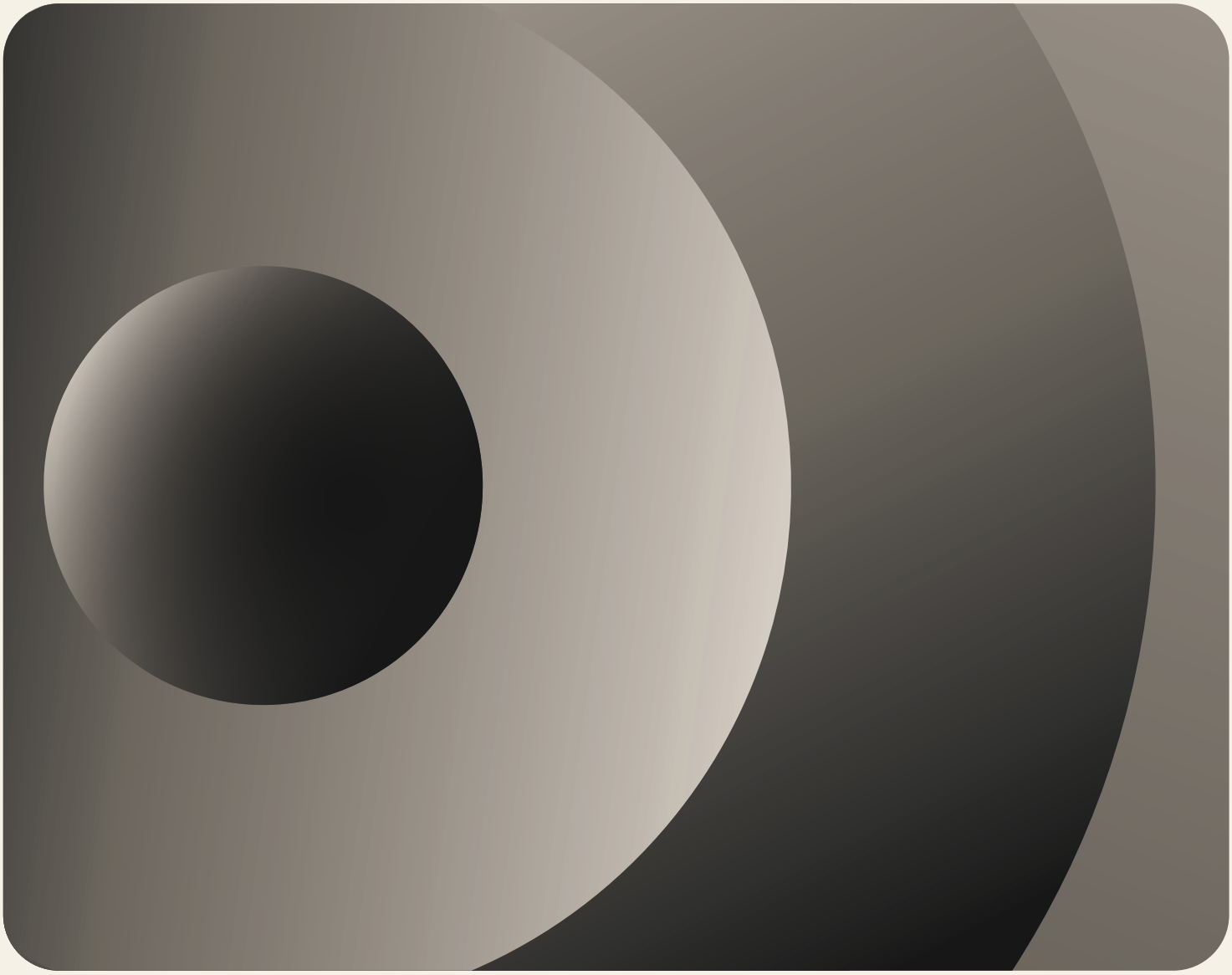
2023

글로벌 기업을 위한 IAM (Identity and Access Management) 평가

2023년 Zero Trust 보안 현황



okta

목차

방법론

설문조사 방법론

Okta는 2023년 4월에 Qualtrics와 협력하여 다양한 산업 분야에 걸친 정보 보안 의사결정권자들을 대상으로 글로벌 설문 조사를 실시했습니다. 여기에서 의사결정권자란 테크놀로지 구매 여부를 결정하는 임원급 이상의 직원을 의미합니다. 설문조사는 13개 국가의 Qualtrics 전문 패널을 통해 영어와 일본어로 진행되었습니다. 본 보고서에 언급된 "Okta의 설문조사" 또는 "설문조사"는 이 설문조사를 말하며, "설문조사 응답자" 또는 "응답자"는 각 기업을 대표하여 응답한 의사결정권자를 말합니다.

Okta의 설문조사 응답자

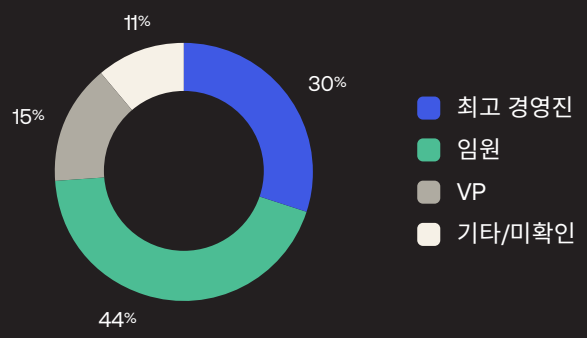
북미 지역(미국, 캐나다), EMEA 지역(덴마크, 핀란드, 프랑스, 독일, 아일랜드, 네덜란드, 노르웨이, 스웨덴, 영국) 및 APJ 지역(일본, 호주)의 정보 보안 의사결정권자 860명을 모집단으로 선정했습니다. 본 보고서는 의료, 공공 부문, 금융 서비스 및 소프트웨어 분야에 초점을 맞추고 있지만 그 외 다른 산업 분야도 다루고 있습니다. (지역 및 산업 분야는 응답자가 자발적으로 밝혔습니다). 공공 부문에는 주/지역 기관을 제외한 3개의 글로벌 지역 기관들이 포함됩니다. 응답자에는 경영진과 부사장 및 이사가 포함되었습니다. Okta 직원이나 고객은 이번 설문조사 대상에서 제외되었습니다.

방법론 세부 정보

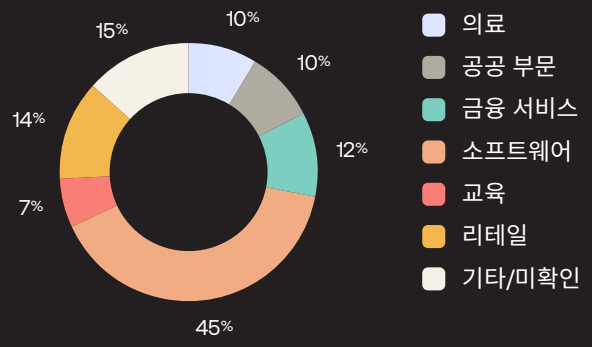
본 보고서에 포함된 차트에서 "전 세계" 또는 "모든" 응답에는 모든 분야(4가지 주요 분야에 국한되지 않음)와 모든 지역(북미, EMEA 또는 APJ 거주 여부에 상관없이)의 응답자가 포함됩니다. 차트 데이터는 편의를 위해 0.5보다 작은 경우 0으로 내리고 그 외에는 가장 가까운 한 자리 숫자로 반올림하였으며, 이에 따라 일부 차트에서는 전체 합산이 정확히 100%가 아닐 수도 있습니다. 또한 응답자가 다수의 관련 질문에 예라고 응답한 경우(예를 들어, 특정 이니셔티브를 시행하였고, 앞으로도 계속해서 시행할 계획인 경우)에는 차트의 데이터 합산이 100%를 초과합니다. ■

설문조사 응답자 통계

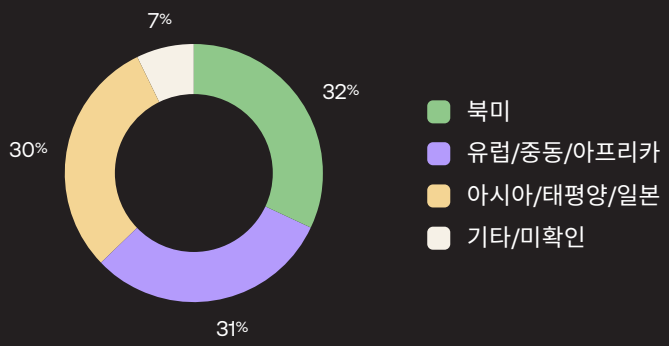
응답자 직책



회사 산업



회사 지역



목표를 넘어서 계획 단계로 접어든 Zero Trust

오늘날 기업들은 직원, 자산 및 인프라를 안전하게 보호할 수단으로 Zero Trust를 적극 도입하고 있습니다.

10년 전에 Zero Trust는 보안 경계에서 희미하게 일렁이는 오아시스와도 같이 먼 개념이었습니다. Zero Trust라는 용어는 Forrester 연구원인 John Kindervag가 2010년에 "절대 신뢰하지 말고 항상 검증하라"는 보안 개념의 필요성이 커지면서 안심하고 보호하자는 의미로 처음 사용했습니다. 하지만 그로부터 10 년이 지나는 동안 Zero Trust는 훌륭한 철학에서 목표의 수준을 넘어 일상적인 비즈니스로 빠르게 진화해왔습니다. Okta의 Zero Trust 현황 연례 설문조사에서도 알 수 있듯이, 현재 그 어느 때보다 많은 기업이 이러한 개념을 비즈니스 전략으로 채택했으며 향후 몇 개월 내로 Zero Trust 보안을 전격 시행하기 위해 구체적인 단계를 밟고 있습니다.

실제로 Okta가 2019년에 Zero Trust 보안 현황 보고서를 처음 발간한 이후로 Zero Trust 전략을 수립한 기업들이 크게 늘면서 아직 계획 단계에 머물러 있거나 그 중요성을 전혀 인지하지 못하는 기업의 수를 크게 넘어선 상황입니다. 전세가 완전히 역전된 것입니다.

데이터 침해와 도난 사건이 끊임없이 폭증하는 가운데 NIST와 CISA의 규정 지침을 보더라도 이러한 역전 상황은 전혀 놀랄 일이 아닙니다. Identity Theft Resource Center의 2022년 연례 데이터 침해 보고서에 따르면 지난해 미국에서 1,802건의 데이터 탈취 사건이 발생하여 4억 2,200만 명 이상의 개인들이 피해를 입었습니다. 항상 그렇듯이 이러한 대규모 공격의 중심에는 아이덴티티가 있습니다. Javelin의 2022년 아이덴티티 사기 연구 보고서를 보면, 2022년 미국의 아이덴티티 사기 피해액만 무려 430억 달러에 달하는데, 이는 2021년 아이덴티티 사기 피해액인 520억 달러에 비하면 힘든 싸움 끝에 얻은 성과입니다. 미국 법무부의 2023년 보고서에서는 아이덴티티 사기를 "거의 모든 주요 범죄에 연루되어 전 세계 모든 국가와 국민의 안보를 위협하고 있다"라고 규정하고 있습니다.

기업 보안 팀이 이러한 위협과 점차 진화하는 공격자들에게 맞서려면 "절대 신뢰하지 말고 항상 검증하라"라는 Zero Trust의 핵심 원칙을 바탕으로 전략을 세워야 합니다. Zero Trust 보안 전략은 기업이 클라우드 보안 환경을 고려하지 않은 기존의 사이버 보안 접근법에서 벗어나 아이덴티티를 보안 역량에 필요한 주요 동인으로 포지셔닝할 수 있는 토대를 형성합니다. 대부분의 기업이 아이덴티티를 전적으로 IT 팀의 소관이라고 여겼습니다. 하지만 Okta의 데이터에 따르면 이제 아이덴티티에 대한 제어 권한은 보안 팀의 영역으로 넘어왔습니다. 그렇다고 Zero Trust의 수혜자가 SecOps 팀만 있는 것은 아닙니다. 이러한 모범 사례를 수용하는 기업은 네트워크 인프라 전반에서 아이덴티티 관리를 더욱 효과적으로 활용하여 새로운 효율을 달성하고 직원 및 고객 경험을 개선할 수 있습니다.

오늘날 기업들이 거시 경제 동향과 클라우드 혁신으로 더욱 복잡한 하이브리드/멀티 클라우드 에코시스템을 도입하게 되면서 파트너, 계약자, 외부 공급업체 등 다양한 직원들이 경계 없이 분산된 리소스와 IT 환경에 액세스하고 있습니다. 아이덴티티는 이러한 직원들을 하나로 묶어주는 실타래와 같습니다. 그리고 강력한 아이덴티티 관리는 이렇게 복합적인 글로벌 팀들이 안전하게, 생산적으로 협업하는 데 필요한 중요 인프라가 되었습니다. 올해 공개한 데이터에서도 알 수 있듯이, 기업들은 모바일 디바이스 관리를 강화하고 SSO(Single Sign-On) 및 다중 요소 인증(MFA)를 자사의 직원과 외부 협력업체에게 추가하며, 프로비저닝/디프로비저닝 워크플로우를 자동화하고, 강력한 Zero Trust 이니셔티브를 통해 조직의 자산과 직원을 안전하게 보호하는 데 주력하고 있습니다.

Zero Trust 보안을 달성하는 과정은 기나긴 여정입니다. 가장 좋은 시기에 수십 년 동안 이어온 실무와 프로세스를 뒤집고 보안 스택을 다시 구축하고, 고된 투자와 소프트웨어 대체 여부를 결정하는 것은 쉽지 않은 일입니다. 게다가 금융 뉴스만 훑어봐도 금새 알 수 있듯이 지금이 시기적으로 그리 좋은 때도 아닙니다. 하지만 Okta의 연례 설문조사를 보면 적합한 테크놀로지와 공급업체를 확보한 글로벌 기업들은 이러한 난제를 풀고 빠르게 앞서나가고 있습니다. 본 보고서의 목적은 오늘날 미래 지향적인 성장 기업들이 Zero Trust 보안 이니셔티브를 어디에서 어떤 식으로 시행하고 있는지 소개하여 목표 단계를 벗어나 조직의 여정에서 계획을 실천하기 위한 방법을 찾을 수 있도록 지원하는 것입니다.

빠르게 확산하고 있는 Zero Trust 이니셔티브

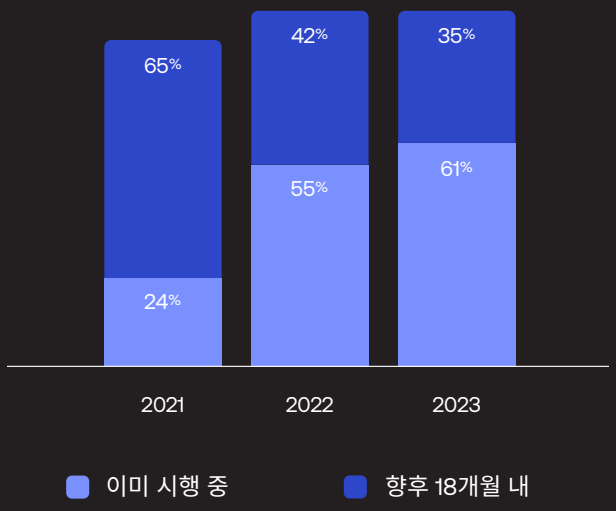
Zero Trust 이니셔티브를 시행하는 기업이 점차 빠르게 증가하고 있습니다. 2021년만 해도 설문조사에 참여한 기업들 중에서 이니셔티브를 시행하는 기업은 25%에도 미치지 못했지만 2022년에는 응답자 중 절반 이상이 이니셔티브를 시행하고 있었고, 올해에는 이 수치가 61%까지 상승했습니다. 기업들이 계획을 빠르게 실천하면서 향후 12~18개월 내로 Zero Trust 이니셔티브를 시행할 계획이라고 응답한 기업의 비율도 전년보다 감소했습니다. 현재는 응답 기업 10곳 중 6곳 이상이 Zero Trust 여정을 이미 시작했으며, 나머지 기업들도 대부분 계획 단계를 확실하게 추진하는 중입니다.

기업 규모를 기준으로 데이터를 자세히 들여다 보면 직원 수가 1,000명 이하인 소규모 기업들은 규모가 큰 기업에 비해 확고한 Zero Trust 보안 이니셔티브를 시행할 가능성이 낮다는 것을 알 수 습니다. 직원 수가 5,001명에서 10,000명 사이인 기업들이 4곳 중 3곳에서 확고한 Zero Trust 이니셔티브를 시행하고 있다고 밝히면서 가장 눈에 띄는 증가세를 보이고 있습니다. 전체를 통틀어 봐도 Zero Trust 이니셔티브를 시행하지 않거나, 향후 18개월 이내에 개발할 계획도 없다고 응답한 기업은 극소수에 불과합니다(전체 10% 미만).

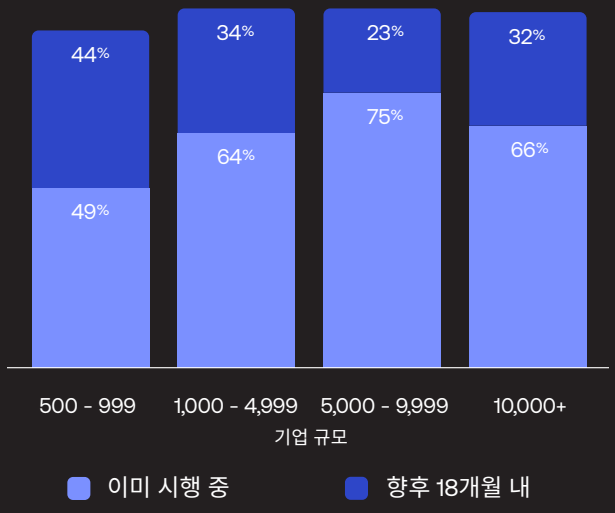
전 세계에서 일상적인 비즈니스로 진화하고 있는 Zero Trust 계획

전 세계적으로 전체 기업의 61%가 확고한 Zero Trust 보안 이니셔티브를 이미 시행 중이며, 28%는 향후 6~12개월 이내에, 7%는 향후 13~18개월 이내에 시행할 계획을 가지고 있습니다. 이러한 동향은 전 지역에서 공통적으로 나타납니다. 이미 시행 중인 이니셔티브의 경우 북미 지역이 선두를 지키고 있는 가운데, EMEA 및 APJ 지역 기업들도 서둘러 기반을 잡고 있으며 두 지역에서 도입을 주저하던 대다수 기업들도 향후 6~12개월 또는 13~18개월 이내에 Zero Trust 이니셔티브를 도입할 계획입니다.

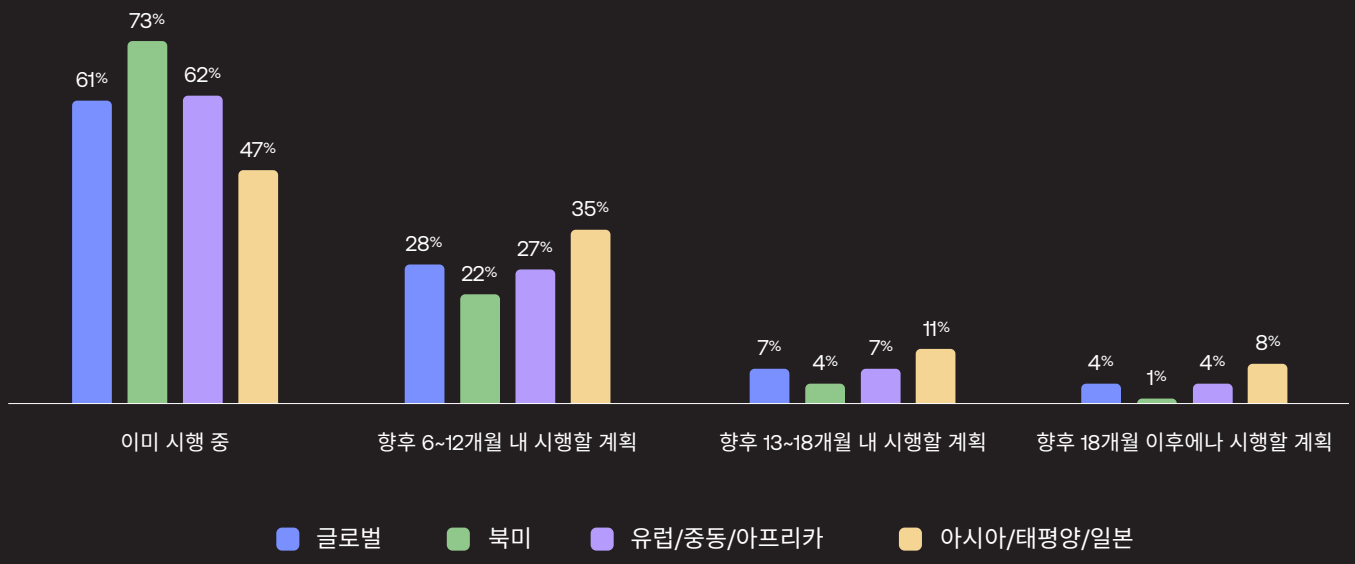
귀사는 현재 확고한 Zero Trust 이니셔티브를 시행 중입니까? 아니면 향후 18개월 이내에 시행할 계획입니까?
모든 응답자



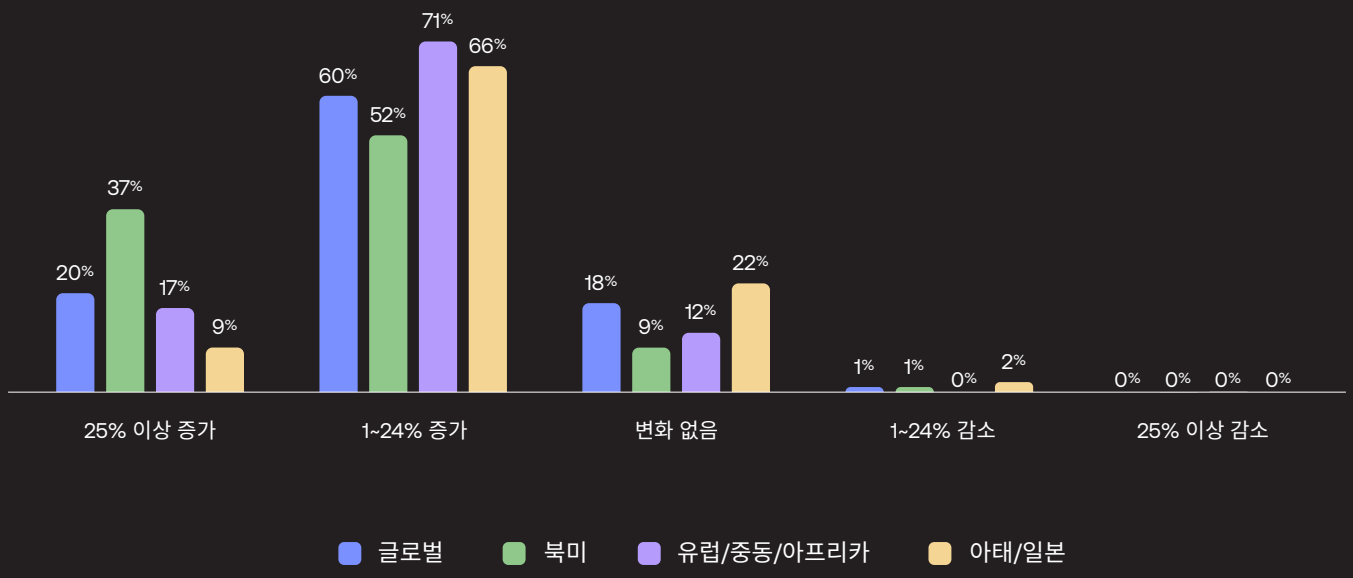
귀사는 현재 확고한 Zero Trust 보안 이니셔티브를 시행 중입니까? 아니면 향후 12~18개월 이내에 시행할 계획입니까?
기업 규모별 비교



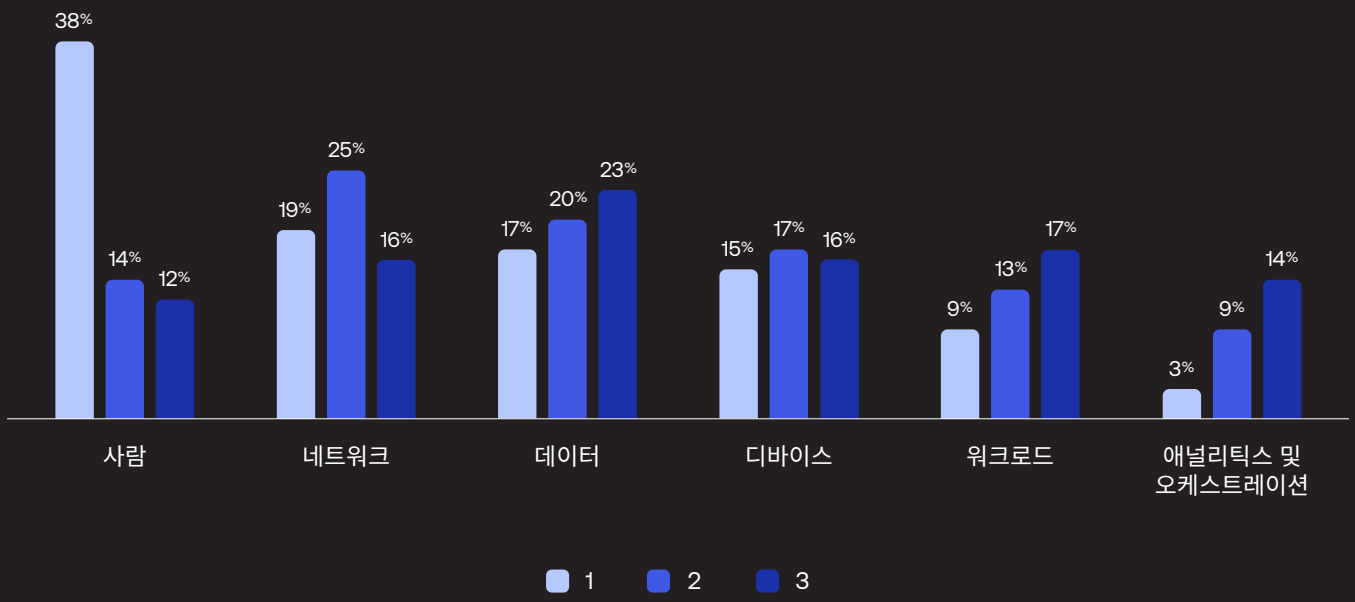
귀사는 현재 확고한 ZT 보안 이니셔티브를 시행 중입니까? 아니면 향후 18개월 이내에 시행할 계획입니까?
지역 간 비교



지난 12~18개월 동안 Zero Trust 예산이 어떻게 바뀌었습니까 (조금이라도 바뀐 경우)?
지역 간 비교



귀사의 보안 프로젝트에서 다음 각 영역의 우선순위를 평가해 주십시오.
(1 = 가장 높음, 3 = 가장 낮음)
모든 응답자



안정적인 수준을 유지하고 있는 Zero Trust 이니셔티브 예산

거시 경제 요인이 모든 지역과 산업에서 인력 수급과 비용 절감을 촉진하는 시대가 된 지금, Zero Trust 보안 이니셔티브 예산은 사실상 손댈 수 없는 것처럼 보입니다. 실제로 설문조사에 참여한 기업들 중에서 이러한 예산을 안정적인 수준으로 유지하는 데 그치지 않고 지난 12~18개월 동안 증액한 기업이 압도적으로 많았습니다. 전 세계적으로 기업의 60%가 작년부터 예산을 1~24% 올렸으며, 그 이상 올린 곳도 20%에 달합니다. 전 지역을 통틀어 예산을 감액한 응답 기업은 3%도 채 되지 않습니다.

