5NINE SOFTWARE

Technology Brief: May 2013

Why Agentless Security Is The Best Choice

by David Davis

Windows Server 2012

Get more white papers from 5nine Software

Future Prospects for Virtual Machines

There are now more servers running as virtual machines than there are physical servers in the world. Gartner estimates that in 2014 roughly 75% of all servers will be virtual with the number continuing to rise, year after year. It's also estimated that an equal number of those virtual servers will use Hyper-V and vSphere. No matter the hypervisor used, it's virtualization that provides the opportunity for server admins to perform so many traditional tasks in new ways that are tremendously more efficient than in the past.

One of the vast improvements offered by virtualization is the ability for tasks that were previously happening inside each VM / Virtual Server to be moved up the stack and now happen at the virtualization host (hypervisor) level.

One of these common administration tasks is to ensure that viruses and malware aren't infecting your company's servers. However, if you have ever sat and watched an anti-virus scan happen on your local desktop, you know how long these tasks can take and how resources intensive they can be. If you are like me, you may have even, at some point, attempted to shut down your antivirus application that was slowing down your entire desktop, just to run more critical applications.

Now picture that fat, resource-intensive, anti-virus client running on every one of your virtualized servers on top of the Hyper-V virtual infrastructure. Do you want those scans slowing down your company's most critical servers?

No, you want to offload this from inside the virtual machine and, instead, use a much faster and efficient method – provided to you by server virtualization.

Top 4 Must Knows About Agentless Security

1. Virtually no performance impact on virtual machines because fast incremental scans are used that leverage the host resources only.
2. The change block tracking (CBT) scan driver allows for AV scans that run up to 50x faster than traditional full scans and will never create an AV storm.
3. Much higher VM to host consolidation ratios are achieved because virtually no system resources are consumed.
4. Agentless architecture eliminates administrative overhead as just a single host install is required.

Understanding Agentless vs. Agent-Based Anti-Malware Solutions

Since virtualization entered the datacenter, traditional (read "legacy") software vendors have been arguing that their agent-based solutions are more efficient than new, cutting edge, agentless solutions. These solutions could be backup, security, or any other solution that requires access to virtual machine data.

If you think about it, agent-based solutions just don't make sense and here are 3 reasons why:

1. CPU and memory overhead on each virtual machine impacts applications and end users.
2. Managing and apdating agents as well as their associated signature files is a waste of your time.
3. When agents start scanning all at the same time, you'll have a storm, slowing down all virtual machines in the Hyper-V infrastructure.

On the contrary, 5nine Security for Hyper-V uses no agents for scanning and prevents all the problems discussed above. Agentless security means that there is no need to manage multiple agents and signature databases, no degradation of performance, you'll get the industry's fastest incremental scanning of virtual machines, and be able to totally eliminate "AV Storms".

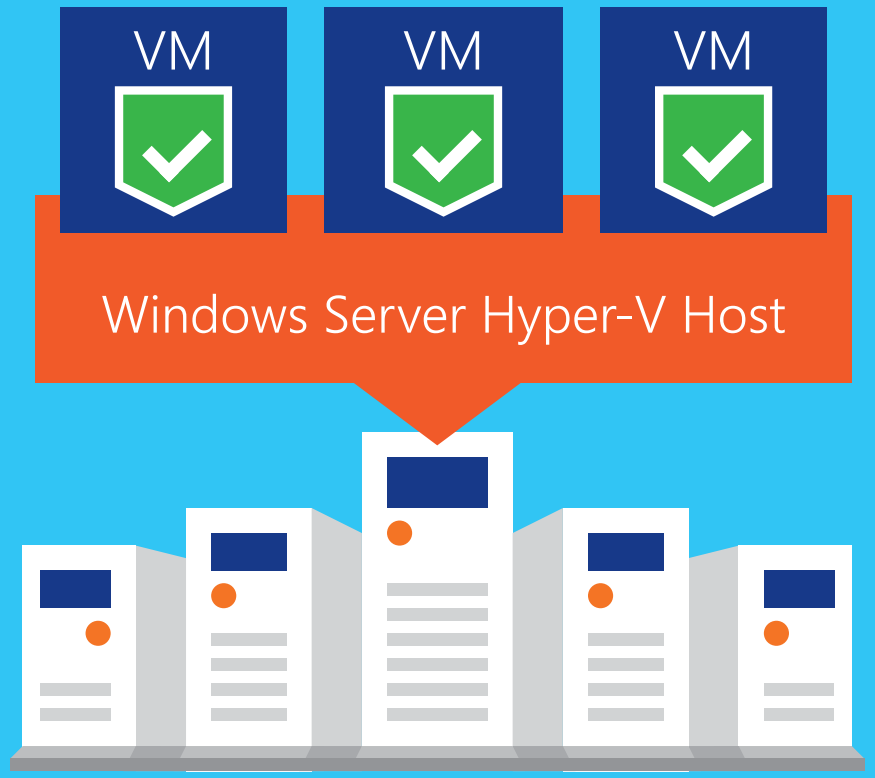
Additionally, even initial scanning of hosts and virtual machine disks provides better performance than 'classic' enterprise / endpoint anti-virus scanning due to how the host CPU and memory resources are utilized.

