모듈 3: AWS 보안

주제

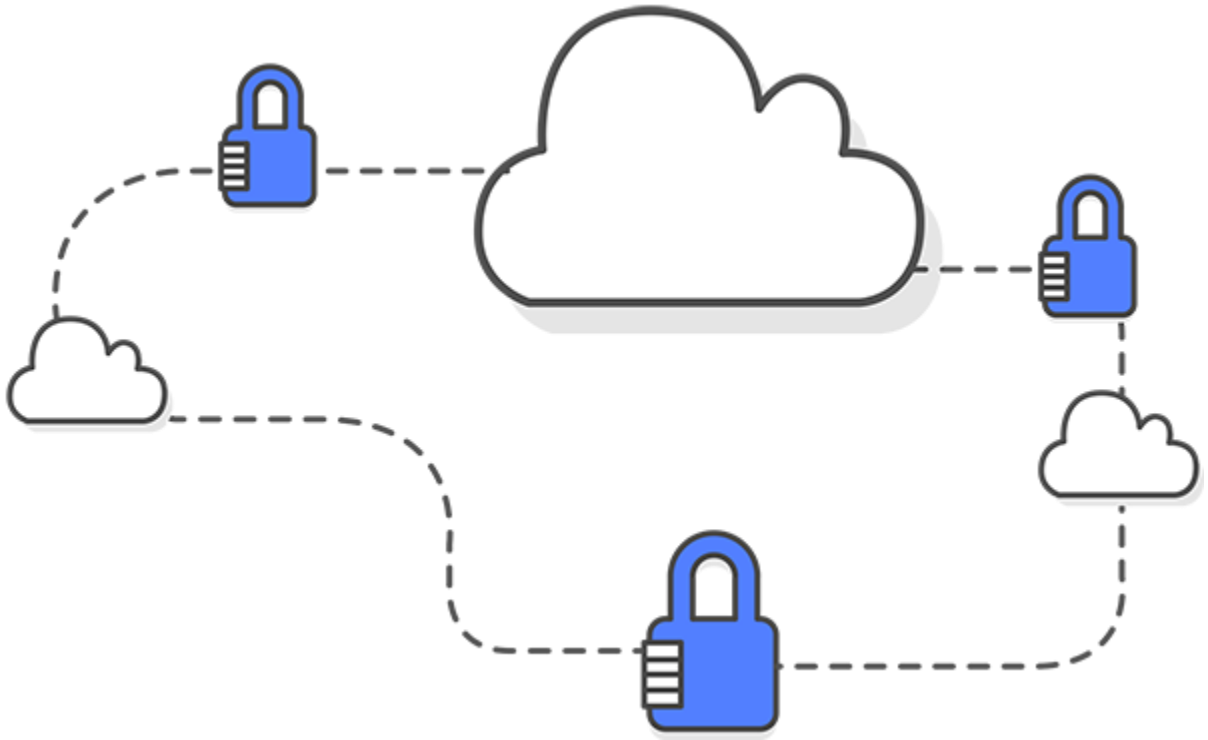
- AWS 보안 소개
- AWS 공동 책임 모델
- AWS 액세스 제어 및 관리
- AWS 보안 규정 준수 프로그램
- AWS 보안 리소스

AWS 보안 소개

AWS 보안 소개

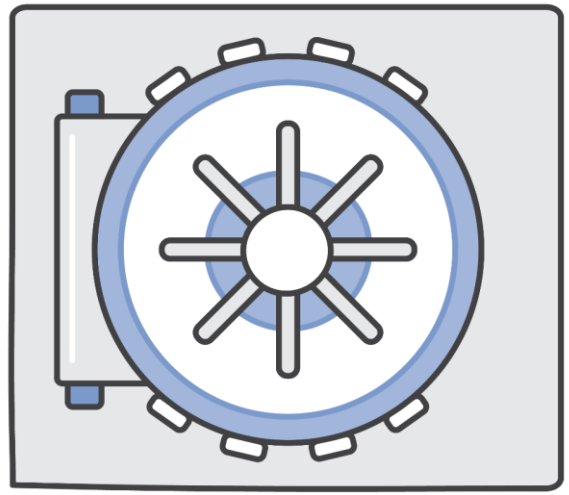
AWS에서는 가장 중요하게 생각하는 것이 보안입니다.

