4 ways Red Hat OpenShift Virtualization improves security focus

Use this checklist to focus your security efforts and apply consistent controls across virtual machines (VMs) and containers in your hybrid cloud. Here are 4 ways you can use Red Hat® OpenShift® Virtualization tools to strengthen security posture and protect workloads.

1 Harden the platform from the ground up

OpenShift Virtualization runs on Red Hat OpenShift, which provides a hardening-ready foundation and can manage both containers and VMs. This provides consistent security enforcement across every workload.

- **Enforce compliance baselines in Red Hat OpenShift with Red Hat's Compliance Operator.** The Compliance Operator lets administrators describe the required compliance state of a cluster and then provides them with an overview of gaps and ways to remediate them.
- **Restrict GPU and USB pass-through to approved devices** to reduce the risk of unauthorized data access or code execution from attached hardware.
- **Disable nonessential feature gates and enforce trusted container registries** using Transport Layer Security (TLS) to limit exposure to unverified images and misconfigurations.

2 Control workloads at every layer

By managing VMs as Kubernetes objects, OpenShift Virtualization gives you fine-grained control over who can create, modify, and interact with workloads. Apply role-based access control (RBAC) and audit policies consistently so that changes to critical VMs follow the same governance model as containerized applications.

- **Restrict executive access, Virtual Network Computing (VNC) console access, and live migration operations to approved administrators** to reduce the risk of unauthorized changes or data exposure.
- **Disable guest-memory overcommit and shareable disks** where they are not required to reduce resource contention between tenants and limit exposure if a single workload is compromised.
- **Enforce consistent error-handling and validation policies** for critical workloads to avoid inconsistent behavior across environments and reduce the risk of silent failures or data corruption.

3 Segment network traffic to enhance security posture

Security in OpenShift Virtualization extends to network configuration. Networking controls apply at both the container and VM levels so you can keep the same microsegmentation model across all workloads.

Apply consistent network policies, observability, and logging across these environments to detect suspicious traffic patterns more quickly and simplify troubleshooting.

- **Use Virtual Local Area Networks (VLANs) to isolate tenant or application traffic** to reduce the risk of lateral movement between network segments.
- **Apply Media Access Control (MAC) address spoof filtering and multinetwork policies** for sensitive workloads to help prevent identity spoofing on the network and keep traffic for high-value applications isolated.
- **Define clear boundaries for secondary networks**, such as Single Root I/O Virtualization (SR-IOV) interfaces, and map them to specific workloads or tenants so that traffic that bypasses the virtual switch remains controlled and auditable.

4 Safeguard data integrity in storage

OpenShift Virtualization brings storage security policies into the same management plane as compute and networking.

You can apply the same encryption, access controls, and replication policies across virtualized and containerized workloads to streamline compliance and recovery planning. Centralizing these controls also makes it easier for storage, security, and platform teams to collaborate on consistent policies and audit them over time.

- **Restrict DataVolume (DV) cloning across namespaces** to keep sensitive datasets within approved boundaries and avoid unintended propagation of regulated or high-risk information.
- **Disable unnecessary shareable disks** to reduce unintended data sharing between workloads and lower the risk of corruption from concurrent writes.
- **Validate errorPolicy settings and storage permissions** for critical data to make sure failed storage operations are handled predictably and only authorized workloads can read from or write to sensitive volumes.

Next steps

Read the full OpenShift Virtualization hardening guide for a comprehensive look at how to harden your organization's IT environment across your hybrid cloud.