SECURITY FOR VIRTUALIZATION:

FINDING THE RIGHT BALANCE

Combining protection and performance
in your virtualized environment

kaspersky.com/beready

KASPERSKY lab

Introduction

> "In the end, they're all servers – and someone somewhere is going to want to break into them."
> John Sawyer

According to a Forrester survey, 85% of companies have either implemented server virtualization, or are planning to do so.[1]

A study by leading analyst Gartner supports the rise and rise of virtualization, predicting that approximately 50% of x86 architecture server workloads will be virtualized by the end of 2012.[2] But, while virtualization has grown in popularity, securing virtual environments has lagged behind.

In fact, in another report Gartner claims that '… in 2012, 60% of virtualized servers will be less secure than the physical servers they replace'.[3]

And yet security threats – particularly from malware – are greater than ever before.

As John Sawyer from influential technology site Tech Center points out, "In the end, they're all servers – and someone somewhere is going to want to break into them."[4]

So what reasons lie behind the apparent paradox of 'fast to virtualize, slow to secure'?

- A perception that a virtual machine is more secure than a physical one.
- Performance and protection issues arising from traditional agent-based anti-malware solutions operating in virtual environments.
- Inadequate protection and increased management overhead of agentless anti-malware solutions.

What's clear is that, so far, the options for securing virtual machines from malware have all involved an unhappy compromise of protection, performance, or management.

1 The CISO's Guide to Virtualization Security, Forrester Research, Inc., January 2012
2 & 3 Gartner: Virtualization security will take time, SCMagazine.com, March 2012
4 Tech Insight: Keeping Server Virtualization Secure, John Sawyer on Darkreading.com, May 2009

Reversing the benefits of virtualization with security

1.0

Eliminating ‘server sprawl’ by virtualizing servers and desktops can bring enormous business benefits.

Some key examples include:

- Cost containment: Virtualization reduces the overall hardware footprint, reducing hardware expenditures, floor space, power consumption, management requirements, etc.
- Speed: Virtualization increases the speed of IT by delivering new capacity on demand. This agility can ultimately result in greater competitiveness of the entire business.
- Stability: Simpler, standardized, redundant systems lead to greater resiliency, ensure better system availability, enabling employees to be more productive whenever and wherever they work .
- Centralized management: Virtual systems can be created instantly, and managed and configured centrally reducing administrative and support costs.
- OS migrations: In virtual environments, these are easier and faster, and ultimately require less ongoing maintenance.

Unfortunately, many businesses undercut the inherent benefits of virtualization when they fail to properly implement anti-malware solutions to protect from data loss and cybercrime.

And it’s a fact that some anti-virus implementations can bog down the virtual infrastructure, reducing consolidation ratios and limiting ROI.

So, what can the prudent IT manager do to maintain an efficient yet well-protected virtual environment – while still realizing the oft-touted business benefits?

In this paper we’ll discuss three security approaches, their effect on achieving virtual ROI, and offer some advice on the best way to protect your virtual, as well as physical and mobile environments.

The NO-PROTECTION option

2.0

"For the past 15 months there has been a real focus on corporations with valuable data that can be monetized. Cyber-gangs are targeting businesses."
Roel Schouwenberg, Senior Researcher for Kaspersky Lab

There is a pervasive myth that virtual machines are inherently more secure than physical machines.

The truth is that while virtual machines may be less prone to threats such as spyware and ransomware, they are just as vulnerable to malware in the form of malicious email attachments, drive-by-downloads, botnet Trojans and even targeted 'spear-fishing' attacks.

These threats persist while the virtual system is active and in use.

According to the National Institute of Standards and Technology: "Virtualization adds layers of technology, which can increase the security management burden by necessitating additional security controls. Combining many systems onto a single physical computer can cause a larger impact if a security compromise occurs. Further, virtualization systems, which rely on a shared resource infrastructure, create a dangerous attack vector in which a single compromised virtual machine impacts the entire virtual infrastructure."[5]

Additional risks to the virtual environment exist:

- Infection in one virtual machine has the ability to infect data stores that other virtual machines use, spreading the infection and compromising additional systems and data.
- One virtual machine can be used to 'eavesdrop' on another virtual machine's traffic.
- Malware has historically been created to avoid virtual systems. Now malware creators are writing code that targets both physical and virtual machines.
- Some malware is designed to survive the 'tear-down' of a non-persistent virtual machine allowing it to 'return' when the virtual machine is re-commissioned.

