Accedere

Why businesses are failing to protect Cloud data?

Accedere

Contents

Accedere

Contents

How Accedere helps conduct a comprehensive assessment of the organization's cloud environment using NIST as a benchmark?

Policies and Procedures

Mitigation Techniques for OWASP Top 10 Cloud Security Issues

About Us

Accedere

Colorado Licensed CPA Firm

Focusing on Cyber Security Audits

Cloud and Data Privacy Experts

Specializing in SOC Attest Reports

Why Accedere?

We are a firm focusing on Cloud Security and Data Privacy

Our team carries extensive experience in the field and are listed with Cloud Security Alliance as Auditors

Our team has several years of Cybersecurity experience with leading industry certifications.

We have specific experience working with cloud controls for clients such as Cisco, Reliance Jio etc.

Our credentials- Our global customers

Accedere

Case Studies & Surveys

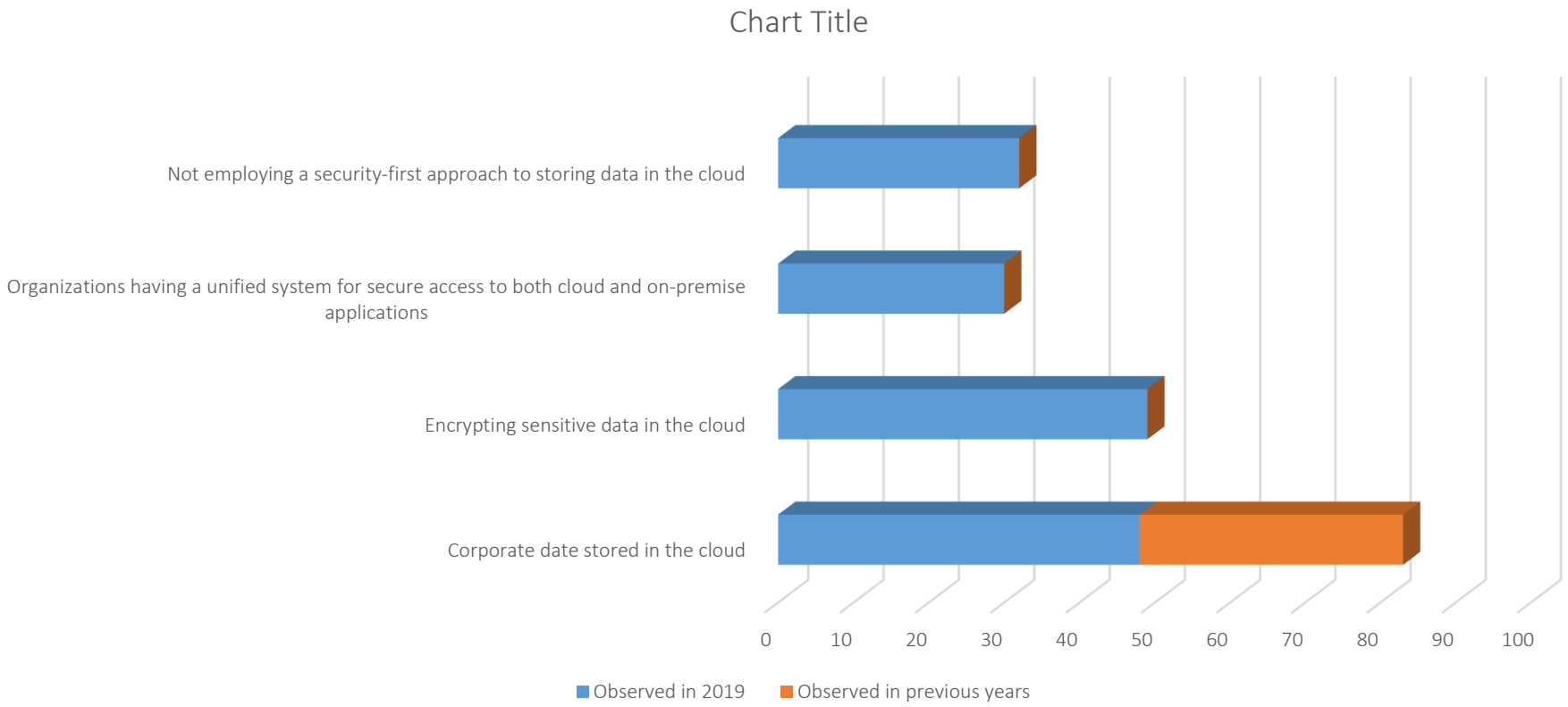
Case Study

For most businesses, the cloud simply works better than so-called on-premises. And it isn't just about money. While any organization is interested in cutting costs, the main drivers of cloud migration are disaster recovery, ease of management, and archival.

