okta

영웅의 탄생

CIAM 완성도에 이르는 길

@okta

okta.com

CIAM 여정 안내서

아이덴티티 및 액세스 관리(IAM, Identity and Access Management)분야의 리더인 Okta는 수천 개의 기업이 보안과 사용성 목표를 달성할 수 있도록 협력해왔습니다. 그 과정에서 각 기업의 아이덴티티 여정의 진척도와 관계없이 각 단계마다 공통의 문제점을 겪는다는 것을 알게 되었습니다.

이 전자책에서는 고객 아이덴티티 및 액세스 관리(CIAM, Customer Identity and Access Management) 완성도에 이르는 길의 네 가지 핵심 단계를 정의하고 살펴보며 완성도 곡선의 각 단계에서 기업이 겪게 되는 문제점을 소개합니다. 또한 각 문제에 대한 솔루션을 제안하고 조직의 진행 과정에 따라 채택해야 하는 도구와 프로세스에 대한 로드맵을 제시합니다.

여정의 각 단계에서 지속적인 CIAM에 도달하기 위한 다음 단계를 명확히 제시합니다. 그럼 시작하겠습니다.

CIAM 완성도에 이르는 길 구축하기

CIAM의 정의

과제는 고객이 기대하는 수준의 디지털 편의성과 보안을 동시에 제공하는 것입니다. 해결 방법은 IAM에 대한 구식 접근법을 버리고, 사용자 아이덴티티를 보호하고 적합한 사람이 적절한 시간 동안 적합한 리소스에 액세스할 수 있게 해주는 최신 테크놀로지로 대체하는 것입니다. 이것이 CIAM입니다.

사내에서 사용 가능한 아이덴티티 기능을 구축하는 일은 복잡하고 시간이 많이 소요되는 작업이며, 잘못될 경우 다수의 보안 취약점을 초래할 수 있습니다. 많은 조직이 애플리케이션을 확장하여 경쟁력 있는 속도로 시장에 출시하기 위해 노력하고 있습니다. 보안 침해 및 데이터 악용 사례가 자주 눈에 띄는 요즘, 고객은 개인 정보를 수집하는 기업과 디지털 경험에 대해 신뢰를 잃어 가고 있습니다. 그러므로 효율성과 사용자 신뢰는 확장을 모색하는 기업에게 새로운 화폐와도 같습니다.

기업이 디지털 자산의 개발 시간을 단축하고 보안 격차를 해소하며 원활한 사용자 경험을 제공하려면 고객의 아이덴티티를 가장 중요시해야 합니다.

CIAM 솔루션은 아이덴티티 계층을 고객 대면 애플리케이션과 포털에 내장하여 데이터와 사용자 계정을 보호하고 웹사이트와 애플리케이션에 대한 쉽고 안전한 액세스를 지원합니다. 이는 조직이 보안과 개인 정보 및 마케팅 요구 사항을 효율적으로 충족할 수 있도록 지원하는 기반입니다.

효과적인 CIAM 솔루션의 세 가지 주요 기능은 **인증, 권한 부여, 사용자 관리**입니다. 이 세 가지 구성 요소는 여정 전체에 걸쳐 진화할 것입니다.

인증의 정의

제대로 된 **인증**은 계정에 로그인하는 사람이 정말로 계정의 주인인지 확인하고 악의적인 행위자가 중요한 사용자 데이터(결제 정보, 주소, SSN 등)에 액세스하지 못하도록 방지합니다.

권한 부여의 정의

효과적인 **권한 부여**를 통해 기업은 애플리케이션 및 리소스와 관련하여 사용자에게 적합한 수준의 액세스를 보장할 수 있습니다.

사용자 관리의 정의

명확한 **사용자 관리**를 통해 관리자는 사용자 액세스 권한을 업데이트하고 보안 정책을 시행하여 보다 원활하고 안전한 경험을 제공할 수 있습니다.

CIAM 아키텍처 시나리오

CIAM은 다음과 같은 조직의 다양한 운영 컨텍스트를 지원합니다.