보안 프로젝트에서 여전히 최우선 순위를 차지하고 있는 사람

조직의 3대 보안 문제를 1위부터 3위까지 나열해 달라는 질문에, 다수의 응답자가 올해 가장 유력한 카테고리로 “사람”을 지목했으며, “네트워크”와 “데이터”가 각각 2위와 3위로 다소 큰 차이를 보였습니다. “사람”은 항상 최우선 순위였지만 올해에는 Zero Trust 보안 이니셔티브에서 아이덴티티의 주요 역할에 대한 중요성이 커지고 있다는 점을 감안하면 예외적인 이상치에 가깝습니다.

목표를 넘어 계획 단계로 접어든 Zero Trust

핵심 요점

실천 계획 단계에서 어느새 일상적인 비즈니스가 되어버린 Zero Trust

Zero Trust를 그저 가설로 치부했던 기업들도 이제는 대체로 계획을 실행하는 단계에 도달했으며, 원활하게 추진하는 기업들도 있습니다. 이러한 역전은 극적으로 일어났습니다. 전략적 Zero Trust 이니셔티브를 이미 시행 중이라고 답한 응답자가 2021년에는 단 24%에 그쳤지만, 작년에는 55%로 증가하더니 올해에는 61%까지 증가했습니다. 지역과 조직의 규모를 막론하고 이러한 추세가 전역에서 나타나고 있습니다. 4가지 주요 산업 중 금융 서비스의 경우 응답 기업의 71%가 Zero Trust 이니셔티브를 이미 시행 중이었으며, 소프트웨어 부문이 69%로 그 뒤를 이었습니다. 지역별로 보면 북미 지역이 가장 두각을 나타내고 있는데, 응답 기업의 73%가 확고한 Zero Trust 이니셔티브를 시행하고 있다고 답했습니다. 반면 APJ 지역은 시행 중인 비율이 47%로 가장 낮았지만 향후 6~12개월 내로 이니셔티브를 시행할 계획인 비율은 35%로 가장 높았습니다.

아이덴티티는 이제 Zero Trust 전략에서 미션 크리티컬 요소로 널리 인정받고 있습니다.

1년 동안 무엇이 달라졌을까요? 지난해에는 응답자의 71%가 Zero Trust 보안 전략에서 아이덴티티의 중요성을 인정한 반면 비즈니스 핵심 요소라고 답한 응답자는 27%에 불과했습니다. 올해에는 상황이 역전되어 응답자의 51%가 아이덴티티를 "매우 중요하다"라고 답했고, "다소 중요하다"라고 응답한 비율은 40%에 달했습니다. 이러한 변화는 놀랄 일이 아닙니다. 하이브리드/멀티 클라우드 환경에서 사람과 자산을 안전하게 보호하려면 기본적으로 강력한 IAM(Identity and Access Management) 전략이 필요하다는 사실을 점차 많은 기업이 깨닫고 있기 때문입니다.

Zero Trust 예산은 시장 동향에도 불구하고 꾸준히 증가하고 있습니다.

거시 경제의 압박으로 전 세계 어디를 가든 예산이 줄고 있지만 Zero Trust에 대한 지출은 계속 늘고 있습니다. 올해 설문조사에서는 무려 80%의 응답자가 Zero Trust 보안 이니셔티브 예산이 전년보다 증가했다고 밝혔습니다. 응답자의 60%가 예산 증액 비율이 1~24%라고 답했고, 20%는 25% 이상으로 크게 올랐다고 답했습니다. 비용 문제는 본 보고서에서 언급하는 3년 동안 고려해야 할 사항에서 빠지지 않았지만 끊임없는 사기와 내부자 위협, 그리고 하이브리드 근무 환경과 원활한 클라우드 액세스에 대한 요구가 증가하면서 규모와 산업을 불문하고 모든 기업이 아이덴티티 기반 보안 대책을 중심으로 예산을 편성할 수밖에 없게 되었습니다.

Zero Trust를 도입하려는 기업들도 힘든 싸움을 계속 이어가고 있습니다.

올해 응답자들은 Zero Trust 도입을 방해하는 가장 큰 문제로 비용 문제와 테크놀로지 격차를 꼽았으며, 개인정보 보호규정/데이터 보안과 인력 부족이 뒤를 이었습니다. 하지만 이제는 상황이 달라졌습니다. 작년에는 한 가지 문제가 유독 두드러지는 경향을 보였지만 올해에는 통합 용이성, 솔루션에 대한 인식, 감사 규정 준수, 이해관계자 승인 등 다양한 문제들이 균형을 이루고 있습니다. 관련 소식을 살펴보면 과거 IT 팀이 관리하던 조직 내 IAM에 대한 팀 관리가 보안 팀에서 주로 관리하는 책임 공유로 바뀌었습니다. ■

아이덴티티: Zero Trust의 핵심

전 세계 기업들이 오늘날 보안 환경에서 아이덴티티의 중추적 역할을 수용하고 있습니다.

기존의 네트워크 경계가 거의 모두 사라진 세상에서 아이덴티티가 보안 출발점으로써 새로운 경계로 자리잡고 있습니다. 세계 어디에서든지 광범위한 승인/미승인 디바이스를 사용해 리소스에 액세스하려고 시도할 때마다 모든 사용자와 디바이스의 아이덴티티를 검증하는 것은 아직까지 쉽지 않은 일입니다.

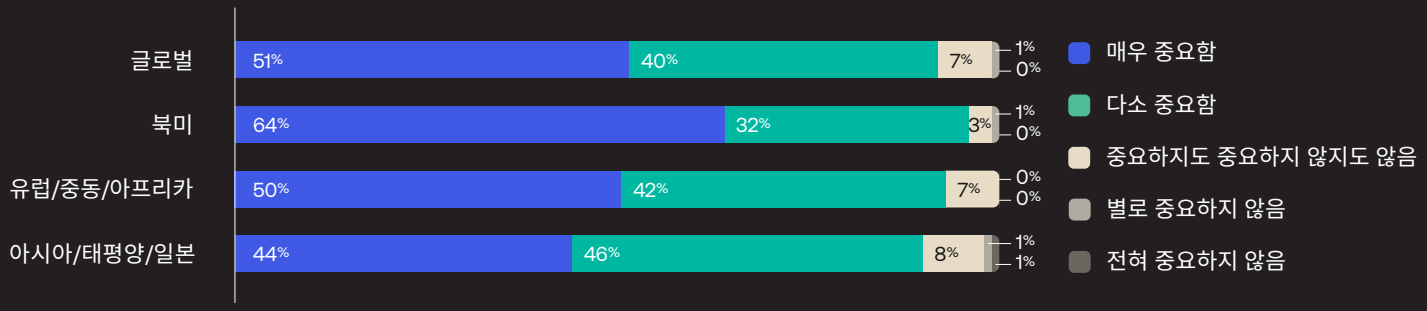
하지만 비즈니스 성공이라는 보상을 얻을 수 있습니다. 올해 데이터에서도 알 수 있듯이, 아이덴티티가 단순한 보안 수단을 넘어 안전한 비즈니스 확장을 통해 수익을 늘리고, 고객 충성도를 강화하고, 자산과 브랜드 평판을 보호할 수 있는 방법이라는 사실을 규모와 산업을 불문하고 점차 많은 기업이 이해하기 시작했습니다.

이러한 동향은 Okta의 2023년 설문조사 결과에서도 잘 드러나는데, 기업들이 Zero Trust 이니셔티브에서 아이덴티티의 중요성을 그 어느 때보다 강조하고 있습니다. 전 세계 응답자들 중에서 아이덴티티가 Zero Trust 보안 전략에 매우 중요하다고 답한 비율은 50%를 상회하여 2022년의 수치를 크게 넘어섰으며, 다음 페이지에서도 언급하겠지만 모든 지역의 응답자들도 그 비율이 증가했습니다.

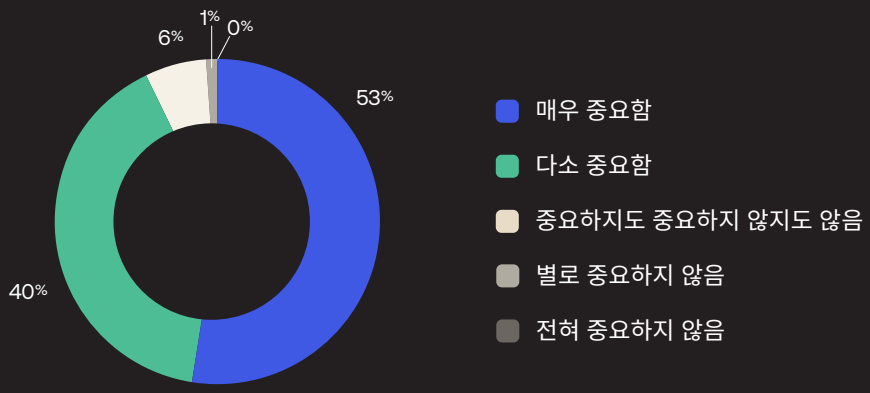
"IT 리더들은 보안 및 비즈니스 목표에 맞춰 IAM 투자를 조율하고 있습니다. 제대로 수행한다면 IAM을 통해 권한 인증, 정책 적용, 프로비저닝 및 디프로비저닝 프로세스를 안전하게 보호하고 마찰을 최소화하며 비즈니스 운영을 뒷받침할 수 있습니다. 이로써 보안과 생산성까지 크게 개선할 수 있습니다."

— IDSA(Identity-Defined Security Alliance)의
2022년 디지털 아이덴티티 보안 동향 보고서

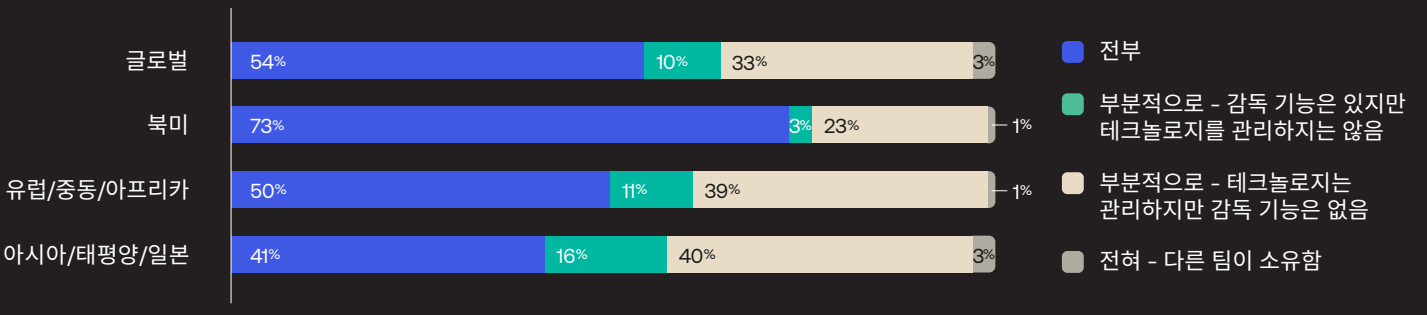
귀사의 전반적인 Zero Trust 보안 전략에서 아이덴티티는 얼마나 중요합니까?
지역 간 비교



귀사의 전반적인 Zero Trust 보안 전략에서 아이덴티티는 얼마나 중요합니까?
경영진 응답자



귀사의 보안 팀은 IAM을 얼마만큼 소유하고 있습니까?
지역 간 비교



참고: 데이터 라벨을 정수로 반올림하기 때문에 각 비율 열의 총합이 정확히 100%가 아닐 수도 있습니다.

확고부동한 아이덴티티의 중요성

Zero Trust 이니셔티브를 뒷받침하는 아이덴티티의 핵심 역할이 더욱 명확해지고 있습니다. 지난해 전 세계 응답자 중에서 아이덴티티가 전반적인 Zero Trust 보안 전략에 매우 중요하다고 응답한 비율은 27%에 불과했지만 올해는 이 수치가 51%까지 증가했습니다. 지역을 기준으로 보면, 북미 지역이 가장 많이 올랐는데, 약 2/3가 아이덴티티가 매우 중요하다고 답했고, 약 1/3이 다소 중요하다고 답했습니다. EMEA 지역과 APJ 지역에서는 응답자의 7%와 8%가 각각 아이덴티티가 중요할 수도 있고, 중요하지 않을 수도 있다고 밝혀 인지적 측면에서 해결해야 할 장벽이 존재하는 것으로 보이며, 특히 APJ 지역에서는 일부(2%) 응답자가 아이덴티티가 다소 중요하지 않거나, 매우 중요하지 않다고 답했습니다.

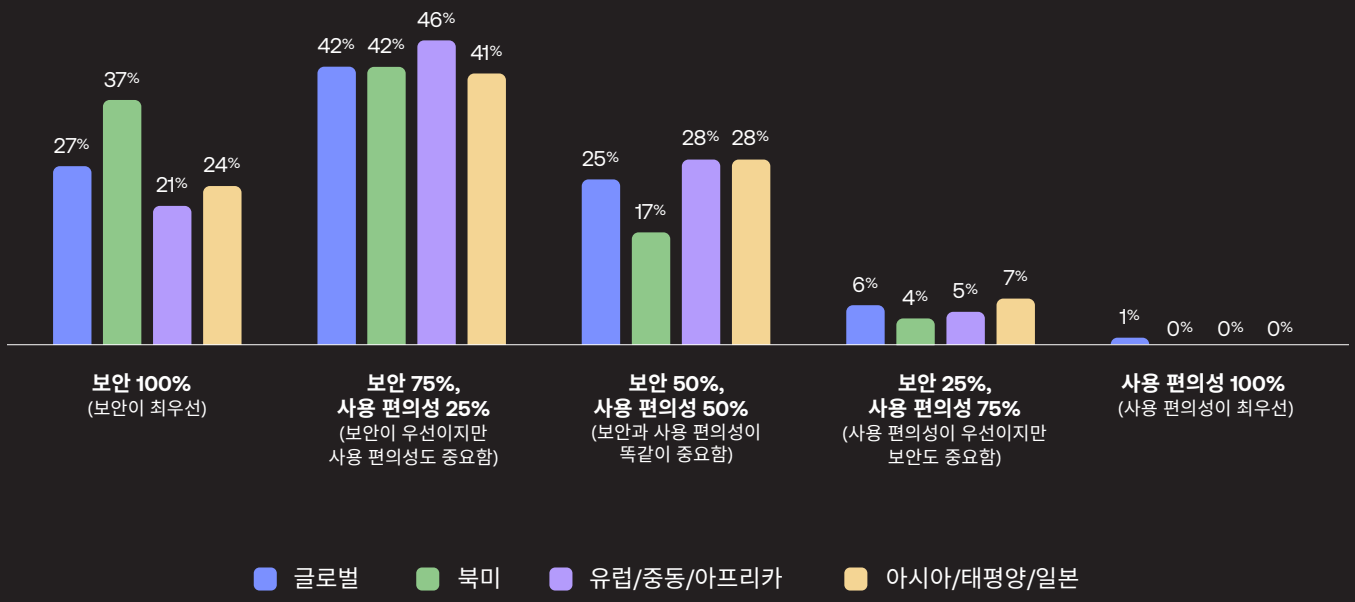
경영진의 동의

경영진 응답자의 대다수가 작년 설문조사와 마찬가지로 아이덴티티의 중요성을 높게 평가하고 있었습니다. 경영진 응답자의 절반 이상이 아이덴티티가 Zero Trsut 전략에 매우 중요하다고 답했으며, 다소 중요하다고 밝힌 응답자도 40%에 달했습니다. (지난해 아이덴티티가 미션 크리티컬한 요소라고 밝힌 경영진 응답자는 26%에 그쳤습니다). 요약하자면, 오늘날 보안 환경에서 아이덴티티의 핵심 역할에 대한 인식이 확산하고 있습니다.

IAM에 대한 변화하는 책임론

빠르게 진화하는 보안 접근법을 알 수 있는 한 가지 방법은 IAM이 조직의 어느 부서에서 관리되는지를 추적하는 것입니다. 지금까지 아이덴티티는 IT 부서가 주로 소유하는 것이었습니다. 하지만 최근 몇 년 동안 피싱과 같은 아이덴티티 기반 위협이 압도적으로 증가하면서 아이덴티티에 대한 소유권이 보안 팀의 책임으로 점차 바뀌었습니다. (Verizon의 2023년 데이터 침해 조사 보고서에 따르면 지난해 유출 사고 중 74%가 인적 요소에 기인하는 것으로 나타났습니다). EMEA 지역에서는 기업의 50%가 보안 팀에서 IAM에 대한 소유권을 가지고 있으며, 북미 지역의 경우 이 수치가 73%에 달합니다. APJ 지역에서는 소유 권한이 더욱 분산되어 있는데, 보안 팀에서 IAM을 전면적으로 관리하는 기업은 41%에 그쳤고, 56%는 보안 팀에서 아이덴티티 또는 테크놀로지 중 하나만 관리하고 있었습니다.

귀사는 보안의 중요성과 사용 편의성의 중요성을 어떻게 조율합니까?
지역 간 비교



사용 편의성보다 더욱 우선시되고 있는 보안

오늘날 하이브리드/멀티 클라우드 기업 네트워크에서 공격 대상이 급증하면서 기업들이 아이덴티티 기반 위협에 점차 취약해지고 있습니다. 이에 따라 기업들은 사용 편의성보다는 보안에 중점을 두고, 때로는 크게 치중하는 식으로 우선순위를 바꾸게 되었습니다. 전 세계적으로 기업의 2/3 이상이 보안을 명백한 최우선 순위라고 얘기하거나, 혹은 우선순위 가중치를 보안에 3/4, 사용 편의성에 1/4만큼 두고 있다고 얘기합니다. 이는 팬데믹으로 인해 원격 근무가 급증하면서 사용 편의성에 중점을 두었던 2021년에 비해 가장 크게 달라진 부분입니다. 보안을 최우선순위로 생각한다고 답한 비율은 북미 지역의 경우 37%였고, EMEA 지역은 21%로 가장 낮았습니다. ■

Workforce Identity 성숙도

기업들은 이제 아이덴티티 관리의 가치를 깨닫게 되었습니다. 성공의 비결은 이 개념을 실행에 옮기는 것입니다.

Zero Trust는 하룻밤 사이에 이루어지지 않습니다. 복잡한 이니셔티브와 우선순위의 변화, 그리고 확장하는 요구사항은 모두 시간과 자원을 요구하기 때문에 기업들도 명확한 프레임워크 없이 자신의 취약점을 파악하여 진행 상황을 벤치마킹하는 데 어려움을 겪을 수 있습니다. 아래에서 자세히 설명하는 Okta의 Workforce Identity 성숙도 모델은 기업이 Zero Trust 여정에서 컨텍스트를 기반으로 아이덴티티 요소를 이해하고 진행 상황을 벤치마킹하는 데 도움이 될 수 있습니다. 전체 단계를 지날 때까지 시간이 걸리기는 하지만 기업은 아이덴티티 중심 보안을 지렛대로 삼아 공격 대상을 줄이고, 악의적인 공격에 대한 대응 속도를 높이며, IT 비용 및 관리 부담을 낮추고, 안전성과 효율성 및 민첩성을 높이는 등 보안을 더욱 강화할 수 있습니다. 다음 페이지에서 전체 4단계를 빠르게 살펴보겠습니다.

Workforce Identity 성숙도

4단계

1단계: 기초 통합 및 간소화	• 수동 관리 감소 • 위험 대상 축소 • 디렉터리 통합
2단계: 확장 보안 제어 계층화	• 입사자/퇴사자 계정 관리 자동화 • IT 생산성 향상 • 관리자 부담 감소
3단계: 고급 경험 자동화 및 개선	• 모든 아이덴티티 시스템 연결 • 모든 관리 프로세스 자동화 • 기존 테크놀로지 대체
4단계: 전략 아이덴티티 최적화 및 확장	• 최신 액세스 경험 구현 • 비밀번호 위험 제거 • 디지털 성숙도 확장

1단계: 기초

통합 및 간소화

1단계에서 기업들은 일반적으로 수동 관리 감소, 아이덴티티 기반 공격에 대한 보안 강화를 목표로 삼습니다. 따라서 사용자와 앱에 대한 수동적인 관리에서 벗어나 보안을 강화하기 위해 노력합니다. 하지만 서로 단절된 일시적 이니셔티브, 의도치 않게 증가하는 위험 대상, 무분별한 디렉터리 증가 등으로 인해 어려움을 겪을 때가 많습니다.

1단계에서 고려해야 할 중요한 아이덴티티 이니셔티브로는 아이덴티티 시스템 통합, 역할 기반 액세스 정책과 함께 기본적인 SSO 및 MFA 구현, 고가용성 아키텍처 설계, SLA 표준 추가, 포괄적인 온프레미스 및 클라우드 앱 인벤토리 개발 등이 있습니다.

2단계: 확장

보안 제어 계층화

2단계에서 기업들은 일반적으로 IT 생산성을 높이고, 관리 시간 및 비용을 절감하기 위해 노력합니다. 하지만 비밀번호에 대한 의존도가 지나치게 높거나, 입사자/퇴자사 계정 관리 등을 위해 수동 프로세스에 투자하는 경우가 있습니다. 2단계 목표에는 생산성 향상, IT 관리자의 부담 완화, 보안 역량 강화, 애플리케이션에 대한 사용자 액세스 간소화가 포함됩니다.

2단계에서 고려해야 할 프로젝트로는 애플리케이션, 계약자 및 비즈니스 파트너에 대한 MFA 확장, 클라우드/온프레미스 애플리케이션에 대한 보안 및 액세스 제어 통합, 역할 기반 액세스 제어 및 동적 액세스 정책 구현, 보안/컴플라이언스 감사 및 모니터링 툴 도입 등이 있습니다.

3단계: 고급

경험 자동화 및 개선

3단계에서는 나머지 수동 프로세스를 모두 자동화하고 모든 아이덴티티 시스템을 단일 통합 관리 솔루션으로 연결합니다. 이로써 기존 테크놀로지를 통합 및 대체하는 동시에 동적인 직원들의 효율을 높이고 모든 시스템을 연결하여 통신하도록 만들 수 있습니다.

3단계에서 고려해야 할 아이덴티티 프로젝트로는 속성 및 정책 기반 액세스 제어 구현, API, 주요 인프라 및 애플리케이션에 대한 최소 권한 액세스 적용 등이 있습니다. 이 단계에서는 일정에 따른 사용자 액세스 재인증을 도입하고, 주요 인프라에 대한 패스워드리스 액세스를 구현할 방법을 찾아야 합니다.

4단계: 전략

아이덴티티 최적화 및 확장

4단계에서는 아이덴티티 기반 시스템을 서로 연결하여 보안과 효율을 크게 높임으로써 조직을 보호합니다. 그리고 최신 액세스 경험을 구현하거나, 비밀번호 관련 위험을 제거하는 등 한층 향상된 목표를 향해 안심하고 집중할 수 있습니다.

이 단계에서는 사고 예방, 탐지 및 대응을 위한 완전 자동화 프로세스 구축, 위험 기반의 적시 액세스 시행, 제로 스탠딩 권한 유지 등 패스워드리스 인증을 완전히 도입하여 수용할 방법을 찾아야 합니다.

Workforce Identity 성숙도

Zero Trust 이니셔티브의 시행

"절대 신뢰하지 말고 항상 검증하라"는 Zero Trust 철학은 미래 지향적인 기업들이 아이덴티티 이니셔티브를 도입하여 우선순위로 삼기 시작하면서 이론적 전략에서 일상적인 비즈니스로 순식간에 바뀌었습니다. 이러한 기업들은 MFA와 SSO를 직원과 외부 사용자를 비롯해 앱, API, 네트워크 인프라의 다른 주요 구성 요소까지 확장하는 일부터 시작해 새로운 보안 기초를 쌓고 있습니다. 점차 복잡해지는 아이덴티티 기반의 Zero Trust 프로젝트를 추진하는 기업들이 전 지역에서 늘고 있으며, 진행 상황도 매우 고무적입니다.

