



## Tresys VM Fortress™ Real Virtual Machine Security White Paper

---

*Virtualization has become a hot technology, and for good reason. It provides numerous cost savings, ease of management, and efficiency benefits. However, virtualization security concerns present an impediment to adoption for many enterprises. Tresys VM Fortress mitigates these challenges by providing strong security separation and control using flexible mandatory access control. The result is security assurance and confidence while ensuring that customers retain all the benefits of virtualization.*

## The Security Challenge with the Virtual Revolution

Virtualization has revolutionized many aspects of IT operations. The benefits of virtualization are many:

- Improved hardware utilization and lower hardware costs.
- Increased operational agility and reduced downtime.
- Size, weight, and power reductions.
- Better “green ” footprint.
- Lower total cost of ownership.

Because of these and other benefits, organizations have been moving server farms to virtual machines (VMs ) for some time. Lately, desktop consolidation and other virtualization uses ( e.g., flexible management, mobile computing, hardware sharing ) are increasing the speed of the virtualization revolution.

However, with these benefits come significant new challenges, in particular security. Often the reasons for separate server and workstation hardware are security concerns; by physically separating sensitive applications and networks, security risks can be mitigated. However, the security risks of multiple VMs sharing the same hardware are not the same as multiple real machines. By reintegrating these separate physical machines onto the same hardware using virtualization, we also reintroduce many of the security concerns that necessitated separate machines in the first place.

Worse, the security solutions the industry has evolved for separate physical machines ( e.g., firewalls, DMZs encryption ) are not adequate for virtual machines.

***“ . . . simply applying the technologies and best practices for securing physical servers won’t provide sufficient protections for VMs ”***

***Gartner Group***

## Addressing the VM Security Challenge

The reason why securing virtual machines ( or any sophisticated software application ) is difficult is that modern software applications are extremely complex. So are the operating systems upon which they depend. This complexity is generally a positive trait, allowing for better and more powerful features. As a result, security solutions have ( and probably always will ) struggled to keep up with the fast moving innovation that epitomizes the software industry.

First and foremost, VM applications concentrate on virtualization, as they should. While security is being touted as one of the big advantages of virtualization, it is in effect a by-product of the real design purpose of VM applications. The principal advertised security value of VM applications is the separation into distinct virtual machines, thereby providing the same level of separation and isolation gained by real machines. While there is some truth to this statement, what we have with VMs is in fact very large, complex software applications *sharing* real resources of a single real machine. Not at all like separate physical machines.

A study by Google<sup>1</sup> demonstrated that VMs, like any other software application, are subject to all the security risks and vulnerabilities common to software today, as well as the vulnerabilities and weaknesses of their underlying operating system. While many practical security enhancements have been added to VM applications, something better is needed.

We believe that *flexible Mandatory Access Control* (MAC) is exactly the right technology to provide the proper security for VM systems. The primary feature of flexible MAC is the concept of *type enforcement*, which has recently become mainstream by the growing acceptance of Security Enhanced Linux (SELinux). SELinux is supported in several Linux distributions including Red Hat Enterprise Linux, Ubuntu, Gentoo, and Debian. Type enforcement features also have or are being incorporated into other operating systems including FreeBSD, OpenSolaris, and various embedded and special purpose systems.

**No virtual machine tested was robust enough to withstand the testing procedure used, and multiple exploitable flaws were presented...to readily escape onto the host system.**

