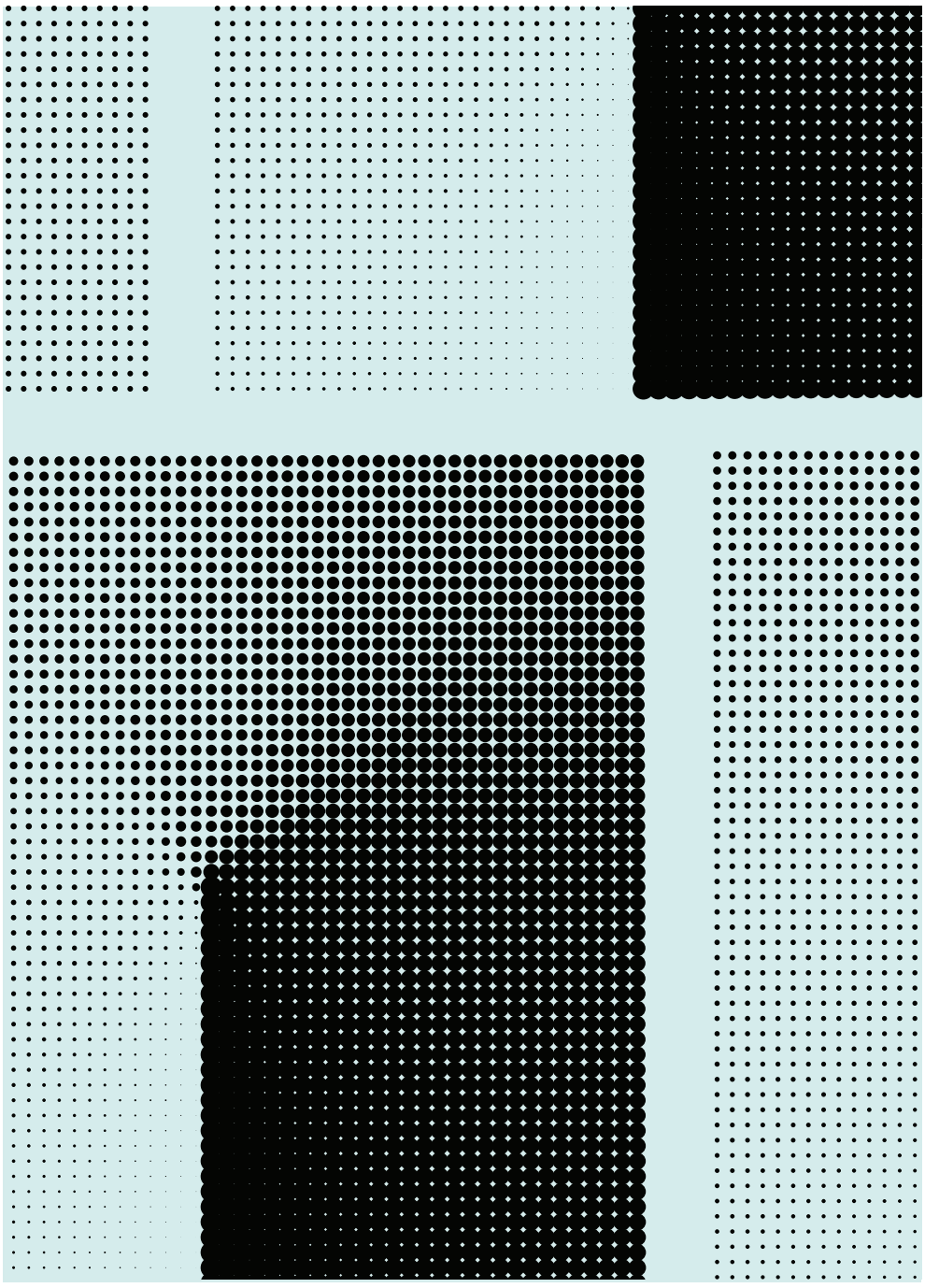
백서
2021년 8월

2021 APAC 지역의 Zero Trust 보안 현황 리포트

아시아 태평양 기업들의 IAM(Identity and Access Management) 보안 성숙도

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



목차

대세가 된 Zero Trust 보안

Zero Trust 보안 접근 방식은 사용자가 적정 수준의 권한을 갖고 적절한 맥락에서 필요한 리소스에 액세스할 수 있게 보장하는 것으로, 이러한 액세스를 지속적으로 평가합니다. 무엇보다 이러한 과정에서 사용자에게 불편이 가중되지 않습니다.

2020년 보고서가 나온 이후 몇 가지 환경 요인으로 인해 Zero Trust 보안 이니셔티브가 급증했습니다. 작년에는 원격 업무의 범위와 규모 및 인식 측면에서 큰 변화가 있었습니다. 현재 조직 리더의 82%가 팬데믹 종식 후 원격 업무를 부분적으로 허용할 계획이며, 47%는 전면 재택 근무를 영구적으로 허용할 계획이라고 합니다[1].

