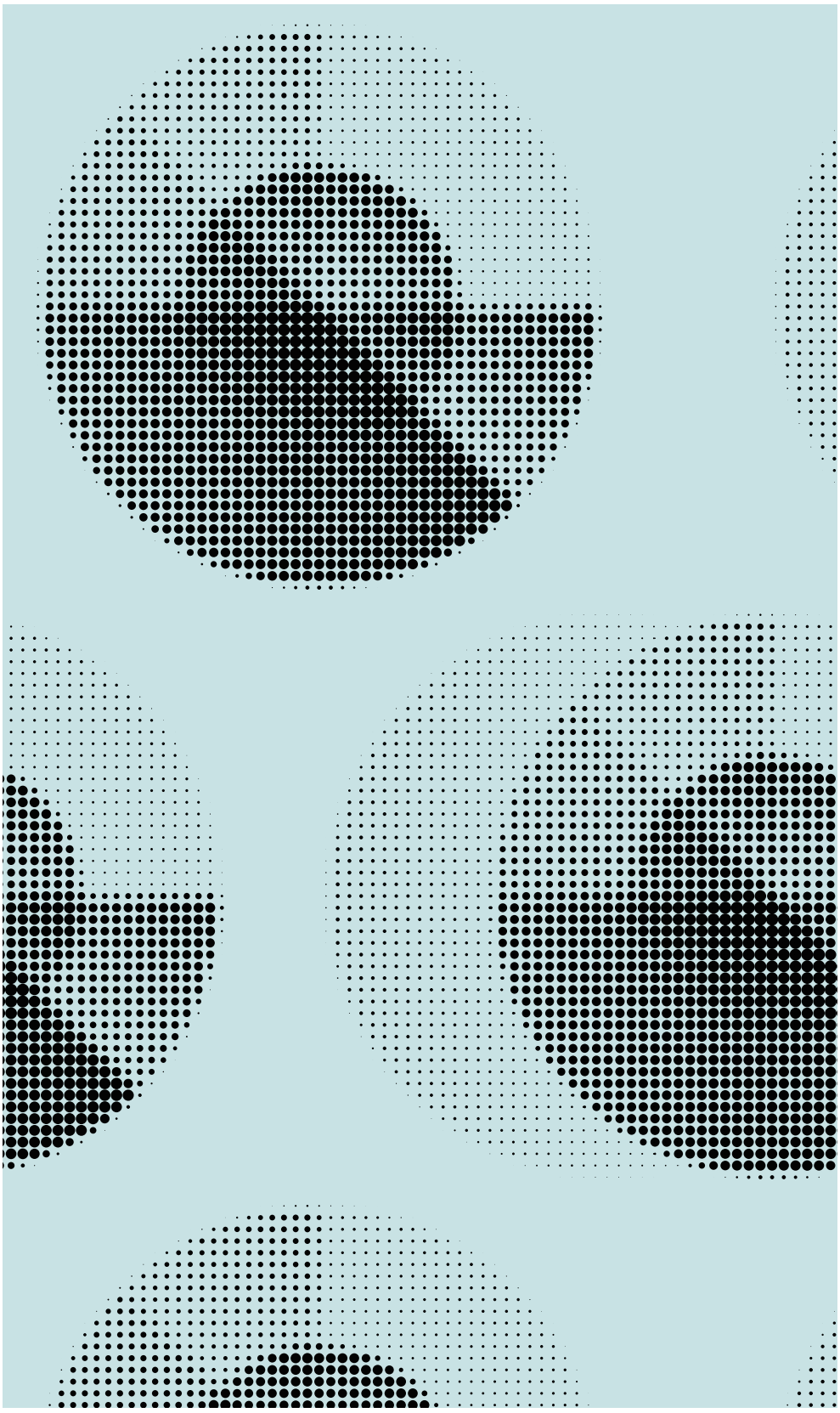
2020년 11월
백서

비밀번호의 한계를 넘다

Okta Inc.
서울 강남구 테헤란로 152
강남파이낸스센터 41층
support.okta.com
050-6626-1877



okta

목차

서론

사용자 이름과 비밀번호를 사용하는 기존의 인증 방식은 50여 년 전부터 디지털 아이덴티티와 보안을 뒷받침하는 초석이었습니다. 하지만 사용자 계정이 끊임없이 늘어나면서 새로운 문제들이 속속들이 발생하고 있는데, 가령 엔드 유저가 여러 개의 비밀번호를 기억해야 한다는 부담을 안게 되었으며 비용을 충당해야 하고, 무엇보다 취약한 자격 증명으로 인해 보안 위험이 증가했습니다. 이러한 문제들은 이제 비밀번호의 유용성까지 위협하고 있습니다. 결과적으로 인증 경험에서 비밀번호를 없애야 한다는 주장이 나날이 설득력을 얻고 있습니다.

