Securing Cloud Applications

What Business Executives Need to Know Before Developing and Deploying on the Cloud

Prepared by:
Russ Schafer, Benjamin Dunn, Nancy Xiao, Eileen Jiang, Saswat Nanda, Sesh Murthy, Prasanna Mulgaonkar

July 2015

CONTENTS

EXECUTIVE SUMMARY

There's no question that the public cloud offers the potential for tremendous benefits when building and managing applications. Developing an enterprise application in the public cloud has become so easy that IT departments and business units have started to adopt this technology for cost and flexibility. But for many enterprises, security risks continue to be a big sticking point, severely limiting their ability to take advantage of the public cloud.

Consider a scenario where a marketing manager needs to quickly create a consumer loyalty application in response to competition. To accelerate time to market, the business might create an application on the public cloud without fully understanding the security requirements and risks. Novice deployments like these are neither compliant with corporate security policies nor adequately monitored throughout the lifecycle of the application. These two key factors increase security risk and may negate the business benefit of creating the new application. To solve this dilemma, enterprises need to make security compliance as simple as provisioning virtual machines.

Consistent and Cost Effective Public Cloud Security: To ensure consistent security compliance across the enterprise, application teams and IT organizations need to apply standard security profiles and controls across private and public cloud infrastructures. Unfortunately, manually applying these profiles is labor intensive and slow. In addition, manual processes are error prone thereby increasing security risk. For these reasons, manual security compliance is 40% of the cost of managing virtual applications in the cloud. Automating cloud security compliance is therefore critical.

One-Touch Security Compliance Across Public and Private Clouds: Raxak Protect^{TM} is a SaaS-based service that empowers IT and application development teams by automating security compliance across private and public clouds. Raxak Protect delivers one-touch security provisioning, continuous compliance, and automated remediation for both novice and expert users. Starting with provisioning and continuing through the application lifecycle, Raxak Protect enables secure, efficient, cost-effective, and error free cloud application deployment.

Automating Security Compliance Through IT Service Management Tools: IT organizations have already trained their business units to request IT services through a services catalog. Cloud Raxak has made it easy for novice and expert users to build applications with built-in security compliance by integrating automated cloud security compliance into the IT service catalog, starting with the HP Cloud Service Automation (CSA).

With over 500 customers, HP CSA is the industry's leading provider of cloud service automation software. The HP CSA and Raxak Protect integration provides the industry's first service management capability with security postures integrated in the Service Catalog. HP CSA clients can now deploy assets in both private and public clouds with the corporate security posture uniformly integrated.

Cloud Raxak simplifies and automates cloud security compliance. It thereby eliminates the risk of moving to the cloud, and enables customers to leverage the flexibility and cost advantages of the cloud.

Third party trademarks and names are the property of their respective owners.

BENEFITS OF CLOUD COMPUTING

Public clouds such as Amazon, Azure, Google, and SoftLayer can be fast, inexpensive and offer rich development environments including Infrastructure as a Service (IAAS) and Platform as a Service (PAAS). Together cloud services like IAAS and PAAS, make it faster and cheaper to develop and deploy on the cloud. It is also easy to make applications highly available and durable.

> *The Brookings Institution estimates that Federal agencies have experienced a* ***50%*** *in savings after moving to the cloud.*

Fast Stand up and Provisioning : With a few minutes and a credit card, a developer can stand up an application infrastructure for development, test or production. This greatly reduces time for setting up new environments and speeds up development. By contrast, traditional data centers take months to order and install the hardware and software needed for developers and testers.

Cheaper Infrastructure: Compared to on-prem infrastructure, the cloud is typically cheaper. For example, the Brookings Institution estimates that Federal agencies have experienced a 50% savings after moving to the cloud *(West 2010)*.

IAAS Provides Flexible Scaling with Identical Infrastructure: Cloud infrastructure as a service (IAAS) enables resources to be ordered on demand, scaled elastically, and is available in multiple locations. In contrast, the on-prem IT environment is relatively fixed, where new computing resources and locations need to be planned in advance.

