Data Sheet

McAfee Management for Optimized Virtual Environments AntiVirus

Now you can have the security you need and the flexibility you deserve.

Key Advantages

Offloads malware scanning.
- Instant protection with low impact on memory and processing.

Prevents antivirus storms.
- Options include on-access and scheduled scans.

Enables flexible deployment.
- Multiplatform (vendor neutral) or agentless on VMware.

Minimizes setup and updates.
- Dedicated, hardened virtual appliance.

Blocks zero-day, unknown threats.
- Real-time file analysis through McAfee Global Threat Intelligence.

Leverages McAfee ePO software.
- At-a-glance visibility, control, and reporting across your endpoints.

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 vendor platforms, or choose an agentless, tuned option for VMware vShield. Either way, you get flexible, top-rated security and high performance.

McAfee MOVE AntiVirus—part of the Intel® Security product offering—supplies anti-malware protection optimized for the resource constraints of virtualized deployments. McAfee MOVE AntiVirus frees hypervisor resources while ensuring up-to-date security scans are run according to policy.

Optimized Scanning Architecture

The dynamic nature of guest desktops and virtual servers requires careful handling. Images must be malware-free when users initiate a session. Anti-malware isn't the only service starting up, and users often begin work in groups, causing peak-demand "antivirus storms" that consume all 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 a hardened virtual appliance/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 virtual machines (VMs) accessing that 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. Intelligent scheduling of on-demand scans ensures that scans don't interfere with hypervisor performance.

Complete Visibility over the Data Center

In data centers, maintaining visibility over the entire virtualized environment can be a struggle for security administrators. The McAfee Data Center Connector for VMware vSphere provides a complete view into virtual data centers and populates key properties like servers, hypervisors, virtual machines, even the cloud, into the McAfee ePolicy Orchestrator® (McAfee ePO™) console. Clients can discover and gain visibility into all VMs, whether or not they have deployed McAfee protections. With this complete visibility, the task of securing the data center becomes simplified. Administrators can monitor hypervisor-to-VM relationships, security status, and power status in near real-time. A customizable, at-a-glance dashboard displays security scan status, executive overviews, and historical security data on assets. With the McAfee Server Security Suite Essentials and McAfee Server Security Suite Advanced, additional Data Center Connectors are available to extend that further into the

intel Security

McAfee MOVE AntiVirus Configurations

McAfee MOVE AntiVirus for Virtual Servers

- McAfee MOVE AntiVirus.
  - Multiplatform deployment.
  - Agentless deployment.
- McAfee MOVE AntiVirus Scheduler.
- McAfee Data Center Connector for vSphere.
- McAfee ePolicy Orchestrator software.

McAfee MOVE AntiVirus for Virtual Desktops

- McAfee MOVE AntiVirus.
  - Multiplatform deployment.
  - Agentless deployment.
- McAfee MOVE AntiVirus Scheduler.
- McAfee Data Center Connector for vSphere.
- McAfee Host Intrusion Prevention System.
- McAfee SiteAdvisor® Enterprise software.
- McAfee Desktop Firewall, Memory Protection, and Web Application Protection.
- McAfee ePolicy Orchestrator software.

Amazon AWS public cloud, the Microsoft Azure cloud, and OpenStack based clouds.

Fine-Grained Policy Management

The familiar McAfee ePO software console lets you configure policies and controls for McAfee MOVE AntiVirus. Data from virtual desktops can be rolled up with data from physical systems to provide unified dashboards and reports. Administrators are able to configure a unique policy per VM, cluster, or data center through the McAfee Data Center Connector, adapting their security needs specifically 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.
- Automatically deploy an SVA on each hypervisor through integration with VMware NSX Service Composer.
- Improved Data Center Connector for VMware vCenter.

Simplified deployment and configuration:

- Deploy and configure the SVA on multiple hypervisors (Agentless).
- Restore quarantined files from within McAfee ePO (Multiplatform).
- Improved diagnostics for AV performance tuning.

Improved resource optimization:

- Flexible tuning policies (Multiplatform).

Agentless Option for VMware Environments

McAfee MOVE AntiVirus leverages VMware's vShield for better efficiency. In agentless deployments, VMware vShield Endpoint uses the hypervisor as a high-speed connection to allow the McAfee MOVE AntiVirus security virtual appliance (SVA) to scan virtual machines from outside the guest image. As it scans, the SVA will direct vShield to cache good files and either delete, deny access to, or quarantine malicious files.

After you install and configure the SVA and the required vShield components on the ESX servers, along with installing the vShield driver on the guest VMs, every image is automatically protected at creation. There's no requirement to install McAfee software on each client VM. Our vMotion-aware implementation means your virtual machines can move from one host to another and be seamlessly protected by the SVA on the target host, with no impact on scans or the user experience. McAfee integration allows you to monitor SVA status within vCenter and receive alerts if the SVA loses connectivity. McAfee ePO software receives event data detailing the specific VM affected in the event a VM is infected.

Multiplatform for Standards and Convenience

In multiplatform installations, the McAfee MOVE AntiVirus agent—a lightweight endpoint component—communicates to the offload scan server to broker the antivirus processing on behalf of each virtual machine. McAfee Agent 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 can be notified of issues through a pop-up alert, and can either delete, deny access to, or quarantine malicious files.

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	VMware, Citrix, Hyper-V	VMware only
Scanning platform	Windows 2008, Windows 2012 R2	Linux Ubuntu 12.4
Deployment scalability	One offload scan server can protect VMs from multiple hypervisors	One security virtual appliance per ESX host
Communication to VMs	Over the network	Over the hypervisor

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com