모바일과 클라우드의 도입이 급증함에 따라 고객, 직원 및 비즈니스를 보다 안전하게 보호하기 위해 대다수의 테크놀로지 및 보안 리더가 종래의 보안 접근 방식에서 탈피했습니다. "신뢰할 수 있는" 내부 네트워크와 "신뢰할 수 없는" 외부 네트워크를 구분하여 보호 경계를 구축하는 방식에서 탈피하여 정부 기관과 업계 분석가가 강력히 권장하는(경우에 따라 의무화하기도 하는) Zero Trust 보안 프레임워크를 도입하고 있습니다.

오늘날의 디지털 환경에서 아이덴티티는 새로운 경계가 되었습니다. 오늘날 사용자의 액세스 및 사용성 요구를 충족하고 데이터 유출과 공급망 공격의 피해를 막기 위해 조직들은 "절대 신뢰하지 말고 항상 검증하라"는 Zero Trust 보안 원칙을 중심으로 보다 강력하고 포괄적인 보안 태세를 갖추기 위해 노력하고 있습니다. 이를 위해서는 기업이 사용자의 불편을 가중시키지 않고 액세스 권한을 지속적으로 평가해야 합니다.

Okta는 오늘날 전 세계 조직들이 Zero Trust 보안에 어떻게 접근하고 있고, 향후 12 ~ 18개월 동안 어떤 방향으로 나아갈지를 알아보기 위해 아시아 태평양 지역(APAC)의 400여 명의 리더를 포함해 700명의 글로벌 보안 리더를 대상으로 Zero Trust 보안 이니셔티브에 대한 설문 조사를 실시하여 세 번째 연례 보고서를 발표했습니다.

[1] Gartner, **"Gartner 설문 조사 결과, 기업 리더의 82%가 원격 업무를 부분적으로 허용할 계획인 것으로 나타남.,"** 2020년 7월 14일

설문 결과 - 아시아 태평양 조직의 5가지 보안 핵심 내용

아시아 태평양 조직들은 Zero Trust 보안을 최우선 과제로 생각하지만 구현 수준은 타 지역의 동종 기업보다 뒤처져있음

코로나19로 인해 아시아 태평양 조직의 77%가 Zero Trust 보안을 최우선 과제로 삼게 되었습니다. 이는 EMEA 지역(76%)과 북미 지역(74%)보다 약간 더 높은 수치입니다.

한편 설문 조사 당시 아시아 태평양 조직의 Zero Trust 보안 전략 구현 수준은 EMEA와 북미 지역 조직보다 확실히 뒤쳐져 있었는데, 미주 및 EMEA 지역의 경우 Zero Trust 보안 전략을 이미 구현한 조직의 비중이 각각 20%인데 반해 아시아 태평양 지역에서는 13%에 불과했습니다.

팬데믹으로 인해 도입이 가속화되고 있는 Zero Trust 보안

전 세계 기업의 4분의 3 이상(78%)이 Zero Trust 보안의 우선 순위가 높아졌다고 답했으며, 약 90%가 현재 Zero Trust 보안 이니셔티브를 진행 중이라고 답했습니다(1년 전에는 41%에 불과함).

Zero Trust 보안 도입의 증가

올해 조직들은 IAM(Identity and Access Management)의 성숙기에 도달하기 위한 여정에 박차를 가했으며 내년 말까지 빠르게 진행할 계획입니다. 2023년까지 조직의 40%가 컨텍스트 기반의 액세스 정책을 구현할 것으로 보이며, 29%는 Okta의 성숙도 곡선에서 2단계로 분류된 API에 대한 보안 액세스를 구현할 것으로 예상됩니다.

새로운 경계가 된 아이덴티티

Zero Trust 보안의 핵심 요구 사항에 대한 질문에서 1위는 바로 "사람"이었는데, 전체 아시아 태평양 조직의 약 절반(44%)이 이렇게 답했습니다. 선두 기업들은 직원, 고객, 파트너, 계약자 및 공급업체를 대상으로 리소스 전반에 걸쳐 강력한 인증을 도입하는 동시에, 네트워크 기반에서 보다 개별화된 디바이스 기반으로의 액세스 결정 방식으로 전환하고 있습니다.

기업의 향상된 보안 수준

IT 리더와 보안 리더가 쉽고 빠르게 도달 가능한 성과 너머의 목표에 관심을 기울이면서, 향후 12 ~ 18개월 동안 Zero Trust 보안 프로젝트의 우선 순위는 IAM 성숙도 곡선의 다음 단계들에 위치한 프로젝트가 될 것입니다. 전체 기업의 3/1 이상이 외부 사용자에 대한 SSO(Single Sign-On) 및 MFA(Multi-Factor Authentication), 컨텍스트 기반 액세스 정책, 자동 계정 프로비저닝/디프로비저닝에 우선 순위를 두고 있습니다.

아시아 태평양 기업들의 최우선 과제가 된 Zero Trust 보안

원격 업무가 빠르게 확산되면서 Zero Trust 보안은 아시아 태평양 전역의 거의 모든 기업에게 최우선 과제가 되었습니다.

대부분의 기업들은 향후 12 ~ 18개월 동안 Zero Trust 보안 이니셔티브를 추가로 구현할 계획이며, 이전보다 더 많은 비용을 지출할 예정입니다. 아시아 태평양 조직의 약 76%는 Zero Trust에 대한 예산을 적정수준, 혹은 대폭 늘릴 것으로 보입니다.

