AWS 보안

클라우드 비즈니스 혁신 보안 모범 사례

목차

고지 사항

서문

클라우드로 이전하면 비즈니스 프로세스, 서비스, 비용 구조 및 규모가 혁신적으로 변합니다. 그리고 보안 방식의 현대화도 필요합니다. 이번 기회에 자체 관리형 온프레미스 보안 및 보증 기술을 완전관리형 서비스 아키텍처로 이전하세요. 그러면 새로운 비즈니스 혁신 아키텍처로 지원 및 확장이 가능해질 것입니다.

조직은 수천 개에 달하는 서드 파티 글로벌 검증 규정 준수 요구 사항을 충족해야 합니다. AWS는 클라우드에서 확장과 보안 작업 자동화를 지원하고 보안 및 규정 준수 책임을 공유하기에 이러한 요구 사항 충족에 도움이 됩니다. 보안 자동화 단계를 구축하면 사람이 직접 구성할 때 발생하는 오류가 감소하고 비즈니스에 중요한 다른 작업에 집중할 수 있는 시간 여유가 생깁니다.

이 eBook의 이점

최고 정보 보안 책임자(CISO) 및 IT 보안 리더와 같은 보안 임원에게 도움이 되는 eBook입니다. 이 eBook을 통해 AWS가 AWS 클라우드 서비스가 실행되는 인프라를 어떻게 보호하는지 알아보세요. 현재 사용하시는 클라우드의 보안 및 보안 서비스에 대한 자신의 역할과 책임을 잘 이해할 수 있을 것입니다.

"데이터 보안 및 재해 복구로 명성이 높은 AWS 덕분에 데이터 센터 외부에 데이터가 안전하게 저장된다는 사실을 쉽게 납득하게 되었습니 다."[1]

Roland Chang, Wesurance Business Development Strategist

"AWS를 선택한 이유는 데이터 보호 표준을 지원하고 필요한 확장성을 제공하기 때문입니다."[2]

Benjamin Sauer, Climedo Head of Health Backend Engineering

1 "**Wesurance Drives Transformation for Insurers with Innovative Digital Solutions on AWS**", 2021년 AWS 사례 연구
2 "**Climedo Health Captures Patient-centric, Compliant, and Secure Clinical Data Using AWS**", 2022년 AWS 사례 연구

AWS의 클라우드 보안

AWS는 현재 사용 가능한 가장 유연하고 안전한 클라우드 컴퓨팅 환경으로 설계되어 있으므로 사용자는 환경을 제어하여 레거시 인프라의 제어 기능을 충족하거나 초과할 수 있습니다. AWS는 인프라 및 애플리케이션 변경 사항의 규정 준수, 보증 및 모니터링을 위한 도구 및 지원을 제공합니다. 또한 수동 보안 검토 없이 보안 기준을 보장하고 혁신을 가능하게 하는 가드레일 생성을 지원함으로써 시간을 절약해 줍니다. 그 결과 보안 기준 위반이나 이상 징후 발생 시 사고에 자동 대응이 이루어져 보안 및 IT 팀은 보안이 아닌 조직의 핵심 비즈니스에 집중할 수 있습니다.

AWS 클라우드 보안의 3가지 이점

1 현존하는 가장 안전한 클라우드 컴퓨팅 환경 인프라에서 애플리케이션을 구축, 실행 및 확장하세요. 정부, 금융 서비스, 의료 등 보안이 매우 중요한 민감한 조직의 요구 사항을 충족하도록 구축된 클라우드 및 네트워크 아키텍처의 이점을 누릴 수 있습니다.

2 조직의 모든 부분에 보안을 자신 있게 통합하고 자동화하여 안전하고 신속하게 실행하세요. AWS는 인프라 및 애플리케이션 보안 검사를 자동화하는 조직 차원의 제어 기능을 제공하여 보안 및 규정 준수 제어 조치를 지속적으로 시행합니다. 그러면 고객은 자동 추론 도구를 구현하여 최고 수준의 보안을 수학적으로 증명할 수 있습니다.

