gamechanger Game Changing Technology for VM Security

Why You Need A New Solution To Protect Your Virtualized Environments

By Brien M. Posey

Virtualization presents challenges legacy anti-malware was never designed to address.

Using anti-malware software to protect servers and network endpoints has been a common practice for decades but legacy malware prevention strategies are not well suited to virtualized environments. This is because virtualization presents significant challenges legacy antimalware solutions were simply never designed to address. These challenges include the nature of virtualization, as well as today's increasingly varied and sophisticated malware threats.

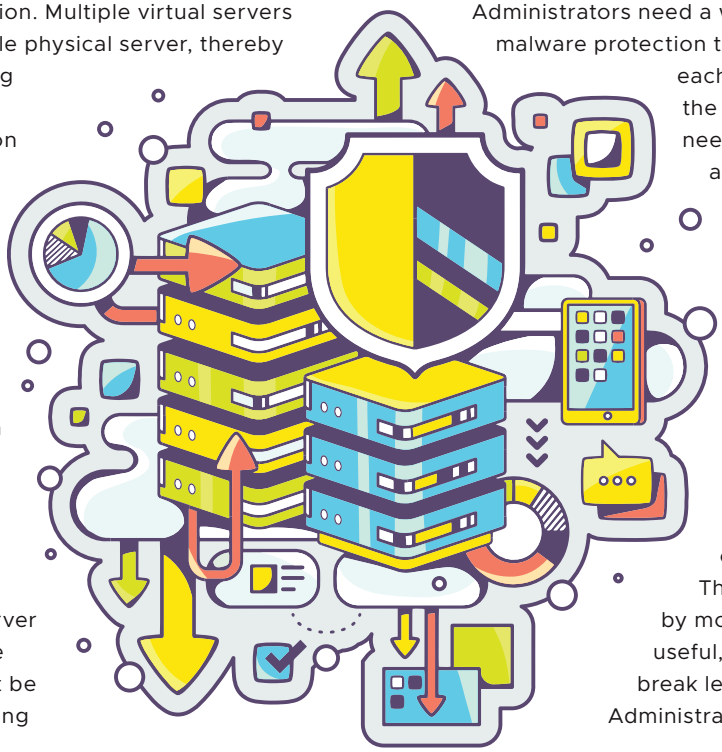
HYPERVISOR RELATED ISSUES

The most common problem with malware scanning in virtualized environments is that the scanning process can consume excessive system resources. Virtualization became popular in the first place because of workload consolidation. Multiple virtual servers can be run on a single physical server, thereby dramatically reducing hardware costs. Because virtualization has such a large impact on cost, organizations strive to achieve the highest possible consolidation ratio without impacting performance. Herein lies the problem.

When used in a virtualized environment, legacy anti-malware solutions rob the server of physical hardware resources that might be better used for hosting additional virtual machines (VMs) or providing added reliability. Typically, each VM has its own copy of the anti-malware software, which increases storage costs unless deduplication is being used. More importantly, simultaneous anti-malware scans can produce CPU and storage I/O storms, which may severely degrade performance until the storm has passed.

Another challenge posed by virtualization is scalability. Although server virtualization was originally intended to be a solution for datacenter consolidation, virtual machines can be so easily created, that VM sprawl has become a significant issue.

Just as it can be difficult to manage large numbers of virtual machines, it can also be difficult to manage the anti-malware software that is running on those VMs. Administrators need a way to centrally manage their malware protection to verify it is up to date, and each VM is protected. Furthermore, the management interface needs to be able to scale to accommodate an ever growing collection of VMs.



Of course, virtualized environments provide benefits far beyond simple workload consolidation. The virtualization infrastructure allows administrators to do things that are impossible in a physical server environment, such as moving a workload from one host to another while the workload continues to run.

The enhanced capabilities offered by modern hypervisors, while useful, can in some circumstances break legacy anti-malware software. Administrators must consider for example,

Wowomnom / Shutterstock.com

what happens if a VM is moved to a different host while a malware scan is taking place. In theory, the malware scan should not be disrupted by the migration, but there have been instances where problems have occurred.

Similarly, major hypervisor vendors such as VMware and Microsoft provide a built-in snapshot feature, which allows a virtual machine to be rolled back to an earlier point in time. While snapshots are convenient, they can be problematic with regard to malware prevention. In fact, virtualization vendors advise against using snapshots as a recovery mechanism because snapshots are not backups. Rolling back a virtual machine to an earlier state can potentially revert the VM's malware signature database to an earlier version, thereby leaving the VM unprotected against newly discovered threats.

Additionally, backups are not a good way of securing the infrastructure. It's always better to prevent an incident rather than to recover from it. Trying to recover from the backup also raises a number of issues, including lost data, time to recover, and inability to address the root cause.

The problem of outdated malware definition files is not related solely to the application of checkpoints. Definitions can also become outdated while a VM is powered off.

