Solution Brief

Secure Virtualization Everywhere

McAfee and VMware secure desktops, networks, data centers, and the cloud

"The combination of McAfee MOVE AV with VMware vShield Endpoint offers customers protection with top-rated security and high performance in their virtual desktop and server environments. This enables users to further embrace virtualization and benefit from the cost savings it provides."

—Parag Patel, vice president, Global Strategic Alliances, VMware

When you need to enhance your business by scaling your use of virtualization and the cloud, turn to McAfee and VMware for a purpose-built, optimized, and secure solution. From desktops to data centers, at your site or in the cloud, we help you extract the greatest efficiency from your virtualized resources while meeting your business needs for agility, security, and compliance.

As you increase your virtualization footprint, the need for security and scalable management increases as well. The McAfee and VMware alliance is committed to developing optimized security and management solutions so you can secure your virtualization and cloud computing infrastructures.

Optimized for vSphere and Against AV Storms

The agentless McAfee MOVE AV solution for endpoints leverages the VMware vShield architecture for high-performance, introspection, and efficient resource utilization, including both on-access and on-demand scanning. McAfee MOVE AV features a hardened, dedicated security virtual appliance (SVA) that integrates directly with vShield Endpoint to provide optimized malware protection for virtual servers and virtual desktops. You install, configure, and maintain only the security virtual appliance, yet every image is protected automatically at creation without the need to install software in guest VMs.

The McAfee SVA runs on the same VMware vSphere hypervisor and performs all the resource-heavy anti-malware scanning you need. We avoid the memory overhead of installing or maintaining an additional agent within each image. This approach prevents AV storms, the resource contention caused by simultaneous scan operations common when traditional antivirus is run within each image.

No gaps in protection

Together, our protection stays with your images through the virtualization lifecycle. After it scans a file, McAfee MOVE AV informs the vShield Endpoint Thin Agent that the file is safe to cache locally and allow users to access. It also informs which files to delete, deny access to, or quarantine. When a VM requests a file, if the file has been cached locally (pre-scanned), the user gets instant access. The MOVE SVA maintains a global cache of "known clean" files so resources are not wasted scanning files that are the same. If a file changes, it is rescanned by the security virtual appliance using the latest signature and global threat intelligence file reputation, providing continuous anti-malware coverage.

Security is uninterrupted when VMs move, since McAfee MOVE AV is vMotion-aware. If a scan is running on an image when it needs to be decommissioned or moved, we just pause the scan and resume scanning using the engine and DAT files on the security virtual appliance in the new location.

Live risk assessments from the cloud

To ensure that scans and assessments are always based on the most up-to-date risk assessment, the McAfee security virtual appliance has a real-time connection to the McAfee Global Threat Intelligence™ (McAfee GTI™) network. If a file appears suspicious, the SVA consults with the ever-expanding knowledgebase in our cloud-based system to determine if a file has a risky reputation. This instantaneous assessment helps detect and block emerging threats that get past signature-based detections. McAfee, with extensive, active research in network, endpoint, vulnerability, and content security, correlates events across threat vectors to protect your virtual desktops and servers with the most accurate threat intelligence. Your deployment benefits from our billions of sensors worldwide.

McAfee MOVE AV

The McAfee® Management Optimized for Virtual Environments AntiVirus (MOVE AV) supports your goals with the security you need and the flexibility you deserve. This is made possible through a choice of multiplatform and agentless solutions integrated with innovative VMware technologies for virtual servers and desktops. Other advanced McAfee solutions, such as McAfee Network Security Platform, work with VMware to secure virtualized network systems and make security manageable.

Protection against rootkits

Through VMware vShield Endpoint integration, your data is doubly protected. We fend off known and unknown malware before files and images are loaded. Then, the introspection of vSphere takes over to manage the image itself. This design neutralizes any rootkit that expects to hijack or deactivate the antivirus agent, since scanning operations are isolated from guest images.