모든 기업이 Zero Trust 보안의 중요성에 동의하고 있고 투자를 늘릴 예정이지만, 아시아 태평양 지역 조직의 Digital Trust 도입 및 전략에는 분명한 격차가 있습니다.

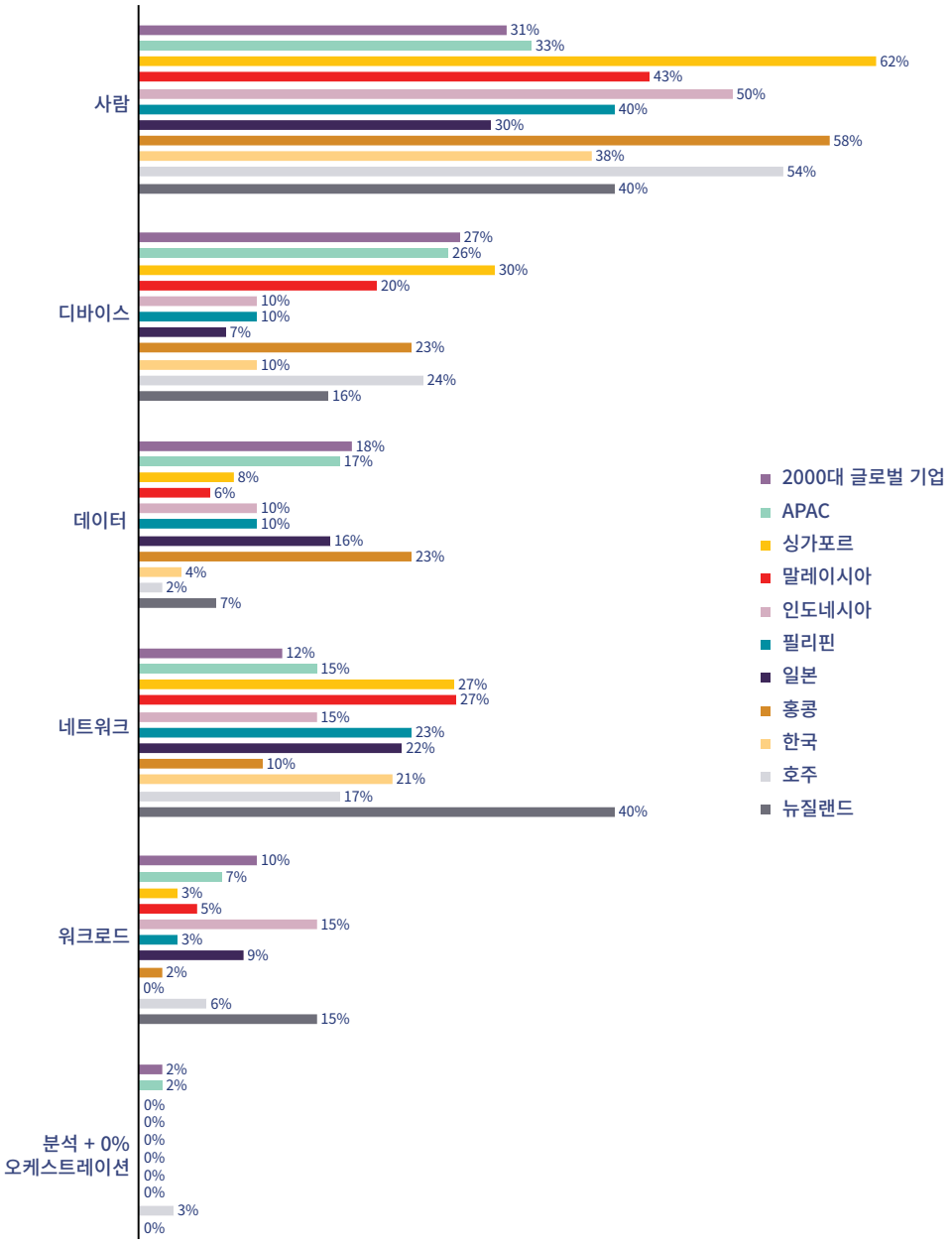
주목할 만한 국가별 트렌드

- **호주**의 경우, 기업의 Zero Trust 보안 전략 추진에 있어 코로나19와 원격 업무 전환에 따른 영향이 가장 낮았는데, 응답 기업의 20%가 영향을 받지 않았다고 답했습니다.
- **일본**은 Zero Trust 보안 도입률이 특히 뒤처져 있습니다.
    - 일본 기업의 82%가 Zero Trust 보안의 우선 순위가 높아졌다고 답했지만, Zero Trust 보안 전략을 이미 구현했거나 구현할 계획이라고 답한 조직은 68%에 불과했습니다.
        - 조직의 32%는 Zero Trust 보안 이니셔티브를 진행하고 있지 않으며, 향후 12 ~ 18개월 동안 이니셔티브를 진행할 계획이 없다고 답했습니다.
- **뉴질랜드** 역시 Zero Trust 보안 전략의 구현 비중이 불과 6.7%로 낮았지만, 93.3%가 향후 12 ~ 18개월 내에 이를 구현할 계획이라고 답했습니다.
- **인도네시아**와 **필리핀**의 경우 보안 부서가 IAM을 총괄하는 비율이 가장 높았지만, IAM 도입 자체는 여전히 낮은 수준(15%)입니다.
- **필리핀** 조직의 경우 Zero Trust 보안 전략을 이미 구현한 비율이 5%로 가장 낮았지만, 95%가 향후 12 ~ 18개월 내로 구현 계획이라고 답했습니다.

