

A background image showing a laptop on a desk with a speedometer overlay. The speedometer has numbers from 0 to 70 and a needle pointing towards 40. The scene is dimly lit, suggesting an office or server room environment.

Trend Micro Enterprise Security

Immediate Protection. Less Complexity. 



Changing the Game
for Anti-Virus in the
Virtual Data Centre

A Trend Micro White Paper | September 2010



CHANGING THE GAME FOR ANTIVIRUS IN THE VIRTUAL DATA CENTRE

I. INTRODUCTION

From its early experimental applications in the 1960s and 1970s, virtualisation was first seriously implemented as a way to control IT capital and operational expenditures through server consolidation. Then in 2005, when Intel and AMD introduced chipsets to specifically support virtual hardware, virtual environments started expanding into line-of-business applications, where they continue to deliver cost efficiency in IT production through resource consolidation. Reducing the cost of IT consistently surfaces in the top 3 list of concerns to CIOs today and as validated by analyst firm, Gartner, virtualisation is one of the key enablers to reducing technology costs. [1]

With the cost-savings of virtualisation widely validated, the focus has turned more to quality of service in virtualisation efforts, with targets for service level agreements, speed and stability. However, as enterprises rush to embrace the benefits of virtualisation, they have also rushed to implement traditionally architected security solutions in virtualised environments. Unfortunately, while this approach is familiar to enterprises, it results in undesirable consequences. At minimum, this approach increases complexity and impacts performance. At its worst, this approach creates new security risks and diminishes the cost efficiencies of server consolidation.

“Having about 90% of our environment now virtualised has significantly reduced our costs and greatly enhanced our disaster recovery capability.”

Gary Whatley, CIO, Corporate Express, based on interview with Gartner January 2009

This white paper reviews the challenges with endpoint security in virtualised environments – including the inherent risks of dynamic virtual machines and the resource impact of security software such as virus-scanners in multiple guest virtual machines, on a single physical host. [2] To address these challenges, a new standard for virtual data centre security is presented; one that combines proven threat protection technology with an innovative architecture for anti-virus protection in virtualised environments.

II. SECURITY CHALLENGES IN THE VIRTUAL DATA CENTRE

Securing the journey to virtualisation is complicated by two factors – (1) risks that are present in the physical data centre, and (2) those that are unique to virtualised environments.

The leaders in enterprise security and virtualisation – Trend Micro and VMware®, respectively – have joined forces to articulate these challenges and to collaborate in specific areas to help customers address them. These challenges directly impact the ability of enterprise virtualisation efforts in their movement from cost-efficiency to quality of services and ultimately, to business agility. It is this last stage where IT can truly be delivered as a service – or via a cloud – and business can request these services on-demand.



CHANGING THE GAME FOR ANTIVIRUS IN THE VIRTUAL DATA CENTRE

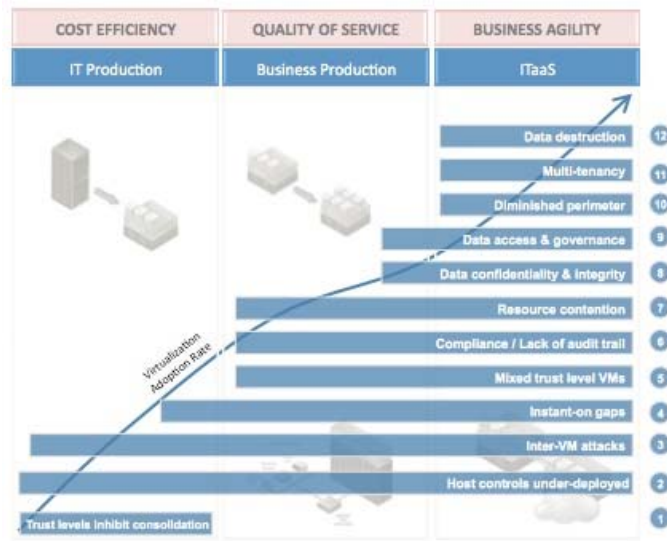


Figure 1: Security challenges along the virtualisation journey

Legacy Approach in the Virtual Data Centre

As enterprises move into the business production stage of virtualisation, security concerns emerge and suddenly the idea of massive consolidation of physical hosts causes panic rather than elation. To address risks to guest virtual machines, security-minded enterprises have deployed existing endpoint security solutions to every guest virtual machine in their virtualised environments. This has resulted in a de facto 'standard' for how anti-virus is handled in the virtual data centre.

