cpl.thalesgroup.com

THALES

패스워드리스 인증:
비밀번호 포기가 더 안전한 보호일 수도 있는 이유

백서

비밀번호는 왜 나쁜가

비밀번호는 소프트웨어와 인터넷 세계에서 가장 오래된 보안 도구 중 하나입니다. 그러나 오늘날의 환경에서 비밀번호는 여러 가지 이유로 비즈니스를 충분히 보호할 수 없습니다.

비밀번호 피로는 열악한 보안으로 이어집니다

정책 기반의 비밀번호 강도 및 회전 교체는 비밀번호 피로를 유발하여 비밀번호 관리를 열악하게 만드는 데 일조합니다. Verizon의 데이터 유출 조사 보고서[1]에 따르면 **직원의 70% 이상이 회사 및 개인 계정에 비밀번호를 재사용한다고 합니다**. 따라서 나쁜 의도를 갖은 사람이 직원의 자격 증명을 남용하여 다른 애플리케이션 및 민감한 고객 정보에 액세스할 수 있습니다.

81%

약한 자격 증명 또는 도난 당한 자격 증명을 사용한 유출

~40

개인이 보유한 온라인 계정 수의 평균은 약 40개

4/5

다른 계정에서도 동일한 비밀번호를 재사용하는 사람

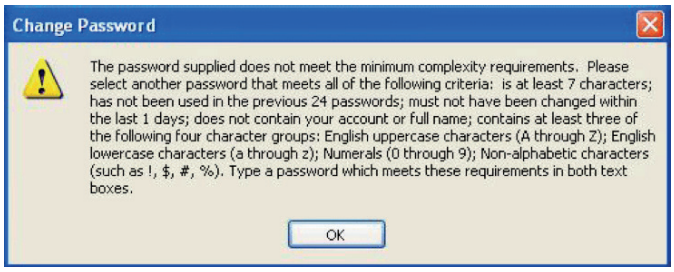
"123456"
"password"

2018년에도 여전히 가장 널리 사용된 비밀번호

사람들은 또한 비밀번호를 기억하는 데 어려움을 겪기 때문에 해킹하기 쉬운 비밀번호를 선택하는 경향이 있습니다. 5백만 개가 넘는 유출된 비밀번호를 분석한 결과, 10%의 사람들이 최악의 비밀번호 25개 중 하나를 사용하는 것으로 나타났습니다[2]. 기업 사용자의 7%는 극히 취약한 비밀번호를 가지고 있었습니다.

비밀번호는 사용자 경험을 악화시킵니다

카네기멜론 대학의 연구에 따르면 비밀번호 정책을 올바르게 작성하면 조직의 보안이 강화될 수 있습니다. 그러나 이 정책이 어떠해야 효과적일 것인지에 대해서는 일치하지 않습니다. 이 점을 잘 보여주는 사례가 있습니다. 보통 사용자들은 비밀번호에 동일한 숫자를 선택하여 넣거나 동일한 위치에 있는 숫자를 사용하여 넣으라는 정책 규칙에 좋지 않은 반응을 보입니다[3].



일부 비밀번호 정책은 그 비밀번호를 기억하거나 입력하기 어렵게 만듭니다. 이 때문에 사용자는 비밀번호를 적어두거나 다른 계정에서 재사용하거나 친구와 공유함으로써 비밀번호 보안이 약화되는 일이 발생합니다. 또한 비밀번호를 자주 잊어버리므로, 결국 고객센터의 업무가 늘어나게 됩니다.