- 보안에 대한 접근 방식
- AWS 환경 제어
- AWS 제품 및 기능



데이터를 안전하게 유지

- 복원력을 갖춘 인프라
- 뛰어난 보안
- 강력한 보호



지속적 개선

- 빠른 혁신
- 끊임없이 진화하는 보안 서비스

필요한 만큼 지불

- 고급 보안 서비스
- 실시간으로 발생하는 위험을 처리
- 더 낮은 운영 비용으로 요구 사항을 충족

규정 준수 요구 사항 충족

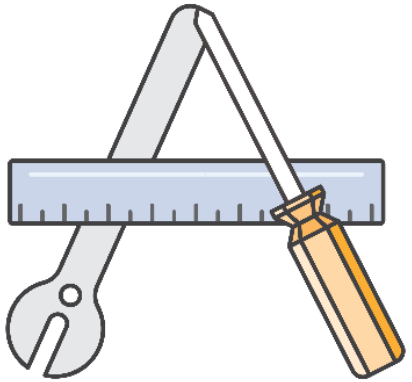
- 거버넌스 지원 기능
  - 추가적인 관리 기능
  - 보안 통제
  - 중앙 자동화

AWS 공동 책임 모델

- AWS 보안 제어 항목 상속
- 제어를 계층화

보안 제품 및 기능

- 도구
  - AWS 및 파트너에서 액세스
  - 모니터링 및 로깅 사용



네트워크 보안

- 내장 방화벽
- 전송 중 암호화
- 프라이빗/전용 연결
- DDoS 완화

인벤토리 및 구성 관리

- 배포 도구
- 인벤토리 및 구성 도구
- 템플릿 정의 및 관리 도구

데이터 암호화

- 암호화 기능
- 키 관리 옵션
  - AWS Key Management Service
- 하드웨어 기반 암호화 키 스토리지 옵션
  - AWS CloudHSM

액세스 제어 및 관리

- Identity and Access Management (IAM)
- Multi-factor authentication (MFA)
- 기업 디렉터리와 통합 및 연동
- Amazon Cognito
- AWS SSO

모니터링 및 로깅

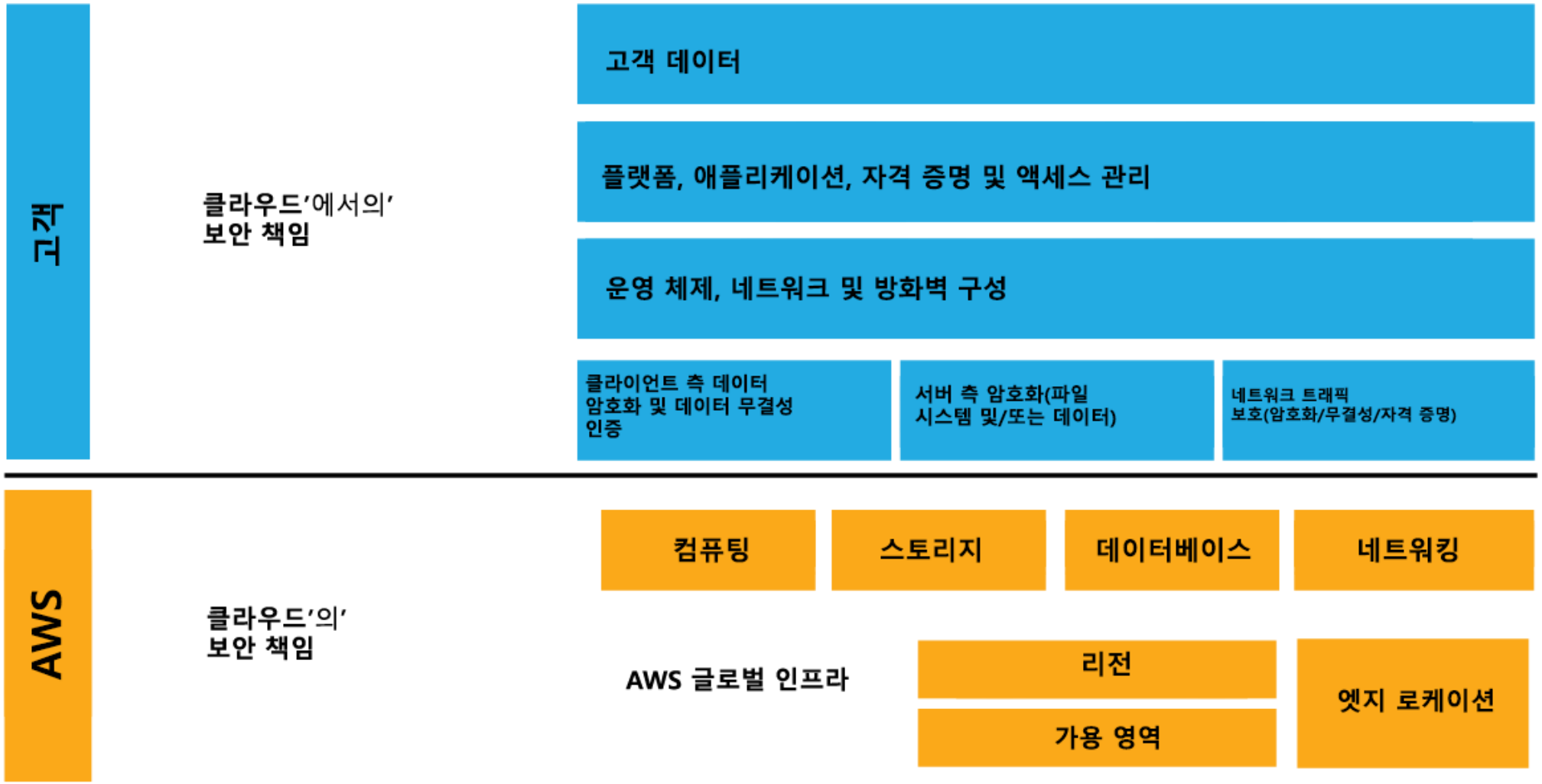
- 위험요소를 낮출 수 있는 도구 및 기능:
  - API 호출에 대한 심층적인 가시성
  - 로그 집계 및 옵션
  - 경고 알림

