STC Cloud Services

Guide to Cloud Workload Protection

Version: 1.0

Date: 03/05/2018

TABLE OF CONTENTS

1. Customer Workload Protection

Security controls in cloud computing are, for the most part, no different than security controls in any IT environment. However, because of the cloud service models employed, the operational models, and the technologies used to enable cloud services, cloud computing may present different risks to an organization than traditional IT solutions.

An organization's security posture is characterized by the maturity, effectiveness, and completeness of the risk-adjusted security controls implemented. These controls are implemented in one or more layers ranging from the facilities (physical security), to the network infrastructure (network security), to the IT systems (system security), and all the way to the information and applications (application security). Additionally, controls are implemented at the people and process levels, such as separation of duties and change management, respectively.

As described earlier in this document, the security responsibilities of both the provider and the consumer greatly differ between cloud service models. STC infrastructure as a service offering, as an example, includes responsibility for security up to the hypervisor, meaning they can only address security controls such as physical security, environmental security, and virtualization security. The customer, on the other hand, is responsible for security controls that relate to the IT system (instance) including the operating system, applications, and data.

2. Shared Security Responsibility Model

The broad categories of cloud services are Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Each category has its own set of security requirements and set of security responsibilities that are split between the cloud service provider and the cloud service customer. It is necessary to understand these requirements and responsibilities when considering a solution that involves one or more cloud services.

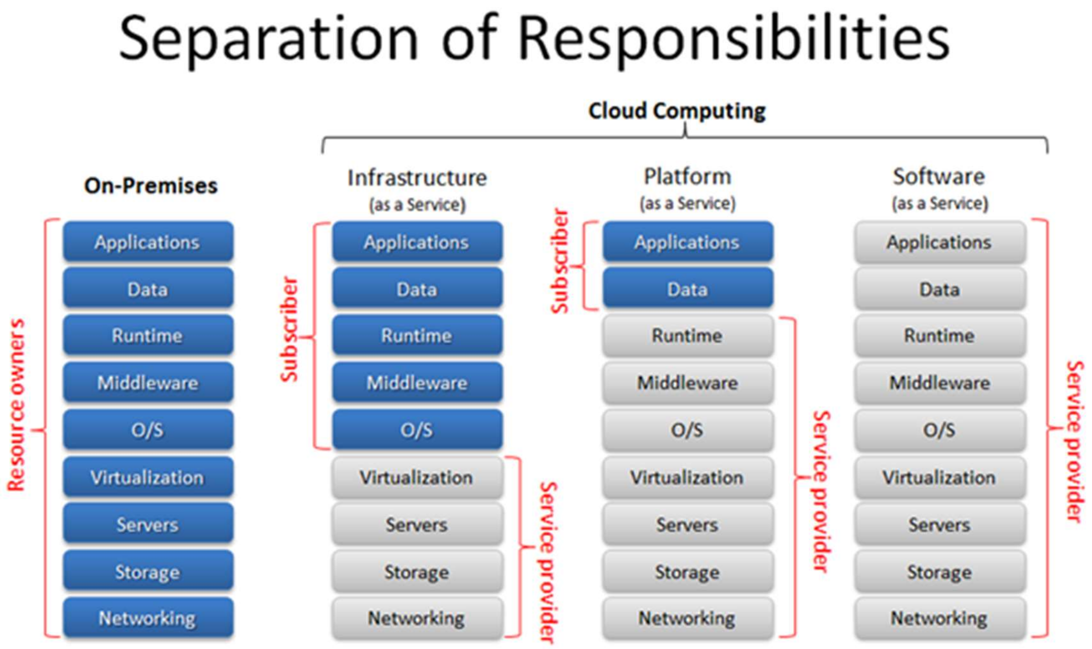

Figure 1: Shared Cloud Security Responsibility Model

Generally, IaaS cloud services involve the cloud service customer taking a substantial amount of responsibility for the security of data, applications, systems, and networks. The capabilities supplied by the cloud service are low-level infrastructure resources. The customer is typically responsible for the security of data both at rest and in motion and must choose appropriate encryption techniques where necessary. For applications, the customer must deploy appropriate security components such as firewalls, identity and authorization management and is also responsible for the security elements of the complete software stack used by the application.

PaaS cloud services typically involve the cloud service provider taking responsibility for security aspects of the software which makes up the platform, including the operating system and any middleware and runtimes made available for use by the customer. The customer still has the responsibility to configure the software appropriately and to choose appropriate options when deploying applications and data to the cloud service – for example, the customer might need to configure a database for encryption of the data it stores.

