CHAPTER 6

Cloud Security and Existing Security Solutions

Learning Objectives

After reading this chapter, you will be able to:

- Provide realistic picture of the current cloud security scenario.
- Understand the detailed analysis of cloud security concerns and various categories of cloud risks.
- Learn about the popular vulnerability assessment tool for cloud.
- Know about VM security challenges.
- Understand cloud computing security architecture.
- Understand open source security solution products in cloud.

6.1 Cloud Security Fundamentals

Cloud security is the first and foremost concern of every industry using cloud services. A cloud vendor must ensure that the customer does not face any difficulties such as loss of data or data theft. There is a possibility that a malicious user can go through the cloud by impersonating a legal user, thereby infecting the cloud services and hence affecting various customers sharing the malicious cloud services. Data integrity, privacy issues, authentication issue, data loss, user-level security and vendor-level security are some of the basic concerns of cloud computing. These fundamental problems in cloud computing scenario can be defined as cloud risks.

6.2 Cloud Risk

When infrastructure, applications, data and storage are hosted by cloud providers, there is a huge chance of risk in each type of service offering. This is known as a cloud risk. Several aspects apart from cost and offered services must be evaluated before choosing a particular cloud provider. Security is of utmost importance while considering a cloud computing environment. Sometimes, the physical location of the servers may also be a factor for sensitive data.

Organizations such as the Cloud Security Alliance (CSA) offer certification to cloud providers that meet their criteria. The CSA's Trusted Cloud Initiative program was created to help cloud service providers enable industry-recommended standards, secure access, compliance management, interoperable identity and follow best practices. Several cloud risks should come under supervision before moving data and services to the cloud. Section 6.3 categorizes various cloud risks, their associated types and existing open source cloud security solution products.

6.3 Cloud Risk Division

Cloud risks have been the biggest concern since the start of the cloud computing era. These risks can be divided into the following four major categories:

1. Policy and organizational risks
2. Technical risks
3. Legal risks
4. Other risks

These categories will be discussed in detail in the following subsections.

6.3.1 Policy and Organizational Risks

Following are policy and organizational risks:

1. **Lock-in:** When applications, data and services are dependent on only one cloud provider, it is known as a lock-in problem. Lock-in is one of the biggest problems of a cloud computing environment. There could be SaaS lock-in, PaaS lock-in and IaaS lock-in. Lock-in problem occurs because of high customization of services according to user demand.
2. **Loss of governance:** The cloud provider may sub-contract or outsource services to third parties (unknown providers) that may not compromise the same guarantees (such as to provide the service in a lawful way) as issued by the cloud provider. Or there is a possibility that the control and operational management of the cloud provider may change, and with that the terms and conditions of their services may also change. Loss of control and governance could lead to the impossibility of fulfilling the security requirements, lack of confidentiality, integrity and availability of data, and a deterioration of performance and quality of service.
3. **Compliance challenges:** Cloud providers make huge investments for external certifications such as SAS 70, PCI DSS and HIPPA. These certifications give them the reputation in the market that they are following the best security practices. However, in some cases particular certification may also be a problem for accessing cloud services. For example, if a client using AWS cloud wants to use the EC2 service and if the EC2 service does not have PCI compliance, then the EC2 service cannot be used for credit card–related transactions. Although customers could use other AWS services, they are restricted from using this particular service.

4. **Cloud service termination or failure:** There must be 24 × 7 support and high availability of all services, but in the competitive world of IT, an inadequate business strategy, lack of financial support and other factors could lead some providers to go out of business or shut down their service portfolio offering. And it is possible that for a short or medium period of time some cloud computing services could be terminated.
5. **Supply chain failure:** There is a possibility that the cloud provider could outsource some services to other third parties. In that case, any interruption or corruption in the chain or a lack of coordination of responsibilities between all parties involved can lead to inaccessibility of services, loss of data confidentiality, availability and integrity economic and reputational losses because of failure to meet customer demand such as cascading service failure and violation of SLA.

6.3.2 Technical Risks

Following are some technical risks:

