규모별 보안: AWS에서 로깅하기

AWS CloudTrail이 API 호출 및 리소스에 대한 변경을 로깅하여 규정 준수에 도움을 주는 방법

2015년 10월

(https://aws.amazon.com/compliance/aws-whitepapers/에서

이 문서의 최신 버전을 보실 수 있습니다.)

목차

요약

API 호출을 로깅하고 모니터링하는 것은 보안의 핵심 구성 요소이자 운영상의 모범 사례일 뿐만 아니라 업계 표준 및 규정을 준수하기 위한 요건이기도 합니다. AWS CloudTrail은 지원되는 AWS 서비스에 대한 API 호출을 기록하고 로그 파일을 Amazon Simple Storage Service(S3) 버킷으로 전달하는 웹 서비스입니다. AWS CloudTrail은 온프레미스 환경에서 겪는 흔한 문제를 완화합니다. 이 서비스는 또한 정책 또는 규제 표준 준수를 보여주는 일뿐만 아니라 보안 및 운영 프로세스 강화도 더 쉽게 만들어 줍니다.

이 문서는 로깅과 관련된 일반적인 규정 요건의 개요를 제공하고 AWS CloudTrail의 기능이 이 요건들을 충족하는 데 어떤 도움이 되는지 자세히 설명합니다. 로그 스토리지를 위한 S3 표준 요금과 선택적으로 알림 사용시 부과되는 SNS 요금 이외에 AWS CloudTrail에 대한 추가 요금은 없습니다.

서론

Amazon Web Services(AWS)는 직접 시작하고 관리할 수 있는 광범위한 주문형 IT 리소스 및 서비스를 종량 과금제 방식으로 제공합니다. AWS API 호출 및 이와 연관된 리소스 구성의 변경 사항을 기록하는 것은 IT 거버넌스, 보안 및 규정 준수의 중요 구성 요소입니다. AWS CloudTrail은 AWS API 호출 및 리소스 변경 사항을 기록하는 간단한 솔루션으로서, AWS 환경에 대해 향상된 사전적 및 사후적 보안 컨트롤을 구축하는 데 도움을 주어, 온프레미스 인프라 및 스토리지 문제점이 주는 부담을 완화해줍니다. 온프레미스 로깅 솔루션을 위해서는 에이전트 설치, 설정 파일 및 중앙 집중식 로그 서버 셋팅, 데이터를 저장할 내구성이 뛰어난 고가의 데이터 스토어 구성 및 유지보수가 필요합니다. AWS CloudTrail은 부담스러운 인프라 설정 없이 단 두 번의 클릭으로 로깅 기능을 활성화하고 AWS 계정에서 이루어지는 모든 API 호출을 시각적으로 더 정확하게 인식할 수 있도록 허용합니다. CloudTrail은 다수의 서버가 동시에 사용하는 API 호출들을 고가용성의 프로세싱 파이프라인으로 지속적으로 캡처합니다. CloudTrail을 활성화하려면 AWS Management Console에 로그인해 CloudTrail 콘솔로 이동한 다음, 클릭을 통해 로깅을 활성화하기만 하면 됩니다. AWS CloudTrail이 지원되는 서비스 및 리전에 대해서는 AWS CloudTrail 웹 사이트에서 자세히 알아보십시오.

이 문서는 일반적인 규정 준수 프레임워크(예: ISO 27001:2005, PCI DSS v2.0, FedRAMP 등) 전반의 로깅 요건을 일일이 조사하고 그 요건들을 일반화된 제어 및 로깅 도메인들로 통합하는 방식으로 개발되었습니다. 이 문서를 보안 및 운영 모범 사례, 내부 정책 준수, 산업 표준, 법적 규제 등과 같은 다양한 사용 사례에 맞게 활용할 수 있습니다. 이 문서는 AWS CloudTrail이 어떻게 기존의 로깅 및 모니터링 활동을 향상시킬 수 있는지 누구나 이해할 수 있게 작성되었습니다.

로그 파일에 대한 액세스 제어

로그 데이터의 무결성을 확보하려면, 로그 파일의 생성 및 저장에 대한 권한을 신중하게 관리하는 것이 중요합니다. 로그 데이터를 보거나 수정할 수 있는 권한은 인가된 사용자만에게만 주어져야 합니다. 온프레미스 환경 하에서의 일반적인 로그 관련 문제는, 인가된 사용자들만 로그 데이터로 액세스가 허용된다는 것을 규제 담당자에게 보여 주는 것이 관건입니다. 이러한 제어를 효과적으로 보여주려면 시간이 걸리고 복잡한 과정이 필요한데, 그 이유는 대부분의 온프레미스 환경이 모든 시스템에 걸쳐 단일한 로깅 솔루션 또는 일관된 로깅 보안을 갖고 있지 않기 때문입니다.

AWS CloudTrail을 사용해 Amazon S3 로그 파일에 대한 액세스를 AWS에서 중앙 통제할 수 있는데, 이렇게 하면 로그 파일에 대한 액세스를 쉽게 제어할 뿐만 아니라 로그 데이터의 무결성 및 기밀성을 보여주는 데 도움이 될 수 있습니다.

