Cloud Security in an Agile World

Written by: Jaret Chiles, Enterprise Cloud Solutions Architect
and Matt Tesauro, Product Security Engineering Lead

Table of Contents

1: Introduction

The conversation of "Why Cloud?" has long since passed for many businesses and the question has transitioned into "How Cloud?" and "Is it safe?" The value the cloud brings to a business is measured in many different ways—from speeding innovation and reducing time to market to streamlining operations and reducing capital expenditures. However, one of the largest inhibitors to cloud adoption remains concern around the security of leveraging a service provider in a multi-tenant environment. Much is at stake protecting your customers and your business, and naturally, you should be cautious. While some of these concerns are beginning to quell over time as cloud technologies continue to mature at a rapid pace, traditional controls and processes must adapt to new platforms, new development methodologies and advanced technologies. In this article, we will discuss securing cloud applications in an agile world, in large part by security testing with the same agility.

2: Managing Risk and Enabling the Business

Information security is managed best by a risk-based approach and leveraging defensive tactics extensively. In a world of multi-tenancy and increased attack surface, this concept is key to ensuring you balance your risks properly. The changing landscape of risk demands decisive action from information security specialists. In an environment where you resist change, business units will find ways to work around IT, resulting in diminished control of your risk posture. When you feel your risk profile in one area may have increased, you need to counterbalance that risk by increasing your security posture in other ways to average out the difference. This allows you to maintain a risk level that is appropriate for your organization and your customers. Enabling your business units by making the cloud easier to consume while also relieving them of their own security, compliance and management requirements can be a winning strategy. You become a partner and preferred solution to the business, rather than leaving business teams to do it on their own and risking unwanted security exposure.

3: Adapting Best Practices for Cloud

First and foremost, you should think of security within the public cloud from a basic controls perspective, and see it within the context of your whole IT organization. Practices such as least privilege-based access controls, proper role-based user management, patching, intrusion detection, file monitoring are essential (see the SANS top 20 critical security controls: **http://www.sans.org/critical-security-controls/**). Many modern application compromises come through their own administrative back doors, so maintaining a security-minded organization and proper internal security controls is increasingly important. None of this is new, though it can be challenging to adhere to many of these tried-and-true best practices in today's BYOD (bring your own device) environments. Training and awareness of your workforce is key. Just as your system administrators have been trained to understand how to harden an operating system, your cloud application developers should be trained on application security. Your entire organization needs to be adept at identifying social engineering attacks such as phishing and mock websites designed to steal credentials and install malware on your systems. Security always starts with people.

SECURITY AWARENESS TRAINING:

- Focus training of your entire organization to recognize social engineering attacks.
- Conduct periodic controlled phishing attacks on your staff to identify spot training opportunities and track the overall awareness levels of your organization.

SYSTEMS ENGINEER TRAINING:

- Ensure engineers understand the importance of hardening operating systems and managing critical controls such as the SANS Top 20 (**http://www.sans.org/critical-security-controls**).

- Teach engineers how to evolve their skill sets on new automation platforms that enable them to operate at web scale.

DEVELOPER TRAINING:

- Consider ethical hacking class exposure to increase developer awareness of common application flaws such as the OWASP Top 10 (**https://www.owasp.org/index.php/Top_10_2013-Top_10**)
- Secure coding classes for all developers.

From the perspective of security for an application deployed into a cloud environment, the greatest challenge to managing controls effectively is the increased pace at which applications are being developed and deployed. It is normal to find development teams now practicing continuous deployment models, making changes many times a day or even many times an hour. The rapidly changing nature by which new resources are provisioned and de-provisioned, within minutes, requires new methods of thinking. What happened on compute node app0137 that was up for 45 minutes, four days ago? This is another one of the conundrums of integrating security effectively into your agile organization. If you make security standards difficult to adopt and to manage, you will fail, or at a minimum you will adversely affect your agility. Above all, gaining visibility into rapidly changing environments is crucial to your success.