1. **Isolation failure:** Because cloud computing works on multi-tenancy and shared resources architecture, there is sharing of computing capacity, storage and network among multiple users. This multi-tenancy also leads toward some threats such as failure of logical or physical separations between memory stacks, storage and routing tables (e.g. side channel attacks, SQL injection attacks and guest-hopping attacks), where the data of multiple customers can be maliciously stored in the same table.
2. **Resource exhaustions:** Cloud service is fully on-demand pay-per-use service. There is a chance of risk in proper allocation of resources to cloud users. Although there are many resource allocation algorithms used for allocating all the resources of a cloud service, insufficient resource provisioning and investments in infrastructure may lead to service unavailability problem or degradation in performance.
3. **Cloud provider malicious insider:** The malicious actions of an insider could possibly have an impact on the confidentiality, integrity and availability of all kind of data. IP all kind of services and, therefore, indirectly on the organization's reputation, customer expectation and the experiences of employees. Taking care of this issue is extremely important in case of cloud computing because cloud architectures contain certain special characteristics that are at very high risk.
4. **Intercepting data in transit:** Cloud services are based on distributed architecture; therefore, transmission of data takes place across multiple physical machines, from one VM to another, images distribution between cloud infrastructure and remote web clients, VPN environment and such. This risk is more vulnerable when data is being transferred from on-premises to cloud or cloud storage to on-premises. Spoofing, man-in-the-middle attacks and sniffing types of attacks could be possible during data transfer–related activities.
5. **Insecure or ineffective deletion of data:** Whenever a provider is altered, resources are scaled down, physical hardware is moved, data may be available beyond the lifetime specified in the security policy. It may be tough to carry out the procedures stated by the security policy because full data deletion is only imaginable by destroying a disk that also stores data from other clients. When a request to delete a cloud resource is made, this may not result

in true wiping of the data (as with most operating systems). For this, true data spreading is required and special procedures must be followed that may not be supported by the standard API (or at all); therefore, an effective encryption mechanism is required to reduce this risk.

6. **Conflicts between customer hardening procedures and cloud environment:** Cloud providers follow different server or instances hardening mechanisms that are little different from traditional server hardening procedures. For example, AWS EC2 service follows security group and the IAM role for securing and authentication of instances, whereas physical servers such as Linux or Windows follow traditional methods for hardening. Users must clearly understand the hardening procedures of cloud providers and which best practices they are using for hardening.
7. **Loss of encryption keys:** This includes disclosure of secret keys (e.g. file encryption, SSL, customer private keys) or passwords to malicious parties, the loss or corruption of those keys, or their unauthorized use for authentication and non-repudiation (digital signature).
8. **Malicious probes or scams:** Malicious probes or scanning, as well as network mapping, are indirect threats to the assets being considered. They can be used to collect information in the context of a hacking effort. A probable impact could be a loss of confidentiality, integrity, and availability of service and data.
9. **Compromise service engine:** All cloud providers rely either on an extremely specific platform or the service engine that is placed just above the physical hardware and manages customer requests at different levels of abstraction. For infrastructure service providers, this software element can be the hypervisor, for platform service providers, it could be hosted application engines. Hacking the service engine may be useful to escape the isolation between different customer environments (jailbreak) and gain access to the data contained inside them, to monitor and adapt the information inside them in a transparent way (without direct interaction with the application inside the customer environment), or to decrease the resources assigned to them, causing a denial of service (DoS attacks).

6.3.3 Legal Risks

Following are some legal risks:

1. **Risk from changes of jurisdiction:** Customer data may be kept in several jurisdictions, some of which may be high risk. If datacenters are located in high-risk countries (e.g. those that lack the rule of law and have an unpredictable legal framework and enforcement, monocratic police states, states that do not respect international agreements), sites could be attacked by local authorities and data or systems subject to enforced disclosure or seizure.
2. **Licensing risks:** Licensing conditions, such as per-seat agreements and online licensing checks may become unusable in a cloud environment; for example, software is charged at per instances basis so if our cloud-based instance increases, the cost of the software also increases exponentially.
3. **Data protection risks:** It can be tough for the cloud customer (in its role of data controller) to efficiently check the data processing that the cloud provider brings out and hence be sure that the data is handled in a lawful way. There may be data security breaches that are not intimated to the controller by the cloud provider. The cloud customer may misplace control of the data administered by the cloud provider. This issue is increased in the case of multiple transfers of data (e.g. between federated cloud providers).

6.3.4 Other Risks

Apart from policy, technical and legal risks, following are some other risks:

1. **Backup lost or stolen:** This risk is possible due to inadequate physical security procedures, AAA vulnerabilities, User provisioning vulnerabilities and user de-provisioning vulnerabilities.
2. **Unauthorized access to premises (including physical access to machines and other facilities):** Because of inadequate physical security procedures, unauthorized access in datacenters is possible. Generally, cloud providers have large datacenters; therefore, physical control of a datacenter must be stronger because the impact of a breach of this issue could be higher.
3. **Theft of computer equipment:** This risk is possible because of inadequate physical security procedures. This risk is mainly related to the datacenter, only authenticated person must be allowed to enter in physical datacenters and dual authentication mechanism should be followed to accesses those machines.
4. **Natural disasters:** Natural disasters are possible any time so there must be a perfect disaster recovery plan. Although, the risk from natural disasters is quite less compared to traditional infrastructures because cloud providers offer redundancy and fault tolerance by default; for example, AWS has various physical regions and multiple availability zone option within a region also.

