Contents

Executive Summary.........................................................................................................................................................2
Defining Cloud Computing................................................................................................................................................2
  SERVICE MODELS............................................................................................................................................................3
  DEPLOYMENT MODELS...................................................................................................................................................5
Security Responsibilities By Cloud Service Model.......................................................................................................5
Shared Security Responsibility With Cloud Service Providers....................................................................................6
  ADMINISTRATIVE CONTROLS.........................................................................................................................................6
  PHYSICAL CONTROLS......................................................................................................................................................6
  LOGICAL CONTROLS........................................................................................................................................................7
Cloud Security and IAAS - A Shared Responsibility....................................................................................................7
Steps For Secure Cloud Adoption......................................................................................................................................8
  STEP 1 - PUT AWAY YOUR AWS “ROOT” ACCOUNT AND USE IAM TO ENABLE ACCESS........................................8
  STEP 2 - ENFORCE STRONG PASSWORD POLICY........................................................................................................8
  STEP 3 - ENABLE MULTI-FACTOR AUTHENTICATION FOR PRIVILEGE USERS....................................................8
  STEP 4 - BUILD A SECURE BASE AMAZON MACHINE IMAGE (AMI).................................................................................9
  STEP 5 - PROTECT THE GUEST OPERATING SYSTEM................................................................................................9
  STEP 6 - CREATE RESTRICTIVE FIREWALL POLICY AND USE HOST-BASED FIREWALLS..........................................9
  STEP 7 - SECURE YOUR APPLICATIONS AND USE HOST-BASED INTRUSION PREVENTION SYSTEM................10
  STEP 8 - FILE INTEGRITY MONITORING & LOGGING....................................................................................................11
  STEP 9 - ENCRYPT SENSITIVE DATA.............................................................................................................................11
  STEP 10 - CONDUCT VULNERABILITY ASSESSMENT....................................................................................................12
  STEP 11 - PERFORM PENETRATION TESTING..............................................................................................................12
  STEP 12 - STAY INVOLVED AND MAINTAIN SECURITY................................................................................................13
Conclusion.........................................................................................................................................................................13
How Trend Micro Can Help Secure Your Journey To The Cloud................................................................................13
Additional References............................................................................................................................................................14
Executive Summary

It seems cloud computing has erupted from nowhere but it has actually been around for decades. It has evolved from a shared resources “time-sharing” model in the 1950s to the 1990s era of “grid computing”. Broadband connectivity has enabled rapid adoption of the Internet, and now we are seeing companies of all sizes getting into the cloud computing game.

Cloud adoption is increasing at a rapid rate as services are backed by technology advancements such as high-speed Internet connectivity and high efficiency manufacturing. These advancements have reduced the cost of storage and enabled service providers to meet and exceed customer expectations. Rapid cloud adoption has however, introduced unique and complex security considerations for users. Now organizations must consider how adopting a cloud-computing model will affect their risk profile related to data security, privacy and availability.

Complicating that assessment is the fact that now within the ultimate security of cloud implementations is an inherent partnership with the cloud service provider. Aspects such as physical security, configuration integrity and personnel vetting is now in the hands of the provider, which most organizations taking advantage of the cloud never see.

As revealed in the 2012 Future of Cloud Computing Survey by North Bridge, one of the most cited reasons for resisting cloud adoption by organizations is the concern around data security and privacy. Researchers predict cloud security will become one of the primary drivers for adopting cloud computing. The Gartner Global IT Council for Cloud Services Report revealed that over 50% companies cited security as their top concern for transitioning to the cloud. There is no surprise that the global cloud security software market is expected to reach $963.4 million in 2014, according to research conducted by TechNavio. As customers begin to understand the importance of security in the cloud, they will demand that vendors make security a priority and thus a market differentiator and competitive advantage for cloud providers.

Amazon Web Services (AWS) has set high standards for the entire Infrastructure as a Service (IaaS) industry by building a solid foundation with comprehensive administrative, physical and logical controls – from strict policies for physical access to its data centers, to well thought-out configuration change management procedures. However, a secure foundation is just the start and to build an end-to-end secure computing environment, organizations must take an active role in protecting systems, applications and data as part of the AWS shared security model.

This paper will discuss what part of the shared responsibility equation customers are responsible for and what some of the recommended security practices are that can help create a secure cloud-computing environment.

Defining Cloud Computing

With the current popularity of “cloud computing”, the term is used and often applied to a variety of computing implementations. It is worth stepping back to understand cloud computing in its different forms.

