

Okta

Introduction

베스핀글로벌 / Premier Partner

문의 / zerotrust@bespinglobal.com

Safe harbor

이 프레젠테이션에는 1995년에 제정된 미국 증권민사소송개혁법(Private Securities Litigation Reform Act)의 "세이프 하버" 조항의 의미 내에서 재무 전망, 제품 개발, 사업 전략 및 계획, 시장 트렌드, 기회 및 포지셔닝에 관한 진술 등을 포함한 "미래 예측 진술"이 포함되어 있습니다. 이러한 미래 예측 진술은 현재의 예상, 추정, 전망 및 예측을 기반으로 합니다. "기대한다", "예견한다", "해야 한다", "믿는다", "희망한다", "목표로 삼는다", "예상한다", "목표", "추정한다", "잠재적", "예측한다", "할 수 있다", "할 것이다", "할지도 모른다", "할 수 있을 것이다", "작정이다", "일 것이다"와 같은 단어와 이러한 용어의 변형이나 이와 유사한 표현은 이러한 미래 예측 진술을 식별하기 위한 것입니다. 단, 모든 미래 예측 진술에 이러한 식별 단어가 포함되어 있는 것은 아닙니다. 미래 예측 진술은 Okta의 통제권을 벗어난 요인이나 상황으로 인해 발생하는 많은 위험 요소와 불확실성의 영향을 받습니다. 예를 들어 Okta 제품 시장은 예상보다, 또는 과거보다 느리게 발전할 수 있고, 운영 결과가 예상보다 더 많이 변동할 수 있으며, 수익 인식 등과 관련된 운영 결과 및 현금 흐름에서 상당한 변동이 있을 수 있습니다. 또한 네트워크, 데이터 또는 고객 데이터에 대한 무단 액세스를 허용하는 네트워크 또는 데이터 보안 사고로 인해 Okta의 평판이 훼손될 수 있고, 서비스 중단을 포함하여 테크놀로지외 관련된 중단 또는 성능 문제를 경험할 수 있으며, 만기일에 전환형 선순위 어음을 지불하지 못할 수도 있고, 전 세계 경제 상황이 악화될 수도 있습니다. 재무 결과에 영향을 미칠 수 있는 잠재적 요인에 대한 추가 정보는 Form 10-Q의 최신 분기 보고서와 증권 거래위원회에 제출된 기타 서류에 포함되어 있습니다. 이 프레젠테이션에 포함된 미래 예측 진술은 프레젠테이션 발표 당시 Okta의 의견일 뿐이며, Okta는 어떠한 의무도 지지 않고 이러한 미래 예측 진술을 업데이트 할 의사도 없습니다.

이 프레젠테이션에서 언급된 모든 미출시 제품이나 특징 또는 기능은 현재 지원이 되지 않으며, 제때 제공되지 않거나 전혀 제공되지 않을 수 있습니다. 제품 로드맵은 제품, 특징 또는 기능을 제공할겠다는 약정이나 의무 또는 약속이 아니므로 이를 토대로 구매를 결정해서는 안 됩니다.

Agenda items

01

Okta 회사 소개
Company overview

02

클라우드 환경,
아이덴티티 관리의 문제
IAM challenges in the era of the cloud

03

Okta의 모범 사례
The best practice with Okta

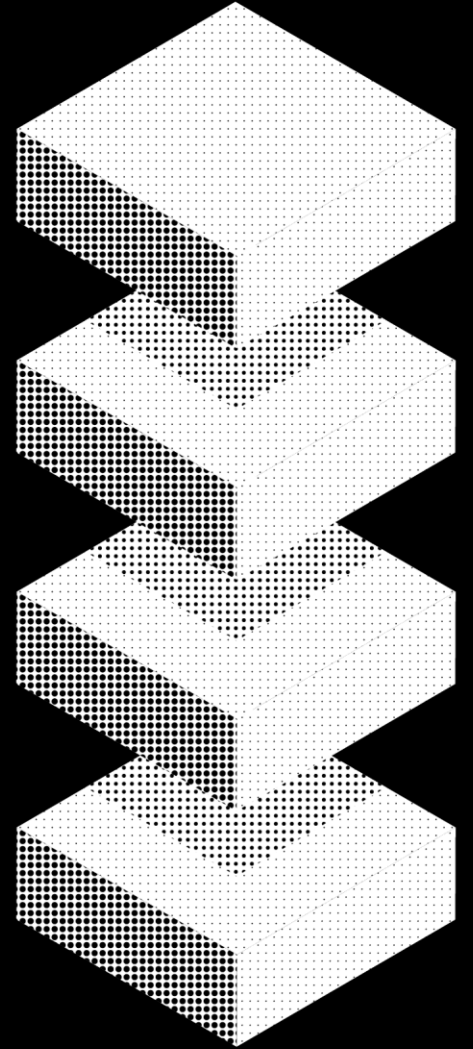
04

시작을 위한 제언
Recommendations for the next steps

01

Okta 회사소개

우리의 미션은 모든 기업이 다양한 기술에 쉽고
안전하게 연결되는 세상을 만드는 것입니다.



Okta, IDaaS 영역의 선두주자



2009년 설립

클라우드 기반
아이덴티티 관리
모델을 개척한 이래,
기술적 혁신을
이어가고 있습니다

- 2017년 나스닥 상장
- 시가총액 23B USD
- 매출 835M USD



전세계 1만+ 고객사

글로벌
엔터프라이즈에서
SMB, 스타트업까지
다양한 고객사가
Okta를 사랑합니다

- US, EMEA, APAC
- 금융, 공공기관을
비롯한 다양한
산업군



일일 접속 사용자 5M+

수많은 사용자들이
오늘도 Okta를 통해
다양한
어플리케이션에
안전하고 편리하게
접속합니다



7000개 이상 앱 연동

인증 설정과
계정관리 자동화를
위한 사전 정의된
연동 커넥터가
준비되어 있습니다

- 업계 최다 앱 지원
- SSO 및 계정관리
라이프사이클
자동화 지원



가트너 MQ IAM 리더

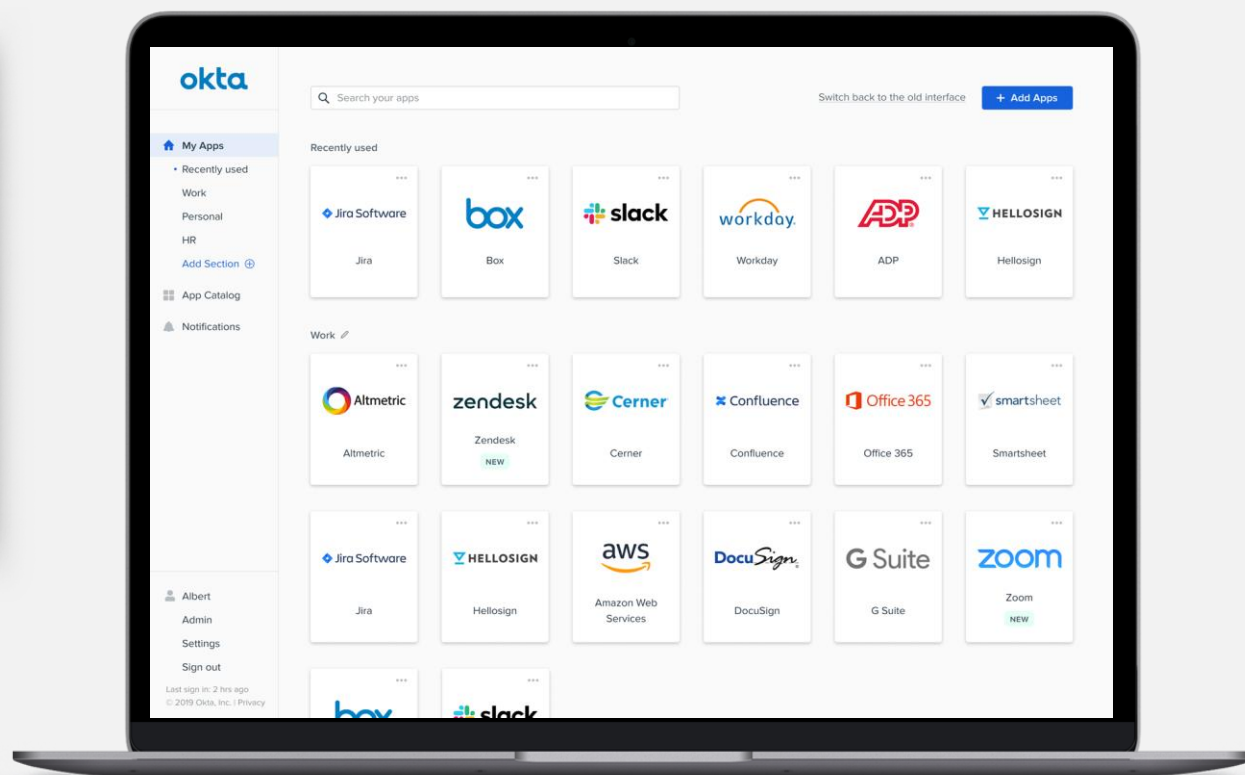
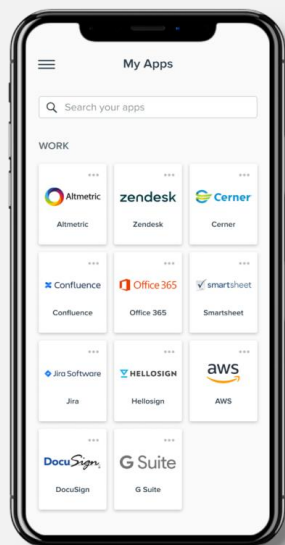
Identity and Access
Management
분야에서 독보적인
경쟁력 및 사용자
만족도를
검증받았습니다

클라우드 기반 모던 아이덴티티 플랫폼

아이덴티티 중심의 접근으로
Zero Trust 보안을 실현합니다

기업 내부 사용자를 위한
Workforce Identity

고객 서비스 앱 개발을 위한
Customer Identity



10,000+ 글로벌 기업이 Okta를 사용합니다



의료복지



컨슈머



테크놀로지



금융



공공기관/NGO



제조/에너지



서비스



미디어



클라우드

--	--	--	--	--	--	--	--	--

Okta

주요 고객 사례



정책 기반의 접근 관리

65,000명 직원이 사용하는 400개 이상의 앱에 대한 SSO를 레거시 ADFS + Ping 시스템에서 클라우드 IAM으로 전환

개발자 포털의 40개 이상 앱을 API Access Management로 관리

CXO 레벨에 MFA를 적용하여 인증 보안 강화

okta



MFA 적용 및 확장

5,000명 정규 및 계약 직원이 Okta 이용하여 25개 이상 내부 어플리케이션 접속

금융사 보안 규제에 대응한 통합 사용자 인증 관리 체계 구축

빠른 어플리케이션 인증 연동 (1개 앱 당 15분 소요)



