International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 06 | June - 2023 SJIF Rating: 8.176 ISSN: 2582-3930

Cloud Security Tools

Rutik Dattatray More
ASM Institute of Management & Computer Studies
Email : rutikmore4207@gmail.com

Abstract :

Cloud computing is one of the biggest developments passed off in the field of information generation during current years. This model has turn out to be greater proper for all institutions, organizations and additionally for private use thanks to the garage of 'valuable statistics' at low costs, access to such facts from everywhere inside the world as well as its ease of use and occasional cost. The goal of this research is to understand tools and the concept of tools that are used in cloud security.

Keywords :Cloud security, Security challenges , Cloud security tools , public cloud private cloud, hybrid cloud.

I. Introduction

Cloud computing helps organizations of all sizes operate at scale, decrease their capital overheads, and assist in managing IT infrastructure. Depending on your needs, there are several different types of cloud deployment you can consider. These are grouped together in three types:

1. Private Cloud

A private cloud is restricted for use within a specific organization. The infrastructure and resources aren't shared with other companies. Such types of cloud deployment are expensive to set up but offer more customization and security.

2. Public Cloud

A public cloud is managed by an external, third-party provider. Space on this cloud server is 'rented' out to organizations, but the external party is responsible for security, maintenance, and other forms of upkeep.

3. Hybrid Cloud

As the name suggests, hybrid cloud functions as a combination of both private and public ones. It's suited for organizations that want both rapid scalability coupled with top-tier encryption.

II. Cloud Security

Cloud security is the protection of data, applications, and infrastructures involved in cloud computing. Many components of security for cloud environments (whether it's a public, private, or hybrid cloud) are similar to for any on-premise IT architecture. High-level security concerns like unauthorized data publicity and leaks, weak access controls, susceptibility to attacks, and availability disruption have an effect on conventional IT and cloud structures alike. But moving to the cloud doesn't come without its own set of security challenges. Let's investigate why cloud security is important for all businesses.

III. Cloud Security Challenges

1. Guard Against Security Breaches

The cost of an average security breach for a company is a cool $3.8 million.This figure rises to $7.9 million for American companies with an average time of 196 days for the detection of the breach in the first place.Data security on the cloud is important because you're no longer in total control. If, for example, you choose to run your applications on either a public or hybrid cloud, you're effectively putting your trust in a third-party.This means you must stay on top of things and ensure that your cloud computing provider understands this responsibility. While it is certainly in the provider's best interest to ensure top-tier security for long-term business prospects, you must, as the client, also go the extra mile.

2. Manage Remote Work

One of the benefits of using cloud computing is the sheer accessibility of data. Your critical

applications can be accessed by employees from anywhere in the world. This results in flexible work arrangements and the possibility to hire staff from all around the globe.However, the downside to this arrangement is that employees might not adhere to cybersecurity best practices. If they're workingfrom coffee shops, for example, they're using public WiFi to access the web — this practice entails an inherent security risk. They might also use personal laptops and phones to carry out their tasks, which means they're more susceptible to malware and phishing attacks.New malware variants for mobile increased by 54 percent in 2017 according to Symantec's Internet Security Threat Report, so this is a real threat. If a malicious virus enters your system, it'll be hard to contain the damage.

3. Comply With Regulations :

Data protection standards like HIPAA and GDPR are rules that businesses must take seriously – otherwise, they will incur the wrath of regulators.These standards were put together to ensure the integrity and security of customer data. At the end of the day, if the customer data stored on the cloud is compromised, it's you who will have to answer to the regulator.You can't simply pass the blame on to a third-party vendor (your cloud computing provider in this case) and expect little to no retribution. Highly-regulated industries such as banking, finance, health, and insurance, legal already have exacting standards in place. The importance of cloud security multiplies in these sectors because of all the risks involved. Sure, a data breach will damage your business reputation and brand, but you'll also be held accountable by external parties.

4. Eliminate Weak Links and Build Access levels

40 percent of organizations using cloud storage accidentally leaked data to the public. This had compromised their business integrity and gave their competition a leg up.These leaks weren't a result of malicious intent; rather, they were a result of poor security best practices. One best practice of cloud security is enforcing access controls on employees by just limiting access to data only to those individuals who need it.This makes it much harder for hackers to infiltrate and prevents errors that lead to data leaks.

