

Red Hat OpenShift Virtualization for defense IT operations

Reduce dependence on legacy virtualization platforms

Defense agencies will continue to host and manage virtual machines (VMs). Today, hundreds of thousands of VMs contribute to defense operations across all agencies, many supporting mission-critical applications and systems. Their IT teams face increasing pressures to optimize costs, be more efficient, and reduce vulnerabilities to their networks.

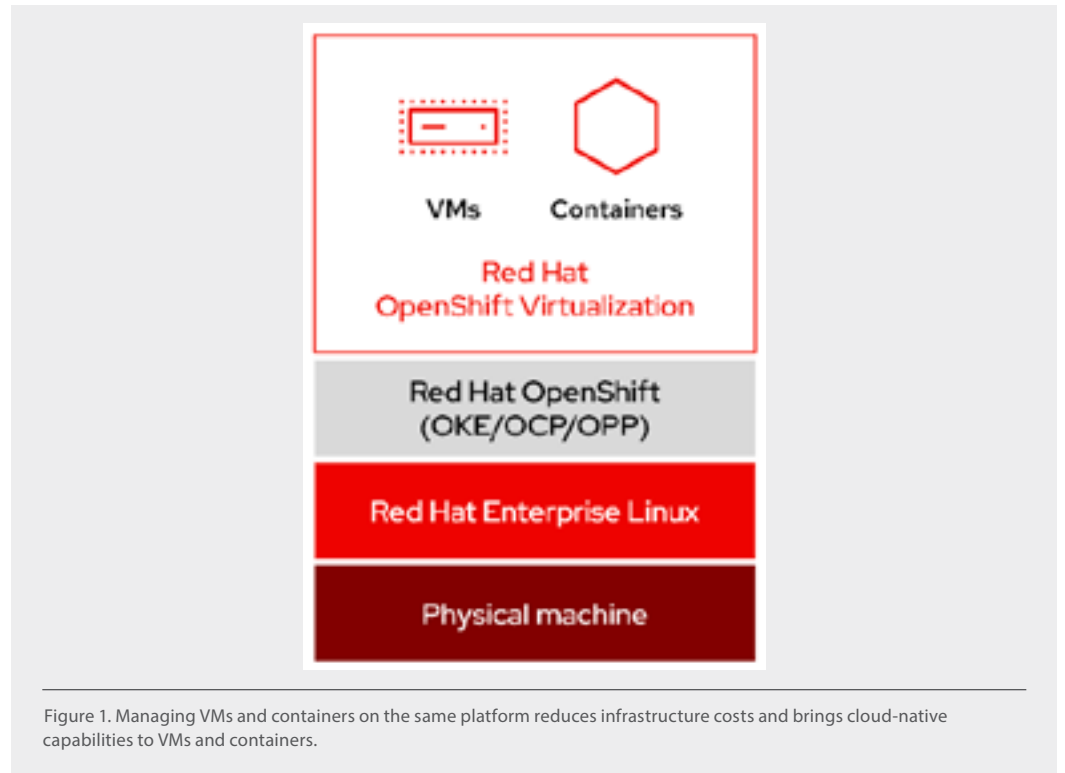
Dependence on the existing VM hosting platform causes operational risk, limits paths to modernization, and inhibits innovation. To maintain dominance in modern warfare and improve their cyber posture, agencies need a modern, cloud-native virtualization infrastructure that:

- ▶ Is secure, trusted, and reliable.
- ▶ Allows rapid delivery of capabilities to support and heighten defense coverage and strength. This requires virtualization infrastructure that can run on any hardware, anywhere—at the tactical edge, in datacenters, and in public clouds.
- ▶ Provides cloud-native development and delivery capabilities to accelerate agencies' modernization efforts, such as automation (e.g., self-healing, software defined storage, and networking), artificial intelligence, and a single source of truth for configuration files.
- ▶ Simplifies infrastructure and reduces maintenance requirements by hosting VMs and containers side-by-side on the same platform.
- ▶ Meets stringent compliance requirements, such as trusted software supply chain for platform components, zero trust strategies, ISO/IEC Standards, and others.

