

RedCannon vDefense — Managed Security Services for Cloud and Data Centers

A recent IDC report forecasts Cloud Computing to be a \$44B market by 2013, making it 10% of the IT-spending. This forecast doesn't even include \$19B of proposed IT-budget expected to be spent by the US Government. However according to a recent Internet survey by Unisys shows that the leading concerns of Enterprise IT professionals looking to adopt Cloud-based computing are the cloud security & data privacy issues.

To address the specific issues of Cloud and Data center based VM data & server isolation, RedCannon has designed its vDefense virtualization security solution to provide Unified Threat Management by combining Virtualization vulnerability monitoring, enterprise compliance enforcement on virtualization & Network-based FW & DDoS prevention in a single off-line network appliance which can monitor & enforce security on an entire cloud server farm.

Zero-Impact Virtual Security Services: 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.

Especially since server-based solutions 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. On top individual server based installation, deployment and management is a huge overhead. Since vDefense Enforcer physically sits outside of each server, there are no server resource impacted and the entire virtualization server bandwidth remains available for deploying Enterprise virtual machines. vDefense provides the most appropriate & scalable solution for Cloud and Data Center virtualization related security services.

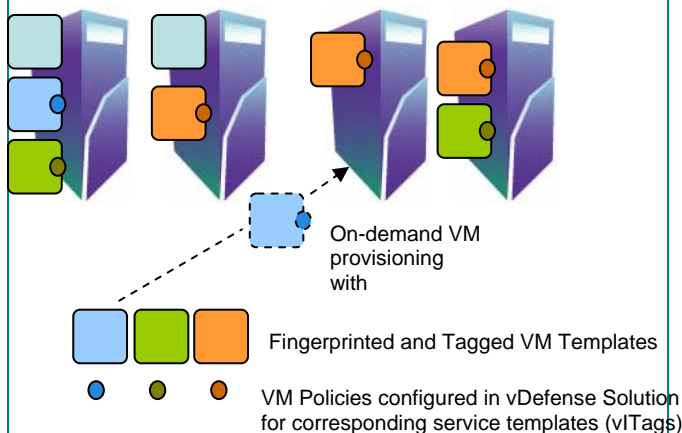
Regulation Compliance Services:

RedCannon vDefense VM Zoning can provide the desired level of segregation to Enterprise customers subscribing on-demand VMs from Cloud or Data Center Service Providers. For example, a provider can offer an a la cart menu of pre-configured PCI-DSS compliant VM templates for

different purposes such as credit card payment processing. These VM templates would be hardened with security and encryption enforcement tools to ensure compliance with PCI-DSS regulations. By creating server and VM Zones, the provider can ensure that when a customer subscribes a VM from the template that it would only run on the designated set of physical servers that would have a separate, fortified data storage as well as network segregation from the rest of the data center traffic. This would help eliminate large number of compliance related questions in an enterprise customer's mind when they are looking to utilize cloud for off-loading their credit card processing. Same can be true for HIPAA and other regulations.

Here is an example for a web-based application Virtual Machine and how vDefense security can be automatically provisioned when a VM instance is created on-demand by a customer

1. Create a VM Object from the Web-server VM template (Blue box in the picture)
 2. Define its VM enforcement policy. – For example to provide network isolation for this VM, configure the VM policy to enforce NIC Isolation on a "Web" port group that is part of Cisco Distributed Switch (VEM) along with other VM enforcement parameters
 3. Add "Web" port group for protection (through RedCannon vCenter Import Wizard) on the Cisco VSM that controls the corresponding port group
 4. Create a network policy for Firewall & network isolation rules to be enforced on that "Web" port group
- Now, whenever a VM gets created/subscribed (on-



demand from a customer) from the Web-server VM Template, it will automatically be fingerprinted at the run-time and the associated VM policy would be enforced on whichever server the VM gets deployed. It would automatically have a vNIC created and assigned to the "wed" port group & the vNIC would inherit the complete set of firewall rules configured in the vDefense network policy. Thus all network traffic originating to-and-from its vNIC will automatically be enforced with the associated Firewall policy ensuring required network & VM isolation.

VM Firewall & Traffic Isolation Services:

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 like network 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 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.

Virtual Caging Services: In the older scheme of hosted & caged data centers a customer would rent a cage and put their servers inside the cage along with customer's own firewall, making it physically & logically segregated from the rest of the network to ensure security and privacy. A virtual-caging-service can allow a large enterprise customer subscribing to Cloud services to subscribe a virtual cage of servers so that regardless of where the physical servers are located, each VM subscribed by that customer would run only on the servers allocated for that customer and no other VMs would be allowed to run on those server preventing any data privacy issues. With VM Zoning the Cloud provider can still efficiently use and allocate its physical data center space for on-demand allocation of servers but provide a guaranteed zoning for all VMs subscribed by an enterprise customer.

As shown here vDefense can be used to create several custom managed service offerings for virtualization security in both Cloud and Data Center environments.