# A Brave New (Security) World

## How Security is Changing to Support Virtualization and Cloud Computing

*A Trend Micro™ White Paper | January 2011*

*Written by Eva Chen*

# A BRAVE NEW (SECURITY) WORLD: HOW SECURITY IS CHANGING TO SUPPORT VIRTUALIZATION AND CLOUD COMPUTING

## I. EXECUTIVE SUMMARY

In the near future, it is anticipated that all aspects of information technology will be movable, dynamic, and interactive – the access, the data, the workload, and all computing. End users' mobile devices will access and store hundreds of gigabytes of data. Virtual servers will mobilize computing power between network segments, data centers, and even outside of the corporate environment and into the public cloud, where computing power is offered as a utility.

As a result of these profound changes, all aspects of information security will be challenged and reconsidered. Traditional network security, which addressed sets of computing power such as machines and data storage as a guarded walled garden, will no longer apply. A new generation of security practices, which emphasize the dynamic aspect of computing power and data, will challenge the status quo.

However, these revolutionary changes will not take place overnight. The major challenge for enterprises will be how to proceed from where they are today, through a transitional or hybrid period, to where they will be in the future. The solution to this challenge will not be a one-size-fits-all approach; each organization will move forward at its own pace as a function of the requirements that it faces and various other interacting factors. Hence, solutions must be sufficiently flexible to accommodate this diversity. This white paper describes the evolution of these changes as enterprises adopt virtualization and then cloud computing. It then describes Trend Micro's vision for the evolution of security as a facilitator of mobility, virtualization, and cloud computing.

## II. INTRODUCTION

According to analysts, the 2009 worldwide network security market grew to over $7 billion, while the business host/endpoint security market grew to over $2 billion. Why is the relative magnitude of these expenditures likely to flip-flop in the future? The answer is that the traditional network security market will shrink as networks become less relevant due to the dynamic movement of computing power and data. Conversely, the market for host security, where the computing power host and the data itself are protected, will grow rapidly; the dynamic host itself will need to become the primary point of protection.

The magnitude of evolving changes in information technology and security are nothing less than dramatic. Imagine if Butch Cassidy and the Sundance Kid were to try to rob a bank today. The assumptions they made 150 years ago about robbing banks are now completely outdated. Banks are maintaining a decreasing amount of actual cash on hand, as electronic banking proliferates. Today, the major threat of theft is not cash at gunpoint in a bank, but identity theft, theft of corporate secrets left in unsecured iPads in taxicabs, and a broad range of sophisticated cyber threats.

The trend toward virtualization and cloud computing is one of the primary drivers of this paradigm shift. Enterprises are adopting virtualization and cloud computing because of the myriad of business benefits they promise, including IT flexibility, scalability, efficiency, cost reduction, and competitive advantage. According to a recent Gartner report, "Virtualization continues as the highest-impact issue challenging infrastructure and operations through 2015. It changes how you manage, how and what you buy, how you

deploy, how you plan and how you charge. It also shakes up licensing, pricing and component management." [1] The scope and prominence of this trend calls for a close look at the impact and role of security in virtualization and cloud computing.

## III. TRADITIONAL NETWORKS AND SECURITY

To best understand the security challenges and opportunities that virtualization and cloud computing bring, it is helpful to first examine how security has evolved from traditional networks of the past to today's networks, and how this evolution is likely to continue with virtualization and cloud computing.

Figure 1 shows a traditional network in which three main types of computing resources are inside the network perimeter – computing resources in the DMZ, mission critical servers, and endpoints. The relatively simple security arrangement consists of firewalls, web and email security, and intrusion detection and prevention systems (IDS/IPS) at the network perimeter. Host-based security consists of anti-malware agents on each computing device within the perimeter.