The cloud service provider typically takes most of the responsibility for security of SaaS cloud services, since the software, data stores and networks are usually configured and controlled entirely by the provider.

3. Identity and Access Management

When creating secure, cloud-enabled workloads, enabling identity and access management is an essential first step. With identity and access management, users are authenticated and authorized, providing user-specific access to cloud resources, services, and applications. Three major elements have to be considered for the cloud environment – Cloud User Role, Device Type, Access Type.

3.1. Cloud User Roles

Within cloud environments, different types of users and identities need to be managed. These include privileged access users, developers, and application users. A comprehensive security strategy encompasses the identity and access management requirements of all of these roles. The solution must be catered to a wide audience, including organizational users, Internet and social-based users, third-party business partner organizations, and vendors.

Privileged access users:

Privileged access users include the following roles:

- Application publishers, operators, and cloud administrators require access to staging and production spaces to create, update, and delete data, applications and their service instances
- Managers and team leads need insight into their team members' or employees' activities and require access to the environments that are used by developers, operators, and administrators.
- Auditors and Testers require access to the cloud services and the applications which run on them. This could be related to legal investigations, security incident audits or for general audits and certification purposes.

Privileged access users' accounts are very sensitive, as they are typically authorized to read sensitive information and to execute potentially destructive actions. Privileged access users' accounts also require an increased level of auditing. Attackers that are able to access such accounts can extract data from database services, deploy malicious applications, or deface or destroy existing applications.

Developer users:

Developers can create, update, and delete applications. Additionally, developers can create cloud service instances and bind those instances to applications. Developer user accounts are authorized to read sensitive information and manipulate applications. They require an increased level of Security and Monitoring.

Application users:

Application users usually have access and control of data which can be sensitive whose loss or modification could affect business reputation as well as lead to legal issues, and other losses. User accounts for services may have access for bulk data updates on the cloud environment.

3.2. Device Type

Within the cloud environment, several device types might be used to access an application. Based on device type, different access rules might be required even for the same user role. These include managed & unmanaged devices:

Managed Device

Devices that have Directory Services membership and/or are controlled by IT under compliance policies in terms of malware protection, patch management and other security controls. This can include mobile devices managed by a Mobile Device Management (MDM) solution.

Unmanaged Device

Devices which include personal devices (laptops, mobile devices), printers, cameras, etc. Unmanaged devices are controlled by the cloud user and may have different access controls based on the cloud application type and user role. For instance, data download from cloud services may be disabled for these types of devices.

3.3. Access Type

Cloud services can be accessed from almost anywhere. It may be desirable to limit user capabilities based on access type. There are two basic access types:

Internal access

User accesses the cloud service from an enterprise network or uses a VPN. In this case, the user can be granted full access for their role.

External access

User accesses the cloud service from the Internet. In this case, the user is granted a specific subset of functionality or alternatively additional authentication steps are required to authorize access.

3.4. Key Components of Identity and Access Management

User role, device type and access type have to be taken into account by customer when designing his Identity and Access Management system used for cloud services. The components described below help to enforce and ensure proper Identity and Access Management for cloud services.

Identity Lifecycle Management

Identity lifecycle management enables cloud service customers to manage user identities in cloud-based platforms, applications and services. Cloud-deployed applications can provision and de-provision user profiles with minimal human interaction. This streamlines access control based on the role, organization, and access policies defined by the cloud service customer. Identity lifecycle management involves:

- User Provisioning – control resource access by role taking into account device and access type.
- Password policies – control minimum password length, password complexity and password expiration.
- Access Request and Modification – resource access requests and modification – monitored and traceable.

- Access de-provisioning – revoke the user permissions and disable accounts.

Segregation of duties

Segregation of duties eliminates conflicts of interest and enables detection of control failures (human errors):

- In-Function separation – different roles for different actions within one function.
- Functional separation – different functions are performed by different roles.
- Third Party separation – a cloud environment is managed by the cloud service provider. Capabilities available to the cloud service provider should be limited; for example, no direct access to cloud service customer data.
- Legal Requirements – only specific roles should access sensitive data such as personally identifiable information (PII).
- Device and Access Type – some roles need limitations based on device and access type.

Identity Services

Identity Service enables cloud deployed applications to authenticate users at an application level, based on a range of identity providers.

For example, the identity service recognizes a subset or combination of the following identity providers:

- Directory Services, including on-premises and cloud based directory services.
- Social identity providers, using OAuth 2.0 or similar protocols.
- Identity APIs.

