

RedCannon vDefense — Security for VMWare and Cisco Virtualization Infrastructure

RedCannon vDefense is a centralized Unified Threat Management solution which combines Virtualization vulnerability monitoring, enterprise compliance enforcement on hypervisor and running VMs, Network-based Firewalling and traffic isolation for VMWare vSphere servers. vDefense solutions includes vDefense Enforcer, a network appliance which can monitor the entire Enterprise virtualization server farm from a single appliance. This revolutionary approach to virtualization security substantially differs from current virtualization security & firewall products, which are typically a VM running on each virtual server

Plug-and-Play Virtualization Security: Unlike all currently available virtualization security solutions which are either GuestOS based (end-point solution) or Server based (VM Appliance), vDefense Enforcer is a network-based device. GuestOS require deployment & management of an endpoint security agent on each GuestOS while Server-based solutions require a VM appliance to be deployed on each server. Both of these approaches tremendously increase deployment & management overhead because of sheer number of instances required to be deployed & managed. vDefense Enforcer however is a plug-and play device. Simply plug the vDefense Enforcer into an available network port on a switch & immediately network, VM & hypervisor policies for each of the configured servers starts getting enforced.

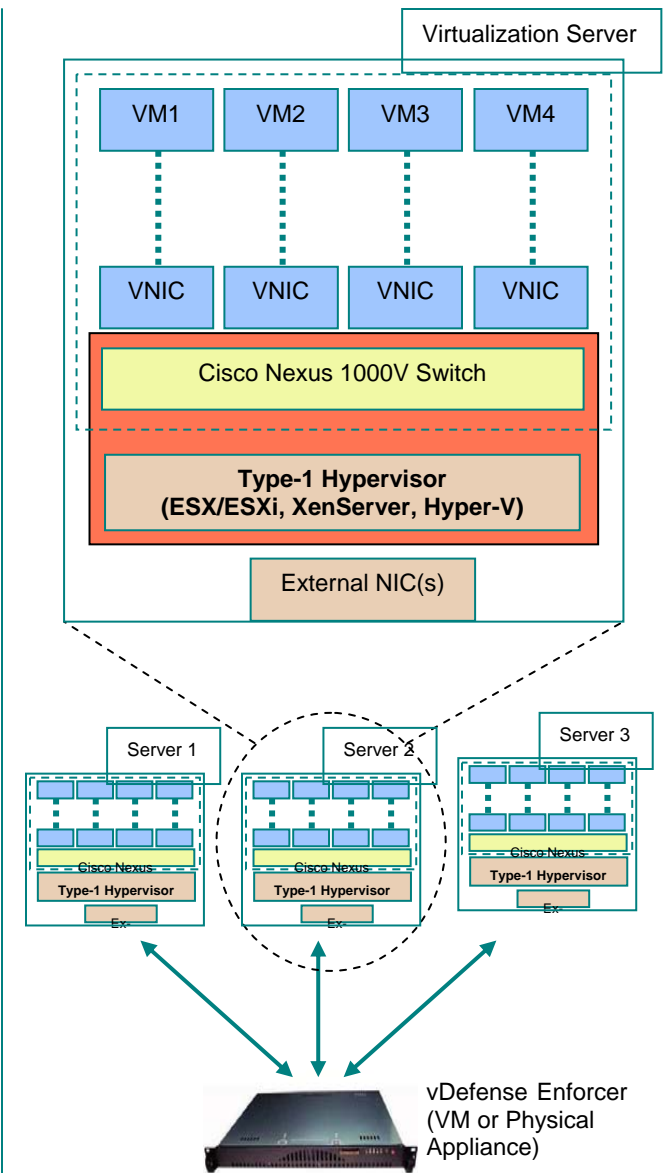
Zero-Server Impact : GuestOS-based (endpoint) security solution would impact the server performance since they require additional processing for each guest VM on the server. The server-based (VM appliances) security software not only run as separate VM, taking away CPU cycles, memory & hard-disk space from production virtual machines for which the servers are deployed in the first place. Moreover in order to enforce firewalling on the VM traffic, some of the server-based FW solutions reconfigure the internal virtual networks, impacting the entire internal virtual networking of the server. If the networking breaks, the critical production VMs are in-accessible. Since vDefense Enforcer physically sits outside of the virtualization server, there are no server resource impacted and the entire virtualization server bandwidth remains available for deploying Enterprise virtual machines.

Hypervisor Compliance Enforcement: Type-1

hypervisors such as VMWare ESX Server are difficult to break in to since they run bare-metal on the hardware without any OS. However the service console which allows access to all server configuration and other functionalities could compromise the security of the entire virtualization environment including VMs running within. Other areas of security concerns and potential exploits are Guest VMs and their corresponding configurations in the hypervisor, virtualization tools either running in the service console (Dom0 for XenServer or Parent Partition for Hyper-V) and communication methods for management tools. vDefense Enforcer not only detects and thwarts potential exploits but also detects configuration related vulnerabilities and enterprise compliance enforcement through Central policy control on the ESX server, the service console, Guest VMs, VM migration and ensures secure network access for VM & VM Host applications.

Migrating policies with VM: Policies for authorized VMs have to stay with VMs regardless of whether VMs move from one Server to another or is copied. vDefense Enforcer uses a unique patent-pending technique called "VM Tagging" to tag authorized VMs. Like electronic tagging of computers, these VM tags allow vDefense 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.