AWS Marketplace

- 공인 파트너가 AWS 고객에게 소프트웨어를 홍보/판매
- AWS에서 실행될 수 있는 온라인 소프트웨어 스토어

AWS 공동 책임 모델

클라우드의 보안



클라우드의 보안

- AWS 글로벌 인프라 보호가 최우선 과제
- 타사 보고서 제공

클라우드의 보안

AWS 기초 서비스

비관리형 서비스

- Amazon EC2
- Amazon EBS

관리형 서비스

- Amazon DynamoDB
- Amazon RDS
- Amazon Redshift
- Amazon EMR
- Amazon WorkSpaces

클라우드의 보안

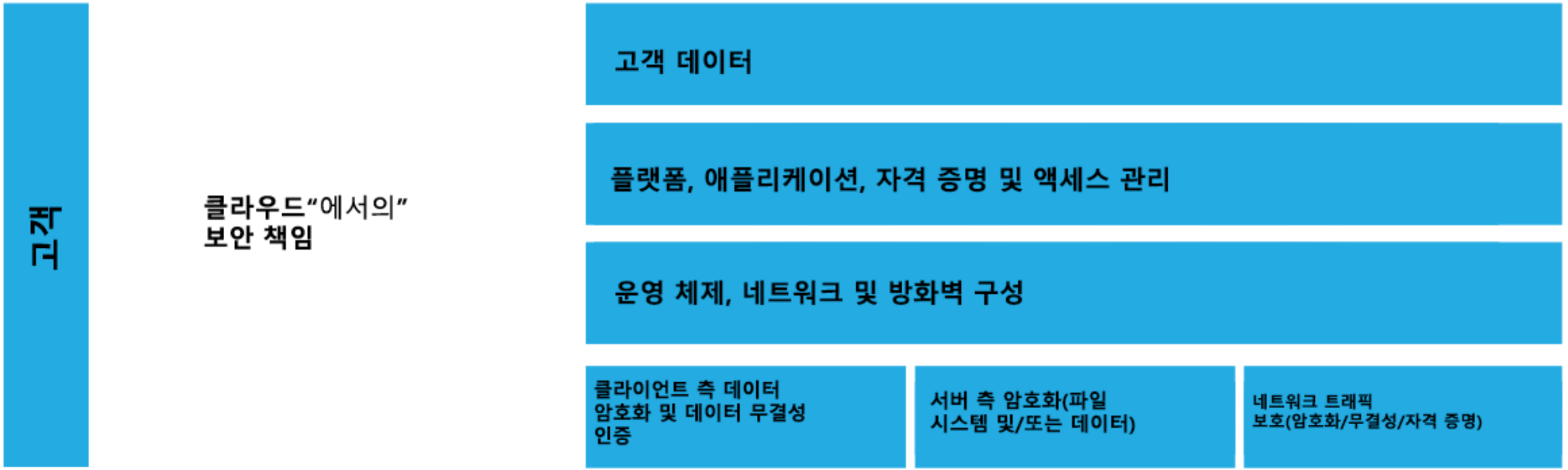
AWS 기초 서비스

비관리형 서비스
(EC2, EBS 등)