하이브리드 IT 접근 및 유저 관리 자동화

에너지, 유통, 도시개발, 금융, 의료 등 다양한 사업 추진을 위한 다수의 SaaS 앱 및 On-Prem 앱에 대한 안전하면서도 편리한 인증 시스템으로 Okta를 선택

직원의 입사, 부서 변경, 퇴사에 따른 계정 관리 자동화

800개 사업부서, 14만 사용자 대상 44개 앱 연동에 단 3개월 소요



사내 검증 이후 Customer Identity로 확장

20만 사내 직원 대상 Okta 도입으로 O365 등 300개 사내 시스템 연동

1천만 엔터프라이즈 고객이 사용하는 Adobe Creative Cloud의 subscription 인증을 9개월 만에 Okta로 구현



글로벌 스케일 웹사이트 인증 처리

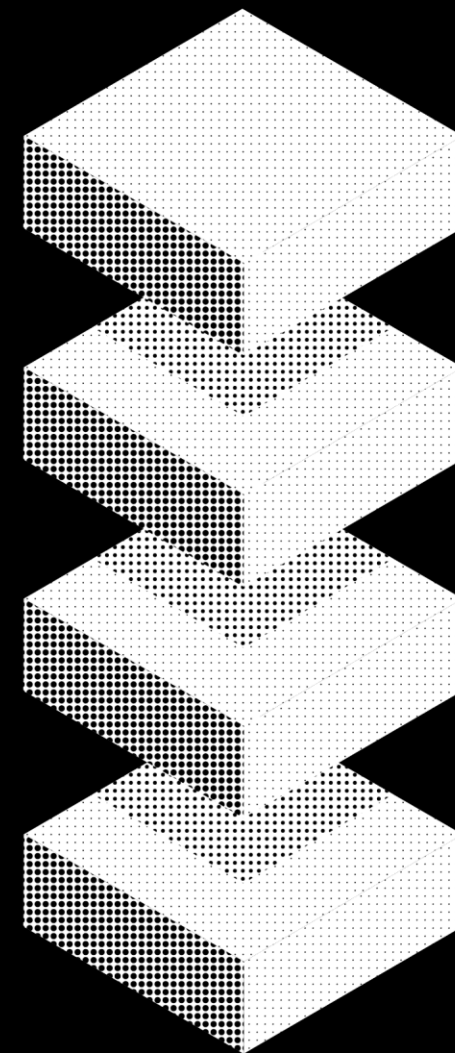
3천2백만 기존 MLB 팬 정보를 Okta로 이전

최대 분당 138,348 토큰 처리 가능하도록 테스트 (2019년 시즌 오픈 시 실제 최대 분당 7,453 토큰 처리 발생)

