AWS 백서

AWS에서 GDPR 규정 준수 탐색

AWS에서 GDPR 규정 준수 탐색: AWS 백서

Table of Contents

AWS에서 GDPR 규정 준수 탐색

게시 날짜: 2020년 12월(문서 개정)

요약

이 문서에서는 Amazon Web Services(AWS)가 고객에게 제공하는 서비스와 리소스에 대한 정보를 제공하여 고객이 자신의 활동에 적용될 수 있는 일반 데이터 보호 규정(GDPR)의 요구 사항을 준수할 수 있도록 지원합니다. 여기에는 IT 보안 표준 준수, AWS C5(Cloud Computing Compliance Controls Catalog) 증명, CISPE(Cloud Infrastructure Services Providers in Europe) 행동 강령 준수, 데이터 액세스 제어, 모니터링 및 로깅 도구, 암호화, 키 관리가 포함됩니다.

일반 데이터 보호 규정 개요

일반 데이터 보호 규정(GDPR)은 2018년 5월 25일부터 시행된 유럽 개인 정보 보호법(2016년 4월 27일 유럽 의회 및 유럽 이사회 규정 2016/679)입니다. GDPR은 EU 데이터 보호 지침(Directive 95/46/EC)을 대체하며, 각 EU 회원국에 구속력이 있는 단일 데이터 보호법을 적용하여 유럽 연합(EU) 전체에서 데이터 보호법을 통합하기 위해 시행됩니다.

GDPR은 EU에 설립되어 있는 조직 또는 EU에서 개인에게 상품이나 서비스를 제공하거나 EU에서 EU 거주자의 행동을 모니터링 할 때 EU 거주자의 개인 데이터를 처리하는 조직의 모든 개인 데이터 처리에 적용됩니다. 개인 데이터는 식별된 또는 식별 가능한 자연인과 관련된 모든 정보입니다.

GDPR에 따라 EU에서 운영하는 조직에 도입되는 변경

GDPR의 핵심 측면 중 하나는 EU 회원국 전체에서 개인 데이터를 안전하게 처리, 사용 및 교환하는 방식에 일관성이 생긴다는 것입니다. 조직은 개인 데이터 처리에 적용되는 규정 준수 정책뿐 아니라 기술적 및 조직적 조치를 구현하고 정기적으로 검토하여 처리 중인 데이터의 보안과 GDPR 준수를 지속적으로 입증해야 합니다. EU 감독 기관은 GDPR 위반에 대해 최대 2천만 유로 또는 전 세계 연간 매출액의 4%(둘 중 더 높은 금액)에 해당하는 벌금을 부과할 수 있습니다.

GDPR을 위한 AWS의 준비

AWS 규정 준수, 데이터 보호 및 보안 전문가는 전 세계 고객과 협력하여 질문에 답하고 고객이 GDPR에 따라 클라우드에서 워크로드를 실행하기 위해 준비할 수 있도록 지원합니다. 또한 이러한 팀은 GDPR의 요구 사항에 대한 AWS의 준비 상태를 검토합니다.

> **Note**
>
> AWS는 GDPR 규정을 준수하면서 모든 AWS 서비스를 사용할 수 있도록 보장합니다.

AWS 데이터 처리 부칙(DPA)

AWS는 고객이 GDPR에 따른 계약 의무를 준수할 수 있도록 GDPR 준수 데이터 처리 부칙(GDPR DPA)을 제공합니다. AWS GDPR DPA는 AWS 서비스 약관에 통합되어 있으며 GDPR을 준수하기 위해 DPA가 필요한 전 세계 모든 고객에게 자동으로 적용됩니다.

2020년 7월 16일, 유럽 연합 사법 재판소(CJEU)는 일명 “모델 조항”인 EU-US 프라이버시 실드 및 표준 계약 조항(SCC)에 관한 판결을 내렸습니다. CJEU는 EU-US 프라이버시 실드가 유럽 연합(EU)에서 미국(US)으로 개인 데이터를 전송하는 데 더 이상 유효하지 않다고 판결했습니다. 그러나 동일한 판결에서 CJEU는 기업이 EU 외부로 데이터를 전송하기 위한 메커니즘으로 SCC를 계속 사용할 수 있다고 확인했습니다.

이 판결에 따라 AWS 고객과 파트너는 일반 데이터 보호 규정(GDPR)을 포함한 EU 데이터 보호법에 따라 계속해서 AWS를 사용하여 유럽에서 미국 및 기타 국가로 콘텐츠를 전송할 수 있습니다. AWS 고객은 GDPR 규정을 준수하여 유럽 연합 외부로 데이터를 전송하기로 할 경우 AWS 데이터 처리 부칙(DPA)에 포함된 SCC를 이용할 수 있습니다. 규제 및 법률 환경이 진화함에 따라 AWS는 고객이 사업을 운영하는 모든 장소에서 AWS의 이점을 지속적으로 활용할 수 있도록 보장하기 위해 노력할 것입니다. 자세한 내용은 EU-US 프라이버시 실드 FAQ를 참조하세요.

GDPR에 따른 AWS의 역할

AWS는 GDPR에 따라 데이터 프로세서와 데이터 컨트롤러의 역할을 모두 수행합니다.

제32조에 따라 컨트롤러와 프로세서는 “자연인의 권리와 자유에 대해 다양한 가능성과 심각도를 나타내는 위험뿐 아니라 구현의 최신 상태 및 비용과 처리의 성격, 범위, 맥락 및 목적”을 고려하는 “...적절한 기술적 및 조직적 조치를 구현”해야 합니다. GDPR은 다음을 포함하여 어떤 유형의 보안 조치가 필요할 수 있는지에 대한 구체적인 제안을 제공합니다.

- 개인 데이터의 가명 처리 및 암호화
- 처리 시스템과 서비스의 지속적인 기밀성, 무결성, 가용성, 복원력을 보장할 수 있는 기능
- 물리적 또는 기술적 사고가 발생할 경우 개인 데이터의 가용성과 액세스 권한을 시기 적절하게 복원할 수 있는 기능
- 처리의 보안을 보장할 수 있도록 기술적 및 조직적 조치의 효과를 정기적으로 테스트, 검사 및 평가하는 프로세스

데이터 프로세서로서의 AWS

고객 및 AWS 파트너 네트워크(APN) 파트너가 AWS 서비스를 사용하여 자체 콘텐츠의 개인 데이터를 처리할 때 AWS는 데이터 프로세서 역할을 합니다. 고객 및 APN 파트너는 AWS 서비스에서 제공하는 제어 기능(보안 구성 제어 기능 포함)을 사용하여 개인 데이터를 처리할 수 있습니다. 이러한 상황에서 고객 또는 APN 파트너는 데이터 컨트롤러 또는 데이터 프로세서 역할을 하고, AWS는 데이터 프로세서 또는 하위 프로세서 역할을 할 수 있습니다. AWS GDPR 준수 데이터 처리 부칙(DPA)에는 데이터 프로세서로서 AWS의 약정이 통합되어 있습니다.

데이터 컨트롤러로서의 AWS

AWS가 개인 데이터를 수집하고 해당 개인 데이터를 처리하는 목적과 수단을 결정할 때 AWS는 데이터 컨트롤러 역할을 합니다. 예를 들어 AWS가 계정 등록, 관리, 서비스 액세스를 위해 계정 정보를 처리하거나 고객 지원 활동을 통해 지원을 제공하기 위해 AWS 계정의 연락처 정보를 처리하는 경우 AWS는 데이터 컨트롤러 역할을 합니다.

공동 보안 책임 모델

보안 및 규정 준수는 AWS와 고객의 공동 책임입니다. 고객이 컴퓨터 시스템과 데이터를 클라우드로 이동하면 고객과 클라우드 서비스 공급자 간에 보안 책임이 공유됩니다. 고객이 AWS 클라우드로 이동하면 AWS는 AWS 클라우드에 제공된 모든 서비스를 실행하는 글로벌 인프라를 보호할 책임이 있습니다. Amazon S3 및 Amazon DynamoDB와 같은 추상화된 서비스의 경우 AWS는 운영 체제와 플랫폼의 보안에 대해서도 책임이 있습니다. 데이터 컨트롤러 또는 데이터 프로세서 역할을 하는 고객 및 APN 파트너는 클라우드에 입력하거나 클라우드에 연결하는 모든 것에 대해 책임이 있습니다. 이러한 책임 구별을 일반적으로 클라우드 자체의 보안과 클라우드 내부의 보안이라고 합니다. 이 공유 모델은 고객의 운영 부담을 줄이고 AWS 클라우드에 인프라를 배포하는 데 필요한 유연성과 제어 기능을 제공할 수 있습니다. 자세한 내용은 AWS 공동 책임 모델을 참조하세요.

GDPR에 따라 AWS 공동 책임 모델이 변경되는 것은 아니며, 이 모델은 클라우드 컴퓨팅 서비스 사용에 중점을 두고 있는 고객 및 APN 파트너에게 관련됩니다. 공동 책임 모델은 GDPR에 따라 AWS(데이터 프로세서 또는 하위 프로세서 역할)와 고객 또는 APN 파트너(데이터 컨트롤러 또는 데이터 프로세서 역할)의 서로 다른 책임을 설명하는 유용한 접근 방식입니다.

강력한 규정 준수 프레임워크 및 보안 표준

GDPR에 따르면 적절한 기술적 및 조직적 조치에는 “처리 시스템과 서비스의 지속적인 기밀성, 무결성, 가용성 및 복원력을 보장할 수 있는 기능”뿐 아니라 신뢰할 수 있는 복원, 테스트 및 전체적인 위험 관리 프로세스가 포함되어야 할 수 있습니다.

AWS 규정 준수 프로그램

AWS는 전 세계 모든 리전에서 보안 및 규정 준수에 대한 높은 기준을 계속 유지하고 있습니다. AWS에서는 언제나 보안을 최우선으로 생각하고 있습니다. 보안은 진정한 '0순위'입니다. AWS는 제어 활동이 의도한 대로 운영되고 있음을 증명하기 위해 정기적으로 독립적인 서드 파티 증명 감사를 거칩니다. 더 구체적으로 말하면, AWS는 리전과 산업에 따라 다양한 글로벌 및 지역 보안 프레임워크에 대해 감사를 받습니다. 현재 AWS는 50개 이상의 다양한 감사 프로그램에 참여하고 있습니다.

이러한 감사 결과는 평가 기관에서 문서화하며 AWS Artifact를 통해 모든 AWS 고객에게 제공됩니다. AWS Artifact는 AWS 규정 준수 보고서에 온디맨드로 액세스할 수 있는 무료 셀프 서비스 포털입니다. 새 보고서가 릴리스되면 AWS Artifact에서 사용할 수 있으므로 고객은 새 보고서에 즉시 액세스하여 AWS의 보안 및 규정 준수를 지속적으로 모니터링할 수 있습니다.