Pay for Use: For the cloud, you only pay for what you use. On-prem resources have to be paid for in advance, and amortized over all the applications that use them.

PAAS Delivers Pre-configured Software Services: Cloud offerings such as platform as a service (PAAS) provide pre-configured services for setting up a development environment. This frees up time and costs since the developer does not have to worry about on-prem duties like provisioning the infrastructure, installing and configuring software, and managing the service. These tasks are costly because they require system administrators and take months to complete.

With so many advantages, why hasn't everyone just moved to the cloud? Security compliance risk is the biggest inhibitor to moving applications to the cloud.

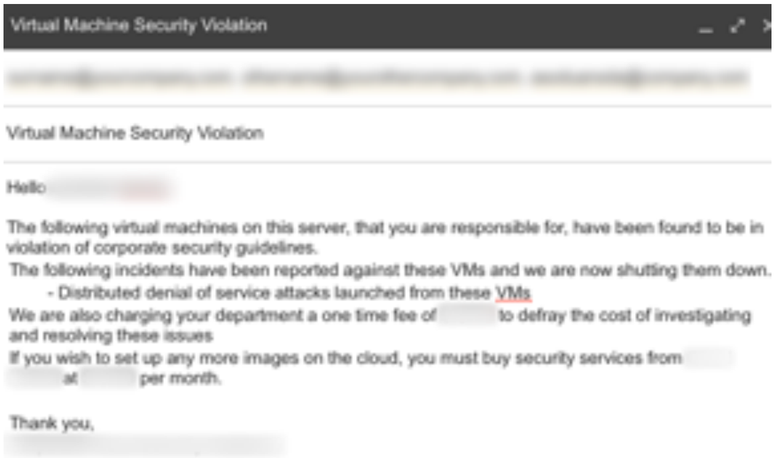
SECURITY COMPLIANCE RISKS

Security compliance is consuming 40% of the cost of managing applications in the cloud and growing. To provide some perspective, there are thousands of security compliance settings required for the operating system, tools and application components of a virtual machine in the cloud. Manual security compliance is slow, error prone, and increases security risk, so an automated solution is needed.

The following security compliance use case is based on our work with a large systems integrator and Fortune 50 company. Based on changes in the market, a Line of Business (LOB) executive decided they needed to quickly create a consumer loyalty application. To accelerate time to market, the LOB decided to use the public cloud. To do this, IT required the LOB to take on the risk of maintaining security compliance.

> *Given that security compliance can be up to **40%** of the cost of managing virtual applications in the cloud, automating these processes is critical.*

With thousands of security settings, the LOB application development team did their best but left the application virtual machine insufficiently protected. This lead to a security breach. The Chief Information Security Officer (CISO) deluged the LOB executive with email requests *(see figure 1)* to resolve the security issues. As a result, the LOB had to shut down the development environment for several months while they studied the problem to make sure it did not recur.



Virtual Machine Security Violation

[redacted]

Virtual Machine Security Violation

Hello [redacted]

The following virtual machines on this server, that you are responsible for, have been found to be in violation of corporate security guidelines.
The following incidents have been reported against these VMs and we are now shutting them down.
- Distributed denial of service attacks launched from these VMs
We are also charging your department a one time fee of [redacted] to defray the cost of investigating and resolving these issues
If you wish to set up any more images on the cloud, you must buy security services from [redacted] at [redacted] per month.

Thank you,
[redacted]

Figure 1: Security compliance violation email example

This is a classic example of the security risk that organizations face with novice LOB application developers. Novice deployments by LOB application development teams are usually not compliant with corporate security policies or adequately monitored throughout the lifecycle of the service, and thus increase the potential for security breaches.

What is the technical scope of the cloud security compliance challenge? There are thousands of security compliance parameters for each application deployed in a virtual machine. Multiply that by the numerous applications that an enterprise might deploy across business units, and you can see why the security compliance technical challenge gets exponentially harder.