**Tavis Ormandy, Google**

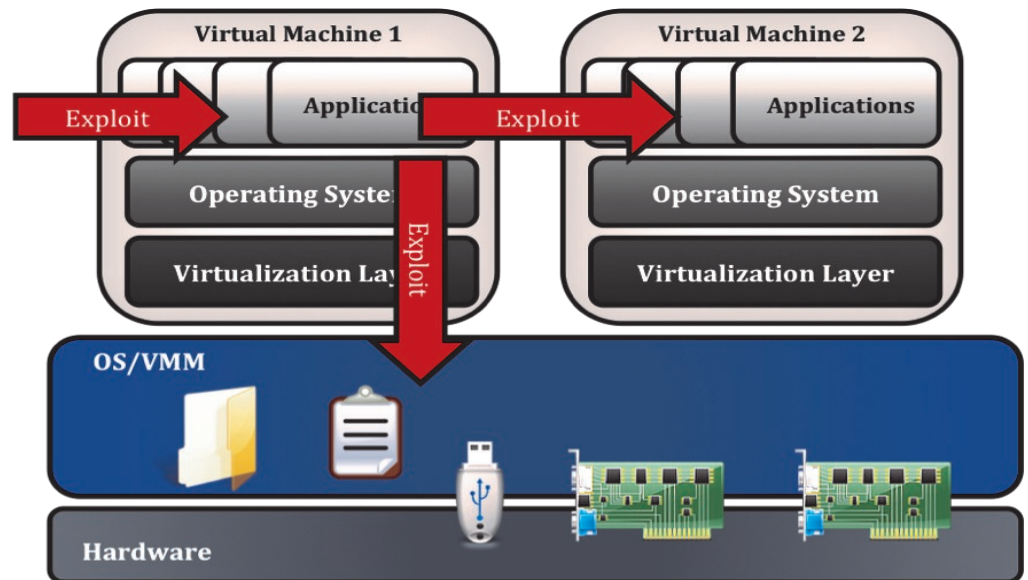


Figure 1. The principal danger with multiple virtual machines sharing the same physical hardware is that a vulnerability in one VM system can be exploited to attack other VM systems or even the real operating system and hardware.

<sup>1</sup> "An Empirical Study into Security Exposure to Hosts of Hostile Virtualized Environments," Tavis Ormandy, Google, Inc, <http://taviso.decsystem.org/virtsec.pdf>.

What flexible MAC provides is a separate, independent, and security-focused mechanism that can isolate and protect individual virtual machines from each other, and control the real resources they can access. We don't have to trust VM processes or even the VM users; flexible MAC will enforce a rigorous mandatory security policy. Most important, we can provide this rigorous security without impacting the functioning of the VM application (unless of course you wish to). For example, flexible MAC can strictly limit which network interface a VM may access regardless of the user's configuration of the VM.

### **Tresys VM Fortress: Flexible, Secure Virtualization**

Using the flexible MAC available in SELinux, we have developed Tresys VM Fortress to provide strong security for virtualization applications that rivals that provided by separate hardware. As a result, Tresys VM Fortress enables an enterprise to get maximum benefit from the value of virtualization while retaining strong security (and even gaining more flexibility).

How does Tresys VM Fortress work? We allow system administrators to easily define *sandboxes* for each VM. A sandbox is a security method for placing an application in a limited, controlled environment that it is safe from other applications (and other applications are safe from it). Virtualization itself is a (weak) type of sandbox, which is nonetheless inadequate for proper security separation.

An flexible MAC-enforced sandbox provides a well-isolated and protected domain for each VM, while allowing the administrator to control which resources (if any) can be shared between VMs. For example, two VMs on the same machine can be restricted to separate network interfaces or prevented from sharing information via cut-and-paste. The enforced flexible MAC sandboxes remain independent of the VM application, and will enforce the security policy regardless of the vulnerabilities, weaknesses, or configuration of the VM application. Not even the VM user can cause a VM to access unauthorized real resources.

As a result of using flexible MAC-enforced sandboxes, exploits and vulnerabilities that impact one VM are contained within that VM, regardless of the vulnerabilities in the virtualization application. The risk of escalating privileges to the access the underlying real system or to attack other VMs is greatly mitigated. Since for many enterprises the primary reason

for separating application onto multiple real machines was increased security confidence, the

## Tresys VM Fortress: Real VM Security

security assurance provided by Tresys VM Fortress provides the confidence needed to consolidate multiple real machines into multiple virtual machines.

Perhaps most important, the strong security of flexible MAC can bring this security confidence to VM applications without impacting the functionality of VMs. With Tresys VM Fortress, the administration decides how many VM sandboxes are needed, what shared resources they may access, and which users can use them. This flexibility allows an enterprise to decide how to consolidate real machines and to decide the security policy for the entire system. Flexible, strong security for virtualization provides the confidence required to enable many enterprises to join the virtualization revolution.

