WHITEPAPER

SECURE VIRTUALIZATION WITH sVirt

Operating Red Hat Virtualization in a secure manner

sVirt delivers the industry's most secure virtualization platform in an easily administered solution.

sVirt features and protections are available to VMs regardless of the guest OS running in the VM.

EXECUTIVE SUMMARY

Virtualization has revolutionized the way organizations in every industry, agency, and government deploy and manage software. Whether executed on a datacenter, cloud, or a mobile platform, virtualization's flexible application deployment improves the automation, scalability, and uptime of limited resources—improving the efficiency of hardware, space, power, and cooling.

While many virtual machine (VM) technologies offer these benefits, not every option is developed specifically to reduce administrative burdens and security threat vectors that are native to the virtual environment.

sVirt, an alternative to proprietary virtualization solutions, provides a powerful, proven, and easily administered technology with:

- **Proven security.** Co-developed with the National Security Agency (NSA) specifically for the virtual environment, sVirt is backed by the reputation of the United States' leading security agency.
- **System resource protection.** Each VM is isolated so data files, network resources, memory, processes, and applications are prescribed access rules based on predetermined labels.
- **Hypervisor and virtual virus attack protection.** sVirt protects virtualization management systems across machines, regardless of the operating system used.
- **Security-Enhanced Linux® (SELinux) integration**. Incorporated as a Red Hat Enterprise Linux feature after the turn of the 21st century, this deep integration with NSA's own SELinux adds another layer of protection for Linux-powered VM resources.
- **Policy-driven security.** The use of labels and rules based on accessor and accessee privileges reduces administrative burdens—decreasing the chances of user error.
- **Embedded solution designs.** sVirt is designed from the ground up directly into the hypervisor, not as a bolt-on aftermarket feature. It's a necessary product component that puts a priority on security.
- **Open source community support.** sVirt is supported by an active open source community—constantly producing maintenance records and enhancements.

CHALLENGE: PHYSICAL MACHINE THREATS FROM VIRTUAL ENVIRONMENTS

Virtual environment threats can escalate quickly. A single compromised application running with a VM can scale to a hypervisor-level, physical machine, or multi-VM threat. These include:

- **Security threats to hypervisors.** Compromised applications running within a VM can attack hypervisors to access real resources—like the host operating system (OS), host applications, or devices within the physical machine. A single vulnerability within a single virtual application can compromise the underlying physical machine.
- **Security threats to other VMs.** Compromised applications running within a VM can attack the hypervisor to access or control other VMs and their resources. Multiple VM file images can be compromised by virtual viruses due to vulnerabilities in a single virtual application—a situation that is complicated by real network administrative techniques that do not directly apply to virtual environments.

SOLUTION: COMPREHENSIVE SECURITY FOR VIRTUAL ENVIRONMENTS

sVirt was developed in partnership with the NSA and the open source community as one of the industry's most secure virtualization products. sVirt pairs kernel-level architecture with the NSA's SELinux mechanism, which has been an important component of Red Hat Enterprise Linux since version 4. SELinux isolates each VM as a protected process so every system resource—from processes and data files to devices and memory—can be labeled and prescribed access rules based on user types.

PROTECTING INDIVIDUAL PROCESSES

Red Hat's virtualization architecture (Figure 1) treats each VM as its own process managed by a kernel-level hypervisor. Because each VM is a process, it can be labeled by SELinux, effectively establishing a security boundary around each VM. Monitored and enforced by the kernel, this security restricts the VM's access to resources outside its boundary, such as host machine data files or other VMs.

