Two Great Ways to Protect Your Virtual Machines From Malware

By Maxim Weinstein, CISSP, Senior Product Marketing Manager

Virtualization promises to reduce operational costs, simplify management and increase availability of servers and virtual desktops. But how do you protect virtual machines from malware without compromising the performance and convenience that you expect from your investment in virtualization?

This paper aims to help IT professionals, including security and virtualization specialists, understand and choose between two modern approaches to securing virtual environments: agentless scanning using vShield Endpoint and client-based scanning optimized for virtual platforms.
Two Great Ways to Protect Your Virtual Machines From Malware

Introduction

Over the past several years, organizations’ technology needs have become increasingly complex. IT departments are now expected to support a mobile workforce, a variety of portable devices, interactive websites, a portfolio of critical business applications, and a set of traditional network services and infrastructure. While IT spending has grown in many organizations, it rarely keeps pace with the demand for services. This leads IT professionals to turn to virtualization as an efficient means of scaling their capabilities.

In the server room or data center, virtualization offers benefits such as simpler management, reduced hardware costs and lower operational expenses. Virtual desktop infrastructure (VDI) extends these benefits to the increasingly mobile workforce, while affording the IT department a layer of control and monitoring not commonly available with traditional endpoint devices.

Security is often cited as an advantage of virtualization as well. In practice, virtualization can be both a security opportunity and a challenge. Yes, virtual platforms provide new security capabilities, like sandboxing, data centralization, and easy duplication of hardened configurations. On the other hand, the ease of deployment and cloning can lead to virtual machine (VM) “sprawl” and the associated difficulty in ensuring that every VM is properly protected. Furthermore, an emphasis on performance and consolidation ratios—the number of VMs hosted per physical server—can lead some IT professionals to sacrifice security to conserve resources.

As the market leader in server virtualization, VMware brings a lot of innovation to how organizations deploy and manage virtual systems. This innovation includes a new approach to protecting VMs from malware: agentless antivirus (AV) based on VMware’s vShield Endpoint technology. VShield Endpoint, included as part of most editions of VMware’s vSphere product, combines the important security benefits of antivirus protection with the high performance and consolidation ratios that organizations demand from their virtual deployments.

In addition to delivering vShield-based AV solutions, some security vendors have invested in optimizing their endpoint clients for VMware and other virtual environments. This leaves IT professionals with many choices for protecting their VMs, and questions about how best to balance security and performance.

This paper examines the challenges with running traditional antivirus products on VMs, examines the advantages and limitations of agentless AV and optimized clients, provides guidance for deciding between the two, and describes Sophos solutions for both approaches.
Challenges with antivirus in a virtual environment

Since the early days of the AV industry, malware protection has followed a familiar model. An antivirus client is installed on each workstation or server to be protected. That client runs in memory, scanning for threats and periodically updating its definitions and engine. In corporate environments, a management console provides centralized deployment, administration, updating and reporting for the clients installed on each system.

This model for threat protection emerged at a time when the systems being protected were all separate pieces of hardware. When systems are consolidated onto virtual platforms, traditional antivirus products can get in the way of optimal performance and scalability. The ease of creating, suspending, deleting and moving virtual machines also leads to challenges with managing protection. Let’s look more closely at both of these issues.

Performance and scalability

Overhead and impact on density
One challenge with traditional AV software is the resource overhead associated with running the client software on each VM. Some AV clients use as much as 500MB of RAM per system. Increasing each virtual machine’s RAM footprint to accommodate that extra load would require an extra 10GB of RAM for a host with 20 guest VMs. For hosts that are bound by the available RAM, the added overhead of traditional security software may prevent the achievement of an optimal VM consolidation ratio.

Scan storms
Scan storms occur when a host’s resources are overwhelmed by many VMs running AV scans at the same time. Because each VM is engaged in nearly identical behavior requiring multiple input/output (I/O) operations and substantial CPU processing, data throughput and system response time can slow noticeably. Even an otherwise speedy SAN or local storage array can be affected by the sheer volume of simultaneous read requests.

