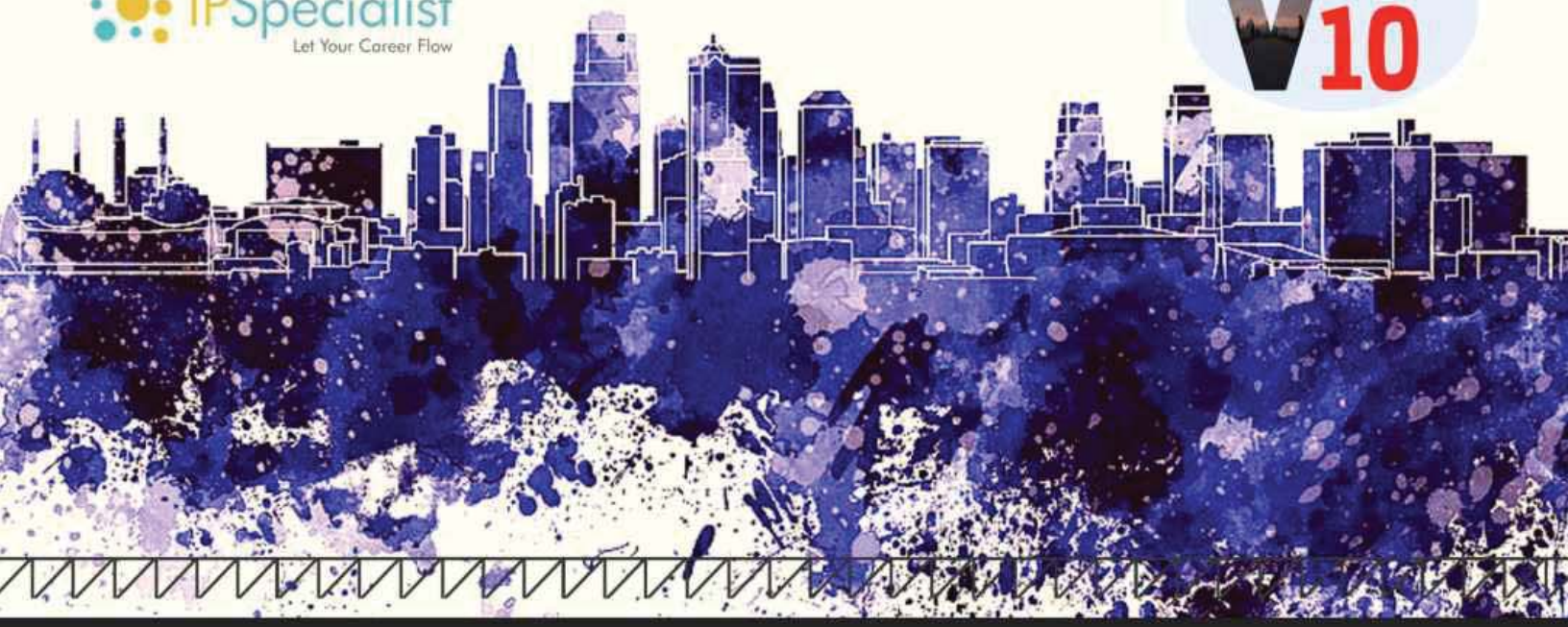
IPSpecialist
Let Your Career Flow

V10



CEH V10 EC-COUNCIL CERTIFIED ETHICAL HACKER

MOST DEMANDING COMPLETE HACKING GUIDE

EXAM: 312-50

C|EH
Certified Ethical Hacker

"To beat a hacker, you need to think like a hacker

MOST ADVANCED HACKING COURSE

www.ipspecialist.net

Chapter 19: Cloud Computing

Introduction to Cloud Computing

Cloud Computing technology is the most popular now a day because of its flexibility and mobility support. Cloud Computing allows the access to personal and shared resources with minimal management. It often relies on the internet. There is also third-party cloud solution available which saves expanding resources and maintenance. Most appropriate example of Cloud computing is Amazon Elastic Cloud Compute (EC2), highly capable, low cost, and flexible. Major characteristics of cloud computing include:

- On-demand self-service
- Distributed Storage
- Rapid Elasticity
- Measured Services
- Automated Management
- Virtualization

