2024년 Duo
Trusted Access 보고서

2024년 Duo Trusted Access 보고서

목차

Trusted Access 보고서 범례

- 섹션 시작
- 관심 분야
- 섹션 계속
- 추가 정보
- 섹션 끝

MFA는 뛰어난 보안 조치이지만 그 자체만으로는 부족합니다. 더욱 정교해진 위협으로 인해 추가적인 보안 계층이 필요합니다.

서론

액세스 관리 및 ID 보안의 새로운 혁신

미래를 탐구할 때 우리는 종종 미지의 것을 예측하는 데 끌리게 됩니다. 답을 찾기 위한 탐구는 끝이 없고 예측을 이끌기 위해 데이터에 크게 의존합니다.

오늘날 조직은 금전적 이득, 사이버 스파이 활동, 중단부터 명예 훼손, 사이버 전쟁에 이르기까지 공격자의 동기가 그 방법만큼이나 다양한 위험한 디지털 환경을 헤쳐나가고 있습니다. 동시에 이러한 조직은 복잡한 IT 스택부터 분산된 하이브리드 인력, 시스템과 애플리케이션에 액세스하는 매우 다양한 디바이스에 이르기까지 다양한 내부 복잡성도 관리합니다. 이렇게 임시 원격 근무 설정에서 하이브리드 업무 모델로 발전하면서 기존의 기업 경계가 사이버 영역의 먼 구석까지 확장되었습니다.

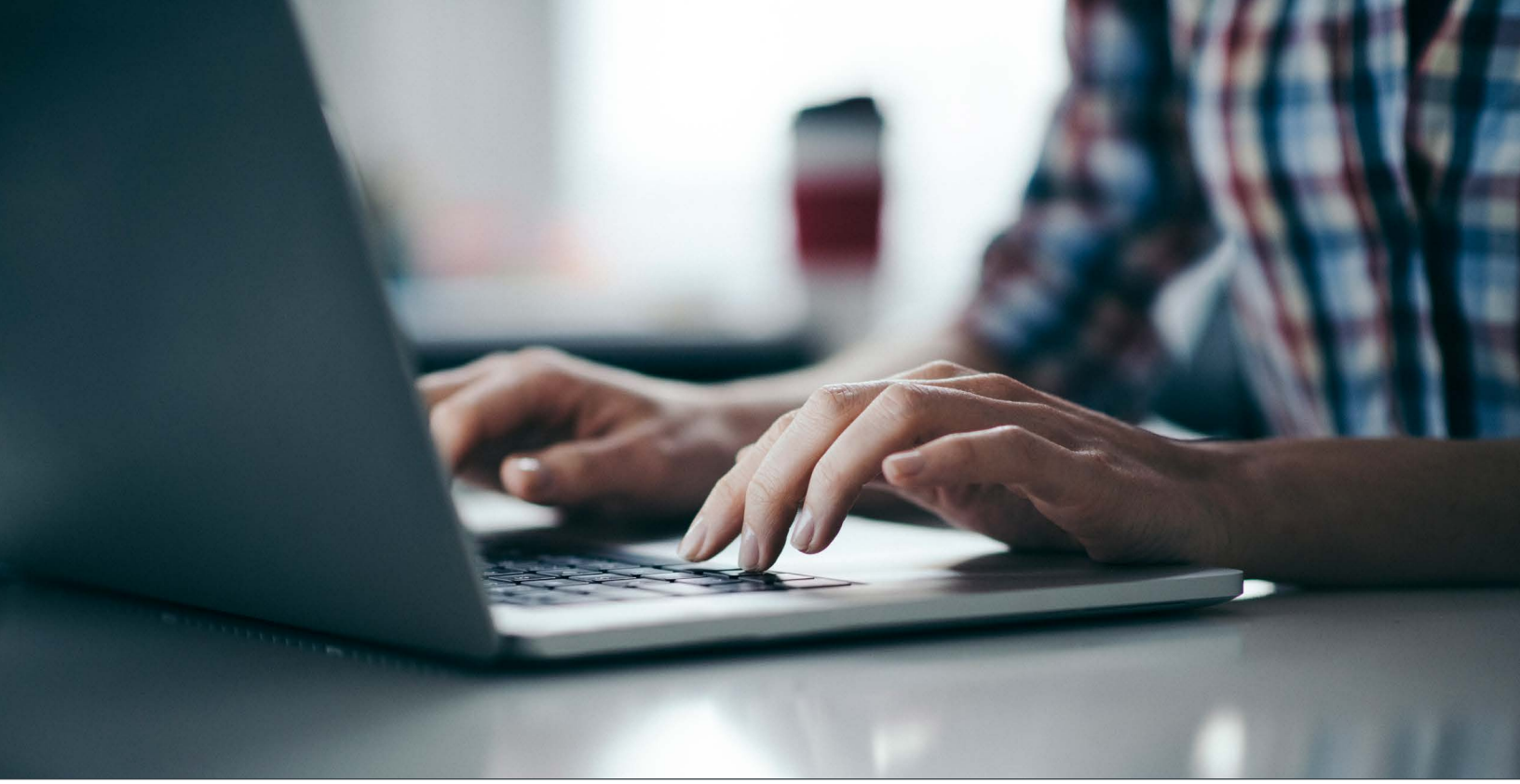
몇 년 전만 해도 IT 인프라 보호는 주로 시스템이 원활하게 실행되도록 하는 것, 즉 "운영을 유지하는 것"과 관련된 것이었습니다. 현재는 보호 범위가 기하급수적으로 확장되어 랜섬웨어부터 국가 주도 해킹에 이르는 수많은 외부 사이버 위협에 대한 완벽한 방어를 포함합니다. 위협 환경이 확대됨에 따라 모든 직원의 액세스 권한이나 디바이스가 잠재적인 엔트리 포인트가 되면서 공격의 표면 영역도 넓어졌습니다. 이런 변화로 인해 IT 부서는 주로 운영 업타임을 관리하는 부서에서 여러 가지 정교한 외부 위협에 대한 필수적인 보호 부서로 변모했습니다.

미래에 어떤 일이 일어날지 정확히 알 수는 없지만 과거의 패턴을 분석하면 미래의 가능성에 대한 인사이트를 얻을 수 있습니다. 예를 들어 이전 버전의 Trusted Access 보고서에서는 기업들이 더욱 향상된 보안 환경에서 위험을 줄이기 위한 노력으로 다단계 인증(MFA)의 채택을 늘리고 있다고 언급했습니다.

조직이 점점 더 정교해지는 사이버 보안 위협을 해결하려고 노력하면서 몇 년 동안 전체적인 종합적인 액세스 관리 솔루션에 대한 요구가 분명해졌습니다. MFA는 뛰어난 보안 조치이지만 그 자체만으로는 부족합니다. 더욱 정교해진 위협으로 인해 추가적인 보안 계층이 필요합니다.

액세스 관리 솔루션은 컨텍스트를 통합하여 사용자의 평소 로그인 시간, 지리위치, 디바이스를 포함한 사용자의 일반적인 행동이나 환경에 대한 정보 등 액세스가 요청되는 상황을 분석할 수 있습니다. 그러면 보안 계층이 추가되어 더욱 전체적이고 동적인 인증 접근 방식을 제공합니다.

본질적으로 인증 프로세스에 컨텍스트를 추가하면 시스템이 합법적인 사용자와 잠재적 위협을 더 잘 구분하여 향상된 보안을 제공하면서 탁월한 사용자 경험을 유지할 수 있습니다. 따라서 컨텍스트는 새로운 형태의 MFA가 됩니다.



위치 또는 디바이스 세부 정보(예: 운영 체제)와 같은 컨텍스트 요인은 수년간 Trusted Access 보고서에 포함되었습니다. 그러나 하이브리드 업무가 확고히 뿌리내린 현실이 되면서 컨텍스트 요인의 중요성은 더욱 커지고 있습니다.

관심이 증가하고 있는 또 다른 영역은 ID의 미래로, 더 구체적으로는 사이버 보안 관점에서 디지털 ID의 확산을 해결하는 방법입니다.

현대 업무 환경에서는 모든 직원이 다양한 시스템, 애플리케이션, 플랫폼에 걸쳐 여러 개의 디지털 ID를 사용할 수 있습니다. 그 범위는 이메일 계정부터 내부 시스템의 액세스 자격 증명, Slack과 같은 협업 플랫폼의 프로필에 이르기까지 다양합니다. 비즈니스가 클라우드 서비스, SaaS(Software-as-a-Service) 플랫폼, 원격 협업 툴 등을 계속 도입하면서 이러한 디지털 ID의 수도 증가하고 있습니다. 이러한 확산은 생산성과 보안에 모두 중요한 영향을 미칩니다.

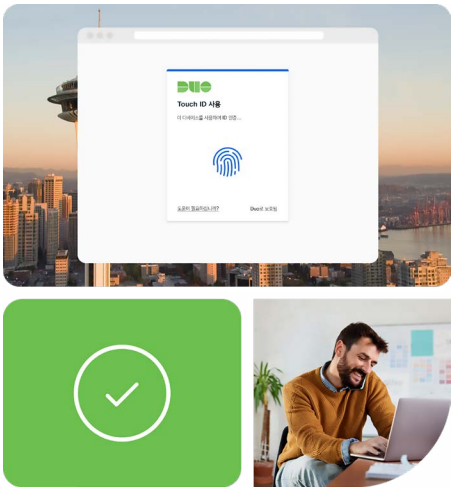
한편으로는 이러한 ID를 통해 더욱 원활하게 협업을 진행하고 필요한 리소스에 액세스할 수 있어 효율성이 개선될 수 있습니다. 반면에 이렇게 수많은 ID를 관리하고 적절한 보안을 보장하는 것은 복잡한 작업이 됩니다. 포괄적인 단일 인터페이스에서 조직의 ID 에코시스템 전반에 대한 위험 가시성을 확보하는 것은 필수가 되었습니다.

이는 ID 위협 탐지 및 대응(ITDR) 기능을 통해 달성할 수 있습니다. ITDR 발전은 ID의 미래에 필수적인 부분으로, 일상 생활에서 점점 더 확산되는 디지털 ID의 보안을 유지하는 데 매우 중요합니다.

문제는 명확합니다. 전 세계적으로 MFA 사용이 계속 확대되면서 공격자의 방법도 증가하고 있습니다. 보안 침해 가능성을 최소화하려면 사용자의 일반적인 행동이나 환경과 같은 컨텍스트 요인뿐만 아니라 포괄적인 단일 인터페이스에서 조직의 ID 에코시스템 전반에 대한 가시성으로 기존 MFA를 강화해야 합니다.

방법론

이 보고서에서는 북미, 라틴 아메리카, 유럽, 중동, 아시아 태평양을 포함한 여러 지역에서 5,800만 개의 엔드포인트와 2,100만 개의 고유 전화에서 약 5,200만 개의 다양한 브라우저를 통해 지난해에 160억 건(지난 4년간 440억 건 이상) 이상의 인증을 분석하여 얻은 인사이트를 자세히 살펴봅니다. 2023년 연간 기간을 2022년 6월 1일부터2023년 5월 31일까지로 정의했습니다.



주요 조사 결과

01

더욱 강력한 인증 방법이 상승하는 추세를 보임

Duo Mobile과 같은 인증 앱은 더욱 강화된 보안과 사용 편의성에 대한 요구를 모두 충족시키며, 91.5%의 계정이 Duo Push를 활성화하여 21% 또는 32억 건 이상의 인증을 처리합니다. 또한 SMS 및 전화 통화의 감소 추세도 하나의 요인으로 관찰되었으며, 2022년 대비 22% 감소한 4.9%의 인증으로 사상 최저치를 기록했습니다.

02

사무실 복귀가 새로운 하이브리드 업무 현실이 됨

지난 해 원격 액세스 애플리케이션에 대한 액세스는 2020년에 정점을 찍은 후 약 25%의 인증으로 감소했습니다. 그 이후 직원을 사무실로 복귀시키는 회사가 늘어나면서 이 범주의 인증 수는 계속 감소했습니다.

03

MFA 사용이 전 세계적으로 계속 확대됨

지난 한 해 동안 Duo를 사용한 MFA 인증 수가 41%까지 증가했으며, 독일과 같은 국가는 매년 52.3%의 인증 증가율을 보이고 있습니다. 아시아 태평양 지역에서는일본, 필리핀, 호주가 지난 해부터 지속적인 증가를 보였으며, 각각 28%, 24.9%, 16.9%씩 증가했습니다. 브라질은 2022년 대비 26.3% 이상의 MFA 사용 증가를 보이며 세 번째로 높은 인증 증가율을 기록하고 있습니다.

04

다양한 디바이스 환경에는 벤더에 구애받지 않는 보안이 필요함

Windows가 액세스 디바이스의 38.2%를 차지하며 계속 선두를 유지하고 있는 반면, 전체 운영 체제 순위에서는 iOS가 33.4%로 강력한 2위를 차지하고 있습니다. Duo 사용자들 사이의 모바일 범주에서는 Apple이 계속해서 가장 강한 영향력을 행사하고 있고, 가장 가까운 경쟁업체는 28.2%의 훨씬 더 낮은 채택률을 보이는 Android입니다. 또한 벤더에 구애받지 않는 보안에서는 잠재적인 보안 격차가 제거되고 보안 시스템이 디바이스 환경의 변화에 쉽게 적응할 수 있어 유연성과 확장성이 향상됩니다.

주요 조사 결과

05

조직이 더욱 엄격한 제어를 통해 오래된 소프트웨어의 위험을 줄임

2023년에는 오래된 디바이스로 인한 인증 실패율이 74.7%까지 증가했습니다. 조직에서 인증을 허용하는 운영 체제(OS)가 많을수록 인증이 오래된 OS에서 수행될 가능성도 높아집니다. 특히 IT 환경을 확장하고 있는 조직에서는 오래된 소프트웨어로 인한 위험을 줄이기 위해 점점 더 엄격한 통제를 실시하고 있습니다.

06

실패한 인증으로 사용자 위험이 강조됨

측정한 모든 인증의 5%가 실패한 인증이었습니다. 데이터를 자세히 살펴본 결과, 실패한 인증의 28%는 시스템에 등록하지 않은 사용자에 의해 발생했다는 사실을 알아냈습니다. 등록되지 않은 사용자가 민감한 데이터나 중요한 시스템에 무단으로 액세스하여 데이터 보안 침해로 이어질 수 있습니다.

07

보안 부채를 줄이기 위한 상위 3가지 정책 그룹

보안 부채를 완화하는 가장 효과적인 전략 중 하나는 포괄적인 위험 관리입니다. 지리적 제한, 보안되지 않은 디바이스 및 세분화된 사용자별 또는 애플리케이션별 액세스 문제를 해결하는 정책은 복잡성을 줄이고 보안 적용 범위를 늘리는 데 도움이 될 수 있습니다. 그러나 96.4%의 조직에는 위치 관련 정책(2FA 허용, 거부 또는 필요)이 없습니다.

08

ID가 새로운 경계가 됨

적절한 가시성, 위협 탐지 및 대응 기능이 없는 ID 인프라는 공격자가 중요한 시스템에 침입할 수 있는 충분한 기회를 제공합니다. Talos IR이 관찰한 23%의 인게이지먼트에서 공격자는 훼손된 자격 증명을 악용하여 유효한 계정에 액세스할 수 있었습니다[1]. 평균적으로 회사의 계정 중 40.26%는 MFA가 없거나 MFA가 취약합니다[2].