Simultaneous scheduled or on-demand scans can lead to a “scan storm,” increasing resource use and decreasing system performance.
There may be times when a scan storm is an acceptable side effect of a high priority activity. In the wake of a malware outbreak, for example, you might run an on-demand scan to find and remove the malware from infected systems. In this case, the performance penalty may be less of a concern than completing the scan as quickly as possible.

In most instances, however, maintaining the best performance and highest availability of your virtual machines is paramount. Scan storms, then, can contribute to a failure to meet service level agreements or otherwise deliver performance in accordance with users’ or management’s expectations.

**Update storms**

Like scan storms, update storms can result in overuse of resources due to simultaneous activity across VMs. In this instance, the culprit is updates to security software’s data (e.g., definition files) and/or the security software itself (e.g., product or engine updates). Because the client running on each VM has to download and install the updates, I/O and network bandwidth are typically the resources hit hardest. Traditional security software typically schedules updates at a specific time of day or at a fixed frequency, increasing the likelihood of concurrent updates.

VDI is especially susceptible to update storms. AV products are often configured to check for updates upon system startup. Furthermore, the master or “gold” image may have been created days, weeks, or months previously, which means the client will require substantial updates to become current. If most users start their workdays around the same time in the morning, it can result in dozens, hundreds, or even thousands of virtual desktops all checking for, downloading, and installing updates simultaneously. The same impact can be seen when an entire virtual server pool is started.

**Managing protection in a dynamic environment**

Ensuring that all systems have security software installed and populated with the latest updates is a challenge in any organization, but the challenge is magnified in virtual environments. It takes very little effort to deploy a new VM, particularly one duplicated from an existing system or gold image. That image, however, may have outdated or nonexistent protection, leading to a protection gap from the time of deployment until the security client has been installed and/or updated. Similarly, a VM—or an entire pool of VMs—that is resumed from a suspended state will have protection that was current as of the time it was suspended and will be unprotected against the latest threats until it updates.

Once again, VDI environments are especially prone to this issue because of the tendency to start new sessions—and frequently new instances—at every login or at the start of each day. Coupled with the delays caused by an update storm, this can leave users of virtual desktops susceptible to new threats for a substantial window of time first thing in the morning, just as they are exposing themselves to malware by opening emails and browsing the web.
Finally, the constant starting, stopping, creating and deleting of virtual machines can make it difficult to clearly identify which machines are protected and with which version of the client software. This can waste IT staff time, make compliance checks difficult, and increase the risk of a machine being inadvertently left unprotected.

Two approaches to addressing the challenges

There are two fundamental approaches to addressing the issues described above. One involves agentless AV scanning, which removes the security client from the VM in favor of a centralized scanner on the host. The second optimizes the traditional managed antivirus client for virtual environments.

Both approaches help mitigate the performance, scalability and management challenges; the main difference is where the scanning takes place—centralized on the host or distributed on each VM. These differences have implications for how the systems are managed and how they perform. There are, of course, also differences in how the two approaches are implemented by different vendors. These differences can affect the performance, manageability and level of protection afforded by each vendor’s solutions.

Agentless scanning

Agentless scanning was popularized by VMware via its vShield Endpoint technology. This technology, included in most recent editions of vSphere, provides a lightweight driver—known as a “thin agent”—to install on each VM. The driver communicates through vSphere with a secure virtual machine (SVM) provided by the security vendor and installed on the host. All of the AV scanning takes place in the SVM, leaving the protected VMs free to allocate their resources to other tasks.

Agentless scanning offers several advantages over a traditional endpoint AV solution:

- No security client to install on each VM, saving time and reducing the risk that someone will fail to deploy protection.
- Lighter use of host resources, as there is no duplication of the client software on each VM.
Two Great Ways to Protect Your Virtual Machines From Malware

- Updates only have to occur at the SVM, not at each client. This eliminates update storms and protection gaps.

- Coordinated scanning on the SVM avoids excessive use of system resources by limiting the number of files and VMs that are scanned concurrently.

- Caching reduces scan times and avoids unnecessary resource use and file access delays. VShield routinely makes use of caching at the VM, and Sophos’s implementation additionally caches files centrally within the SVM.