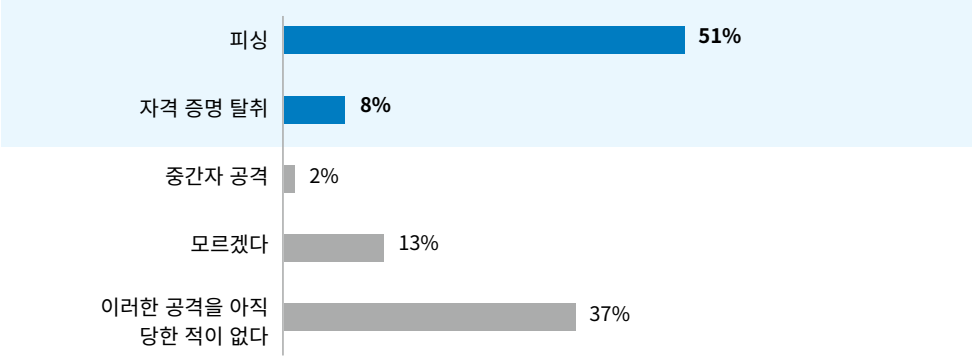
새로운 패스워드리스 보안 표준의 등장과 함께 소비자 또는 이와 유사한 경험에 대한 기대치 상승, 그리고 급증하는 비용으로 인해 이론에 머물렀던 비밀번호 제거가 현실이 되었습니다. 본 백서에서는 고객과 직원의 인증을 위한 비밀번호 제거 사례를 살펴보고, 기업이 패스워드리스 인증을 구현하기 위한 여정에서 시행할 수 있는 단계적 조치를 알아보겠습니다.

비밀번호의 한계를 넘어서기 위한 노력

패스워드리스 인증의 필요성을 이해하는 것은 비밀번호에 따른 문제점을 인식하는 데서 출발합니다. 비밀번호와 관련된 주요 문제점은 다음과 같이 분류할 수 있습니다.

취약한 계정 보안

비밀번호는 보안/아이덴티티 기반 공격을 초래했습니다. 예를 들어 자격 증명 침해, 피싱, 비밀번호 살포 공격, 부실한 비밀번호 관리 등으로 인해 비밀번호가 취약해지면 계정 탈취(ATO) 공격이 발생할 수 있기 때문입니다. 기업은 먼저 다중 요소 인증(MFA)과 같은 별도의 인증 계층을 활용하여 이러한 공격에 대비할 수 있습니다.



응답자의 59%가 자격 증명 탈취 또는 피싱을 경험했다고 밝혔습니다.
Ponemon Authentication Report 2019

그렇다고 MFA가 완벽한 솔루션이라는 것은 아닙니다. 이 테크놀로지의 문제점은 SMS와 같은 2차 요소가 널리 사용되고 있지만 인증이 보장되지 않는 취약점으로 인해 해커들의 표적이 된다는 것입니다.

> 해킹 관련 보안 사고 중 81%가 취약하거나 탈취된 비밀번호 때문인 것으로 드러났습니다.
>
> Gus Shahin
> CIO, Flex

미흡한 사용자 경험

비밀번호는 계속해서 사용자에게 불편을 야기하고 있습니다. 비밀번호를 선택하는 모범 사례는 다양하지만 적어도 비밀번호는 고유하고 추측하기 어려우면서도 쉽게 기억할 수 있는 것이어야 합니다. 옥스포드(Oxford) 대학에서 실시한 설문조사에 따르면, 온라인 상품 구매자의 약 1/3이 비밀번호를 기억하지 못해 구매를 포기하는 것으로 나타났습니다.