구매부터 구축, 시즌 오픈까지 9개월 만에 완료

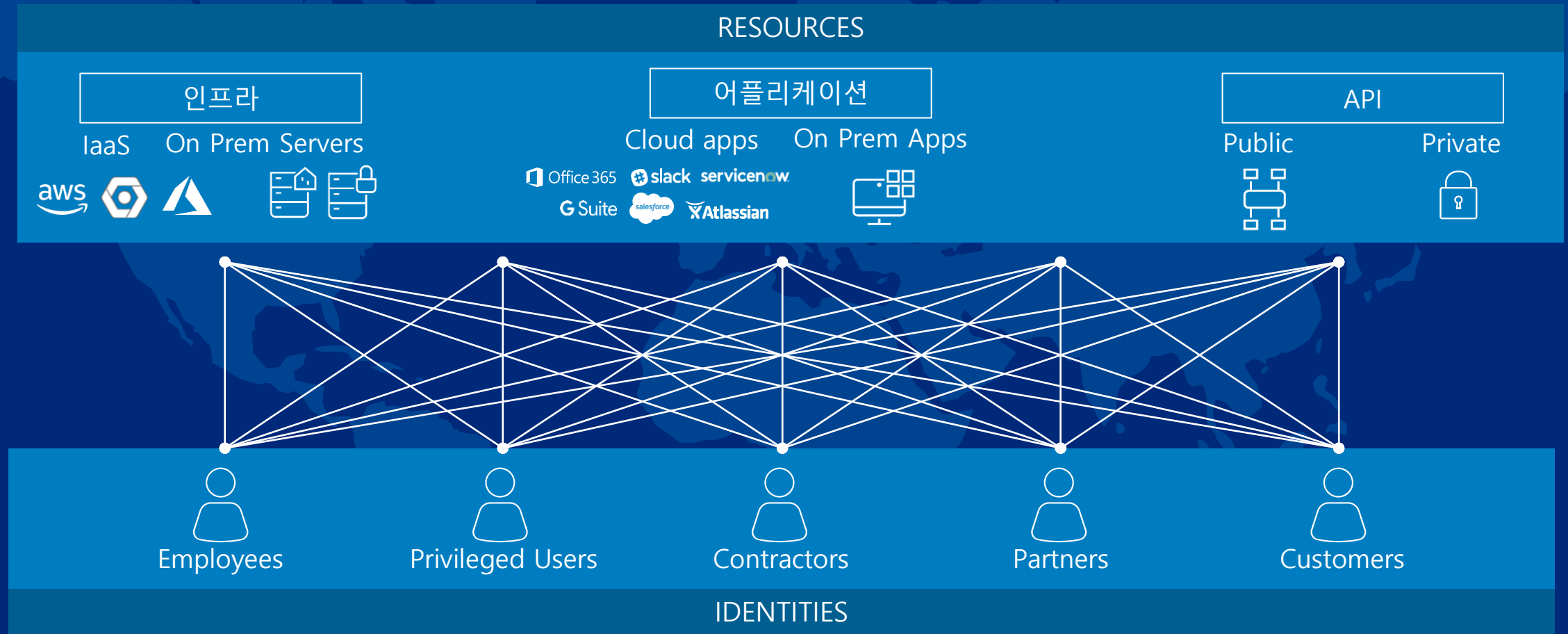
02

클라우드 환경, 아이덴티티 관리의 문제



하이브리드 IT 환경: 클라우드, 원격 근무, 디지털 전환

사용자도 기업 IT 리소스도 다양한 장소에서 다양한 형태로 연결되어야 함



데이터 유출 사고 원인: 아이덴티티 보안 미비

81%

데이터 유출 사고의 81%가
취약 패스워드, 계정 탈취로 발생

91%

Phishing Attack의 91%가
사용자 계정을 목표로 함

80%

보안 침해 사고 80%가
관리 권한을 가진 계정에서 발생

Identity가 정보 보안의 가장 취약한 연결고리

¹Source: 2017 Verizon Data Breach Investigations Report

²Source: 2016 Verizon Data Breach Investigations Report

³The Forrester Wave: Privileged Identity Management, Q3 2016

Zero Trust: 새로운 보안 사상의 목표



적합한 사용자만이



적합한 권한을 가지고



적절한 자원에



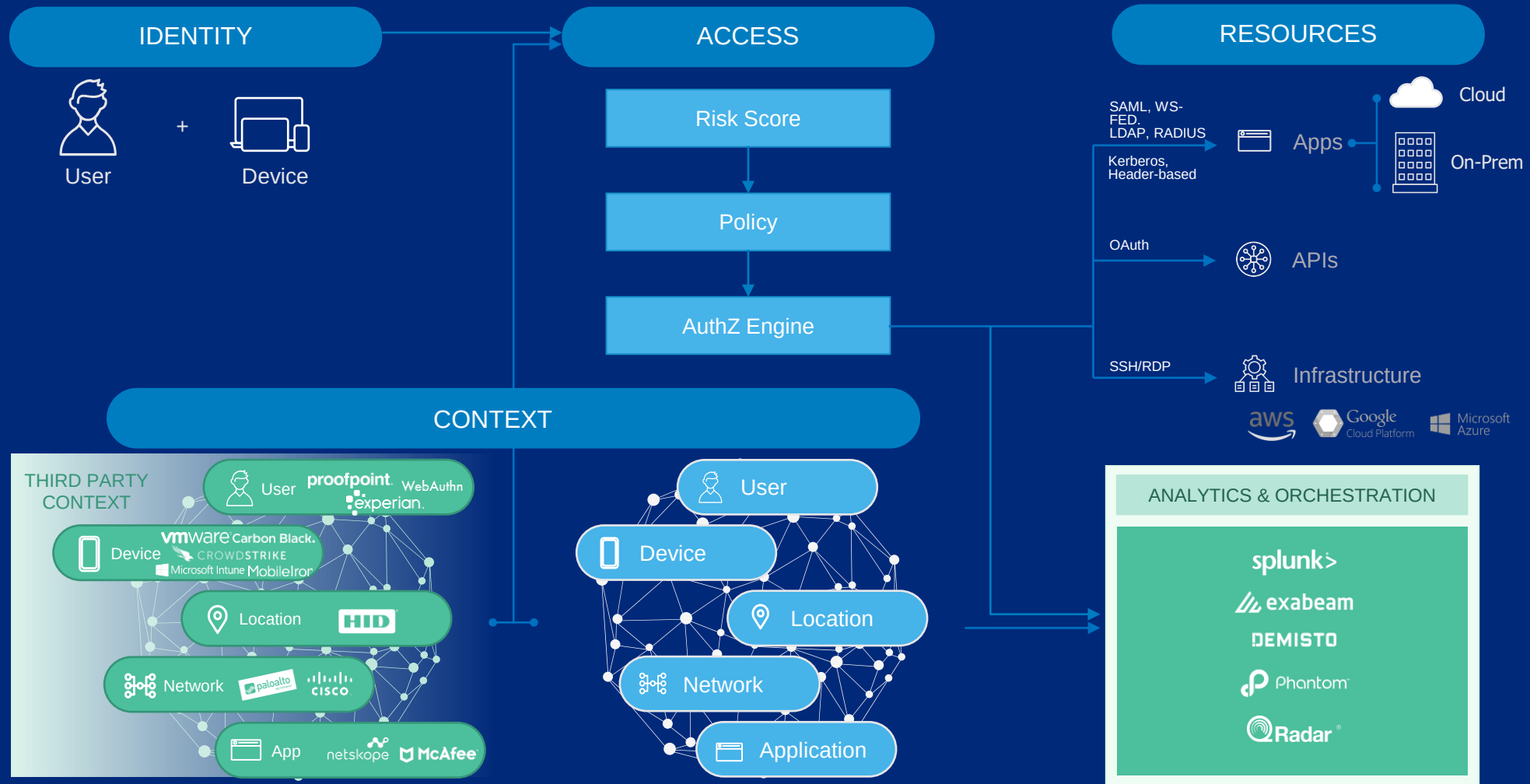
적합한 맥락에서



이러한 조건을
지속적 검증

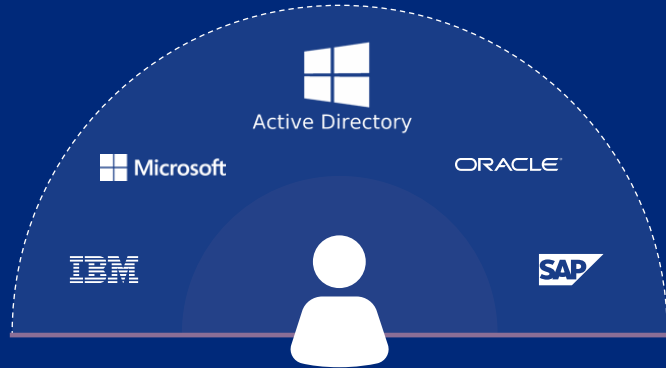
보안에 대한 고려가 사용자 편의성에 대치되지 않아야 함

Zero Trust 실현에 아이덴티티는 필수요소



Software as a Service: 단일 벤더 시대의 종말

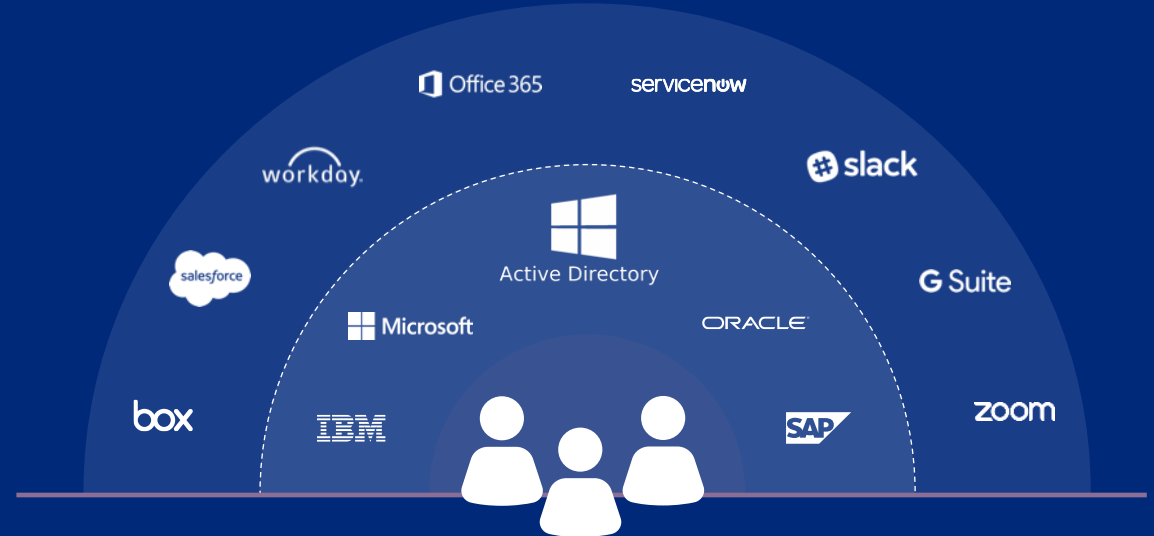
무수히 많은 고도로 전문화된 벤더들이 세분화된 분야에서 치열하게 경쟁 → The Best of Breed 조합



평생직장을 꿈꾸는 정직원

과거

거의 모든 IT 시스템을
몇몇 특정 벤더에서 공급



다양한 장소에서 다양한 형태로 근무하는 지식 노동자

현재

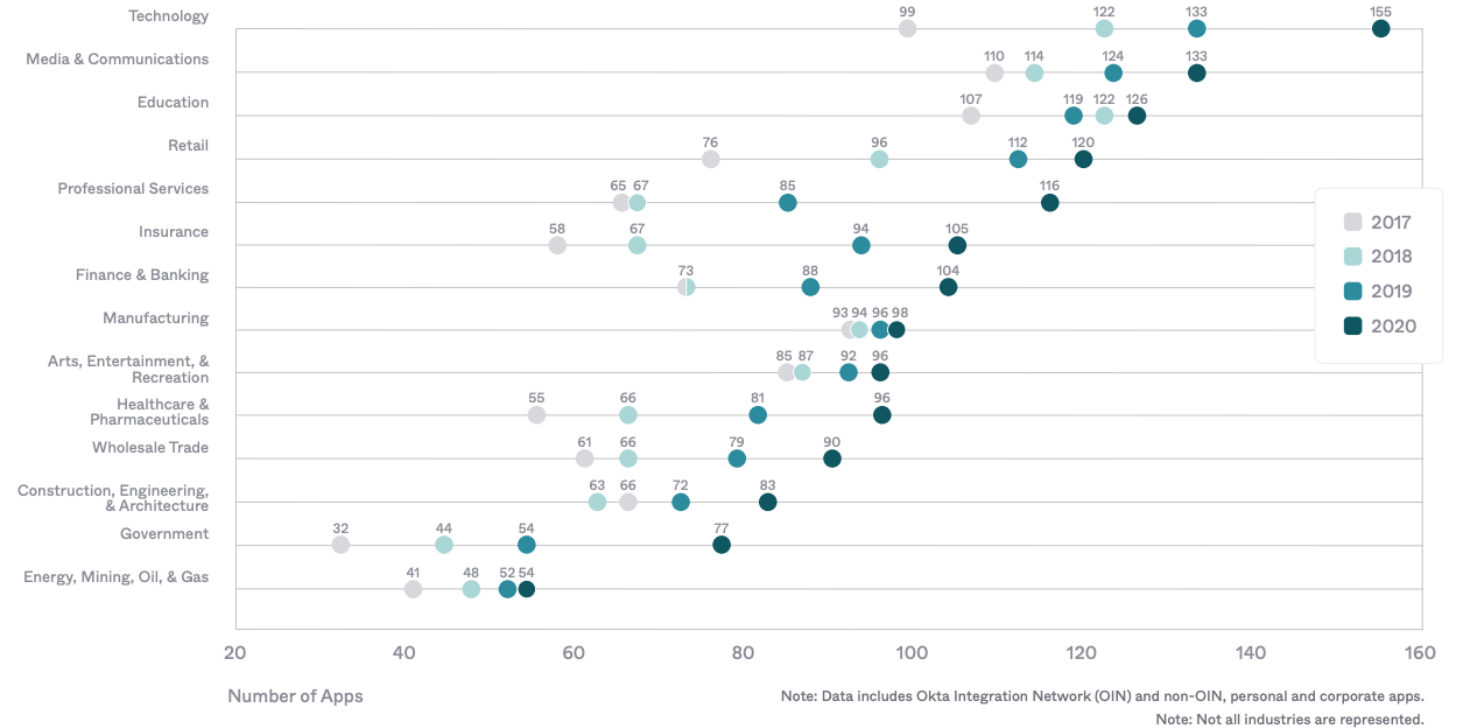
직원 생산성 향상을 위해
분야별 최고의 기술을 도입

앱 사용 트렌드

Okta 자체 발간 보고서인
Business@Work에 따르면...

- 2020년 Okta 고객사가 평균적으로 사용하는 앱 종류는 **88개**
- 매년 모든 산업군에서 지속적으로 증가
- 산업 별로는 Technology 기업 평균이 155개로 가장 높고, Energy 평균이 54개로 가장 낮음
- Technology, Professional Service, Finance & Banking 그리고 Government 분야에서 2019년에 비해 앱 사용 숫자가 큰 폭으로 증가

Average Number of Apps per Customer, by Industry



SaaS 앱 증가 시 아이덴티티 문제

사용자 (기업 임직원 및 고객)

✗ 비밀번호 피로도 증가

- 각 앱에서 관리하는 비밀번호 기억 및 관리 필요
- 동일한 비밀번호를 여러 앱에 사용하면서 보안 위험이 발생

✗ 앱 액세스 요청 및 관리 복잡도 증가

- 앱마다 담당 관리자에게 액세스 권한 요청
- 비밀번호 분실 시 제각각의 방식으로 리셋 요청
- 앱이 늘어날 때마다 기억해야 할 접속 URL 증가

✗ 부서/업무 변경 시 필요한 액세스 파악에 업무 지연

관리자 (IT 운영 관리자 및 보안 담당자)

✗ 사용자 계정 관리 작업량 증가

- 사용자 전입/이동/전출 시 계정 생성/수정/삭제를 위한 IT 부서 운영인력 작업량 증가
- 각 앱마다 서로 다른 사용자 계정 관리 방식을 숙지하고 적응해야 함

✗ 체계적인 액세스 정책 수립이 어려움

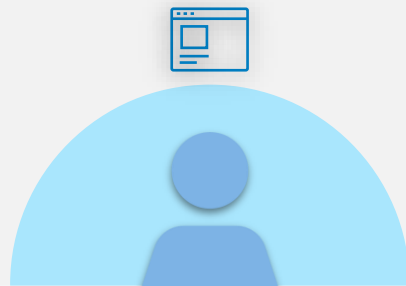
- 아이디/패스워드 발급 또는 무효화 외에 앱 접근에 대한 중앙 통제 혹은 체계화된 정책 수립이 어려움

✗ 보안 가시성이 떨어짐

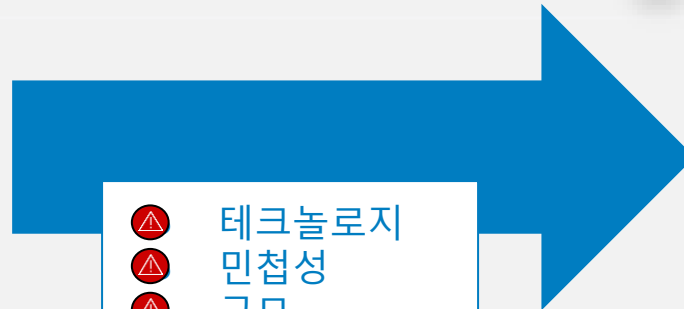
- 누가 어떤 앱에 언제 어떻게 로그인하는지에 대해 개별 앱에서 각각 확인해야 함

