ForeScout

Technical Note

Network Access Control in Virtual Environments

Contents

Security Considerations in Virtual Environments

Virtualization has taken the industry by storm and has been a game-changing technology for IT. Organizations have embraced virtualization because it is the single most effective way to reduce IT expenses, providing efficiencies and capabilities that just aren't possible when constrained within a physical world. However, in the race to achieve these efficiencies and cost savings, the associated information security risks are often overlooked. There are several challenges that need to be addressed to ensure the necessary level of security and compliance within your virtual environment.

- Virtualization obfuscates the endpoints. A physical machine can have dozens or hundreds of virtual machines (VMs) on it. And VMs move around from one physical machine to another, based on load, to meet business and service-level requirements. This makes it difficult to enforce security policies, especially those that were originally designed for a physical environment (predicated on identifying an endpoint based on permanent attributes such as an IP or MAC address).
- The abstraction and flexibility provided by virtualization creates a lack of visibility into the environment. Detecting rogue, unmanaged or unapproved VMs is all the more challenging, while being paramount in virtual environments with various shared resources.
- Just as in physical networks, virtual machines can serve as file shares, databases, web servers, application servers and more. Therefore, virtual workloads require the same access control measures that are needed for physical servers. For example, controls such as network access audit trails may be required if you're subject to external regulations.
- In physical environments, it is easy to segment network traffic because organizations tend to use dedicated hardware for different applications, data sets and departments. But with virtualization's efficient load balancing, separating network traffic becomes more challenging. VMs move between physical servers, increasing the possibility of untrusted VMs communicating with sensitive VMs on the same virtual switch.
- When a virtual machine is not required, it can be stored offline as an image in rest state. At offlining time, it may be up-to-date with all OS patches, security applications, signatures and virus definitions. But in the intervening rest period, new vulnerabilities arise, and new security patches and virus definitions/signatures are issued. Offlined VMs need to be made up-to-date and fully compliant when placed back into production.
- On virtual machines, restricted devices such as removable storage media can be more easily added at runtime as this action doesn't actually require any hardware manipulations, potentially circumventing security policy and increasing the risk of data leakage.
- Unlike physical environments, where you have to schedule cabling and get permission to put a new server in place, virtual environments allow you to get a new server up and running in a few seconds. Consequently, well-meaning employees who aren't qualified to maintain and patch servers can install new servers or revive old ones that are not managed by hypervisor management systems or are non-compliant with security policies. Since VMs share physical resources, a misconfiguration or vulnerability in one VM can potentially compromise other workloads.
- Last but not least, is the growing concern of virtual machine "sprawl" powered by the ease of VM creation and cloning. Many IT managers would be hard pressed to list exactly how many VMs they're running. As more VMs are added, keeping track of them becomes harder and the number of unmanaged VMs increases, thereby introducing the potential for some VMs to run with obsolete security policies or without the latest software updates.

Addressing Virtualization Security Challenges using NAC and Endpoint Compliance

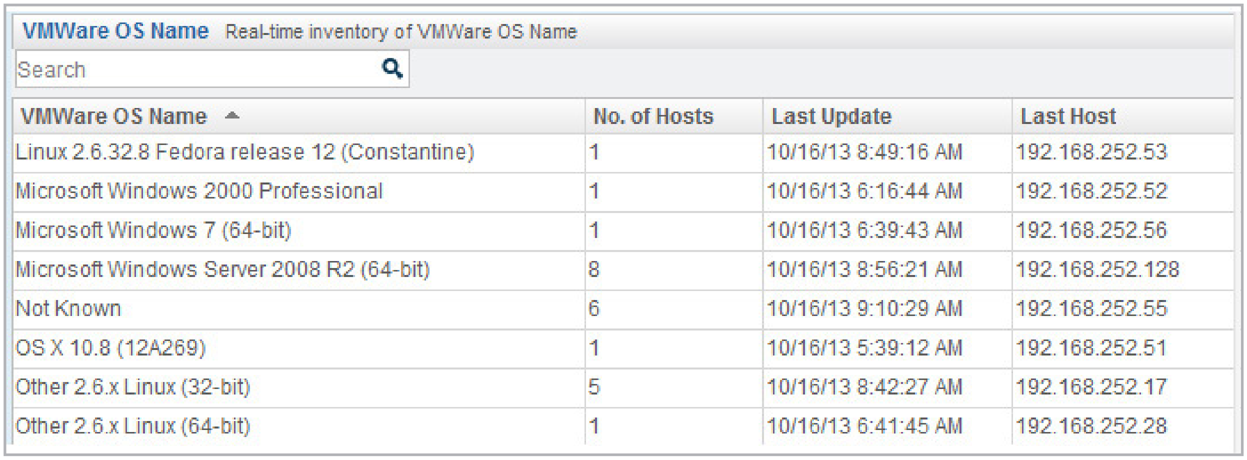
To ensure that your virtual environments are just as secure as your physical environments, you need virtualization-aware security solutions that can enforce consistent security policies across both environments. Virtualization-aware NAC systems such as ForeScout CounterACT™ can be deployed within your virtual infrastructure to address several of the security concerns discussed above.