Moreover, cybercriminals have begun to shift their focus from consumers to corporations.

Roel Schouwenberg, Senior Researcher for Kaspersky Lab, comments, "For the past 15 months there has been a real focus on corporations with valuable data that can be monetized. Cyber-gangs are targeting businesses."

Malware threats continue to rise at an alarming rate.
In early 2011, leading anti-virus vendor Kaspersky Lab was tracking 35 million threats in its master database. One year later that database has nearly doubled to over 67 million. Kaspersky now sees an average of 70,000 new threats every day. One in every 14 web downloads now contains malware. Both physical and virtual machines alike are susceptible.

In short, there has never been a more serious need for premium protection, both in the physical and the virtual worlds.

5 Guide to Security for Full Virtualization Technologies, National Institute of Standards & Technology

The AGENT-BASED PROTECTION option

3.0

Many organizations have implemented a traditional, agent-based, anti-virus methodology.

This involves loading a full copy of anti-virus software on each virtual machine. While this approach can provide robust protection, there is typically a steep cost in deploying redundant software across a shared resource.

As the anti-virus software and signature database is loaded on each virtual machine, the underlying redundant resource requirements negatively impacts memory, storage, and CPU availability. This increases hardware utilization and decreases performance. Specific symptoms include:

Resource contention

- Scanning storms – when multiple virtual machines begin scheduled scans simultaneously, processing power of the host machine can be drained resulting in host utilization and performance issues, (even potentially crashing the host).
- I/O storms – similar to a scanning storm, this may occur when all virtual machines with local signature database download updates simultaneously.
- Duplication/redundancy – duplication of signature databases and redundant file scanning unnecessarily consumes valuable system resources.

Instant-on gaps

Virtual machines can be easily taken off line and go dormant for long intervals. When they are brought back online (awakened), the virtual machines may have security gaps, such as unpatched software vulnerabilities and outdated virus signature databases.

VM sprawl and security visibility

Virtual machines can be created in minutes, often without the IT department's knowledge or consent. Visibility then becomes an issue; as security managers cannot protect virtual machines that they cannot see.

Agent-based anti-virus in virtual environments, particularly in virtual desktops, can hamper ROI as it impedes the performance of the guest, limits the density of the virtual cluster and allows for unnecessary risk.

The AGENTLESS PROTECTION option

4.0

With the growth of the virtualization market, anti-malware vendors have begun creating anti-virus software specifically designed to operate in virtual environments.

A virtual appliance provides anti-virus protection to many virtual machines. This improves performance by offloading the anti-virus processing from all the individual virtual machines, dramatically reducing overall memory footprint, extending the physical hardware capabilities and increasing consolidation ratios (density).

This agentless approach, while driving better ROI, can create two problems that should be addressed:

1. Narrower protection:
Modern agent-based anti-virus software may include layered protection modules such as application control, web filtering, host intrusion protection, personal firewall and more.

Agentless anti-virus solutions designed for virtual environments have a narrower scope, providing traditional anti-virus protection only.

If these robust tools are absent, the remaining anti-virus detection engine should be the best available in order to compensate for shortcomings that may have otherwise relied on additional protection layers.

If the agentless solution has poor detection rates (as qualified by a third-party testing organization) the purchaser might be unknowingly accepting unnecessary risk.

There also may be circumstances where critical systems may require agent-based anti-virus applications. This creates a mixture of both anti-virus protection methods that must be administered and maintained, increasing administrative costs.

2. Physical and virtual system management:
All companies that have deployed virtualization maintain both physical and virtual environments.

Today this requires multiple management consoles as both types of systems must be managed and maintained separately, doubling administrative overhead and increasing cost.

Agentless anti-virus solutions are definitely a solid step forward in efficiency, but the wrong agentless solution can negatively impact the desired ROI.

The RIGHT PROTECTION option

5.0

The vast majority of IT professionals would agree that having no anti-virus protection is not an option.

Which leaves the flawed alternatives of agent-based and agentless based virtual anti-virus solutions, or a middle way that combines the best of both approaches, without compromising the ROI and other business achievable from server virtualization.

