Accelerate mission impact of the IC multicloud strategy with containers

> "The IC must discover, access, process, and analyze information and foster enterprise-wide information sharing and collaboration. Central to this is a fully featured cloud environment that enables portability of services, analytics, applications, and data across multiple IC IE fabrics, environments, and geographic locations."

Strategic plan to advance cloud computing in the Intelligence Community

Sample use case

Portable containers unlock the value of the multicloud strategy. For example, an agency can:

- Train an ML model on Amazon SageMaker, Microsoft Azure ML, or TensorFlow.
- Containerize the trained model.
- Deploy the container to a hardware environment anywhere in the world—even a tablet.

facebook.com/redhatinc
@RedHat
linkedin.com/company/red-hat

Executive summary

Containers accelerate and increase the mission impact of the multicloud strategy. With a robust management and standardized platform, containers allow for moving applications while preserving functionality between approved, classified clouds, on-premise servers, and edge devices. Red Hat® OpenShift® offers the Intelligence Community (IC) the advantage of deploying, managing, scaling, and hardening applications anywhere, anytime, and at any scale.

The 3 Rs of the multicloud: The right place, right time, and right scale

In November 2020, the Central Intelligence Agency (CIA) awarded its Commercial Cloud Enterprise (C2E) contract to 5 major cloud vendors.[1] U.S. intelligence agencies will soon have greater flexibility in choosing their environment, be in a position to optimize capabilities and costs for any given application, and be equipped to switch freely as capabilities and mission needs evolve. Once onboarded and available, mission decision makers will be able to choose the **right place** to deploy applications, blending deployments across 5 classified clouds, agency datacenters, and edge devices.

The addition of the 4 cloud environments at the **right time** provides agencies access to the same cloud capabilities as their private sector counterparts. To succeed, agencies need to take the value-focused adoption approach that has worked for the private sector. To take full advantage of the multicloud strategy, the IC needs a standardized container platform that separates applications from the hosting environment. After modifying applications once, agencies can freely move them to any approved platform. Using a standardized platform helps make the mission flexible, resilient, and future-ready.

A multicloud strategy empowers agencies to deliver applications at the **right scale** by considering the edge as an extension of the overall strategy. The same cloud-native application architectures and cloud management models used at the hyperscale level must also be applied at the tactical and mission level. Providing the same agnostic Kubernetes application programming interfaces (APIs) and enterprise-level management at all scales is the basis of the platform approach.

Overcoming barriers to the IC multicloud strategy

The roadblock for the IC is that most IC applications are tied to a particular hardware or cloud environment. An application originally written for datacenter servers, for example, usually needs significant modifications before it can be deployed to the cloud and vice versa. Rewriting every application for every allowed environment is time-consuming and costly. For time-sensitive operations, inability to swiftly move an application to an environment with superior capabilities can impede the mission.

Previously, the IC could deploy high-side applications only in agency datacenters or a specific provider's classified cloud. When all C2E environments are onboarded, agencies will have the flexibility to choose the right hosting solution to deliver the mission the right way. An agency might

[1] *"CIA makes awards for intelligence community's next massive cloud contract." Washington Technology, 20 Nov. 2020.*

use Cloud A for its superior machine learning (ML) algorithms and Cloud B to comply with rules prohibiting sole-source procurement. Another agency might choose Cloud C because its datacenter location is closest to an operation.

A significant challenge to adopting a multicloud strategy is modifying traditional applications to run on a new hosting environment, which can take months or years. Moreover, the effort needs to be repeated for every new feature iteration of the contract that delivered the capability, and rewriting every application for multiple environments is not sustainable. In addition, Federal Acquisition Regulation (FAR) rules can require extensive rework to stick with a single hosting solution every time a new contract is not sustainable.

To maximize mission value from the multicloud strategy, intelligence agencies need applications and code that reduce Level of Effort (LOE), accelerate time to mission, and give missions the flexibility to take full advantage of the best available capabilities. Code and applications need to be:

- **Portable.** The goal is to "write once, deploy anywhere"—whether in a classified cloud, datacenter, or edge device—making sure that applications behave consistently in every environment.
- **Security-focused.** Safeguarding high-side applications deployed in classified clouds requires using trusted code, anticipating and remediating vulnerabilities, managing access, integrating security testing throughout the application life cycle, and ensuring workload security at runtime. Achieving this requires a zero trust approach—provided that every interaction is untrusted until proven otherwise.
- **Scalable.** Application workloads are unpredictable. With too few resources, application performance worsens, whereas costs rise unnecessarily with too many. The ideal state is to automate resource provisioning, replicating application instances when demand is high and shutting them off when demand tapers off.
- **Manageable.** Operations teams are responsible for scaling applications, introducing new versions, and managing tasks, such as monitoring, logging, and debugging. They need automation, insights, governance, and a standardized management console for all locations where code is running.