고객은 클라우드 보안에 대한 ISO 27017, 클라우드 프라이버시에 대한 ISO 27018, SOC 1, SOC 2 및 SOC 3, PCI DSS 레벨 1 등과 같은 엄격한 국제 표준의 규정 준수를 입증하는 국제적으로 인정받는 인증과 승인을 활용할 수 있습니다. 또한 AWS는 고객이 독일 정부에서 지원하는 증명 체계인 BSI C5(Common Cloud Computing Controls Catalogue)와 같은 현지 보안 표준을 충족하도록 지원합니다.

AWS 자격증 프로그램, 보고서 및 서드 파티 증명에 대한 자세한 내용은 AWS 규정 준수 프로그램을 참조하세요. 서비스별 자세한 내용은 범위 내 AWS 서비스를 참조하세요.

C5(Cloud Computing Compliance Controls Catalogue)

C5(Cloud Computing Compliance Controls Catalog)는 독일에서 연방 정보 보안국(BSI)이 도입한 독일 정부에서 지원하는 증명 체계입니다. 이 표준은 클라우드 공급자를 위한 독일 정부의 보안 권장 사항의 맥락 내에서 조직이 일반적인 사이버 공격에 대한 운영 보안을 입증할 수 있도록 지원하기 위해 만들어졌습니다.

데이터 보호의 기술적 및 조직적 조치와 정보 보안 조치는 기밀성, 무결성 및 가용성을 보장하기 위한 데이터 보안을 목표로 합니다. C5는 데이터 보호에도 관련될 수 있는 보안 요구 사항을 정의합니다. AWS 고객과 해당 규정 준수 고문은 워크로드를 클라우드로 이전할 때 AWS에서 제공하는 IT 보안 보

증 서비스의 범위를 이해하기 위한 리소스로 C5 증명을 사용할 수 있습니다. C5는 클라우드 관련 제어 기능뿐만 아니라 IT-Grundschutz와 동등한 규제 기관에서 정의한 IT 보안 수준을 포함합니다.

C5는 데이터 위치, 서비스 포지셔닝, 관할 지역, 기존 인증, 정보 공개 의무 및 전체 서비스 설명과 관련된 정보를 제공하는 추가 제어 기능을 포함합니다. 고객은 이 정보를 사용하여 법적 규정(예: 데이터 프라이버시), 자체 정책 또는 위협 환경이 클라우드 컴퓨팅 서비스 사용과 어떻게 관련되는지 평가할 수 있습니다.

데이터 액세스 제어

GDPR 제25조는 컨트롤러가 "기본적으로 각 특정 처리 목적에 필요한 개인 데이터만 처리하도록 적절한 기술적 및 조직적 조치를 구현해야 한다"고 명시합니다. 다음 AWS 액세스 제어 메커니즘은 권한이 있는 관리자, 사용자 및 애플리케이션만 AWS 리소스와 고객 데이터에 대한 액세스 권한을 얻도록 허용하여 고객이 이러한 요구 사항을 준수하도록 지원할 수 있습니다.

AWS Identity and Access Management

AWS 계정을 생성하면 AWS 계정에 대한 루트 사용자 계정이 자동으로 생성됩니다. 이 사용자 계정은 AWS 계정에 있는 모든 AWS 서비스와 리소스에 대한 완전한 액세스 권한을 가지고 있습니다. 일상적인 작업에 이 계정을 사용하는 대신, 처음에 추가 역할 및 사용자 계정을 만들 때와 이 계정이 필요한 관리 활동에만 이 계정을 사용해야 합니다. AWS에서는 처음부터 최소 권한의 원칙을 적용하는 것이 좋습니다. 이렇게 하려면 작업마다 다른 사용자 계정과 역할을 정의하고 각 작업을 완료하는 데 필요한 최소 권한 집합을 지정합니다. 이 접근 방식은 GDPR에 도입된 핵심 개념인 설계를 통한 데이터 보호를 조정하기 위한 메커니즘입니다. AWS Identity and Access Management(IAM)는 AWS 리소스에 대한 액세스를 안전하게 제어하기 위해 사용할 수 있는 웹 서비스입니다.

사용자와 역할은 특정 권한이 있는 IAM 자격 증명을 정의합니다. 권한 있는 사용자는 IAM 역할을 수임하여 특정 작업을 수행할 수 있습니다. 역할을 수임하면 임시 자격 증명이 생성됩니다. 예를 들어, IAM 역할을 사용하여 Amazon S3 버킷 및 Amazon Relational Database Service(Amazon RDS) 또는 Amazon DynamoDB 데이터베이스와 같은 다른 AWS 리소스에 액세스하는 데 필요한 임시 자격 증명과 함께 Amazon Elastic Compute Cloud(Amazon EC2)에서 실행되는 애플리케이션을 안전하게 제공할 수 있습니다. 마찬가지로 실행 역할은 로그 스트리밍을 위한 Amazon CloudWatch Logs 또는 Amazon Simple Queue Service(Amazon SQS) 대기열의 메시지 읽기와 같은 다른 AWS 서비스 및 리소스에 액세스하는 데 필요한 권한과 함께 AWS Lambda 함수를 제공합니다. 역할을 생성할 때 정책을 역할에 추가하여 권한 부여를 정의합니다.

고객이 리소스 정책을 모니터링하고 의도하지 않은 퍼블릭 또는 교차 계정 액세스 권한이 있는 리소스를 식별할 수 있도록 IAM Access Analyzer를 활성화하여 AWS 계정 외부에서 액세스할 수 있는 리소스를 식별하는 포괄적인 검색 결과를 생성할 수 있습니다. IAM Access Analyzer는 정책에서 허용하는 가능한 액세스 경로를 확인하기 위해 산술 논리 및 추론을 사용하여 리소스 정책을 평가합니다. IAM Access Analyzer는 새 정책 또는 업데이트된 정책을 지속적으로 모니터링하며, IAM 역할에 대한 정책뿐 아니라 Amazon S3 버킷, AWS Key Management Service(AWS KMS) 키, Amazon SQS 대기열, Lambda 함수와 같은 서비스 리소스에 대한 정책을 사용하여 부여된 권한을 분석합니다.

Access Analyzer for S3은 인터넷에 있는 모든 사용자 또는 조직 외부의 AWS 계정을 포함한 다른 AWS 계정에 대한 액세스를 허용하도록 버킷이 구성된 경우 사용자에게 알립니다. Amazon S3용 Access Analyzer에서 위험 버킷을 검토할 때 클릭 한 번으로 버킷에 대한 모든 퍼블릭 액세스를 차단할 수 있습니다. AWS에서는 특정 사용 사례를 지원하기 위해 퍼블릭 액세스가 필요한 경우를 제외하고 버킷에 대한 모든 액세스를 차단하는 것이 좋습니다. 모든 퍼블릭 액세스를 차단하기 전에 애플리케이션이 퍼블릭 액세스 없이 계속 올바르게 작동하는지 확인하세요. 자세한 내용은 Amazon S3을 사용하여 퍼블릭 액세스 차단을 참조하세요.

또한 IAM은 마지막으로 액세스한 정보를 제공하여 사용되지 않는 권한을 식별할 수 있도록 지원하므로 연결된 보안 주체에서 해당 권한을 제거할 수 있습니다. 마지막으로 액세스한 정보를 사용하면 정책을 구체화하고 필요한 서비스와 작업에만 액세스를 허용할 수 있습니다. 그러면 최소 권한 모범 사례를 더 효과적으로 준수하고 적용할 수 있습니다. IAM에 또는 전체 AWS Organizations 환경에 걸쳐 존재하는 엔터티 또는 정책에 대해 마지막으로 액세스한 정보를 볼 수 있습니다.

AWS STS를 통한 임시 액세스 토큰

AWS Security Token Service(AWS STS)를 사용하면 AWS 리소스에 대한 액세스를 부여하는 임시 보안 자격 증명을 생성하여 신뢰할 수 있는 사용자에게 제공할 수 있습니다. 임시 보안 자격 증명은 IAM 사용자에게 제공하는 장기 액세스 키 자격 증명과 거의 동일하게 작동하지만, 다음과 같은 차이점이 있습니다.

- 임시 보안 자격 증명은 단기 사용을 위한 것입니다. 유효 시간을 15분에서 최대 12시간까지 구성할 수 있습니다. 임시 자격 증명이 만료된 후 AWS는 해당 자격 증명을 인식하지 못하거나 해당 자격 증명으로 수행하는 API 요청으로부터 어떠한 종류의 액세스도 허용하지 않습니다.
- 임시 보안 자격 증명은 사용자 계정과 함께 저장되지 않습니다. 그 대신 임시 보안 자격 증명은 요청 시 동적으로 생성되어 사용자에게 제공됩니다. 임시 보안 자격 증명이 만료될 때(또는 만료되기 전에) 사용자는 새 자격 증명을 요청할 수 있습니다(해당 사용자에게 이렇게 할 권한이 있는 경우).

이러한 차이점이 있으므로 임시 자격 증명을 사용할 때 다음과 같은 이점이 있습니다.

- 애플리케이션에 장기 AWS 보안 자격 증명을 배포하거나 포함할 필요가 없습니다.
- 임시 자격 증명은 역할 및 ID 페더레이션의 기반입니다. 사용자의 임시 AWS 자격 증명을 정의하여 AWS 리소스에 대한 액세스 권한을 사용자에게 제공할 수 있습니다.
- 임시 보안 자격 증명에는 사용자 지정할 수 있는 제한적인 수명이 있습니다. 따라서 자격 증명을 교체하거나 더 이상 필요하지 않을 때 명시적으로 취소할 필요가 없습니다. 임시 보안 자격 증명이 만료된 후에는 해당 자격 증명을 다시 사용할 수 없습니다. 자격 증명이 유효한 최대 시간을 지정할 수 있습니다.

멀티 팩터 인증

보안을 강화하기 위해 AWS 계정과 IAM 사용자에 대해 2팩터 인증을 추가할 수 있습니다. 멀티 팩터 인증(MFA)을 활성화하면 AWS 관리 콘솔에 로그인할 때 사용자 이름과 암호(첫 번째 요소)뿐 아니라 AWS MFA 디바이스의 인증 응답(두 번째 요소)을 입력하라는 메시지가 표시됩니다. AWS 계정 및 해당 계정에서 생성한 개별 IAM 사용자에 대해 MFA를 활성화할 수 있습니다. 또한 MFA를 사용하여 AWS 서비스 API에 대한 액세스를 제어할 수 있습니다.

