AWS 백서

AWS 보안 소개

AWS 보안 소개: AWS 백서

Table of Contents

AWS 보안 소개

게시 날짜: 2021년 11월 11일(문서 개정)

요약

Amazon Web Services(AWS)는 높은 가용성과 신뢰성을 고려하여 설계된 확장 가능한 클라우드 컴퓨팅 플랫폼과 다양한 애플리케이션을 실행할 수 있는 도구를 제공합니다. 고객의 시스템과 데이터의 기밀성, 무결성 및 가용성을 보호하는 것은 고객의 신뢰와 신용을 지키는 것과 마찬가지로 AWS에게 매우 중요합니다. 이 문서는 보안에 대한 AWS의 접근 방식을 소개하기 위해 작성되었습니다. 또한, AWS 환경에서의 보안 제어 기능 및 고객의 보안 목표를 달성하기 위해 AWS가 제공하는 제품 및 기능도 일부 소개합니다.

AWS 인프라의 보안

AWS 인프라는 현존하는 가장 유연하고 안전한 클라우드 컴퓨팅 환경 중 하나입니다. 애플리케이션 및 데이터를 빠르고 안전하게 배포할 수 있도록 확장성과 안정성이 뛰어난 플랫폼으로 설계되었습니다.

이 인프라는 보안 모범 사례 및 표준뿐만 아니라 클라우드 고유의 요구 사항을 고려하여 구축 및 관리됩니다. AWS는 중복 및 계층화 제어, 지속적인 검증 및 테스트, 상당한 부분의 자동화를 통해 기본 인프라를 상시 모니터링하고 보호합니다. 또한 이러한 제어 기능이 모든 신규 데이터 센터 또는 서비스에 복제되도록 보장합니다.

보안에 가장 민감한 고객의 요구 사항을 충족할 수 있도록 데이터 센터와 네트워크 아키텍처가 구축되었으므로, 모든 AWS 고객이 이러한 이점을 활용할 수 있습니다. 즉, 기존 데이터 센터에 대한 비용 투자 및 운영 오버헤드 없이도 높은 보안성을 지닌 탄력적인 인프라를 확보할 수 있게 됩니다.

AWS는 공유 보안 책임 모델에 따라 운영됩니다. AWS는 기본 클라우드 인프라의 보안을 담당하며, 사용자는 AWS에 배포하는 워크로드의 보안을 담당합니다(그림 1). 이를 통해 AWS 환경에서 고객의 비즈니스 부문에 가장 적합한 보안 제어 기능을 구현하는 데 필요한 유연성과 민첩성을 확보할 수 있습니다. 민감한 데이터를 처리하는 환경에 대한 액세스는 엄격하게 제한하고, 공개하려는 정보에 대해서는 약간 완화된 제어 기능을 적용할 수 있습니다.