Directory services support the identity service by hosting user profiles and associated credentials:

- User identities and group or role membership to determine access policies, rights and privileges
- Resource and service descriptions and locations

Types of directory services include:

- LDAP based directory services – use LDAP access protocol (e.g., Microsoft Active Directory, OpenLDAP, etc.).
- Directory cloud services – manage user profiles, associated credentials and password policies. A directory cloud service means that cloud applications do not need their own user repository.

Single Sign-On

Single Sign-On (SSO), also known as Federation Services, provide for seamless transition between applications – in and out of a cloud environment – without the need to have an authentication mechanism for each application. SSO can support multiple Identity Providers (IDP) and directory services.

There are several common SSO configurations:

- Kerberos based – This method will initially prompt users for username and password and will acquire ticket-granting ticket from IDP.
- Security Assertion Markup Language (SAML) – XML-based solution that exchanges user authentication information between IDP and service provider seamless for the user based on current credentials.
- Other shared authentication schemes are OAuth, OpenID, OpenID Connect, Facebook Connect, etc.

It is recommended to use an encrypted connection between service provider and identity provider for authentication data exchange.

Privileged Account Management

Privileged accounts are the accounts that have administrative/system (such as root, admin, sys, etc.) access to cloud resources (virtual servers, databases, virtual network appliances, etc.). The need for special management measures for such accounts is necessary because of the high impact of any security breach related to these accounts, even more so where the applications and data involved are subject to special regulations (e.g. PII, financial records, etc.).

Privileged Account Management tools provide solutions for privileged accounts including centralized management, delegation, logging and monitoring. PAM tools provide increased security such as multi factor authentication, threat analytics, and session and password management. These tools can be used for on premises services as well as cloud services.

Multifactor authentication

The use of multiple authentication controls can combat increasing levels of identity theft. Examples of Multi Factor Authentication include one-time passwords, certificates, and tokens. It is important to note that authentication has to come from more than one source.

To maintain the user experience while improving login security, risk-based authentication controls are used. These controls change the level of required authentication based on a user's location, past activity, operation being performed, preferences, or other factors. Multifactor authentication is available with Identity Services, SSO and Privileged Account Management tools.

Reporting

Reporting provides a user-centric view of access to resources, or a resource-centric view of access by users. The reports address:

- Which users have access to each resource
- Which access is being exploited by each user and under what conditions
- Which users have changed access rights

Integration of cloud service provider reporting tools with existing on-premises reporting and incident response systems needs consideration.

4. Virtual Infrastructure Security

4.1. Instance Protection

There is no single unified threat management tool for servers either physical or virtual; cloud service customers invested in a VM collection are going to need more than one protection layer. There are roughly four different functional areas that these layers cover:

- Compliance and auditing. This includes the ability to produce reports on various compliance requirements, such as ISO/IEC 27001 and PCI standards, and the ability to audit access and administrative logs.
- Host Intrusion detection (IDS) and File Integrity Monitoring. These are the features most cloud customers should take into considerations when designing VM security.
- Access controls. This includes being able to restrict unauthorized users from accessing any protected virtual machine. Some products have the ability to tie access control roles to particular Identity Services, making policy deployments easier and more powerful.
- Antivirus/anti-malware protection. Similar to antivirus tools in the physical world, these provide protection against exploits inside a VM.

4.2. Virtual Network security

Controlled network boundaries are an important aspect of security when a customer uses a cloud service. Some important factors to consider when designing a virtual private network are:

- Proper network segmentation is important. A common pattern is a three tier approach, where one network segment talks directly to the users (such as a web server), one network segment does processing (such as an application server), and the most protected network segment holds machines that perform persistent data storage (such as a database server).
- Controls, such as firewalls, between segmented networks are also important. Make firewall rules as narrow as possible to meet business objectives. Review the logs periodically, particularly on internal boundaries, for misconfigurations or attackers trying to spread laterally. Also consider using an IPS or next generation firewall that can alert for malicious traffic or reconnaissance efforts.
- Use transport level security, such as TLS, in any cases where sensitive data is transmitted.
- For Internet facing web services, consider the use of a Web Application Firewall (WAF). A WAF acts as a proxy between end users and the service and can provide an extra layer of protection to block common application attacks such as SQL injection.
- If everyone who needs to access the application is on the corporate network, make it accessible only from the corporate network, either via firewall rules or a VPN tunnel.

5. Application Security

Cloud application security plays a critical role in protecting digital assets. Effective application security requires an understanding of threats, deployment of the right security measures, and continual vulnerability management. Ineffective practices can circumvent infrastructure and data security controls and expose systems to hackers. This section identifies the threats, security measures, and vulnerability considerations when engineering and deploying cloud application services.