로그 파일에 대한 액세스 제어	일반적인 로깅 요건	AWS CloudTrail이 규정 요건을 충족시키는 방법
	로그에 대한 무단 액세스를 방지하는 컨트롤이 있습니다.	AWS CloudTrail은 로그 파일에 대한 액세스를 제한할 수 있는 권한을 제공합니다. 로그 파일에 읽기전용 액세스만 허용하기 위해, AWS Identity and Access Management(IAM) 역할 및 Amazon S3 버킷 정책을 구성함으로써, 로그 파일에 접근해 데이터를 변경하려는 시도를 방지하고 제어할 수 있습니다. 자세히 알아보기. 뿐만 아니라 AWS CloudTrail 로그를 저장하는 Amazon S3 버킷에 대한 AWS Multi-Factor Authentication(MFA)을 활성화함으로써 인증 및 인가 제어를 강화할 수 있습니다. 자세히 알아보기.
	로그 레코드에 대한 액세스가 역할 기반인지 확인하는 컨트롤이 있습니다.	AWS CloudTrail은 상세한 역할 기반 권한 설정을 통해, 로그 파일에 대한 사용자 액세스를 제어할 수 있는 능력을 제공합니다. AWS Identity and Access Management(IAM)는 사용자들을 위해 AWS CloudTrail에 대한 액세스를 안전하게 제어할 수 있게 해줍니다. 또한 IAM 역할과 Amazon S3 버킷 정책을 사용해 AWS CloudTrail 로그 파일을 저장하는 S3 버킷에 대한 역할 기반 액세스를 적용할 수 있습니다. 자세히 알아보기.

로그 파일 생성 및 구성 오류에 대한 알림 받기

상세한 API 호출 또는 리소스 변경에 대한 로그 내역 중, 구성 오류에 대한 실시간에 가까운 알림은, 효과적인 IT 거버넌스와 내부 및 외부 준수 요건을 지키는데 매우 중요합니다. 운영상의 관점에서 보더라도 로깅을 적절히 구성하여 사용자 및 리소스의 활동을 감독할 수 있는 기능은 필수적입니다. 그러나 온프레미스 환경에서 로깅 인프라가 지닌 가변성과 광범위성으로 인해, 구성의 오류나 로깅 구성의 변경이 있는 경우 능동적인 모니터링과 알림이 엄청난 부담이 되었습니다.

일단 계정에 대한 AWS CloudTrail을 활성화하면, AWS CloudTrail은 S3 버킷으로 로그 파일을 저장할 것입니다. 선택 사항으로, CloudTrail은 SNS 특정 topic으로 로그 파일 전송하여 SNS 알림을 배포하여, 배포 즉시 조치를 취할 수 있게 합니다. 이러한 알림에는 Amazon S3 버킷 로그 파일 주소가 포함되어 있어 해당 로그 파일에서 발생한 알람에 대해 신속하게 객체 메타데이터에 액세스할 수 있도록 허용합니다. 게다가 AWS Management Console은 로그 파일이 잘못 구성되어 로깅이 더 이상 발생하지 않는 경우 이를 알려 줍니다.

로그 파일에 대한 알림 받기 생성 및 구성 오류	일반적인 로깅 요건	AWS CloudTrail이 규정 요건 준수를 돕는 방법
	로그 생성 또는 실패 시 알려주고 구성 오류 발생 시 조직이 정의한 작업을 따릅니다.	AWS CloudTrail은 AWS Management Console을 통해 로깅 구성의 문제점에 관해 즉각적인 알림을 제공합니다. 자세히 알아보기.
	로그 구성 오류와 관련된 알림은 사용자를 관련 로그를 보도록 유도하여 부가적인 세부 정보를 얻을 수 있게 합니다(불필요한 세부 정보는 알려 주지 않습니다).	AWS CloudTrail은 새 로그 파일이 작성될 때마다 Amazon S3 버킷 로그 파일 주소를 기록합니다. AWS CloudTrail은 로그 파일 생성에 대한 알림을 게시함으로써 로그 파일 생성 시 고객들이 실시간에 가까운 조치를 취할 수 있습니다. 알림은 Amazon S3 버킷으로 전송되어 AWS Management Console에 표시됩니다. 옵션 사항으로, Amazon SNS 메시지를 API 또는 AWS Management Console을 통해 구성된 모바일 디바이스나 분산된 서비스에 푸시할 수 있습니다. 로그 파일 생성에 대한 SNS 메시지는 로그 파일 주소를 담고있는데, 이를 통해 필요한 정보만 제공되도록 제한하는 한편, 쉽게 링크를 통해 알람 이벤트에 대한 부가적인 세부 정보를 얻을 수 있습니다. 자세히 알아보기.

AWS 리소스 및 로그 파일에 대한 변경 사항 관리

리소스에 적용된 변경 내역을 이해하는 것은 IT 거버넌스 및 보안의 중대한 구성 요소입니다. 뿐만 아니라 이 로그 데이터에 대한 변경 및 무단 액세스를 방지하는 것은 변경 관리 프로세스의 무결성과 변경 관리에 대한 내부, 업계 및 규제 요건을 준수할 수 있는 능력에 영향을 미칩니다. 온프레미스 환경에서 직면하게 되는 주요 문제는 리소스 변경 또는 로그에 대한 변경을 추적할 수 있는 능력인데, 그 이유는 무한한 것처럼 느껴지는 데이터 양을 모니터링할 수 있는 가용 리소스가 제한적이기 때문입니다.

