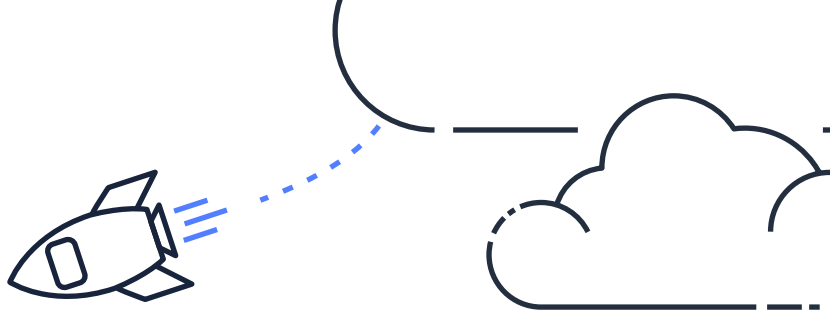
보안 및 규정 준수

빠른 참조 가이드
2021

주의

고객은 본 문서에 포함된 정보를 독립적으로 평가할 책임이 있습니다. 본 문서는: (a) 정보 제공만을 목적으로 하며, (b) 예고 없이 변경될 수 있는 현재 AWS 제품 제공 및 관행을 나타내며, (c) AWS와 그 계열사, 공급업체 또는 라이선스 제공자로부터 어떠한 약정이나 보증도 생성하지 않습니다. AWS 제품 또는 서비스는 명시적이든 묵시적이든 어떠한 종류의 보증, 진술 또는 조건 없이 "있는 그대로" 제공됩니다. 고객에 대한 AWS의 책임 및 의무는 AWS 계약에 의해 관리되며, 본 문서는 AWS와 고객 사이의 어떠한 계약에도 속하지 않으며 계약을 변경하지도 않습니다.



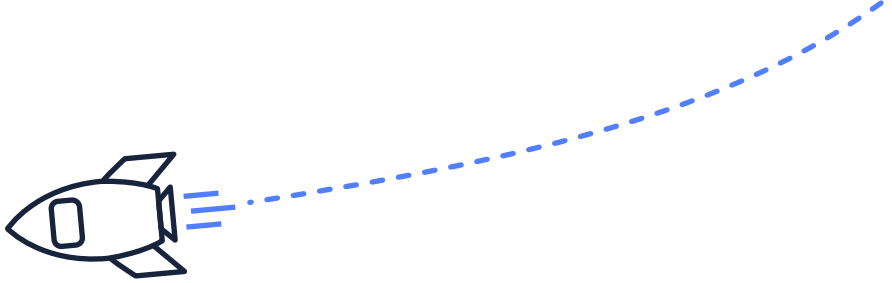
목차

개요

AWS에서 보안은 최우선 과제입니다.

즉 보안은 당사의 문화와 프로세스에 깊게 녹아들어 있으며, 당사가 수행하는 모든 작업에 배어들어 있습니다. 이는 고객에게 무엇을 의미할까요? AWS 고객은 보안에 가장 민감한 조직의 요구 사항을 충족하도록 전세계에 구축된 데이터 센터 및 네트워크 아키텍처의 이점을 누릴 수 있습니다. 또한 전역 보안 동향에 대한 뛰어난 인사이트를 지닌 엔지니어가 설계한 고급 보안 서비스를 이용할 수 있으며, 이러한 서비스는 당사의 AWS 파트너 중 고객이 이미 알고 있으며 신뢰하는 제품을 사용하여 협업하도록 설계되어 있습니다. 즉 사용자의 클라우드 인프라에 대한 심도 있는 가시성 및 지속적인 모니터링과, 태스크를 자동화하는 능력으로 위험을 줄여 성장에 따른 필요를 충족하는 보안을 선택할 수 있습니다.

보안 및 규정 준수 빠른 참조 가이드(QRG)는 당사가 AWS 인프라의 보안 및 규정 준수를 유지하는 방법에 대한 광범위한 개요와, 사용자가 이용할 수 있는 보안 및 규정 준수 서비스의 개요를 사용자에게 제공하기 위해 생성되었습니다.



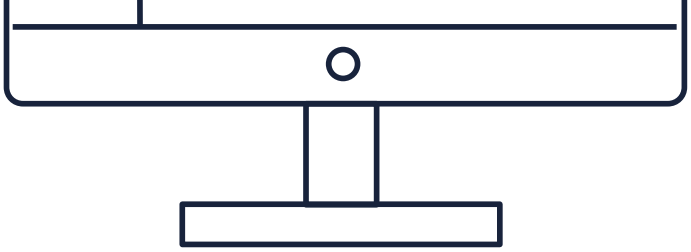
AWS를 통한 보안의 이점

이 가이드가 처음 발행된 몇 년 전부터, 퍼블릭 클라우드 제공자에 대한 관점은 변화해 왔습니다.

보안은 더 이상 마이그레이션의 걸림돌 또는 감속 요소로 여겨지지 않습니다. 대신 귀사의 디지털 비즈니스 결정, 공급 업체 및 기술 선택, 그리고 투자 전략을 가이드하기 위해 사용할 수 있는 주요 차별점으로 여겨집니다. 이미 많은 고객들이 AWS가 현재 사용 가능한 가장 유연하고 안전한 클라우드 컴퓨팅 환경을 제공하도록 설계되었다는 확신을 갖고 마이그레이션을 실시했습니다. 이러한 고객들은 조직의 보안을 강화하면서 핵심 비즈니스에 집중할 수 있도록 운영 방식을 혁신했습니다. AWS 고객으로서 사용자는 AWS를 통한 보안의 다섯 가지 주요 이점을 깨달을 수 있습니다.

최고의 가시성 및 제어를 통해 안전하게 조정

AWS를 통해 고객은 데이터 저장 위치, 액세스 허용자 및 고객이 소속된 조직이 언제든 사용할 수 있는 리소스 항목에 대해 제어할 수 있습니다. 실시간에 가까운 보안 정보에 대한 지속적인 모니터링과 결합한 세분화된 자격 증명 및 액세스 제어를 통해 사용자는 정보 저장 위치에 상관 없이, 올바른 리소스에 항상 올바른 액세스 권한을 부여했는지 확인할 수 있습니다. 당사의 보안 자동화 및 동작 모니터링 서비스를 사용하여 구성 변경 등의 의심스러운 보안 이벤트를 사용자 환경 전반에서 탐지하여 확장에 따른 위험을 줄이세요. 사용자의 기존 솔루션을 당사의 서비스와 통합하여 기존 워크플로를 지원하고, 운영을 능률화하며, 규정 준수 보고를 간소화하도록 지원할 수도 있습니다.



심도있게 통합된 서비스로 자동화 및 위험 감소

AWS에서 보안 작업을 자동화하면 구성 변경 시의 수작업 오류를 줄이고 팀이 비즈니스에 중요한 다른 업무에 더 많은 시간을 내 집중할 수 있으므로 보안이 향상됩니다. 새로운 방식으로 작업을 자동화하기 위해 결합할 수 있는 다양한 심층 통합 솔루션 중에서 선택하여, 고객의 보안 팀이 개발자 및 운영 팀과 긴밀하게 협력하여 코드를 보다 빠르고 안전하게 만들고 배포할 수 있습니다. 예를 들어 기계 학습 등의 기술을 사용하여 AWS는 사용자가 AWS 콘솔에서 클릭 몇 번으로 자동으로, 그리고 지속적으로 민감한 데이터를 탐색, 분류 및 보호할 수 있게 해줍니다. 인프라와 애플리케이션 보안 검사를 자동화하면 보안 및 규정 준수 제어를 지속적으로 시행하여 기밀성, 무결성 및 가용성을 항상 보장할 수 있습니다. 하이브리드 환경에서 AWS의 정보 관리 및 보안 도구를 통해 자동화하여 AWS가 온프레미스 및 레거시 환경의 원활하고 안전한 확장으로서 통합하도록 할 수 있습니다.legacy environments.

최고 수준의 개인 정보 보호 및 데이터 보안 표준 구축

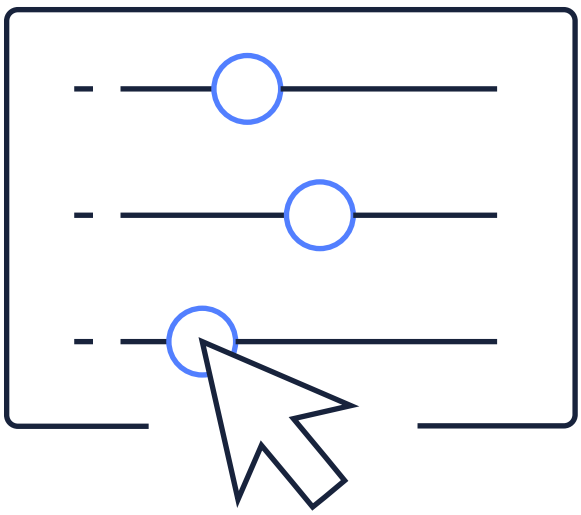
AWS는 고객이 개인 정보와 데이터 보안에 깊은 관심을 가지고 있다는 것을 잘 알고 있습니다. 당사의 고객들이 데이터 보안에 매우 주의를 기울이고 있기 때문에, 당사에서는 세계적인 수준의 보안 전문가 팀이 당사 시스템을 매일 24시간 내내 모니터링하며 고객 콘텐츠를 보호합니다. AWS에서는 데이터를 암호화하고 이동하고 보존하는 등의 데이터에 대한 액세스 권한을 고객이 항상 소유하므로 가장 안전한 글로벌 인프라를 구축할 수 있습니다. AWS 전역 네트워크 전반을 흐르는 모든 데이터는 당사의 데이터 센터와 리전을 서로 연결합니다. 이 데이터는 보호된 시설을 떠나기 전 물리적 계층에서 자동으로 암호화됩니다. 추가적인 암호 레이어 또한 존재합니다. 예를 들어 모든 VPC 교차 리전 피어링 트래픽, 그리고 고객 또는 서비스 간 TLS 연결이 이에 해당합니다. 당사는 고객이 데이터를 쉽게 암호화하고, 옮기거나 저장해 둘 수 있도록 지원하는 도구를 제공하며, 승인된 사용자만이 해당 항목에 액세스할 수 있도록 보장합니다. 사용자는 당사의 AWS 키 관리 시스템(KMS)이 FIPS 140-2 레벨 2 유효화 하드웨어 보안 모델(HSMs)을 통해 관리하는 키를 사용할 수 있습니다. 또는 FIPS 140-2 레벨 3 유효화 HSMs를 사용하는 AWS CloudHSM를 갖춘 자체 암호화 키를 관리할 수 있습니다. 또한 사용자가 리전 및 로컬 데이터 개인정보 보호 법률 및 규제를 준수함을 증명하기 위해 필요한 제어 및 가시성을 제공합니다. 당사의 전역 인프라 설계는 사용자가 콘텐츠가 물리적으로 위치한 리전에 대한 완전한 제어권을 유지하도록 해서 사용자가 데이터 상주 요건을 충족하도록 지원합니다.

