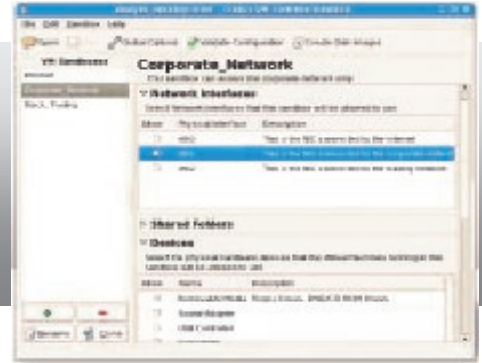


# VM Fortress™

Secure Virtualization

Platform Security Solution



*Tresys VM Fortress generates and deploys hardened systems running virtual machines in independently configured environments separated by Mandatory Access Controls. This contains the guest operating systems and limits potential damage to other guests and the host OS.*

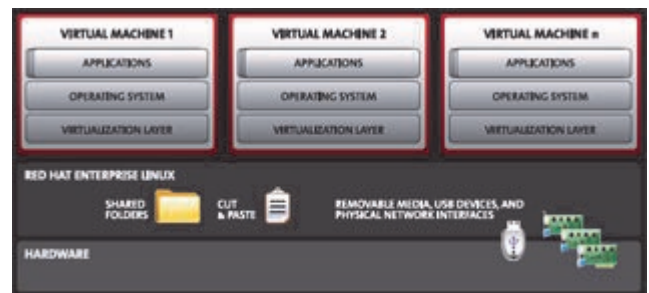
Virtualization adds a new layer of IT security complexity for today's businesses. Now rather than securing one operating system (OS) per server or workstation, administrators must secure the host OS, all of the guests, and the virtualization package. To make matters worse, numerous security vulnerabilities have been exploited that allow attackers to take over a host via a guest virtual machine (VM).

Tresys VM Fortress™ solves this problem by providing strong, independent control over workstation resources and strictly limiting what each VM can access. Administrators simply configure sandboxes that specify which network and file system resources a VM can access. Restrictions are then enforced using the Mandatory Access Controls (MAC) provided by SELinux. Once the access policies are deployed on the system, they cannot be modified...even if an attacker obtains root privileges.

## Tresys VM Fortress™

Tresys VM Fortress is a workstation virtualization security solution that uses a simple GUI whereby administrators can provision "sandboxes". Sandboxes may be pre-loaded with one or more virtual images, or the end user can be given the ability to instantiate VMs within sandboxes at run-time. Access to various resources can be controlled for each sandbox:

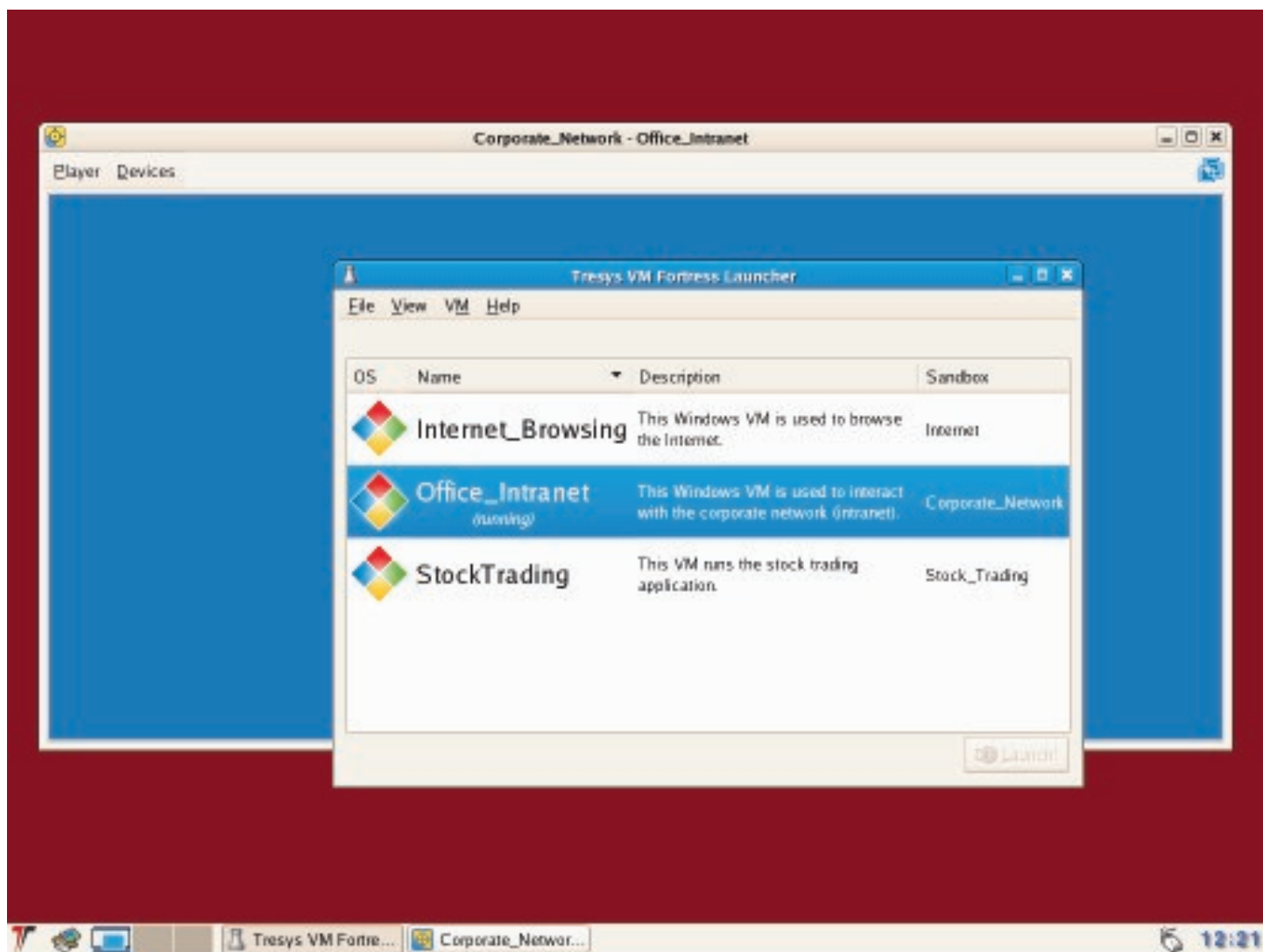
- Network connections / configurations,
- Shared folders,
- USB Devices,
- Removable media, and
- Cut & paste activities.



Other system information may also be configured, including user names and passwords. Once completed, an automated installation package is created that includes the host OS, the guest VM images, and the security configuration for the host system. Desktops can be deployed using removable media or various network protocols.