AWS CloudTrail은 생성, 변경, 삭제 등 AWS 리소스에 대한 변경을 추적할 수 있도록 허용합니다. 뿐만 아니라 AWS CloudTrail은 API 호출의 로그 기록을 검토함으로써 하나의 이벤트를 조사해 무단 또는 예기치 않은 변경을 누가 시작했는지, 발생 시점은 언제인지, 그리고 어디서 비롯되었는지 검토함으로써 그러한 변경이 발생했는지 여부를 결정하는 데 도움을 줍니다. 선택 사항으로, CloudTrail은 특정 SNS 토픽으로 로그 파일 전송 알림을 전달함으로써 Amazon S3 버킷에 새로운 로그 파일이 전송되자마자 즉시 조치를 취할 수 있습니다.

IT 리소스 및 로그 파일에 대한 변경 사항 관리	일반적인 로깅 요건	AWS CloudTrail이 규제 요건 준수를 돕는 방법
	시스템 구성 요소에 대한 변경 사항의 로그를 제공합니다(시스템 수준 객체의 생성 및 삭제 포함).	AWS CloudTrail은 시스템 변경 이벤트에 대한 로그 데이터를 생성해 AWS 리소스에 대한 변경 사항을 추적할 수 있게 해줍니다. AWS CloudTrail은 AWS Management Console, AWS 명령줄 인터페이스 또는 AWS 소프트웨어 개발 키트(SDK)를 통한 API 호출을 사용해 이루어진 변경 사항들을 로깅함으로써 AWS 리소스의 생성부터 삭제까지 AWS 리소스에 발생한 모든 변경 사항을 볼 수 있도록 해줍니다. 자세히 알아보기.
	로그와 연관된 변경 또는 실패 관련 로그에 대한 수정을 방지하는 컨트롤이 있습니다.	기본적으로 API 호출 로그 파일은 S3 서버 쪽 암호화(SSE)를 사용해 암호화되어 S3 버킷에 배치됩니다. 로그 데이터에 대한 수정은 AWS CloudTrail 로그 파일을 저장하는 Amazon S3 버킷에 대해 읽기 전용 액세스 권한을 적용하여 IAM 및 MFA를 통해 통제할 수 있습니다. 자세히 알아보기.

로그 파일 저장

업계 표준 및 법적 규정에 따라 로그 파일을 다양한 기간동안 저장하도록 요구될 수 있습니다. 예를 들어 PCI DSS는 로그를 1년 동안 저장하도록 요구하고, HIPAA는 최소한 6년 동안 기록을 보유할 것을 요구하며, 기타 요건들은 로깅되는 데이터에 따라 저장 기간이 더 길어지거나 가변적이어야 한다고 규정하고 있습니다. 따라서 다양한 시스템의 다양한 데이터에 대한 로그 파일 저장 요건을 관리하는 것은 관리 및 기술 측면에서 부담이 될 수 있습니다. 뿐만 아니라 일관성 있고 안전한 방식으로 방대한 볼륨의 로그 데이터를 저장 및 보관하는 일은 많은 조직에게 쉽지 않은 일입니다.

AWS CloudTrail은 Amazon S3 및 Amazon Glacier와 원활하게 통합되도록 설계되어 있어, S3 버킷 및 수명 주기 규칙에 대한 사용자 정의를 허용해 스토리지 요구 사항을 충족시켜줍니다. AWS CloudTrail은 로그에 확정되지 않은 만료 기간을 제공함으로써 로그 저장 기간을 사용자 정의하여 규제 담당자의 요건을 충족할 수 있습니다.

	일반적인 로깅 요건	AWS CloudTrail이 규제 요건 준수를 돕는 방법
로그 파일 저장	로그는 최소한 1년 동안 저장됩니다.	로그 파일 저장을 쉽게 하려면 모든 리전 및 여러 계정에 분산되어 있는 로그 파일을 하나의 S3 버킷에 집계하도록 AWS CloudTrail을 구성할 수 있습니다. AWS CloudTrail은 Amazon S3 버킷에 쓰여진 로그 파일에 대해 원하는 만료 기간을 구성함으로써 로그 저장 기간을 사용자 정의할 수 있도록 합니다. CloudTrail 로그 파일에 대한 보존 정책을 제어합니다. 선택한 기간 동안 또는 기한 없이 로그 파일을 보유할 수 있습니다. 기본적으로 로그 파일은 특정 기한이 없이 저장됩니다. 또한 자신의 로그 파일 데이터를 Amazon Glacier로 옮겨 콜드 스토리지와 관련된 비용 절감도 추가로 가능합니다. 자세히 알아보기.
	조직이 정의한 기간 동안 로그를 저장합니다.	
	복원성을 위해 로그를 실시간으로 저장합니다.	AWS CloudTrail은 내구성이 뛰어난 스토리지 인프라인 Amazon S3를 최대한 활용해 로그 파일 복원성을 제공합니다. Amazon S3의 표준 스토리지는 연간 99.999999999%의 내구성과 99.99%의 객체 가용성을 지니도록 설계되었습니다. 자세히 알아보기.

로그 데이터에 대한 사용자 지정 보고 생성

운영 및 보안의 관점에서, API 호출 로깅은 사용자 행동을 분석하고 특정 이벤트를 이해하는 데 필요한 데이터 및 컨텍스트를 제공합니다. 또한 API 호출 및 IT 리소스 변경 로그를 사용해, 권한이 있는 사용자들만이 규정 준수 요건을 지키면서 귀하의 환경에서 특정 작업을 수행해왔다는 것을 보여줄 수 있습니다. 그러나 다양한 시스템의 로그와 연관되어 있는 볼륨 및 가변성으로 인해, 사용자들이 수행한 활동 및 IT 리소스의 변경 사항을 명확히 이해하는 것은 온프레미스 환경에서는 까다로운 일이 될 수 있습니다.