비밀번호는 사용자 보안을 방해할 수 있습니다

아이러니하게도, 비밀번호는 공격 경로로 쓰이게 됨으로써 보안에 해를 끼칠 수 있습니다. Verizon의 2018년 데이터 유출 조사 보고서에 따르면 **해킹 관련 위반의 81%**는 비밀번호가 약하거나 도난당했거나 재사용되었기 때문이었습니다[4]. 중간자(MITM) 공격과 맨 인 더 브라우저(MITB) 공격과 같은 위협은 모방한 로그인 화면을 만들어 놓고 사용자가 여기에 비밀번호를 입력하도록 유인하는 방식을 사용합니다. 클라우드에서는 훨씬 더 위험합니다. 클라우드에서 호스팅되는 로그인 페이지가 완전히 노출되므로, 악당이 outlook.com과 같이 공개적으로 알려진 로그인 페이지를 대상으로 피싱 또는 무차별 대입 공격을 가할 수 있습니다.

1 https://enterprise.verizon.com/resources/reports/dbir/
2 https://www.vice.com/en_us/article/paqd4m/too-many-people-are-still-using-password-as-a-password
3 https://cups.cs.cmu.edu/passwords.html
4 https://enterprise.verizon.com/resources/reports/DBIR_2018_Report_execsummary.pdf

비밀번호 규칙에 초점을 맞추는 것은 방해가 될 뿐입니다. 그 이유를 이해하기 위해서는 비밀번호에 대한 다양한 공격과 공격 작업에 비밀번호가 활용되는 방식을 살펴보는 것이 중요합니다. 오늘날 비밀번호를 알아내는 가장 일반적인 방법은 다음과 같습니다[5]:

공격	다른 이름	빈도	난이도
크리덴셜 스터핑	유출 리플레이, 리스트 클리닝	매우 높음 – 매일 시도되는 계정 수 2천만 개 이상	매우 쉬움: 저장 데이터 정책이 열악한 유출 사이트에서 수집한 자격 증명을 구매하고 다른 시스템에서 일치 여부를 테스트합니다. 리스트 클리닝 도구는 쉽게 구할 수 있습니다.
피싱	자격 증명 탈취	매우 높음. 전체 수신 메일의 0.5%.	쉬움: 사용자에게 헛된 희망을 품게 하거나 위협을 느끼게 만드는 이메일을 보내고 링크를 통해 위조 사이트에 로그인하도록 유인합니다. 자격 증명을 포착합니다. Modlishka나 이와 유사한 도구를 사용하면 쉽게 실행할 수 있습니다.
패스워드 스프레이	추측, 해머링, 로우 앤 슬로우	매우 높음 – 공격 중 최소 16%에 해당. 하루에 수십만 개가 뚫릴 때도 있음. 수백만	사소함: 간단하게 획득한 사용자 목록을 놓고 수많은 사용자 ID에 대해 동일한 비밀번호를 넣어봅니다. 탐지를 피하기 위해 속도를 조정하고 많은 IP에 걸쳐 분산합니다. 도구는 저렴한 비용으로 쉽게 구할 수 있습니다.

유출 발생 시, 치명적인 결과로 이어질 수 있습니다. 데이터 유출로 인해 도난당한 기록의 평균 비용은 $148이며, **총 발생 비용은 $3,860,000입니다**[6].

별 진척 없는 비밀번호 문제

지금까지 조직들은 기존 비밀번호와 병행하거나 아니면 이를 대체하는, 다양한 인증 방식을 구현함으로써 이 문제를 해결하려고 시도해 왔습니다. 가장 널리 사용되는 방법은 멀티 팩터 인증(MFA)이라고도 하는 투팩터 인증(2FA)입니다.

멀티 팩터 시스템의 일부로 사용되는 인증 팩터는 온갖 유형이 있지만, 넓은 의미로는 다음의 세 가지 유형 중 하나에 속하는 편입니다.

- **지식 팩터** ("당신이 아는 어떤 것"): 특정 정보를 알고 있음을 보여주면 시스템이 사용자를 승인합니다. 예를 들어 PIN, 보안 질문에 대한 답변, 세금 환급 세부정보 등이 있습니다.
- **소유 팩터** ("당신이 가진 어떤 것"): 특정 물리적 장치가 있음을 증명할 수 있으면 시스템이 사용자를 승인합니다. SMS 코드, 인증 앱, USB 키, 무선 태그, 카드 리더기 등이 이에 해당합니다.
- **속성 팩터** ("당신의 고유한 어떤 것"): 시스템이 생체 인식 비교를 통해 사용자를 승인합니다. 지문 스캐너, 망막 스캐너, 음성 인식 등이 이에 해당합니다.

