STC Cloud Services

Cloud Shared Security Responsibility Model

Version: 1.0

Date: 03/05/2018

TABLE OF CONTENTS

1. Cloud Shared Security Responsibility Model

Ensuring that cloud services are designed, maintained and used securely is a shared responsibility between the Provider (STC) and the Customer. This shared model can help reduce customer's operational burden as STC operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates.

The customer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the STC Cloud provided security group firewall.

2. Customer Security Responsibilities

In addition to the business and risk considerations, the implementation of security controls in a cloud environment requires specialized technical knowledge and skills. It is therefore crucial that, prior to migrating business operations into a cloud environment, the Customer engage its technical, legal, due diligence, information security and compliance teams to work together to define its needs and evaluate potential cloud service offerings against those needs.

It is important to note that all cloud services are not created equal. Clear policies and procedures should be agreed upon between the Customer and STC Cloud for all security requirements. Responsibilities for operation, management and reporting should be clearly defined and understood for each requirement and acknowledged, in writing, in contractual agreements.

The following steps should be followed by any organization looking to migrate to or evaluate our cloud services:

- UNDERSTAND your risk and security requirements first.
- CHOOSE a deployment model that aligns with your and your industry's security and risk requirements.
- EVALUATE different service options.
- KNOW what you want from your Cloud Provider.
- REQUEST written assurances that security controls will be in place, and periodic verification (e.g. compliance reports) that controls continue to be maintained.
- REVIEW the service and written agreements periodically to identify whether anything has changed.

STC wants to work with their Customers to understand their security and compliance needs. STC wishes to maintain open communication and monitoring to avoid any misunderstandings or gaps in security responsibilities. Moreover, the allocation of responsibility between STC Cloud and Customers for managing security controls does not

exempt Customers from the responsibility of ensuring that their data is properly secured according to applicable security requirements.

3. Cloud Deployment Models

The main differences between cloud service categories relate to how control is shared between STC and Customer, which in turn affects the level of responsibility for both parties. It should be noted that, other than in a self-managed private cloud scenario, the Customer rarely has any control over hardware, and it is the degree to which virtual components, applications and software are managed by the different parties that differentiates the cloud service categories. As a general rule, SaaS provides Customers with the least amount of control, whereas IaaS offers the most control for the Customer.

Responsibility	Service Models		
	IaaS	PaaS	SaaS
Security Governance, Risk and Compliance (GRC)	Customer	Customer	Customer
Data Security	Customer	Customer	Customer
Application Security	Customer	Customer	Shared
Platform Security	Customer	Shared	STC Cloud
Infrastructure Security	Shared	STC Cloud	STC Cloud
Physical Security	STC Cloud	STC Cloud	STC Cloud

Figure 1: Security Responsibility based on Cloud Deployment Models

The level of security responsibility across the cloud service categories generally migrates towards the Customer as the Customer moves from a SaaS category (least Customer responsibility) to an IaaS category (most Customer responsibility). The greatest level of responsibility for STC to maintain security and operational controls, is present in the SaaS service category.

It is expected that as the industry and the Customer requirements evolve as cloud offerings mature, there will be additional cloud service categories besides those listed above. However, this guidance document focuses on the prevailing three cloud service categories: SaaS, PaaS and IaaS.

In all deployment models, and particularly in public cloud environments, it is important for all parties to understand the specific elements of the cloud service category used and its associated risks. Any cloud deployment model that is not fully self-managed is by nature a shared responsibility model, where a portion of responsibility for the cloud service falls under the realm of STC Cloud and a portion of responsibility also falls to each Customer. The level of responsibility that comes on STC or the Customer is determined by the cloud service category being utilized, for example, IaaS, PaaS or SaaS.

4. Cloud Shared Security Responsibility Model

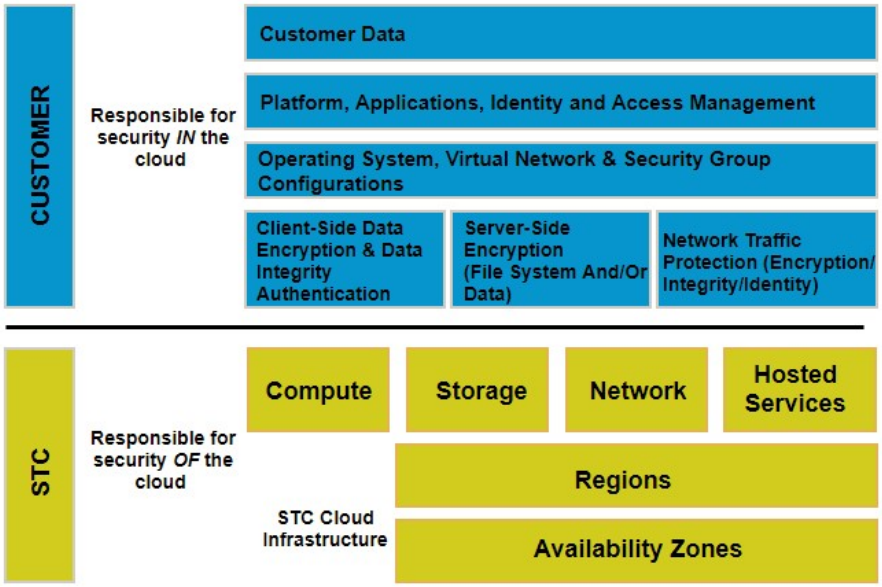

Figure 2: Shared Responsibility Model

STC Responsibility "Security of the Cloud"