정규직, 계약자, 파트너, 공급업체 등 언제든지 안정적으로 액세스해야 하는 직원들로 인력의 구성이 점차 복잡해지면서 전 세계 기업들은 강력한 아이덴티티 기반의 Zero Trust 보안 역량을 구축하는 데 있어 큰 진전을 보이고 있습니다. 예를 들어, MFA를 외부 사용자(올해 응답자의 34%가 보안 대책 마련)와 직원(33%)에게 우선적으로 적용하고 있습니다.

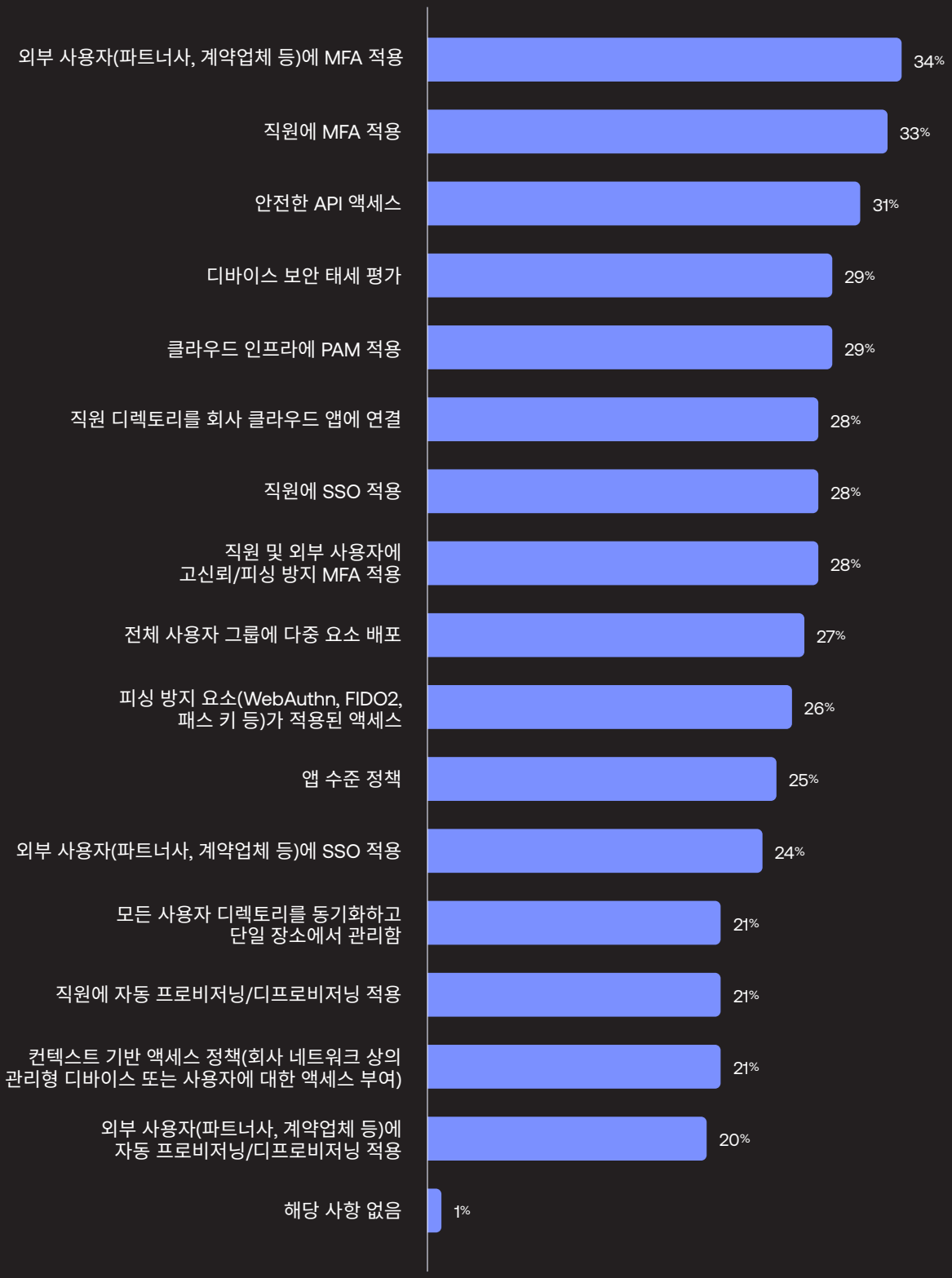
산업별 데이터를 보았을 때 설문조사에 참여한 기업들이 올해 이미 시행하고 있다고 응답한 주요 보안 이니셔티브는 다음과 같습니다.

- **의료:** MFA를 외부 사용자와 직원에게 적용, 디렉터리를 클라우드 앱에 연결
- **공공 부문:** MFA를 외부 사용자와 직원에게 적용, API에 대한 액세스 보호
- **금융 서비스:** MFA를 직원과 외부 사용자에게 적용, 클라우드 인프라에 대한 권한 있는 액세스 관리
- **소프트웨어:** MFA를 직원과 외부 사용자에게 적용, API에 대한 액세스 보호

설문조사에 참여한 기업들이 위와 같은 보안 이니셔티브를 계속해서 구상한 덕분에 올해 데이터는 상당히 고른 분포를 보이고 있는데, 클라우드에 대한 권한 있는 액세스 관리, API에 대한 액세스 보호, 직원에 대한 MFA 적용이 예정된 3대 이니셔티브로 나타났습니다.

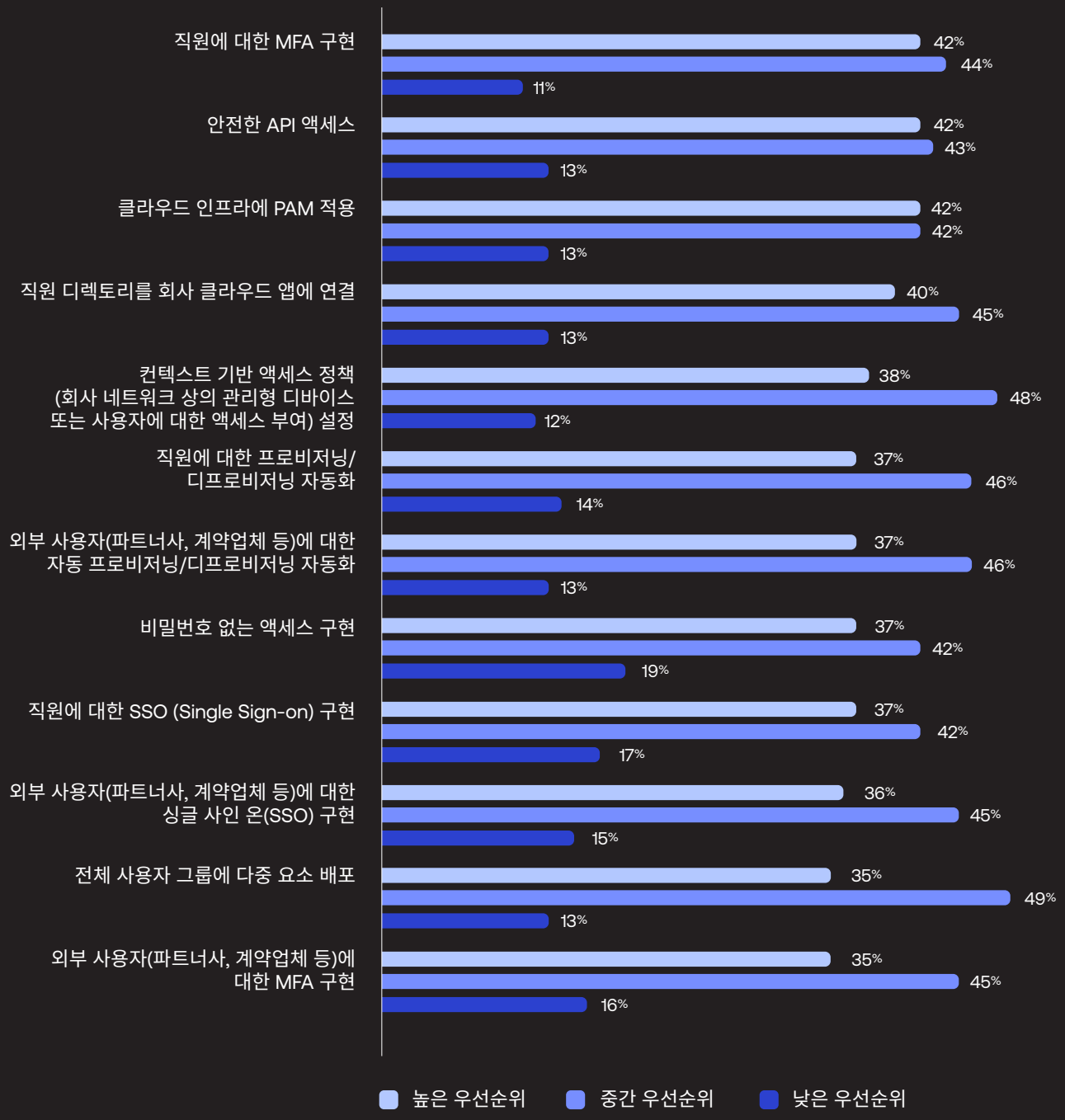
2021년과 2022년에는 직원에 대한 MFA 및 SSO 적용이 이미 시행한 보안 대책 목록에서 1위와 2위를 차지했으며, 클라우드 앱과 직원 디렉터리의 연결이 근소한 차이로 3위를 차지했습니다. 2021년에는 외부 사용자에 대한 SSO 적용이 향후 12~18개월 동안의 최우선 순위였지만 2022년에는 클라우드 인프라에 대한 권한 있는 액세스 관리가 최우선순위로 꼽혔습니다.

다음 중 귀사에서 이미 시행한 보안 이니셔티브는 무엇입니까?
모든 응답자



귀사가 향후 12~18개월 동안 추진할 이들 보안 이니셔티브의 우선순위를 평가해 주십시오.

모든 응답자



참고: 데이터 라벨을 정수로 반올림하기 때문에 각 비율 열의 총합이 정확히 100%가 아닐 수도 있습니다.

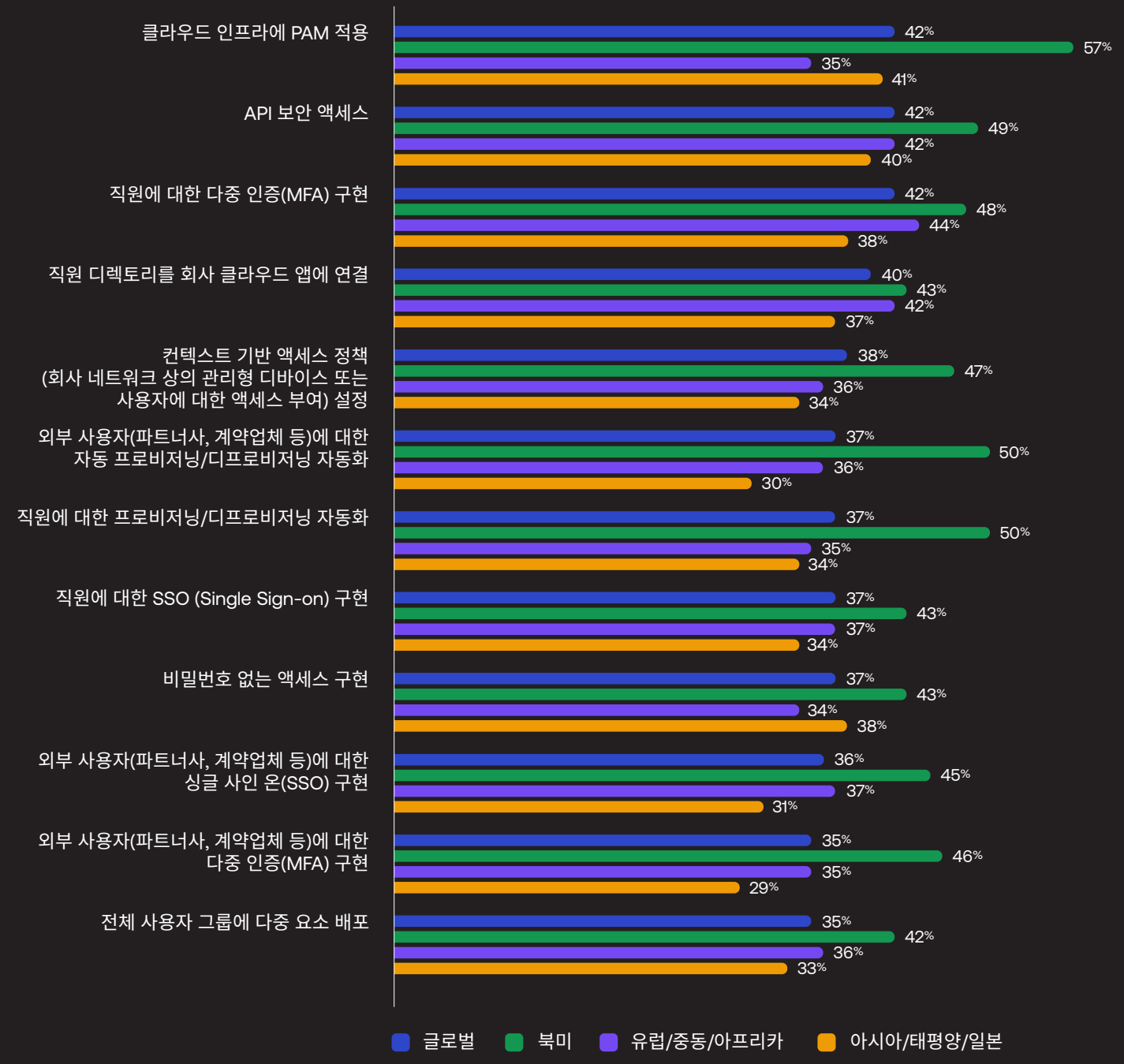
Workforce Identity 성숙도

시행 계획

2021년	#1	외부 사용자에 대한 SSO 적용(57%)
	#2	컨텍스트 기반의 액세스 정책(43%)
	#3	파트너, 계약자 같은 외부 사용자에 대한 다중 요소 인증(MFA) 적용(42%)
2022년	#1	클라우드 인프라에 대한 권한 있는 액세스 관리(45%)
	#2	API에 대한 액세스 보호(41%)
	#3	직원 프로비저닝/디프로비저닝 자동화(38%)
2023년	#1	클라우드 인프라에 대한 권한 있는 액세스 관리(42%)
	#2	API에 대한 액세스 보호(42%)
	#3	직원에 대한 다중 요소 인증(MFA) 적용(42%)

Okta는 매년 설문조사에서 응답자에게 향후 12~18개월 동안 시행할 계획인 Zero Trust 솔루션을 나열해달라고 요청하고 있습니다. 매년 전 세계적으로 가장 많은 응답 세 가지를 살펴보면 흥미로운 동향이 눈에 띕니다. 2021년에는 기업들이 외부 사용자에게 SSO와 MFA를 적용하고, 액세스 정책을 강화하는 데 가장 큰 관심을 뒀습니다. 이렇게 시행된 솔루션들이 다수의 기업들 사이에서 자리를 잡으면서 기업들의 관심도 클라우드에 대한 권한 있는 액세스 및 API에 대한 액세스 보호, 직원 프로비저닝/디프로비저닝 자동화(작년), 직원에 대한 MFA 적용(올해)으로 바뀌었습니다.

귀사가 향후 12~18개월 동안 추진할 보안 이니셔티브 중 우선순위가 높은 것은 무엇입니까?
(차트에는 "우선순위가 높은" 응답만 포함됨)
지역 간 비교



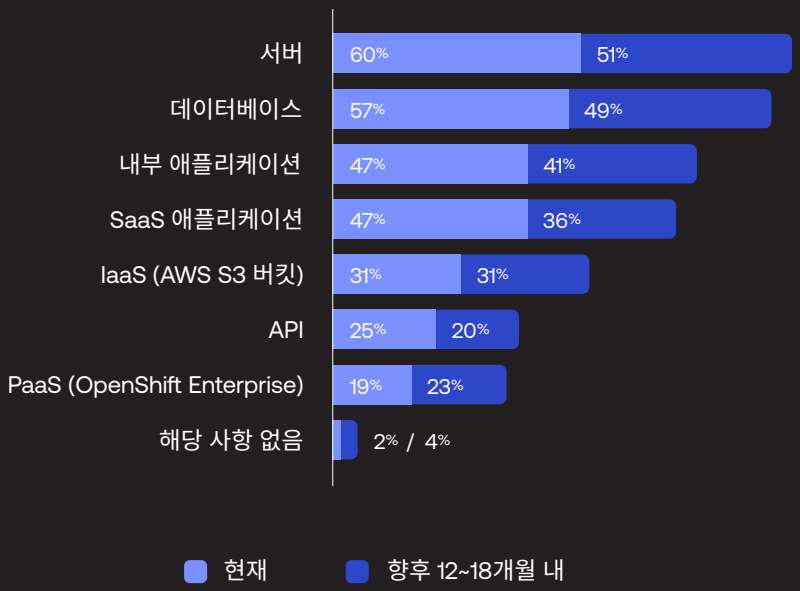
보안 이니셔티브에 우선순위를 두고 있는 북미 지역 기업들

올해 데이터를 더욱 자세히 들여다 보면, 지역별로 편차가 나타나는 것을 알 수 있습니다. 모든 유형의 보안 이니셔티브에 높은 우선순위를 두는 비율은 북미 지역 응답자가 가장 많았습니다. 특히 예정된 보안 이니셔티브 중에서 클라우드에 대한 권한 있는 액세스 관리와 프로비저닝/디프로비저닝 자동화가 가장 큰 비율을 차지했습니다. EMEA 지역에서는 직원에 대한 MFA 적용, API에 대한 액세스 보호, 클라우드 앱에 대한 직원 디렉터리 연결이 우선순위가 가장 높은 이니셔티브였습니다. APJ 지역 기업들은 보안 이니셔티브에 높은 우선순위를 설정하는 비율이 평균적으로 낮았지만, 클라우드 인프라에 대한 권한 있는 액세스 관리와 API에 대한 액세스 보호가 상위권을 차지하고 직원에 대한 MFA 적용, 패스워드리스 액세스 구현, 클라우드 앱에 대한 직원 디렉터리 연결이 근소한 차이로 뒤를 이으며 계획 중인 이니셔티브가 고르게 분포되는 양상을 보였습니다.

Workforce Identity 성숙도

인증 보호

다음 중 MFA/SSO를 이미 확대 적용하고 있는 리소스 클래스는 무엇이며, 향후 12~18개월 내에 확대 적용할 예정인 리소스 클래스는 무엇입니까?
모든 응답자



참고: 복수의 답안을 선택한 응답자들로 인해 각 비율 열의 총합이 100%를 넘을 수도 있습니다.

MFA/SSO 보호에 필요한 리소스로 가장 많은 비율을 차지한 서버와 데이터베이스

지난해 보고서에서는 MFA/SSO를 내부 애플리케이션과 서비스형 소프트웨어(SaaS) 앱까지 확대 적용하려는 모습이 두드러졌습니다. 하지만 올해는 핵심 네트워크 구성요소로 관심이 바뀌었습니다. 응답자 5명 중 3명(60%)이 이미 서버에 MFA 및/또는 SSO를 사용하고 있다고 답했으며, 여기에 데이터베이스까지 새로운 아이덴티티 기반 보호 리소스로 떠오르면서 MFA 및/또는 SSO를 데이터베이스에 확장 적용한다고 답한 비율도 57%에 달했습니다. 지역 관점에서 보면 지역별로 유의미한 차이점은 나타나지 않았습니다. 북미, EMEA 및 APJ 지역에서는 MFA/SSO를 이미 확대 적용하는 기업이든, 이러한 보안 솔루션을 앞으로 확장할 계획인 기업이든 상관없이 모두 서버, 데이터베이스 및 앱(내부 및 SaaS 앱)을 최고의 클래스로 꼽았습니다.

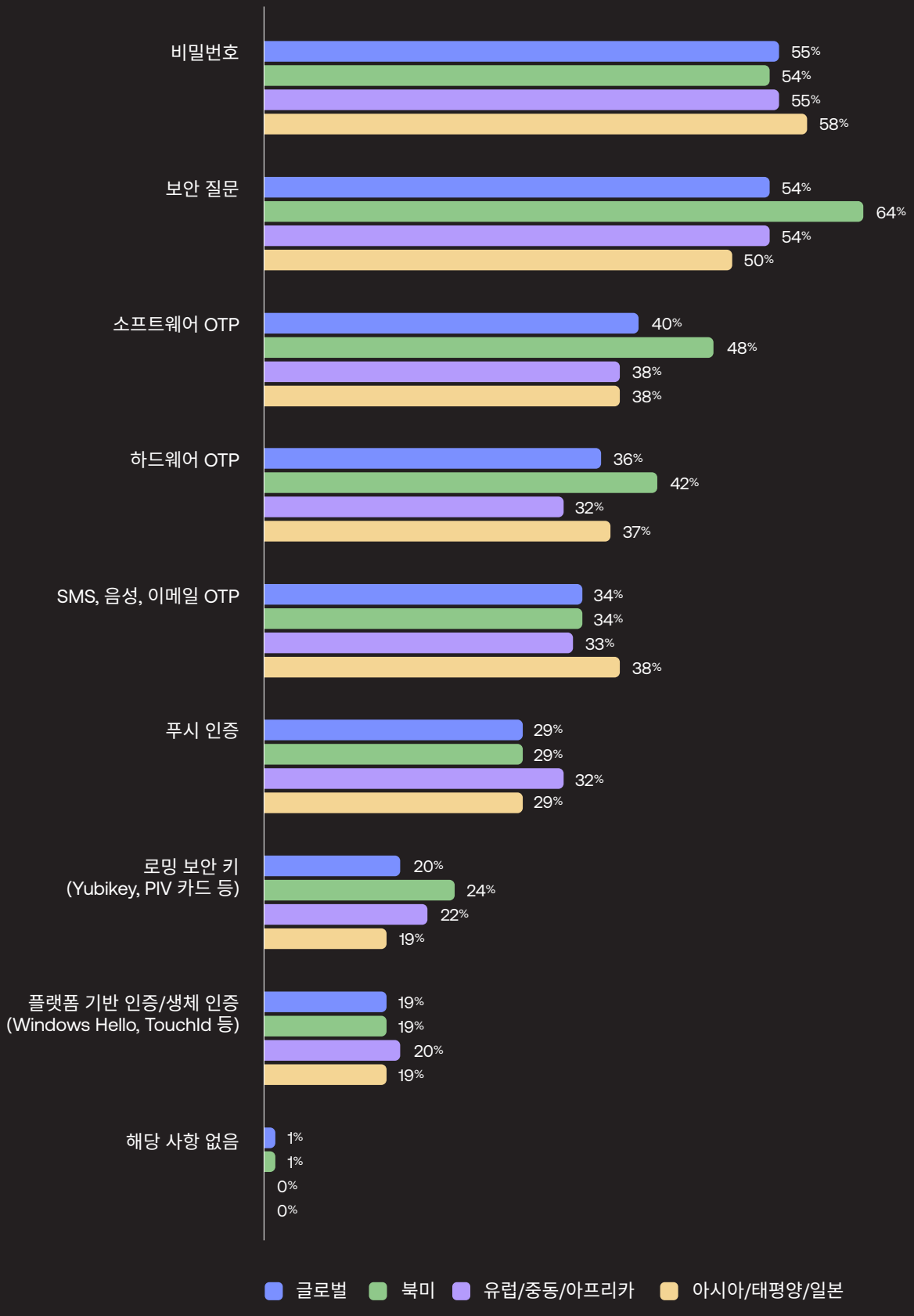
더욱 강력한 인증 서비스를 통한 비밀번호 격차 해소

비밀번호는 보안 수준이 떨어지는 데도 불구하고 아직까지 확고한 인증 표준으로서 남아 있다 보니 전 지역의 응답 기업 중 절반 이상이 아직까지 비밀번호를 사용하고 있습니다. 보안 질문(마찬가지로 보안 수준이 떨어지는 요소)은 EMEA와 APJ 지역을 비롯한 전 세계에서 두 번째로 가장 많이 사용되고 있는 반면, 북미 지역에서는 가장 많이 사용되고 있습니다. 전체적으로 보면, 사이버 범죄자들의 공격에 비교적 쉽게 노출될 수 있는데도 불구하고 기업들은 보안 수준이 낮은 요소(하드웨어 OTP, SMS/음성/이메일 OTP 포함)를 많이 사용하고 있습니다.

물리적 토큰 OTP, 푸시 인증 서비스 등 보안 수준이 중간인 요소들은 비교적 소수의 기업이 사용하고 있으며(각각 36%, 29%), 플랫폼 기반 인증 서비스나 생체 인식과 같이 보안 수준이 높은 요소를 사용하는 기업은 19%에 그쳤습니다. MFA는 주요 인증 서비스로 계속 사용될 것으로 보이며, 금융 서비스나 공공 부문과 같은 산업은 관련 규정이 증가함에 따라 패스워드리스를 비롯해 보안 수준이 높은 피싱 차단 인증 요소로 전환할 가능성이 높습니다.

귀사에서 내/외부 사용자를 인증할 목적으로 사용하는 인증 요소를 선택하십시오.