- **Physical vs. Virtual:** But inherent differences in physical and virtual architectures must be considered. For example, each operating system (OS) instance in the physical environment runs directly on a dedicated hardware platform. In contrast, each OS instance in the virtual environment runs within a guest virtual machine and multiple guests run on the "hypervisor" layer. This hypervisor is a layer of abstraction between virtual machines and the underlying hardware, allowing for dynamic allocation of system resources. With these fundamental differences, routine actions just as file scans and network requests for software updates are sure to behave differently.
- **Cumbersome Anti-Virus Management:** Virtualisation infrastructure (VI) administrators may leverage efficiencies by using templates to accelerate deployment. And security administrators leverage centralised management of anti-virus. But even with some level of automation, deployment and ongoing management of antivirus in each guest virtual machine is not scalable. The process is cumbersome enough in the physical environment, and only exacerbated by the dynamic nature of virtual environments.

Legacy Anti-virus Management

1. Configure the agent at setup
2. Reconfigure the agent as necessary over time
3. Patch/upgrade the agent
4. Roll out pattern updates



CHANGING THE GAME FOR ANTIVIRUS IN THE VIRTUAL DATA CENTRE

This legacy approach results in three key challenges for virtualised environments:

- Instant-On Gaps
- Resource Contention
- Compliance / Lack of Audit Trail

Instant-On Gaps

Beyond server consolidation, enterprises take advantage of the dynamic nature of virtual machines by provisioning and decommissioning them as needed, for test environments, scheduled maintenance, disaster recovery, and to support 'task workers' who need computational resources on-demand. As a result, when virtual machines are activated and inactivated in rapid cycles, it is impossible to rapidly and consistently provision security to those virtual machines and keep them up-to-date. Dormant virtual machines can eventually deviate so far from the baseline that simply powering them on introduces massive security vulnerabilities. And new virtual machines, even when built from a template with anti-virus, cannot immediately protect the guest without configuration of the agent and pattern file updates. In short, if a guest virtual machine is not online during the deployment or updating of anti-virus software, it will lie dormant in an unprotected state and be instantly vulnerable when it does come online.

Resource Contention

Resource-intensive operations such as regular anti-virus scans and pattern file updates can quickly result in an extreme load on the system. When anti-virus scans or scheduled updates simultaneously kick into action on all virtual machines on a single physical system, the result is an "anti-virus storm". This 'storm' is like a run on the bank, where the 'bank' is the underlying virtualised resource pool of memory, storage and CPU. Server applications and virtual desktop/VDI environments are hampered by this performance impact.

The legacy architecture also results in linear growth of memory allocation as the number of virtual machines on a single host grows. In physical environments, anti-virus software must be installed on each operating system. Applying this architecture to virtual systems means that each virtual machine requires additional significant memory footprint – an unwanted drain on server consolidation efforts.

IT Compliance Challenges

Industry regulations and enterprise security policies must evolve to keep pace with virtualisation technologies, which present a unique set of challenges to compliance efforts. Visibility and control into system and network activity are even more complex in virtual environments, since traditional host-based security software and network security appliances are not integrated into the introspection layer. The most effective way to address the issue comes by integrating the anti-virus capability directly into the virtualisation platform, using hypervisor introspection – the ability to monitor and control what goes in and out of the hypervisor layer. Taking advantage of these efficiencies requires collaboration with virtualisation platform providers.

“PCI DSS 2.0 will expand definition of system components to include virtual components.”

PCI DSS 2.0 and PA-DSS 2.0

Summary of Changes – Highlights,

August 2010



CHANGING THE GAME FOR ANTIVIRUS IN THE VIRTUAL DATA CENTRE

III. A NEW APPROACH IS NEEDED

As effective as today's malware detection may be in physical environments, implementing a solution designed for these environments creates new challenges in the virtual world by not taking into account their inherent differences.

Address drawbacks of legacy approach: Antivirus operations which cause the greatest problems in a virtualised environment must be identified and a solution to streamline those operations must be developed. For instant-on gaps, the solution must provision and manage virtual machines in a fully-protected state, so that security in the guest virtual machine is persistent, regardless of when the last anti-virus pattern file update or scheduled scan occurred. For resource contention issues, the solution must compensate for resource utilisation spikes caused by these aforementioned anti-virus activities.