예를 들어 Amazon EC2에서 모든 AWS API 작업에 대한 전체 액세스를 허용하지만, 사용자가 MFA를 통해 인증되지 않은 경우 `StopInstances` 및 `TerminateInstances`와 같은 특정 API 작업에 대한 액세스를 명시적으로 거부하는 정책을 정의할 수 있습니다.

```
        {
         “Version”: “2012-10-17”,
         “Statement”: [
             {
                “Sid”: “AllowAllActionsForEC2”,
                “Effect”: “Allow”,
                “Action”: “ec2:*”,
                “Resource”: “*”
             },
            {
                “Sid”: “DenyStopAndTerminateWhenMFAIsNotPResent”,
                “Effect”: “Deny”,
                “Action”: [
                    “ec2:StopInstances”,
                    “ec2:TerminateInstances”
               ],
                “Resource”: “*”,
                “Conditions”: {
                    “BoolIfExists”: {“aws:MultiFactorAuthPresent”:false}
                 }
            }
       }
}
```

Amazon S3 버킷에 추가 보안 계층을 추가하려면 MFA Delete를 구성할 수 있습니다. 이렇게 하면 버킷의 버전 관리 상태를 변경하고 객체 버전을 영구적으로 삭제하려는 경우 추가 인증이 필요합니다. MFA Delete는 보안 자격 증명이 손상된 경우 보안을 강화합니다.

MFA Delete를 사용하려면 하드웨어 또는 가상 MFA 디바이스를 사용하여 인증 코드를 생성할 수 있습니다. 지원되는 하드웨어 또는 가상 MFA 디바이스 목록은 멀티 팩터 인증 페이지를 참조하세요.

AWS 리소스에 대한 액세스

AWS 리소스에 대한 세분화된 액세스 권한을 구현하려면 리소스에 따라 각 사용자에게 서로 다른 수준의 권한을 부여할 수 있습니다. 예를 들어 일부 사용자만 Amazon EC2, Amazon S3, DynamoDB, Amazon Redshift 및 기타 AWS 서비스에 완전히 액세스할 수 있도록 허용할 수 있습니다.

다른 사용자의 경우 일부 Amazon S3 버킷에 대한 읽기 전용 액세스만 허용하거나, 일부 Amazon EC2 인스턴스만 관리하거나 결제 정보에만 액세스할 수 있는 권한을 허용할 수 있습니다.

다음 정책은 특정 Amazon S3 버킷에 대한 모든 작업을 허용하고 Amazon S3가 아닌 모든 AWS 서비스에 대한 액세스를 명시적으로 거부하기 위해 사용할 수 있는 방법 중 하나의 예입니다.

```
      {
         “Version”: “2012-10-17”,
         “Statement”: [
             {
                “Effect”: “Allow”,
                “Action”: “s3:*”,
                “Resource”: [
                     “arn:aws:s3:::bucket-name”,
                     “arn:aws:s3:::bucket-name/*”
                 ],
              },
              {
                “Effect”: “Deny”,
                “NotAction”: “s3:*”,
                “NotResource”: [
                     “arn:aws:s3:::bucket-name”,
                     “arn:aws:s3:::bucket-name/*”
                 ]
               }
            ]
}
```

사용자 계정이나 역할에 정책을 연결할 수 있습니다. IAM 정책의 다른 예는 IAM 자격 증명 기반 정책 예를 참조하세요.

리전 서비스 액세스의 경계 정의

고객은 자신의 콘텐츠에 대한 소유권을 유지하고 콘텐츠를 처리, 저장 및 호스트할 수 있는 AWS 서비스를 선택합니다. AWS는 사용자의 동의 없이 어떤 목적으로도 사용자의 콘텐츠에 액세스하거나 사용자의 콘텐츠를 사용하지 않습니다. 공동 책임 모델을 기반으로 콘텐츠가 저장되는 AWS 리전을 선택하면 특정 지리적 요구 사항에 따라 선택한 위치에 AWS 서비스를 배포할 수 있습니다. 예를 들어 콘텐츠가 유럽에만 위치하도록 하려면 AWS 서비스를 유럽 AWS 리전 중 하나에만 배포하도록 선택할 수 있습니다.

IAM 정책은 특정 리전의 서비스에 대한 액세스를 제한하는 간단한 메커니즘을 제공합니다. IAM 보안 주체에 연결된 IAM 정책에 글로벌 조건(`aws:RequestedRegion`)을 추가하여 이 정책을 모든 AWS 서비스에 적용할 수 있습니다. 예를 들어, 다음 정책은 `Deny` 효과가 있는 `NotAction` 요소를 사용하며, 이 요소는 요청된 리전이 유럽이 아닌 경우 문에 나열되지 않은 모든 작업에 대한 액세스를 명시적으로 거부합니다. CloudFront, IAM, Amazon Route 53 및 AWS Support 서비스의 작업은 널리 사용되는 AWS 글로벌 서비스이므로 거부해서는 안 됩니다.

```
      {
         “Version”: “2012-10-17”,
         “Statement”: [
             {
                “Sid”: “DenyAllOutsideRequestedRegions”,
                “Effect”: “Deny”,
                “NotAction”: [
                     “cloudfront:*”,
                     “iam:*”,
                     ”route53:*”,
                     “support:*”
                 ],
                 “Resource”: “*”,
                 “Condition”: {
                    “StringNotLike”: {
                        “aws:RequestedRegion”: [
                              “eu-*”
                        ]
                    }
                 }
             }
          ]
}
```

이 샘플 IAM 정책을 AWS Organizations에서 서비스 제어 정책(SCP)으로 구현할 수도 있습니다. 이 정책은 조직 내의 특정 AWS 계정 또는 조직 단위(OU)에 적용되는 권한 경계를 정의합니다. 이렇게 하면 복잡한 다중 계정 환경에서 리전 서비스에 대한 사용자 액세스를 제어할 수 있습니다.

새로 시작된 리전에는 지리적 제한 기능이 있습니다. 2019년 3월 20일 이후에 도입된 리전은 기본적으로 비활성화되어 있습니다. 이 리전을 사용하려면 먼저 활성화해야 합니다. AWS 리전이 기본적으로 비활성화되어 있는 경우 AWS 관리 콘솔을 사용하여 리전을 활성화하고 비활성화할 수 있습니다. AWS 리전을 활성화하거나 비활성화하여 AWS 계정에 있는 사용자가 해당 리전의 리소스에 액세스할 수 있는지 여부를 제어할 수 있습니다. 자세한 내용은 AWS 리전 관리를 참조하세요.

웹 애플리케이션 및 모바일 앱에 대한 액세스 제어

AWS는 고객 애플리케이션 내에서 데이터 액세스 제어를 관리하기 위한 서비스를 제공합니다. 웹 애플리케이션과 모바일 앱에 사용자 로그인 및 액세스 제어 기능을 추가해야 하는 경우 Amazon Cognito를 사용할 수 있습니다. Amazon Cognito 사용자 풀은 수억 명의 사용자로 크기 조정할 수 있는 안전한 사용자 디렉터리를 제공합니다. 사용자의 자격 증명을 보호하려면 멀티 팩터 인증(MFA)을 사용자 풀에 추가할 수 있습니다. 또한 적응형 인증도 사용할 수 있습니다. 이 인증은 위험 기반 모델을 사용하여 다른 인증 요소가 필요할 수 있는 시간을 예측할 수 있습니다.

Amazon Cognito 자격 증명 풀(페더레이션 자격 증명)을 사용하면 누가 리소스에 액세스했으며 어디에서 액세스가 시작되었는지(모바일 앱 또는 웹 애플리케이션)를 확인할 수 있습니다. 이 정보를 사용하여 액세스 시작 위치(모바일 앱 또는 웹 애플리케이션)와 자격 증명 공급자의 유형을 기반으로 리소스에 대한 액세스를 허용하거나 거부하는 IAM 역할 및 정책을 생성할 수 있습니다.

모니터링 및 로깅

GDPR 제30조는 "...각 컨트롤러와 해당되는 경우 컨트롤러 대리인은 자신의 책임으로 처리 활동 기록을 유지 관리해야 한다"고 명시합니다. 이 문서에는 모든 개인 데이터의 처리를 모니터링할 때 기록해야 하는 정보에 대한 세부 정보도 포함되어 있습니다. 컨트롤러와 프로세서도 시기 적절하게 위반 알림을 보내야 하므로 인시던트를 빠르게 감지하는 것이 중요합니다. 고객이 이러한 의무를 준수할 수 있도록 AWS는 다음과 같은 모니터링 및 로깅 서비스를 제공합니다.

AWS Config를 사용한 자산 관리 및 구성

AWS Config에서는 AWS 계정에 있는 다양한 유형의 AWS 리소스 구성을 자세히 볼 수 있습니다. 이 보기에는 리소스가 서로 관련되는 방식과 리소스가 이전에 구성된 방식이 포함되므로 시간 경과에 따라 구성과 관계가 어떻게 변경되는지 확인할 수 있습니다.

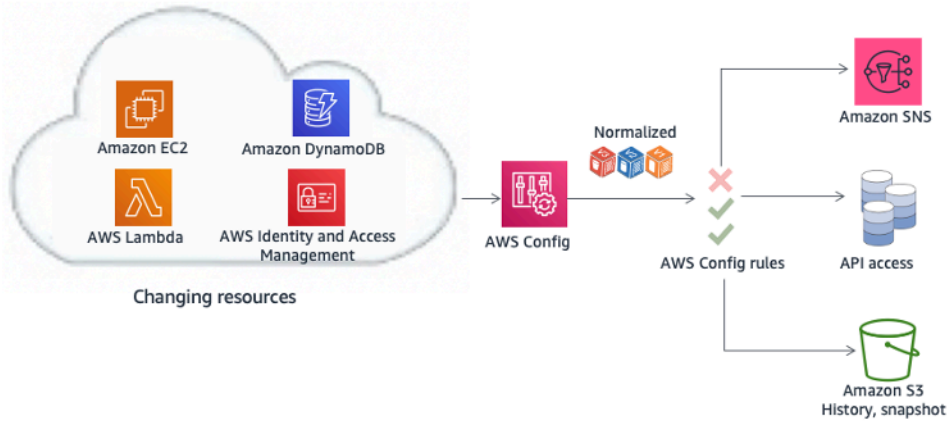

그림 1 – AWS Config를 사용하여 시간 경과에 따른 구성 변경 모니터링

AWS 리소스는 AWS에서 작업할 수 있는 엔터티입니다. 예를 들면 EC2 인스턴스, Amazon Elastic Block Store(Amazon EBS) 볼륨, 보안 그룹 또는 Amazon Virtual Private Cloud(Amazon VPC)가 있습니다. AWS Config에서 지원되는 AWS 리소스의 전체 목록은 지원되는 AWS 리소스 유형을 참조하세요.

