

Akamai Identity Cloud와 함께 살펴보는 데이터 개인정보 보호 요구사항 준수 가이드

Akamai Identity Cloud가 컴플라이언스를 지원하는 방법

데이터 유출과 남용이 지속됨에 따라 전 세계에서 개인정보(PI) 관련 법률 및 규정이 지속적으로 제정되고 있습니다. 기업이 여러 개인정보 보호 및 데이터 보호 법률의 차이를 이해하는 것은 쉬운 일이 아닙니다. 유럽 연합의 GDPR(General Data Protection Regulation)부터 미국의 캘리포니아 소비자 개인정보 보호법(CCPA), 호주의 APA(Privacy Act), 일본의 APPI(Protection of Personal Information) 및 캐나다의 PIPEDA(Personal Information Protection and Electronic Documents Act)에 이르기까지 각 규정마다 차이점을 보입니다.

많은 고객사들이 특정 개인정보 보호법과 Akamai의 컴플라이언스 지원 방식에 대해 자주 문의하고 있습니다. 데이터 개인정보 보호에 도움이 되도록 전 세계의 여러 데이터 보호 및 개인정보 보호 규정에 대한 일반적인 요구사항 목록을 취합했습니다. 각각의 요구사항에 대해 간략하게 설명하고 고객 ID 및 접속 관리(CIAM) 솔루션인 **Akamai Identity Cloud**가 이러한 문제를 해결하는 데 어떤 도움을 줄 수 있는지 말씀드리겠습니다.

CIAM은 소프트웨어 솔루션과 결합된 체계적인 접근 방식을 지향합니다. 이 소프트웨어는 기업이 보안을 유지하고 규제를 준수하면서 고객의 개인 정보를 수집 및 관리하는데 핵심적인 역할을 합니다. CIAM을 통해 기업은 마케팅 자동화 및 콘텐츠 관리 시스템 내의 고객 데이터를 활용할 수 있습니다. 동시에 고도로 개인화된 고객 경험을 지속적으로 제공하고 규제 요구사항과 데이터 프라이버시에 대한 고객의 증가하는 요구사항에 부합할 수 있습니다.

다음 가이드를 통해 Akamai Identity Cloud가 전 세계의 다양한 개인정보 보호법 및 요구사항에서 발생하는 공통적인 데이터 보호 의무 11가지 항목을 어떻게 준수하는지 확인할 수 있습니다.

Akamai Identity Cloud와 함께 살펴보는 데이터 개인정보 보호 요구사항 준수 가이드

목차

동의 획득 및 관리 2

거부할 권리 3

아동에 대한 부모의 동의 4

데이터 주체의 접속 권리 5

정정 권리 6

개인정보 제거 및 삭제 권리("잊혀질 권리") 7

데이터 이동성 8

벤더 리스크 관리 9

유출 통보 10

기업의 책임 11

데이터 레지던시 및 전송 12

결론 13

글로벌 컴플라이언스 레퍼런스 아키텍처 14

동의 획득 및 관리

기업이 진행하는 일부 활동의 경우, 기본적인 데이터 사용은 개인의 사전 동의를 기반으로 합니다. 데이터를 반드시 사용해야 하는 상황과 유효한 동의 획득에 대한 요구사항은 규제에 따라 다릅니다. 글로벌 데이터 보호법에 따라 동의를 관리하고 동의를 승인 및 철회할 수 있는 개인의 선택을 존중해야 하지만 실제로 이를 실행하는 것은 어려울 수 있습니다.

Identity Cloud의 지원 방법

Identity Cloud는 기업이 동의를 수집하게 해주며 사용자가 이를 보고 수정 및 취소할 수 있는 설정 센터 셀프서비스 포털을 제공합니다.

사용자 경험과 양식을 맞춤형으로 제공하여 옵트인 및 옵트아웃 시나리오를 모두 지원할 수 있습니다. 또한 계정을 등록하거나 로그인을 한 이후 등 고객 여정의 모든 단계에 걸쳐 동의를 요청할 수 있습니다. 사용자에게 셀프서비스 기반으로 언제든지 동의를 관리할 수 있는 권한을 제공할 수 있습니다.

동의 및 설정은 고객 데이터 기록의 일부로 사용자 데이터와 함께 감사 가능한 방식으로 저장됩니다. 모든 사용자 데이터는 이동 및 저장 상태에서 암호화됩니다. 접속 로그는 투명성과 책임을 위해 사용자가 실행한 조치의 증거를 제공합니다.