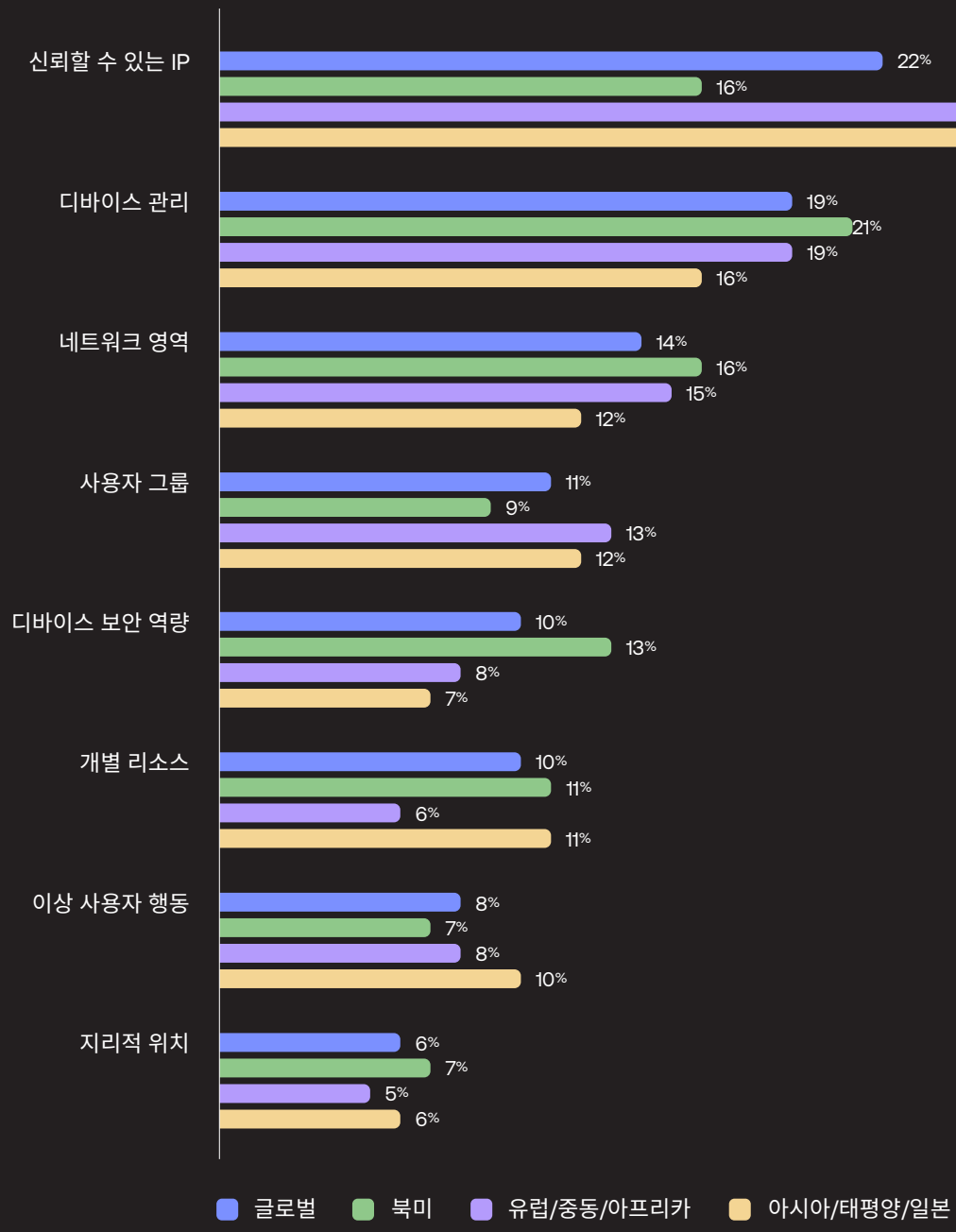
지역 간 비교



Workforce Identity 성숙도

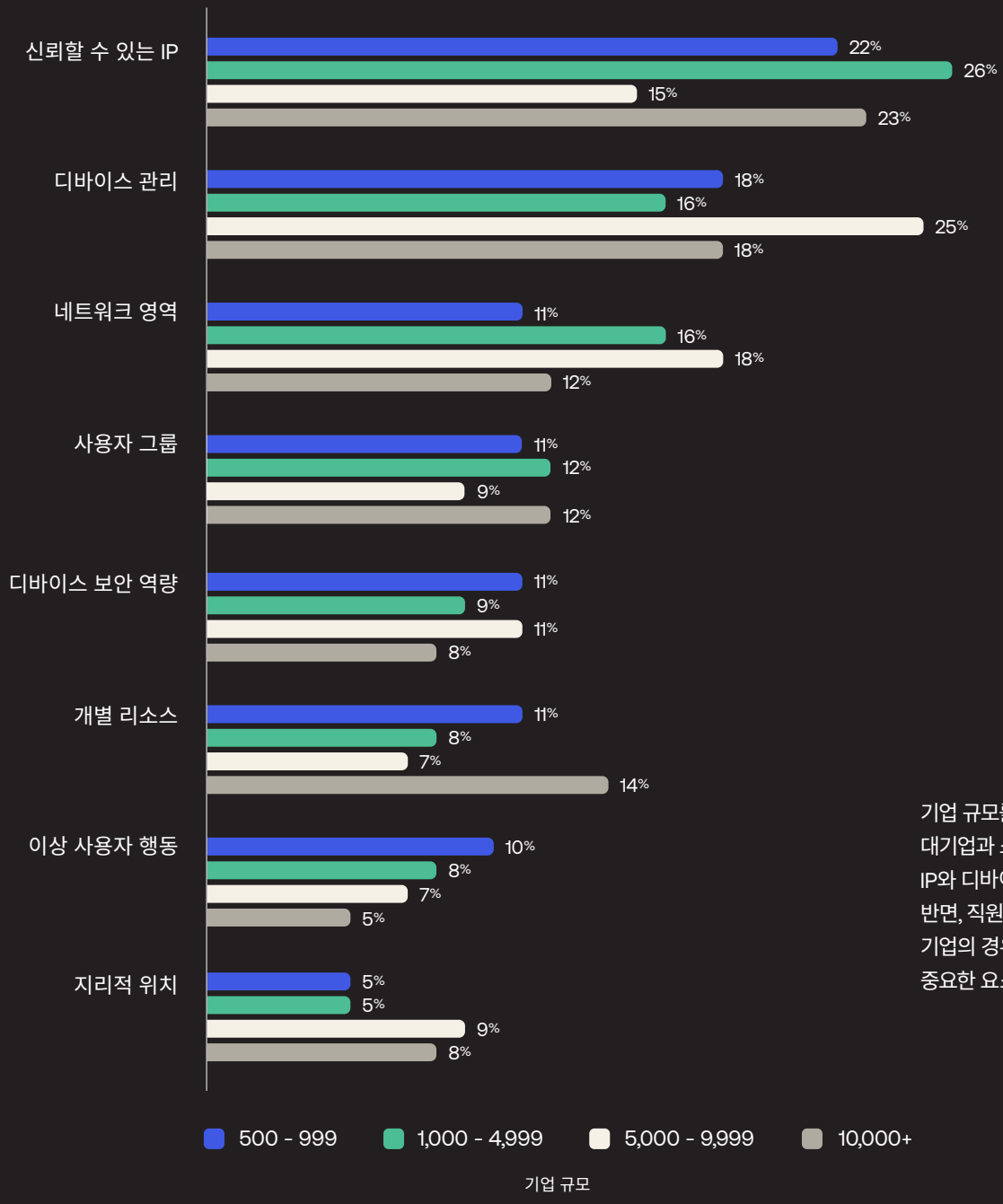
내부 리소스에 대한 액세스 승인

귀사의 내부 리소스에 대한 액세스를 제어하고 승인할 때 가장 중요한 요소는 무엇입니까?
지역 간 비교



전 세계적으로, 특히 APJ 및 EMEA 지역에서 내부 리소스에 대한 액세스를 제어하고 승인할 때 신뢰할 수 있는 IP가 가장 중요한 요소로 평가받고 있습니다. 오직 북미 지역에서만 이 요소가 디바이스 관리(전 세계에서 두 번째로 가장 중요한 요소)에 이어 근소한 차이로 1위를 차지했습니다. 작년에는 디바이스 신뢰, 지리적 위치, 신뢰할 수 있는 IP가 3대 핵심 요소로 지목되었습니다.

귀사의 내부 리소스에 대한 액세스를 제어하고 승인할 때 가장 중요한 요소는 무엇입니까?
기업 규모 기준



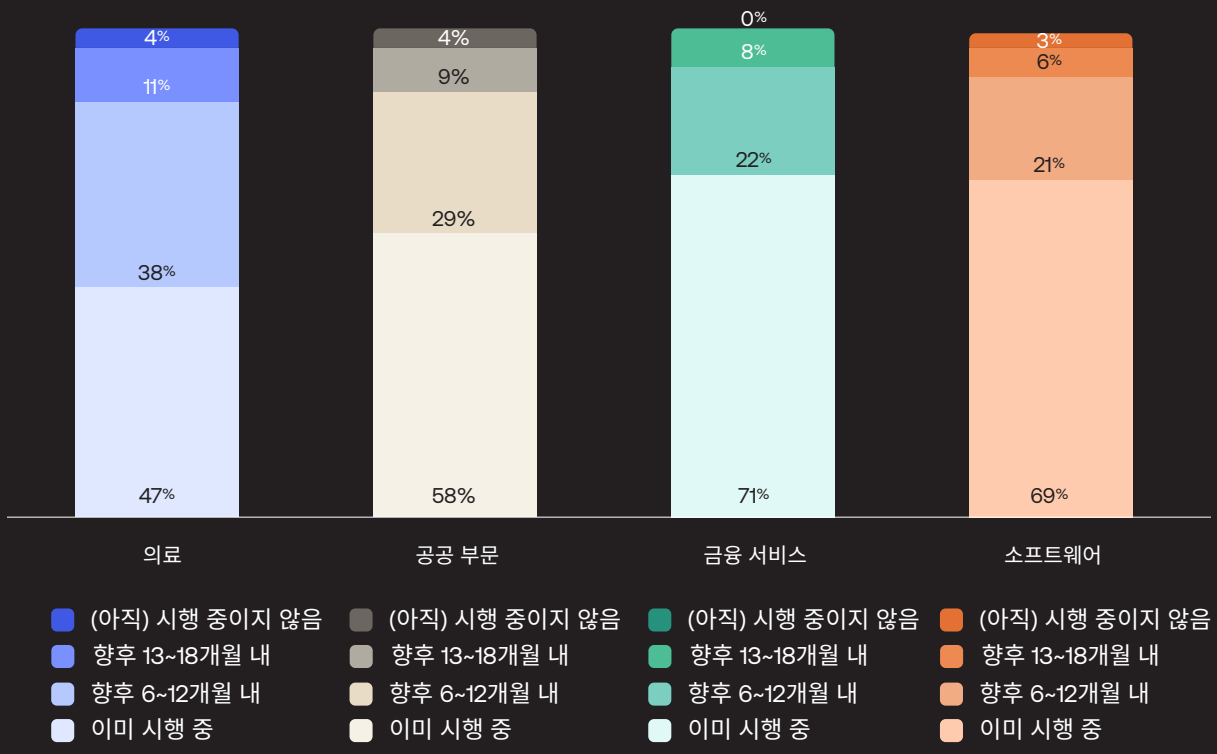
기업 규모를 기준으로 데이터를 살펴보면 대기업과 소기업의 경우 신뢰할 수 있는 IP와 디바이스 관리가 1, 2위를 차지한 반면, 직원 수가 5,000~9,999명인 기업의 경우에는 디바이스 관리가 가장 중요한 요소로 나타났습니다. ■

산업별 Zero Trust 진행 상황

주요 산업 분야에 대한 세부 정보 탐구

Zero Trust 여정은 기업 우선순위나 실무가 그렇듯이 산업에 따라 큰 차이를 보입니다. 올해 설문조사에서도 4대 산업, 즉 의료, 공공 부문, 금융 서비스, 소프트웨어를 중심으로 데이터를 살펴봤습니다. 특히 의료, 공공 부문 및 금융 서비스는 규제가 심하다 보니 Zero Trust 보안 이니셔티브에 투자하여 에코시스템을 안전하게 보호하고 규정을 따를 수 있는 인센티브가 추가됩니다. 전체 데이터를 따져보면, 4가지 산업 모두 작년보다 개선된 듯 보이지만 여전히 진정한 의미의 Zero Trust 보안 환경을 구현할 방법을 찾고 있습니다.

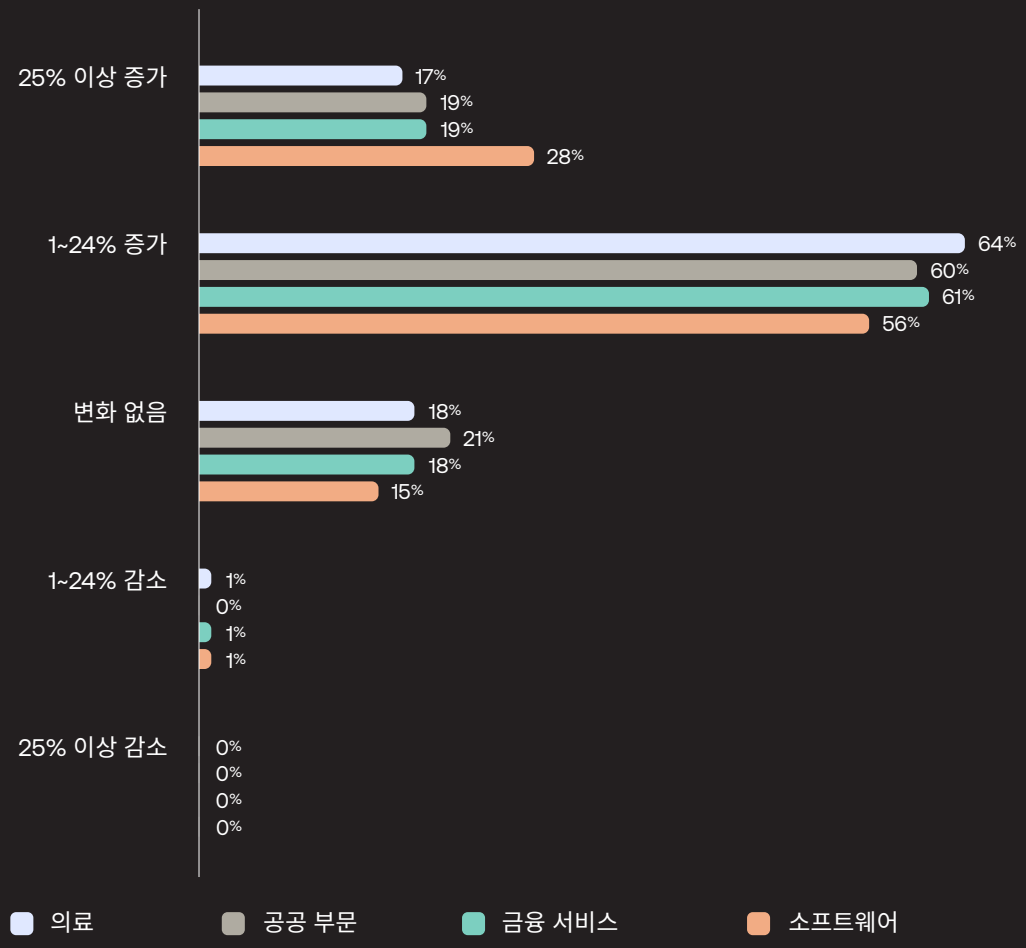
귀사는 현재 확고한 Zero Trust 보안 이니셔티브를 시행 중입니까? 아니면 향후 12~18개월 이내에 시행할 계획입니까?
산업별 비교



금융 서비스와 소프트웨어는 Zero Trust 도입에서 모든 분야를 앞서나가고 있습니다.

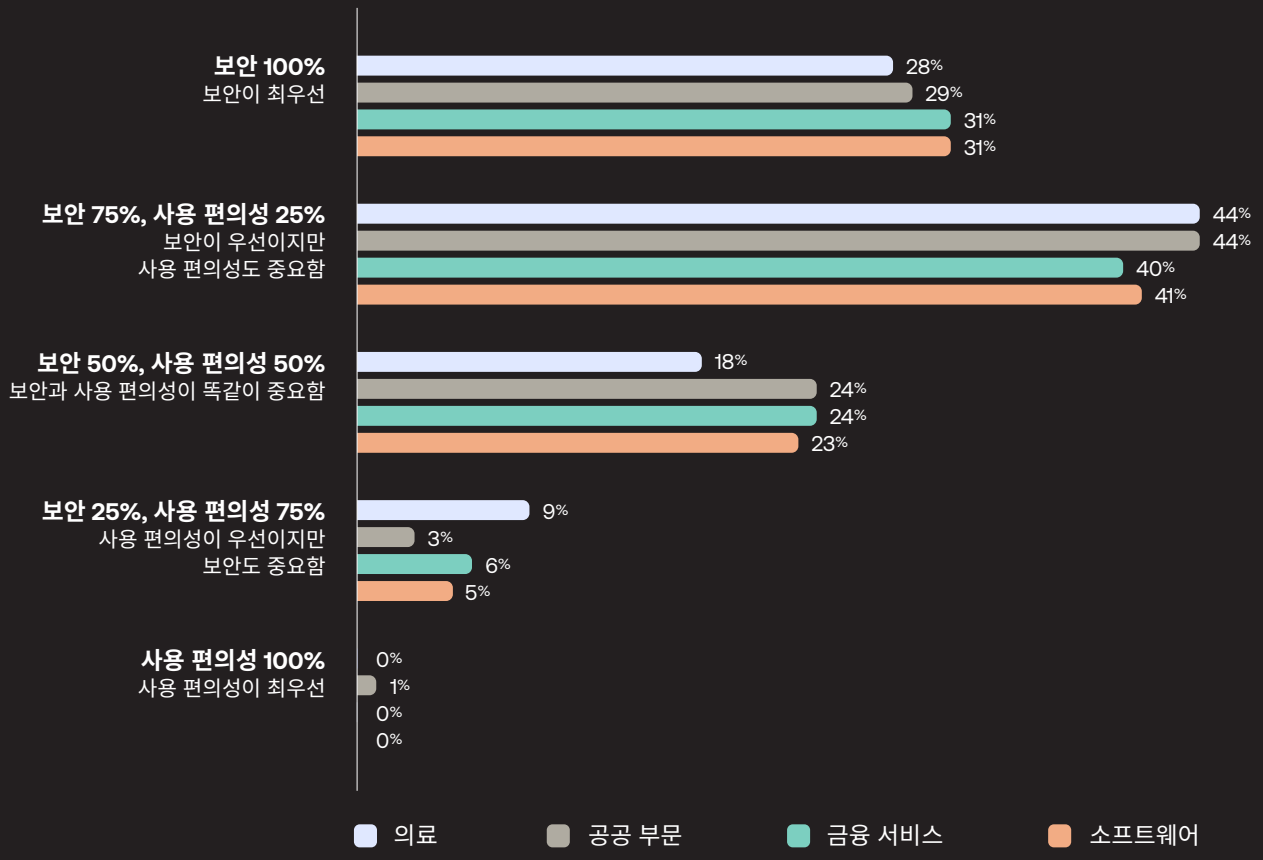
올해 설문조사를 보면 산업 전반에서 Zero Trust를 지향하고 있다는 것을 알 수 있습니다. 4가지 주요 산업에 종사하는 응답자 중 "현재 Zero Trust 이니셔티브를 시행하고 있지 않거나, 앞으로 18개월 동안 시행할 계획도 없다"고 응답한 비율은 4% 미만입니다. 자세한 내용은 다음 페이지에서 다루겠지만 금융 서비스 및 소프트웨어 분야에 종사하는 기업들은 현재 이니셔티브를 시행 중인 비율이 비교적 높고(각각 71%, 68%), 의료 분야와 공공 부문이 근소한 차이로 뒤를 이었습니다.

귀사는 Zero Trust 전략을 도입하면서 보안 이니셔티브 예산이 지난 12개월 동안 어떻게 바뀌었습니까(조금이라도 바뀐 경우)?
산업별 비교



다른 산업에서는 비용 절감을 요구하는 거시 경제의 압박이 거세지만 4가지 주요 산업에 종사하는 기업들은 Zero Trust 보안 이니셔티브에 대한 투자를 중단할 생각이 전혀 없습니다. 4가지 산업에 걸친 응답 기업 5곳 중 4곳이 보안 이니셔티브 예산을 전년 대비 증액했으며, 전체 산업을 통틀어 봐도 보안 예산을 감액한 기업은 거의 없었습니다.

귀사는 보안의 중요성과 사용 편의성의 중요성을 어떻게 조율합니까?
산업별 비교



이렇게 가분수 형태의 보안 관련 차트에서 얻는 핵심 요점은 틀릴 수가 없습니다. Identity Theft Resource Center의 2022년 데이터 침해 보고서에 따르면 현재 데이터 유출 사고가 하루에 다섯 차례 가까이 발생하고 있으며, 이러한 상황에서는 사용 편의성이 보안성에게 밀릴 수밖에 없습니다. 4가지 주요 산업에 종사하는 응답자 중 보안과 사용 편의성에 각각 75%와 25%의 비중을 두고 있다고 답한 응답자가 가장 많았으며, 각 산업마다 보안을 최우선순위로 삼는다고 답한 비율이 두 번째로 많았습니다. 직원과 계약자를 대상으로 마찰을 최소화하는 것도 중요하지만 규제가 심한 산업에서는 사용자 경험을 최적화하지 못하는 위험이 보안 또는 규정을 위반하는 위험보다 크지 않습니다.

산업별 Zero Trust 진행 상황

의료

의료 분야는 진행 속도가 느릴 때도 있지만 여기에서 속한 기업들은 Zero Trust를 계획하여 실행하는 데 적극적으로 나서고 있습니다. 의료 분야에 종사하는 응답자들은 대부분 Zero Trust 이니셔티브를 시행하고 있거나, 가까운 미래에 시행할 계획을 가지고 있습니다. 의료 분야에서는 다수의 기업들이 아직까지도 보안 수준이 낮아 위험한 인증 요소에서 탈피하는 데 어려움을 겪고 있지만, 이들은 대체로 아이덴티티의 중요성을 인지하여 MFA와 SSO를 내/외부 사용자는 물론이고 데이터베이스와 기타 리소스까지 확대 적용하고 있습니다.

100%에 근접하는 Zero Trust 정의 및 계획 수립 단계

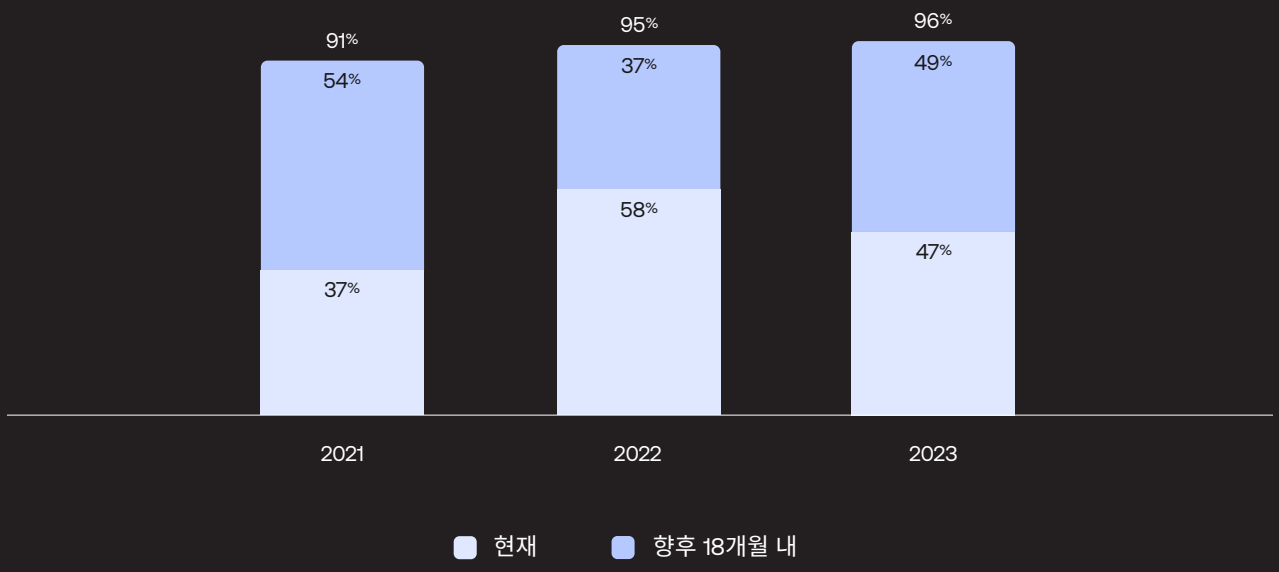
의료 산업에서는 지난 3년 동안 Zero Trust 이니셔티브에 대한 관심이 커졌다가 사그라들었지만 그리 큰 변동은 없었습니다. 올해 설문조사에 참여한 의료 기업들 중 Zero Trust 이니셔티브를 이미 시행하고 있거나, 향후 18개월 이내에 시행할 계획이라고 답한 비율도 단 4%에 불과합니다. 하지만 이니셔티브를 시행 중이거나 가까운 미래에 시행할 예정인 의료 기업의 총 수가 해를 거듭할수록 100%에 근접하고 있습니다. (올해는 이니셔티브를 이미 시행 중이라고 답한 기업의 수가 작년 보고서보다 적었습니다. The Wall Street Journal의 보도에 따르면, 이렇게 줄어든 이유는 2022년 IT 지출 감소에 기인할 가능성이 높지만 지금은 상황이 달라질 수도 있습니다). 모든 상황을 종합해 볼 때, 앞으로 Zero Trust 이니셔티브를 시행하는 의료 기업들이 늘어나는 동시에 이미 시행 중인 기업들은 이니셔티브를 발전시켜 나갈 것입니다.