AWS Config를 사용하여 다음을 수행할 수 있습니다.

- AWS 리소스 구성을 평가하여 설정이 올바른지 확인합니다.
- AWS 계정과 연결된 지원되는 리소스의 현재 구성에 대한 스냅샷을 가져옵니다.
- 계정에 있는 하나 이상의 리소스 구성을 가져옵니다.

- 하나 이상의 리소스 구성 기록을 가져옵니다.
- 리소스가 생성, 수정 또는 삭제될 때 알림을 받습니다.
- 리소스 간의 관계를 확인합니다. 예를 들어 특정 보안 그룹을 사용하는 모든 리소스를 찾습니다.

규정 준수 감사 및 보안 분석

AWS CloudTrail를 사용하면 AWS 계정 활동을 지속적으로 모니터링할 수 있습니다. AWS 관리 콘솔, AWS SDK, 명령줄 도구 및 상위 수준 AWS 서비스를 통해 수행된 API 호출을 포함하여 계정에 대한 AWS API 호출 기록이 캡처됩니다. CloudTrail을 지원하는 서비스에 대해 AWS API를 호출한 사용자 및 계정, 호출이 수행된 소스 IP 주소, 호출이 발생한 시간을 확인할 수 있습니다. API를 사용하여 CloudTrail을 애플리케이션에 통합하고, 조직을 위해 트레일 생성을 자동화할 수 있으며, 트레일의 상태를 확인하고, 관리자가 CloudTrail 로깅을 활성화 및 비활성화하는 방법을 제어할 수 있습니다.

여러 리전 및 여러 AWS 계정에서 단일 Amazon S3 버킷으로 CloudTrail 로그를 집계할 수 있습니다. AWS에서는 로깅을 위해 지정된 AWS 계정(로그 아카이브)에서 제한된 액세스 권한으로 Amazon S3 버킷에 로그(특히 AWS CloudTrail 로그)를 작성하는 것이 좋습니다. 버킷에 대한 권한은 로그 삭제를 방지해야 하며, Amazon S3 관리형 암호화 키(SSE-S3) 또는 AWS KMS 관리형 키(SSE-KMS)와 함께 서버 측 암호화를 사용하여 저장된 데이터를 암호화해야 합니다. CloudTrail 로그 파일 무결성 검증을 사용하여 CloudTrail이 로그 파일을 전송한 후 로그 파일이 수정되었는지, 삭제되었는지 또는 변경되지 않았는지 확인할 수 있습니다. 이 기능은 산업 표준 알고리즘(해시의 경우 SHA-256, 디지털 서명의 경우 RSA 포함 SHA-256)을 사용하여 구축되었습니다. 따라서 감지되지 않으면서 CT 로그 파일을 수정, 삭제 또는 위조하는 것은 컴퓨팅 면에서 어렵습니다. AWS 명령줄 인터페이스(AWS CLI)를 사용하여 CloudTrail이 파일을 전송한 위치에서 파일의 유효성을 검사할 수 있습니다.

감사 목적이나 문제 해결 활동을 위해 Amazon S3 버킷에 집계된 CloudTrail 로그를 분석할 수 있습니다. 로그를 중앙 집중화하면 보안 정보 및 이벤트 관리(SIEM) 솔루션과 통합하거나 Amazon Athena 또는 CloudTrail Insights와 같은 AWS 서비스를 사용하여 로그를 분석하고 Amazon QuickSight 대시보드를 사용하여 로그를 시각화할 수 있습니다. CloudTrail 로그를 중앙 집중화하면 동일한 로그 아카이브 계정을 사용하여 CloudWatch Logs 및 AWS 로드 밸런서와 같은 다른 소스의 로그도 중앙 집중화할 수 있습니다.

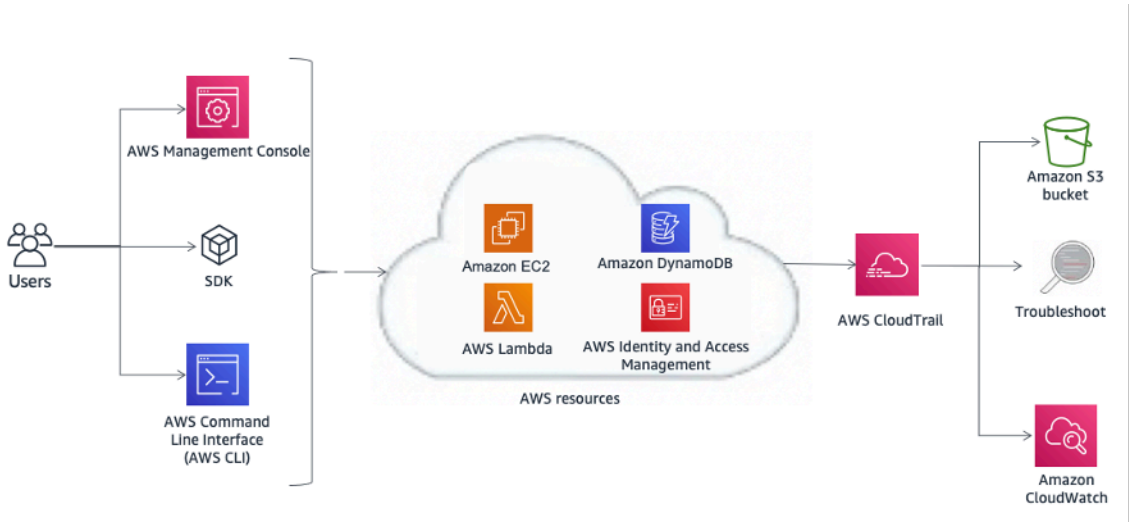

그림 2 – AWS CloudTrail을 사용한 규정 준수 감사 및 보안 분석을 위한 아키텍처의 예

AWS CloudTrail 로그는 사전 구성된 Amazon CloudWatch 이벤트도 트리거할 수 있습니다. 이러한 이벤트를 사용하여 이벤트가 발생했음을 사용자 또는 시스템에 알리거나 수정 작업을 수행할 수 있습니다. 예를 들어 Amazon EC2 인스턴스에서 활동을 모니터링하려는 경우 CloudWatch 이벤트 규칙을 생성할 수 있습니다. Amazon EC2 인스턴스에서 특정 활동이 발생하고 이벤트가 로그에 캡처되면 규칙에 따라 AWS Lambda 함수가 트리거되어 관리자에게 이벤트에 대한 알림 이메일이 전송됩니다(그림 3 참조). 이메일에는 이벤트가 발생한 시간, 작업을 수행한 사용자, Amazon EC2 세부 정보 등과 같은 세부 정보가 포함됩니다. 다음 다이어그램은 이벤트 알림의 아키텍처를 보여 줍니다.

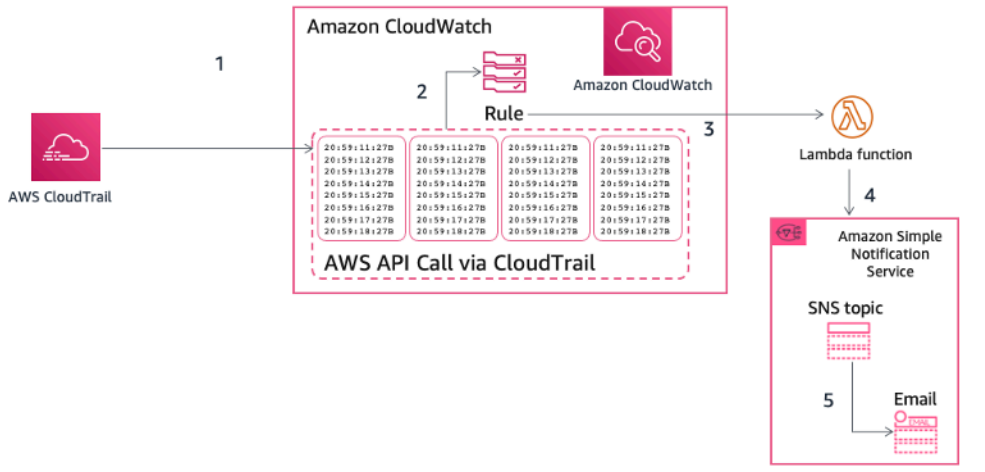

그림 3 – AWS CloudTrail 이벤트 알림의 예

로그 수집 및 처리

CloudWatch Logs를 사용하면 Amazon EC2 인스턴스, AWS CloudTrail, Route 53 및 기타 소스의 로그 파일을 모니터링, 저장 및 액세스할 수 있습니다. CloudWatch Logs에 로그를 게시하는 AWS 서비스 설명서 페이지를 참조하세요.

로그 정보에는 예를 들어 다음과 같은 정보가 포함됩니다.

- Amazon S3 객체에 대한 액세스의 세분화된 로깅
- VPC 흐름 로그를 통한 네트워크의 흐름에 대한 자세한 정보
- 규칙 기반 구성 확인 및 AWS Config 규칙을 사용한 작업
- CloudFront의 웹 애플리케이션 방화벽(WAF) 기능을 사용하여 애플리케이션에 대한 HTTP 액세스 필터링 및 모니터링

Amazon EC2 인스턴스 또는 온프레미스 서버에 CloudWatch 에이전트를 설치하여 사용자 지정 애플리케이션 지표와 로그도 CloudWatch Logs에 게시할 수 있습니다.

CloudWatch Logs Insights를 사용하여 로그를 대화식으로 분석하고 쿼리를 수행하여 운영 문제에 더 효율적이고 효과적으로 대응할 수 있습니다.

CloudWatch Logs는 구독 필터를 구성하여 거의 실시간으로 처리할 수 있으며 Amazon OpenSearch Service(OpenSearch Service) 클러스터, Amazon Kinesis 스트림, Amazon Kinesis Data Firehose 스트림 또는 Lambda와 같은 다른 서비스로 전송하여 사용자 지정 처리 또는 분석에 사용하거나 다른 시스템에 로드할 수 있습니다.

CloudWatch 지표 필터를 사용하여 로그 데이터에서 찾을 패턴을 정의하고 이 패턴을 숫자 CloudWatch 지표로 변환할 수 있으며 비즈니스 요구 사항을 기반으로 경보를 설정할 수 있습니다. 예를 들어 일상적인 작업에 루트 사용자를 사용하지 않는 것이 좋다는 AWS 권장 사항에 따라, CloudTrail 로그(CloudWatch Logs에 전송됨)에 대한 특정 CloudWatch 지표 필터를 설정하여 사용자 지정 지표를 생성하고 루트 자격 증명이 AWS 계정에 액세스하는 데 사용되는 경우 관련 이해 관계자에게 알리는 경보를 구성할 수 있습니다.