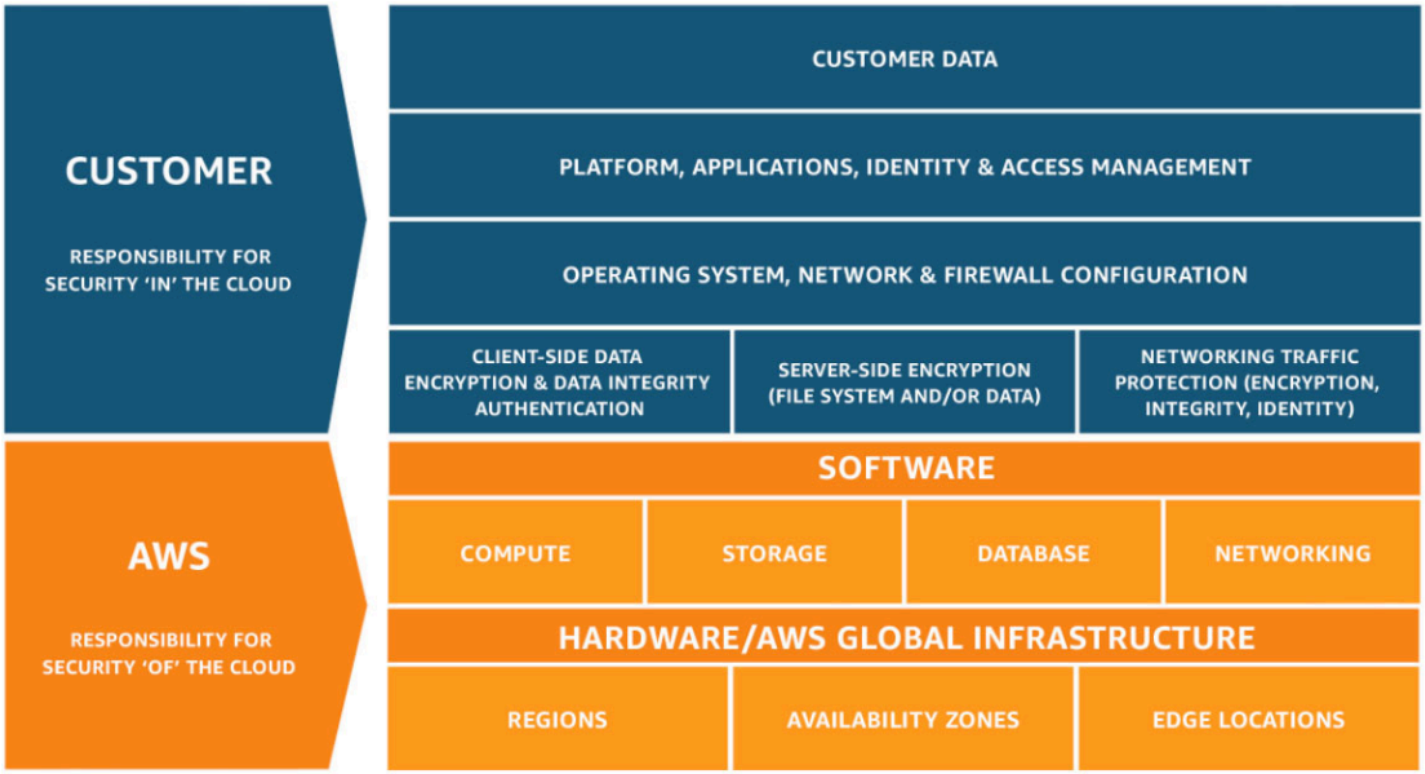

그림 1: AWS 공동 보안 책임 모델

보안 제품 및 기능

AWS와 그 파트너는 고객의 보안 목표를 충족하는 데 도움이 되는 다양한 도구와 기능을 제공합니다. 이러한 도구는 온프레미스 환경에 배포하는 제어 기능과 유사하게 작동합니다. AWS는 네트워크 보안, 구성 관리, 액세스 제어 및 데이터 보안 전반에 걸쳐 보안 전용 도구 및 기능을 제공합니다. 또한 고객의 환경에서 발생하는 상황을 완벽하게 파악할 수 있도록 모니터링 및 로깅 도구도 제공합니다.

주제

인프라 보안

AWS는 개인 정보 보호를 강화하고 네트워크 액세스를 제어하기 위해 다음과 같이 몇 가지 보안 기능과 서비스를 제공합니다.

- Amazon VPC에 내장된 네트워크 방화벽을 사용하여 프라이빗 네트워크를 생성. 인스턴스 또는 애플리케이션에 대한 액세스 제어. 고객이 AWS 서비스 전반에서 TLS를 사용하여 전송 중 암호화를 제어할 수 있습니다.
- 사무실 또는 온프레미스 환경에서 프라이빗 또는 전용 연결을 지원하는 연결 옵션
- 계층 3 또는 4와 계층 7에 적용되는 DDoS 방어 기술. 이러한 기능은 애플리케이션 및 콘텐츠 전송 전략의 일환으로 적용할 수 있습니다.
- AWS 보안 시설 간 AWS 글로벌 및 지역 네트워크의 모든 트래픽 자동 암호화

인벤토리 및 구성 관리

AWS는 클라우드 리소스가 조직 표준 및 모범 사례를 준수하도록 보장하면서 신속하게 마이그레이션할 수 있는 다양한 도구를 다음과 같이 제공합니다.