6.4 Cloud Computing Security Architecture

There are several proposed and research-based cloud security architectures in the market. Following is a generic view of cloud computing security architecture:

Figure 6.1 shows an architectural view of the security issues to be addressed in a cloud computing environment for providing security to the customer. We have defined four layers on the basis of cloud computing services categorization. The cloud computing categorization is the same as we have already discussed in detail, that is, Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). This section presents the four layers shown in Figure 6.1 and maps different security issues in each layer.

There are four layers in the generic architecture of cloud, i.e. user layer, service provider layer, VM layer and datacenter layer, which are described as follows:

1. **Data center layer:** This layer is related to traditional infrastructure security concerns. It consists of physical hardware security, theft protection, network security and all physical assets security.
2. **VM layer:** This layer involves VM level security issues, VM monitoring, hypervisor-related security issues and VM isolation management issues.

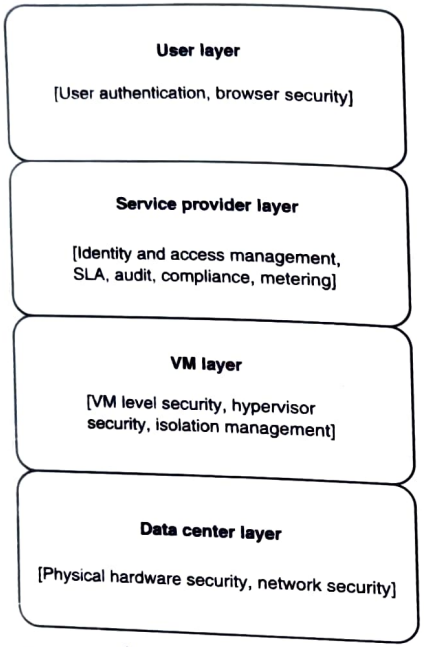

Figure 6.1 | Cloud security architecture.

3. **Service provider layer:** This layer is responsible for identity and access management, service level agreement (SLA), metering, compliance and audit-related issues.
4. **User layer:** This is the first layer of user interaction. It is responsible for user authentication and authorization and all browser-related security issues.

6.5 VM Security Challenges

As discussed in Chapter 2, virtualization is the key technology in cloud computing and because of the evolving nature of virtualization, there are many virtualization-related threats. Over the last couple of years, we have observed some great features of virtualization that can open unwanted security vulnerabilities. Unfortunately, some features are frequently implemented before the linked security consequences are fully understood. Some of the items labeled as threats here could also be considered unbelievable benefits. The objective of listing these items is to increase the alertness of the potential downside, while encouraging people to consider through the implementations with respect to security.

1. **Communication between VMs or between VMs and the host:** VMs serve some key requirements for any organization such as the following:

- Sharing one physical computer resource among multiple companies or organizations.
- Consolidation of different services into one physical computer.
- Providing a general hardware platform to host multiple operating systems.

In virtualization technology, basically the operating system enables the VM layer for logging keystrokes and passing regular screen updates to all guest VMs. These screen updates and key strokes are logged to files out on the host and enables monitoring of secured terminals within the VM.

Some VM technology provides full accesses to all guest VMs and guest VMs can easily access all critical resources of the guest operating system such as the file system level access. There must be a strong layer of isolation and security between guests and the host VM. It is the responsibility of VM users to discuss and understand this isolation issue with their respective VM vendor.

2. **VM escape:** VMs allow us to share the resources of the host computer and provide isolation between VMs and their host.

   In an ideal situation, any program that runs under the VM should not communicate to any other program inside that or any other VM, but because of some architecture limitations or some other bugs, software affect this isolation.

   It may so happen that a program running inside a VM can totally bypass the VM layer and acquire full access to the host system. Such a situation is known as *VM escape*. Because of the host's privileged position, the result may be a total collapse in the security model of the system.

3. **VM monitoring from the host:** It is not normally considered a limitation or a bug when one can start monitoring, changing or communicating with a VM application *from the host*. In this case, the host itself starts controlling; therefore, the host requires more strict security environments compared to each individual VM. The host can affect VMs behavior in the following ways, although it depends on the kind of VM technology being used.
   - Start, stop, pause and restart VMs.
   - Monitor and configure resources available to the VMs, including CPU, memory, disk and network usage of VMs.
   - Adjust the number of CPUs, amount of memory, amount and number of virtual disks, and number of virtual network interfaces available to a VM.
   - Monitor the applications running inside the VM.
   - View, copy and possibly modify the data stored on the VM's virtual disks.

   As all network packets coming from or going to a VM pass through the host; the host is generally able to monitor network traffic for its VMs. This same condition may occur in a co-hosting facility where one host has the privileges to monitor network traffic for all its hosted machines.