AWS CloudTrail은 비정상적인 행동 탐지, 특정 객체와 관련된 이벤트 활동 조회, 또는 계정에 대한 단순 감사 추적 제공에 사용할 수 있는 데이터를 산출합니다. AWS CloudTrail이 제공하는 이벤트 데이터에서 25개 이상의 다양한 필드를 사용해 현재 로깅 분석을 전개함으로써 쿼리를 만들고 내부 조사, 외부 준수 등에 초점을 맞춘 사용자 지정 보고서를 생성할 수 있습니다. AWS CloudTrail은 로그 관리 또는 보안 사고 및 이벤트 관리(SIEM) 솔루션들을 사용하여 API 호출을 모니터링해 원하지 않는 알려진 특정 행동을 찾아내고 경보를 생성할 수 있도록 해줍니다. AWS CloudTrail이 제공하는 풍부한 데이터로 인해 조사 시간을 단축하고 사고 응답

시간을 줄일 수 있습니다. 뿐만 아니라 AWS CloudTrail이 제공하는 데이터를 이용해 API 호출에 대한 심도 있는 보안 분석을 수행할 수 있게 됨으로써 즉각적인 경보를 발생시키지 않지만 보안상의 문제를 나타내는 것일 수도 있는 의심스러운 행동 및 잠재 패턴을 식별할 수 있습니다. 끝으로 AWS CloudTrail은 보안, 분석 및 알림에 대한 레디 투 런(ready-to-run) 솔루션을 보유한 광범위한 파트너들과 함께 작업합니다. AWS CloudTrail 웹 사이트에서 파트너 솔루션에 대해 자세히 알아보십시오.

로그 데이터에 대한 사용자 지정 보고 생성	일반적인 로깅 요건	AWS CloudTrail이 규제 요건 준수를 돕는 방법
	액세스되는 시스템과 수행되는 작업에 따라 리소스에 대한 개별 사용자들의 액세스를 로깅합니다. "개별 사용자들의 액세스"에는 시스템 관리자 및 시스템 운영자에 의한 액세스가 포함되고, "리소스"에는 감사 추적 로그가 포함되어 있습니다.	AWS CloudTrail은 루트, IAM 사용자, 연동 사용자, 또는 사용자들 대신 액세스 메서드를 사용해 활동을 전개하는 모든 사용자 또는 서비스를 포함해 로깅된 AWS 리소스에 액세스하는 모든 사용자들이 전개하는 활동을 로깅함으로써 종합적이고 상세한 API 호출 보고서를 생성할 수 있는 능력을 제공합니다. 자세히 알아보기.
	조직이 정의한 빈도로 로그를 생성합니다.	AWS CloudTrail을 통해 로그 분석 도구를 사용할 수 있게 됨으로써 거의 실시간으로 로그를 생성하고 API 호출 후 15분 이내에 Amazon S3 버킷에 로그 데이터를 일반적으로 전송하여 사용자 지정 빈도로 로그 파일 데이터를 가져올 수 있습니다. 로그 파일을 산업별 주요 로그 관리 및 분석 솔루션에 입력하여 분석할 수 있습니다. 자세히 알아보기.
	로깅 활동 시작 시점에 대한 로그를 제공합니다.	AWS CloudTrail은 AWS CloudTrail 로깅을 활성화하고 비활성화하는 것을 비롯한 모든 API 호출을 로깅합니다. 이를 통해 CloudTrail이 언제 활성화 또는 비활성화되는지 추적할 수 있습니다. 자세히 알아보기.
	단일 내부 시스템 클록에 동기화된 로그를 생성해 일관된 타임스탬프 정보를 제공합니다.	AWS CloudTrail은 ISO 8601 기본 날짜 시간 형식 표준과 일치되도록 협정 세계시(UTC)에 이벤트 타임스탬프를 생성함으로써 단일 내부 시스템 클록으로부터 로그 데이터를 생성합니다. 자세히 알아보기.
	부적절하거나 비정상적인 활동이 발생했는지 여부를 보여줄 수 있는 로그를 제공합니다.	AWS CloudTrail은 AWS 계정에서 일어난 권한 부여 실패를 기록해 API 호출을 모니터링할 수 있게 해줌으로써 제한된 리소스에 대한 액세스 시도 또는 기타 비정상적인 활동을 추적할 수 있게 합니다. 자세히 알아보기.
	충분한 이벤트 상세 정보를 가진 로그를 제공합니다.	AWS CloudTrail은 유형, 데이터 및 시간, 위치, 소스/오리진, 결과(예외, 오류 및 보안 이벤트 정보 포함), 영향받은 리소스(데이터, 시스템 등), 연결된 사용자 등의 세부 정보를 지닌 API 호출을 제공합니다. AWS CloudTrail은 사용자, 이벤트 발생 시각, 사용자의 IP 주소, 사용자가 제공하는 요청 파라미터, 서비스가 반환한 응답 요소, 그리고 옵션인 오류 코드와 오류 메시지를 식별하는 데 도움이 됩니다. 자세히 알아보기.