STC is responsible for what is known as Security of the cloud. This covers STC Cloud global infrastructure elements including Regions, Availability Zones, and Edge Locations, and the foundations of its Compute, Storage, Database, and Network services. At all times, STC Cloud performs the operations, security and maintenance of the physical servers and hypervisor OS.

STC controls access to their data centers where customer data resides. This covers physical access to all hardware and networking components and any additional data center facilities including generators, uninterruptible power supply (UPS) systems, power distribution units (PDUs), computer room air conditioning (CRAC) units, and fire suppression systems. STC can provide several reports from third-party auditors who have verified our compliance with a variety of computer security standards and regulations.

Customer Responsibility "Security in the Cloud"

With the Cloud infrastructure secured and maintained by STC Cloud, the responsibility for what goes into the cloud falls onto the customer. This covers both client and server side encryption and network traffic protection, security of the operating system, virtual network, and firewall configuration, followed by application security and identity and access management.

How much of this additional security the customer wishes to implement is entirely the customer's decision. What customers choose may depend on the nature of their business or on existing controls that they may already have in place. We recommend tightening security as much as possible to minimize exposure to external threats that could compromise customer's environment.

Figure 3 illustrates how control of the different cloud layers and activities are often shared across different cloud service categories:

Customer
STC Cloud

Cloud Layer / Activities	Description of Layer	Service Models		
		IaaS	PaaS	SaaS
Data	Data or information contained within applications, databases & operating systems.	Customer	Customer	Customer
Application Program Interface (API) or Graphical User Interface (GUI)	The interface by which cloud service users interact with the application. The current most common API is RESTful HTTP or HTTPS. The current most common GUI is an HTTP- or HTTPS-based website.	Customer	Customer	STC Cloud
Applications	The actual application being used by one or more cloud service users.	Customer	Customer	STC Cloud
Solution Stack or Technology Stack	This is the programming language used to build and deploy applications. Examples are .NET, Python, Ruby, Perl, etc.	Customer	Customer	STC Cloud
Operating Systems (OS)	In a virtualized environment, the OS runs within each VM. Alternatively, if there is no underlying hypervisor present, the operating system runs directly on the storage hardware.	Customer	STC Cloud	STC Cloud
Virtual Machines (VM)	A virtual container executed on a hypervisor on a host. A set of system isolation technologies that provide various degree of security isolation with the host machine's OS kernel.	Customer	STC Cloud	STC Cloud
Virtual Network Infrastructure	For communications within and between virtual machines	Customer	STC Cloud	STC Cloud
Containers	Virtualization technique that allows execution of multiple isolated user space instances while sharing the same underlying OS kernel	STC Cloud	STC Cloud	STC Cloud
Hypervisors	When virtualization is used to manage resources, the hypervisor is responsible for allocating resources to each virtual machine. It may also be leveraged for implementing security.	STC Cloud	STC Cloud	STC Cloud
Processing and Memory	The physical hardware that supplies CPU time and physical memory	STC Cloud	STC Cloud	STC Cloud
Data Storage	The physical hardware used for file storage like hard drives, removable disks, backups, etc.	STC Cloud	STC Cloud	STC Cloud
Network	This can be a physical or virtual network like interfaces and devices, communications infrastructure, physical routers & switches, etc. It is responsible for carrying communications between systems and possibly the internet.	STC Cloud	STC Cloud	STC Cloud
Physical facilities / Data Centers	The actual physical building where the cloud systems are located	STC Cloud	STC Cloud	STC Cloud

Figure 3: Responsibility Control between Customer and STC Cloud

Customer
STC Cloud

Cloud Layer / Activities	Description of Layer	Service Models		
		IaaS	PaaS	SaaS
Subscribe and Create Marketplace Account		Customer	Customer	Customer
Configure Virtual Network		Customer	STC Cloud	STC Cloud
Provision VM with OS		Customer	STC Cloud	STC Cloud
Assign VMs with IP Addresses		Customer	STC Cloud	STC Cloud
Install patches and updates for the hypervisor OS		STC Cloud	STC Cloud	STC Cloud
Download and install patches and updates for the VM OS		Customer	STC Cloud	STC Cloud
Maintain documentation of the virtual environment		Customer	Customer	STC Cloud
Upload data to the virtual servers		Customer	Customer	STC Cloud
Take backup of the virtual servers		Customer	Customer	STC Cloud
Upload data to the applications		Customer	Customer	Customer
Take backup of the application data		Customer	Customer	Customer
Creating access for end-users		Customer	Customer	Customer

Figure 3: Responsibility Control between Customer and STC Cloud (continued)