According to the 2019 Thales Cloud Security Study, organizations are failing to protect sensitive data in the cloud. Businesses are taking advantage of the cloud, but not applying adequate security.

Surveys

Following were the observations noted from the Thales surveys:

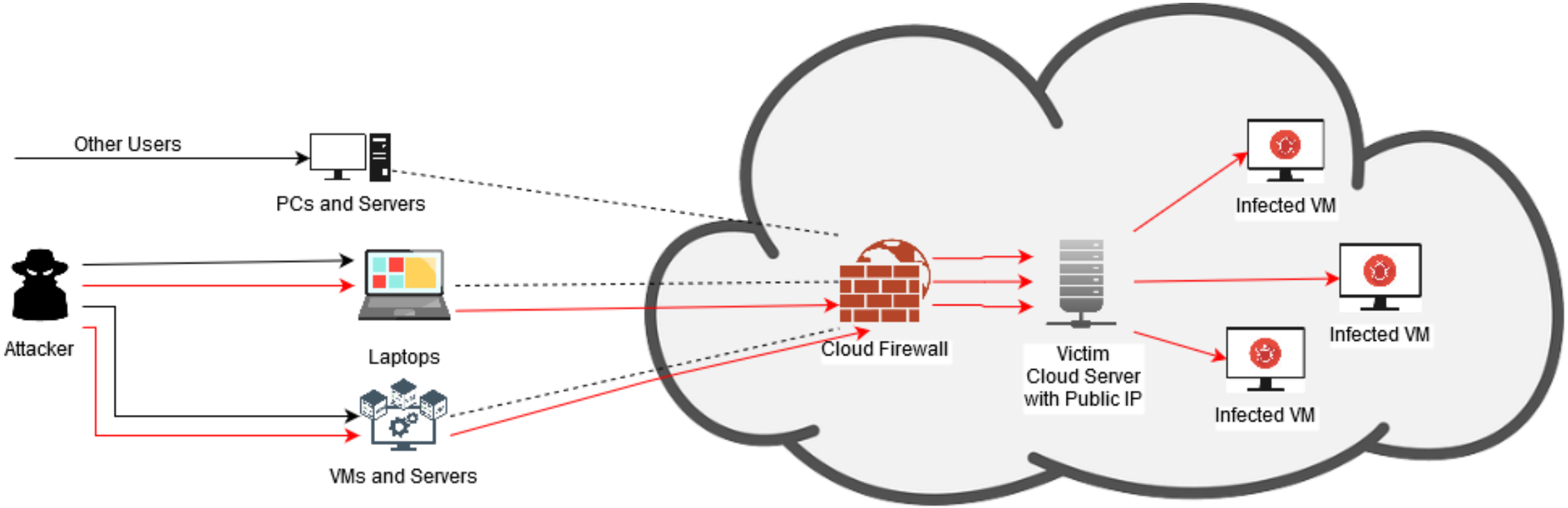


Accedere

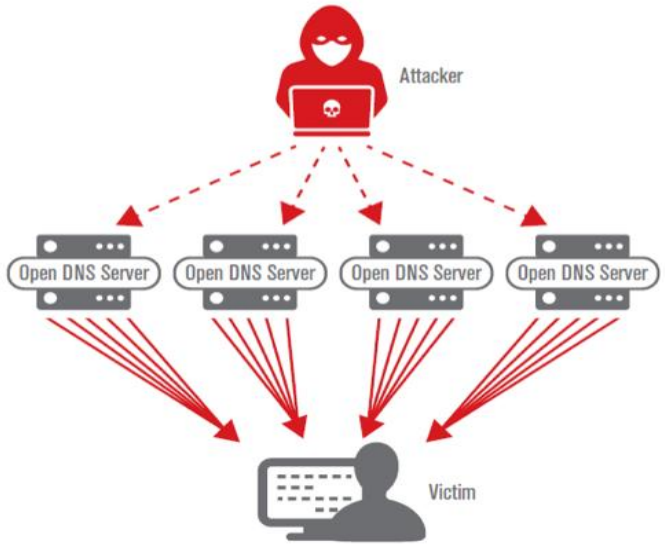
Attack Scenario

Understanding the Attack Scenario

During an **attack**, an outside party attempts to flood an organization's systems using a numerous amount of connections to **overwhelm** the system. Since the hackers can use programs or bots to generate numerous attacks, organizations cannot block just one IP address from shutting down a specific process.

