

# Securing the Virtual Desktop: Removing the Last Barrier to Widespread Adoption

by Simon Crosby, Chief Technology Officer, Datacenter and Cloud Division, Citrix Systems, Inc.

In May 2010, McAfee and Citrix announced a strategic partnership and collaboration agreement to make virtual desktop security simpler and more scalable for large enterprise deployments. The collaboration between the two leaders in security and virtualization will enable Citrix XenDesktop customers to extend management of desktop security to virtual environments using the McAfee® ePolicy Orchestrator® platform. The partnership is the direct result of growing customer demand for integrated security management in large-scale enterprise deployments of desktop virtualization.

As a company with some experience in virtualization, including the leading product for desktop virtualization, Citrix XenDesktop, Citrix knows a thing or two about this topic. What we don't claim to be is an expert on security. At Citrix, we recognize how vital security is for desktop and server virtualization. But, rather than trying to build security into our virtualization offering, we believe that a better approach is to work with partners who have that domain expertise. The partnership between Citrix and McAfee makes a lot of sense for our customers because it enables them to achieve the benefits they're seeking from virtualization.

This is important because, despite the demonstrable benefits, companies are moving more slowly than expected to adopt virtualization, especially desktop virtualization (or VDI). In fact, it's been estimated that perhaps only 40 percent of companies that could benefit from VDI have deployed desktop virtualization. Analysts like Gartner have suggested that this slower adoption has to do primarily with concerns over the way security impacts performance in a virtualized environment. Those concerns have been well founded—until now.

Here's why. Lacking a virtualization-optimized security solution, IT organizations have applied security to virtual machines and virtual desktops the same way they applied endpoint security in the past: one security agent per endpoint. Treating each virtual machine (VM) as an endpoint that needs to be protected, IT organizations have

typically deployed one security agent in each VM or virtual desktop.

This model makes sense for traditional endpoints, but it causes huge problems in a virtualized environment. Because a single physical machine can host a large number of VMs or virtual desktops, each one with its own security agent, the physical server ends up with multiple copies of security agents, signature files, threat databases, and so on. This approach wastes CPU, memory, and storage.

But the real issue is performance. If those endpoint protection systems all update themselves at exactly the same time, it creates what I call "an anti-virus storm," which hammers performance. This model can quickly max out the CPU and memory, bog down the network, and create I/O bottlenecks. For example, you might have 120 security systems running in parallel on the same server. It's no wonder IT administrators are worried about performance.

To address the performance issue of security for virtualization, some virtualization vendors have tried to strengthen their security capabilities. We applaud them for the effort, but at Citrix we don't think it's the right approach. As I mentioned above, we believe an integrated, best-of-breed approach is far better for our customers. At Citrix, we freely admit that "finding bad guys" is not our forte. From our perspective, a partnership with McAfee is really a perfect match of a very rich security portfolio with an extremely rich delivery portfolio.

**Editorial Brief**    **Securing the Virtual Desktop: Removing the Last Barrier to Widespread Adoption**

With that in mind, Citrix and McAfee together have taken an approach that moves the security function outside the virtual machine and allows the virtual infrastructure to confer security on the hosted guest virtual machines. One advantage of this approach is the ability to secure the virtual infrastructure itself, which is also vulnerable and needs to be appropriately protected. But the bigger benefit is performance.

The McAfee Management for Optimized Virtual Environments (McAfee MOVE) platform, supporting Citrix XenDesktop, provides security management designed specifically for virtualized environments. Rather than running endpoint security in each virtual machine, McAfee MOVE AntiVirus for VDI delivers a virtual appliance that consolidates scanning processes and signature updates, efficiently protecting all virtualized desktops and dramatically improving scalability.

By moving security outside the virtual machine, we can now enable intelligent scanning, allowing IT administrators to schedule scans when they are most convenient, based on hypervisor loads or when images are offline. This approach also gives

you the ability to off-load the processing-intensive actions from the individual VMs. And it simplifies the work of IT by centralizing security management so you easily manage all virus scanning and virus signature file updates with a single console such as McAfee ePolicy Orchestrator. By reducing CPU, memory, and storage requirements while simplifying desktop security, we've been able to enhance the security and scalability of virtual desktop deployments.

The results are groundbreaking. In McAfee and Citrix tests, McAfee MOVE AntiVirus for VDI enabled an increase of three times the number of virtual machines, as compared to endpoint security implemented within the individual virtual machine. This kind of efficiency is an absolute necessity for companies looking at virtualizing the desktop. We believe that it removes the biggest barrier standing in the way of widespread adoption.

For more information about how the McAfee/Citrix partnership can help you realize the benefits of secure desktop virtualization, visit [www.mcafee.com/citrix](http://www.mcafee.com/citrix) or [www.mcafee.com/virtualization](http://www.mcafee.com/virtualization).



**Simon Crosby** is the CTO of the Datacenter and Cloud Division at Citrix. He was founder and CTO of XenSource prior to its acquisition by Citrix. Prior to XenSource, Mr. Crosby was a principal engineer at Intel and the founder of CPlane Inc., a network optimization software company.



McAfee, Inc.  
2821 Mission College Boulevard  
Santa Clara, CA 95054  
888 847 8766  
[www.mcafee.com](http://www.mcafee.com)

The information in this document is provided only for educational purposes and for the convenience of McAfee customers. The information contained herein is subject to change without notice, and is provided "AS IS" without guarantee or warranty as to the accuracy or applicability of the information to any specific situation or circumstance.

McAfee, the McAfee logo, and McAfee ePolicy Orchestrator 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 ©2010 McAfee, Inc. 14103brf\_virtualization\_0910\_fnl\_ASD