최대 규모의 보안 파트너 및 솔루션 에코시스템

이미 알고 신뢰하는 익숙한 솔루션 공급 업체의 보안 기술 및 컨설팅 서비스를 사용하여 AWS의 이점을 확장해 보십시오. 당사는 심도 있는 전문성과 초기 마이그레이션부터, 진행 중인 일상적인 관리까지 모든 단계의 클라우드 적용을 성공적으로 보호함이 입증된 제공자를 주의깊게 선택했습니다. 기술 및 컨설팅 파트너에 대한 전역 프로그램인 AWS 파트너 네트워크(APN)에서 보안 중심 솔루션 및 서비스를 귀사의 특정 워크로드 및 사용 사례에 제공하도록 특화된 많은 기업들 중 선택하십시오. AWS 파트너 솔루션은 사용자의 워크로드에 자동화, 민첩성 및 크기 조정을 사용합니다. 서비스형 소프트웨어(SaaS) 제품을 포함하는 이러한 클라우드 기성 소프트웨어 솔루션을 쉽게 찾고, 구매하며, 배포하고 관리하십시오. 이러한 작업은 AWS Marketplace에선 단 몇 분이면 해결됩니다. 이러한 솔루션들은 함께 작동하여 온프레미스에서는 불가능한 방식으로, 광범위한 워크로드 및 사용 사례에 적용할 수 있는 솔루션을 통해 사용자의 데이터를 보호합니다.

가장 종합적인 보안 및 규정 준수 제어 이어가기

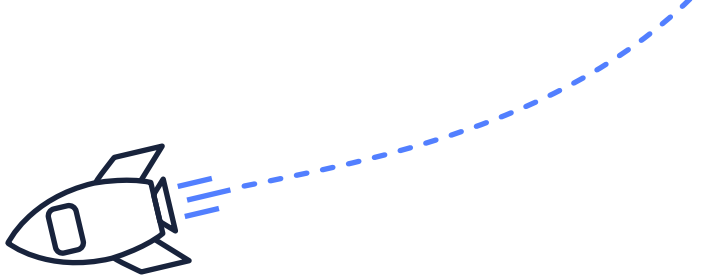
고객의 규정 준수 노력을 지원하기 위해 AWS는 금융, 소매, 의료, 정부 등 다양한 분야에 대한 보안 및 규정 준수 스탠더드를 고객이 충족하도록 당사가 지속적으로 모니터링하는 수천 개의 글로벌 규정 준수 요구 사항에 대한 서드 파티 검증을 정기적으로 수행합니다. AWS에서 운영하는 최신 보안 제어를 이어가며 사용자의 자체 규정 준수 및 인증 프로그램을 강화하는 동시에, 특정 보안 보장 요건을 실행하는 데 소요되는 비용 및 시간을 감축하기 위해 사용 가능한 도구에 액세스할 수 있습니다. AWS는 타 제품 및 서비스보다 많은 보안 스탠더드 및 규정 준수 자격증을 지원합니다. 여기에는 SOC 2, PCI-DSS, HIPAA/HITECH, FedRAMP, GDPR, FIPS 140-2 및 NIST 800-171이 포함되며, 고객이 전역의 사실상 모든 규제 기관에 대한 규정 준수 요건을 충족하도록 지원합니다.



당사의 책임 공유 방식

AWS로 IT 인프라를 이동 시 사용자는 공동 책임 모델을 채택합니다. 이 공동 책임 모델은 고객의 운영 부담을 덜어줍니다. 당사가 호스트 운영 체제 및 가상화 계층부터, 서비스가 작동하는 시설의 물리적 보안에 이르기까지 IT 구성 요소 계층을 운영, 관리, 제어하기 때문입니다. 고객은 IT 환경 운영에 대한 책임을 당사와 공유하듯 IT 제어의 관리, 운영 및 확인도 공유합니다.

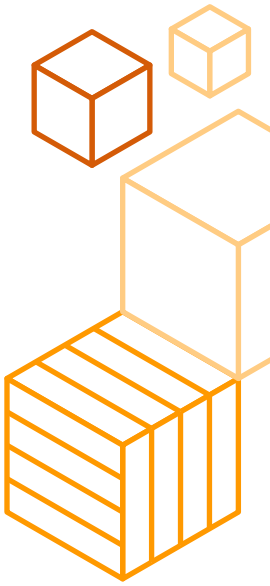
요약하자면 AWS는 **클라우드 "자체"의 보안**을 담당하며, 고객으로서 사용자는 아래에 자세히 설명한 **클라우드 "내부"의 보안**을 담당합니다.



클라우드 "자체"의 보안

AWS에는 클라우드 "자체의" 보안에 대한 책임이 있습니다. 고객 정보, 자격 증명, 애플리케이션 및 장치를 보호하도록 설계된 AWS 데이터 센터와 네트워크의 이점을 누릴 수 있습니다. 그리고 사용자는 전역 규제 기관의 규정 준수 요건을 충족하도록 지원하기 위해 생성된 가장 종합적인 규정 준수 제어를 이어갑니다.

AWS 보안 보증



당사의 공동 책임 모델을 통해 고객은 IT 환경에서 위험을 효과적이고 효율적으로 관리할 수 있으며, 구축되고 광범위하게 알려진 프레임워크 및 프로그램을 갖춘 당사의 규정 준수를 통해 효과적인 위험 관리에 대한 확실성을 제공합니다.

당사가 전역 서비스 및 시설에서 효과적으로 운영되고 있는 유비쿼터스 제어 환경을 유지하고 있음을 입증하기 위해 당사는 서드 파티의 독립적인 평가를 추구합니다.

당사의 제어 환경은 전체 AWS 제어 환경의 다양한 측면을 활용하는 정책, 프로세스 및 제어 활동을 포함합니다.

AWS 인증, 프로그램, 보고서 및 서드 파티 증명

AWS는 외부 인증 기관 및 독립 감사 기관과 협력하여 고객에게 정책, 프로세스 및 컨트롤에 대한 다양한 정보를 제공합니다. 해당 내용은 AWS에서 확립 및 운영됩니다.

프로그램의 전체 목록을 확인하려면 여기를 방문하십시오.
aws.amazon.com/compliance/programs

이 집합적인 제어 환경은 당사 제어 프레임워크의 운영 효과를 지원하는 환경을 구성 및 유지하는 데 필요한 인력, 프로세스 및 기술을 포괄합니다. 당사는 선도적인 클라우드 컴퓨팅 산업 기관에서 확인한 적용 가능한 클라우드 관련 제어를 당사 제어 환경에 통합했습니다. 당사는 이러한 산업 그룹을 모니터링하여 사용자가 실행할 수 있는 모범 사례를 식별하고, 고객 제어 환경을 관리하여 고객을 보다 효과적으로 지원합니다.

당사는 업계 및 정부 요건에 대한 준수 여부를 검증하는 데 도움이 되는 규정 준수 상태를 입증합니다. 당사는 외부 인증 기관 및 독립 감사 기관과 협력하여 고객에게 당사가 확립 및 운영하는 정책, 프로세스 및 제어에 대한 상세 정보를 제공합니다. 당사는 규정 준수 인증서, 보고서 및 기타 문서를 AWS Artifact라고 알려진 자체 서비스 포털을 통해 고객에게 직접 제공합니다. 사용자는 이 정보를 사용하여 적용 가능한 규정 준수 스탠더드에서 요구하는 자체 제어 평가 및 확인 절차를 수행할 수 있습니다.

"저희가 AWS의 보안 인증 레벨을 달성할 수 있는 방법은 존재하지 않습니다. 저희는 AWS 클라우드 내 고객의 논리적 분리로 큰 자신감을 얻었습니다. 특히 저희의 가상 네트워킹 환경을 사용자 지정하여 저희 특정 요건을 충족할 수 있는 Amazon VPC을 통할 때 그러했습니다."

- Michael Lockhart
IT 인프라 관리자

GPT
The GPT Group

고객은 당사가 당사의 위험 및 규정 준수 프로그램에 대하여 고객의 규정 준수 프레임워크에 제공하는 정보를 통합할 수 있습니다. 당사는 수천 가지의 보안 제어를 사용하여 당사가 전역 스탠더드 및 모범 사례에 대한 규정 준수를 유지하고 있음을 모니터링합니다.

