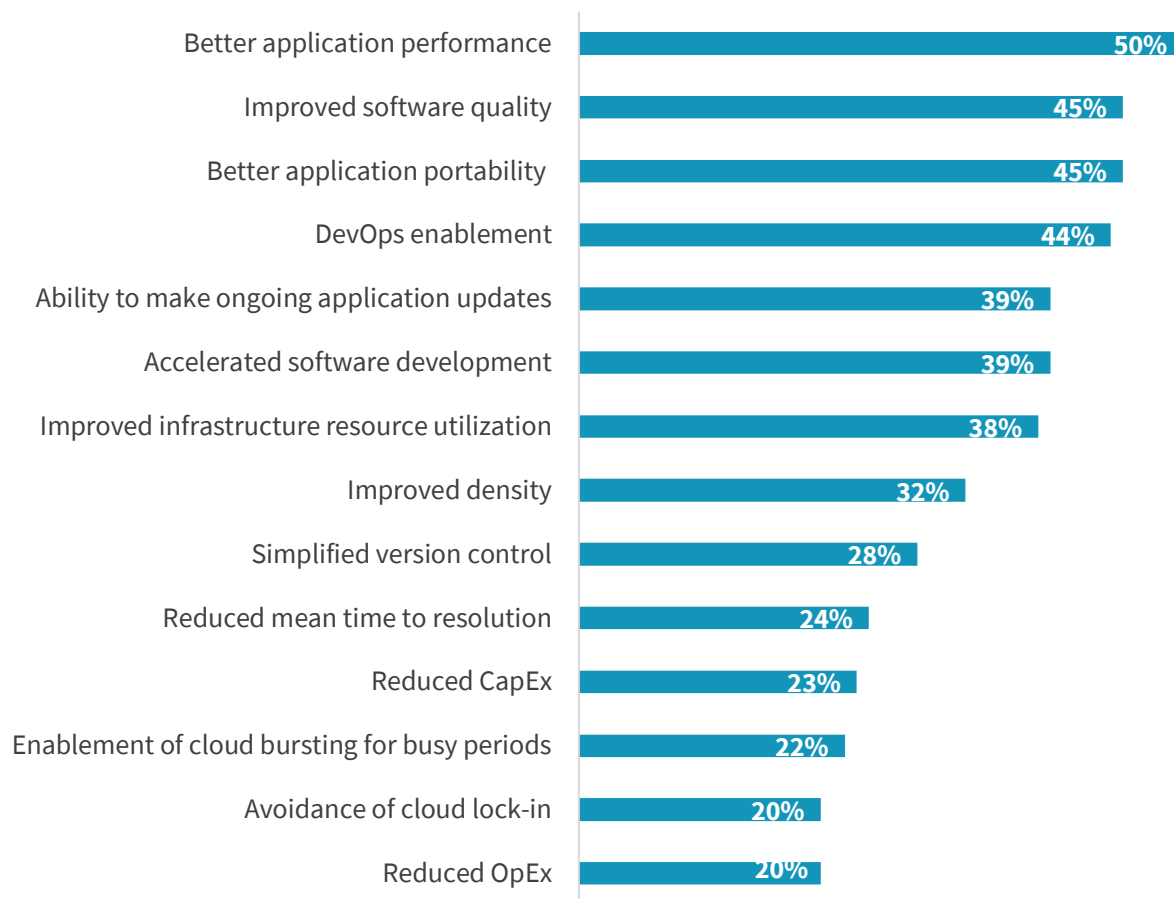By Mark Bowker, Senior Analyst

October 2020

Contents

Taking the Next Step to Accelerate Secure Application Development

Organizations increasingly are using containers to modernize, improve security, and speed application development in hybrid and multi-cloud environments. As shown in Figure 1, businesses that use containers see improvements in application performance, software quality, and application portability.[1]

Figure 1. Better Application Performance, Software Quality, and Application Portability Top Container Benefits

Which of the following benefits has your organization achieved, or does it expect to achieve, due to the utilization of container technology? (Percent of respondents, N=332, multiple responses accepted)

Benefit	Percent
Better application performance	50%
Improved software quality	45%
Better application portability	45%
DevOps enablement	44%
Ability to make ongoing application updates	39%
Accelerated software development	39%
Improved infrastructure resource utilization	38%
Improved density	32%
Simplified version control	28%
Reduced mean time to resolution	24%
Reduced CapEx	23%
Enablement of cloud bursting for busy periods	22%
Avoidance of cloud lock-in	20%
Reduced OpEx	20%

Source: Enterprise Strategy Group

Containers are becoming a standard for implementing SecDevOps workflows. Survey respondents said that while 22% of production applications/workloads run on containers today, they expect 34% of production applications/workloads to run on them in the following two years.[2]

Additionally, 86% of survey respondents say they are under pressure to accelerate the development and launch of new products and services (see Figure 2)[3]—a finding that no doubt contributes to increased container use.