관리형 서비스

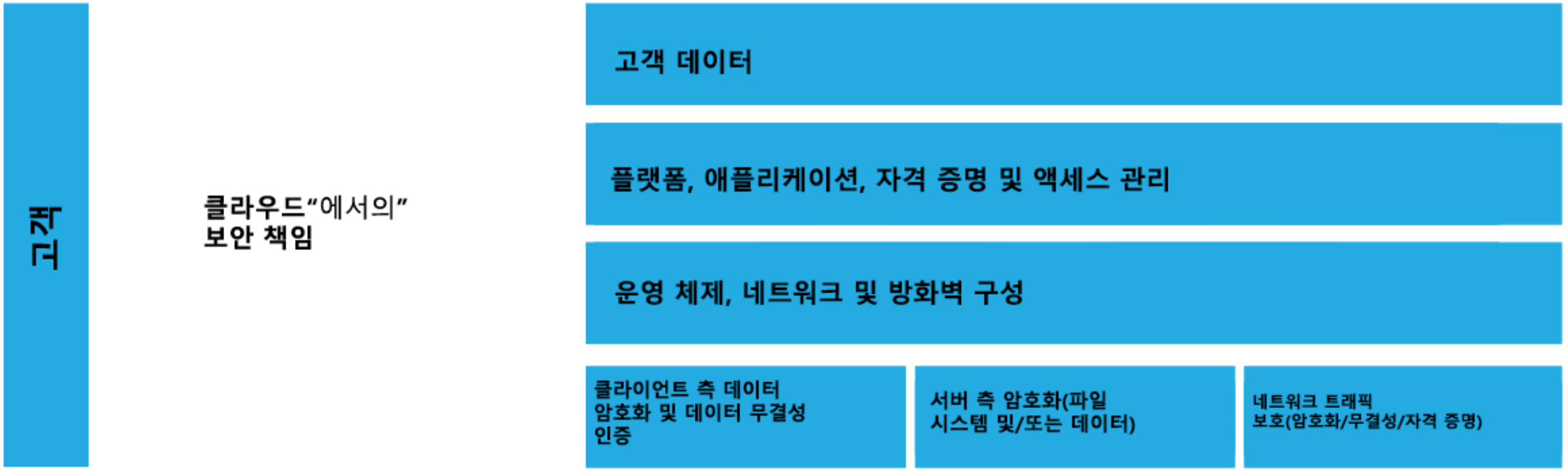
- 상속된 제어 항목
  - 물리적
  - 환경
- 공동 제어
  - 패치 관리
  - 구성 관리
  - 인식 및 교육
- 고객 특정
  - 서비스/통신 보호
  - 영역 보안

클라우드에서의 보안



- 무엇을 저장할지
- 어떤 AWS 서비스를
- 어느 위치에서
- 어떤 콘텐츠 형식 및 구조로
- 누구에게 액세스 권한이 있는지

클라우드에서의 보안



- 고객이 제어권 유지
- 서비스에 따라 모델이 달라짐

클라우드에서의 보안

AWS Service Catalog

- 가상 머신 이미지
- 서버
- 소프트웨어
- 데이터베이스

클라우드에서의 보안

이점

- 공통 IT 서비스를 중앙에서 관리
- 일관된 거버넌스 구현
- 규정 준수 요건 충족
- 승인된 IT 서비스를 신속하게 배포

예

고객 책임:

고객 책임:

- 게스트 OS
- 애플리케이션
- 보안 그룹

요약

- AWS와 고객은 보안 책임을 공유
  - **AWS**: 클라우드의 보안
  - **고객**: 클라우드에서의 보안
- 고객은 보안 조치에 대해 완전한 제어권 보유
- 고객은 AWS Service Catalog를 사용할 수 있음
- '인프라' 서비스