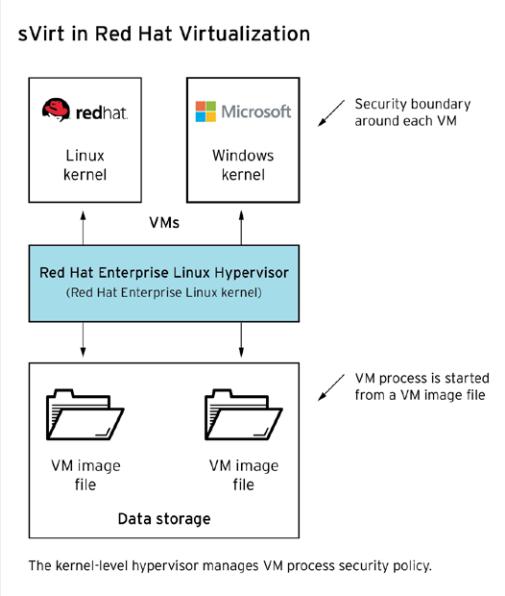


Figure 1: Red Hat's virtualization architecture

REDUCING ADMINISTRATIVE ERRORS

Administrative errors continue to be the leading cause of security holes in virtual environments.[1] sVirt extends the SELinux labeling scheme to VMs, thereby using SELinux's proven capabilities and providing additional important benefits for security administration. sVirt dynamically labels the VM processes according to the policy established on the file images (Figure 2), ensuring processes do not access resources outside themselves. These process labels are applied automatically and dynamically, eliminating administrative burdens of manually labeling resources and enabling an entirely policy-driven security solution.

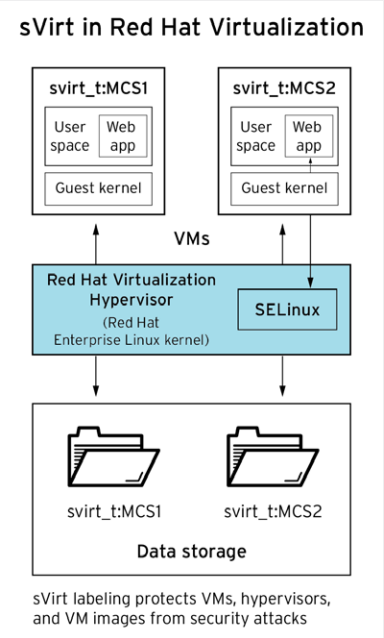


Figure 2: sVirt labeling

MAKING AVAILABILITY A PRIORITY

All sVirt features and protections are available to VMs regardless of the guest OS. The product integrates with Linux or Windows VMs and includes the advanced SELinux feature if the guest OS is Red Hat Enterprise Linux.

Managed by a kernel-level hypervisor, the boundaries are monitored and enforced by the kernel itself. Built from the ground up on the Linux kernel, sVirt is easily implemented—simply enable the Kernel-Based Hypervisor (KVM) kernel module in the host machine to activate Red Hat Virtualization and sVirt. After VM image files are created and labeled, sVirt automatically coordinates the boundary process to protect the host, hypervisor, and other VMs.

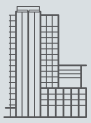
1 *Wueest, C., Barcena, M. B., & O'Brien, L. (2015, May 1). Security Response: Mistakes in the IaaS Cloud Could Put Your Data at Risk. Retrieved July 20, 2016, from http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/mistakes-in-the-iaas-cloud-could-put-your-data-at-risk.pdf*

WHERE TO GET RED HAT SECURE VIRTUALIZATION

- Red Hat Enterprise Linux 5.6 and higher, including 6.x and 7.x
- Red Hat Enterprise Virtualization 3.0 and higher
- Red Hat Virtualization 4.0

FOR MORE INFORMATION

- Virtualization: redhat.com/en/technologies/virtualization
- Security and insights: redhat.com/en/insights/security
- Red Hat Security blog: access.redhat.com/blogs/product-security
- Virtualization security guide: access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Virtualization_Security_Guide/index.html
- SELinux users and administrators guide: access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/SELinux_Users_and_Administrators_Guide/



ABOUT RED HAT

Red Hat is the world's leading provider of open source software solutions, using a community-powered approach to provide reliable and high-performing cloud, Linux, middleware, storage, and virtualization technologies. Red Hat also offers award-winning support, training, and consulting services. As a connective hub in a global network of enterprises, partners, and open source communities, Red Hat helps create relevant, innovative technologies that liberate resources for growth and prepare customers for the future of IT.

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

redhat.com
INC0422238_0716

NORTH AMERICA
1 888 REDHAT1

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