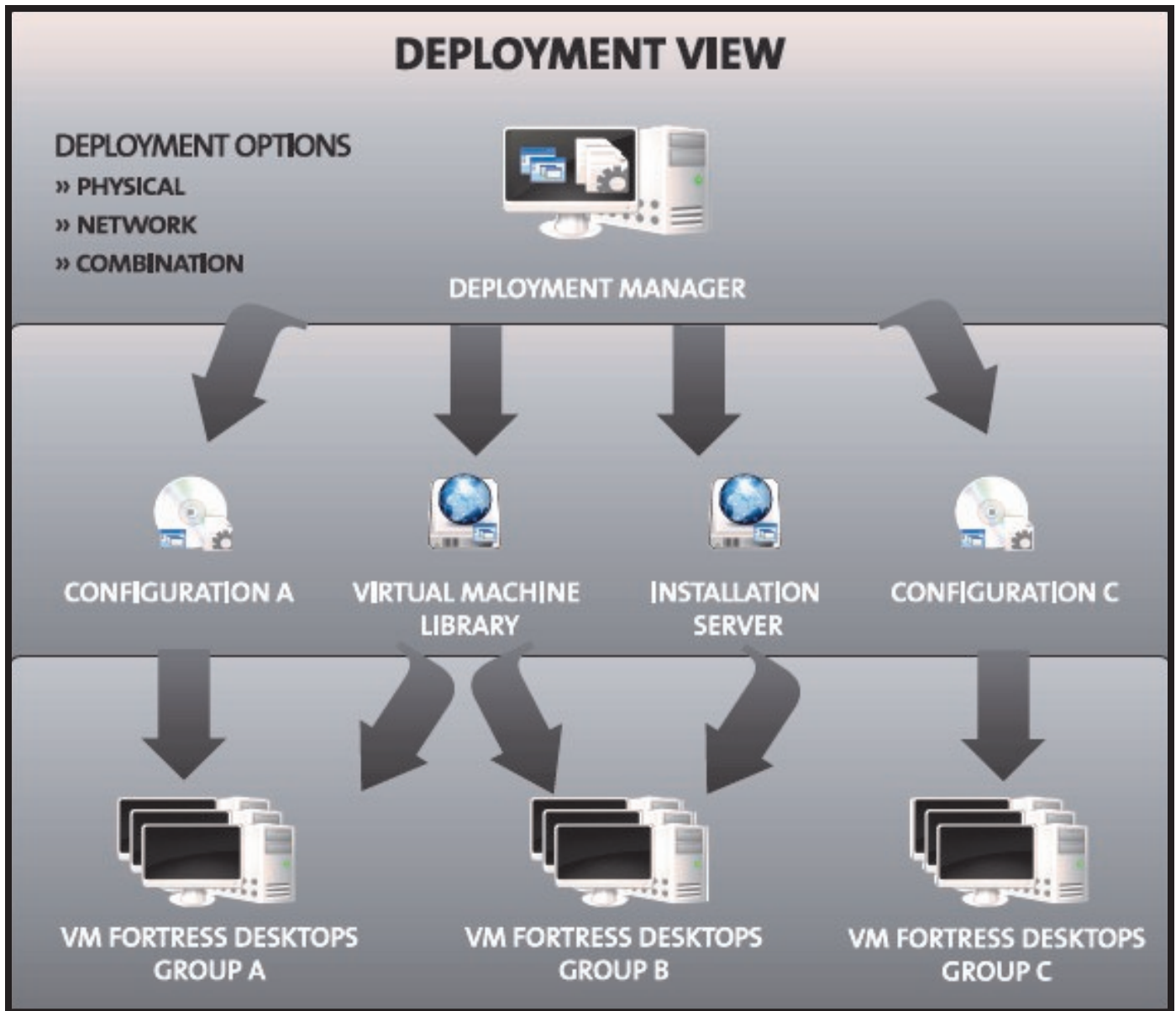
The administrator can specify how the VMs are started: automatically or manually by the user after login. A simplified user experience is provided on the virtualization desktops, based on the user's limited need to interact with the host. This provides a very flexible, secure way to deploy virtualization across an enterprise.

## Tresys VM Fortress™ Workstation Interface



- Deployed virtualization desktops present a simplified and locked down user environment. The primary application is the Launcher. This presents a list of virtual machine the user can start. The desktop can also be configured to start the VMs automatically.
- VM images can be stored locally or deployed over the network. Users can even be given permission to instantiate new VMs from a list of acceptable images (either locally or over the network). When a new VM is added, a fresh copy of the VM image is adapted to the system security settings. Multiple virtual machines can be run simultaneously in separate windows or full-screen, in different workspaces, or even on different displays.
- VMware Workstation and Player are both supported, including Workstation features like snapshots.
- Users can manipulate some configuration items: sound card volume, mouse configuration, user password. But the user's ability to run other application on the host is restricted.

# Tresys VM Fortress™ Deployment Management



Configurations created on a Deployment Manager can utilize your existing virtualization infrastructure to deploy virtualization workstations. You can deploy systems using CD/DVDs for the entire process, utilize various network options to perform a completely diskless installation, or any combination that makes sense for your environment.