아직은 평균보다 약간 뒤처져 있지만 곧 따라잡을 예정인 의료 분야

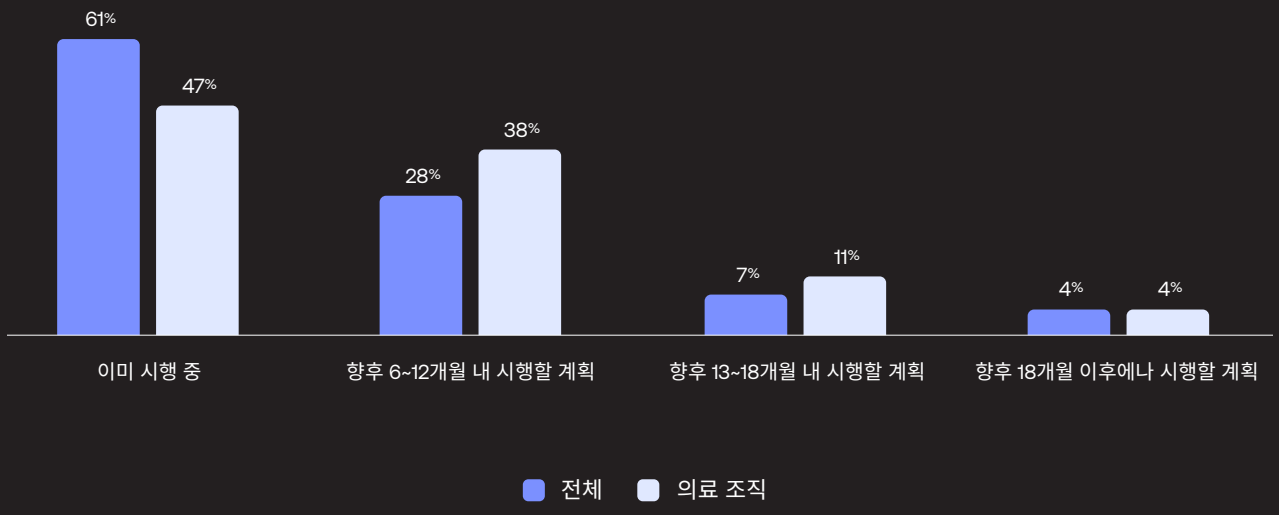
의료 기업의 성과와 글로벌 기업의 성과를 비교하면, 현재 Zero Trust 이니셔티브를 시행 중인 의료 기업의 수는 글로벌 평균에 미치지 못합니다. 하지만 이러한 기업들도 이 수치를 따라잡기 위해 부단히 노력하고 있으며, 향후 6~12개월 내 시행 계획을 따져보면 오히려 의료 기업이 38%이고, 글로벌 기업이 28%로 글로벌 기업들을 압도합니다.

의료 산업에 종사하는 응답자들에게 Zero Trust 보안 전략에 대한 아이덴티티의 중요성을 물어본 결과, 10명 중 9명 이상이 아이덴티티가 매우 중요하거나, 다소 중요하다고 답했습니다. 의료 분야의 기업들에게는 개인 식별 정보가 너무나 민감하여 보안이 무엇보다 중요하다는 점을 감안하면 이러한 설문조사 결과도 그다지 놀랄 일이 아닙니다.

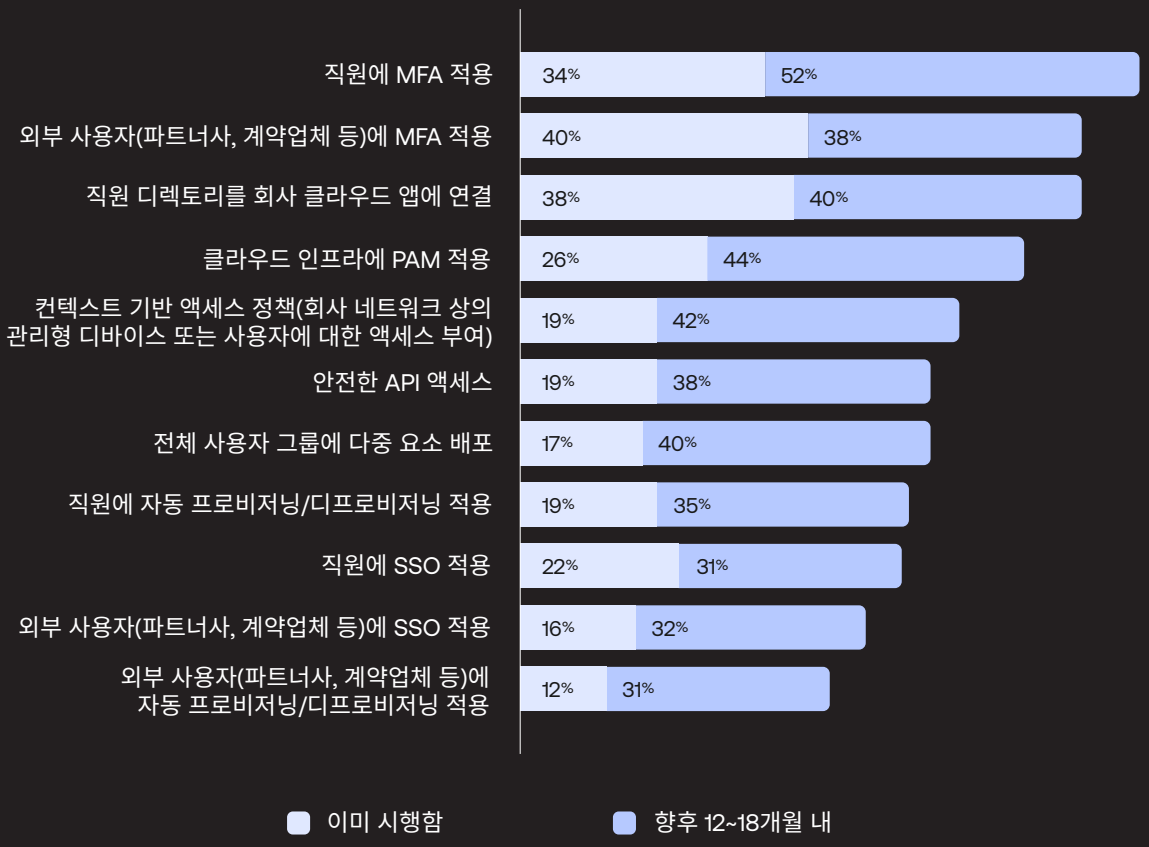
귀사는 현재 확고한 Zero Trust 보안 이니셔티브를 시행 중입니까? 아니면 향후 18개월 내에 시행할 계획입니까?
의료 분야 연도별 비교



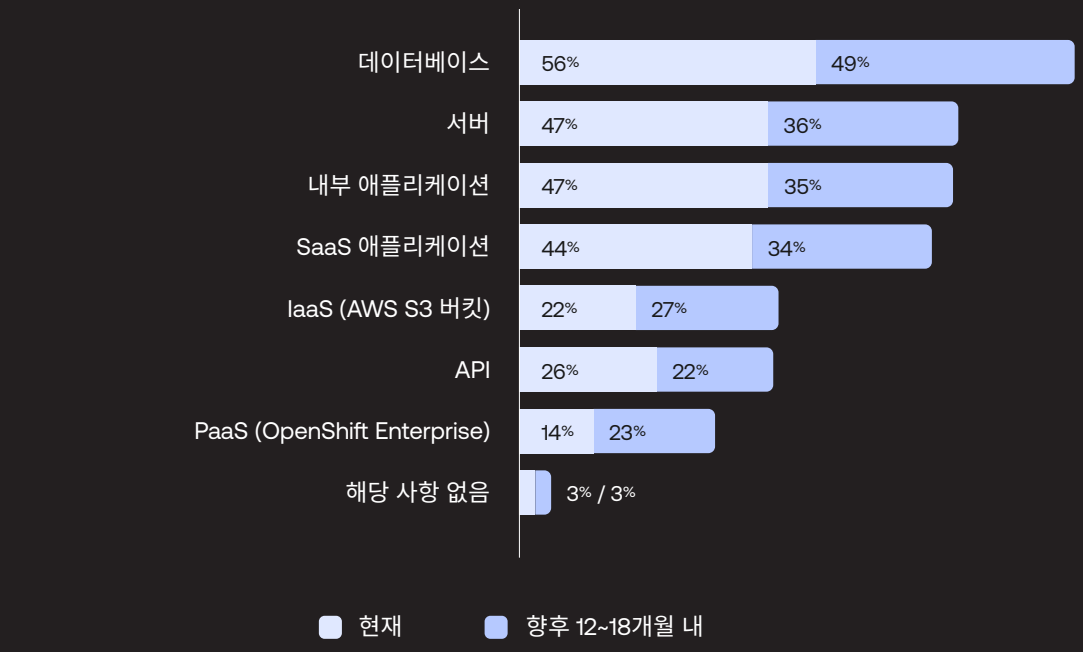
귀사는 현재 확고한 Zero Trust 보안 이니셔티브를 시행 중입니까? 아니면 향후 수개월 내에 시행할 계획입니까?
의료 분야 응답자와 전체 응답자 간 비교



다음 중 귀사에서 이미 시행하고 있거나, 향후 12~18개월 이내에 시행할 예정인 이니셔티브는 무엇입니까?
의료



다음 중 SSO 및/또는 MFA를 이미 확대 적용하고 있는 리소스 클래스는 무엇이며, 향후 12~18개월 내에 확대 적용할 예정인 리소스 클래스는 무엇입니까?
의료



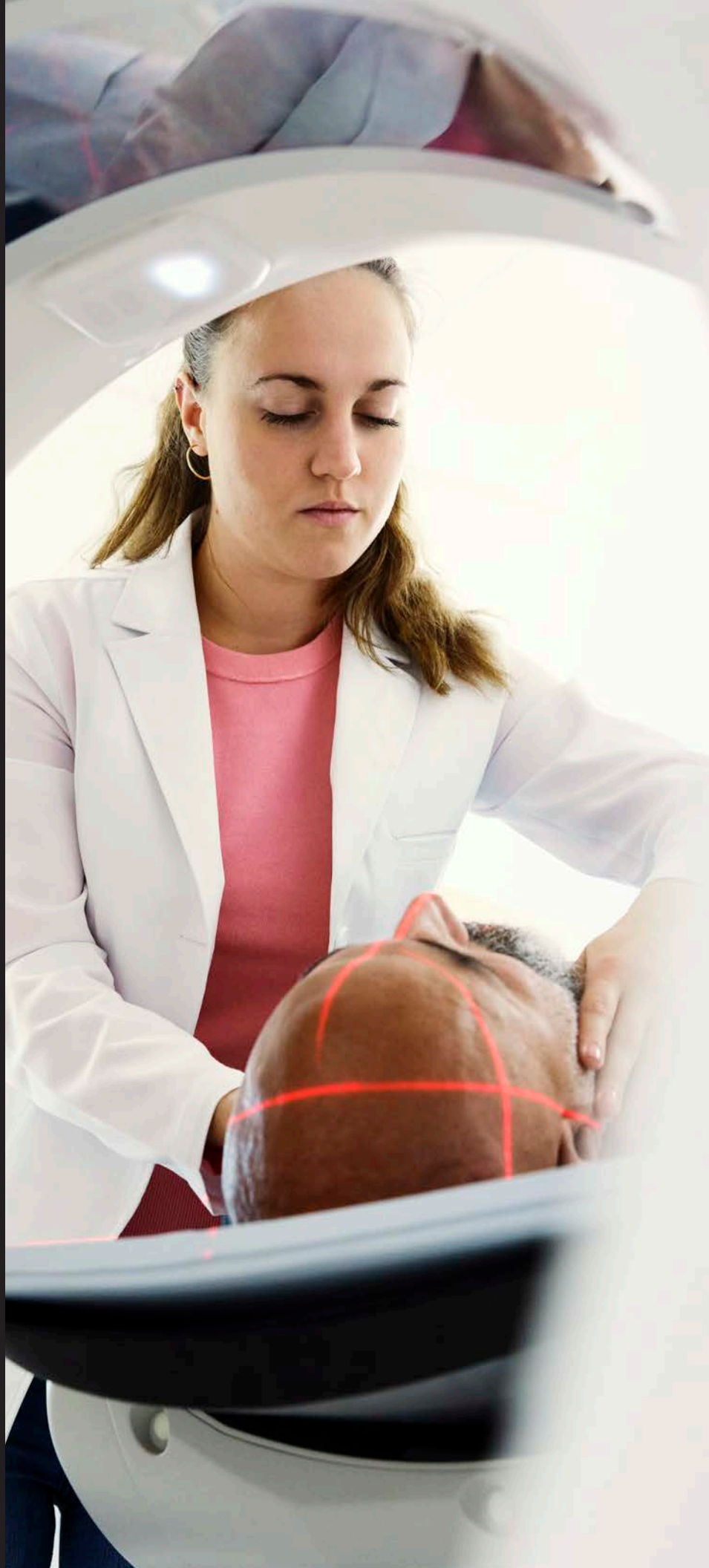
참고: 복수의 답안을 선택한 응답자들로 인해 각 비율 열의 총합이 100%를 넘을 수도 있습니다.

의료 분야에서 가장 많이 시행하는 MFA 및 디렉터리 연결 이니셔티브

의료 기업에게 가장 인기 있는 이니셔티브로는 직원 및 외부 사용자에 대한 MFA 적용으로, 올해도 마찬가지였습니다. 클라우드 앱에 대한 직원 디렉터리 연결 역시 이미 시행 중인 보안 이니셔티브에서 항상 상위 3위 안에 포함됩니다. 설문조사에 참여한 의료 기업 중 1/3 이상이 MFA를 직원에게 이미 적용하고 있었으며, 향후 MFA를 직원에게 추가할 계획이라고 답한 기업도 52%로 가장 많았습니다. 그 밖에 SSO, 프로비저닝 자동화와 같은 이니셔티브는 올해 의료 기업들이 계획 중인 우선순위에서 하위권으로 떨어졌습니다.

SSO/MFA 보안 순위에서 상위권을 차지한 데이터베이스, 서버 및 앱

의료 기업들은 SSO 및/또는 MFA 보안을 데이터베이스까지 확장하여 적용한 비율이 가장 많았습니다. 그 이유는 중요한 환자 정보가 데이터베이스에 저장되어 사이버 범죄자들의 주요 표적이 되기 때문입니다. 그렇다고 SSO/MFA를 서버와 내부 및 SaaS 앱에 확대 적용하는 비율이 의료 기업들이 이미 도입하고 있거나 앞으로 도입할 계획인 이니셔티브에서 크게 뒤처지는 것도 아닙니다.



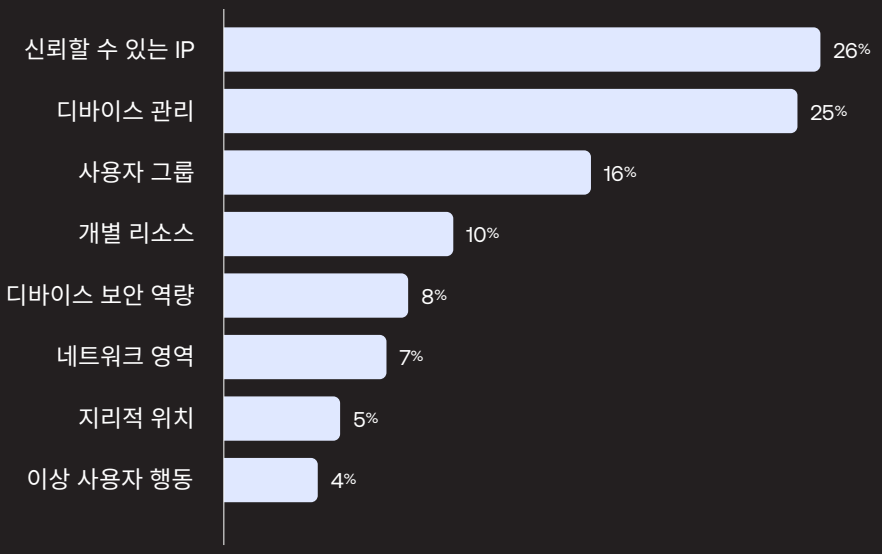
액세스 제어 요소에서 상위권을 차지한 신뢰할 수 있는 IP와 디바이스 관리

설문조사에 참여한 의료 기업 중 내부 리소스에 대한 액세스를 제어하고 승인할 때 신뢰할 수 있는 IP 또는 디바이스 관리를 최우선으로 고려하는 비율이 50%를 넘으면서 각각 1위와 2위로 전 세계 응답자들의 선택을 받았습니다. 그 다음으로 사용자 그룹과 개별 리소스가 액세스를 제어하고 승인할 때 두 번째로 많이 이용하는 요소였습니다.

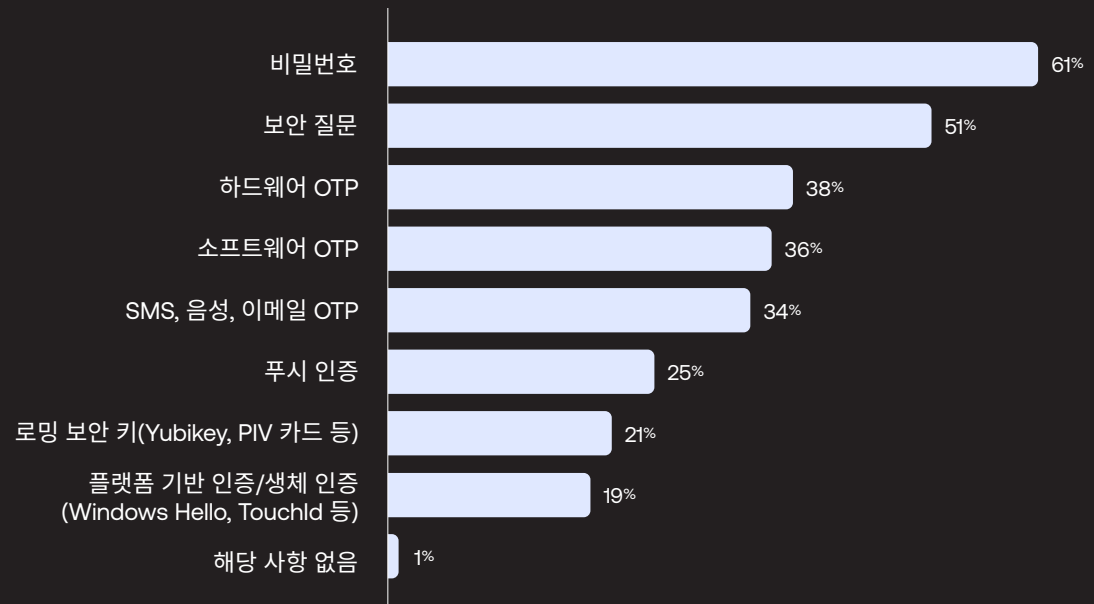
의료 분야에서 가장 많이 이용되는 인증 요소인 비밀번호와 보안 질문

비밀번호는 아직까지 의료 기업들이 가장 많이 이용하는 인증 요소입니다. 응답자의 61%가 비밀번호를 사용한다고 밝힌 것으로 보아, 의료 분야에서 패스워드리스의 미래는 요원해 보입니다. 이어서 보안 질문이 2위를 차지했는데, 설문조사에 참여한 의료 기업 중 50% 이상이 사용하고 있다고 밝혔습니다. 하드웨어, 소프트웨어, SMS/음성/이메일 등의 형태로 제공되는 일회용 비밀번호(OTP)가 사실상 공동 3위를 차지했고, 플랫폼 기반의 인증 서비스와 생체인식을 인증 요소로 사용한다고 답한 비율은 가장 적었습니다.

귀사의 내부 리소스에 대한 액세스를 제어하고 승인할 때 가장 중요한 요소를 평가해 주십시오.
의료



귀사에서 내/외부 사용자를 인증할 때 사용하는 인증 요소를 선택하십시오.
의료



산업별 Zero Trust 진행 상황

공공 부문

Zero Trust를 통해 보안을 강화해야 한다는 부담을 글로벌 공공 부문만큼 안고 있는 산업은 아마 없을 것입니다. 예를 들어 북미 지역에서 미국의 연방 Zero Trust 전략을 보면, 모든 연방 기관은 2024년 9월까지 특정 사이버 범죄 기준과 목적을 달성하여 점차 진화하는 지속적 위협 캠페인에 맞설 수 있는 안보 역량을 강화해야 한다고 명시하고 있습니다. 미국 정부의 지침은 이게 다가 아닙니다. 국가 사이버 안보 전략과 국무부의 Zero Trust 전략 및 로드맵도 있습니다.

올해 Okta는 북미, EMEA 및 APJ 지역의 공기업들을 대상으로 설문조사를 실시했습니다. (본 보고서에서 주 또는 지역 기관은 공기업에서 제외했습니다). 설문조사에서 공기업의 58%가 이미 Zero Trust 이니셔티브를 시행 중이었고, 38%가 곧 시행할 계획이라고 답했습니다. 이러한 기업들은 SSO 및/또는 MFA를 사용해 중요한 리소스를 안전하게 보호하는 동시에 인프라와 자산을 보호할 목적으로 강력한 경계를 구축하고 있습니다.

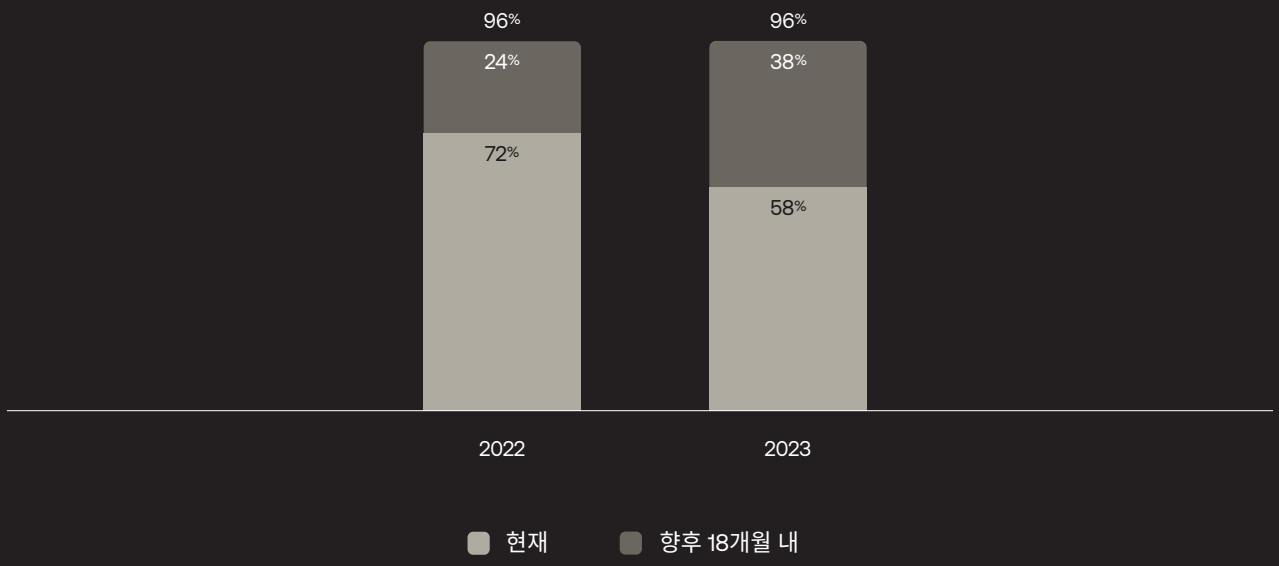
Zero Trust 이니셔티브에 거의 모두 동참하고 있는 공기업들

Zero Trust를 향한 공기업의 노력은 변함이 없습니다. 2022년부터 2023년까지 Zero Trust를 이미 시행하고 있거나 곧 시행할 예정인 공기업의 전체 비율은 96%를 꾸준히 유지했습니다. 지난해 설문조사에 참여한 공기업 중 무려 72%가 Zero Trust 이니셔티브를 시행했습니다. 하지만 여기에서 놓치지 말아야 할 사실은 지난해 공기업 응답자들은 거의 모두(86%) 북미 지역 종사자였다는 것입니다. 올해에는 설문조사 범위를 넓힌 덕분에 설문조사에 참여한 공기업 중 북미 지역 기업은 31%에 불과했으며, 이렇게 넓이진 표본 조사로 인해 Zero Trust 이니셔티브를 이미 시행 중이라고 답한 비율은 58%에 그쳤지만 곧 시행할 계획이라고 답한 비율도 38%에 달했습니다.

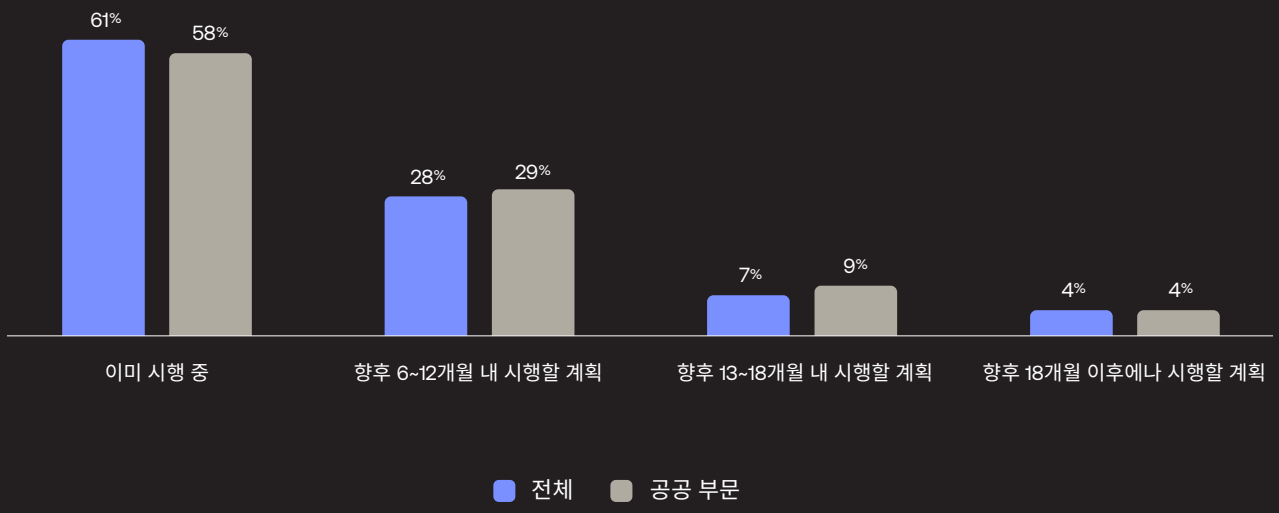
이니셔티브에서는 뒤처지지만 계획에서 앞서가는 공기업들

올해 설문조사에 참여한 공기업 중 Zero Trust 보안 이니셔티브를 이미 시행 중인 기업의 비율이 글로벌 평균과 거의 같은 수치를 보였습니다. 전체 기업 중 61%가 관련 프로그램을 이미 진행 중인 반면 공기업들은 58%가 시행하고 있습니다. 대부분이 정부 지침에 따른 조치이긴 하지만 1/3에 달하는 공기업이 향후 6~12개월 이내에 이니셔티브를 시행할 계획을 세우면서 글로벌 평균을 근소한 차이로 앞서고 있습니다.

