Securing the Cloud for the Enterprise

A Joint White Paper from Symantec and VMware
Securing the Cloud for the Enterprise
A Joint White Paper from Symantec and VMware

Contents

Executive summary ................................................................. 1
1.0 Overview ................................................................. 2
  1.1 Enterprise computing trends .................................................. 2
  1.2 Transitions in the journey .................................................. 3
  1.3 Evolving threat and compliance landscape .................................. 4
  1.4 A security strategy for the cloud .......................................... 4
2.0 Key elements of cloud security .............................................. 6
  2.1 Infrastructure ................................................................. 6
  2.2 Information ................................................................. 7
  2.3 Identity ................................................................. 8
  2.4 Devices ................................................................. 9
3.0 Recommendations ............................................................. 10
  3.1 Virtual Infrastructure ....................................................... 10
  3.2 Private cloud ............................................................. 12
  3.3 Public cloud ............................................................. 13
Conclusion ............................................................................... 14
Executive summary
The arrival of cloud computing is changing the landscape for information technology (IT) more completely than has any trend or innovation since the first commercial use of the Internet, 15 years ago. Cloud computing redirects energy and resources that IT has traditionally consumed in operations and maintenance, turning it toward innovation that serves business—and lowers costs. The various approaches to taking full advantage of the cloud include public or private models of software, platform, and infrastructure services. These cloud approaches to information technology offer solutions to the challenges presented by device proliferation, the exponential growth in volumes of data, and the accelerated changes demanded by the increasingly fast pace of business.

But surveying the transformation of classic IT operations also reveals some of the questions that, unanswered, can impede the journey from static, tightly coupled technology "stacks" to the cloud. How do IT strategists and decision-makers balance the promises of cloud computing, be it on the public or private horizon, and the security needed to safeguard information assets and ensure regulatory compliance? While the increased agility that comes with moving to the cloud solves many current technology challenges, the journey to cloud computing also accelerates the erosion of perimeter enforcement and trust boundaries. The models for addressing cloud security are being developed, but there is often a large gulf to bridge between security policies and mechanisms for the cloud and the existing controls understood by the enterprise—and its auditors—today.

Beginning with a firm foundation in data center virtualization, a journey to the cloud takes IT to private clouds, which leverage and enhance existing technology assets. Undertaken with the right guidance and information, this journey includes an evolutionary transformation of information security in the realms of infrastructure, information, identity, and devices. In undertaking this journey to a private cloud, enterprise IT can make the right decisions about security controls that will scale to hybrid and public clouds—while establishing familiar controls for securing the sensitive information in those clouds.
1.0 Overview

1.1 Enterprise computing trends

The key trends driving the next generation of computing are virtualization, cloud computing, and mobility. The initial phase—adoption of virtualization in the data center—has been driven by the cost reductions that accompany improved server utilization. The evolution of this new infrastructure layer, from hypervisor-driven virtualization to a private cloud architecture defined by services, is enabling IT to meet business demands for increased agility and flexibility at an accelerated pace.

The on-demand and pay-per-use attributes of public clouds, including Software as a Service (SaaS) clouds, lead to widespread adoption among business units. Enterprise users also bring in a variety of mobile devices to access personal and enterprise cloud services, both inside and outside enterprise firewalls. This user-centric experience can be characterized as information on demand, delivered anywhere and to whatever device is being used. Finally, these trends are accompanied by an explosion in the quantity of data being created, shared, and managed by enterprises.

These trends are accompanied by security threats of increasing sophistication that represent a new generation of complex advanced persistent threats (APTs) such as Stuxnet and Hydraq. These exotic names are among the latest in what has been a series of concerns regarding the unintended exposure of information and the exploitation of resources that depend on IT-managed services. This continuously evolving and unpredictable threat landscape is coupled with the explosion of data and its pervasiveness across clouds and devices. These trends have created greater challenges in information protection, as the WikiLeaks incident and the Epsilon data breach indicate. Moreover, enterprises are subject to an ever-increasing barrage of government- and industry-mandated information protection standards.

Relevant concern for enabling the IT journey to a cloud computing architecture centers on unresolved questions about information security and, by extension, compliance. To make public clouds effective at the projected scale, cloud infrastructures are designed as multi-tenant computing environments. In order to serve their business needs with public cloud offerings, IT managers need to weigh the security of internal dedicated infrastructure against the improved economics of a shared cloud environment. Analysts and enterprises consistently identify these security questions as the foremost consideration of cloud adoption. To resolve these questions, it is important to identify those features of the cloud that call for a unique security strategy, in contrast to traditional data center approaches.