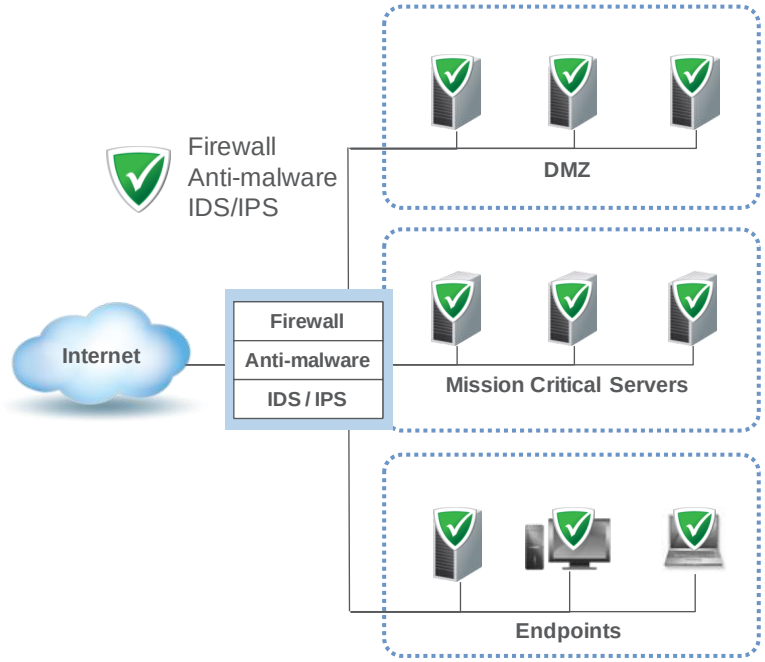


*Figure 1. In a traditional network, host-based security agents on each machine primarily consist of anti-malware, while perimeter security includes a firewall, web and email security, and IDS/IPS.*

As hackers discovered a way to penetrate the network perimeter despite the security there, and as insider threats grew, customers identified the need for deeper protection on all devices within the network (see Figure 2). So that the hosts could defend themselves, DMZ resources, servers, and endpoints were equipped with firewalls and IDS/IPSs. At nearly the same time, new devices expanded the definition of the

endpoint. Enterprises increasingly allowed employees to connect to the network through their laptops. And hence, organizations extended their networks to accommodate these tools. As these endpoints roamed outside the network and reconnected, resilient security was needed to protect them. And the agents installed on all of the devices within the network (and accessing remotely) needed to be updated regularly by some type of protection network and centralized management.

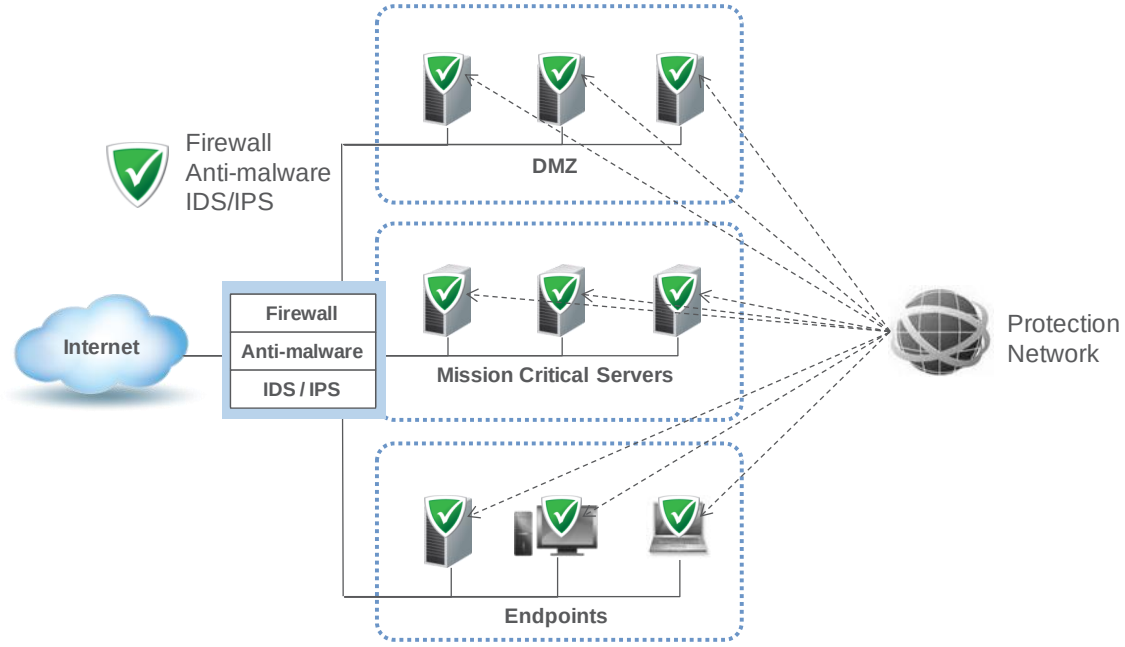


*Figure 2. In many of today's networks, host agents provide deeper protection, networks are expanded to include mobile/remote endpoints, and some type of protection network is implemented.*