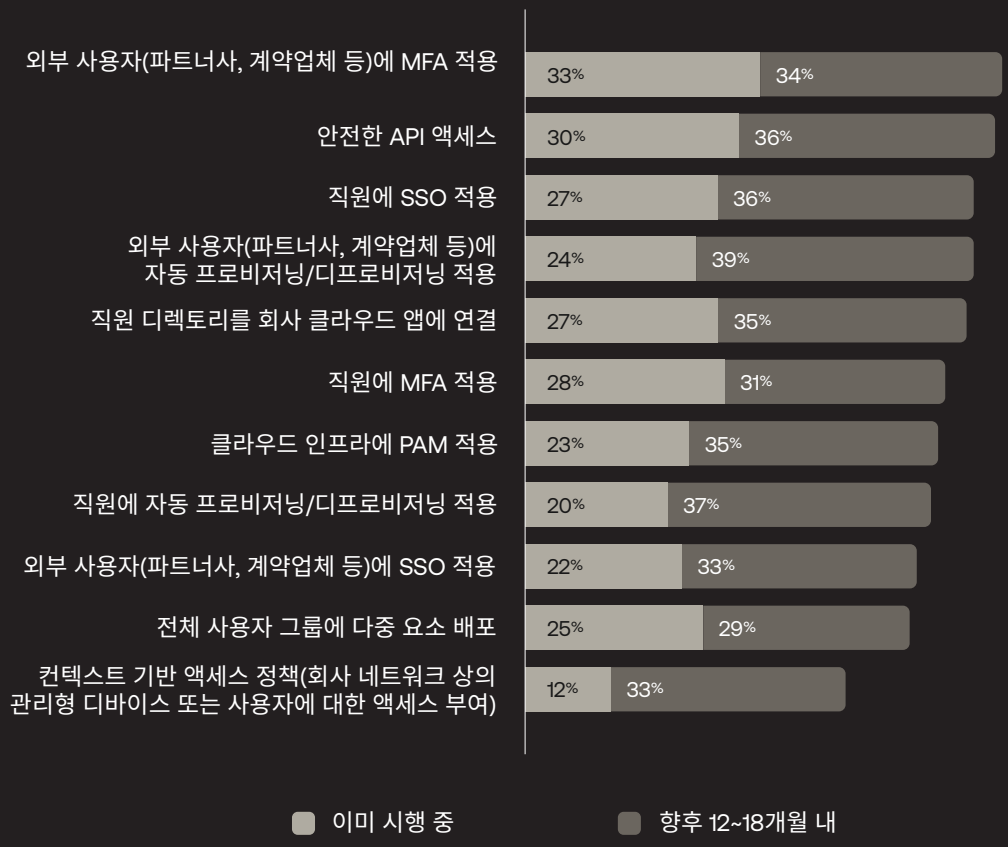
귀사는 현재 확고한 Zero Trust 보안 이니셔티브를 시행 중입니까? 아니면 향후 18개월 내에 시행할 계획입니까?
공공 부문 연도별 비교



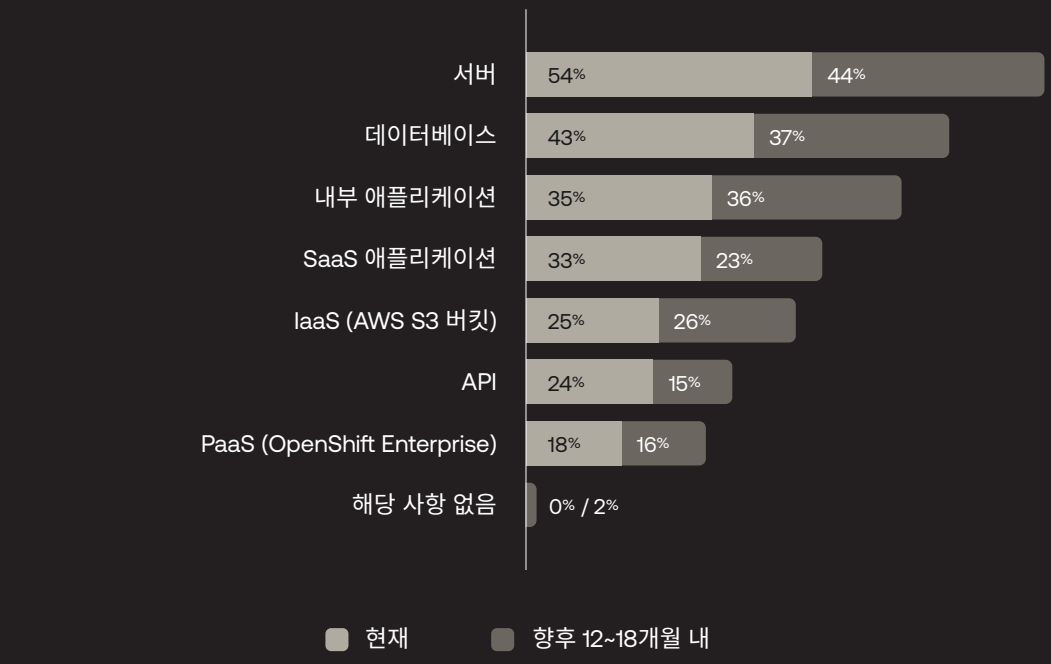
귀사는 현재 확고한 Zero Trust 보안 이니셔티브를 시행 중입니까? 아니면 향후 수개월 내에 시행할 계획입니까?
공공 부문 응답자와 전체 응답자 간 비교



다음 중 귀사에서 이미 시행하고 있거나, 향후 12~18개월 이내에 시행할 예정인 이니셔티브는 무엇입니까?
공공 부문



다음 중 SSO 및/또는 MFA를 이미 확대 적용하고 있는 리소스 클래스는 무엇이며, 향후 12~18개월 내에 확대 적용할 예정인 리소스 클래스는 무엇입니까?
공공 부문



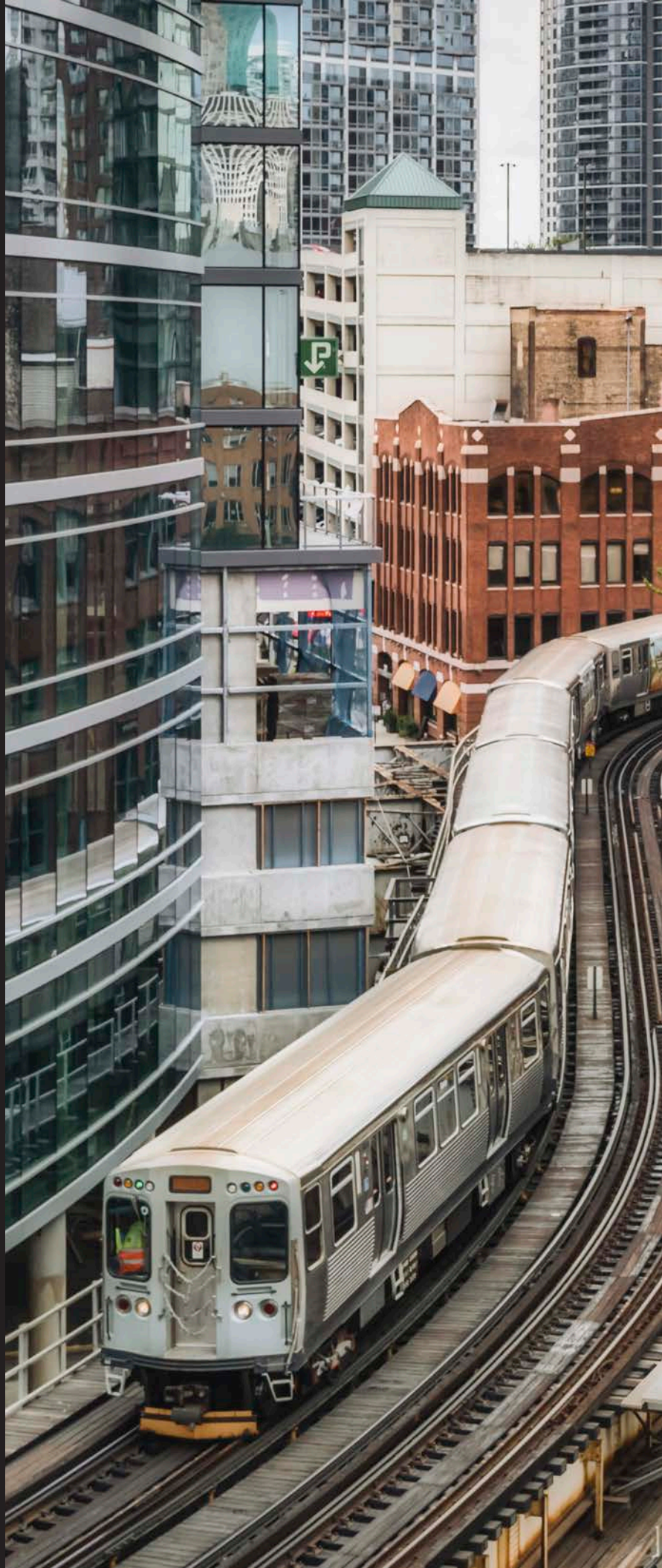
참고: 복수의 답안을 선택한 응답자들로 인해 각 비율 열의 총합이 100%를 넘을 수도 있습니다.

공공 부문 이니셔티브에서 가장 인기 있는 “외부 사용자에 대한 MFA 적용”과 “API 액세스 보호”

각국의 정부 기관들은 다양한 해외 계약자 및 외부 파트너와 협력하기 때문에 외부 사용자(파트너 및 제3자 공급업체 포함)에 대한 MFA 적용과 API 액세스 보호라고 답한 공기업 응답자의 비율이 각각 33%와 30%로 가장 많은 것도 그리 놀랄 일이 아닙니다. 또한 향후 12~18개월 이내에 MFA를 외부 사용자에게 확대 시행할 예정인 공기업도 34%에 달합니다. 뒤이어 직원에 대한 SSO 시행과 외부 사용자에 대한 프로비저닝/디프로비저닝 자동화가 2위를 차지했습니다.

SSO/MFA 보안을 우선적으로 서버와 데이터베이스까지 확장

현재 공공 부문에서는 SSO 및 MFA 보호와 관련하여 서버와 데이터베이스가 주축을 이루고 있습니다. 설문조사에 참여한 공기업 중 절반 이상이 SSO 및/또는 MFA 보안을 서버에 이미 적용 중이라고 답했고, 43%는 데이터베이스에 적용하고 있다고 답했습니다. 2위는 기업의 약 1/3이 확대 시행 중인 내부 앱과 SaaS 앱이 차지하였고, IaaS, API 및 PaaS가 그 뒤를 이었습니다.



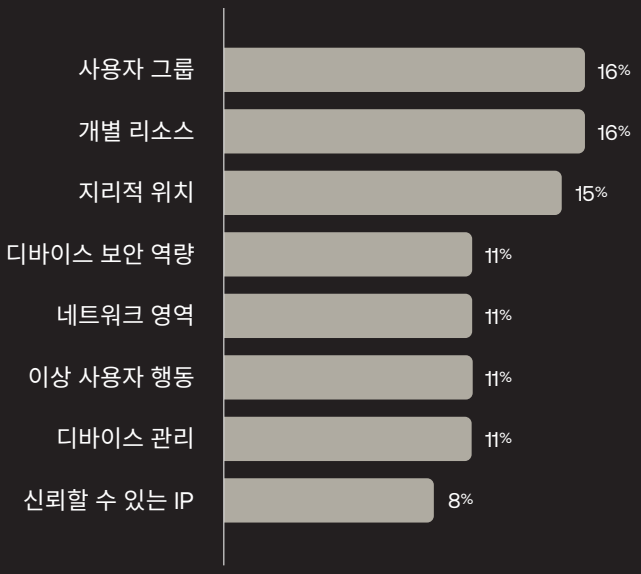
리소스에 액세스할 때 무엇보다 중요한 “사용자 그룹” 및 “리소스” 요소

공기업들은 반갑지 않은 시선으로부터 조직의 디지털 자산을 보호하는 데 특히 신경을 씁니다. 내부 리소스에 대한 액세스를 제어하고 승인할 때 가장 많이 적용하는 요소는 사용자 그룹이었으며 개별 리소스와 지리적 위치가 그 뒤를 이었고, 나머지 요소들은 비슷한 비율을 보였습니다.

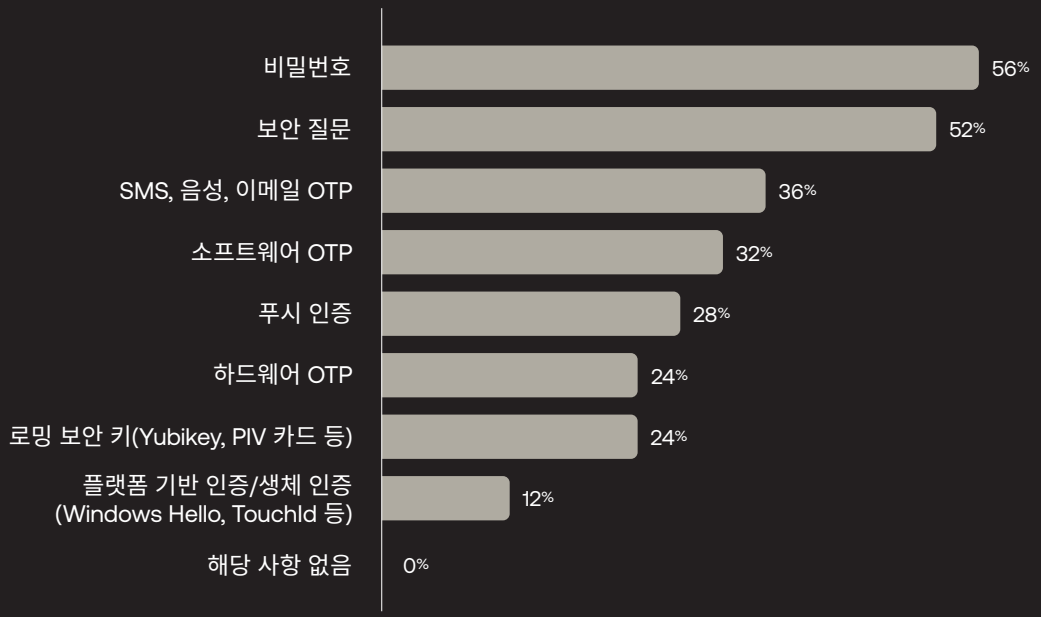
사용자 인증 시 아직도 가장 많이 사용되고 있는 “비밀번호”와 “보안 질문”

본 보고서에서 다른 요소보다 비밀번호와 보안 질문을 인용한 응답자가 더 많았던 것처럼, 공공 부문에서는 보안 수준이 비교적 낮은 인증 요소들이 아직도 많이 사용되고 있습니다. 하지만 소프트웨어/하드웨어 OTP, SMS/음성/이메일 OTP 같이 보안 수준이 높은 요소들이 인기를 끌며 분위기가 달라지고 있습니다. (OTP 요소는 일회용이라는 특성 때문에 저장 및 해킹이 가능한 비밀번호와 보안 질문에 비해 근본적으로 더 안전합니다). ■

귀사의 내부 리소스에 대한 액세스를 제어하고 승인할 때 가장 중요한 요소를 평가해 주십시오.
공공 부문



귀사에서 내/외부 사용자를 인증할 때 사용하는 인증 요소를 선택하십시오.
공공 부문



산업별 Zero Trust 진행 상황

금융 서비스

금융 서비스 기업은 사이버 공격의 주된 표적으로, 지난 몇 년간 보안 사고로 특히 큰 피해를 입었습니다. 일례로 2022년 미국 내 79곳 이상의 금융 서비스 기업의 보고에 따르면, 데이터 유출로 인해 1,000명 이상의 소비자들이 피해를 입었으며 대규모 유출 사고가 일어날 때마다 수백만 명의 소비자가 피해를 입은 것으로 나타났습니다. Zero Trust는 이러한 기업들에게 앞으로 중요한 시스템과 고객 데이터를 안전하게 보호할 수 있는 방법을 제시합니다. 현재 금융 서비스 기업 중 2/3 이상이 Zero Trust 이니셔티브를 이미 시행 중이며, 나머지 기업들도 대부분 이니셔티브를 계획 중입니다.

기업 10곳 중 7곳이 Zero Trust 이니셔티브를 시행하고 있는 금융 서비스 분야

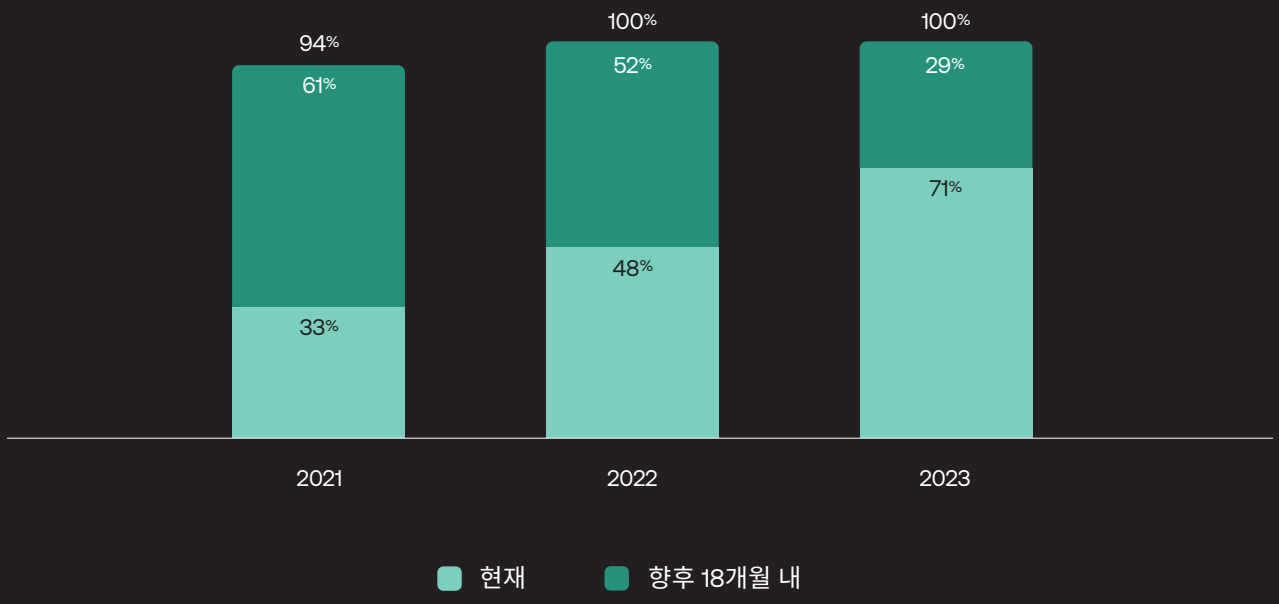
보안 사고로 인한 피해는 걷잡을 수 없이 커질 수 있습니다. IBM의 2023년 데이터 유출 비용 보고서에 따르면, 보안 사고 1건당 평균 피해액만 445만 달러에 이릅니다. 따라서 금융 서비스 분야에서 Zero Trust 이니셔티브를 시행하는 기업이 매년 늘어나는 것도 우연이 아닙니다. 2021년에는 금융 서비스 분야에 종사하는 응답자들 중 확고한 Zero Trust 이니셔티브를 시행하고 있다고 밝힌 비율이 1/3에 불과했지만 2022년에는 이 수치가 절반 가까이 상승했습니다. 올해는 설문조사에 참여한 금융 서비스 기업 중 무려 71%가 현재 Zero Trust 이니셔티브를 시행하고 있다고 답했습니다. 3년 연속 상승 곡선이라는 점에서 매우 인상적인 결과입니다.

Zero Trust 이니셔티브의 대중화를 주도하고 있는 금융 서비스 분야

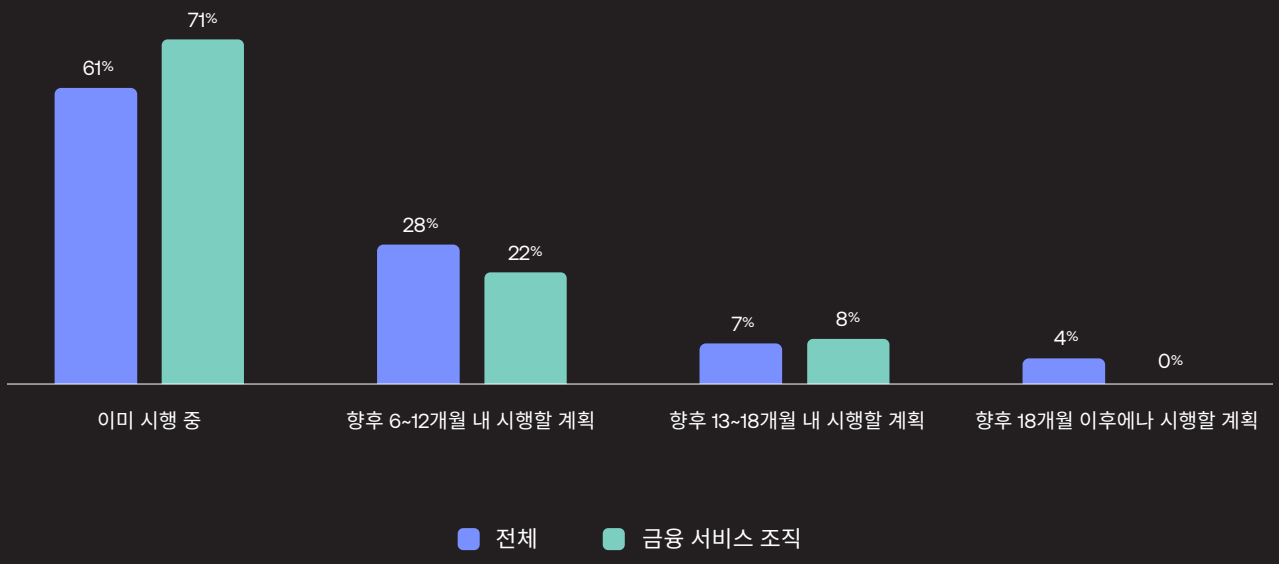
금융 서비스 기업의 2/3 이상이 확고한 Zero Trust 이니셔티브를 이미 시행 중이며, 향후 12개월과 18개월 이내에 시행할 예정인 기업은 각각 22%와 8%인 것으로 나타났습니다. 또한 이니셔티브를 이미 시행 중인 비율이 글로벌 평균을 넘어섰으며, 설문조사에 참여한 금융 서비스 기업들 모두 Zero Trust 이니셔티브를 이미 시행 중이거나 18개월 이내에 시행할 계획이라고 답했습니다.

제로 트러스트에 대한 아이덴티티의 가치 측면에서 금융 서비스 분야는 전적으로 동의하고 있습니다. 금융 서비스 응답자 중 90% 이상이 아이덴티티가 Zero Trust 전략에 매우 또는 다소 중요하다고 답했으며, 매우 중요하다고 답한 비율도 50%에 육박합니다. 중요하지 않거나, 매우 중요하지 않다고 응답한 비율은 약 2%에 불과합니다.

