Craft a cloud service security policy

Discover how purpose, scope, background, actions, and constraints shape a cloud security policy

Judith M. Myerson

June 23, 2011

For economic reasons, often businesses and government agencies move data center operations to the cloud whether they want to or not; their reasons for not liking the idea of hosting in a cloud are reliability and security. To help ease business security concerns, a cloud security policy should be in place. In this article, the author explains how to craft a cloud security policy for managing users, protecting data, and securing virtual machines.

A carefully crafted security policy outlines what cloud computing service consumers and providers should do; it can save providers many hours of management time if they develop a security policy.

The security policy is shaped by four things:

- What type of cloud service the provider hosts: Software as a Service (SaaS), Platform as a Service (PaaS), or Infrastructure as a Service (IaaS).
- Whether it is public or private.
- How much control the consumer has over the operating systems, hardware, and software.
- How the user, resource, and data requests threshold policies are applied to each cloud service type.

Other variables to consider that can affect the policy landscape are:

- What proactive behavior application changes took place in order for an in-house application to work well and be secured in the cloud.
- Whether the provider is internal within an organization-controlled data center or hosted externally by a member of the telecommunications industry.
- Whether the type of industry the consumer represents is broad, such as retail, energy and utilities, financial markets, health care, or chemical or petroleum.

To satisfy consumer demand to review a security policy, all providers should provide consumers with copies of the policy (as well as threshold policies discussed in a previous article). The providers should encourage consumers to send security questions that might need to be resolved or require negotiation before the consumer rents or subscribes to a cloud service type.
This article starts with a description of the security focus for each cloud type and how you can use a checklist to get started on writing the policy with examples on purpose, scope, background, actions, and constraints.

What security focus? Watch the drama

A cloud security policy focuses on managing users, protecting data, and securing virtual machines. It is influenced by how much control a consumer can have over deployed applications, operating systems, hardware, software, storage and networking for a cloud delivery model.

Now watch the drama in three short acts.

Act I: Managing access with SaaS

In the first act, the SaaS security policy focuses on managing access to specific applications rented to consumers whether they are private individuals, businesses, or government agencies. Managing access includes risk mitigation of identity theft or spoofing.

Here are the control variables that influence SaaS security focus:

- **SaaS end user**: The only control an end user has is to access the provider’s application from a desktop, laptop, or mobile.
- **SaaS provider**: At a minimum, the provider controls operating systems, hardware, network infrastructure, application upgrades, and patches. The provider sets the user threshold levels.

Act II: Protecting data with PaaS

In this second act, the PaaS security policy focuses on protecting data in addition to managing access to applications. Data protection includes risk mitigation of the PaaS as command and control centers to direct operations of a botnet for use in installing malware applications.

Here are the control variables that influence PaaS security focus:

- **PaaS application developer**: The developer controls all the applications found in a full business life cycle created and hosted by independent software vendors, startups, or units of large businesses. The developer builds, deploys, and runs, say, a custom retail management application, and manages upgrades and patches to all functionalities of this application. As part of the life cycle, the developer uses spreadsheets, word processors, backups, billing, payroll processing, and invoicing.
- **PaaS provider**: At a minimum, the provider controls operating systems, hardware, network infrastructure, and resource management. The provider sets the user, resource and data requests threshold levels.

Act III: Managing virtual machines with IaaS

In this final act, the IaaS security policy focuses on managing virtual machines in addition to protecting data and managing user access to the infrastructure of traditional computing resources underlying the virtual machines. Management of virtual machines includes risk mitigation of the IaaS as command and control centers to direct operations of a botnet for use in malicious updates of the virtual infrastructure. The control variables that influence IaaS security:
• **IaaS infrastructure and network specialist:** The specialist controls the operating systems, network equipment, and deployed applications at the virtual machine level. The infrastructure specialist can scale up or down virtual servers or blocks of storage area.

• **IaaS provider:** At a minimum, the provider controls the infrastructure of traditional computing resources in the cloud environment. The provider sets the user, resource and data requests threshold levels.

**Pencils ready: Your checklist**

Don't know where to start? No worries; I present you with a checklist of what should be included in a security policy. Put the pencil behind your ears or in your jacket pocket so you will not lose it.

In this simplified scenario, here are some hints for each checklist item as follows.