## IV. VIRTUALIZATION

Virtualization renders the traditional network model less relevant, as live migration and sprawl make applications and data more dynamic, and network chokepoints fade. With this "de-perimeterization," security must now be extended all the way to each logical host node, wherever that node exists.

The host security agents provide deeper security and can move as the computing power moves. However, as enterprises adopt virtualization, deployment of a host security agent to each of the hosts becomes more complex; keeping up with the "instant" nature of these virtual servers and desktops is challenging.

# A BRAVE NEW (SECURITY) WORLD: HOW SECURITY IS CHANGING TO SUPPORT VIRTUALIZATION AND CLOUD COMPUTING

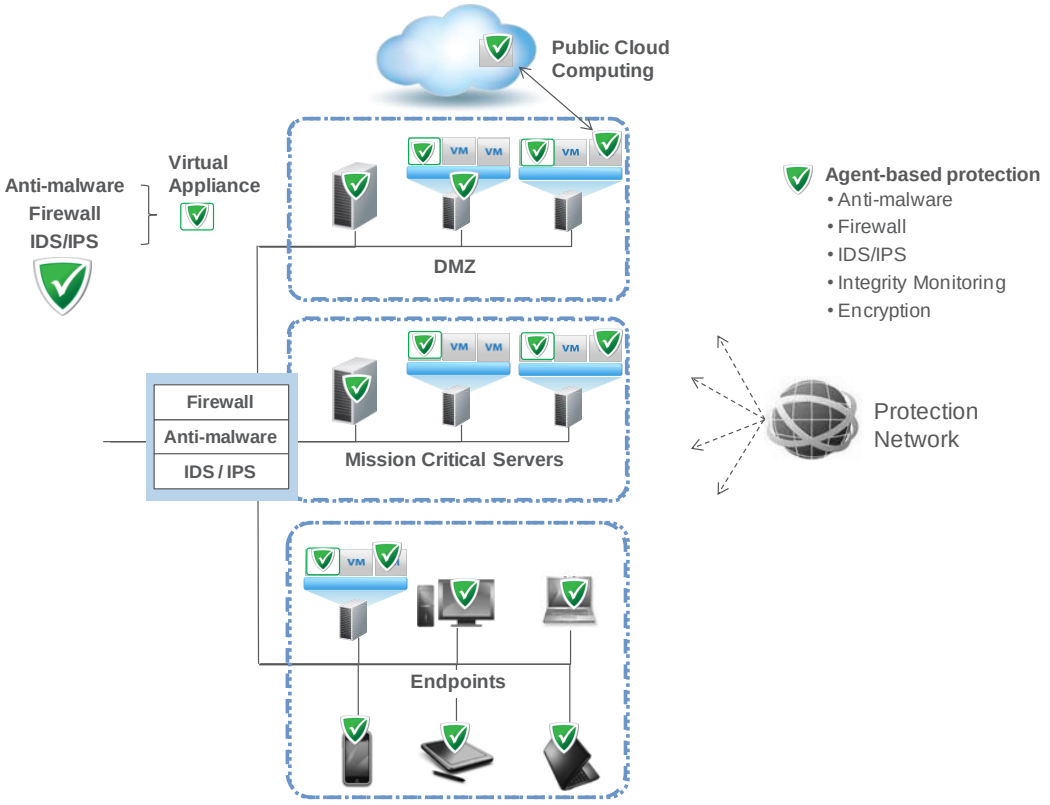


*Figure 3. When organizations move toward virtualization, the traditional network model becomes less relevant, and security must be extended to each logical host node. Here, a virtual appliance extends security to VMs.*

As they begin to implement virtualization, organizations typically add virtual machines (VMs) initially alongside traditional physical machines in a hybrid arrangement, as shown in Figure 3. To provide the needed security, enterprises need a virtual appliance – a software image designed to run on a virtual machine. The introduction of this appliance allows organizations to bring security into the hypervisor itself to provide more effective protection. This also allows visibility to inter-VM traffic and provides other security benefits specific to virtualization, such as inter-VM security, virtual patching for hosts that are created, and efficiency of anti-malware module performance.