ForeScout CounterACT is available in both physical and virtual appliance form factors. The CounterACT virtual appliance can enforce security controls in virtualized networks. CounterACT deploys out-of-band and provides you the visibility, protection and compliance management capabilities you need for virtual environments. As you virtualize more of your IT workloads, CounterACT offers centralized (unified) management and policy enforcement across virtual and non-virtual environments.

Let's explore how CounterACT helps address some common security challenges within your virtual infrastructure.

Visibility and Profiling of VMs

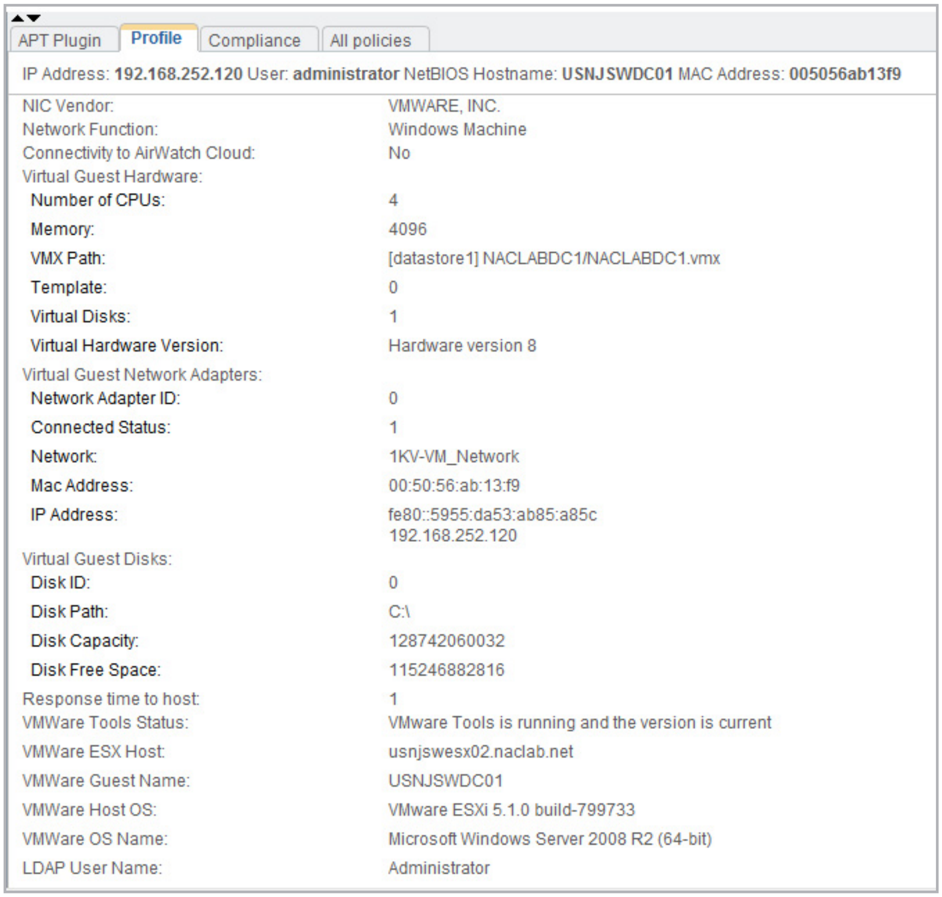
ForeScout CounterACT gives organizations the visibility they need into their virtual infrastructure and the workloads residing within their virtual machines (see Figure 1). Through its industry-leading profiling engine, CounterACT can determine detailed virtual machine and software attributes of each endpoint. By integrating with hypervisor management suites such as VMware vCenter (via the ForeScout Open Integration Module), CounterACT is able to attain additional vendor-specific information such as virtual machine UUIDs that can be utilized for better endpoint classification and more effective policy enforcement (see Figure 2).