- 조직 표준에 따라 AWS 리소스의 생성 및 폐기를 관리하는 배포 도구

- AWS 리소스를 식별하고 지속적으로 해당 리소스의 변경 사항을 추적하고 관리하는 인벤토리 및 구성 관리 도구
- EC2 인스턴스용으로 사전 구성되고 강화된 표준 가상 머신을 생성하기 위한 템플릿 정의 및 관리 도구

데이터 암호화

AWS는 클라우드의 저장된 데이터에 보안 계층을 추가하여 확장 가능하고 효율적인 암호화 기능을 다음과 같이 제공합니다.

- Amazon EBS, Amazon S3, Amazon RDS, Amazon Redshift, Amazon ElastiCache, AWS Lambda 및 Amazon SageMaker와 같은 대부분의 AWS 서비스에서 사용 가능한 저장 시 데이터 암호화 기능
- AWS가 암호화 키를 관리하도록 할 것인지 아니면 자체 키를 완벽하게 제어할 수 있도록 할 것인지 선택할 수 있는 AWS Key Management Service 등의 유연한 키 관리 옵션
- AWS CloudHSM을 사용하여 규정 준수 요건을 충족하도록 지원하는 전용 하드웨어 기반 암호화 키 스토리지
- Amazon SQS용 서버 측 암호화(SSE)를 사용하여 중요한 데이터를 전송하기 위한 암호화된 메시지 대기열

또한 AWS는 AWS 환경에서 개발하거나 배포하는 서비스와 암호화 및 데이터 보호를 통합할 수 있는 API를 제공합니다.

자격 증명 및 액세스 제어

AWS는 AWS 서비스 전반에서 사용자 액세스 정책을 정의, 시행 및 관리하는 기능을 다음과 같이 제공합니다.

- AWS Identity and Access Management(IAM)를 사용하면 소프트웨어 및 하드웨어 기반 인증자에 대한 옵션을 포함하여 권한 있는 계정에 대한 AWS 리소스 AWS Multi-Factor Authentication을 통해 개별 사용자 계정을 정의할 수 있습니다. IAM을 사용하면 Microsoft Active Directory 또는 기타 파트너의 제품 및 서비스와 같은 기존 자격 증명 시스템을 사용하여 직원 및 애플리케이션에 AWS Management Console 및 AWS 서비스 API에 대한 연동 액세스 권한을 부여할 수 있습니다.
- AWS Directory Service를 사용하면 기업 디렉터리와 통합 및 연동하여 관리 오버헤드를 줄이고 최종 사용자 환경을 개선할 수 있습니다.

- AWS Single Sign-On(SSO)을 사용하면 AWS Organizations의 모든 계정에 대한 SSO 액세스 및 사용자 권한을 중앙에서 관리할 수 있습니다.

AWS는 대부분의 서비스에 기본 자격 증명 및 액세스 관리 연동을 제공하며, API를 자체 애플리케이션 또는 서비스와 연동합니다.

모니터링 및 로깅

AWS는 AWS 환경에서 발생하는 상황을 확인할 수 있는 도구와 기능을 다음과 같이 제공합니다.