---

[1] Source: ESG Master Survey Results, *Trends in Modern Application Environments*, December 2019.
[2] Ibid.
[3] Ibid.

Figure 2. Organizations Are Under Pressure to Accelerate Development and Launch New Products and Services

Do you believe your company is under pressure to develop and launch new products and services at an accelerating pace? (Percent of respondents, N=332)

Don't know/no opinion, 1%

No, 13%

Yes, definitely, 38%

Yes, somewhat, 48%
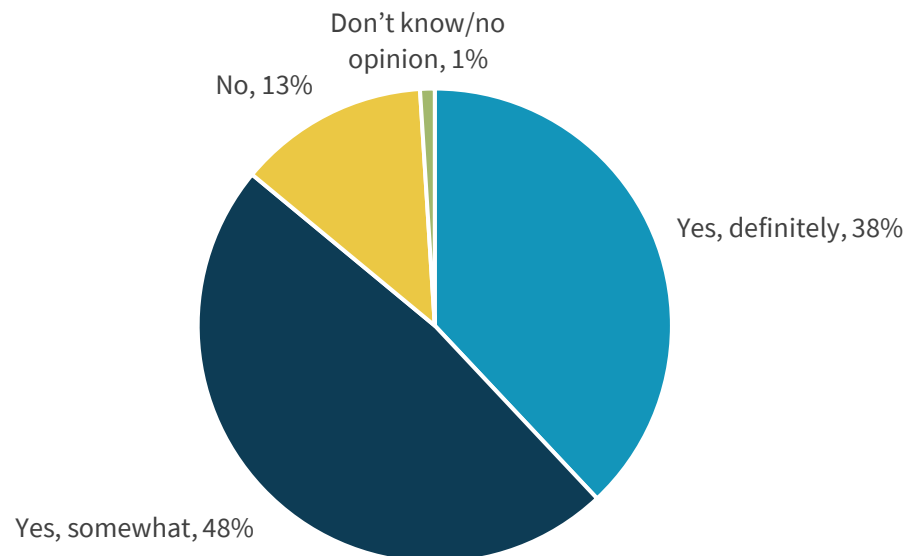
Source: Enterprise Strategy Group

As organizations attempt to increase the pace of development, certain challenges can impede progress:

- Running infrastructure, security, and operations instead of pushing out as much code as possible to innovate the business.

- Developing in complex, multi-cloud environments and distributed on-premises locations while enabling teams to collaborate.

- Modernizing legacy apps while waiting for development-test-production machines and encountering scalability and availability issues.

Many businesses on an application development modernization journey choose Kubernetes, a scalable, trusted open source container platform for hosting cloud-native applications. Leading Kubernetes platforms include IBM Cloud Kubernetes Service, which has been providing an enterprise-focused production experience for many years, and Red Hat OpenShift, IBM's hybrid and multi-cloud strategic platform.

Red Hat OpenShift on IBM Cloud (managed OpenShift) is the first as-a-service offering of OpenShift 4. Managed OpenShift adds features to IBM's Kubernetes foundation that increase agility and flexibility for simplifying SecDevOps and for developing and managing workloads in clouds and distributed locations.

Addressing Application Development Challenges with Red Hat OpenShift on IBM Cloud

Red Hat OpenShift on IBM Cloud (ROKS) is a managed cloud service with built-in features and functions to help organizations solve development challenges related to new apps and modernizing legacy apps. IBM isolates, protects, and

runs the high-availability Kubernetes masters, while organizations control the worker nodes. ROKS provides full administrative cluster access with fine-grained access rights along with safeguards to avoid breaking the API/master side of clusters.

Instead of investing in, maintaining, and managing infrastructure, organizations can focus on their line-of-business objectives supported by capabilities such as:

- Automated provisioning and infrastructure configuration.

- Automated OpenShift installation, configuration, and scaling.

- Automatic upgrades.

- Automated regulatory compliance for the OpenShift environment, including regulations such as Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry (PCI), System and Organization Controls (SOC1, SOC2, and SOC3), and International Organization for Standardization (ISO).

- Cloud platform integration, including services such as monitoring, logging, key management, identity and access management, storage, and vulnerability scanning.