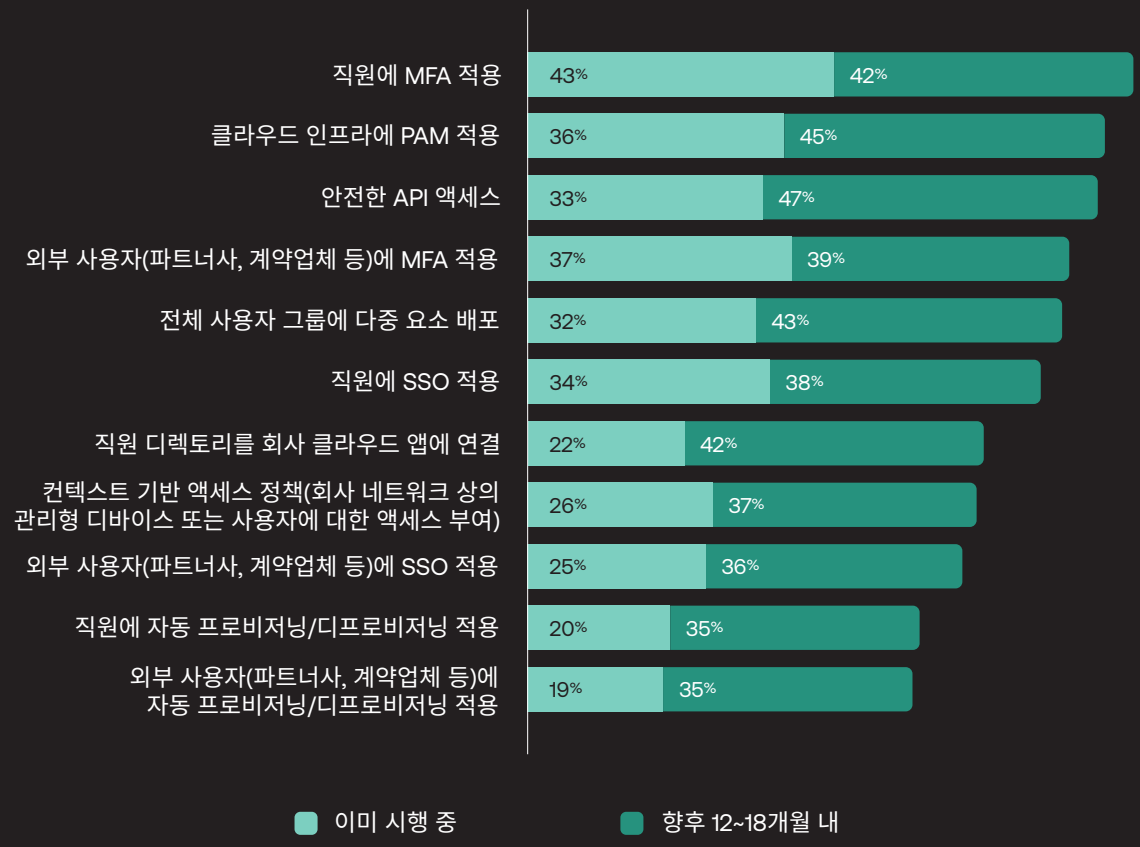
귀사는 현재 확고한 Zero Trust 보안 이니셔티브를 시행 중입니까? 아니면 향후 18개월 내에 시행할 계획입니까?
금융 서비스 연도별 비교



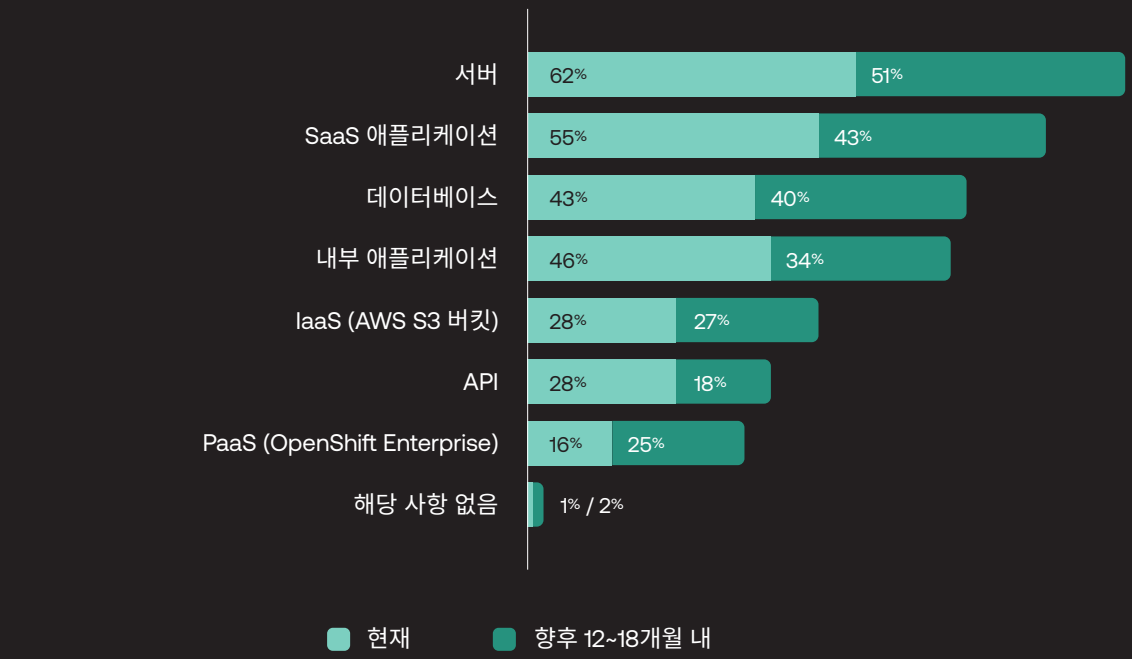
귀사는 현재 확고한 Zero Trust 보안 이니셔티브를 시행 중입니까? 아니면 향후 수개월 내에 시행할 계획입니까?
금융 서비스 응답자와 전체 응답자 간 비교



다음 중 귀사에서 이미 시행하고 있거나, 향후 12~18개월 이내에 시행할 예정인 이니셔티브는 무엇입니까?
금융 서비스



다음 중 SSO 및/또는 MFA를 이미 확대 적용하고 있는 리소스 클래스는 무엇이며, 향후 12~18개월 내에 확대 적용할 예정인 리소스 클래스는 무엇입니까?
금융 서비스



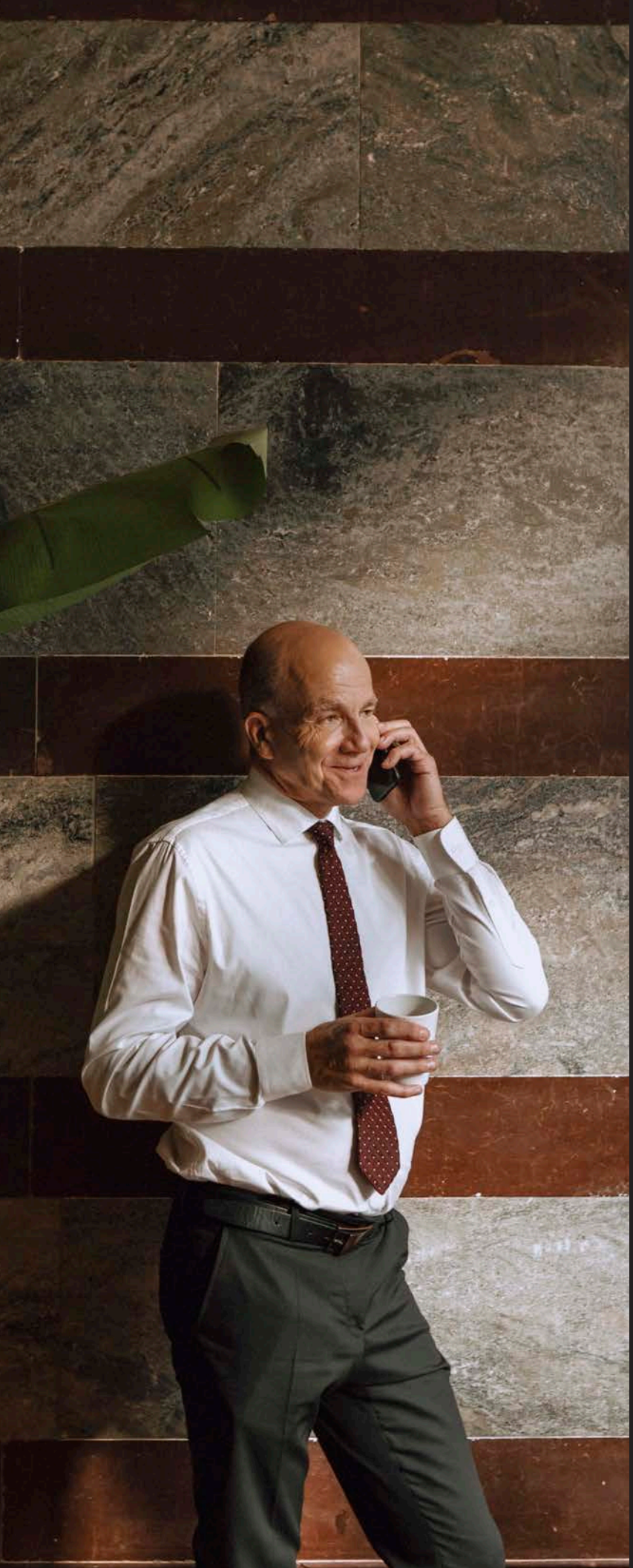
참고: 복수의 답안을 선택한 응답자들로 인해 각 비율 열의 총합이 100%를 넘을 수도 있습니다.

금융 서비스 분야에서 가장 인기 있는 이니셔티브: MFA, 권한 있는 액세스 관리

직원에 대한 MFA 적용은 올해 금융 서비스에 종사하는 응답자 중 43%가 이미 시행 중이고, 42%가 향후 12~18개월 이내에 시행할 예정이라는 점에서 금융 서비스 기업들에게 가장 인기 있는 Zero Trust 이니셔티브라고 할 수 있습니다. 다음으로 클라우드에 대한 권한 있는 액세스 관리가 36%로 2위를 차지했고, API에 대한 액세스 보호가 33%로 그 뒤를 이었습니다. 그 밖에 순위로는 외부 사용자에 대한 SSO 적용과 프로비저닝/디프로비저닝 자동화가 있었습니다.

SSO 및/또는 MFA가 가장 많이 적용되는 서버와, 그 뒤를 이은 SaaS 애플리케이션

금융 서비스 기업들은 62%가 SSO 및/또는 MFA를 이미 서버까지 확대 적용하여 액세스를 보호하고 있으며, 51%가 가까운 미래에 서버까지 범위를 확대 적용할 계획을 세우면서 서버에 대한 모니터링을 강화하고 있습니다. (복수 선택 가능). SaaS 앱, 데이터베이스 및 내부 앱은 금융 서비스 기업들이 이러한 아이덴티티 보안 조치를 적용하거나, 적용할 계획을 세울 때 가장 많이 언급된 리소스였습니다.



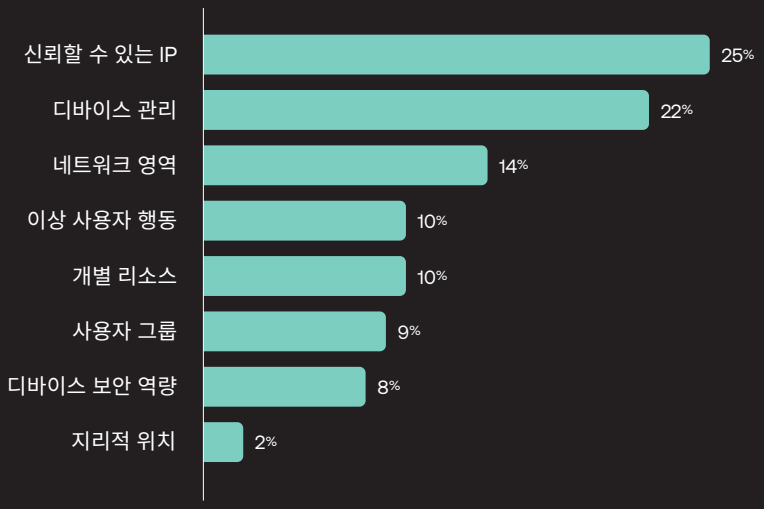
액세스 승인 요소에서 1, 2위를 차지한, 신뢰할 수 있는 IP와 디바이스 관리

금융 서비스 기업들이 내부 리소스에 대한 액세스를 제어하고 승인하려면 사용자가 어디에 있는지, 그리고 사용자가 어떤 디바이스를 사용하는지를 먼저 파악해야 합니다. 응답자 4명 중 1명이 신뢰할 수 있는 IP가 가장 중요한 액세스 승인 요소라고 답했으며, 22%는 디바이스 관리가 가장 중요한 요소라고 답했습니다. 이어서 네트워크 영역, 변칙적인 사용자 행동, 개별 리소스, 지리적 위치 순이었습니다.

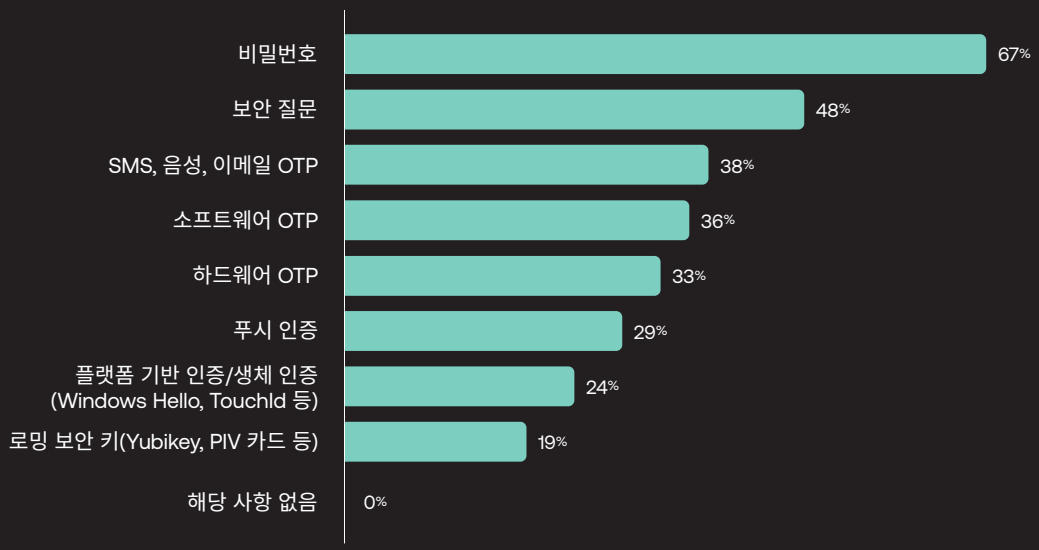
금융 서비스 분야에서 가장 많이 사용되는 인증 요소: 비밀번호, 보안 질문

응답자의 2/3가 현재 사용 중인 인증 요소로 비밀번호를 언급했듯이, 비밀번호는 아직도 금융 서비스 기업에서 가장 많이 사용하는 인증 요소입니다. 지식 기반 인증 요소인 보안 질문이 48%로 2위를 차지했고, 금융 서비스 분야 응답자의 약 1/3이 OTP 옵션을 택했습니다.

귀사의 내부 리소스에 대한 액세스를 제어하고 승인할 때 가장 중요한 요소를 평가해 주십시오.
금융 서비스



귀사에서 내/외부 사용자를 인증할 때 사용하는 인증 요소를 선택하십시오.
금융 서비스



산업별 Zero Trust 진행 상황

소프트웨어

앞선 두 해에는 소프트웨어가 나머지 주요 산업에 비해 뒤처지는 경우도 있었습니다. 하지만 꾸준히 성장하면서 Zero Trust 보안 이니셔티브를 추진한 결과, 본 보고서에서 강조한 것처럼 규제가 비교적 심한 주요 산업에 대한 인센티브가 부족함에도 불구하고 이제는 평균을 넘어서고 있습니다. 특히 소프트웨어 기업들은 올해 설문조사에서 다른 주요 산업에 비해 보안 수준이 더 높은 인증 요소를 사용하고 있다는 점에서 인증 기법 향상에 기여하고 있습니다.

소프트웨어 기업 중 2/3가 Zero Trust 이니셔티브 시행

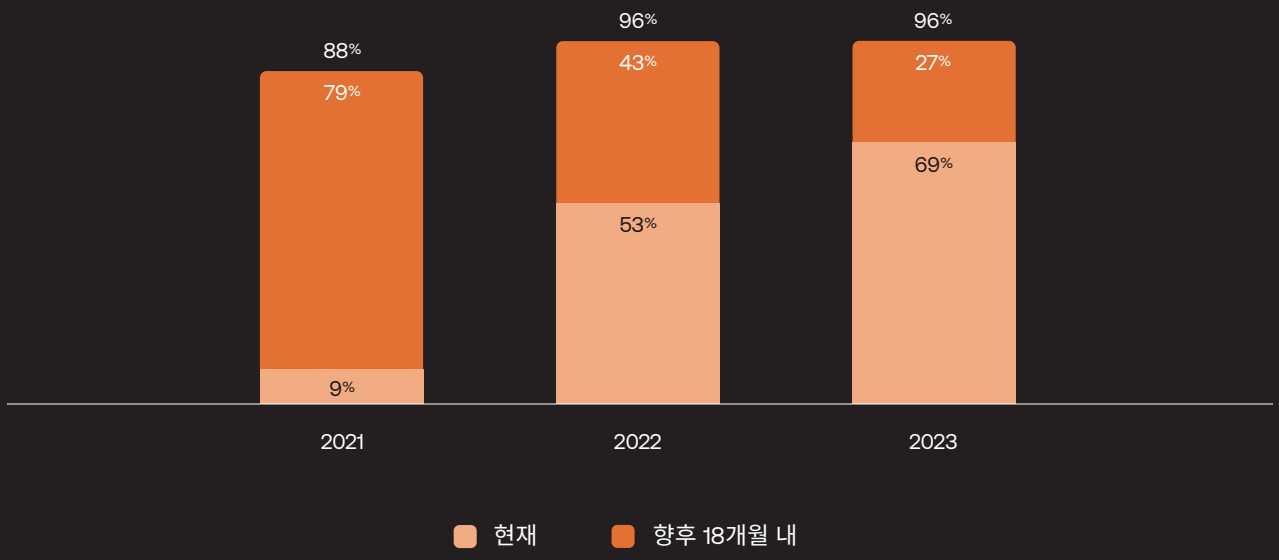
소프트웨어 기업들이 Zero Trust 여정에서 주요 산업 기업들을 빠르게 따라잡고 있습니다. 2021년 보고서에서는 현재 Zero Trust 이니셔티브를 시행하고 있다고 밝힌 소프트웨어 분야 응답자들이 10명 중 1명 미만이었지만 현재는 이 수치가 70%에 육박하며, 나머지 응답자들도 대부분 가까운 미래에 시행할 계획이라고 밝혔습니다. 설문조사에 참여한 소프트웨어 기업들 중에서 Zero Trust 이니셔티브를 시행하지 않고 있거나, 향후 18개월 이내에 시행할 계획도 없다고 응답한 비율은 단 4%에 불과합니다.

ZT 이니셔티브 시행에서 주요 산업 기업을 압도하고 있는 소프트웨어 기업

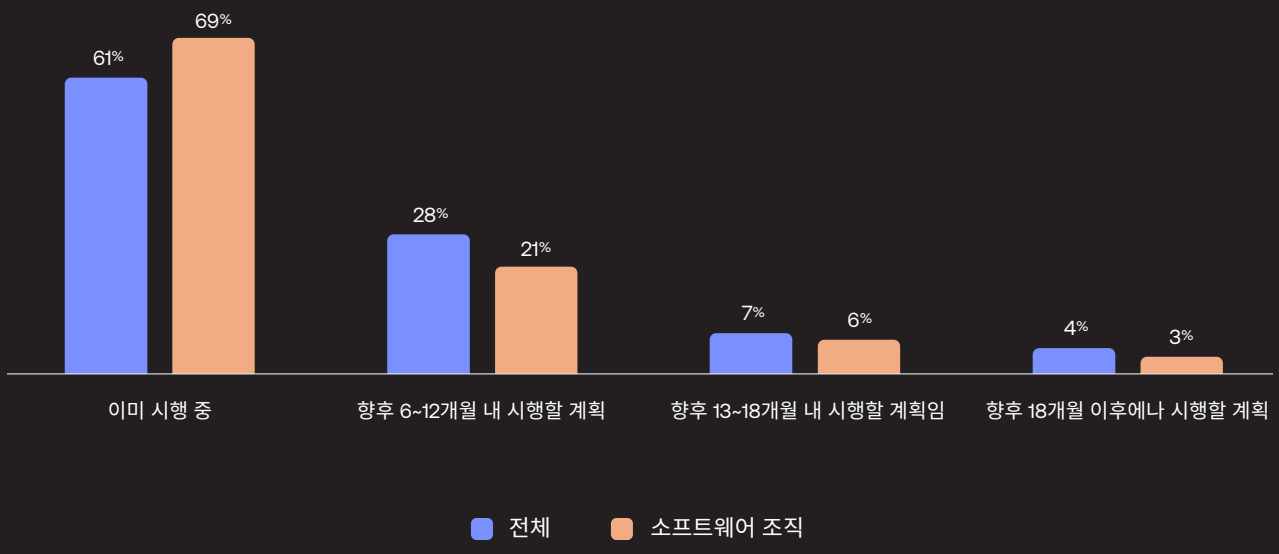
현재 소프트웨어 기업들은 확고한 Zero Trust 보안 이니셔티브를 시행하는 비율이 69%로, 전체 글로벌 평균인 61%를 상회합니다. 아직까지 주저하는 기업들도 향후 6~12개월 이내에(21%), 13~18개월 이내에(6%) 또는 18개월 이후(3%)에 이니셔티브를 시행할 계획이라고 답했습니다.

Okta의 설문조사 결과, 소프트웨어 분야는 Zero Trust에 대한 아이덴티티의 가치를 다른 주요 산업보다 더 잘 알고 있었습니다. Zero Trust 보안 전략에 대한 아이덴티티의 중요성에 관한 질문에, 소프트웨어 산업 응답자 10명 중 9명이 매우 중요하거나(54%), 다소 중요하다고(37%) 답한 반면, 다소 중요하지 않다고 응답한 비율은 1% 미만이었습니다.

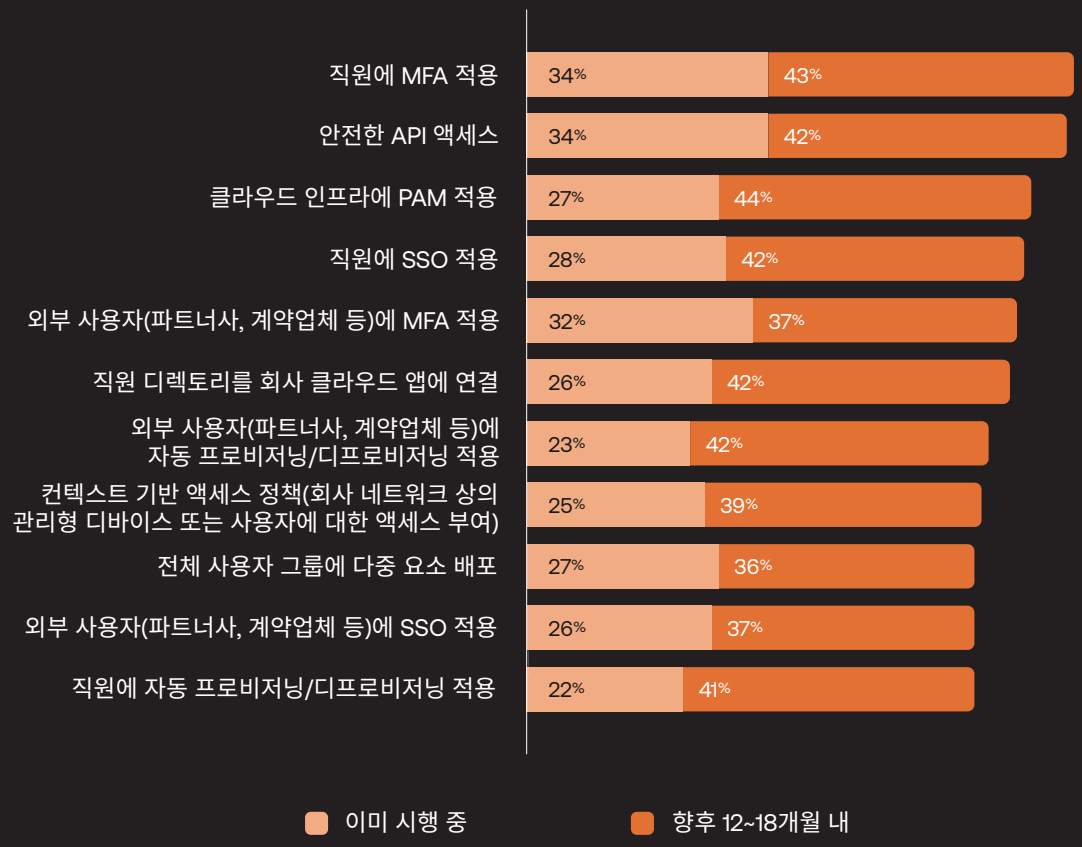
귀사는 현재 확고한 Zero Trust 보안 이니셔티브를 시행 중입니까? 아니면 향후 18개월 내에 시행할 계획입니까?
소프트웨어 분야 연도별 비교



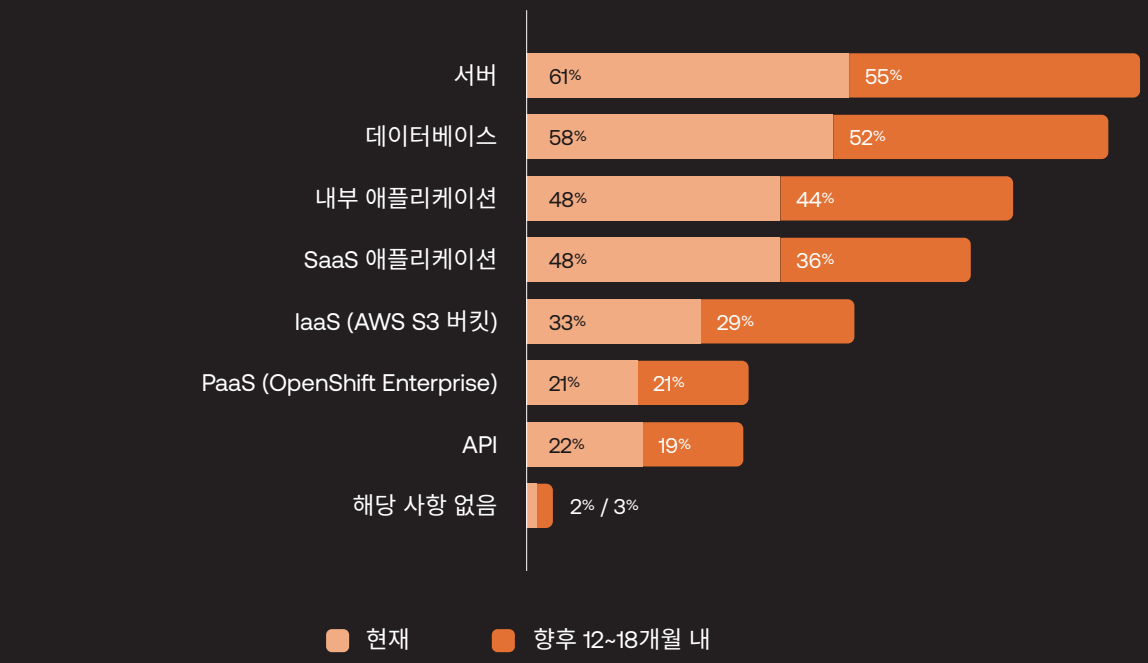
귀사는 현재 확고한 Zero Trust 보안 이니셔티브를 시행 중입니까? 아니면 향후 수개월 내에 시행할 계획입니까?
소프트웨어 분야 응답자와 전체 응답자 간 비교



다음 중 귀사에서 이미 시행하고 있거나, 향후 12~18개월 이내에 시행할 예정인 이니셔티브는 무엇입니까?
소프트웨어



다음 중 SSO 및/또는 MFA를 이미 확대 적용하고 있는 리소스 클래스는 무엇이며, 향후 12~18개월 내에 확대 적용할 예정인 리소스 클래스는 무엇입니까?
소프트웨어



참고: 복수의 답안을 선택한 응답자들로 인해 각 비율 열의 총합이 100%를 넘을 수도 있습니다.