• **Purpose:** What's it about? I'm curious
• **Scope:** Don't jump over a fence
• **Background:** Want to know more?
• **Actions:** Ready? Roll up your sleeves
• **Constraints:** Work with them

Briefly state what the security policy is intended to do. You can use a template like this to give you an idea how to state the purpose:

**Purpose:** What's it about? I'm curious

The purpose of the security policy is to mitigate risks of a cloud service type being installed with malware applications designed to maliciously raise:

• The resource threshold level originally set by the Resource Threshold Policy. Abnormally high levels indicate malicious resource instances may cause guaranteed levels of service availability set forth in a service level agreement (SLA) to slide. One risk mitigation tool to consider is a threshold level monitoring of resource instances.

• Maximum levels originally set by User Threshold Policy (based on limits in a user license). When the maximum level goes above the user limit, a hacker or disgruntled employee could pose as an authorized user when they are not. Some risk mitigation tools to consider are personnel background checks and revocation of user access.

• Data request threshold levels originally set by the Data Request Threshold Policy. Abnormally high threshold levels could cause high network latency due to backup of the data requests in a queue. One risk mitigation tool to consider is a threshold level monitoring of data requests.

**Scope: Draw a boundary around your policy, please**

Define the scope by "drawing" a boundary around the security policy. Within its boundaries, specify which cloud service type the provider hosts and the consumers rents and subscribe, what threshold policies are applied, and how the security policy is applied.

For example, if the provider hosts all three cloud service types, he needs to state whether:
• The end user rents on a specific application within a threshold level set by User Threshold Policy.
• The application developers rent only the PaaS to customize or change parameters to a specific SaaS application running on the PaaS and whether the PaaS is within the threshold levels set by User, Resource, and Data Request Policies.
• The application developers and their SaaS users can purchase subscriptions to a co-resident SaaS application on the PaaS and whether they are within all three types of threshold levels.
• The infrastructure and network specialist rents the IaaS to build a virtual infrastructure environment and to run the PaaS on this IaaS and whether they are within all three types of threshold levels.

For each of the above four scenarios, the provider needs to find out if the consumer will stay within the fence (comply with the terms of the security policy on access controls, data protection, and virtual machine management). If the consumer strays out of the fence after agreeing to comply, the consumer runs the risk of violating the policy. In this case the provider must indicate the consequences of not complying to make sure the consumer stays within the fence.

Here is a template to use when you state the scope:

This policy applies to all SaaS end users, PaaS application developers, and IaaS infrastructure and network architects. They must consent to all of the provisions of this security policy and agree to comply with all of its terms and conditions on access controls, data protection and virtual machine management. Any end user, developers and network architects whose actions violate this policy on another related threshold policies and IT policy and regulations shall be subject to limitations or loss of service with the provider.

**Background: Look what's behind the policy**

The first things the consumer wants to know are whether the provider is internal or external and what the boundaries of controls management between the provider and the consumer are (for example, the SaaS end user has the least control), how the provider would manage access controls, provide data protection, and manage virtual machines and respond to cloud security attacks or incidents.

Next, the consumer wants to know what security focus for user, resource, and data request threshold policy is for SaaS, PaaS and IaaS. The consumer also wants to know how threshold levels are related to guaranteed levels of service availability as set forth in a service level agreement (SLA).

In the Christmas buying crunch drama (see [Build proactive threshold policies on the cloud](#)), the consumer sees resource instances are surging beyond the threshold level causing the system to create additional resource instances to balance workload demands dynamically in the cloud. This required additional users, data requests and security.

Then the consumer sees how performance is sliding down due to unexpected system problems, causing threshold levels for user, resource, and data requests to be out of alignment with the
original settings established in the threshold policies. Or the consumer experiences a cloud (and threshold levels) crash or attack in the middle of processing a business task or developing an application; then finds out too late the cloud has been used as a command and control center to direct the operations of a botnet to install malware applications.

In either case, the consumer wants to know how the security policy covers the issues of restoring the system (and threshold levels) and how quickly he gets credits, free time, or the right to terminate as set forth in the SLA.

Here is a template you can use to give you an idea of what to include.

The cloud service provider is hosted externally by IBM®, a member of the telecommunication industry.

If a surge in workload demands, users, and data requests exceed threshold levels and will cause system performance to slide down from the guaranteed levels of availability for 30 days, the provider must give consumers credits, free time, or the right to terminate the service as set forth in the SLA. The provider must notify the consumer of the exceptions or constraints to the threshold and security policies.

A user license contains three types of maximum limits:

- Users accessing concurrently the application.
- Resource instances to be allocated to each user.
- Data requests the user can handle during a surge in workload demands.

