Solution Brief

Expand Virtualization. Maintain Security.

Key security decisions for virtualized infrastructures

As enterprises make virtualization mission-critical for servers and desktops, IT teams must support more users, more workloads, and more geographies, as well as new requirements like "just-in-time" provisioning and self-service. McAfee® Management for Optimized Virtual Environments AntiVirus (McAfee MOVE AntiVirus) tailors security systems to the special technical and management requirements of virtualization. It helps you securely achieve the desired efficiencies of virtualization while delivering a positive user experience.

Virtualization is an established part of industry-standard data centers with private cloud adoption increasing to 77% in 2016.[1] Through support of key programs, such as cloud computing, bring-your-own-device (BYOD), and server and data center consolidation, virtualization enables the twin goals of business savings and organizational flexibility. Virtualization is mission-critical for success. Yet it presents distinct operational and risk management challenges compared to traditional physical security installations. The new operational model of virtualization requires reassessment of traditional security operational processes, policies, and deployment decisions.

Performance Bottlenecks

The most obvious issue is scanning performance. In a traditional deployment, each system—desktop or server—runs anti-malware locally, scanning on access or on a schedule to ensure that the host remains uninfected. However, that per-node model is too resource-intensive for virtual environments. In events called "scan storms," scan operations can consume all available hypervisor memory and processing resources and prevent users from obtaining new sessions. Historically, many administrators have opted to turn off scanning or skip software updates in favor of maintaining performance.

However, as a mainstream enterprise platform, virtualized environments have become a new frontier for cybercriminals who exploit software and configuration vulnerabilities. Without current and active security scanning, virtualized infrastructure offers a fertile hunting ground for data thieves and attackers.

Update your security software.

A criminal's first target is an image running without any up-to-date anti-malware. You must maintain the security software on running and offline images as well as image templates (or gold images). Only freshly updated system security features and anti-malware content will be effective against attackers.

intel Security

As you scale up a virtualized desktop infrastructure (VDI), you may support thousands of virtual machines (VMs) being provisioned and decommissioned daily, making security maintenance less predictable. While perpetually running physical servers can be scheduled for security updates at a convenient time—when usage is low—desktop users must have security updates work around the dynamic workflows of VMs. Live images will move offline and be stored and inactive overnight—or for a few hours. Then users will expect instant access to their virtualized systems without delays for boot and scanning operations.

Data centers house a blend of assets.
Data centers add further process complexity. Server, storage, and network resources blend together to deliver maximum utilization, but this commingling has two ramifications. First, you lose the security advantages of physical separation between databases, application servers, web servers, and other software. Physical isolation frustrates the expansion hopes of malware authors and hackers. To compensate, stronger security must be designed into virtualized systems, including those in the cloud.

Second, management processes must change, since previously distinct server, storage, and network functions now share the same management console. Where these resources used to have separate administrators and policies, they must now coexist in one policy and procedure environment, often managed by a single virtualization administrator, a "super user." In this situation, processes and alerts compete for management visibility, and policies may need to be normalized. Administrators have to find ways to collaborate operationally.

Multiple vendors can create challenges.
Many organizations add the challenge of vendor diversity to these changes. Different virtualization vendors have different strengths, and many companies require a second source for mission-critical software. As a result, your deployment may include a mix of hypervisors. You must secure images and report on your compliance while accommodating the different attributes of each offering.

How do you meet compliance requirements?
As if these issues were not enough, you must show that your virtualized systems meet the compliance expectations previously—and usually still—imposed on your physical systems. Today's regulations specify regular maintenance of anti-malware. For example, the Massachusetts privacy law (201 CMR 1700)[2] requires "Reasonably up-to-date versions of system security agent software, which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis."

All of these problems represent practical concerns about day-to-day security operations for virtualized systems within a dynamic threat landscape. Traditional models of security from the physical world must be extended—or supplanted—in favor of security optimized for the realm of virtualization.

Optimize Operations with McAfee MOVE AntiVirus

When Intel Security began working with the virtualization community several years ago, we saw these operational issues begin to emerge. We responded with specialized technology that enables the best of our security capabilities to work efficiently within a virtualized server and desktop deployments. McAfee MOVE AntiVirus offers malware protection and security without compromising performance. You get the most value out of powerful virtualization technology while maintaining user productivity and security of the guest operating system (OS) in the VM.

Our solution offers the flexibility to choose your preferred deployment model—one that works across multiple virtualization platforms—or an "agentless" tuned option for VMware NSX and VMware vCNS. Both options take full advantage of our proven, industry-leading anti-malware. In addition, McAfee MOVE AntiVirus for Virtual Desktops (VDI) provides intrusion prevention and web application security for extra protection against malicious attacks.

Scan when you can and only when you need to.
McAfee MOVE AntiVirus frees hypervisor resources to serve other functions while ensuring that up-to-date security scans run according to policy. A hardened virtual or physical appliance takes on responsibility for processing scans, maintaining configurations, and updating .DAT signatures, allowing the hypervisor to remain devoted to supporting guest images.

Integration of McAfee MOVE AntiVirus with the virtualization management software allows us to avoid "scan storms" caused by many images requesting provisioning and scanning at once. Further, McAfee MOVE AntiVirus for Virtual Servers can intelligently schedule scans based on hypervisor and resource availability. Active VMs do not need to be taken offline to be scanned. However, when images move offline, McAfee can scan and update the images to keep them ready for use.

