Trend Micro Deep Security

VMware Global Technology Alliance Partner

Changing the Game with Agentless Security for the Virtual Data Center

A 2012 Trend Micro White Paper

I. INTRODUCTION

From its early experimental applications in the 1960s and 1970s, virtualization 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 specifically to 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. Today, reducing the cost of IT is consistently in the top list of concerns of CIOs. However, the benefits of virtualization go beyond the cost savings.

Virtualization simplifies IT infrastructure to create a more dynamic and flexible datacenter and serves as the catalyst for cloud computing. With a self-service portal, IT resources can be delivered as a service with the automatic provisioning of virtual machines (VMs). And virtual desktop infrastructure (VDI) delivers desktops as a managed service, providing users access to their desktops, applications, and data anywhere, any time, on any device. Not only do these benefits reduce both capital and operational expenditures, but they also provide resource agility that promotes business innovation and growth.

However, as enterprises rush to embrace the benefits of virtualization, they have also rushed to implement traditionally architected security solutions in virtualized environments. Unfortunately, while this approach is familiar to enterprises, it results in undesirable consequences when deployed on virtual platforms. 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.

This white paper reviews the challenges of applying traditional security in virtualized environments, including the inherent risks of dynamic virtual machines and the resource impact of security software in multiple guest virtual machines on a single physical host. To address these challenges, a new standard for virtual datacenter security is presented; one that combines proven threat protection technology with an innovative architecture for agentless security protection in virtualized environments.

The leaders in enterprise security and virtualization, Trend Micro and VMware®, respectively, have joined forces to articulate these challenges and to collaborate to help customers address them. These challenges directly impact the ability of enterprise virtualization efforts in their movement from cost-efficiency to quality of services and ultimately, to business agility.

II. SECURITY CHALLENGES IN THE VIRTUAL DATACENTER

Securing virtual environments is complicated by two factors: (1) risks that are present in the physical datacenter and (2) those that are unique to virtualized environments.

Figure 1 below shows the anticipated adoption rate of the virtualization stages on the journey to the cloud. The virtualization stages include basic server virtualization in which businesses just begin to consolidate, followed by further server virtualization of more critical line-of-business applications and VDI, and finishing with cloud computing by deploying private, public, or hybrid clouds. If businesses introduce traditional agent-based security into their virtual environments during this journey, the virtualization

adoption rate will most likely fall short of their anticipated progress due to reduced density and ROI. This is caused by the negative impact of traditional security on performance and resources in virtual environments. Without the foundation of a secure, efficient virtual environment, businesses may also reduce their adoption of cloud computing.

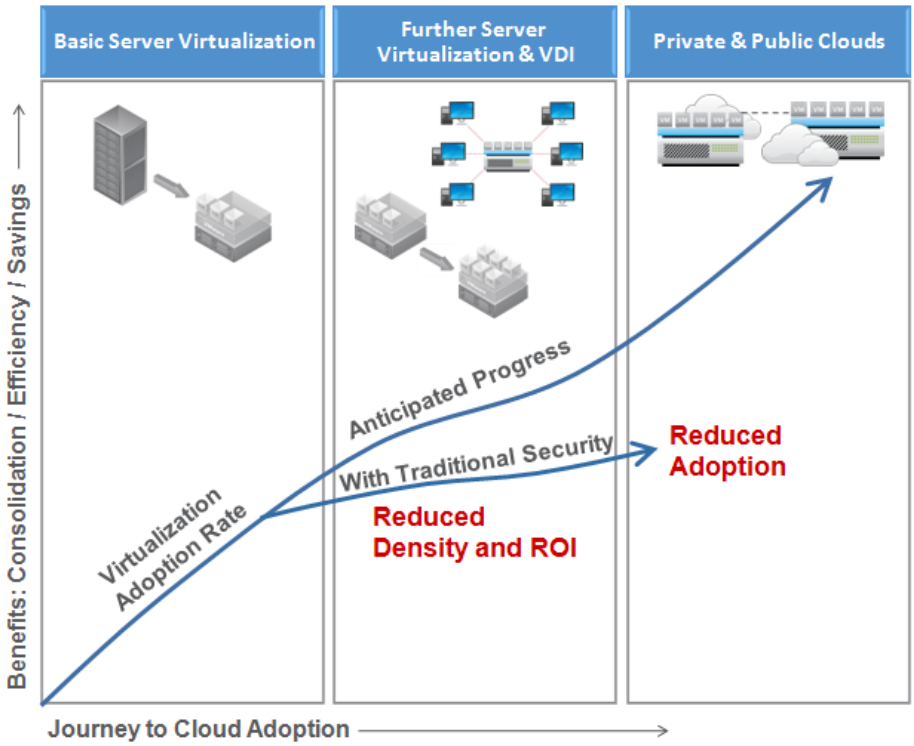

Figure 1: Impact of Traditional Agent-based Security on Virtualization and Cloud Adoption Rates