5.1. Threat Modeling

Establishing a collective understanding of threats to application services is vital. Threat modelling offers insight to the development team on actions, behaviours, or conditions that affect cloud applications and potentially lead to security incidents. The development team can plan to avoid identified threats by means of secure design, coding, configuration, integration, and security testing practices.

The output of the threat modelling process should be applied in technical design, programming, systems integration and security testing. Threat models are particularly important input to operational security control validation and penetration testing.

5.2. Security Measures

Cloud applications must be engineered to address the threats identified during the threat modelling process. It's important to build security measures into the application rather than retrofit controls after deployment. Building security into the application proves much more effective in preventing attacks and reduces solution complexity. There are several frameworks such as OWASP Secure Software Development Lifecycle and Microsoft Security Development Lifecycle that provide guidance for building security into the software development life cycle.

5.3. Secure Coding

Implementing secure coding practices reduces the likelihood of security-related design weaknesses and security defects. Developers perform secure coding by following the guidance from the design recommendations to avoid dangerous programming, software configuration, and integration errors.

The focus of secure coding includes:

- Input validation
- Output encoding
- Session management
- Credential and password handling
- Protection of sensitive data in storage and in motion
- Error handling and logging
- Protection of log information
- Selection and proper use of APIs and network services

There are general secure coding practices guidelines available to help educate developers including OWASP Secure Coding Practices and the CERT Top 10 Secure Coding Practices.

5.4. Security Testing

Effective security testing is essential to identify cloud application vulnerabilities. The testing process must focus on the relevant threats (e.g., OWASP ASVS) to ensure effective security measures are in place. Cloud application security testing emphasizes:

- Attack surface review – A comparison of the original (identified during design) and final (after code development process is completed) attack surface is performed to identify variances. The threat model is updated to reflect any changes in the attack surface. This information is taken into account during the testing process.
- Fuzzing – This method tests code that processes input across trusted boundaries such as web service interfaces, network sockets, and file exchange. Fuzz testing injects invalid or malformed data to discover exploitable privilege level elevation vulnerabilities. Several fuzz testing methods are used to expose buffer overruns, unhandled exceptions, and other weaknesses.
- Web Application Scanning & Penetration Testing – A form of dynamic application testing, this entails an external application scan (authenticated and unauthenticated) to discover vulnerabilities. This may include vulnerabilities such as cross-site scripting, insecure certificates, insecure ciphers, and remote code execution that must be addressed prior to production release. Organizations should perform web application scans periodically to identify vulnerabilities that may surface in the application environment over time. Periodic penetration testing is performed to verify vulnerabilities can be exploited and identify the extent of exposure. To ensure cloud applications are secure, penetration testing should include, at a minimum, OWASP Top 10 vulnerabilities.

5.5. Cloud Application Security Controls

Application security controls are applied during the development process. These controls address:

- Cryptography - should be used to protect sensitive data in use, in transit, and at rest.
- Identity and Access Management - is critical to application security. Managing logical access to applications and data to control who has access to what is essential to reducing risk
- Web Application Firewall (WAF) - protect web-based applications from known vulnerabilities such as SQL injections, buffer overflow, parameter tampering (e.g., path manipulation), and information leakage. Both inbound and outbound web server traffic is filtered and traffic is inspected to prevent attacks.
- API Security - APIs are pervasive in cloud environments. It is imperative that secure development methods are adopted and validation of API security is performed during the testing process.

The common API vulnerabilities developers must be aware of include

- No or weak authentication
- Weak password complexity
- Use of non-federated access
- Session tokens with no expiration
- Lack of logout/session expiration

6. Data Security

6.1. Data Classification

Data security and data protection starts with clearly understanding the data and the organizational, industry and regulatory requirements for protecting it. Regulated data such as PII requires a more granular understanding, as the applicable rules and regulations can vary widely based on the specifics of the type of PII as well as the jurisdiction applying to the data.

The protection applied to data should reflect its nature and the impact of unauthorized disclosure, modification or loss. An insufficient level of protection can imply legal and reputational risk. Too much protection can have a negative impact on the cost and performance of the system.

6.2. Data Encryption

Encryption of data is a common technique used to protect data where required based on the sensitivity of the data or on the applicable organizational or regulatory requirements.

Encryption in transit - Encrypting data in transit is usually achieved via techniques such as Transport Layer Security (TLS). When using TLS, certificate checking is required, to avoid "man in the middle" attacks. When TLS is not feasible, there are typically secure options for a given protocol, such as SFTP in place of FTP, or point to point IPSEC tunnels. Encryption in transit when on public networks is absolutely essential.

Encryption on private networks is also highly recommended, and will typically be expected by most cloud customers.

