McAfee™
Together is power.

McAfee Management for Optimized Virtual Environments AntiVirus

Security for your private cloud without sacrificing performance

Traditional antivirus does not play well with virtualized infrastructure. McAfee® Management for Optimized Virtual Environments AntiVirus (McAfee MOVE AntiVirus) brings optimized, advanced malware protection to your virtualized desktops and servers. Implement across multiple hypervisors, or choose an agentless, tuned option for VMware NSX or VMware vCNS. Either way, you get top-rated security for instant threat detection and containment with minimal impact on virtual machine (VM) performance. McAfee MOVE AntiVirus optimizes anti-malware protection for virtualized deployments, freeing hypervisor resources while ensuring up-to-date security scans are run according to policy.

Optimized Scanning Control

The dynamic nature of guest desktops and virtual servers requires careful handling. Images must be malware-free when users initiate a session. This can be challenging, since users often begin work in groups, causing peak-demand "antivirus storms" that consume resources and prevent users from obtaining a session.

To eliminate scanning bottlenecks and delays, McAfee MOVE AntiVirus offloads scanning, configuration, and .DAT update operations from individual guest images to an offload scan server. We build and maintain a global cache of scanned files to ensure that once a file is scanned and confirmed to be clean, subsequent VMs accessing the file won't have to wait for a scan.

Memory resource allocation for each VM decreases and can be released back to the resource pool for more effective utilization.

McAfee MOVE AntiVirus allows separate policies for on-access and on-demand scanning to enable fine-tuned security execution. For instance, administrators can assume some reasonable level of risk for real-time, on-access scans to avoid degrading performance and then use on-demand scanning with more rigid policies running at a later time when there's less impact.

Complete End-to-End Visibility Across All Clouds

Poor visibility makes it difficult to implement proper security policies for virtualized environments. McAfee Cloud Workload Discovery for private cloud, covering

Key Advantages

- **Offloads malware scanning:** Instant protection with low impact on memory and processing
- **Prevents antivirus storms:** Options include on-access and on-demand scans
- **Enables flexible deployment:** Multiplatform (all major hypervisors, Windows VMs) or agentless (VMware, Windows, and Linux VMs)
- **Improves resource optimization:** Elastic provisioning of offline scanners with event notifications (multiplatform)
- **Blocks zero-day, unknown threats in seconds:** Local reputation intelligence combined with behavioral analytics in a sandbox (multiplatform, additional module sold separately)
- **Leverages McAfee® ePolicy Orchestrator® (McAfee ePO™) console:** End-to-end visibility and control across physical, virtual, and cloud deployments

VMware and OpenStack, provides a complete view into virtual data centers and populates key properties such as servers, hypervisors, and VMs into the McAfee ePO console. Once administrators gain visibility into the security status of all VMs and can monitor hypervisor-to-VM relationships in near real time, securing your virtual data center becomes a lot easier. A customizable dashboard displays security scan status, executive overviews, and historical security data on assets.

McAfee Server Security Suite Essentials and McAfee Server Security Suite Advanced extend visibility and control across Amazon Web Services (AWS) and Microsoft Azure public clouds and physical servers.

Fine-Grained Policy Management

The familiar McAfee ePO console lets you configure policies and controls for McAfee MOVE AntiVirus. You can roll up virtual data with data from your physical systems and public clouds to provide unified dashboards and reports. Administrators are able to configure a unique policy per VM, cluster, or data center through McAfee Cloud Workload Discovery, adapting security specifically according to the makeup of the data center.

Additional McAfee MOVE AntiVirus Features

Management and visibility:

- Instantly schedule an on-demand scan on a VM or group of VMs.
- Increase scanning precision with targeted on-demand scans.

- Automatically deploy an offload scanner on each hypervisor through integration with VMware NSX Service Composer.
- Stay on top of issues with dashboards, reports, and email alerts.

Simplified deployment and configuration:

- Deploy and configure an offload scanner on multiple hypervisors (agentless).
- Restore quarantined files using the McAfee ePO console (multiplatform).
- Detailed diagnostics for antivirus performance tuning.
- Seamless agentless and multiplatform policy management.

Agentless Option for VMware

McAfee MOVE AntiVirus leverages VMware NSX or VMware vCNS for better efficiency. In agentless deployments, these use the hypervisor as a high-speed connection to allow the McAfee MOVE AntiVirus security virtual machine (SVM) to scan VMs from outside the guest image. As it scans, the SVM will direct VMware NSX or VMware vCNS to cache good files and either delete, deny access to, or quarantine malicious files.