의무	동의 획득 및 관리
EU GDPR	4조 (11), 7 (3)
캘리포니아 CCPA	섹션 1798.120
캐나다 PIPEDA	별첨 1 4.3절
멕시코 LFPDPPP	법률 8조 및 9조
호주 APA	APP 가이드라인 챕터 B.34
일본 APPI	16조
싱가포르 PDPA	13 및 16조
브라질 LGPD	7조 (1) 및 8조
아르헨티나 LPDP	섹션 5
인도 PDP 법안 2019	11절

거부할 권리

거부할 권리는 다이렉트 마케팅이나 통계 분석과 같은 특정 데이터 처리에 개인 데이터가 사용되는 것을 거부하는 권리입니다.

Identity Cloud의 지원 방법

Identity Cloud는 사용자가 승인하는 데이터 종류를 선택하거나 선택 해제할 수 있도록 맞춤형 설정 센터를 제공합니다.

이 사용자 인터페이스 및 설계는 사용자가 수락하는 데이터 처리 종류를 선택하고 프로필에 대해 다른 작업을 진행할 수 있는 등록 및 로그인 경험과 통합됩니다. 설정은 고객 데이터 레코드의 일부로서 사용자 데이터와 함께 저장되며 이동 및 저장 시에는 암호화됩니다. 클라이언트가 호스팅하는 페이지에서 API를 통해 기본 설정을 업데이트할 수도 있습니다.

의무	활동 처리에 거부할 권리
EU GDPR	21조
캘리포니아 CCPA	섹션 1798.120
캐나다 PIPEDA	별첨 1 4.3.8절
멕시코 LFPDPPP	22조, 27조 ff
호주 APA	명확한 내용 없음
일본 APPI	30조 APII
싱가포르 PDPA	명확한 내용 없음
브라질 LGPD	18조 VIII
아르헨티나 LPDP	16조 및 30조
인도 PDP 법안 2019	7 (d), 11 (e)절

아동에 대한 부모의 동의

특정 연령에 도달하지 않은 개인의 동의는 효력이 없습니다. 적용되는 연령 제한보다 어린 개인의 경우, 법적 보호자가 대신하여 유효한 동의를 제공할 수 있습니다. 유효한 동의에 대한 연령 제한은 국가별로 상이합니다.

Identity Cloud의 지원 방법

Identity Cloud는 연령 때문에 관련 법률에 따라 유효한 동의를 제공할 수 없는 아동의 개인 데이터를 수용하는 것을 방지하는 나이 제한 기능이 있습니다.

의무	아동에 대한 부모의 동의
EU GDPR	8조
캘리포니아 CCPA	섹션 1798.120 (c)
캐나다 PIPEDA	별첨 1 4.3절
멕시코 LFPDPPP	규제 및 가이드 11 및 12페이지의 89조 III
호주 APA	APP 가이드라인 챕터 B.47, 52 53
일본 APPI	명확한 내용 없음
싱가포르 PDPA	PDPA 선정 주제에 대한 권고사항, 2018년 8월 31일
브라질 LGPD	14조 § 1
아르헨티나 LPDP	18조
인도 PDP 법안 2019	16 (2)절

데이터 주체의 접속 권리

개인이 처리되는 개인 데이터에 접속할 수 있는 권리입니다. 데이터의 사용 및 공개에 대한 추가 정보를 확인할 수 있는 권리를 포함하기도 합니다.

Identity Cloud의 지원 방법

Identity Cloud는 사용자가 언제든지 자신의 데이터에 접속할 수 있는 맞춤형 설정 센터를 제공합니다. 셀프서비스 포털을 통해 사용자는 고객 지원 서비스 없이도 제공되는 정보의 범위와 정확성을 손쉽게 확인하여 데이터 설정을 제어할 수 있습니다.

의무	데이터 주체의 접속 권리
EU GDPR	15, 20조
캘리포니아 CCPA	섹션 1798.100
캐나다 PIPEDA	별첨 1 4.9절
멕시코 LFPDPPP	법률 22-23조, 29-35조 및 규제 101조
호주 APA	APP 12 및 APP 가이드라인 챕터 12
일본 APPI	19조
싱가포르 PDPA	21조
브라질 LGPD	9조 및 18조 (2)
아르헨티나 LPDP	27조
인도 PDP 법안 2019	17 (3)절

정정 권리

처리 중인 개인 데이터를 수정할 수 있는 권한을 개인에게 제공합니다.