Types of Cloud Computing Services

Cloud Computing Services are categorized into the following three types: -

- Infrastructure-as-a-Service (IaaS)
- Platform-as-a-Service (PaaS)
- Software-as-a-Service (SaaS)

Infrastructure-as-a-Service (IaaS)

Infrastructure services, (IaaS) also known as Cloud infrastructure service is basically a self-service model. IaaS is used for accessing, monitoring and managing purpose. For example, instead of purchasing additional hardware such as firewall, networking devices, server and spending money on deployment, management, and maintenance, IaaS model offers cloud-based infrastructure to deploy remote datacenter. Most popular examples of IaaS are Amazon EC2, Cisco Metapod, Microsoft Azure, Google Compute Engine (GCE).

Platform-as-a-Service (PaaS)

Platform as a service another cloud computing service. It allows the users to develop, run and manage applications. PaaS offers Development tools, Configuration management, Deployment Platforms, and migrate the app to

hybrid models. It basically helps to develop and customize applications, manage OSes, visualization, storage and networking, etc. Examples of PaaS are Google App Engine, Microsoft Azure, Intel Mash Maker, etc.

Software-as-a-Service (SaaS)

Software as a Service (SaaS) is one of the most popular types of Cloud Computing service that is most widely used. On-demand Software is centrally hosted to be accessible by users using client via browsers. An example of SaaS is office software such as office 365, Cisco WebEx, Citrix GoToMeeting, Google Apps, messaging software, DBMS, CAD, ERP, HRM, etc.

Cloud Deployment Models

The following are the Deployment models for Cloud Services.

Deployment Model	Description
Public Cloud	Public clouds are hosted by a third party offering different types of Cloud computing services.
Private Cloud	Private Clouds are hosted personally, individually. Corporate companies usually deploy their private clouds because of their security policies.
Hybrid Cloud	Hybrid Clouds are comprised of both Private and public cloud. Private cloud is for their sensitive and public cloud to scale up capabilities and services.
Community Cloud	Community Clouds are accessed by multiple parties having common goals and shared resources.

Table 19-01. Cloud Deployment Models

NIST Cloud Computing Reference Architecture

Following Architecture is a generic high-level conceptual reference architecture presented by NIST (National Institute of Standards and Technology). NIST cloud computing reference architecture, which identifies the major Components and their functions in cloud computing. NIST Architecture is intended to facilitate the understanding of the requirements, uses, characteristics, and standards of cloud computing.