Traditional Agent-based Security Approach in the Virtual Datacenter

As enterprises move into the business production stage of virtualization, security concerns emerge and suddenly the idea of massive consolidation of physical hosts causes apprehension rather than elation. To address risks to guest virtual machines, security-minded enterprises have deployed traditional agent-based security solutions to every guest virtual machine in their virtualized environments. This has resulted in a de facto "standard" for how virtual machine security is handled in the virtual datacenter.

- **Physical vs. Virtual**: 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 such as file scans and network requests for software updates will behave differently.

- **Cumbersome Security Management**: Virtualization infrastructure (VI) administrators may leverage efficiencies by using templates to accelerate deployment. And security administrators leverage centralized management of server security. But even with some level of automation, deployment and ongoing management of security 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.

Traditional Agent-based Security Management

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

This traditional agent-based security approach results in three key challenges for virtualized environments:

- Instant-on gaps
- Resource contention
- Compliance / Lack of audit trail

Figure 2 shows security challenges for virtualization and cloud environments, including the challenges listed above that are a result of deploying traditional agent-based security on virtual machines.

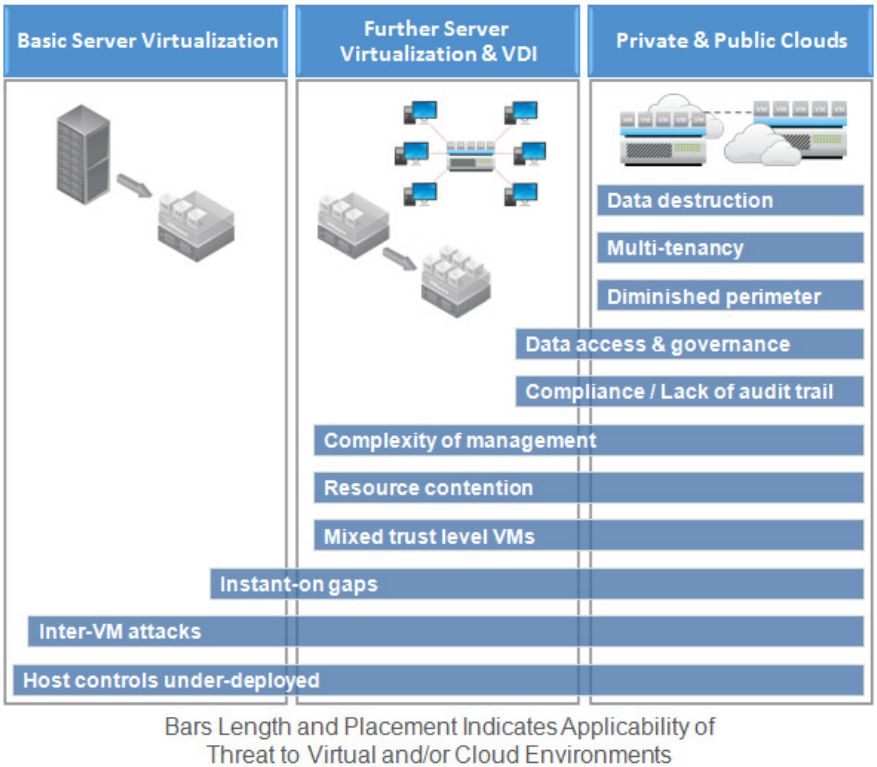

Figure 2: Security Challenges that Apply to Virtual and/or Cloud Environments

Businesses need virtualization-aware security that addresses standard security concerns as well as risks specific to virtualization environments while not creating new security issues. Here is a discussion of the three key challenges created by applying traditional agent-based security to virtual environments.