- IBM Global Site Reliability Engineering support.

Built-in High Availability and Resiliency

The default multi-zone deployment spreads masters and worker nodes across data centers to:

- Protect against a single data center failure.

- Minimize cluster outages.

- Maintain API and workload accessibility.

- Provide a unique 99.99% financially backed SLA.

Reduced infrastructure requirements help prevent over- or under-provisioned applications, and the pay-for-use, as-a-service model enables users to control versions and licensing in a single account. On-demand scalability is backed by public cloud growth in 30+ global IBM data centers.

Without infrastructure obstacles to slow them down and divert their attention, developers can concentrate on delivering innovative products and services. Efficiency increases because managed OpenShift allows developers to collaborate easily, and teams spend less time diagnosing and fixing issues. The continuous delivery pipeline is integrated with management tools that promote consistency across on-premises and cloud workloads.

Simplifying and Improving the User Experience

The common entry point to Red Hat OpenShift on IBM Cloud is a graphical user interface suitable for all types of users, including new or experienced developers and operations staff. Users can choose which OpenShift version they want to use with either a classic or virtual private cloud (VPC) infrastructure. After a one-time, point-and-click cluster setup, users can automate tasks through APIs or IBM Cloud Schematics, which enables infrastructure as code and automates provisioning of IBM Cloud resources. A Slack community for IBM Cloud offers a channel for engaging users and connecting them with IBM developers.

The OpenShift API, tools, and support for the OpenShift dashboard provide a familiar interface for users running OpenShift in their own data centers, in geographically dispersed locations on IBM Cloud, or in other vendor clouds. The Red Hat

Marketplace and operators are integrated into Red Hat OpenShift for IBM Cloud, enabling users to bring in content from IBM, Red Hat, and ISVs.

Users own the timing decision of lifecycle upgrades. IBM does not want to switch Kubernetes versions and break something in customer deployments. After a user submits a request, everything in the stack is upgraded transparently node by node. With no downtime or disruption to schedule around, teams remain productive.

Add-on managed components are available as users advance their skills or project requirements change. These include:

- **Kubernetes Terminal**. This simple CLI integrates with the console to provide an easy, quick way to troubleshoot or deploy something. Users log in to a cluster and run commands.

- **Diagnostics and debug tool.** This feature delivers cluster insights into issues such as performance or latency. Users select and run tests or conduct health checks against nodes, pods, or other deployed components. Logs can be exported and passed on to IBM support.

- **Static Route.** Rules can be added to worker nodes to manage routing between clusters and other networks. When extending on-premises data centers and resources to IBM Cloud, users have a direct link or VPN solution by creating a default route for local IP ranges to cloud directly to a cluster.

Effortless Cluster Management

The intuitive graphical interface offers CLI and API alternatives, along with:

- Fully managed master nodes.

- High-availability masters.

- User-controlled worker nodes.

- Worker node auto-recovery and auto-scaling.

Other features and functions integrate with IBM Cloud DevOps via open toolchains to further simplify the user experience. Standard, customizable templates support Kubernetes and OpenShift. For example, users can save time while they develop a Kubernetes application, develop and test microservices on Kubernetes with Helm, or do a progressive rollout in Kubernetes using Iter8. Further, developer pipelines are automatically provided for purposes of deploying workloads, gaining DevOps insights, tracking issues, managing keys, using Eclipse IDE and GitHub, and more.

Adding Development Security, Agility, and Flexibility with Red Hat OpenShift on IBM Cloud

Managed OpenShift adds features to IBM's Kubernetes foundation to simplify SecDevOps and to improve workload manageability. Security consistency across hybrid clouds is the most common cloud-native application security challenge, cited by 43% of survey respondents.[4] IBM Cloud addresses this concern by being the only public cloud that offers FIPS 140-2 encryption, which is especially important in securing highly regulated workloads. IBM also makes available integrated offerings, tightly coupled within the UX of RedHat OpenShift on IBM Cloud. For instance, LogDNA and Sysdig are IBM-supported; keeping data within IBM Cloud removes the need for third-party vendor support or troubleshooting conversations.

 These additional capabilities enhance security, agility, and flexibility:

---

[4] Source: ESG Master Survey Results, *Leveraging DevSecOps to Secure Cloud-native Applications*, December 2019.

- **Logging with IBM Cloud Log Analysis with LogDNA.** Complete searches rapidly using intuitive, natural language capabilities and send search results to development teams that own an affected microservice.