The US National Institute of Standards and Technology (NIST) defines cloud computing by describing five essential characteristics, three cloud service models, and four cloud deployment models. The visual representation of NIST cloud computing is shown in the figure on the following page.
This model defines several service and deployment models that are relevant to the assessment of which parties are responsible for what security.

**Service Models**

The three most common service models for cloud computing are as follows:

**INFRASTRUCTURE AS A SERVICE (IAAS)**

The capability provided to the customer is to provision processing, storage, networks, and other fundamental computing resources where the customer is able to deploy and run arbitrary software, which can include operating systems and applications. The customer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications. (Examples: Amazon’s AWS and Terremark)

**PLATFORM AS A SERVICE (PAAS)**

The capability provided to the customer is to deploy onto the cloud infrastructure customer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The customer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly...
configuration settings for the application-hosting environment. (Examples: Google AppEngine and Microsoft Azure).

SOFTWARE AS A SERVICE (SAAS)

The capability provided to the customer is to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The customer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings. (Examples: Salesforce.com, Trend Micro HouseCall).

The following diagram from the PCI Security Standards Council provides a good example of how control is assigned between the customer and service provider in these different models:

![Figure 2 - Customer and Service Provider Control](image-url)
Deployment Models

How customers deploy the services from these providers also varies and generally falls into one of the following three models.

PUBLIC
This type of cloud infrastructure is open to public or to a large industry group. The organization offering this type of cloud service generally owns, manages and operates on its own premises.

VIRTUAL PRIVATE OR ON-SITE VIRTUALIZED
The cloud infrastructure is operated solely for a single organization. It may be managed by the organization or by a third party and may be located on-premise or off-premise.

HYBRID IT
The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

Simply put, there are numerous security characteristics specific to each cloud model and cloud customer, and provider security duties differ greatly between the cloud models.

Security Responsibilities by Cloud Service Model

To address the security needs of workloads running in the cloud, first organizations need to understand who is responsible for protecting those workloads. The roles and responsibilities transfer among the different cloud computing service models.

The cloud provider in an IaaS model is typically responsible for the security of the underlying infrastructure whereas in the SaaS model the cloud provider is responsible for securing the infrastructure and the application. The providers’ responsibility to provide security controls implementation increases as we move higher in the stack of a SPI model (i.e. SaaS, PaaS, IaaS) while cloud customer responsibility increases as we move lower in the stack of a SPI model. This responsibility concept is illustrated in the figure to the left.

Figure 3 - Security Responsibilities view based on SPI Model
For example, the IaaS model, such as Amazon Web Services (AWS), gives organizations the most freedom in leveraging the benefits of cloud computing but it also requires customers to take an active role in securing their own data and applications. So it’s important to understand risk mitigation best practices when choosing AWS as a vendor of choice, and whether it is an IaaS model in a public or private virtual cloud (PVC) offering.

Shared Security Responsibility with Cloud Service Providers

While the specifics of the threats that face cloud computing implementations are not new, the way that they are mitigated and who is responsible, is different. For example, “inside threats” in a traditional IT model still apply to the cloud-computing model. But in a cloud service offering, the primary controls, e.g. administrative and physical controls, which can help mitigate this type of threat, are now provided by the cloud service provider.

When an organization chooses to secure their data they implement one or more of the three types of controls.

**ADMINISTRATIVE CONTROLS**

Administrative controls (also called procedural controls) consist of approved written policies, procedures, standards and guidelines. Administrative controls form the framework for running the business and managing people. When workloads are run in a traditional enterprise IT infrastructure, it is considered a trusted environment because it is either physically located within the organization’s on-premise facilities and/or directly managed by the organization. Complete control over the networking infrastructure is exercised and includes physical access to the facility, background checks to hire new employees and implementing change management processes.

When migrating to the cloud, applications and data are now in an environment that is not controlled directly by the organization. In its place is a separately managed and maintained infrastructure hosted externally with the cloud provider. Now, instead of controlling the IT environment directly through the implementation of various controls that are defined by the organization, this is now achieved through the relationship with the cloud service provider and their associated service level agreements (SLAs).

Accordingly, it is important that when selecting a cloud provider, organizations understand that specific administrative controls, industry certifications and third party attestations exist. For example, for AWS, these can be found at aws.amazon.com/aws.