- 비즈니스와 소비자 간 IAM
- 비즈니스 간 IAM
- 일반 웹 애플리케이션에 대한 Single sign-on
- SPA 및 API
- 휴대 장치 및 API

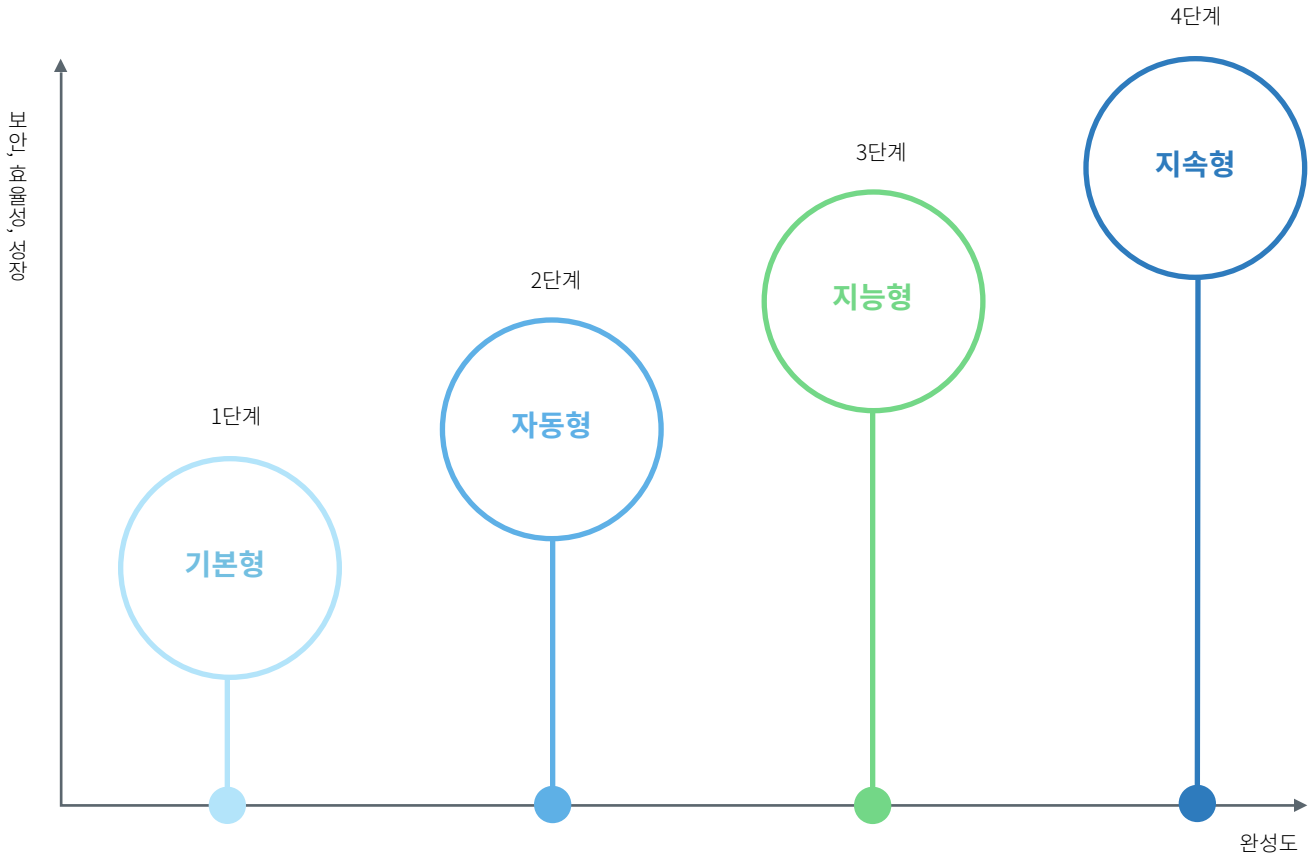
조직에 어떤 시나리오를 적용하든지 관계없이 고객 대면 제품을 출시할 때는 몇 가지 절차를 거쳐야 하는데, 여기에는 애플리케이션 구축, API 보안, 사용자 보호, 기업 아이덴티티 통합 등이 포함됩니다.

항상 강력한 CIAM 인프라를 구현하면 고객의 데이터와 이들의 액세스를 보호하여 제품의 신뢰도를 높일 수 있습니다.

CIAM 완성도 곡선

조직은 저마다 다르기 때문에 CIAM 완성도에 있어서도 서로 다른 단계에 위치해 있습니다. 이를 다음의 네 가지 단계로 정의합니다. **기본형, 자동형, 지능형, 지속형**

귀하의 조직은 CIAM 완성도 곡선에서 어디쯤에 있습니까?



각 단계를 자세히 살펴보고 CIAM 완성도에 이르기 위해 기업이 취해야 할 조치에 대해 알아봅니다.

1단계: 기본형

제품 및 시장 적합성 입증

이 단계에서는

- 훌륭한 제품 아이디어를 갖고 있으며 실현 가능성을 입증하고자 합니다.
- 프로젝트 초기 단계에 있습니다.
- 팀의 규모가 작습니다.
  - 거의 모든 팀원이 애플리케이션 출시와 관련된 업무를 맡고 있습니다.
  - 폭넓은 경력을 보유한 테크놀로지 책임자가 한두 명 있습니다.
  - 아이덴티티 전담 전문가가 없습니다.
- 로젝트가 수명 주기 초반 단계에 있어 아직 매출이 없으며 초기 액세스 잠재 고객이 있습니다.
- 팀의 주된 초점은 애플리케이션의 비즈니스 가설을 설계, 구축 및 검증하는 것입니다.