**Boot Options**

CD/DVD  
PXE

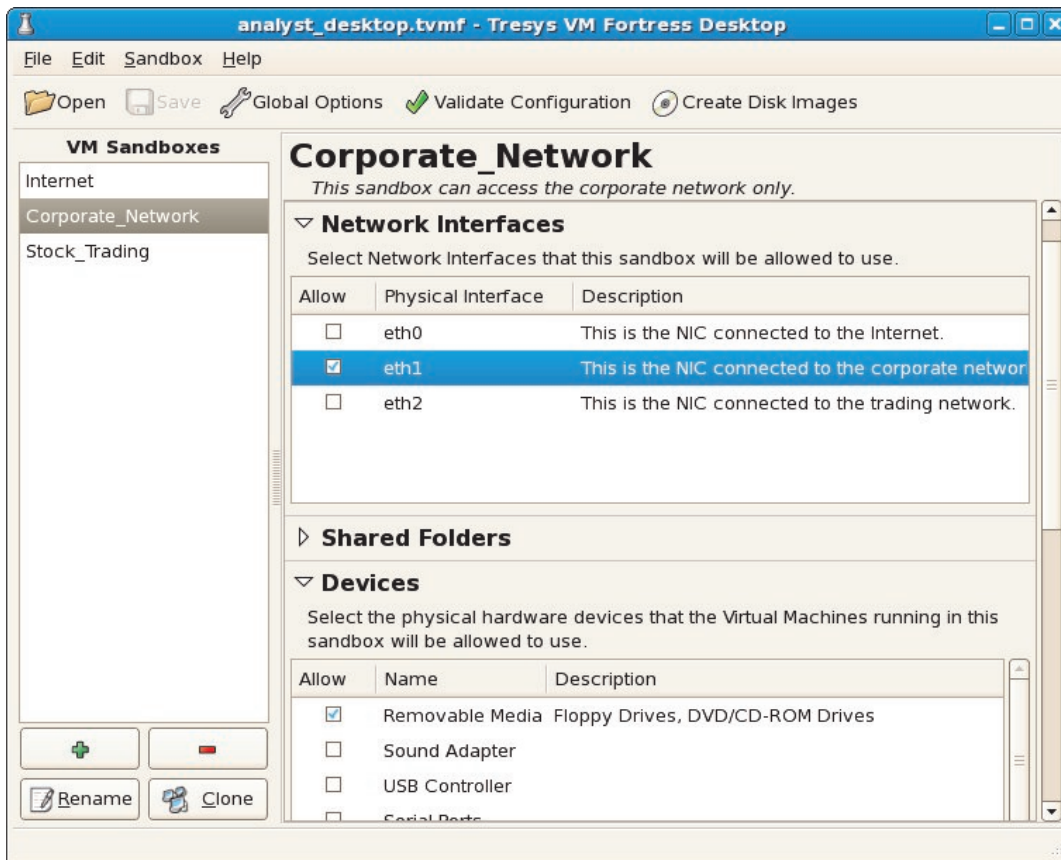
**Host Installation**

CD/DVD  
NFS  
HTTP

**VM Distribution**

CD/DVD  
FTP/SFTP  
HTTP  
Samba

# Tresys VM Fortress™ Deployment Manager



## Configurable Access Control

Tresys VM Fortress Desktop controls access to many system devices including:

- Network cards
- USB devices
- Removable media (floppies, CDs, DVDs)

Controlled information sharing between virtual machines can be enabled or disabled to meet your environment needs

- Shared folders
- Cut & Paste

## Supported Platforms

- Red Hat Enterprise Linux v5 - 32 & 64 bit x86
- VMware Workstation v6 & Player v2

## About Tresys

Tresys innovates and applies advanced technologies to quickly solve the needs of customers requiring agile responsiveness to security requirements. By leveraging secure open source software, our products and services support the most sensitive security missions around the world. As a result Tresys enjoys a distinct reputation for shifting the way governments and businesses approach security. For more information, visit: [www.tresys.com](http://www.tresys.com).