These substantial benefits do come with some limitations. For example, because the vShield Endpoint driver is available only for Windows, there is no support for agentless scanning of other platforms. Similarly, vShield Endpoint is a proprietary VMware technology, so other hypervisors are not supported.

Another limitation is an inherent result of the agentless architecture: vShield Endpoint only supports the scanning of files. Without an agent, there is no way to detect malware running in RAM or to take advantage of advanced security features like HIPS or web filtering.

The lack of a local client also limits the ability to clean up a detected infection; in case of an infection, you may be required to use a dedicated cleanup tool, manually remove the malware and revert to a clean snapshot. User notification, too, is limited by the lack of a local client: if a user tries to open a malicious file, s/he will simply see a Windows error message indicating that the file is not accessible. Also, it is not possible to configure policies per VM, but only per host. This could be an issue in environments with a broad diversity of virtual systems running on a single host, or where VMs cannot be restricted to a specific host.

Finally, the use of a central scanner can potentially create a performance bottleneck, if many VMs are requesting on-access scans of files simultaneously. Caching minimizes the risk of this issue in most real-world scenarios, but it could be a concern in certain environments.
Optimized client

Because agentless scanning is not viable or ideal for every situation, security vendors have also responded by optimizing their antivirus clients for virtualized environments. Optimizations available in Sophos products, for example, include:

• The ability to stagger scans and/or updates to avoid scan and update storms.

• Enabling memory sharing on VMware's ESXi hypervisor so total RAM usage on the host is minimized when identical clients are running across multiple VMs.

• Allowing the client to be built into the gold image without creating duplicate or conflicting entries in the management console as clones are deployed. (This can also reduce boot up storms resulting from clients being deployed automatically by the management server to each new VM.)

• Keeping definition files and updates small to minimize the time and resources required to update multiple VMs.

These optimizations can be supplemented by thoughtful policy configuration. For example, you may wish to group VMs separately from physical devices to allow for different scan, exclusion and cleanup settings. One application of this, for example, would be to disable automatic cleanup of detected malware on virtual desktops, which can easily be discarded and replaced with clean images.

Installing a virtualization-optimized client on each VM avoids most of the issues described earlier while providing many of the benefits of traditional security software:

• Additional layers of protection, including web scanning, HIPS and application control.

• Support for a broader range of operating systems and hypervisors.

• Ability to set policies per VM rather than per host, and for the policy to follow the VM if it moves to a new host.

There are some limitations to this approach as well. Even with memory sharing, use of hardware resources is likely to be higher (compared to agentless scanning) on hosts with large numbers of VMs. In highly dynamic environments, where virtual machines are routinely created and discarded, update and deployment lag are likely to remain issues. In addition, keeping track of all the VMs in the management console—including removing ghost entries for VMs that no longer exist—can be time-consuming in these situations.
Agentless or optimized client: How to choose

Every virtual environment is different. For some, the simplicity and speed of vShield-powered agentless scanning will be ideal. For others, the flexibility and additional protection that come with installing clients on each VM will be critical. There may even be organizations that benefit from using agentless protection on some VMs and optimized clients on others.

The following table summarizes the strengths and limitations of each approach and is offered as a guide to help you decide which is best suited to your environment. Note that the exact capabilities will vary from one vendor to another.