정교한 사이버 공격이 보편화된 환경에서는 ID 위협 탐지 및 대응 기능으로 액세스 관리 솔루션을 강화하여 포괄적인 단일 인터페이스에서 조직의 ID 에코시스템 전반에 대한 가시성을 제공해야 합니다.

각주:

1. "**텔레메트리 동향**" (6~7페이지 참조)
2. **보고서**(Oort), 섹션 2 "Multi Factor Authentication: Full Coverage Remains Elusive" 참조

01 수십억 건의 인증

지속적으로 비밀번호를 강화하고 있는 MFA

다단계 인증(MFA)은 강력함을 유지하면서 기존 비밀번호를 사용하는 방식의 보안을 한층 더 강화합니다. 지난 한 해 동안 Duo를 사용한 MFA 인증 수가 41% 증가했습니다.

Push에 대한 선호도

Duo Push는 가장 많이 사용된 인증 방법으로, 전체 인증의 21%를 차지합니다.

계속 증가하는 비밀번호 없는 액세스 채택

보안 키 및 TouchID와 같은 생체 인식 기술을 포함한 WebAuthn 지원 요소를 채택하는 계정이 2022년에서 2023년 사이에만 53% 증가했습니다.

월별 성공한 인증 수(10억)

2019년 5월 이후 Duo의 인증 성공 횟수는 416억 건, 월 평균 8억 6630만 건

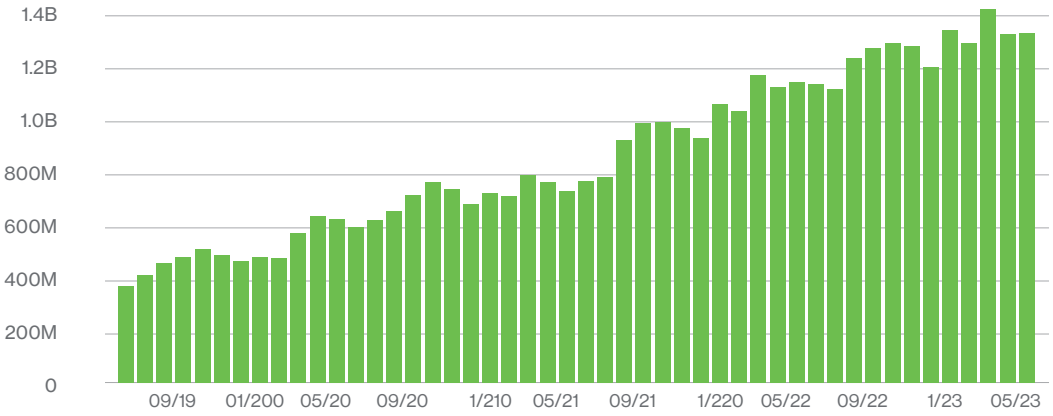
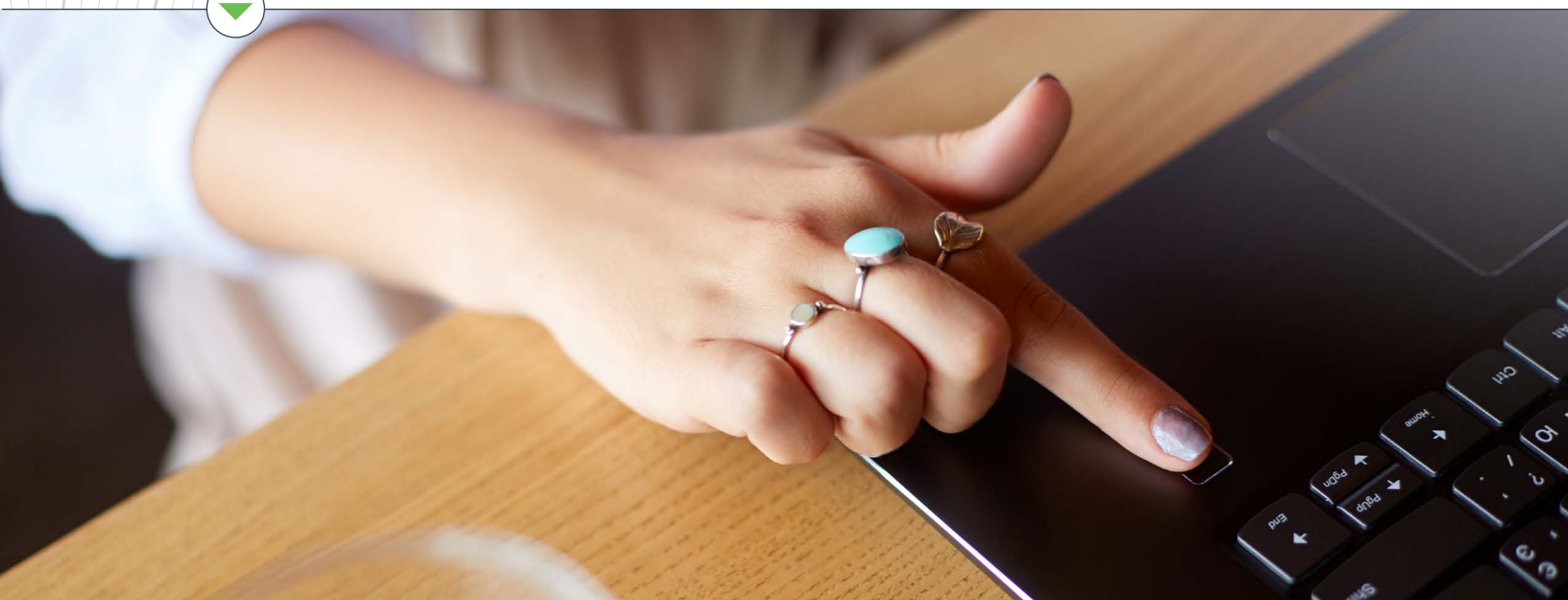


그림 1 월별 성공한 인증 수



더욱 강력한 인증 방법이 상승하는 추세를 보임

비밀번호를 유일한 인증 방법으로 사용할 때의 취약점은 잘 문서화되어 있습니다. 비밀번호는 추측, 해독, 피싱 또는 도용할 수 있으며, 사용자가 여러 서비스에서 비밀번호를 재사용하거나 간단하고 쉽게 해독할 수 있는 비밀번호를 만들어서 이러한 취약점이 악화되는 경우가 많습니다. 반면, 다단계 인증(MFA)은 잠재적인 공격자에게 추가적인 장애물을 도입하여 이러한 위험을 완화합니다. 비밀번호가 유출되더라도 공격자가 사용자의 물리적 디바이스나 생체 인식 정보에 액세스할 수 있는 가능성이 현저히 낮습니다.

그러나 최근 세간의 이목을 끈 사이버 공격에서 두 번째 요소만 활성화한다고 해서 계정을 침투할 수 없는 것이 아니라는 사실이 확인되었습니다. 모든 인증 방법이 동일한 것은 아닙니다. FIDO2 보안 키 및 WebAuthn 지원 생체 인식과 같은 요소는 SMS 문자나 전화 통화와 같이 더 약하지만 접근성이 높은 요소에 비해 익스플로잇하기가 더 어려운 것으로 입증되었습니다.

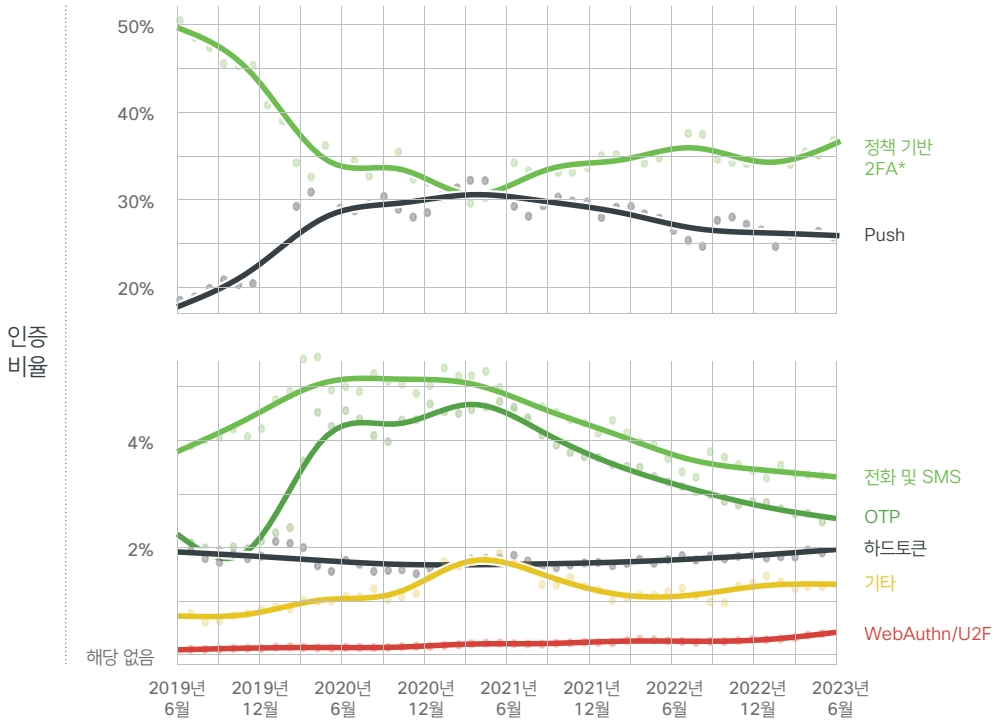


그림 2 시간 경과에 따른 요인 개수별 인증 비율

*이 컨텍스트에서는 사용자에게 **우회 상태**를 할당했거나 계정에서 Duo 기억 디바이스를 활성화한 인증이 정책 기반 2FA에 포함되어 사용자에게 강력한 인증을 제공하면서 중단 없는 원활한 로그인 환경을 유지합니다. Duo **위험 기반 기억 디바이스**는 위험 신호에 대한 응답으로 기억 디바이스 세션 기간을 조정하여 Duo의 기억 디바이스 기능에 대한 보안을 강화합니다.

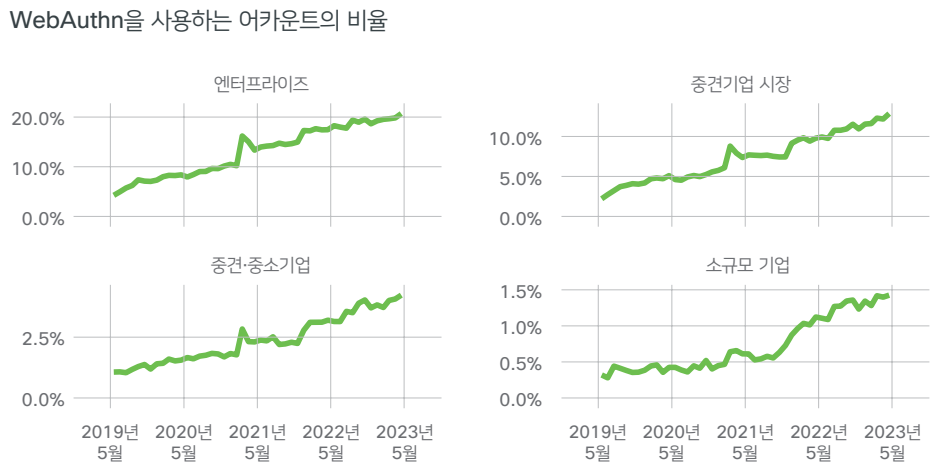


그림 03 인증에 WebAuthn을 사용하는 계정의 비율

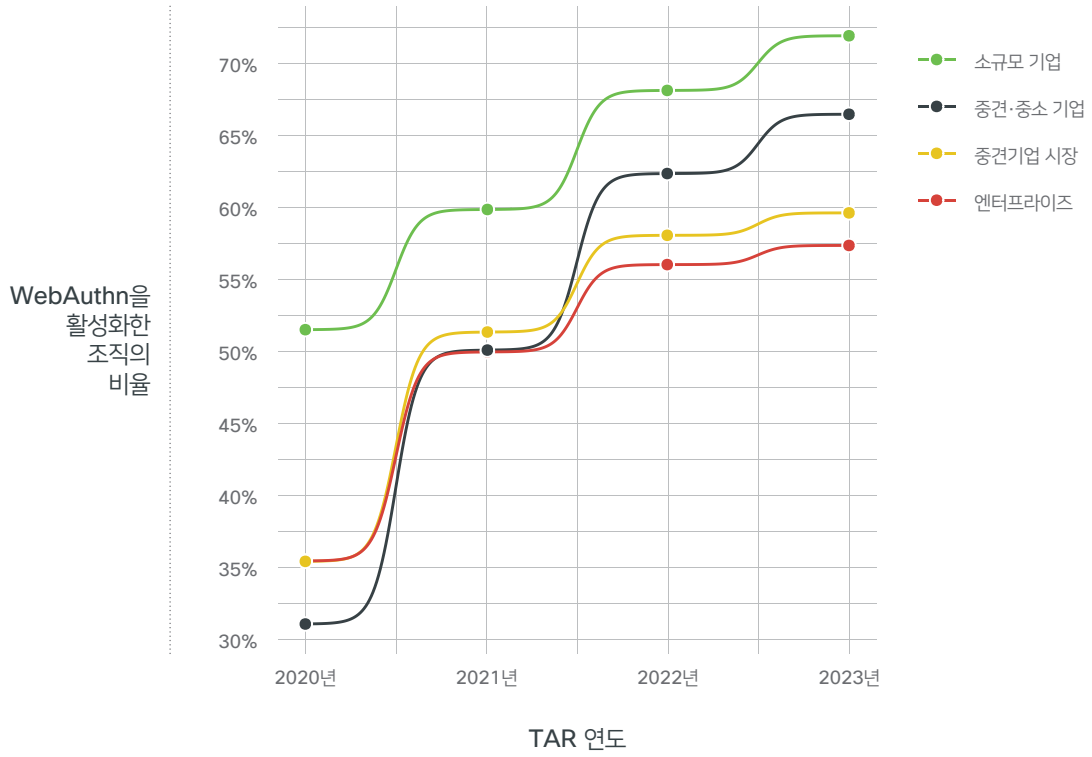


그림 04 시장 부문별 WebAuthn 채택 현황

다행히 **Duo Mobile**과 같은 인증 앱은 더욱 강화된 보안과 사용 편의성에 대한 요구를 모두 충족시킵니다. 91.5%의 계정이 Duo Mobile 애플리케이션을 통해 사용할 수 있는 원터치 인증 방법인 Duo Push를 활성화하여 21% 또는 32억 건 이상의 인증을 처리합니다. 또한 SMS 문자 및 전화 통화의 감소 추세도 하나의 요인으로 관찰되었으며, 2022년 대비 22% 감소한 4.9%의 인증으로 사상 최저치를 기록했습니다. 피싱 방지 MFA와 더욱 스마트한 액세스 정책의 이점이 중견·중소 기업과 대기업에서 모두 호응을 얻으면서 WebAuthn 및 하드 토큰과 같은 더 안전한 방법이 그 자리를 차지하고 있습니다.