AWS 액세스 제어 및 관리

AWS IAM

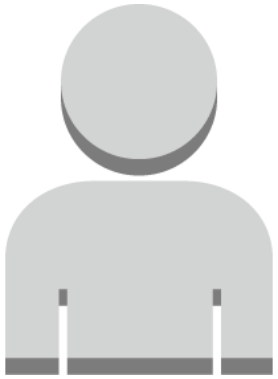
- AWS 리소스에 대한 액세스 제어
  - 인증
  - 권한 부여

클라우드 서비스에 대한 액세스

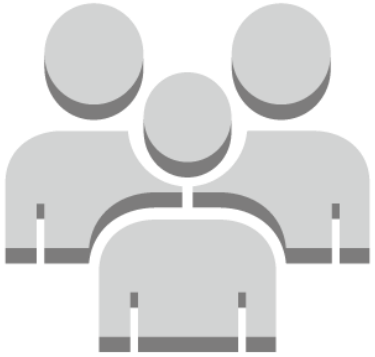
- 컴퓨팅
- 스토리지
- 데이터베이스
- 애플리케이션 서비스

AWS IAM

- 사용자와 그룹을 생성
- 권한과 역할을 부여



사용자



그룹

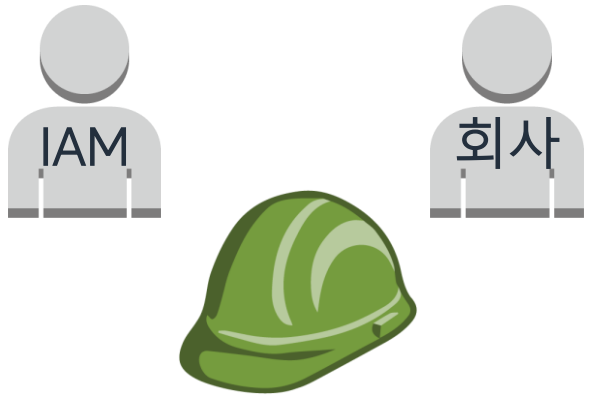
권한

역할

AWS IAM

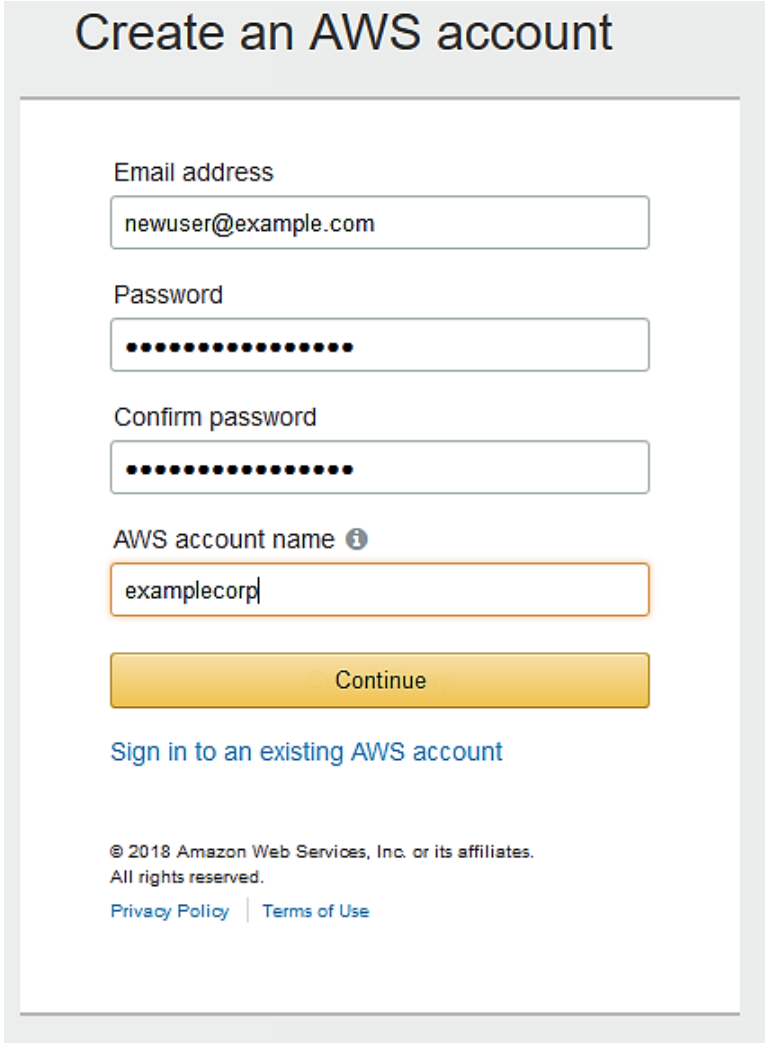
기능

- 사용자와 액세스 권한을 관리
- 역할과 그 권한을 관리
- 연동 사용자와 해당 권한을 관리



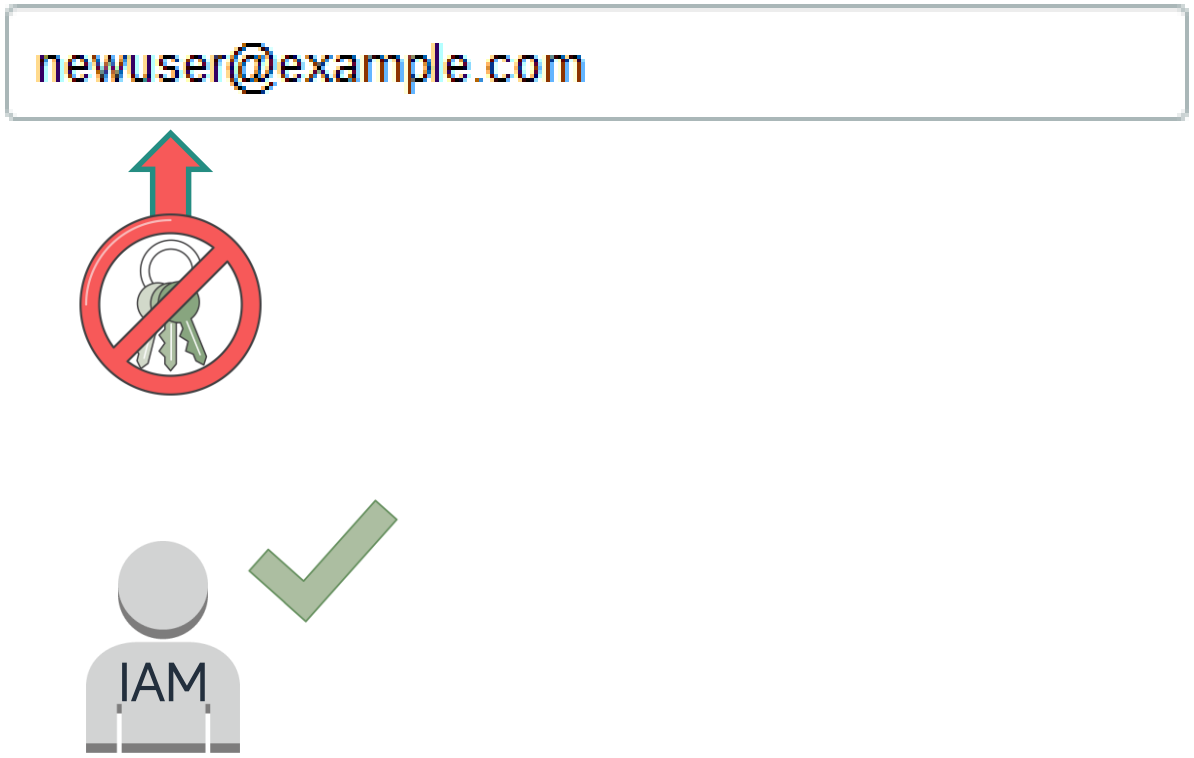
AWS 계정 루트 사용자

계정 루트 사용자는 모든 AWS 서비스에 대한 전체 액세스 권한이 있습니다.



