SOLUTION BRIEF

McAfee MOVE AntiVirus: Advanced Security Integrated with VMware NSX

Driven by business demands, technology advantages, and cost savings, enterprise technology leaders have eagerly embraced server virtualization and virtual desktop infrastructure (VDI). The next logical step is moving to the software-defined data center (SDDC), which virtualizes the entire infrastructure and delivers it as a service, with the control of this data center completely automated by software. The SDDC has many benefits for lines of business and IT, including simplified data center management, automation of repeatable IT processes, and faster delivery of IT services. IT leaders acknowledge that greater agility, improved efficiency, and lower costs are great reasons to consider switching to an SDDC, but an additional driver is that SDDCs deliver fundamentally better data center security.

SDDCs are defined by three pillars: server virtualization, storage virtualization, and network virtualization. Virtual networks are isolated by default, and VMware NSX network virtualization provides software-based micro-segmentation to enable security controls at the virtual machine (VM) level. If your organization has invested in the high-performance VMware virtual infrastructure and is considering deployment of an SDDC, the integration of McAfee® Management for Optimized Virtual Environments AntiVirus (McAfee MOVE AntiVirus) with virtualized security for endpoint and network, VMware NSX is an important step toward making an SDDC with advanced security a reality.

VMware NSX: A Critical Component of VMware's SDDC Portfolio

Previously, the virtual network component of the SDDC had been the missing link. In spite of the technology advances in virtualization, networking lagged behind—until the emergence of VMware NSX, a software layer that enables enterprises to deploy networking and security for any application on any hardware resource or VM.[1] VMware NSX embeds networking and security functionality that is typically handled in hardware directly into the hypervisor. VMware NSX provisions virtual networking environments without command line interfaces or other direct administrator intervention. You can connect both virtual and physical machines to the network within one data center or across multiple data centers.

The chief advantages of VMware NSX are high scalability, agility, and security. For example, a single controller can support 100,000 VMs and 10,000 virtual networks—and it only takes seconds to deploy, configure, and reconfigure a network. A key advantage of VMware NSX is providing visibility to all of the VMs and network services in the SDDC. In addition, the stateful VMware NSX firewall and microsegmentation design make your SDDC more secure.

Advanced Virtual Machine Security Services for the SDDC: McAfee MOVE AntiVirus

McAfee MOVE AntiVirus offers the ability to integrate with network security and is included in McAfee Server Security Suite Advanced and McAfee Server Security Suite Essentials, two server security suites for comprehensive protection in physical or virtual environments, on premises, or in the cloud. McAfee MOVE AntiVirus has always delivered optimized, offloaded antivirus for VMs through its lightweight endpoint agent for multiplatform installations and agentless mode for VMware vShield, and it is enabled and certified for dynamic VMware NSX environments.

McAfee MOVE AntiVirus is an established industry-leading product, protecting some of the world's largest virtualized deployments. It provides:

- Optimized security for virtualized environments
- Standardized security across all major hypervisors
- The simplest and most effective security deployment, management, and monitoring for virtualized environments

McAfee MOVE AntiVirus rounds out McAfee certification of McAfee Network Security Platform's virtual intrusion prevention and detection system (IPS) with the Open Security Controller from Intel. McAfee is the only security company to offer both network and endpoint security for VMware NSX deployments.

Ease of Deployment and Instant Protection

McAfee® ePolicy Orchestrator® (McAfee ePO™) software, the single-pane manageability solution for all McAfee endpoint security solutions, including McAfee MOVE AntiVirus, is the window into the security of your SDDC. You can discover and import all VM workloads from VMware's vCenter into the McAfee ePO console with Cloud Workload Discovery. This also allows you to view the virtualization properties and protection status of your VMs.

Using Cloud Workload Discovery, administrators can get quick insights, protect workloads through VMware NSX or VMware vShield, and view the details on the McAfee ePO console.

McAfee MOVE AntiVirus Security Virtual Machines (SVMs) are deployed automatically, so there's no need to install them manually on new hosts that appear in the VMware NSX environment. The McAfee MOVE AntiVirus SVMs automatically provide antivirus protection for VMs. SVMs are managed directly by McAfee ePO software. The SVM offloads scanning of VMs, minimizing performance impact.

Agentless deployment speeds time-to-protection without disrupting performance

Agentless deployment protects Microsot Windows and Linux VMs. McAfee MOVE AntiVirus or VMware vShield Endpoint uses the hypervisor as a high-speed connection to allow the McAfee MOVE AntiVirus SVM to scan VMs outside of the guest VM or desktop, so as not to disrupt or bog down computing activity. As it scans,

the SVM will direct either VMware vShield Manager or VMware NSX Manager to cache good files or delete or deny access to malicious files. After you install the SVM and components on the VMware ESX servers, every virtualized image—guest desktop or guest OS—is automatically protected as it is created. There's no McAfee software (agent) on guest VMs—McAfee MOVE AntiVirus communicates with the VMs via VMware tools. Additionally, VMs can be moved from one host to another without affecting security.

Deployment of agentless McAfee MOVE AntiVirus with VMware vShield Endpoint and VMware NSX are supported simultaneously, making it extremely easy and seamless for customers who already have VMware vShield Endpoints to make the transition when they deploy a VMware NSX environment.