사무실 복귀가 새로운 하이브리드 업무 현실이 됨

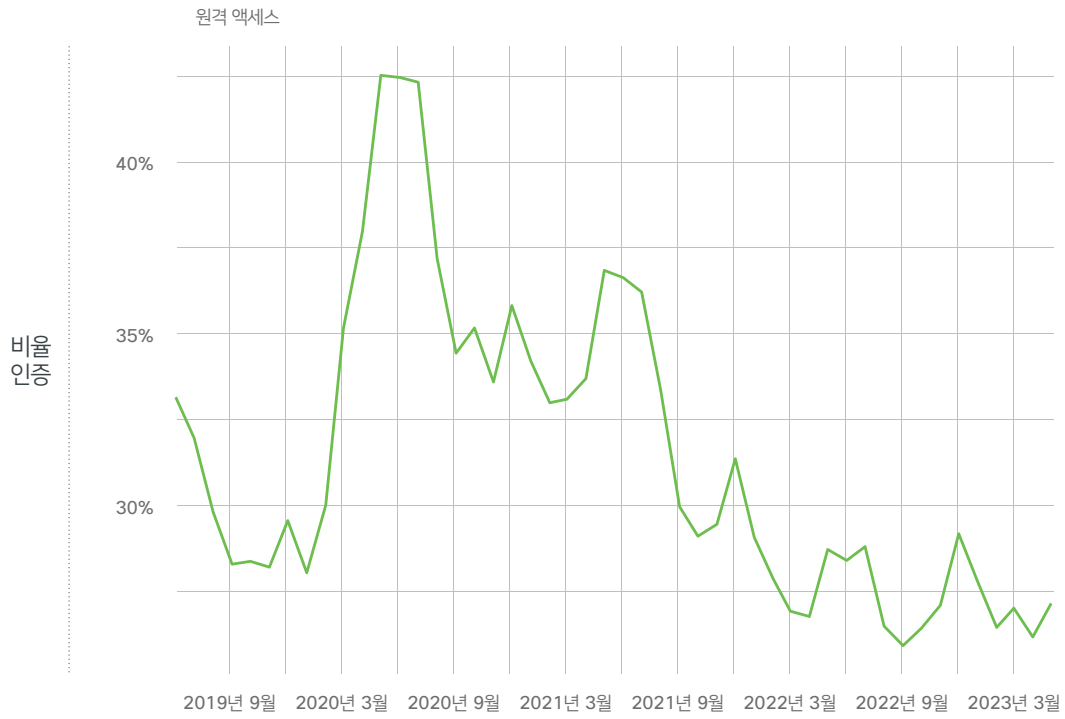
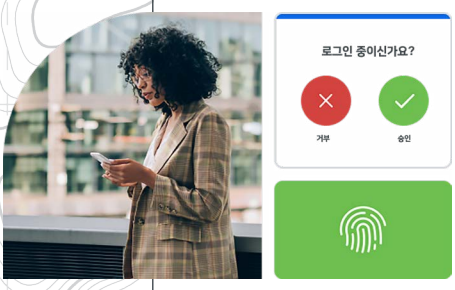


그림 05 원격 액세스 애플리케이션에 대한 인증

원격 액세스 애플리케이션은 사용자가 인터넷이나 로컬 네트워크 연결을 통해 다른 컴퓨터나 네트워크에 원격으로 액세스하고 제어할 수 있도록 하는 소프트웨어 앱입니다. 이러한 앱은 문제 해결, 파일 전송, 원격 관리 또는 원격 위치에서 사무실 컴퓨터의 파일 및 소프트웨어 액세스 등 다양한 용도로 사용됩니다.



지난해 원격 액세스 애플리케이션에 대한 인증 수는 거의 25%에 도달했습니다. 이 수치는 2020년에 정점을 찍었던 팬데믹 이전 수준보다 낮습니다. 그 이후 직원을 사무실로 복귀시키는 회사가 늘어나면서 이 범주의 인증 수는 계속 감소했습니다. 12월과 1월 연휴 기간에는 전반적으로 인증 수가 감소하는 반면, 1분기에는 교육, 소매, 의료 서비스 등 일부 산업에서 인증 수가 급증했습니다.

배경 지식...

출장에서 복귀, 지정된 사무실 정책, 단순한 독감 시즌 등에 따라 예측 가능한 인증 요청이 급격히 증가하거나 감소하기 시작합니다. 직원이 휴가를 가거나, 원격으로 근무하거나, 다양한 일정으로 업무를 수행하면 흐름이 끊깁니다. 이러한 변화로 인해 직원들이 평소 사용하던 업무용 단말기뿐만 아니라 다양한 위치와 디바이스에서 회사 네트워크에 연결하면서 원격 액세스 요청이 급증할 수 있습니다. 따라서 IT 시스템은 혼합되어 유입되는 온프레미스 및 오프사이트 로그인 시도를 처리해야 하고 VPN과 기타 원격 액세스 기술에 대한 의존도가 높아집니다.

또한 계절적 변동으로 인한 수요를 충족하기 위해 비즈니스가 확장되면 임시 직원이 증가할 수 있습니다. 이러한 유입으로 인해 임시 자격 증명을 추가로 만들고 관리해야 하며, 인증 시스템에 새로 입력할 항목도 많아집니다. 시즌이 끝나면 시즌 자격 증명이 취소되므로 그에 따른 유출이 발생합니다.

이러한 차이는 단순히 볼륨만 변경하는 것이 아니라 인증의 특성도 변경합니다. 이러한 시기에는 사이버 위협 위험이 급증하는 경우가 많기 때문에 강력한 보안 조치에 대한 요구도 높아집니다. 따라서 계층화된 보안 접근 방식이 훨씬 더 중요해지며 MFA는 최소 요구 사항으로 포함해야 합니다.

이러한 피크 타임에는 IT 환경의 인증 프로토콜이 탄력적이면서 안전하여 시스템의 무결성을 유지하는 동시에 급증된 다양한 로드를 수용하도록 확장되어야 합니다. IT 직원은 보안 침해 시도를 나타낼 수 있는 비정상적인 활동을 감시하기 위해 경계 태세를 유지하고 있어야 합니다.

공격자로부터 선제 대비

ID 위협 환경은 빠르게 진화하고 있으며 신뢰할 수 있는 ID 공급자가 공격을 받고 있습니다. CISA에 따르면 공격자는 ID 정책 격차를 적극적으로 익스플로잇하여 중요한 애플리케이션에 대한 액세스 권한을 획득합니다. Cisco Secure 준비도 지수 연구[3]에 따르면 증가된 위험에 관계없이 85%의 조직이 최신 공격으로부터 보호할 준비가 되어 있지 않다고 느끼고 있습니다.

공격자들이 만들어내는 공격 유형에 대처하려면 ID 인프라 전반에 대한 가시성이 필수입니다. Duo를 통한 MFA 인증이 눈에 띄게 증가했지만 또 다른 연구에 따르면 시장 전반에 보안 격차가 여전히 존재하며 평균적으로 회사의 계정 중 40%는 MFA가 없거나 MFA가 취약합니다[4]. 특히 변화의 시기에는 강력한 액세스 관리 및 ID 가시성이 매우 중요합니다. 잠시 동안은 적절하게 균형을 맞출 수 있지만 새로운 위협, 변화하는 사용자 행동 및 복잡한 IT 환경으로 인해 중단이 발생할 수 있습니다.

이러한 이유로 최신 보안 이니셔티브에는 "설정한 후에는 신경쓸 필요가 없는" 접근 방식이 아니라 ID, 중요 애플리케이션 및 인적 자원 정보 시스템(HRIS) 전반에 대한 지속적인 모니터링이 필요합니다. 보안 환경이 진화하면서 많은 비즈니스는 최신 공격 표면을 완화하기 위해 Zero Trust 액세스 정책 전략을 채택하고 있습니다. 성숙한 Zero Trust 전략을 구현한 조직은 Zero Trust 전략이 없는 조직보다 보안 탄력성에서 30% 더 높은 점수를 받았습니다[5].

2023년에는 푸시 기반 인증과 문제 없는 사용자를 이용하는 두 가지 특정 유형의 MFA 표적 공격이 확산되는 것을 목격했습니다.

01 **푸시 괴롭힘**

사기성 로그인 시도에 대한 푸시 알림을 여러 번 연속으로 보내 사용자가 푸시를 수락하도록 괴롭히는 공격입니다.

02 **푸시 피로**

지속적인 MFA는 사용자가 로그인 세부 사항에 덜 주의를 기울이게 하여 무심코 푸시 로그인 요청을 수락하게 만든다는 것을 의미합니다.

Duo는 이미 WebAuthn FIDO2 인증을 지원하여 MFA 기반 공격에 대한 가장 강력한 보호 기능을 제공합니다. 하지만 조직 전체에 비밀번호 없는 환경을 구축하는 것은 긴 여정임을 잘 알고 있습니다. 이 보고서의 데이터 기간 동안 모든 Duo 고객이 일반적으로 사용할 수 있게 된 더욱 유연한 스텝업 인증 기능인 Duo Verified Push가 5,600개 이상의 계정에서 활성화되었다는 것은 고무적인 일입니다.

공격자의 기법이 더욱 정교해짐에 따라 다층적인 방어 시스템이 중요해졌습니다.

사용자에 대한 신뢰는 필수적이지만 더 이상 충분하지 않습니다. 외부 벤더와 계약업체가 추가되면 폐쇄적이고 관리되는 엔드포인트 전용 액세스 정책이 더욱 복잡해집니다. 모든 Duo 버전에 제공되는 **Duo Trusted Endpoints**는 조직이 디바이스를 직접 관리할 수 없는 경우에도 보안을 한층 더 강화합니다. 관리자는 관리형 또는 비관리형, 회사 제공, 계약업체 소유, 개인 등 모든 엔드포인트에 대해 신뢰 정책을 정의하고 MFA를 우회할 수 있는 경우에도 공격자의 알 수 없는 디바이스를 중지할 수 있습니다.

마찰 증가로 사용자 채택에 어려움을 겪는 경우가 종종 있습니다. 보안과 생산성의 균형을 맞추는 일환으로 위험 변화를 고려하기 위해 **Duo 기억 디바이스**를 강화했습니다. 사용 중인 디바이스가 인식되면 신뢰가 유지되는 한 안전하게 생성된 디바이스 토큰을 사용하여 인증합니다.

액세스 보안은 위험 수준에 맞춰 조정되어야 하지만 조직은 모든 로그인에 마찰을 더하기 위해 승인을 얻는 데 어려움을 겪을 수 있습니다. Duo의 **위험 기반 인증** 솔루션은 이러한 문제를 해결하여 환경 위험 신호가 위치 변칙이나 알려진 공격 패턴과 같은 잠재적인 위협이 있음을 나타내는 경우에만 더 안전한 방법으로 전환합니다. 보안 팀이 모든 사용자에 대해 **Verified Duo Push**를 활성화하든, 위험 기반 접근 방식을 통해 활성화하든 조직은 위험 수용범위 및 조직의 요구에 따라 액세스 보안 결정을 내릴 수 있습니다.

IT 팀은 ID 보안 프로그램이 강력한 MFA 요소 및 지능형 스텝업과 같은 올바른 툴을 사용하여 강력한 기반 위에 구축되도록 해야 합니다. 이러한 툴과 정책이 마련되면 **ID 위협 탐지 및 대응**(ITDR)을 통해 IT 보안 전문가에게 사전 예방적 툴과 사후 대응적 툴을 모두 제공하여 조직의 ID 보안 태세를 강화할 수 있습니다.

ITDR은 정책의 잘못된 구성, ID 공급자와 HRIS 간의 불일치, 과도한 권한을 사전에 탐지하는 데 도움이 됩니다. 또한 휴면 계정이나 비활성 계정, MFA가 비활성화된 계정과 같은 위험도가 높은 시나리오를 파악할 수 있으며, 이는 2023 Cisco Talos '연례 보고서'[6]에 언급된 추세입니다. 사후 대응적 측면에서 IT 팀은 툴을 사용해 새로운 MFA 디바이스 등록, 위험한 SSO 세션, 슈퍼맨(비현실적인 이동) 로그인, 새로운 디바이스나 위치에서 액세스 등의 의심스러운 활동에 대응할 수 있습니다.

각주:

3. "**시스코 사이버 보안 준비상태 지수**" 참조, 기업의 준비상태가 5가지 핵심 요소에 대한 준비상태와 19개 보안 솔루션의 구축 상태에 따라 Beginner, Formative, Progressive, Mature의 4가지 단계로 분류됨
4. **ID 보안 상태 보고서**(Oort), 섹션 2 "Multi Factor Authentication: Full Coverage Remains Elusive" 참조
5. 시스코에서 발행한 **보안 성과 보고서, Vol 3**에서 더 많은 결과 참조(Renner)
6. **Cisco Talos 연례 보고서** 전문 참조

공격 표면 증가

02

전 세계 MFA 사용의 지속적인 증가

데이터에 따르면 Duo의 다단계 인증 보안으로 보호되는 전 세계 고객 기반이 지속적으로 증가하고 있습니다. 지난 한 해 동안 Duo를 사용한 MFA 인증 수가 **41%**까지 증가했으며, 독일과 같은 국가는 매년 **52.3%**의 인증 증가율을 보이고 있습니다. 아시아 태평양 지역에서는 일본, 필리핀, 호주가 지난 해부터 지속적인 증가를 보였으며, 각각 **28%**, **24.9%**, **16.9%**씩 증가했습니다. 측정 첫 해에 브라질은 2022년 대비 **26.3%** 이상의 MFA 사용 증가를 보이며 세 번째로 높은 인증 증가율을 기록하고 있습니다.

이는 주로 증가하는 사이버 위협에 대한 대응책으로 향상된 보안 조치의 중요성에 대한 인식이 높아지고 있는 추세를 나타낼 뿐만 아니라 GDPR, C5, AgID, HIPAA 등의 국제 컴플라이언스 요구 사항을 반영한 것이기도 합니다.