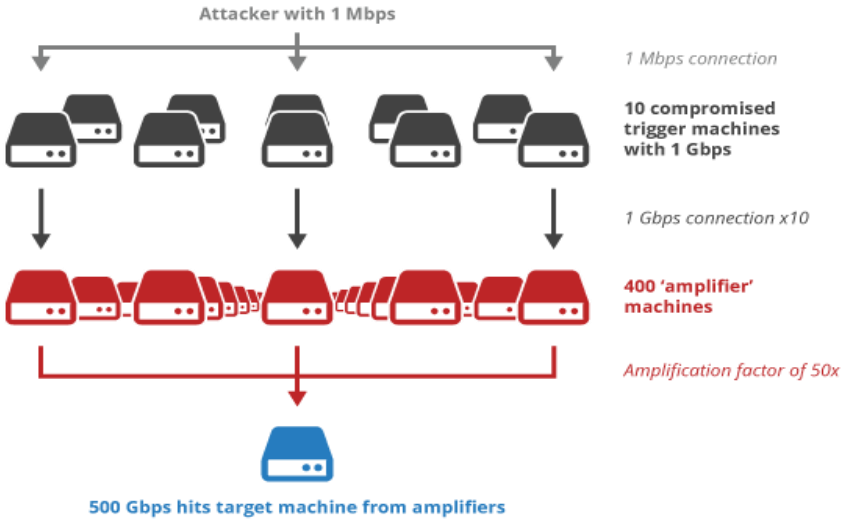


Types of Attacks



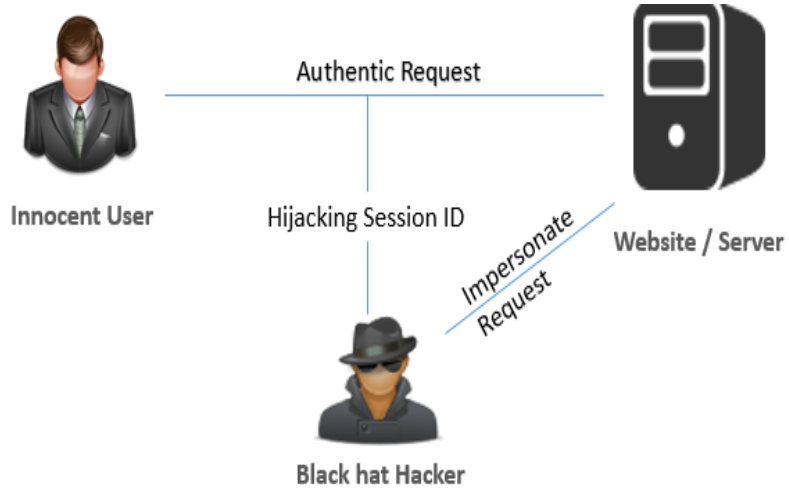
Volume-based Attacks

Attacker use high traffic to inundate the network bandwidth.



Protocol-based Attacks

Attacker focuses on exploiting server resources



Application Attacks

Attacker focuses on web applications and are considered the most sophisticated and serious type of attacks

Accedere

Major Reasons for Cloud Threats

The Challenges

Following are the listed threats as well as the possible vulnerabilities concerning the reported threats observed in Cloud Environments:

Threat Name	Possible Vulnerabilities
Data Breaches	Targeted Attack
	Simple Human Errors
	Application Vulnerabilities
	Poor Security Policies
	Natural Disasters
Data Loss	Natural Disasters
	Simple Human Errors
	Hard Drive Failure
	Power Failures
	Malware Infection

The Challenges

Threat Name	Possible Vulnerabilities
Malicious Insider	Former Employee
	System Administrator
	Third-Party Contractor
	Business Partner
Denial of Service	Weak Network Architecture
	Insecure Network Protocol
	Vulnerable Application
Vulnerable System and API	Weak API Credentials
	Key Management
	Operating System Bugs
	Hypervisor Bugs
	Unpatched Software

Accedere

OWASP Top 10 Cloud Security Issues

OWASP Top 10 Risks

#1. Accountability and Data Ownership

Using a third party to store and transmit data adds to a new layer of risk. Cloud service providers often also operate across geographical jurisdictions. Data protection regulations such as the General Data Protection Regulation (GDPR) require that the data processors as well as the data controllers, meet the requirements of the regulation. It is important to ensure accountability of data protection, including recovery and backup, with any third-party Cloud providers you use.