Of course, IT managers and business owners must incorporate the business’s specific compliance requirements into the cloud transition plan, and this document cannot directly address that challenge. Still, a good understanding of the technical requirements for securing a cloud infrastructure is a key enabler to making correct choices to assure compliance for cloud operations.

Examining these requirements we can define key principles to which security for the cloud should adhere—and from which a determination of trustworthiness may be made.
1.2 Transitions in the journey

The journey to the cloud is characterized by a series of transitions in the infrastructure used by IT to deliver services. The most powerful of these is the adoption of virtualization in the data center—and the next is the shift of IT from production of services to delivery of services. Private clouds achieve this evolutionary transition while allowing enterprises to reuse existing investments in their data centers and applications. Public clouds offer a more radical transition to an on-demand, outsourced infrastructure. A common theme running through these transitions is the loss of control and visibility from a security perspective.

Towards the Cloud: Transitions

Security: Loss of Control and Visibility

Physical Infrastructure

Silo-ed
Physical Segmentation
Static Security
Extensive Investments

Virtualization

Pooled Resources
Logical Segmentation
Collapsed Infrastructure
Preserve Legacy Investments

Private Cloud

Service Delivery
Virtual Data Center
Dynamic Perimeters
Automation
Virtual Security Appliances

Public Cloud (Saas, PaaS, IaaS)

Outsourced & On-demand Data Center
Multi-Tenancy
Mis(Trust): Provider Security Controls
Limited Visibility

IT: Production to Service Delivery

Higher Efficiency, Increased Agility
1.3 Evolving threat and compliance landscape

The threat landscape is characterized by increasingly sophisticated attacks, such as those related to WikiLeaks and those that expose subscribers to marketing and even electronic gaming networks. These attacks typically combine micro-targeting, social engineering, technical exploitation of multiple “zero-day” vulnerabilities, and the ability to defeat built-in resilience. Today, these threats tend to originate from organized crime syndicates—and, in some cases, nation states—and are targeted towards stealing intellectual property and financial assets. Traditional signature-based approaches to detecting malware are becoming less useful, and reputation-based approaches are demonstrating increasing effectiveness. The explosion of data sets being created, used, and shared places enormous strains on these traditional threat detection and information protection techniques. For example, the WikiLeaks incident demonstrates how large-scale data breaches can occur when inconsistent information classification is combined with weak access control policies and the absence of monitoring and continuous, real-time auditing.

In the public cloud, the service provider is responsible for security controls for large parts of the service stack. This has a twofold impact on enterprises securely adopting cloud services:

- Limited visibility into the cloud service providers’ security controls
- Limited flexibility in deploying additional security controls at the cloud service provider

Threats targeted at cloud providers include hijacking of infrastructure and services, exploits against service provider interfaces, and the acts of malicious insiders. Other essential characteristics of the cloud, such as multi-tenancy and its on-demand nature, also open up new avenues of attack.

At the same time, governments and industries across the world have mandated regulations and standards to protect sensitive information. These include privacy regulations for protecting personal data, such as the EU Data Protection Directive; industry-specific regulations, such as Sarbanes-Oxley and the Payment Card Industry (PCI) Data Security Standard; and regulations for safeguarding government data, such as the U.S. Federal Information Security Management Act of 2002 (FISMA). Some of these regulations—EU Data Protection, for example—also mandate geographic data residency requirements. Addressing compliance involves risk and scope assessments based on information flows, security infrastructure controls, and continuous assessments of those controls.

1.4 A security strategy for the cloud

Traditional approaches to security in the enterprise have been based on control—control of devices, of infrastructure, of information—and of processes inside enterprise firewalls. In the borderless enterprise, information resides in the cloud and is accessed from many devices outside the perimeter of the traditional enterprise.