결론

온프레미스에서 실행하는 거의 모든 작업을 AWS에서도 실행할 수 있습니다. 웹 사이트, 애플리케이션, 데이터베이스, 모바일 앱, 이메일 캠페인, 분산 데이터 분석, 미디어 스토리지 및 프라이빗 네트워크 등이 그 예입니다. AWS가 제공하는 서비스는 다른 서비스와 연계되어 동작하도록 설계되어 완전한 솔루션으로 구축할 수 있습니다. AWS CloudTrail은 사용자 활동을 로깅하는 간단한 솔루션을 제공하여 복잡한 로깅 시스템을 실행해야 하는 부담을 줄여 줍니다. AWS로 워크로드를 마이그레이션하는 것이 주는 또 다른 이점은, 제공되는 많은 거버넌스 활성화 기능을 활용함으로써 실제로 더 높은 보안 수준을 달성할 수 있다는 것입니다. 클라우드상의 인프라를 전달하는 것이 온프레미스 전달보다 우월한 이점이 있는 것과 동일한 이유로, 클라우드 기반 거버넌스는 더 많은 가시성, 보안 제어, 중앙 자동화를 제공함으로써 더 낮은 초기 비용, 더 쉬운 작업, 개선된 민첩성 등의 이점을 제공합니다. AWS CloudTrail은 AWS를 사용하는 IT 리소스에 대한 높은 수준의 거버넌스를 달성하기 위해 사용할 수 있는 서비스 중 하나입니다.

추가 리소스

다음 링크는 AWS 로깅과 관련된 일반적인 질문에 대한 답변입니다.

- AWS로 할 수 있는 작업은 무엇입니까? 자세히 알아보기.
- AWS를 사용하려 하는데 처음에 어떻게 시작해야 하나요? 자세히 알아보기.
- AWS CloudTrail을 사용하려 하는데 처음에 어떻게 시작해야 하나요? 자세히 알아보기.
- AWS CloudTrail에 FAQ 목록이 있나요? 자세히 알아보기.
- AWS를 사용하는 동안 규제를 잘 준수하려면 어떻게 해야 하나요? 자세히 알아보기.
- AWS를 사용하는 동안 감사를 준비하려면 어떻게 해야 하나요? 자세히 알아보기.

부록: 규정 준수 프로그램 인덱스

위 백서의 정보는 로깅 요건 도메인별로 제시되었습니다. 참고 사항으로, 일반적인 규제 준수 프레임워크별 로깅 요건이 아래 표에 나열되어 있습니다.

AWS 규정 준수 프로그램	규제 준수 요건
지불 카드 산업(PCI) 데이터 보안 표준(DSS) 레벨 1 AWS는 PCI DSS의 레벨 1을 준수합니다. PCI 정책 준수 기술 인프라에서 애플리케이션을 실행하여 클라우드상의 신용카드 정보를 저장, 처리, 전송할 수 있습니다. 자세히 알아보기.	**PCI 5.2:** 모든 안티바이러스 메커니즘이 현재 활발히 실행되고 있고 감사 로그를 생성하고 있는지 확인합니다.
	PCI 10.1: 시스템 구성 요소에 대한 모든 액세스(특히 루트와 같은 관리자 권한을 사용한 액세스)를 각 개별 사용자에게 연결하는 프로세스를 수립합니다.
	PCI 10.2: 모든 시스템 구성 요소에 대한 자동화된 감사 추적을 실행함으로써 다음 이벤트들을 재구성합니다. **10.2.1:** 카드 소지자 데이터에 대한 모든 개별 액세스 **10.2.2:** 루트 또는 관리 권한이 있는 개인이 수행하는 모든 작업 **10.2.3:** 모든 감사 추적에 대한 액세스 **10.2.4:** 잘못된 논리적 액세스 시도 **10.2.5:** 식별 및 인증 메커니즘 사용 **10.2.6:** 감사 로그 초기화 **10.2.7:** 시스템 수준의 객체 생성 및 삭제
	PCI 10.3: 각 이벤트마다 모든 시스템 구성 요소에 대해 최소한 다음과 같은 감사 추적 항목들을 기록합니다. **10.3.1:** 사용자 식별 **10.3.2:** 이벤트 유형 **10.3.3:** 날짜 및 시간 **10.3.4:** 성공 또는 실패 표시 **10.3.5:** 이벤트가 시작된 지점 **10.3.6:** 영향을 받은 데이터, 시스템 구성 요소 또는 리소스의 ID나 이름
	PCI 10.4.2: 시간 데이터는 보호됩니다.
	PCI 10.5: 감사 추적을 보호함으로써 변경되지 않도록 할 수 있습니다.
	PCI 10.5.1: 직무와 관련해 필요한 사용자들로 감사 추적 열람을 제한합니다.
	PCI 10.5.2: 비인가된 수정으로부터 감사 추적 파일을 보호합니다.
	PCI 10.5.3: 감사 추적 파일을 중앙 집중식 로그 서버 또는 변경하기 어려운 미디어에 신속히 백업합니다.