4. **VM monitoring from another VM:** Isolation is a basic characteristic of VM technology; it is usually referred as a security defect when one VM can easily monitor another without definite configurations and privilege to do so. The memory protection built into most modern CPUs should be inherited in the hypervisor too. If the hypervisor memory is implemented

properly then individual VM protection takes place automatically. It will not disturb other VM's memory address space. Because VMs do not have direct access to the host file systems, VMs should not be able to directly access the virtual disk of each other's VM on the host machine.

If network traffic is more complicated then there could be an issue with isolation depending on how the network connections are set up with the VMs, but if there is a dedicated physical channel for each host VM, then guest VMs should not be able to sniff each other's network packets.

There could be the case of a virtual hub also, if the VM uses a virtual hub for connecting all VMs host machine, then guest VM may sniff the packets of host VM or other guest VMs using ARP poisoning or some other spoofing technique. Virtualization technology must ensure all possible preventions to such attacks.

5. **Denial of service:** Because various computing resources like CPU, memory, network and hard disk are shared among multiple VMs and host machine. This may create a denial of service attack against another VM.

   This can be avoided by limiting the access of VM resources. There are many virtualization techniques that are used for restricting the allocation of resources to individual VMs. If proper virtualization configuration is implemented, the host machine can prevent denial of service attack among hosts and guest VMs.

6. **External modification of a VM:** In a business application scenario, users' VMs have the privilege of accessing employee databases through a secured application. Database security is more critical in a virtual environment. Database is placed inside a secured VM environment so that any external user is not allowed to access the database outside of the application. If a VM where database is installed becomes accessible from outside because of a malicious attack, then the database can be corrupted or modified and the system trust can be broken.

   This secure VM should be executed by digitally signing every VM and validating the signature before execution. The signing key should be used very carefully and never be placed anywhere else, otherwise it can be compromised.

7. **External modification of the hypervisor:** Because the hypervisor is mainly responsible for the enablement of virtualization while making the process of more self-protected and secure VM, it does not affect the working of any underlying hypervisor. Therefore, the first thing is to protect the hypervisor from any external unauthorized access and changes.

8. **Mixed trust level VMs:** Enterprises must take care of mission critical–related information while leveraging the benefits of virtualization. After applying some self-protection system and some external security mechanism such as integrity checking, file monitoring, log assessment, firewall protection and antivirus detection, the VM can be more secure in mixed environments.

9. **Resource contention:** Whenever some resource-consuming operations like malware or antivirus scanning, files and patch updates are executed on VMs, the results of these operations produce high loads on the systems and hamper server applications and VDI environments.

To avoid such situations, each VM requires additional significant memory footprint because just like traditional architecture, the antivirus must be installed on each operating system and the same kind of protection is required for each VM, too.

More virtualization-sensitive technology is needed for optimal resource utilization and increasing VM performance so that dedicated antivirus and file scanning should not affect the memory footprint on the virtual hosts.

6.6 Vulnerability Assessment Tool for Cloud

As discussed earlier, security in cloud services is comparatively the most important concern.

Generally, cloud providers take care of all security issues. For example, one of the biggest cloud service provider AWS offers series of administration and security services like Identity and Access Management, CloudTrail, CloudWatch, Trusted Advisor and Directory Services, though it provides one CloudHSM service which stands for Cloud Hardware Security Module. It is a dedicated hardware device which stores cryptography encryption and decryption keys.

Clients always seek some definite assurance that their data must be fully secure while using cloud services. Thereby cloud computing best practices suggest that consumers should enable security in each layer and leverage some third party security service provider also.

To address this important concern, cloud service providers have partnered with third parties to allow these entities to independently test their environment. In the following subsections, some most popular third party cloud security and vulnerable assessment tools in current industry scenario are discussed.

6.6.1 Netskope

Netskope (Fig. 6.2) is a service that monitors cloud app policies for specific groups or users. It monitors user's devices, browser session, location and every activity like sharing, downloading or editing content.

Netskope security solution is quite useful for any organization where employees can use their preferred cloud apps. In addition, any unwanted activity is blocked by Netskope fine-grained policy.

6.6.1.1 Features of Netskope

Following are the key features of Netskope:

1. Creates one policy which can control all your cloud apps.
2. Provides single point of control.
3. Provides more granular level security to all your apps.
4. Provides detailed audit trail report in case of any security breach.