**PHYSICAL CONTROLS**

Physical controls monitor and control the environment of the workplace and computing facilities. They also monitor and control access to and from such facilities. Administrative and technical controls ultimately depend on proper physical security controls. An administrative policy allowing only authorized employee access to the data center serves no purpose if there is no physical access control stopping an unauthorized employee access to the facility. In a traditional IT model the organization is responsible for implementing these physical controls to secure the computing facility, while separating the network and workplace environments and putting up environmental safeguards.

When moving to cloud services, physical controls implementation is the responsibility of the cloud provider. It is important to understanding the specific physical controls and map them to ensure that these meet the organization’s requirements. For example, the AWS infrastructure is housed in Amazon-controlled data centers throughout the world. Only those within AWS who have a legitimate business need to access such information know the actual location of these data centers. The data centers themselves are secured with a variety of
physical controls such as security guards, multiple authentication and dual factor authentication - all part of preventing unauthorized access to their data centers.

LOGICAL CONTROLS

Logical controls (also called technical controls) use software and data to monitor and control access to information and computing systems. For example: passwords, network and host-based firewalls, intrusion prevention systems, access control lists, and data encryption are logical controls. Control over the implementation of the logical controls varies depending upon the cloud service model. In the IaaS cloud service model, you have complete control of the logical control implementations that are associated with the systems (i.e. instances).

When choosing logical controls to protect instances, consider answering questions such as:

- Is the selected control scale based on the demand?
- Is it “cloud aware” and is it integrated with provider API’s to provide an instant view when the instances scale up and down?
- Can it be extended from existing IT infrastructure to the cloud infrastructure to help enforce consistent security policy and provide a single policy management interface?
- Does it have the capability to automatically detect new resources and install needed access controls?
- Can security policies be enforced as soon as the instance is brought online to reduce the window of exposure?
- Does it integrate with cloud management tools? For example, when selecting an encryption solution to encrypt data at rest, is the selected control “cloud aware”?

From this, we can see that the advantages of technology solutions that allow for centralized management of both current in-house infrastructures as well as the cloud, are clear.

Cloud Security and IaaS – A Shared Responsibility

So for organizations leveraging cloud providers, security becomes a shared responsibility. The model below lays out in more detail the various areas that organizations leveraging an IaaS like AWS, are responsible for along with the associated security controls and security practices.

AWS provides security up to the hypervisor, meaning they will address security controls such as physical security, environmental security, and virtualization security. The cloud customer is responsible for security controls that relate to the IT system (i.e. instance), including the guest operating system, middleware technologies and applications.

Figure 4 – Shared Responsibilities Model

that relate to the IT system (i.e. instance), including the guest operating system, middleware technologies and applications.
Steps for Secure Cloud Adoption

AWS customers are responsible for the security of their workloads running on AWS. This includes protecting instances, applications running on them, and protecting AWS credentials to name a few. Amazon provides tools such as AWS IAM (Identity & Access Management) service, Multi Factor authentication (MFA) solution, security groups, and AWS CloudHSM to help with security responsibilities. In addition, Amazon recommends leveraging third party security solutions to create a complete end-to-end secure environment for all workloads.

Below is a discussion of some of the best practices that help protect AWS credentials, guest operating system security, running application software security, and/or configuration of the AWS security group firewall. These practices will help build a secure computing environment.

STEP 1 - PUT AWAY YOUR AWS “ROOT” ACCOUNT AND USE IAM TO ENABLE ACCESS
An AWS account is the first entity that is created when initiating a relationship with AWS. This account is considered a “root” account and provides access to all AWS resources including billing information. It is recommended to not use this account and instead leverage the AWS IAM service to create users, groups and roles to interact with AWS.

To manage AWS accounts easily and with added security, it is recommended that customers create users and groups and then assign permissions specific to their functional requirements. Assigning permissions to allow users access to AWS is no different then the approach used in the traditional IT model i.e. assigning permissions at the group level. It is more convenient to manage permissions at the group level than individual users. Groups can be created according to job functions (e.g. administrators, managers, testers etc.), and relevant permissions for each group can be established and then IAM users can be assigned to those groups.

When creating security policies (set of permissions) to control access to AWS resources, use the “least privilege” model. Following this model will require some research by the customer to correctly determine the right set of permissions that allow users to perform their job duties. Users can also leverage AWS IAM groups to enforce the “separation of duties” security practice. Amazon provides default built-in policy templates, which include predefined permissions. These templates can be used for common use cases such as Administrative Access and Read-only Access.