Many virtualization experts recommend NOT installing traditional agent-based solutions on Hyper-V hosts as scanning virtual machine disk files can cause virtual machine performance latency or, in some cases, corruption of virtual machine disk files.

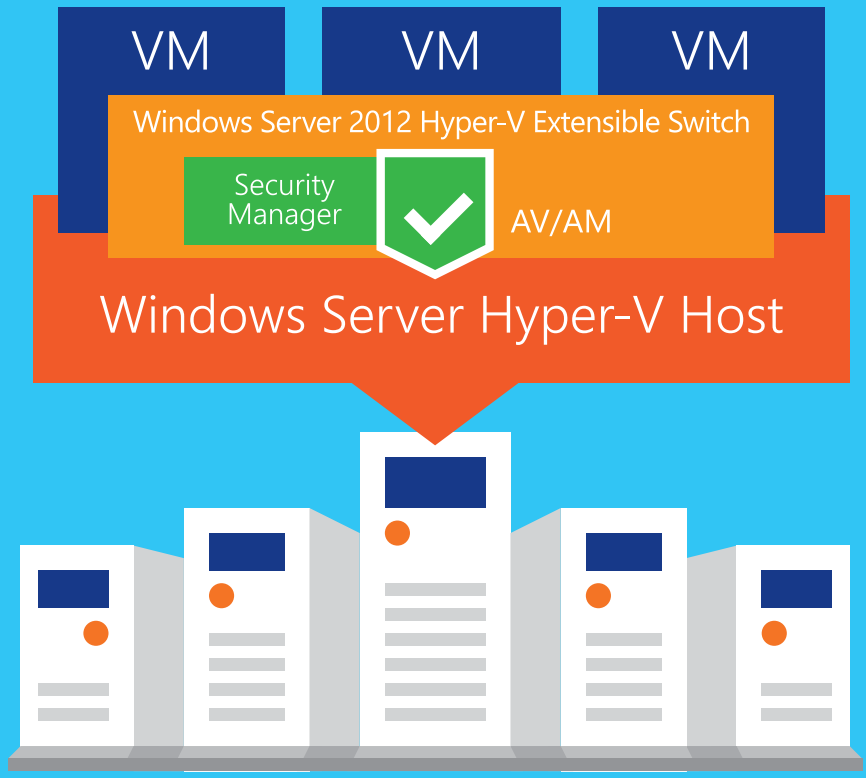
Note: 5nine's agentless anti-malware will install a thin agent on a virtual machine if "on access" scanning protection is enabled.

Undoubtedly, agentless security protection is the more modern and most efficient option. To back that claim up, let's review the performance test results.

Old Way: Agent-based



New Way: Agentless



Performance Tests Prove – Agentless Anti-Malware Is Faster

In performed tests, it was found that 5nine's agentless anti-virus / anti-malware solution was able to perform the same full scan of a virtual machine, once the initial full scan was completed, between 10 to 70 times faster than agent-based solutions.