Ensure efficiency of new approach: This new approach must also leverage existing investments, not simply for reasons of cost efficiency but also for staff training requirements. It must also not "rock the boat" in other areas of the business; security policies, industry regulations, and compliance requirements must all continue to be met, and met visibly via audit trails and other insight reports.

IV. THE PLATFORM – VMWARE VSHIELD ENDPOINT

VMware is the global leader in virtualisation and cloud infrastructure, delivering customer-proven solutions to more than 190,000 customers, including more than 97% of Fortune 1000 and 94% of Global 500 companies. Continuing innovation in the virtual data centre, VMware has extended its platform, allowing the hypervisor introspection necessary to optimise security functions in virtualised environments, with VMware vShield Endpoint.

VMware vShield Endpoint strengthens security for virtual machines and their hosts while improving performance by orders of magnitude for endpoint protection. vShield Endpoint enables offloading of antivirus processing to a dedicated security-hardened virtual machine, provided by Trend Micro. It also enables massive reduction in memory footprint for security on virtual hosts by eliminating anti-virus software from the guest virtual machines and centralising those functions to the dedicated security virtual machine. VI administrators can centrally manage VMware vShield Endpoint through the vShield Manager console, which integrates with VMware vCenter™ Server to manage the platform for Trend Micro anti-virus solutions.

How it works

vShield Endpoint plugs directly into the VMware vSphere™ platform, is deployed on a per host basis and consists of three components:

- Hardened virtual appliance (provided by Trend Micro)
- Driver for virtual machines to offload file events
- VMware Endpoint Security (EPSEC) ESX module to link the first two components at the hypervisor layer



CHANGING THE GAME FOR ANTIVIRUS IN THE VIRTUAL DATA CENTRE

The vShield Endpoint driver is enabled for protected vSphere-based virtual machine and requires only a few megabytes of memory for operation. [3] The driver monitors virtual machine file events and notifies the antivirus engine, which scans and returns a disposition for the file(s). It also supports scheduled full and partial file scans initiated by the antivirus engine in the virtual security appliance. When remediation is required, administrators can specify the actions to take using the existing anti-virus manager, while vShield Endpoint enforces remediation action automatically within the respective virtual machines.

V. THE SOLUTION – TREND MICRO™ DEEP SECURITY

The VMware vShield Endpoint platform enables the optimisation of anti-virus solutions in virtualised environments. Building on this platform as a strategic partner, Trend Micro is the first to deliver a solution to the aforementioned challenges in securing virtualised environments with Trend Micro™ Deep Security.

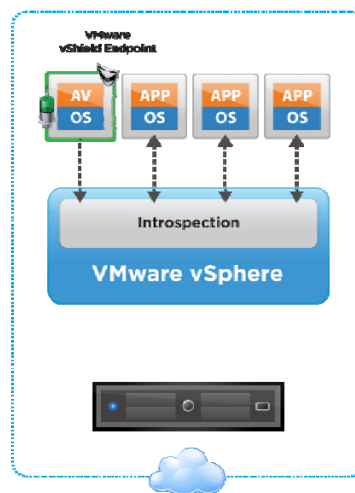


Figure 2: VMware vShield Endpoint and Trend Micro Deep Security

The combination of the two is what allows enterprises to effectively address the challenges of instant-on gaps and resource contention in the virtual data centre. This unprecedented innovation changes the game for anti-virus in the virtual data centre.

Trend Micro Deep Security provides the security virtual appliance that hosts the antivirus engine and performs familiar actions such as scheduled (and on-access) file scans, pattern file updates, checks for file disposition (known malware or not), and instructions on enforcement action (e.g. quarantine, deletion). The actual execution of the enforcement action is performed by the VMware vShield Endpoint technology, which monitors and controls hypervisor and guest virtual machine file activity.



CHANGING THE GAME FOR ANTIVIRUS IN THE VIRTUAL DATA CENTRE

Always-On Security to Address Instant-On Gaps

For environments protected by Trend Micro Deep Security and VMware vShield Endpoint, virtual machines are protected through their entire lifecycle with the assurance that any file access will automatically be scanned for the latest known threats. The Trend Micro Deep Security virtual appliance is deployed with the necessary security hardening to ensure that the anti-virus engine is always present and available to perform these tasks.