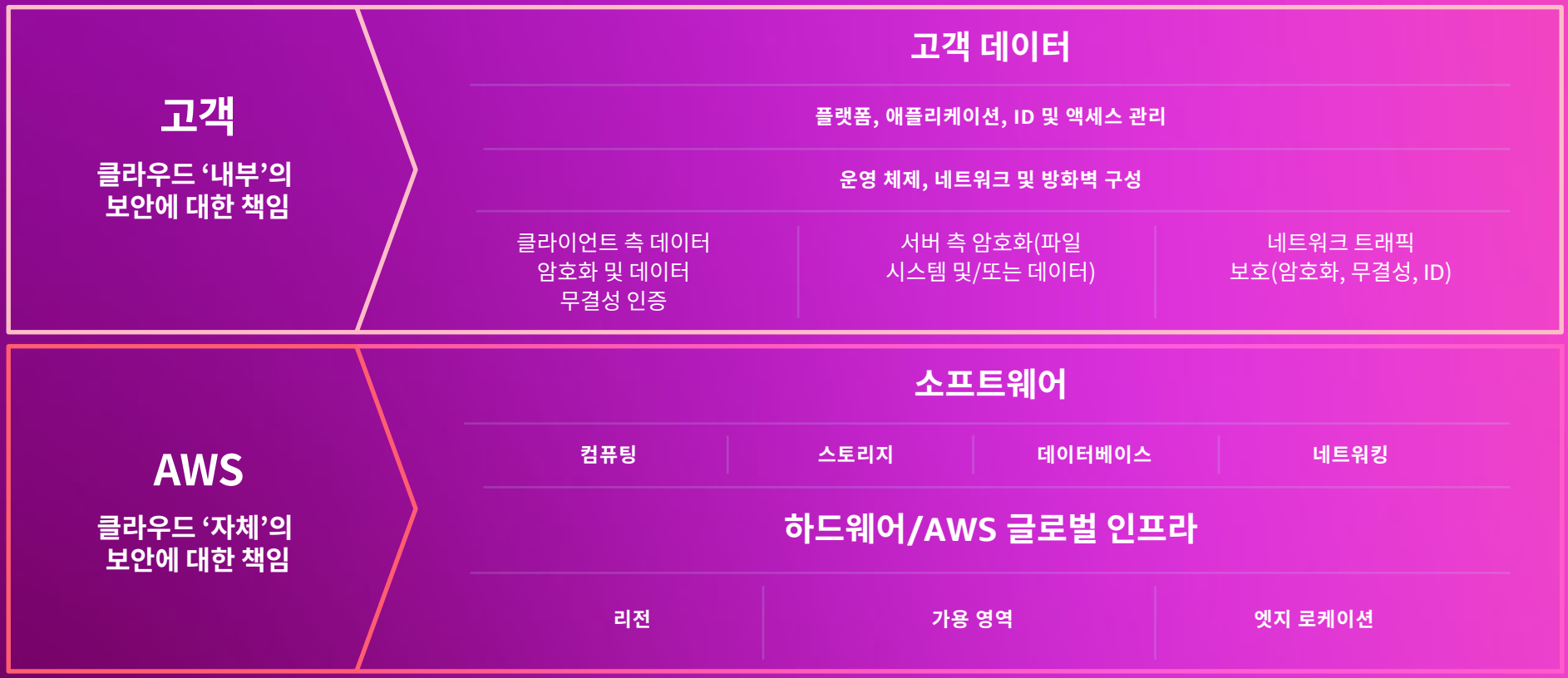
3 조직의 엔드 투 엔드 보안을 달성하는 데 도움이 되는 광범위한 보안 서비스 및 파트너 솔루션 포트폴리오를 통해 혁신하세요. AWS 보안 서비스 및 솔루션은 고객이 위험 식별부터 해결까지 최적 보안 태세의 모든 단계를 구현할 수 있도록 지원합니다. 고객은 AWS Professional Services와 AWS 파트너 네트워크의 보안 기술 및 컨설팅 서비스를 사용하여 AWS의 이점을 더 폭넓게 누릴 수 있습니다.