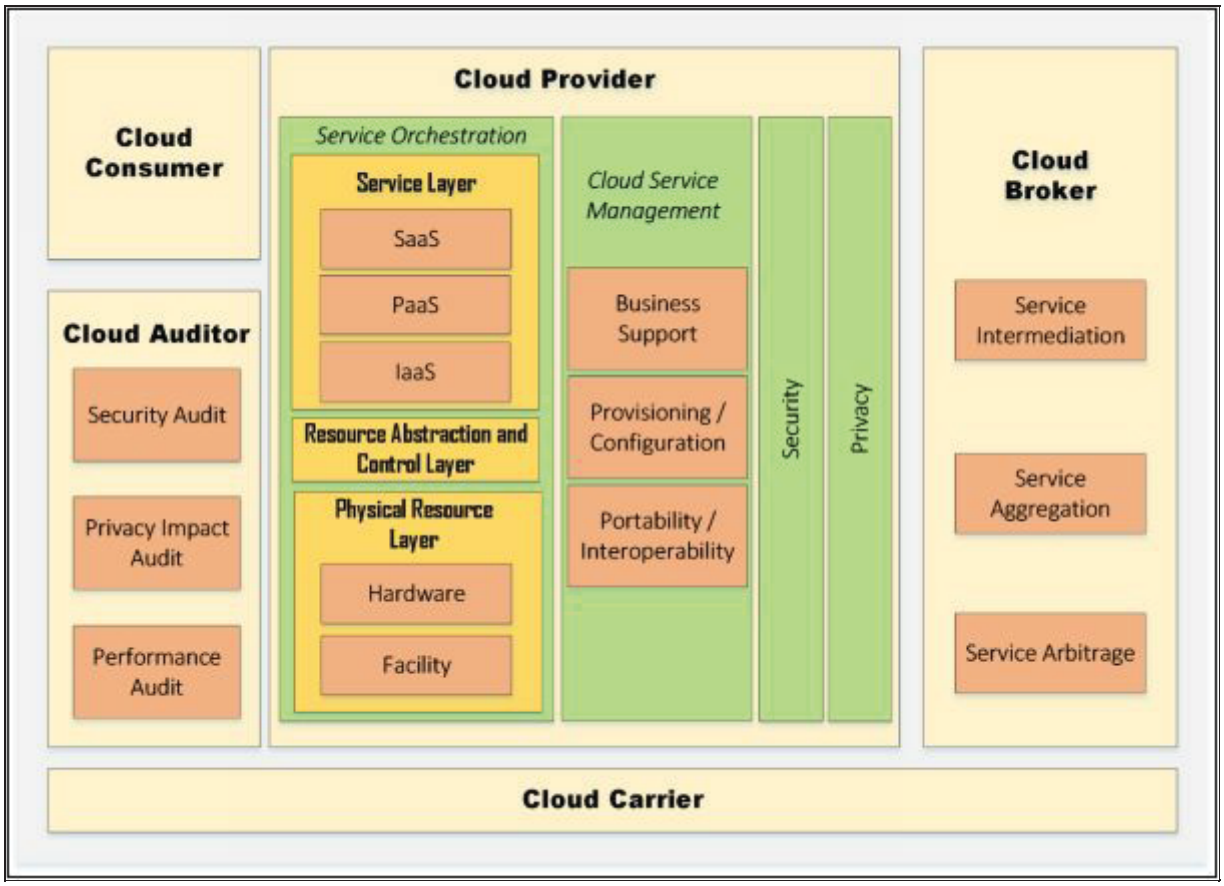


Figure 19-01. NIST Cloud Computing Reference Architecture

NIST Cloud Computing Architecture defines Five Major Actors, Cloud Consumer, Cloud Provider, Cloud Carrier, Cloud Auditor and Cloud Broker.

Actor	Definition
Cloud Consumer	A person or organization that maintains a business relationship with, and uses service from, Cloud Providers.
Cloud Provider	A person, organization, or entity is responsible for making a service available to interested parties.
Cloud Auditor	A party that can conduct an independent assessment of cloud services, information system operations, performance and security of the cloud implementation.
Cloud Broker	An entity that manages the use, performance, and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers.

Cloud Carrier	An intermediary that provides connectivity and transport of cloud services from Cloud Providers to Cloud Consumers.

Table 19-02. Actors

Cloud Computing Benefits

There are abundant advantages of cloud computing in which some most important are discussed here;

Increased Capacity:

By using cloud computing, the users have not worry about the capacity of infrastructure as the cloud platform provides the unlimited capacity or simply we can say that by using a cloud platform, the customer can use as much capacity as he wants or as small capacity as he needs.

Increased Speed:

Cloud computing environment has dramatically reduced the time, and cost of new IT services thus increased the speed for organizations to access the IT resources.

Low Latency:

By using cloud computing, the customers have a facility of implementing their applications with just a few clicks, so they can do all tasks easily at minimal costs, i.e., not too much time consumed as well as minimum latency is produced.

Less Economic Expense

The major advantage of Cloud Computing is a Less economic expense. No need to purchase dedicated hardware for a particular function. Networking, Datacenter, firewall, application and other services can be easily virtualized over cloud saving the cost of purchasing hardware, configuration and management complexity and less maintenance cost.

Security

In terms of security, cloud computing is also efficient. Major advantages include less investment over security with effective patch management and security updates. Disaster recovery, dynamically scaling defensive resources and other security services offers protection against cloud computing threats.

Understanding Virtualization

Virtualization in computer networking is a process of deploying a machine or multiple machines virtually on a host. These virtually deployed machines use the system resources of the host machine by logical division. Major Difference between a physically deployed machine and a virtual machine is of system resources and hardware. Physical deployment requires separate dedicated hardware for an on Operating system whereas a virtual machine host can support multiple operating systems over a single system sharing the resources such as storage.