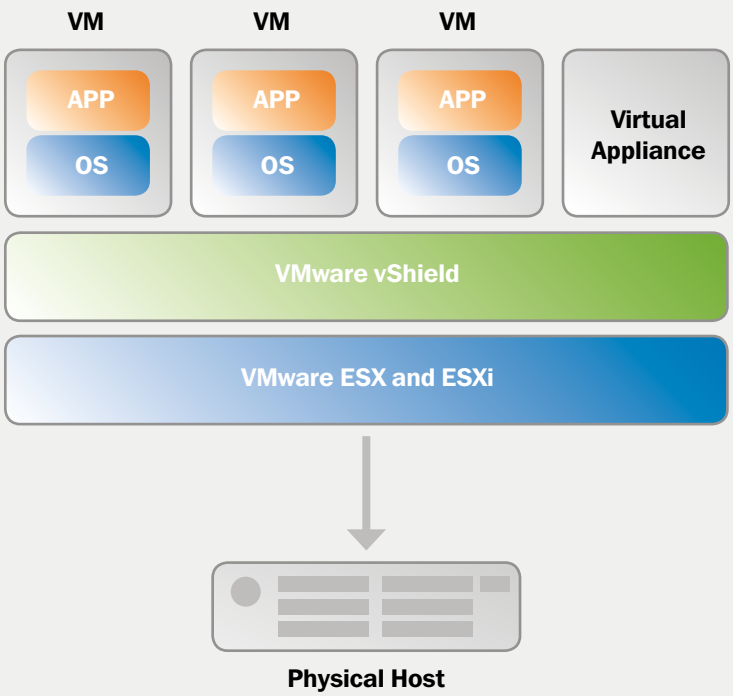
This 'right protection' option features a virtual appliance that integrates into VMware's vShield Endpoint to provide real-time anti-malware scanning capabilities for all guests on a physical host.

Endpoint uses a virtual appliance on the host, connected to each virtual machine through a small driver. The driver offloads the scanning and updating processes from the individual virtual machines to the virtual appliance.

This reduces host-resource utilization problems. Instead of several anti-virus agents running full bore, the virtual appliance — acting as a centralized hub — eases the load on the host.

As illustrated, a virtual security platform using VMware vShield Endpoint includes three components:

1. vShield Manager (a module installed via vShield Manager into the vSphere Hypervisor on physical boxes).
2. vShield Endpoint – A stub agent that is automatically installed in each virtual machine to capture file event context.
3. A security appliance from an anti-malware vendor that supports vShield Endpoint APIs.



vShield Endpoint uses vSphere 4.1 or 5.0 'plumbing' to deliver the files for inspection to the chosen security appliance.

This provides a remedy to the issues affecting both agent-based and agentless security solutions, as outlined above:

- **Manageability/Visibility/Agility/Flexibility:** A single-pane view of all protected machines (whether virtual or physical) enabling easy management. Protection status, security events and reports are presented clearly and intuitively. Administrators have visibility into the logical and physical structure that resembles familiar VMware management tools. This allows them to effectively manage security operations and take quick actions (such as remediation, diagnostics or forensics).
- **Effective detection and malware remediation:** Integrates anti-malware technology with powerful controls such as web content filtering, application controls and granular device controls.
- **Efficiency:** There is no redundancy and duplication of the anti-virus engine or database. In addition, this form factor addresses the redundancy and resource contentiousness issues associated with agent-based anti-virus.
- **Automatic Protection, ease of deployment/compliance:** The combination of vShield Endpoint Security and anti-malware technology provides automatic protection for VMware virtualized environments. Once the virtual appliance is deployed on a host, all guest virtual machines (whether current or newly-created) will be automatically protected with the latest signatures. (a centralized signature database means protection is always up-to-date, regardless of whether the virtual machine was previously off line.) This also addresses many compliance issues.
- **Integration of security policy enforcement:** With tight integration with VMware's platform and tools, the protection (and security settings) seamlessly follows the workload as it moves from one host to another, without interruption. It also affords the flexibility to configure and apply different security settings to selected virtual machine groups and perform deep scans on selected virtual machines.

Conclusion

6.0

Companies are intrigued by the attractive value proposition that virtualization presents. However, the challenges related to managing traditional agent-based and agentless virtual assets significantly limit potential benefits.

The 'right protection' overcomes the failings of legacy protection solutions, with an approach that mirrors that of virtualization itself – flexible, adaptable, scalable and capable of delivering fast ROI and providing the right balance between protection and performance.

About Kaspersky Lab

Kaspersky Lab is the only vendor today that delivers outstanding protection and management of physical, virtual, and mobile devices from one management console. Kaspersky truly is the 'right protection' option, optimized for virtual systems.

Security for Virtualization. Get the right balance with Kaspersky.

kaspersky.com/beready

Be Ready for What's Next.