비용 증가

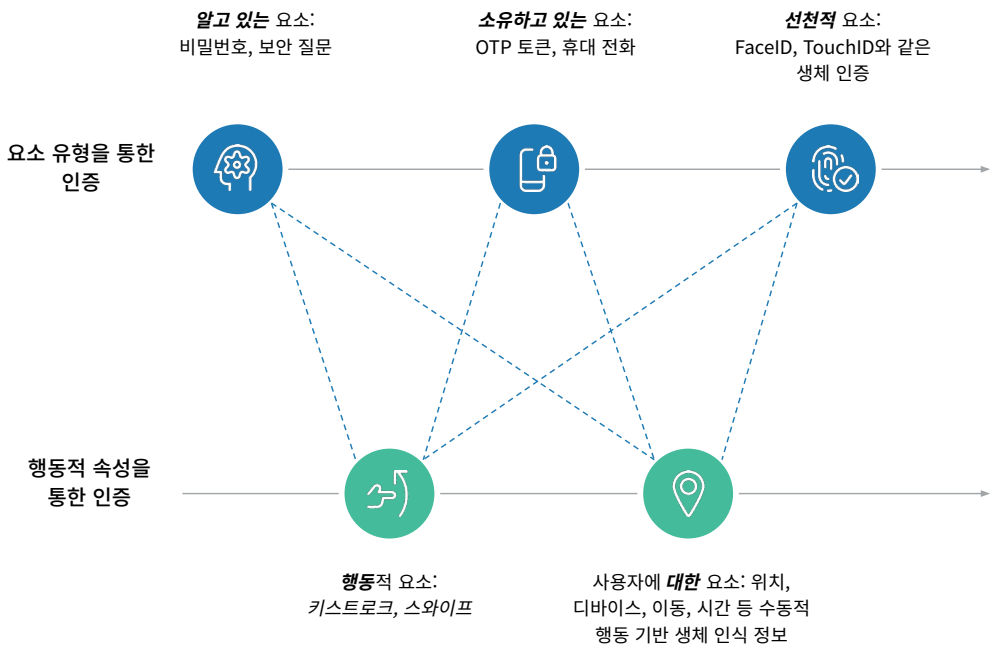
비밀번호를 사용하는 이점이 무색해질 정도로 비밀번호 관련 비용이 증가하고 있습니다. 비밀번호 관리는 사용자들이 콜센터에 전화하는 주된 이유 중 하나이기도 합니다. 비밀번호로 인한 지원 부담을 줄이는 것은 조직이 반드시 달성해야 할 과제입니다.

12.6	분/주 비밀번호를 입력하거나 리셋하는 데 소요되는 주당 평균 시간
$5,217,456	기업별 연간 평균 생산성/노동 손실 비용

출처: Ponemon Authentication Report 2019

현재의 인증 방식에 대한 평가

현재의 인증 방식은 지식, 소유, 생체 인증과 같은 요소를 사용합니다. 기업은 이러한 요소 중 한 가지 이상을 행동적 속성과 조합하여 액세스 결정을 내리는 경우가 많습니다. 이렇게 보안 계층을 추가하면 공격자가 사용자의 계정에 액세스할 수 있는 가능성이 줄어든다고 생각하기 때문입니다.



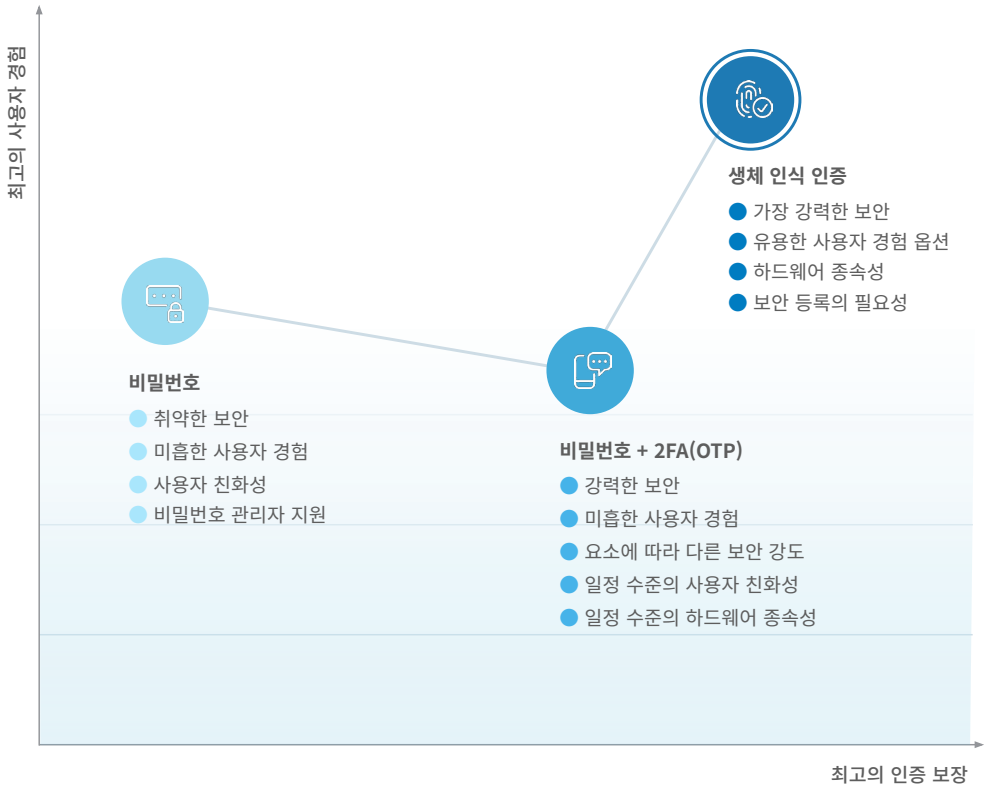
인증 방식을 평가할 때는 크게 두 가지 핵심 속성을 살펴봐야 합니다.