TECHNICAL CHALLENGES WITH SECURITY COMPLIANCE

Noncompliant Cloud Templates Propagate Security Holes

A common practice for novice developers using the cloud is to speed up the development process by using template virtual machines for their cloud applications. However, unless the templates are continuously vetted for security, this increases the potential for security breaches

__50%__ of cloud application security parameters are incorrectly configured but __95%__ of those errors could be corrected through automation.

Cloud Raxak's research has shown that *50% of cloud application security parameters are not being set correctly* by application developers who use the public cloud. We confirmed this by checking the security settings for the virtual machines from major cloud providers against industry standard DISA security implementation guidelines. Trying to update thousands of security parameters manually, is slow, error prone, and increases security risk. The good news is that *95% of security parameters can be configured automatically.*

Compliance Requires Setting Thousands of Security Parameters for OS, Tools and Apps

In cloud applications, the entire application stack above the hypervisor is software defined. There could be over a thousand parameters *(see figure 2)* that must be identified, set and checked for security compliance.

Standard application packages and tools like databases, web servers, app servers and firewalls also have a long list of security settings. The rest of the virtualized network and storage infrastructure also needs to be correctly configured for security compliance purposes. Most users rely on the cloud service provider to configure these layers correctly.

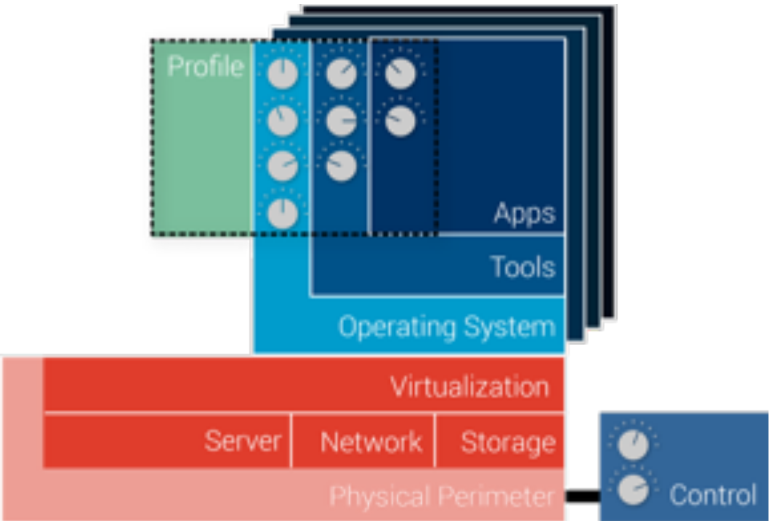


Figure 2: Thousands of security parameters need to be set across the operating system, tools and applications.

Current Security Compliance Solutions are Inadequate

Current methods are inadequate in addressing this critical security challenge. Manual setting and remediation of these security configurations is not feasible in the cloud because security attacks are automated and can dynamically morph into new attacks.

The only proactive and financially feasible solution to this problem is to automatically apply security profiles when an application is created, and then audit and remediate that application throughout its complete lifecycle.

AUTOMATING AND SIMPLIFYING CLOUD SECURITY COMPLIANCE

Simplifying and automating cloud compliance enables novice users to use the cloud without risk, speeds up DevOps, cuts compliance costs, and eliminates human error. This facilitates moving workloads to the cloud.

Raxak Protect Overview

Raxak Protect^{TM} is a SaaS-based security offering that empowers IT and application development teams by automating security, and ensuring compliance across their private and public clouds. Starting with provisioning, Raxak Protect provides continuous compliance throughout the application lifecycle. This enables cloud apps to be deployed securely, quickly, cost-effectively, and without human error.

Security compliance comprises 40% of the cost of managing applications in the cloud. Raxak Protect automates these processes, providing significant savings. Through intelligent automation, Raxak Protect makes compliance as easy as spinning up a server in the cloud. By integrating security compliance directly into the cloud application development, test, and operational processes, Raxak Protect accelerates deployment, reduces costs, and simplifies auditing.