VMWare OS Name Real-time inventory of VMWare OS Name

VMWare OS Name ▲	No. of Hosts	Last Update	Last Host
Linux 2.6.32.8 Fedora release 12 (Constantine)	1	10/16/13 8:49:16 AM	192.168.252.53
Microsoft Windows 2000 Professional	1	10/16/13 6:16:44 AM	192.168.252.52
Microsoft Windows 7 (64-bit)	1	10/16/13 6:39:43 AM	192.168.252.56
Microsoft Windows Server 2008 R2 (64-bit)	8	10/16/13 8:56:21 AM	192.168.252.128
Not Known	6	10/16/13 9:10:29 AM	192.168.252.55
OS X 10.8 (12A269)	1	10/16/13 5:39:12 AM	192.168.252.51
Other 2.6.x Linux (32-bit)	5	10/16/13 8:42:27 AM	192.168.252.17
Other 2.6.x Linux (64-bit)	1	10/16/13 6:41:45 AM	192.168.252.28

Figure 1: Visibility of VMs using ForeScout CounterACT.



IP Address: **192.168.252.120** User: **administrator** NetBIOS Hostname: **USNJSWDC01** MAC Address: **005056ab13f9**

NIC Vendor:	VMWARE, INC.
Network Function:	Windows Machine
Connectivity to AirWatch Cloud:	No
Virtual Guest Hardware:	
Number of CPUs:	4
Memory:	4096
VMX Path:	[datastore1] NACLABDC1/NACLABDC1.vmx
Template:	0
Virtual Disks:	1
Virtual Hardware Version:	Hardware version 8
Virtual Guest Network Adapters:	
Network Adapter ID:	0
Connected Status:	1
Network:	1KV-VM_Network
Mac Address:	00:50:56:ab:13:f9
IP Address:	fe80::5955:da53:ab85:a85c 192.168.252.120
Virtual Guest Disks:	
Disk ID:	0
Disk Path:	C:\
Disk Capacity:	128742060032
Disk Free Space:	115246882816
Response time to host:	1
VMWare Tools Status:	VMware Tools is running and the version is current
VMWare ESX Host:	usnjswesx02.naclab.net
VMWare Guest Name:	USNJSWDC01
VMWare Host OS:	VMware ESXi 5.1.0 build-799733
VMWare OS Name:	Microsoft Windows Server 2008 R2 (64-bit)
LDAP User Name:	Administrator