Amazon S3 서버 액세스 로그, Elastic Load Balancing 액세스 로그, VPC 흐름 로그 및 AWS Global Accelerator 흐름 로그와 같은 로그를 Amazon S3 버킷으로 직접 전송할 수 있습니다. 예를 들어 Amazon Simple Storage Service 서버 액세스 로그를 활성화하면 Amazon S3 버킷에 수행하는 요청에 대한 자세한 정보를 얻을 수 있습니다. 액세스 로그 레코드에는 요청 유형, 요청에 지정된 리소스, 요청이 처리된 날짜 및 시간과 같은 요청 세부 정보가 포함됩니다. 로그 메시지의 콘텐츠에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 Amazon Simple Storage Service 서버 액세스

로그 형식을 참조하십시오. 서버 액세스 로그는 버킷 소유자에게 자신이 제어하지 않는 클라이언트에서 수행된 요청의 특성에 대한 인사이트를 제공하기 때문에 많은 애플리케이션에 유용합니다. 기본적으로 Amazon S3은 서비스 액세스 로그를 수집하지 않지만, 로깅을 활성화하면 Amazon S3은 몇 시간 이내에 액세스 로그를 버킷에 전송합니다. 더 빠른 전송이 필요하거나 여러 대상에 로그를 전송해야 하는 경우 CloudTrail 로그를 사용하거나 CloudTrail 로그와 Amazon S3을 함께 사용하는 것이 좋습니다. 대상 버킷에서 기본 객체 암호화를 구성하여 저장된 로그를 암호화할 수 있습니다. 객체는 Amazon S3 관리형 키를 사용하는 서버 측 암호화(SSE-S3) 또는 AWS Key Management Service(AWS KMS)에 저장된 고객 마스터 키(CMK)를 사용하는 서버 측 암호화로 암호화됩니다.

Amazon S3 버킷에 저장된 로그는 Amazon Athena를 사용하여 쿼리하고 분석할 수 있습니다. Amazon Athena는 표준 SQL을 사용하여 S3의 데이터를 분석할 수 있는 대화형 쿼리 서비스입니다. Athena를 사용하면 데이터를 Athena에 집계하거나 로드할 필요 없이 ANSI SQL을 통해 임시 쿼리를 실행할 수 있습니다. Athena는 비정형, 반정형 및 정형 데이터 집합을 처리할 수 있으며 Amazon QuickSight와 통합되어 간편한 시각화를 제공합니다.

또한 로그는 자동 위협 탐지에 유용한 정보 소스입니다. Amazon GuardDuty는 VPC 흐름 로그, CloudTrail 관리 이벤트 로그, CloudTrail, Amazon S3 데이터 이벤트 로그 및 DNS 로그와 같은 여러 소스의 이벤트를 분석하고 처리하는 지속적 보안 모니터링 서비스입니다. 이 서비스는 악성 IP 주소 및 도메인 목록과 같은 위협 인텔리전스 피드와 기계 학습을 사용하여 AWS 환경 내에서 예기치 않게 발생할 수 있는 무단 활동과 악의적 활동을 찾아냅니다. 리전에서 GuardDuty를 활성화하면 이 서비스는 CloudTrail 이벤트 로그 분석을 즉시 시작합니다. 이 서비스는 독립적이고 중복되는 이벤트 스트림을 통해 CloudTrail에서 직접 CloudTrail 관리와 Amazon S3 데이터 이벤트를 사용합니다.

Amazon Macie를 사용하여 대규모 데이터 검색 및 보호

GDPR 제32조에 따르면 "...컨트롤러와 프로세서는 위험에 적절한 수준의 보안을 보장할 수 있는 적절한 기술적 및 조직적 조치를 구현해야 하며, 이러한 조치에는 적절한 경우 특히 다음이 포함됩니다. […]

(b) 처리 시스템 및 서비스의 지속적인 기밀성, 무결성, 가용성, 복원력을 보장할 수 있는 기능

[…]

(d) 처리의 보안을 보장하는 기술적 및 조직적 조치의 효과를 정기적으로 테스트, 검사 및 평가하기 위한 프로세스"

지속적인 데이터 분류 프로세스를 유지하는 것은 보안 데이터 처리를 데이터 특성에 맞게 조정하는 데 중요합니다. 조직에서 민감한 데이터를 관리하는 경우 데이터가 상주하는 위치를 모니터링하고, 데이터를 적절하게 보호하며, 규정 준수 요구 사항을 충족하는 데 필요한 데이터 보안 및 개인 정보 보호를

시행하고 있다는 증거를 제공해야 합니다. 고객이 민감한 데이터를 대규모로 식별하고 보호할 수 있도록 지원하기 위해 AWS는 개인 식별 정보(PII) 감지를 위한 패턴 매칭 및 기계 학습 모델을 사용하여 S3 버킷에 저장된 민감한 데이터를 검색하고 보호하는 완전 관리형 데이터 보안 및 데이터 개인 정보 보호 서비스인 Amazon Macie를 제공합니다. Amazon Macie는 이러한 버킷을 스캔하고, 여러 범주의 민감한 데이터를 감지하도록 설계된 관리형 데이터 식별자를 사용하여 버킷의 데이터를 범주별로 분류합니다. Macie는 전체 이름, 이메일 주소, 생년월일, 국가 식별 번호, 납세자 식별 또는 참조 번호 등과 같은 PII를 감지할 수 있습니다. 고객은 조직의 특정 시나리오(예: 고객 계정 번호 또는 내부 데이터 분류)를 반영하는 사용자 지정 데이터 식별자를 정의할 수 있습니다.

Amazon Macie는 버킷 내부의 객체를 지속적으로 평가하고 정의된 데이터 범주와 일치하는 암호화되지 않거나 퍼블릭으로 액세스할 수 있는 데이터에 대한 검색 결과 요약(그림 4)을 자동으로 제공합니다. 이 데이터에는 AWS Organizations에서 정의한 것 이외에 AWS 계정과 공유되는 암호화되지 않거나 퍼블릭으로 액세스할 수 있는 객체 또는 버킷에 대한 경고가 포함될 수 있습니다. Amazon Macie는 AWS Security Hub와 같은 다른 AWS 서비스와 통합되어 실행 가능한 보안 결과를 생성하고 이 결과에 대해 자동 대응 작업을 제공합니다(그림 5).

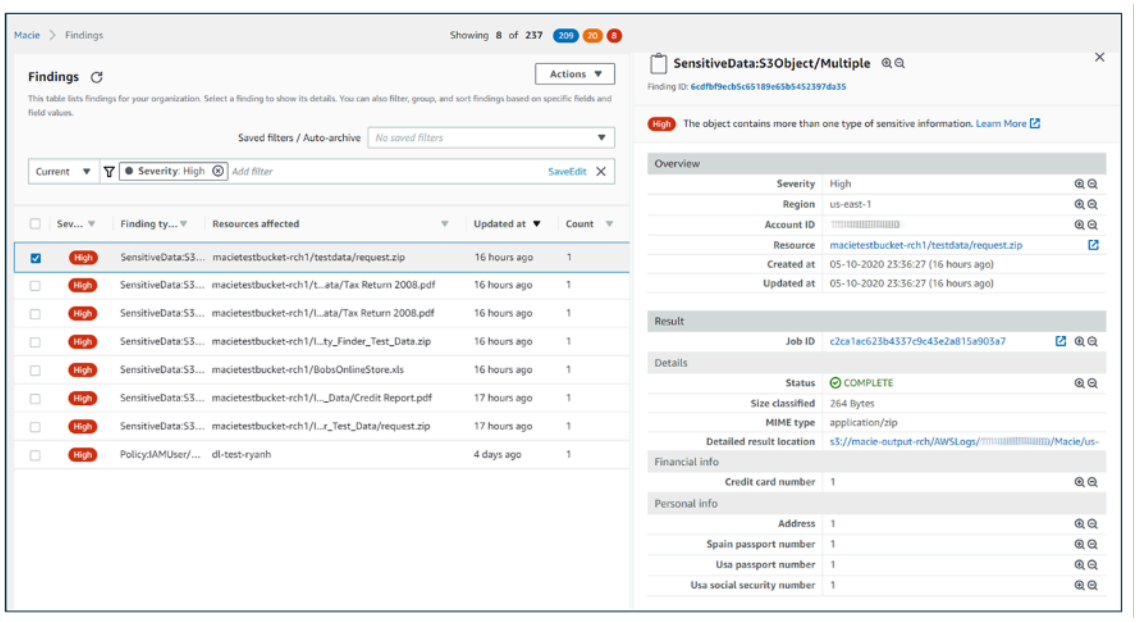

그림 4 – 데이터 검사 및 검색의 예

중앙 집중식 보안 관리

많은 조직에는 환경에 대한 가시성 및 중앙 집중식 관리와 관련된 문제가 있습니다. 보안 설계를 신중하게 고려하지 않으면 운영 범위가 증가함에 따라 이러한 문제가 악화될 수 있습니다. 거버넌스와 보안 프로세스를 분산된 방식으로 고르지 않게 관리하면서 동시에 지식이 부족하면 환경이 취약해질 수 있습니다.

AWS는 IT 관리 및 거버넌스에 대한 가장 까다로운 요구 사항을 해결하는 데 도움이 되는 도구와, 설계를 통한 데이터 보호 접근 방식을 지원하는 도구를 제공합니다.

AWS Control Tower는 새롭고 안전한 다중 계정 AWS 환경을 설정하고 관리하는 방법을 제공합니다. 이 서비스는 모범 사례 블루프린트를 기반으로 하는 다중 계정 환경인 랜딩 존의 설정을 자동화하고 사전 패키지 목록에서 선택할 수 있는 가드 레일을 사용하여 거버넌스를 활성화합니다. 가드 레일은 보안, 규정 준수 및 운영을 위한 거버넌스 규칙을 구현합니다. AWS Control Tower는 AWS IAM Identity Center(IAM Identity Center) 기본 디렉터리를 사용하여 자격 증명 관리를 제공하고 IAM Identity Center 및 IAM을 사용하여 교차 계정 감사를 활성화합니다. 또한 CloudTrail에서 나오는 로그와 Amazon S3에 저장되는 AWS Config 로그를 중앙 집중화합니다.