5NINE SOFTWARE

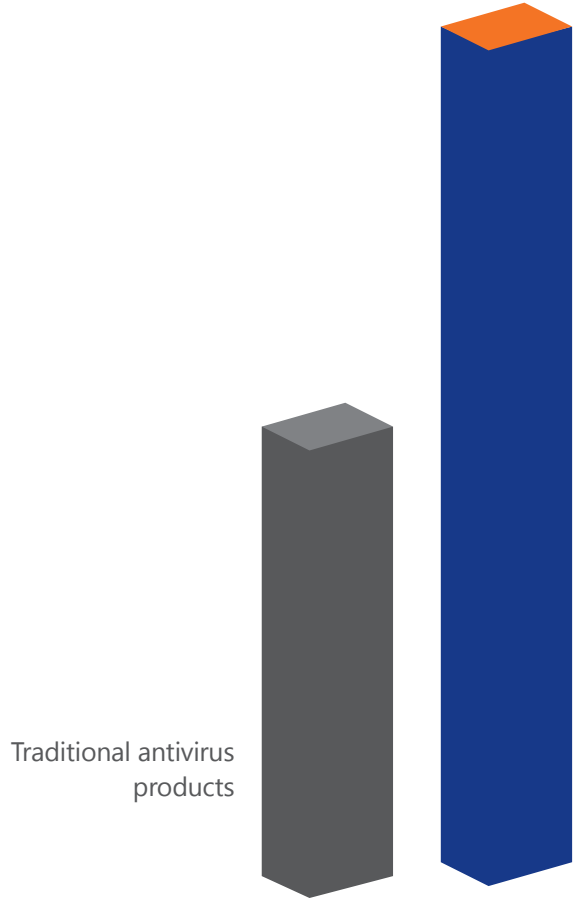
agentless anti-virus

up to

x70

faster
than other agent-based solutions in full scan of a Virtual Machine

Initial full scans of hosts and VMs, depending on amount of VMs, are 40 to 100% faster than traditional antivirus products. Time savings equates to resource savings across every VM running antivirus software.



5NINE SOFTWARE

agentless anti-virus

up to

100%

faster
than traditional antivirus products in initial full scans of hosts and VMs

Performance Tests Prove – Agentless Anti-Malware Is Faster

5nine Software's Security for Hyper-V shows an incremental full scan of hosts and VM averaging between 40 seconds and three minutes, depending on changes to the VM virtual disk and memory.

Additionally, those same scans took significantly fewer server resources to run. In our tests, resource consumption was less, across the board, including average CPU utilization, network I/O utilization, and physical memory utilization.

If you multiply these tremendously faster scan times and lower resource utilization rates across all your tens or hundreds of virtual machines, you will realize massive resource savings allowing you to further capitalize on your virtual infrastructure investment by add more virtual machines on your existing hardware and hypervisor infrastructure.

My Recommendation

Every virtual infrastructure needs security protection. Too many enterprises use the "hard outer shell, soft center" approach to security where they assume that if they have a firewall protecting the entire enterprise, they are secure.

This is a false sense of security as there are too many ways for malicious attackers (or just their malware) to enter the datacenter. Once in the datacenter, applications outages tend to occur when just a single tier-1 server is impacted by malware.

As the number of servers in the data center grows and we consolidate them with virtualization, ensure that you are protecting your most critical assets in the datacenter – the virtual infrastructure.

Do you protect that critical asset with a slow and bloated legacy security tool? No. The overwhelming facts support the agentless approach (despite what the legacy vendors will tell you).

I've tested 5nine Security for Hyper-V in my own lab and it worked as promised to protect my virtual infrastructure.

I recommend that you try it for yourself with the free 5nine Security for Hyper-V evaluation, available from the www.5nine.com website.

About the Author

David Davis is the author of best-selling VMware vSphere and Microsoft Hyper-V video training library from www.TrainSignal.com.

He has written hundreds of virtualization articles on the Web, is a vExpert,VCP, VCAP-DCA, and CCIE #9369 with more than 18 years of enterprise IT experience. His personal website is www.VMwareVideos.com.

@davidmdavis

About 5nine Software

5nine Software is the premier virtualization security management company, offering the first and only agent-less security management and compliance solution for Microsoft Hyper-V.

Our powerful, yet easy-to-use solutions help over twenty-thousand organizations worldwide safeguard their investments in virtual infrastructures by providing innovative security management software designed to reduce costs, increase productivity and mitigate risks.

We deliver innovative and practical solutions to help IT professionals more effectively plan, create and manage their virtual infrastructures.

Download 5nine Security Manager trial

Download Now