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 that includes security, cannot immediately protect the guest without configuration of the agent and conducting security updates. In short, if a guest virtual machine is not online during the deployment or updating of security 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 security scans and pattern file updates can quickly result in an extreme load on the system. When antivirus scans or scheduled updates simultaneously kick into action on all virtual machines on a single physical system, the result is an “antivirus storm.” Similar “storms” can occur with other types of security scans and updates as well. These “storms” are like a run on the bank, where the “bank” is the underlying virtualized resource pool of memory, storage, and CPU. Server applications and virtual desktop environments are hampered by this performance impact.

The traditional agent-based architecture also results in linear growth of memory allocation as the number of virtual machines on a single host grows. In physical environments, security 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 virtualization technologies, which present a unique set of challenges to compliance efforts. Virtual machines can be reverted to previous instances, paused, and restarted, all relatively easily. They can also be readily cloned and seamlessly moved between physical servers. Vulnerabilities or configuration errors may be unknowingly propagated. Also, it can be difficult to maintain an auditable record of the security state of a virtual machine at any given point in time.

Visibility and control into system and network activity are 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 virtual machine security capabilities directly into the virtualization 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 virtualization platform providers.

III. A BETTER APPROACH IS NEEDED

As effective as today's server and endpoint security solutions 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 traditional agent-based security approach**: Virtualization-aware security operations must be employed that avoid creating new security issues in virtualized environments. 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 security update or scheduled scan occurred. For resource contention issues, the solution must prevent resource utilization spikes caused by antivirus and other security "storms" by coordinating and staggering scans and updates through an awareness of the shared resource environment.

- **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 reports.

IV. INTEGRATING SECURITY WITH THE VMWARE PLATFORM

VMware is the global leader in virtualization and cloud infrastructure, delivering customer-proven solutions to more than 350,000 customers, including 100% of the Fortune 500 and 98% of the Fortune Global 500 companies. Continuing innovation in the virtual datacenter, VMware has extended its platform, allowing the hypervisor introspection necessary to optimize file-level security functions, such as antivirus and file integrity monitoring, in virtualized environments with VMware vShield Endpoint. In addition, leveraging other VMware application programming interfaces (APIs) enables network-level security integration into the VMware virtualization platform, including intrusion detection and prevention, Web application protection, application control, and firewall.

Figure 3 below summarizes the use of VMware vShield Endpoint and other VMware APIs to enable various types of agentless security within a dedicated security virtual appliance. The figure specifically shows how Trend Micro has used these APIs to offer a range of security capabilities in its Deep Security server security platform.