AWS Security Hub는 중앙 집중화를 지원하고 조직에 대한 가시성을 향상할 수 있는 또 다른 서비스입니다. Security Hub는 Amazon GuardDuty 및 Amazon Inspector와 같은 AWS 계정 및 서비스 전체에서 보안 및 규정 준수 결과를 중앙 집중화하고 우선 순위를 지정하며, 서드 파티 파트너의 보안 소프트웨어와 통합하여 보안 추세를 분석하고 우선 순위가 가장 높은 보안 문제를 식별하는 데 도움이 될 수 있습니다.

Amazon GuardDuty는 고객이 Amazon S3에 저장된 AWS 계정, 워크로드 및 데이터를 더 정확하고 쉽게 모니터링하고 보호하도록 지원할 수 있는 지능형 위협 탐지 서비스입니다. GuardDuty는 AWS CloudTrail 관리 이벤트, CloudTrail, Amazon S3 데이터 이벤트, Amazon Virtual Private Cloud 흐름 로그 및 DNS 로그를 포함한 여러 소스에서 AWS 계정 전반에 걸쳐 수십억 개의 이벤트를 분석합니다. 예를 들어 GuardDuty는 비정상적인 API 호출, 알려진 악성 IP 주소에 대한 의심스러운 아웃바운드 통신, 또는 DNS 쿼리를 전송 메커니즘으로 사용하는 잠재적 데이터 도난을 탐지합니다. GuardDuty는 기계 학습 기반 위협 인텔리전스 및 서드 파티 보안 파트너를 활용하여 더 정확한 결과를 제공할 수 있습니다.

Amazon Inspector는 Amazon EC2 인스턴스에 배포된 애플리케이션의 보안 및 규정 준수를 개선하는 데 도움이 되는 자동 보안 평가 서비스입니다. Amazon Inspector는 애플리케이션의 노출, 취약성, 모범 사례에 대한 편차를 자동으로 평가합니다. 평가를 수행한 후, Amazon Inspector는 심각도 수준에 따라 우선순위가 지정된 자세한 보안 평가 결과 목록을 제공합니다.

Amazon CloudWatch Events를 사용하면 AWS 계정을 설정하여 다른 AWS 계정으로 이벤트를 전송하거나 다른 계정 또는 조직의 이벤트 수신자가 될 수 있습니다. 이 메커니즘은 보안 인시던트 이벤트가 발생할 때마다 필요에 따라 적시에 시정 조치(예: Lambda 함수 호출 또는 Amazon EC2 인스턴스에서 명령 실행)를 수행하여 교차 계정 인시던트 대응 시나리오를 구현하는 데 매우 유용할 수 있습니다.

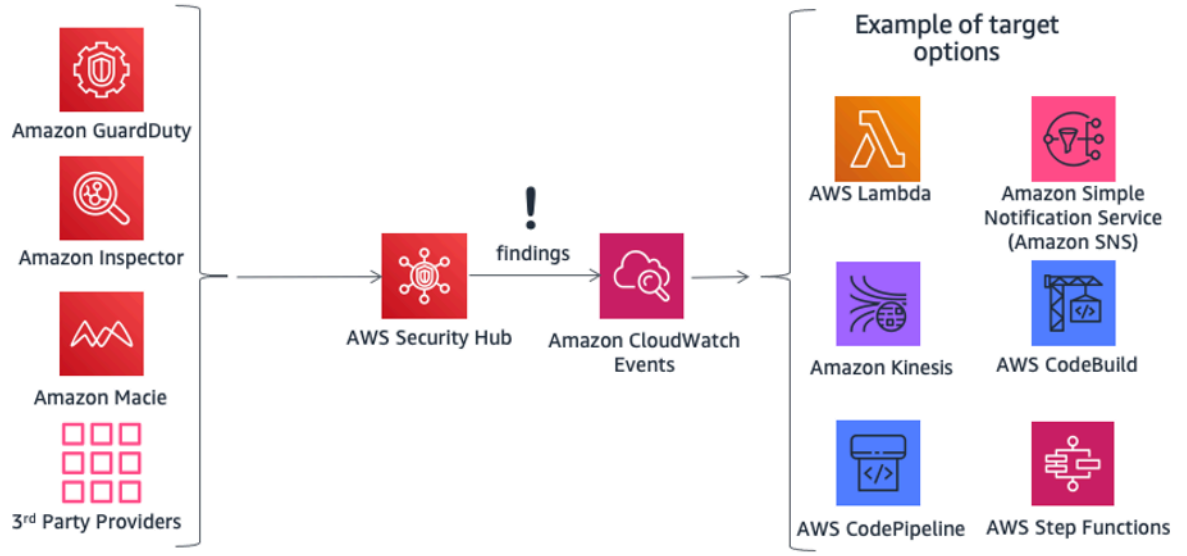

그림 5 – AWS Security Hub 및 Amazon CloudWatch Events를 사용한 조치 수행

AWS Organizations는 복잡한 환경을 중앙에서 관리하고 제어할 수 있도록 지원합니다. 이 서비스를 사용하면 다중 계정 환경에서 액세스, 규정 준수 및 보안을 제어할 수 있습니다. AWS Organizations는 조직 내의 특정 계정 또는 조직 단위(OU)에 사용할 수 있는 AWS 서비스 작업을 정의하는 서비스 제어 정책(SCP)을 지원합니다.

AWS Systems Manager는 AWS 인프라에 대한 가시성과 제어를 제공합니다. 통합 콘솔에서 여러 AWS 서비스의 운영 데이터를 볼 수 있으며 서비스 전체에 걸쳐 운영 작업을 자동화할 수 있습니다. 최근 API 활동, 리소스 구성 변경, 운영 경고, 소프트웨어 인벤토리 및 패치 규정 준수 상태에 대한 정보를 얻을 수 있습니다. 또한 다른 AWS 서비스와의 통합을 사용하면 운영 요구 사항에 따라 리소스에 대해 작업을 수행하여 환경을 규정 준수 상태로 유지할 수 있습니다.

예를 들어 Amazon Inspector를 AWS Systems Manager와 통합하면 Amazon EC2 인스턴스가 시작될 때 Amazon Elastic Compute Cloud Systems Manager를 사용하여 Amazon Inspector 에이전트를 자동으로 설치할 수 있기 때문에 보안 평가가 간소화되고 자동화됩니다. 또한 Amazon EC2 시스템 관리자 및 Lambda 함수를 사용하여 Amazon Inspector 결과에 대한 자동 수정도 수행할 수 있습니다.

AWS에서 사용자의 데이터 보호

GDPR 제32조는 조직이 "…개인 데이터의 가명 처리 및 암호화[...]를 포함하여 위험에 적절한 수준의 보안을 보장할 수 있는 적절한 기술적 및 조직적 조치를 구현…"해야 한다고 규정합니다. 또한, 조직은 개인 데이터를 무단 공개 또는 액세스로부터 보호해야 합니다.

암호화를 사용할 경우 올바른 키가 없으면 데이터를 읽을 수 없기 때문에 개인 데이터 저장과 관련된 위험을 줄일 수 있습니다. 철저한 암호화 전략은 일부 보안 위반을 포함한 다양한 보안 이벤트의 영향을 완화하는 데 도움이 될 수 있습니다.

저장된 데이터 암호화

저장된 데이터 암호화는 규정 준수와 데이터 보호에 필수적입니다. 이 기능은 유효한 키가 없으면 사용자나 애플리케이션이 디스크에 저장된 민감한 데이터를 읽을 수 없도록 하는 데 도움이 됩니다. AWS는 저장 시 암호화 및 암호화 키 관리를 위한 다양한 옵션을 제공합니다. 예를 들어 AWS KMS에서 생성하고 관리하는 CMK와 함께 AWS 암호화 SDK를 사용하여 임의 데이터를 암호화할 수 있습니다.

암호화된 데이터는 미사용 시 안전하게 저장할 수 있으며 CMK에 대한 액세스 권한이 있는 당사자만 해독할 수 있습니다. 결과적으로 봉투 암호화된 기밀 데이터, 권한 부여 및 인증된 암호화를 위한 정책 메커니즘, AWS CloudTrail을 통한 감사 로깅을 얻을 수 있습니다. 일부 AWS 기반 서비스에는 데이터를 비휘발성 스토리지에 쓰기 전에 데이터를 암호화할 수 있는 옵션을 제공하는 미사용 시 암호화 기능이 내장되어 있습니다. 예를 들어 AES-256 암호화를 사용하여 Amazon EBS 볼륨을 암호화하고 Amazon S3 버킷을 서버 측 암호화(SSE)에 맞게 구성할 수 있습니다. 또한 Amazon S3은 클라이언트 측 암호화도 지원하므로 Amazon S3으로 전송하기 전에 데이터를 암호화할 수 있습니다. AWS SDK는 객체의 암호화 및 암호 해독 작업을 쉽게 할 수 있도록 클라이언트 측 암호화를 지원합니다. 또한 Amazon RDS는 투명한 데이터 암호화(TDE)를 지원합니다.

내장된 Linux 라이브러리를 사용하여 Linux Amazon EC2 인스턴스 스토어의 데이터를 암호화할 수 있습니다. 이 방법은 파일을 투명하게 암호화하여 기밀 데이터를 보호합니다. 따라서 데이터를 처리하는 애플리케이션은 디스크 수준의 암호화를 인식하지 못합니다.

다음 두 가지 방법을 사용하여 인스턴스 스토어의 파일을 암호화할 수 있습니다.

- 디스크 수준 암호화 — 이 방법을 사용하면 전체 디스크 또는 디스크 내의 블록이 하나 이상의 암호화 키를 사용하여 암호화됩니다. 디스크 암호화는 파일 시스템 수준 아래에서 작동하고, 운영 체제의 구애를 받지 않으며, 이름 및 크기와 같은 디렉터리 및 파일 정보를 숨깁니다. 예를 들어 파일 시스템 암호화(Encrypting File System)는 디스크 암호화를 제공하는 Windows NT 운영 체제의 NTFS(New Technology File System)에 대한 Microsoft 확장 기능입니다.

- 파일 시스템 수준 암호화 — 이 방법을 사용하면 파일과 디렉터리가 암호화되지만 전체 디스크나 파티션은 암호화되지 않습니다. 파일 시스템 수준 암호화는 파일 시스템 위에서 작동하며 운영 체제 간에 이동할 수 있습니다.

NVMe(Non-Volatile Memory express) SSD 인스턴스 스토어 볼륨의 경우 디스크 수준 암호화가 기본 옵션입니다. NVMe 인스턴스 스토리지의 데이터는 인스턴스의 하드웨어 모듈에 구현된 XTS-AES-256 블록 암호를 사용하여 암호화됩니다. 하드웨어 모듈을 사용하여 암호화 키를 생성하며, 암호화 키는 각 NVMe 인스턴스 스토리지 디바이스에 고유합니다. 인스턴스가 중지되거나 종료되면 모든 암호화 키가 손상되어 복구가 불가능해집니다. 자체 암호화 키는 사용할 수 없습니다.