- AWS CloudTrail에서는 AWS Management Console, AWS SDK, 명령줄 도구 및 상위 수준의 AWS 서비스를 통해 수행된 API 호출 등 계정의 AWS API 호출 이력을 확보하여 클라우드에서 AWS 배포를 모니터링할 수 있습니다. 또한, CloudTrail을 지원하는 서비스에 대해 AWS API를 호출한 사용자 및 계정, 호출을 수행한 소스 IP 주소, 호출이 발생한 시점을 파악할 수 있습니다.
- Amazon CloudWatch는 몇 분 이내에 사용할 수 있는 안정적이고 확장 가능하며 유연한 모니터링 솔루션을 제공합니다. 더 이상 자체 모니터링 시스템과 인프라를 설정, 관리, 확장할 필요가 없습니다.
- Amazon GuardDuty는 악성 활동 및 무단 행위를 지속적으로 모니터링하여 AWS 계정 및 워크로드를 보호하는 위협 탐지 서비스입니다. 이 서비스는 자동 응답을 트리거하거나 사용자에게 알릴 수 있도록 Amazon CloudWatch를 통해 알림을 표시합니다.

이러한 도구와 기능은 비즈니스에 영향을 주기 전에 문제를 발견하고, 보안 태세를 개선하고 사용자 환경의 위험 프로필을 줄이는 데 필요한 가시성을 제공합니다.

AWS Marketplace의 보안 제품

프로덕션 워크로드를 AWS로 이전하면 조직은 보안 환경을 유지하면서 민첩성, 확장성 및 혁신을 개선하고 비용을 절감할 수 있습니다. AWS Marketplace는 고객 온프레미스 환경의 기존 제어 솔루션과 동등한 수준 또는 동일하거나 해당 솔루션과 연동되는 업계 최고 수준의 보안 제품을 제공합니다. 이러한 제품은 기존 AWS 서비스를 보완하여 클라우드 및 온프레미스 환경에 포괄적인 보안 아키텍처와 보다 원활한 환경을 배포할 수 있도록 해줍니다.

보안 가이드

AWS는 AWS 및 파트너가 제공하는 온라인 도구, 리소스, 지원 및 전문 서비스를 통해 고객에게 전문 지식과 가이드를 제공합니다.

AWS Trusted Advisor는 맞춤형 클라우드 전문가 역할을 하는 온라인 도구로, 모범 사례에 따라 리소스를 구성할 수 있도록 지원합니다. 또한 AWS 환경을 검사하여 보안 격차를 해소하고, 비용을 절감하고 시스템 성능을 개선하며 안정성을 높일 수 있는 기회를 찾습니다.

AWS 고객 지원 팀은 배포 및 구현 과정을 안내하고, 발생할 수 있는 보안 문제를 해결하는 데 적합한 리소스를 제공하는 1차 담당자 역할을 합니다.

AWS 엔터프라이즈 지원은 15분 간의 응답 시간을 제공하며 전담 기술 지원 관리자와의 전화, 채팅 또는 이메일을 통해 연중무휴 24시간 이용할 수 있습니다. 이 컨시어지 서비스는 고객의 문제를 최대한 신속하게 해결할 수 있도록 보장합니다.

AWS 파트너 네트워크는 고객 온프레미스 환경의 기존 제어 솔루션과 동등한 수준 또는 동일하거나 해당 솔루션과 연동된 업계 최고 수준의 수백 가지 제품을 제공합니다. 이러한 제품은 기존 AWS 서비스를 보완하여 클라우드 및 온프레미스 환경에 포괄적인 보안 아키텍처와 보다 원활한 환경을 배포할 수 있도록 하며, 전 세계 수백 개의 인증된 AWS 컨설팅 파트너를 통해 보안 및 규정 준수 요구 사항을 해결하도록 지원합니다.

AWS Professional Services는 가장 중요한 워크로드를 AWS 클라우드로 마이그레이션할 때 자신감을 높이고 기술 역량을 개발할 수 있도록 지원하는 보안, 위험 및 규정 준수 전문 사례를 보유하고 있습니다. AWS Professional Services를 통해 고객은 검증된 설계를 기반으로 보안 정책 및 실무 사례를 개발하고, 고객의 보안 설계가 내부 및 외부 규정 준수 요구 사항을 충족하도록 할 수 있습니다.

