Solution Brief:

What You Don't Know, Can Hurt You:

Controlling VM Sprawl and Managing the Transition from Physical to Virtual Machines

Shavlik

Solution Brief:

What You Don't Know, Can Hurt You

Abstract

The adoption rate of Virtual Machines has exploded at most organizations, driven by the improved cost effectiveness of increased server utilization. The savings in rack space, hardware costs, power consumption, and many other factors are driving this steadily increasing trend. However, this boom in logical servers has resulted in a substantial increase in the number of devices connected to the network, and each needs to be individually configured, patched, and secured. Fortunately, Shavlik Technologies provides a single tool set, single process for physical and virtual machines that simplifies and automates critical IT operations.

The Reality of Virtualization

In the past few years, medium-to large-sized organizations have implemented at least some level of virtualization. This trend, which leverages a single physical resource such as a server to function as multiple logical servers, is growing at an explosive rate. Research firm IDC estimates that between 2006 and 2009, virtualization grew at a compound annual growth rate of almost 50 percent. Virtualization is quickly becoming a reality at most organizations.

This rapid growth in virtualization is driven by a number of factors. These include better utilization of idle or available processing power within servers, reduced rack space and power consumption, less hardware acquisition and maintenance costs, easier backup, improved high availability and disaster recovery, and centralized software management.

Virtual Machines -Real Exposure

While there are many benefits to virtualization, organizations must take care to apply appropriate security safeguards. Virtualization can actually increase the need for security, and system and security administrators need to plan for and implement defenses accordingly. Because each virtual machine has its own network address and can be scanned, hacked, infected, and compromised just like a dedicated physical device, applying security to each individual virtual machine is as critical as securing dedicated physical devices.

According to a The Info Pro's Wave 6 server study, manageability of virtual machines is the number one concern of IT professionals at Fortune 1000

companies and mid-market enterprises alike.

Although virtualization may cause the number of physical devices in an organization to be reduced, the number of logical machines usually increases. It's not uncommon to experience an enormous increase in the number of logical servers. Because virtualization allows new servers to be added without the costs of deploying new hardware, there is a strong tendency to increase the number of logical servers. Rapid adoption of virtualization technology often out paces the ability of IT operations and IT security to react to manage these virtual machines over their lifecycle.

With the increased number of servers to safeguard, security and IT administrators need to aggressively and continuously monitor for new devices, servers, and services. Prior to virtualization, when adding a new device meant deploying new hardware, the addition of new servers and applications was naturally throttled due to budget, hardware acquisition, rack space, and other time consuming activities. These physical constraints created a natural process for IT operations and security teams to be notified when new servers were being added. Virtualization eliminates much of this process and structure, and as a result new servers and applications can appear significantly faster and easier, often times without the coordination of the security team. New virtual servers can appear without authorization at all. Security administrators must be equipped with tools to proactively discover new virtual devices as soon as they appear.

With the additional number of virtual devices, security administrators must have robust and comprehensive ways of tracking and managing the security configuration and patch status of each and every virtual system. Each one needs individual attention. For example, an unpatched virtual machine can still be exploited, even if the host system is patched and not vulnerable. A common mistake is for IT or security administrators to assume that a well-protected host insulates the virtual systems running behind it. That is not the case. A UNIX based host, or any host for that is up to date with all security patches, perfectly configured and hardened will not protect a virtual Microsoft IIS server running underneath. Likewise, virtual machines and appliances potentially carry embedded vulnerabilities and require special consideration for patching and updates. To establish an effective security baseline, each and every virtual machine needs individual attention and management.

Solution Brief:

What You Don't Know, Can Hurt You

Shavlik- Detection, Protection, and Management of Your Virtual Machines

Containing the spread of virtual machines, aka VM sprawl, is a challenge for IT security and operations. Shavlik Technologies' innovative agentless approach thoroughly and dynamically discovers and catalogs the physical and virtual assets IT must manage. Organizations will discover physical and virtual machines they didn't know they had and uncover software applications they didn't know were installed. By eliminating these blind spots, enterprises can quickly close the gaps in their security and policy compliance.