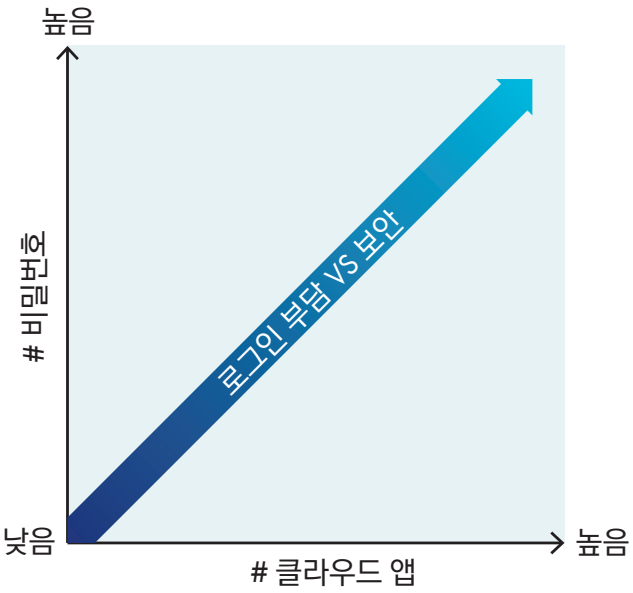
MFA 방법 한 가지는 SMS **메시지**를 이용하는 것입니다. 이 MFA 모델은 매우 유용할 수 있지만 위험이 따릅니다. 첫째, 일부 평판이 좋지 않은 서비스는 광고를 위해 사용자의 전화번호를 사용하거나 금전적 이득을 위해 그것을 판매할 수 있기 때문에 사용자가 전화번호를 알려줄 만큼 신뢰할 수 있는 서비스여야 할 것입니다. 전화번호가 장치와 연결되어 있지 않기 때문에, 해커는 사용자의 전화기를 만질 필요도 없이 SMS 기반 인증을 우회할 수 있습니다. 해커가 하는 것은 SIM 교체 공격이라는 방법인데, 이것은 공격 대상의 휴대전화 통신사에 전화를 걸어 담당자를 속이고 그 대상의 전화번호를 자신이 갖고 있는 SIM 카드로 이전하도록 하기만 하면 됩니다.

일회용 비밀번호(OTP)는 계정 생성 중에 생성된 비밀 키를 기반으로 코드를 암호화 방식으로 생성하므로 보안이 향상됩니다. 즉, 수신 서비스 및/또는 모바일 서비스가 없는 경우에도 자신의 장치에서 유효한 코드를 받을 수 있습니다. OTP 기반 멀티 팩터 인증은 사용자의 스마트폰에 모바일 토큰 형태로 제공되거나 암호생성기 같은 독립형 장치로 제공될 수 있습니다.

점점 더 복잡해지는 액세스 환경과 유례없이 많은 액세스 포인트로 인해 조직은 멀티 팩터 인증을 추가해야 할 충분한 이유가 있습니다. 그러나 보호해야 할 수많은 클라우드 서비스 때문에 각각의 로그인 시도마다 항상 MFA를 적용하는 것은 사용자 경험 관점에서 실용적이지 않습니다.

5 https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Your-Pa-word-doesn-t-matter/ba-p/731984
6 https://www.ibm.com/security/data-breach

지금은 클라우드 기반 기술(및 위협)의 증가가 불편한 인증 배포로 인해 방해받고 싶지 않은 (점점 증가하는) 이동 인력과 충돌하고 있는 중요한 변곡점입니다. 필요한 것은 강력한 보안과 편의성을 제공하는 패스워드리스 인증 방법입니다. 지금까지 이러한 유형의 솔루션은 적합한 기술의 부재로 인해 활성화되지 못했습니다. 그러나 상황은 변하고 있습니다.



