5NINE
SOFTWARE

White Paper

PROTECT

Windows Server 2012 / R2
Hyper-V and Windows 8.x
with Free Security from 5nine Software

By David Davis

Microsoft Partner Network

With the Microsoft Windows operating system being the most popular OS in the world, it's undeniable that it's also the most popular operating system to attack.

Just about every network in the world is infected with some kind of virus or malware application, all transmitted over the Internet.

Unprotected Windows systems are the ideal target for attackers.

However, even if you were protected from those, there are new viruses and malware created every day.

When viruses and malware aren't used, port-scanning applications could find an open port on your system to gain access.

So what's the solution?

Comprehensive Multi-level Protection

Because there are multiple ways that your system could be attacked, you must use a comprehensive, multi-level security protection solution for your Windows systems. You may be using Windows 8.x (with or without Hyper-V) on your laptop or Windows Server 2012, R2, or Hyper-V in your enterprise datacenter. No matter the modern Windows OS that you use, the multi-level protection system that you should choose is the same.

You need a solution that protects you from:

- Current viruses

- Future viruses

- Network-based attacks

If you just have a single Windows system to secure then your job is easier than if you are running Hyper-V (on either Windows 8.x or Win dows 2012/R2) and hosting tens or hundreds of virtual machines per server.

While single Windows systems (Windows 8.x or 2012/R2) still need protection, hosts that are running Hyper-V with multiple virtual machines (or even hundreds) need protection even more as they have many more attack surfaces.

The answer is to use a security protection solution that is comprehensive enough to protect not only the attacks mentioned above on the host but also protect from the same attacks on virtual machines. Better yet, that protection system should be smart enough to scan virtual machine disk files running inside Hyper-V without you having to install agents inside each of your virtual machines. This agentless, host-based approach is much more efficient, and comprehensive, allowing you to scan, potentially, hundreds of virtual machines from a single host system, much faster than traditional endpoint anti-virus solutions ever could.

Additionally, if you select a solution that can perform incremental anti-virus scanning based on block-tracking, you can achieve AV scanning 50 times faster than legacy AV solutions that use agents and are based on file scanning.

To sum up "comprehensive multi-level protection" for Windows, it should include:

- Agentless anti-malware and anti-virus scanning for Windows hosts and virtual machines that works by block tracking, not by file scanning

- Intrusion detection to protect against malicious attacks, denial of service attacks, cross-site scripting, and more

- Virtual Firewall for network-based attack protection

- Performance analysis to determine if the Windows system is currently overtaxed with too many running virtual machines or not enough resources configured.

How 5nine Free Security and Compliance Scanner Can Help?

Recently I tried a new free tool from 5nine software that helps to ensure that all of your Windows 8/8.1 or 2012/R2 systems are secured with the multi-level comprehensive protection as I described. 5nine Security and Compliance Scanner can provide that protection for both your Windows hosts (running 8/8.1 or 2012/R2) as well as any virtual machines running inside Hyper-V.

I tested the free 5nine Security and Compliance Scanner from www.5nine.com myself, and recommend that you do as well. If you download the small installer and go through the short installation, here's what you'll see:

Figure 1. 5nine Security and Compliance Scanner
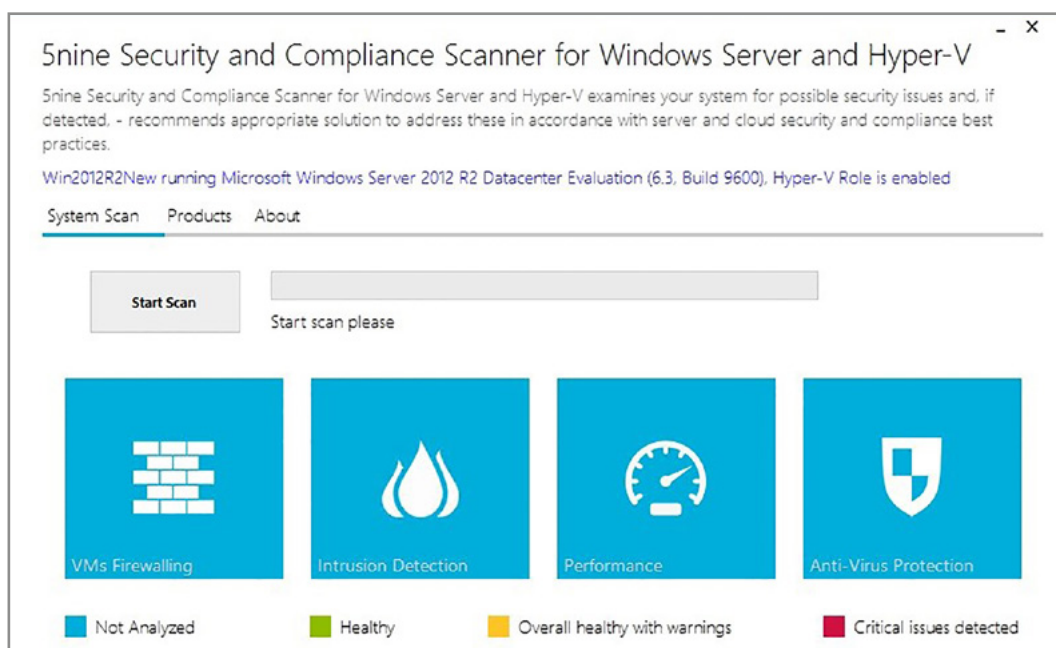
By clicking Start Scan, the tool will do the following:

- Checks to see if a virtualization firewall is installed (assuming you are using Hyper-V)

- Verifies that an intrusion detection system is enabled

- Analyzes system performance to see that adequate resources are available and that virtual machines are running normally

- Scans the host and any VM (virtual machine) agentlessly to verify that no viruses or malware are running or on disk

For example, here are the results of a security scan if no virtual machine anti-virus, no IDS, and no VM firewalling are detected:


Figure 2. Security Issues Found
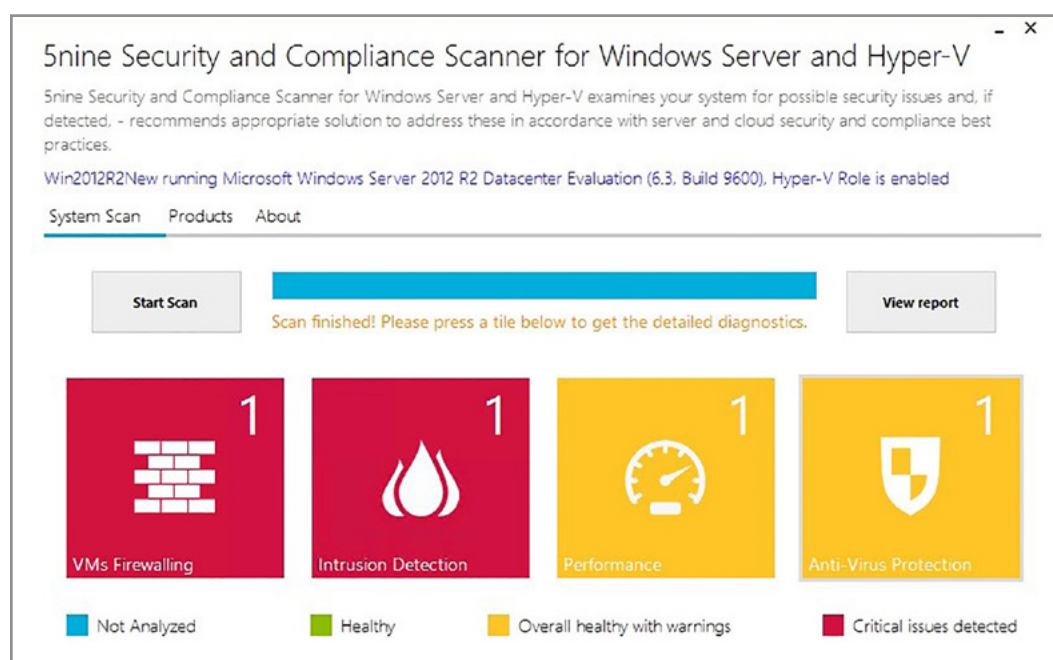
By clicking on any of the four main tiles, you'll be given the chance to either enable the free 5nine Cloud Security or purchase the full version, as you see in Figure 3 below.

5nine Cloud Security Free Edition provides a simple virtual firewall and agentless anti-virus for hosts and virtual machines. The full edition of 5nine Cloud Security Manager will add real-time agentless monitoring and network traffic filtering across hosts and virtual machines.

No matter which edition you select, 5nine Cloud Security Manager will utilize special block tracking technology to perform incremental anti-virus scans (of hosts and VMs) which will result in AV scans that are **50x faster** than legacy AV products.