**Agentless or optimized client? Factors to consider**

<table>
<thead>
<tr>
<th></th>
<th>Agentless</th>
<th>Optimized client</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Performance</strong></td>
<td>• Scales well for large VMware deployments</td>
<td>• For small number of VMs, may use fewer resources than agentless</td>
</tr>
<tr>
<td></td>
<td>• Marginal performance cost per VM is minimal</td>
<td>• Marginal performance cost per VM is moderate</td>
</tr>
<tr>
<td></td>
<td>• Performance is optimized out of the box</td>
<td>• Requires extensive configuration for optimal performance</td>
</tr>
<tr>
<td><strong>Compatibility</strong></td>
<td>• Windows VMs only</td>
<td>• VMs can be any OS with an available client</td>
</tr>
<tr>
<td></td>
<td>• vSphere only</td>
<td>• Works with most hypervisors</td>
</tr>
<tr>
<td><strong>Management</strong></td>
<td>• Initial setup is more complex</td>
<td>• Builds on traditional AV infrastructure</td>
</tr>
<tr>
<td></td>
<td>• Managed per host, not per VM</td>
<td>• Requires greater attention in large deployments</td>
</tr>
<tr>
<td></td>
<td>• Some products require a separate console (Sophos’s does not)</td>
<td></td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>• File-level antivirus/anti-malware scanning</td>
<td>• File-level antivirus/anti-malware scanning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Automated malware cleanup/removal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HIPS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Web filtering</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Application control</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Other features</td>
</tr>
<tr>
<td><strong>End user experience</strong></td>
<td>• No AV-specific notifications; users only see OS “access denied” messages</td>
<td>• Local client provides notifications</td>
</tr>
<tr>
<td></td>
<td>• No local configuration, cleanup, or other tools</td>
<td>• Users may have options and tools, as configured by IT</td>
</tr>
</tbody>
</table>

As may be evident from the table above, small deployments with just a few VMs on a single host may find that it is easier to manage each VM with an installed client. In contrast, large, dynamic environments are likely to see immediate performance and management benefits from moving to an agentless configuration. In situations where agentless scanning seems ideal for most VMs, but certain machines require a higher level of protection or are running non-Windows platforms, a hybrid approach may be warranted.
Two Great Ways to Protect Your Virtual Machines From Malware

Sophos makes it simple

Sophos offers both agentless AV and client-based protection optimized for virtual environments. With centralized management through our intuitive Sophos Enterprise Console, Sophos makes it simple to protect every virtual machine in your organization. Our partnership with VMware, Citrix and Microsoft means that our products have been tested to work seamlessly with the most popular hypervisors.

Agentless scanning for virtual servers and desktops

**Sophos Antivirus (SAV) for vShield** is our high performance agentless solution for virtual servers and desktops. Designed to take full advantage of vShield Endpoint, SAV for vShield’s advanced caching keeps scan times and resource use to a minimum. The centralized scanner uses our sophisticated threat detection engine coupled with Live Protection, a real-time connection to the correlated threat intelligence provided by SophosLabs. This means every VM is defended against both known malware and previously unseen threats.

Unlike some agentless products that require dedicated consoles, Sophos Antivirus for vShield is managed through Sophos Enterprise Console. Protected hosts can be configured alongside managed workstations and servers running our security client.

Server protection for Windows, Linux, Mac and UNIX

**Sophos Server Protection** gives you the flexibility to deploy whatever combination of agentless and client-based protection meets your server room needs. Minimize threats to your critical data with agentless SAV for vShield or our high performance Sophos Antivirus for Windows, Linux, UNIX or Mac. Manage all of them through a single interface with Sophos Enterprise Console.

Endpoint protection for virtual desktops

**Endpoint protection** solutions from Sophos provide complete, layered security for your virtual desktops. A single, efficient client incorporates antivirus, firewall, HIPS, data loss prevention, web protection and more. Our Virtualization Scan Controller allows you to stagger scan times to avoid scan storms, and the client can be incorporated into your gold image for no-fuss deployment. The Sophos Enterprise Console makes it simple to manage protection for all your virtual desktops, traditional workstations and servers.
Two Great Ways to Protect Your Virtual Machines From Malware

Conclusion

In a fairly short time, virtualization has become an everyday IT tool, thanks to the efficiency and ease of management it brings to the server room. Preserving these benefits while securing VMs against malware, however, has its challenges. Fortunately, thanks to new technology and product enhancements, these challenges can be overcome. Indeed, with agentless scanning, we even see virtualization technology being used to deliver AV protection in a new and more efficient way.

With a range of complete security solutions that incorporate Sophos Antivirus for vShield, our optimized endpoint client and our simple-to-manage Sophos Enterprise Console, Sophos offers security made simple for your virtual environment and your entire organization.