Consistent Policies, Seamless Management

McAfee offers the most comprehensive, truly integrated security management approach. Integration of McAfee MOVE AntiVirus with VMware NSX makes it possible to see policy changes immediately in McAfee ePO software. This is the keystone of effective security management. With the VMware NSX certification, McAfee can now extend its proven VM security to the SDDC, providing security administrators with the confidence to extend the benefits of secure virtualization to the data center. McAfee offers both network and endpoint security for the VMware NSX environment—two essential elements of a successful and secure SDDC. Security administrators can view instant synchronization among policies created in McAfee ePO software, and assignment rules done via VMware NSX will be passed down to the VMs via McAfee ePO software.

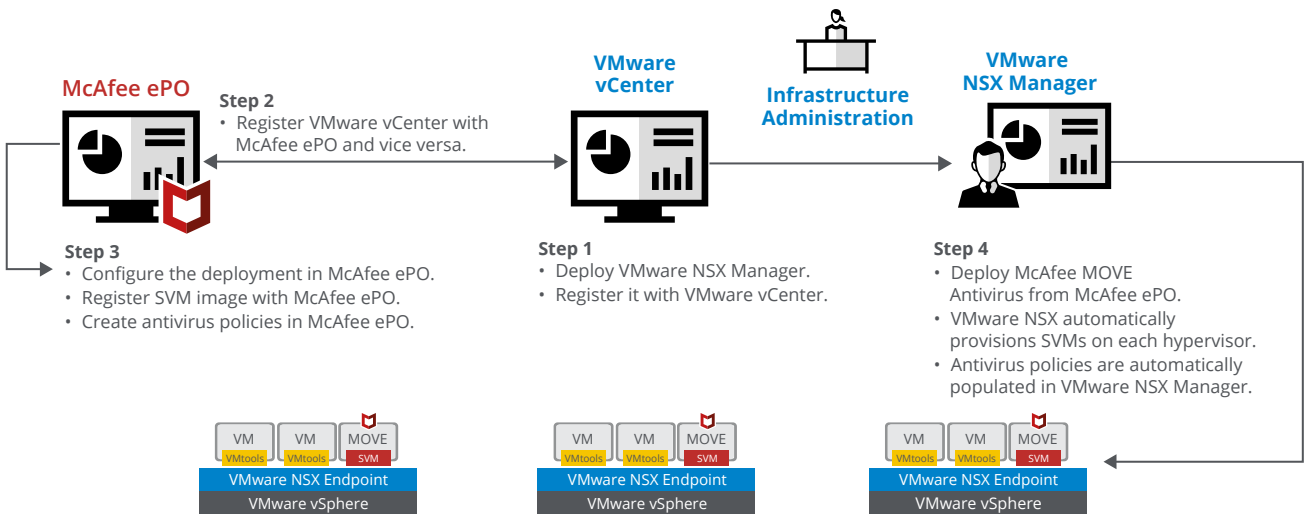

Figure 1. How to deploy McAfee MOVE Antivirus with VMware NSX in your data center.

Start by registering the McAfee MOVE AntiVirus SVM with McAfee ePO software in the deployment wizard. You can manage your antivirus policy in McAfee ePO software. Policies will automatically show up in the VMware NSX Manager. Next, assign a policy to a VM or a group of VMs in the VMware NSX console. The policy association will then be reflected immediately in the McAfee ePO console. Here are some typical policy management scenarios:

- **Example 1:** When a VM changes groups, VMware NSX automatically changes the policy based on the assignment rules, and that change is reflected in McAfee ePO software immediately.
- **Example 2:** After registering the McAfee MOVE AntiVirus service in the McAfee ePO server, agentless scan policies are exported from McAfee ePO software to VMware NSX in real time, which helps the VMware administrator understand the sets of policies that were created and modified by the security administrator. When a scan policy from McAfee ePO software is removed, it is also deleted from VMware NSX Manager if it is not included in any of the VMware NSX security policies.

Tag Virtual Machines According to Vulnerability Level

McAfee MOVE AntiVirus automatically tags VMs to enable immediate remediation actions. Custom tags display details about the security posture of VMs, which helps administrators organize VMs across various groups or vulnerability levels. For example, if a VM with no anti-malware is detected, it is immediately tagged in VMware NSX, enabling the VMware NSX firewall to quarantine the unprotected VM. Or, if malware is found on a VM, a VMware-defined tag is set in VMware NSX, so that the security administrator can respond appropriately. The tag will be automatically cleared during the next on-demand scan as long as the McAfee antivirus engine has cleaned the malware.

Summary

McAfee MOVE for AntiVirus has a track record of providing optimized antivirus protection for the virtual environment without impacting performance and agility. With VMware NSX network virtualization, McAfee can now automate VM security to the SDDC, providing security administrators with the confidence to advance security efficiently and at scale. McAfee solutions with NSX can automate both network and endpoint security for SDDC environments.

1. https://www.youtube.com/watch?v=PciyGPCykLI

Learn More

Get more details about **McAfee MOVE AntiVirus**, and start building out your secure SDDC.

McAfee
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

2724_0317
MARCH 2017