41%

지난 한 해 동안 Duo를 사용한 MFA 인증의 증가율

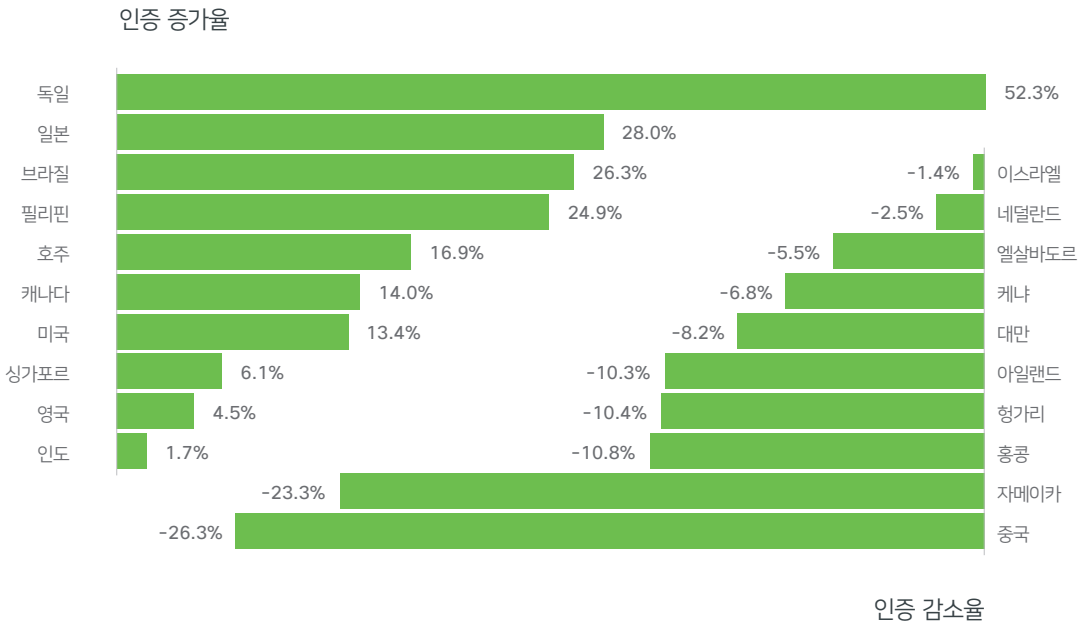


그림 6 액세스 디바이스 IP 주소를 기준으로 인증 볼륨이 증가하거나 감소한 상위 10개 국가

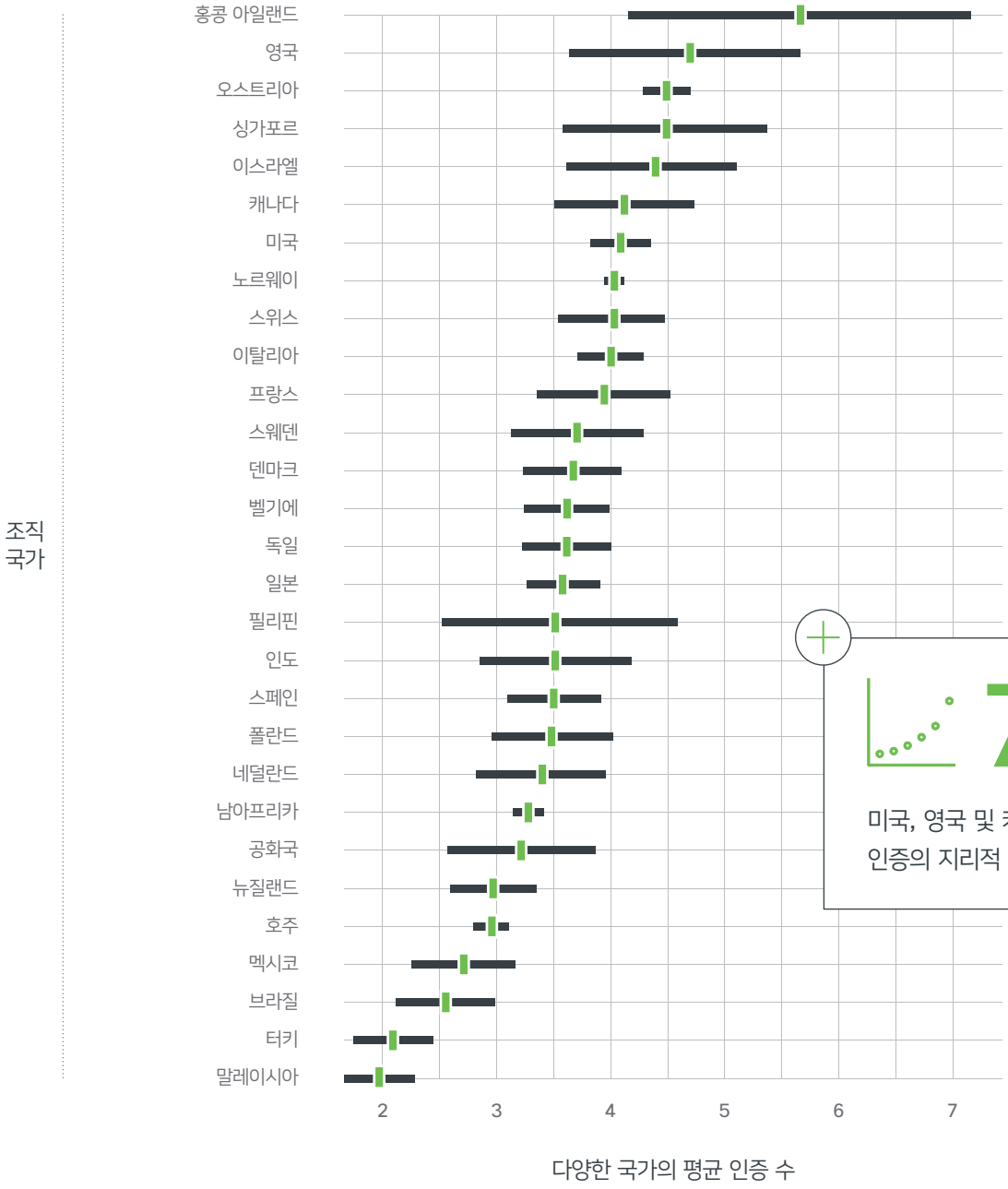


그림 7 특정 국가의 조직이 액세스한 평균 국가 수

그림 7에서는 작년에 확인한, 조직이 운영되는 지리적 다양성에 대한 통계를 다시 살펴봅니다. 특히 홍콩과 같이 조직이 발견될 때 사용자가 인증되는 평균 국가 수를 살펴봅니다. 비즈니스 관심사가 계속 다양해지고 확산되면서 홍콩은 평균 5.6개의 다른 국가에서 가장 높은 평균 인증 확산율을 보였습니다. 미국, 캐나다 및 영국의 조직은 인증이 평균 4개의 다른 국가에서 들어오는 것으로 확인되었는데, 이는 지난해에 확인된 평균 1.5개~1.75개 국가에서 72% 증가한 수치입니다.

국제적으로 분산된 인력으로 인해 더 많은 직원, 계약업체, 클라이언트 및 서드파티가 다양한 디바이스, 네트워크, 운영 체제 등의 다양한 위치에서 조직의 비즈니스 디지털 인프라에 액세스할 수 있게 되어 추가적인 취약점을 유발할 수 있습니다. 더 큰 규모의 네트워크 및 엔드포인트에서 데이터와 리소스에 액세스할 수 있습니다. 이는 'ID가 새로운 경계가 됨' 및 '컨텍스트가 새로운 MFA임'이라는 개념을 지원합니다. ID 보안은 끊임없이 진화하는 문제이므로 조직이 사용자 여정에서 발생하는 모든 문제를 해결하는 것은 어려운 일입니다.

또한 국제적인 입지는 기술 스택의 다양성을 증가시킬 뿐만 아니라 지리적으로 다양한 사용자 기반의 물리적 과제 범위를 확장할 수도 있습니다. 또한 IT 시스템은 혼합 기술 스택과 다양한 데이터 보호 및 개인정보 보호법을 충족해야 합니다. 이로 인해 IT 팀이 처리해야 하는 복잡성이 증가하게 됩니다.

조직 규모와 마찬가지로 글로벌화로 인해 둘 이상의 ID 공급자가 존재할 가능성이 높아집니다. 또한 대규모 조직은 다른 회사를 인수할 수 있으며, 각 회사에는 기존 ID 공급자가 있을 수 있습니다. 조직은 하나의 ID 공급자 아래에 모든 것을 통합하는 대신, 복잡하고 혼란스러울 수 있지만 여러 ID 공급자를 유지하는 것을 선택하기도 합니다.

둘 이상의 ID 공급자(IdP)를 지원할 확률이 높아지면서 ID 관리의 복잡성도 증가합니다. 적절한 보안 조치를 마련하지 않으면 훼손된 자격 증명처럼 ID 기반 공격에 익스플로잇될 수 있는 잠재적인 보안 격차나 취약점이 발생할 수 있습니다.

글로벌 비즈니스 관행에서는 조직이 공격을 탐지, 대응, 보고하는 데 도움이 되는 벤더에 구애받지 않는 더욱 광범위한 액세스 관리가 필요합니다.

ID가 새로운 경계가 됨

ID 보안은 액세스 관리의 핵심 요소입니다. ID 및 액세스 관리(IAM) 시스템은 ID 보안 및 인증을 통해 리소스에 대한 액세스를 효과적이고 안전한 방식으로 관리할 수 있습니다. 따라서 이 보고서 작업을 진행하던 시기에 밝혀진 ID 보안 추세에 대해 잠시 검토하는 시간을 가졌습니다.

ID 보안에서 격차가 발생하는 데는 몇 가지 이유가 있습니다. 일부 회사의 경우 클라우드 마이그레이션에서 메시지가 표시됩니다. 회사가 성장하고 운영을 클라우드로 전환하면서 새로운 IAM 시스템을 도입해야 하지만 이전 IAM 시스템 사용을 완전히 중단하지 않는 경우가 많습니다. 다른 회사의 경우 온프레미스 디렉터리에서 클라우드 기반 디렉터리로 마이그레이션하면서 둘 다 유지하기도 합니다. 세 번째 그룹의 경우 하나 이상의 회사를 인수한 회사로 구성되며 다양한 ID 플랫폼을 지원합니다.

또 다른 요인은 운영 과제 형태로 나타납니다. ID 보안은 IT 기능에 속하는 경우가 많으며 효과적인 보안에 필요한 리소스와 관심을 받지 못할 수 있습니다. IAM 시스템을 관리하고 지속적으로 모니터링하며, 규정 준수를 보장하고, 보안 사고에 대응하려면 기술과 인력에 대한 투자가 필요합니다.

경우에 따라 클라우드 마이그레이션 및 운영 확장을 위해 새로운 IAM 시스템을 도입해야 합니다. 기업 인수 합병, 운영의 글로벌화, 지리적으로 다양한 사용자 기반 등으로 인해 ID 인증 추적이 더욱 복잡해졌습니다.

디지털 혁신에서 ID 보안은 리소스 부족이나 우선순위 지정으로 인해 어려움을 겪을 수 있으며, 일반적으로 보안 기능이 아닌 IT 기능으로 분류됩니다. 적절한 가시성 및 위협 탐지 기능이 없는 ID 인프라는 공격자가 중요한 시스템에 침입할 수 있는 충분한 기회를 제공합니다. 일반적으로 ID는 조직의 IT 팀에서 관리해 왔습니다. ID는 최상위 공격 벡터이므로 ID 팀과 보안 운영 센터(SOC)를 ITDR과 통합하여 모든 사람이 동일한 정보를 파악할 수 있도록 하는 것이 중요합니다.

적절한 가시성 및 위협 탐지 기능이 없는 ID 인프라는 공격자가 중요한 시스템에 침입할 수 있는 충분한 기회를 제공합니다.

Talos 관점

사이버 공격자는 민첩하며 국가 후원을 포함하여 상당한 리소스를 지원받는 경우가 많습니다. 이로 인해 민감한 정보에 액세스하기 위해 신원을 표적으로 삼을 수 있는 지능형 지속 위협이 증가했습니다.

하지만 새로운 일이 아닙니다. 공격자는 수년간 공격 활동에서 ID를 표적으로 삼았습니다. 예를 들어 추가적인 보호 기능이 부족한 온프레미스 ID 디렉터리 또는 VPN은 여러 공격의 희생양이 되었습니다. 늘어난 ID 범위의 관리 또한 공격 표면이 확장되었다는 지표입니다. Talos 사고 대응(Talos IR)에서는 공격자들이 일반적으로 권한 및 액세스 권한이 확장된 벤더 및 계약업체 계정(VCA)을 표적으로 삼는 경우가 반복적으로 확인되었습니다. VCA는 서드파티에 대한 신뢰로 인해 계정 감사 중에 간과되는 경우가 많기 때문에 공격자의 쉬운 표적이 됩니다.

Talos 2023 연례 보고서에서는 유효한 계정에 대한 손상된 자격 증명이 초기 액세스 벡터의 23%를 차지하여 유효한 계정을 두 번째로 일반적인 MITRE ATT&CK 기법으로 사용하는 것으로 관찰되었습니다[7]. 주요 취약점 중 하나는 MFA가 부적절하게 구현되었거나 MFA가 부족하다는 점이지만, 일부 인게이지먼트에서 공격자들은 MFA 피로나 푸시 폭탄 공격을 통해 MFA를 우회할 수 있습니다. ITDR은 유효한 계정 공격과 관련된 위험을 표면화하고 HRIS의 정보를 ID 공급자 및 중요 애플리케이션과 연결하여 쉽게 달성할 수 있는 자격 증명 공격을 완화할 수 있습니다.

23%

유효한 계정의 손상된 자격 증명으로 구성된 초기 액세스 벡터의 비율

ID 확산

조직은 사용자가 동기화되지 않은 여러 시스템에서 관리하는 수많은 계정과 ID를 사용할 때 발생하는 "ID 확산"으로 인해 어려움을 겪고 있습니다. 이는 많은 보안 및 IT 팀에 지속적인 보안 위험 및 운영 과제를 제시합니다.

ID 확산은 점점 더 큰 문제가 되고 있습니다. Talos IR 연구에서는 직원의 개인 디바이스에 저장된 자격 증명과 같이 회사의 가시성 범위를 벗어난 디바이스에서 가져온 자격 증명의 경우 어떻게 훼손되었는지 파악하기가 어려웠다고 지적했습니다. 한 보고서에 따르면 평균적으로 회사마다 회사 데이터에 액세스하는 개인 계정(Gmail, Yahoo, Hotmail, iCloud 등)이 340.5개 있다고 합니다[8]. BYOD 및 경계 없는 업무 문화로 인해 확인되지 않거나 관리되지 않는 직원 ID가 점점 늘어나고 있습니다.

340.5

평균적으로 회사 데이터에 액세스하는 개인 계정 수

각주:

7. **Talos IR 2023 연례 보고서**, "텔레메트리 동향" (6~7페이지 참조)
8. **ID 보안 상태** 보고서(Oort), 섹션 3 "Identity and Access Management: Poor Hygiene Enabling Attackers" 참조

03 디바이스 신뢰 구축

수많은 디바이스에 대한 가시성을 확보하고 보안을 유지하는 것은 여전히 진행 중인 싸움이며, 특히 고등 교육 분야와 같이 다양한 엔드포인트가 있는 조직과 산업에서는 더욱 그렇습니다. 강력한 인증 메커니즘은 보안 프로토콜의 핵심이며, 네트워크에 액세스하는 사용자의 ID를 확인하는 데 필수적인 방어선입니다. 하지만 강력한 인증은 사이버 보안 퍼즐의 한 조각일 뿐입니다.

사용자가 신뢰할 수 있는 디바이스 및 네트워크를 사용하여 기업 데이터에 액세스하도록 하면 또 다른 복잡성이 추가됩니다. 복잡한 공급망 운영, 서드파티 파트너십, 계약업체 디바이스 등이 있는 IT 환경은 관리되지 않는 외부 디바이스와 알 수 없는 엔드포인트의 위험을 초래할 수 있습니다. 이러한 가변성으로 인해 전용 보안 계층이 없으면 가시성과 신뢰를 보장하는 것이 어렵습니다. 강력한 엔드 유저 인증을 사용하더라도 관리되지 않는 네트워크 및 디바이스 보안의 불확실성이 취약점으로 남아 있을 수 있습니다.

이런 맥락에서 ID 중심 보안은 역동적이고 다차원적인 노력입니다. 여기에는 고급 인증, 네트워크 보안 솔루션, 엔드포인트 보호, 지속적인 모니터링, 지식이 풍부하고 성실한 인력을 통합하는 포괄적이고 적응력 있는 전략이 필요합니다.