For example, use configuration management solutions with hardened templates such as Chef, Puppet Saltstack or Ansible and auto-provision read-only security agents to all of your hosts. Leverage those security agents to report to an aggregation service to manage security standards seamlessly on your cloud servers. Automate the security posture of your servers. By following these guidelines, you centralize the focus of many of your security efforts:

HARDENED OS CONFIGURATION MANAGEMENT TEMPLATES:

- Regularly assess a set of centralized server templates or recipes from your configuration management solution rather than trying to assess hundreds of cloud servers, changing your stance from reactive to proactive.
- Upon identifying a weakness, adjust your centralized templates and automate resolution to all existing servers rather than fixing them each manually. This is a highly effective use of scarce security resources.

MANAGE DATA EFFECTIVELY:

- Classify data, understand how it flows in your environment, and tier types of data in accordance with the security controls built into your environment.
- Encrypt all your secrets. Do not let sensitive data transfer or rest in clear text. Consider third party payment gateways for PCI data or manage encryption effectively within your application layer.

AUTOMATE DEPLOYMENT OF READ-ONLY SECURITY AGENTS:

- Enable the ability to review historical events by reviewing the aggregated data. Establish thresholds, which raise meaningful security alerts to avoid analysis paralysis.

- Use security agent tools such as CloudPassage Halo client to simplify the management and monitoring of distributed and variable compute resources. (**http://www.rackspace.com/blog/cloudpassage-secure-your-cloud-servers/**)

SEND SYSTEMS EVENTS AND APPLICATION EXCEPTIONS TO A CENTRALIZED LOGGING REPOSITORY:

- Logging unexpected events reveals server or application anomalies. (**https://airbrake.io/pages/home**)
- Avoid needing to log in to cloud servers individually to review logs.

Automate everything you can, and centralize the resources you need to assess your security posture. Consider comparing your strategy to the CSA Cloud Control Matrix (**https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3/)**. This is key to adapting traditional security best practices to a cloud model.

4. Testing at Cloud Speed

If you do not automate your security assessment tool sets, you will leave gaps as your application scales. Cycle time for software is getting shorter with continuous delivery as the goal, which means traditional manual code scanning windows during QA are no longer sustainable. Creating artificial delays to inject traditional security processes is not the answer. Fighting the business desire to obtain the first-to-market advantage forces internal conflict and removes the advantages accrued from leveraging the strengths of cloud service providers. Become part of the solution and change the game from the inside by automating all possible processes. Automate software testing, operational infrastructure (as we touched on in the previous section), and security testing.

To accomplish security successfully in a cloud world, the modern security engineer must think like a developer. Sprints break software into little pieces and we need to do the same as we adapt our security processes to fit an agile model:

TESTING IN PIECES:

- Break your testing into little pieces by focusing on new or changed components of an application.
- Use your application threat model to understand the most crucial bits that deserve the highest priority.

LONG- AND SHORT-RUNNING TEST:

- Testing time drives testing frequency. Reduce low value in cycle testing and conduct long running tests out of band of the development process.
- Code for tests need to be optimized. Ensure vulnerability tests are applicable to the services or code in scope.