1단계 목표 및 문제점:

목표

- 목표는 시장 출시 속도입니다. 기본 아이덴티티를 전제로 하는 최소한의 실행 가능한 조기 제품을 빠르게 출시해야 합니다.
- 잠재 고객에게 제품을 선보이고자 합니다.
- 해당 문제를 해결 중이라는 것을 입증하고자 합니다.

문제점

- 제품을 출시해야 합니다.
- 학습과 동시에 반복해야 합니다.
- 제품에 대한 KPI 세트를 정립하고 단기간 내에 피드백을 수집해야 합니다.
- 기본적인 보안 문제로 인해 프로젝트가 정상 궤도를 이탈할 수 있습니다.
- 엔지니어링 리소스가 제한되어 있으며 설계에 적합한 아이덴티티의 위치에 대한 인사이트가 부족합니다.

구축 vs. 구매

이 시점에서 일반적으로 기업은 CIAM 솔루션을 직접 구축하기 위해 시간과 리소스를 투입할 것인지, 아니면 타 공급 업체와 협력할 것인지를 결정합니다. 도구를 내부적으로 구축하고 관리하다 보면 개발자가 귀중한 시간을 빼앗길 수 있습니다. 외부 솔루션을 활용하면 회사의 민첩성이 유지됩니다. 다루기 어려운 내부 CIAM 시스템을 유지할 필요가 없으므로 팀이 제품 개선에 시간과 리소스를 투입할 수 있기 때문입니다.

요구 사항

CIAM 솔루션은 다음 요소의 빠른 설정과 통합을 지원해야 합니다.

- 사용자 등록 및 온보딩
- 사용자 로그인
- 사용자 액세스 권한
- 사용자 권한 부여
- 사용자 관리
- 비밀번호 리셋 및 계정 복구 절차

솔루션

CIAM 플랫폼의 핵심 구성 요소

도입부에서 언급한 대로 효과적인 CIAM 솔루션의 세 가지 주요 특징은 다음과 같습니다.

- 인증(로그인) 사용자
- 관리(등록)
- 권한 부여(액세스 규칙, 정책)

맞춤형 사용자 흐름

사전 정의된 맞춤형 사용자 흐름은 최고의 사용자 및 고객 지원 기능을 신속하게 제공할 수 있습니다.

- 셀프 서비스 등록
- 비밀번호 리셋
- 계정 및 사용자 이름 복구

자격 증명 복구

자격 증명 복구에는 보안 질문과 같은 지식 검증, 그리고 이메일 링크 리셋과 같은 기본적인 소유자 확인 절차를 포함시켜야 합니다.

자격 증명 복구 메커니즘은 고객이 비밀번호를 리셋할 수 있도록 이메일 복구와 같은 보조 수단을 지원해야 합니다.

자격 증명 복구 메커니즘은 일회용 또는 제한된 시간 사용만을 지원해야 합니다.

개발자 효율성

개발자는 레거시 코드와 불량 코드의 디버깅 및 유지 관리 작업에 평균 **일주일당 17.3 시간**을 투입합니다. 적합한 CIAM 플랫폼을 사용하면 개발 속도를 높이고 향후 유지 관리 부담을 덜 수 있습니다. 핵심 고객과 제품 경험에 집중할 수 있으므로 팀이 사용 가능한 최고의 도구와 생산 준비가 완료된 아이덴티티 통합 기능을 손쉽게 구축할 수 있습니다.

CIAM 솔루션을 통해 엔지니어의 개입 없이도 보안 정책을 유지 및 업데이트할 수 있어야 합니다.

중앙 집중형 아이덴티티 관리

이는 보안 팀과 관리 팀에게 코드 없이도 보안 정책을 관리하는 능력과 규모 확장에 따라 일관된 프레임워크를 적용하는 능력을 부여합니다.