개인정보 처리방침

AWS는 고객의 개인 정보를 철저하게 지킵니다. 고객은 항상 자신의 콘텐츠를 소유하는데, 여기에는 이를 암호화하고, 이동시키며, 보유를 관리하는 능력이 포함됩니다. 당사는 고객이 데이터를 쉽게 암호화하고, 이동하거나 저장해 둘 수 있도록 지원하여 승인된 사용자만이 해당 항목에 액세스할 수 있도록 보장합니다.

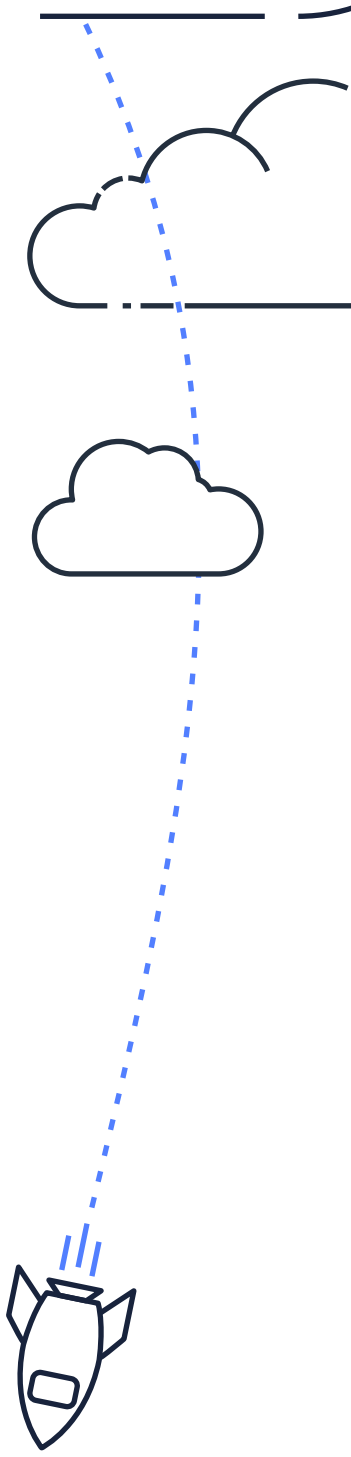
AWS는 사용자가 조직에 해당하는 리전 및 로컬 데이터 개인 정보 보호 법률 및 규정을 준수하도록 지원하는 제어를 제공합니다. 당사의 전역 인프라 설계는 사용자가 데이터가 물리적으로 저장된 장소에 대한 완전한 제어권을 유지하도록 해서 사용자가 데이터 상주 요건을 충족하도록 지원합니다.

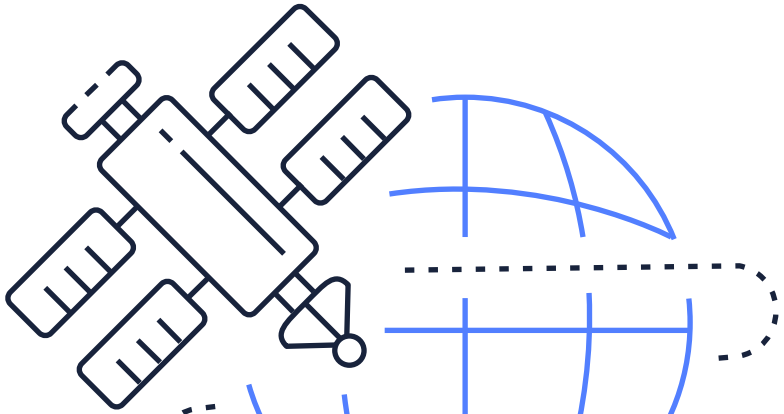
AWS를 통해 고객은 액세스 허용 사용자 및 고객이 소속된 조직이 언제든 사용할 수 있는 리소스 항목에 대해 인지합니다.

실시간에 가까운 보안 정보에 대한 세분화된 자격 증명 및 액세스 제어, 지속적인 모니터링을 통해 사용자는 정보 저장 위치에 상관 없이, 리소스의 액세스 레벨이 항상 올바른지 확인할 수 있습니다.

시스템 전체에서 구성 변경 및 보안 이벤트를 감지하는 당사의 활동 모니터링 서비스를 사용하고, 기존 솔루션과 서비스를 통합하여 운영 및 규정 준수 보고를 단순화하여 위험을 줄이고 성장을 지원합니다.

자세히 알아보기: aws.amazon.com/compliance/data-privacy-faq





가용 영역

- 리전
- 제공 예정

고객의 콘텐츠가 저장되는 장소

AWS 데이터 센터는 전 세계 여러 장소에 클러스터 형태로 구축됩니다. 당사는 주어진 위치에 있는 데이터 센터 클러스터를 AWS 리전이라고 합니다.

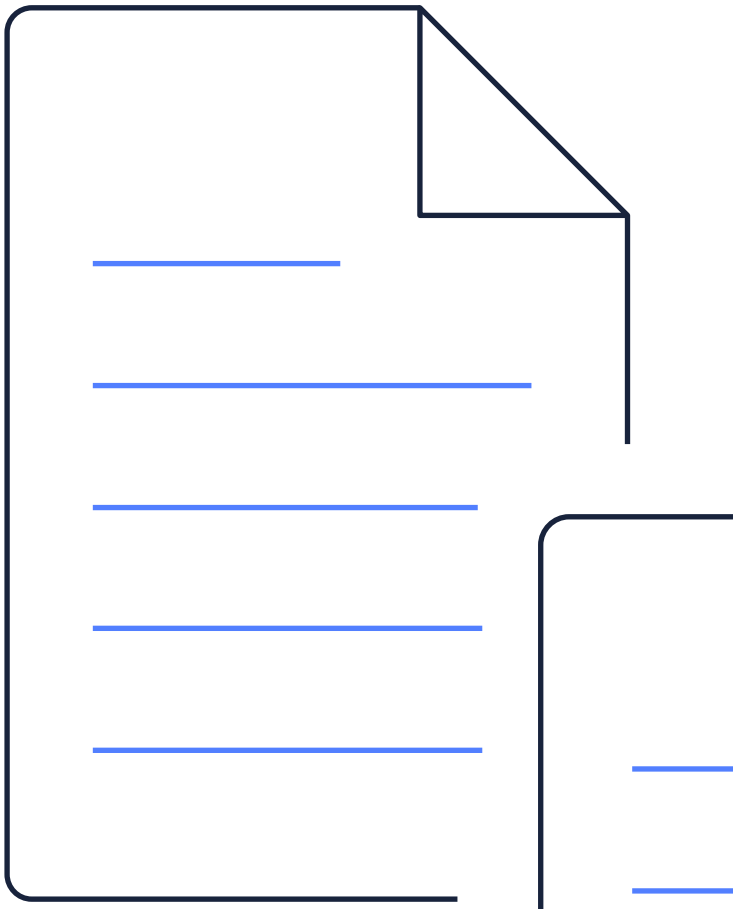
사용자는 전역의 수많은 AWS 리전에 대한 액세스 권한을 가지며, 하나의 AWS 리전, 모든 AWS 리전 또는 AWS 리전의 모든 조합을 사용하도록 선택할 수 있습니다.

사용자는 데이터가 물리적으로 저장된 AWS 리전에 대한 완전한 제어를 유지하여, 사용자의 규정 준수 및 데이터 보관 요건을 충족할 수 있습니다. 예를 들어 유럽 고객이라면, EU(프랑크푸르트) 리전에 고객의 AWS 서비스를 배타적으로 배포하도록 선택할 수 있습니다. 이러한 선택을 했다면, 사용자의 콘텐츠는 다른 AWS 리전을 선택하지 않는 한 독일에 배타적으로 저장됩니다.

데이터 센터 개요

2006년부터 클라우드 컴퓨팅을 시작한 선구자로서 AWS는 안전하고 더욱 빠르게 혁신적으로 클라우드 인프라를 구축합니다. AWS는 데이터 센터의 설계 및 시스템을 지속적으로 혁신하여 사람의 실수로 인한 위험과 자연적 위험으로부터 데이터 센터를 보호합니다. 또한, 제어를 구현하고 자동화 시스템을 구축하며, 보안 및 규정 준수 확인을 위한 서드 파티 감사를 실시합니다. 그 결과로 엄격한 규제를 받는 전 세계 대부분의 조직들이 AWS를 신뢰합니다.

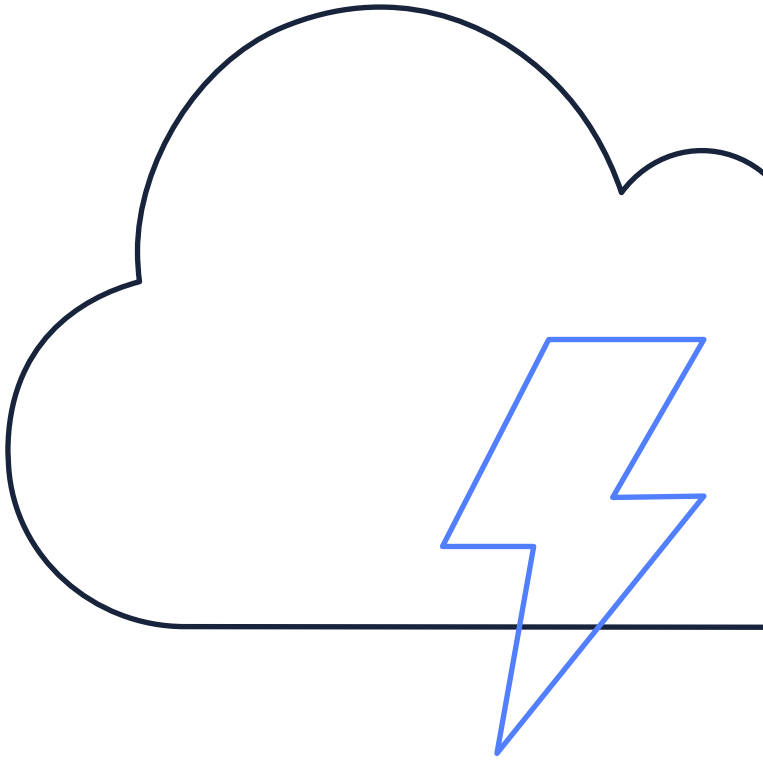
더 많은 정보를 확인하려면
여기를 방문하십시오.
aws.amazon.com/compliance/
data-center/controls/



비즈니스 연속성

당사의 인프라는 높은 수준의 가용성을 갖추고 있으며, 당사는 사용자가 복원력을 갖춘 IT 아키텍처를 배포하기 위해 필요한 기능을 제공합니다. 당사 시스템은 고객에 대한 영향은 최소화하며 시스템 또는 하드웨어 장애를 견디도록 설계되었습니다.