Open source container technology

Container technology makes multicloud deployments possible. Containers are in use in the IC and throughout the federal government and have become the go-to solution in the public sector for rapid innovation and increased DevSecOps capabilities. Containers package up application code with everything the code needs to run, including libraries, dependencies, and system settings. Along with a robust management platform, containers are the key to executing the mission anywhere, anytime, the right way, and at the right scale. Enterprise-class tools for developing and managing containerized applications allow agencies taking advantage of containers to deliver the mission with:

Portability. With a robust container management platform, DevSecOps teams can "build once, run anywhere," as shown in Figure 1. Once built, containerized applications are stored in the management platform via a registry and delivered through the infrastructure in the datacenter or an approved cloud. Push them to any approved environment with a few clicks. No modifications are typically needed. If another host or location becomes a better fit for the workload, push the container to the new hosting environment, and shut it down on the old one. The application has access to the new

Part of a zero trust architecture

Red Hat OpenShift and Red Hat Advanced Cluster Security for Kubernetes can be built on zero trust architecture, allowing agencies to:

- Use built-in auditing and monitoring.
- Control configuration management.
- Inherit the security capabilities of Red Hat Enterprise Linux®.
- Use policy to help ensure that APIs are used and focused on security.
- Apply macro-segmentation to control which traffic enters or exits the internal services communication network.
- Apply micro-segmentation and restrict internal cluster communications.
- Augment Red Hat Enterprise Linux resource management in Red Hat OpenShift.
- Enforce supply chain controls and platform access for workloads.
- Consider the context of the request when granting or denying access.
- Integrate existing access control and identity provider services.

hosting environment capabilities within hours versus weeks or months usually required to modify traditional applications for another environment. If a cluster is already present in the target environment, deployment takes just minutes.

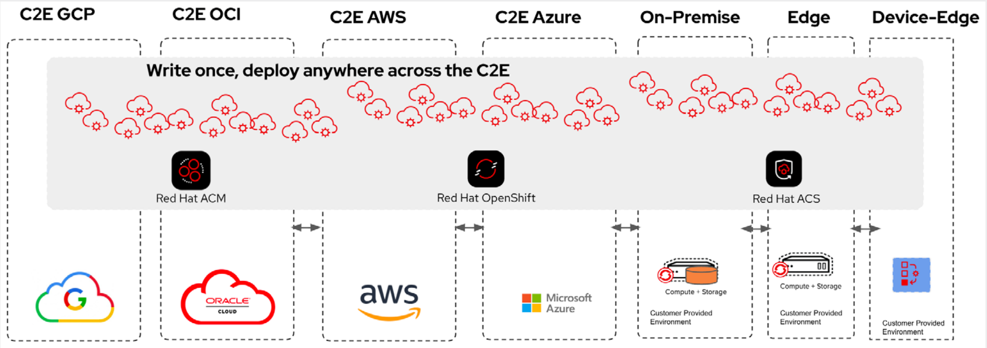

Figure 1. Containerized applications can run on the approved environment with the based capabilities for the mission.

Security. A robust, security-focused container management platform isolates containers from one another, using a secure overlay network. Combined with IPSec, communication between containers needs to be explicitly allowed to help prevent the spread of malware. Containers work well with DevSecOps—a process that integrates security throughout the development process, rather than waiting until the end when remediation takes longer. Some container orchestration platforms provide additional security capabilities, such as risk profiling and threat detection. Read more about container security.

Scalability. Container-based applications managed through a robust container management platform can be configured to automatically replicate themselves when demand is high and to shut down when no longer needed. This capability allows agencies to preconfigure or manually set rules pertaining to where to deploy the replicated containers—not necessarily the current. For example, imagine an agency anticipating increased demand for preprocessing a data source in Haiti ahead of a hurricane. In this case, the container platform could create additional instances of the container in the cloud cluster closest to data, whether the vendor is AWS, Azure, Google Cloud, or Oracle. If that location is taken down the next day by flooding or wind damage, the agency can quickly add resources in the next closest location. This flexibility and resiliency is not possible with stovepipe applications that are tied to a particular hardware platform. Agencies gain even more flexibility to deliver the mission anywhere when the same container management platform works regardless of the location—the various clouds, the agency datacenter, and edge devices.