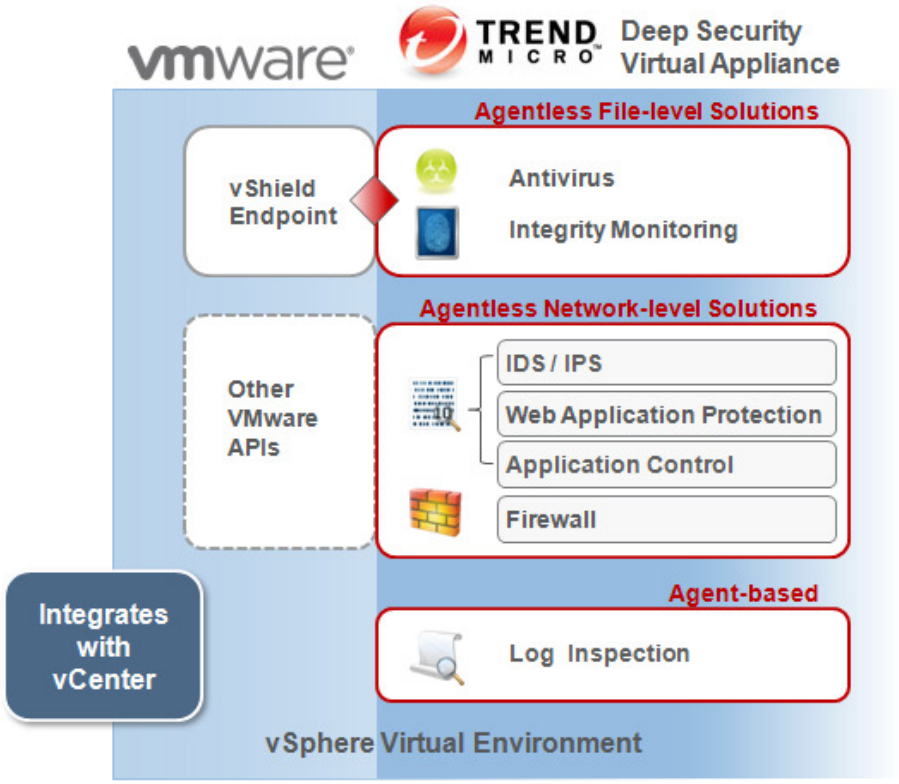

Figure 3: Integrating Security into the VMware Ecosystem

VMware vShield Endpoint

vShield Endpoint is a unique solution that optimizes host and endpoint security for use in vSphere and View environments. vShield Endpoint improves performance by offloading key security functions to a dedicated security appliance, eliminating the security agent footprint in virtual machines. The hardened, tamperproof security virtual appliance, delivered by Trend Micro, uses robust and secure hypervisor introspection capabilities in vSphere to prevent compromise of the protection capabilities. This advanced architecture frees up system resources, improves performance, and eliminates the risk of security "storms."

Using detailed activity logs from the security service, organizations can demonstrate compliance and satisfy auditor requirements. Administrators can centrally manage vShield Endpoint through the included VMware vShield™ Manager console, which integrates seamlessly with VMware vCenter™ Server to facilitate unified security management for virtual datacenters.

How vShield Endpoint Works with Trend Micro Deep Security Virtual Appliance

vShield Endpoint is a VMware API that is leveraged by Trend Micro Deep Security. 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)
- vShield Endpoint in-guest driver (part of VMTools)
- vShield Endpoint Hypervisor module connects the Deep Security virtual appliance to the in-guest driver

The vShield Endpoint in-guest driver is enabled for protected vSphere-based virtual machines and requires only a few megabytes of memory for operation. As of vSphere 5, the in-guest driver is a part of VMTools. The driver monitors virtual machine file events and notifies the dedicated security virtual appliance of these events and returns a disposition for the file(s) for security activities such as antivirus and file integrity monitoring. 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 security manager, while vShield Endpoint enforces remediation action automatically within the respective virtual machines.

By using the vShield Endpoint and Trend Micro Deep Security virtual appliance, separate security agents are not required on each guest virtual machine to provide this protection. Figure 4 below demonstrates the traditional agent-based approach that requires security agents on each guest virtual machine, including separate agents for each individual server security point product. This is compared to the new security approach that integrates with VMware vShield Endpoint to enable the use of a dedicated security virtual appliance and an agentless approach to security across the guest virtual machines—increasing performance and virtual machine density.

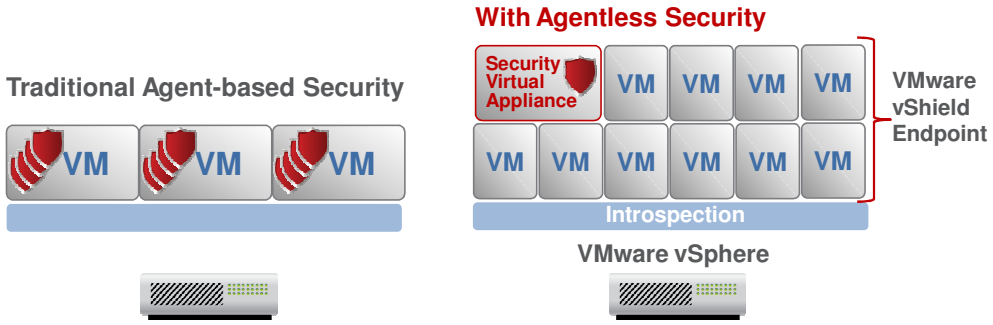

Figure 4: Traditional Agent-based Security Compared to a Better Approach Using Agentless Security: VMware vShield Endpoint + Trend Micro Deep Security

Other VMware APIs for Security Integration

For security capabilities that protect on the network level and do not require the use of a VMware driver to monitor file events and scans, agentless security can be provided through integration with other VMware APIs.

How Deep Security Works Leveraging Other VMware APIs for Security

- The dedicated, security-hardened virtual appliance by Trend Micro (Deep Security solution) integrates with VMware APIs to protect virtual machines from network-based threats
- The VMware APIs enable Deep Security to communicate with the guest virtual machines to implement security such as intrusion detection and prevention, Web application protection, application control, and firewall
- This approach enables security that protects the virtual server and desktop network systems without deploying in-guest security agents

V. THE SOLUTION - TREND MICRO™ DEEP SECURITY

Building on the VMware platform as a strategic security partner, Trend Micro is the first to deliver a solution that provides agentless security to protect virtualized environments and avoid the aforementioned security challenges. This solution, Trend Micro ™ Deep Security, offers a dedicated security virtual appliance that integrates with the VMware virtualization platform and enables agentless security for guest virtual machines.

