McAfee
An Intel Company

McAfee MOVE AV

The security you need, and the flexibility you deserve

Traditional antivirus does not play well with virtualized infrastructure. McAfee® MOVE AntiVirus brings optimized, advanced malware protection to your virtualized desktops and servers. Choose one efficient solution across multiple vendor platforms or an agentless, tuned option for VMware vShield. Either way, you get both flexible, top-rated security and high performance. For proactive protection, we integrate real-time threat intelligence and unify security management across physical and virtual infrastructure.

Key Advantages

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

Prevents AV storms
- Options include on-access, scheduled, and selective scans

Flexible deployment
- Multi-platform 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

Adds intrusion and web protection
- Desktop firewall, memory protection, and web application protection

Leverages McAfee ePolicy Orchestrator® (McAfee ePO™)
- At-a-glance visibility, control, and reporting across your endpoints

McAfee Management for Optimized Virtual Environments AntiVirus (MOVE AV) lets you capture the efficiencies promised by virtualized infrastructure without sacrificing security. It supplies proven, industry-leading[1] anti-malware optimized for the technologies and resource constraints of virtualized deployments. Intrusion prevention and web application security offer extra layers of protection against malicious attacks.

McAfee MOVE AV frees hypervisor resources to serve other functions while ensuring up-to-date security scans are run according to policy.

An Optimized Scanning Architecture

The dynamic nature of guest desktops and virtual servers requires careful handling. Images must be maintained malware free while offline, or scanned without delay when users initiate a session. Yet anti-malware isn't the only service starting up and users often begin work in groups, causing peak demand "AV storms" that consume all resources and prevent users obtaining a session.

To eliminate scanning bottlenecks and delays, McAfee MOVE AV offloads scanning, configuration, and DAT update operations from individual guest images to a hardened virtual appliance. 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. Virtual servers have the option of on-access or on-demand scans to ensure scans don't interfere with hypervisor performance.

Multi-platform or Agentless

McAfee first delivered a multi-platform solution for virtualized deployments that leveraged a standard agent on each image and supported all the major hypervisor vendors. We now also offer an adaptive, agentless solution tightly integrated with VMware vShield. Each approach has its strengths. By offering both, we give you ultimate flexibility.

How flexible? Perhaps you have a mix of Citrix Xen Desktop and VMware View virtual desktops as well as a virtual server farm running VMware vSphere. We have you covered with consistent protection managed within a single console.

Multi-platform for Standards and Convenience

In multi-platform installations, the McAfee MOVE AV agent runs in each guest image. A McAfee ePolicy Orchestrator® (McAfee ePO™) agent manages policies and scanning functions on each guest image, as well as the activities of the McAfee MOVE AV Offload Scan Server. You can designate and scan a gold image for use as a clean master. Pre-populating global caches with clean images delivers the fastest VM boot-up time.

When a user accesses a file, the MOVE 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 files can be moved to quarantine to await a decision.

During the session, a lightweight endpoint component communicates to the Offload Scan Server to broker the antivirus processing on behalf of each virtual desktop. Each VM can be configured with unique, individual policies set in the McAfee ePO console, or the VMs can be managed as a group.

McAfee MOVE AV Configurations

McAfee MOVE AV for virtual desktops

- McAfee MOVE AntiVirus
  - Multi-platform deployment
  - Agentless deployment
- McAfee VirusScan Enterprise for Windows
- McAfee VirusScan Enterprise for Linux
- McAfee Host Intrusion Prevention System (Host IPS)
- McAfee SiteAdvisor Enterprise
- McAfee ePolicy Orchestrator

McAfee MOVE AV for virtual servers

- McAfee MOVE AntiVirus
  - Multi-platform deployment
  - Agentless deployment
- McAfee VirusScan Enterprise for Windows
- McAfee VirusScan Enterprise for Linux
- McAfee VirusScan Enterprise for Offline Virtual Images
- McAfee ePolicy Orchestrator
- McAfee MOVE Scheduler

Leverage vShield for Efficiency

In agentless deployments, VMware vShield Endpoint uses the hypervisor as a high-speed connection to allow the MOVE 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 or delete or deny access to malicious files.

After you install the SVA and components on the ESX servers, every image is automatically protected at creation. There's no McAfee software on client VMs. 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 user experiences. Hypervisor introspection in vSphere prevents compromise of anti-malware.

McAfee integration allows you to monitor SVA status within vCenter and receive alerts if the SVA loses connectivity. And McAfee ePO receives event data detailing the specific VM affected.

Real-time Protection for Users

Thanks to McAfee Global Threat Intelligence™, McAfee MOVE can check suspicious files against our cloud-based file reputation service to identify emerging threats. For added protection and policy compliance, McAfee MOVE AV for Virtual Desktops includes McAfee Host Intrusion Prevention (IPS) and McAfee SiteAdvisor® Enterprise. The desktop firewall and advanced memory protection of Host IPS restrict the activities of malware to prevent malicious activity and preserve file integrity. McAfee SiteAdvisor Enterprise alerts users to malicious and risky URLs and gives administrators policy-based control over web usage.

Protection for Servers and Offline Images

McAfee MOVE AV for Virtual Servers adds extra protection for full on-demand scans and offline images. McAfee MOVE Scheduler orchestrates on-demand scans based on hypervisor and resource availability, so that VMs remain usable during scans. Integration with McAfee VirusScan® Enterprise for Offline Virtual Images ensures that offline VM images are scanned and running current DATS so they are ready when needed.

Management Simplicity

The familiar McAfee ePO console lets you configure policies and controls for McAfee MOVE AV behavior to match the rules you use to manage systems in your physical infrastructure. Data from virtual desktops and servers can be rolled up with data from other systems within unified dashboards and reports.

Get Moving

McAfee solutions equip you with the security you need, and the flexibility you deserve. Learn more at http://www.mcafee.com/move.

Feature	Multi-Platform Deployment	Agentless Deployment
Antivirus Features		
On-access scanning	✓	✓
On-demand scanning		✓
GTI file reputation	✓	✓
File quarantine action	✓	
Architecture		
Hypervisor/platform support	Supports major hypervisors	VMware only
Scanning platform	Windows 2008	Linux
Deployment scalability	450 VMs per Offload Scan Server	One Security Virtual Appliance per ESX host
Communication to VMs	Network	VMware vShield: VMCI channel

[1] http://www.av-comparatives.org/images/stories/test/ondret/avc_od_aug2011.pdf

McAfee
An Intel Company

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

43600ds_move-av_0312_fnl_ETMG