다양한 디바이스 환경

디바이스 신뢰를 구축하는 시작점은 디바이스의 운영 체제, 사용하는 브라우저, 패치 레벨, 기업 보안 정책 준수 등 디바이스 자체를 포괄적으로 이해하는 것입니다. 모든 디바이스의 보안 태세는 OS 및 브라우저의 현재 상태와 무결성의 영향을 많이 받기 때문에 이러한 이해는 매우 중요합니다. 오래된 소프트웨어에는 익스플로잇될 수 있는 패치되지 않은 취약점이 많기 때문에 문제 없는 디바이스를 네트워크 내에서 트로이 목마로 바꿔버릴 수 있습니다.

디바이스를 신뢰할 수 있는지 확인하려면 IT 및 보안 팀이 다음과 같은 몇 가지 주요 질문에 답변할 수 있어야 합니다.

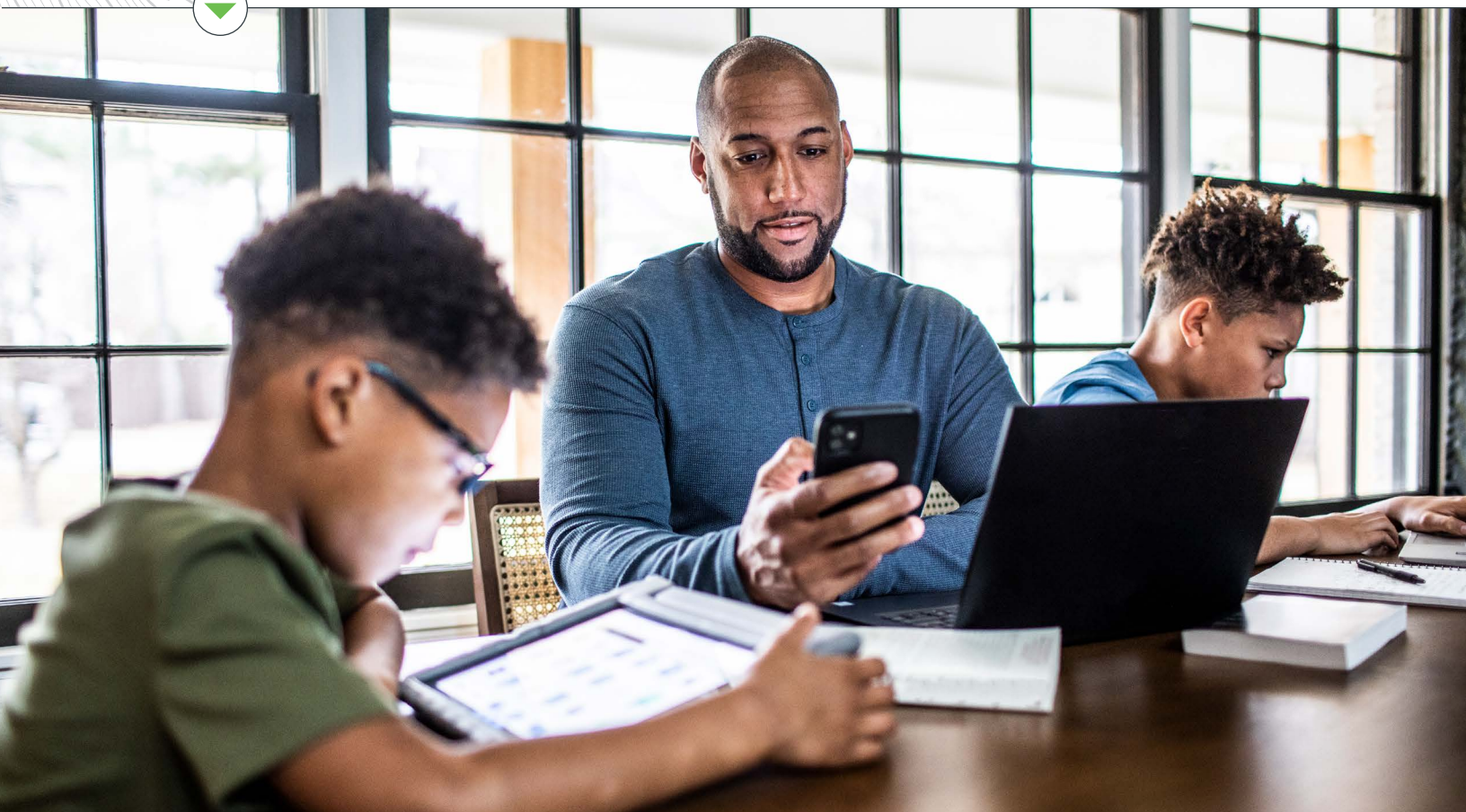
- 권한 없는 애플리케이션이나 소프트웨어가 있나요?
- 디바이스가 암호화되어 있고 보안 설정이 기업의 표준에 따라 구성되어 있나요?
- 디바이스에서 실행되는 OS는 무엇인가요?
- 이 OS는 계속 지원되며 보안 업데이트를 받고 있나요?
- 설치되어 있는 브라우저 버전은 무엇이며, 자동으로 업데이트되도록 설정되어 있나요?

먼저 Duo 고객들이 사용하는 브라우저와 OS에 대해 알아보겠습니다.

모바일 및 비전통적인 운영 체제 플랫폼이 꾸준한 채택률을 보이며, 측정된 인증의 61.8%를 차지하고 있습니다. Windows가 여전히 선두 자리를 지키고 있지만 혼합 IT 환경으로 인해 플랫폼에 구애받지 않는 보안 고려 사항이 더 많아질 수 있습니다.

상위 OS		모바일 OS 사용 현황	
Windows:	38.2%	**iOS:**	71.7%
iOS:	33.4%	**Android:**	28.2%
Mac OS X:	13.7%	**Windows:**	0.0%
Android:	13.1%		
Chrome OS:	1.1%		
Linux:	0.45%		

Windows가 계속 선두를 유지하고 있지만 전체 순위에서는 iOS가 33.4%로 강력한 2위를 차지하고 있습니다. 모바일 범주에서는 Apple이 계속해서 가장 강한 영향력을 행사하고 있고, 가장 가까운 경쟁업체는 28.2%의 훨씬 더 낮은 채택률을 보이는 Android입니다.



계속해서 우위를 점하고 있는 Chrome

Google Chrome은 기업에서 가장 많이 사용하는 브라우저로 계속해서 선두 자리를 지키고 있습니다. 이 선두 자리를 대체할 만한 다른 브라우저는 없는 것으로 보입니다.

주요 브라우저

Chrome:	41.7%	모바일용 **Chrome:**	7.7%	**Firefox:**	3.3%
모바일용 **Safari:**	13%	모바일용 **Safari WebView:**	4.7%	모바일용 **Chrome iOS:**	2.9%
Edge Chromium:	12.6%	**Safari:**	4.6%	**Edge:**	0.1%

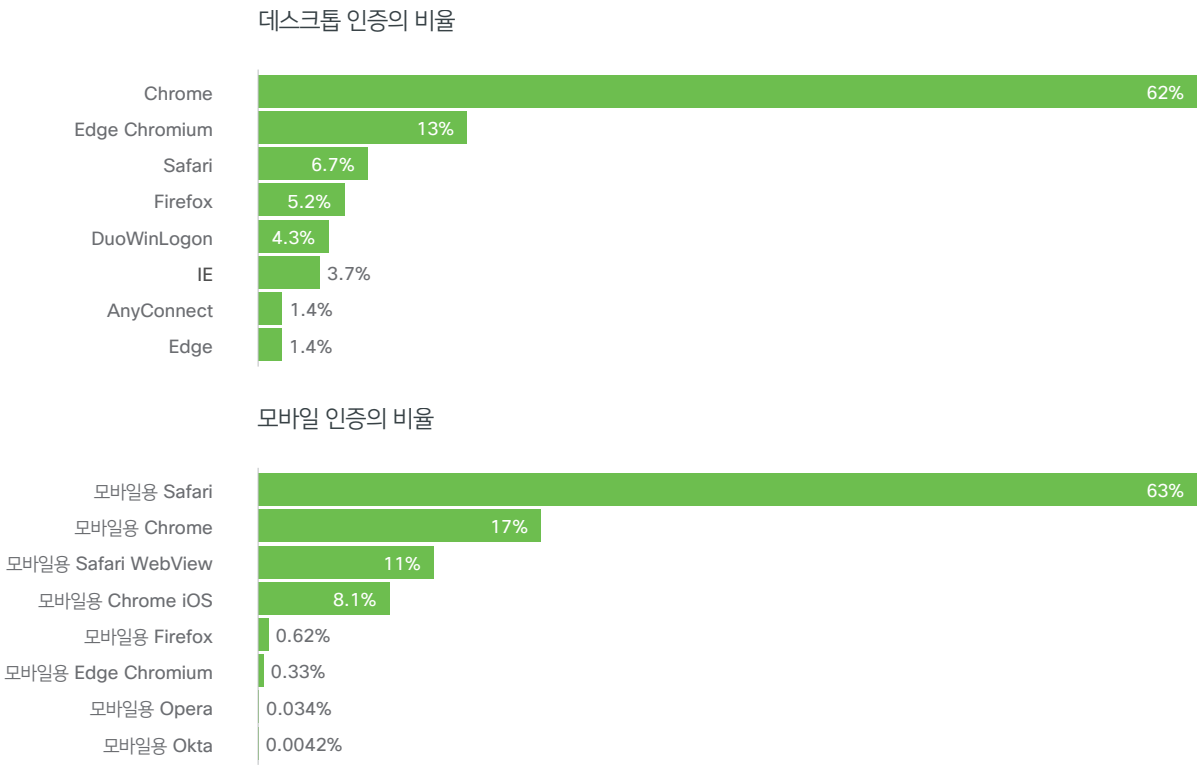


그림 8 인증에 사용되는 다양한 브라우저

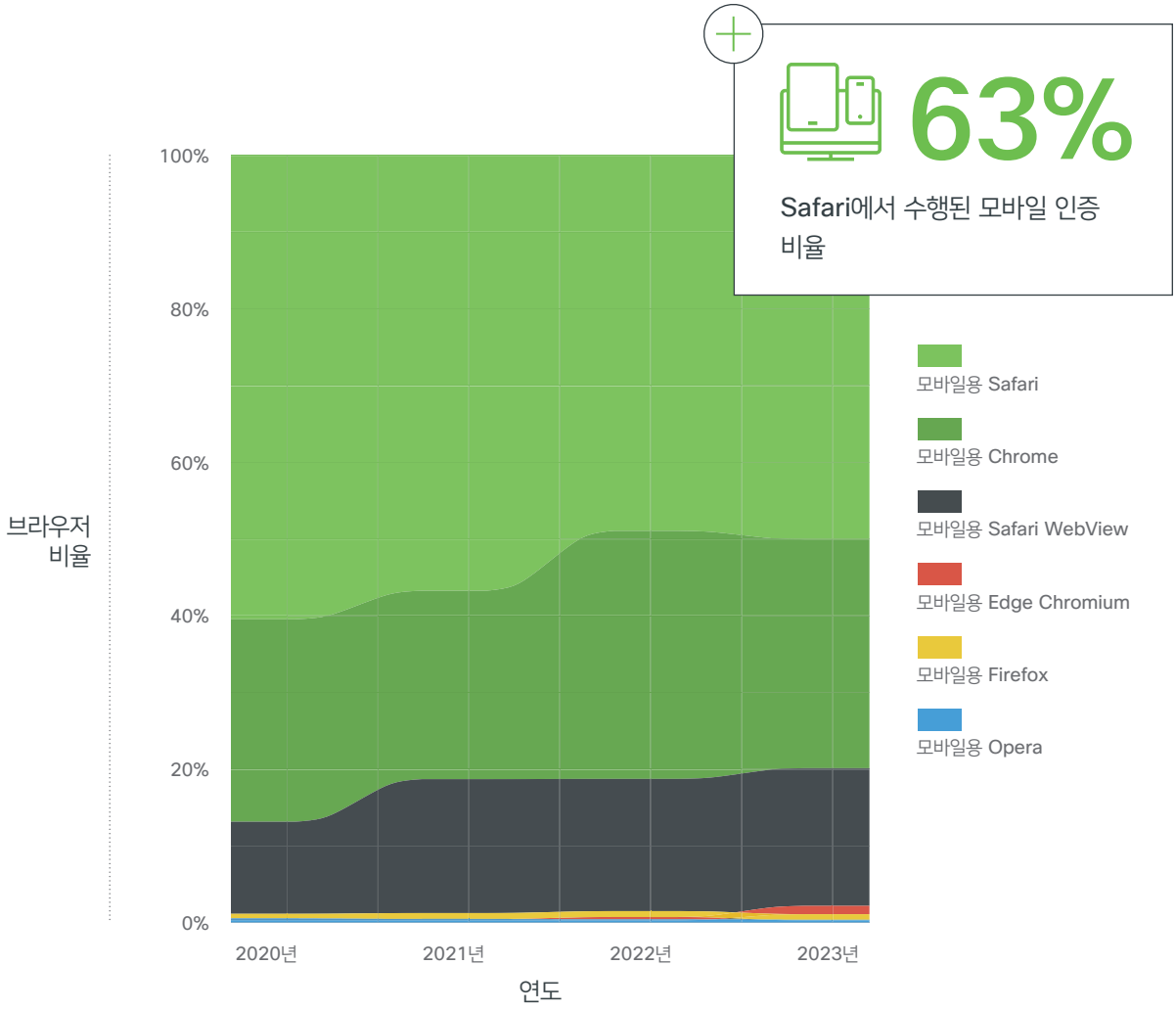


그림 9 사용된 모바일 브라우저의 비율

다양한 시스템과 브라우저를 사용하는 IT 환경에서는 더욱 엄격한 디바이스 기반 정책을 채택해야 할 필요성이 더욱 커졌습니다.

디바이스 가시성: 보이지 않는 부분까지 보호

디바이스 신뢰를 유지 관리하는 것은 정기적인 평가와 업데이트가 필요한 지속적인 프로세스입니다. 여기에는 액세스 권한을 부여하기 전에 설정된 매개변수 내에서 디바이스가 작동하고 있는지 여부를 확인하는 자동화된 컴플라이언스 확인이 포함될 수 있습니다. 예를 들어 더 이상 지원되지 않는 OS 버전을 실행하는 경우처럼 디바이스 성능이 저하되면 검토를 위해 플래그를 지정하거나, 민감한 리소스에 대한 액세스를 차단하거나, 제한적이고 제어된 액세스를 제공하여 잠재적 위험을 완화할 수 있습니다.

이는 Google Chrome과 같은 애플리케이션 및 브라우저가 매주 성능 및 보안 버그 수정을 고려하여 패치 빈도를 높이기 때문에 중요합니다. 하지만 사람들은 얼마나 자주 애플리케이션을 다시 실행하고 업데이트할까요? 측정된 160억 건의 인증 중에서 모바일이 아닌 인증의 62%는 Chrome 브라우저에서 발생한 것으로 나타났습니다. 액세스 디바이스 패치 레벨을 확인하고 사용자가 오래된 디바이스 문제를 자체 해결하도록 요청하는 기능이 더욱 중요해졌습니다.

가시성은 다양한 툴과 사례를 통해 확보할 수 있습니다. 예를 들어 엔드포인트 관리 시스템은 네트워크에 연결된 모든 디바이스의 상태에 관한 실시간 인사이트를 제공하는 대시보드를 제공합니다. 자동화된 인벤토리 툴은 사용 중인 디바이스, 소프트웨어 버전 및 패치 기록을 추적할 수 있습니다. 이러한 모니터링은 지속적인 관리뿐만 아니라 잠재적인 보안 사고에 신속하고 정확하게 대응하기 위해서도 반드시 필요합니다.