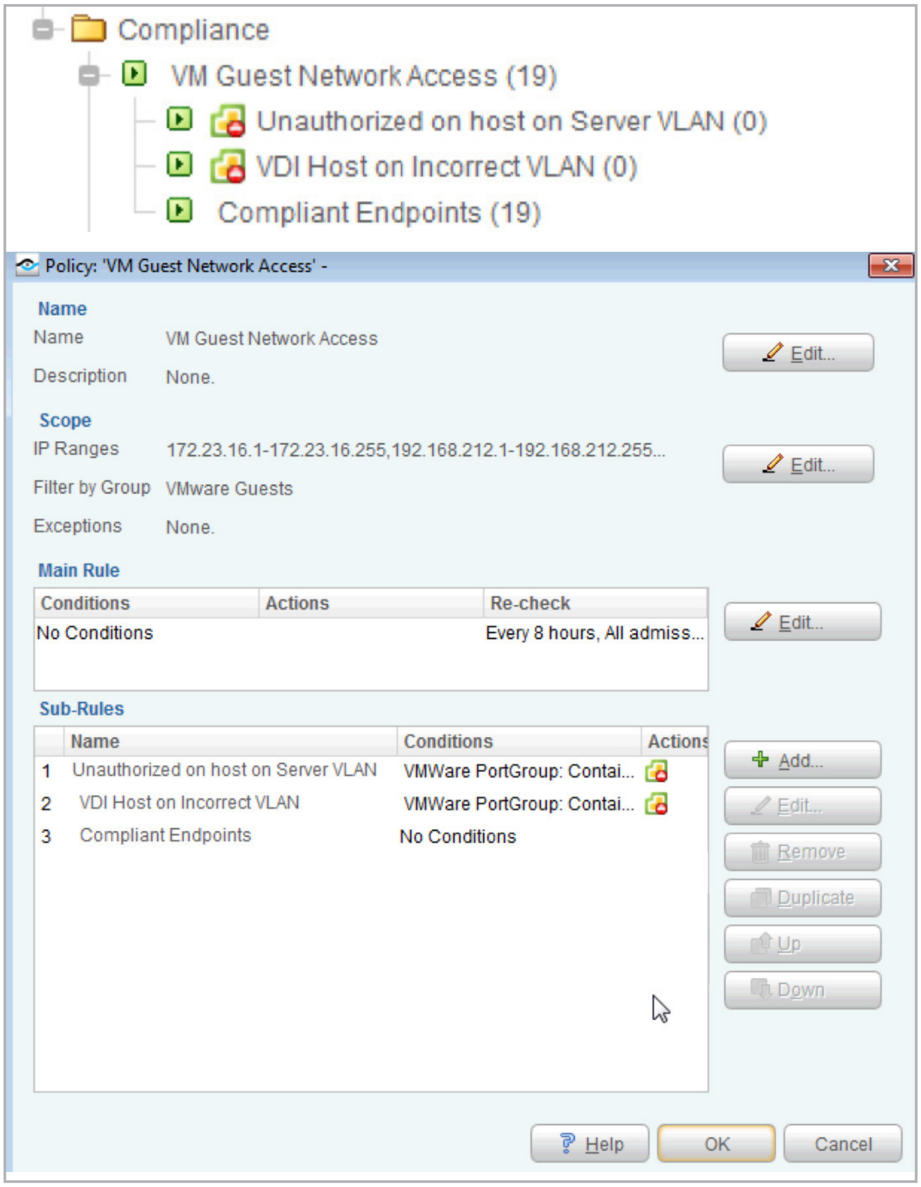
Figure 2: Profiling Virtual Machines using ForeScout CounterACT

Identification of Rogue or Unapproved VMs

Hypervisor management systems can provide a list of managed VMs, but cannot indicate if there are any VMs in the environment that should not be there. ForeScout CounterACT can identify and inventory virtual assets in real-time; classify them by VM image, physical host and virtual network membership; and determine which assets are actively managed by the hypervisor management system. (This last function requires the ForeScout Open Integration Module which allows CounterACT to pull information from VMware vCenter.) CounterACT polices can ensure that only authorized VMs gain access to appropriate network resources. Rogue VMs can be quarantined through the use of CounterACT's virtual firewall to protect the rest of the environment and improve virtual infrastructure stability.

Endpoint Compliance Management of VMs

CounterACT can assess the security posture of virtual machines and ensure they comply with policies and audit requirements. When virtual environment violations are detected, CounterACT can notify an administrator and/or automatically quarantine a workload. It can trigger remediation actions such as installing patches, updating security software and definitions, enabling or disabling services/ports/peripherals, and updating various configuration settings (see Figure 3).



- Compliance
  - VM Guest Network Access (19)
    - Unauthorized on host on Server VLAN (0)
    - VDI Host on Incorrect VLAN (0)
    - Compliant Endpoints (19)

Policy: 'VM Guest Network Access' -

Name

Name: VM Guest Network Access

Description: None.