AWS 비즈니스 지속성 계획에는 환경 파괴를 방지하고 줄이기 위한 조치가 요약되어 있습니다. 이 계획은 이벤트 전, 진행 동안, 그리고 후에 취할 단계에 대한 운영 세부 정보를 포함합니다. 해당 비즈니스 지속성 계획은 다른 시나리오의 시뮬레이션을 포함하는 테스팅으로 지원됩니다. 테스트 진행 동안, 그리고 그 후에 AWS는 사용자 및 프로세스 성능, 시정 작업, 지속적인 향상 목표와 학습한 교훈을 문서화합니다.



"AWS는 비용 효율적 방식으로 정보를 저장하게 해주어 AWS가 관리하게 된 이후에는 필요 인프라를 지원하는 부담이 경감되었습니다. 이는 우리와 고객에게 정말 윈윈입니다."

- **Michael Lockhart**
IT 인프라 관리자

Nasdaq

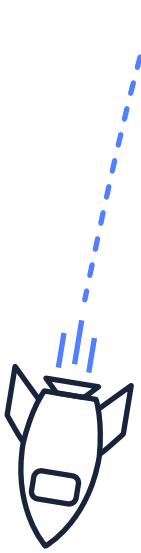
재해 복구

AWS 클라우드는 순간 탐지를 확장하는 "파일럿 라이트" 환경부터 신속한 장애 조치를 취할 수 있는 "상시 대기" 환경까지 다양한 재해 복구 아키텍처를 지원합니다.

이 기능이 복수의 AWS 가용 영역 전반에 애플리케이션을 배포할 수 있게 하여 사용자는 자연 재해 또는 시스템 장애를 포함하는 대부분의 실패 모드에서도 복원력을 유지할 수 있습니다. 모든 데이터 센터는 온라인으로 고객에게 서비스를 제공한다는 점을 기억하십시오. "콜드" 데이터 센터는 없습니다. 장애 시 자동화된 프로세스는 고객 데이터 트래픽을 장애 지역에서 먼 곳으로 이동합니다. 사용자는 AWS 인프라를 사용하여 두 번째 물리적 현장에 인프라 비용을 지출하지 않고도 핵심 IT 시스템의 재해 복구를 가속화할 수 있습니다. 사용자에게 AWS 인프라에 구축된 사용자 정보 시스템의 백업 및 복원을 관리하고 테스트할 책임이 있음을 기억하십시오. AWS는 물리적, 가상 및 클라우드 기반 서버의 신속하고 신뢰할 수 있는 복구를 AWS에 제공해 가동 중지 시간 및 데이터 손실을 최소화하는 **CloudEndure Disaster Recovery**를 제공합니다.

더 많은 정보를 확인하려면 여기를 방문하십시오.
aws.amazon.com/cloudendure-disaster-recovery/

클라우드 "내부"의 보안



AWS가 클라우드 "자체"의 보안으로 차별화되지 않은 과도한 작업을 처리하지만, AWS 고객으로서의 사용자는 여전히 클라우드 "내부"의 보안을 책임집니다. 사용자는 업데이트 및 보안 패치 설치를 포함하여 게스트 운영 시스템 관리를 책임집니다. 또한 관련 애플리케이션 소프트웨어 관리는 물론 선택한 방화벽의 구성을 책임집니다. 사용자의 책임은 선택한 AWS 서비스, 이러한 서비스를 사용자 IT 환경에 통합하는 방식, 그리고 해당하는 법률 및 규제에 따라 달라집니다.

AWS 리소스를 안전하게 관리하기 위해 사용자는 다음 네 가지 작업을 수행해야 합니다.

1. 사용자 인벤토리 및 리소스 관리를 자동화하여 보유 항목을 파악하고, 적절하게 보호합니다.

2. 사용자 리소스 상에 게스트 OS 및 애플리케이션을 안전하게 구성합니다(보안 구성 설정, 패치 작업 및 맬웨어 방지 소프트웨어).

3. 리소스에 대한 변경을 관리합니다(변경 관리).

4. 사고 대응 및 재해 복구 계획을 만들고 자동화합니다.

Identity and Access Management

AWS Identity Services는 사용자가 자격 증명, 리소스 및 허가를 규모에 따라 안전하게 관리하게 해줍니다. AWS를 통해 사용자는 인력 및 고객 대면 애플리케이션에 대한 자격 증명 서비스를 보유하여 빠르게 시작하고, 워크로드 및 애플리케이션에 대한 액세스를 관리합니다. AWS는 또한 다음 서비스로 사용자에게 자유를 선사합니다. **IAM Access Analyzer**를 통해 직원의 자격 증명과 세분화된 허가를 관리하는 지점을 선택하여 적절한 액세스를, 적절한 사용자에게 적시에 부여할 수 있습니다. **AWS Identity & Access Management(IAM)** 등의 서비스는 사용자가 AWS 서비스 및 리소스에 대한 액세스를 안전하게 관리할 수 있게 해주는 반면에 **AWS Organizations**는 AWS 계정 간 거버넌스 및 관리를 중앙화하는 기능을 부여하며, **AWS Single Sign-On(SSO)**을 통해 사용자는 클라우드 통합 인증(SSO)을 사용할 수 있습니다.

"저희는 보안과 Identity and Access Management를 올바르게 처리하면 저희 엔지니어가 명확하고 신뢰할 수 있는 벽 내부의 제품에 집중할 수 있을 거라고 생각합니다. 따라서 저희는 감사를 할 수 있는 자체 서비스 보안 기반을 AWS IAM를 통해 구현했습니다."

- **Rob Witoff**
이사

coinbase

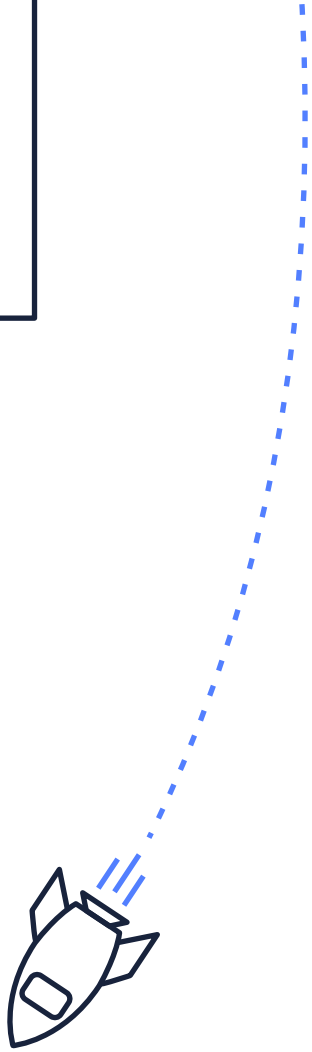
AWS Security and Identity Services

클라우드 "내부"의 보안을 구축하도록 지원하기 위해 AWS는 혁신적인 보안 서비스의 광범위한 선택지를 제공합니다. 해당 서비스는 고객 자체 보안 및 규제 요건을 간단하게 충족하도록 지원할 수 있습니다. 당사의 보안 서비스 및 솔루션은 핵심 전략 이점을 고객이 조직의 최상의 보안 태세에 구현하도록 지원하기 위해 중요한 다음 영역에 전달하는 데 중점을 두고 있습니다.

데이터 보호

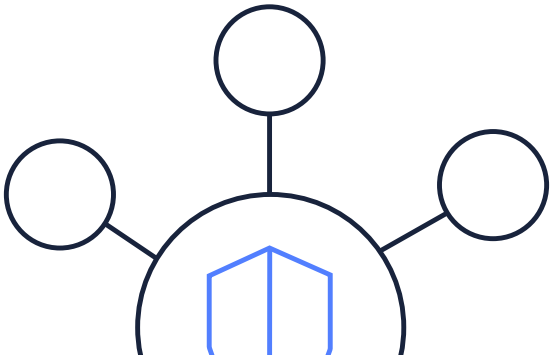
AWS는 사용자의 데이터, 계정, 워크로드를 승인되지 않은 사용자로부터 보호하도록 지원하는 서비스를 제공합니다.

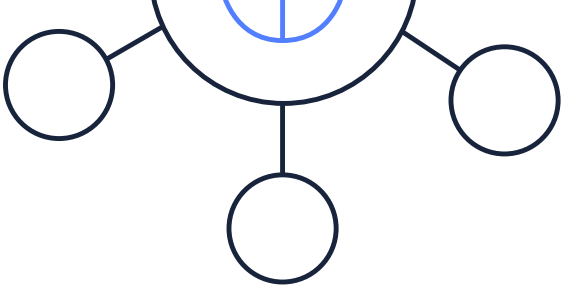
AWS 데이터 보호 서비스는 암호화, 키 관리 및 위협 탐지 기능을 제공하여 사용자의 계정 및 워크로드를 지속적으로 모니터링하고 보호하도록 지원합니다. **Amazon Macie**를 통해 사용자는 당사의 데이터 보호 서비스를 사용하여 민감한 데이터를 대량 탐색 및 보호할 수 있습니다. **AWS Key Management Service(KMS)**를 사용하여 데이터를 암호화하거나 데이터에 디지털 서명을 하기 위해 사용하는 키를 쉽게 생성 및 제어할 수 있습니다. **AWS Secrets Manager**로 보안 암호를 순환, 관리 및 검색할 수 있습니다. **AWS CloudHSM**으로 자체 암호 키를 쉽게 생성 및 사용할 수 있습니다. 그리고 **AWS Certificate Manager**를 사용하여 퍼블릭 및 프라이빗 인증서를 쉽게 프로비저닝, 관리 및 배포할 수 있습니다.



