

White Paper

Information Security, Virtualization, and the Journey to the Cloud

By Jon Oltsik

August, 2010

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

Contents

Executive Summary	3
Virtualization Remains White Hot	3
A Stepping Stone to the Cloud.....	4
Enterprise Phase.....	5
Dynamic Phase	6
Cloud Phase	6
What about Security?	6
Virtualization and Cloud Computing Security Evolution	7
Security Improvements will Continue Throughout the Journey to the Cloud	9
The Bigger Truth	10

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of the Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at (508) 482-0188.

Executive Summary

According to ESG research, virtualization technology investments top the priority list in 2010 as nearly 60% of large and small organizations will increase their spending on virtualization technology. 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 just the beginning of a multi-year journey from IT virtualization to a future of cloud computing. ESG believes that resource optimization, efficiency, and, surprisingly, IT security will improve through this journey. This paper concludes:

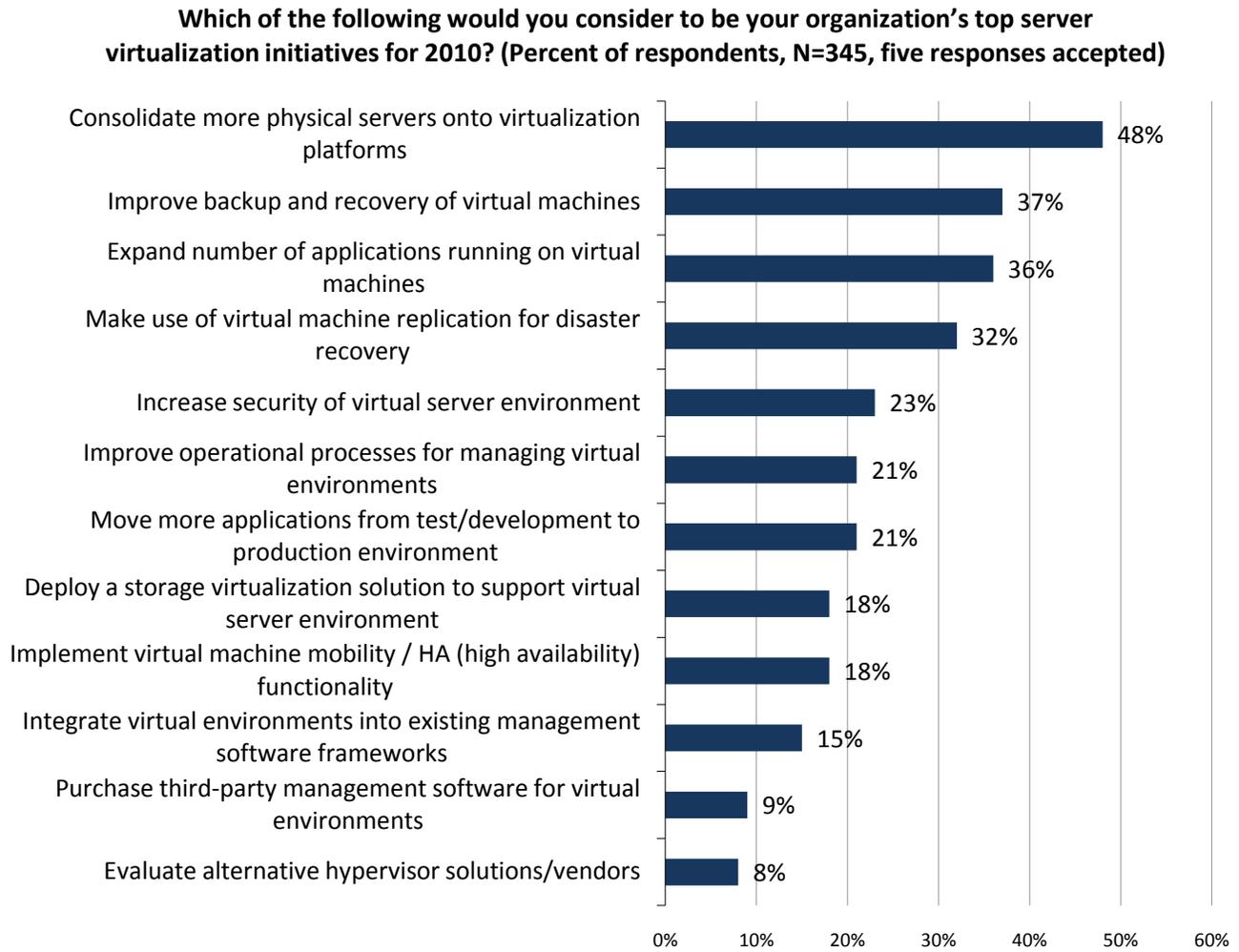
- **Virtualization is the “onramp” for the journey to the cloud.** ESG believes that thus far, virtualization projects have been focused on test and development or workload consolidation. Moving forward, IT organizations will use these experiences as the “onramp” for a virtualization journey that culminates in dynamic public/private cloud computing. To reach this destination, they will proceed through three phases: 1) an enterprise phase where new virtualization skills and tools align virtualization technologies with mission critical systems, 2) a dynamic phase where technology silos and IT organizations merge to take advantage of the automation and mobility of virtualization and create real private clouds, and 3) a cloud phase where open standard private clouds 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, understand all of the security safeguards designed into virtualization technologies, and are unaware of many new 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 dynamic phase begins, security vendors will tightly integrate with virtualization management for automation, monitoring/reporting, policy management, and command-and-control. Finally, in the 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 White Hot