Scope

IP Ranges: 172.23.16.1-172.23.16.255,192.168.212.1-192.168.212.255...

Filter by Group: VMware Guests

Exceptions: None.

Main Rule

Conditions	Actions	Re-check
No Conditions		Every 8 hours, All admiss...

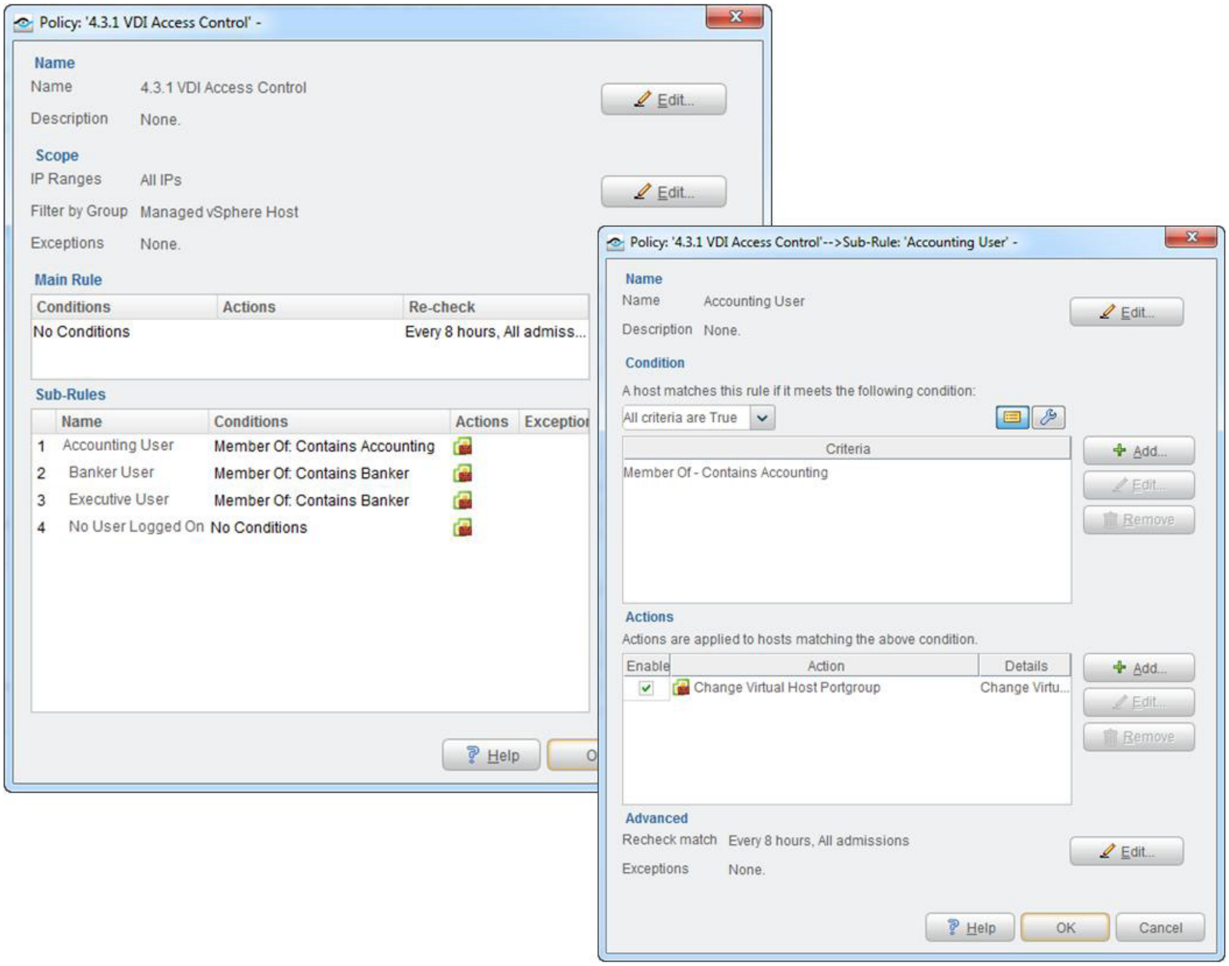
Sub-Rules

	Name	Conditions	Actions
1	Unauthorized on host on Server VLAN	VMWare PortGroup: Contai...	
2	VDI Host on Incorrect VLAN	VMWare PortGroup: Contai...	
3	Compliant Endpoints	No Conditions	