엣지 및 네트워크 보호

고객은 직접 생성한 규칙에 따라 트래픽을 필터링하는 AWS 서비스를 사용하여 웹 애플리케이션을 보호할 수 있습니다. 예를 들어 사용자는 IP 주소, HTTP 헤더, HTTP 본문 또는 URI 열에 기반한 웹 요청을 필터링하며, 이는 사용자가 SQL 삽입 또는 사이트 간 스크립팅 등의 일반적인 공격 패턴을 차단하도록 해줍니다. **AWS Web Application Firewall(WAF)**를 사용하여 일반적인 웹 도용으로부터 사용자의 웹 애플리케이션을 보호합니다. **AWS Shield**를 통해 DDoS 보호 기능을 관리합니다. **AWS Firewall Manager**로 AWS Organizations 내 사용자의 계정 및 애플리케이션 전반에서의 방화벽 규칙을 중앙에서 구성 및 관리합니다. 그리고, **AWS Network Firewall**을 사용하여 단 몇 번의 클릭으로 사용자의 AWS Network Firewall 전반에 네트워크 보안 기능을 배포합니다.





위협 탐지 및 관리

AWS는 사용자가 사용자 클라우드 환경 내에서 네트워크 활동 및 계정 동작을 지속적으로 모니터링하여 위협을 식별하게 해줍니다. 당사의 서비스를 통해 사용자는 비즈니스에 영향을 주기 전에 문제를 발견하고, 보안 태세를 개선하고, 사용자 환경의 위험 프로필을 줄이는 데 필요한 가시성을 확보할 수 있습니다. **Amazon GuardDuty**를 사용자의 관리형 위협 탐지 서비스로 사용합니다. **Amazon Detective**로 보안 데이터를 분석 및 시각화하여 잠재적 보안 문제의 근본 원인을 신속하게 파악합니다. **Amazon Inspector**로 보안 평가를 자동화하여 AWS에 배포한 애플리케이션의 보안 및 규정 준수를 개선하도록 지원합니다. 그리고 **AWS Security Hub**를 사용자가 보안 알림을 중앙에서 확인 및 관리하고, 보안 확인을 자동화할 수 있는 통합 보안 및 규정 준수 센터로 사용합니다.

AWS Security and Identity Services에 대한 더 많은 정보를 확인하려면 여기를 방문하십시오.
aws.amazon.com/products/security

규정 준수 및 데이터 개인 정보 보호, Amazon Security Hub, Systems Manager 및 CloudWatch

AWS는 규정 준수 상태에 대한 종합적인 보기를 제공하며, 조직이 따르는 AWS 모범 사례와 산업 표준을 기반으로 자동화된 규정 준수 검사를 사용하여 환경을 지속적으로 모니터링합니다. **AWS Audit Manager**를 사용하여 사용자의 AWS 사용을 지속적으로 감사해 위험과 규정 준수를 평가하는 방식을 간소화할 수 있습니다. **AWS CloudTrail**로 사용자 활동 및 API 사용을 추적합니다. **AWS Config**로 사용자의 AWS 리소스 구성을 기록 및 평가합니다. 그리고 **AWS Artifact**를 AWS의 규정 준수 보고서에 대한 온디맨드 액세스용 자체 서비스 포털로 사용합니다. 또한 **AWS Security Hub의 기본 보안 모범 사례 스탠더드**를 사용하여 배포한 계정 및 리소스가 보안 모범 사례에서 이탈하는 시점을 탐지할 수 있으며, **Config의 Conformance Packs**로 이상적인 구성 설정 대비 사용자 AWS 리소스의 구성 설정을 평가할 수 있습니다.

범위 내의 AWS 서비스

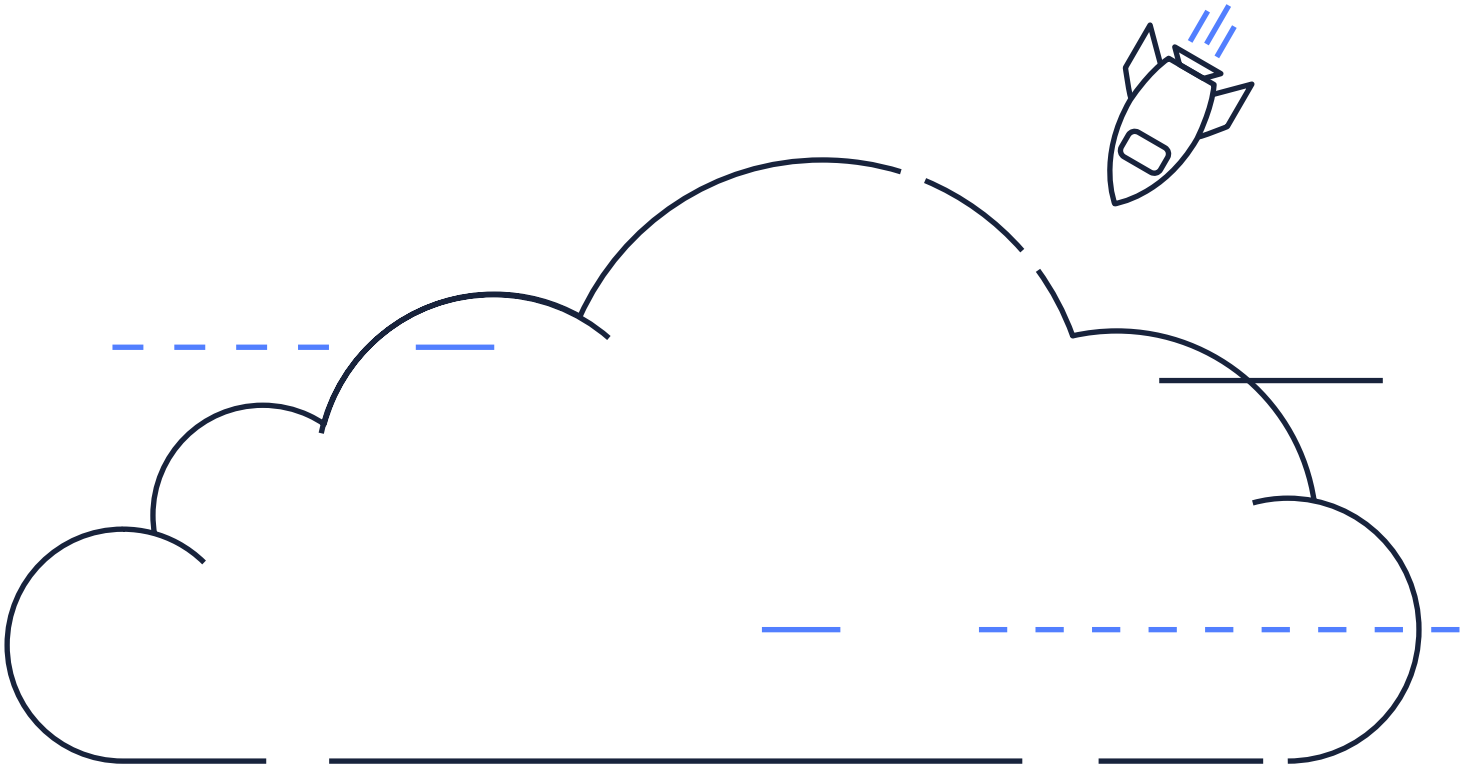
예상 사용 사례, 피드백 및 요구에 기반하여 당사의 규정 준수 프로그램의 범위에 서비스를 포함시킵니다. AWS에 구축한 항목의 특징에 따라, 사용자는 서비스가 고객 데이터를 처리할지 또는 저장할지 여부와 이것이 사용자의 고객 데이터 환경 규정 준수에 어떻게 영향을 미칠지, 미치지 않을지를 결정해야 합니다.

더 많은 정보를 확인하려면 당사의 Services in Scope 웹페이지를 방문하십시오.
aws.amazon.com/compliance/services-in-scope

클라우드 "내부"의 보안에 대한 AWS 모범 사례

자체 AWS 마이그레이션 전략을 생성하거나 AWS에서 기존 워크로드를 재방문한다면, 사용자가 강력한 보안 기반을 구축하는 데 도움이 될 수 있는 업계 승인 표준 및 프레임워크가 많이 있습니다.

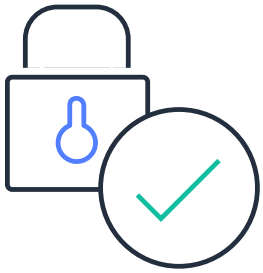
CIS, ISO 27001, 및 NIST Cybersecurity Framework(CSF) 등의 프레임워크는 IT 거버넌스 및 보안 관리 시스템을 구축하기 위한 구조화된 접근 방식을 제공하고 AWS Security Hub는 이러한 스탠더드 대비 자동화된 보안 확인 기능을 제공합니다. AWS는 또한 AWS Cloud Adoption Framework, AWS Well-Architected, 그리고 AWS 기본 보안 모범 사례 스탠더드를 통해 당사의 자체 모범 사례 가이드를 제공합니다.