The data is clear: Virtualization technology is the top IT spending priority for 2010. 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. Virtualization technology also appears to be an IT “gift that keeps on giving.” ESG research points out that IT organizations are capitalizing on virtualization technology by consolidating more servers on virtual platforms, improving backup/recovery on virtual servers, expanding the number of applications deployed on virtual servers, and using server virtualization technologies like [VMware](#) VMotion to improve disaster recovery (see Figure 1).¹

¹ Source: ESG Research Report, [2010 IT Spending Intentions Survey](#), January 2010.

Figure 1. Top Server Virtualization Initiatives for 2010



Source: Enterprise Strategy Group, 2010.

A Stepping Stone to the Cloud

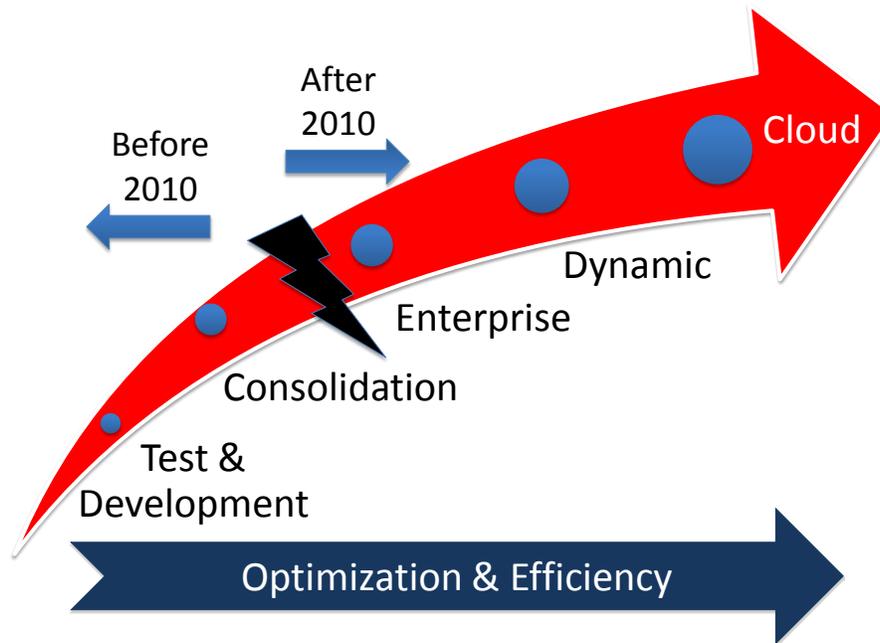
Clearly, virtualization is becoming an increasingly core technology for enterprise IT. Most companies use server virtualization for test/development and server consolidation today. Many are also migrating business-critical enterprise applications to virtual servers or developing new applications for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

ESG believes that 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 2010, 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. Dynamic phase
3. 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, 2010.