Benefits of Virtualization in Cloud

The major advantage of virtualization is cost reduction. Purchasing dedicated hardware not only cost enough but it also requires maintenance, management, and security. Additional hardware consumes space and power consumptions whereas Virtualization support multiple machines over single hardware. Furthermore, virtualization also reduces administration, management and networking tasks, ensures efficiency. Virtualization over the cloud is even more effective where no need to install even single hardware. All virtual machines deployed over a host is owned by cloud over the internet. You can easily access them from anywhere any time.

Cloud Computing Threats

As cloud computing is offering many services with efficiency, and flexibility, there are also some threats, from which cloud computing is vulnerable. These threats include Data loss/breach, insecure interfaces and APIs, malicious insider, privileges escalations, natural disasters, hardware failure, authentication, VM level attacks and much more.

Data Loss/Breach

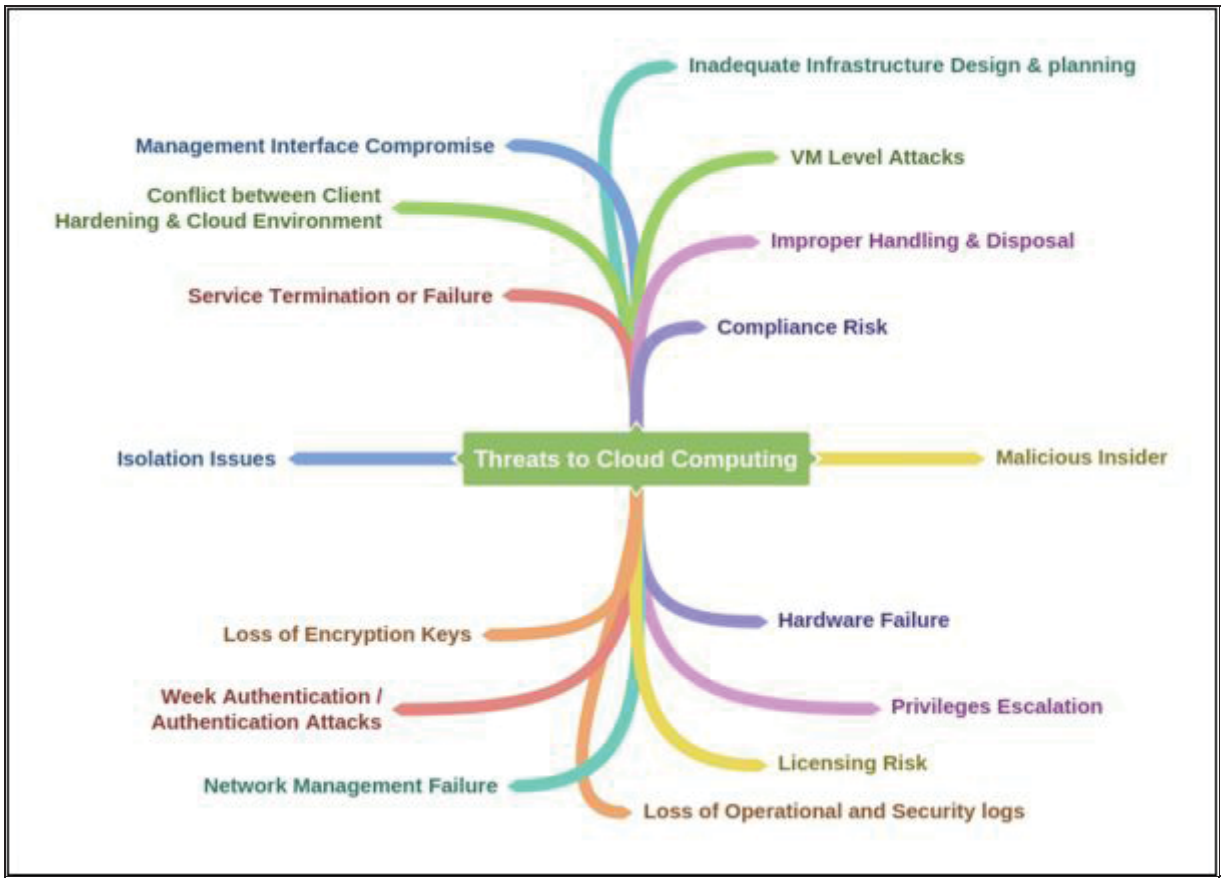
Data loss and Data breach are the most common threat to every platform. Improper Encryption or losing Encryption keys may result in Data modification, erasing, data steal, and misuse.