Traditional physical infrastructure is characterized by single tenancy, physically segmented infrastructure, and static security controls at perimeters, all of which are commonly used to implement trust zones in physical infrastructure. In the virtualized environment of shared infrastructure and mobile workloads, these perimeters are constantly evolving. Security controls must therefore be available on demand in the virtual fabric, and a security policy framework is needed that can

1-Cloud Architecture, Security Guidance for Critical Areas of Focus in Cloud Computing v2.1, section 1
consistently apply the right policies to manage privilege isolations and trust zones in the presence of dynamic workloads and variable perimeter horizons. By building similar security controls and policy framework in both private and public infrastructure clouds, this approach offers a path from the private cloud to public infrastructure clouds while providing assurance of the required security and accountability.

The cloud-based enterprise is characterized by interactions among three elements: the virtualized on-premise data center, a variety of cloud services, and mobile devices. Key security and risk management concerns that are barriers to adoption of cloud computing include the following:

- **Risk assessment.** On which clouds and devices is my sensitive data residing?
- **Governance.** How do I achieve compliance (e.g., PCI) in an environment where my information and applications are distributed across many clouds?
- **Managing Entitlements.** Who has access to my sensitive data, from which devices, and from which locations? Is this access permitted, and do I have visibility of when it is exercised?
- **Devices.** Are employee devices sufficiently secured to access corporate data and applications?

New security patterns and practices are emerging to address these challenges in this cloud-based environment. These are based on IT regaining control by setting policies consistently across physical, virtualized, and private cloud, and public cloud infrastructures; acquiring visibility into policy deployment and enforcement; and, finally, auditing those policy controls. Governance, protection, visibility, and auditability are key elements to establishing confidence and trust in the cloud. These must be achieved in the increasingly scalable enterprise in a cost-effective fashion.
2.0 Key elements of cloud security
The key security constructs on the basis of which security policies will be defined and enforced are infrastructure, information, identity, and end-user devices. Residing on a combination of public clouds and on-premise virtualized infrastructure, workloads are decoupled from their underlying infrastructure. In the borderless enterprise, flexible and secure information controls require policies that use rich information classification models, federated identities, and context–based authorization.

2.1 Infrastructure
Virtualization allows all storage, compute, and networking capabilities in the data center to be aggregated into a reusable pool of resources. The evolution from siloed infrastructure to pooled resources enables dynamic allocation of applications and services, thereby offering increased agility and reduced cost through greater utilization. A private cloud model built on the strengths of the underlying virtualization model offers new opportunity to leverage visibility and control and extend it to hybrid and even public clouds, where the potential for loss of control is significant. Extending this potential for a “better-than-physical” model that leverages the virtualization hypervisor for control and visibility is a route to secure public cloud computing that serves the demands of both business owners and IT principals.
Workloads may be allocated dynamically on different infrastructure components based on scalability or high availability/disaster recovery (HA/DR) requirements, or to optimize utilization. This dynamic ability to relocate a workload’s supporting resources according to capacity and availability can be securely enabled, given the following attributes:

- **Virtualized security.** Security controls must be available across the virtual infrastructure so that workloads are consistently protected as they are motioned. This security must be available on an ad hoc basis to support dynamically constructed relationships between virtual resources such as virtual networks, virtual storage, and virtual machines (VMs). This requirement is best served when these security services are themselves delivered as virtual appliances and are available on-demand across the virtual infrastructure. For example, network security controls for isolating VM traffic within hosts must be available as VMs. They can then be automatically deployed on hosts where the workload is migrated. These controls must be optimized for the virtual infrastructure so that they minimize resource contention such as boot storms, which occur when many VMs that share a host attempt to boot up concurrently, and antivirus (AV) storms, which result from endpoint agents attempting to run concurrent scans, creating large spikes in I/O operations and compute overhead.

- **Automated provisioning and lifecycle management.** These virtual security appliances must be configured on demand when a workload arrives at a host—i.e., policies must follow the workload. This requires automated provisioning of these security services that is integrated with cloud management infrastructures. A new lifecycle context emerges for patching, configuration management, and backup and recovery. Patch management complexity increases, including the addition of a new layer—a hypervisor—for configuration and update. There is also the need to patch offline images and templates. Lifecycle management policies and tools must address this.

- **Logical security policies.** Workloads are not tied to specific devices. Thus, their security policies cannot be tied to physical devices—such as fixed IPs, Media Access Control (MAC) addresses, and subnets—either.

- **Dynamic trust zones.** A trust zone represents a collection of workloads that share common security and compliance policies. These may span a set of shifting hosts including both private and public clouds as well as physical infrastructure. Attaching policies to workloads is a steppingstone to addressing security and compliance in the public cloud; workloads can be migrated to the public infrastructure cloud as long as the same set of policies can be enforced in a consistent and visible manner. It is worth noting that physical monitoring tools lose visibility into virtual resources such as vSwitches. Visibility must be “exported” in order to integrate these two views.