STEP 2 - ENFORCE STRONG PASSWORD POLICY
The need for a strong password policy seems obvious but it is extremely important to prevent passwords from being guessed or cracked. The role that passwords play in securing customer systems is often underestimated and overlooked. Passwords provide the first line of defense against unauthorized system access. Amazon allows the customer to define and enforce password policies such as a passwords minimum length and whether it requires a non-alphabetic character. It is recommended that customers define and enforce strong password policy, which requires users to update their credentials at a regular interval of time e.g. 90 days.

STEP 3 - ENABLE MULTI-FACTOR AUTHENTICATION FOR PRIVILEGE USERS
When enforcing a strong password policy for authentication and using AWS IAM service to define authorization levels, consider enabling multi-factor authentication (MFA) for privilege and administrative users. AWS MFA is an additional layer of security that offers enhanced control over AWS account settings and the management of
the AWS services and resources.

Today, many organizations require additional security controls when an administrative user has even greater access to the system. It is recommended that AWS resources be protected by configuring AWS MFA for all privilege users. A privilege user could be a user who has access to instances with permissions that can disrupt business operations. For example, a privilege user is a user with access to AWS resources and permissions to terminate production instances.

By enabling MFA, extra security is added by requiring all such users to enter a unique authentication code from their authentication device when accessing AWS websites or services. This will prevent anyone with unauthorized knowledge of email addresses and passwords from impersonating system controls.

Amazon provides two choices to enable MFA; either use of hardware base token devices from third-party vendors or software base tokens running an AWS MFA compatible application virtual token service on a smartphone, tablet, or computer.

STEP 4 - BUILD A SECURE BASE AMAZON MACHINE IMAGE (AMI)

When using a pre-configured operating system template aka Amazon Machine Image (AMI) or a customized configuration AMI to create a virtual machine within the Amazon Elastic Compute Cloud (EC2), the customer is responsible for performing the appropriate due diligence before using the instance to host applications. The customer has full root access or administrative control over this virtual system. AWS does not have any access rights to customer instances and cannot log into the guest OS hence cannot vouch for the integrity or security of that instance. It is recommended that customers go through an exercise of operating system hardening to ensure only required applications and services are enabled.

It will help reduce the attack surface if running software services are streamlined, and instances are configured down to the bare minimum, for example, disabling password-only access to hosts, utilizing some form of multi-factor authentication to allow access to critical instances and disabling remote “root” account logins.

STEP 5 - PROTECT THE GUEST OPERATING SYSTEM

Amazon has a very robust process for implementing and managing the administrative and physical control types as well as securing the virtualization or hypervisor layer (Host OS), but it is the customer’s responsibility to continuously maintain and equip their AWS instances with defensive security controls and regularly assess their effectiveness.

Amazon EC2 provides tools such as AWS Security Groups for securing cloud-based servers. It is recommended that customers take advantage of these basic tools to implement basic security and then implement additional security by leveraging technology solutions such as; anti-virus, host-based firewalls, host-based intrusion prevention, file integrity monitoring, log inspection, encryption and key management solutions.

Protecting the guest operating system also means applying regular security updates and OS patches. For example, updating security patches for an instance hosting “always-up” web applications may be extremely difficult and costly. To ease patch management difficulties it is recommended that customers use vulnerability shielding, aka “virtual patching” solutions. This will ensure that application availability goals are met without compromising security.

STEP 6 - CREATE RESTRICTIVE FIREWALL POLICY AND USE HOST-BASED FIREWALLS

Amazon provides tools such as AWS (EC2) firewall for securing cloud-based servers. Every Amazon EC2
instance is protected by either one or more security groups which contains sets of firewall rules that specify which type of network traffic should be delivered to that particular instance. By default, the firewall operates in a deny-all mode and customers must explicitly open the ports needed to allow inbound traffic.

Often enough the firewall policy contains an overly permissive set of rules which create security holes. It is recommended that customers lockdown their firewall policy and only allow communication that is absolutely required. Creating a restrictive traffic management and security design on a per-instance basis is their job. For example, customers should not open remote access (RDP or SSH) to all of their production instances instead they should use “Bastion Hosts” to get remote access to production instances and lock down administrative access to only the “Bastion Host” from the external network.

The AWS EC2 security groups give customers basic firewall with semi-Statefull protection capabilities to control only incoming communications (except when using AWS VPC services). It does not prevent a server from initiating outbound communications and it does not have any logging options available for any rules that are configured which could be important in some cases e.g. troubleshooting and monitoring. It is recommended that customers take advantage of these security groups to restrict ingress (incoming) communications and then implement additional security by leveraging technology such as host-based firewalls to strengthen network-based security in Amazon EC2. Customers should choose a host-based Bi-directional Statefull firewall with logging and alerting capabilities. This will help them create a “defense in depth” security posture.