디지털 시대, 다양한 고객 참여 방식

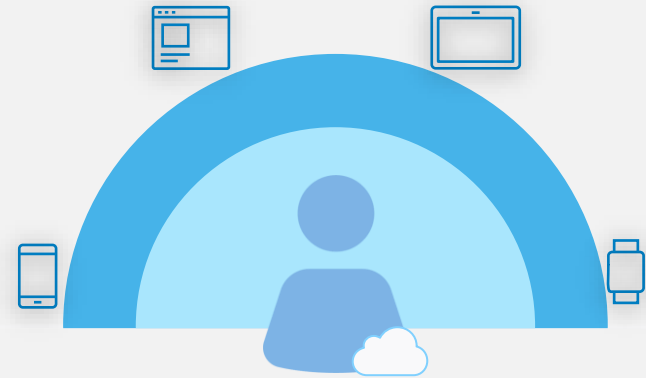
온라인에서도 웹과 앱, API 등 다양한 채널로 고객 서비스가 이루어짐



웹사이트
온프레미스
오프라인 매장



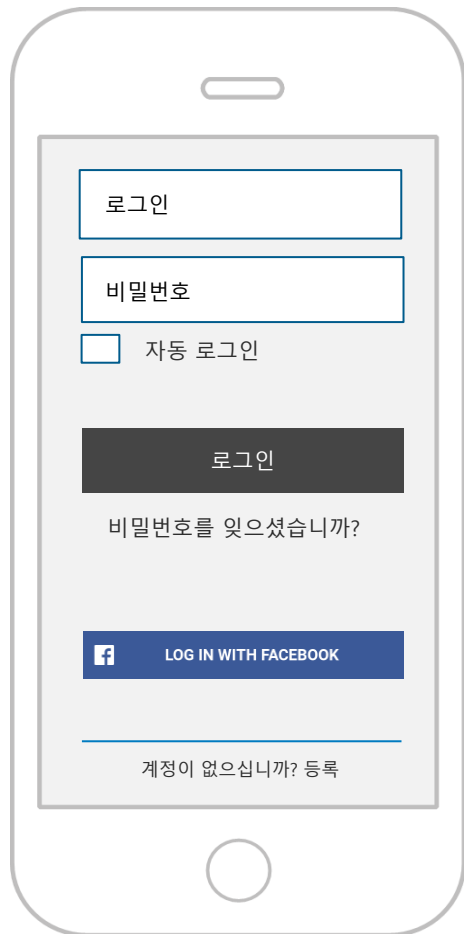
테크놀로지
민첩성
규모



앱 및 마이크로서비스
클라우드
옴니 채널

아이덴티티 구축은 복잡하고 시간이 걸림

한정된 개발자 리소스가 비즈니스 코어 서비스가 아닌, 인증 구축에 장기간 투입



okta

1개월

- 비밀번호 저장 및 보안
- API 게이트웨이 통합
- 또 다른 IDP에 통합
- API 리소스 서버 구축
- OAuth 토큰 해지에 아이덴티티 라이프사이클 통합
- 네트워크 게이트웨이 통합

4개월

- 토큰 스토어 구축
- OAuth 2.0 구현
- OIDC 구현
- 등록, 로그인 및 계정 복구 워크플로우
- MFA 정책
- 프로비저닝 커넥터
- SSO 커넥터

1년-3년

- 양방향 동기화에 AD 통합
- 유연한 사용자 프로필, 그룹, 디렉토리 앱 서버, 데이터베이스 및 최신 암호화 방식을 탑재한 확장 가능한 사용자 리포지토리
- 멀티테넌트 지원

2개월

- 음성, SMS, RSA 토큰 MFA
- 비밀번호 및 사용자 마이그레이션
- SSL 종단

3개월

- OAuth 권한 검증 서버 구축
- 헬프 데스크 UI

6개월

- SSO를 위한 SAML 구현
- 프로비저닝 엔진
- 소셜 인증 및 프로필 동기화
- 네이티브 모바일 앱에 내장된 푸시 기능을 통한 MFA

개발자 다수: 보안 코드 작성 교육을 받지 않음



OWASP의 10대 중요 웹 애플리케이션 보안
리스크 목록에서 2위에 오른 인증 실패

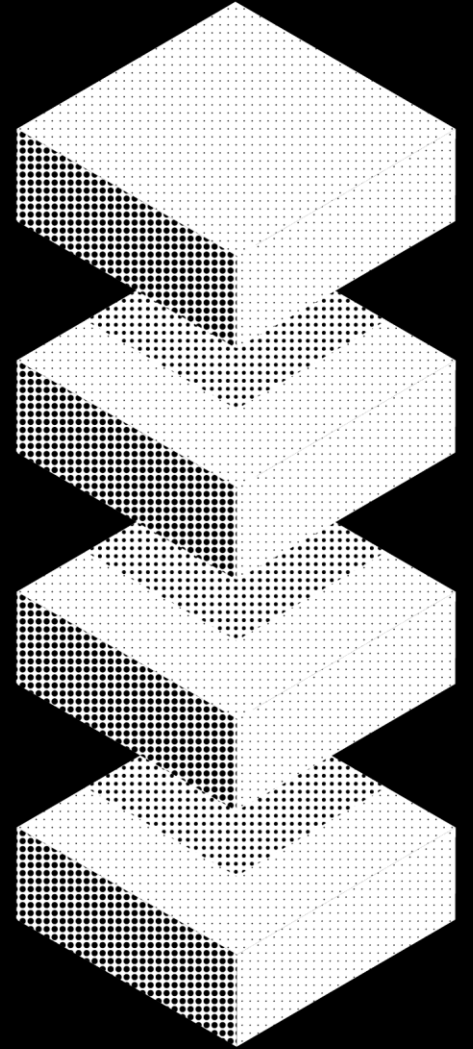
공통 취약점:

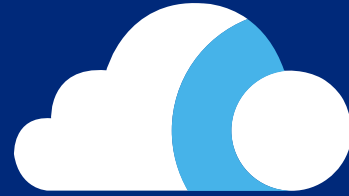
- 자격 증명 스템핑(stuffing)과 같은 자동화된 공격 허용
- 무차별 대입(brute force) 공격 허용
- 취약한 자격 증명 복구 프로세스 사용
- 취약한 해시 알고리즘 비밀번호 사용
- 비효과적인 MFA 운영
- URL에서 세션 ID 노출
- 로그인 성공 이후 세션 ID를 교체하지 않음
- 세션 ID 또는 토큰을 적절하게 무효화하지 않음

Okta의 모범사례

사용자가 업무에 필요한 다양한 SaaS 앱에 쉽고
안전하게 접근하게 하려면?

여러 클라우드 시스템을 도입하면서도 IT 운영의
효율성과 보안의 가시성을 유지하려면?





Okta Identity Cloud

Workforce Identity



Single
Sign-On



Universal
Directory



Advanced
Server Access



Adaptive
MFA



Lifecycle
Mgmt.



Access
Gateway



API Access
Mgmt.