Configured for extra confidence

McAfee MOVE features a pre-built security virtual appliance template. The McAfee MOVE AV for Virtual Desktops suite also includes memory protection, firewall, intrusion prevention, and web safety protection, to protect users from encountering or being infected by emerging threats. McAfee MOVE AV for Virtual Servers includes scanning of offline virtual images, so dormant virtual machines can be maintained and ready for use when brought back online. McAfee Data Center Security Suite for Server–Hypervisor Edition packages comprehensive security for virtualized servers with per-hypervisor licensing. These protections receive real-time risk decisions from the McAfee GTI network, too, for constant coverage against zero-day threats

Visibility through McAfee ePO and vCenter

McAfee ePO works with VMware vCenter to streamline monitoring and incident management. We integrate the MOVE AV SVA with the VMware vCenter management environment to provide detailed event information in McAfee ePO dashboards and reports. McAfee ePO maintains the MOVE AV policy and delivers content updates to the McAfee SVA. The MOVE SVA notifies the file filter portion of vShield to implement the assigned policy to build the event for reporting. The MOVE SVA also queries vCenter to map the VM universally unique identifier to the Guest VM Hostname in order to provide the administrator with details as to which VM was infected.

Strong security in the network

Integrated endpoint security for virtual environments is just one element of the expanding strategic relationship between VMware and McAfee. In addition to McAfee MOVE AV, McAfee offers several network and content security solutions that support VMware environments. For example, the McAfee Network Security Platform next-generation intrusion prevention system helps you apply consistent network security across physical or virtual environments.

Like McAfee MOVE AV, McAfee Network Security Platform connects to the dynamic McAfee GTI network to help you identify and shut down malicious traffic. Through integration with IP and file reputation services, Network Security Platform can help you profile and block incoming malware or the malicious external IP addresses that are attempting denial of service or buffer overflow attacks.

Additionally, native access to VMware vCenter tools lets you integrate network security across virtual environments and merge network security data with McAfee ePO and McAfee MOVE AV event data for a unified and centralized view of events.

Security and Compliance for the Data Center and Beyond

McAfee and VMware continue to do more so that your virtualized infrastructure can be efficient, secure, compliant, and highly manageable. To support your overall risk management strategy, data integration with the McAfee Enterprise Security Manager now allows your virtualized assets to be monitored as part of your security and information event management (SIEM) program. This integration permits real-time visibility of all activity on all systems, networks, databases, and applications leveraging the collection and analysis of a broad range of security data at "big data" volume: millions or billions of records every day. In addition, each administrator can create custom dashboards to monitor their data and interests and define reports on specific assets, including a blend of physical and virtual hosts. Support for roles makes it easier to match security to the collaborative administrative world of virtualized data centers.

Get moving

McAfee has teamed up with VMware to help you capture all the benefits of virtualization without cutting corners on security and compliance. Learn more at mcafee.com/virtualization.

McAfee ePolicy Orchestrator

The McAfee ePolicy Orchestrator® (McAfee ePO™) platform delivers and enforces policies and allows you to deploy McAfee software to all your virtual machines. You can enforce the same rules on virtual desktops and virtual servers, and aggregate all data into customized dashboards and reports, leveraging templates to support your governance and regulatory requirements.

Common controls for all your virtual and physical systems

Even the most extensively virtualized environments still have some physical infrastructure: Laptops, mobile devices, firewalls, and more. With its extensive integrations across McAfee and third-party products, McAfee ePO makes it easier to administer consistent policies and compliance across physical and virtual infrastructure.

McAfee Products that Support VMware APIs

- McAfee MOVE AV (agentless support for VMware vshield)
- McAfee Network Security Platform (includes native inspection of virtual environments through full integration with the VMware vShield Network Security API)
- McAfee VirusScan Enterprise
- McAfee Host Intrusion prevention

McAfee
An Intel Company

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

60211brf_secure-virt-everywhere_0513_ETMG