OWASP Top 10 Risks

#2. User Identity Federation

Digital identity is a key part of cybersecurity. It controls vital areas such as privileged access to sensitive resources. As enterprises increase their use of Cloud apps and have data stored across Cloud services, control of access through identity management is crucial.

OWASP Top 10 Risks

#3. Regulatory Compliance

OWASP points out the issues of meeting compliance across geographical jurisdictions. For example, if your organization is based in Europe but you use a U.S. Cloud provider, then it might be difficult to map the compliance requirements of EU-centric data protection, and vice versa.

OWASP Top 10 Risks

#4. Business Continuity and Resiliency

Outsourcing your IT infrastructure to a third-party cloud provider increases the risk of attaining business continuity for the simple reason that it is outside your control. An outage of Cloud services can have serious repercussions for a business. When Amazon went down for 13 minutes, they lost an estimated $2,646,501.

OWASP Top 10 Risks

#5. User Privacy and Secondary Usage of Data

Once data enters the Cloud realm, it is much more difficult to control across its life cycle.
For example, social media sites can be difficult to manage, often defaulting to ‘share all’. Data mining of data for secondary use in targeted ads is a privacy risk.

OWASP Top 10 Risks

#6. Service and Data Integration

The safe transmission of data is a particular risk in Cloud computing models where it is transmitted over the internet.

OWASP Top 10 Risks

#7. Multi-Tenancy and Physical Security

Cost savings often dictate that Cloud servers are used in a multi-tenancy setup. This means that you will share server resources and other services, with one or more additional companies. The security in multi-tenancy environments is focused on the logical rather than the physical segregation of resources. The aim is to prevent other tenants from impacting the confidentiality, integrity, and availability of data.

OWASP Top 10 Risks

#8. Incident Analysis and Forensic Support

If a data breach occurs, you must understand how to identify and manage critical vulnerabilities so you respond to the incident as quickly and effectively as possible. Cloud computing can make the forensic analysis of security incidents more difficult. This is because audits and events may be logged to data centers across multiple jurisdictions.

OWASP Top 10 Risks

#9. Infrastructure Security

This covers the entire gamut of how to harden the attack surface of a Cloud infrastructure. It includes configuring tiers and security zones as well as ensuring the use of pre-established network and application protocols. It also includes regular risk assessments with updates to cover new issues.

OWASP Top 10 Risks

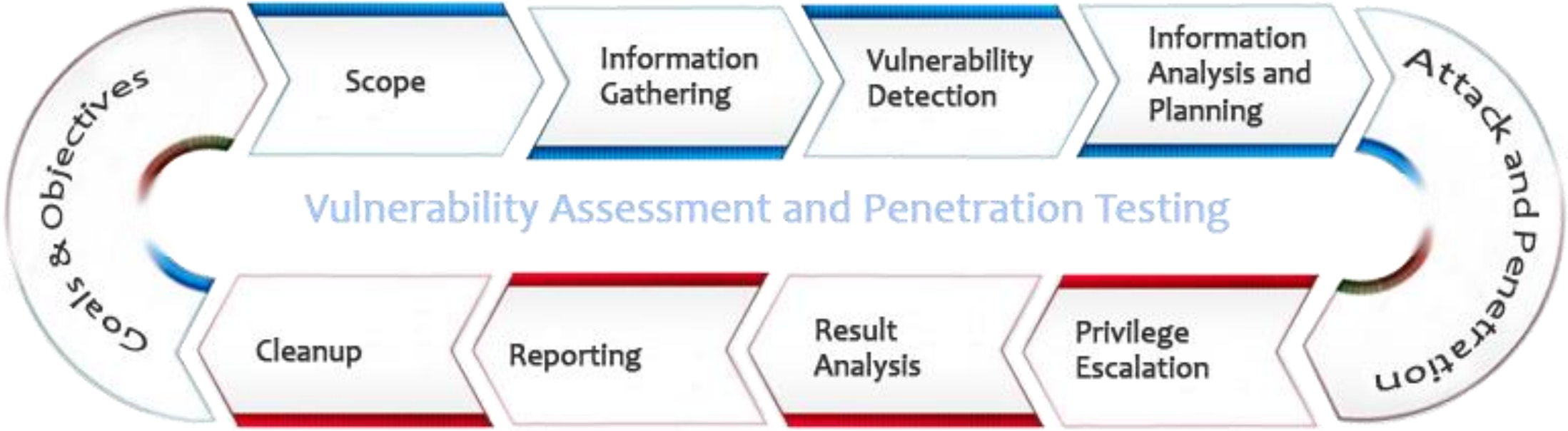
#10. Non-Production Environment Exposure

Risks need to be accounted for across the entire life cycle of application development and implementation. This includes pre-production environments where design and test activities occur. Because these environments may have less stringent security applied, they may well open up security and privacy risks.