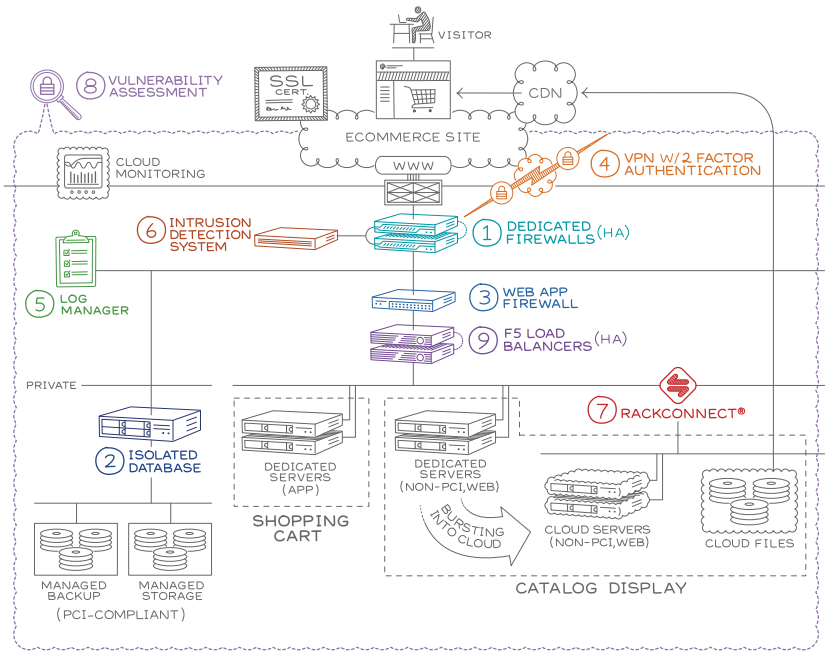
SMOKE TEST VERSUS FULL REGRESSION TEST:

- Smoke test early and often. Make sure new code snippets are tested quickly.
- Full regression tests on regular timed intervals. Complete comprehensive tests out of band of the development cycle.

To truly embrace the development culture and enable rapid cloud adoption you must understand the frameworks from which your development teams operate. Familiarize yourself with the workflow, identify integration points, and find ways to integrate without creating delays. You can further enable your development teams by creating tests they can use to resolve issues you discover. For example, if you recognize a cross-site scripting vulnerability in a web application, make the test you used to discover the flaw easily repeatable, easy to understand, and provide it to the development team. This way they can validate whether the issue has been resolved without needing to consume your scarce security resources. This dependency injects delays into the deployment process. Think of this as TD(S), test driven security, much as the way many agile development teams think of TDD, test driven development.

5. Hybrid Cloud Applications

We believe strongly that a well-developed, well-managed, and properly encrypted cloud application can be as secure as any application hosted by traditional technologies. We have worked with thousands of enterprises and this result requires significant rethinking and some retooling to match traditional IT security. Integrating security into your development practices and updating your tooling to adapt to elasticity greatly improves your security posture in the cloud. As mentioned earlier, traditional methods of securing your cloud application continue to play an important role. Traditional security controls can and should help your organization continue to manage your security posture in your journey to the cloud. The same traditional and familiar concepts are easily achievable with Rackspace hosted hybrid cloud security architectures.



Dedicated firewalls, load balancers, web application firewalls, network-based intrusion detection systems and log managers are all able to support a cloud application within the Rackspace hosted Hybrid Cloud architecture. As shown in the reference architecture below, this approach can provide customers with the best of both the dedicated and cloud worlds.

Hybrid cloud architectures enable you in many ways that a pure cloud solution simply cannot. When security and compliance are of the utmost importance for your data, here are some additional points to consider with a hybrid architecture:

- Ensure your ingress/egress points within your cloud environment only permit desirable traffic.
- Leverage intrusion detection systems, web application firewalls and log managers to continuously monitor the health of your environment.
- Tier your most critical or sensitive data assets into a single-tenant dedicated environment and leverage multi-tenant public cloud for product catalogs and less sensitive data.

6. Leveraging Cloud Tools Partners

Among the many benefits of leveraging a mature cloud service provider, one that shouldn't be overlooked is the availability of a mature partner ecosystem. In a world where the first mover often wins, you should focus your resources on your differentiators and creating new value and revenue streams for your business. Consider the maturing ecosystem around cloud security partners and tools to enable you to do so. Some of these tools are difficult to build in-house effectively, and may take away from the revenue generating efforts your DevOps teams are charged with. Rackspace has a large cloud tools marketplace with many security-focused partners like Alert Logic, CloudPassage, Imperva, RSA, and many others.