인증 보장/보안

권한이 있는 사용자만 계정에 액세스할 수 있는 인증 기법인가?

사용자 경험

- 등록과 인증 및 복구 절차가 원활한 인증 기법인가?
- 모든 사용자 그룹, 디바이스 유형, 소프트웨어 플랫폼을 대상으로 완전한 인증을 지원하는 인증요소인가?



패스워드리스 인증 시작하기

비밀번호의 한계를 넘어서기 위해서는 세심한 접근이 필요합니다. 비밀번호를 제거하려면 먼저 위협, 테크놀로지, 사용자 여정, 비용, 도입 문제, 구현 등의 측면을 살펴보면서 점진적으로 접근하는 것이 좋습니다.

위협

- 자격 증명 위반
- 중간자
- 브라우저 조작
- 비밀번호 살포
- 무차별 대입 공격

테크놀로지

- 브라우저 지원
- 테크놀로지 접근 방식
- 플랫폼 인증요소 vs 외부 인증요소

사용자 여정

- 등록 프로세스
- 인증 프로세스
- 복구 프로세스

비즈니스 고려 사항

- 지원
- 통합
- 디바이스 도입
- 규정 준수 요건

도입 문제

- 널리 사용되는 비밀번호
- 널리 사용되는 비밀번호 관리자
- 프로비저닝이 간편한 비밀번호

구현

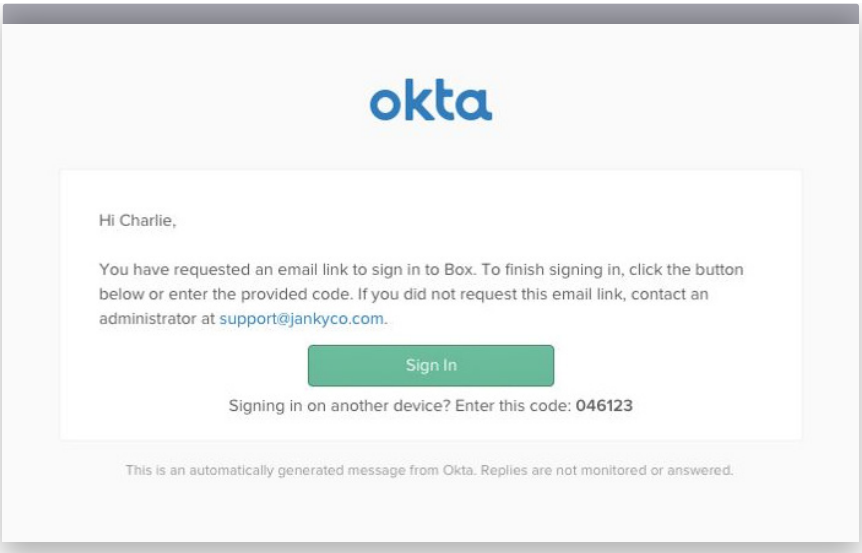
- 보안 및 규정 준수 요건
- 웹사이트 지원

패스워드리스 인증을 향한 일반 접근 방식

갖가지 테크놀로지를 사용하면 비밀번호를 제거하여 패스워드리스 인증으로 전환할 수 있습니다. 이메일 매직 링크와 같은 접근 방식에서는 보안 이메일 본문에 인코딩된 OTP 토큰이나 라이브 링크를 남기는 반면, WebAuthn과 같은 접근 방식에서는 공개/비공개 키 기반 암호화를 이용해 보안 인증을 보장합니다.

Okta는 다양한 패스워드리스 인증 접근 방식을 제공합니다. 이번 섹션에서는 주요 패스워드리스 인증 접근 방식을 몇 가지 살펴보겠습니다.