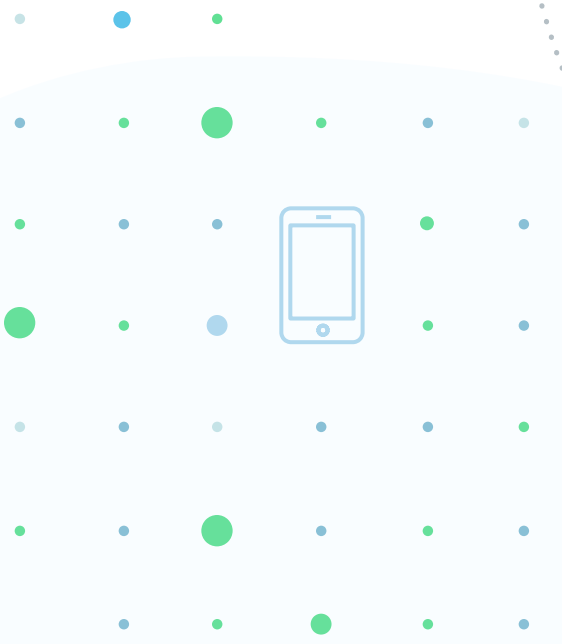
CIAM 솔루션은 기본 보안 모범 사례와 최신 아이덴티티 표준에 부합해야 합니다.

보안

포함 사항:

- 암호화 및 해싱
- OIDC/OAuth와 같은 개방형 아이덴티티 표준
- 보안 사양 정의 부문의 권위자인 Okta의 플랫폼 채택하기

현대의 CIAM 플랫폼은 사용자 자격 증명을 안전하게 저장하며, 두 번째로 많이 사용되는 웹 애플리케이션 보안 위험인 손상된 인증 흐름을 완화합니다.



1 CIAM 완성도 지침의 1단계 마무리하기

인증

- 인증 표준
- 소셜 인증
- 비밀번호 리셋 흐름

권한 부여

- OIDC 및 OAuth 기반 권한 부여 표준
- 권한 부여 서버

사용자 관리

- 간소화된 온보딩
- 셀프 서비스 등록
- 간소화된 관리

중앙 집중형 관리 UI

- 액세스 정책
- 보안 정책
- 일관된 구현

개발자 경험

- 도구: SDK, API, 위젯
- 설명서: 지침, 애플리케이션 샘플
- 개발자 에코시스템 전반에 걸친 통합 기능

Okta 플랫폼으로 이러한 기능을 구현하는 방법을 알아보려면 Customer Identity 데모를 시청하세요.

기본 CIAM 완성도를 달성한다는 것은 중대한 아이덴티티 보안 기능을 애플리케이션에 구축하여 시장에 성공적으로 출시했다는 것을 뜻합니다. 이제 증가하는 고객층으로 제품을 확장할 때입니다.

2 2단계

2단계: 자동형

중앙 집중 및 확장

이 단계에서는

- 애플리케이션이 큰 인기를 얻었고 이제 고객을 위해 제품을 추가로 구축하고자 합니다.
- 더 많은 개발자와 테크놀로지 관리자, 제품 관리자를 고용하여 팀의 규모가 커지고 있습니다.
- 최고 테크놀로지 책임자(CTO, Chief Technical Officer), 제품 부사장 또는 프로젝트를 이끄는 엔지니어링 부사장이 있습니다.
- 고급 기능이나 엔터프라이즈급 기능을 원하는 유료 고객층이 성장 중입니다. 이러한 기능을 구축하기 위한 시간이나 경험이 충분하지 않을 수 있습니다.
- 계획의 우선 순위를 설정해야 하지만 고객은 보다 정교한 아이덴티티 기능과 통합 기능을 원합니다.
- 경영진과 기업의 목표가 조직과 제품의 확장, 그리고 지속 가능한 장기적 성장을 위한 효율성 개발에 맞춰져 있습니다.

2단계 목표 및 문제점:

목표

- 사내에서 기능을 구축할 만큼 아이덴티티가 중요한지 결정해야 합니다.
- 2개 이상의 제품 분야를 출시했고 이전 제품의 성공에 이어 또 다른 성공을 거두고자 합니다.
- 첫 제품의 우수 고객이 두 번째 제품도 채택하도록 해야 합니다.

문제점

- 조직은 GDPR, CCPA 등 다양한 규정 준수 요건을 충족해야 합니다.
- 조직의 팀이 아이덴티티 시스템의 프로토콜, 표준, 통합 기능 및 운영상의 문제와 관련하여 필요한 경험과 전문 지식이 부족할 수 있습니다.

요구 사항

CIAM 솔루션은 외부 아이덴티티의 위험과 관리 부담을 해소하는 데 도움이 되어야 합니다.

- 엔드 유저는 기존의 ID 공급자를 사용해 로그인할 수 있어야 합니다.
- 기존의 LDAP 또는 Active Directory에 인증을 위임할 수 있어야 합니다.

CIAM 솔루션을 통해 최신 표준을 준수하고 지속적인 캐치업 없이도 최상의 접근법과 보안 사례를 선택할 수 있어야 합니다.