Raxak Protect Features and Benefits

Raxak Protect:

- Automates security compliance throughout the entire application lifecycle.
- Delivers one-touch security compliance for both novice and expert users.
- Enables cloud apps to be deployed securely, quickly, cost-effectively, and without human error.
- Minimizes novice user risk through service catalog tools like HP Cloud Service Automation.
- Enables consistent app security compliance across private and public clouds.

Table I summarizes the key features required for a cloud security compliance solution. The following sections of this white paper detail the need for each security compliance component, and how Raxak Protect implements them.

Table I: Key Components required for a Cloud Security Compliance Solution

COMPONENT	VALUE
I. Scalable and Flexible API-based Architecture	– Scales to variable cloud workloads. – Deployed as SaaS or on-prem appliance.
II. Agent-less Security Compliance	– Secure, efficient and non-intrusive.
III. Standardized and Custom Security Profiles	– Standard security profiles for DevOps. – Custom security for unique workloads.
IV. Complete Application Lifecycle Security Compliance	– Security throughout application lifecycle. – Automatic correction of errors. – More accurate and simplified audits
V. One-touch Security Compliance Through Service Catalog integration	– Eliminates novice user compliance risk. – Seamless integration with tools like HP CSA.
VI. Consistent Security for Private and Public clouds	– Seamless security posture across clouds.

CLOUD SECURITY COMPLIANCE COMPONENTS

I. Scalable and Flexible API-based Architecture

Modern cloud workloads are built to scale-out using instantaneously available cloud resources. Typical examples include high performance computing, Hadoop, e-commerce, media-streaming, and cloud native workloads like Netflix. In fact, most applications that are built to run natively on the cloud use elastic scaling features. This poses two problems for compliance systems:

- Assets can be created and destroyed within minutes. In order to ensure that these workloads are compliant, it is necessary to immediately attach a profile to the asset, verify compliance, log findings, and continuously monitor the compliance status. The compliance system therefore needs to support rapid bursting.
- Cloud workloads can grow and use an enormous number of assets. It is not unusual to see tens of thousands of virtual machines in a high performance computing cluster, where the compliance system has to quickly apply and check thousands of rules on thousands of virtual machines within minutes.

> *"Cloud Raxak makes the application of a security profile to a VM as simple as spinning up the VM in a cloud. For highly elastic applications like Hadoop, this simplifies the process of securing the application."*
>
> **- David Richards, CEO, WanDisco**

Raxak Protect^{TM} Agent-less and Scalable SaaS Architecture: Raxak Protect's compliance platform is based on a highly scalable, agent-less, API driven, SaaS architecture *(see figure 3)*. It can also be run on-prem as an appliance. Raxak Protect is designed with a robust cloud-scale architecture that can rapidly handle large load changes without impacting the performance of each asset. Raxak Protect makes optimal use of design patterns that build multi tenancy, isolation, and redundancy as the basis of our operation. This modern architecture enables the platform to scale to cloud workloads of any size.

