

Anti-Virus Optimized for Virtualized Environments

McAfee® MOVE Anti-virus delivers support for VDI and server virtualization without compromising performance or security



Enterprises have started to deploy virtual desktop infrastructure (VDI) and solutions, and they struggle with the persistent or dynamic options for their end users. Adding to the complexity of these projects is the challenge of ensuring user performance and expectations. Capacity planning and understanding how to achieve predictable resource utilization, while at the same time supporting virtualized servers with diverse operating parameters and protecting against malware, has been operationally challenging. McAfee Management for Optimized Virtual Environments (MOVE) Anti-virus for virtual desktops and servers is uniquely designed to relieve the overhead of traditional virus scan, yet provide the protection and performance essential for success.

Virtual Desktop Anti-Virus Problem

Enterprises are considering or may have already deployed VDI and want the flexibility to either build images dynamically at logon, or serve persistent images from the data center to the end user. The ability to provide more control over data and access drives return on investment; however, moving to serve these endpoints from within the data center does have some infrastructure implications that were not previously considered. The dynamic nature of provisioning desktops and their overall load in a virtualized environment is hard enough to model and capacity plan. Anti-virus that is not designed for virtual environments makes this task significantly more complex. Even though the user desktop has been virtualized and can run traditional anti-virus software within the individual virtual machine, the accumulative performance impact on the infrastructure has been found to be extensive. This directly affects the total number of virtual desktops that can be supported and decreases the expectations of operational returns. With today's persistent threats and proliferation of malware, running endpoints without anti-virus is not an option. With the consolidation of corporate data within the data center, the need to be more vigilant and provide constant protection actually increases as activity at the endpoint is now closer to critical data and servers than ever before. Virtualization provides the ability to quickly repair and mitigate the spread of viruses by generating pristine desktop images and decreasing risk, but on-access and on-demand virus scanning is still essential in these environments.

How Is McAfee MOVE Anti-Virus for Virtual Desktops Different?

McAfee enables customers to use their current McAfee Virus Scan protection and optimize it for virtualized environments. McAfee MOVE Anti-virus is an add-on component that is designed to support on-demand, on-access, and update functions within virtual desktop environments, greatly reducing the infrastructure impacts seen with traditional anti-virus deployments. Supporting all VDI types with VMware View and Citrix XenDesktop, a lightweight endpoint component communicates to the McAfee MOVE virtual appliance to broker the anti-virus processing on behalf of each virtual machine desktop. This enables each virtual machine to be configured with unique and individual policies as set in McAfee ePolicy Orchestrator® (ePO™) management console, or the option to be managed as a collective work group. Images created dynamically or persistently will have protection throughout the VDI session. Within

virtualized environments, ensuring that .DAT updates are timely and on-access scanning is enabled provides the active protection during each session which is so important. Even though you can reimage quickly, the goal is to prevent you from having to perform this activity in the first place. McAfee MOVE Anti-virus for virtual desktops provides this capability, and is highly effective at not degrading the user experience or greatly impacting the load of the hypervisor.

The scalability that can be achieved when anti-virus scanning is performed outside of the individual virtual machine dramatically reduces the resource requirements needed within the overall environment. McAfee can support up to 100,000 desktops (virtual and physical) and is continually updated from McAfee's Global Threat Intelligence (GTI). McAfee MOVE virtual appliance provides the most recent signatures, and it handles the offload processing of on-access and on-demand scanning, updating each virtual machine with the results. Memory resource allocation for each virtual machine decreases and can be released back to the resource pool for more effective utilization. Regardless of a virtual machine desktop's previous state, McAfee MOVE virtual appliance supplies and ensures continuous protection through its active sessions.

Virtual Servers and Anti-Virus

Servers normally are configured to provide on-demand anti-virus scanning during nonbusiness hours to minimize disruption. When these systems are migrated into a virtual environment, scheduling of multiple virtual servers can cause CPU spikes and interfere with other operational activities that need to occur, such as patching and backups that also get scheduled during these time periods. Today, the best practice is to randomize the scheduling of on-demand scanning, but it is not ideal and is not hypervisor-aware. Being hypervisor-aware gives more flexibility to understand the overall state and load of the hypervisor to minimize operational scheduling impacts driving efficient security processing.

How Is McAfee MOVE Anti-Virus for Virtual Servers Different?

McAfee MOVE virtual appliance provides the ability, akin to virtualized desktops, to broker services on behalf of virtual servers to provide McAfee Virus Scan improved performance specifically for virtualized environments. This provides the operational flexibility that is lacking today with the support of continuous anti-virus protection and refined security management scheduling. McAfee was one of the original providers of server offline scanning, and now extends the scheduling capabilities to go beyond the state of the virtual machine, making them hypervisor-aware and able to schedule scanning based on the overall load of the hypervisor. When diverse servers are deployed within a single hypervisor, this ensures that critical operational activities are not disrupted or foregone due to unexpected resource issues.

For today's systems where 24x7 performance is required, server virtualization allows for flexible provisioning and migration within hypervisors to accommodate resource requirements. McAfee MOVE Anti-virus for virtualized servers can provide offline security for servers that are not active. This ensures that they are protected and ready to initialize immediately without the delay of virus scanning. Servers that are continually performing due to their service-level agreements can be protected with McAfee MOVE Antivirus by optimizing the McAfee Virus Scan through hypervisor-aware scheduling to minimize the overall operational impact of the security processing.

McAfee MOVE Anti-Virus Optimized for Virtualized Environments

Whether you are deploying virtual desktops or well underway with server virtualization within your data center, McAfee MOVE Anti-virus products provide optimized protection that specifically addresses the common problems encountered in virtualized environments with traditional anti-virus solutions. McAfee MOVE Anti-virus provides malware protection and security without compromising on performance, helping our customers get the most of this new technology and ensuring active protection of their business data.

Next Steps

For more information about McAfee MOVE Anti-virus, please visit www.mcafee.com/virtualization or contact your local McAfee representative or reseller near you.