Identity Cloud의 지원 방법

Identity Cloud는 사용자 및 서비스 담당자가 언제 어디서나 데이터 기록을 편집할 수 있기 때문에 데이터가 정확하고 최신 상태입니다. 정정 활동은 기록되고 감사가 가능하며 사용자의 데이터 제어에 대한 증거로 사용할 수 있습니다.

의무	정정 권리
EU GDPR	5 (1) d, 16조
캘리포니아 CCPA	섹션 1789.100 (a)
캐나다 PIPEDA	별첨 1 4.9.5절
멕시코 LFPDPPP	11 (2), 22조 및 법률 24, 28-31, 35
호주 APA	APP 13 및 APP 가이드라인 파트 13
일본 APPI	19조
싱가포르 PDPA	22조
브라질 LGPD	8조 및 18조 (III)
아르헨티나 LPDP	29조
인도 PDP 법안 2019	18절

개인정보 제거 및 삭제 권리("잊혀질 권리")

여러 법은 개인의 '잊혀질 권리'를 포함하고 있습니다. 본인의 개인정보를 삭제하여 씨드파티와 공유하거나 또는 씨드파티를 통한 처리에 노출되지 않게 하는 것입니다.

Identity Cloud의 지원 방법

Identity Cloud는 백업 삭제를 포함해 데이터 기록을 안전하게 삭제(복구 불가)함으로써 데이터가 유출되는 것을 차단할 수 있습니다. 사용자 또는 서비스 담당자는 언제 어디서나 잊혀질 권리를 행사할 수 있습니다.

의무	제거 권리("잊혀질 권리")
EU GDPR	17조
캘리포니아 CCPA	섹션 1798.105 면제: 1798.145 (g)(3)
캐나다 PIPEDA	별첨 1 4.9.5절
멕시코 LFPDPPP	법률의 11 (3), 22, 28-32, 35조
호주 APA	APP 4, APP 가이드라인 챕터 4.2 및 APP 13 및 APP 가이드라인 챕터 13
일본 APPI	19조 APPI
싱가포르 PDPA	25조
브라질 LGPD	LGPD 18 (VI)조
아르헨티나 LPDP	31조
인도 PDP 법안 2019	18, 20절

데이터 이동성

기업은 개인에게 일반적으로 사용되고 시스템이 인식 가능한 양식의 사본을 제공해야 합니다. 이를 통해 사용자는 불편 없이 자신의 데이터를 다른 기업에 전송할 수 있습니다.

Identity Cloud의 지원 방법

Identity Cloud는 사용자가 데이터 다운로드를 요청할 수 있는 맞춤형 설정 센터를 제공합니다. 기업은 쉽게 데이터 이동 요청을 처리하고 사용자 데이터를 보관하고 있는 Identity Cloud나 다른 시스템에서 데이터를 다운로드할 수 있습니다. Identity Cloud로 이벤트를 트리거하고 규정 요구사항을 충족하는 데 필요한 데이터를 수집하고 전달하는 프로세스를 시작할 수 있습니다. Identity Cloud가 갖고 있는 사용자 데이터는 인간 및 기계 모두 판독 가능한 오픈 표준 파일 형식인 JSON으로 제공 가능합니다.

의무	데이터 이동성 권리
EU GDPR	20조
캘리포니아 CCPA	섹션 1798.100
캐나다 PIPEDA	명확한 내용 없음
멕시코 LFPDPPP	명확한 내용 없음
호주 APA	소비자 데이터 권리장전(고객에게만 해당)
일본 APPI	명확한 내용 없음
싱가포르 PDPA	권리 협의 중
브라질 LGPD	11, 17, 18, 40조
아르헨티나 LPDP	33조
인도 PDP 법안 2019	19절

벤더 리스크 관리

기업은 개인 데이터를 자체적으로 처리하는지 또는 써드파티 서비스 공급자를 통해 대신 처리하는지 여부와 관계없이 데이터 보호 및 보안을 보장해야 합니다. 따라서 벤더 리스크 관리가 종합적인 컴플라이언스의 핵심입니다.

Identity Cloud의 지원 방법

Akamai는 신뢰할 수 있는 서비스 사업자로서 기술적 조직적 차원의 조치를 통해 고객을 대신해 개인정보 IT 프로세스의 데이터 보호 및 보안을 보장합니다. Akamai Identity Cloud의 인증과 증명은 이러한 조치의 타당성을 입증하는 증거로서 효과적인 리스크 완화 효과를 제공합니다.