The virtual appliance is deployed to protect each VM behind it. Each physical machine now operates almost like a network. Because organizations tend to put similar applications on the same physical machines, deployment of a virtual appliance enables organizations to set more granular security rules on that virtual edge, compared to the overall data center perimeter security rules. This also simplifies operation of perimeter firewall/IDS/IPS rules editing. At the same time, this arrangement enables “agentless” protection for the entire virtual network segment. This improves performance for the overall structure and provides essential security in case the host security agent is not yet deployed or missing because of a platform limitation. The virtual security appliance also can provide the network admission

control (NAC) function; it can inform or alert an administrator, or prevent a VM that does not have proper security treatment from being initiated or moved onto a server.

Hence, as the data center consolidates, the new security model emphasizes defense in depth, where:

1. Perimeter security, such as the traditional firewall/IDS/IPS, remains at the front line, mainly defending against the outside-in attack – attempts to penetrate the first line of defense from outside.

2. Virtual appliances on the virtual network edge handle more granular security rules, especially related to application security and virtual shielding. This not only enhances perimeter security but also reduces the frequency of changes needed to the perimeter devices. This layer also provides essential security in case a host security agent is not deployed.

3. A host-based security agent on each of the hosts dynamically senses and changes the security policy as the computing/workload moves, for example, from inside the corporate network, to roaming outside the corporate network, or to another data center or to the cloud.

This approach raises the concept of "dial-it right" security. Security that is "dialed up" to increase protection consumes system and IT staff resources, but security that is "dialed down" reduces protection while preserving system and IT staff resources. Considerations that influence the level of security needed include regulatory requirements, the sensitivity/confidential nature of the data, and security policies. Finding the appropriate balance on a case-by-case basis is easier to do as the protection is implemented closer to the target destination of the incoming

## Radical Transformation at the Endpoint

Virtualization is bringing a radical transformation at the endpoint. Before virtualization, a user's activity was linked to a single physical desktop or laptop node, which was secured by an installed agent. Today, desktop virtualization – which is running the desktop in the data center – is a reality. But the desktop changes are much more extensive than the transfer of the desktop operating system (OS) and applications into a VM in the data center. The desktop is being disassembled on the backend intrusion detection and prevention with OS, applications, and user personas discretely managed and stored – only to be recomposed via the network into what appears to be the familiar workspace for each user at log-in. The OS is further decomposed into base images common to other users, and "deltas" unique to each user. Applications appear to be local, but they can be streamed into the workspace while actually running on another VM or as a software-as-a-service (SaaS) application in the public cloud.

This workspace is now accessed by a physical client that is increasingly remote and mobile. The trend that began with thin terminals is expanding to iPads and other tablets, smartphones, and Build Your Own (BYO) PCs. The accessibility of the virtual desktop from multiple locations and devices has expanded the user workspace to be everywhere and anywhere. The desktop is now mobile, ubiquitous, thin, and heterogeneous.

The user session now defines the desktop and spans multiple network locations within the data center and remotely out across the WAN. Hence, an agent can no longer reside in a single location and provide coverage of the desktop; endpoint security must now span multiple network locations.

traffic. The reason is that perimeter security must scan all traffic entering the network – a difficult task because various types of traffic, such as Linux-, UNIX, and Microsoft Windows-based traffic, are bound for different parts of the network for different purposes. But scanning closer to the target can be more granular, because only specific types of traffic are appropriate for the target, such as only Linux traffic for traffic bound to that platform. For this reason, virtual appliance scanning can be more efficient; the virtual appliance is closer to the target destination than a perimeter scanning device.

## V. CLOUD COMPUTING

Virtualization is a catalyst to cloud computing; for example, it is accelerating transformation of data centers into private clouds. As organizations move toward cloud computing, they are able to move applications from their resources to cloud resources and back, to achieve business benefits.