Rackspace Cloud Tools: **https://cloudtools.rackspace.com/home**

7. Summary

Managing security in the cloud is about adapting to an agile world where development is rapid and resources are variable. Traditional security controls and proper perimeter defenses have not gone away, but additional tools and assessment methodologies should be leveraged to offset risks associated with rapid development and multi-tenant service provider environments to protect sensitive data. Here are some concepts we covered that will help you adapt in an agile cloud world:

1) TRAINING AND AWARENESS

a. Teach your staff how to protect their own systems and avoid social engineering threats

b. Enable system engineers to learn newer infrastructure automation tools

c. Expose developers to training on application security best practices and common attacks

2) DEFINE STANDARDS FOR INFRASTRUCTURE AND DEVELOPMENT

a. Follow standard systems security best practices and automate them

b. Encrypt all of your secrets and manage your data effectively

c. Aggregate logging at all levels of your environment and automate a meaningful notification system

3) INTEGRATE SECURITY INTO YOUR LIFE CYCLE

a. Create threat models of your applications and focus on securing critical portions

b. Break down security scanning to align them with code sprints

c. Enable development teams to conduct security tests in accordance with your needs

4) TECHNOLOGY CONSIDERATIONS

a. Consider pros and cons of leveraging multiple technology platforms for hybrid cloud solutions

b. Tier highly sensitive data in single-tenant environments while leveraging public cloud services for your more elastic workloads

c. Leverage security partners and service providers to enable your teams to focus on revenue-generating activities

When adapting security to the cloud model and leveraging these best practices we believe a cloud application can be as secure, or more secure, than an application deployed in a traditional environment. Based on the evolution of cloud technologies and the modernization of the toolsets that operational teams, developers and security engineers leverage, we expect that over time the concerns about security on public cloud services will diminish. Security will still be an important topic, but not because of inherent limitations or security gaps in the technology on the cloud.

If you have questions or would like to discuss security in depth with our cloud experts, reach out to your trusted advisors at Rackspace.

References:

http://www.sans.org/critical-security-controls/ – SANS Twenty Critical Controls for Effective Cyber Defense

https://www.owasp.org/index.php/Top_10_2013-Top_10 – OWASP 2013 Top 10 Application Security Flaws

https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3/ – CSA Cloud Controls Matrix v3

http://www.rackspace.com/security/ – Rackspace Security Portal

About Rackspace

Rackspace® Hosting (NYSE: RAX) is the open cloud company, delivering open technologies and powering hundreds of thousands of customers worldwide. Rackspace provides its renowned **Fanatical Support®** across a broad portfolio of IT products, including Public Cloud, Private Cloud, Hybrid Hosting and Dedicated Hosting. The company offers choice, flexibility and freedom from vendor lock in.

GLOBAL OFFICES

Headquarters Rackspace, Inc.
5000 Walzem Road | City of Windcrest, San Antonio, Texas 78218 | 1-800-961-2888 | Intl: +1 210 312 4700
www.**rackspace**.com

UK Office
Rackspace Ltd.
5 Millington Road
Hyde Park Hayes
Middlesex, UB3 4AZ
Phone: 0800-988-0100
Intl: +44 (0)20 8734 2600
www.rackspace.co.uk

Benelux Office
Rackspace Benelux B.V.
Teleportboulevard 110
1043 EJ Amsterdam
Phone: 00800 8899 00 33
Intl: +31 (0)20 753 32 01
www.rackspace.nl

Hong Kong Office
9/F, Cambridge House, Taikoo Place
979 King's Road,
Quarry Bay, Hong Kong
Sales: +852 3752 6465
Support +852 3752 6464
www.rackspace.com.hk

Australia Office
Level 4, 210 George Street,
Sydney, NSW 2000
Phone: 1-800-722577
www.rackspace.com.au

rackspace®
the open cloud company