### 2.2 Information

In the cloud-based environment, information flows from the physical infrastructure onto various clouds, and is then shared by many users across different devices and geographies. Data governance concerns commonly arise in the areas of IP protection (WikiLeaks, for example); regulatory governance, such as consumer privacy laws (Mass Data Privacy Law, for example); industry compliance requirements (such as PCI and HIPAA); and data mobility. A consistent set of policies is needed for compliance and governance across cloud platforms that IT may not always control. These policies are required for identifying sensitive information; controlling its transmission, storage, and use in the cloud; and sharing it among users and devices. These policies must be consistently enforced across private and public clouds and physical infrastructure.
Information classification has traditionally been used to identify and secure sensitive data, be it at rest or in motion. For instance, security controls that use information attributes can be used to monitor and control the spread of sensitive data across clouds and devices. Once sensitive information is identified, required policies can be applied to specific use cases, enabling regulatory compliance. These include storage policies such as encryption or plain text, access control policies for primary storage, transmission policies across trust zones in multi-tenant data centers, device transmission and storage policies, and data protection policies—for example, backup and retention.

Policies protecting information are organized on the basis of information attributes. In addition to basic attributes such as type, size, permissions, location, age, owner, and keywords, extended attributes—such as who has accessed a document and how often it has been accessed, what sensitive content it contains, and the document’s reputation (such as its author)—must also be considered. These information attributes are the foundational elements for classifying information, identifying sensitive content, and applying policies for securing that information in the cloud.

Given the dynamic nature of the trust zones in a multi-tenant cloud infrastructure, security on the wire is not merely an important factor for securing information; rather, it is fundamental in removing physical topology from the requirements for establishing trusted communication within a zone. The natural result is a larger quantity of data in motion that must be secured. Storage and network devices—aware of the radical changes in infrastructure hosting and placement—help to deliver this capability. When these devices combine encryption with compression, many of the conditions for enabling this transport security are met.

2.3  Identity
In the extended enterprise, many devices are being used to access a variety of cloud-based services. Traditionally IT has used enterprise identity to control user access and entitlement to a variety of on-premise information and application assets. This principle must be extended to identities at cloud service providers, controlling what information employees can access in which clouds, from which devices, and in which locations.

Federated identity for cloud computing involves:

- **Extending enterprise credentials to cloud applications and infrastructure.** Existing policy for strong password controls and unique IDs that are consistent with those used by enterprise resources prevents the use of weak or shared passwords and can enforce secure logins for corporate data.

- **Enabling single sign-on to SaaS applications and Infrastructure as a Service (IaaS) service portals.** Because of the maturity of directory services and distributed authentication mechanisms enjoyed by enterprises today, universal single sign-on can be extended to corporate-approved SaaS and Web-based applications with an approach that consolidates access and manages availability for users.

- **Expanding access controls to the cloud.** Existing role-based access control should be applicable to access of cloud resources. With internal roles extended to manage access to specific applications, only approved sales roles would have access to a customer relationship management (CRM) SaaS, and only data center administrators could access a cloud storage portal. Thus, existing mechanisms that monitor and audit access control are also enlisted in the cloud compliance effort.
For example, cloud providers offer their own identity services and entitlement models. For access control purposes, the separate cloud identities must be tied to the respective enterprise identities; further, policies must ensure that cloud provider entitlements are consistent with on-premise entitlements at all times.

Enterprise social networks are an important use case that is enabled by secure sharing of information. Context-based authorization is critical in securely sharing information across different devices outside the physical infrastructure. Context-based authorization augments user identity with attributes such as device location, device identity, and strong authentication credentials (such as second factor). Authorization policies must use such attributes to precisely control information flow between clouds, users, and devices.

Beyond user identities, authentication is also an infrastructure and platform consideration—in particular, the authentication of different layers of the infrastructure to one another. Any infrastructure must be able to determine and report its secure and authenticated state before it makes a trust assertion on behalf of the objects and sessions it hosts. Additional considerations for authentication have to do with infrastructure and applications, particularly regarding hybrid cloud implementations. This is particularly true when IaaS is combined with Platform as a Service (PaaS), because PaaS introduces another abstraction layer that obscures the underlying IaaS details.

