White Paper

The Continuing Evolution of Virtualization, Cloud Computing, and Information Security

By Jon Oltsik

April, 2012

This ESG White Paper was commissioned by Trend Micro and is distributed under license from ESG.

Contents

Executive Summary

According to ESG research, increased use of server virtualization is a top priority for 2012; more than 60% of large and small organizations will increase spending in this area. Why? Because its optimization and efficiency benefits are measurable and real. Given this, many firms plan to expand their use of virtualization by increasing the number of virtual servers in use, virtualizing applications, and moving forward with virtual desktop projects.

This progress is part of a multi-year journey from IT virtualization to an increasing use of cloud computing. In fact, ESG research indicates that 46% of organizations are using SaaS today, 27% consume IaaS, and 23% are already utilizing PaaS.

Resource optimization, efficiency, and flexibility will improve through this transition, but IT security can also progress. This paper concludes:

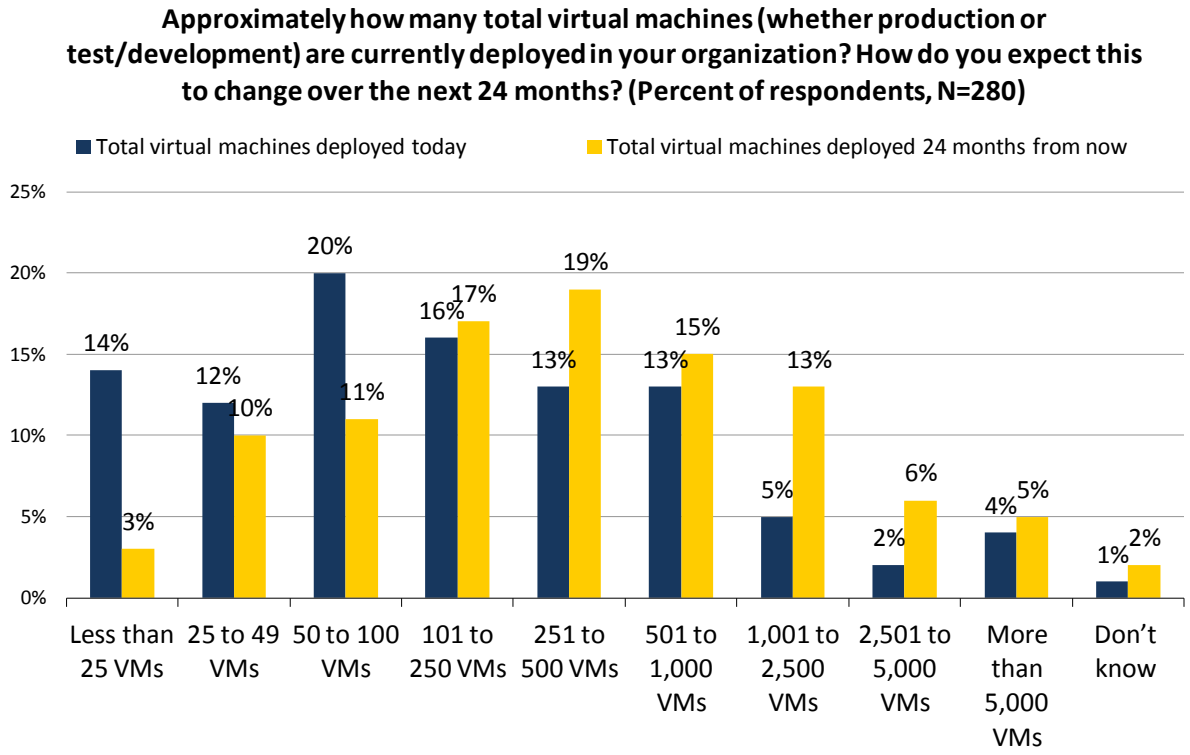
- **Virtualization is the "on ramp" for the journey to the cloud.** Thus far, virtualization projects remain focused on workload consolidation. Moving forward, IT organizations will use these experiences as the "on ramp" where virtualization experience culminates in dynamic public/private cloud computing. To reach this destination, they will proceed through three phases: an enterprise phase where virtualization skills and tools align virtualization technologies with mission critical systems, a private cloud phase where technology silos and IT organizations merge to take advantage of the automation and mobility of virtualization and create real private clouds, and a dynamic cloud phase where private clouds and individual workloads interoperate seamlessly with community and public clouds.
- **Security concerns—and misinformation—remain.** While the benefits of virtualization and cloud are understood, real security issues and virtualization security knowledge remain elusive. Risk-averse security professionals believe that virtualization does not map with existing physical security controls. They don't understand the security safeguards designed into virtualization technologies and are unaware of many advances in virtualization security technologies and tools.
- **Security can improve through each step of the journey.** As the journey to the cloud progresses, CISOs' concerns will be addressed one by one. During the enterprise phase, security vendors will take advantage of APIs, standards, and partnerships to deliver new solutions with virtual form factors and intelligence. As the private cloud phase begins, security vendors will tightly integrate with virtualization management for automation, monitoring/reporting, policy management, and command-and-control. Finally, in the dynamic cloud phase, in-house security organizations will be able to enforce security policies or monitor security events in private and public clouds. The important point here is that, with the right planning, training, and technology implementation, the move to virtual IT can actually improve security defenses, increase visibility, automate operations, and decrease costs.