However, taking advantage of this computing power further strains the security model. Agents are needed, as discussed above, that move with the workload, which includes the operating system, applications, and data. Yet business requirements such as stringent regulatory compliance require more sophisticated "smart" agents that can adjust the level of protection to suit various tasks. Enterprises are experiencing significant pressure to comply with a wide range of regulations and standards such as Payment Card Industry Data Security Standards (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), and Gramm-Leach-Bliley Act (GLBA) in addition to auditing practices such as Statement on Auditing Standards (SAS70) and International Organization for Standardization (ISO) standards. Enterprises need to prove compliance with security standards, regardless of the location of regulated systems, including on-premises servers, on-premises virtual machines, and off-premises virtual machines running on cloud computing resources.

As a result, anti-malware, firewalls, and IDS/IPS are not sufficient in agent-based protection (see Figure 3). Some of the regulations listed above include requirements for encryption to protect critical information such as cardholder data and personally identifiable information. This may include full disk encryption (FDE), Advanced Encryption Standard (AES) security, and Federal Information Processing Standards (FIPS) 140-2 compliant security. The multi-tenant nature of the cloud amplifies these requirements. Integrity monitoring of critical operating system and application files is also needed to detect malicious or unexpected changes that could signal compromise of computing resources. And log inspection is needed to provide visibility into important security events buried in log files in cloud resources. Table 1 shows that the security controls used in the traditional approach are also needed in a new hybrid cloud environment.

| Security Control | Traditional Network : (Walled Garden) | New Network: (Hybrid Cloud) |
|---|---|---|
| Firewall | ✓ | ✓ |
| IDS / IPS | ✓ | ✓ |
| Web Application Protection | ✓ | ✓ |
| File integrity monitoring | ✓ | ✓ |
| Log inspection | ✓ | ✓ |
| Ant-malware | ✓ | ✓ |
| Encryption | ✓ | ✓ |
| Messaging | ✓ | ✓ |
| | | |

*Table 1. The security controls used in the traditional approach are also needed in a new hybrid cloud environment.*

## VI. TREND MICRO'S VIEW

To provide effective security in the virtualization and cloud computing age, next generation security should include an optimal combination of approaches that protects traditional physical resources, virtual resources, and workloads wherever they may be, including in the cloud (see Figure 4). The Trend Micro Smart Protection Network™ provides oversight and ensures that all resource and workload agent protection is resilient and up-to-date. Security moves with workloads, as needed, and security is deployed on the hypervisor to protect all guest operating systems from a single location.