최고의 기준

AWS 팀은 콘텐츠의 지속적 보호를 지원하기 위해 시스템을 연중무휴로 꾸준히 모니터링합니다.

클라우드 보안 - 공동 책임

고객이 IT 인프라를 AWS로 이전할 때 공동 책임 모델을 수락하게 됩니다. 이 공동 책임 모델에서는 AWS가 호스트 운영 체제 및 가상화 계층에서 서비스가 운영되는 시설의 물리적 보안에 이르는 IT 구성 요소 계층을 운영, 관리 및 제어하므로 고객의 운영 부담 감소 등의 여러 이점을 제공합니다. 고객은 IT 환경 운영에 대한 책임과 더불어 IT 제어의 관리, 운영 및 검증 책임도 AWS와 공유하게 됩니다.



AWS - 클라우드 보안

AWS는 AWS에서 제공하는 모든 서비스가 실행되는 인프라를 보호할 책임이 있습니다. AWS 인프라는 AWS 서비스를 실행하는 하드웨어, 소프트웨어, 네트워킹 및 시설로 구성됩니다. 호스트 운영 체제부터 시설의 물리적 보안에 이르기까지 조직의 운영 부담을 줄여줍니다. 정보, ID, 애플리케이션 및 장치가 보호된다는 사실을 알기에 마음이 편안합니다.

AWS 보안 감사

최고의 클라우드 제공업체인 AWS는 널리 알려진 기존 **프레임워크 및 프로그램**을 통해 포괄적인 규정 준수 제어 기능을 제공합니다. 전 세계 규제 기관의 규정 준수 요구 사항 충족을 지원하는 제어 기능이 고객에게 자동 제공됩니다. 그 결과, 고객의 보안 감사 비용이 획기적으로 감소할 뿐만 아니라 고객의 사내 규정 준수 및 인증 프로그램도 강화됩니다.

전 세계적으로 확산된 AWS IT 제어 환경 및 시설의 효율성과 효과적인 운영은 서드 파티 독립 평가를 통해 검증합니다. AWS 전체 제어 환경의 여러 측면과 관련된 정책, 프로세스 및 제어 활동도 검증을 받습니다.

개인 정보 보호

개인 정보 보호는 주로 데이터 액세스 권한을 부여받는 사람을 제어하는 것입니다. AWS를 사용하면 누가 콘텐츠에 액세스하고 있으며 조직이 특정 시점에 어떤 리소스를 사용 중인지 파악할 수 있습니다. 항상 리소스에 대한 적절한 수준의 액세스를 부여하세요. 정보가 저장된 위치에 관계없이 세분화된 ID 및 지속적인 모니터링을 활용하여 거의 실시간에 가까운 보안 정보를 제공하시기 바랍니다.

시스템 전체에서 구성 변경 및 보안 이벤트를 감지하는 AWS의 활동 모니터링 서비스를 사용하여 위험을 줄이고 성장을 지원하세요. 기존 솔루션에 AWS 서비스를 통합하여 운영 및 규정 준수 보고를 단순화하시기 바랍니다. AWS는 조직에 적용되는 지역 및 현지 개인 정보 보호법과 규정의 준수를 지원하는 제어 기능을 제공합니다.

규정 준수 제어

AWS는 다음을 비롯한 143가지 보안과 규정 준수 인증을 지원합니다.

SOC	DoD CC SRG	C5	HITRUST CSF
PCI	HIPAA BAA	K-ISMS	FINMA
ISMAP	IRAP	ENS High	GSMA
FedRAMP	MTCS	OSPAR	PiTuKri

데이터 상주

AWS 데이터 센터는 전 세계 다양한 위치에서 클러스터 형태로 구축되며, AWS 리전이라고 부릅니다. 사용자는 고객의 콘텐츠가 저장될 AWS 리전을 직접 선택합니다. 특정 지리적 요구 사항에 따라 선택한 위치에 AWS 서비스를 배포하여 규정 준수 및 데이터 상주 요구 사항을 충족합니다. 예를 들어, 데이터를 호주에만 저장하려는 호주 지역 AWS 고객의 경우 아시아 태평양(시드니) AWS 리전만을 AWS 서비스 배포 지역으로 선택할 수 있습니다. **전 세계**의 기타 유연한 스토리지 옵션을 알아보세요.

