Don’t only “**Secure Your Cloud, Save Your Money”** as well by following this guide.

May 2020

https://securityspoc.com

Know your Cloud Responsibilities

"Organizations using cloud services are responsible for confidentiality and integrity of their own data, even it is stored at cloud service provider's end."

Data outside of enterprise network adds a significant risk to the organization business. Legislations and regulators requires organizations to showcase regular compliance to applicable standards such as PCI-DSS, ISO 27001, GDPR and etc. A small Security breach may cost millions to the organizations as penalty for not being prudent.

"Typically the organization's data in Cloud is stored in multi-tenant environment where the resources are logically separated but coupled together to perform the required operations such as compute, store, and etc. to minimize the cost and provide scalability."

In next few slides we have documented some of the best practices for commonly used AWS resources to ensure cyber security of your Cloud deployment with saving a little money.

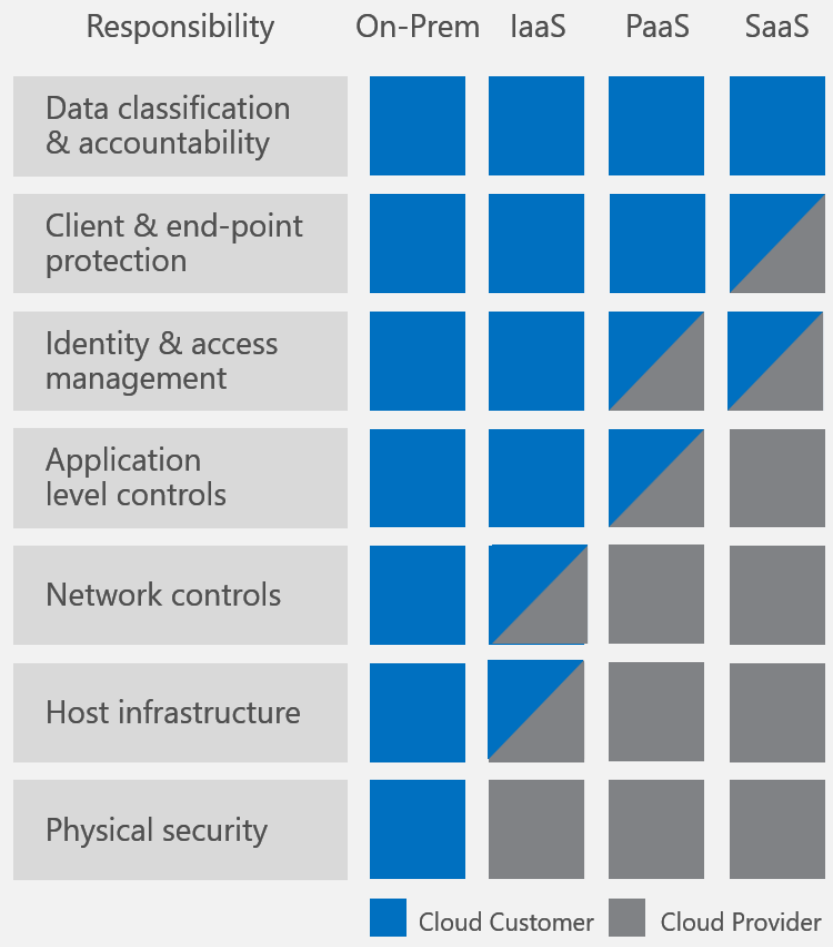

Image Courtesy of gallery.technet.microsoft.com

Start

IAM Security Practices

© Security Spoc Limited is registered in London, UK. All rights reserved.

Identity Access Management

79% of Companies Reported Identity-Related Breach in Past Two Years

The causes of identity-related breaches were:

- Phishing, as cited by 66% of respondents.
- Stolen credentials (32%) was another popular technique.
- Others included poorly managed privileges (28%),
- Brute-force attacks (24%), and socially engineered passwords (23%).

Source: Identity Defined Security Alliance Report

Identity Access Management Security Practices

1. Restrict usage of root user account

When you first create an AWS account, the initial user that get created is known as root user which is a privileged account having access to all AWS resources. Unrestricted or compromised root account may allow the unauthorized access

Solution:

a) Disable root access keys and enable MFA for root user account
b) Create a IAM user that has all admin privileges and use that to manage all the AWS resources

2. Create IAM Groups and Roles

Assigning permission using IAM polices at user level may introduce the privilege creep where user may get unnecessary permissions which defeats the least privilege principle.

Solution:

a) Don't assign the IAM or inline polices to the user
b) Assign the IAM or inline policies to defined group/role and add the user to the group/role. This prevents the risk of privilege creep
c) Follow the least privilege principle and allow only required permission to the role/group
d) Create IAM roles for custom applications requiring access to AWS resources

3. Regular review of IAM Credentials

Remember the Cloud Customer is responsible for all the data in cloud. A compromised credential may leave your data at risk of unauthorized access which may leads to implication of penalty from regulators and applicable standards.

Solution:

a) Regular review should be conducted for IAM polices and associated permissions at user/group/role level
b) Best practice is to disable the users and access keys which were not used from 90 days.

4. Monitor IAM activities

In absence of monitoring, an attacker who have successfully compromised an IAM credential may have unauthorized access to the AWS resources. Attacker may use the available resources to benefit their motives such as crypto mining, DDoS attack and etc.