Figure 3. Virus Protection Status
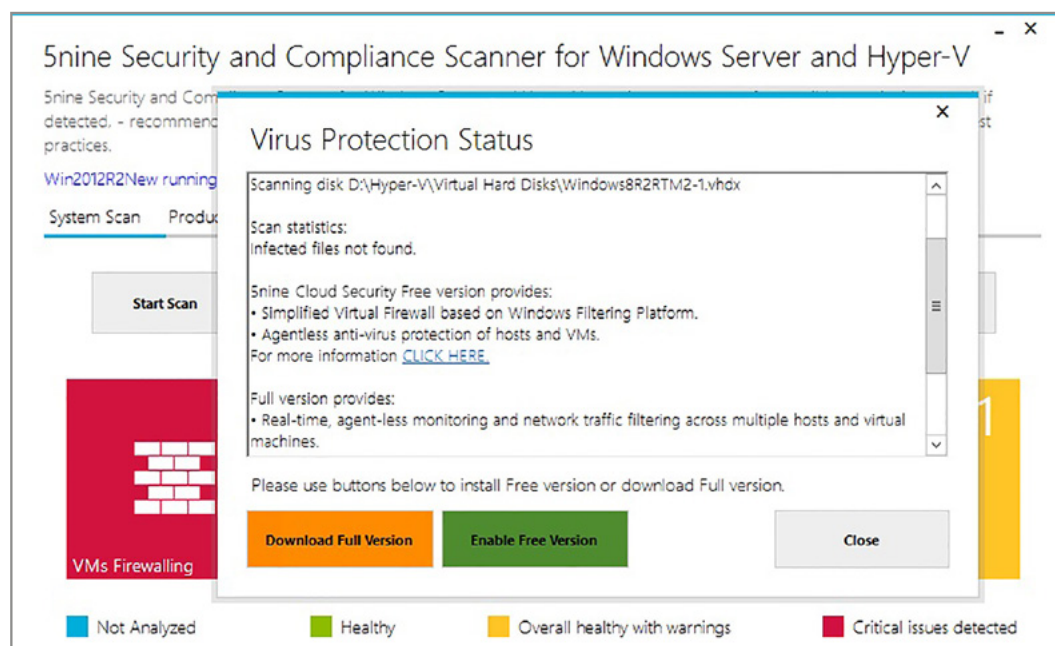
If you click on the Virtual Firewall Status tile, you may find that you need protection for your virtual network (shown in Figure 4). 5nine Cloud Security free edition offers basic virtual network protection for Hyper-V VMs.

Figure 4. Virtual Firewall Status Scan
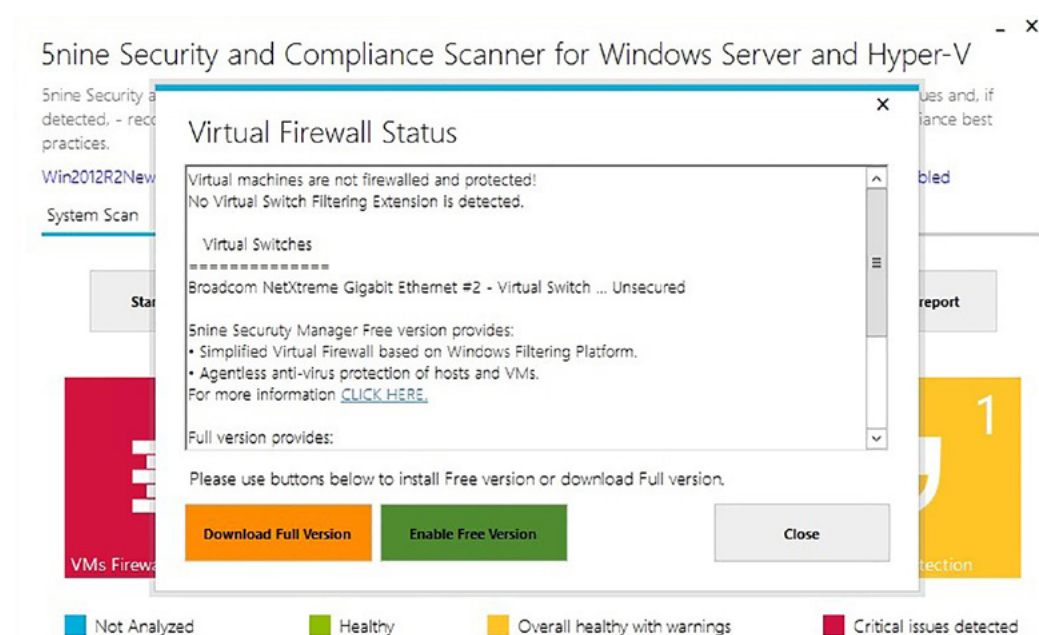
Alternatively, if you already have free 5nine Cloud Security installed and you have selected VMs for firewalling, you will still be prompted to try the full edition (shown in Figure 5). The full version of 5nine Cloud Security provides real-time / on-access AV protection and stateful packet inspection (SPI) across the virtual network.