Anti-Virus Offload Solves Resource Contention Issues

With this innovative new technology, organisations can now improve performance and maintain consolidation ratios by offloading activities such as anti-virus scans from individual virtual machines to a single Trend Micro virtual appliance on each protected vSphere host.

- **Reclaim memory to maintain consolidation ratios:** Reducing memory allocation per guest virtual machine enables administrators to increase server consolidation ratios significantly. Rather than deploy hundreds of megabytes of anti-malware software to every guest virtual machine on a physical machine, organisations can now deploy a single anti-virus engine to a virtual appliance and leverage a very small footprint driver in each virtual machine to perform the necessary offload. The benefits are especially obvious in VDI (VMware View™) environments where consolidation ratios of 200:1 are not uncommon. [4] With this massive reduction in memory allocation, cost savings can be realised and enterprises can extend the usefulness of their physical servers and achieve even higher server consolidation ratios.
- **Centralise scanning and updates to prevent anti-virus storms:** With this new architecture, Deep Security handles CPU and I/O intensive file scans and pattern file updates, leaving guest virtual machines with more resources to perform business critical functions. The solution prevents antivirus storms and bottlenecks associated with these simultaneous scans and updates by serialising operations across virtual machines on a given host.

Visibility and Control to Simplify Compliance Efforts

Trend Micro Deep Security addresses a number of compliance aspects beyond security:

- **Single function per server:** A recent update to PCI DSS 2.0 suggests that virtualisation technology will be acceptable even in cases where Requirement 2.2.1 – “one primary function per server” – must be satisfied. To this point, the security virtual appliance is a single-purpose virtual machine that provides anti-virus protection – nothing else.
- **Visibility through introspection:** The solution uses robust and secure hypervisor introspection capabilities through vShield Endpoint, ensuring the deepest visibility into file activity for anti-virus scans. The majority of industry regulations and enterprise data security policies call for active monitoring of file system activity for malicious software and Trend Micro goes further to perform these scans on virtual systems.



CHANGING THE GAME FOR ANTIVIRUS IN THE VIRTUAL DATA CENTRE

- **Logging of vSphere and Trend Micro Events:** Detailed logging of relevant security events via the Trend Micro and VMware solutions is provided, helping address regulatory requirements and enterprise policies which may require forensics data for investigations.
- **Separation of Duties:** This new architecture enables security administrators to implement and manage anti-virus policies for the virtual environment through Deep Security Manager, the same interface used to secure the physical environment. Similarly, the VI administrator can use vCenter to deploy vShield Endpoint, along with the Trend Micro virtual appliance. Neither persona can manage the other infrastructure, by design. This separation of duties between VI administrator and security administrator plus detailed logging of activity helps enterprises demonstrate compliance and satisfy auditor requirements.

VI. BENEFITS EXTEND BEYOND THE SOLUTION

Trend Micro delivers a powerful solution to the problems of resource contention and instant-on gaps by acting directly on the hypervisor layer, resulting in IT management and resource efficiencies without impacting performance.

Simplified Management

Initial deployment and ongoing management of anti-virus is difficult enough in the physical data centre. The new solution addresses these challenges in the virtual data centre.

- **Streamline antivirus management:** With VMware vShield Endpoint and Trend Micro Deep Security, administrators need only deploy the enterprise anti-virus engine and signature file updates to the Deep Security Virtual Appliance. Essentially, there is no need for many of the cumbersome tasks with the legacy approach:
 1. NO configuring the agent at setup
 2. NO reconfiguring the agent as necessary over time
 3. NO patching/upgrading the agent
 4. NO rolling out pattern updates
- **No retraining of administrators required:** Role-based access control through VMware vCenter, integrated with the Trend Micro management consoles, allows individuals to continue their daily operations with minimal disruption. Administrators can define a role on the vCenter that permits only authorised administrators to deploy the Trend Micro Deep Security virtual appliance to virtual hosts. The Trend Micro console can also be configured to restrict access to Deep Security policies and security operations for optimum scheduling of essential updates to avoid resource contention.



CHANGING THE GAME FOR ANTIVIRUS IN THE VIRTUAL DATA CENTRE

Better Security

Trend Micro Deep Security provides better security in large measure because it embodies an approach to security that is efficient in the virtual data centre environment. For the past twenty years, the security industry has been running antivirus on the same system that requires protection, inadvertently presenting an invitation to attack.