Network Traffic Isolation: RedCannon vDefense Enforcer has a VM-aware stateful Firewall with built-in DDoS detection and mitigation using traffic-shaping. Utilizing the Cisco Nexus1000V based traffic control engine running within the hypervisor, vDefense Enforcer enforces firewalling for all VM-to-VM, Network-to-VM & Server-to-VM Traffic. vDefense 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 vSphere) specific protocols as well as VM traffic. Through centrally distributed policy for the vDefense, it can create internal rules to allow or reject specific traffic such as VMotion for VM Migration & Hypervisor Service Console, Dom0 or Parent partition Access.



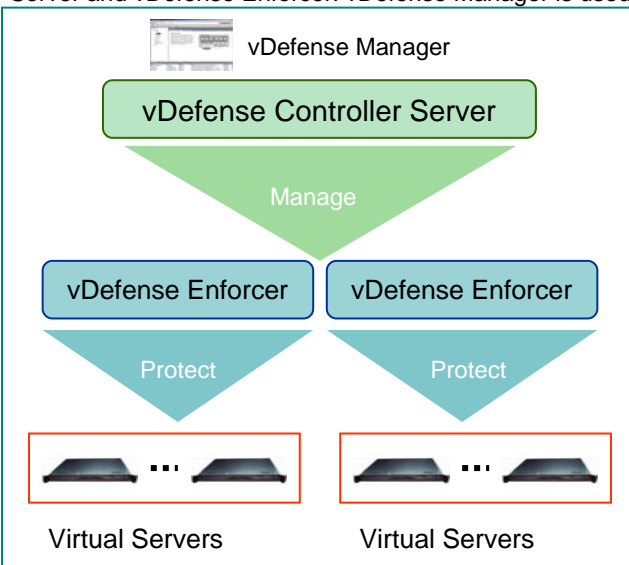
RedCannon vDefense — Security for VMWare and Cisco Virtualization Infrastructure

Total Integration with Virtualization

Infrastructure: vDefense is one of the few solutions available that are tightly integrated with VMWare vCenter and Citrix XenCenter virtualization management suits. An intelligent import Wizard allows the IT admin to instantly identify & secure virtualization servers, VM templates and running VMs for policy enforcement along with their respective network-interfaces for firewalling. This level of integration makes virtualization security administration, management and maintenance extremely efficient and cost-effective.

vDefense Enforcer is the only currently available solution which leverages existing Cisco virtual-switch infrastructure to seamlessly build firewalling and DDoS detection & mitigation. An easy to administer firewall policy template can be configured and applied across the entire virtualization server farm by click & apply configuration. vDefense can automatically identify Cisco VSM & VEM association for vNICs which are configured for protection, configure the port profiles appropriately and continuously monitor rules to make sure traffic policies are maintained and enforced dynamically.

Scalable Policy Management: vDefense Solutions have a 3-tier management hierarchy of vDefense manager console, vDefense Controller Management Server and vDefense Enforcer. vDefense Manager is used



for policy creation, deployment, software change management, log collection & report generation for all vDefense modules within the organization or it's Data Center. vDefense Controller appliance can manage up to 50 vDefense Enforcers simultaneously to provide a scalable deployment across an entire virtualization farm.

VM & Hypervisor Policy Enforcement Module

- Supports
 - VMWare ESX/ESXi (VI 3.5 & VI 4.0)
 - Citrix XenServers (ver 5.0 & above)
 - Microsoft Hyper-V*
- Detect all configured & running VMs
- Enforce VM Policies on each authorized VM
- VM Isolation by controlling VM-to-VM & VM-to-NW traffic

Enterprise Compliance Module

- VM Zoning to enforce compliance for select VM Zones to run on select Virtualization servers
- Enforce instant VM Sprawl Control on unauthorized VMs

NW Enforcer Module

- Integrated L2-L7 Network Firewall utilizing Cisco Nexus 100V switching infrastructure
- Stateful Analysis of Applications such as HTTP, FTP, SMTP/POP/IMAP, IM & others
- Full support for VMWare Management Protocols
- DoS & DDoS detection & mitigation using rate-shaping
- MAC & IP Address spoofing for all VMs & VMHost

Scalable Deployment

- 3-Tier Architecture supported by a vDefense Manager Console, vDefense Controller the Management Server & vDefense Enforcer Appliances deployed across entire Enterprise & it's data centers
- Utilizes standard Enterprise software distribution methods for initial installation of agents.

Centralized Administration & Management

- Multi-user tiered access via Web console
- Provides centralized policy creation and administration
- Complete change-management for policies & software
- Web-based statistics, alerts and reporting

vDefense Features:

- ▶ Virtualization Vulnerability Monitoring and Intrusion Prevention
- ▶ Enterprise Compliance Enforcement on Virtualization Servers & VMs
- ▶ Firewalling for VM-to-VM, VM-to-Network & VM-to-Server traffic
- ▶ Up to 500 Servers & 5000 VMs supported from a single Enforcer
- ▶ Throughput scales to true wire-speed gigabit processing
- ▶ No Server or VM reconfiguration required
- ▶ Policy Enforcement for Hypervisor, VMs, Service Console & Network traffic
- ▶ Web-based Central Configuration, Change Management & Reporting
- ▶ Real-time Stats & Alerts
- ▶ Eliminate Virtualization Vulnerabilities & exploits, such as:
 - ▶ 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
- ▶ Appliance
 - ▶ VM appliance or 1U rack-mountable box
 - ▶ Off-line Enforcement (No in-line connection)
 - ▶ Plug-and-Play with Cisco Nexus 1000V switch and VMWare vSphere infrastructure