AWS로 마이그레이션: AWS Cloud Adoption Framework

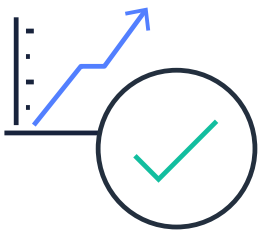
AWS Professional Services는 수천 건의 고객 마이그레이션에 기반한 Cloud Adoption Framework(CAF)를 생성하여 조직이 성공적이고 안전한 클라우드 마이그레이션을 계획하도록 지원했습니다. 각 조직의 경로가 달라지기 때문에, 미리 계획을 수립하고 비즈니스 목표와 원하는 결과를 올바른 프로세스 및 기술과 연결하는 것이 중요합니다. CAF는 대부분의 조직에 적용되는 일반 원칙에 기반한 계획 수립 및 전략 고려 사항에 사용하는 여섯 가지 관점에 중점을 두고 있습니다. 세 가지 관점(비즈니스, 사람 및 거버넌스)은 비즈니스 기능에 중점을 둔 반면 기술적 관점은 플랫폼, 보안 및 운영 관점에서 고려합니다. 여섯 가지 관점을 종합하면, 조직의 리더가 올바른 이해 관계자를 파악하고, 기존의 기능 및 프로세스의 격차를 파악해 클라우드로의 전환을 계획 및 지시하도록 해줍니다.

CAF의 보안 관점은 기업 고객과 그들의 클라우드 채택 여정에서 협업한 AWS 경험을 담고 있습니다. 이는 식별 및 선택을 제어하기 위한 위험 기반 접근 방식(예: 보안 지도 제작)을 구성하는 방법, 반복을 통해 성숙을 구현하는 보안 프로그램을 구축하는 방법 및 AWS가 AWS 클라우드에서 보안 모델을 설정하는 방법을 고객에게 설명하는 방식을 상세하게 설명합니다.



보안 관점 기능:

- Identity and Access Management(IAM)는 고객이 AWS를 고객의 자격 증명 관리 수명 주기, 그리고 인증 및 권한 부여 소스에 통합하도록 지원합니다.
- Detective Control은 AWS 환경 내 잠재적 보안 인시던트를 식별하도록 돕는 지침을 제공합니다.
- Infrastructure Security는 고객이 모범 사례를 준수하고 또한 산업 또는 규제 의무를 충족하기 위해 필요할 수 있는 제어 방법론을 구현하도록 지원합니다.
- Data Protection은 고객이 전송 중이거나 유휴 데이터를 보호하는 적절한 보호 수단을 구현하도록 지원합니다.
- Incident Response는 고객이 보안 인시던트에 대한 대응을 정의하고 실행하도록 지원합니다.



추가 자료: **AWS Cloud Adoption Framework:** aws.amazon.com/professional-services/CAF/

보안 및 복원력 워크로드에 대한 모범 사례: AWS Well-Architected

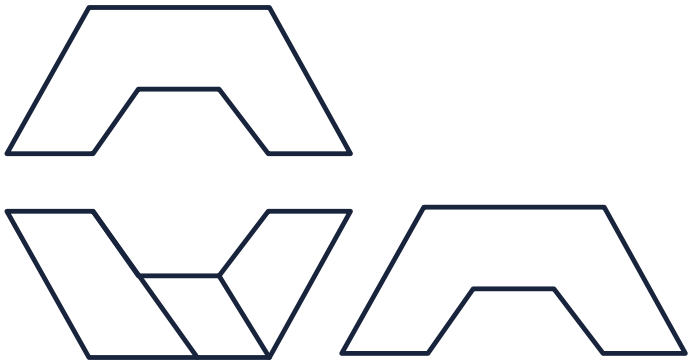
AWS Well-Architected는 모범 사례 세트로 "Well-Architected 상태인가?"라는 질문에 답하도록 돕는 AWS 관리 콘솔에서 이용할 수 있는 도구입니다. Well-Architected는 다섯 가지 중요 원칙을 조사하여 워크로드 수준(사용자 인프라, 시스템, 데이터 및 프로세스)에 집중합니다.

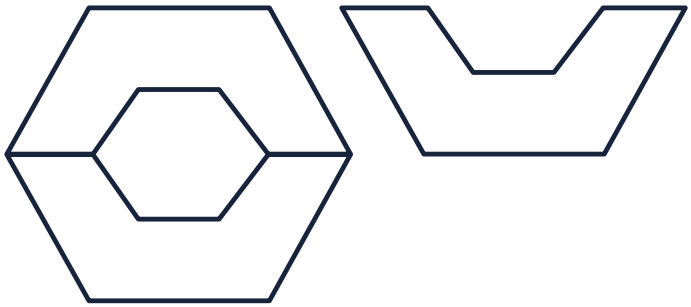
- 운영 우수성
- 보안
- 안정성
- 성능 효율성
- 비용 최적화

보안 원칙의 구성 요소는 다섯 가지입니다.

- Identity and Access Management
- 탐지
- 인프라 보호
- 데이터 보호
- 인시던트 대응

Well-Architected는 올바른 AWS 서비스를 선택하기 위한 보안 구현 및 접근 지침을 제공하여 이러한 핵심 보안 관례가 사용자의 워크로드에 마련되어 있도록 보장합니다. 사용자는 이러한 구성 요소가 CAF 보안 관점에 속한 내용과 유사하다는 것을 알아챌 수도 있습니다. 그 이유는 전략 수준에서 식별되는 이러한 기능 차이는 기술 계층에서 다루어져야 하기 때문입니다. 비즈니스 요건부터 기술 아키텍처 및 운영까지의 추적 가능성은 보안이 고객 조직의 모든 수준에 적용되고 비즈니스 필요를 충족하는지 확인하기 위한 핵심 구성 요소입니다.





AWS Well-Architected Tool(AWS WA Tool)은 AWS 관리 콘솔을 통해 이용 가능한 서비스로, 사용자의 아키텍처를 AWS 모범 사례로 측정하는 일관적인 프로세스를 제공합니다. AWS WA Tool은 제품 수명 주기 전반에 걸쳐 다음과 같이 사용자를 지원합니다.

- 의사 결정 문서화 지원

- 모범 사례에 기반하여 워크로드 향상을 위한 권장 사항 제공

- 워크로드를 더 안정적이고 안전하고 효율적이고 비용 효과적으로 만들도록 지도

오늘, 사용자는 AWS WA Tool을 통해 AWS Well-Architected Framework에서 도출한 모범 사례를 사용하여 워크로드를 문서화하고 측정할 수 있습니다. 이러한 모범 사례는 AWS 솔루션스 아키텍트들이 다년간에 걸쳐 다양한 비즈니스를 위한 솔루션을 구축한 경험을 기반으로 개발되었습니다. 이 프레임워크는 아키텍처 측정을 위한 일관된 접근 방식을 제공하며, 시간이 지남에 따라 변화하는 요구에 맞게 규모가 조정되는 설계를 구현하는 지침을 제공합니다.

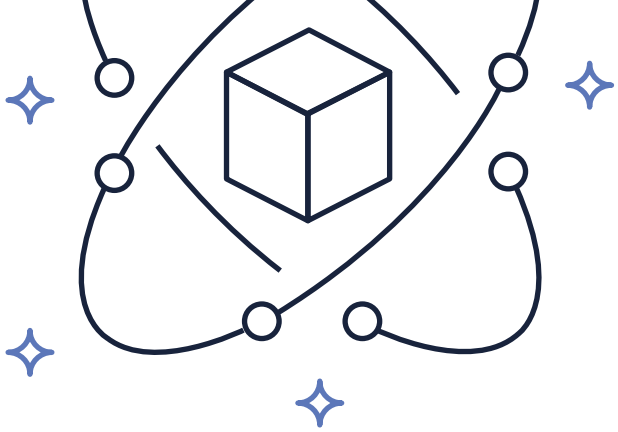
추가 자료:

AWS Well-Architected Framework 개요
aws.amazon.com/architecture/well-architected/

Well-Architected Framework의 보안 원칙
d1.awsstatic.com/whitepapers/architecture/AWS-Security-Pillar.pdf

AWS Well-Architected Tool:
aws.amazon.com/well-architected-tool/

Well-Architected Tool과 함께 시작하기
docs.aws.amazon.com/wellarchitected/latest/userguide/getting-started.html



AWS 보안 모범 사례 확인 자동화: AWS Security Hub의 기본 보안 모범 사례 스탠더드

AWS 기본 보안 모범 사례 스탠더드는 사용자의 배포된 계정 및 리소스가 보안 모범 사례에서 이탈 시 탐지하는 제어 세트입니다. 해당 스탠더드는 사용자가 지속적으로 사용자의 모든 AWS 계정 및 워크로드를 평가하여 모범 사례를 벗어나는 영역을 신속하게 식별하도록 해줍니다. 이는 사용자 조직의 보안 태세를 향상 및 유지하는 방법에 대해 실행 가능하며 규정하는 지침을 제공합니다.

추가 자료:

AWS 기본 보안 모범 사례 스탠더드:
docs.aws.amazon.com/securityhub/latest/userguide/securityhub-standards-fsbp.html

"원격 의료 시장에서 보호된 건강 정보를 다룰 때, 보안이 가장 중요합니다. AWS는 저희가 오늘날 업무를 수행하는 데 있어 가장 중요한 역할을 합니다. 보안 및 규정 준수는 가장 중요한 문제입니다. 이를 갖추지 못했다면, 나머지는 중요하지 않습니다."