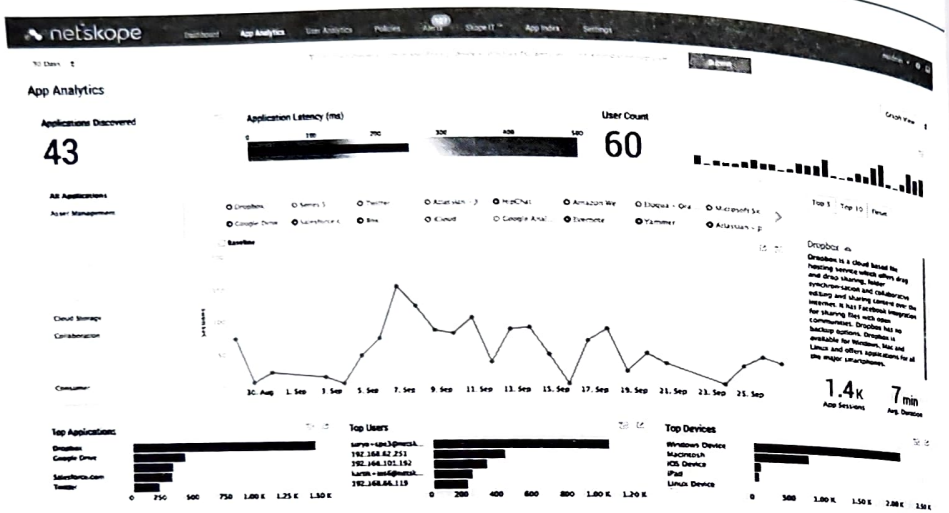

Figure 6.2 | Netskope. (From www.netskope.com)

6.6.2 CipherCloud

CipherCloud (Fig. 6.3) security software encrypts data directly at your business gateway. It is one platform which can protect all your clouds. This is why CipherCloud got tremendous growth and acquired more than 2.5 million business users and 250 million customer records over the last few years.

Figure 6.3 | CipherCloud. (From www.ciphercloud.com)

6.6.2.1 Features of CipherCloud

Following are the key features of CipherCloud:

1. Encrypts data during uploading process and also decrypts during downloading process.
2. Provides security solution for each type of cloud service including database or any kind of cloud app.
3. Provides data loss preventions and also detects malware functions.

6.6.3 Skyhigh Networks

Skyhigh (Fig. 6.4) cloud security service enables IT to quickly and easily adopt the cloud services. With Skyhigh, you can effectively manage your employees to use cloud services while ensuring business compliance of your organization's data privacy, security and internal policies.

Figure 6.4 | Skyhigh. (*Courtesy*: Skyhigh Networks)

6.6.3.1 Features of Skyhigh Networks

Following are the key features of Skyhigh networks:

1. Uses reverse proxy technology to allow contextual access to the cloud.
2. Provides consistent policies across clouds and grants direct access to clouds without having VPNs or any specific device agents.
3. Implements data loss protection techniques and granular level access, and also encrypts data.

6.6.4 Okta

Okta (Fig. 6.5) is a common solution for all cloud-based business applications. It is pre-integrated with Google, Microsoft, Salesforce.com and other cloud providers.

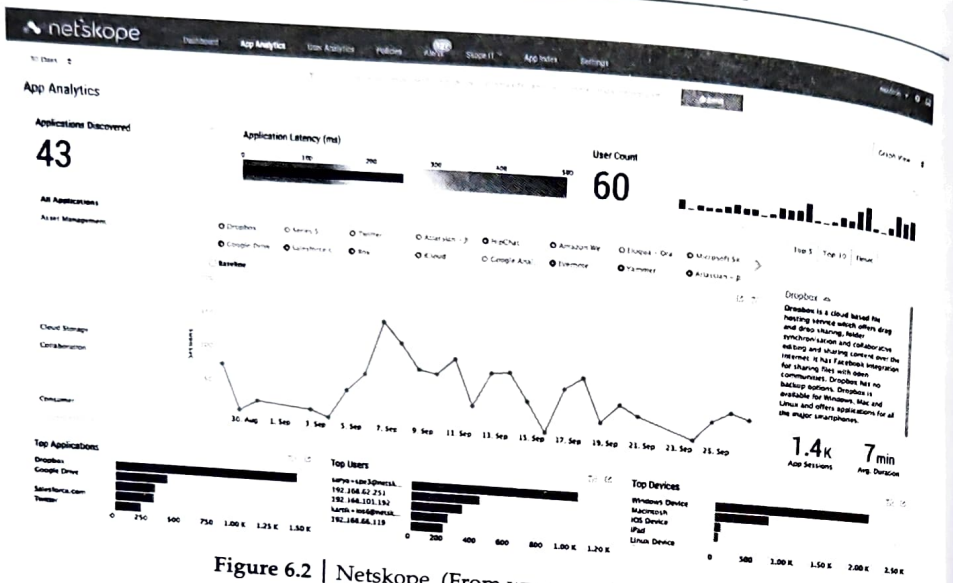

Figure 6.2 | Netskope. (From www.netskope.com)

6.6.2 CipherCloud

CipherCloud (Fig. 6.3) security software encrypts data directly at your business gateway. It is one platform which can protect all your clouds. This is why CipherCloud got tremendous growth and acquired more than 2.5 million business users and 250 million customer records over the last few years.