이메일 매직 링크



이메일 기반 패스워드리스 인증은 보편화된 방식입니다. 이 방식의 핵심은 비밀번호 리셋 프로세스에 있습니다. 보안 링크가 사용자에게 전송되면 사용자는 이 링크를 통해 비밀번호를 우회하여 새로운 비밀번호를 설정할 수 있습니다. 이는 대부분의 사용자가 수십 번 내지 수백 번에 걸쳐 이용해봤을 정도로 친숙한 방식입니다. 이 인증 방식은 Slack이나 Medium과 같은 앱에서 사용되면서 인기를 끌었습니다. 진정한 패스워드리스 인증 방식은 비밀번호 리셋 프로세스를 개선합니다. 앱 설계자가 비밀번호를 비롯한 관련 리셋 과정을 제거하고 한시적이거나, 또는 사용자 라이프사이클로 제한된 일회성 보안 링크를 사용자의 이메일 주소로 전송합니다. 사용자가 이 링크를 클릭하면 인증이 이루어지며, 로그인 상태를 오랫동안 유지할 수 있는 쿠키가 설정됩니다. 따라서 사용자가 비밀번호를 설정하거나, 저장하거나, 입력할 필요가 전혀 없기 때문에 모바일 디바이스에 특히 적합한 기능입니다. 이러한 패스워드리스 인증 방식은 하드웨어 종속성을 요하지 않기 때문에 소비자 애플리케이션에 매우 유용합니다.

사용 사례

- 로그인 횟수가 많지 않은 패턴
- WebAuthn을 대체할 수 있는 패스워드리스 인증 방식
- 비밀번호 기반 공격 저지

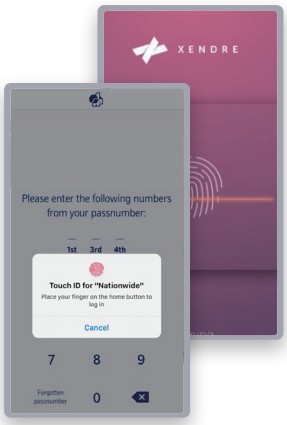
이점

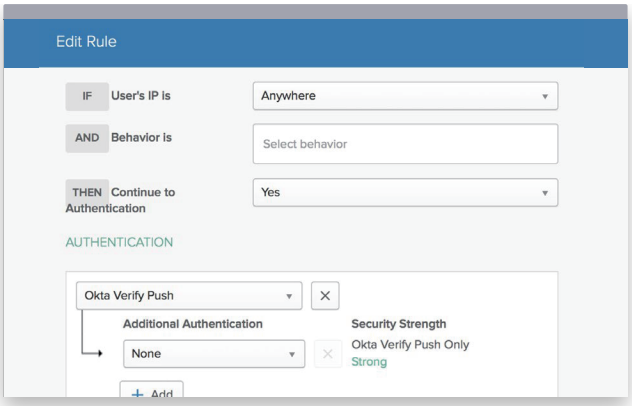
- 손쉬운 배포 및 사용
- 원활한 온보딩
- 하드웨어 종속성 없음
- 익숙하여 쉽게 받아들일 수 있는 사용자 경험
- 데스크톱과 모바일에서 일관된 경험 제공

해결 과제

- 이메일 계정을 안전하게 보호할 수 있는 보안 위임
- 링크(이메일) 공유를 제어하거나 확인할 수 있는 수단 부재
- 이메일이 암호화되지 않을 경우 중간자 공격에 취약함

인증요소 시퀀싱





Okta Adaptive MFA의 컨텍스트 기반 인식 기능과 ThreatInsight의 인텔리전스 기능을 결합하면 다양한 인증요소를 이용해 패스워드리스 솔루션을 안전하게 구성할 수 있습니다. 위협 수준이 낮을 때는 로그인 경험이 간소화되어 사용자가 필요한 데이터와 앱에 더욱 쉽게 액세스할 수 있습니다. 하지만 로그인에 따른 위협 수준이 높을 때는 별도의 인증요소가 필요합니다. 예를 들어 관리자가 Okta Verify 모바일 앱을 기본 인증요소로 설정할 수 있습니다. 이때 사용자가 알려진 장소와 디바이스에서 로그인하면 Okta에서 사용자가 액세스 권한을 얻기 위해 동의한 앱을 통해 인증 요청을 전송합니다.

하지만 Adaptive MFA가 비정상적인 위협을 감지하여 로그인 요청에 따른 위험 수준이 증가하게 되면 Okta에서 WebAuthn 같은 2차 인증요소를 사용하라는 메시지를 사용자에게 표시할 수 있습니다.