Unified platform for VMs and containers: Red Hat OpenShift Virtualization

A modern application platform

An included feature of all Red Hat® OpenShift® subscriptions, Red Hat OpenShift Virtualization is a modern application platform for running and deploying new and existing VM workloads alongside containers on the same OpenShift nodes. They behave as they would on a traditional VM platform while gaining the advantages of modern DevSecOps and GitOps pipelines. OpenShift is available as a fully managed public cloud service edition or as a self-managed edition that can be deployed across agencies' hybrid cloud, including the tactical edge.



Simplify VM lifecycle by adding cloud-native capabilities

Red Hat OpenShift Virtualization is a Kubernetes Operator built atop the open source [KubeVirt](#) project. It provides additional capabilities that simplify management of VMs at large scale, including push-button automation and cloud native capabilities built into OpenShift. These capabilities include monitoring and alerting, traffic management and telemetry, serverless environments, continuous integration/continuous delivery (CI/CD) pipelines, GitOps, and more. Using either a graphical user interface (GUI) or command-line interface (CLI), defense agencies can:

- ▶ Warm-migrate VMs onto the OpenShift platform at scale using the free tool, Migration Toolkit for Virtualization. The toolkit can import VMs from VMware vSphere, Nutanix, and other OpenShift clusters, and image repositories. Source VMs continue running while the data is copied, minimizing downtime. When all data is copied, the administrator stops the running VM and the new instance begins running in the new location.
- ▶ Create and manage new Windows and Linux® VMs.
- ▶ Manage network interface controllers and storage disks attached to VMs.
- ▶ Live migrate VMs between nodes in datacenters, cloud, and edge for continuity of operations.

Mission value of OpenShift Virtualization for defense

With Red Hat OpenShift Virtualization, defense agency software teams can preserve their existing investment in VMs while benefitting from the simplicity and speed of a modern hybrid cloud application platform.

Reduced operational risk. Bringing enterprise-class stability to open source software, Red Hat OpenShift lets agencies host VMs on any hardware platform, avoiding reliance on any single vendor. In addition, use of open source components supports defense agency efforts to strengthen the security of end-to-end software supply chains. Open source provides the visibility and traceability that proprietary software lacks, reducing the risk that components will inject malicious software or code into the enterprise.

Technology force multiplier. With a single platform for VMs, container-based, and serverless workloads, defense IT teams can standardize infrastructure deployment and use a common, consistent set of established tools. Defense IT software teams can also integrate Red Hat OpenShift with open source development tools they already use for container management, such as GitLab for DevSecOps and JFrog Artifactory for image storage. In addition to reducing Day 2 operational costs, consolidating VMs, Kubernetes containers, and serverless workloads on a single platform lowers infrastructure costs.

A path to infrastructure modernization. OpenShift Virtualization supports defense agency infrastructure modernization goals, which call for preserving existing virtualization investments while adopting modern application lifecycle practices such as DevSecOps and automation.

Automation and self healing. Used in conjunction with OpenShift Virtualization, Red Hat Ansible® Automation Platform can automate Day 2 VM operations such as configuration changes, patching, and rebooting. Automation also supports the goals of operating without disruption during local emergencies.

Increased flexibility and resilience. Envision a scenario in which VMs for a mission-critical system need to be stood up in a new location within 6 hours. With traditional VM hosting platforms, IT staff need to manually configure the VM for the new environment, a time-consuming and error-prone process that might not be completed by the mission deadline. When Red Hat OpenShift Virtualization is paired with Ansible Automation Platform, VM migration can be executed automatically. Code and files are stored in a centralized Git repository to ensure the configuration is accurate and secure.

Faster time to production for new VMs. By combining OpenShift Virtualization with modern application development processes and tools, such as Red Hat Trusted Software Supply Chain, [Red Hat OpenShift Dev Spaces](#), and [Red Hat Developer Hub](#), defense agencies can achieve the objective of delivering resilient software at the speed of relevance.




eSecurity compliance. Red Hat provides experts to help customers secure and validate their OpenShift Container environments. This includes implementing security practices such as zone isolation and microsegmentation, ensuring they meet all necessary requirements and can be validated against standards like DISA, STIG, BSI and E8.

For more information, check out [Red Hat OpenShift Virtualization](#).



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
 1888 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