Virtualization Remains a Top Priority

The data is clear: Virtualization technology remains a top IT spending priority for 2012. Why? The obvious reason is that virtualization technology offers a multitude of operational and cost benefits. Organizations continue to use server and desktop virtualization to centralize IT resources, improve hardware optimization, reduce system maintenance, and streamline IT operations. Given current virtualization benefits and impending cloud computing strategies, most organizations will ramp up their use of virtualization technology at an aggressive pace. Over the next few years, many enterprises will deploy many hundreds—or even thousands—of VMs (see Figure 1).[1]

[1] Source: ESG Research Report, *Data Center Networking Trends*, January 2012.

Figure 1. Server Virtualization Use Will Increase Over the Next 24 Months



Source: Enterprise Strategy Group, 2012.

A Stepping Stone to the Cloud

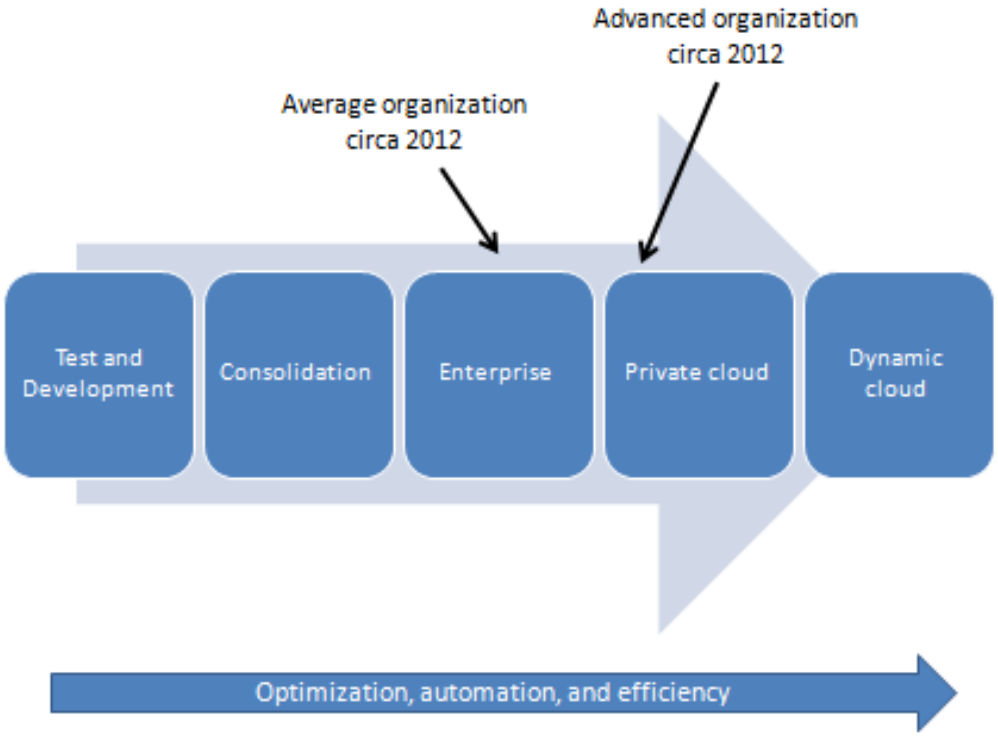
Clearly, virtualization is becoming an increasingly core technology for enterprise IT. Most companies currently use it for test/development and server consolidation. Many are also migrating business-critical enterprise applications to virtual servers or developing new applications for virtual infrastructures. All this activity, however, is just the beginning.