솔루션

→ 사용자 관리의 확장

적절한 CIAM 솔루션은 기존의 아이덴티티를 이용해 사용자를 애플리케이션에 연결할 수 있어야 합니다.

또한 고객 또는 파트너의 LDAP나 Active Directory를 연결해 사용자 계정을 기존의 사용자 저장소에 동기화하고 아이덴티티 관리에 따른 위험을 해소해야 합니다.

→ 표준 및 미래 대비

CIAM 솔루션은 **OpenID Connect, OAuth, SAML**과 같은 최신 인증 표준을 지원하며 최신 사양에 맞게 지속적으로 조정되어야 합니다.

- 자동화를 통해 최신 **표준**을 채택하는 것은 확장 과정에서 매우 중요합니다.

보안 및 아이덴티티 표준이 주기적으로 바뀌고 있기 때문에 다음에 대한 추적이 필요합니다.

- 표준 및 프로토콜
  - JWT
  - SAML
  - OAuth2.0/OIDC
  - FIDO
  - PKCE
- ID 제공자
  - Apple을 통한 로그인
  - 소셜 인증

CIAM 솔루션은 프로비저닝이나 디프로비저닝과 같은 프로세스를 자동화하고 데이터 개인 정보를 관리해야 합니다.

→ 수명 주기 관리로 자동화된 프로비저닝

적합한 CIAM 플랫폼은 수명 주기 내 고객의 위치와 연결된 자동 워크플로우를 제공합니다.

- 이에 따라 스택 전체의 다운스트림 애플리케이션과 시스템에 사용자를 프로비저닝 또는 디프로비저닝할 수 있습니다.

CIAM 솔루션은 기업이 규모를 확장하고 목표가 커짐에 따라 보안을 강화해야 합니다.

- 안전하지 않거나 손상된 비밀번호에 자동으로 플래그를 지정해야 합니다.

이는 개발자 리소스를 사용하지 않고도 자동화되어야 합니다.

→ 비밀번호 보안

최신 아이덴티티 시스템을 통해 관리자는 다음을 수행할 수 있습니다.

- 비밀번호 복잡도 지정하기
- 흔한 비밀번호 확인하기
- 손상된 비밀번호 확인하기

CIAM 솔루션은 사용자 여정에서 가장 취약한 지점 중 하나를 보호해야 하는데, 바로 계정 또는 비밀번호 리셋 흐름입니다.

→ 성장하는 고객층의 요구 사항 충족하기

최신 솔루션은 자격 증명 리셋을 위해 강력한 수준의 보안을 활용하는 안전한 비밀번호 리셋 흐름을 지원합니다. 지원 사항:

- 보안 질문
- SMS
- 음성
- 비밀번호 재설정을 위한 일회용 비밀번호

CIAM 솔루션을 통해 엔드 유저에게 발생하는 마찰을 최소화하면서 애플리케이션 내 보안을 손쉽게 강화할 수 있어야 합니다. 필요 사항:

- 계정 탈취 방지
- 확실성 수준을 제공하고 사용자가 토큰의 소유자인지 확인

→ MFA로 사용자 보호하기

고객과 사용 사례에 적합한 인증 요소를 선택하여 구현해야 합니다. 여기에는 소유 여부의 증명을 확인하는 기능, 암호화 보안, 그리고 SMS, Google Auth, 이메일 등의 일반적인 수단이 포함됩니다.

인증 확실성 수준의 다양한 유형을 살펴보세요.

CIAM 솔루션은 확장이 가능해야 하며 맞춤형 인증 논리를 허용해야 합니다.

→ 후크를 통해 확장된 플랫폼 기능

다음과 같은 작업을 수행하기 위해 CIAM 솔루션으로 인증과 같은 핵심 플랫폼 프로세스를 확장할 수 있어야 합니다.

- 등록, 사용자 가져오기, 인증

솔루션이 내부 사용자용, 외부 사용자용에 관계없이 애플리케이션을 구동하는 기반 API를 포함해야 합니다.

→ API 액세스 관리

API 액세스 관리는 애플리케이션 백 엔드 및 기타 백 엔드 프로세스에 Oauth2 클라이언트 자격 증명 권한 부여 흐름을 사용해 액세스에 대한 상세 제어를 제공합니다.

CIAM 솔루션의 대시보드에 API 액세스 정책 및 액세스 권한 부여가 구성되어야 합니다.