Trend Micro Deep Security provides a comprehensive server security platform. Tightly integrated modules easily expand the platform to ensure server, application, and data security across physical, virtual and cloud servers, as well as virtual desktops. Deep Security provides a wide range of agentless security options for VMware virtual machines:

- Antivirus
- File integrity monitoring
- Intrusion detection and prevention
- Web application protection
- Application control
- Bidirectional stateful firewall

These security options integrate in the same virtual appliance for increased protection on VMware virtual machines. Agent-based security and log inspection are also available, enabling businesses to combine agentless and agent-based deployment configurations that best support their virtual desktops and their physical, virtual, and cloud servers.

The combined security of Trend Micro Deep Security with the VMware virtualization platform allows enterprises to effectively address the challenges of instant-on gaps and resource contention while providing the visibility and control needed for compliance of virtual machines. This unprecedented innovation changes the game for security in the virtual datacenter.

Always-On Security to Address Instant-On Gaps

For environments protected by Trend Micro Deep Security's dedicated security virtual appliance, virtual machines are protected through their entire lifecycle. New, reactivated, and cloned virtual machines are protected with the assurance that any file access will automatically be scanned for the latest known threats and network-level security will always be up to date. Trend Micro Deep Security virtual appliance is deployed with the necessary security hardening to ensure that the security is always present and available to perform these tasks.

Security Activity Offload Solves Resource Contention Issues

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

- **Reclaim memory to maintain consolidation ratios**: Using agentless security on the dedicated security virtual appliance reduces memory allocation per guest virtual machine and enables administrators to increase server consolidation ratios significantly. Rather than deploy hundreds of megabytes of security software to every guest virtual machine on a physical host, organizations can now deploy a security virtual appliance and leverage a very small footprint VMware 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. With this massive reduction in memory allocation, cost savings can be realized and enterprises can extend the usefulness of their physical servers and achieve even higher server consolidation ratios.

- **Centralize scanning and updates to prevent security storms**: With this new architecture, Deep Security handles CPU and I/O intensive file scans and updates on the security virtual appliance, leaving guest virtual machines with more resources to perform business critical functions. The solution prevents antivirus and other security storms and bottlenecks associated with these simultaneous scans and updates by serializing 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:

- **Visibility through introspection**: The solution uses robust and secure hypervisor introspection capabilities through vShield Endpoint, ensuring the deepest visibility into file activity for antivirus and file integrity monitoring. The majority of industry regulations and enterprise data security policies call for active monitoring of file system activity for malicious software and change control, and Trend Micro had designed a solution to efficiently perform these scans on virtual systems.

- **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 security 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.

Trend Micro Deep Security delivers a powerful solution to the problems of instant-on gaps and resource contention, while also providing the visibility and control needed for compliance. This is achieved by acting directly on the hypervisor layer, resulting in IT management and resource efficiencies without impacting performance.

VI. ADDRESSING OTHER SECURITY RISKS IN VIRTUAL ENVIRONMENTS

Trend Micro Deep Security is a virtualization-aware solution that avoids the additional security issues caused by using a traditional agent-based security solution on virtual machines. However, it is also designed to address risks specific to virtual environments. Looking back to the security challenges for virtual environments in Figure 2 on page 3 (listed again in the lower right), Deep Security addresses these risks enabling businesses to safely deploy virtual machines in virtual and cloud environments.

Server Security Platform

Deep Security is a server security platform for physical, virtual, and cloud servers as well as virtual desktops. By enabling the deployment of physical and virtual server protection in the same solution, businesses can avoid the under-deployment of host controls. Host-level security in addition to security on the virtual machine level can all be managed through the same console.

Self-defending Virtual Machines

Many of the security risks in virtual environments are a result of the shared resource infrastructure. A virtual machine may be at risk due to being housed next to another, more dangerous virtual machine. For example, inter-VM attacks occur when one virtual machine attacks another on the same physical host (this can also include hypervisor compromises, such as hyperjacking or guest VM escape). Similarly, mixed trust level VMs occur when critical applications or data are housed next to more vulnerable virtual machines. And multi-tenancy generally refers to public cloud environments where you have no control over your neighbors' virtual machines.