**Actions: Roll up your sleeves**

Here are 10 suggestions for actions to take to make consumers happy:

- **Action #1.** Send consumers copies of the security policy for review and questions to be resolved before the consumer signs up for a cloud service.
- **Action #2.** Indicate in a SaaS user license the maximum limit on concurrent users, resource instances for those users and data requests each user can handle.
- **Action #3.** Refer to threshold levels in the resource, user, and data requests threshold policies and each policy to the guaranteed levels of service availability.
- **Action #4.** Send notice to the consumer on planned proactive behavior changes to the application developed at a data center intended to replace the application currently running in the SaaS cloud.
- **Action #5.** Indicate whether cloud access is 24 hours a day or during normal working hours.
- **Action #6.** Permit the PaaS application developers and their SaaS users to subscribe to a co-resident SaaS application.
- **Action #7.** Require background checks on all intended cloud users to before granting them access to the cloud. The depth of background checks depend on the type of cloud service, whether the cloud is public or private, and the type of industry the intended users represent.
- **Action #8.** Require training programs for approved cloud users on security awareness and labeling and handling of data.
- **Action #9.** Require assurance that duties are separated from one role to another when assignment roles to cloud users of, particularly, the PaaS.
• **Action #10.** Give advanced notice on scheduled maintenance or upgrades to user access management, data protection technologies and virtual machines.

Here are some templates you can use:

**Security training:** The provider sets minimum requirements for security training for approved cloud users on security awareness and data labeling and handling.

**Scheduled maintenance:** The provider sets a schedule of maintenance including upgrades to user access management, data protection technologies and virtual machines.

**Service availability:** The provider sets the availability of cloud access during normal working hours.

**Service co-residence:** The provider sets the requirements for co-residence of SaaS applications on the PaaS.

**User threshold policy:** The provider sets user threshold levels below the maximum number of users that can access concurrently. The policy must state that the number of concurrent users is in proportion to the number of resource instances available to the users and that it is part of the security policy.

**Background checks:** The provider sets requirements for background checks for intended cloud users.

**SaaS user license:** The provider sets maximum limit on:

- Users that can concurrently access the application.
- Resource instances that users can use to access and run the application.
- Data requests that users can send and receive concurrently using the available resource instances.

**Constraints: Work with them**

There will most probably be some constraints in your way, such as:

- Service priority issues to different groups of consumers, depending on the roles assigned by the organization to consumers. An end user with administrative privileges has a higher priority over the end user that do not have them in accessing a SaaS application.
- Change management governance groups. To reflect changes, update the security policy, threshold policies, and SLA.
- Service exceptions to a cloud service type. Here’s a hint: Accidental of cutting fiber optics not within direct control of the provider, scheduled maintenance (planned and unplanned) and scheduled proactive behavioral upgrades to applications.
- Security penalties for not complying with all of the security policy's terms and conditions. Specify the consequences of noncompliance with the security policy and IT policy regulations.

Here are some templates you can use.
SaaS end user who functions as an administrator of a user license has a higher priority over other end users in accessing a licensed application. Due to recent organization change, policy governance group moved from Department FGH to Department RST. This requires an update to the security policy, threshold policies, and the SLA.

Service exceptions currently cover:

- Scheduled proactive application behavioral changes or upgrades.
- Botnet attack against the provider's host.
- Provider's scheduled maintenance.
- Provider's normal service availability from 7AM to 6PM and restricted service availability from 8PM to 11PM.

**In conclusion**

Crafting a security policy requires planning ahead of time to resolve the issues on how purpose, scope, and background of the policy should be stated. Developers should communicate with the both the cloud service consumer and provider on the issues of how much control a consumer should have, what actions the provider should take and what constraints to the policy are. Most important of all, the consumer should get a copy of the security policy (as well as those copies of the threshold policies) from the provider for review and questions to be resolve before negotiating with the provider.
Related topics

• The author discusses threshold policy in the articles "Balance workload in a cloud environment: Use threshold policies to dynamically balance workload demands," "Cloud computing versus grid computing: Service types, similarities and differences, and things to consider," and Build proactive threshold policies on the cloud."
• The author discusses proactive vs. reactive ways of making application changes when you migrate them to the cloud in the article "Change app behavior: From in house to the cloud."
• The author discusses cloud service security and how to mitigate risks to cloud services to ensure high uptime availability in the article "Cloud services: Mitigate risks, maintain availability."
• In the developerWorks cloud developer resources, discover and share knowledge and experience of application and services developers building their projects for cloud deployment.
• More developerWorks resources that match this article can be found at SOA and web services at developerWorks and industries at developerWorks.
• See the product images available for IBM SmartCloud Enterprise.
• The next steps: Find out how to access IBM SmartCloud Enterprise.

© Copyright IBM Corporation 2011
Trademarks
(www.ibm.com/developerworks/ibm/trademarks/)