

VMFW™ Enforcer for ESX/ESXi Servers

RedCannon VMFW VM Enforcer for ESX is a VM Appliance which can be seamlessly deployed as a VM within ESX server to control & enforce security policies on ESX Server as well authorized VMs running within it's virtual environment. Through central policy control, VM Enforcer can prevent uncontrolled VM sprawl, Unauthorized VM migration, VM Poaching and a host of other virtualization specific vulnerabilities .

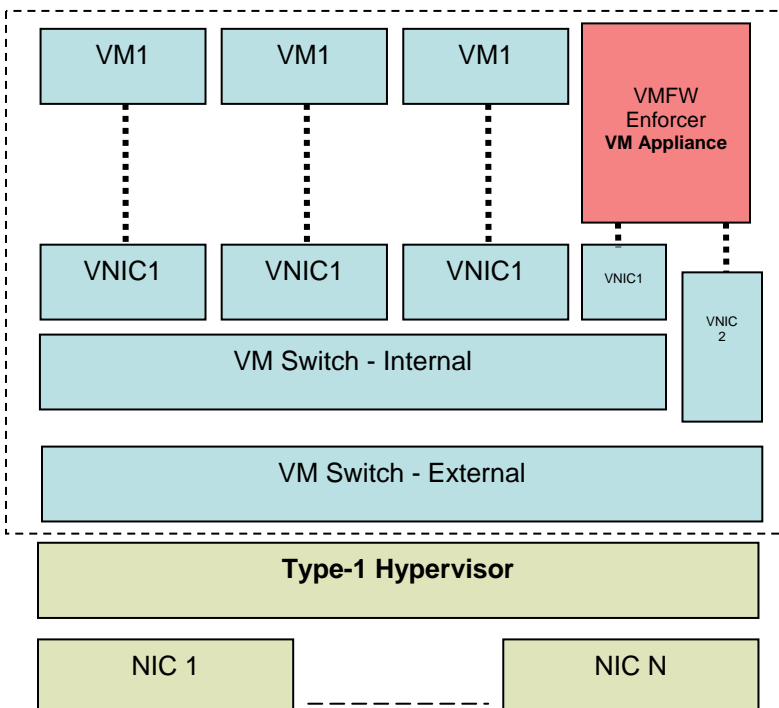
RedCannon VM Firewall is a Unified Threat Management solution for Enterprise Virtualization through Virtualization vulnerability monitoring, enterprise compliance enforcement on virtualization & Network-based FW & IPS in a single VM Appliance. VMFW Enforcer for ESX is designed to enforce Enterprise security policy on the ESX & ESXi servers by controlling VMs & their behavior as well protecting against potential ESX-based virtualization related vulnerabilities.

Secure VM Environment (VME) Requirements: An Enterprise VM Security Policy needs to ensure that enforcements are made across every machine that is or can potentially act as virtualization host. Policies such as the following & many more need to be addressed in an Enterprise virtualization Environment.

- Which VMs are allowed to run on which ESX server
- Allow more than a certain number of VMs on each server?
- Should you allow VM Migration? To which ESX server?
- Allow VI Console Access? From which computers?

Hypervisor Enforcement: Type-1 hypervisors such as VMWare ESX Server are extremely difficult to break-in to since they run bare-metal on the hardware without any OS. However the service console which allows access to certain server functionality could compromise the security of the entire virtualization environment including VMs running within. Central policy control on the ESX server. VM migration as well to secure network access for VM& VM Host applications.

Persistent VM Tagging: Policies for authorized VMs have to



stay with VMs regardless of whether VMs move from one Sever to another or is copied. VMFW Enforcer uses a unique patent-pending technique called "VM Tagging" to tag authorized VMs. Like electronic tagging of computers, these VM tags allow VMFW Enforcer to identify each VM & it's derived VMs uniquely and thus enforcing central policies for these VMs. The VM Tag moves with the VM whether the VM migrates from one server to another. VM tags also can be used to tag VM templates which subsequently used to create VMs in server environment, retaining the tagged identity of the original VM template.

Complete Network Enforcement: RedCannon VMFW Enforcer also has a VM-aware stateful Firewall with built-in network-based IDS. It eliminate OS & network vulnerabilities from the ESX Server & all the VMs running within. VMFW Enforcer can be configured just like any other network based firewall with allow or reject rules for certain types of traffic. In addition however it has the built-in intelligence to detect VMWare Virtual Infrastructure (VMWare VI) specific protocols as well as VM traffic. Through centrally distributed policy for the VMFW, it can create internal rules to allow or reject ESX/ESXi specific traffic such as VMotion for VM Migration & ESX/ESXi Service Console Access.

VMFW Manager is used for policy creation, deployment, software change management, log collection & report generation for all VMFW modules including Enforcer for all VMWare ESX/ESXi deployments within the organization or it's Data Center.

Eliminate Virtualization Vulnerabilities:

- VMSprawl Control
- Incorrect VM Isolation
- VM Poaching
- Uncontrolled VM Migration
- VM Denial Of Service
- Unauthorized VMs & VM Hosting
- Potential Hyperjacking
- Unintentional VM Tools exposure
- Dangers of VM Escape
- Guest VM OS & network vulnerabilities

Specifications:

- Supports VMWare ESX/ESXi Servers
- VM Appliance for seamless plug-in to ESX/ESXi environment
- Web interface for VM n/w config & for file down/up load
- Separate management LAN i/f