**STEP 7 - SECURE YOUR APPLICATIONS AND USE HOST-BASED INTRUSION PREVENTION SYSTEM**

Creating a restrictive firewall policy and augmenting AWS EC2 firewall with a host-based firewall is not enough. The traditional firewalls are designed to reduce the attack surface but they still have to allow traffic on open ports. For example, if the customer is running a web based application and their firewall policy allows traffic on port 80/443 of the application then the firewall will allow all such traffic. It lacks the intelligence to determine if the allowed traffic is legitimate traffic. Securing an application involves many important elements ranging from secure coding practices to penetration testing; it could simply mean following a practice which allows access to encrypted sensitive information only “on-demand” and not caching it into memory.

Today, customer demand requires that businesses run short development cycles with increased functionality and rich feature sets. This can result in the release of applications that aren’t properly secured which in turn could potentially harm a customer’s business reputation. If an organization has developed a web application that is accessible externally over the Internet, one that interacts with in-house or third party technologies, then inevitably it is susceptible to security holes.

The most common web application vulnerabilities that an application could potentially be facing are SQL injection and Cross Site Scripting (XSS) attacks. To protect an application from these attacks customers should consider using web application protection technologies such as host base intrusion prevention systems (HIPS).
A good HIPS solution can help address patch management challenges by providing virtual patching capabilities. This provides protection against known zero-day attacks and shields the system and applications from various vulnerabilities. When selecting the HIPS solution, it is recommended that customers map their computing environment to the vendors rule-set coverage to ensure appropriate protection, e.g. if the computing environment is based on Linux OS and the vendor has a small rule-set for Linux base OS then it may not be the best choice for that computing environment.

**STEP 8 - FILE INTEGRITY MONITORING & LOGGING**

The next step is to ensure the continuous integrity of critical system files, application configuration files, and application logs. File integrity monitoring is emerging as a critical aspect of information security. It provides an early indication of a compromised system and it is required by various compliance standards such as PCI. It is recommended that customers implement file integrity monitoring and log analysis solutions to detect any unauthorized modifications to their system components – files, registry, services, processes and critical system files. Logging is another important component of information security. If logs are not taken, security incidents can not be captured and if log and security events are not monitored, incidents can not be detected. It is important to enable logging for all components that provide visibility into computing environments including; operating system, firewall, antivirus software, intrusion prevention, and application logs.

There are many solutions available to customers from host-based solutions to a MSSP. If a customer has already established a monitoring solution and is collecting logs to a central server, then instances running in the cloud are just another resource that must be monitored. Firewall configuration changes may be required to allow logs from the cloud environment to reach the central log-collection server on-premises in addition to securing the data transmission path.

**STEP 9 - ENCRYPT SENSITIVE DATA**

It is important that customers do their due-diligence and evaluate the nature, sensitivity and classification of moving data and accept the potential consequences of putting the sensitive data in the public cloud. Sensitive data could be user identity and credentials as well as any personally identifiable information (PII) such as social security number.

When data is moved to public cloud it may become subject to the regulations of an unknown jurisdiction so it’s important that customers instruct their cloud provider to store their data in a specific region. For example, if a European company is storing the data in a US region, it becomes subject to the USA Patriot Act, which allows
the US government to access data stored within US borders. Amazon does allow its customers to specify their geographical region preferences when using AWS services. Customers must ensure they inform Amazon of their preferred region for data storage, appropriate for their business.

Once data is in the cloud, whether in a public cloud or in PVC environment, customers should consider encrypting it for both “in-flight” and “at-rest” states. For example, if customers need to send sensitive data between their web application and their users' browser, then they should always encrypt the channel and use SSL. If customers need to protect server-to-server communication, such as between their application web server and database, it is recommended that they consider IPSec or SSL.

When choosing an encryption solution to protect sensitive data “at-rest” whether an open source solution or built-in OS solution, (e.g. Microsoft Encrypting File System (EFS), eCryptfs or a commercial solution), customers must evaluate each solution and see what fits best with their security practice. Is encrypting individual files enough to meet security requirements or is encryption of the entire volume required? Another important factor when selecting a solution is the key management and custodianship of these keys. Does the security practice require that the encryption keys not leave the premises? If the answer is yes, then OS built-in solutions cannot be used since they all require that encryption keys be stored on the system.