Identity Cloud는 강력한 사용자 인증, 네트워크 기반 위협에 대한 정교한 보호 메커니즘을 제공하며, 모두 Akamai의 웹 애플리케이션 방화벽인 **Kona Site Defender**로 보호됩니다. 또한 기업은 알아야 하는 사항을 바탕으로 접속 제어를 유지할 수 있습니다. Identity Cloud는 다음과 같은 주요 보안 보증 프로그램의 **인증 및 규정 준수**를 유지하고 이에 관해 감사 또는 평가를 받습니다.

- ISO 27001:2013
- ISO 27018:2014(클라우드 내 PII 보안)
- SOC 2 Type 2 (5가지의 신뢰 서비스 원칙: 공통 기준/보안, 가용성, 기밀 유지, 처리 무결성 및 개인정보 보호)
- HIPAA/HITECH(저장 및 전송 상태의 의료 정보 보호) 보안 규칙 준수
- EU-US 개인정보 보호 프레임워크

의무	벤더 리스크 관리
EU GDPR	32조
캘리포니아 CCPA	섹션 1798.81.5
캐나다 PIPEDA	별첨 1 4.7절
멕시코 LFPDPPP	19조
호주 APA	APP 11
일본 APPI	20조
싱가포르 PDPA	24조
브라질 LGPD	46조 ff
아르헨티나 LPDP	19조
인도 PDP 법안 2019	24절

Akamai Identity Cloud와 함께 살펴보는 데이터 개인정보 보호 요구사항 준수 가이드

유출 통보

기업은 데이터가 유출되었을 때 이 사실을 파악하자마자 일정 시간 이내에 통보해야 합니다. 일반적으로 이 통보에는 위반 기업, 접속된 데이터 유형, 영향을 받는 개인의 대략적인 수, 개인에 대한 예상 또는 실제 피해, 완화 조치 등에 대한 설명이 포함됩니다. 필수 보고 내용 및 통보 기한 및 통보 대상은 국가별로 다릅니다.

Identity Cloud의 지원 방법

Akamai는 절차 및 관련 커뮤니케이션 정책을 포함한 정보 보안 이벤트 관리 정책을 실행하여 기업의 데이터 유출 통보 의무를 지원합니다. 이러한 정책과 절차는 ISO 27001:2013 인증 Identity Cloud 정보 보안 관리 시스템의 일부입니다.

의무	유출 통보
EU GDPR	33조
캘리포니아 CCPA	섹션 1798.29 (a) 및 1798.82 (a)
캐나다 PIPEDA	10.1절 ff.
멕시코 LFPDPPP	20조
호주 APA	파트 IIIC APA
일본 APPI	명확한 내용 없음
싱가포르 PDPA	2019년 데이터 유출 관련 가이드라인
브라질 LGPD	48조
아르헨티나 LPDP	20조
인도 PDP 법안 2019	25절

기업의 책임

개인 데이터를 관리하는 각 기업은 해당 데이터 보호법에 따라 데이터 IT 프로세스의 보호 및 보안에 대한 책임을 집니다. 이를 위해서 기업은 데이터 IT가 처리하는 데이터, 위치, 목적 및 데이터에 접속하는 서드파티에 대해 항상 알고 있어야 합니다.

Identity Cloud의 지원 방법

Identity Cloud는 기업이 데이터 처리 활동에 대한 책임을 확립하는 데 도움을 줍니다. 데이터 기록의 편집을 포함하여 수집된 데이터 요소에 대한 감사 가능한 기록을 유지합니다.

Identity Cloud는 적절한 기술적·조직적 방법으로 저장된 데이터를 보호하는 것 외에도 세부적인 역할 및 속성 기반 접속 제어와 로그 메커니즘을 제공하여 모든 데이터 접속 증거를 제공합니다. 이러한 보호 조치는 개인 데이터를 처리하기 위해 Identity Cloud를 사용하는 기업이 책임감 있게 행동하고 있다는 것을 보여줍니다.

의무	기업의 책임
EU GDPR	5 (2)조
캘리포니아 CCPA	섹션 1798.100
캐나다 PIPEDA	별첨 1 4.1절
멕시코 LFPDPPP	14조
호주 APA	APP 1 가이드라인의 챕터 1
일본 APPI	15조 ff
싱가포르 PDPA	3조
브라질 LGPD	6 (10)조
아르헨티나 LPDP	10조
인도 PDP 법안 2019	22 ff. 및 29절

데이터 레지던시 및 전송

내부 기업 또는 법적 요구사항으로 인해 데이터 레지던시가 기업에서 중요한 역할을 담당합니다. 법적 데이터 레지던시 법률은 러시아 및 중국에 적용됩니다. 데이터 레지던시 요구사항이 없는 국가들도 많지만, 데이터 전송 요구사항은 데이터를 국내에서 보호하기 위해 실시되고 있습니다.