# A BRAVE NEW (SECURITY) WORLD: HOW SECURITY IS CHANGING TO SUPPORT VIRTUALIZATION AND CLOUD COMPUTING

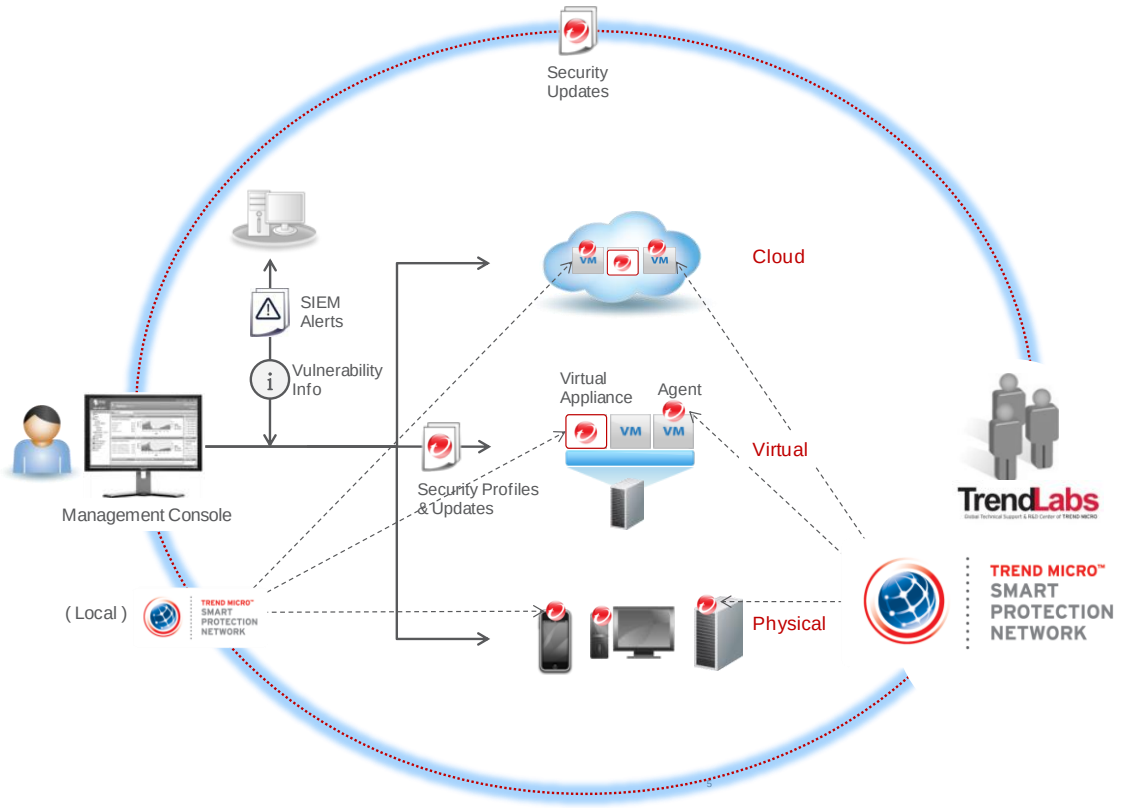


*Figure 4. Trend Micro's vision of next generation security includes an optimal combination of approaches that protects traditional physical resources, virtual resources, and workloads wherever they may be, including in the cloud.*

The host will provide most of the needed security functionality in a virtualized, and ultimately, cloud computing environment. These host-based security controls will represent the virtualization of security. This means, for one, that security will need to keep up with the instant provisioning that is the hallmark of virtualization. But this can be turned into an opportunity, because a defined security policy can be implemented immediately as each new device is provisioned. This is an example of how virtualization offers an enormous and exciting opportunity to further enhance security. This evolution of security also provides opportunities to avoid downtime as a result of infection or security breach, hence maintaining business continuity and helping ensure regulatory compliance.

In this host-dominated paradigm, the security vendors that have experience designing and implementing host-based security are likely to be best positioned to offer this expanded and enhanced virtualized security to organizations. Designing security for large numbers of hosts and endpoints is completely different than designing security for a network. Vendors with extensive experience addressing the specific needs and opportunities of host-based security, as well as developing best practices in this space, are likely to lead the next generation of security.



TREND MICRO™

This shift will change how IT dollars are spent on security; host-based solutions will gradually receive more attention and spending. But the shift will not occur overnight. The migration of firewalls to the desktop took about ten years; the evolution of traditional networks to first virtualization and then cloud computing will take time.

## VII. CHARACTERISTICS OF NEXT GENERATION SECURITY STRATEGY

Trend Micro delivers on the promise of a next generation security strategy – one that will enable enterprises to fully realize the substantial business benefits and cost savings of virtualization and cloud computing – with the following commercially available elements today:

- **Cloud architecture:** Security should be architected from the ground up to integrate with and leverage virtualization and cloud computing technologies and models.
- **Mobility**: In a world driven by increasing mobility, such as 3G networks, vMotion, and cloud computing, and the consumerization of IT such as smartphones and tablets, security must be mobile too. It must travel with the data, applications, and devices it is entrusted to protect.
- **Thin endpoint**: The endpoint protection presence must be as small as possible to fit on smaller/thinner devices such as virtual machines, smartphones, and USB-based devices, and consume fewer resources such as memory, CPU time, and I/O.
- **Speed**: Security must be fast to provision, quick to update – given the pace of discovery of new threats and vulnerabilities, and the speed with which virtual machines can be provisioned or moved from a dormant to active state – and impose a minimal impact on system performance.
- **Simplicity**: Security should be simple to operate; easy to integrate with existing solutions and IT infrastructure; and include automation, notifications, reporting and other features that reduce management and maintenance time.
- **Breadth of protection**: A broad range of fundamental security controls – including anti-virus, encryption, data loss prevention (DLP), firewalls, IDS/IPS, file integrity monitoring, and log inspection – should be virtualized and operate seamlessly in virtualized and cloud computing environments. Point security solutions are not sufficient.
- **Effective, accessible, supported, and compliant protection**: Given the trend towards consumerization, and buy-your-own-computer provisioning models, security solutions should be both globally available and readily accessible to consumers, provide effective protection, be aligned with corporate IT standards, and be backed by global support.