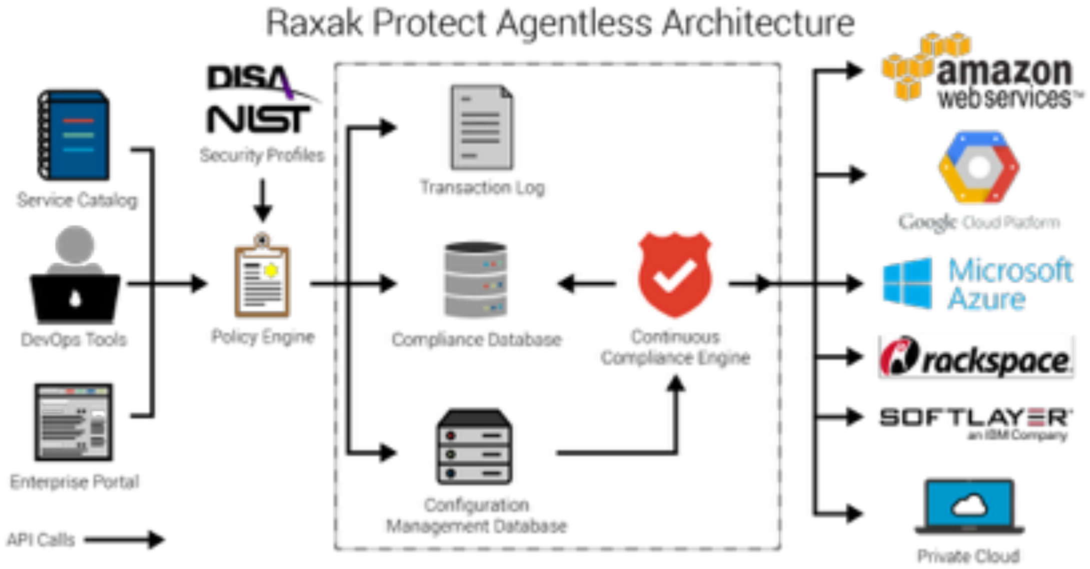


Figure 3: Raxak Protect agent-less and scalable SaaS architecture

II. Agent-less Security Compliance

Challenges with Agent-based Approaches

Using agents within cloud application virtual machines is a simple of way of ensuring compliance, but can lead to many other problems inherent in agent-based approaches to enterprise solutions. Unless a task absolutely requires agents, it is strongly recommend against using them in security compliance systems. The three key challenges with using agents in security compliance are:

- ***Insecure:*** Agent-based systems are susceptible to malware attacks. Malware scans for and and turns off agents. This compromises the agent and thereby compromises application security compliance.

- ***Intrusive:*** Agent-based systems consume app resources without the system owner having any control. In addition, these agents are frequently deleted due to resources issues leaving apps unprotected.

- ***Inefficient:*** The interaction of the application and the agent needs to be rigorously tested in advance of deployment. When the agent needs to be upgraded, the process can be difficult and require downtime.

Benefits of Raxak Protect^{TM} Agent-less Security Compliance

Raxak Protect is an agent-less SaaS solution that is built to access the application workload being tested on standard encrypted network channels. As outlined below, Raxak Protect agent-less security compliance is more secure, non-intrusive, and highly efficient.

- ***More Secure***
  Resistant to Malware attacks: Since the compliance scans are initiated by the external Raxak Protect SasS servers, any security breach like malware will not compromise application security scanning and remediation. Since there are no local agents in the application, the malware cannot disable the security.
  More Reliable and Trustworthy Security: Advanced persistent threats (APTs) and kernel rootkits cannot modify the security scanners, so the security compliance checks are more reliable and trustworthy.

- ***Non-Intrusive***
  Agent-less systems host the security compliance scanner on the SaaS servers, so the impact on system resources is extremely light. Through intelligent automation, it checks each security parameter without impacting application performance. In contrast, agent-based systems consume more resources because of extensive book-keeping, logging, and other unpredictable administrative actions.

- ***Highly Efficient***
  ***Scales Dynamically**:* Raxak Protect is architected to grow and scale with the workloads being tested. This is critical in high performance computing in which the workloads grow and shrink dynamically.
  Consistent Security Everywhere: By updating security policy through a central server, Raxak Protect can ensure consistent and updated security compliance across every workload without needing downtime to have local agents updated. With new security flaws surfacing all the time, Raxak Protect keeps your application workloads protected with the latest in security compliance parameters.

The net result is that agent-less compliance systems are more secure, non-intrusive, and highly efficient.

Third party trademarks and names are the property of their respective owners.

III. Standardized (DISA STIGS) and Custom Security Profiles

Standard Security Profiles- DISA STIGS

One of the common issues that novice users face when using the cloud is understanding how to secure workloads. Fortunately there are numerous security standards that outline the necessary measures for security.