Developer



One App



Enterprise

Customer Identity



Directories



Integrations



Insights



Identity Engine

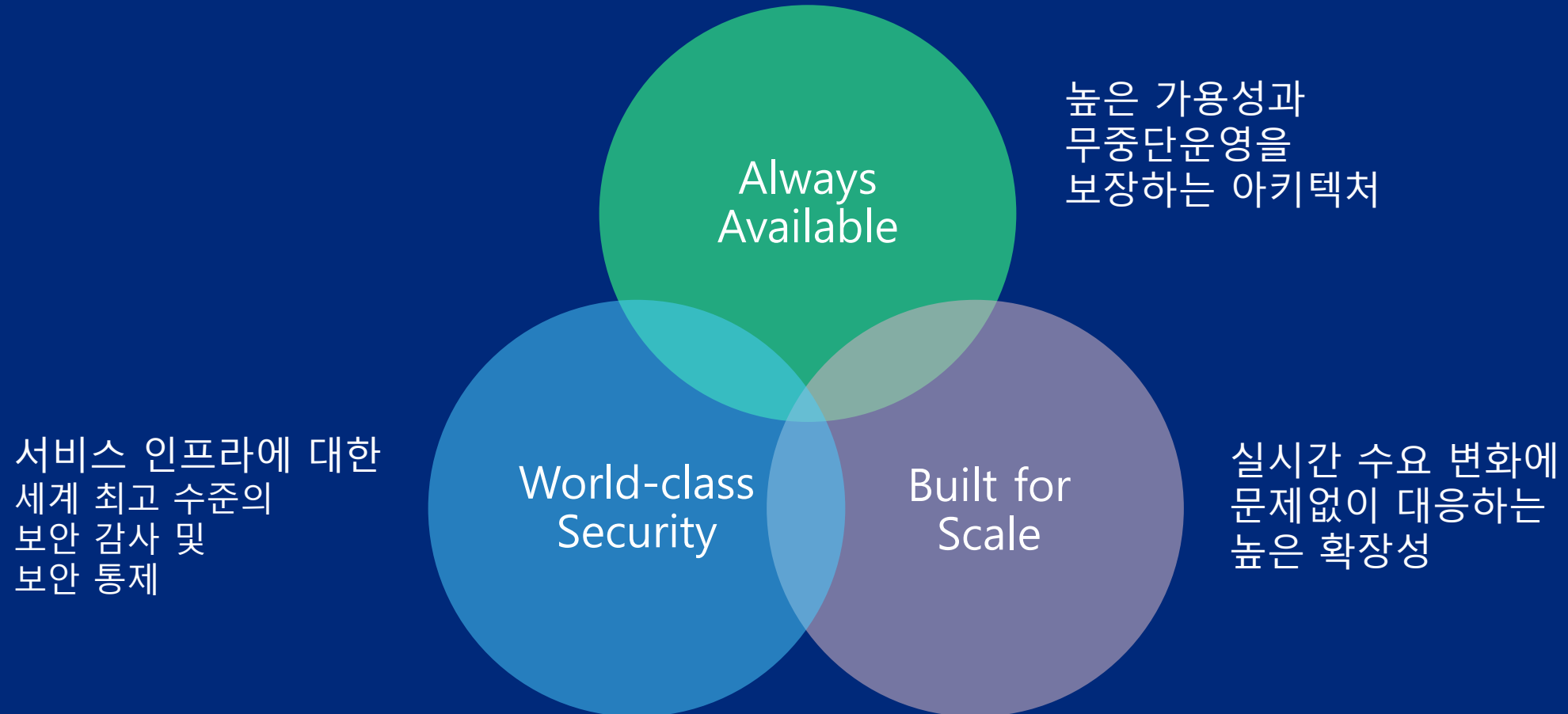


Workflows



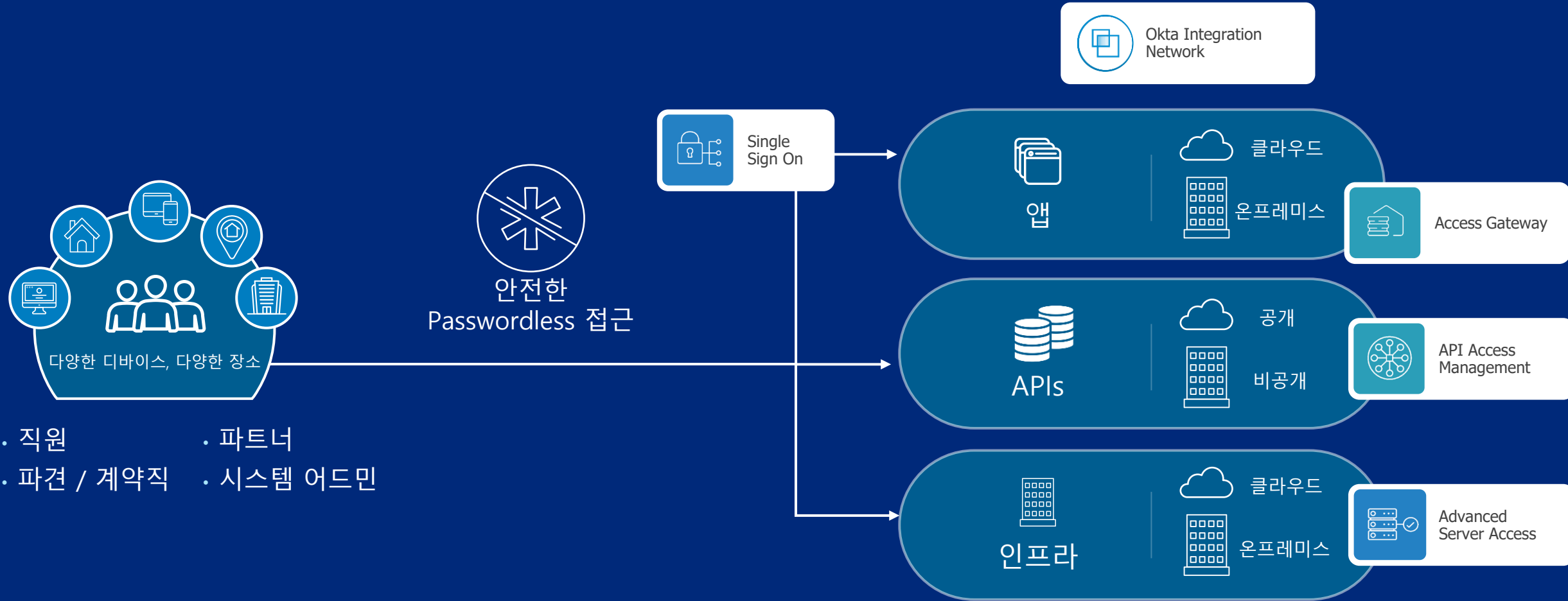
Devices

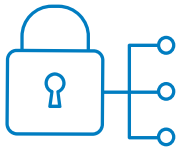
Okta의 'Always-On' 아키텍처는 고객사의 비즈니스 연속성을 담보한 디지털 전환을 가능케 합니다.



장소에 구애받지 않는 업무 환경 구현

모든 사용자, 리소스, 디바이스에 대해 필요한 곳에 안전한 액세스를 제공





Single Sign-On

회사의 모든 디지털 리소스를 안전하고 편리하게 연동

Product Highlights



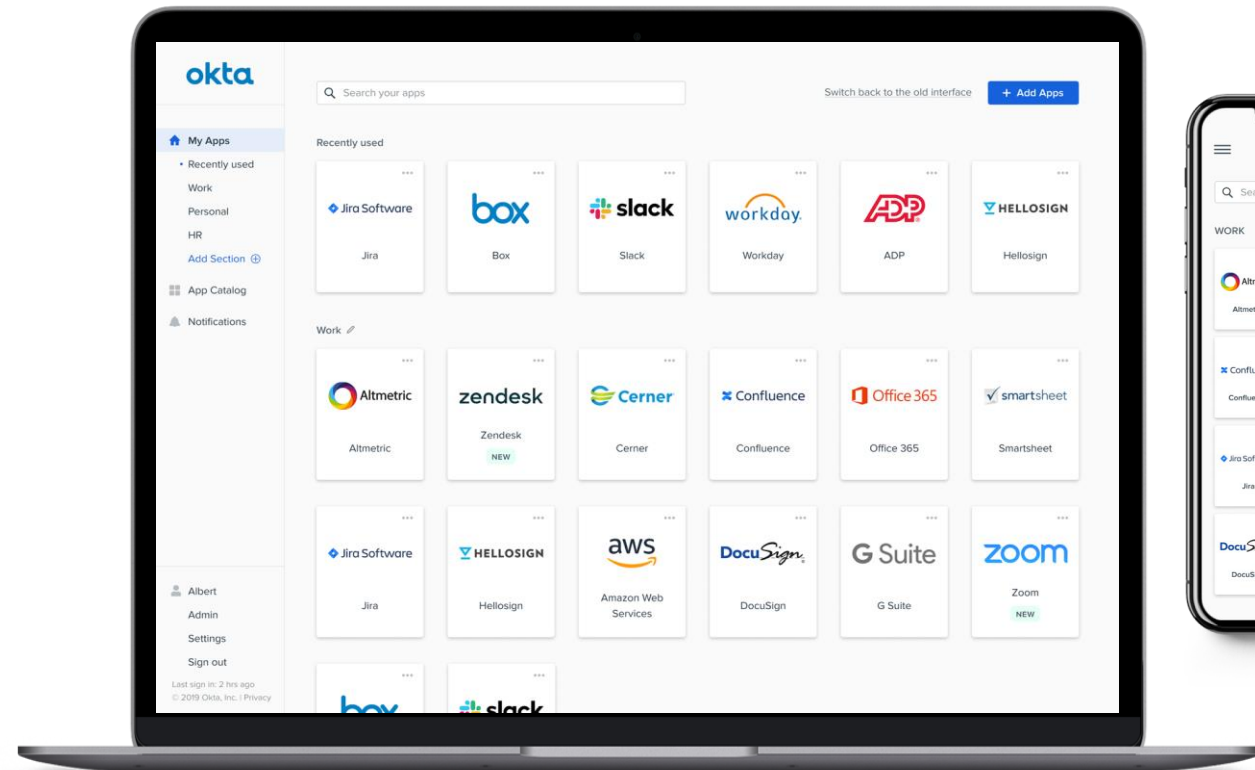
아이디/암호 관리 최소화로
보안 향상 및 사용자 편의성 증진



6500개 이상 연동 템플릿으로
신속한 SaaS 앱 사내 도입



세련된 관리자 콘솔, 중앙화된 정책
설정, 실시간 리포트로 사용자 접근
관련 가시성 및 통제 향상





Access Gateway

온 프레미스 앱을 최소한의 변경으로 Okta에 연결

Product Highlights



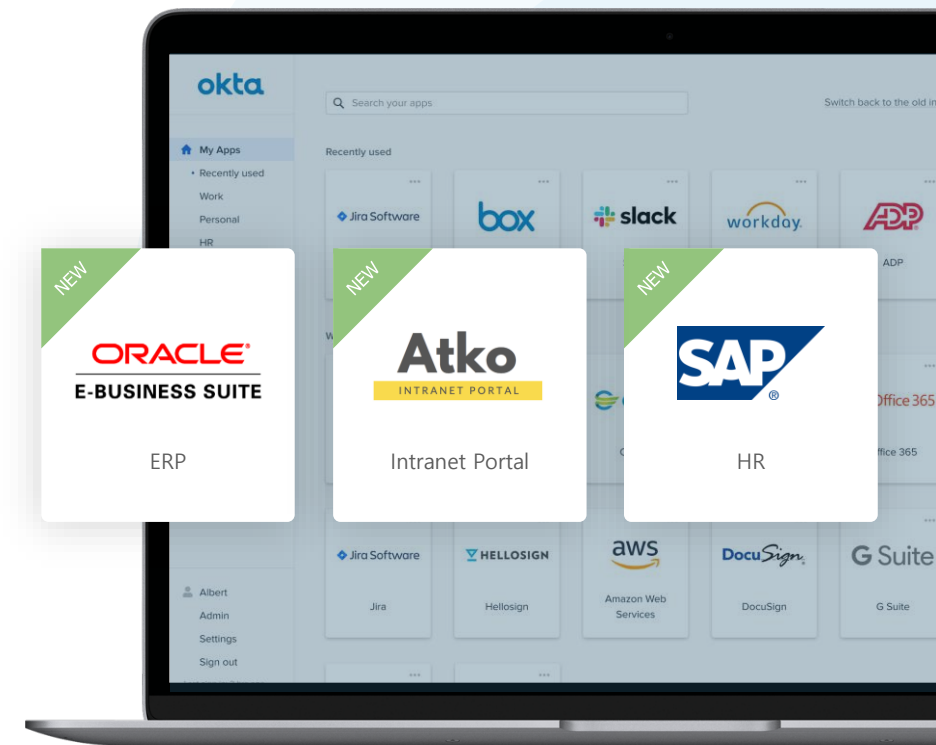
Okta의 SSO와 적응형 MFA를 온 프레미스 앱에 코드 변경 없이 적용