Accedere

Vulnerability Assessment and Penetration Testing Phases

Phases


Goals & Objectives
Scope
Information Gathering
Vulnerability Detection
Information Analysis and Planning
Attack and Penetration
Vulnerability Assessment and Penetration Testing
Cleanup
Reporting
Result Analysis
Privilege Escalation

Phases

Reconnaissance:
Also known as footprinting. It's a process of gathering data or preliminary inspection of an area of interest over a short period of time.

Scanning:
Collect more detailed information based on the previous phase. Also known as enumeration.

Gaining access:
This is the actual attack phase; so, the risk level is considered highest.

Maintaining access:
If the intentions of the hacker will not be satisfied by acquiring access, then maintaining that access is also important.

Phases

Covering tracks:
It is in the best interest of the hacker to erase his fingerprints from the scene. Rootkits to an extent does the job, but a hacker can modify log files to hide all those programs or applications that he has installed, from the view of the computer system.

Gathering logs:
Keeping a record of the scans or reports gathered from the attack/scan performed.
Testing outcomes:
Detailed technical report
Executive summary
High-level fixation solutions

Accedere

How VA PT can help organizations know about the risk?

Assessments

Vulnerability Assessment and Penetration Testing (VAPT) are two types of assessments:

- Vulnerability scanners alert with flaws in code.

- Penetration test attempt to exploit if any malicious activity is possible and identify which flaws pose a threat to the application, or if there is a threat by unauthorized access.

Cloud Assessments

Unlike information technology systems in a traditional data center, in cloud computing, responsibility for mitigating the risks that result from these software vulnerabilities is shared between the **CSP** and the **cloud consumer**. The risks include **unauthorized access to customer data, security risk at vendor, Compliance and legal risks, risk related to lack of control, and availability risk**.

Cloud application audit addresses these risks and safeguards the organization for Cloud functionalities.

Accedere

How Accedere helps conduct a comprehensive assessment of the organization's cloud environment using NIST as a benchmark?

Scope

As part of a Cloud Configuration Review, we conduct interviews with application stakeholders (business analysts, developers, testers, program and product managers, etc.) to understand your application's business context and security criteria. Following this, we assess the tool analysis of your cloud environment. The following are some of the security concerns we review during a Cloud Configuration Review:

Scope

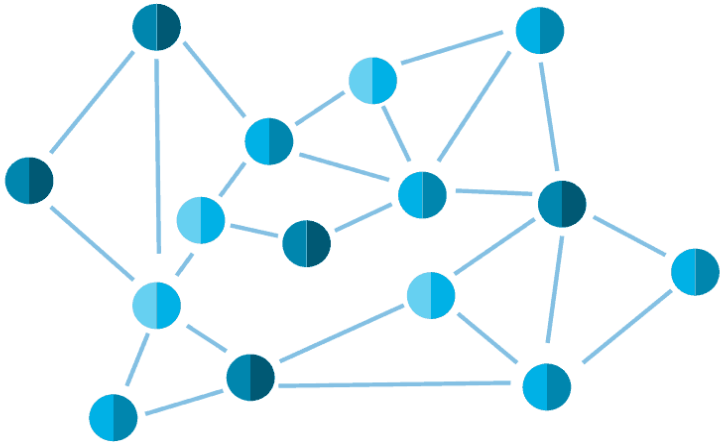
#1. Authentication, authorization, and identity management

We assess your approach to access controls, including federation and realization as identity access management (IAM) policy. We evaluate the proper use of security groups to ensure that the principles of least privilege and separation of duties are followed. Other concerns include the protection of privileged accounts using appropriate technologies (e.g., multi-factor authentication) as well as key management methodologies implemented (i.e. Encryption standards).

