REFLEX SECURITY

Virtualization Data Center Management and Security

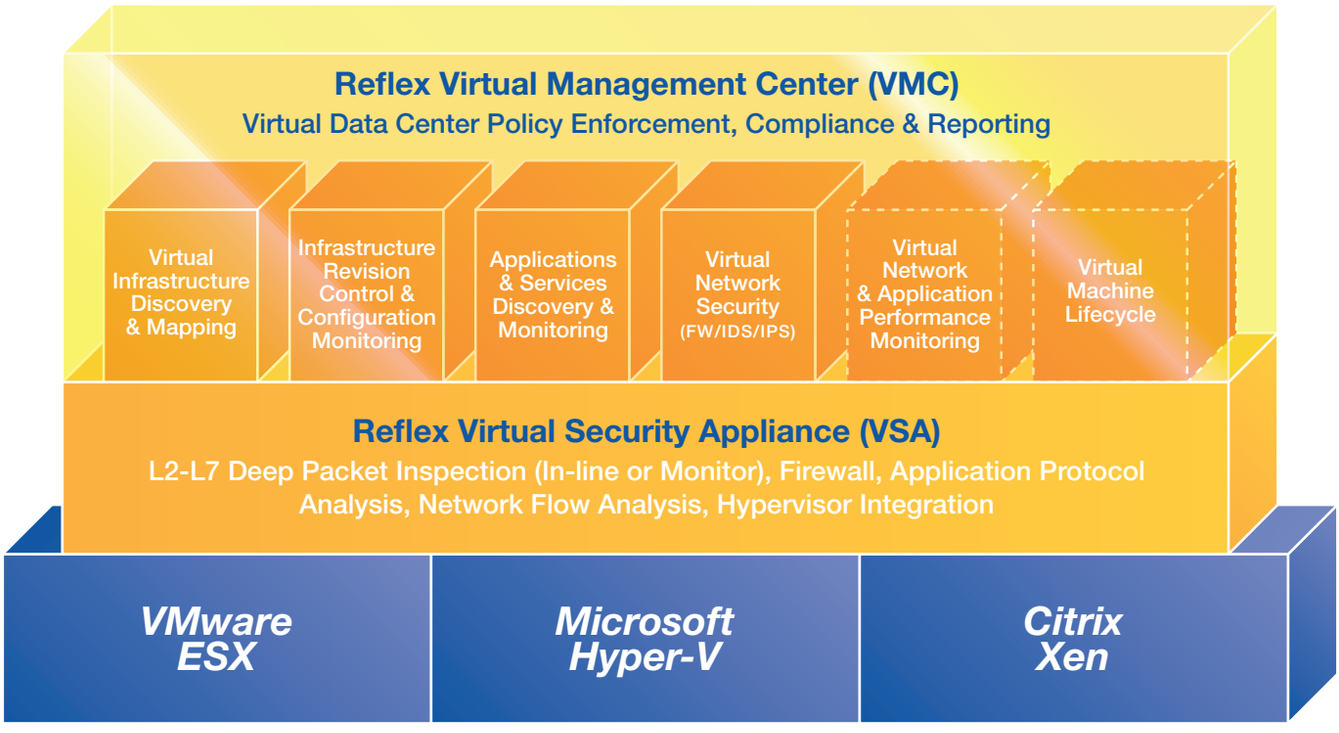
Reflex helps organizations realize the cost savings and productivity benefits of virtualization. Reflex's Virtualization Management Solution enables next generation data centers to enforce IT policies, ensure compliance with government mandates, and manage and protect virtual servers, desktops, and networks across VMware, Microsoft and Citrix platforms. Purpose-built for virtualization on a strong security foundation, Reflex's Virtualization Management Center provides the essential tools needed to bridge the gap between security and management in the virtualized data centers. Virtualization management must be tied back to security and how changes or events within the virtual environment can impact your entire business.

Reflex Virtualization Management Center (VMC)

Reflex VMC is a software solution which bridges the gap between security and management in the virtual data center. Reflex's VMC runs as a single virtual machine which can discover and map each element of the virtual infrastructure while providing centralized visualization, revision control, policy management and reporting functions. The VMC also manages the Virtual Security Appliance (VSA), the virtual monitoring and control software that runs on each physical host. VSA can run in off-line monitoring mode or in-line enforcement mode. This architecture enables the VMC to scale to thousands of virtual machines spanning multiple locations. The VMC automatically monitors and filters all virtual network traffic (including all application protocols) and enforces IT and business policies.