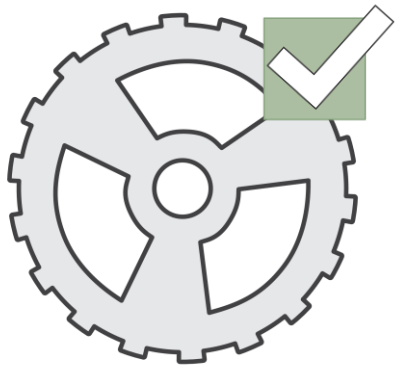
AWS 계정 루트 사용자

- 권장 사항
  1. 루트 사용자 액세스 키를 삭제합니다.
  2. IAM 사용자를 생성합니다.
  3. 관리자 액세스 권한을 부여합니다.
  4. IAM 자격 증명을 사용하여 AWS와 상호 작용합니다.



AWS IAM: 인증

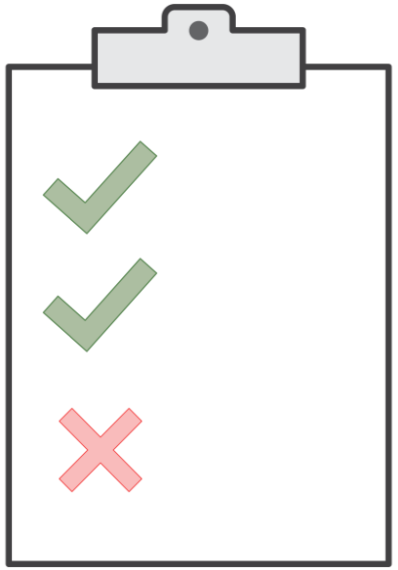
- 프로그래밍 방식 액세스
  - 액세스 키 ID 및 보안 액세스 키를 활성화



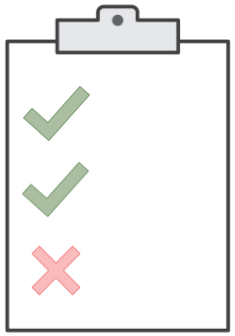
- 관리 콘솔 액세스
  - AWS 계정 이름과 암호 사용
  - MFA에서 코드를 입력하라는 메시지 표시

AWS IAM: 권한 부여

- AWS 서비스에 액세스
  - 권한 부여
- 권한 할당
  - AWS IAM 정책 생성



AWS IAM: 정책 지정



IAM 정책

IAM 사용자

IAM 그룹

IAM 역할

IAM 모범 사례

- AWS 루트 계정 액세스 키를 삭제
- Multi-Factor Authentication(MFA)을 활성화
- IAM 사용자에게 꼭 필요한 권한만 부여
- IAM 그룹을 사용
- IAM 암호 정책을 적용

IAM 모범 사례

- 역할
  - 애플리케이션에 대해 역할을 사용
  - 자격 증명을 공유하기보다는 역할을 사용
- 자격 증명
  - 자격 증명을 주기적으로 교체
  - 불필요한 사용자와 자격 증명을 제거
- 보안 강화를 위해 정책 조건 사용
- AWS 계정 내 활동을 모니터링

AWS 보안 규정 준수 프로그램

개요

- AWS 규정 준수 접근 방식
- AWS 위험 및 규정 준수 프로그램
- AWS 고객 규정 준수 책임

AWS 규정 준수 접근 방식

- AWS와 고객이 제어권을 공유
- AWS 책임
  - 매우 안전하고 제어된 플랫폼을 제공
  - 다양한 보안 기능을 제공
- 고객 책임
  - IT 구성