오래된 소프트웨어를 사용한 인증

최신 상태가 아닌 경우로 인한 인증 실패

2023년에는 오래된 디바이스로 인한 인증 실패율이 74.7%까지 증가했습니다. 이는 오래된 디바이스를 관리하는 정책이 있는 조직의 비율이 6.9% 감소했다는 사실에도 불구하고 나타난 결과입니다. 아시아 태평양 지역이 가장 높은 순위를 차지했는데, 3.8%의 인증이 오래된 브라우저에서 발생했습니다.

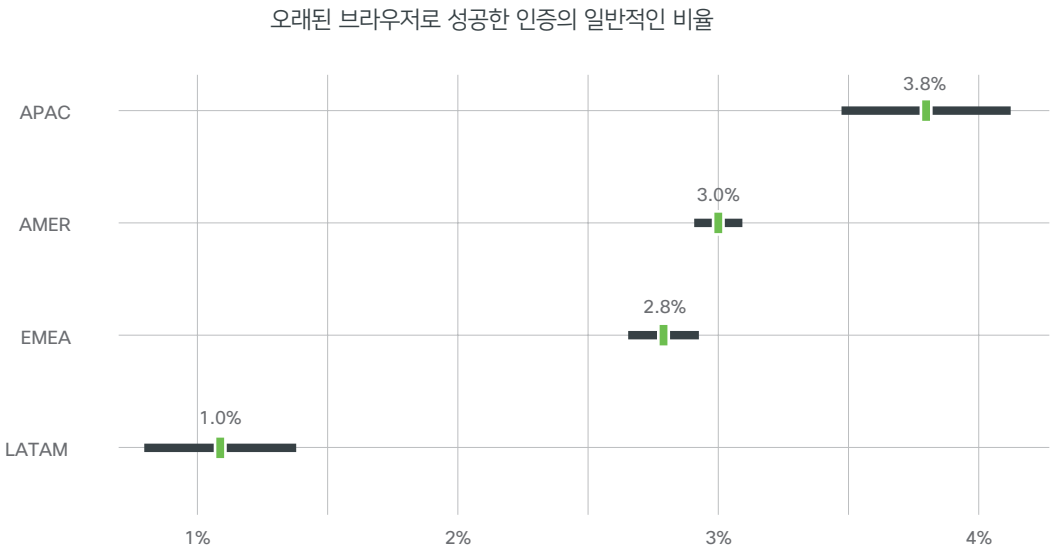


그림 10 오래된 브라우저를 사용하여 성공한 인증의 일반적인(기하 평균) 비율

디바이스 신뢰의 핵심은 기업 애플리케이션과 데이터에 대한 액세스를 요청하는 디바이스에 대해 완벽한 가시성을 확보하는 능력에 있습니다. 끊임없이 진화하는 디지털 위협 환경에서 오래된 소프트웨어에 의존하는 IT 환경 내에서 인증하는 것은 오래된 지도를 보면서 항해하는 것과 비슷합니다.

오래된 소프트웨어에는 패치되지 않은 취약점이 포함된 경우가 많으며, 이는 사이버 공격자에게 숨겨진 공개 백도어와 같습니다. 이러한 취약점은 잘 문서화되어 있으며 퍼블릭 도메인에 유지되면서 쉽게 익스플로잇되어 악의적인 주체가 무단으로 액세스할 수 있는 보물 지도를 제공할 수 있습니다. 이 시나리오에서는 각 인증 이벤트가 도박이므로 보안 결함을 사용하여 자격 증명을 손상시킬 가능성이 높아집니다.

또한 지원 수명이 지난 소프트웨어는 더 이상 개발자로부터 업데이트를 받지 못합니다. 즉, 새로운 위협이 나타나도 인증 메커니즘이 정적으로 유지되고 현대의 사이버 공격자들이 사용하는 정교한 기법에 대해 점점 더 효과가 없어지게 됩니다. 동적 공격에 대해 정적으로 방어하는 것입니다.

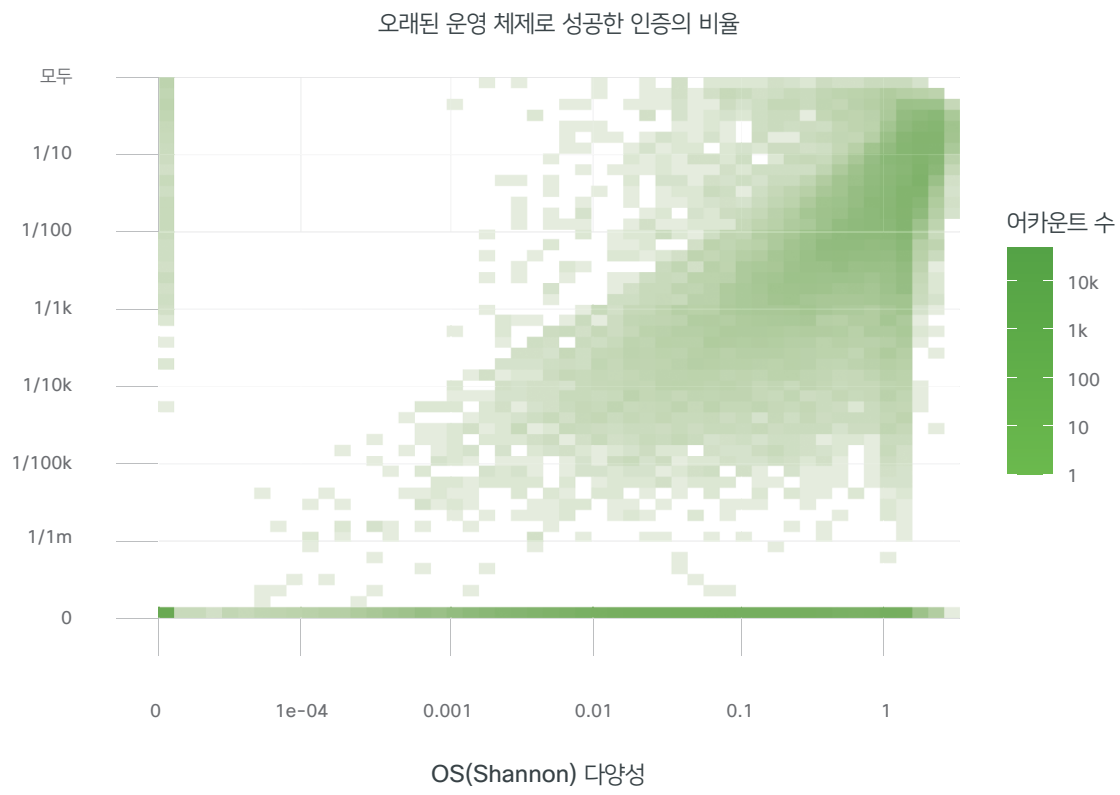


그림 11 OS 다양성 및 오래된 운영 체제를 사용하는 인증 비율

수평축은 조직 내에서 인증에 사용되는 OS가 (생태학적 의미에서) 얼마나 "다양한지"를 보여줍니다. 숫자가 클수록 동일한 비율의 인증을 공유하는 OS가 더 다양하다는 의미입니다. 수직축은 오래된 OS로 수행된 인증의 비율입니다. 아래쪽의 가로줄은 OS를 최신 상태로 유지하는 조직을 나타내고, 왼쪽의 세로줄은 단일 OS만 사용하는 조직을 나타냅니다.

그림 11의 데이터에 따르면 조직에서 인증을 허용하는 운영 체제가 많을수록 인증이 오래된 OS에서 수행될 가능성도 높아진다는 상관관계가 있습니다. 이는 IT 환경이 확장되면서 빠르게 현실이 되고 있습니다.

오래된 인증 소프트웨어를 사용하는 것은 안전망 없이 줄타기를 하는 것과 같습니다. 보안 침해, 데이터 도난 및 그에 따른 많은 결과에 대한 명분을 주는 것입니다. IT 환경의 보안과 효율성을 유지하려면 디지털 위협 환경에 맞춰 진화하는 강력한 최신 디바이스 신뢰 방법에 투자하여 가시성을 제공하고 문제를 해결할 수 있도록 해야 합니다. 이는 단순한 모범 사례가 아니라 디지털 시대의 책임 있는 IT 관리의 기본 원칙입니다.

69%

암호화 사용 증가율

암호화 및 방화벽…

하이브리드 업무 모델을 사용하는 조직은 VPN(Virtual Private Network) 사용, 엄격한 방화벽 정책 적용, 데이터 암호화 시행, 안전한 홈 네트워크 설정 등도 고려해야 합니다. Duo Endpoint Health를 검토했으며, 특히 조직이 일반적으로 다양한 보호 조치의 사용을 늘리거나 줄이는지 알아보고자 했습니다. 조직별로 보면, 평균적으로 조직의 암호화 사용 비율이 69% 증가한 것으로 나타났습니다.

기업의 디바이스 예방 조치는 설정한 후에는 신경 쓸 필요가 없는 정책이 아니라 지속적으로 진화하는 요구 사항입니다. 이와 같은 책임은 디바이스의 단종 프로세스까지 확장되어 모든 데이터가 안전하게 지워지고 보안 위협을 초래하지 않는 방식으로 디바이스가 폐기되도록 합니다. 마찬가지로 사용자 액세스 수준도 불필요하거나 과도한 권한을 완화하도록 조정해야 합니다. 정기적인 감사와 컴플라이언스 확인을 통해 디바이스 및 ID 예방 조치 관행이 준비되어 있을 뿐만 아니라 효과적으로 시행되고 업데이트되는지 확인합니다.

다른 디바이스 속성 중에서도 특히 운영 체제와 브라우저를 지속적으로 관리하고 모니터링하여 조직은 강력한 보안 태세를 시행하고 맹목적으로 신뢰가 부여되는 것이 아니라 검증 가능하고 규정을 준수하는 디바이스 동작에 기반하도록 할 수 있습니다.

강력한 정책 제어

04

이전 섹션에서는 조직이 관리해야 하는 해결되지 않은 위험과 취약점이 누적된 보안 부채라는 중요한 문제를 살펴보았습니다. 보안 부채는 오래된 소프트웨어, 레거시 시스템, 기술 수정사항, 보안 패치 적용 지연 등 다양한 원인으로 인해 발생할 수 있습니다. 강력한 보안 태세를 유지하고 잠재적 보안 침해에 대한 조직의 노출을 최소화하려면 이러한 부채를 줄이는 것이 필수적입니다.

보안 부채를 완화하는 가장 효과적인 전략 중 하나는 포괄적인 위험 관리입니다. 여기에는 조직의 IT 인프라 내 취약점 식별, 평가 및 우선순위 지정이 포함됩니다. 조직은 가장 큰 위험이 어디에 있는지 파악함으로써 가장 시급한 보안 문제를 먼저 해결하기 위해 리소스와 노력을 더욱 효과적으로 할당할 수 있으며 이를 통해 전반적인 보안 부채를 줄일 수 있습니다.

인증 실패 경험을 통해 배우기

정책 데이터를 검토하는 과정에서 주목할 만한 몇 가지 결과를 발견했습니다. 더욱 강력한 인증 방법으로 전환하는 과정에서 Duo Push 기반 인증이 전체 글로벌 정책의 99.3%를 차지했습니다. 모바일 1회성 패스코드는 정의된 정책의 91.4%를 차지했습니다. WebAuthn이 글로벌 정책의 69.2%를 차지한다는 점은 더욱 흥미로운 결과 중 하나였습니다.

실패한 인증을 측정하는 것도 중요합니다. 측정된 모든 인증 중 5%가 실패한 인증인 것으로 확인되었습니다. 데이터를 자세히 살펴본 결과, 실패한 인증의 28%는 시스템에 등록하지 않은 사용자에 의해 발생했다는 사실을 알아냈습니다.

69.2%

더 강력한 인증 방법을 위한 유망한 움직임인 Webauthn이 포함된 글로벌 정책의 비율

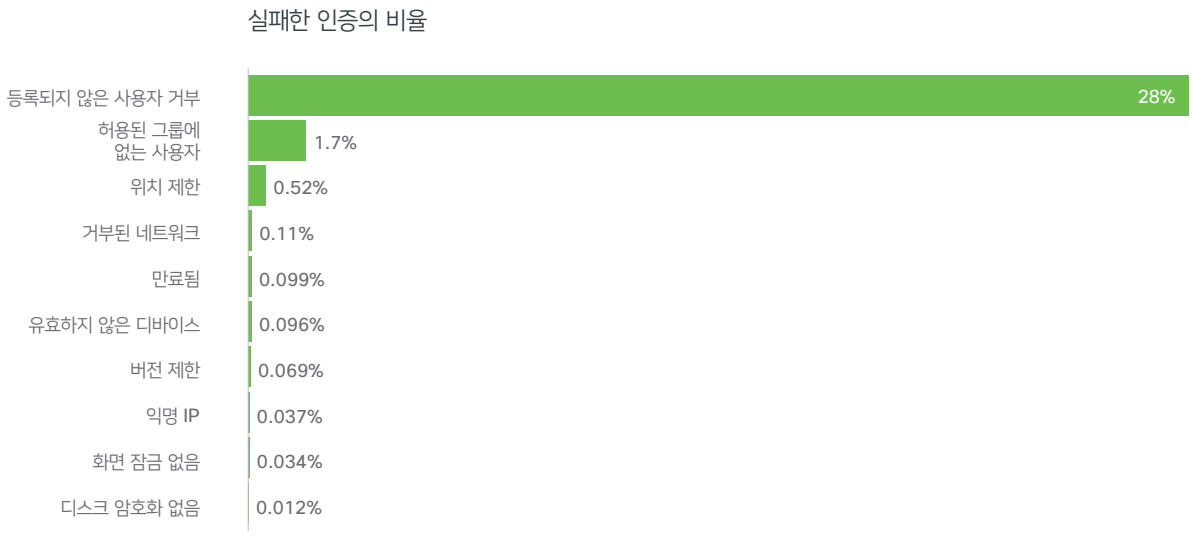
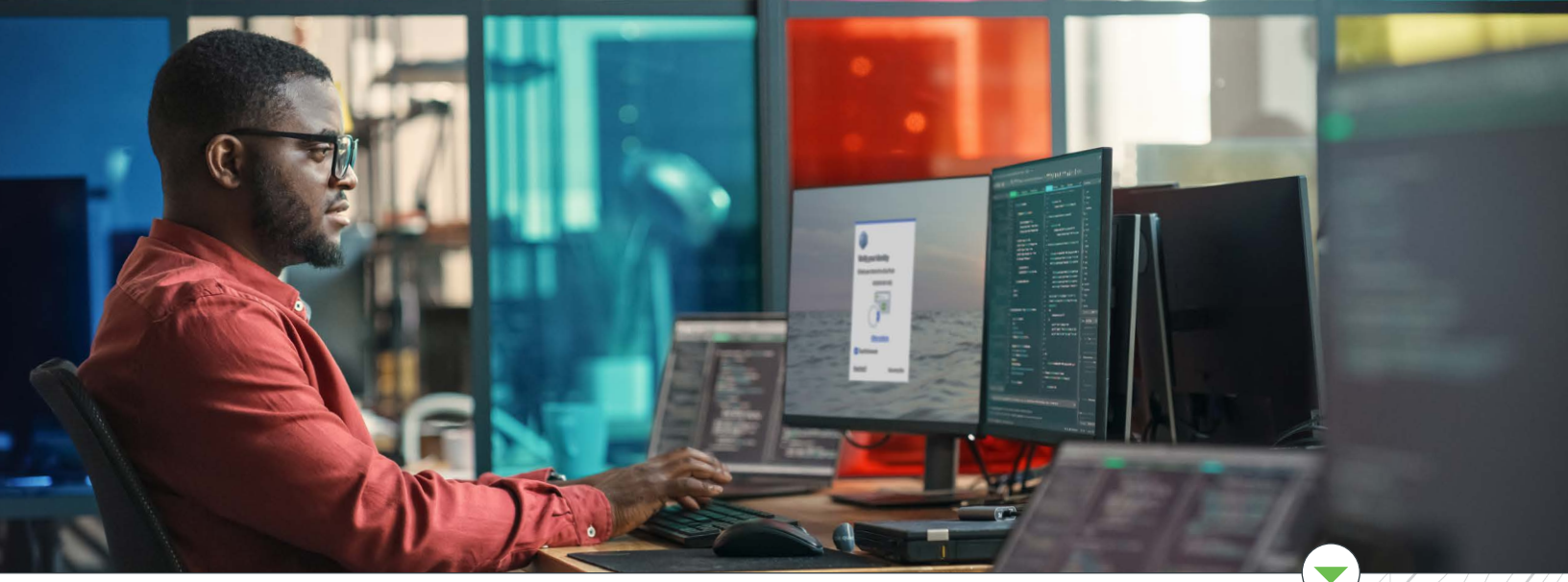