- **Policies and controls**: Because most enterprises will need to support a hybrid model of physical, virtual, and cloud computing resources for the foreseeable future, security policies and controls should be consistently available and expressed across these different environments.

## VIII. TREND MICRO SOLUTIONS

Advanced solutions specifically designed to secure this environment can decrease risk, increase performance, simplify management, and ultimately future-proof data center security. To this arena, Trend Micro provides security built for virtualization and cloud environments. Trend Micro delivers leadership in safeguarding data, forward-thinking technology such as the Trend Micro Smart Protection Network™, and solutions that ensure business continuity and regulatory compliance. Trend Micro offers the following solutions in this area:

- Trend Micro™ Deep Security provides advanced protection for systems in the dynamic data center – from virtual desktops to physical, virtual or cloud servers. Deep Security combines intrusion detection and prevention, firewall, integrity monitoring, log inspection and anti-malware capabilities in a single, centrally-managed enterprise software solution. The solution can be deployed in both agentless (virtual appliance) and agent-based configurations.

- Trend Micro™ SecureCloud™ is a hosted, key-management and data-encryption solution designed to protect and control confidential information deployed into public and private cloud-computing environments. Efficient and user-friendly, SecureCloud helps ensure regulatory compliance, plus it provides the freedom to move between cloud vendors without being tied to any one provider's encryption system.

- Trend Micro™ OfficeScan™ delivers protection for virtual and physical desktops on and off the corporate network. It is the industry's first Virtual Desktop Infrastructure (VDI) optimized endpoint security solution. It accelerates protection, reduces resource use, and applies virtual patching.

- The Trend Micro™ Smart Protection Network™ infrastructure delivers advanced cloud protection, blocking threats in real-time before they reach users. Leveraging a unique, cloud computing 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.

- Trend Micro™ Mobile Security protects smartphones and PDAs from data loss, infections, and attacks from a central enterprise console that can also manage desktop protection.

Trend Micro security products are proven, reliable, and ready to use, as certified by third-party authorities. For more information, visit www.trendmicro.com/virtualization.

## IX. NEXT STEPS

Enterprises that are seeking help to support their virtualization and cloud computing initiatives should ask their vendors these key questions:

- How and when did the vendor support the latest virtualization security APIs from VMware and other market-leading vendors?
- What is the vendor's consumer mobile security product roadmap? Do they have solutions that protect tablets, smartphones, and other mobile devices?
- What is the vendor's cloud-client architecture? How do they leverage cloud computing to deliver more effective protection?

The transition to virtualization and then cloud computing will result in hybrid IT arrangements that can create security vulnerabilities and complexities. The moderate to lengthy duration of this transition period for many enterprises necessitates working closely with a security partner to help ensure provision of effective security during all stages in the transition. This vendor should offer a strong track record of host-based security – because virtualization and cloud computing security will primarily reside at the host – and present a thoroughly-considered vision of the future.

## X. CONCLUSION

The IT world is evolving rapidly, and consumers/employees are adopting emerging mobile devices almost overnight. Mobility is king. And enterprises seek to reap the benefits of virtualization and cloud computing sooner rather than later. As a facilitator of these changes – and to help ensure that enterprises realize the available benefits – security can smooth the ride through upcoming difficult transitional periods. To do this, the locus of security is shifting from the network to the host. As the leading provider of host-based technology solutions for 22 years, Trend Micro is uniquely positioned to guide industry leaders during these challenging times.

## XI. FOR MORE INFORMATION

For more information, visit www.trendmicro.com/virtualization

## XII. ABOUT TREND MICRO

Trend Micro Incorporated, a global leader in Internet content security and threat management, aims to create a world safe for the exchange of digital information for businesses and consumers. A pioneer in server-based antivirus with over 20 years experience, we deliver top-ranked security that fits our customers' needs, stops new threats faster, and protects data in physical, virtualized and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology and products stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit www.trendmicro.com.

Please visit www.trendmicro.com.

## XIII. REFERENCE

1. “ATV: Virtualization Reality,” Gartner research report. ID number G00205779, July 30, 2010.