Virtualization technology is evolving rapidly, driven by innovation, technology industry cooperation, and new types of IT skills. Furthermore, this maturation makes virtualization an essential foundational technology for cloud computing. As of 2012, many organizations will use virtualization technologies as a stepping stone as they proceed through the three distinct phases of the "journey to the cloud" (see Figure 2).

1. Enterprise phase
2. Private cloud phase
3. Dynamic cloud phase

IT optimization and efficiency improve through each phase as integration and automation replace "islands of technology" and manual operational tasks.

Figure 2. From Virtualization to Cloud Computing



Source: Enterprise Strategy Group, 2012.

Enterprise Phase

During the test/development phase, virtualization technology was mostly used by software development and engineering groups. In the consolidation phase, virtualization technology was primarily utilized by system and application administrators. This isolation transitions through the enterprise phase as virtualization becomes a unified IT building block and impacts the entire IT organization—networks, management tools, and security enforcement safeguards must be able to distinguish between physical and virtual assets and respond accordingly.

To proceed gracefully through the enterprise phase, advanced organizations are:

- **Assessing their IT inventory.** Historically, IT infrastructure was deployed organically by disparate business units and IT groups. This leads to a potpourri of assets and configurations like operating system revisions, development tools, network VLANs, etc. The move to virtualization/cloud provides a great opportunity to rationalize IT assets and configuration variety. To move forward most efficiently, IT managers should get their arms around this wide assortment and make some hard decisions about corporate standards, upgrades and technology choices, and strategic vendors.
- **Rethinking the IT organization.** To preserve functional technology benefits while capitalizing on virtualization and cloud computing, IT organizations must collaborate more closely than in the past. This means cross-training all of IT on virtualization technology with a focus on the overlap of functional technology expertise. Savvy CIOs will go one step further and make necessary organizational and compensation changes to get all of IT on board. For example, IT groups should be organized and compensated based upon virtualization and cloud computing deployment projects and business services rather than functional technology metrics alone.

- **Pushing vendors on virtualization support.** To increase benefits and achieve success, virtualization projects need to be supported by surrounding technologies like networking, IT management, and security. IT managers should assess vendor commitment to virtualization/cloud computing, partnering with those that are on board and eliminating the laggards.

Private Cloud Phase

The enterprise phase creates an infrastructure where many IT assets move from physical to virtual. With this foundation, large organizations can then construct their own private clouds offerings. With the help of cloud orchestration platforms like Eucalyptus and OpenStack, IT infrastructure can offer real cloud-like agility with services like on-demand provisioning, rapid elasticity, location-independent resource pooling, and pay-per-use accounting.

As this transition occurs, CIOs will need to plan for:

- **Massive scale.** According to ESG research, most organizations run approximately five to ten virtual machines per physical server today. As hypervisors and server hardware advance, this ratio will grow precipitously. Soon, IT will be responsible for exponentially more virtual assets than the physical assets they currently manage. IT managers must plan for this while seeking out new solutions that take advantage of virtual asset and network ubiquity to help IT monitor, manage, and secure asset sprawl while improving optimization and efficiency.
- **VM mobility.** While tools like VMware VMotion are already in use, the private cloud phase depends upon ubiquitous VM mobility across banks of servers and geographically distributed data centers. CIOs should ensure that VM mobility is constantly monitored, governed by tight processes, and supported by all of the elements making up the IT infrastructure. Furthermore, networks must be capable of moving latency-sensitive applications from place to place without disrupting business operations.
- **New levels of automation.** Self-service and pay-as-you-go models demand tight IT integration as well as new tools for command-and-control, monitoring, and chargeback. IT managers will need support from existing vendors as they integrate multiple applications and evaluate new add-on options for some of this burgeoning functionality.

Dynamic Cloud Phase

In this final and ongoing phase, private clouds will join others to form community clouds between partners, integrate with external service providers as hybrid clouds, or be completely replaced by public cloud services. The technology underpinnings will be in place to make this happen, but CIOs should also consider:

- **IT business decisions.** At this juncture, virtualization and cloud computing technologies effectively bridge internal and external IT options. When this happens, IT decisions can be viewed through a more focused business lens. Smart CIOs will immediately offload non-critical applications and closely scrutinize the cost of public cloud computing options for every new IT initiative.
- **Standards.** Rather than simply moving workloads to the cloud, many applications will run on-site and in the public cloud simultaneously. Without standards, this could result in difficult deployments and make it virtually impossible to change public cloud providers once in place. Insist on standards to obviate this burden.
- **Extending management tools into the cloud.** Enterprise-based management systems will be called upon to manage resources regardless of their location. For example, when a server moves from the data center to a third-party facility, tried and true enterprise security tools will track this movement, ensure policy enforcement, and monitor and report on cloud-based activities for security analysts and compliance auditors. Make sure that all management tools support virtual form factors that can move around the cloud with virtual applications and data.