AWS 규정 준수 프로그램	규제 준수 요건
지불 카드 산업(PCI) 데이터 보안 표준(DSS) 레벨 1 AWS는 PCI DSS의 레벨 1을 준수합니다. PCI 정책 준수 기술 인프라에서 애플리케이션을 실행하여 클라우드상의 신용카드 정보를 저장, 처리, 전송할 수 있습니다. 자세히 알아보기.	**PCI 10.5.4:** 내부 LAN에서 외부로 연결되는 기술에 대한 로그를 로그 서버에 작성합니다.
	PCI 10.5.5: 로그에 대해 파일 무결성 모니터링 기능 또는 변화 감지 소프트웨어를 사용함으로써 기존 로그 데이터를 변경하면 반드시 알림이 생성되도록 되어 있는지 확인합니다(단, 새로운 데이터를 추가한다고 해서 알림이 생성되어서는 안 됨).
	PCI 10.6: 모든 시스템 구성 요소의 로그를 최소한 매일 검토합니다. 로그 검토에는 침입 탐지 시스템(IDS), AAA(인증, 권한 부여 및 계정 관리 프로토콜) 서버 등 보안 기능을 수행하는 서버(예: RADIUS 서버)가 포함되어야 합니다.
	PCI 10.7: 최소 1년간은 감사 추적 이력을 보존하되, 그 중 최소 3개월은 즉각적인 분석이 가능해야 합니다(예: 온라인, 아카이브, 또는 백업에서 복원 가능).
	PCI 11.5: 중요 시스템 파일, 구성 파일, 또는 콘텐츠 파일이 무단으로 수정된 경우 담당자에게 알릴 수 있도록 파일 무결성 모니터링 도구를 배포합니다. 소프트웨어를 구성해 최소한 매주 중요 파일 비교를 수행합니다.
	PCI 12.2: 이 사양의 요건들과 일치하는 매일 수행할 수 있는 운영상의 보안점검 절차를 개발합니다(예: 사용자 계정 유지보수 절차 및 로그 검토 절차).
	PCI A.1.2.d: 각 엔터티의 액세스 및 권한을 고유한 카드 소지자 데이터 환경으로 제한합니다.
	PCI A.1.3: 로깅 및 감사 추적이 활성화되어 있고, 각 엔터티의 카드 소지자 데이터 환경이 고유하며, PCI DSS 요건 10과 일치하는지 확인합니다.
	PCI 11.4: 침입 탐지 시스템 및/또는 침입 방지 시스템을 사용해 카드 소지자 데이터 환경의 주변뿐만 아니라 카드 소지자 데이터 환경 내부의 임계점에서 발생하는 모든 트래픽을 모니터링하고 의심스러운 위반을 담당자에게 알립니다. 모든 침입 탐지 및 방지 엔진, 기준, 서명을 최신 상태로 유지합니다.

AWS 규정 준수 프로그램	규제 준수 요건
지불 카드 산업(PCI) 데이터 보안 표준(DSS) 레벨 1 AWS는 PCI DSS의 레벨 1을 준수합니다. PCI 정책 준수 기술 인프라에서 애플리케이션을 실행하여 클라우드상의 신용카드 정보를 저장, 처리, 전송할 수 있습니다. 자세히 알아보기.	**PCI 11.5:** 중요 시스템 파일, 구성 파일, 또는 콘텐츠 파일이 무단으로 수정된 경우 담당자에게 알릴 수 있도록 파일 무결성 모니터링 도구를 배포합니다. 소프트웨어를 구성해 최소한 매주 중요 파일 비교를 수행합니다.
SOC(Service Organization Control) 2 (SOC 2) SOC 2 보고서는 미국 공인 회계사 협회(AICPA) 트러스트 서비스 원칙에 규정된 기준으로 컨트롤 평가를 확장하는 인증 보고서입니다. 이러한 원칙에는 보안, 가용성, 처리 무결성, 기밀성 및 AWS와 같은 서비스 조직에 적용할 수 있는 개인 정보 보호와 관련된 주요 사례 규제 항목이 정의되어 있습니다. 자세히 알아보기.	**SOC 2 보안 3.2.g:** 다음 문제를 포함하지만 이에 국한되지 않은 정의된 시스템에 대한 논리적 액세스를 제한하기 위한 절차가 있습니다. 시스템 구성, 수퍼유저 기능, 마스터 암호, 강력한 유틸리티, 보안 디바이스(예: 방화벽)에 대한 액세스 제한.
	SOC 2 보안 3.3: 설비, 백업 미디어, 그리고 방화벽, 라우터, 서버와 같은 기타 시스템 구성 요소들을 포함하지만 이에 국한되지 않은 정의된 시스템에 대한 물리적 액세스를 제한하는 절차가 있습니다.
	SOC 2 보안 3.7: 시스템 보안 위반 및 기타 사고에 대한 식별, 보고, 조치를 위한 절차들이 있습니다.
	SOC 2 가용성 3.5.f: 다음 문제를 포함하지만 이에 국한되지 않은 정의된 시스템에 대한 논리적 액세스를 제한하기 위한 절차가 있습니다. 시스템 구성, 수퍼유저 기능, 마스터 암호, 강력한 유틸리티, 보안 디바이스(예: 방화벽)에 대한 액세스 제한.
	SOC 2 가용성 3.6: 설비, 백업 미디어, 그리고 방화벽, 라우터, 서버와 같은 기타 시스템 구성 요소들을 포함하지만 이에 국한되지 않은 정의된 시스템에 대한 물리적 액세스를 제한하는 절차가 있습니다.