2 CIAM 완성도 지침의 2단계 마무리하기

인증

- SSO
- 비밀번호 정책
- 안전한 리셋 흐름

MFA

- 기본 수준 인증 요소: SMS, 이메일, Google 인증자

권한 부여

- **API 액세스 관리** 및 API 액세스 정책
- 사용자 권한 부여에 대한 일관된 보기를 위해 API 게이트웨이와 통합

사용자 관리

- 단일 정보원, 특성 수준 마스터링, 사용자 프로필
- 하나의 아이덴티티에 대한 다중 프로필
- 사용자 숙련도

고급 인바운드 페더레이션

- 일반 OIDC
- SAML
- 단일 사용자 프로필(집계)
- 사용자 단일 뷰
- 계정 조정

Okta와 함께 이러한 기능을 구현하려면 지금 바로 **무료 개발자 플랜**을 이용해보세요.

이 단계가 완성되었다면 제품 도달 범위가 확장되고 사용자 관리와 규정 준수 및 보안 기능이 더욱 정교해진 것입니다. 확장이 지속됨에 따라 귀사는 더 강력한 보안 기능과 새로운 고객 경험 기능에 투자하고자 할 것입니다.

3 3단계

3단계: 지능형

손상 없이 최적화하기

이 단계에서는

- 제품으로 시장을 선도하는 위치에 있습니다.
- 까다로운 관계자(제품, 엔지니어링, 마케팅 팀 등)가 모두 특정 아이덴티티 요구 사항을 가지고 있습니다.
- 제품을 최적화함과 동시에 다음의 사항도 수행해야 합니다.
  - 확고한 시장 입지를 수립 및 확장 경쟁 우위를 유지
  - 사용자와 애플리케이션을 안전하게 보호
  - 조직 전체에서 개발 팀 유지

3단계 목표 및 문제점:

목표

- 기업의 데이터와 인프라, 그리고 사용자를 보호해야 합니다.
- 고객 경험을 간소화하고 마찰을 제거하며 개인화와 분석을 통해 새로운 기능을 적용해야 합니다.
- 제품의 수명 주기를 마케팅 엔진에 연결하고 브랜딩과 분석에 집중해야 합니다.

문제점

- 각 팀은 저마다의 우선 순위와 트레이드오프를 갖고 있으며 고객에게 유용한 기능을 제공하면서 이를 잘 조율해야 합니다.
- 시스템의 모듈성과 안전을 보장하도록 마이크로서비스와 API를 사용하는 인프라를 지속적으로 개선해야 합니다.

요구 사항

CIAM 솔루션은 등록 경험에 높은 수준의 확실성을 제공해야 합니다.

- 엔드 유저는 기존의 ID 공급자를 사용해 로그인할 수 있어야 합니다.
- 기존의 LDAP 또는 Active Directory에 인증을 위임할 수 있어야 합니다.

CIAM 솔루션은 매우 안전하고 원활하며 액세스 가능하고 신뢰할 수 있는 사용자 경험을 제공해야 합니다.

CIAM 솔루션은 보안 위험을 믿을 수 있게 식별하고 완화해야 합니다.

아이덴티티 전략은 고객 데이터를 저장하고 연결하는 중앙 시스템을 비롯해 규정 준수 요건을 충족하는 자동화된 정책을 포함해야 합니다.

솔루션

정교한 온보딩

CIAM 솔루션에는 아이덴티티 증명과 계정 확인 기능이 적용되어 적법한 사용자만 승인하여 플랫폼에 온보딩해야 합니다.

- 등록 프로세스는 사용자를 인증하고 실제 아이덴티티에 연결해야 합니다.

적절한 CIAM 프로세스를 이용하면 **아이덴티티 해결을 아이덴티티 인증으로 전달**할 수도 있습니다.

적응형 MFA

이 솔루션은 생체 인식(터치 ID, 페이스 ID 등) 및 행동적 입력을 사용해 필요 시 위험과 추가 인증을 할당하는 적응형 지능 계층을 제공합니다.

플랫폼 데이터

Okta의 플랫폼을 사용해 더 많은 이벤트 데이터와 활동 데이터를 범위 안에 가져오면 선제적인 위험 탐지와 공격 방지가 가능합니다.

개인 정보 및 규정 준수

수월한 삭제 및 업데이트, 다운로드를 위해 중앙 연결 시스템의 사용자 수명 주기 및 데이터 관리를 강화하여 **개인 정보 및 보안 준수 요구 사항을 충족**할 수 있습니다.

CIAM 솔루션에는 비밀번호가 필요 없는 강력한 인증자가 필요합니다.

→ **비밀번호 없는 인증**

매직 링크 이메일나 WebAuthn을 사용한 비밀번호 없는 테크놀로지를 통해 도난 또는 손상된 비밀번호에 의해 발생하는 모든 아이덴티티 공격을 제거할 수 있습니다.