Abusing Cloud Services

Abusing Cloud Services includes using service for malicious intents as well as using these services abusively. For example, Dropbox cloud service was abused by an attacker to spread massive phishing campaign. Similarly, it can be used to host, malicious data and Botnet command and control, etc.

Insecure Interface and APIs

Software User Interface (UI) and Application Programming Interface (APIs) are the interfaces used by customers to interact the service. These interfaces can be secure by performing Monitoring, Orchestration, Management and provisioning. These interfaces must be secure against malicious attempts.


Threats to Cloud Computing
Inadequate Infrastructure Design & planning
Management Interface Compromise
VM Level Attacks
Conflict between Client Hardening & Cloud Environment
Improper Handling & Disposal
Service Termination or Failure
Compliance Risk
Isolation Issues
Malicious Insider
Hardware Failure
Loss of Encryption Keys
Week Authentication / Authentication Attacks
Privileges Escalation
Licensing Risk
Network Management Failure
Loss of Operational and Security logs

Cloud Computing Attacks

In Cloud Computing, the following are the most common attacks that are being in used by an attacker to extract sensitive information such as credentials or gaining unauthorized access. Cloud Computing Attacks includes: -

- Service Hijacking using Social Engineering Attacks
- Session Hijacking using XSS Attack
- Domain Name System (DNS) Attack
- SQL Injection Attack
- Wrapping Attack
- Service Hijacking using Network Sniffing
- Session Hijacking using Session Riding
- Side Channel Attack or Cross-guest VM Breaches
- Cryptanalysis
- Dos / DDoS Attacks

Service Hijacking using Social Engineering Attacks

We have already discussed social engineering attacks. Using Social Engineering techniques, the attack may attempt to guess the password. Social Engineering attacks result in unauthorized access exposing sensitive information according to the privilege level of the compromised user.

Service Hijacking using Network Sniffing

Using Packet Sniffing tools by placing himself in the network, an attacker can capture sensitive information such as passwords, session ID, cookies, and another web service-related information such as UDDI, SOAP, and WSDL

Session Hijacking using XSS Attack

By launching Cross-Site Scripting (XSS), the attacker can steal cookies by injecting malicious code into the website.

Session Hijacking using Session Riding

Session Riding is intended for session hijacking. An attacker may exploit it by attempting cross-site request forgery. The attacker uses currently active session and rides on it by executing the requests such as modification of data, erasing data, online transactions and password change by tracking the user to click on a malicious link.

Domain Name System (DNS) Attacks

Domain Name System (DNS) attacks include DNS Poisoning, Cybersquatting, Domain hijacking and Domain Snipping. An attacker may attempt to spoof by poisoning the DNS server or cache to obtain credentials of internal users. Domain Hijacking involves stealing cloud service domain name. Similarly, through Phishing scams, users can be redirected to a fake website.

Side Channel Attacks or Cross-guest VM Breaches

Side Channel Attacks or Cross-Guest VM Breach is an attack which requires the deployment of a malicious virtual machine on the same host. For example, a physical host is hosting a virtual machine that is offering the cloud services hence the target of an attacker. The attacker will install a malicious virtual machine on the same host to take advantage of sharing resources of the same host such as processor cache, cryptographic keys, etc. Installation can be done by a malicious insider, or an attacker by impersonating a legitimate user.

Similarly, there are other attackers that are discussed earlier are also vulnerable to Cloud Computing such as SQL Injection attack (injecting malicious SQL statements to extract information), Cryptanalysis Attacks (weak or obsolete encryption) Wrapping Attack (duplicating the body of message), Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks.

Cloud Security

Cloud Computing Security refers to the security implementations, deployments, and preventions to defend against security threats. Cloud Security includes Control policies, deployment of security devices such as application firewalls, Next Generation IPS devices and hardening the infrastructure of Cloud computing. It also includes some activities that are to be taken from the service providers end as well as actions that should be taken at the user end.