AWS 규정 준수 프로그램	규제 준수 요건
SOC(Service Organization Control) 2 (SOC 2) SOC 2 보고서는 미국 공인 회계사 협회(AICPA) 트러스트 서비스 원칙에 규정된 기준으로 컨트롤 평가를 확장하는 인증 보고서입니다. 이러한 원칙에는 보안, 가용성, 처리 무결성, 기밀성 및 AWS와 같은 서비스 조직에 적용할 수 있는 개인 정보 보호와 관련된 주요 사례 규제 항목이 정의되어 있습니다. 자세히 알아보기.	**SOC 2 가용성 3.10:** 시스템 가용성 문제, 관련 보안 위반 및 기타 사고에 대한 식별, 보고, 조치를 위한 절차가 있습니다.
	SOC 2 기밀성 3.3: 데이터 처리의 기밀성에 관련된 시스템 절차는 문서화된 기밀성 정책과 일치합니다.
	SOC 2 기밀성 3.8.1: 다음 문제를 포함하지만 이에 국한되지 않은, 시스템에서 유지되는 기밀 정보 리소스 및 해당 시스템에 대한 물리적 액세스를 제한하는 절차가 있습니다. 시스템 구성, 수퍼유저 기능, 마스터 암호, 강력한 유틸리티, 보안 디바이스(예: 방화벽)에 대한 액세스 제한.
	SOC 2 기밀성 3.13: 시스템 기밀성 및 보안 위반과 기타 사고에 대한 식별, 보고, 조치를 위한 절차가 있습니다.
	SOC 2 기밀성 4.2: 시스템 기밀성 및 관련 보안 정책과 일치하는 목표를 달성할 수 있는 엔터티의 지속적인 능력에 대한 잠재적 장애를 식별하고 그에 대처하는 프로세스가 있습니다.
	SOC 2 무결성 3.6.g: 다음 문제를 포함하지만 이에 국한되지 않은 정의된 시스템에 대한 논리적 액세스를 제한하기 위한 절차가 있습니다. 시스템 구성, 수퍼유저 기능, 마스터 암호, 강력한 유틸리티, 보안 디바이스(예: 방화벽)에 대한 액세스 제한.
	SOC 2 무결성 4.1: 시스템 처리 무결성 및 보안 성능은 주기적으로 검토되고 정의된 시스템 처리 무결성 및 관련 보안 정책과 비교됩니다.
	SOC 2 무결성 4.2: 정의된 시스템 처리 무결성 및 관련 보안 정책과 일치하는 목표를 달성할 수 있는 엔터티의 지속적인 능력에 대한 잠재적 장애를 식별하고 그에 대처하는 프로세스가 있습니다.
ISO(국제 표준화 기구) 27001 ISO 27001은 널리 채택되는 글로벌 보안 표준으로서, 정보 보안 관리 시스템별 요건을 개략적으로 기술합니다. 주기적인 위험 평가에 기반을 둔 회사 및 고객 정보 관리에 대한 체계적 접근 방식을 제공합니다. 자세히 알아보기.	*저작권법으로 인해 AWS는 ISO 27001에 대한 요건 설명은 제공할 수 없습니다. ISO.org를 비롯한 다양한 소스에서 온라인으로 ISO 27001 표준 복사본을 구매할 수 있습니다.*

AWS 규정 준수 프로그램	규제 준수 요건
FedRAMP(연방 위험 및 인증 관리 프로그램) FedRAMP(연방 위험 및 인증 관리 프로그램)는 클라우드 제품 및 서비스의 보안 평가, 권한 부여 및 지속적 모니터링에 대해 최대 Moderate 등급까지 표준 방식을 제공하는 범정부 프로그램입니다. 자세히 알아보기.	**FedRAMP NIST 800-53 Rev 3 AU-2:** 조직: a. 위험 평가 및 미션/비즈니스 요구를 바탕으로 정보 시스템이 다음 이벤트를 감사할 수 있어야 하는지 결정합니다. [배정: 조직이 정의한 감사 가능 이벤트 목록] b. 보안 감사 기능을 감사 관련 정보를 요구하는 다른 조직 엔터티들과 조율함으로써 상호 지원을 강화하고 감사 가능한 이벤트 선택에 대해 안내합니다. c. 감사 가능한 이벤트 목록이 보안 사고에 대한 사후 조사를 지원하기에 충분하다고 여겨지는 이유를 제시합니다. d. 현재 위협 정보 및 위험에 대한 지속적 평가를 바탕으로 정보 시스템 내부에서 다음 이벤트들을 감사할지 결정합니다. [배정: 식별된 각 이벤트에 대한 감사(또는 감사가 필요한 상황)의 빈도에 따라 감사되도록 AU-2 a.에서 정의된 조직 정의 감사 가능 이벤트들의 하위 집합.
	FedRAMP NIST 800-53 Rev 4 AU 2: 조직: a. 정보 시스템이 다음 이벤트를 감사할 수 있어야 하는지 결정합니다. [배정: 조직이 정의한 감사 가능 이벤트] b. 보안 감사 기능을 감사 관련 정보를 요구하는 다른 조직 엔터티들과 조율함으로써 상호 지원을 강화하고 감사 가능한 이벤트에 대한 선택을 안내합니다. c. 감사 가능한 이벤트들이 보안 사고에 대한 사후 조사를 지원하기에 충분하다고 여겨지는 이유를 제시합니다. d. 정보 시스템 내에서 다음 이벤트를 감사할지 결정합니다. [배정: 식별된 각 이벤트에 대한 감사(또는 감사가 필요한 상황)의 빈도에 따라 감사되도록 AU-2 a.에서 정의된, 조직 정의 감사 가능 이벤트들의 하위 집합.
	FedRAMP NIST 800-53 Rev 3 AU-3: 정보 시스템은 최소한 어떤 유형의 이벤트가 발생했고, 그 이벤트가 언제(날짜와 시간) 어디서 발생했으며, 이벤트의 소스, 이벤트의 결과(성공 또는 실패), 그리고 그 이벤트와 연결된 사용자/주체의 자격 증명 등을 설정하기에 충분한 정보를 담은 감사 레코드를 생성합니다.
	FedRAMP NIST 800-53 Rev 4 AU-3: 정보 시스템은 최소한 어떤 유형의 이벤트가 발생했고, 그 이벤트가 언제(날짜와 시간) 어디서 발생했으며, 이벤트의 소스, 이벤트의 결과, 그리고 그 이벤트와 연결된 사용자 또는 주체의 자격 증명 등을 설정하는 정보를 담은 감사 레코드를 생성합니다.
	FedRAMP NIST 800-53 Rev 3 AU-4: 조직은 감사 레코드 스토리지 용량을 할당하고 감사를 구성해 그 용량이 초과될 가능성을 줄입니다.
	FedRAMP NIST 800-53 Rev 4 AU-4: 조직은 [배정: 조직 배정 감사 레코드 스토리지 요건]과 일치하도록 감사 레코드 스토리지 용량을 할당합니다.