Figure 5. Virtual Firewall Status Scan with Free Version Installed
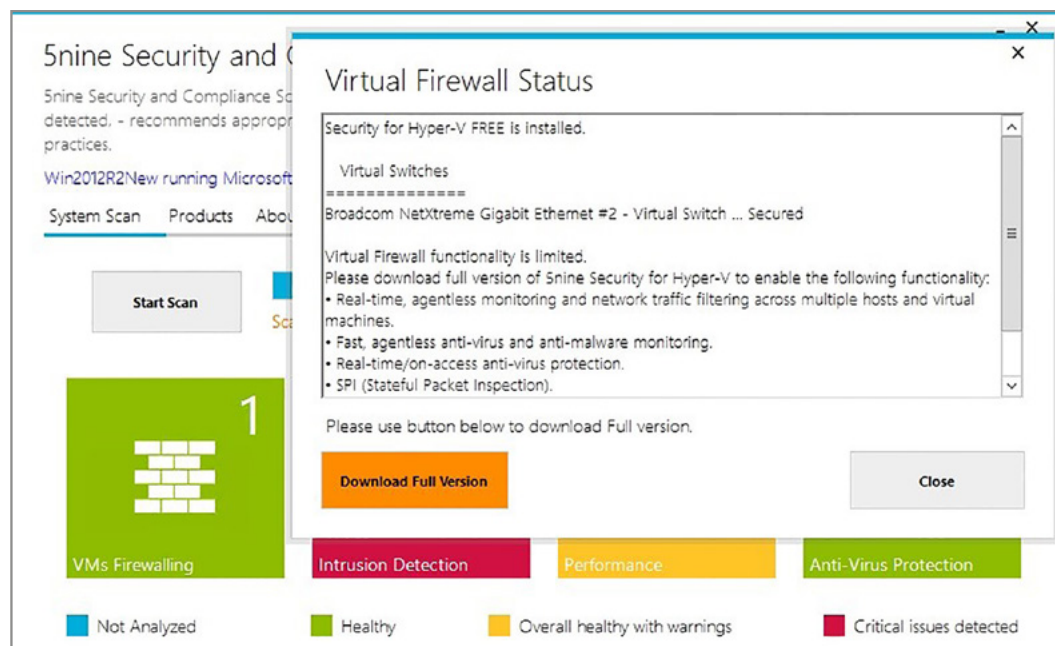
Next, the intrusion detection scan tells us that, on this machine, intrusion detection is not enabled and provides us a link to download it.

Figure 6. Intrusion Detection Scan Status
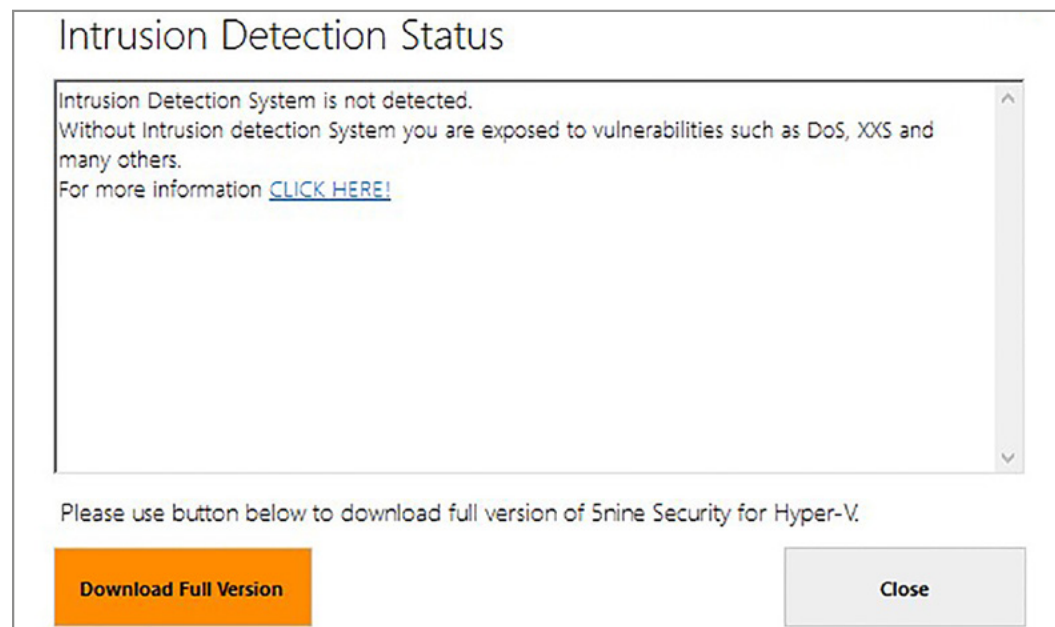
From there, 5nine scanner checks system resource utilization and virtual machine status, ensuring that there are enough memory, CPU, and disk available to ensure reliable and secure system performance (shown in Figure 7, below).