Figure 3: CounterACT policy to detect unauthorized VMs on the server VLAN

Enforcing Role-based Access Control

ForeScout CounterACT provides authentication and access control in virtual environments to reduce the risk from unwarranted or unauthorized access (see Figure 4). It can monitor traffic coming from the physical network to the virtual network as well as traffic between VMs, and can apply consistent access controls across your entire network. Most other NAC products cannot do this, because they require 802.1X which is not supported in virtual environments. CounterACT includes multiple network access control technologies which are effective in both physical and virtual environments. CounterACT also monitors post-connection traffic for anomalous endpoint behavior and malicious activity to maximize the flexibility and benefit that virtualization affords your organization.



Policy: '4.3.1 VDI Access Control' -

Name

Name 4.3.1 VDI Access Control

Description None.

Scope

IP Ranges All IPs

Filter by Group Managed vSphere Host

Exceptions None.

Main Rule

Conditions	Actions	Re-check
No Conditions		Every 8 hours, All admiss...

Sub-Rules

	Name	Conditions	Actions	Exceptio
1	Accounting User	Member Of: Contains Accounting		
2	Banker User	Member Of: Contains Banker		
3	Executive User	Member Of: Contains Banker		
4	No User Logged On	No Conditions		

Policy: '4.3.1 VDI Access Control'-->Sub-Rule: 'Accounting User' -

Name

Name Accounting User

Description None.

Condition

A host matches this rule if it meets the following condition:

All criteria are True

Criteria
Member Of - Contains Accounting

Actions

Actions are applied to hosts matching the above condition.

Enable	Action	Details
☑	Change Virtual Host Portgroup	Change Virtu...

Advanced

Recheck match Every 8 hours, All admissions

Exceptions None.

Figure 4: Access Control in Virtual Environments using ForeScout CounterACT

Deploying CounterACT in Virtual Infrastructure

ForeScout CounterACT's ability to deploy within virtual environments gives organizations the much needed visibility, control and compliance management to protect their virtual assets. CounterACT offers out-of-the-box integration with virtual switches offered within VMware vSphere and Microsoft Hyper-V (most other NAC solutions lack integration with virtual environments).

The flexibility of the CounterACT architecture to run in both physical and virtual environments benefits organizations that want to centrally manage and enforce consistent security policies across their IT infrastructure. Virtual appliances can be deployed inside the virtual environment to place policy enforcement closer to the workload and information they are protecting. Physical or virtual appliances can be deployed in the physical network. Both types of appliances can be centrally managed using the CounterACT Enterprise Manager.

CounterACT virtual appliances integrate with both variations of virtual switches offered within vSphere and Hyper-V — the standard vSwitch and the distributed vSwitch (dvSwitch). Additionally, CounterACT can integrate with the hypervisor management suite (such as vCenter) via the ForeScout Open Integration Module to obtain vendor specific information that can be used in policy enforcement.

Standard vSwitch

A standard vSwitch allows several VMs on a single physical host to share a physical network interface and to communicate with each other using the same protocols as physical switches. It emulates a traditional ethernet switch to the extent that it forwards frames at the data link layer. It is limited in its manageability and does not offer any remote management or administration features.

The standard vSwitch offers a promiscuous mode which allows a CounterACT virtual appliance to passively listen to traffic on the physical interface. This is beneficial for monitoring traffic entering and exiting the virtual network and allows CounterACT to enforce security controls at the boundary between the physical and virtual environment.

CounterACT can profile VMs connected to the standard vSwitch, assess their security posture, and identify rogue or unmanaged VMs on the vSwitch. Also, CounterACT can control network access for users and devices on the physical network attempting to communicate with hosts on the vSwitch. One limitation that is inherent in the standard vSwitch is the inability for CounterACT to see traffic within the vSwitch fabric (i.e. the source and destination are both VMs connected to the vSwitch). Thus, CounterACT cannot control traffic between VMs within the standard vSwitch.