AWS Marketplace는 독립 소프트웨어 공급자가 제공하는 수천 개의 소프트웨어 목록이 있는 디지털 카탈로그로, AWS에서 실행되는 소프트웨어를 간편하게 찾고 테스트하고 구매하고 배포할 수 있습니다. AWS Marketplace 보안 제품은 기존 AWS 서비스를 보완하여 클라우드 및 온프레미스 환경에 포괄적인 보안 아키텍처와 보다 원활한 환경을 배포할 수 있도록 해줍니다.

AWS 보안 공지는 현재 취약성 및 위협에 대한 보안 공지를 제공하며, 고객이 AWS 보안 전문가와 협력하여 부정 사용 보고, 취약성 및 침투 테스트 등의 문제를 해결할 수 있도록 지원합니다. 또한 취약성 보고를 위한 온라인 리소스도 있습니다.

AWS 보안 설명서에는 보안 및 규정 준수 목표를 충족하도록 AWS 서비스를 구성하는 방법이 나와 있습니다. AWS 고객은 보안에 가장 민감한 조직의 요구 사항에 부합하도록 구축된 데이터 센터 및 네트워크 아키텍처의 혜택을 누릴 수 있습니다.

AWS Well-Architected Framework는 클라우드 설계자가 애플리케이션을 위한 안전하고, 성능이 뛰어나고, 탄력적이며, 효율적인 인프라를 구축할 수 있도록 지원합니다. AWS Well-Architected Framework에는 정보 및 시스템 보호에 중점을 둔 보안 요소가 포함되어 있습니다. 주요 내용으로는 데이터의 기밀성 및 무결성, 권한 관리를 통한 사용자 권한 식별 및 관리, 시스템 보호, 보안 이벤트 탐지를 위한 제어 기능 설정이 있습니다. 고객은 AWS Management Console에서 AWS Well-Architected Tool를 사용하거나 APN 파트너 중 한 곳의 서비스를 사용할 수 있습니다.

AWS Well-Architected Tool는 워크로드의 상태를 검토하고 최신 AWS 아키텍처 모범 사례와 비교하는 데 유용합니다. 이 무료 도구는 AWS Management Console에서 제공되며, 운영 효율성, 보안, 안정성, 성능 효율성 및 비용 최적화와 관련된 일련의 질문에 답변한 후 사용할 수 있습니다. 그러면 AWS Well-Architected Tool에서 확립된 모범 사례를 사용하여 클라우드를 설계하는 방법에 대한 계획을 제공합니다.

규정 준수

AWS 규정 준수는 고객이 AWS 클라우드에서 보안 및 데이터 보호를 유지하기 위해 AWS에서 구현되는 강력한 제어를 이해할 수 있도록 지원합니다. AWS 클라우드에 시스템을 구축하면 AWS와 고객은 규정 준수 책임을 공유합니다. AWS 컴퓨팅 환경은 SOC 1/SSAE 16/ISAE 3402(이전의 SAS 70), SOC 2, SOC 3, ISO 9001 / ISO 27001, FedRAMP, DoD SRG, PCI DSS Level 1.i 등 지역 및 업종에 따른 인증 기관의 인증과 더불어 지속적으로 감사를 받습니다. 또한 AWS에는 고객이 AWS에서 실행되는 환경의 규정 준수를 확립하는 데 도움이 되는 템플릿 및 제어 매핑을 제공하는 보증 프로그램도 있습니다(전체 프로그램 목록은 AWS 규정 준수 프로그램 참조).

GDPR을 준수하면서 모든 AWS 서비스를 사용할 수 있도록 보장합니다. 즉, 고객은 서비스 보안을 유지하기 위해 AWS가 이미 취하고 있는 모든 조치의 혜택을 누릴 수 있을 뿐만 아니라 GDPR 규정 준수 계획의 일부로 AWS 서비스를 배포할 수 있습니다. AWS는 고객이 GDPR 계약상의 의무를 준수할 수 있도록 GDPR 규정 준수 데이터 처리 부록(GDPR DPA)을 제공합니다. AWS GDPR DPA는 AWS 서비스 약관에 통합되어 있으며 GDPR을 준수하기 위해 이를 필요로 하는 전 세계 모든 고객에게 자동으로 적용됩니다. Amazon.com, Inc.는 EU-US Privacy Shield에 따라 인증을 받았으며 AWS는 본 인증의 적용을 받습니다. 이를 통해 개인 데이터를 미국으로 전송하기로 선택하는 고객이 데이터 보호 의무를 충족할 수 있습니다. Amazon.com Inc.의 인증은 EU-US Privacy Shield 웹 사이트(https://www.privacyshield.gov/list)에서 확인할 수 있습니다.