CIAM 솔루션은 보안 스택이 일관되게 작동할 수 있도록 심층적인 보안을 제공해야 합니다.

→ **보안 확장 가능성**

봇 완화 솔루션이나 웹 애플리케이션 방화벽과 같은 보안 제품은 CIAM 솔루션과 함께 작동하여 모든 공격을 방지합니다.

CIAM 솔루션은 고객 여정에서 사용자 편의성을 구현해야 합니다.

→ **마찰 최소화를 위한 최적화**

점진적 프로파일링을 통해 시간 경과에 따라 사용자 특성을 포착하는 맞춤형 경험을 구축하여 마찰을 줄일 수 있습니다.

CIAM 솔루션은 확장이 가능하며 맞춤형 인증 논리를 허용해야 합니다.

→ **플랫폼 확장 가능성**

CIAM 솔루션은 **후크**와 같은 기능으로 확장 가능성을 지원해야 합니다. 이러한 확장 포인트는 사용자 여정 중 등록, 사용자 가져오기, 인증과 같은 단계에 포함되어야 합니다.

솔루션은 각 관계자의 특정 요구 사항을 충족해야 합니다.

→ **통합 기능**

Okta의 통합 기능은 사용자 아이덴티티의 모든 부분을 연결해 각 상황(발권 및 지원, 고객 관계 관리, 전자 상거래 플랫폼 등)에 맞는 최적의 시스템을 선택할 수 있게 해줍니다.

CIAM 솔루션은 유수의 개인 정보 및 규정 준수 공급 업체와 협력해야 합니다.

→ **스택 중심의 Okta**

CIAM 솔루션은 아이덴티티, 마케팅 및 설정 도구의 각 요소 전체에서 데이터 특성 및 원활한 동기화 변경을 표시해야 합니다. 최신 CIAM 솔루션은 고객 선호도와 개인 정보 준수 요건을 추적하는 개인 정보 도구와 통합될 수 있습니다.

3 CIAM 완성도 지침의 3단계 마무리하기

인증

- 비밀번호 없는 인증

MFA

- 적응형 인증

사용자 관리

- 등록 후크
- 점진적 프로파일링

맞춤화

- Hooks
- 개인화

통합 기능

- ID 인증 통합 기능 부정
- 행위 및 위험 통합 기능
- 보안 통합 기능
- 동의 및 개인 정보 통합 기능

Okta의 이점을 자세히 알아보시려면 다음 리소스를 참고하세요.

- 적응형 다중 요소 인증
- 비밀번호 없는 인증
- 플랫폼 Okta Hooks

이 시점에서는 애플리케이션이 고객에게 강력한 보안을 제공하며 비밀번호 없는 보안도 가능합니다. 고객 데이터를 사용 및 보관함으로써 삶의 질을 개인별로 개선하고 데이터 개인 정보 규정을 완벽히 준수할 수 있습니다. 업계 최고의 통합 기능 덕분에 아이덴티티 보안이 엄격히 유지되며 위험을 선제적으로 탐지하여 완화할 수 있습니다. 고객은 신뢰를 갖고 서비스를 간편하게 이용할 수 있고, 기업은 고급 기능을 탐색할 수 있게 됩니다.

4 4단계

4단계: 지속형

새로운 표준의 주도와 정립

이 단계에서는

- 귀사의 제품이 시장을 확고하게 주도합니다.
- 디지털 전환 프로젝트에 대한 지지 기반이 확고해집니다.
- 보안과 사용자 경험을 모두 최적화하는 옴니 채널 전략을 보유하고 있습니다.
- 귀사의 제품이 고급 부정 행위 및 위험 방지 솔루션과 확실히 통합됩니다.
- 아이덴티티를 장기적인 전략이 필요한 지속적인 여정으로 간주하게 됩니다.
- 사내에 아이덴티티 전문가와 CIAM의 책임자가 있습니다.

4단계 목표:

목표

보안

- 사용자가 적절한 시기에 인증할 수 있어야 합니다.
- 보안 응답과 오케스트레이션을 자동화해야 합니다.
- 여러 보안 정책과 규칙을 축소하고자 합니다.

옴니 채널 경험

- 저장소, 휴대 장치, 웹 등 다양한 채널에 걸쳐 사용자를 추적하고자 합니다. 고객 여정과 경험을 지원 및 통일하고자 합니다.
- 채널 전반의 부정 행위를 줄이고자 합니다.

세분화된 권한 부여 및 위험 기반 권한 부여

- 위험 및 사용자의 컨텍스트에 기반한 동적인 권한 부여가 필요합니다.

규정 준수

- 디자인별 개인 정보, 진화하는 규정에 적합한 데이터 처리와 스토리지 연습이 필요합니다.