Since 1998, Defense Informations Systems Agency's (DISA) Field Security Operations has played an integral role enhancing the Department of Defense's security systems by providing Security Technical Implementation Guides (STIGS), which contain technical guidance to lock down information systems and software that might otherwise have vulnerabilities to malicious attacks. These guidelines are an excellent starting point for ensuring security compliance of your infrastructure and specify the desired security state of your computer assets.

Raxak Protect Provides Out of the Box Security Profiles

Cloud Raxak keeps up with the rapidly changing security compliance landscape so users don't have to. Raxak Protect provides out of the box industry standard profiles based on NIST and DISA STIGS. These security profiles are API based so they are constantly updated.

Raxak Protect^{TM} Supports Custom Profiles

Senior executives, like the Chief Information Security Officer (CISO), should have the ability to create custom security profiles through the compliance system. The Raxak Protect profile editor gives CISOs the freedom to make three kinds of adjustments:

- Disabling rules in a standard profile.
- Adding rules to a standard profile.
- Customizing a rule based on parameters to suit their enterprise. For example the rule: "No world readable files" can be customized as "No world writable files except for a <whitelist of enterprise exceptions>". This prevents unnecessary findings and tickets from being created.

With Raxak Protect, CISOs can use the flexibility of software defined security to apply targeted profiles on a set of computer assets based on their needs. For example, the set of virtual machines in the database layer can be configured to drop all incoming communications except from the application server. In addition, different profiles can be created to optimize for different phases in the application lifecycle. For example, applying more flexible rules during development and then transitioning to stricter controls during production.

IV. Complete Application Lifecycle Security Compliance

Knowing what to do for security compliance is only part of the story. Manual application of security profiles is ineffective, inefficient, and inconsistent on a cloud scale. To provide complete application lifecycle security compliance, three features are critical:

- Automated application of security profiles at the time assets are created.
- Automated remediation of findings.
- Logging and audit-ready reporting of findings and remediation actions.

Raxak protect provides all three capabilities and thereby provides complete app life-cycle compliance.

Automating Application of Security Profiles

A Raxak Protect^{TM} profile is associated with an asset at the time of creation in one of two ways:

- Through integration with the enterprise service catalog. The composite service calls the Raxak Protect API with the profile and the list of assets newly created.
- The autoscaling program calls the Raxak protect API every time a new asset is created.

Once the profile is applied to the target computer assets, they are continuously monitored for any deviation from the state specified in the profile; any deviations are recorded as findings.

Logging and Audit-ready Reporting of Findings

Raxak Protect records all findings and remediation actions in a non-repudiatable log. This log is retained according to compliance policies. It is best to examine this log for correlation with security incidents and change procedures.

Automatic Remediation of Findings

Raxak Protect provides the capability to automatically remediate findings. This is important for cloud workloads that are not under change control such as high performance computing, Hadoop, development, and test workloads. Remediating findings as they are detected improves the security posture of these workloads. Remediations are logged and should be examined later.

For workloads that are under change control, Raxak protect creates a ticket that documents the security violation and the manual remediation action by Raxak Protect. These tickets can be remediated in the change control window by the system administrator using the Raxak Protect tool.