비즈니스 연속성

AWS 인프라는 높은 수준의 가용성을 제공하며 복원력이 높은 IT 아키텍처를 배포하는 데 필요한 기능을 제공합니다. AWS 시스템은 시스템 또는 하드웨어 장애 발생 시에도 고객에게 미치는 영향을 최소화하면서 원활하게 작동하도록 설계되었습니다.

재해 복구

애플리케이션을 여러 AWS 가용 영역에 분산하면 자연 재해나 시스템 장애를 비롯한 대부분의 장애 모드에서도 복원력을 유지할 수 있습니다. **AWS Elastic Disaster Recovery**는 저렴한 스토리지, 최소 컴퓨팅, 특정 시점 복구를 사용하여 온프레미스 및 클라우드 기반 애플리케이션을 빠르고 안정적으로 복구하여 가동 중단 시간 및 데이터 손실을 최소화합니다.

"AWS를 사용하면 모든 민감한 데이터가 분할되고, 제어되고, 암호화됩니다. 데이터에 문제가 생겨도 아키텍처의 익명화, 토큰화, 암호화 설계로 데이터가 유출되지 않습니다."[3]

Bryan Carroll, TNEX CEO 겸 공동 창립자

3 "**TNEX Launches Vietnam's First Digital Bank in Nine Months on AWS**", 2021년 AWS 사례 연구

고객 - 클라우드의 보안

클라우드 보안과 관련해서 힘들고 어려운 일은 AWS에서 주로 처리하지만, 게스트 운영 체제 및 관련 애플리케이션 소프트웨어 관리를 포함한 클라우드 보안 책임은 고객에게 있습니다.

AWS 리소스를 안전하게 관리하는 방법

사용하는 서비스, 서비스의 IT 환경 통합, 관련 법과 규제에 따라 책임 범위가 다릅니다. AWS 서비스를 선택할 때 이 모든 것을 고려해야 합니다. AWS는 기업의 보안 및 규정 준수 요구 사항을 충족하도록 환경의 보안 태세를 높이는 데 도움이 되는 다양한 수준의 지원을 제공합니다. 사용 가능한 도구 및 서비스에는 문서화된 모범 사례, 전문 서비스, 보안 및 규정 준수 태세 확인을 자동화하는 솔루션 등이 있습니다.

AWS 보안 및 ID 서비스의 이점

클라우드에서 보안을 구축하는 데 도움이 되도록 AWS는 고객의 자체 보안 및 규정 요구 사항을 충족하는 다양한 혁신적인 보안 서비스를 제공합니다.

ID 서비스

ID 관리, 액세스 제어 및 거버넌스는 규모에 상관없이 모든 유형의 조직을 위한 기본 보안의 기반입니다. AWS를 통해 보안 팀과 IT 팀은 현대적 클라우드 중심 ID 솔루션과 제로 트러스트 아키텍처를 채택하여 하이브리드 인력을 안전하게 지원하고, 액세스 경험을 개선하며, 권한을 관리하고, 엄격한 규정 준수 의무를 충족할 수 있습니다.

데이터 보호 및 개인정보

AWS는 데이터 보호에 필요한 **기술적, 운영적, 계약적 조치**를 제공합니다. AWS를 통해 데이터의 개인정보 보호 기능을 관리하고, 데이터가 사용되는 방식, 데이터에 액세스할 수 있는 사람, 암호화하는 방법을 제어할 수 있습니다. AWS는 현존하는 가장 유연하고 안전한 클라우드 컴퓨팅 환경에서 이렇게 다양한 기능을 지원합니다.

네트워크 보호

AWS의 네트워크 및 애플리케이션 보호 서비스를 사용하면 조직 전체의 모든 네트워크 제어 지점에서 세분화된 보안 정책을 시행할 수 있습니다. AWS 네트워크 및 애플리케이션 보호 서비스는 트래픽을 검사하고 필터링하여 무단 리소스 액세스를 방지하는 유연성이 뛰어난 솔루션을 제공합니다.