그림 12 인증 실패 원인의 비율



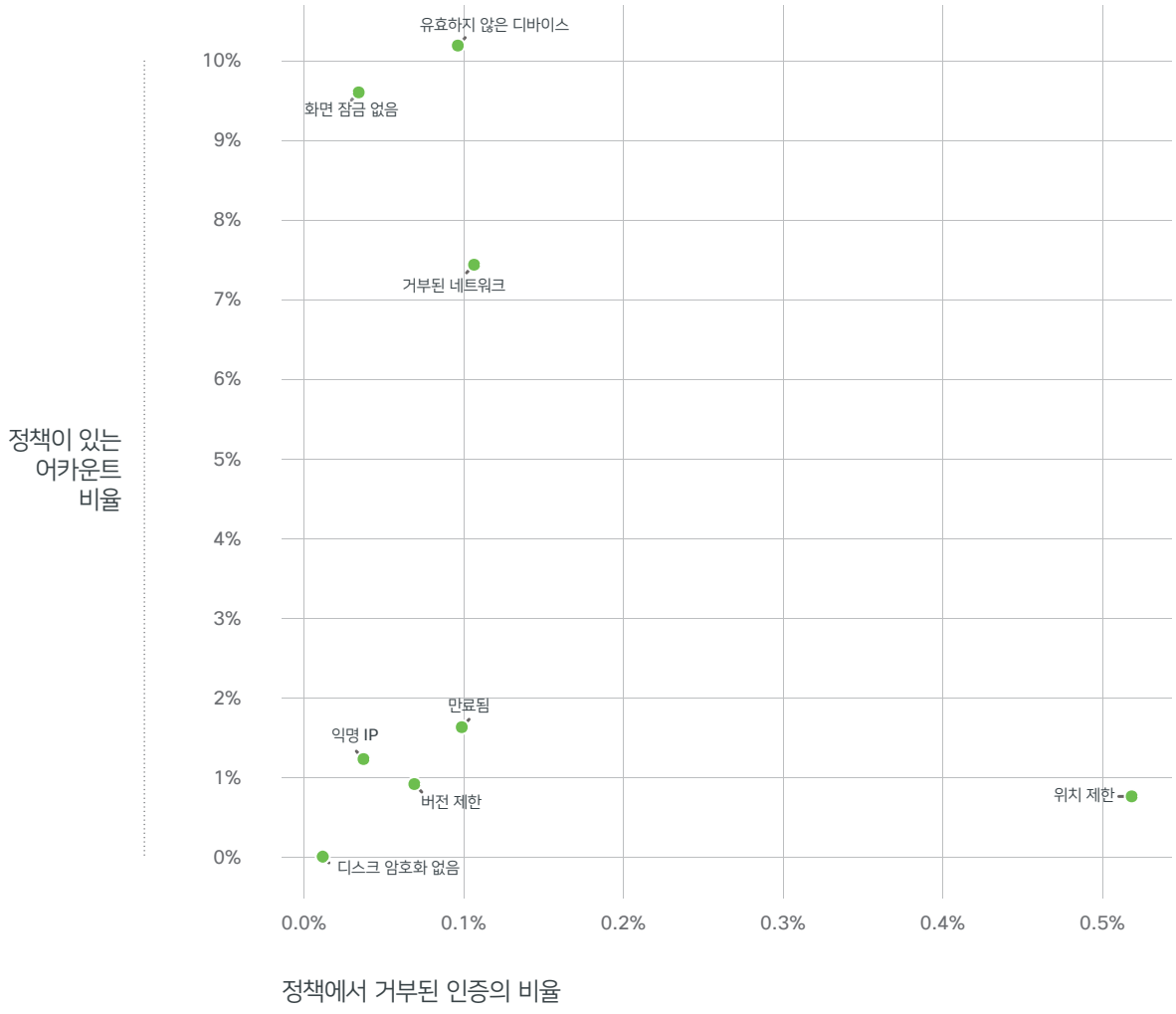


그림 13 인증 실패 원인의 비율

여기에서 위치 관련 정책을 보유한 조직은 **1%**도 안되지만 실패의 상당 부분을 차지하고 있음을 알 수 있습니다. 사용자 등록으로 발생한 실패를 제거하면 정책 설정의 영향을 받는 실패한 인증을 확대할 수 있습니다.

강력한 디바이스 기반 정책의 이점

이 위험 감소 전략의 초석은 환경의 모든 에셋에서 일관된 보안 정책을 구현하는 것입니다. 디바이스 기반 정책은 위치나 사용자에 관계없이 조직 내 모든 디바이스에 적용되는 일관된 보안 프레임워크를 제공하기 때문에 특히 중요합니다. 이러한 정책은 강력한 인증 조치 시행, 정기적인 패치 및 업데이트 적용, 방화벽 및 안티바이러스 소프트웨어 구성, 사용자 권한 관리 등을 포함하여 다양한 측면의 디바이스 보안을 제어할 수 있습니다.

일관된 디바이스 기반 정책은 다음과 같은 여러 가지 이유로 이점이 있습니다.

일관성: 모든 디바이스가 동일한 보안 표준을 준수하도록 보장하므로 공격자가 악용할 수 있는 보안 체인의 취약한 링크를 차단하는 데 도움이 됩니다.

확장성: 조직이 성장함에 따라 도입될 수 있는 새로운 디바이스에 수립된 정책이 자동으로 적용되므로 규모에 따라 보안을 관리하기가 더 수월해집니다.

컴플라이언스: 조직은 디바이스 기반 정책을 통해 모든 디바이스가 업계 표준 및 법률을 준수하도록 하여 벌금 및 기타 처벌의 위험을 줄임으로써 규정 요구 사항을 충족할 수 있습니다.

자동화: 이러한 정책은 대부분 자동으로 시행되므로 수동 개입의 필요성과 그에 따른 인적 오류가 줄어듭니다.

가시성 및 제어: 일관된 정책을 구현하면 정책 위반을 더 쉽게 탐지하고 해결할 수 있으므로 디바이스 보안의 모니터링 및 제어에 도움이 됩니다.

보안 부채를 줄이기 위한 상위 3가지 정책 그룹

보안 부채를 줄이기 위한 노력은 복잡하고 다차원적이지만 이러한 노력의 기반은 포괄적인 디바이스 기반 정책의 일관된 적용에 있습니다. 이러한 접근 방식은 보안 부채를 근본적으로 해결하여 위험을 줄이고 더욱 안전하고 탄력적인 조직 환경을 조성합니다.

액세스 디바이스와 보안 정책 간의 상호 작용은 조직의 사이버 보안 프레임워크에서 핵심적인 측면입니다. 기업 리소스에 액세스하려는 디바이스가 네트워크에 진입하기 전에 특정 보안 표준을 충족하는지 확인하기 위해 엄격한 보안 정책이 마련되어 있습니다. 디바이스가 규정된 이러한 기준을 충족하지 못하면 조직의 디지털 에셋 보호를 목표로 하는 일련의 자동화된 대응이 트리거됩니다.

Duo의 데이터에 따르면, 디바이스 기반 정책을 구현하는 조직은 안전하지 않은 것으로 간주되는 위치에서 시도하는 액세스, 그리고 출발 위치가 될 수 없는 곳에서 시도하는 액세스를 가장 흔히 차단합니다. 또한 조직은 유효하지 않고 오래된 디바이스, 그리고 화면 잠금이나 디스크 암호화 기능이 없는 디바이스를 차단하는 정책을 설정하기도 합니다. 이는 디바이스를 보호하고, 다른 사람이 데이터를 보지 못하도록 데이터 전송을 차단할 수 있는 간단한 보안 조치이기 때문입니다.

복잡성은 줄이고 보안 적용 범위는 늘리는 데 도움이 되는 3가지 정책 유형은 다음과 같습니다.

01

첫 번째로, **지리적 제한**은 일반적인 보안 조치입니다. 특히 데이터 상주 및 주권을 지정하는 법률이나 기업 정책에 의해 규제되는 민감한 데이터와 관련된 시나리오에서 사용됩니다. 사용자가 허용 목록에 지정되지 않은 위치에서 시스템에 액세스하려고 시도하면 보안 프로토콜이 즉각적으로 개입하여 인증이 실패하게 됩니다. 이 지리적 제한은 국제 사이버 범죄자의 무단 액세스를 포함하여 다양한 위협을 효과적으로 억제합니다.

연구 결과에 따르면, 많은 조직이 지역 기반 정책을 구현하는 데 필요한 조치를 취하지 않습니다. 실제로 지난 해에는 특정 지리적 위치를 거부하는 정책을 사용하는 조직의 비율이 2020년 이후 20% 감소한 것으로 보고되었습니다. 2023년에는 96.4%의 조직에 위치 관련 정책(2FA 허용, 거부 또는 필요)이 없었습니다. 그러나 지리적 위치 거부를 사용하는 기업 중에서 91%는 러시아나 중국 중 하나를 차단하고, 63%의 조직은 두 국가를 모두 차단합니다.

96.4%

위치 관련 정책이 없는 조직의 비율

시간 경과에 따른 국가 거부율

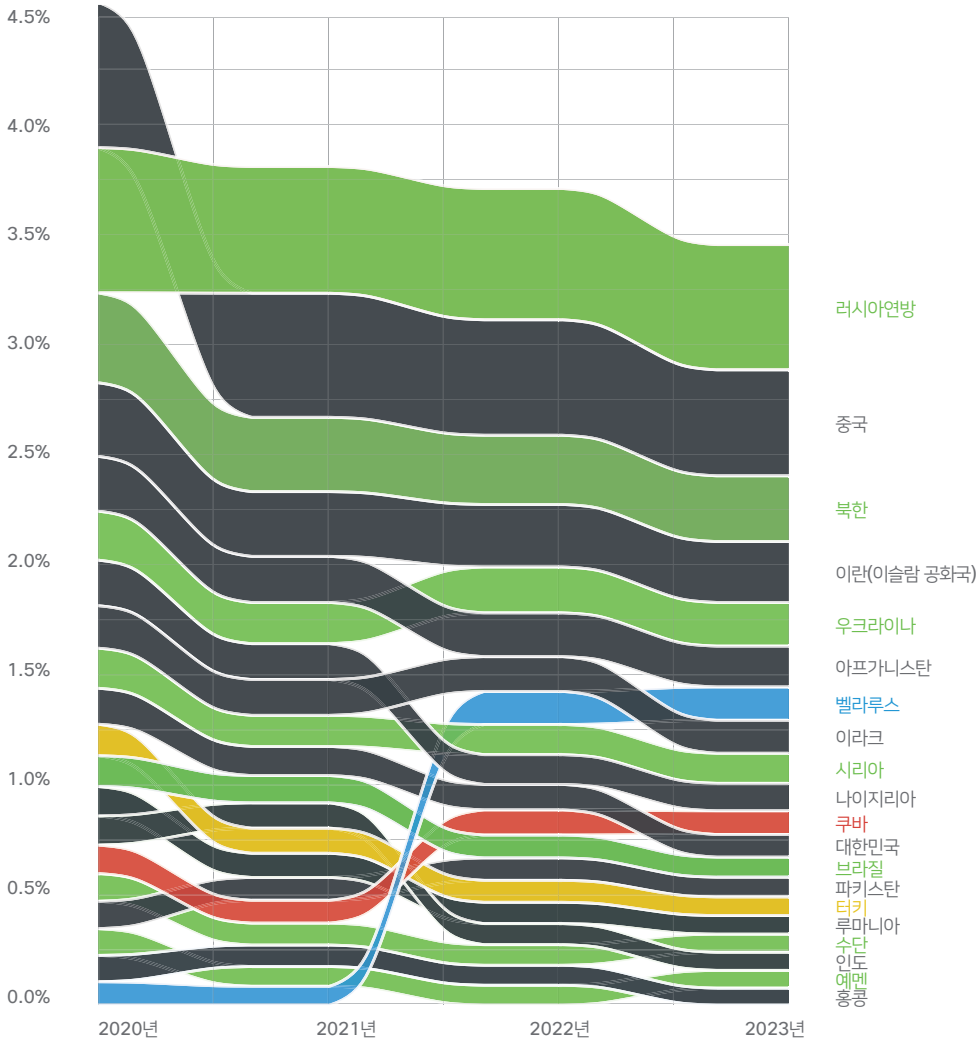


그림 14 특정 국가에 초점을 맞춘 거부 정책을 사용하는 계정의 비율

02

두 번째로, **유효하지 않거나 오래된 디바이스**의 사용은 심각한 위험을 초래합니다. 더 이상 지원되지 않거나 최신 보안 패치로 업데이트되지 않은 디바이스에는 사이버 공격자가 익스플로잇할 수 있는 취약점이 가득한 경우가 많습니다. 보안 정책은 운영 체제 버전, 설치된 보안 패치 및 기타 중요한 보안 구성을 포함하는 보안 태세를 기반으로 이러한 장치를 탐지하도록 설계되었습니다. 이러한 영역 중 부족한 부분이 있는 디바이스가 발견되면 사용자의 로그인이 금지되거나 현재 보안 표준을 준수하도록 디바이스를 업데이트하라는 메시지가 표시될 수 있습니다.

예를 들어 모바일용 Safari는 성공적인 인증에 사용될 가능성이 높지만 오래되거나 단종되었을 가능성도 높습니다. 그림 16에서는 대부분의 계정에서 "최신" 업데이트로 작동하는 브라우저가 20~40%에 불과하다고 보고합니다.