What about Security?

The ESG virtualization and cloud lifecycle provides a roadmap built upon virtualization with the ultimate destination of ubiquitous cloud computing. This phased process addresses existing issues around virtualization skills and technology complexity, but what about security? Good question, as this is a major hurdle that can't be ignored. According to a recent ESG survey, 28% of IT professionals believe that security issues are actually holding organizations back from using virtualization technologies while over 40% say that security concerns limit their use of cloud computing throughout the enterprise.

Which security issues are frightening CISOs? ESG believes that the primary concerns include:

- **Hypervisor security.** Since hypervisors are a common gateway for all VMs residing on a server, some security professionals are worried about hypervisor security. For example, a hypervisor-based root kit could "hyperjack" the hypervisor, exposing all resident VMs. Similarly, an adversary could launch a VM escape attack where a VM could break free from the hypervisor and interact with all other resident VMs. While some of these exploits have not been seen "in the wild," security professionals realize that it is only a matter of time.
- **Virtualizing security zones.** Many business applications and IT services are protected in security zones, surrounded by security controls such as firewalls, IDS/IPS, gateway filters, and Access Control Lists (ACLs) for security policy enforcement. Security professionals may wonder how they can recreate these controls in a virtual environment in order to provide adequate protection for virtualized applications with different trust levels residing on common servers.
- **Instant-on gaps.** Since physical systems take time to deploy, security professionals are generally confident that they have ample checks and balances to ensure that new servers are provisioned with the right security safeguards. With virtualization, however, days and weeks needed for provisioning turn into a few keystrokes. CISOs worry that automated instantiation of VMs may circumvent security processes and leave VMs—and critical corporate assets—unprotected. VMs can also be left dormant, reactivated, easily cloned, or moved around the network. CISOs need to ensure that security can be coordinated across the network to ensure that all VMs adhere to security policies and minimize risk.
- **Resource contention.** Security tools, like malware protection, depend upon CPU cycles, memory, and storage resources for pattern matching, system scans, and signature databases. Running traditional anti-malware software for each VM not only wastes resources, but can also cause system contention. This tends to happen when a central scheduler launches simultaneous system scans on multiple VMs collocated on the same server. In this scenario, security scanning activities immediately consume massive amounts of CPU and memory, thus usurping resources from application workloads. This can have a profound impact on system performance while also limiting VM per physical server consolidation ratios.
- **Cloud data security.** Mention cloud computing and CISOs worry about data confidentiality, integrity, and availability. Why? By its very nature, cloud computing is designed for multi-tenancy and shared infrastructure, which could expose private data to accidental or malicious breaches. Security executives become extremely concerned about these inherent risks combined with immature cloud security controls and oversight.
- **Visibility and reporting.** Security and monitoring tools for threat management, event detection, and regulatory compliance always viewed the world in terms of physical assets in the past. When physical servers become VMs running side by side on the same server, many tools can't distinguish one virtual server from another.

These legitimate concerns are already impacting virtualization and cloud deployment progress. For virtualization and, ultimately, cloud computing to deliver on their promised benefits, security gaps must be addressed.

Virtualization and Cloud Computing Security Evolution

Yes, many of these security concerns are real, but fortunately, security is a "top of mind" issue for security vendors—not just CISOs. Rather than leaving security as an afterthought, virtualization, cloud computing, and security vendors are designing security into products, opening security and virtualization platform APIs, integrating solutions, and building virtualization intelligence into security technology defenses. The goal? Bake security protection into virtualization and cloud computing technology itself. This effort will ultimately make virtualization/cloud computing MORE secure than legacy technologies and also transition today's stovepipe and laborious security operations to a new efficient and automated cloud computing model.