전송 중인 데이터 암호화

AWS는 AWS 내부 및 외부의 리소스를 포함하여 한 시스템에서 다른 시스템으로 전송 중인 데이터를 암호화할 것을 적극 권장합니다.

AWS 계정을 생성하면 Amazon Virtual Private Cloud(Amazon VPC)라는 AWS 클라우드의 논리적으로 격리된 섹션이 계정에 프로비저닝됩니다. 여기에서 사용자가 정의하는 가상 네트워크에 AWS 리소스를 시작할 수 있습니다. 자체 IP 주소 범위, 서브넷 생성, 라우팅 테이블 및 네트워크 게이트웨이 구성 선택을 포함하여 가상 네트워킹 환경을 완전히 제어할 수 있습니다. 또한 기업 데이터 센터와 Amazon VPC 간에 하드웨어 가상 사설 네트워크(VPN) 연결을 생성할 수 있으므로, AWS 클라우드를 기업 데이터 센터의 확장으로 사용할 수 있습니다.

Amazon VPC와 기업 데이터 센터 간의 통신을 보호하기 위해 여러 VPN 연결 옵션 중에서 선택할 수 있으며 필요에 가장 적합한 옵션을 선택할 수 있습니다. AWS Client VPN을 사용하면 클라이언트 기반 VPN 서비스를 사용하여 AWS 리소스에 안전하게 액세스할 수 있습니다. AWS Marketplace에서 제공하는 서드 파티 소프트웨어 VPN 어플라이언스를 사용할 수도 있습니다. 이 어플라이언스는 Amazon VPC의 Amazon EC2 인스턴스에 설치할 수 있습니다. 또는 IPsec VPN 연결을 생성하여 VPC와 원격 네트워크 간의 통신을 보호할 수 있습니다. 원격 네트워크에서 Amazon VPC로 전용 프라이빗 연결을 생성하려면 AWS Direct Connect를 사용할 수 있습니다. 이 연결을 AWS Site-to-Site VPN과 결합하여 IPsec 암호화 프라이빗 연결을 생성할 수 있습니다.

AWS는 AWS API를 사용할 때 전송 중 암호화를 제공하는 TLS 프로토콜을 통신에 사용하여 HTTPS 엔드포인트를 제공합니다. AWS Certificate Manager(ACM) 서비스를 사용하여 워크로드를 위해 시스템 간의 암호화된 전송을 설정하는 데 사용하는 프라이빗 및 퍼블릭 인증서를 생성, 관리 및 배포할 수 있습니다. Elastic Load Balancing은 ACM과 통합되며 HTTPS 프로토콜을 지원하는 데 사용됩니다. Amazon CloudFront를 통해 콘텐츠를 배포하는 경우 이 서비스는 암호화된 엔드포인트를 지원합니다.

암호화 도구

AWS는 AWS에서 저장되고 처리되는 데이터를 보호하는 데 도움이 되는 확장성 높은 다양한 데이터 암호화 서비스, 도구 및 메커니즘을 제공합니다. AWS 서비스 기능 및 개인 정보 보호에 대한 자세한 내용은 개인 정보 보호 고려 사항을 위한 AWS 서비스 기능을 참조하세요.

AWS의 암호화 서비스는 저장된 데이터 또는 전송 중인 데이터의 무결성을 유지하기 위해 설계된 광범위한 암호화 및 스토리지 기술을 사용합니다. AWS는 암호화 작업을 위한 네 가지 기본 도구를 제공합니다.

- AWS Key Management Service(AWS KMS)는 마스터 키와 데이터 키를 모두 생성하고 관리하는 AWS 관리형 서비스입니다. AWS KMS는 많은 AWS 서비스와 통합되어 고객 계정의 AWS KMS 키를 사용하는 서버 측 데이터 암호화를 제공합니다. AWS KMS 하드웨어 보안 모듈(HSM)은 FIPS 140-2 레벨 2로 검증되었습니다.
- AWS CloudHSM은 FIPS 140-2 레벨 3로 검증된 HSM을 제공합니다. 이 모듈은 마스터 키와 데이터 키를 포함하여 다양한 자체 관리형 암호화 키를 안전하게 저장합니다.
- AWS 암호화 서비스 및 도구
  - AWS Encryption SDK는 모든 형식의 데이터에 대한 암호화 및 암호 해독 작업을 구현하는 클라이언트 측 암호화 라이브러리를 제공합니다.
  - Amazon DynamoDB Encryption Client는 데이터를 Amazon DynamoDB와 같은 데이터베이스 서비스로 전송하기 전에 데이터 테이블을 암호화하는 클라이언트 측 암호화 라이브러리를 제공합니다.

AWS Key Management Service

AWS Key Management Service는 데이터를 암호화하는 데 사용되는 암호화 키를 쉽게 생성하고 제어할 수 있는 관리형 서비스이며, 하드웨어 보안 모듈(HSM)을 사용하여 키의 보안을 보호합니다. AWS KMS는 다른 여러 AWS 서비스와 통합되어 이러한 서비스로 저장하는 데이터를 보호할 수 있도록 지원합니다. 또한 AWS KMS는 AWS CloudTrail과도 통합되어 규제 및 규정 준수 요구 사항에 맞게 모든 키 사용에 대한 로그를 제공합니다.

AWS Management Console에서 또는 AWS SDK나 AWS CLI를 사용하여 간편하게 키를 생성하고 가져오고 교체할 수 있을 뿐 아니라 사용 정책을 정의하고 사용을 감사할 수 있습니다.

AWS KMS의 CMK는 사용자가 가져오거나 사용자를 대신하여 KMS에서 생성되거나 어느 쪽이든 상관없이 모두 내구성이 우수한 스토리지에 암호화된 형식으로 저장되므로 필요할 때 항상 사용할 수 있습니다. 마스터 키로 이미 암호화된 데이터를 다시 암호화할 필요 없이 KMS에서 생성된 CMK를 KMS에

서 1년에 한 번 자동으로 교체하도록 선택할 수 있습니다. KMS에서는 이전에 암호화한 데이터를 자동으로 해독하기 위해 이전 버전의 CMK를 항상 사용할 수 있으므로 사용자는 CMK의 이전 버전을 추적할 필요가 없습니다.

AWS KMS의 모든 CMK에 대해 키 정책 또는 IAM 정책 내의 키 정책 조건 및 권한 부여를 포함한 다양한 액세스 제어를 통해 누가 해당 키에 액세스할 수 있으며 어떤 서비스에 키를 사용할 수 있는지를 제어할 수 있습니다. 또한 사용자가 자체 키 관리 인프라에서 키를 가져와서 KMS에서 사용할 수도 있습니다.

예를 들어 다음 정책은 `kms:ViaService` 조건을 사용하여 특정 리전(us-west-2)의 Amazon EC2 또는 Amazon RDS에서 특정 사용자(`ExampleUser`) 대신 요청을 수행하는 경우에만 고객 관리형 CMK를 지정된 작업에 사용할 수 있도록 허용합니다.

```
        {
         “Version”: “2012-10-17”,
         “Statement”: [
             {
                “Effect”: “Allow”,
                “Principal”: {
                    “AWS”: “arn:aws:iam::111122223333:user/ExampleUser”
                 }
                “Action”: [
                     “kms:Encrypt*”,
                     “kms:Decrypt”,
                     ”kms:ReEncrypt*”,
                     “kms:GenerateDataKey*”,
                     “kms:CreateGrant”,
                     “kms:ListGrants”,
                     “kms:DescribeKey”
                 ],
                 “Resource”: “*”,
                 “Condition”: {
                    “ForAnyValue:StringEquals”: {
                        “kms:ViaService”: [
                              “ec2.us-west-2.amazonaws.com”,
                              “rds.us-west-2.amazonaws.com”
                        ]
                     }
              }
}
```

AWS 서비스 통합

AWS KMS는 여러 AWS 서비스와 통합되었습니다. 통합 서비스의 전체 목록은 KMS 웹 사이트를 참조하세요. 이러한 통합 덕분에 AWS KMS CMK를 사용하여 이러한 서비스에 저장하는 데이터를 쉽게 암호화할 수 있습니다. 여러 통합 서비스에서는 고객 관리형 CMK를 사용할 수 있을 뿐 아니라 AWS 관리형 CMK도 사용할 수 있습니다. AWS 관리형 CMK는 자동으로 생성되고 관리되지만 해당 CMK를 생성한 특정 서비스 내에서만 사용할 수 있습니다.

감사 기능

AWS CloudTrail은 AWS KMS에서 저장하는 키의 각 사용을 로그 파일에 기록하며, 이 로그 파일은 CloudTrail의 구성에서 지정한 Amazon S3 버킷으로 전송됩니다. 기록되는 정보에는 사용자, 시간, 날짜, 수행된 작업, 사용된 키에 대한 세부 정보가 포함됩니다.

보안

AWS KMS는 아무도 마스터 키에 액세스할 수 없도록 설계되었습니다. 이 서비스는 일반 텍스트 마스터 키를 디스크에 저장하지 않고, 메모리에 계속 남겨 두지 않으며, 키를 사용하는 호스트에 액세스할 수 있는 시스템을 제한하는 등의 광범위한 강화 기법으로 마스터 키를 보호하도록 설계된 시스템을 기반으로 합니다. 서비스의 소프트웨어를 업데이트하기 위한 모든 액세스는 AWS 내의 독립적인 그룹에서 감사하고 검토하는 다자간 액세스 제어를 통해 제어됩니다.

AWS KMS에 대한 자세한 내용은 AWS Key Management Service 백서를 참조하세요.

AWS CloudHSM

AWS CloudHSM은 FIPS 140-2 레벨 3로 검증된 하드웨어에서 암호화 키를 생성하고 사용할 수 있도록 하여 데이터 보안에 대한 기업, 계약 및 규정 준수 요구 사항을 충족할 수 있도록 지원하는 클라우드 기반 하드웨어 보안 모듈(HSM)입니다.

AWS CloudHSM을 사용하면 암호화 키와 HSM에서 수행하는 암호화 작업을 제어할 수 있습니다.