Identity Cloud의 지원 방법

Identity Cloud는 중국 및 러시아 지역을 포함하여 고객의 요청에 대응하기 위해 다양한 데이터 레지던시 설정을 제공합니다. 중국에서는 준거법에 따라 해당 지역에 저장된 개인 식별 정보(PII)를 암호화하지 않습니다.

러시아의 경우 Identity Cloud Russia 솔루션을 통해 "러시아 우선 표기(Write First in Russia)" 접근 방식과 유럽 연합의 보조 데이터센터에서 발생하는 고객 PII의 애플리케이션 호스팅 및 데이터 스토리지를 제공합니다.

Akamai는 개인정보 보호 인증 프로그램의 검증을 받았으며 데이터를 다른 국가로 전송할 때 국가별 데이터 보호 수준을 유지하기 위해 고객과 표준 계약 조항을 협의합니다.

의무	데이터 레지던시/데이터 전송 요구사항
EU GDPR	46조 ff.
캘리포니아 CCPA	해당 없음
캐나다 PIPEDA	별첨 1 4.1.3절
멕시코 LFPDPPP	36조 ff.
호주 APA	APP 8
일본 APPI	24조
싱가포르 PDPA	26조
브라질 LGPD	33조 ff.
아르헨티나 LPDP	23조 ff.
인도 PDP 법안 2019	33절 ff.

결론

데이터 개인정보 보호법과 규정은 기업이 개인 데이터 처리에 대한 책임을 지고, 써드파티의 개인 데이터 처리에 대한 통제권은 개인이 유지할 수 있도록 합니다. Akamai Identity Cloud는 개인이 자신의 데이터를 관리할 수 있게 하며 기업이 개인정보를 처리할 때 투명성과 책임을 위해 기록을 제공합니다. Identity Cloud는 관련 데이터 보호법을 준수하고 개인 데이터를 안전하게 보호하며 고객의 신뢰를 구축하는 데 도움을 주는 사용이 간편한 툴과 프로세스를 제공합니다.