Distributed vSwitch

A distributed vSwitch is a single logical switch that spans across multiple hypervisors. This allows VMs to maintain consistent network configurations regardless of the hypervisors they reside on. The dvSwitch improves on the standard vSwitch by adding granular features such as VLAN trunking, security profiles and port mirroring. The mirror-port replicates traffic from all interfaces on the dvSwitch.

The addition of port mirroring on the dvSwitch allows a CounterACT virtual appliance to monitor and control traffic that traverses the dvSwitch fabric. Similar to a standard vSwitch deployment, CounterACT can profile VMs, assess their security posture and identify rogue or unmanaged VMs. Also, CounterACT can control network access for users and devices accessing the virtual environment from the physical network.

Complete Traffic Visibility

CounterACT can be used to monitor both vSwitch and dvSwitch channels to provide complete visibility and control over inter-VM traffic on the virtual switch fabric as well as traffic to and from the VMs to the physical network.

The table below shows CounterACT functionality available with each type of vSwitch.

Function	Standard vSwitch	Distributed vSwitch
Virtual Traffic Visibility and Control[1]	N	Y
Physical Traffic Visibility and Control[2]	Y	N
VLAN Assignment	Y	Y
Network Interface Blocking	Y	Y
VM Visibility and Profiling	Y	Y
Identify/Quarantine Rogue or Unmanaged VMs	Y	Y
VM Security Posture Assessment	Y	Y
Role-based Network Access Control from Physical Network into Virtual Environment	Y	Y

[1] Traffic only traversing within the Virtual Switch (VM <-> VM)
[2] Traffic traversing between the Virtual Switch and the physical network (VM <-> Physical Network)

Case Study: School TAPS NAC Appliance for Virtualized Environment

A boarding school in the UK has adopted ForeScout CounterACT for its VMware environment.

CounterACT monitors network traffic to discover network devices, including virtual machines; builds an inventory of device characteristics; and enforces policies configured by the security administrator. Because CounterACT is deployed out-of-band, the problems of network latency and the possibility of introducing a single point of failure are minimized.

The boarding school has deployed both physical and virtual CounterACT appliances. The two types of appliances perform identically. All CounterACT appliances are centrally controlled by the ForeScout CounterACT Enterprise Manager. The school runs their CounterACT virtual appliances on VMware ESX 3.5 and 4.x.

The functionality of both physical and virtual CounterACT appliances includes:

- Providing visibility to all users, devices, and applications in use on the network
- Identifying security gaps
- Automating guess user access
- Blocking rogue devices and unauthorized programs
- Blocking attacks inside the network

Since installation, CounterACT has done a fantastic job of automating the guest and pupil network by eliminating endpoint security issues throughout the campus. The school was consolidating their data center and welcomed the opportunity to extend the CounterACT deployment with the virtual appliance.

To deploy the virtual appliance, they simply added computing resources for the virtual appliance. The installation was straightforward and gave them more flexibility to allocate capacity as they need it, plus giving them the protection of running such a system within their protected virtual environment.

About ForeScout

ForeScout delivers pervasive network security by allowing organizations to continuously monitor and mitigate security exposures and cyber attacks. The company's CounterACT appliance dynamically identifies and assesses all network users, endpoints and applications to provide complete visibility, intelligence and policy-based mitigation of security issues. ForeScout's open ControlFabric™ technology allows a broad range of IT security products and management systems to share information and automate remediation actions. Because ForeScout's solutions are easy to deploy, unobtrusive, flexible and scalable, they have been chosen by more than 1,500 enterprises and government agencies. Headquartered in Campbell, California, ForeScout offers its solutions through its network of authorized partners worldwide. **Learn more at www.forescout.com.**

ForeScout

ForeScout Technologies, Inc.
900 E. Hamilton Ave.,
Suite 300
Campbell, CA 95008
U.S.A.

T 1-866-377-8771 (US)
T 1-408-213-3191 (Intl.)
F 408-213-2283
www.forescout.com