One of the myths surrounding virtual machines is that the low-level infrastructure and interfaces that connect them to the network and management systems are subtly different, and prevent many systems and applications from working with them. For example, it's commonly (but wrongly) thought that patch management systems will not effectively work with virtual machines. Fortunately this is not the case.

While it's true that the system hosting the virtual machine acts as a proxy, it's not true that this causes problems for patch management. Today's virtual machine host implementations are so well done that the proxies are capable of handling even low level system oriented tasks such as system shut-downs, re-starts, reconfigures, and system updates. Patch management, as implemented by Shavlik Technologies, works equally well with virtual machines and their physical counterparts.

Virtual machines have the same visibility to Shavlik's patch and vulnerability management products as do dedicated machines. Existing and new virtual devices are dynamically discovered through a tight integration with virtual infrastructure layer. Likewise, security baselines are determined and established in the same manner.

When it comes time to apply security updates to virtual machines, administrators treat them just like dedicated physical devices. Virtual machines require the same patches as dedicated devices, and the patches are tested, received, applied, rolled back if necessary, and managed in the same way.

Shavlik

Additional Dividends from Shavlik

Not only are Shavlik products compatible with virtual machines, organizations using them will find additional benefits that are not available in other patch and vulnerability management solutions.

Asset Management - Eliminate Your Virtual Blind Spots

Shavlik's asset management delivers a dynamic, up-to-date method for IT to track software, hardware, and virtual assets. Shavlik eliminates static views and cumbersome spreadsheets by leveraging its innovative agentless approach to thoroughly and dynamically discover and catalog the assets IT must manage. Organizations will discover physical and virtual machines they didn't know they had and uncover software applications they didn't know were installed. By eliminating these blind spots, IT security and operations can quickly close the gaps in security and policy compliance. By consolidating software, hardware, and virtual machine asset information in one location, enterprises have all relevant information about their assets at their fingertips, enabling them to make informed decisions with confidence and accuracy.

Shavlik's virtual machine asset management makes it easier for IT operations to have immediate visibility into the resources virtual machines are consuming from their hypervisor host. The information collected about virtual machine assets identifies how much memory or CPU are assigned to virtual machines and correlates that to the virtual machine host so IT operations has immediate understanding whether they can provision additional virtual machines to a specific host. Other important virtual asset details include hosting server name, Operating System installed, uptime, power state, hard drives (allocated and free space), and Network Cards. Software asset data – software applications installed, version, date installed, etc. – round out the view of how a virtual machine is being utilized and how it needs to be managed and protected.

All of this information, in a single location, gives IT operations powerful tools for decision making regarding the use of their virtual assets over their entire lifecycle.

Agentless Approach – Easiest Way to Patch Virtual Machines

Shavlik patch management does not require agents. This has particular advantages for organizations rolling out virtualization because of the numbers of new virtual devices. Not only can these new devices be protected by Shavlik, patch and vulnerability management can be done easily, from a single console, in a matter of minutes. This is a tremendous advantage over solutions that require agents to be installed on each new virtual machine. Deploying and maintaining hundreds or thousands of agents on virtual machines within large organizations is a time consuming, tedious, and expensive effort. An agentless approach is less expensive to acquire, easier to deploy and maintain, and provides immediate protection. With Shavlik's agentless approach, organizations can rapidly accelerate their level of security because they can begin assessment, remediation and generating useful reports within minutes of a new virtual machine going active. There is little to no impact on the data center or staff. This is critical given the nature of continuous operations in large data centers. All of these benefits of an agentless approach are magnified in a virtual machine environment, not only because of the rapid growth of virtual machines, but because they are more dynamic in nature - coming and going at a much quicker pace than physical, dedicated servers.

