AWS 공동 책임 모델

AWS는 사용자 환경의 일부를, 고객은 다른 부분을 책임짐

고객 : 클라우드 내부 보안

AWS 클라우드 내에서 생성하고 배치하는 모든 것의 보안을 책임짐

보안 요구사항 관리, 액세스 권한의 부여, 관리, 해지

AWS : 클라우드 자체의 보안

AWS는 클라우드 자체의 보안 책임짐

인프라의 모든 계층에서 구성 요소 운영, 관리 및 제어 (물리적 보안 포함)

물리적 인프라

- 데이터 센터의 물리적 보안
- 하드웨어 및 소프트웨어
- 인프라
- 네트워크 인프라
- 가상화 인프라

사용자 권한 및 액세스

IAM

- AWS 서비스와 리소스에 대한 액세스 안전하게 관리
- 보안 요구사항에 따른 유연성 제공
- IAM 사용자, 그룹 및 역할, IAM 정책, Multi-Factor Authentication

AWS 계정 루트 사용자

루트 사용자

- 모든 AWS 서비스 및 리소스에 대한 전체 액세스 권한 을 가짐
- 일상 작업에는 사용 X

IAM 사용자

- AWS 서비스 및 리소스와 상호작용하는 사람 또는 애플리케이션
- (이름 + 자격 증명) 구성
- 권한을 부여받아 사용

IAM 정책

- AWS 서비스 및 리소스에 대한 권한을 허용하거나 거부하는 문서

IAM 그룹

- IAM 사용자의 모음

IAM 역할

- `임시로 권한에 액세스` 하기 위해 수임하는 자격 증명
- 이전 역할에 대한 권한을 포기하고 새 역할에 지정된 권한을 수임

AWS Organizations

- `여러 계정을 통합하고 관리`
- 조직 생성 시 상위 컨테이너 루트 자동 생성
- `서비스 제어 정책(SCP)` → 중앙 제어 : `개별 멤버 계정`, `조직 단위` 적용

조직 단위

- 정책 적용 시 지정된 권한 자동 상속
- 특정 보안 요구 사항이 있는 워크로드 / 애플리케이션 간편하게 격리

AWS Artifact

- 보안 및 규정 준수 보고서 및 일부 온라인 계약에 대한 `온디맨드 액세스` 를 제공하는 서비스

1. AWS artifact Agreements

특정 유형의 정보를 사용하기 위해 AWS와 계약 체결

계정에 대한 계약 검토, 수락 및 관리 가능

2. AWS Artifact Reports

외부 감사 기관이 작성한 규정 준수 보고서 제공 (`ISO`)

최신 상태로 유지됨

고객 규정 준수 센터

- 감사자 학습 경로 포함
- 규제 대상 기업들이 어떻게 감사 과제를 해결했는지 확인 가능

서비스 거부 공격

- 서비스 거부 `DOS` 공격은 사용자들이 웹 사이트 / 애플리케이션을 이용할 수 없게 만드는 의도적인 시도
- 공격이 `단일 소스` 로부터 발생

분산 서비스 거부(DDOS) 공격

- `여러 소스` 로부터 공격

AWS Shield

AWS Sheild Standard

- 모든 AWS 고객 `자동 보호` 무료 서비스 (DDOS)
- `실시간` 으로 악성 트래픽을 탐지하고 완화

AWS Sheild Advanced

- 정교한 DDOS 공격 탐지 및 완화
- `CloudFront`, `Route 53` , `Elastic Load Balancing` 과도 통합됨
- 사용자 지정 규칙 작성 → WAF와 통합

추가 보안 서비스

AWS Key Management Service (AWS KMS)

- `저장 시` / `전송 중` 암호화
- 암호화 키를 사용하여 암호화 가능 (IAM에서 관리 가능)

AWS WAF

- 웹 애플리케이션으로 들어오는 네트워크 요청을 모니터링할 수 있는 `방화벽`
- `CloudFront`, `Application Load Balancer` 와 함께 작동
- `ACL` (액세스 제어 목록) 사용

Amazon Inspector

- `자동 보안 평가` 실행 → 애플리케이션 보안 및 규정 준수 개선
- EC2 인스턴스에 대한 오픈 액세스, 취약 SW 설치와 같은 `보안 취약성 검사`

Amazon GuardDuty

- AWS 인프라 및 리소스에 대한 `지능형 위협 탐지` 기능 제공
- 네트워크 및 계정 활동 모니터링 - 소스 데이터 지속적으로 분석