- **Monitoring with IBM Cloud Monitoring with Sysdig.** No need to add management complexity by standing up a separate monitoring service. Both the default dashboard and create-your-own dashboard provide overview and detailed views. Administrators can consolidate metrics for all clusters, give different users and teams differing levels of access, and create notifications and alerts. When an alert is triggered, administrators can use the assisted capture feature to grab data in real time to provide context.

- **Key management.** When organizations want to go beyond the default Kubernetes encryption, managed OpenShift offers two additional layers. The first is IBM Key Protect, which enables "bring your own key." Users own their keys and manage their lifecycles. The second is the IBM Hyper Protect Crypto Services key management and cloud hardware security module, which enables "keep your own key." Keys are fully owned by users, and IBM doesn't have access to data or applications. If a key is lost, the physical server that stores keys in IBM Cloud must be replaced.

- **Air gapping clusters.** Public and private IP addresses can be set up on master and worker nodes. Private clusters are available only from the IBM backbone. Users can mix and match public and private—for example, make an API accessible for CI/CD purposes or make workloads accessible on the internet because customer applications run there.

Container Security and Isolation

In addition to isolated computing, networking, and storage resources, managed OpenShift provides:

- User-managed keys.

- Private clusters and hosted private registries.

- Automatic encryption of secrets and volumes.

- Image security enforcement controls with support for Red Hat Notary.

- **Vulnerability Advisor.** This feature increases security and prevents errors because the insights it provides into images allows administrators to fix issues before code goes into production. Vulnerability Advisor conducts automatic or scheduled inspection of images stored in the IBM Cloud Container Registry, and it provides Docker and container scanning to detect vulnerabilities and configuration weaknesses. Administrators can set policies to warn users or block them from deploying images that contain vulnerabilities.

Increasing Value with IBM Cloud Services

Users can take advantage of more than 200 IBM, third-party, and open source services to get more out of their investment in Red Hat OpenShift on IBM Cloud. In addition to applying IBM Cloud Pak OpenShift entitlements, users can:

- Bring IBM Watson, weather data, internet of things, analytics, and data services to an application. For example, consider repackaging and modernizing a traditional, monolithic application as a container and adding Watson voice-to-text and visual recognition without rewriting code.

- Receive persistent volumes (file, block, and object) or software-defined storage.

- Integrate with IBM Cloud identity and access management to provide access down to the namespace or project level.

Deploying IBM Cloud Services Anywhere with IBM Cloud Satellite

While many organizations are moving workloads to public cloud, others are not because they have data location requirements and/or latency issues. Mixing on-premises and cloud workloads across vendor platforms can create challenges related to consistency, visibility, management, security, and compliance. As a solution to hybrid and multi-cloud complexity, a distributed cloud provides businesses with the flexibility to run applications anywhere while retaining control through the public cloud.

As IBM's distributed cloud offering, IBM Cloud Satellite provides fully managed IBM Cloud services anywhere—on-premises data centers, colocation centers, or edge locations. Red Hat OpenShift on IBM Cloud, IBM Cloud Databases, continuous delivery pipelines, AI, and other services can be controlled through a single view within the public cloud. Using IBM Cloud Satellite, organizations can:

- Achieve consistency and development speed across distributed cloud environments.

- Consume IBM Cloud managed services in any location.

- Maintain end-to-end security where data and workloads reside.

- Simplify management with one dashboard, common identity and access control, and centralized visibility.

The Bigger Truth

Businesses need to modernize application development, push out more code faster, assure development consistency across teams and clouds, and revitalize legacy apps. To accomplish these objectives, organizations want to pursue cloud-native application development and take advantage of Kubernetes. Unfortunately, they are stopped sometimes by lack of clarity about how to get started or by what appears to be a daunting effort.

IBM talked with a lot of companies about their objectives and challenges and took this research into account in developing managed OpenShift. In the interviews, IBM heard loudly and clearly the priorities of simplifying the experience for all types of users across cloud and distributed locations and enabling click-and-go efficiency. As a result, managed OpenShift should resonate with SecDevOps decision makers looking to get out from under burdensome infrastructure ownership to focus on accelerating application development.

In addition, IBM was thoughtful about a couple of important things. One is maintaining and extending the experience of current OpenShift users who can continue to work with familiar interfaces and controls. Another is building on a well-established Kubernetes foundation to increase efficiency, promote consistency, and reduce risk.

Red Hat OpenShift for IBM Cloud is well worth evaluating by organizations that want the benefits of as-a-service and secure, always-on apps.

ESG

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com   contact@esg-global.com   508.482.0188