Shavlik – Only Vendor Patching Offline Virtual Machines

The unique advantage of using Shavlik solutions to secure virtual machines is the ability to discover, inventory, and patch ALL virtual machines, both online and offline. As mid-to large-sized organizations have discovered, patching offline machines can be a real headache. For various reasons, most enterprises have a significant number of virtual images offline at any given time. Patch management systems can't patch what they can't see, so anything that is being serviced, or offline for any reason does not get patched. While there are various techniques to deal with this and ease the pain, it's still painful. Everyone wants to see a report that says for a particular critical vulnerability, "100% of the organization's applicable machines have been patched." Closure for each patch is greatly desired, and no security officers want to report to upper management that "77% of the vulnerable machines have been patched." Until that report says 100%, a

certain amount of anxiety or even nausea remains as an awful pit in the stomach of those responsible.

Being able to protect a virtual machine begins will discovering the system dynamically, as it is added to the virtual infrastructure. Shavlik has tightly coupled its solution with the virtual infrastructure layer so new virtual machines, regardless of their power state, are identified when Shavlik's solution performs a scan. This interrogation of the virtual infrastructure keeps VM sprawl at bay by ensuring that new virtual machines are detected, protected, and managed as they are provisioned.

Shavlik Technologies has developed a way to patch all virtual machines, even those that are offline. This ensures that offline virtual images can be in a constant state of readiness to be deployed. Shavlik is the only vendor capable of doing this, and it's a huge benefit to their customers. For example, many enterprises intentionally have a significant number of virtual machines offline at given periods. One such usage is to increase overall uptime and high availability. Virtual machines have made it much easier for organizations to have redundant machines for peak processing periods, or to be used during maintenance, or for hot standby machines in case of a server failure. However, it's time consuming and difficult operationally to bring these offline machines online just for patch management. Shavlik customers have the benefit of being able to perform full vulnerability management, including patching, for all of their virtual machines, even those that are offline. IT and security staff can quickly verify and report that 100% of the organization's vulnerable machines – physical, virtual, and offline – have received a specific critical patch and are protected.

Since offline machines can remain offline while they are being patched, another plus for Shavlik customers is improved security. Offline machines don't have to be on the network and thus at risk to the very vulnerability they are being patched for.

Furthermore, this feature allows the window of vulnerability to be significantly reduced. For example, some critical patches should be applied immediately, but require a system reboot. For operational reasons it may be difficult for an organization to shut down a server to apply the patch, so they remain operating with the vulnerability until they can address it. However, with the ability to utilize virtual redundant servers protected by Shavlik, the organization can immediately

patch an offline standby server, and bring it online as the production server. This gives the organization near immediate protection from the vulnerability without having to dispend service. The primary server, can now also be safely patched while offline and not vulnerable to attack.

Summary Conclusions

It's clear that virtualization, although a relatively new trend, is seeing explosive adoption rates. The benefits of virtualization that are driving this strong trend are not limited to just operational savings, but with the right security infrastructure, include a number of security dividends as well.

While it's true that implementing virtualization without proper security actually increases an organization's vulnerabilities, it's also true that when properly safeguarded with Shavlik's agentless solutions and their unique ability to secure offline virtual servers, an organization can experience an improved level of security.

Shavlik's agentless and unique capability of patching offline virtual servers and machines gives organizations several benefits, including:

- *Dynamic discovery of virtual machines as they are added to the virtual infrastructure.*
- *Proactively engaging in a continuous and ongoing process to provide vulnerability and patch management for virtual machines.*
- *Quick and automatic discovery of new virtual machines, even before they come online.*
- *Scanning of existing and new virtual machines for vulnerabilities. Report shortcomings and, if desired, automatically remediate them.*
- *Patch virtual machines while they are offline, and not subject to attack.*
- *Allow organizations to respond immediately to critical vulnerabilities that require rebooting.*

Shavlik's powerful technologies and features for discovering, managing, and securing virtual machines make it possible for organizations to experience all of the above, and many more benefits. Being able to achieve this without deploying agents makes it possible from both a cost and IT resource perspective, to effectively and efficiently respond to the significant increase in the total number

Solution Brief:

What You Don't Know, Can Hurt You

of logical servers and devices caused by the implementation and growth of virtual machines.

The myth that virtual machines can't be adequately patched is just that…a myth. With Shavlik not only can they be efficiently patched and managed, virtual machines can experience greater security and advantages than their physical counterparts.