관리자는 인증 방식과 요소를 선택하기에 앞서 인증을 보장하는 수준이 각각 다르다는 점을 고려해야 합니다. 또한 사용자 컨텍스트를 가이드로 삼아서 가급적이면 로그인을 간소화하고 사용 편의성을 높여야 합니다. 보안 질문과 같은 지식적 요소는 사용이 간편하지만 U2F와 같은 소유적 요소에 비해 보안 강도가 떨어집니다. 이러한 점을 고려한다면 사용자가 회사 네트워크를 통해 사무실에서 로그인할 때는 소유적 요소를 선택하여 인증을 간소화하고, 디바이스, 네트워크 또는 장소에 따라 위험 수준이 증가하는 경우에 대비해 더욱 강력한 보안 요소를 갖추는 것이 효과적입니다.

관리자들 역시 회사의 가용 테크놀로지를 고려하여 적합한 요소를 선택해야 합니다. 예를 들어 스마트폰을 이용하지 않는 직원들이 있다면 Okta Verify가 제대로 작동하지 않으므로, 이때에는 SMS OTP 같은 다른 요소를 사용하는 것이 좋을 수도 있습니다.

사용 사례

- 세션 위험에 따른 로그인 경험 변경
- 더욱 엄격한 인증 보장 요소 페어링을 통한 인증 경험 제공

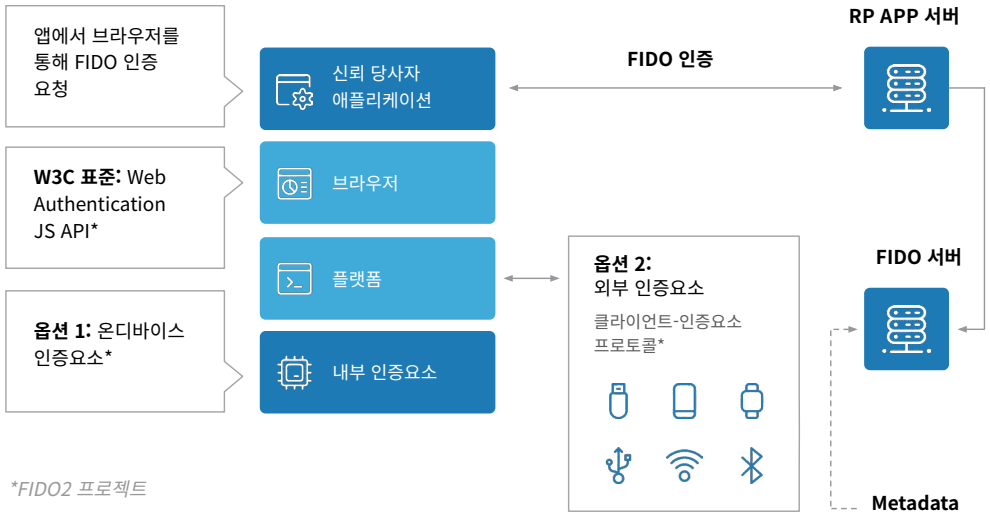
이점

- 엄격한 인증을 보장하는 로그인
- 데스크톱과 모바일에서 일관된 경험 제공

해결 과제

- 잠재적 하드웨어 종속성

Webauthn



WebAuthn은 표준 기반의 패스워드리스 인증 프레임워크입니다. 이 프레임워크에서는 웹 애플리케이션이 등록 디바이스(휴대전화, 노트북 등)를 인증요소로 사용하여 사용자 인증을 간소화하는 동시에 안전하게 보호할 수 있습니다. 이러한 새로운 표준이 등장함에 따라 WebAuthn을 지원하는 브라우저 기반의 웹 애플리케이션에서 이러한 디바이스 인증요소를 사용하여 사용자를 안전하게 인증할 수 있습니다. Google Chrome, Mozilla Firefox, Microsoft Edge, Apple Safari, Opera 등 플랫폼에 빠르게 도입되고 있다는 점(Windows Hello를 지원하는 MSFT Edge, Google Android 등)은 FIDO2/WebAuthn을 실제로 배포할 방법이 있다는 것을 의미합니다. 디바이스 자체가 WebAuthn에 사용되기 때문에 이제 기업은 YubiKey 같은 로밍 인증요소를 사용하거나, 지원되는 플랫폼을 통해 배포할 수 있습니다.