To this point, creating a “defense-in-depth” model around data, application, host and network, has been discussed. By applying this security principle customers have implemented security controls around their data that are layered on top of each other. This ensures the protection of data even when one defensive control fails e.g. if an intruder is able to pass firewall control then the host-based intrusion prevention system is there to provide protection.

STEP 10 - CONDUCT VULNERABILITY ASSESSMENT
The main objective of the vulnerability assessment (VA) is to find as much vulnerability as possible that an attacker can use to cause damage to an organization. This vulnerability assessment can be run against customer networks, systems or the web applications. There are many tools, services or a combination of both available that can be used to conduct vulnerability assessments. It is recommended that a trained security assessor, either internal or from an external company, perform this assessment even if customers are using a tool to perform this exercise. A trained security assessor may find more security flaws and help customers fine-tune their existing security controls or add more controls.

STEP 11 - PERFORM PENETRATION TESTING
Once customers have created their desired security posture around their running instances, it is recommended that they evaluate the security of their systems by conducting penetration testing to safely exploit system vulnerabilities, including OS service and application weaknesses.

By conducting the vulnerability assessment, customers have identified the vulnerabilities but not the potential consequences if the vulnerabilities are exploited. For example, the vulnerability scan may show a SQL injection vulnerability, but when they attempt to exploit it in the penetration testing, it could reveal personally identifiable information (PII) or data that is with-in the risk tolerance of the organization.

Penetration testing is very useful approach to validating the effectiveness of the defensive mechanisms. This exercise will help customers determine if their security controls implementation can withstand real world attacks. Amazon understands the critical importance of penetration testing in any secure application deployment, hence it has established a policy for its customers to request permission to conduct penetration tests. The PCI Data Security Standard, FISMA, NIST, and other legislative and industry regulations also mandate
penetration testing.

**STEP 12 - STAY INVOLVED AND MAINTAIN SECURITY**

In a traditional IT computing model, security is not a one-time exercise. The same rule applies in the cloud-computing model. Customers need to stay involved and maintain their security practice. Customer responsibility doesn't end after selecting AWS as a vendor of choice, creating their security framework and moving workloads to the cloud. Most likely customers will continue to migrate new workloads to the cloud or acquire new services to meet business needs. As customer requirements change, they must evaluate the changes from a security perspective and deploy updated or new controls to provide protection. Customers need to ensure the ongoing management aspect of security continues which may involve documenting implemented controls and monitoring changes.

**Conclusion**

Cloud provides many attractive options to improve business agility and flexibility. But taking advantage of these benefits means continuing to be responsible for numerous aspects of security. While these concerns should not discourage adopting cloud computing, it is necessary to understand responsibilities in this shared security model and adapt security practices to this new environment.

**How Trend Micro can Help Secure Your Journey to the Cloud**

Trend Micro understands that to fully embrace the cloud, the unique security challenges posed by it must be delivered in a way that preserves its economic and operational benefits. Trend Micro has been working closely with Amazon Web Services to ensure that Trend Micro delivers elastic, flexible and scalable security solutions that are compatible with the AWS environment. Together, the two companies are helping organizations understand and overcome the main adoption barrier of deploying applications in reliable cloud service programs - security.

Trend Micro delivers the broad range of security capabilities needed as part of the cloud’s shared responsibility model. These are done in a way that reflects the elastic nature of the cloud with fast deployment and automated management.

To find out more about Trend Micro solutions for the Cloud, check out [WWW.TRENDMICRO.COM/CLOUDPSECURE](http://WWW.TRENDMICRO.COM/CLOUDPSECURE)
Additional References

The NIST Definition of Cloud Computing - Special Publication 800-145

Amazon Web Services: Overview of Security Processes

Security Guidance for Critical Areas of Focus in Cloud Computing

2012 Future of Cloud Computing Survey Results - North Bridge
http://northbridge.com/2012-cloud-computing-survey

Cloud Security Market Swelling - TechNavio Research
http://www.telecomasia.net/content/cloud-security-market-swelling-41-caqr

AWS IAM Best Practices

Information Security

Security groups: a quick review
http://aws.typepad.com/aws/security/

Trend Micro Cloud Security Blog
http://www.trendmicro.com/cloud

Trend Micro & Amazon Web Services PCI & Cloud Webinar
http://www.trendmicro.com/cloudpci