- Cory Costley
최고 제품 책임자

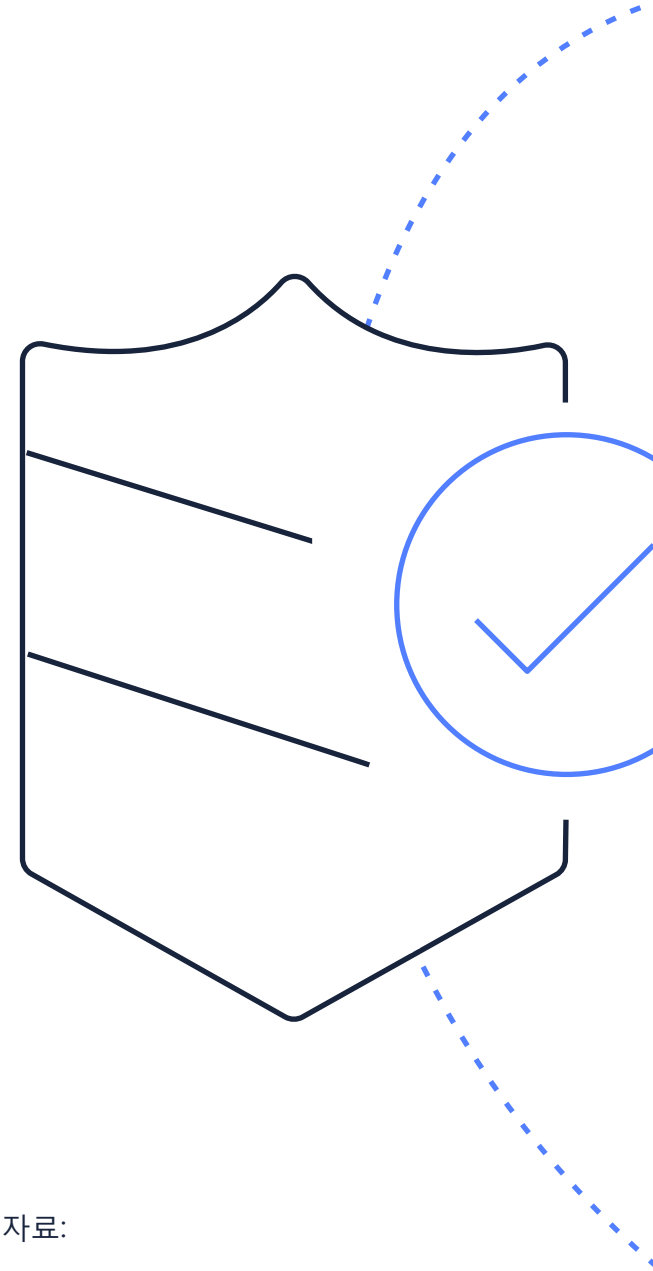
Avizia

추가적인 고객 후기를 당사 웹사이트에서 확인하십시오.
aws.amazon.com/compliance/testimonials/

공급 업체의 영향을 받지 않는 사이버 보안 안내: NIST 사이버보안 프레임워크

사용자의 비즈니스 필요, 규정 준수 의무 및 기술 요건에 따라, 사용자가 공유 보안 책임 모델로 전환함에 따라 사용자의 보안 전략은 변경되기 쉽습니다. 사용자의 보안 프로그램을 중요 인프라 사이버 보안을 위한 NIST 프레임워크(CSF) 등의 업계 프레임워크로 맞추는 작업은 사용자가 비즈니스의 모든 측면에서 보안을 고려했는지 확인하기 위해 권장됩니다. 또한 이를 통해 사람들이 정서적 유대관계를 맺고 있는 기존 솔루션(긍정적 또는 부정적)과 비교하기 보다는, 편향되지 않은 보안 목표를 기반으로 신기술 및 신흥 기술을 평가할 수 있습니다. 이상적으로는, 사용자 조직은 이미 사용자의 조직적 보안 프로그램을 위한 프레임워크를 사용합니다. 하지만 그렇지 않다면, 사용자는 CSF를 고려할 수 있습니다.

하지만 ISO 27001:2013 정보 보안 관리 시스템 및 COBIT 등의 다른 잘 알려진 스탠더드가 있는데도 왜 CSF를 써야 할까요? 사용자가 여기에서 어떤 프레임워크를 적용하든, CSF는 사용자 조직 전반의 사이버 보안 위험을 이해하고 이에 대해 소통하기 위한 무료의, 간단하며 효과적인 방법을 제공합니다. 해당 기술 및 산업의 영향을 받지 않는 접근 방식을 통해 이사회 수준부터 DevSecOps 팀까지 사용자 비즈니스 전반에 걸쳐 사용할 수 있는 공통 분류법을 사용할 수 있습니다. 전체 CSF 방법론을 적용하지 않기로 선택했을지라도, 식별, 보호, 탐지, 대응 및 복원의 다섯 가지 핵심 기능은 쉽게 이해되고, 사용자의 비즈니스에 요구되는 방식으로 다른 스탠더드 또는 제어 요건에 매핑될 수 있습니다. 해당 CSF는 국제적으로, 그리고 산업 전반에 채택됩니다.



추가 자료:

AWS 상의 클라우드 거버넌스 최적화: NIST Cybersecurity Framework, AWS Cloud Adoption Framework 및 AWS Well-Architected 통합
aws.amazon.com/blogs/security/optimizing-cloud-governance-on-aws-integrating-the-nist-cybersecurity-framework-aws-cloud-adoption-framework-and-aws-well-architected/

AWS 클라우드에서 NIST CSF에 맞추기
d1.awsstatic.com/whitepapers/compliance/NIST_Cybersecurity_Framework_CSF.pdf

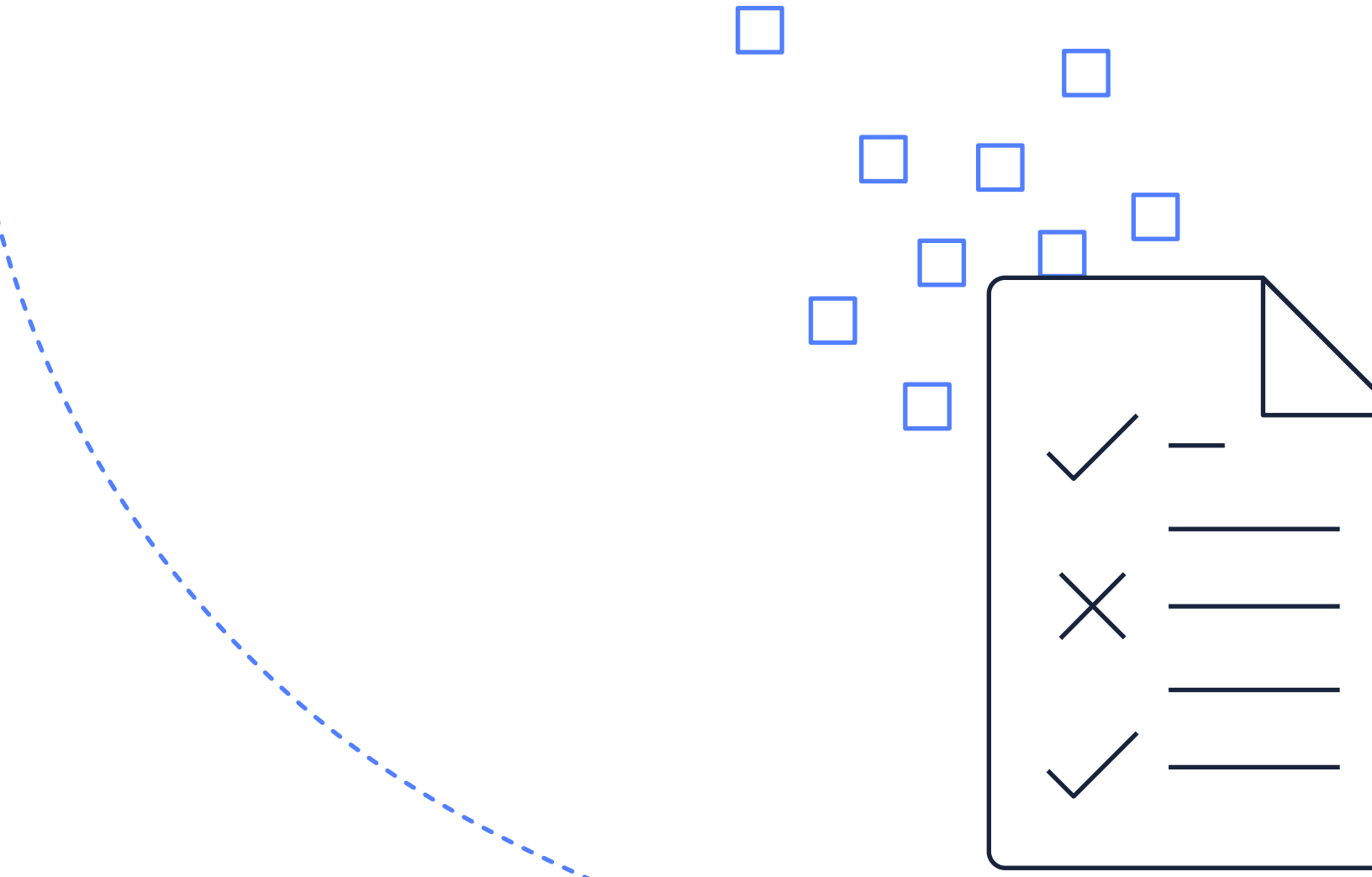
모두 종합하기

조직의 보안에 대한 획일적인 접근 방식은 존재하지 않으며, 단지 기술적 측면에만 국한되지도 않습니다. 사용자 요구 사항 및 비즈니스 컨텍스트를 평가하고, 사용자의 차이와 사이버 보안 위험을 이해하고, 보안 아키텍처에 대해 시도한 실제 사례를 적용하여, 거버넌스에서 운영까지 사용자 조직 사례 전반에 보안이 통합되었는지 확인할 수 있습니다.