인증된 환경에서 운영함으로써 고객이 수행해야 하는 감사 범위와 비용을 줄일 수 있습니다. AWS는 하드웨어 및 데이터 센터의 물리적 및 환경적 보안을 포함하여 기본 인프라에 대한 평가를 지속적으로 수행하므로 고객은 이러한 인증과 포함된 제어 기능을 활용할 수 있습니다.

기존 데이터 센터에서는 일반적인 규정 준수 활동이 수동적이고 주기적인 경우가 많습니다. 이러한 활동에는 자산 구성 확인 및 관리 활동에 대한 보고가 포함됩니다. 게다가, 결과 보고서는 게시하기도 전에 이미 최신 상태가 아닐 수 있습니다. AWS 환경에서 운영하면 고객이 AWS Security Hub, AWS Config, AWS CloudTrail와 같은 내장된 자동화 도구를 활용하여 규정 준수를 검증할 수 있습니다. 이러한 작업은 일상화, 지속화 및 자동화되어 있으므로 이러한 도구를 사용하면 감사 수행에 필요한 노력이 줄어듭니다. 수작업에 소요되는 시간을 단축함으로써 회사의 규정 준수 역할을 필요한 관리 부담 중 하나에서 위험을 관리하고 보안 상태를 개선하는 역할로 전환할 수 있습니다.

참고 문헌

추가 정보는 다음 리소스를 참조하세요.

내용	참조
AWS에서의 클라우드 보안을 위한 주요 주제, 연구 분야 및 교육 기회	AWS 클라우드 보안 학습
비즈니스, 인력, 거버넌스, 플랫폼, 보안 및 운영의 6가지 중점 영역에 대한 가이드를 제공하는 AWS Cloud Adoption Framework	AWS Cloud Adoption Framework
AWS에서 사용 중인 특정 제어 기능, AWS를 기존 프레임워크에 연동하는 방법	Amazon Web Services: 위험 및 규정 준수
보안, 자격 증명 및 규정 준수 모범 사례	보안, 자격 증명 및 규정 준수 모범 사례
보안 원칙 - AWS Well-Architected Framework	보안 원칙 - AWS Well-Architected Framework

문서 수정

이 백서의 업데이트에 대한 알림을 받으려면 RSS 피드를 구독하세요.

업데이트 기록-변경	update-history-description	update-history-date
백서 업데이트됨	참고 문헌 링크가 업데이트되었습니다.	2021년 11월 11일
백서 업데이트됨	최신 서비스, 리소스 및 기술이 업데이트되었습니다.	2020년 1월 22일
최초 게시	AWS 보안 소개가 게시되었습니다.	2015년 7월 1일

고지 사항

고객은 본 문서에 포함된 정보를 독자적으로 평가할 책임이 있습니다. 본 문서는 (a) 정보 제공만을 위한 것이며, (b) 사전 고지 없이 변경될 수 있는 현재의 AWS 제품 제공 서비스 및 사례를 보여 주며, (c) AWS 및 자회사, 공급업체 또는 라이선스 제공자로부터 어떠한 약정 또는 보증도 하지 않습니다. AWS 제품 또는 서비스는 명시적이든 묵시적이든 어떠한 종류의 보증, 진술 또는 조건 없이 '있는 그대로' 제공됩니다. 고객에 대한 AWS의 책임과 법적 책임은 AWS 계약서에 준하며 본 문서는 AWS와 고객 간의 계약에 포함되지 않고 계약을 변경하지도 않습니다.