요구 사항

솔루션

사용자는 긴 세션 시간을 기대하며 기업은 세션 시간에서 마찰을 최대한 줄이고자 합니다.

→

유용한 위험 신호

CIAM 플랫폼은 다양한 센서로부터 위험 신호를 수집 및 분석하여 세션 위험을 식별해야 합니다.

센서는 내부 위험 신호와 타사 위험 신호가 결합한 것일 수 있습니다. 위험 신호는 다음과 같은 범주로 설정될 수 있습니다.

- 네트워크
- 위치
- 디바이스
- 트랜잭션

위험 점수가 특정 기준치를 넘어설 경우 CIAM 플랫폼은 사용자의 아이덴티티를 강제로 재확인하거나 세션을 강제 종료할 수 있습니다.

세션 위험 점수 계산은 고정된 시간 간격으로 예약되거나 애플리케이션의 특정 사용자 이벤트에 의해 트리거 될 수 있습니다.

보안 응답과 오케스트레이션을 자동화해야 합니다.

→

유연한 보안 워크플로우

인시던트 응답 및 아이덴티티 오케스트레이션을 지원하는 보안 워크플로우는 인시던트 보강 및 조정을 권장하게 됩니다.

아이덴티티 및 보안 정책 관리에 소요되는 시간과 인력을 절감해야 합니다.

→

보안 정책 절감

CIAM 솔루션의 AI/ML 기능이 관리자가 관리해야 하는 보안 정책의 수를 줄여줍니다.

채널 전반에서 사용자를 추적하고 각 채널 사이에서 원활한 경험을 제공하고자 합니다.

옴니 채널 사용자 경험

모든 사용자 참여 채널은 CIAM 솔루션을 통해 인증하거나 인증 데이터를 저장해야 합니다.

모든 디지털 채널은 표준 프로토콜로 인증하여 사용자에 대한 단일 뷰를 제공해야 합니다.

Okta의 **보안 정보 및 이벤트 관리(SIEM, Security Information and Event Management) 애플리케이션 및 대시보드**는 Okta와 타사 옴니 채널 인증 도구의 로그 집합을 표시할 수 있습니다.

모든 데이터 노출에 대해 세분화된 제어가 필요합니다.

규정 및 제어

위험 기반 인증은 특정 데이터 요소에 액세스할 수 있는 사람과 데이터에 액세스할 수 있는 장소를 결정합니다.

애플리케이션과 데이터 소스 또는 유형에 세분화된 액세스 제어를 지원해야 합니다.

Open Banking 사양 및 강력한 고객 인증(SCA, Strong Customer Authentication) 트랜잭션 서명을 지원해야 할 가능성이 높습니다.

산업 표준 충족

CIAM 솔루션의 인증 엔진을 통해 트랜잭션 읽고 쓰기에 대한 **재무 등급 API (FAPI) 지원**이 제공되어야 합니다.

기존 인증 요소를 통해 SCA 트랜잭션 서명이 지원되어야 합니다.

4 CIAM 완성도 지침의 4단계 마무리하기

MFA

- 지속형 인증
- 타사 위험 신호
- 다중 모델 AI 위험 엔진
- 보안 및 아이덴티티 오케스트레이션 및 응답

권한 부여

- 세분화된 권한 부여

표준

- FAPI
- SCA

통합 기능

- 옴니 채널 인증 통합 기능

CIAM 완성도

Okta의 이점을 자세히 알아보시려면 다음 리소스를 참고하세요.

- 위험 기반 인증 보안과 편의성 중에서 하나를 포기할 필요가 없습니다.
- Okta 인사이트
- Okta + PlainID

CIAM 완성도에 이르는 길에서 모두 사라진 장애물

CIAM을 제품 로드맵에 내장하는 것은 초보 제품 개발자와 자리를 잡은 시장 리더 모두에게 매우 중요한 일입니다. CIAM 완성도 곡선에서 자사의 현재 위치를 파악하면 성공을 모니터링하고 주력 분야를 식별하여 경쟁 우위를 제공하는 분야를 명확히 이해할 수 있습니다.

최고의 애플리케이션이나 디지털 서비스를 구축하려면 집중식 자율 경영 팀이 필요합니다. CIAM 파트너로 Okta를 선택한다면 가장 자신 있는 영역에 시간과 리소스를 할애하면서 규정을 모니터링하고 통합 기능을 구축할 수 있습니다. Okta의 CIAM 솔루션은 사용자와 함께 성장하며 개발자가 중요한 작업에 집중할 수 있도록 지원합니다.

지금 연락하여 Okta를 통해 CIAM 완성도에 이르는 방법을 알아보세요.