현대적 사용자 경험과 클라우드 모델을 통한 보안 강화



레거시 아이덴티티 제품의 구축 및 운영 비용, 복잡한 관리, 벤더 리스크에서 해방





API Access Management

보안 정책을 API로 확장

Product Highlights



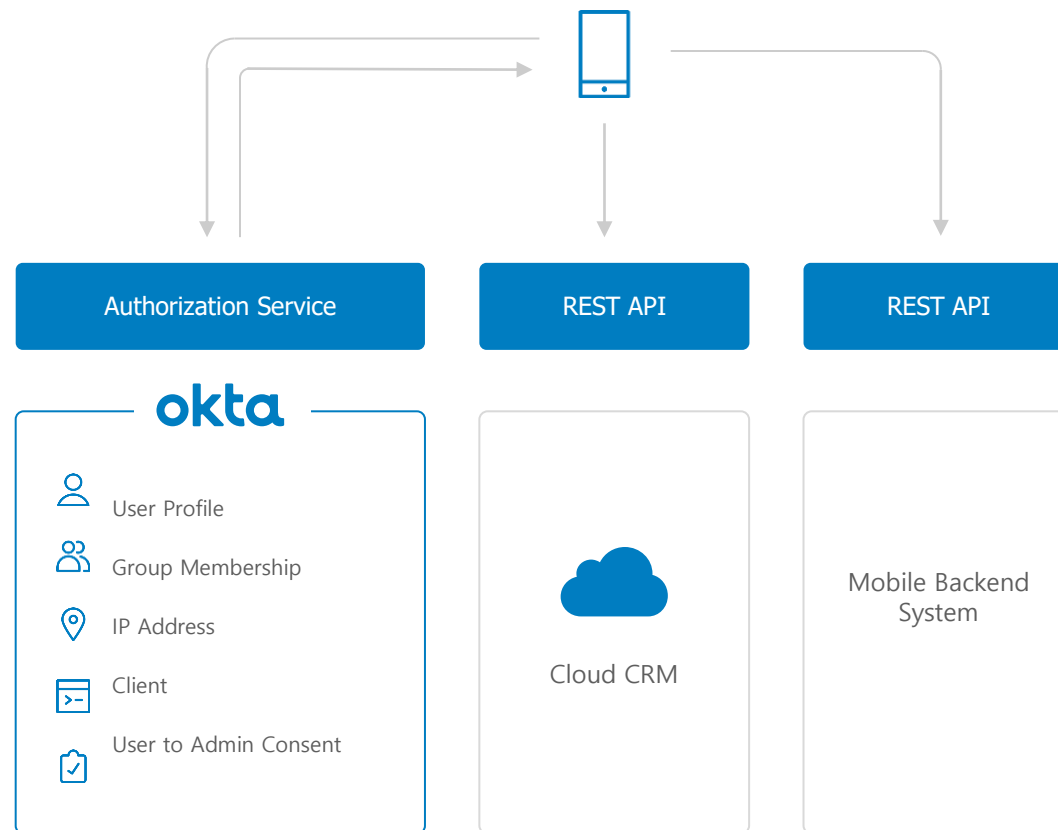
수 분 내에 기존 API 게이트웨이와 연동



OAuth 2.0 프로토콜: 다양한 개발툴, SDK, 교육자료, 우수사례로 안전하고도 빠른 개발



개발자 도구 자유도에 대한 침해 없이
권한 정책 중앙화로 보안 및 컴플라이언스
요구사항 충족





Advanced Server Access

제로 트러스트 기반의 접근 관리를 클라우드 인프라로 확장

Product Highlights



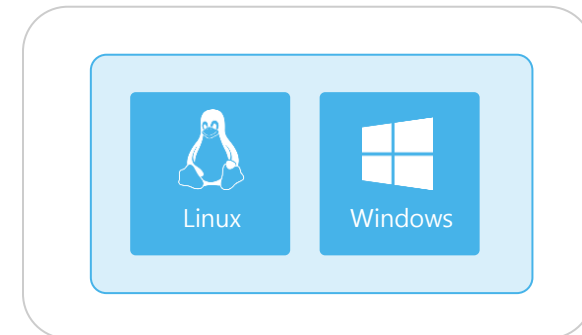
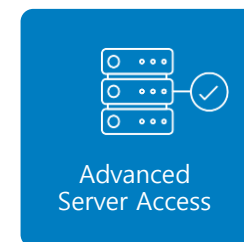
Linux와 Windows 서버에 대해
패스워드 없이 실시간 인증 구현



서버 사용자와 그룹 계정에 대한
End-to-End 라이프사이클 자동화

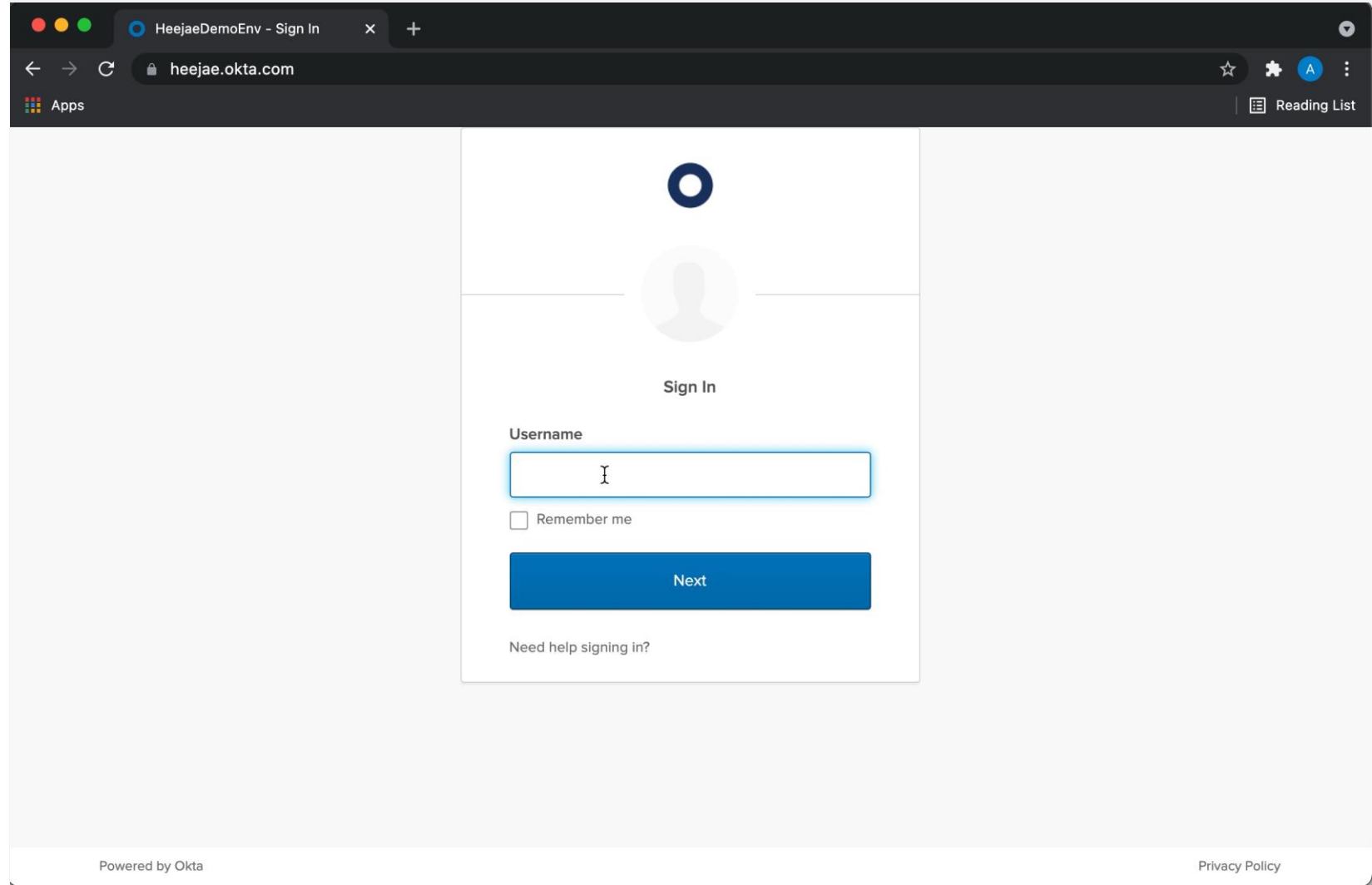


세부적인 Role 기반의 접근 관리와
커맨드 수준의 권한 관리



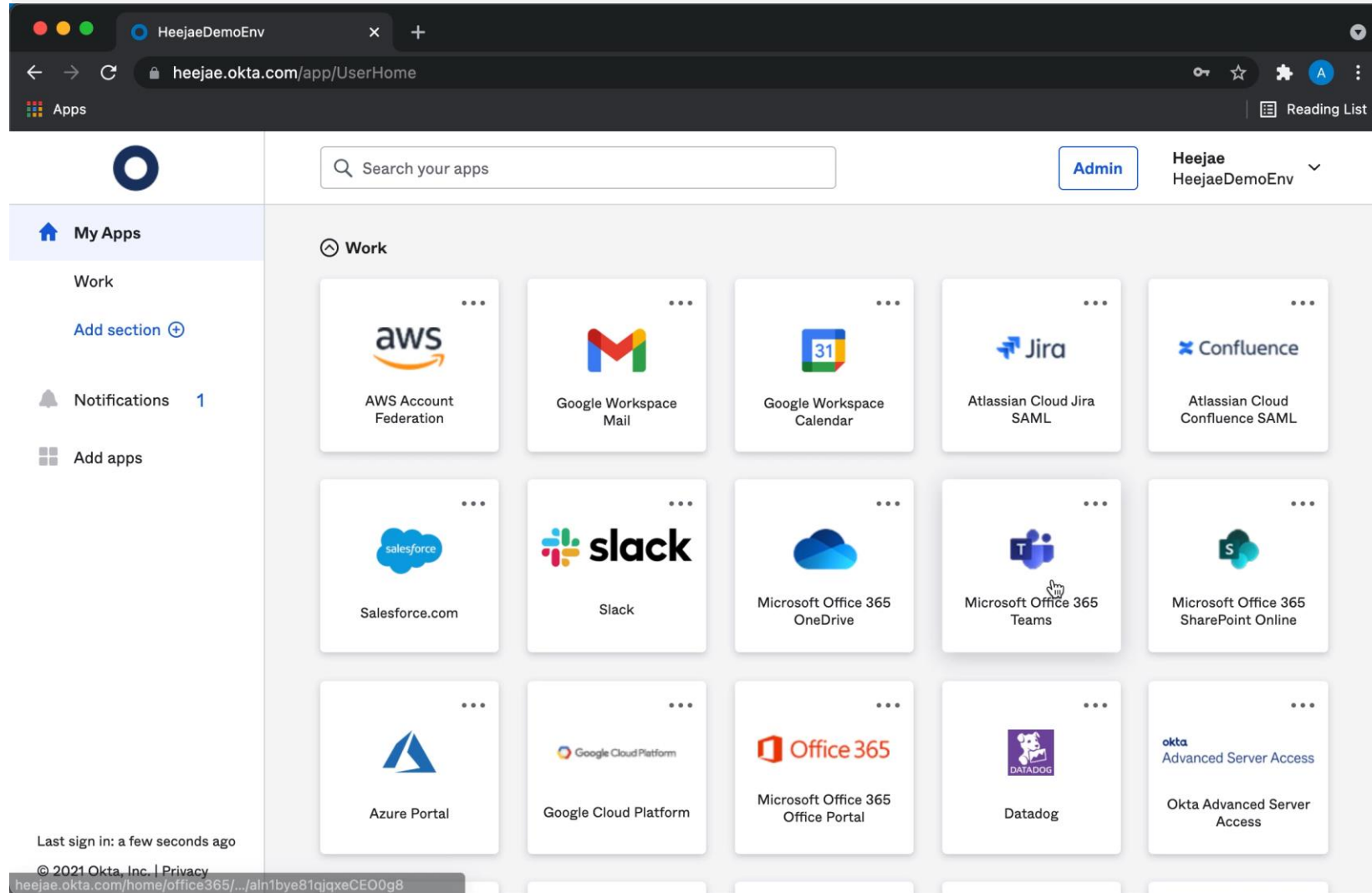
한 번의 인증으로 모든 앱에

Okta의 Single Sign On 기능을
통해 한 번의 인증으로 자신에게
할당된 모든 앱을 확인하고
편리하고 안전하게 액세스할 수
있습니다.