Cloud Security Control Layers

Application Layer

There are several security mechanisms, devices, and policies that provide support at different cloud security controls layers. At the Application layer, Web application firewalls are deployed to filter the traffic and observe the behavior of traffic. Similarly, Systems Development Life Cycle (SDLC), Binary Code Analysis, Transactional Security provide security for online transactions, and script analysis, etc.

Information

In Cloud Computing, to provide confidentiality and integrity of information that is being communicated between client and server, different policies are configured to monitor any data loss. These policies include Data Loss Prevention (DLP) and Content Management Framework (CMF). Data Loss Prevention (DLP) is the feature which offers to prevent the leakage of information to outside the network. Traditionally this information may include company or organizations confidential information, proprietary, financial and other secret information. Data Loss Prevention feature also ensures the enforcement of compliance with the rules and regulations using Data Loss Prevention policies to prevent the user from intentionally or unintentionally sending this confidential information.

Management

Security of Cloud Computing regarding management is performed by different approaches such as Governance, Risk Management, and Compliance (GRC), Identity and Access Management (IAM), Patch and Configuration management. These approaches help to control the secure access to the resources and manage them.

Network layer

There are some solutions available to secure the network layer in cloud computing such as the deployment of Next-Generation IDS/IPS devices, Next-Generation Firewalls, DNSSec, Anti-DDoS, OAuth and Deep Packet Inspection (DPI), etc. Next-Generation Intrusion Prevention System, known as NGIPS, is one of the efficiently-proactive components in the Integrated Threat Security Solution. NGIPS provide stronger security layer with deep visibility, enhanced security intelligence and advanced protection against emerging threat to secure complex infrastructures of networks.

Cisco NGIPS Solution provides deep network visibility, automation, security intelligence, and next-level protection. It uses the most advanced and effective intrusion prevention capabilities to catch emerging sophisticated network attacks. It continuously collects information regarding the network, including operating systems information, files and applications information, devices and user's information. This information helps NGIPS to determine network maps and host profiles which lead to contextual information to make better decisions about intrusive events.

Trusted Computing

The root of Trust (RoT) is established by validating each component of hardware and software from the end entity up to the root certificate. It is intended to ensure that only trusted software and hardware can be used while still retaining flexibility.

Computer and Storage

Computing and Storage in cloud computing can be secured by implementing Host-based Intrusion Detection or Prevention Systems HIDS/HIPS. Configuring Integrity check, File system monitoring and Log File Analysis, Connection Analysis, Kernel Level detection, Encrypting the storage, etc. Host-based IPS/IDS is normally deployed for the protection of specific host machine, and it works closely with the Operating System Kernel of the host machine. It creates a filtering layer and filters out any malicious application call to the OS.

Physical Security

Physical Security is always required on priority to secure anything. As it is also the first layer OSI model, if the device is not physically secured, any sort

of security configuration will not be effective. Physical security includes protection against man-made attacks such as theft, damage, unauthorized physical access as well as environmental impact such as rain, dust, power failure, fire, etc.

Responsibilities in Cloud Security

Cloud Service Provider

Responsibilities of a cloud service provider include to meet the following security controls: -

- Web Application Firewall (WAF).
- Real Traffic Grabber (RTG)
- Firewall
- Data Loss Prevention (DLP)
- Intrusion Prevention Systems
- Secure Web Gateway (SWG)
- Application Security (App Sec)
- Virtual Private Network (VPN)
- Load Balancer
- CoS/QoS
- Trusted Platform Module
- Netflow and others.

Cloud Service Consumer

Responsibilities of a cloud service consumer include to meet the following security controls: -

- Public Key Infrastructure (PKI).
- Security Development Life Cycle (SDLC).
- Web Application Firewall (WAF).
- Firewall
- Encryption.
- Intrusion Prevention Systems
- Secure Web Gateway
- Application Security
- Virtual Private Network (VPN) and others.