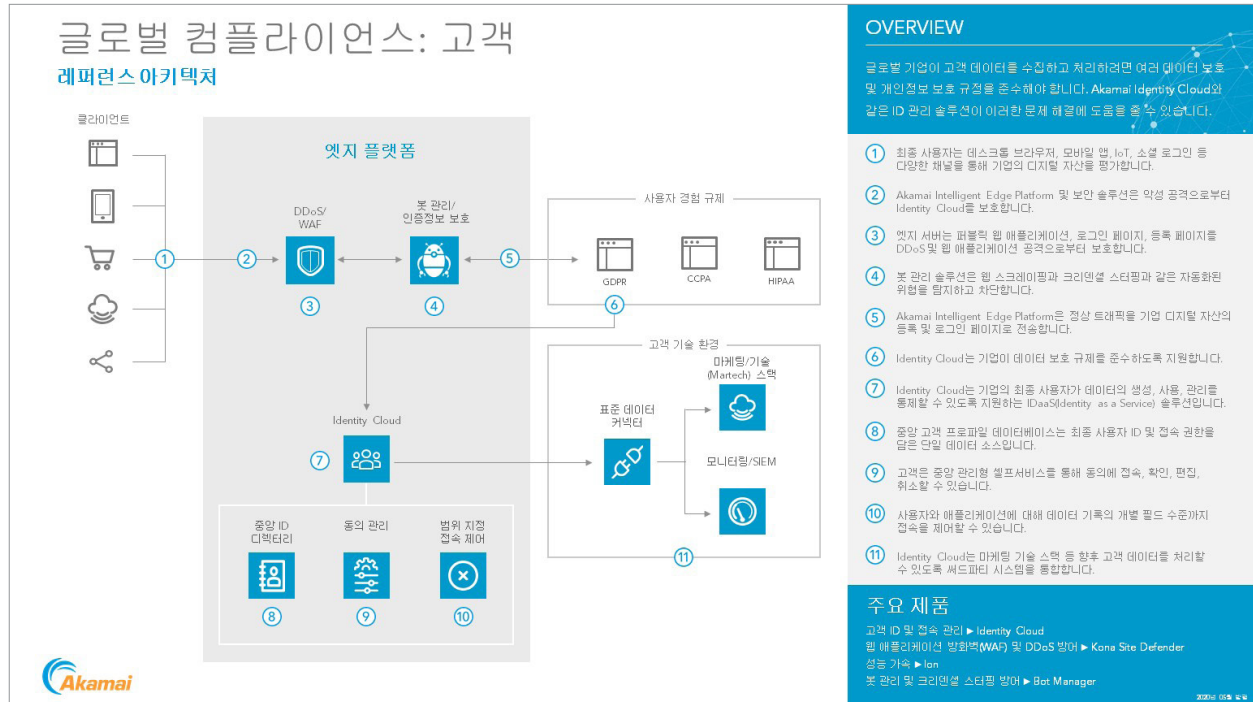
법률 및 규제

지역	법률	링크
유럽연합(EU)	GDPR(General Data Protection Regulation)	GDPR
캘리포니아	CCPA(California Consumer Privacy Act)	CCPA
캐나다	캐나다 개인정보 보호 및 전자문서에 관한 법률(The Personal Information Protection and Electronic Documents Act, PIPEDA)	PIPEDA
멕시코	민간기업의 개인정보 보호에 관한 연방 법률(The Federal Law on the Protection of Personal Data held by Private Parties, Ley Federal de Protección de Datos Personales en Posesión de los Particulares) 2010 및 2011 관련 규제	LFPDPPP
호주	APA(Australian Privacy Act), 개인정보 보호법 1988 / APP(Australian Privacy Principles)	APA APP
일본	APPI(Act on Protection of Personal Information)	APPI
싱가포르	PDPA(Personal Data Protection Act 2012)	PDPA
브라질	일반 데이터 개인정보 보호법, LGPD(Lei geral de Proteção de Dados Pessoais)	LGPD
아르헨티나	아르헨티나 개인정보 보호법, LPDP(Ley de Protección de Datos Personales)	LPDP
인도	인도 개인정보 보호 법안(PDP 법안 2019)은 인도 의회에 제출되었으며 2020년 5월 현재 논의 중입니다. 완전성을 위해 백서의 일부로 포함되었습니다.	PDB 법안 2019 (제안서)

글로벌 컴플라이언스 레퍼런스 아키텍처

글로벌 기업이 고객 데이터를 수집하고 처리하려면 여러 데이터 보호 및 개인정보 보호 규정을 준수해야 합니다. Akamai Identity Cloud와 같은 ID 관리 솔루션은 이러한 문제를 관리하는 데 도움이 됩니다.

글로벌 컴플라이언스: 고객



<https://www.akamai.com/kr/ko/solutions/akamai-architectures.jsp> 에서 더 많은 레퍼런스 아키텍처를 확인하시기 바랍니다.



Akamai는 전 세계 주요 기업들에게 안전하고 쾌적한 디지털 경험을 제공합니다. Akamai의 Intelligent Edge Platform은 기업과 클라우드 등 모든 곳으로 확장하고 있고 고객의 비즈니스가 빠르고, 스마트하며, 안전하게 운영될 수 있도록 지원합니다. 대표적인 글로벌 기업들은 Akamai 솔루션을 통해 멀티 클라우드 아키텍처를 강화하고 경쟁 우위를 확보하고 있습니다. Akamai는 가장 가까운 곳에서 사용자에게 의사 결정, 앱, 경험을 제공하고 공격과 위협을 먼 곳에서 차단합니다. Akamai 포트폴리오는 엣지 보안, 웹·모바일 성능, 엔터프라이즈 접속, 비디오 전송 솔루션으로 구성되어 있고 우수한 고객 서비스, 애널리틱스, 24시간 연중무휴 모니터링 서비스를 제공합니다. 대표적인 기업과 기관에서 Akamai를 신뢰하는 이유를 알아보려면 Akamai 홈페이지(www.akamai.com) 또는 블로그(blogs.akamai.com)를 방문하거나 Twitter에서 @Akamai를 팔로우하시기 바랍니다. 전 세계 Akamai 연락처 정보는 www.akamai.com/locations에서 확인할 수 있습니다. Akamai 코리아는 서울시 강남구 강남대로 382 메리츠타워 21층에 있으며 대표전화는 02-2193-7200입니다. 2020년 07월 발행.