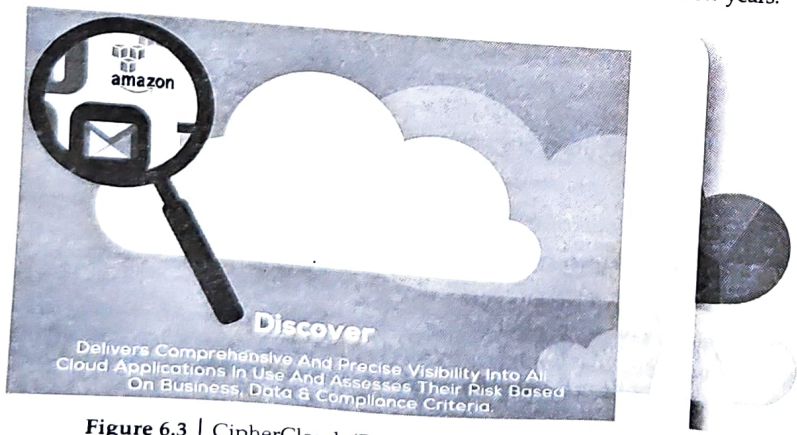

Figure 6.3 | CipherCloud. (From www.ciphercloud.com)

6.6.2.1 Features of CipherCloud

Following are the key features of CipherCloud:

1. Encrypts data during uploading process and also decrypts during downloading process.
2. Provides security solution for each type of cloud service including database or any kind of cloud app.
3. Provides data loss preventions and also detects malware functions.

6.6.3 Skyhigh Networks

Skyhigh (Fig. 6.4) cloud security service enables IT to quickly and easily adopt the cloud services. With Skyhigh, you can effectively manage your employees to use cloud services while ensuring business compliance of your organization's data privacy, security and internal policies.

Figure 6.4 | Skyhigh. (*Courtesy*: Skyhigh Networks)

6.6.3.1 Features of Skyhigh Networks

Following are the key features of Skyhigh networks:

1. Uses reverse proxy technology to allow contextual access to the cloud.
2. Provides consistent policies across clouds and grants direct access to clouds without having VPNs or any specific device agents.
3. Implements data loss protection techniques and granular level access, and also encrypts data.

6.6.4 Okta

Okta (Fig. 6.5) is a common solution for all cloud-based business applications. It is pre-integrated with Google, Microsoft, Salesforce.com and other cloud providers.

Okta cloud solution provides single sign on (SSO) for all types of cloud service providers including business app or mobile app. This service eliminates the need of time authentication for each service.

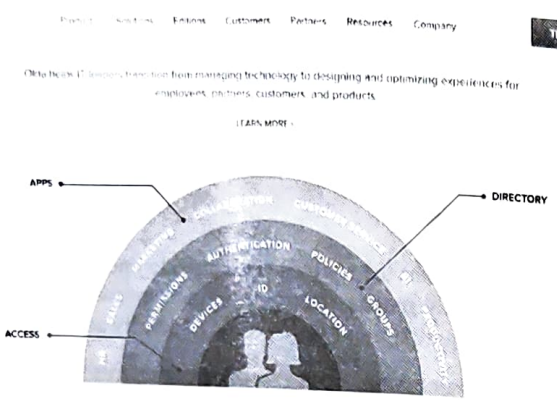

Figure 6.5 | Okta. (From www.okta.com)

6.6.4.1 Features of Okta

Following are the key features of Okta:

1. Okta offers multiple authentication factor and provides support for mobile devices and applications.
2. Okta supports full user cycle; organizations can deploy their own LDAP solution without any problem.
3. Okta helps managing access policies from one centralized position to control all cloud-based apps.
4. Okta also provides role-based administration through which we can set more granular level control for each type of access.

6.6.5 Qualys

Qualys (Fig. 6.6) security solution covers all aspects of cloud services including asset discovery, network security, Web app security, threat security and compliance monitoring. It proactively checks the vulnerabilities of your network and cloud services.

6.6.5.1 Features of Qualys

Following are the key features of Qualys:

1. Qualys can quickly scan all Web apps keeping data safe whenever you are using SaaS, IaaS and PaaS.
2. Qualys security solution uses automation to test the entire Web application more efficiently and fix the vulnerabilities very quickly.
3. Qualys helps in seeing the details of all security attacks through one interactive dashboard.

4. Qualys always verifies system process to ensure the proper enablement of password policies and compliance certificates like PCI, HIPAA, FISMA and others.

