ORACLE
CLOUD

Making Sense of the Shared Responsibility Model

Security Obligations for Enterprises Using Cloud Services

ORACLE WHITE PAPER | JANUARY 2017

ORACLE

Introduction

Cloud adoption promises the benefit of increased flexibility and significant cost savings. Hence, migrating business-critical applications to the cloud is becoming a growing priority for companies of all sizes. A recent survey of more than 250,000 information security professionals revealed that more than 77 percent of organizations have already adopted cloud services and 10 percent of those companies using cloud services describe themselves as heavy users.

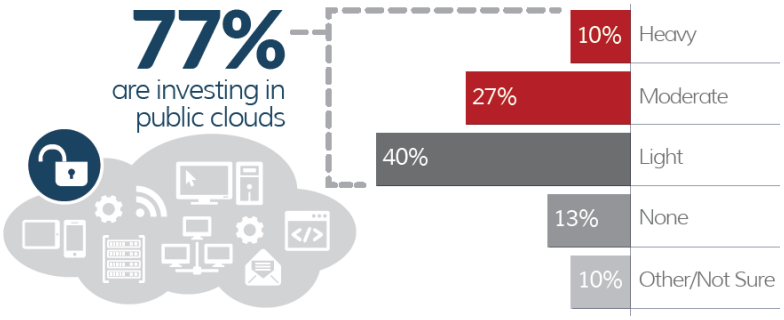

Figure 1. More and more companies are using applications in the public cloud.

Although many enterprises adopt new applications on a regular basis, few have real-world experience in securely adopting cloud services. Migrating enterprises' business-critical needs to the cloud has a much larger ramification than any single software upgrade. More often than not, cloud adoption is part of a companywide initiative that represents a new paradigm of doing business. With such high importance and expectations, enterprises spend significant time and resources to evaluate all aspects of the cloud service including its features, capabilities, redundancy, global infrastructure, and service level agreements (SLAs). However, one section in the cloud service provider's (CSP) terms of services document gets overlooked time and time again: the shared responsibility model.

The shared responsibility model is spelled out in the terms of services document of every CSP from Microsoft to Amazon. However, it is arguably the least understood and most misconceived concept. Simply put, the shared responsibility model outlines the CSP's responsibility to maintain a secure and continuously available service and enterprises' responsibility to ensure secure use of the service. Why is such a concept so difficult to comprehend and open to varying interpretations? Is the difference between *security of the service* and *secure use of the service* so significant? Aren't enterprises moving to the cloud so they don't have to deal with these types of responsibilities?

This white paper examines the root cause behind the confusion, some unfortunate scenarios that resulted from the confusion, and how some enterprises are successfully addressing and embracing the shared responsibility model.

The shared responsibility model outlines the cloud service provider's responsibility to maintain a secure and continuously available service and enterprises' responsibility to ensure secure use of the service.

Misconception of Cloud Service Security Infrastructure

Much of the misconception over the shared responsibility model stems from preconceived notions and past experiences with traditional software models. Take the Microsoft Office suite of products, for example. At a high level, deployment of traditional Microsoft Exchange email requires:

- Integration with Active Directory for employee/user information
- Installation of the actual Windows or mailbox servers
- Installation of Edge Transport servers to handle spam filtering and mail flow
- Deployment of outlook email client to PCs and laptops

With no servers or clients to deploy, enterprises incorrectly assume migrating Exchange to the cloud only requires:

- Integration of on-premises Active Directory with cloud services
- Configuration of spam filtering and other mail flow in the cloud service

Enterprises overlook all the on-premises security measures that the traditional Exchange application relies on. Firewalls are configured to block logins from specific locations such as embargoed countries. Intrusion prevention systems block logins from suspicious or known-to-be-malicious IP addresses. A behavior analytics platform detects insider threats or attacks using compromised credentials. Security information and event management (SIEM) and log management solutions alert administrators of changes to critical configurations. Since these and other security measures protect all applications in the enterprise campus, they are often taken for granted in the context of any one particular application. These examples of security measures are needed to ensure secure use of the service and hence the responsibility for their installation and upkeep falls squarely on the enterprise.