McAfee MOVE AntiVirus allows separate policies for on-access scanning (OAS) and on-demand scanning (ODS) so that tuning and security can be executed with greater control. This means that you can accept some reasonable level of risk for real-time OAS to minimize impact on performance and then use ODS to catch the holes permitted by more lenient OAS policies at a later time when there will be less impact.

"McAfee MOVE AntiVirus provides McKesson with comprehensive and consistent malicious code protection for our virtual environment. As we continue to adopt emerging technologies, particularly cloud computing solutions, implementing McAfee MOVE AntiVirus provides us with additional security in our virtual environment. The solution makes sizing and deployment simpler and ensures that every system is deployed with the same level of protection."

—Patrick Enyart
Senior Director
McKesson Information Security

Apply the latest insights.
To keep scans as current as possible without slowing down performance, McAfee MOVE AntiVirus downloads and applies the most up-to-date signatures to the offload scan server, not to individual VMs. McAfee MOVE AntiVirus consults McAfee Global Threat Intelligence (McAfee GTI) for real-time file reputation when unknown files seem suspicious. McAfee MOVE AntiVirus in multiplatform deployments can enhance intelligence from McAfee GTI 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 and automatically immunizes all endpoints from newly detected malware.

Going beyond anti-malware scanning, McAfee MOVE AntiVirus for Virtual Desktops includes advanced memory protection to restrict malicious activities and preserve file integrity. To help users avoid risky websites that can introduce malware to the image while in operation, McAfee also includes web reputation alerts and policy-based controls over web usage. Together, these tools reduce the attack surface of your virtualized systems. For the most potent protection, other tools like application whitelisting can be included to prevent undesired applications or malware from disrupting operations.

Use resources efficiently.
As scanning demand fluctuates in multiplatform deployments, SVMs can automatically be added to or removed from the resource pool to scale your scanning power up or down for unlimited scalability and efficient resource utilization. Event notifications help administrators understand SVM usage trends to further optimize resource management.

Virtual Server and Network Security: Smarter Together

Virtualization also changes the way organizations approach network security and virtual machine protection. When physical infrastructure is virtualized, new strategies are required to create and maintain security boundaries in the absence of physical partitions so that threats don't take advantage of siloed security to exploit weaknesses.

McAfee MOVE AntiVirus integration with McAfee Network Security Platform through McAfee Threat Intelligence Exchange provides a layered security approach for unified perimeter and virtual machine protection. Threat details collected from malware encounters at network gateways can propagate through McAfee Data Exchange Layer, a high-speed integration and communication layer, in milliseconds, reaching all endpoints and immunizing them against threats. Conversely, McAfee Network Security Platform can leverage malware detection at the endpoint by McAfee MOVE AntiVirus to block downloads.

Manage it all with ease.
McAfee MOVE AntiVirus uses the same McAfee® ePolicy Orchestrator® (McAfee ePO™) security management console that administrators know already from security management for Intel Security physical endpoints. Within one policy and console system, each administrator can create custom dashboards to monitor their data and interests and create reports on specific assets, including a blend of physical and virtual hosts—both endpoints and servers. The McAfee Data Center Connector for vSphere offers a complete view into virtual data centers based on VMware and populates key properties such as servers, hypervisors, and VMs through the McAfee ePO console. McAfee Server Security Suite Essentials and McAfee Server Security Suite Advanced extend visibility and control across Amazon Web Services and Microsoft Azure public clouds, physical servers, and OpenStack.

Standardize or specialize.
The choice of a multiplatform or agentless-based implementation means you can support both current and evolving vendor relationships. The multiplatform solution uses a lightweight agent within each guest image to manage policies and scans, leveraging an offload scan server for on-access scans. This approach allows you to mix Citrix, Microsoft, VMware, and Microsoft hypervisors for greater flexibility or to accommodate different user communities.

Our agentless alternative integrates very closely with VMware to leverage your investment in hypervisor technology. McAfee MOVE AntiVirus works through VMware NSX or VMware vCNS to scan virtual machines from outside guest images, with no Intel Security software within the image itself. Through VMware vMotion, scanned VMs can migrate from one host to another without affecting the user or the scanning systems. McAfee ePO software integration with VMware NSX and VMware vCNS streamlines monitoring and incident management.

Your organization may want to take advantage of the flexibility inherent in McAfee MOVE AntiVirus to support both agentless and multiplatform deployments. Unified policy management provides security administrators with the ability to define and manage consistent security policies across these deployments from McAfee ePO software.

Achieve continuous compliance.
The common McAfee ePO platform also allows you to ensure that policies are consistent across both physical and virtual systems. To support compliance processes, you can create an auditor view of pertinent data and run ad hoc or scheduled reports specific to regulations.

Move Ahead

You can now match security to the unique requirements of virtualization. Intel Security has optimized its anti-malware and endpoint protections to work within and around the design and processes that deliver virtualization efficiencies. Scanning stays out of the way of active users, while security software and signature update processes respect the online-again, offline-again nature of desktop and server images.

Our flexible design lets you work with the vendors you prefer and still meet security and compliance standards. Intel Security helps you discover, secure, and grow your virtualization environment, without letting your users and data fall prey to today's cybercriminals. We continue to invest in integration and optimization across our broad product portfolio to enable you to deploy the strongest security with the greatest efficiency as you expand your use of virtualization.

For more information about McAfee MOVE AntiVirus, please visit **www.mcafee.com/virtualization**, **www.mcafee.com/us/products/move-anti-virus.aspx**, and **www.mcafee.com/virtual-desktops** or contact your local McAfee representative or reseller.

1. **http://www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2016-state-cloud-survey**
2. 201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth **http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf**

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