앱 추가, 15분이면 충분합니다

Okta Integration Network에
등록된 7,000개 이상의 사전
정의된 템플릿을 이용하면
SAML/OIDC에 대한 전문 지식이
없이도 앱을 빠르게 연동하고
배포할 수 있습니다



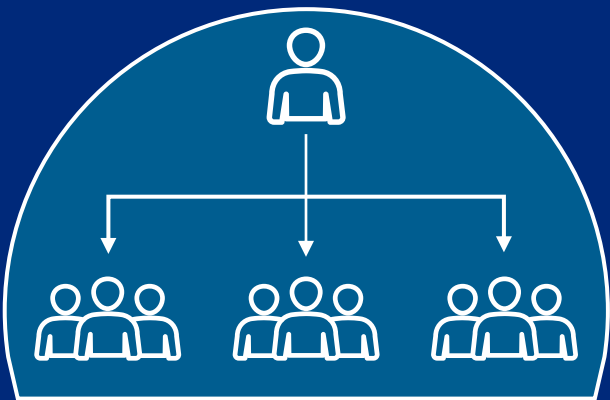
Okta Integration Network

SSO and Provisioning	Directories and HR-as-a-Master	Workflows	MFA-for-VPN	3rd Party MFA Factors	Endpoint Security and Management
 Office 365  slack  salesforce  box  G Suite  zoom  aws  ATLASSIAN	 Microsoft Active Directory LDAP  workday.  UltiPro™  Namely™  bambooHR™  SAP SuccessFactors	 Office 365  slack  salesforce  box  G Suite  zoom  aws  ATLASSIAN	 paloalto NETWORKS  CISCO  FORTINET  Pulse Secure	 DUO  Google Authenticator  HYPR	 vmware®  MobileIron  Carbon Black.  TANIUM
7,000+ OUT-OF-THE-BOX INTEGRATIONS					

API Gateways	Security Analytics	Email Security	Application Delivery Controllers	Cloud Access Security Brokers	Identity Proofing
 apigee Google Cloud Platform  MuleSoft™  Kong  aws  software AG	 splunk >  sumologic  LogRhythm™  RAPID7  IBM  exabeam  Radar	 proofpoint.	 f5  citrix NetScaler  Akamai	 McAfee™  netskope  CISCO Cisco Cloudlock	 experian.  acuant
ADVANCED INTEGRATIONS VIA APIS					

유저 관리 자동화

IT 팀



통합, 중앙 관리 및 통제
(디렉토리, HR 시스템, 클라우드 앱)



Universal
Directory

okta

일반 사용자



파견 / 계약직
비즈니스 파트너

직원
시스템 어드민

리소스 자동 할당
(앱, 서버, 파일, 폴더)



Lifecycle
Mgmt.



Universal Directory

모든 사용자, 그룹, 장비를 한 곳에서 관리

Product Highlights



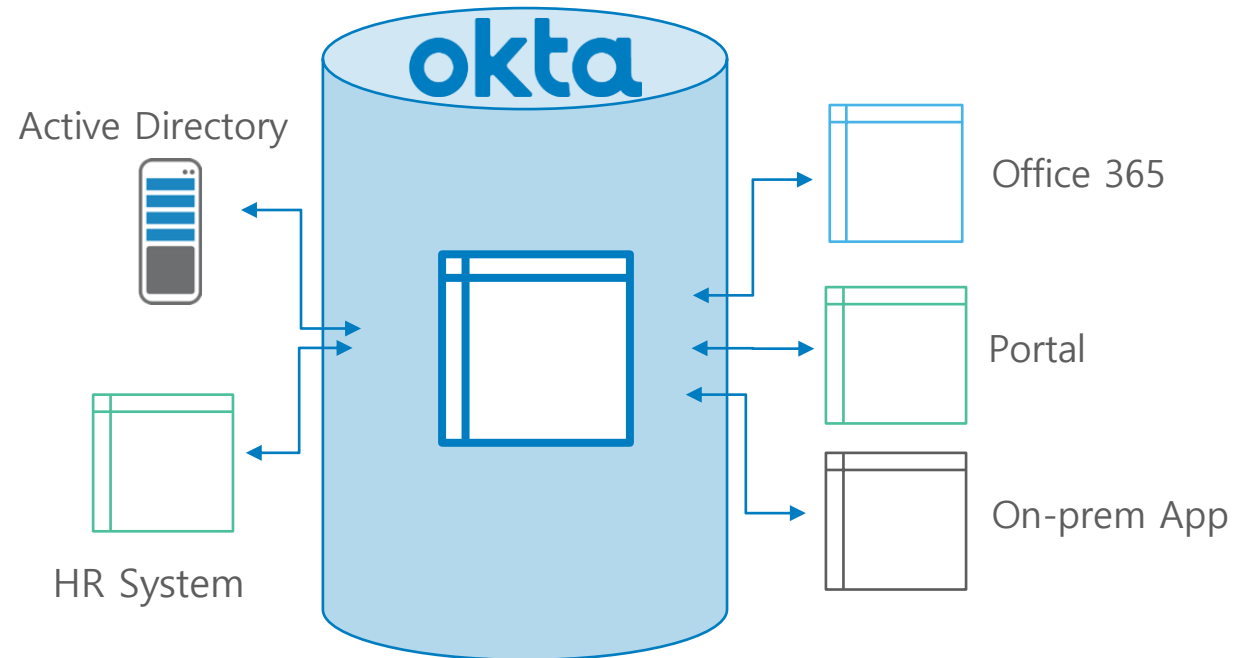
사용자 정보가 사내 모든 디렉터리와 어플리케이션에서 동일하도록 보장



AD/LDAP 관리에 따른 IT 비용 절감 및 AD 의존도 최소화로 IT 인프라 현대화



패스워드/MFA 사용자 셀프서비스로 IT 서비스데스크 티켓 감소





Lifecycle Management

모든 사용자의 전입/이동/전출 등 라이프사이클 상태 관리

Product Highlights



전입/전출 프로세스 자동화로 생산성 향상



사용자 상태에 따라 적절한 권한을 적절한 시점에 부여 혹은 제거하여 보안 강화



접근 통제의 중앙화를 통한 감사 대비

HR System



- ✓ Automated
- ✓ Streamlined
- ✓ Synchronized



Active Directory



Productivity suite



Video/chat app



Email app



CRM app



ITSM app



사용자 정보 통합 관리

사용자에게 어떤 앱이 할당되어 있는지, 어떤 그룹에 속해 있는지, 그리고 사용자 프로파일에 어떠한 정보들이 저장되어 있는지 한 곳에서 파악하고 관리할 수 있습니다

The screenshot displays the Okta Admin Dashboard for the organization 'HeejaeDemoEnv'. The dashboard provides a comprehensive overview of user management, including the number of users, groups, and SSO applications, along with their status and pending tasks.

Overview

Metric	Value	Change	Period
Users	21	↑ 11%	last 7 days
Groups	33	↑ 6%	last 7 days
SSO Apps	44		

Updated at 6 Jun, 23:55

Status

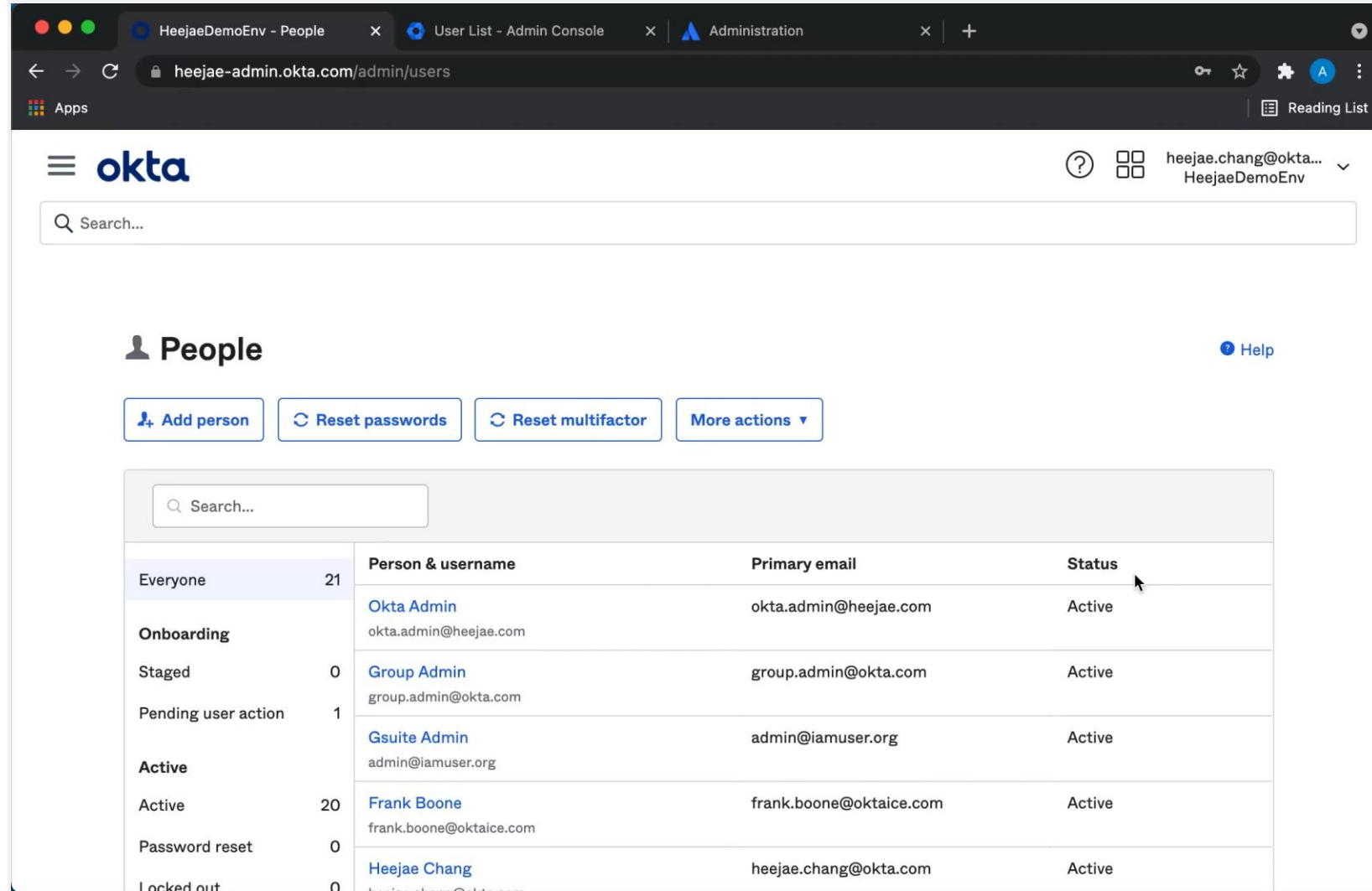
Service	Status
Okta service	Operational
Agents	Operational

Tasks

Type	Items	Description
To-do	257	Application accounts need deprovisioning
Info	15	Applications can be updated to use provisioning
Info	3	Applications can be updated to use SAML

Okta에서 앱 사용자 라이프사이클 통합 관리

SCIM 표준 API를 통해 연동된
앱의 사용자 생성, 사용자 정보
수정, 사용자 비활성화를
Okta에서 자동화하여 IT 운영
부담을 최소화하세요



The screenshot shows the Okta Admin Console interface. The top navigation bar includes the Okta logo, a search bar, and the user profile 'heejae.chang@okta... HeejaeDemoEnv'. The main content area is titled 'People' and features a search bar and several action buttons: 'Add person', 'Reset passwords', 'Reset multifactor', and 'More actions'. Below these buttons is a table listing users. The table has columns for 'Person & username', 'Primary email', and 'Status'. The 'Status' column is highlighted by a mouse cursor. The table lists several users, including 'Okta Admin', 'Group Admin', 'Gsuite Admin', 'Frank Boone', and 'Heejae Chang'.