The "Set It and Forget It" Myth

In preparation for cloud application adoption, many enterprises plan their IT resources assuming that the bulk of their efforts and resources will be needed during the initial on-boarding process. Many companies believe that once the various service settings are configured according to sound guidelines, the ongoing maintenance will require significantly fewer resources. After all, the IT staff should gain experience and familiarity with the cloud service as part of the initial setup. Unfortunately, this is not the case in real-world deployment. And it is one of the most common reasons why enterprises falter on their part of the shared responsibility model.

As part of the initial cloud service adoption, IT administrators define roll-out plans that include, among other things, key configuration settings for the service. These settings include user-specific security requirements such as the complexity and rotation of credentials. They also include privilege settings for users and administrators, identifying which users have access to which applications as well as which administrators can create new users or change existing privileges. Although these settings are well defined initially, enterprises naturally drift away from them as they attempt to better support the overall business. Also, if adjustments are not restored to the original settings, then those temporary changes become permanent.

Although IT administrators can and should check for configuration drifts on a regular basis, such efforts are rarely practiced with any vigor due to the amount of resources needed. For example, chasing down the reason why a configuration was changed six months ago by an administrator who is no longer with the company can be very time consuming. Unfortunately, simply reverting the configuration without thorough investigation is not an option. As many IT administrators can attest, such an action usually results in a late night phone call from an angry executive who just realized critical data needed for a board meeting tomorrow cannot be accessed.

As a result, many IT administrators simply follow the "don't fix it if it's not broken" model. Some enterprises defer checks for configuration drifts to a quarterly audit exercise, but, more commonly, they simply wait to react to incidents to correct the settings. Unfortunately, both approaches lead to configuration drifts which leave the enterprise vulnerable to attacks and result in significant financial burden.

When You Don't Keep Your Side of the Bargain

Lack of clear understanding on what security measures the enterprise must provide as well as the enterprises' inability to minimize configuration drifts often have significant impact. There are many real-world examples of lapses in enterprise visibility and security that have devastating outcomes.

ENTERPRISE LOSES MILLIONS DUE TO DISGRUNTLED EMPLOYEE

Industry	Manufacturing
Time of incident	2015
Use of cloud services	The enterprise migrated many of their internal applications—as well as applications for their partners—to the cloud.
Incident detail	A disgruntled employee launched dozens of Amazon Web Service (AWS) instances before resigning.
How incident was detected	The enterprise only became aware of the incident after they received a hefty bill from Amazon.
Obligations under the shared responsibility model	The user who launched the AWS instances was a valid and privileged user. However, the enterprise lacked any automated system to detect and alert them of anomalous, unusual activity—such as launching multiple AWS instances.
Impact of the incident	The total amount was not disclosed, but it is estimated to be millions of US dollars.
Response to the incident	The enterprise has since deployed a cloud security solution that, among other things, automatically monitors cloud security settings and alerts them of activities such as launching new AWS instances.

ENTERPRISE CLOSES DOORS AFTER A RANSOM ATTACK

Industry	Hosting provider
Time of incident	2014
Use of cloud services	The enterprise leveraged cloud services to host customer data that was the backbone of its business model.
Incident detail	A hacker gained access to AWS credentials via a phishing attack against a privileged user. After gaining privileged access, the hacker demanded ransom in return for control of the cloud environment.
How incident was detected	The enterprise was investigating a distributed denial of service (DDoS) attack when the IT group discovered the ransom demand intentionally left by the hacker, revealing the true nature of the attack.
Obligations under the shared responsibility model	The enterprise lacked sufficient security to thwart the initial phishing attack. However, more importantly, the enterprise had no automated tools in place to detect suspicious behavior indicative of compromised credentials or creation of backup administrator users.
Impact of the incident	Once the enterprise attempted to regain control of its cloud service, the hacker used a backup administrator account to delete all data from the cloud service.
Response to the incident	Due to the severity of the attack, the enterprise closed its doors and ceased operations within days.

HEALTHCARE PROVIDER FACES FINES DUE TO HIPAA VIOLATION

Industry	Healthcare
Time of incident	2014
Use of cloud services	A healthcare provider adopted cloud services for their productivity suite.
Incident detail	Due to misconfiguration, the email solution bypassed the check to ensure that personal health information (PHI) is not transmitted externally.
How incident was detected	The oversight was detected only after a quarterly audit of their configuration. Once discovered, the healthcare provider promptly reported the incident.
Obligations under the shared responsibility model	The healthcare provider lacked automatic alerts to notify IT professionals when critical configuration settings changed.
Impact of the incident	The financial implication is still being determined, but is expected to be on par with the US$1.5 million maximum penalty.
Response to the incident	The healthcare provider has since deployed a cloud security solution that automatically alerts their IT staff of critical configuration changes in real-time.