Scope

#2. Cloud networking

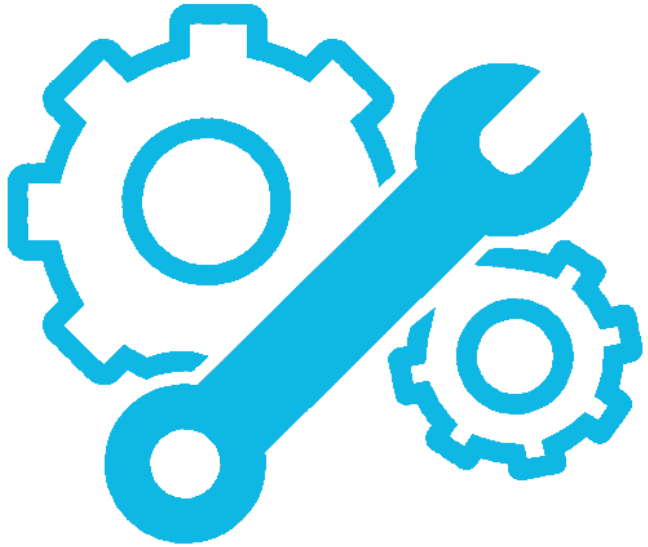
We check your cloud networking configuration for proper isolation of sensitive cloud workloads from one another, correct use of network security groups and network ACLs, validation of authorization to make network changes, proper encryption of network traffic within and outside the cloud environment, and other controls required to guarantee secure networking in the cloud infrastructure.



Scope

#3. Cloud compute

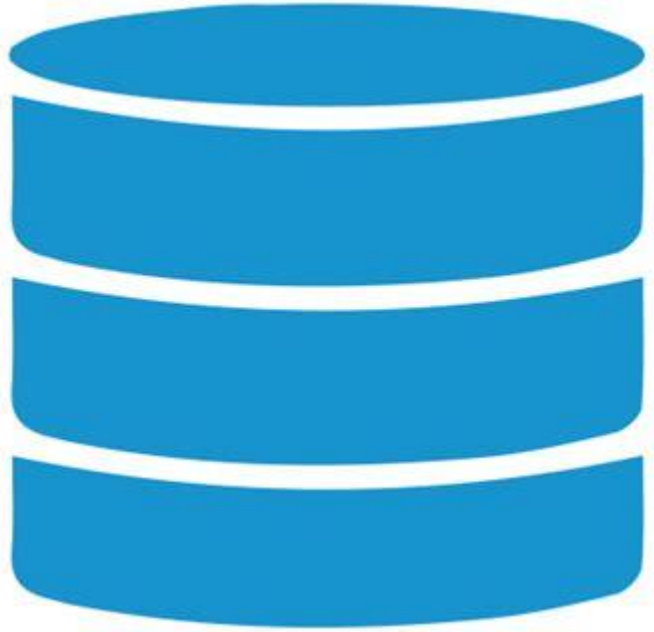
We review the implementation of cloud virtual machines to ensure that they have been appropriately granted and secured to access company workloads.



Scope

#4. Cloud storage

We evaluate the implementation of controls used to protect cloud storage, including object storage, block storage, file storage, message queues, and other storage services used by the application. We determine whether data directed to application storage is properly protected in motion and at rest and not exposed to unauthorized parties, including anonymous users – a situation that is prevalent with many cloud service implementations.



Scope

#5. Other services

We assess other services you may have implemented to support your cloud workload, including database services (SQL or NoSQL based), server-less functions (e.g., AWS Lambda and Azure Functions), logging and monitoring services, and backup and disaster recovery infrastructure. In each case, we review the service's configuration, identify security misconfiguration scenarios, and determine whether these exist on your infrastructure.