소프트웨어 분야에서 가장 많이 시행하고 있는 이니셔티브: 직원에 대한 MFA 적용과 API 보안

직원에 대한 MFA 적용과 API 액세스 보호는 설문조사에 참여한 소프트웨어 기업들이 모두 중요하게 생각하는 보안 이니셔티브입니다. 두 카테고리에서 소프트웨어 기업 응답자의 34%가 이니셔티브를 이미 시행 중이라고 밝혔고, 5명 중 2명 이상이 향후 12~18개월 이내에 하나만, 혹은 둘 다 시행할 계획이라고 답했습니다. 소프트웨어 분야에 종사하는 기업들이 이미 시행 중인 보안 이니셔티브에서 외부 사용자에 대한 MFA 적용이 32%로 뒤를 이었습니다.

SSO/MFA 확장 시 가장 많이 사용되는 리소스: 서버, 데이터베이스

올해 소프트웨어 기업들은 대부분 SSO(Single Sign-On) 및/또는 다중 요소 인증(MFA)을 서버(61%)와 데이터베이스(58%)로 확장하여 액세스를 보호하는 데 힘썼습니다. 또한 설문조사에 참여한 응답자 중 48%가 현재 SSO 및/또는 MFA를 사용해 내부 앱을 보호하고 있다고 답했고, SaaS 리소스를 보호하고 있다고 답한 비율도 이와 동일했습니다.

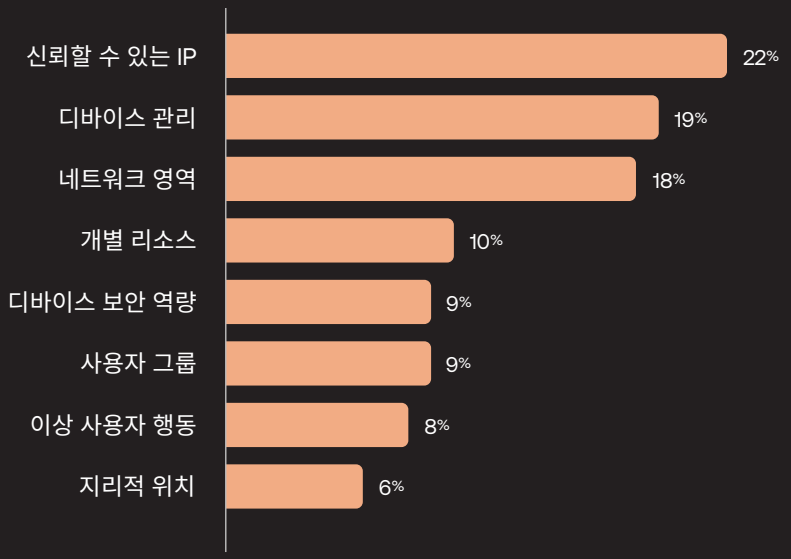
리소스에 액세스할 때 가장 중요한 요소: 신뢰할 수 있는 IP, 디바이스 관리

소프트웨어 기업들은 내부 리소스에 대한 액세스를 제어할 때 22%가 신뢰할 수 있는 IP를 가장 중요한 요소로 생각하고 있으며, 디바이스 관리와 네트워크 영역이 각각 19%와 18%로 2위와 3위를 차지했습니다. 10명 중 1명이 개별 리소스(예: 중요한 시스템)를 가장 중요한 요소로 선택한 반면 9%는 디바이스 보안 역량 또는 사용자 그룹을 선택했습니다. 소프트웨어 분야 응답자들 사이에서 중요하게 생각하는 요소로 가장 적은 선택을 받은 것은 지리적 위치였습니다.

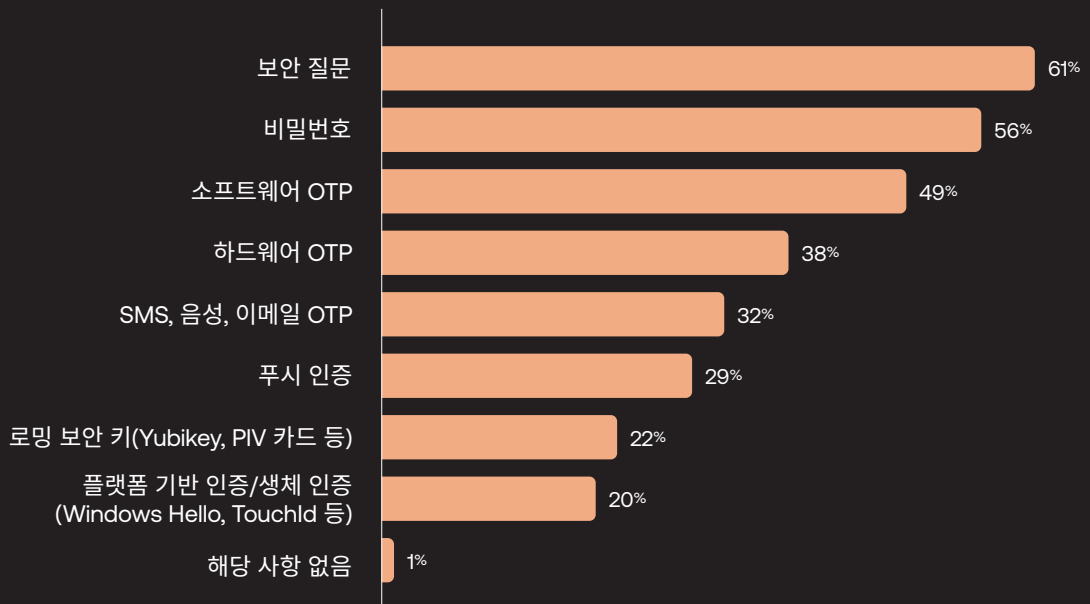
비밀번호를 제치고 소프트웨어 기업들에게서 가장 많이 사용하는 인증 요소로 선택받은 보안 질문

본 보고서에서 소프트웨어는 주요 산업 중 유일하게 비밀번호를 인증 요소로 가장 많이 사용하는 분야가 아닙니다. 응답 기업의 56%가 아직까지 사용하고 있다고 답해 2위를 차지하긴 했지만 소프트웨어 응답 기업의 61%가 보안 질문을 지목해, 적어도 소프트웨어 분야에서는 비밀번호가 설 자리를 잃고 있는 것처럼 보입니다. 무엇보다 분명한 점은, 보안 질문과 비밀번호 모두 보안 수준이 낮다 보니 OTP처럼 보안 수준이 높은 요소들이 그 자리를 대체하고 있습니다.

귀사의 내부 리소스에 대한 액세스를 제어하고 승인할 때 가장 중요한 요소를 평가해 주십시오.
소프트웨어



귀사에서 내/외부 사용자를 인증할 때 사용하는 인증 요소를 선택하십시오.
소프트웨어



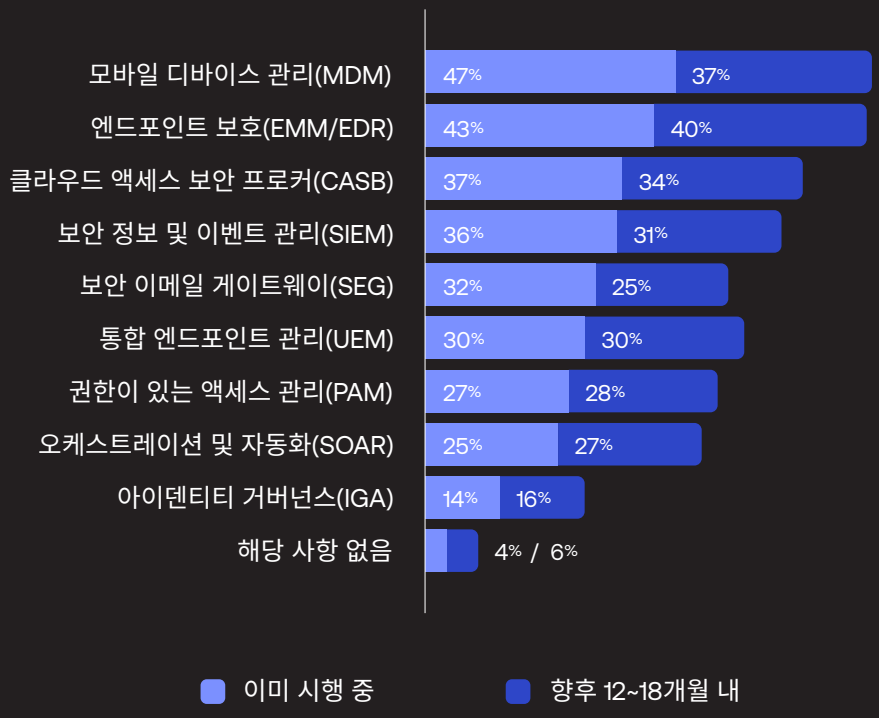
아이덴티티 기반 보안

진화하는 기업 에코시스템

아이덴티티가 새로운 보안 경계로 자리잡으면 보안 전략에서 자연스럽게 가장 중요한 역할을 하게 됩니다. 이제는 하이브리드/멀티 클라우드 기업들이 자사의 IAM 솔루션을 보안 시스템과 연계해야만 보안 팀도 인증을 받은 직원들의 효율을 떨어뜨리는 일 없이 조직 안팎의 위협을 차단할 수 있습니다. 다시 말해서 아이덴티티 관리 툴과 보안 스택을 통합하여 진정한 의미의 Zero Trust 에코시스템을 구축해야 합니다.

Okta는 보안 팀과 IT 팀 리더에게 어떤 툴을 IAM 시스템에 통합하여 사용하고 있는지, 그리고 가까운 미래에 어떤 툴을 통합할 계획을 가지고 있는지 물었습니다. 설문조사 결과, 보안 정보 및 이벤트 관리(SIEM)가 가장 많은 선택을 받으며 지난해와 다소 달라진 모습을 보였습니다. 모바일 디바이스 관리(MDM)는 현재 가장 널리 통합되어 있는 시스템입니다. Okta의 설문조사에 따르면, IAM 솔루션과 직접 통합할 때 "가장 중요하여" 우선적으로 고려할 3가지 시스템으로 SIEM, MDM 및 엔드포인트 보호가 꼽혔습니다.

다음 중 귀사에서 IAM 시스템에 이미 통합했거나, 향후 12~18개월 이내에 통합할 예정인 솔루션은 무엇입니까?
모든 응답자



2023년에 가장 인기가 많은 IAM 통합 솔루션: 모바일 디바이스 관리

모바일 디바이스 관리는 오랜 시간 꾸준히 인기를 끌면서(2021년 7위, 2022년 4위) 올해 가장 인기 있는 IAM 통합 솔루션으로 등극했습니다. 2021년에는 응답자의 11%가 MDM을 IAM 시스템에 통합했다고 밝힌 반면, 지금은 이 수치가 47%로 상승했습니다. 또한 향후 12~18개월 이내에 MDM을 통합할 계획인 응답자 비율도 37%에 달합니다. 업계는 앞으로도 통합 솔루션을 기반으로 강력한 보안 모니터링 및 보호 툴과 신뢰할 수 있는 엔드포인트 관리를 제공하는 데 주력할 것입니다.

지역별로 가장 중요하게 생각하는 솔루션

- 북미: 모바일 디바이스 관리, CASB, 엔드포인트 보호
- EMEA: SIEM, 이메일 게이트 보호, 통합 엔드포인트 관리
- APJ: 모바일 디바이스 관리, SIEM, SOAR, 엔드포인트 보호

이러한 IAM 통합 솔루션들은 함께 작동하여 거버넌스를 간소화하는 동시에 정책 기반 액세스 제어와 인증 세분화, 그 밖에 직관적인 자동화를 안전하게 지원하여 미래 지향적인 기업을 뒷받침합니다.

다음 중 Zero Trust 보안을 지원할 목적으로 IAM 시스템과 통합할 때 가장 중요하다고 생각하는 솔루션은 무엇입니까?
글로벌 우선순위

IAM 통합 솔루션에서는 SIEM, MDM 및 엔드포인트가 상위권을 차지하고 있습니다.

전 세계 응답자들에게 위에 있는 잠재적 IAM 통합 솔루션를 높음, 중간, 낮음의 우선순위로 분류해 달라는 질문에, 48%가 SIEM을 높은 우선순위로 선택해 가장 많은 비율을 차지했고, MDM과 엔드포인트 보호가 각각 43%로 그 뒤를 이었습니다. 중간 우선순위에서는 SOAR과 UEM이 통합 솔루션으로 비교적 높은 순위를 얻었고, 낮은 우선순위에서는 17%를 넘은 솔루션 카테고리가 없었습니다. ■

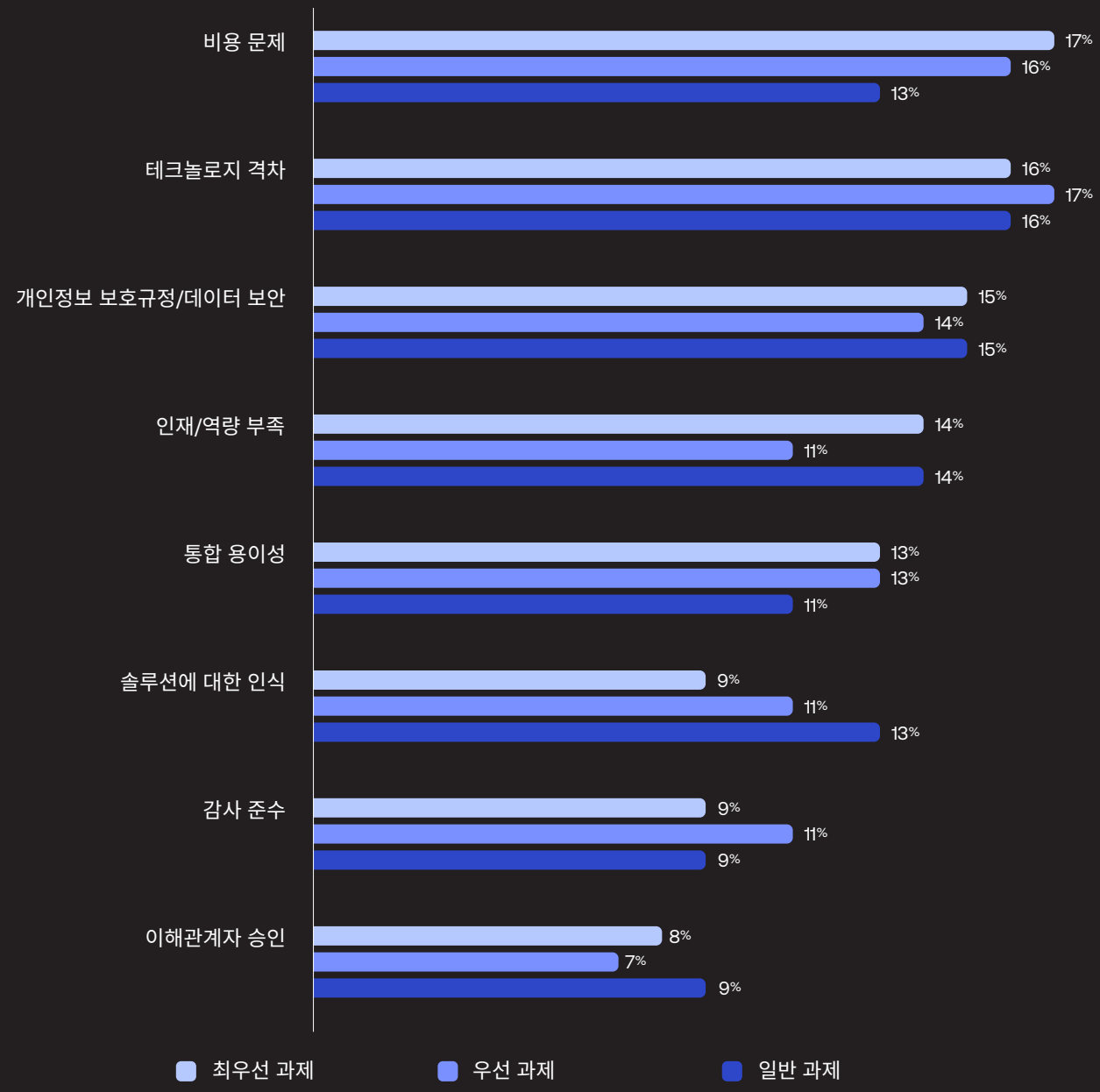
참고: 데이터 라벨을 정수로 반올림하기 때문에 각 비율 열의 총합이 정확히 100%가 아닐 수도 있습니다.

Zero Trust를 향한 기나긴 여정

기업들은 시스템 문제를 극복하고 미션 크리티컬 Zero Trust 이니셔티브를 시행하고 잇습니다.

Zero Trust는 오늘날 하이브리드/멀티 클라우드 환경에서 전 세계로 분산된 팀을 위해 액세스 및 프로비저닝을 자동화하는 동시에 내/외부 위협을 완화하여 기업을 안전하게 보호할 수 있는 유일한 방법입니다. 이러한 개념이 널리 알려지면서 규모, 분야 및 지역을 막론하고 대다수의 기업이 Zero Trust 계획을 수립하거나 추진하고 있습니다. 하지만 적합한 소프트웨어, 파트너 및 프로세스가 없다면 이러한 원리를 적용해 Zero Trust의 비전을 완전하게 실현하기가 어려워질 수 있습니다. 올해 데이터에서도 알 수 있듯이 전 세계 기업들은 비용 문제, 테크놀로지 격차, 역량 부족 등 다양한 보안 관련 문제로 끊임없이 어려움을 겪고 있습니다.

Zero Trust 솔루션 도입에 따른 세 가지 주요 과제:



올해 Zero Trust 도입에 따른 주요 과제: 비용 문제 및 테크놀로지

올해 응답자들은 Zero Trust 보안 이니셔티브 시행에 따른 주요 과제로서 비용 문제, 테크놀로지 격차, 개인정보 보호규정/데이터 보안을 가장 많이 언급했습니다. 개인정보 보호규정은 올해 새롭게 등장했지만 비용은 늘 반복적으로 나타나는 과제입니다. 2021년에는 비용 문제가 두 번째로 가장 많이 언급된 과제였습니다(첫 번째로 많이 언급된 과제는 인재/역량 부족이었고, 세 번째는 테크놀로지 격차였습니다). 2022년에는 비용 문제가 인재/역량 부족과 이해관계자 승인에 이어 3위를 차지했습니다. 올해도 인재/역량 부족 문제가 비교적 상위권을 유지하고 있지만 이해관계자 승인 문제는 순위가 떨어졌습니다. 그 이유는 신뢰할 수 있는 전문가들도 Zero Trust 개념의 타당성을 인정하고 있기 때문으로 보입니다.

직책을 기준으로 올해 데이터를 살펴보면 전반적인 동향도 다소 바뀌고 있습니다. 설문조사에 참여한 임원들은 개인정보 보호규정과 인재 부족을, 부사장들은 통합 용이성과 개인정보 보호규정을, 그리고 이사들은 감사 준수와 통합 용이성을 최우선 과제로 꼽았습니다.

Zero Trust를 향한 기나긴 여정

Zero Trust에 도달하는 과정

Zero Trust 여정은 기업마다 다릅니다. 예를 들어 최신 솔루션을 도입하여 빠르게 진화하는 보안 위협에 앞서나가려는 기업에게는 복합적이고 전략적인 이니셔티브 시행이 중요하면서도 오랜 시간이 걸리는 과제일 수 있습니다. 이러한 상황에서도 수많은 기업들이 자신의 계획을 꾸준히 이행하고, 경제적으로 불확실한 시기에 Zero Trust 이니셔티브 예산을 늘리며, 강력한 클라우드 보안을 향해 나아가고 있습니다.

기업이 진정한 의미의 Zero Trust에 도달하려면 먼저 데이터 보안 및 개인정보 보호 문제(규제 지침 포함)를 해결하는 동시에 직원들이 생산성을 발휘할 수 있도록 뒷받침해야 합니다. 또한 기존 테크놀로지 스택 및 에코시스템에 쉽고 빠르게 통합하여 투자 가치를 극대화할 수 있는 솔루션이 필요합니다. 그 밖에 답답할 정도로 지속되는 역량/인재 부족과 같이 고질적인 과제를 해결하는 데도 앞장서야 합니다.

다행스러운 점은, 이해관계자에게서 승인을 받는 일이 점차 쉬워지고 있고, 강력한 아이덴티티 관리의 이점도 더욱 투명해지고 있다는 사실입니다. Zero Trust의 가치가 단순히 보안에만 국한되지 않는다는 사실을 이제는 기업 리더들도 대부분 인지하고 있습니다. Zero Trust는 직원 및 고객 경험을 개선하고, 하이브리드 팀에게서 유의미한 협업을 이끌어내며, 원활하고 안전한 경험을 통해 고객의 신뢰를 강화하고 수익을 높일 수 있는 전략적 비즈니스 요인이기도 합니다.

오늘날 기업들이 직면한 가장 중요한 과제는 아마도 새로운 아이덴티티 경계를 안전하게 보호하는 일일 것입니다. 하지만 기업이 진정한 의미의 아이덴티티 기반 Zero Trust에 성공적으로 도달한다면 클라우드의 이점을 충분히 활용하여 민첩성, 혁신 및 비즈니스 성장의 기회를 새롭게 열어갈 수 있을 것입니다.

Zero Trust를 향한 기나긴 여정

주요 이점 살펴보기

- **실천 계획 단계에서 어느새 일상적인 비즈니스가 되어버린 Zero Trust**

  Zero Trust는 달성해야 할 목표를 지나 이제 일상적으로 수행하는 단계에 이르렀습니다. 대부분의 기업이 Zero Trust 이니셔티브를 이미 시행하여 보안과 경쟁력을 높이는 데 활용하고 있습니다. 그렇지 못한 기업들도 전반적으로 확고한 계획을 세우고 일정에 맞춰 추진하고 있습니다.

- **아이덴티티는 이제 Zero Trust 전략에서 미션 크리티컬 요소로 널리 인정받고 있습니다.**

  오늘날 급변하는 하이브리드/멀티 클라우드 기업 환경에서 아이덴티티가 새로운 경계로 자리잡으면서 이제는 기업이 자신 있게 확장하여 성공의 길로 나아가려면 강력한 아이덴티티 관리가 필수 전략입니다.

- **Zero Trust 예산은 시장 동향에도 불구하고 꾸준히 증가하고 있습니다.**

  경제가 좋지 안다고 해서 외부 공격과 내부 위협이 쉬어가는 것은 아닙니다. 보안 예산도 마찬가지입니다. 오늘날 기업들이 아이덴티티 기반 보안 이니셔티브를 통해 보안을 강화하는 데 주력하는 이유도 바로 여기에 있습니다.

- **Zero Trust를 도입하는 기업들도 힘든 싸움을 계속 이어가고 있습니다.**

  Zero Trust 보안 전략을 설계하고, 계획하고, 구현하려면 다수의 이해관계자들이 연관되어 있기 때문에 복합적인 이니셔티브가 필요합니다. 또한 개인정보 보호규정, 테크놀로지 격차, 비용 문제, 그 밖에 문제를 일으키는 요인들로 인해 기업마다 성공에 이르는 길도 각양각색입니다.

Okta의 Workforce Identity 성숙도 모델을 통해 기업의 현재 위치를 벤치마킹할 수 있는 방법을 포함해 자세한 내용을 알고 싶으신가요?? 여기에 해결 방법이 있습니다.

Okta 소개

Okta는 세계적인 아이덴티티 기업입니다. 독보적인 아이덴티티 파트너로서 누가 어디에서 어떤 디바이스 또는 앱을 사용하든 안전을 보장합니다. 평판이 높은 브랜드 기업들도 Okta에 대한 신뢰를 바탕으로 안전한 액세스, 인증 및 자동화를 구현하고 있습니다. Okta Workforce Identity Cloud와 Customer Identity Cloud는 유연성과 중립성을 무엇보다 중요하게 생각하기 때문에 비즈니스 리더들도 맞춤형 솔루션과 7,000개 이상의 통합 앱과 인프라를 통해 혁신에 집중하여 디지털 트랜스포메이션을 앞당길 수 있습니다. Okta는 고객이 아이덴티티의 주인인 세상을 만들어갑니다. okta.com에서 자세한 내용을 알아보세요.

면책 고지

okta

Okta Inc.
100 First Street
San Francisco, CA 94105
info@okta.com
1-888-722-7871