V. One-touch Security Compliance through Service Catalog Integration

Eliminates Novice User Compliance Risk

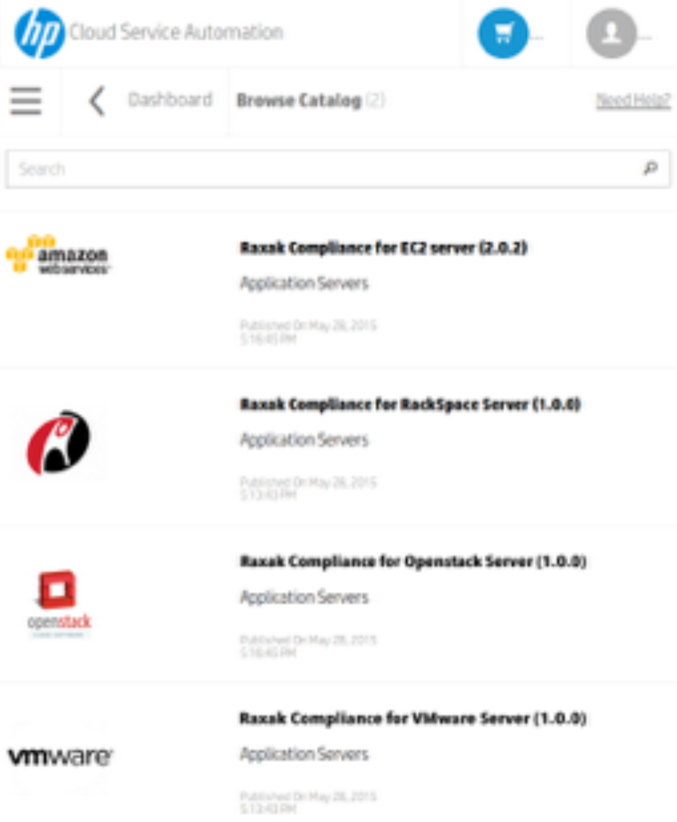
IT organizations have already trained their business units to request IT services through a service catalog. Integrating automated cloud security compliance into the service catalog will make it easy for novice and expert users to develop applications with built-in security compliance.

One Touch Security Application through Service Catalogs

With over 500 customers, HP's Cloud Service Automation is the industry's leading provider of Cloud Service Automation software. The HP CSA and Raxak Protect^{TM} integration provides the industry's first service management capability with security postures integrated in a service catalog *(see figure 4)*. This provides a turn-key solution for simple and quick provisioning of security compliant applications on both public and private clouds.

> *"The tight integration with HP service management tools provides enterprise customers a turn-key solution for automating application security compliance across both public and private clouds."*
>
> **-Atul Garg, VP/ GM, HP Cloud and Automation**

Once the cloud application is deployed, HP CSA calls the Raxak Protect API to enforce the corporate compliance profile. This enforcement continues on a specified periodic basis through the lifecycle of the asset. The compliance logs and reports are stored in an audit-ready immutable form, and seamlessly integrated with the HP CSA interface.



Raxak Compliance for EC2 server (2.0.2)
Application Servers
Published On May 28, 2015 5:16:45 PM

Raxak Compliance for RackSpace Server (1.0.0)
Application Servers
Published On May 28, 2015 5:13:43 PM

Raxak Compliance for Openstack Server (1.0.0)
Application Servers
Published On May 28, 2015 5:16:45 PM

Raxak Compliance for VMware Server (1.0.0)
Application Servers
Published On May 28, 2015 5:13:43 PM

Figure 4: One-Touch compliance through the IT service catalog using HP's industry-leading Cloud Service Automation software.

Third party trademarks and names are the property of their respective owners.

VI. Consistent Security Profile Across Public and Private Clouds

Public and Private Clouds

The public cloud is commonly used as a development and test environment. The final deployment platform is a private cloud on-prem. In these circumstances, it is desirable for the compliance system to apply the same security profile across both the private on-prem and public cloud deployments.

Raxak Protect enables Consistent Security Compliance across Public and Private clouds

Raxak Protect^{TM} enables enterprises to develop once and deploy anywhere. The security profile that is attached to the application at the start of development, apply through the complete application lifecycle. This holds true whether the application is deployed on the public cloud, or on-prem. The key features that make it easy to achieve consistent security compliance across all assets, on- and off-prem are summarized in Table II below.

Table II: Raxak Protect Features for Consistent Security Compliance Across Public and Private Clouds

FEATURE	VALUE
SaaS or On-prem Appliance	– Some enterprises do not allow shared models for compliance. – Raxak protect can operate as a SaaS or on-prem as an appliance.
Virtual and Bare Metal	– On most public clouds, a customer is restricted to virtual machines. However, on-prem, performance sensitive workloads such as databases often run bare-metal. – Raxak Protect provides flexibility by supporting both virtual and bare-metal resources.
Novice User Support	– The enterprise service catalog is a proven method to support novices users with cloud security compliance. – Raxak Protect is integrated into the service catalog of leading service management tools like HP Cloud Service Automation.
DevOps Support	– While developers are experts at standing up efficient applications, they are not skilled in security compliance. – Raxak Protect enables developers to add automated security compliance during development, so the application can be monitored throughout it's lifecycle.