무엇이 변했으며, 왜 희망적인가

최근 몇 년 동안, 특히 정부 기관 및 규제 기관에서 사용자의 온라인 보안 및 개인 정보 보호에 대한 인식이 증가했습니다. 과거에는 조직이 데이터 유출 및 보안 사고를 겪으면 그 후 법적 및 재정적 영향이 거의 없을 것으로 예상했지만 이제는 더 이상 그렇지 않습니다.

규제 기관도 조치를 시행하기 시작하여 자신의 데이터 보호 관행에 강력한 인증을 추가하는 기업이 늘고 있습니다. 가장 관련성이 높은 규제 조치로는 액세스 보안의 표준을 정의하는 일반 데이터 보호 규정(GDPR)이 있습니다. 규칙을 준수하지 않고 고객의 데이터를 보호하지 못하는 회사는 엄중한 벌금을 부과 받습니다. GDPR은 EU 관할권에만 적용되지만, EU에 기반을 두지 않고도 이 지역에서 사업을 하는 회사가 많기 때문에 이제는 보안의 황금 기준으로 간주됩니다.

강력한 인증을 채택하는 회사가 더 많아지고 비밀번호 훼손으로 인한 데이터 유출이 늘어나는 시기에, 회사가 비밀번호만을 이용한 인증이 적절한 보안이라는 것을 GDPR 규제 기관에 입증하기는 점점 더 어려워질 것입니다. 이로 인해 회사는 비밀번호에서 강력한 인증으로 이전하는데 드는 비용보다 훨씬 높은 벌금을 부과 받을 수 있습니다.

업계에 특화된 다른 규정들은 인증 기술 사용에 대해 더 명시적입니다. 유럽의 전자상거래 및 온라인 금융 서비스를 규제하고 2 팩터 인증을 의무화한 지불 서비스 지침 2(PSD2)가 그 예입니다. PSD2는 또한 보안 카드, 모바일 장치 및 생체 인식 스캐너를 사용하여 보안을 약화시키지 않고 사용자 경험을 향상할 것을 권장합니다.

마지막으로 미국 국립표준기술연구소(NIST)의 디지털 신원 가이드라인은 조직이 비밀번호 및 일회용 비밀번호에서 벗어나 강력한 최신 인증을 채택해야 한다고 명시하고 있습니다. 보다 구체적으로, NIST는 장치에 신규 계정을 만들 때 그 자격 증명으로 암호화 개인 키를 생성해 사용할 것, 그리고 그것을 현재 대부분의 스마트폰이 지문 데이터를 안전하게 저장하듯이 동일한 방식으로 안전하게 저장할 것을 권장합니다.

생체 인식, 위치 정보 및 기타 센서가 통합된 모바일 디바이스의 확산과 같은 기술 혁신으로 인해, 어댑티브 또는 컨텍스트 인증이 가능해졌고 그에 따라 패스워드리스 인증을 채택할 수 있었습니다. 이런 다양한 센서가 백그라운드에서 사용자 행동에 대한 데이터를 수집하므로, 사용자 측에서는 해야 할 일이 전혀 없습니다. 이렇게 센서로 수집된 메트릭을 이용해 사용자 행동을 정기적 및 주기적으로 확인함으로써, 사용자 인증을 원활한 지속적 프로세스로 변환합니다.

IP 주소, 모바일 매개변수, 알려진 장치, 운영체제, 컨텍스트 또는 위험 기반 인증 같은 다양한 속성을 평가함으로써, 한 개인이 애플리케이션에 로그인할 때마다 신원을 지속적으로 확인할 수 있습니다. 사실 사용자가 알지 못하는 상태에서도 이렇게 할 수 있습니다. 기업은 사용자 경험을 향상시키고 IAM 정책을 적용하는 한편, 보다 강력한 보안을 촉진하는 패스워드리스 인증을 채택하기 위해 노력합니다.

