# FOCUS Brief: Secure Virtualization Management, Reflex Systems


## Abstract

As virtual infrastructures become more prevalent and complex, supporting both production server workloads and centralized desktops, the ability to both monitor and manage security throughout that virtual infrastructure becomes vital. Reflex Systems has brought together a new generation of products to create their Secure Virtualization Management suite. The Reflex suite bridges the gaps between virtualization security, network management and root cause analysis.

This FOCUS Brief describes what is driving IT to seek improved security and manageability of the virtual infrastructure, and details Reflex Systems' Secure Virtualization Management solution, listing key benefits. The Brief concludes with a FOCUS assessment.


## Introduction

Prior to virtualization, network switches provided a secure perimeter to the datacenter. When IT organizations implement virtualization, some of these switches move from physical perimeter devices to virtual switches inside a physical server. This shift created the need for security solutions to secure the virtual switches as well to maintain the perimeter. Going a step further, as companies build out their virtual server infrastructure it also becomes necessary to have visibility of all components, integrating security at all levels of the virtual management stack. For example, if a virtual machine (VM) goes down, was it under attack or was the failure caused by a configuration change, or CPU or memory limitations? As Reflex Systems founder and CTO Hezi Moore explains, "If you can't see it, you can't manage it and you certainly can't secure it."

## Drivers

Companies have gained significant benefits through consolidation using server and desktop virtualization technologies. However, the move to virtualization has also created challenges:

- Within the virtualized infrastructure, some of the components that interact with the virtual hosts have also become virtualized, such as virtual switches, virtual NICs, and virtual HBAs. Depending on which hypervisor is used, administrators have varying degrees of visibility of these virtualized components.

**Product Name**
Secure Virtualization Management
**Company**
Reflex Systems, Inc.
Founded in 2000
First product released in 2006
www.reflexsystems.com
**Funding**
Privately held
VMworld 2008 Best of Show

- Virtualization and live migration make monitoring and auditing of the dynamic virtual environment more difficult. In addition, human error can leave security holes open for inter-VM attacks, Worms, Malware, etc.
- Virtualization removes physical isolation of servers, increasing security concerns for virtual servers that reside on the same physical server. In addition, companies are held to regulatory compliance measures around privacy and tracking such as HIPPA, SOX, and others.
- When a virtual machine goes down, discovering why the failure occurred is challenging. With a virtual infrastructure and multi-tier applications involving multiple virtual machines and virtual switches, it is often extremely difficult to correlate a failure to its true root cause.
- Performance bottlenecks can occur at all levels of the application stack, both physical and virtual. The ability to monitor virtual network bottlenecks and correlate those to virtual machines is challenging.

These issues are driving IT to seek solutions that both provide visibility, security, and flexible management of the entire virtual infrastructure. Reflex Systems' Secure Virtual Management solution delivers the next level of virtual security management that addresses these issues.

# FOCUS Brief: Secure Virtualization Management, Reflex Systems

## Solution Description

Today, Reflex Systems' Secure Virtualization Management solution is made up of two primary components; the Reflex Virtual Management Center (VMC) and the Reflex Virtual Security Appliance (VSA). These components provide the following:

- **Virtual infrastructure discovery and mapping** including the entire application stack through the OS, VMs and virtual components, e.g., virtual switches, as well as physical components including storage and network components.
- **Revision control and monitoring** including roll-back and fault correlation.
- **Application and services discovery and monitoring** to detect configuration changes, potential and current bottlenecks, and failures, within the application/server stack.
- **Virtual network security** including firewalls, intrusion detection, and intrusion prevention to protect virtual switches as securely as physical switches
- **Virtual network and application performance monitoring** with trending over time to correlate with configuration changes in the entire infrastructure, virtual and physical for root-cause analysis. This includes the ability to track packets through the infrastructure to glean detailed performance information.
- **Virtual machine lifecycle monitoring and management** including configuration capture and correlation of security, configuration changes, performance and application relationships throughout the lifespan of the VM, bridging the gap between configuration management, performance and security.
- **Support for** VMware ESX, Citrix XenServer and Microsoft Hyper-V hypervisors.

As a leader in virtualization security, Reflex also has been involved with VMware's VMsafe initiative since its inception. VMsafe is an API that will allow security solutions to tightly integrate at a very low level with ESX to better secure the virtual infrastructure. Reflex has a working prototype that will be available when VMware delivers it initial ESX VMsafe release.

## Key Benefits

Reflex began providing virtual network security with their Virtual Security Appliance, released in 2006. It soon became clear that broader monitoring and management of the virtual infrastructure was required to truly manage security in this new virtual environment. Reflex expanded their product suite to address the broader requirements by providing:

- Analysis and trending over time, rather than just a point in time
- Correlation with other environmental information such as configuration changes, security events, and traffic analysis
- The ability to track packets at any stage from the physical NIC on the host to a virtual NIC on a VM.

## FOCUS Assessment

Integrated management, troubleshooting and root cause analysis are fast becoming one of the biggest challenges IT faces with this new virtual infrastructure. The ability to discover, monitor and manage, and provide analysis and trending over time of all components of this infrastructure, both virtual and physical is essential to determining the root cause of unexpected behavior, whether slowed performance or failure. Reflex has raised the bar on virtualization security and carries the concept to the next level of integrated management for virtual environments.

## About FOCUS

**FOCUS** delivers research, analysis, and consulting, focused on systems, software, and storage. Focus areas include server, desktop, and application virtualization/streaming; systems, storage, and enterprise management (physical and virtual); high availability, disaster recovery, and business continuity; blade systems (server, workstation, and PC); storage, network, and I/O virtualization; storage and storage networking (NAS, SAN, Fibre Channel, iSCSI); and business benefits of technology (ROI, TCO).
www.focusonsystems.com