Cloud Computing Security Considerations


Cloud Computing Countermeasures & Security Considerations
Software Configuration Management (SCM)
Strong Key Generation
Disaster Recovery Plan
Patching & Updates
AICPA SAS 70 Type II Audits
Data Integrity
Load Balancing
Backup
VPN
SSL
Strong AAA mechanism
Cryptography Implementation
Reliability
Quality of Service (QoS)
Monitoring Activities
Prohibit Credentials Sharing
Service Level Agreement (SLA)
Higher Multi-Tenancy
Supply Chain Management

Cloud Security Tools

Core CloudInspect

Core Security Technologies offers "Core CloudInspect," A cloud Security testing solutions for Amazon Web Services (AWS). This is a tool that profits from the Core Impact and Core Insight technologies to offer penetration-testing as a service from Amazon Web Services for EC2 users.

CloudPassage Halo

Cloud Passage Halo provides a broad range of Security controls. It is a Focused Cloud Security Solution which prevents attacks and detects an indication of compromise. Cloud Passage Halo operates under the ISO-27002 security standards and is audited annually against PCI Level 1 and SOC 2 standards. Cloud Passage Halo is the only workload security automation platform that offers on-demand delivery of security controls across data centers, private/public clouds, virtual machines, and containers – at speed and scale. Unlike traditional security systems, Halo and its robust APIs integrate with popular CI/CD toolchains and processes, providing just-in-time feedback to fix vulnerabilities early in the development cycle. This lets DevOps teams perform while providing security teams the validation they require. Halo easily integrates with popular infrastructure automation and orchestration platforms, allowing Halo to be easily deployed to monitor the security and compliance posture of workloads continuously.