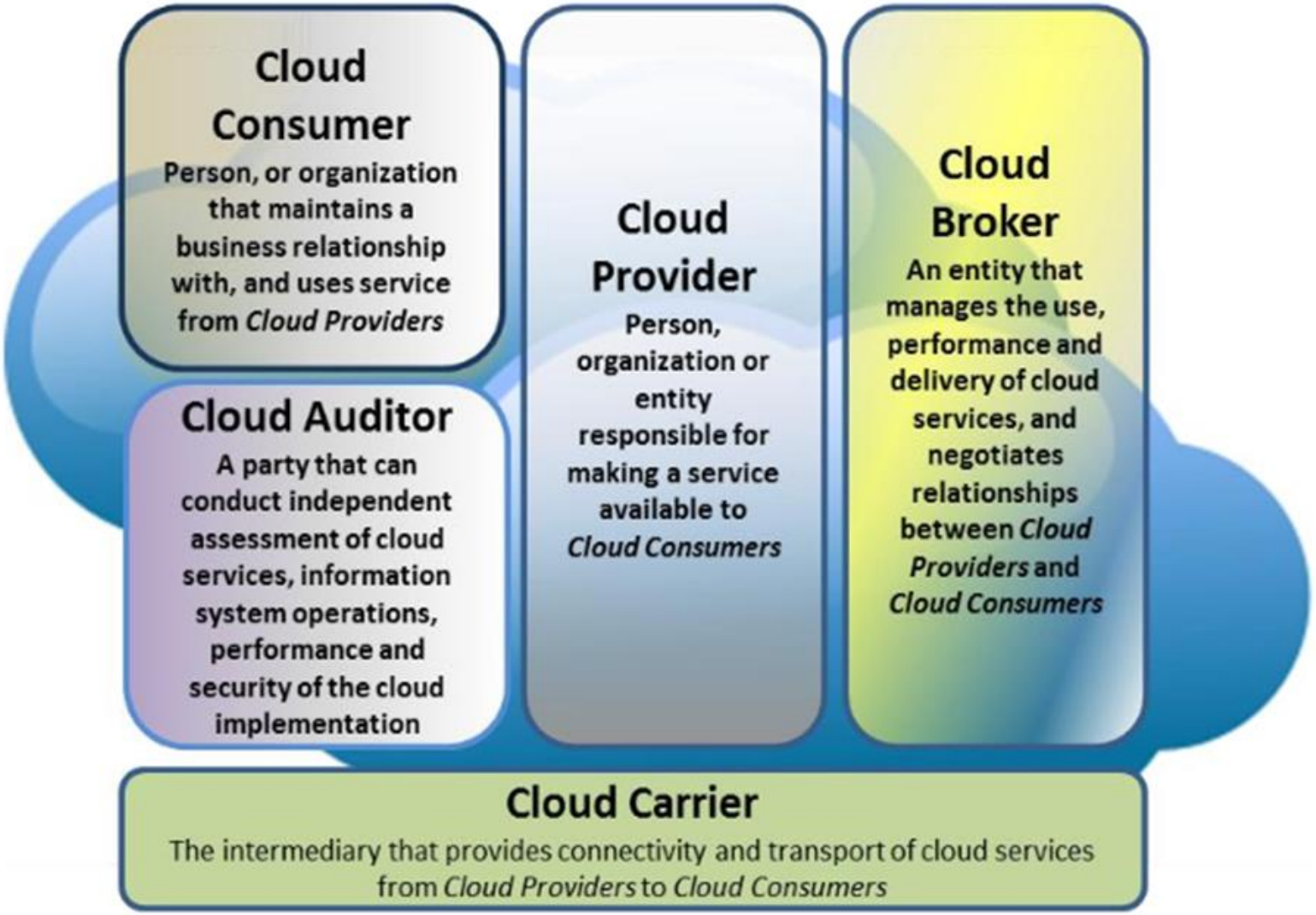
Scope

At the end of a configuration review, we deliver a summary of your implemented security controls, our opinion on the effectiveness of these controls, and remediation guidance detailing how to improve poorly implemented controls. We can provide a sample of a configuration review deliverable on request.

Compliance with NIST Framework

The NIST cloud computing definition is widely accepted and valuable in providing a clear understanding of cloud computing technologies and cloud services. A security framework like NIST, with its recommended set of security processes and controls, along with a risk assessment and management approach to match the appropriate set of controls to the business and threat environment, is an efficient way to meet these needs. Using an established framework can take the guesswork out of the process for smaller organizations while allowing larger and more mature security operations to justify their decisions and resource requests to management and auditors.

Five major actors defined in the NIST cloud computing reference architecture:



	Primary Product Categories		
NIST CSF Functions		Area of focus	Best Practice
Proactive	Identify	Configuration management	AppSec testing
		System management	Governance, risk, and compliance
		Vulnerability assessment	Penetration testing
		Awareness training	
	Protect	Access management	Encryption
		Data masking	Intrusion prevention systems
		DDOS filtering	Secure image/container
		Endpoint protection	Strong authentication
		Firewall	Firewall policy management
		Ops skills training	
Reactive	Detect	Intrusion detection system	Data analytics
		Network monitoring	Data loss prevention
		SIEM	
	Respond	Incident response services	Endpoint detect/respond
		Trouble ticket systems	Forensic analysis
	Recover	System/endpoint backup	High-avail/mirroring services

Compliance with NIST Framework

NIST Standard 800-145 defines 3 Cloud Service Areas:

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

According to the NIST Cloud Security Framework, the security baselining is equivalent to IaaS, PaaS and SaaS Service Models.

Accedere

Policies and Procedures

Policies and Procedures

Information security policies: An overall direction and support help establish appropriate security policies. The security policy is unique to your company, devised in the context of your changing business and security needs.

Asset management: This component covers organizational assets within and beyond the corporate IT network., which may involve the exchange of sensitive business information.

Human resource policy: Policies and controls pertaining to your personnel, activities, and human errors, including measures to reduce risk from insider threats and workforce training to reduce unintentional security lapses.

