DATA SHEET

McAfee
Together is power.

McAfee Security Suite for Virtual Desktop Infrastructure

The security you need with minimal performance impact

Adoption of virtual desktops is happening right now, but strong desktop security has to be designed into the solution so that it protects your business without causing performance issues or impacting desired server density. Traditional antivirus does not work well within a virtualized infrastructure. The answer? McAfee® Security Suite for Virtual Desktop Infrastructure (VDI), which provides comprehensive security optimized for virtual desktops.

McAfee Security Suite for VDI provides anti-malware protection optimized for virtualization, whitelisting to protect from zero-day threats, desktop intrusion protection, and data protection. It also warns users about malicious websites and/or blocks them.

Optimized Scanning Architecture

The dynamic nature of virtual desktops requires careful handling. Images must be malware-free while offline or scanned without delay 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 Management for Optimized Virtual Environments AntiVirus (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 will not 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. This intelligent scheduling of on-demand scans ensures that scans do not interfere with hypervisor performance.

Fine-Grained Policy Management

The McAfee® ePolicy Orchestrator® (McAfee ePO™) console offers the ability to configure policies and controls for McAfee MOVE AntiVirus. Data from virtual desktops can be rolled up with data from other systems within unified dashboards and reports. Administrators can configure a unique policy per VM, resource pool, cluster, or data center through Cloud Workload Discovery for private cloud, adapting their security needs specifically to the makeup of the data center.

Key Advantages

- Offers discovery and visibility with McAfee ePO software and Cloud Workload Discovery
- Provides a unique combination of blacklisting and whitelisting to protect virtual desktops from malware
- Optimizes virtualization security for minimal performance impact
- Adds intrusion and web protection with memory protection and web application protection
- Leverages McAfee ePO software to achieve at-a-glance visibility, control, and reporting across endpoints
- Enables flexible agentless and multiplatform deployment
- Supports elastic provisioning of offline scanners to scale with demand (multiplatform)
- Integrates with local reputation intelligence for faster threat response (multiplatform)

Agentless Deployment 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 VMware 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 our software on each client VM. Our vMotion-aware 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.

McAfee MOVE AntiVirus integration with vCNS allows you to monitor SVM status within VMware vCenter and receive alerts if the SVM loses connectivity. McAfee ePO software receives event data detailing the specific VM affected in the event a VM is infected. Deep integration with NSX synchronizes policies created in McAfee ePO software 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.

Multiplatform for All Hypervisors

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 desktop. A McAfee ePO software agent manages policies and scanning. There is also the ability to designate and scan a gold image for use as a clean master. As a result, an administrator can pre-populate global caches with clean images to help deliver faster virtual desktop boot-up times.

When a user accesses a file, 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 files can be moved to quarantine to await a decision. Each virtual desktop can be configured with unique, individual policies set in the McAfee ePO console, or virtual desktops can be managed as a group.

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

McAfee Security Suite for VDI Configuration

- McAfee MOVE AntiVirus
  - Multiplatform deployment
  - Agentless deployment
- Cloud Workload Discovery for private cloud (VMware and OpenStack)
- McAfee VirusScan® Enterprise for Windows
- McAfee VirusScan Enterprise for Linux
- McAfee Host Intrusion Prevention for Desktops
- McAfee Application Control for Desktops
- McAfee SiteAdvisor® Enterprise technology
- McAfee ePolicy Orchestrator

McAfee MOVE AntiVirus in multiplatform deployments can enhance global reputation intelligence from McAfee Global Threat Intelligence with local data from McAfee Threat Intelligence Exchange, an additional module sold separately, to instantly identify and combat the ever-growing number of 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. It automatically immunizes all virtual desktops from newly detected malware.

Feature	Why You Need It
Virtualization security	▪ Improve the security of workloads deployed on virtual desktop infrastructures without compromising performance and resource utilization. ▪ Agentless deployment optimized for VMware helps deliver great performance and VM density. No need to install/update our agents in each virtual desktop—this reduces complexity and greatly improves usability. ▪ Multiplatform deployment for all hypervisors supports elastic provisioning of offline scanners to scale with demand and integrates with local reputation intelligence for faster threat response.
Core endpoint protection	▪ McAfee antivirus protection scans faster, uses less memory, and requires fewer CPU cycles while protecting better than other products. ▪ Host intrusion prevention safeguards businesses against complex security threats that may otherwise be unintentionally introduced or allowed. ▪ McAfee SiteAdvisor® Enterprise blocks users from interacting with dangerous websites and allows customization of policies to restrict access to potentially harmful websites, thereby ensuring policy compliance.
Application whitelisting	▪ Significantly lowers host performance impact over traditional endpoint security controls ▪ Protects against zero-day and advanced persistent threats (APTs) without signature updates, resulting in quicker time-to-protection ▪ Dynamic whitelisting requires lower operational overhead compared to legacy whitelisting techniques.

Feature	Why You Need It
Cloud Workload Discovery	▪ Provides full visibility of private cloud workloads and their underlying platforms to identify weak security controls
File and removable media protection (encryption)	▪ Encryption is made exceptionally easier and less risky to deploy with file and removable media protection. ▪ Near native performance on encrypted hosts through optimized implementation of Intel® AES-NI technology ▪ Delivers policy-enforced, automatic, transparent file/folder encryption, and removable media encryption (USB Drives, CDs, DVDs) ▪ Enables users to encrypt removable USB media and transfer information in a secure manner ▪ Enables secure access to data on network shares
Centralized management with McAfee ePO software	▪ Centrally manage physical, virtual, and cloud deployments for better security control, including policy management, deployment, visibility and security management across all platforms. ▪ Simplifies operational processes and reduces time investment for administrative staff ▪ Lowers hardware costs due to reduced server footprints

Learn More

McAfee solutions equip you with the security you need with minimal impact on performance. Visit **www.mcafee.com/virtual-desktops**.

McAfee™
Together is power.

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