Solution:

a) Use AWS CloudTrail for monitoring the users activity
b) Configure the CloudWatch and filters to raise an alarm for unusual activities such as changes are made to an IAM role, root account changes, deletion of files or logs etc.

Start

S3 Bucket Security Practices

© Security Spoc Limited is registered in London, UK. All rights reserved.

AWS S3 Buckets

Insecure S3 bucket exposed over 30,000 people PII data

An unsecured Amazon S3 bucket owned by cannabis retailer THSuite was found leaking the data of more than 30,000 individuals. THSuite provides business process management software services to cannabis dispensary owners and operators in the U.S.

Source: Trend Micro

S3 Bucket Security Practices

1. Secure access to S3 buckets

If not configured properly, S3 buckets may allow unauthorized access to the data impacting confidentiality and integrity.

Solution:

a) Allow access to the S3 buckets using IAM roles following least privilege access principle
b) Use S3 bucket polices for additional layer of security for critical data
c) Enable Multi-factor authentication (MFA) delete
d) Allow S3 bucket access to VPC using VPC Endpoint only

2. Encryption of S3 buckets

Storing data in S3 bucket without encryption may allow access to clear-text data stored in compromised S3 buckets. This may effect the credibility of an organization in complying to standards and regulations.

Solution:

a) Enable server side encryption which encrypts objects before storing them in S3 bucket and reduce the risk to data with key stored in separate mechanism
b) Encryption can be achieved by using AWS managed keys in SSE-S3, SSE-KMS and SSE-C mechanism
c) Using custom key store for storing keys incurs huge cost, but do provide an extra layer of security
d) Encrypt data in transit using aws:SecureTransport condition

3. Save money set lifecycle policy

Organizations having Cloud also requires to showcase the conformity to data retention requirement where they need to store the certain data for number of years as per regulations. This add significant cost to company for storing data in Cloud.

Solution:

a) Lifecycle policy secure your data and saves you money by moving your data to AWS Glacier
b) AWS Glacier provides cost effective solution for storing data for longer period of time. Later this data can also be deleted if not required by data retention policy

4. Monitor S3 buckets

In absence of monitoring controls the auditing cannot be performed to validate the user access and actions, intentional or unintentional damage to S3 objects.

Solution:

a) Enable AWS CloudTrail for monitoring the user activities performed on S3 objects
b) Integrate the CloudTrail with the CloudWatch and configure filters to raise an alarm for unusual activities such as deletion of objects, disabling encryption deletion of files or logs etc.
c) Use AWS Config to monitor compliance to best practices
d) Use Amazon Macie with Amazon S3 for identifying and tracking PII

IAM Security Practices

VPC Security Practices

© Security Spoc Limited is registered in London, UK. All rights reserved.

AWS Virtual Private Cloud

Attackers installed rootkits on cloud servers which granted them the remote control

AWS SGs provide a robust boundary firewall for EC2 instances. however, this firewall does not eliminate the need for network administrators to keep all external-facing services fully patched.

Source: Sophos

Virtual Private Cloud Security Practices

1. Proper Isolation of VPC environments

Isolated but loosely coupled VPC environments also pose risks in Cloud. This may allow an adversary to escalate the access to other VPC subnets and environments leading to compromise of data and asset.

Solution:

a) Ensure having separate subnet for DMZ, database and application server in VPC
b) Create distinct VPCs for production, staging and development environment
c) Never use the default VPC created by AWS

2. VPC Peering Saves you Money

Inter VPC access should not be allowed using gateway or internet, this may allow an attacker to access the data in transit. Using Transit Gateway puts huge cost at customers.

Solution:

a) Enable VPC peering to allow distinct VPCs to connect with each other using AWS private network. Small organization may utilize the many-to-many where individual VPCs connects to each other which maintains confidentiality
b) Using Transit Gateway in combination with VPC peering where large number of VPCs are required to connect with each other. This allows to save the hourly and connection cost relative to Transit Gateway where some of VPC are connected using VPC peering

3. Create Secure Networks & Save Money

Organizations that have large Cloud setup relies on using the technologies to secure data and underlying infrastructure. Designing secure network and saving cost becomes priority.

Solution:

a) Use Network ACLs and Security Groups in combination to provide layered security approach
b) Using centralized NAT gateway or EC2 instance equipped with IDS/IPS saves you money and provide protection in case of large number of VPCs require egress route
c) Use centralized VPC Endpoints to access AWS resources

4. Monitor VPC

In absence of monitoring controls the auditing cannot be performed to validate the inbound and outbound traffic, provisioning and modification of VPC components. Auditing enables organizations to showcase compliance to regulations.

Solution:

a) Enable CloudTrail to record all activities such as provisioning, configuring and modification of VPC components
b) Enable VPC Flow logs to record all data flowing in and out of VPC
c) Integrate the CloudTrail with the CloudWatch and configure filters to raise an alarm for unusual activities
d) Use AWS Config for identifying the changes to VPC resources

S3 Security Practices

What's more?

© Security Spoc Limited is registered in London, UK. All rights reserved.

Your “Single Point of Contact for Information Security “

Thank You !

“The world of business is becoming more uncertain, as with new system architectures come new cyber threats. No longer can the mechanisms deployed in the past be relied on for protection”

Nick Gaines, Group IS Director, Volkswagen UK

VPC Security Practices

https://securityspoc.com