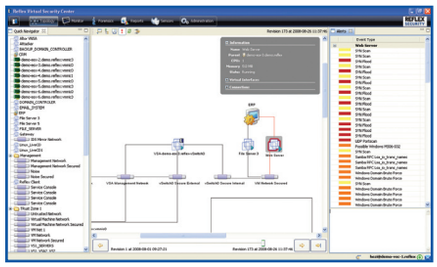
Reflex Virtual Security Appliance (VSA)

Reflex VSA provides security controls by integrating firewall, L2-L7 deep packet inspection, application protocol awareness, network flow analysis and hypervisor integration complete virtual security solution. Reflex VSA can safeguard communications between virtual components and resources outside the host machine. This provides a complete security perimeter around and between virtual machines (VM) and reduces the risk of virtual machine intrusion, infection, compliance violations or other consequences.



Virtual Infrastructure Discovery and Mapping

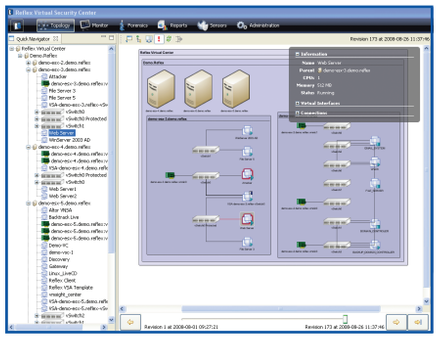
Since you can't control what you can't see, visibility is key in managing, monitoring and securing the dynamic virtual infrastructure. Administrators need a logical visual representation of their virtual environment in order to understand the virtual network, track changes and address virtualization challenges that have security implications like server sprawl, server mobility, configuration and infrastructure changes.



Virtual Infrastructure Logical Topology

Revision Control & Configuration Monitoring

To maintain secure configuration in virtual environment, organizations need the ability to track all infrastructure changes in real-time as well as historically to identify unauthorized configuration changes, configuration errors and enforce policies across the entire virtual network infrastructure. Revision Control allows users to monitor the virtual environment through a timeline-based graphical topology view and correlate security events and alerts in context to perform forensic analysis and control the dynamic environment.



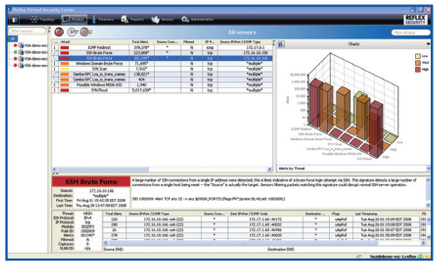
Revision Control and Inventory View

Application and Services Discovery and Monitoring

Application/services visibility and awareness inside the virtual infrastructure identifies which applications/services are running on which virtual machines. Utilizing VMC and VSA, administrators can detect application dependencies and misconfigurations, reduce overall security risks and optimize the virtual network infrastructure to support its service level business requirements. This capability is done at the network level and eliminates the need to deploy agents with every virtual machine.

Virtual Network Security

Integrated firewall and deep packet inspection provides a complete security around and between virtual machines to reduce the risk of virtual machine intrusion, infection, compliance violations or other consequences. Reflex VSA can inspect virtual network traffic for known malicious activity, detect network anomalies and alert users of the event. If deployed in-line, VSA can take action and block packets based on network policy. Policy enforcement at the virtual network layer provides the user the capabilities to address security incidents in the virtual environment.



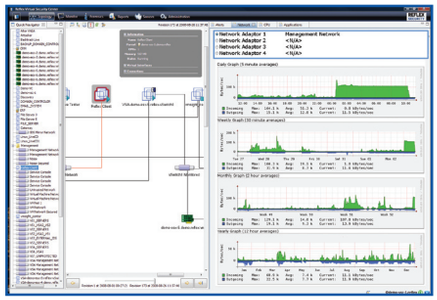
Virtual Network Security Events

Virtual Network Performance & Monitoring

Monitoring and managing virtual network performance enables organizations to increase business efficiency and business continuity in the datacenter. The ability to detect network bottlenecks inside the virtual infrastructure, over-utilized VMs, performance issues of a critical applications, and network outages will allow administrators to improve the service level for critical applications, quickly troubleshoot issues and optimize virtual infrastructure.

Virtual Machine Lifecycle

Monitoring the health of a virtual machine throughout its lifecycle is essential to managing your virtual environment securely. Reflex VMC provides vital information about the VMs and the surrounding virtual infrastructure to manage VM sprawl, track VM changes and performance, and monitor security events throughout the VM life span. These events and changes must be managed in context with security to accurately understand the impact on the network and ultimately the business.



Performance Monitoring

System Resource Requirements

Component	vCPU (min, max)	RAM (min, recommended)	Available Storage
Reflex VMC Server	1	1G, 2G	4GB
Reflex VSA(each)	1,4	512, 768M	60MB
Reflex VMC Client*	1	1G	200MB

*** Client is supported on Microsoft Windows™ XP SP3 and Microsoft Windows™ Vista SP1**

REFLEX SECURITY
53 Perimeter Center East, Suite 175
Atlanta, GA 30346 USA
Tel +1.770.408.2034
fax +1.770.408.2035
www.reflexsecurity.com