### 2.4 Devices

Enterprise IT has traditionally exercised tight control on end-user devices supported within the enterprise. Consumerization has led a wide variety of end-user devices based on different platform technologies to be introduced into the enterprise. Further, these devices may be used to access personal as well as corporate data and services. Policies are required to enable and provision these devices, control access from them, and secure information transmission.

Device identities provisioned by mobile device management systems must be used for authentication, and these become an important attribute for context-aware authorization. The objective is not only to secure the device, but also to control access from that device based on its current security profile. For example, a corporate Windows® device may be granted full access to applications and documents on the enterprise network, whereas an off-premise iPad® may have access to documents only through secure document viewers.

Information and applications reside on devices as well as in data centers, in the cloud and on premise. Users have been trained to install natively built apps from app stores. Detecting and blocking installation of harmful third-party apps is another important policy control.

In private, infrastructure-oriented clouds it is possible to implement a technical strategy that abstracts the desktop environment from the device. Virtual desktops (VDI), one solution in this category, help to bridge current application workloads to an “any device, anywhere” use case.
3.0 Recommendations
By building on what is already in place today, it is possible to forge a path to public, private, and hybrid clouds—often with a greater ability to both assert information controls and validate their effectiveness. Each stage in the journey to the cloud has a unique set of concerns and recommendations for addressing them. People, processes, and technical controls must evolve consistently to address these concerns. Security and compliance must be addressed in a unified and consistent fashion across physical, virtual and cloud environments. These recommendations are cumulative and evolutionary—for example, those for the virtualization stage apply to the later stages as well.

Towards the Cloud: Security Recommendations

3.1 Virtual Infrastructure
The new infrastructure layer introduced by virtualization must be protected, as do the guest operating systems and applications running on it. The rapid pace at which VMs can be created, modified, and distributed breaks static physical infrastructure security models, and that must be addressed. Defense in depth requires that policies, practices, and technologies for securing traditional physical infrastructure practices be augmented to protect virtual infrastructures.
The uniform set of application programming interfaces (APIs) provided by the new infrastructure layer and the introspection capability that allows hypervisors to monitor guest operating systems offer greater potential for improved security than does physical infrastructure.

**Virtual Security: Better than Physical**

---

**Physical Security**

Expensive
- Specialized hardware appliances
- Multiple point solutions

Complex
- Spaghetti of different rules and policies

Rigid
- Policy directly tied to implementation
- Not virtualization or change aware

---

**Virtual Security**

Cost Effective
- Virtual appliances with broad functionality
- Single framework for comprehensive protection

Simple
- No sprawl in rules, VLANs, agents
- Relevant visibility for VI admins, network and security teams
- Simplified compliance

Adaptive
- Virtualization and change aware
- Program once, execute everywhere
- Rapid remediation

---

**Recommendations for protecting the virtual infrastructure**

- **Secure the infrastructure stack.** Secure individual components of the stack, including hypervisors, management servers, and interfaces. The stack must be hardened per a variety of guidelines, including those from the National Institute of Standards and Technology and VMware, using controls such as those offered in Symantec™ Protection Suite. Workloads in different trust zones must be isolated using controls such as the VMware™ vShield. For services that are to be self-defending, it is equally critical that endpoint security tools...
such as Symantec™ Endpoint Security be optimized to address the scenarios introduced with the high-density cloud deployments of VMs.

- **Secure information.** Pooled infrastructure allows VMs to access shared networks and storage servers. Access to storage servers by VMs must be monitored and controlled for sensitive content. Physical network security appliances that are blinded to traffic between VMs must be augmented with virtual firewalls and integrated with data loss prevention (DLP) to detect transmission of sensitive content. Encryption may be used as a compensating control to enforce isolation in this shared infrastructure. Dynamic content-based encryption offers finer granularity than whole disk encryption. Offline images are considered to be in scope in compliance regulations; they must therefore be protected for confidentiality and integrity, and any vulnerabilities must be managed before activation.

- **Enforce compliance of the accelerated configuration changes.** Compliance includes policies for controlling the creation, use, and modification of virtual machines and for configuring new infrastructure elements—including the hypervisor, virtual networks (network access control, for instance), virtual storage, and management (separation of duties, for example)—as well as their relationships. Assurance of compliance is critical for isolating different trust zones in this shared infrastructure. Because VMs are transient—leading to dynamic asset inventories—continuous compliance must be enforced.