After you install and configure the SVM and VMware NSX or VMware vCNS components on VMware ESX servers, along with installing the VMware NSX or VMware vCNS endpoint driver on guest VMs, every image is automatically protected without installing McAfee software on each client VM. Our vMotion-aware

McAfee MOVE AntiVirus Configurations

McAfee MOVE AntiVirus for Virtual Servers
- McAfee MOVE AntiVirus:
  – Multiplatform deployment
  – Agentless deployment
- Cloud Workload Discovery for private cloud (VMware and OpenStack)
- McAfee ePO software

McAfee MOVE AntiVirus for Virtual Desktops
- McAfee MOVE AntiVirus:
  – Multiplatform deployment
  – Agentless deployment
- Cloud Workload Discovery for private cloud, covering VMware and OpenStack
- McAfee Host Intrusion Prevention System
- McAfee SiteAdvisor® Enterprise
- Memory Protection, and Web Application Protection
- McAfee ePO software

implementation means that your VMs can move from one host to another and be seamlessly protected by the SVM on the target host, with no impact on scans or the user experience.

Integration of McAfee products with VMware vCNS allows you to monitor SVM status within VMware vCenter and receive alerts if the SVM loses connectivity. The McAfee ePO console receives event data detailing the specific VM affected in the event a VM is infected. Deep integration with VMware NSX synchronizes policies created in the McAfee ePO console and rules assigned in VMware NSX. Tagging of vulnerable machines with no anti-malware protection or machines with malware enables immediate quarantining of VMs through the VMware NSX firewall.

Deployment of agentless McAfee MOVE AntiVirus with VMware vCNS and VMware NSX are supported simultaneously, making it extremely easy and seamless for VMware vCNS customers to transition to VMware NSX.

Multiplatform for All Major Hypervisors

In multiplatform installations, including vSphere, Hyper-V, KVM, and XenServer, the McAfee MOVE AntiVirus agent—a lightweight endpoint component—communicates to the SVM to broker the antivirus processing on behalf of each VM. McAfee MOVE AntiVirus agent maintains a local cache and manages policies and scanning functions. You can designate and scan a gold image for use as a clean master. Pre-populating the local cache with clean images delivers the fastest VM boot-up time.

Upon file access, the McAfee MOVE AntiVirus offload scan server performs an on-access scan, providing a response back to the VM. Users are notified of issues through a pop-up alert and can then take action to either delete, deny access to, or quarantine malicious files.

As scanning demand fluctuates in multiplatform deployments, SVMs can automatically be added to or removed from the resource pool to scale your power up or down for unlimited scale and efficient resource utilization. Event notifications help administrators understand SVM usage trends to optimize resource management.

McAfee MOVE AntiVirus in multiplatform deployments can enhance global reputation intelligence from McAfee Global Threat Intelligence (McAfee GTI) with local data from McAfee Threat Intelligence Exchange, an additional module sold separately, to instantly identify and combat ever-increasing unique malware samples. Using McAfee Threat Intelligence Exchange, McAfee MOVE AntiVirus coordinates with McAfee Advanced Threat Defense to dynamically analyze the behavior of unknown applications in a sandbox and automatically immunizes all endpoints from newly detected malware. McAfee MOVE AntiVirus integration with McAfee Network Security Platform through McAfee Threat Intelligence Exchange provides a layered security approach for unified perimeter and virtual machine protection.

Unified Policy Management for Agentless and Multiplatform

Many organizations may want to take advantage of the ability of McAfee MOVE AntiVirus to support both agentless and multiplatform deployments. McAfee

MOVE AntiVirus gives security administrators the ability to define and manage consistent security policies using one extension point in the McAfee ePO console so that management of these different methods is seamless and easy.

Learn More

McAfee solutions equip you with the security you need and the flexibility you deserve.

Learn more at http://www.mcafee.com/move.

Architecture	Multiplatform Deployment	Agentless Deployment
Hypervisor/platform support	All major hypervisors, including VMware, Citrix, Hyper-V, and KVM	VMware
Scanning platform	Windows 2008, Windows 2012 R2, Windows Server 2016	Linux Ubuntu 16.04
Deployment scalability	One SVM can protect VMs from multiple hypervisors. SVMs can be elastically provisioned.	One SVM per ESX host
Communication to VMs	Over the network	Over the hypervisor
Virtual machine protection	Windows	Windows and Linux

McAfee
Together is power.