McAfee Security Suite for Virtual Desktop Infrastructure

The Security You Need and the Flexibility You Deserve

Adoption of virtual desktops (VDIs) 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 VDI, which provides comprehensive security optimized for virtual desktops.

Key Advantages

- Discovery and visibility for VMware vSphere environments with McAfee ePO software and McAfee Data Center Connector for VMware vSphere. The unique combination of blacklisting and whitelisting protects physical and virtual from malware.
- Optimized virtualization security for minimal performance impact.
- Protect from unknown threats by preventing unwanted applications from running on your virtual desktops.
- Adds intrusion and web protection with desktop firewall, memory protection, and web application protection.
- Leverages McAfee ePO software to achieve at-a-glance visibility, control, and reporting across endpoints.

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 from accessing 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 (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

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

McAfee Security Suite for VDI Configuration

McAfee MOVE AntiVirus for Virtual Desktops (VDI).

- McAfee MOVE AntiVirus.
  - Multihypervisor deployment.
  - Agentless deployment.
- McAfee Data Center Connector for vSphere.
- McAfee VirusScan® Enterprise for Windows software.
- McAfee VirusScan Enterprise for Linux software.
- McAfee Host Intrusion Prevention System.
- McAfee Application Control for Desktops.
- McAfee SiteAdvisor® Enterprise technology.
- McAfee ePolicy Orchestrator software.

Agentless Deployment Leverages VMware vShield for 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 installation and configuration of the SVA and the required vShield components on 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 that 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 for monitoring of the SVA status within vCenter and receives alerts if the SVA loses connectivity. McAfee ePO software receives event data detailing the specific VM affected in the event a VM is infected.

Multihypervisor for Standards and Convenience

In multihypervisor 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 functions. 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 software console, or the virtual desktops can be managed as a group.

Learn More

McAfee solutions equip you with the security you need, and the flexibility you deserve. Visit **www.mcafee.com/virtual-desktops**.

Feature	Why You Need It
Virtualization security	• Improve the security of workloads deployed on virtual desktop infrastructures without compromising performance and resource utilization. • Multihypervisor and agentless deployment choices: deployment for mixed vendor virtualization environments (VMware, Citrix, Hyper-v). • Agentless deployment optimized for VMware help deliver great performance and VM density. No need to install/update McAfee agents in each virtual desktop—this reduces complexity and greatly improves usability.
Core endpoint protection	• Antivirus protection for physical servers that is number one ranked by NSS Labs against zero-day exploits and evasion attacks. • 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.
Full visibility of virtual machines in the private cloud	• Automatically discovers virtual machines in the private cloud (VMware vSphere).
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	• Single-pane-of-glass manageability for physical and virtual machines, including those in the private and public cloud for greater security visibility. • Simplifies operational processes and less time investment for administrative staff. • Lowers hardware costs due to reduced server footprints.

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

Intel and the Intel logo are registered trademarks of the Intel Corporation in the US and/or other countries. McAfee, the McAfee, ePolicy Orchestrator, McAfee ePO, VirusScan, and SiteAdvisor are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other marks and brands may be claimed as the property of others. Copyright © 2014 McAfee, Inc. 61145ds_vdi_0614B_fnl