Encryption at rest - Encryption of data at rest requires consideration of where to apply the encryption, and its scope. Encryption at rest can be applied at the operating system/storage level, the middleware level, or the application level. OS/storage encryption typically involves using file system encryption, such as Linux Unified Key Setup. Middleware encryption involves encryption capabilities built into the middleware used by the application, such as Transparent Data Encryption in Microsoft SQL Server or DB2 Native Encryption in IBM DB2. Application encryption is encryption applied in the application code itself.

Key Management - The management of encryption keys is one of the most typically overlooked aspects of data protection. Key management involves the creation and deletion, secure storage, access control and auditing, and rotation of keys. If keys are not properly protected, malicious access to keys undermines the entire effort of data encryption. Key protection is now becoming a regulatory requirement, with proof of key protection required.

6.3. Database Activity Monitoring

Most regulatory rules, as well as organizational policies, require close activity logging and auditing of all data activity. This involves logging not only activity associated with access to the data, but also logging all changes or events that occur on the data. Logging must be at a granular level, with visibility to all events associated with individual data elements. Data activity monitoring techniques involve the ability to define thresholds and rules for what constitutes normal activity, and alerting if data activity exceeds the normal baselines. Many technologies exist to aid in the implementation of data activity monitoring, particularly for data stored in databases.

7. Monitoring & Vulnerability Management

7.1. Security Monitoring

Security monitoring enables an organization to proactively monitor, track, and react to security incidents. It is necessary to have end-to-end visibility and integration of security processes and tooling throughout the organization. Security monitoring creates a complete audit history for incident management and compliance purposes. The use of cloud services increases the surface area of security risk exposure. Advanced, multi-stage attacks exist that evade detection by signature based tools. DevOps and related agile initiatives have introduced faster infrastructure changes and shrinking threat detection opportunities. These trends combine to offer a substantial challenge to security monitoring and intelligence for cloud applications.

7.2. Vulnerability Management

One of the most important aspects of cloud security is vulnerability management. There are many security risks, which are constantly evolving as cloud adoption is expanding. Cloud empowers end-users and developers more than ever before, allowing them to continuously integrate and deploy applications to and from a cloud by using multiple APIs.

Effective vulnerability management in the cloud requires a focus on the following items:

- Subscribe to Common Vulnerability Exposure (CVE) lists
- Analyze CVE data to identify and prioritize relevant vulnerabilities
- Develop a plan to remediate vulnerabilities in a timely manner
- Test to verify vulnerabilities have been remediated

Vulnerability management in the cloud should cover multi-phases process, those phases are:

- Identifying
- Classifying
- Remediating
- Mitigation.

8. Security Governance, Risk, and Compliance

When using cloud services, it is vital to apply appropriate governance to the use of those cloud services, to identify and mitigate risk, and to ensure compliance both with external laws and regulations and with organizational security policy.

8.1. Security Policy and Governance

An organization's security policy plays a great role in determining how the organization's IT systems achieve security goals. When adopting cloud services, the security policy must extend to include cloud service security policies, that take into account the different environment involved in using cloud services. Cloud service security policy needs to take account of the three major categories of cloud service – IaaS, PaaS and SaaS. This is because the level of responsibility varies with each of these categories of cloud service. The business strategy, competitive differentiation, and industry regulation guidelines are prominent factors that shape a corporate IT strategy. The security strategy drives security governance.

Security governance ensures that the company:

- Enforces the IT security policy through security controls.
- Educates employees and end users about security guidelines with emphasis in cloud risks.
- Meets industry and compliance regulations.
- Achieves operational efficiency across security controls.
- Continually assesses risks and addresses them through security controls.
- Ensures that security capabilities of suppliers and sub-processors involved in the solution is also taken into consideration

The security controls are split across various layers of security, including identity and access management, data, applications, network and server infrastructure, physical security, and security intelligence. When an organization adopts cloud services, the cloud security policy has to be updated to define the required security controls for extending the IT security policy onto cloud-based systems.

8.2. Risk Assessment and Risk Treatment

A key element of security governance is appropriate treatment of risk. This requires that a risk assessment is performed on customer’s use of cloud services. This in turn requires adequate information from the cloud service provider about their risk management policies and the security controls which are applied to cloud services.

8.3. Compliance

Compliance is another key factor in security governance. There is a need to ensure that the cloud service customer and the cloud service provider comply with laws, regulations and organizational policies. For the customer, this may be achieved by appropriate periodic audits. For the provider, this is often handled through certifications to relevant standards, which take place regularly and which result in public certification notices that can be used by cloud service customers as assurance that the provider complies.