아이덴티티: Zero Trust의 토대

아이덴티티를 회사의 새로운 보안 경계로 삼게 되면 IAM이 사용자, 디바이스, 데이터 및 네트워크 전반을 중앙에서 제어하는 역할을 하게 됩니다. 실제로 최근 Gartner는 "아이덴티티 우선주의" 보안을 보안 및 리스크와 관련한 올해 가장 중요한 트랜드 중 하나로 지목했습니다[2]. 어떤 사용자가 어떤 리소스에 대한 액세스 권한을 가지고 있는지에 대한 가시성과 제어를 제공하고, 자격 증명 탈취나 잘못된 프로비저닝 또는 인증과 같은 위험 요소를 최소화하기 때문입니다.

귀사에게 있어 Zero Trust 보안의 최우선 순위는 무엇입니까?

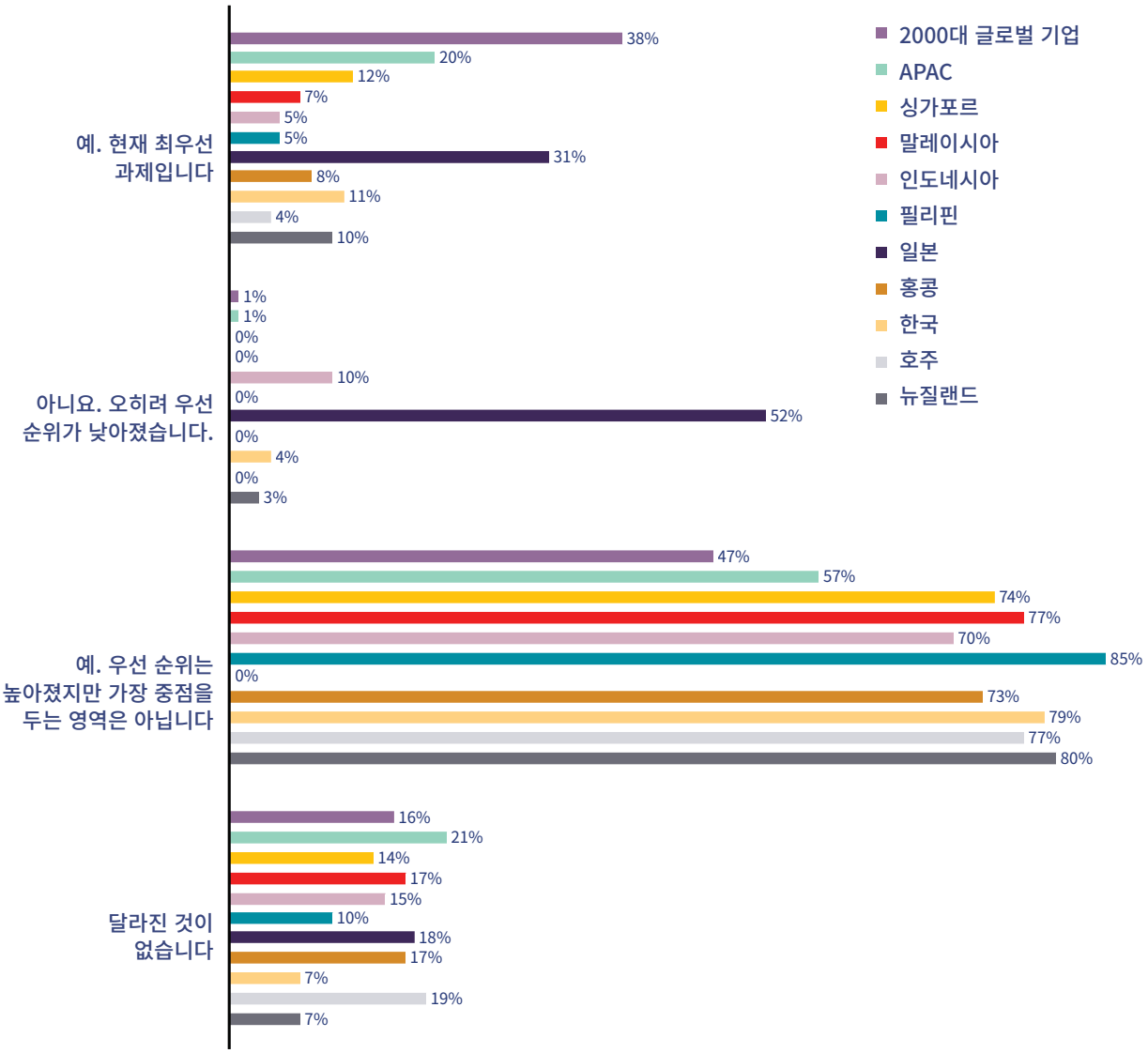


[2] Gartner, "Top Security and Risk Trends for 2021(2021 주요 보안 및 위험 트렌드)," 2021년 4월 5일