IV. Cloud Security Tools

It doesn't count what size you're while it comes to shielding your network. Big company, small company, startup: Hackers will nevertheless need your statistics and they'll still stealthily poke holes for your network anyplace they can.You need to get security measures in location and fast. That's why "safety as a service" agencies have become important for all trying to deploy security for everything from documents to your complete business. Security as a service may be loosely defined as a "software as a service" protection tool that doesn't require any on-premise hardware or software distribution.

V. Security Tools that are used on large basis

1. Okta :

One of the most crucial parts approximately securing your network is simply knowing who is inner of it. Okta focuses simply on identification management — knowing who's where and why. It knows each your employees for people accessing data at the backend, in addition to your forward-facing access-ers, which include clients and partners. It will help you manipulate logins throughout all of your applications as well, such as Google Apps, Salesforce, Workday, Box, SAP, Oracle, Office 365, and more. Furthermore, it may track all of those from any kind of device. Features encompass privilege providing from one dashboard, the ability to implement guidelines across devices, single sign-on options, and more.

2. Proof Point :

When we communicate about assault vectors — holes inside the network from where attacker can get in — e mail pops out as one of the weakest links. Proofpoint specially focuses on e mail, where cloud-only services tailored to both companies and small to medium sized businesses. Not only does it ensure none of the

bad stuff receives in, but it additionally protects any outgoing facts. Proofpoint further promises that while it stores data to prevent information loss, it does no longer have the keys to decrypt any of the information.To loss, it does not have the keys to decrypt any of the information.

3. Cipher Cloud :

CipherCloud is to secure all those other "as a service" merchandise you use, along with Chatter box, Office 365, Amazon Web Services,Gmail, and more. It guarantees to guard that prized company records you're just giving away to these services, in addition to your communications, and more. It does this through many of the manner we've already visible including encryption, visitors monitoring, anti-virus scans, and more. It additionally provides mobile safety support.

4. White-hat Security :

White Hat Security is centered on shielding your website from the floor up, including within the coding process. It presents its Sentinel product suite as a carrier to assist your guard your web sites with five kind of products.

These encompass a product that offers you contemporary threat facts so that you can avoid coding vulnerabilities into your internet site from the get go. Another facilitates you identify issues in pre-production before the internet site is ever launched, and its business enterprise product facilitates you test for main logic troubles as soon as you're live. The general Sentinel line will help your verify your Web apps for holes and will even act as a firewall that surely patches discovered problems. White Hat in addition takes gain of its studies arm so that you can offer you with updated statistics on threats observed out of doors your network.

5. Zscaler :

Zscaler calls its product the "Direct to Cloud Network," and like a lot of those products, boasts that it's tons easier to install and may be plenty more efficient than traditional appliance security. The company's products guard you from advanced persistent threats by monitoring all the traffic that comes inside and outside of your community as a kind of "checkpost in the cloud." But you don't need to clear out all that visitors in from one valuable point. You can Monitor specific, local networks as nicely given the ability of the cloud. Zscaler also protects iOS and Android gadgets within your company, that could then be monitored through its special mobile online dashboard.

6. Centrify :

Similar to Okta, Centrify additionally focuses on identification management across quite a number of gadgets and applications. The idea is to place all your users personnel and customers alike into one central area to be monitored and controlled via enforced agency policies. It will protect when a person signs into your Network be it via on-premise software program or cloud applications. It additionally has a product that works especially Samsung Knox the cellphone manufacturer's supposedly extra-protected mobile protection software program. This product provides devices running Knox with sign-on options and helps IT departments control these gadgets through Centrify.

Conclusion

In this Research I have given brief overview regarding Cloud security and tools. Providing the easiest way of overcoming the challenges faced by cloud security, In this paper the concept of security tools have divided into 4 Components : CloudComputing (Introduction) , Cloud Security , Cloud security Challenges , Cloud security tools. The present paper provides the basic knowledge of cloud security tool so that the reader can have better understanding about security tools .

Reference

[1] Cloud based Security Tools : Venture Beat.

[2] SaaS based Security Tools to protect network by Meghan Kelly.