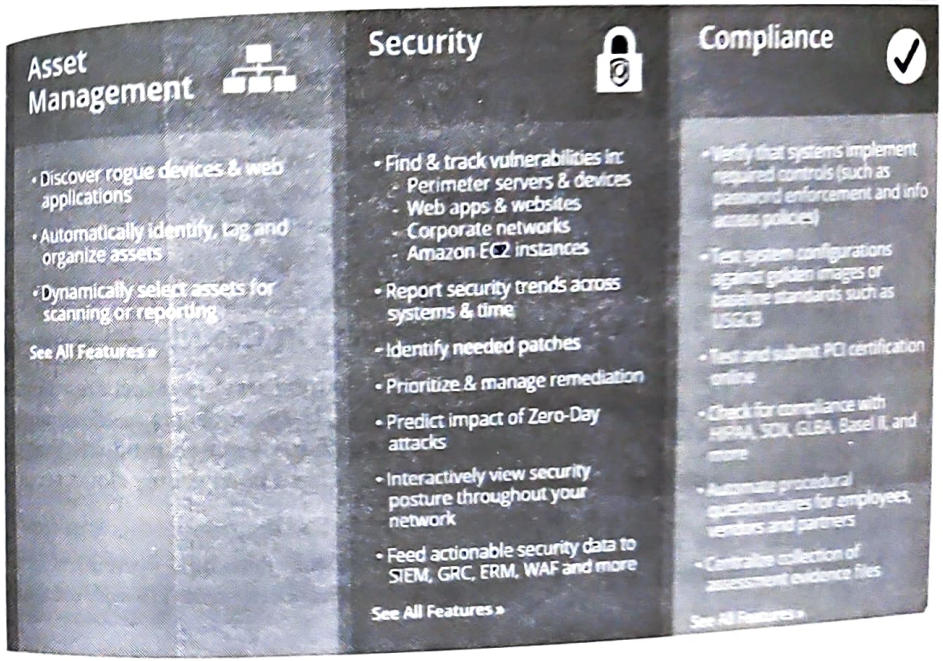

Figure 6.6 | Qualys. (From www.qualys.com)

6.6.6 Vaultive

Vaultive cloud security is one of the most trusted solutions. It ensures business to move on cloud and complies with many regulations like HIPAA, PCI, GLBA and others. Vaultive security solution works on the principle of transparency network proxy which means encryption of data takes place the moment data leave the network and reach out to any cloud application.

6.6.6.1 Features of Vaultive

Following are the key features of Vaultive:

1. Vaultive encryption engine supports all types of cloud-based services.
2. Vaultive helps in directly encrypting SaaS applications without any modification.
3. Vaultive follows the cloud security best practices where customer always holds the encryption keys.

Following are some evolving cloud security and vulnerability assessment tools:

1. Boxcryptor (www.boxcryptor.com)
2. Zscaler (www.zscaler.com)
3. Certify (www.centrify.com)
4. SilverSky (www.silversky.com)
5. HyTrust (www.hytrust.com)
6. Prevoty (www.prevoty.com)
7. Bitium (www.bitium.com)

6.7 Open Source Security Solution Products in Cloud

There are various security solutions for all types of cloud computing services. Most are commercial solutions developed by some other third-party companies. Users or clients need to pay for those security solution products. Here we discuss some open source solution products that can be downloaded and used by anyone. Following are some prominent open source cloud security solution products:

1. **OSSEC–HIDS (Open source security host-based intrusion detection system):** OSSEC (www.ossec.net) is an open source host-based intrusion detection system (HIDS). According to their Website:

   "OSSEC is a scalable, multi-platform, open source Host based Intrusion Detection System (HIDS). It has a powerful correlation and analysis engine, integrating log analysis, file integrity checking, Windows registry monitoring, centralized policy enforcement, rootkit detection, real-time alerting and active response. It runs on most operating systems, including Linux, OpenBSD, FreeBSD, MacOS, Solaris and Windows."

   OSSEC works on a server–client model. The OSSEC server must be installed on Linux/Unix machines and clients (also called agents) can be installed on any operating system. It could be cloud-based instances as well.

   Multiple installation options are available with OSSEC. It could be installed on a stand-alone machine or multi-host scenario, where one instillation is a server and others are agents. The communication between the OSSEC server and the agent is always encrypted.

   OSSEC works well with cloud instances. The OSSEC server and agents can be installed on AWS instances and can monitor file integrity checking, real-time file monitoring and logs inspections.

2. **SNORT**: SNORT is a fully open source network intrusion prevention system (NIPS) and network intrusion detection system (NIDS). It can perform real-time analytics on IP networks. It has three main modes of working – sniffer, packet logger and network intrusion detection. It can be used with AWS EC2 instances also. SNORT host-based IDS supports tracking of running processes, detection of configuration changes, tracking of file access and detection of any abnormal behavior.

   SNORT provides in-flight data encryption for cloud instances; for example, in AWS, all incoming traffic passes through the Elastic Load Balancer, which is used as an HTTPS terminator. It works as proxy traffic for backend IDS instances as HTTP. SNORT is used here for packet analyzing and to decide whether to reject or accept the packet. After transmission, SNORT analyzes the outbound packet and logs the results.