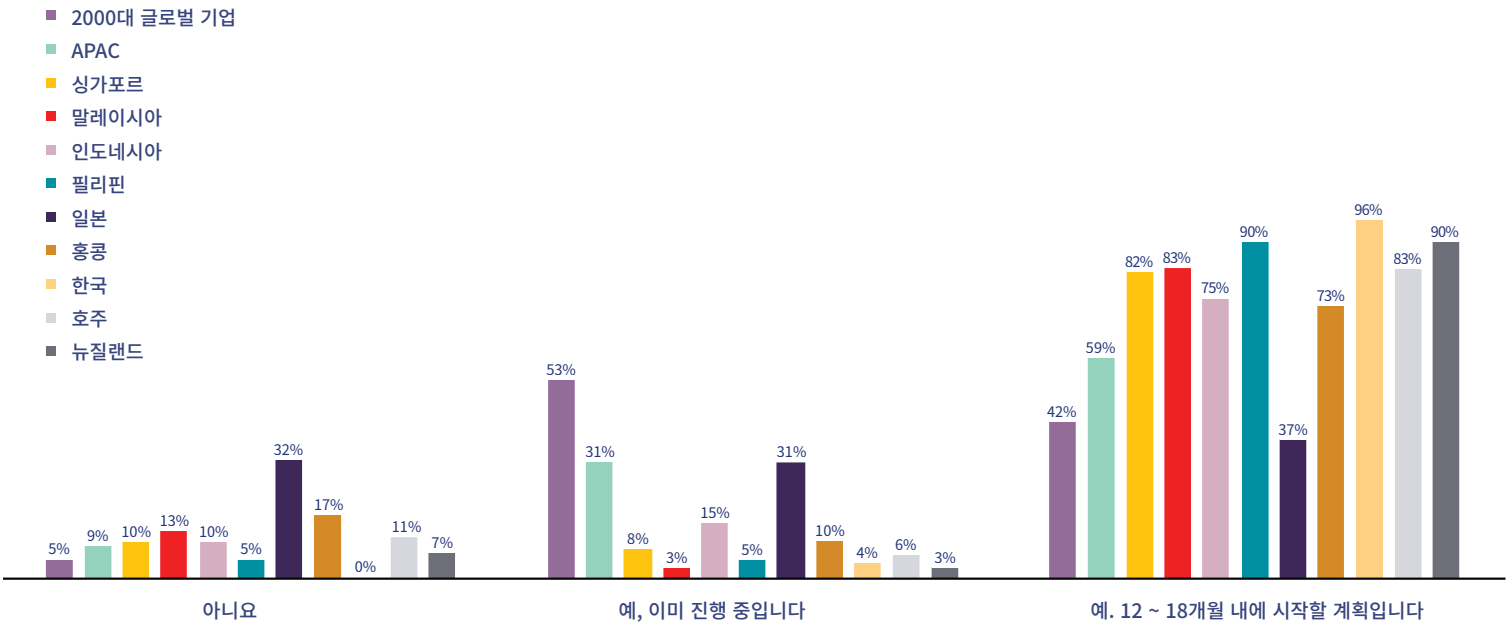
아이덴티티 기반 보안의 부상

지난 해 Zero Trust 보안과 IAM 우선 순위의 변화 양상을 살펴보면, 팬데믹으로 인해 조직의 Zero Trust 보안 도입이 가속화되었고 이를 달성하기 위해 많은 팀들이 더 많은 예산을 할당받은 것으로 나타났습니다. 아시아 태평양 조직의 약 90%가 Zero Trust 보안 이니셔티브를 현재 진행 중이거나, 향후 12 ~ 18개월 내에 시작할 계획이라고 밝혔습니다. 한편 일본에서는 68%만이 이러한 의사를 밝혔는데, 응답 기업 중 32%는 Zero Trust 보안 이니셔티브를 추진하고 있지 않으며, 향후 12 ~ 18개월 내에 진행할 계획이 없다고 밝혔습니다.

국가별 비교: 코로나19와 원격 업무로 인해 Zero Trust 보안이 귀사의 우선 과제로 급부상했습니까?



국가별 비교: Zero Trust 보안 이니셔티브를 현재 진행 중이거나, 혹은 향후 12 ~ 18개월 내에 시작할 계획입니까?