패스워드리스 인증 – 다층적 접근

패스워드리스 인증은 비밀번호를 다른 신원 확인 방법으로 대체하여 보증 수준과 편의성을 향상시킵니다. 이 유형의 인증은 사용자의 로그인 경험을 더 쉽게 만들고 텍스트 기반 비밀번호 고유의 취약성을 극복하는 데 큰 이점이 있기 때문에 큰 호응을 얻었습니다. 사용하기 편리하고, 각 애플리케이션에 제공되는 보안 수준이 높은 것이 이점이며, 무엇보다도 기존의 비밀번호가 필요 없습니다.

Gartner에 따르면 2022년까지 50%의 사례에서 거대 글로벌 기업 60%와 중간 규모의 직원 수를 가진 기업 90%가 패스워드리스 인증 방법을 구현할 것으로 예상됩니다. 이 변화는 현재의 5% 미만에 비하면 매우 급격하게 증가하는 것입니다[7].

7 패스워드리스 접근을 채택하여 보안을 향상하십시오, https://www.gartner.com/smarterwithgartner/embrace-a-passwordless-approach-to-improve-security/

패스워드리스 인증에는 다양한 층위가 있어 다양한 수준의 보안을 제공할 수 있습니다. 특정 모델의 구현은 기업이 비즈니스 및 보안 위험과 보호할 데이터의 민감도에 기반하여 적용하고 싶어하는 인증 및 연계 접근에 따라 다릅니다.

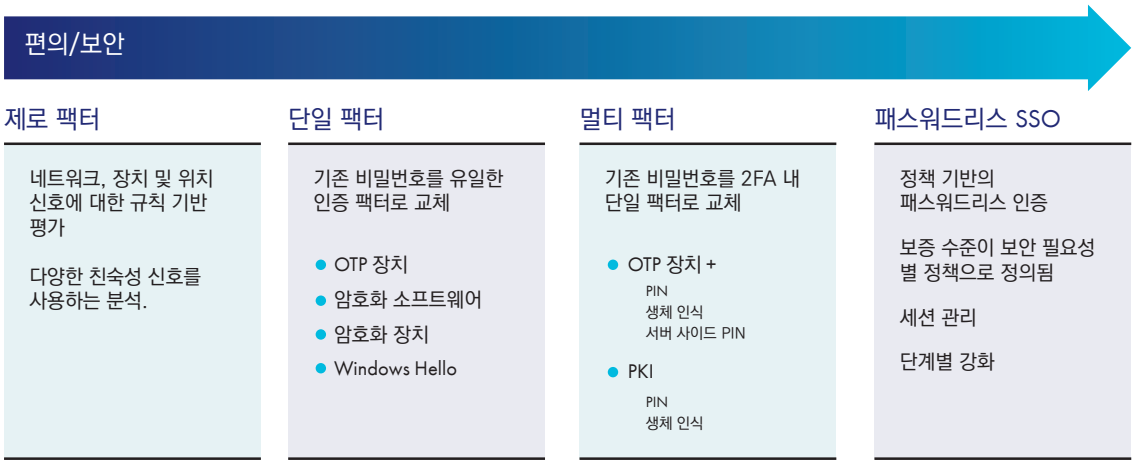
제로 팩터의 패스워드리스 인증은 규칙 또는 지식 기반 인증(예: 보안 질문)이나 장치 및 위치 지표를 친숙성 신호로 이용하는 방법이 포함될 수 있습니다. 신원 확인을 완전히 보장할 수 없다는 것이 제로 팩터 인증의 단점이므로, 백업 방법으로 사용하거나 다른 인증 방법과 함께 사용하는 것이 이상적입니다.