AWS 보안 정보

AWS는 다음을 통해 보안 정보를 공유

- 산업 인증 취득
- 보안 및 제어 사례를 게시
- NDA 체결 후 문서 직접 제공

보증 프로그램

AWS, 인증 기관 및 독립적 감사자가 다음을 제공

- 인증/증명
- 법률, 규정 및 개인 정보
- 준수/프레임워크

AWS 위험 및 규정 준수 프로그램

AWS 위험 및 규정 준수 프로그램

- AWS 제어 항목에 대한 정보 제공
- 고객이 자사의 프레임워크를 문서화하도록 지원

AWS 위험 및 규정 준수 프로그램

AWS 위험 및 규정 준수 프로그램의 구성 요소

- 위험 관리
- 제어 환경
- 정보 보안

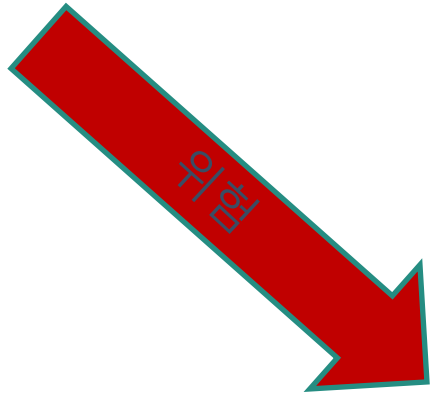
위험 관리

AWS 관리

- 비즈니스 플랜
  - 위험 관리 포함
  - 최소한 2년에 한 번 재평가
- 책임
  - 위험 식별
  - 적절한 조치 구현
  - 다양한 내부/외부 위험 평가

위험 관리

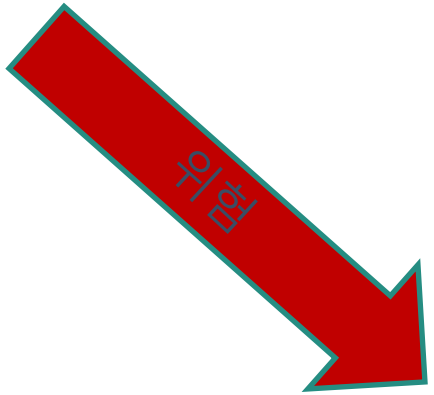
- 다음을 기반으로 하는 정보 보안 네트워크
  - COBIT(Control Objectives for Information and related Technology)
  - AICPA(미국 공인회계사 협회)
  - NIST(National Institute of Standards and Technology)



위험 관리

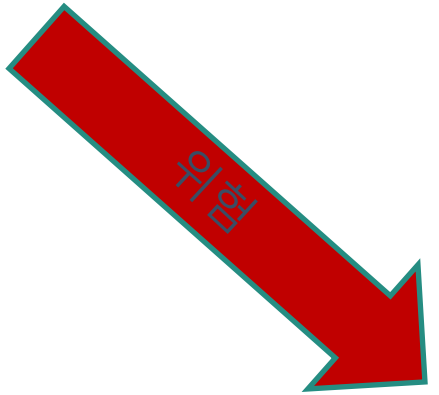
AWS

- 보안 정책 유지
- 직원에게 보안 교육 제공
- 애플리케이션 보안 검토 수행
  - 기밀성
  - 무결성
  - 데이터 가용성
  - 정보 보안 정책에 대한 일치성



위험 관리

- AWS 보안
  - 서비스 엔드포인트를 스캔하여 취약성을 확인
  - 취약성을 개선하기 위해 알림
- 독립적인 보안 회사
  - 스캔이 고객 스캔을 대체하지는 않음
  - 고객은 클라우드 인프라를 스캔하도록 요청할 수 있음



제어 환경

- 정책, 프로세스, 제어 활동을 포함
- AWS 서비스 제품을 안전하게 제공
- AWS의 제어 프레임워크를 효과적으로 운영하도록 지원
- 제어 항목을 통합
- 주요 사례를 확보하기 위해 모니터링

정보 보안

- 다음을 보호하도록 설계됨
  - 기밀성
  - 무결성
  - 가용성
- 보안 백서 발행

고객 규정 준수

고객 요구 사항

- 전체 IT 제어 환경에 대한 거버넌스 유지 관리
- 이해 항목
  - 필요한 규정 준수 목표
  - 위험 허용 범위에 따른 검증
- 제어 환경 구성
- 제어 환경의 효율성 확인
- 고객 규정 준수 기본 접근 방식

요약

AWS 보안 규정 준수 프로그램

- AWS 고객은 보안 및 데이터 보호를 유지하기 위한 제어 환경을 이해할 수 있습니다.
- 규정 준수 책임 공유

AWS 보안 리소스

AWS 보안 리소스

- AWS는 다음을 통해 보안 및 제어 환경을 알립니다.
  - 인증 및 증명
  - 백서 및 웹 콘텐츠
  - NDA 체결 후 문서 제공

AWS Trusted Advisor

- '맞춤형 클라우드 전문가'입니다.
- 모범 사례를 준수하는 데 도움이 됩니다.
- AWS 환경을 검사합니다.
- 보안 결함을 제거하는 데 도움이 됩니다.
- 다음을 위한 기회와 모범 사례를 찾습니다.
  - 비용 최적화
  - 성능
  - 보안
  - 내결함성
  - 서비스 한도