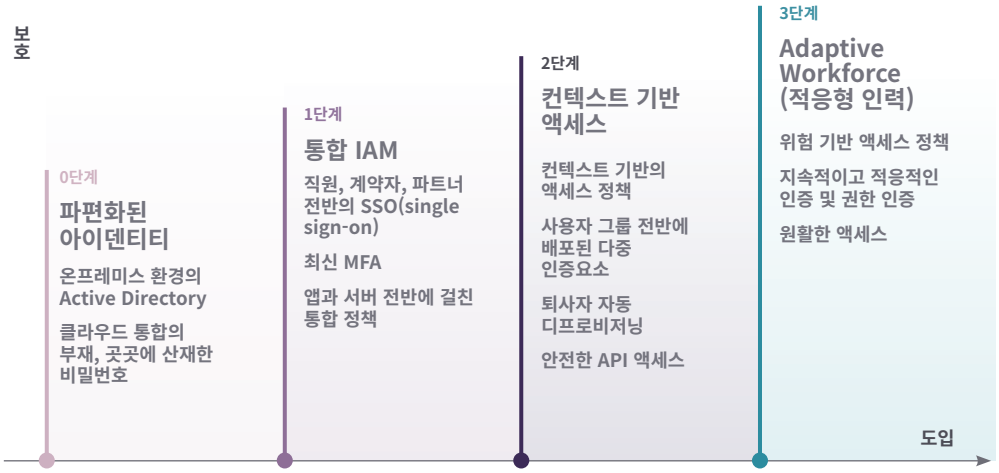


예상대로, 2000대 글로벌 기업에 속하는 기업들의 경우 보안 팀이 IAM을 관리하고 있었고, Zero Trust 보안 이니셔티브를 이미 진행하고 있는 비율이 높은(70%) 것으로 확인되었습니다. 한편, 보안 팀이 IAM에 적극적으로 개입하지 않는 기업에서는 이 비율이 53%에 불과했습니다.

아시아 태평양 지역의 경우, 아이덴티티 관리에 대한 전권을 가진 보안 팀은 10%에 불과했고, 14%는 권한이 전혀 없었습니다. 따라서 아이덴티티 관리에 대한 보안 팀의 적극적인 참여가 조직의 Zero Trust 보안에 매우 중요할 것으로 보입니다.

Zero Trust 보안 성숙도의 진화: 2021년

아이덴티티 및 액세스 성숙도 곡선



Zero Trust 보안 프로젝트는 기업이 관리하는 리소스 유형에서부터 배포하는 인증 방식에 이르기까지 모든 것을 아우릅니다. 이를 위해 Okta의 IAM 곡선은 조직이 관리하는 리소스 유형에서부터 사용자의 프로비저닝/디프로비저닝 방식에 이르기까지 모든 것에 대한 조직의 아이덴티티 기반 보안 전략을 검토합니다. 또한 배포하는 인증 방식과 시행 중인 정책, 그리고 향후 비즈니스 우선 순위도 함께 살펴봅니다.

IAM 성숙도 곡선은 다음과 같은 단계로 나뉩니다.

0단계에서는 조직들이 클라우드 테크놀로지를 수용하기 시작했지만, IAM 플랫폼이나 온프레미스 리소스에 이러한 솔루션을 아직 통합하지 않은 상태입니다.

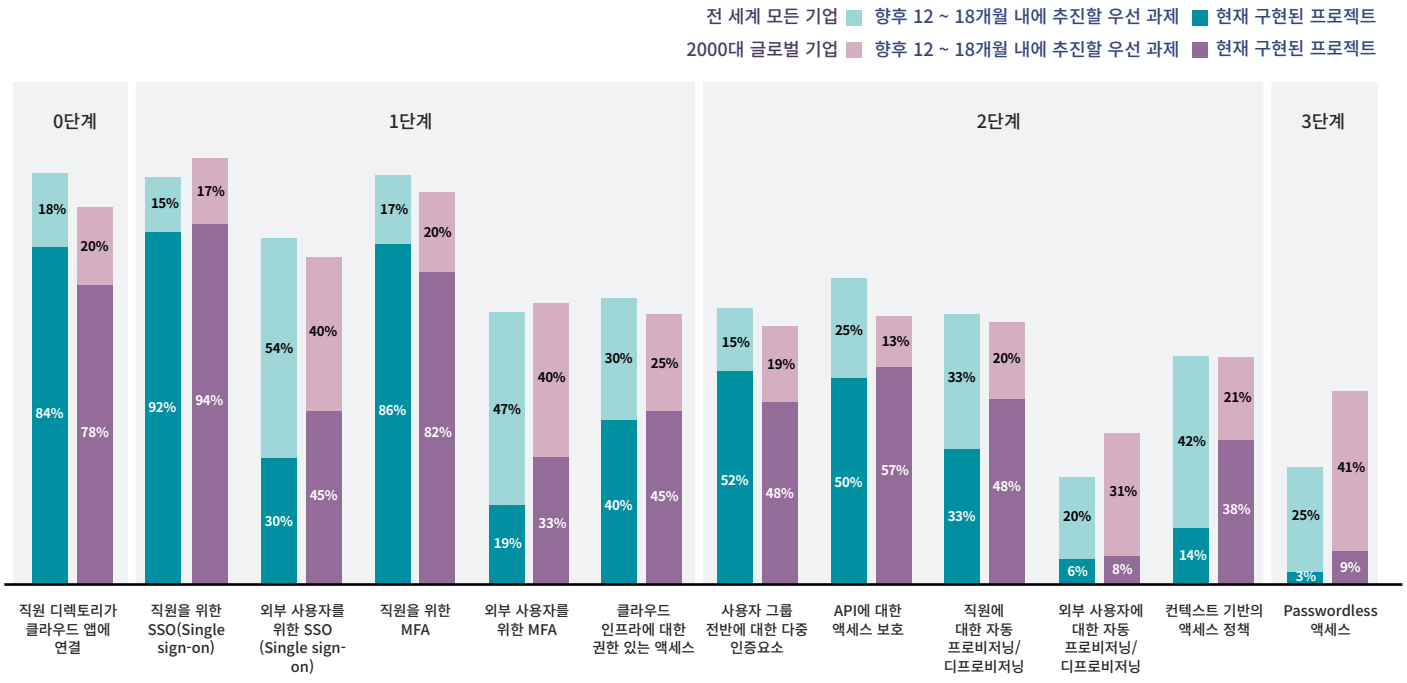
1단계에서는 팀들이 통합 IAM 에코시스템을 수용하고 직원이 주요 리소스에 액세스할 수 있도록 SSO(single sign-on)와 MFA를 구현하여 취약한 비밀번호 인증을 제거합니다.