### 3.2 Private cloud

The private cloud brings attributes of the public cloud—such as self service, rapid provisioning, and elastic workloads—to the enterprise. These attributes are provided by the service automation layer, which logically untethers applications and trust zones from the underlying network infrastructures. The automation layer dynamically allocates resources based on service-level agreements (SLAs). In this dynamic environment, security controls must be on demand and elastic to be dynamically deployed with the underlying workload.

**Recommendations for protecting the private cloud**

- **Secure the infrastructure.** The infrastructure controls used in securing virtualization must be made available on an on-demand and elastic basis. As a workload is migrated or scaled up, the security policies associated with that workload must be deployed at the new resources. Virtualized security controls such as server lockdown, configuration management, firewalls, DLP, and encryption can be instantiated on-demand, and the appropriate policies configured into them at the new hosts and networks. These security controls must support open, programmatic interfaces so that they can be integrated with the service automation layer that is responsible for workload management.

- **Secure information.** Because host and networks may be shared by workloads of different trust levels, the security policies associated with a workload must be aware of the sensitivity of the information. For example, a low-trust workload must not be allowed access to sensitive content used by another high-trust workload that shares hosts and networks. Detective controls such as DLP can be used to identify sensitive content, and compensating controls such as encryption can be used to secure information.

- **Sustain compliance.** Because workloads are dynamic, the underlying infrastructure(s) supporting that workload must be assessed continuously.
3.3 Public cloud

A key shift in the journey to the public cloud is the outsourcing of the data center. Enterprises’ control over infrastructure, processes, and people is reduced. A public infrastructure cloud implementing a set of security controls that are consistent and compatible with those used on-premise provides a greater degree of assurance and takes advantage of known good operations practice. Identifying sensitive information and then applying encryption-based security controls for its transmission and storage are key compensating controls that apply to all cloud service models.

Recommendations for protecting the public cloud

- **Secure the infrastructure.** Public clouds that deliver IaaS allow control to be deployed at the compute and network layers. Consistency of controls is achieved when the public infrastructure offers standardized controls that can consume the same policies as on-premise controls. Security policies that are tied to workloads are implemented consistently in the public infrastructure cloud and on-premise.

- **Secure information.** Information transmission between on-premise infrastructure and clouds and between clouds and devices must be secured based on sensitivity. Similarly, information storage must be secured on both clouds and devices. Encryption is a key compensating control for securing information in the cloud during both transmission and storage. Key management processes such as creation, destruction, rollover, and escrow must be managed centrally and consistently across on-premise and cloud infrastructure. Key management must be coupled with federated identity to enforce consistent access control on-premise and in the cloud. Data transmission must be secured using SSL or IPSec virtual private networks (VPNs). For SaaS cloud services, these are the primary compensating controls for implementing data privacy.

- **Enable federated identity.** Federated identity based on single sign-on solutions must be used to enforce consistent access control policies across on-premise and cloud infrastructures. Based on context such as devices, geo-location, and data sensitivity, strong authentication must be deployed. For deploying encryption, key management is often coupled with federated identity.
Conclusion

Clouds offer great promise in improving IT’s agility and flexibility to respond to the requirements of the business cost effectively. The security challenges raised by the loss of control and visibility in the journey to the cloud can be addressed in terms of securing infrastructure, information, identities, and devices. Applying these principles to each of the stages of the journey—from virtualization to private and public clouds—will help address security and compliance concerns in an evolving threat and compliance landscape. The set of security technologies and products offered by Symantec and VMware can help the enterprise accelerate this journey to the cloud, and can help ensure that standards for security and compliance are not only maintained, but actually enhanced by meeting the opportunity presented by this cloud journey.
About Symantec
Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

About VMware
VMware delivers virtualization and cloud infrastructure solutions that enable IT organizations to energize businesses of all sizes. With the industry-leading virtualization platform—VMware vSphere®—customers rely on VMware to reduce capital and operating expenses, improve agility, ensure business continuity, strengthen security, and go green. With 2010 revenues of $2.9 billion, more than 250,000 customers and 25,000 partners, VMware is the leader in virtualization, which consistently ranks as a top priority among CIOs. VMware, headquartered in Silicon Valley with offices throughout the world, can be found online at www.vmware.com.