서비스별 보안 가이드

각 AWS 서비스에는 보안 가이드가 있으며 당사 AWS 문서 웹사이트에서 이용할 수 있습니다. 이 문서에는 보안 및 규정 준수 목표를 충족하도록 AWS 서비스를 구성하는 방법이 있습니다.

docs.aws.amazon.com/security/



Partners and Marketplace

사용자가 AWS 고객으로서 실현하는 이점 중 하나는 이미 익숙하며, 당사의 AWS 보안 및 규정 준수 서비스와 원활하게 작동하는 광범위한 보안 파트너 및 솔루션 네트워크에 액세스할 수 있다는 점입니다.

당사의 AWS 파트너 네트워크(APN) 솔루션은 자동화, 민첩성, 사용자 워크로드 크기 조정을 지원하며, 필요하고 사용하는 항목에 대해서만 지불합니다. 이미 알고 신뢰하는 보안 적격 파트너의 기술 및 컨설팅 서비스를 사용하여 AWS의 이점을 확장할 수 있습니다. 초기 마이그레이션부터 일상적인 운영까지, 당사의 APN 파트너는 그들의 심도있는 전문성을 활용하여 고객이 클라우드 채택 여정의 모든 단계를 보호할 수 있도록 지원합니다.

보안 중심 솔루션 및 서비스를 귀사의 특정 워크로드 및 사용 사례에 제공하도록 특화된 AWS 보안 적격 파트너를 갖춘 APN 기술 및 컨설팅 파트너의 글로벌 목록에서 선택하십시오. 증가한 민첩성, 자동화, 그리고 APN 파트너 솔루션으로 워크로드의 크기 조정을 통해 혜택을 얻고, AWS Marketplace를 이용해 쉽고 빠르게 검색, 구매, 배포하며, 서비스형 소프트웨어(SaaS) 제품을 포함하는 파트너 클라우드 솔루션을 관리할 수 있습니다.

더 많은 정보를 확인하려면 여기를 방문하십시오. aws.amazon.com/security/partner-solutions 및 aws.amazon.com/marketplace/solutions/security

추가 리소스

AWS 보안 블로그 및 소셜 미디어

다음에서 이용할 수 있는 AWS 보안 블로그를 팔로우하여 AWS Security 서비스 업데이트, 시작 및 혁신적인 솔루션을 최신 상태로 유지하십시오. aws.amazon.com/blogs/security

Twitter 팔로우: twitter.com/awssecurityinfo 및 twitter.com/awsidentity

AWS Training and Certification

이제 막 클라우드를 시작하거나, 기존의 IT 기술 역량을 구축하려고 하거나, 혹은 클라우드 지식을 넓히려는 경우에, AWS 교육은 모든 사용자 수준과 목적에서 맞게 고객의 조직과 직원들의 이해도를 높이고 클라우드를 더 효과적으로 사용할 수 있도록 도움이 됩니다. www.aws.training 방문하기

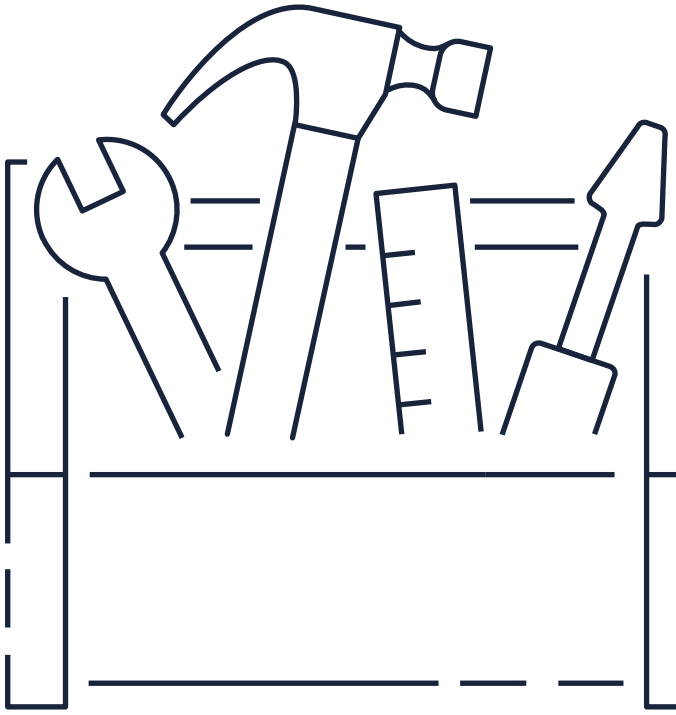
AWS 공인 보안 – 전문 분야는 AWS 워크로드 보안에 최소 2년 이상의 실무 경험을 갖춘 보안 역할을 수행하는 개인을 대상으로 합니다.

방문:
aws.amazon.com/certification/certified-security-specialty

보안, 자격 증명, & 규정 준수 아키텍처 센터

사용자의 보안 및 규정 준수 목표를 AWS 인프라 및 서비스와 문서, 블로그, 비디오, 기타 리소스를 사용하여 충족하는 방식을 학습합니다.

방문:
aws.amazon.com/architecture/security-identity-compliance



AWS Cloud Audit Academy

Cloud Audit Academy(CAA)는 감사, 위험 및 규정 준수 역할을 하고, 클라우드 내 규정된 워크로드 평가에 관련된 사용자를 위해 설계되었습니다. CAA 커리큘럼은 광범위하게(클라우드 및 산업의 영향을 받지 않음) 시작하여 학습자가 AWS 및 산업별 콘텐츠를 진행하며 범위를 좁히는 수준별 학습 경로로 구성됩니다.

방문: aws.amazon.com/compliance/auditor-learning-path

AWS Security Fundamentals

AWS 액세스 제어, 데이터 암호화 방법 및 AWS 인프라에 대한 네트워크 액세스 보안 방법과 같은 AWS 클라우드 보안 개념의 기본 측면을 학습하는 무료 자체 학습 과정입니다. AWS 클라우드의 고객 보안 책임을 다루며, 또한 이용 가능한 다른 보안 지향 서비스도 다룹니다.

방문:
aws.amazon.com/training/course-descriptions/security-fundamentals

AWS Professional Services

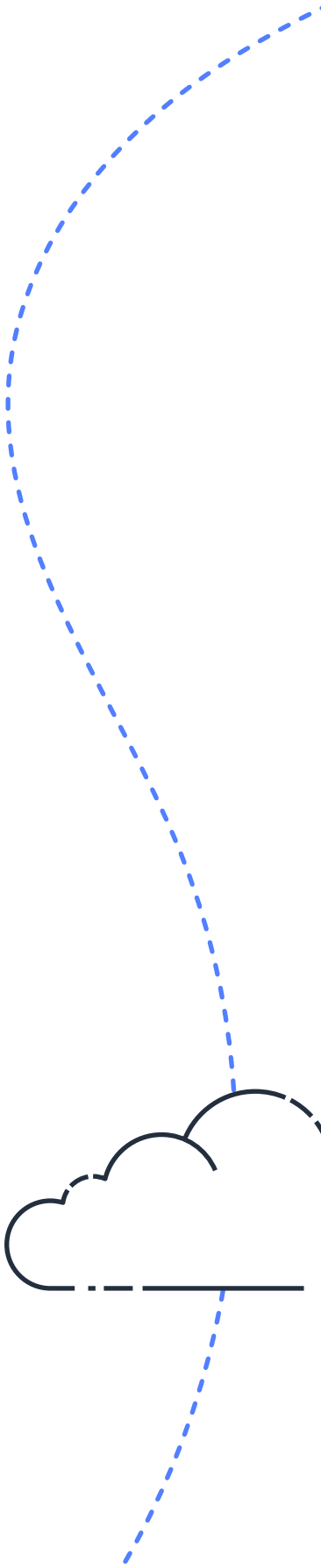
AWS Professional Services 조직은 AWS 클라우드를 사용 시 원하는 비즈니스 결과를 실현할 수 있도록 지원하는 글로벌 전문가 팀입니다. 이 팀은 당사의 글로벌 전문 분야 사례를 통해 집중 가이드를 제공하며, 이 가이드는 다양한 솔루션, 기술 및 산업을 다룹니다. 고객의 클라우드 마이그레이션 여정을 지원하고, AWS 및 업계 모범 사례에 따라 기존 계정 및 워크로드를 보호하는 데 도움이 되는 다양한 보안 중심의 제품 및 서비스를 사용할 수 있습니다.

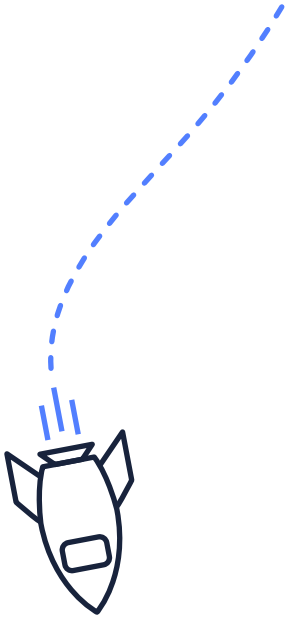
방문: aws.amazon.com/professional-services/

AWS Well-Architected Security Labs

보안 랩은 핸즈온랩 형식의 문서 및 코드로 사용자가 구조적 모범 사례를 사용하여 학습, 측정 및 구축하도록 지원합니다. 랩은 100은 입문, 200/300은 중급, 400은 고급 수준으로 범주화됩니다.

방문: wellarchitectedlabs.com/security





AWS 보안 및 규정 준수 빠른 참조 가이드
검토에 시간을 내주셔서 감사합니다.

보다 자세한 정보는 AWS 보안 및 규정 준수 웹사이트에서 확인할 수 있습니다.
aws.amazon.com/security/

그리고 당사의 보안 서비스에 대한 정보는 여기에서 확인할 수 있습니다.
aws.amazon.com/products/security/