사용 사례

- 표준 기반 패스워드리스 인증
- 확장 가능한 인증 경험

이점

- 계정 탈취: 피싱, 자격 증명 스터핑, 비밀번호 살포 공격 등 아이덴티티 기반 공격 저지
- 자격 증명 관리 불필요
- 사용자 인증 경험 개선
- 비밀번호 관리를 위한 조직의 지원 감소

해결 과제

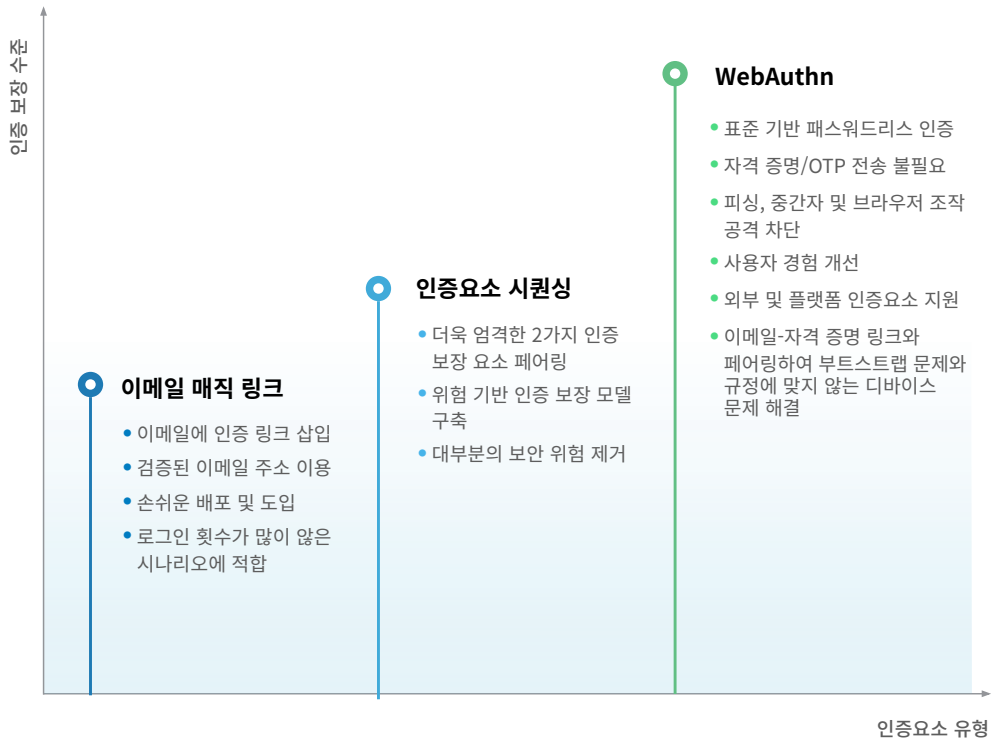
- 하드웨어 및 브라우저 지원 필요
- 안전한 사용자 부트스트랩 및 복구 프로세스 필요
- 이메일-자격 증명 링크 등 대체할 수 있는 다른 패스워드리스 인증 방식과의 페어링 필요

자세한 내용은 Webauthn 백서를 참조하세요.