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 ends in the enterprise phase as virtualization becomes a strategic 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, smart organizations will have to:

- Assess the IT inventory.** Historically, IT infrastructure was deployed organically by disparate business units and IT groups. This means that there is likely to be a potpourri of assets and configurations like operating system revisions, development tools, network VLANs, etc. While virtualization technology could probably support most of this mess, 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.
- Re-think the IT organization.** To preserve functional technology benefits while capitalizing on virtualization and cloud computing, the IT organization must collaborate more closely than in the past. This means cross-training all of IT on virtualization technology with a focus on the overlap with their functional technology expertise. Savvy CIOs will go one step further and make necessary organizational and compensation changes to get all of IT onboard. 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.
- Push 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.

Dynamic Phase

The enterprise phase builds a virtual/cloud computing technology where most of IT becomes virtual. With this foundation, large organizations can then create their own private clouds offering on-demand self-service, rapid elasticity, location independent resource pooling, and pay-per-use accounting.

As organizations transition to the dynamic phase, 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 manage today. 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 dynamic 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.

Cloud Phase

In this final and ongoing phase, internal clouds will join others to form community clouds between partners or integrate with external service providers as hybrid clouds. 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 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 Research survey, 28% of IT professionals believe that security issues are actually holding organizations back from using virtualization technologies more prominently 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. After all, if a malicious code attack could compromise or bypass the hypervisor, all of the resident VMs could be vulnerable.
- **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 wonder how in the world 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.
- **Initial security protection.** 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.
- **Resource contention.** Security tools like malware protection depend upon processing, 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. When a central scheduler launches full system scans on multiple collocated VMs simultaneously, even the most powerful server hardware will be brought to its knees.
- **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 between one virtual server and another.

These legitimate concerns are already impacting virtualization 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 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. More recently, VMware 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 level, and optimize server hardware investment. 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.** Trend Micro 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. 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, security controls can be configured to shield VMs from known and unknown vulnerabilities, eliminating the need for patching fire drills. All of this protection, including IDS/IPS, firewall, Web application protection, and anti-malware, can also be provided without an agent footprint on the VM.
- Aligning security with virtual intelligence.** To overcome the resource issues of running security software on each VM, VMware recently 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. This simplifies virtualization security deployment and minimizes the server resources needed. Trend Micro works with vShield Endpoint to offer agentless, virtualization-aware anti-malware. 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 the VMsafe APIs to provide IDS/IPS, firewall, and Web application protection without requiring an agent footprint on the VM.
- Providing granular visibility for security monitoring and reporting.** Through VMware’s VMsafe 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, large 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 may lead to the creation of vulnerable unprotected VMs	Trend Micro integrates with vCenter to detect newly provisioned VMs and protect them with specific configurable security controls.
Security technologies consume excessive server resources	Trend Micro integrates with vShield Endpoint and VMsafe to eliminate the need for security software or agents on each VM and conserve resources.
Security technologies can’t monitor security or compliance controls at the VM level	Through VMsafe, 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 also 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 throughout the Journey to the Cloud

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 phase of the lifecycle. Moving to the dynamic and 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 with 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 and the Open Virtualization Format (OVF), a platform independent, efficient, extensible, and open packaging and distribution format for virtual machines.
- **More data encryption.** Sensitive data moving between private and public clouds must remain protected at all times. Beyond VPNs, data will be encrypted and controlled by the data owner rather than corporate IT or public cloud providers. When encrypted data needs to be processed, cloud services will automatically ask the data owner for an encryption key to proceed. Of course, this demands more distributed, advanced, and intelligent key management in the future. ESG sees this evolving through key management standards like KMIP over the next few years.

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 is being widely embraced by organizations large and small and is delivering optimization, operational, and cost benefits across the board. This will continue as plenty of workloads and even desktops that can be virtualized in a fairly straightforward manner remain. To maximize ROI, CIOs will likely virtualize all that they can.

ESG believes that virtualization technology is just the beginning. IT deployment will evolve through several phases of a maturity lifecycle as virtualization becomes a stepping stone on a journey to 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 intelligence. This holds the promise to improve protection AND security automation.

For virtualization to reach its 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. Smart CIOs will make sure to 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 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.**