비밀번호가 "당신이 아는 어떤 것" 팩터와 관련된 **단일 팩터 인증**으로 간주되지만, 업계에서는 이것의 사용을 중단하면서 "당신이 가진 어떤 것" 팩터를 활용하는 단일 팩터 인증 솔루션을 채택하고 있습니다. 이러한 솔루션에는 OTP를 생성하는 장치 또는 암호화 소프트웨어 및/또는 하드웨어를 사용하는 것이 포함됩니다. 조직은 단일 팩터 체계를 통해 유일한 인증 팩터로서의 기존의 비밀번호를 다른 수단으로 대체할 수 있습니다. 단일 팩터의 패스워드리스 인증은 제로 팩터보다 안전하지만, 여전히 멀티 팩터 인증의 보안 수준을 제공하지는 못합니다. 장치의 TPM에 저장된 암호화 비밀에만 의존하는 Windows Hello가 단일 팩터 인증 모델의 한 예입니다. 즉 "당신이 가진 어떤 것"에 대한 비밀은 사용자의 장치에 저장되어 있는 것이지 별도의 위치에 저장되어 있는 것이 아닙니다.

멀티 팩터의 패스워드리스 인증 체계는 조직이 MFA 배포에서 하나의 팩터로서의 비밀번호를 OTP 장치나 PIN 또는 생체 인식과 결합된 PKI 기반 솔루션의 조합으로 대체할 수 있게 해줍니다. 일반적으로 PIN 또는 생체 인식은 특정 장치에 고유하지만, 인증 서버에서 PIN을 정의하고 확인 평가하여 그 보안을 강화할 수 있습니다.

오늘날의 차세대 인증 및 액세스 관리 체계는 다양한 어댑티브 및 멀티 팩터 방식에 광범위한 유연성을 제공하며, 유연한 액세스 정책 내에서 결합하여 다양한 액세스 시나리오에 맞는 적절한 수준의 패스워드리스 보안을 제공할 수 있습니다.

패스워드리스 인증 모델



패스워드리스 인증이 꼭 보안을 저하시키는 것은 아닙니다

실제로 어떤 것이 안전한가에 대한 대답은 일반적으로 "위협 모델에 따라 다르다"입니다. 이 경우도 다르지 않습니다. 패스워드리스 인증 시스템의 보안은 궁극적으로 높은 수준의 확실성으로 개인의 신원을 확인하는 체계의 능력에 달려 있습니다. 간단하게 말해서, 패스워드리스 방법은 기저에서 사용되는 인증만큼이나 안전합니다.

예를 들어, 계정 소유자의 휴대 기기에 보안 푸시 알림을 사용하는 것은 일반적으로 비밀번호보다 더 안전한 것으로 간주됩니다. SMS는 안전하지 않은 통신 채널이며 SMS 인증 시스템에 대한 공격의 여러 유형이 문서화되어 있기 때문에 계정 소유자의 모바일 장치에 대한 SMS 코드의 보안 수준이 떨어질 수 있습니다.

비밀번호는 집요하고 자금력이 충분한 공격자에 맞서 취하는 경로가 아닙니다. 최선의 방어 방법은 기존의 비밀번호를 없애고 대신 멀티 팩터 인증, 어댑티브 보안 및 이상 탐지를 결합하여패스워드리스 보안을 심층적으로 실행하는 것입니다. 이런 패스워드리스 인증의 배포는 구현 방식에 따라 다양한 수준의 보안 요구 사항에 맞을 수 있습니다.

하나로 모든 것을 만족시킬 수 없습니다

단일 회사 내에서 다양한 식별 및 액세스 관리 사용 사례를 고려할 때, 인증 솔루션은 모든 경우에 다 적합한 것이 아닙니다. 보안 및 비즈니스 책임자는 자신의 기업에서 하나 이상의 사용 사례의 요구를 충족시키는 인증 솔루션을 찾아야 합니다. 일부 방법은 광범위한 사용 사례에 적합하며, 많은 벤더들은 다양한 개별 방법을 제공하거나 지원하는 도구를 제공합니다. 그러나 보안 책임자는 모든 사용 사례에서 자신의 요구를 충족하는 단일 솔루션을 찾지 못할 수도 있습니다.