3. **CryptSync:** The best way to protect files is to encrypt them before moving to other servers. CryptSync provides an additional layer of security that makes it difficult for attackers to view files. CryptSync uses two folders that work synchronously. One folder contains current working files that are unencrypted and the other folder contains encrypted files.
4. **Crypton:** Crypton is developed by the SpiderOak and licensed under the AGPL. It enables applications to encrypt data in a Web browser itself before moving to cloud locations. Crypton is a library that allows developers to write secure cloud applications, where all data is encrypted on the client side itself before moving to cloud storage. Crypton supports JavaScript library for Web applications that offer an object storage API. Data storage backend of Crypton is built with compatibility of PostgreSQL, Redis and Node.js.
5. **TrueCrypt:** TrueCrypt is an open-source disk encryption application. It provides real-time and transparent encryption. It creates virtual encrypted disk within a file and mounts it as a real disk. It supports Linux, Mac OS and Windows platforms also. AWS Import/Export supports device encryption using TrueCrypt for import to Amazon S3 and export from Amazon S3.

Summary

In this chapter, we have learned about the most important concern of cloud computing. All cloud service providers and cloud service users first take care of this foremost concern. The chapter has provided a detailed explanation of cloud security fundamentals, cloud risks categories, cloud vulnerability assessment tools according to current industry trends, various VM-related internal security challenges, cloud computing security architecture and some open source security solution products of cloud computing. In the next chapter, we will learn about cloud middleware and some best practices of cloud computing.

Multiple Choice Questions

1. Identify the principle on which CryptSync works.
   (a) Encryption of files before moving to other servers
   (b) Encryption of files after moving to network
   (c) Encryption of files before reaching to other servers
   (d) Encryption/decryption of data during uploading and downloading processes

2. Which one of the following categories does SNORT security tool belong to?
   (a) Host-based intrusion detection system
   (b) Client side data encryption
   (c) Server side data encryption
   (d) Network intrusion detection system

3. How can the denial of service be avoided?
   (a) By network firewall
   (b) By operating system firewall
   (c) By limiting the access of VM resources
   (d) By using intrusion detection system

4. Where does lock-in problem exist?
   (a) In SaaS
   (b) In PaaS
   (c) In IaaS and PaaS
   (d) In SaaS, PaaS and IaaS

5. How many security layers are there in cloud computing security architecture?
   (a) 2
   (b) 3
   (c) 4
   (d) 5

6. Which one of the following categories does OSSEC security tool belong to?
   (a) Network intrusion detection system
   (b) Host-based intrusion detection system
   (c) Client side data encryption
   (d) Server side data encryption

7. Which type of cloud risk is isolation failure?
   (a) Legal risk
   (b) Technical risk
   (c) Policy and organizational risks
   (d) Other risks

8. Which type of cloud risk(s) are data protection risks?
   (a) Legal risk
   (b) Technical risk
   (c) Policy and organizational risks
   (d) Other risks

9. What is the purpose of AWS CloudHSM service?
   (a) Identification and management service
   (b) Directory service
   (c) Dedicated hardware device which stores cryptography encryption and decryption keys
   (d) On-demand cloud security tool for intrusion detection and prevention

10. Which one of the following options is the key feature of Netskope cloud security service?
    (a) One policy can control all your cloud apps
    (b) Network and VM monitoring
    (c) Encryption/decryption of data during uploading and downloading processes
    (d) Open source service

11. Which one of the following options is the key feature of CipherCloud?
    (a) Data prevention
    (b) Data loss monitoring
    (c) Encryption/decryption of data during uploading and downloading processes
    (d) Network and VM monitoring

12. Identify the technology on which Skyhigh security works.
    (a) Transparency network proxy
    (b) Reverse proxy technology
    (c) Single sign on (SSO)
    (d) On-demand

13. Identify the principle on which Vaultive security solution works.
    (a) Principle of transparency network proxy
    (b) Reverse proxy technology
    (c) Single sign on (SSO)
    (d) On demand

14. Which one of the following options is the key feature of Okta security solution?
    (a) On demand
    (b) Anytime accessible
    (c) Single sign on
    (d) VM protection

15. Which one of the following options is evolving cloud security and vulnerability assessment tools?
    (a) SilverSky
    (b) OSSEC
    (c) SNORT
    (d) CloudHSM

Review Questions

1. Which policy and organizational risks are associated with cloud computing?
2. What do you understand by compromise service engine risk?
3. List out some key legal risks associated with cloud computing.
4. Explain the security concerns associated with each layer of cloud security architecture.
5. How do open source products provide security in a cloud scenario? Explain with the help of OSSEC and SNORT.