AWS 규정 준수 프로그램	규제 준수 요건
FedRAMP(연방 위험 및 인증 관리 프로그램) FedRAMP(연방 위험 및 인증 관리 프로그램)는 클라우드 제품 및 서비스의 보안 평가, 권한 부여 및 지속적 모니터링에 대해 최대 Moderate 등급까지 표준 방식을 제공하는 범정부 프로그램입니다. 자세히 알아보기.	**FedRAMP NIST 800-53 Rev 3 AU-5:** 정보 시스템: a. 감사 처리 실패 시 조직 담당자에게 지정된 알림. b. 다음과 같이 추가 조치를 취하십시오. [배정: 조직이 정의한 취해야 할 조치(예: 정보 시스템 종료, 가장 오래된 감사 레코드 덮어쓰기, 감사 레코드 생성 중단)].
	FedRAMP NIST 800-53 Rev 4 AU-5: 정보 시스템: a. 알림[배정: 조직이 정의한 담당자] 감사 처리 실패 시. b. 다음과 같이 추가 조치를 취하십시오. [배정: 조직이 정의한 취해야 할 조치(예: 정보 시스템 종료, 가장 오래된 감사 레코드 덮어쓰기, 감사 레코드 생성 중단)].
	FedRAMP NIST 800-53 Rev 3 AU-6: 조직: a. 부적절한 또는 비정상적인 활동을 알리기 위해 정보 시스템 감사 레코드를 검토 및 분석[배정: 조직이 정의한 빈도]하고, 지정된 조직 담당자에게 결과를 보고합니다. b. 조직 운영, 조직 자산, 개인, 기타 조직, 또는 국가에 대한 위험에 변화가 있을 때 법 집행 정보, 지능 정보 또는 기타 신뢰할 수 있는 정보 출처를 바탕으로 정보 시스템 내 감사 검토, 분석, 보고의 수준을 조정합니다.
	FedRAMP NIST 800-53 Rev 3 AU-6: 조직: a. 부적절한 또는 비정상적인 활동을 알리기 위해 [배정: 조직이 정의한 빈도] 정보 시스템 감사 레코드를 검토 및 분석합니다. b. 그 결과를 [배정: 조직이 정의한 담당자 또는 역할]에 보고합니다.
	FedRAMP NIST 800-53 Rev 3 AU-8: 정보 시스템은 내부 시스템 클록을 사용하여 감사 레코드에 대한 타임스탬프를 생성합니다.
	FedRAMP NIST 800-53 Rev 4 AU-8: 정보 시스템: a. 내부 시스템 클록을 사용해 감사 레코드에 대한 타임스탬프를 생성합니다. b. 협정 세계시(UTC) 또는 그리니치 표준시(GMT)에 매핑될 수 있고 [배정: 조직이 정의한 시간 측정의 세부 수준]을 만족하는 타임스탬프에서 시간을 생성합니다.
	FedRAMP NIST 800-53 Rev 3 AU-9: 정보 시스템은 감사 정보 및 감사 도구를 무단 액세스, 수정, 삭제로부터 보호합니다.
	FedRAMP NIST 800-53 Rev 4 AU-9: 정보 시스템은 감사 정보 및 감사 도구를 무단 액세스, 수정, 삭제로부터 보호합니다.

AWS 규정 준수 프로그램	규제 준수 요건
FedRAMP(연방 위험 및 인증 관리 프로그램) FedRAMP(연방 위험 및 인증 관리 프로그램)는 클라우드 제품 및 서비스의 보안 평가, 권한 부여 및 지속적 모니터링에 대해 최대 Moderate 등급까지 표준 방식을 제공하는 범정부 프로그램입니다. 자세히 알아보기.	**FedRAMP NIST 800-53 Rev 3 AU-10:** 정보 시스템은 특정 작업을 수행했다는 것을 거부하는 개인으로부터 보호합니다.
	FedRAMP NIST 800-53 Rev 4 AU-10: 정보 시스템은 특정 작업[배정: 부인 방지에 의해 다루어지며 조직이 정의한 작업]을 수행한 사실을 거부하는 개인으로부터 보호합니다.
	FedRAMP NIST 800-53 Rev 3 AU-11: 조직은 [배정: 레코드 조직이 정의한, 레코드 보존 정책과 일치하는 시간 주기]에 대한 감사 레코드를 보유함으로써 보안 사고에 대한 사후 조사를 지원하고 규제 및 조직 정보 보존 요건을 충족합니다.
	FedRAMP NIST 800-53 Rev 4 AU-11: 조직은 [배정: 레코드 조직이 정의한, 레코드 보존 정책과 일치하는 시간 주기]에 대한 감사 레코드를 보유함으로써 보안 사고에 대한 사후 조사를 지원하고 규제 및 조직 정보 보존 요건을 충족합니다.