Security Challenges for Virtual Environments

- Host controls under-deployed
- Inter-VM attacks
- Instant-on gaps
- Mixed trust level VMs
- Resource contention
- Complexity of management
- Compliance / Lack of audit trail
- Data access & governance
- Diminished perimeter
- Multi-tenancy
- Data destruction

The solution to all of these risks is to provide protection at the virtual machine level, creating virtual machines that can defend themselves regardless of the risks created by neighboring virtual machines. Trend Micro Deep Security provides a server security platform with tightly integrated modules for a range of serve security capabilities. This combined protection secures virtual machines against both file- and network-based threats, and enables virtual machines to defend themselves whether deployed in a shared resource infrastructure of a virtual data center, private cloud, or public cloud.

Encryption for Virtual and Cloud Data

Other security challenges are concerned with data access in the shared resource infrastructure of virtual environments, including data access and governance, and data destruction. Businesses are worried that unauthorized individuals might be able to access data. This could be by criminals, service providers, or even other departments in the same organization. Also, if data is migrated, there is the concern that there might be data remnants exposed in previous locations. Diminishing perimeter and multi-tenancy can be part of this data access risk as virtual and cloud environments enable applications and data to be accessed anywhere, anytime, from any device, but while sharing resources on the same physical host.

Encrypting data stored on virtual and cloud servers can eliminate these risks. Even if data is accessed by an unauthorized source, the information is unreadable and remains secure. Trend Micro Deep Security provides this protection through integration with the encryption solution, Trend Micro SecureCloud. SecureCloud offers encryption with simple, policy-based key management for data stored in physical, virtual, and cloud servers, supporting both vSphere and vCloud environments. Through integration with Deep Security, SecureCloud validates that servers have up-to-date security prior to releasing encryption keys.

Simplified Management

Complexity of management is the remaining security risk for virtual environments in the list above. Initial deployment and ongoing management of security is difficult enough in the physical datacenter. The dynamic nature and potential for virtual machine sprawl through ease of provisioning makes it even more difficult to achieve and maintain consistent security in a virtual environment.

- **No security agent management**: With VMware vShield Endpoint and Trend Micro Deep Security, administrators only deploy the enterprise security solution and updates to the Deep Security virtual appliance, eliminating many of the cumbersome tasks required of traditional agent-based security:
    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 security 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 authorized 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. And Deep Security shield vulnerabilities with virtual patching, eliminating the pains of emergency patching, frequent patch cycles, and costly system downtime.

VII. WHY TREND MICRO

As the largest pure-play security provider with over 20 years of experience and the recognized leader in server, virtualization, and cloud security[1], Trend Micro is uniquely positioned to help businesses make the most of virtualization and cloud computing. As part of this expertise, Trend Micro is a leading VMware security partner, providing Trend Micro Deep Security as the first partner solution designed specifically to:

- Integrate with vShield Endpoint APIs
- Integrate with other VMware APIs for network-level protection
- Deliver agentless anti-malware—available since 2010
- Deliver multiple agentless security options

Deep Security acquired more than 1,000 customers for agentless antimalware in its first year with virtual desktop consolidation ratios up to three times higher than leading traditional physical desktop antimalware solutions, giving organizations superior performance and protection that has been proven by extensive independent testing. The unique security framework of Deep Security provides multiple agentless security modules for VMware virtual machines—all on one security platform.

VIII. CONCLUSION

It is only natural that enterprises would address security challenges in the virtual data center with familiar approaches, but inherent differences between physical and virtual infrastructure produce undesirable results with traditional agent-based security solutions. Trend Micro, in collaboration with VMware, offers an innovative approach to virtual machine protection for VMware virtual datacenters and vCloud environments with Trend Micro Deep Security. This unprecedented approach protects enterprise applications and data from breaches and business disruptions without emergency patching.

Deep Security addresses key challenges with the traditional agent-based security approach while also protecting against risks specific to virtual environments. This comprehensive, centrally managed platform ensures server, application, and data security across physical, virtual, and cloud servers, as well as virtual desktops. It helps simplify security operations while enabling regulatory compliance and accelerating the ROI of virtualization and cloud projects.

Learn more about Trend Micro Deep Security at http://www.trendmicro.com/deepsecurity .
Learn more about VMware vShield Endpoint at http://www.vmware.com/products/vshield-endpoint/.

1. Sources: IDC 2011, Worldwide Endpoint Security Revenue Share by Vendor, 2010; Technavio 2011, Global Virtualization Security Management Solutions; and Technavio 2012, Global Cloud Security Software Market.