How long will it be before virtualization and cloud computing security surpasses traditional defenses? Good news: it is already happening. First off, virtualization technology design offers some immediate security benefits. It can be used to standardize VM images and centralize server provisioning, helping to eliminate error-prone manual processes and reduce patch management cycles. Furthermore, large organizations can use mobility tools like VMware vMotion and versioning to create and back up versions of critical VMs more frequently than in the past. This can make recovery far more straightforward than with physical systems. Finally, virtualization and cloud computing security is rapidly improving through the efforts of leading virtualization and IT security providers.

As an example of industry cooperation, virtualization veteran VMware, along with security leader Trend Micro, is actively addressing the specific security issues described above by:

- **Shrinking the hypervisor footprint to minimize the attack surface.** Past hypervisors like VMware ESX were based upon 2 GB Linux-based operating systems. This provided lots of functionality, but also a large attack surface for hackers and cybercriminals. VMware has removed the OS management console in its ESXi hypervisor, placing necessary management functionality directly in the core kernel. This served to shrink the code base dramatically—ESXi is now only about 100 MB. This change also helped reduce the number of hypervisor vulnerabilities and patches, streamlining security operations.
- **Virtualizing the security perimeter.** To address server trust levels and security visibility, Trend Micro's Deep Security product now provides firewall, IDS/IPS, and integrity monitoring controls at the VM level. In essence, this creates a security perimeter around each VM, allowing large organizations to virtualize existing security zones, collocate applications with different trust levels, and optimize server hardware investments. Beyond traditional OS and network security safeguards alone, Trend Micro Deep Security also offers a Web application firewall at the VM level.
- **Linking security and VM provisioning and management.** Trend Micro deploys a dedicated virtual appliance on each host physical server and integrates with VMware vCenter so that when a new VM is provisioned, Trend Micro tools immediately provide an umbrella of pre-defined protection at the VM level. Trend Micro's virtual appliance also ensures that dormant, reactivated, and cloned VMs are instrumented with the right security controls for policy compliance. Non-critical VMs may be configured in "alert mode," sending a message to security administrators upon detecting suspicious behavior, while business-centric applications can be provisioned in IPS mode to immediately block malicious activities between collocated VMs or between VMs and the network. Additionally, virtual patching provides security controls that can be configured to shield VMs from known and unknown vulnerabilities, eliminating the need for patching fire drills and downtime. All of this protection, including IDS/IPS, firewall, file integrity monitoring, Web application protection, and anti-malware, can also be provided without an agent footprint on the VM for flexibility in deployment configurations.
- **Aligning security with virtual intelligence.** To overcome the resource issues of running security software on each VM, VMware introduced vShield Endpoint for virtual data centers and cloud environments. Rather than implement a security agent on each VM, vShield enables the creation of a single virtual security appliance that acts as an endpoint security proxy for other VMs using a small footprint VMware driver. This simplifies virtualization security deployment and minimizes the server resources needed. Trend Micro works with vShield Endpoint to offer agentless, virtualization-aware anti-malware and file integrity monitoring. When two collocated VMs are scheduled for simultaneous scans, Trend Micro staggers

scanning activity to curtail resource utilization. In addition to vShield Endpoint, Trend Micro also integrates with other VMware APIs to provide network-level protection with IDS/IPS, firewall, and Web application protection without requiring a security agent footprint on the VM.

- **Encrypting cloud data.** To secure data in shared resource and multi-tenant environments, Trend Micro enables sensitive data encryption and key management control by the data owner rather than corporate IT or public cloud providers. When encrypted data needs to be processed, cloud services automatically ask the data owner for an encryption key to proceed. Of course, this also demands the type of distributed, advanced, and intelligent key management provided by Trend Micro products.
- **Providing granular visibility for security monitoring and reporting.** Through VMware's APIs, Trend Micro can collect VM-level operating system and application logs and monitor all VM-to-VM traffic across virtual switches. In this way, data center and cloud computing security specialists have immediate visibility into security events and suspicious insider behavior. Once these events are detected, organizations can then use Trend Micro and VMware tools to assess problems, remediate systems, and develop rules to block similar incidents in the future. Aside from incidence response, this visibility can also help align virtualization and cloud computing security with regulatory compliance requirements and reporting needs.