Manageability. Container management platforms provide robust management tools to manage development, security, delivery, and operations of Kubernetes-based container solutions. These management tools let users define and enforce governance and security rules, automate deployment models, deploy platform capabilities to new environments, and more. The ability to manage all resources within the platform makes it possible to blend the different environments into a single automated deployment model.

Preintegrated companion tools

Every release of every Red Hat product is validated to work with all other Red Hat products, saving agencies the time and expense of integrating multiple tools and maintaining those integrations. Use Red Hat OpenShift with:

- Red Hat Enterprise Linux.
- Red Hat Advanced Cluster Management.
- Red Hat Advanced Cluster Security.
- Red Hat OpenShift Data Foundation Essentials.
- Red Hat Application Foundations.
- Red Hat Quay, a container image registry.
- Red Hat Ansible® Automation Platform.

OpenShift Platform Plus

Includes these core capabilities in a convenient package:

- Red Hat Enterprise Linux.
- Red Hat Advanced Cluster Management.
- Red Hat Advanced Cluster Security.
- OpenShift Data Foundation Essentials.
- Red Hat Application Foundations.
- Red Hat Quay, a container image registry.

Our credentials

Red Hat is the #2 overall contributor to Cloud Native Computing Foundation (CNCF) projects.[2] We represent our customers in key communities, advancing new capabilities and fixing issues. Using our software to build applications gives the Intelligence Community early access to the latest innovations in security and performance.

Advantages of Red Hat OpenShift Platform Plus

Kubernetes is the leading open source technology for building, scaling, and managing containers. Standardizing on 1 Kubernetes platform will help the community adopt containers sooner and minimize training. Kubernetes platforms vary in terms of security, support, and ease of management. Red Hat's Kubernetes platform Red Hat OpenShift Platform Plus meets intelligence agencies' rigorous requirements for security, scalability, and ease of management.

Agencies can accelerate adoption of containers and simplify management by standardizing on OpenShift Platform Plus. Currently in operations throughout the federal government and in the private sector, OpenShift Platform Plus multiplies the impact of the multicloud strategy by supporting agencies' efforts to deliver the mission anywhere, anytime, the right way, and at the right scale. With this platform, agencies can:

- Deploy applications in any approved location: the classified clouds in the C2E contract, an agency datacenter, and edge devices.
- Automatically scale the number of container copies, based on current demand.
- Enforce agency security controls throughout the container life cycle.
- Strengthen security with:
  - Visibility into application usage.
  - Context-based risk profiling.
  - Container runtime detection of security threats.
  - Control over which sets of application elements (pods) can communicate, limiting the spread of malware.
  - Control over the software supply chain to make sure code used in application development is trusted.
  - Container scanning through Red Hat Advanced Cluster Security.

The cryptographic components of Red Hat OpenShift are FIPS 140-certified, and the Defense Information Systems Agency (DISA) has released Secure Technical Implementation Guidelines (STIG). See the latest certifications.

- Provide software-defined storage for containers. OpenShift Data Foundation helps teams develop and deploy applications quickly and efficiently across clouds, datacenters, and edge OpenShift Platform Plus-managed capabilities.
- Red Hat OpenShift Dev Spaces uses Kubernetes and containers to provide developers and other IT team members with a consistent, security-focused, zero configuration development environment. The experience is as fast and familiar as an integrated development environment (IDE) on a laptop.
- OpenShift Platform Plus integrates and works out of the box with a number of companion tools from Red Hat's portfolio.

[2] *"Kubernetes project journey report." Cloud Native Computing Foundation, 8 June 2023.*

- Manage all clusters (on any cloud) and applications from a single console. Red Hat Advanced Cluster Management for Kubernetes provides enterprise-class management tools that work with every platform in the C2E contract.

Get started on your multicloud strategy

Contact us for more information on these multicloud management tools and take the initial steps toward developing a multicloud strategy.

Learn more

Learn about Red Hat's work with the Intelligence Community.

Understanding containers

What is container security?

Authority to Operate

Red Hat OpenShift has achieved Authority to Operate (ATO). It is already in use in more than 1 intelligence agency and the Department of Defense (DoD). Red Hat OpenShift is available on the AWS Marketplace for the U.S. Intelligence Community.

About Red Hat

Red Hat helps customers standardize across environments, develop cloud-native applications, and integrate, automate, secure, and manage complex environments with award-winning support, training, and consulting services.

facebook.com/redhatinc
@RedHat
linkedin.com/company/red-hat

North America
1 888 REDHAT1
www.redhat.com

Europe, Middle East, and Africa
00800 7334 2835
europe@redhat.com

Asia Pacific
+65 6490 4200
apac@redhat.com

Latin America
+54 11 4329 7300
info-latam@redhat.com