탐지 및 대응

AWS 탐지 및 대응 서비스는 함께 작동하여 개발 수명 주기 초기에 보안 사례를 적용하면서 보안 위험을 지속적으로 식별하고 우선순위를 지정하여 전체 AWS 환경에서 보안 태세를 강화하고 보안 운영을 간소화하도록 지원합니다.

규정 준수

AWS의 규정 준수 및 데이터 개인 정보는 규정 준수 상태에 대한 종합적인 가시성을 제공하며, 관련 산업 표준과 AWS 모범 사례를 기반으로 하는 자동화된 규정 준수 검사를 사용하여 지속적으로 환경을 모니터링합니다.

AWS Cloud Adoption Framework - 보안 관점

성공적이고 안전한 클라우드 도입 여정은 **AWS Cloud Adoption Framework (AWS CAF)**에서 AWS 경험과 모범 사례를 사용하는 것부터 시작합니다. 보안 관점에서 이 프레임워크는 향상된 보안 기능과 복원력 높은 워크로드를 구축하는 모범 사례를 제공합니다. 보안 준비 상태를 식별하여 우선 순위를 지정하고 데이터 및 워크로드의 기밀성, 무결성 및 가용성을 달성하는 데 도움이 되는 9개 기능을 소개합니다. CISO, 최고 커머셜 책임자(CCO), 내부 감사 리더, 보안 아키텍트와 엔지니어 등이 공통 이해 관계자입니다.

AWS Cloud Adoption Framework의 9가지 기능

1. 보안 거버넌스
2. 보안 감사
3. ID 및 액세스 관리
4. 위협 탐지 및 모니터링
5. 취약성 관리
6. 인프라 보호
7. 데이터 보호
8. 애플리케이션 보안
9. 사고 대응

1 보안 거버넌스

효과적인 보안 프로그램을 구현하려면 보안 역할, 책임, 책임성, 정책, 프로세스 및 절차를 비롯한 특정 항목을 정의, 개발, 유지 관리 및 전달해야 합니다. 책임성을 명확하게 정의해야 보안 프로그램이 더욱 효과를 발휘합니다.

2 보안 감사

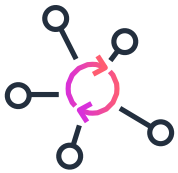
보안 프로그램의 효과를 높이려면 지속적인 모니터링, 평가 및 관리가 중요합니다. 보안 제어에 대한 신뢰와 확신이 생기면 규제 요구 사항을 효과적으로 충족할 수 있습니다.

3 ID 및 액세스 관리

AWS에서 실행하는 워크로드가 계속해서 확장되면서 적절한 사람들이 적절한 조건에서 적절한 리소스에 액세스할 수 있도록 하는 것이 중요합니다. ID 및 액세스 관리는 안전한 AWS 워크로드 운영에서 핵심적인 역할을 수행합니다. 사람 ID와 기계 ID에 인증과 권한을 부여해야 합니다. 권한 관리를 통해 최소 권한의 기능으로 광범위하고 세분화된 액세스를 제공할 수 있습니다.

4 위협 탐지 및 모니터링

위협 탐지는 환경을 지속적으로 모니터링하여 사용 중인 자산 및 리소스의 정상적이고 합법적인 동작을 식별하는 데 필요합니다. 기계 학습, 이상 탐지, 자동화된 모범 사례 검사, 잠재적인 구성 오류, 잘못된 행동 또는 무단 사용에 대한 지능적인 취약성 관리와 같은 기술을 사용하면 신속하게 판단하고 전달함으로써 해결 시간을 단축할 수 있습니다.



5 취약성 관리

서버 및 컨테이너 워크로드에서 광범위하고 동적인 소프트웨어와 소프트웨어 버전 세트를 사용할 수 있습니다. 새로운 소프트웨어 취약성이 정기적으로 발표됩니다. 취약성 관리는 신속하게 잠재적 노출을 자동 식별하고 우선 순위를 지정하여 수정 작업에서 중요한 역할을 합니다.