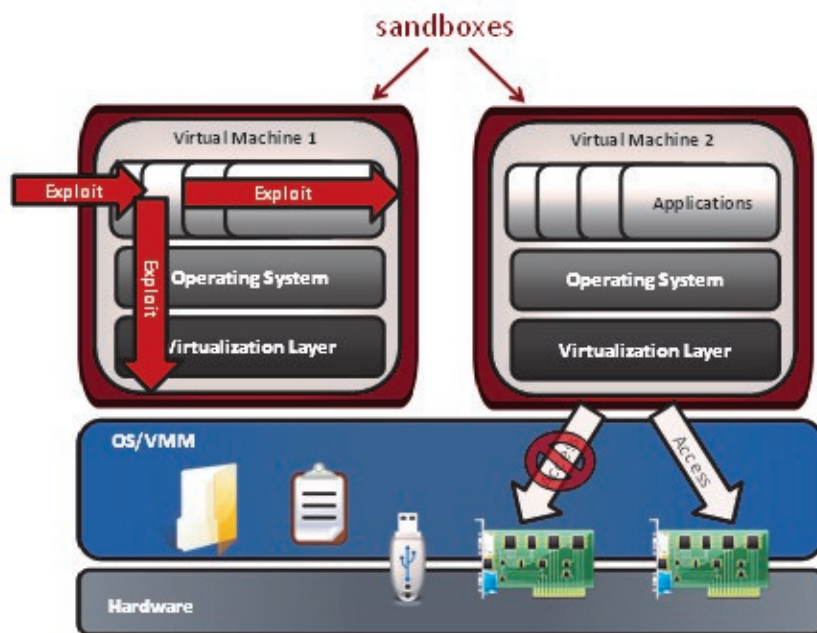


Figure 2. Tresys VM Fortress encapsulates each VM in a sandbox built independently using the strong security mechanisms of flexible MAC. As a result exploits in one VM are contained and cannot be escalated to another VM or the underlying system. In addition, strong limits can be placed on the resources that VMs can share.

### Summary

Tresys VM Fortress uses the security strength of flexible mandatory access control as available in SELinux to provide strong separation and resource sharing control for virtual machines. As a result, the benefits of virtualization can be realized without losing the security protections gained through the use of distinct hardware.

Tresys VM Fortress currently supports Red Hat Enterprise Linux as the host operating system ( with SELinux ) and VMWare workstation or player ( as the virtualization application ). Additional host platforms and virtualization applications are planned.

One of best uses of Tresys VM Fortress is desktop consolidation where security and real separation are significant concerns. Example applications include any environment where a user has two or more workstations to keep multiple networks or application separate. Other applications include sharing workstations (with each user having their own VMs), pooled mobile computing (where the real data is kept in VMs and the laptops are shared), and test environments (where applications need to be tested in controlled, isolated environments). We are also working on extending this technology to the server environment as well as to the “ borrowed ” hardware problem (where you can take your secure environment on mobile media to any available hardware platform).

The virtualization revolution provides tremendous advantages and opens new paths to adoption for many enterprises. With Tresys VM Fortress, this flexibility is available with strong, easy to apply security.

## Contact Us

8840 Stanford Blvd., Suite 2100  
Columbia, MD 21045  
United States  
[www.tresys.com](http://www.tresys.com)

## About Tresys

Tresys provides security solutions that enable customers to achieve greater success by making information technology systems more secure. The combination of acclaimed research and development prowess and practical approach to security solutions has earned the company a distinct reputation in the security market. Tresys has successfully delivered products and services that meet and exceed the needs of the most sensitive security missions, including those at defense and intelligence agencies around the world. These proven accomplishments and a continuing pursuit of thought leadership are part of a strategy that is shifting the way governments and businesses approach sensitive security issues.



Headquartered in Columbia, Maryland, Tresys clients and partners include the U.S. U.K. and Australian Departments of Defense, IBM, General Dynamics, Red Hat and Cisco.

---

Copyright ©2008 Tresys Technology, LLC. All Rights Reserved.

Other names and brands may be claimed as the property of others. Information regarding third party products is provided solely for educational purposes.

Tresys is not responsible for the performance or support of third party products and does not make any representations or warranties whatsoever regarding quality, reliability, functionality, or compatibility of these devices or products.