Table 1. VMware and Trend Micro Address Security Concerns

Security Concern	VMware and Trend Micro Solution
Hypervisor security	VMware ESXi shrinks the hypervisor footprint from 2 GB to 100 MB. Also minimizes vulnerabilities and patching.
Physical security trust zones cannot be emulated in virtual technologies	Trend Micro provides security controls like firewalls, IDS/IPS, Web application protection, and integrity checking at the VM level.
Rapid VM provisioning and dormant, reactivated, or cloned VMs may lead to the creation of vulnerable, unprotected VMs	Trend Micro provides a dedicated security virtual appliance that integrates with vCenter to detect newly provisioned VMs and ensure that all VMs have up-to-date security, protecting them with specific configurable security controls.
Security technologies consume excessive server resources	Trend Micro integrates with vShield Endpoint and other VMware APIs to eliminate the need for security software or agents on each VM and conserve resources.
Data is vulnerable in the shared resource environment of the cloud	Encryption with policy-based key management and server validation keeps data that is stored in the cloud secure.
Security technologies can't monitor security or compliance controls at the VM level	Through VMware APIs, Trend Micro can monitor VM-level activity and all VM-to-VM traffic within a physical server.

To further secure virtual systems, virtualization and cloud computing security technologies should be supported by best practices. This means hardening hypervisors and VMs, creating a defense-in-depth virtual architecture, setting up tight access controls for VMs, and taking advantage of specific virtualization administrative controls.

Security Improvements Will Continue

The security progress described above is just the beginning. Relating these security advances back to ESG's "journey to the cloud," advances made by VMware and Trend Micro fit into the enterprise and private cloud phases of the lifecycle. Moving to the dynamic cloud phase, ESG expects:

- **Increased automation.** Automated security controls are currently part of IT's process for VM provisioning. In the future, this will extend to user self-service as well. Users of private or public clouds will be provided with simple security choices that include basic descriptions of each level of protection and associated prices. In this way, security controls will be provisioned and billed without any IT intervention.

- **Greater use of VM identity management.** As VMs continue to proliferate, IT and cloud providers will need better tools to identify individual VMs and associate them with their properties and privileges. ESG believes this requirement will drive tighter identity management of VMs. This identity infrastructure will likely be built on top of two existing technology underpinnings: some form of PKI (or identity-based key generation) and the Open Virtualization Format (OVF), a platform independent, efficient, extensible, and open packaging and distribution format for virtual machines. Trend Micro is actually ahead of the field with security and identity integration. For example, Trend Micro SecurityCloud checks the identity and security status of authorized servers before releasing encryption keys for decryption of sensitive data on a local or cloud-based VM.
- **Greater data integration and visibility.** To preserve an end-to-end view of IT security, public cloud providers must be able to share data with enterprise customers and provide transparent visibility into the IT assets consumed. This calls for standard security data formats, secure and trusted data exchange, and new scalable tools with advanced analytics and visualization capabilities. Trend Micro Deep Security is being designed for this type of use case.

Anchored by current security advances like those driven by VMware and Trend Micro, ESG expects security improvements at an increasing pace. As large organizations rationalize and standardize their IT portfolios, establish a foundation of virtualization/cloud computing best practices, and implement new technologies, security protection and efficiency will continually improve.

The Bigger Truth

A few things discussed in this paper are absolute certainties. Virtualization technology has become an IT staple for organizations large and small as it delivers optimization, operational, and cost benefits. This will continue as plenty of server workloads and even desktops that can be virtualized in a fairly straightforward manner remain. To maximize ROI, CIOs will virtualize all that they can.

Virtualization technology is just the beginning. IT deployment is already proceeding through a maturity lifecycle, with virtualization acting as both a foundation and stepping stone to greater adoption of cloud computing. CIOs and CISOs have a distinct opportunity through this process: each phase can increase optimization and efficiency, as well as enhance security as security technologies gain virtualization and cloud intelligence. This holds the promise to improve protection AND security automation.

For virtualization and cloud computing to reach their potential, IT managers must also roll up their sleeves for the work ahead. Current technologies and security defenses must be assessed, documented, and migrated to virtual alternatives. Staff must be educated, trained, and reorganized into more cohesive, cross-functional, project-based units. Finally, technology plans must be mapped out through the remaining phases of the maturity model. Savvy CIOs will evaluate the roadmaps and development plans of leading technology vendors so they can pick the right partners for the virtualization and cloud journey that lies ahead. With visible virtualization/cloud leadership, commitment, and cooperation, VMware and Trend Micro should be amongst the top choices as CIOs and CISOs choose their partners for their own cloud journeys.

Enterprise Strategy Group | **Getting to the bigger truth.**

20 Asylum Street | Milford, MA 01757 | Tel:508.482.0188 Fax: 508.482.0218 | www.enterprisestrategygroup.com