6 인프라 보호

클라우드에서 성공적으로 운영하고 모범 사례 및 규제 의무를 충족하기 위해서는 제어 방법이 매우 중요합니다. 정보 보안 프로그램의 핵심은 워크로드 내의 시스템과 서비스를 의도하지 않은 무단 침입 및 잠재적 취약성으로부터 지키는 것입니다.

7 데이터 보호

워크로드를 설계하려면 먼저 보안과 관련된 기본 사례부터 마련해야 합니다. 기본 보안 사례는 잘못된 관리 예방이나 규제 의무 준수 같은 목표를 지원하는 데 큰 도움이 됩니다. 모든 데이터는 저장 및 전송 중에 암호화되고 민감한 데이터는 별도 계정에 저장되어 위험과 취약성을 줄여야 합니다.

8 애플리케이션 보안

소프트웨어 개발 프로세스 중에 보안 결함이 식별되는 경우, 보안을 최우선으로 고려하여 시간, 노력 및 비용을 절약합니다. 애플리케이션 개발 단계에서 보안 정책을 마련하면 보안 격차가 최소화되어 안심할 수 있습니다.

9 사고 대응

보안 사고의 잠재적 영향에 대응하고 완화하기 위해서는 준비가 중요합니다. 비즈니스 중단을 최소화하고 사고 발생 시 문제 격리, 억제 및 포렌식 수행과 같은 작업을 효과적으로 운영하려면 보안 사고가 일어나기 전에 적절한 도구 및 제어 기능을 마련해야 합니다.

AWS 마이그레이션 전략 수립

성공적이고 안전한 클라우드 도입 여정을 계획하거나 AWS에서 기존 워크로드를 재작업할 때 강력한 보안 기반을 구축하는 데 도움이 되며 업계의 인정을 받는 표준과 프레임워크가 있습니다.

AWS Cloud Adoption Framework는 성공적이고 안전한 클라우드 마이그레이션 계획을 지원하여 IT 거버넌스 및 보안 관리 시스템 구축에 도움이 됩니다. AWS Well-Architected Framework는 보안 인프라 구축을 지원하는 동시에 AWS 보안 모범 사례에 대한 자동화된 검사를 통해 보안 AWS 계정의 보안을 지속적으로 평가할 수 있습니다.

AWS Well-Architected Framework

AWS Well-Architected Framework는 클라우드 아키텍트가 워크로드 수준에 집중하여 다양한 애플리케이션과 워크로드를 위한 안전하고 성능이 뛰어나고 복원력이 높고 효율적인 인프라를 구축할 수 있도록 도와주는 도구입니다. 이 프레임워크의 보안 원칙은 다음과 같은 5가지 요소로 구성됩니다.

- ID 및 액세스 관리
- 탐지
- 인프라 보호
- 데이터 보호
- 사고 대응

AWS Well-Architected Framework는 올바른 AWS 서비스를 선택하는 방법과 안전한 구현 지침을 제공하고 워크로드에서 이러한 핵심 보안 사례를 구현하는 데 도움을 줍니다.

AWS 보안 모범 사례에 대한 자동 검사: AWS Security Hub

조직의 보안 태세를 유지하려면 배포된 계정과 리소스에서 보안 모범 사례 위반이 발생할 때 감지할 수 있어야 합니다. **AWS 기초 보안 모범 사례 표준**은 일련의 제어 기능을 활용하여 모든 AWS 계정과 워크로드를 지속적으로 평가하고 클라우드 보안을 지속적으로 개선하기 위한 실행 가능하고 규범적인 지침을 제공합니다.

자세히 알아보기

클라우드에서 워크로드 보안 시작하기

AWS의 보안, ID 및 규정 준수를 통해 클라우드로 안전하게 이전하는 방법을 자세히 알아봅니다.

자세히 알아보기 ›

보안 콘텐츠 액세스

AWS Security Hub에서 AWS의 보안 및 고객 관련 제품 콘텐츠를 자세히 알아봅니다. 다양한 보안 주제를 다루는 유용한 웨비나, 백서, 빠른 참조 가이드 및 eBook을 확인합니다.

자세히 알아보기 ›