2단계로 넘어가면 기업들이 API와 같은 다른 리소스에 대한 액세스 제어를 확장하고 인증 의사 결정을 효과적으로 알리기 위해 풍부한 컨텍스트와 다양한 인증요소를 사용함으로써 보안 모범 사례를 추가로 도입합니다.

3단계에 도달한 기업들은 passwordless 방식의 지속적인 액세스 솔루션을 포함해 Zero Trust에 대해 완전한 위험 기반 인증 접근 방식을 성공적으로 도입합니다.

응답 기업의 대부분이 여전히 0단계 또는 1단계 프로젝트에 집중하고 있었던 작년과 달리, 올해에는 응답 기업 전원이 2022년까지 1단계에 확실히 진입할 것으로 예상됩니다. 2023년까지 아시아 태평양 조직의 40%가 컨텍스트 기반의 액세스 정책을 구현할 것으로 보이는데, 29%는 Okta 성숙도 곡선에서 2단계로 분류된 API에 대한 보안 액세스를 구현할 것으로 예상됩니다.

전 세계 모든 기업 및 2000대 글로벌 기업: 현재 귀사가 구현한 프로젝트는 무엇이며, 향후 12 ~ 18개월 내에 추진할 우선 과제는 무엇입니까?



아시아 태평양 지역에서는 직원을 위한 SSO(조직의 84%가 구현) 및 MFA(84%)와 같은 1단계 프로젝트가 대부분의 기업에서 이미 구현된 상태였습니다. API에 대한 보안 액세스(35%)를 포함해 여러 2단계 전략 및 솔루션에 대한 구현도 양호했습니다. 반면 컨텍스트 기반의 액세스 정책을 보유한 기업은 단 3%에 불과했고, 40%는 향후 12 ~ 18개월 내에 이를 구현할 계획이라고 밝혔습니다.

여기에서 알 수 있듯이, 이들은 현재 아시아 태평양 기업들이 간과하고 있는 영역입니다. 한 예로 passwordless 액세스를 구현한 조직은 아무도 없었고, 향후 2년 내에 이를 구현할 계획이라고 답한 조직은 10%에 불과했습니다.

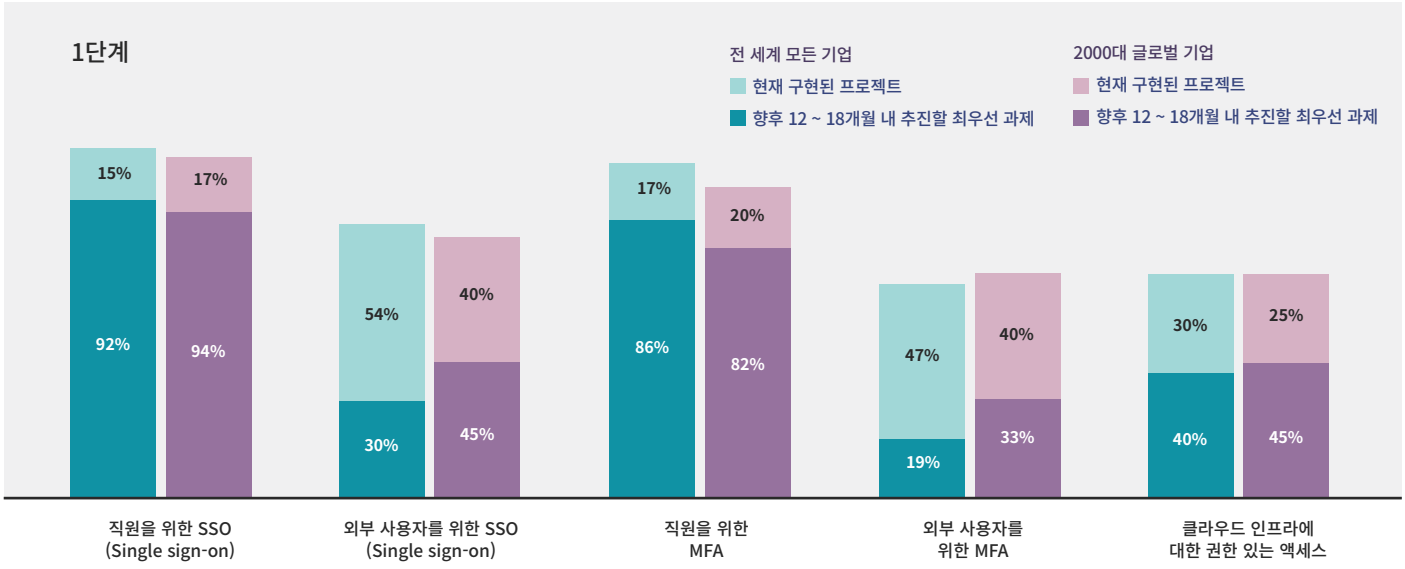
2023년이면 1단계 프로젝트를 도입한 아시아 태평양 기업이 67%를 넘어설 것으로 예상됨