인증 방법을 선택하기 전에 보안 책임자는 다음의 기준을 평가해야 합니다.

- **신뢰 VS 위험**. 위험에 적합한 인증이 모범 사례가 되는 원칙입니다. 책임자는 각 사용 사례마다 그 위험 수준에 상응하는 최소한의 신뢰 수준을 평가해야 합니다. 그런 다음 필요한 신뢰 수준에 맞는 인증 방법을 선택합니다.
- **총소유비용(TCO) VS 정당하고 사용 가능한 예산**. 클라우드 기반 환경의 효율성 및 자동화된 인증 프로비저닝 워크플로우와 같은 운영 비용을 절감할 수 있는 요소를 고려합니다.
- **사용자 경험(UX)/고객 경험(CX) VS 사용자 요구**. CX는 가산점이 많이 붙는 선택 기준입니다. 탈레스에서 매년 발행하는 액세스 관리 및 인증 설문조사에서 IT 전문가의 65% 이상이 액세스 관리 및 인증 솔루션을 구현할지 여부를 결정하는 주요 동인으로 최종 사용자를 위한 간소화된 액세스를 꼽았습니다.
- **기타 기술 및 운영 요구 사항 및 제약 조건**. 액세스 관리 및 인증 솔루션이 기존의 조직 IT 프레임워크 및 보호가 필요한 애플리케이션과 통합되는 방법 등이 있습니다.

패스워드리스 싱글사인온

싱글사인온(SSO)은 최종 사용자가 한 세트의 로그인 자격 증명만 입력하여 여러 애플리케이션에 액세스할 수 있게 하는 세션 및 사용자 인증 서비스 사용 사례입니다. 사용자는 단순히 SSO 포털이나 애플리케이션에 로그인한 후 다시 인증할 필요 없이 (한 세션 동안, 예를 들어 통상적인 하루의 업무 일과 동안) 모든 애플리케이션에 원활하게 액세스할 수 있습니다. SSO가 조직이 중요한 액세스 문제를 해결하는 동시에 생산성 및 사용자 경험 측면에서 명확한 이점을 제공하는 데 도움이 되는 것은 사실입니다.

SSO와 함께 패스워드리스 솔루션을 구현하면 패스워드리스 인증을 한 단계 더 시행하므로 사용자 경험을 크게 향상시킬 수 있습니다. 사용자가 인증한 다음 다시 인증하지 않고도 다른 앱 및 서비스에 액세스할 수 있습니다.

항상 그렇듯이 사용자 편의성과 경험은 보안 위험과 반비례합니다. SSO의 경우, 사용자가 사내 또는 클라우드에서 여러 앱에 액세스하기 위해 동일한 자격 증명을 재사용하므로 보안 위험이 증가하게 됩니다. 따라서 SSO 솔루션이 정책 기반 액세스를 지원하여 인증 및 조건부 액세스를 강화할 수 있도록 하는 것이 중요합니다. 이는 사용자 프로필과 데이터 액세스의 민감도에 따라 다양한 액세스 사례에 대해 각기 다른 정책을 시행할 수 있음을 의미합니다.

조직은 편의성과 보안 간에 필요한 균형을 유지하기 위해 두 가지의 위험 관리 모범 사례를 구현할 수 있습니다.

- 첫 단계의 패스워드리스 인증 솔루션이 적합한 보증 수준을 충족할 것
- 로그인 시나리오가 변경되면 인증 수준이 적절하게 올라가도록 조건부 액세스 정책을 적용할 것

액세스 관리 및 사용자 인증의 미래를 살펴보면, 패스워드리스 인증은 지속적인 패스워드리스 SSO로 더욱 발전할 것입니다. 즉 지속적인 로그인 세션 내에서 사용자의 행동이 모니터링되고 사전 정의된 시나리오 및 규제 준수에 기반한 재인증 정책에 따라 추가적으로 신원 확인이 작동되는 방식입니다. 재인증을 작동할 수 있는 사용자 행동으로는 대용량 파일 다운로드, 데이터베이스 내의 민감한 정보 액세스, 서비스 설정 재구성, 위치 변경 등이 있습니다.