As illustrated by the preceding examples, the gaps in security from confusion over the shared responsibility model have led to devastating results. Many enterprises have suffered significant financial losses, and some have even closed their doors. Fortunately, enterprises are learning from these scenarios to better address their part of the shared responsibility model and improve their overall cloud security posture.

Other Side of the Coin for the Shared Responsibility Model

The shared responsibility model can seem one-sided with enterprises burdened with a majority of the necessary security measures. Although less sensationalized than some of the headline-catching incidents, there are several real-world examples of cloud service providers reacting to meet their obligations in the shared responsibility model.

HACKERS USE GOOGLE APPS TO LAUNCH ATTACKS

Impacted service	Google Apps
Time of incident	2015
Incident detail	A hacker used Google Apps (specifically, Google Drive) to launch phishing attacks. The hacker created a fake login page on Google Docs and used it to capture login credentials. The fake login page looked authentic, including the use of a google URL (google.com/…).
How incident was detected	The attack went unnoticed until Google was alerted by security vendors.
Obligations under the shared responsibility model	Technically, there was not a lapse in the shared responsibility model since this attack did not impact the availability and security of the Google Apps service. Nonetheless, Google had to react quickly to ensure their infrastructure was not being used for malicious intent and to restore overall confidence in the service.

TRADITIONAL VULNERABILITY DISCOVERED IN OFFICE 365

Impacted service	Microsoft Office 365
Time of incident	2013 and 2014
Vulnerability detail	A cross site scripting (XSS) vulnerability in Microsoft Office 365 enabled any user within the company to gain full administrative privileges over the enterprise Office 365 environment.
How vulnerability was detected	The vulnerability was first identified by an Office 365 reporting firm during an audit.
Obligations under the shared responsibility model	Upon notification of the vulnerability, Microsoft remedied the problem within 2 months. Microsoft encourages detection of vulnerabilities in its products with the goal of addressing them before they can be exploited. This is a standard business practice for the company and one of several ways Microsoft is addressing its obligations under the shared responsibility model.

Addressing the Shared Responsibility Model

Enterprises must take a new approach to ensure secure use of cloud services and fulfill their obligations under the shared responsibility model. The traditional approach of relying on firewalls, proxies, and other solutions to secure the perimeter of the enterprise network doesn't apply to cloud services. Focusing only on the initial configuration of the service—and expecting the same level of security as the configuration drifts and changes—has also proven to be unrealistic. Unfortunately, even when enterprises recognize the limitations of these approaches, the solution may not seem readily evident.

The IT budget is always under scrutiny, especially as enterprises adopt cloud services. In fact, the promise of lower IT spend is a commonly expected benefit of adopting cloud services. Given these conditions, enterprises often lack the resources to fulfill their part of the shared responsibility model. They certainly lack the dedicated resources to manually audit cloud service configurations on a regular basis.

Enterprises are turning to cloud-based security automation services to fill the gaps they cannot afford to close. These solutions are tightly coupled with business critical services—such as Microsoft Office 365, Google Apps, AWS, and Box—to alert enterprises of critical configuration changes. In some cases the configurations can even be reverted back automatically. With user behavior analytics, these solutions can also identify compromised credentials and risky or anomalous behaviors indicative of an attack.

Cloud security automation represents a much-needed solution to address the shared responsibility model as enterprise adoption of cloud services continues to accelerate.

About Oracle CASB Cloud Service

Oracle CASB Cloud Service brings an innovative approach to securing your entire cloud footprint. As the pioneer of API-based cloud access security brokers (CASBs), Oracle CASB Cloud Service is the only solution to provide visibility and security across software-as-a-service (SaaS), infrastructure- as-a-service (IaaS), and platform-as-a-service (PaaS) environments.

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

ORACLE

CONNECT WITH US

blogs.oracle.com/oracle
facebook.com/oracle
twitter.com/oracle
oracle.com

Integrated Cloud Applications & Platform Services

Making Sense of the Shared Responsibility Model
January 2017