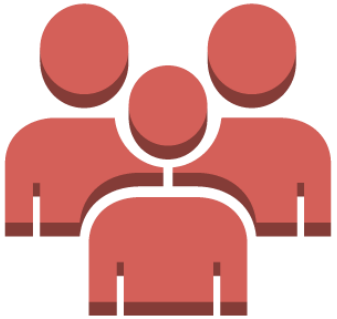
AWS 계정 팀

- 1차 담당자
- 배포를 안내
- 보안 문제를 해결할 수 있는 적절한 리소스 안내

AWS Enterprise Support*

- 15분 내 응답
- 전화, 채팅 또는 이메일로 연중무휴 24시간
- 전담 기술 지원 담당자

*자세한 내용은 다음 참조:
https://aws.amazon.com/premiumsupport/enterprise-support/



AWS Professional Services 및 AWS 파트너 네트워크

- APN에는 전 세계에 분포된 수백 명의 공인 AWS 컨설팅 파트너가 있습니다.
  - 보안 정책을 개발하도록 지원
  - 규정 준수 요구 사항을 충족하도록 지원

AWS 공고 및 게시판

- 현재 취약성 및 위협에 대한 공고/게시판
- 고객은 전문가와 협력하여 다음을 해결합니다.
  - 침해 사례 신고
  - 취약성
  - 침투 테스트

AWS 감사자 학습 과정

- 내부 작업이 어떻게 AWS에서 규정을 준수하는지 이해
- 규정 준수 웹 사이트 방문:
  - 추천 교육
  - 자습형 실습
  - 감사 리소스

AWS 규정 준수 솔루션 안내서

- 공동 책임 모델 이해
- 규정 준수 보고서 요청
- 보안 질문서 작성
- 범위 내 서비스
- AWS 보안 블로그
- 사례 연구
- FAQ

*자세한 내용은 다음 참조:
https://aws.amazon.com/compliance/resources/

지식 확인

- AWS Trusted Advisor란 무엇입니까?
  - 애플리케이션 배포를 확인하는 데 도움이 되는 파트너 프로그램
  - 클라우드로 마이그레이션하는 데 도움이 되는 Professional Services 제품
  - 모범 사례를 따르도록 리소스를 구성하는 데 도움이 되는 온라인 도구
  - 계정에 대한 액세스를 관리하는 데 도움이 되는 AWS 서비스

지식 확인

- IAM 정책을 생성할 때 사용자에게 부여할 수 있는 두 가지 유형의 액세스는 다음 중 무엇입니까? (2가지 선택)
  - 기관 액세스
  - 권한이 부여된 액세스
  - 프로그래밍 방식 액세스
  - AWS Management Console 액세스
  - 관리 루트 액세스

지식 확인

- 다음 중 AWS Identity and Access Management(IAM)의 기능이 아닌 것은 무엇입니까?
  - 연동 사용자와 권한을 관리
  - 서비스와 그 용량을 관리
  - 역할과 그 권한을 관리
  - 사용자와 그 액세스 권한을 관리

지식 확인

- 다음 중 AWS가 클라우드에서 데이터를 보호하기 위한 지침으로 고객에게 제공하는 리소스는 무엇입니까? (2가지 선택)
  - AWS Trusted Advisor
  - AWS 보안 학습 과정
  - 고객 추천사
  - 공인 파트너 솔루션
  - AWS Enterprise Support

지식 확인

- 다음 중 AWS가 제공하는 몇 가지 보안 이점은 무엇입니까? (2가지 선택)
  - 안전한 글로벌 인프라
  - 인벤토리 및 애플리케이션 관리
  - 공동 협업 모델
  - 데이터 스토리지
  - 규정 준수 요구 사항 충족

지식 확인

- 다음 중 AWS 위험 및 규정 준수 프로그램을 구성하는 요소는 무엇입니까? (3가지 선택)
  - 제어 환경
  - 위험 관리
  - 물리적 보안
  - 자격 증명 관리
  - 정보 보안
  - 보안 원칙
  - 자동화 환경

지식 확인

- 공동 책임 모델에서 '클라우드에서의 보안'의 예는 다음 중 무엇입니까? (2가지 선택)
  - 컴퓨팅 보안 표준 및 규정 준수
  - 서비스가 운영되는 시설의 물리적 보안
  - 콘텐츠가 저장되는 국가
  - 콘텐츠와 함께 사용되는 AWS 서비스
  - 글로벌 인프라 보호

지식 확인

- 최초 로그인 후 AWS 계정 루트 사용자를 위한 모범 사례로 AWS가 권장하는 것은 다음 중 무엇입니까?
  - 루트 사용자 계정을 삭제
  - 루트 사용자 계정에 대한 모든 권한을 취소
  - 루트 사용자 계정에 대한 권한을 제한
  - 루트 사용자 액세스 키를 삭제

지식 확인

- 다음 중 AWS 보증 프로그램에 포함되는 것은 무엇입니까? (2가지 선택)
  - 업계 모범 사례
  - 고객 추천사
  - 법률, 규정 및 개인 정보
  - 파트너 검증
  - 인증/증명

지식 확인

- 공동 책임 모델에서 AWS가 책임을 지는 클라우드 보안 측면은 다음 중 무엇입니까?
  - 클라우드의 보안
  - 클라우드에 대한 보안
  - 클라우드를 위한 보안
  - 클라우드에서의 보안