패스워드리스 인증과 지속적 인증은 서로 얽혀 있습니다

인증은 기본적으로 토큰이나 비밀번호나 지문을 활용하여 '예'와 '아니요' 중 하나를 결정하는 것입니다. 즉 시스템은 사용자 신원을 확인하고 그에 따라 액세스를 허용 또는 거부합니다. 기존의 인증 방법은 처음 로그인할 때 사용자의 인증을 한 번만 확인합니다. 이런 일회성 인증은 사용자가 작업 환경을 변경하면 취약성이 생길 수 있습니다. 따라서, 사용자의 신원을 지속적으로 평가해야 합니다.

지속적인 인증 세션은 사용자가 장치에서 장치로, 앱에서 앱으로 이동할 때, 매 액세스 지점마다 일정 기간에 걸쳐 사용자의 신원이 맞는지 확인합니다. 액세스 관리 서비스는 지속적으로 투명한 방식으로 개인의 신원을 재확인하며, 정책에 따라 작동되거나 액세스 이상이 발견된 경우에만 추가 인증이 필요합니다.

투명한 인증 방식에서는 어댑티브 및 컨텍스트 속성에 따라 인증 여부를 결정하기 때문에 사용자가 매번 명시적으로 인증을 받아야 할 필요가 없습니다. 거대한 사용자 행동[8] 데이터 소스를 가진 모바일 장치 덕분에 투명한 인증이 보안과 사용성을 향상시킵니다.

센서 기반 데이터의 풍부하고 잠재적으로 원활한 특성은 작업별 임계값 지정을 통해 애플리케이션 및 데이터 액세스에 보다 세분화된 접근 방식을 제공할 수 있는 투명한 인증을 제공합니다. 따라서 애플리케이션 내에서 사용자의 조치는 시간이 지남에 따라 평가되며 어떤 행동을 취했는지에 따라 추가 인증이 요구됩니다. 따라서, 예를 들어, 사용자가 애플리케이션으로부터 대량의 데이터를 다운로드하기 시작하면, 액세스 관리 서비스는 더 높은 정도의 신원 확인이 가능한 인증 이벤트를 작동시킬 수 있습니다.

이러한 체계의 장점은 사용자의 로그인 부담을 크게 줄이면서도 매우 높은 수준의 액세스 보안을 유지할 수 있다는 것입니다. 또한 앱의 민감도, 사용자 프로필, 기타 조건에 따라 액세스 시나리오마다 각기 다른 인증 방법을 적용할 수 있는 유연성이 있습니다.

패스워드리스 SSO로 시작하기

Gartner가 예측했듯이, 대다수의 조직은 향후 몇 년 동안 패스워드리스 인증으로 마이그레이션을 시작할 것입니다. 이 조직들은 일반적인 사용자가 액세스하는 애플리케이션과 데이터를 찾아내어 자체적으로 고유한 패스워드리스 SSO 구현을 시작할 수 있습니다. 이러한 지식을 바탕으로, 데이터 액세스의 민감도와 관련 위험을 평가한 다음, 각 데이터 세트마다 적합한 수준의 인증 보증을 매핑할 수 있습니다. 그런 다음 보안과 편의성을 극대화할 수 있도록 자체 정의된 패스워드리스 SSO 프로그램에 따라 액세스 정책을 설정할 수 있습니다.

8 Alotaibi, Furnell and Clarke (2015), "모바일 디바이스 보안을 위한 투명한 인증 시스템: 리뷰(Transparent authentication systems for mobile device security: A review)", IEEE, https://ieeexplore.ieee.org/document/7412131

대한민국 – 서울특별시 용산구 한남동 독서당로 98 여선교회관 6층
| 전화: 82.2.3278.8202 팩스: 82.2.3278.8290 |
이메일: krsales.cpl@thalesgroup.com

> cpl.thalesgroup.com <