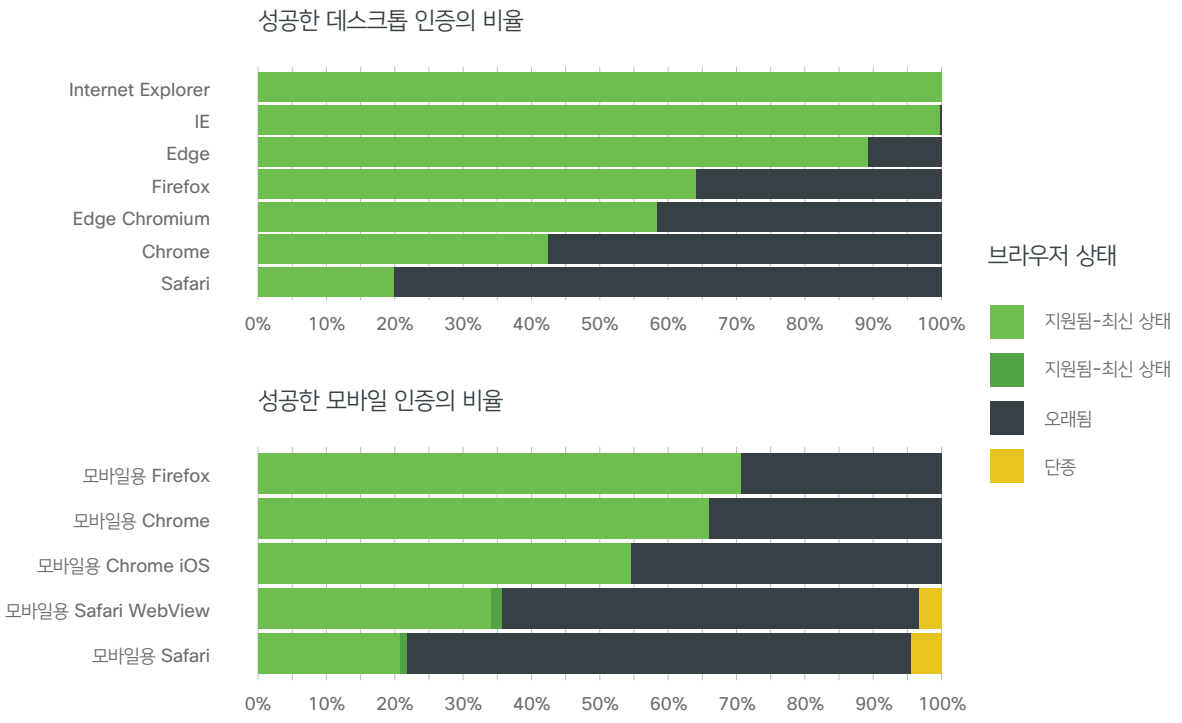


그림 15 브라우저 및 브라우저 업데이트 상태별 인증 비율

모바일용 Safari는 모바일 인증의 가장 큰 비율을 차지하지만 최신 상태일 가능성이 가장 낮은 모바일 브라우저이기도 합니다.

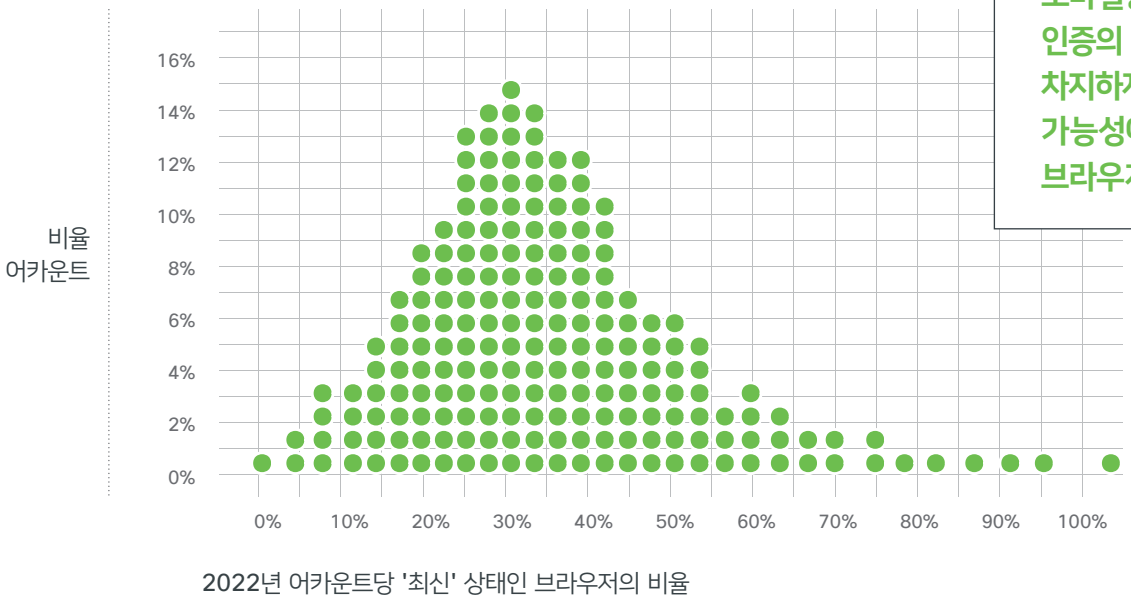


그림 16 계정 내 최신 브라우저의 비율

03

세 번째로, 사용자 그룹별 또는 애플리케이션 수준별로 세분화된 액세스 정책은 **최소 권한 액세스**를 위한 토대를 마련합니다. 오늘날 조직은 서드파티 에코시스템에 의존하여 중요한 비즈니스 기능을 보완하고 지원합니다. 규정 요구 사항 외에도 알 수 없는 게스트, 휴면 또는 고아 계정이 있으면 관리 오버헤드가 추가되고 민감한 리소스에 대한 무단 액세스의 벡터가 될 수 있습니다. 조직은 계정을 관리하고 계정이 액세스할 수 있는 항목을 제한하는 정책 및 절차를 구현해야 합니다. 여기에는 강력한 다단계 인증 시행, 정기적인 게스트 계정 검토 및 감사, 더 이상 필요 없는 계정 비활성화 등이 포함될 수 있습니다.

ID 보안 상태 2023 보고서에 따르면, 평균적인 조직에는 비활성 계정이 많이 있으며, 이는 전체 ID의 24% 이상에 해당합니다. 이러한 계정은 매월 500건이 넘는 공격을 경험합니다. 사용자 기반에 복잡성을 더하는 것은 전체 ID의 3.24%를 초과하는 게스트 계정입니다.

평균적인 조직에서는 매년 비활성 계정에 대한 공격이 500건 넘게 확인됩니다.

이러한 정책을 효과적으로 적용하려면 조직은 직원 교육 및 인지 프로그램에도 투자해야 합니다. 결국 가장 정교한 정책도 인간의 실수로 인해 훼손될 수 있습니다. 조직은 게스트 계정과 관련된 잠재적인 위험과 신뢰할 수 있는 외부 사용자에게만 액세스 권한을 부여하는 것의 중요성에 대해 사용자를 교육해야 합니다. 정기적인 교육 세션, 시뮬레이션 및 보안 훈련을 통해 모범 사례를 뿌리내리며 보안 위협을 사전에 식별하고 대응할 수 있는 경계심이 강한 인력을 만들 수 있습니다.

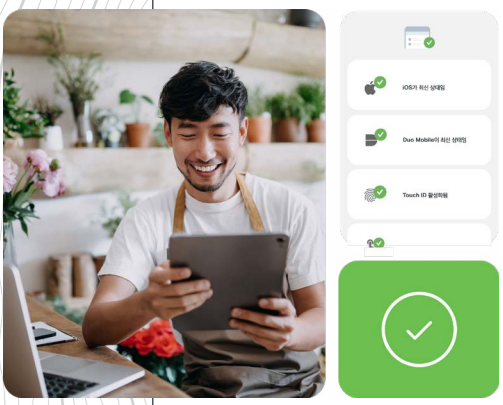
이러한 엄격한 접근 제어는 사용자에게 불편을 주기도 하지만, 사이버 공격이 점점 더 정교해지는 시대에 필요한 방어책입니다. 규정을 준수하는 디바이스, 그리고 더 나아가 해당 사용자만 조직의 시스템과 상호 작용할 수 있도록 하여 기업 데이터 및 서비스의 무결성, 기밀성 및 가용성을 유지합니다.

맺음말

ID 보안의 미래

무분별한 ID 확산이 취약점을 조성합니다. 그런데 기존의 ID 인프라는 보안이 아닌 IT 운영을 염두에 두고 구축되었습니다. ID와 보안 환경이 통합되고 있지만 대부분의 대규모 조직에서 보안 팀은 계속 IAM 팀과 별개로 작업하고 있습니다. 인재 부족으로 인해 조직의 보안 유지가 더욱 어려워지고 있습니다. 중소 규모 조직에서 IT 부서는 소수의 사람들이 수많은 업무를 처리하는 곳으로, 보안 팀이 없을 수도 있습니다. ID 위협 탐지 및 대응과 같은 새로운 보안 기술을 통해 ID와 보안 팀 간의 격차를 해소할 수 있습니다.

운영상의 문제 외에도 조직은 인적 자원 제약 문제, 즉 ID 관리를 사람에게 의존하는 문제와 씨름하고 있습니다. ID 보안은 복잡하며 다음과 같은 여러 가지 요소를 관리해야 합니다.



사용자 ID: 특정 사용자를 나타내며 일반적으로 인증을 위한 고유한 자격 증명과 연결됩니다.

디바이스 ID: 고유하게 식별되고 사용자와 연결될 수 있습니다. 디바이스의 상태와 신뢰도는 사용자가 특정 리소스에 액세스할 수 있는 능력에 영향을 미칠 수 있습니다.

속성: 사용자의 역할, 위치, 부서 등 ID의 속성입니다. 속성을 사용하여 액세스 정책을 결정하고 시행할 수 있습니다.

권한: ID에 부여된 권한 및 액세스 권한으로, ID가 액세스할 수 있는 리소스와 수행할 수 있는 작업을 결정합니다.

IAM 예방 조치가 취약하면 조직의 ID 공격 표면이 늘어나고 공격자에게 기회가 제공될 수 있습니다. 디바이스, 속성, ID, 권한 간에 더 많은 관계가 형성될수록 어떤 ID가 어떤 작업을 수행하는지 확인하고 추적하는 것이 점점 더 어려워집니다.

여러 소스의 ID 관련 데이터를 통합하거나 상황에 맞는 상태 정보를 IT에서 SOC로 전달할 수 있는 솔루션이 없으면 사고 조사도 어렵습니다. 직원, 계약업체, 서비스 계정 등을 포함하여 잘못 구성되고 사용되지 않는 계정에 대한 가시성도 중요합니다.

액세스 관리와 함께 ID 위협 탐지 및 대응 기능을 갖추는 것이 필수 조건이 되고 있습니다. 동시에 이러한 기능은 ID 기반 공격의 성공 가능성을 최소화하는 동시에 ID와 애플리케이션 전반에 전체적인 적용 범위를 제공하는 데 도움이 될 수 있습니다.

ID 기반 공격을 더 효율적으로 해결하려면 IAM 애널리틱스가 이러한 솔루션에 내재되어 있어야 합니다. 이러한 방식으로 IT 관리자는 고객의 전체 엔터프라이즈 스택에 걸쳐 취약한 인증에서 강력한 피싱 방지, 비밀번호 없는 다단계 배포로 마이그레이션하여 모든 보안 격차를 신속하게 해결할 수 있습니다.

컨텍스트가 새로운 MFA임

데이터가 가장 중요하지만 컨텍스트도 중요한 환경에서 강력한 액세스 관리는 기업 보안을 지속적으로 강화하는 데 그치지 않고 보안을 재구성합니다. 비밀번호 의존 시스템의 내재된 취약점을 해결하고 끊임없이 진화하는 위협 환경에 대해 더욱 강력하고 동적인 방어를 구축합니다.

세부적인 로깅 및 알림 메커니즘은 노이즈를 이해하는 데 매우 중요합니다. MFA를 통해 인증을 시도하면 두 번째 요소 또는 세 번째 요소가 실패할 경우 알림을 트리거하여 실시간 위협 탐지를 제공하고 즉각적인 대응을 가능하게 합니다. 따라서 보안 침해와 탐지 사이의 간격인 "체류 시간"을 크게 줄일 수 있으며, 이는 보안 사고로 인한 손상을 완화하는 데 매우 중요합니다.

잘 모르는 복잡성을 탐색할 때 취해야 할 단계가 이해하기 쉽지만 구현하기 어려울 수 있다는 것을 알고 있습니다. 사이버 위협이 점점 더 복잡해지고 정교해짐에 따라 IAM 모범 사례 채택은 현대 조직의 에셋, 평판 및 미래를 보호하는 데 필수적인 보안 프로토콜의 진화로 자리를 잡았습니다.

권장 사항:

- 조직 전체에서 **강력한 MFA**를 채택하고 권한 있는 계정에 대해 FIDO2 보안 키와 같은 피싱 방지 MFA만 요구하는 방향으로 나아가고 있습니다.
- 푸시 괴롭힘 및 푸시 피로 공격을 무력화하고 조직을 **비밀번호 없는 액세스**로 안내하는 **Verified Duo Push**를 활성화합니다.
- 관리되거나 관리되지 않는 **신뢰할 수 있는 디바이스**에만 기업 리소스에 대한 액세스 권한이 부여되도록 합니다.
- 사용자 생산성을 방해하지 않는 지능형 요소 스텝업을 통해 조직의 위험 수준과 중점 요소를 고려하는 데이터에 입각한 사용자 **인증 정책**을 설정합니다.
- 최신 **SSO(Single Sign-On)** 솔루션을 정책 시행 툴로 활용하여 각 애플리케이션에 Zero Trust 및 최소 권한 액세스 원칙을 적용합니다.
- **Duo 위험 기반 인증**과 같이 사용자 및 디바이스 텔레메트리를 평가하는 솔루션을 활용하여 알려진 위협 패턴 및 변칙을 파악합니다. 로그인 시도에서 컨텍스트 및 위험을 평가합니다.
- ITDR을 통해 환경의 IAM 복잡성을 식별하고 확보된 가시성을 기반으로 취약점을 평가합니다. **ID 위협 탐지 및 대응** 기능을 활용하여 포괄적인 단일 인터페이스에서 ID 에코시스템 전반에 대한 가시성을 확보합니다.

기여자

데이터 과학

Cyentia Institute

Elizabeth Gilbert

Kevin Pelaez, 박사

Rose Putler, M.S.

작성자

Katherine Yang

Michael Parker

Slavka Bila

프로덕션

Yolina Nenov

Taylor Stewart

디자인 및 개발

Amanda Cash

Chris Canote

Clayton Chu

Mary Jane Duty

Tony Ly

참조

- **"2023 ID 보안 상태: 인력 보호,"**
  Oort, 2023
- **"보안 탄력성 확보: 보안 성과 보고서의 결과, Vol 3"**
  시스코, 2023년 1월 10일
- **"시스코 사이버 보안 준비상태 지수,"**
  시스코, 2023년 3월
- **"Cisco Talos 2023 연례 보고서,"**
  Cisco Talos, 2023년 12월 5일
- **"사고 대응 트렌드 Q2 2023: 데이터 도난 갈취 증가, 여전히 가장 많이 표적이 되는 의료 서비스 업종,"**
  Cisco Talos, 2023년 7월 6일

duo.com에서 30일 무료 평가판을 시작하고 모든 사용자, 디바이스, 애플리케이션을 빠르게 보호하세요.