Policies and Procedures

Physical and environmental security: These guidelines cover security measures to protect physical IT hardware from damage, loss, or unauthorized access. While many organizations are taking advantage of digital transformation and maintaining sensitive information in secure cloud networks off-premise, the security of physical devices used to access that information must be considered.

Communications and operations management: Systems must be operated with respect and maintenance to security policies and controls. Daily IT operations, such as service provisioning and problem management, should follow IT security policies and ISMS controls.

Policies and Procedures

Access control: This policy domain deals with limiting access to authorized personnel and monitoring network traffic for anomalous behavior. Access permissions relate to both digital and physical mediums of technology. The roles and responsibilities of individuals should be well defined, with access to business information available only when necessary.

Information system acquisition, development, and maintenance: Security best practices should be maintained across the entire lifecycle of the IT system, including the phases of acquisition, development, and maintenance.

Policies and Procedures

Information security and incident management: Identify and resolve IT issues in ways that minimize the impact on end-users. In complex network infrastructure environments, advanced technology solutions may be required to identify insightful incident metrics and proactively to mitigate potential issues.

Business continuity management: Avoid interruptions to business processes whenever possible. Ideally, any disaster situation is followed immediately by recovery and procedures to minimize damage.

Policies and Procedures

Risk management: Identification, evaluation, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability or impact of unfortunate events or to maximize the realization of opportunities.

Change management: Guidelines to prepare, equip and support individuals to successfully adopt **change** in order to drive organizational success and outcomes.

Accedere

Mitigation Techniques for OWASP Top 10 Cloud Risks

Mitigation Techniques

As a part of the assessment, we provide guidelines and procedures for risk & threat mitigation. Following are the Mitigation techniques for the Top 10 OWASP cloud risks specified above:

1. Accountability and Data Ownership

Vendor risk management and accountability are the way to manage this issue. The Cloud vendor should have a set of security policies which you can map to your own, to ensure compatibility with your industry standards in data protection.
This should include the Cloud vendor's use of technologies like robust authentication, encryption, and disaster recovery policies.

Mitigation Techniques

2. User Identity Federation

Implement a modern identity service or platform to provide robust, persistent, verified identity controls. Use this as a basis for controlling access to resources using a privileged access model.

3. Regulatory Compliance

Use a Cloud vendor who understands and applies solutions for the various data protection laws. They should also know how to handle cross-jurisdiction data protection requirements.

4. Business Continuity and Resiliency

You need to make sure that your Service Level Agreements (SLAs) cover data resilience, protection, privacy, and that the vendor has a robust disaster recovery process in place.

Mitigation Techniques

5. User Privacy and Secondary Usage of Data

This can be a very difficult risk to mitigate. Security awareness training is one non-technical approach that can help to reduce the exposure of personal data. Compliance frameworks like GDPR would expect an organization to perform a Data Protection Impact Assessment (DPIA) which extends to their Cloud vendor. Other approaches such as 24/7 monitoring, encryption technologies, and multi-factor authentication can help augment privacy.

6. Service and Data Integration

Secure Sockets Layer and the more recent Transport Layer Security (SSL/TLS) should be fundamental protocols used by your Cloud vendor. These protocols, based on encryption, allow the safe movement of data across an Internet connection.

Mitigation Techniques

7. Multi-Tenancy and Physical Security

If you are in a multi-tenancy agreement there are some ways you can mitigate the risk of sharing your Cloud space with others. Starting with good design, your Cloud vendor can configure the server for logical separation. The system can also have an architecture built for isolation so that a quarantined virtual infrastructure is created for each tenant. Technologies like encryption also help to prevent data exposure.

8. Incident Analysis and Forensic Support

Check out your Cloud vendor policy on handling, evaluating and correlating event logs across jurisdictions. Do they have technologies in place, such as virtual machine imaging, to help in the forensic analysis of security incidents?

Mitigation Techniques

9. Infrastructure Security

Put in place various measures to improve general security. For example, privileged access management using robust authentication, secure configuration of server and services, and tiered architecture. A cloud cybersecurity assessment can also be helpful to understand your cloud cybersecurity posture, get strategic Cloud security recommendations and secure your critical assets before, during or after Cloud migration.

Mitigation Techniques

10. Non-Production Environment Exposure

In test environments, avoid using real or sensitive data. Ensure that individuals working on the pre-production system have privileged access to security measures in place. Make sure to leverage the concept of ‘privacy by design’ by implementing appropriate technical and organizational measures as well as effective data protection principles through the entire project lifecycle.

Accedere

Thank you.

We look forward to the opportunity of working with you.

Accedere

accedere.io