Legacy anti-malware tools typically do not protect virtual machines when powered off. Anti-malware vendors commonly recommend excluding virtual hard disk files and other virtual machine components from host level anti-malware scans. Hence, a virtual machine that has been powered down is essentially left unprotected.

The variety of ways in which malware infections can occur have rendered traditional disk scanning techniques ineffective by themselves.

When that VM is eventually powered on, its malware definition files may be outdated, depending on how long it was powered off. This leaves the VM vulnerable to threats that may have been discovered since the VM's definitions were updated.

On the surface, allowing a VM to be powered on even though it contains an outdated malware definition file might seem a non-issue. After all, the malware scanning engine should perform a definition update soon after the VM is booted. The problem is a VM can become infected, even when it is powered off. There are a number of different methods that can be used to gain access to a virtual hard disk's file system while the corresponding VM is powered down. It is possible for a VM to become infected as a result of an administrative action or a direct malware injection into the virtual hard disk file, even if the VM is not running.

Backups are not a good way of securing the infrastructure. It's always better to prevent an incident rather than to recover from it.

THE MALWARE EVOLUTION

Long ago, malware was spread by sharing floppy disks. Although floppy disks are extinct, malware continues to be a threat because it evolves as technology progresses. Today, malware is commonly spread through malicious websites or e-mail messages containing malware links or attachments.

The variety of ways in which malware infections can occur have rendered traditional disk scanning techniques ineffective by themselves. Although media scans are important, they can no longer be the basis of an organization's entire malware prevention strategy.

The biggest problem with relying solely on storage level scans is that regardless of how good a scanning engine might be, there is always a possibility a threat might not be recognized. The only way to prevent undetected threats from infecting a VM is to block undesirable actions from ever occurring.

One such technique that can be used to prevent malware infections is application whitelisting with Default Deny mode. Random code is never allowed to execute on a VM. The VM should only be allowed to run operating system files, and designated applications.

Default Deny allows authorized code to run unimpeded, while any code that has not been explicitly authorized is prohibited from running. Blocking all unauthorized code from executing prevents malware from being able to run, even if the scanning engine fails to detect the infection.

Kaspersky Lab Protects Virtual Server And Virtual Desktop Environments

Understanding the key to achieving comprehensive protection

As a well-established player in the anti-malware industry, Kaspersky Lab understands that the key to achieving comprehensive protection against malware is to practice defense in depth. In keeping with this philosophy, Kaspersky Lab has created a product called Kaspersky Security for Virtualization (KSV). As its name implies, Kaspersky Security for Virtualization is specifically designed to protect virtual servers and virtual desktop environments. The software is engineered to work with virtualization platforms from VMWare, Microsoft, Citrix, and KVM.

While KSV is at its core, an anti-malware product, it also utilizes security tools not traditionally associated with malware prevention. Some of these mechanisms include application whitelisting (which Kaspersky Lab refers to as application startup and privilege control), URL shielding, and even an Intrusion Prevention System.

What may be even more impressive is the way Kaspersky Lab engineered its security solution to address the unique requirements of a virtualized environment.

What may be even more impressive is the way Kaspersky Lab engineered its security solution to address the unique requirements of a virtualized environment. Rather than consuming excessive hardware resources, and complicating anti-malware management by placing a separate copy of the scanning engine and definition files on each VM, Kaspersky Lab takes a tiered approach to VM protection.

In VMware environments for example, Kaspersky Lab uses a Security Virtual Machine (SVM) that integrates into the NSX environment, without the need for an agent. The SVM contains the malware scanning engine, and the malware definition database. Its job is to scan VMs for malware in an automated and non-disruptive way. Because there is a limit to the number of VMs that an SVM can protect, organizations can deploy redundant SVMs, which provide load balancing and fault tolerance. Kaspersky Lab also offers another NSX integrated component called Network Attack Blocker to guard virtual machines (even those on software defined networks) against a variety of network based exploits. It's also worth noting that KSV can scan machines while they are offline or powered off. This allows for scanning off-hours and is very efficient.

Kaspersky Lab's approach provides centralized protection for VMs. The absence of a VM level scanning engine means that problems related to scan storms are avoided, as are the headaches associated with trying to make sure that every VM's scanning engine is kept up to date.

This approach also helps to avoid the risks associated with booting VMs that may have outdated malware definitions. Because the malware signature database is centrally located, VMs can be protected from the moment they are powered on.

The second tier of Kaspersky Lab's approach to VM protection is a lightweight agent that can optionally be installed into VMs. The light agent provides memory and process protection, as well as application, device, and Web controls. KSV technologies guard against crypto-malware and other types of ransomware, and the agent also uses a firewall and a Host Intrusion Prevention System to guard against other exploits.

These features collectively provide solid protection against malware, but they also go a long way toward improving the overall security of an organization's virtual machines. Furthermore, Kaspersky Lab easily monitors the entire security infrastructure in real time through a centralized and scalable management console, which provides a single pane of glass for security professionals.

For more information, visit usa.kaspersky.com

KASPERSKY lab