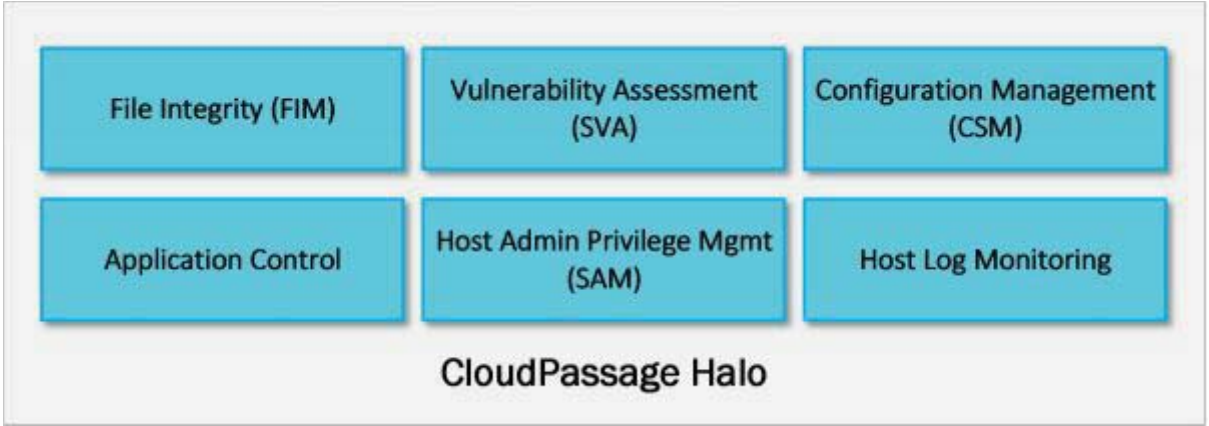
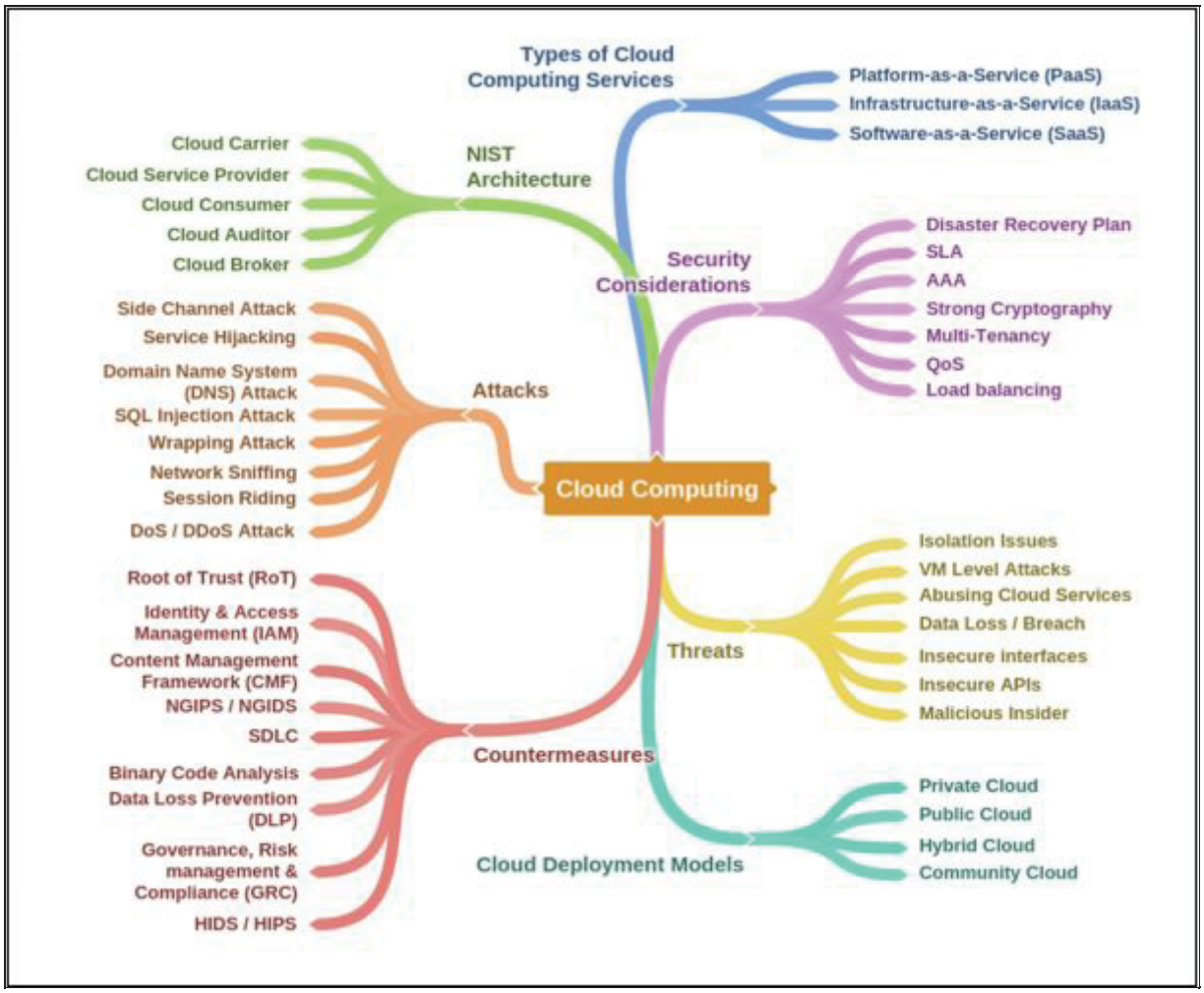


Figure 19-02. Cloud Passage Halo Components

Mind Map


Cloud Computing
Types of Cloud Computing Services
Platform-as-a-Service (PaaS)
Infrastructure-as-a-Service (IaaS)
Software-as-a-Service (SaaS)
NIST Architecture
Cloud Carrier
Cloud Service Provider
Cloud Consumer
Cloud Auditor
Cloud Broker
Security Considerations
Disaster Recovery Plan
SLA
AAA
Strong Cryptography
Multi-Tenancy
QoS
Load balancing
Attacks
Side Channel Attack
Service Hijacking
Domain Name System (DNS) Attack
SQL Injection Attack
Wrapping Attack
Network Sniffing
Session Riding
DoS / DDoS Attack
Threats
Isolation Issues
VM Level Attacks
Abusing Cloud Services
Data Loss / Breach
Insecure interfaces
Insecure APIs
Malicious Insider
Countermeasures
Root of Trust (RoT)
Identity & Access Management (IAM)
Content Management Framework (CMF)
NGIPS / NGIDS
SDLC
Binary Code Analysis
Data Loss Prevention (DLP)
Governance, Risk management & Compliance (GRC)
HIDS / HIPS
Cloud Deployment Models
Private Cloud
Public Cloud
Hybrid Cloud
Community Cloud