You should know that intrusion detection, real-time anti-virus / on-access protection, and full-featured kernel mode virtual firewall are available only in the full version of 5nine Cloud Security.
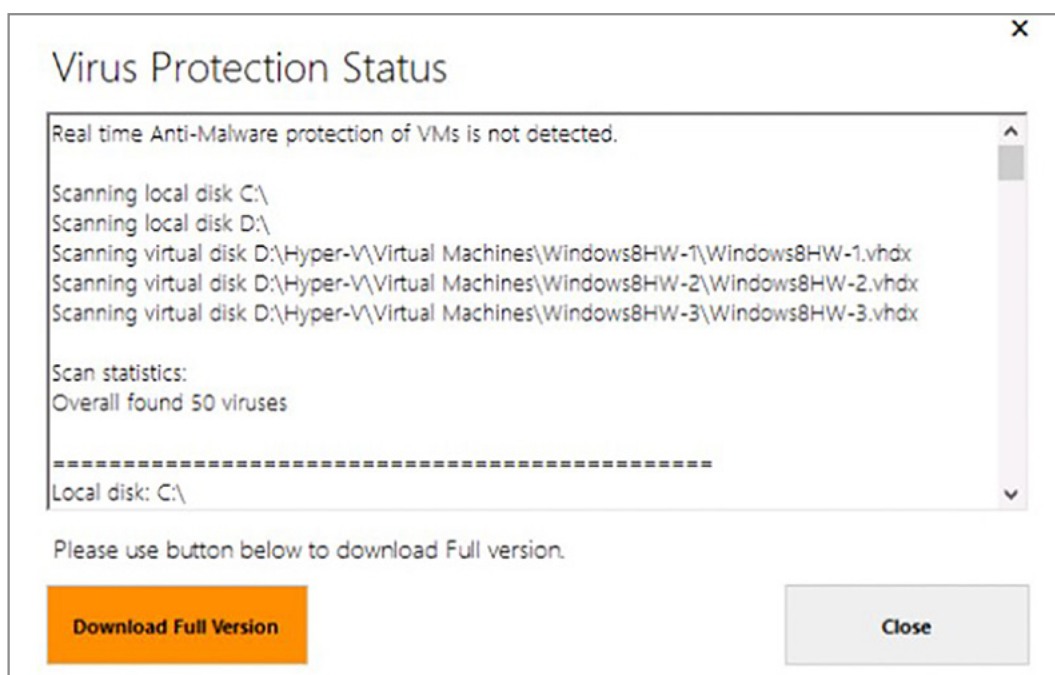