패스워드리스 인증을 위한 미래 설계

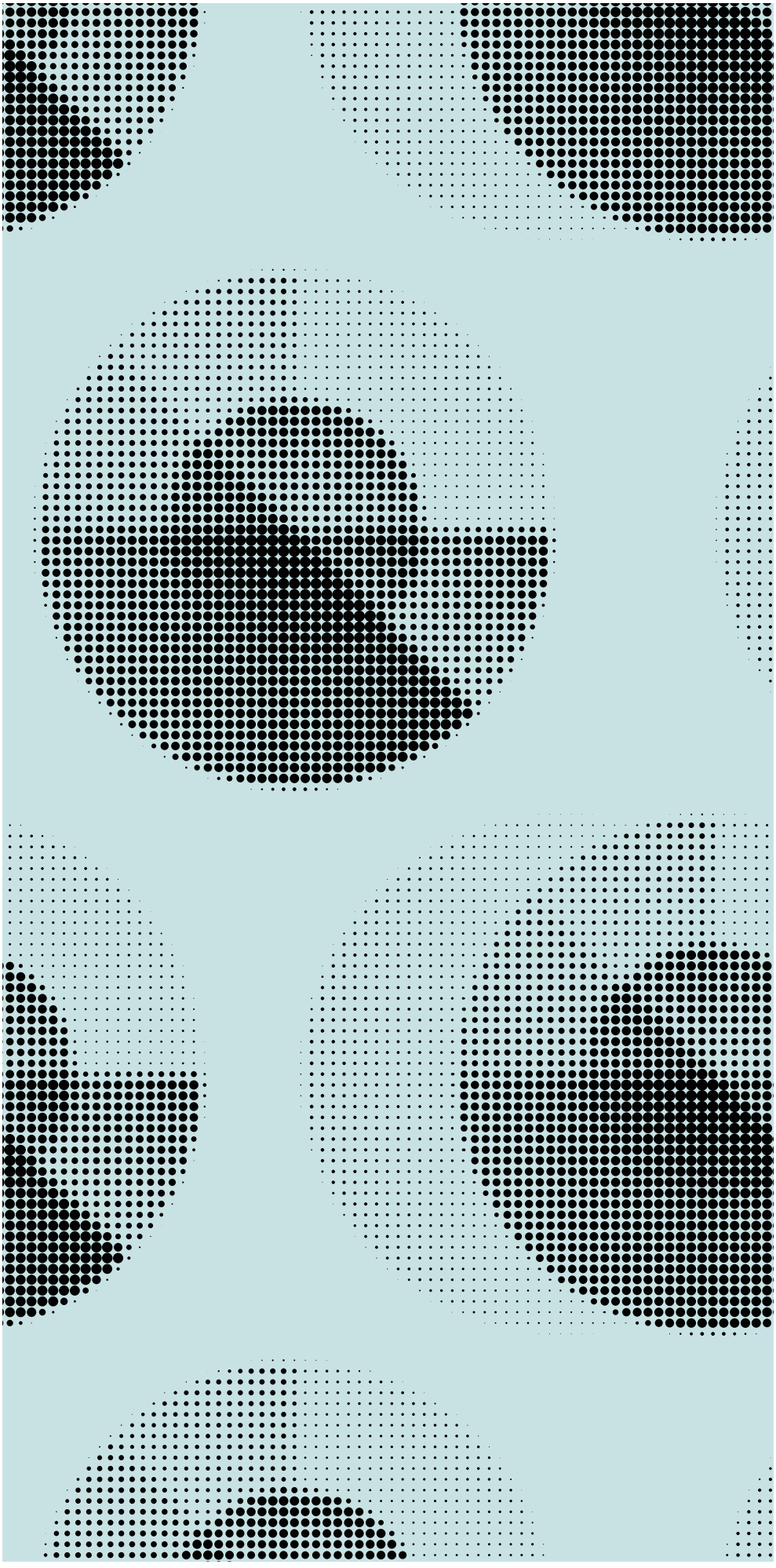
패스워드리스 인증 도입은 기업이 서비스를 통해 다양한 보안 위험을 관리하여 원활한 고객 경험을 선사하는 데 가장 효과적인 방법 중 하나입니다. 오늘날 기업들도 패스워드리스 인증을 점차 도입하는 추세입니다. 패스워드리스 인증은 혁명적인 프로세스라기 보다는 진화하는 프로세스에 가깝습니다. 따라서 이러한 여정을 시작하는 기업들을 위해 Okta가 몇 가지 간단한 옵션과 함께 진정한 패스워드리스 인증으로 나아가는 데 필요한 로드맵을 알려드리겠습니다. 패스워드리스 인증으로 전환하려면 세심한 사고와 계획이 필요합니다. 즉, 보안 등록에서부터 비밀번호 마이그레이션, 배포 가능성, 복구, 오프보딩 등 전체 인증 라이프사이클을 고려해야 합니다. 제반 사항과 요건을 모두 파악해야만 유리한 위치에서 패스워드리스 인증 여정을 완성하여 아이덴티티 공격을 차단하고, 만족할 만한 고객 경험을 선사하며, 비즈니스의 성장을 도모할 수 있습니다.

Okta와 함께 하는 패스워드리스 인증 여정



Okta 소개

Okta는 기업 아이덴티티 분야에서 독자적인 선두 기업입니다. Okta Identity Cloud는 기업들이 사람과 테크놀로지를 적시에 안전하게 연결할 수 있도록 지원합니다. 6,500개 이상의 애플리케이션 및 인프라 공급업체가 사전에 통합되어 있어 Okta 고객들은 자신의 비즈니스에 가장 적합한 테크놀로지를 손쉽고 안전하게 사용할 수 있습니다. 또한 20th Century Fox, JetBlue, Nordstrom, Slack, Teach for America, Twilio 등 8,950개 이상의 기업들이 Okta를 통해 자사 인력과 고객의 아이덴티티를 보호하고 있습니다. 자세한 내용은 okta.com에서 확인할 수 있습니다.



okta