CONCLUSION

Enterprises want to take advantage of the flexibility and cost benefits of running applications in the public cloud. The challenge for the Chief Information Security Officer is to achieve consistent application security compliance across both private and public clouds. Security compliance is 40% of the cost of managing virtual applications in the cloud, so automating these processes is critical.

Raxak Protect^{TM} solves this dilemma by automating and simplifying security compliance across public and private clouds. Starting with provisioning, Raxak Protect provides continuous compliance throughout the application lifecycle. This enables cloud apps to be deployed securely, quickly, cost-effectively, and without human error. Through intelligent automation, Raxak Protect makes compliance as easy as spinning up a server in the cloud. By integrating security compliance directly into the development, test, and operational processes, Raxak Protect accelerates deployment, reduces costs, and simplifies auditing. Raxak Protect key features and are outlined in Table III below.

Table III: Raxak Protect Features and Benefits

FEATURE	BENEFITS
Automated, Efficient and Consistent Across Public and Private Clouds	– Automated compliance enables cloud apps to be deployed securely, quickly, cost-effectively, and without human error – Consistent security profiles across public and private clouds.
Scalable and Flexible API-based Architecture	– Architecture dynamically scales with variable app workloads – Flexibility to deploy as SaaS or on-prem appliance
Agent-less Security Compliance	– Agent-less security compliance systems are more secure, non-intrusive, and highly efficient. – Resistant to malware attacks, more reliable, don't require resources that impact app performance, don't require system downtime to update, and scale dynamically to app workloads.
Complete Application Lifecycle Security Compliance	– Security throughout application lifecycle. – Automatic correction of errors. – More accurate and simplified audits
One-touch Security Compliance through Service Catalog integration	– Eliminates novice user compliance risk – Provides a turn-key solution for simple and quick provisioning of security compliant apps on both public and private clouds. – One-Touch compliance through the IT service catalog using HP's industry leading Cloud Service Automation software.
Standard and Customer Security Profiles	– Security templates based on industry standard DISA STIGS – Standardized profiles make it easy to deploy security compliance across all virtual machines in private and public clouds. – CISO's can create custom profiles to match workload security and compliance requirements.

ABOUT CLOUD RAXAK

Cloud Raxak automates and simplifies the delivery of cloud security compliance across enterprises. Raxak Protect is a unique SaaS security solution that allows cloud users to apply DISA and NIST approved technical controls across private and public cloud virtual machines. Cloud Raxak is located in Los Gatos, California.

Cloud Raxak is an HP Gold Partner and integrated into HP's industry leading Cloud Service Automation software. Cloud Raxak is also an IBM Global Entrepreneur and supports the IBM Cloud platform.

Gold Partner

IBM Global Entrepreneur

REFERENCES

"Business Agility in the Cloud." Harvard Business Review. June 2014. Verizon. 13 July 2015. https://hbr.org/resources/pdfs/tools/Verizon_Report_June2014.pdf

Carvaolho, Larry. Marden, Matthew. "Quantifying the Business Value of Amazon Web Services." IDC. May 2015. Amazon. 13 July 2015. http://d0.awsstatic.com/analyst-reports/IDC_Business_Value_of_AWS_May_2015.pdf

Bernd Grobauer, Tobias Walloschek, Elmar Stöcker, "Understanding Cloud Computing Vulnerabilities", IEEE Security & Privacy, vol.9, no. 2, pp. 50-57, March/April 2011, doi:10.1109/MSP.2010.115

West, Darrell. "Saving Money Through Cloud Computing." The Brookings Institution. N.p., 07 Apr. 2010. Web. 13 July 2015. http://www.brookings.edu/research/papers/2010/04/07-cloud-computing-west