Person & username	Primary email	Status
Okta Admin okta.admin@heejae.com	okta.admin@heejae.com	Active
Group Admin group.admin@okta.com	group.admin@okta.com	Active
Gsuite Admin admin@iamuser.org	admin@iamuser.org	Active
Frank Boone frank.boone@oktaice.com	frank.boone@oktaice.com	Active
Heejae Chang heejae.chang@okta.com	heejae.chang@okta.com	Active

리스크 수준에 따른 접근 관리

적절한 시점에 적절한 사람에게 적절한 자원에 대한 접근만을 허가





Adaptive Multi-Factor Authentication

회사의 중요 리소스에 대한 접근 시 Context 적용하여 보안 강화

Product Highlights



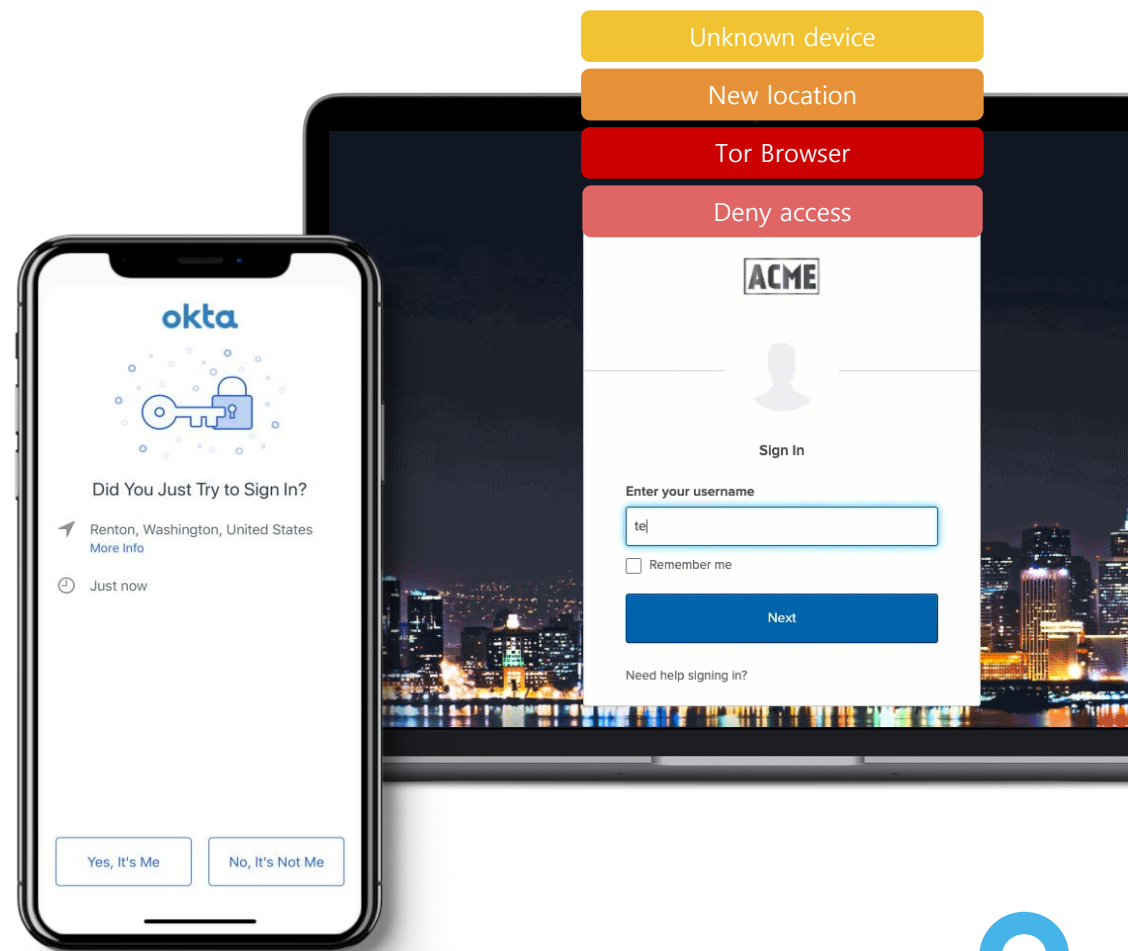
관리자, 보안팀, 개발자 모두에게
용이한 MFA 도입 및 관리



사용자 경험 중심의 MFA 등록 및
인증 프로세스 설계

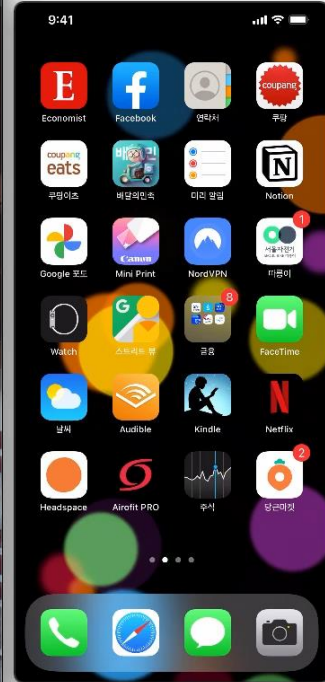
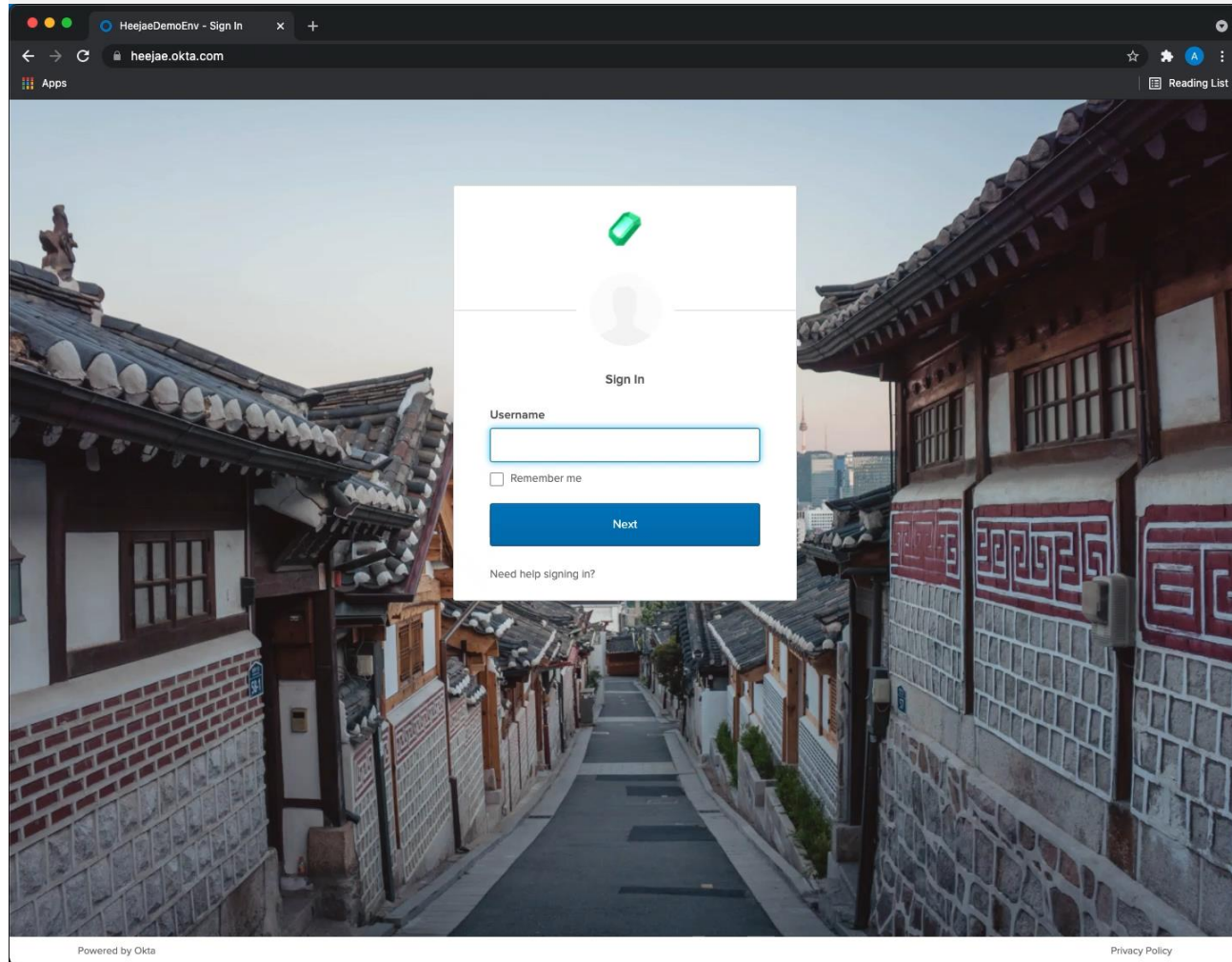


Context 기반의 지능형 접근 제어



Passwordless 인증

FIDO2 기반 생체인식과 Okta
Verify 등 Okta가 지원하는
다양한 MFA를 조합하여
Passwordless 인증을 경험하세요



유연하고 강력한 정책설정

Okta 전체 인증, Password 설정,
앱 각각의 인증에 대해 그룹
기반의 정책 설정과 컨텍스트
기반의 룰 설정으로 쉽고 빠르게
강력하고 유연한 보안 정책을
설정할 수 있습니다

The screenshot shows the Okta Admin Console interface. The left sidebar contains a navigation menu with categories like Dashboard, Directory, Applications, Security, Workflow, Reports, and Settings. The 'Authentication' section is expanded, showing a list of policies: 1. Allow access only inside the office, 2. Factor Sequencing outside of the company, 3. Demo Passwordless, and 4. Default Policy. The main content area displays the configuration for the selected policy, 'Allow access only inside the office'. It includes a description, assigned groups (DevOps Admins), and a table of rules.

Priority	Rule Name	Access	Status	Actions
1	No access outside of the company	Denied	Active	Info Edit Delete
2	Okta verify only inside the office	Allowed	Active	Info Edit Delete



The Industry's Most Reliable and Secure Platform, Period.

Single
Sign-On



Universal
Directory



Lifecycle
Management



API Access
Management



Adaptive
Multi-Factor
Authentication



Developer
SDKs



okta

베스핀글로벌 / Premier Partner

문의 / zerotrust@bespinglobal.com

BESPIN GLOBAL
HELPING YOU ADOPT CLOUD.