AWS 및 AWS Marketplace 파트너는 AWS 플랫폼 내에서 민감한 데이터를 보호하기 위한 다양한 솔루션을 제공하지만, 암호화 키 관리에 대한 엄격한 계약 또는 규제 요구 사항이 적용되는 애플리케이션과 데이터의 경우 때로는 추가적인 보호가 필요합니다. 이전에는 민감한 데이터(또는 민감한 데이터를 보호하는 암호화 키)를 온프레미스 데이터 센터에 저장하는 것이 유일한 옵션이었을 수 있습니다. 이로 인해 이러한 애플리케이션을 클라우드로 마이그레이션하지 못하거나 성능이 크게 저하되었을 수 있습니다. AWS CloudHSM을 사용하면 안전한 키 관리를 위한 정부 표준에 따라 설계되고 검증된 HSM 내의 암호화 키를 보호할 수 있습니다. 데이터 암호화에 사용되는 암호화 키를 안전하게 생성, 저장 및 관

리하여 사용자만 이러한 키에 액세스할 수 있도록 할 수 있습니다. AWS CloudHSM은 애플리케이션 성능을 저하시키지 않으면서 엄격한 키 관리 요구 사항을 준수할 수 있도록 지원합니다.

AWS CloudHSM 서비스는 아마존 VPC와 함께 작동합니다. AWS CloudHSM 인스턴스는 사용자가 지정하는 IP 주소를 사용하여 Amazon VPC 내부에서 프로비저닝되므로, Amazon EC2 인스턴스에 대한 간단한 프라이빗 네트워크 연결을 제공합니다. Amazon EC2 인스턴스 근처에 HSM 인스턴스를 배치하면 네트워크 대기 시간이 감소하므로 애플리케이션 성능이 향상할 수 있습니다. AWS는 다른 AWS 고객으로부터 격리되는 HSM 인스턴스에 대한 전용 독점(단일 테넌트) 액세스를 제공합니다. 여러 리전 및 가용 영역에서 사용할 수 있으므로 AWS CloudHSM에서는 안전하고 내구력 있는 키 스토리지를 애플리케이션에 추가할 수 있습니다.

AWS 서비스 및 서드 파티 애플리케이션과 통합

CloudHSM을 Amazon Redshift, Amazon RDS for Oracle 또는 서드 파티 애플리케이션(예: SafeNet Virtual KeySecure)과 함께 신뢰할 수 있는 루트, Apache(SSL 종료) 또는 Microsoft SQL Server(투명한 데이터 암호화)로 사용할 수 있습니다. 또한 자체 애플리케이션을 작성할 때 AWS CloudHSM을 사용할 수 있으며 PKCS#11, Java JCA/JCE, Microsoft CAPI 및 CNG를 포함한 표준 암호화 라이브러리를 계속 사용할 수 있습니다.

감사 활동

보안 및 규정 준수를 위해 리소스 변경 사항을 추적하거나 활동을 감사해야 하는 경우 AWS CloudTrail을 사용하여 계정에서 수행된 AWS CloudHSM을 통한 관리 API 호출을 검토할 수 있습니다. 또한, syslog를 사용하여 HSM 어플라이언스의 작업을 감사하거나 syslog 로그 메시지를 자체 로그 수집기로 전송할 수 있습니다.

AWS 암호화 서비스 및 도구

AWS는 모범 사례 암호화를 구현하기 위해 사용할 수 있는 광범위한 암호화 보안 표준을 준수하는 메커니즘을 제공합니다. AWS 암호화 SDK는 Linux, macOS 및 Windows를 지원하는 Java, Python, C, JavaScript 및 명령줄 인터페이스에서 사용할 수 있는 클라이언트 측 암호화 라이브러리입니다. 이 도구 키트는 키 파생 및 서명 기능이 있는 256비트 AES-GCM과 같이 안전하고 인증된 대칭 키 알고리즘 제품군을 포함한 고급 데이터 보호 기능을 제공합니다. 이 도구 키트는 Amazon DynamoDB를 사용하는 애플리케이션을 위해 특별히 설계되었으므로 DynamoDB 암호화 클라이언트를 사용하면 사용자는 테이블 데이터가 데이터베이스로 전송되기 전에 테이블 데이터를 보호할 수 있습니다. 또한 데이터를 검색할 때 데이터를 검증하고 해독합니다. 클라이언트는 Java와 Python에서 사용할 수 있습니다.

Linux DM-Crypt 인프라

Dm-crypt는 사용자가 암호화된 파일 시스템을 탑재할 수 있는 Linux 커널 수준 암호화 메커니즘입니다. 파일 시스템 탑재는 파일 시스템을 디렉터리(탑재 지점)에 연결하여 운영 체제에서 사용할 수 있게 하는 프로세스입니다. 탑재한 후에는 추가 상호 작용 없이 파일 시스템의 모든 파일을 애플리케이션에서 사용할 수 있습니다. 하지만 이러한 파일은 디스크에 저장할 때 암호화됩니다.

디바이스 매퍼는 블록 디바이스의 가상 계층을 만드는 일반적인 방법을 제공하는 Linux 2.6 및 3.x 커널의 인프라입니다. 디바이스 매퍼 암호화 대상은 커널 암호화 API를 사용하여 블록 디바이스의 투명한 암호화를 제공합니다. 이 문서의 솔루션은 LVM(Logical Volume Manager)이 논리적 볼륨에 매핑한 디스크 지원 파일 시스템과 함께 dm-crypt를 사용합니다. LVM은 Linux 커널에 대한 논리적 볼륨 관리를 제공합니다.

설계를 통한 기본적인 데이터 보호

사용자나 애플리케이션이 AWS Management Console, AWS API 또는 AWS CLI를 사용하려고 할 때마다 요청이 AWS로 전송됩니다. AWS 서비스는 요청을 수신하고 일련의 단계를 실행하여 특정한 정책 평가 로직에 따라 요청을 허용할지 또는 거부할지를 결정합니다. 루트 자격 증명 요청을 제외하고 AWS에서 모든 요청은 기본적으로 거부됩니다(기본 거부 정책이 적용됨). 따라서 정책에 따라 명시적으로 허용되지 않은 모든 요청이 거부됩니다. 정책 정의와 모범 사례에서 AWS는 최소 권한 원칙을 적용할 것을 제안합니다. 이 원칙에 따르면, 모든 구성 요소(예: 사용자, 모듈 또는 서비스)는 작업을 완료하는 데 필요한 리소스에만 액세스할 수 있어야 합니다.

이 접근 방식은 “컨트롤러는 기본적으로 각 특정 처리 목적에 필요한 개인 데이터만 처리되도록 적절한 기술적 및 조직적 조치를 구현해야 한다"고 명시하는 GDPR 제25조와 일치합니다.

또한 AWS는 아키텍처 설계 시작부터 보안을 포함하기 위한 강력한 메커니즘인 코드형 인프라를 구현하는 도구를 제공합니다. AWS CloudFormation은 보안 정책 및 프로세스를 포함한 모든 인프라 리소스를 설명하고 프로비저닝하는 공통 언어를 제공합니다. 이러한 도구와 방법을 사용하면 보안이 코드의 일부가 되며 조직의 요구 사항에 따라 버전 관리, 모니터링 및 수정(버전 관리 시스템 사용)할 수 있습니다. 이렇게 하면 보안 프로세스 및 정책이 아키텍처 정의에 포함될 수 있고 조직의 보안 조치에서 지속적으로 모니터링될 수 있기 때문에 설계를 통한 데이터 보호를 실현할 수 있습니다.

AWS를 사용할 때의 이점

표 1 – AWS가 GDPR 규정 준수 탐색을 지원하는 방식

영역	설명	AWS 서비스 및 도구
강력한 규정 준수 프레임워크	적절한 기술적 및 조직적 조치에는 “처리 시스템과 서비스의 지속적인 기밀성, 무결성, 가용성 및 복원력을 보장할 수 있는 기능”이 포함되어야 할 수 있습니다.	SOC 1 / SSAE 16 / ISAE 3402(이전의 SAS 70) / SOC 2 / SOC 3 PCI DSS 레벨 1 ISO 9001 / ISO 27001 / ISO 27017 / ISO 27018 NIST FIPS 140-2 C5(Common Cloud Computing Controls Catalog)
데이터 액세스 제어	컨트롤러는 "…기본적으로 각 특정 처리 목적에 필요한 개인 정보만 처리하도록 적절한 기술적 및 조직적 조치를 구현해야 합니다."	AWS Identity and Access Management(IAM) Amazon Cognito AWS Shield 및 AWS WAF AWS Resource Access Manager Amazon CloudFront AWS Organizations AWS CloudTrail
모니터링 및 로깅	“각 컨트롤러와 해당되는 경우 컨트롤러 대리인은 자신의 책임으로 처리 활동 기록을	AWS Config Amazon CloudWatch AWS Control Tower

영역	설명	AWS 서비스 및 도구
	유지 관리해야 합니다.” “...컨트롤러와 프로세서는 위험에 적절한 수준의 보안을 보장할 수 있는 적절한 기술적 및 조직적 조치를 구현해야 합니다 [...]”	Amazon GuardDuty Amazon Inspector Amazon Macie AWS Systems Manager AWS Security Hub AWS 도구 및 SDK
AWS에서 데이터 보호	조직은 "개인 정보의 가명 처리 및 암호화를 포함하여 위험에 적절한 수준의 보안을 보장할 수 있는 적절한 기술적 및 조직적 조치를 구현"해야 합니다.	AWS Certificate Manager AWS CloudHSM AWS Key Management Service

기여자

이 문서를 작성하는 데 도움을 주신 분들입니다.

- Tim Anderson, Amazon Web Services 기술 산업 전문가
- Carmela Gambardella, Amazon Web Services 공공 부문 솔루션스 아키텍트
- Giuseppe Russo, Amazon Web Services 보안 보증 관리자
- Marta Taggart, Amazon Web Services 선임 프로그램 관리자
- Luca Iannario, Amazon Web Services 공공 부문 솔루션스 아키텍트

문서 수정

날짜	설명
2017년 11월	최초 게시
2020년 12월	새로운 AWS 서비스 및 기능 추가를 포함하도록 업데이트했습니다.

고지 사항

고객은 본 문서에 포함된 정보를 독자적으로 평가할 책임이 있습니다. 본 문서는 (a) 정보 제공 용도로만 제공되고, (b) 고지 없이 변경될 수 있는 현재 AWS 제품 제공 및 사례를 보여 주며, (c) AWS 및 자회사, 공급자 또는 라이선스 제공자의 어떠한 약정이나 보증도 나타내지 않습니다. AWS 제품 또는 서비스는 명시적이든 묵시적이든 어떠한 종류의 보증, 진술 또는 조건도 없이 “있는 그대로” 제공됩니다. 고객에 대한 AWS의 책임과 법적 책임은 AWS 계약서에 준하며 본 문서는 AWS와 고객 간의 계약에 포함되지 않고 계약을 변경하지도 않습니다.