- **Eliminate the target of attack:** The Deep Security solution is agent-less since no anti-virus software is installed in the guest virtual machine. And as described above, the anti-virus technology is deployed in a hardened security virtual appliance. Furthermore, the VMware vShield Endpoint driver in each guest virtual machine only allows certain communication with the Deep Security Virtual Appliance. Most attacks against anti-virus products anticipate an encounter with a full-blown client anti-virus installation on the guest virtual machine, but such attacks will bear no fruit with this new approach.
- **Eliminate vulnerabilities to common attack methods:**
The Deep Security Virtual Appliance, where the anti-virus engine runs, is hardened against common attack methods, such as those used by the Conficker worm. Only specific actions related to malware protection are permitted between the virtual appliance and the guest virtual machines. And because the appliance is always on, there are no instant-on gaps; the protection underlies the virtual machines at all times.

Common Attack Methods

1. Uninstalling the anti-virus program
2. Stopping the anti-virus program
3. Modifying registry keys that are required by the anti-virus program

VII. WHY TREND MICRO

Singularly focused on content security since its founding 20 years ago, Trend Micro provides core competency and expertise in content security. Trend Micro continues to provide innovation with the Trend Micro™ Smart Protection Network™, correlating real-time data on new and unknown threats and delivering continuously updated protection in an environment that's ideally suited to protect both physical and virtual environments. The Smart Protection Network infrastructure delivers advanced protection from the cloud, blocking threats in real-time before they reach the corporate network. Leveraging a unique, cloud-client architecture, it is powered by a global network of threat intelligence sensors, email, Web, and file reputation technologies that work together to dramatically reduce infections.

Technology from the Smart Protection Network feeds directly into the Deep Security anti-virus technology, allowing for smaller footprint pattern files. The Deep Security Virtual Appliance is the most recent offering of virtualisation-ready solutions, helping enterprises go further to reduce operational costs through centralised management of anti-virus for both physical and virtual environments.

With over one billion U.S. dollars in annual revenue, over 1,000 threat researchers—and over 4,000 employees—around the world, Trend Micro has the size, the speed, and the unique in-the-cloud core technology infrastructure required to handle today's enterprise security.



CHANGING THE GAME FOR ANTIVIRUS IN THE VIRTUAL DATA CENTRE

VIII. CONCLUSION

It is only natural that enterprises would address security challenges in the virtual data centre with familiar approaches, but inherent differences between physical and virtual infrastructure produce undesirable results with legacy solutions. Trend Micro, in collaboration with VMware, offers an innovative approach to anti-virus protection for VMware virtual data centres with Trend Micro Deep Security. This unprecedented approach addresses key challenges with the legacy approach while also addressing simplifying management, enabling IT compliance and improving overall security of the solution.

Security Challenge in Virtualised Environment	Solution Benefit
Instant-On Gaps	<ul style="list-style-type: none">• Automatic protection until IT can install anti-virus
Resource Contention	<ul style="list-style-type: none">• Always current antivirus patterns through centralised deployment in a virtual appliance• Maintain consolidation ratios by reclaiming memory• Prevent anti-virus storms with centralised scanning
IT Compliance Challenges	<ul style="list-style-type: none">• Single function per server to address PCI DSS and other regulations• Visibility through introspection• Logging of vSphere, Deep Security events
Management Complexity	<ul style="list-style-type: none">• Enable separation of duties• Streamline anti-virus management• No retraining of administrators required
Security Risks with Legacy Anti-virus	<ul style="list-style-type: none">• Eliminate the target of attack• Eliminate vulnerabilities to common attack methods

Learn more about Trend Micro Deep Security at <http://www.trendmicro.com>.

Learn more about VMware vShield Endpoint at <http://www.vmware.com/products/vshield-endpoint/>.



CHANGING THE GAME FOR ANTIVIRUS IN THE VIRTUAL DATA CENTRE

IX. REFERENCES

[1] "Meeting the Challenge: The 2009 CIO Agenda", January 2009, pages 32 and 45

[2] Software that detects and clean viruses, spyware, Trojans and other forms of malware are often referred to as anti-virus or anti-malware. In this paper we will refer to it as anti-virus

[3] Initially, the driver must be deployed using existing methods for virtual machine provisioning, such as templates. VMware is considering including this as an in-guest driver for VMware Tools.
Source: VMware

[4] Source: VMware[®] ROI TCO Calculator <http://roitco.vmware.com/vmw/>

©2010 by Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo, and TrendLabs are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice. [WP01_TMES_081012GB]