Figure 7. 5nine Security Scanner Checking System Performance
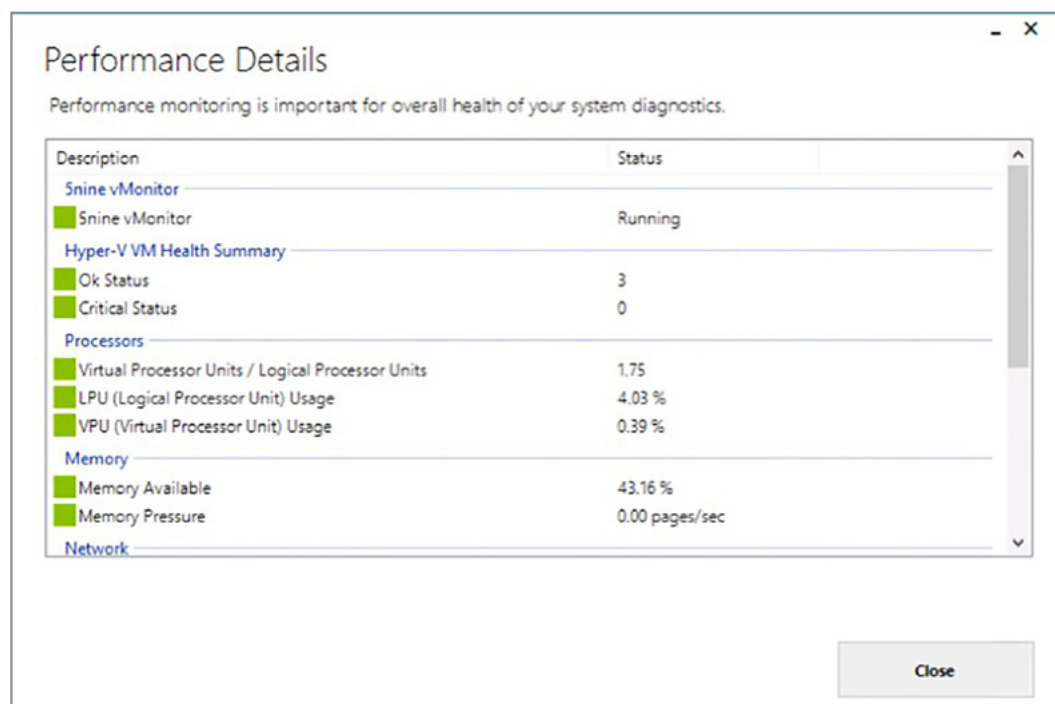
Finally, 5nine Security Scanner scans the local disk and any VHDXs on a Hyper-V enabled host for viruses and malware.

In the example below, you can see that 5nine security scanner found **50 viruses!**

Figure 8. 5nine Security Scanner Checking for Viruses and Malware

If you are missing any of the components that make up the comprehensive security protection solution that I described, 5nine Security Scanner will recommend either a free or commercial solution that can protect you.

Who Needs the Free 5nine Security Scanner?

There are many solutions that have very specific use cases and can help only certain companies or IT Pros. What is so great about 5nine Security Scanner is that, as it's free, and it works on any Windows 8.x or Windows 2012 /R2 server – 5nine Security Scanner is for just about everyone – small businesses (SMB), medium enterprises (SME), large enterprises, and even managed service providers (MSP)!
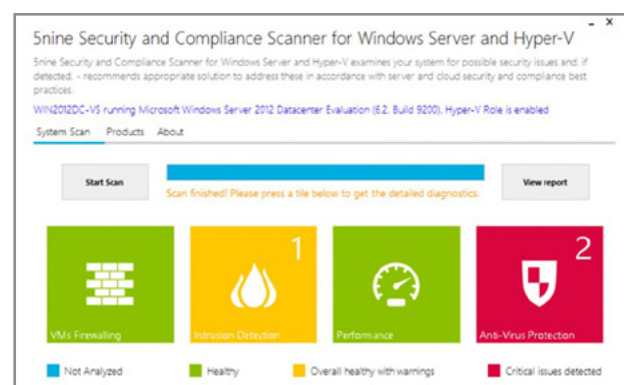
5nine Security Scanner helps:

1. Large enterprises and hosting companies by testing to see what is installed, what's infected, and what is secure across their large environments – using Hyper-V or not. With that information, they will easily see how 5nine's large-scale virtualization security tools can help them.

2. Small and Medium Businesses who need completely free agentless anti-virus and anti-malware for their Windows 2012 servers or for their personal Windows 8 desktops (using Hyper-V or not)

Recommended Action

With 5nine Security Scanner now being a complete free tool available to ensure that your Windows 2012 and Windows 8 hosts and virtual machines are secure, there isn't a good reason NOT to use it.

According to Microsoft, a virus, malware or a network attack has hit more than 40% of US users in the last year.

Don't be one of them! Ensure that you, and your datacenter, are protected!

Download the Free 5nine Security and Compliance Scanner, today!

About the Author

David Davis is a video training author at Pluralsight. com, the global leader in video training for IT pros.

He holds several certifications including VCP5, VCAP-DCA, CCIE #9369, and has been awarded the VMware vExpert award 5 years running.

Additionally, David has spoken at major conferences like VMworld and authored hundreds of articles for websites and print publications, mostly around virtualization.

David's personal blog is www.VirtualizationSoftware.com

Get more White Papers from 5nine Software ➔