1단계: 통합 IAM

1단계 기업들은 인증 메커니즘에 다수의 보안 계층을 추가함으로써 권한이 있는 사용자가 필요한 리소스에 원활하게 액세스할 수 있게 하는 효과적인 방법을 찾고 있습니다.

현재 84% 이상의 기업이 1단계 프로젝트 5개 중 최소 2개를 도입했으며, 2000대 글로벌 기업 중 70%가 2023년까지 5개 프로젝트를 모두 구현할 것으로 예상됩니다. 하지만 아시아 태평양 지역에서는 이 기간(2023년까지) 내에 5개 프로젝트를 모두 구현하리라고 예상하는 기업이 아무도 없었습니다.

1단계에 대한 전 세계 모든 기업과 2000대 글로벌 기업 간 비교: 현재 귀사가 구현한 프로젝트는 무엇이며, 향후 12 ~ 18개월 내에 추진할 우선 과제는 무엇입니까?



향후 2년 동안 아시아 태평양 기업들은 파트너, 계약자 및 공급업체와 같은 외부 사용자에 대한 액세스를 보호하는 프로젝트에 우선 순위를 둘 것입니다. 아시아 태평양 기업의 약 17%는 SSO 프로젝트를 시작할 것으로 예상되며, 40%와 25%는 MFA 프로젝트를 추진할 것으로 보입니다.

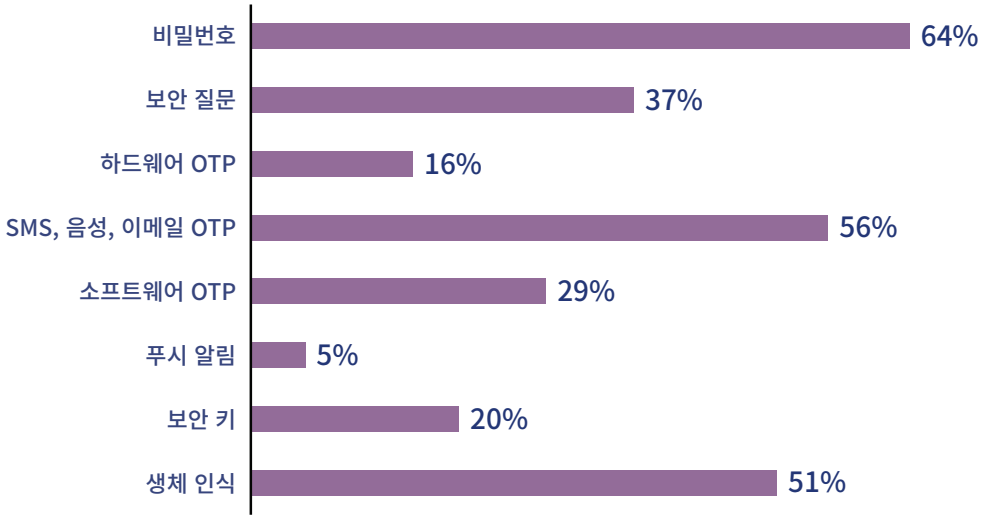
2단계: 컨텍스트 기반 액세스

2단계를 평가하기 위해 자사의 조직이 사용자 그룹 전반에 다중 인증요소를 적용하거나 API에 대한 보안 액세스를 제공하는 등 보호 솔루션을 배포하고 있는지를 물었습니다.

아시아 태평양 지역에서는 2023년까지 2단계 프로젝트 5개 중 4개를 구현한 기업이 약 절반에 달할 것으로 전망됩니다. 같은 기간 동안 아시아 태평양 기업에서 이러한 프로젝트 중 2개(API에 대한 액세스 보호 및 프로비저닝/디프로비저닝 자동화)의 도입율은 70%를 넘을 것으로 예상됩니다.

보안 인증요소

아시아 태평양 기업들이 현재 구현한 보안 인증요소



인상적인 점은 전 세계 기업의 49%가 보증 수준이 높은 인증요소인 생체 인식을 사용하고 있다는 사실입니다. 하지만 대다수의 기업이 아직도 사회 공학적 공격으로 탈취할 수 있는 비밀번호나 보안 질문과 같이 보증 수준이 낮은 인증요소에 의존하고 있었습니다(각각 89% 및 63% 도입)

3단계: Adaptive Workforce(적응형 인력)

기업은 Zero Trust 보안의 다음 단계로 나아가기 위해 보증 수준이 높은 인증요소를 사용하여 passwordless 액세스를 도입할 수 있습니다.

비밀번호에만 의존하게 되면 비밀번호 스프레이 공격과 자격 증명 스터핑 공격에 취약해집니다. 인증요소 시퀀싱이나 WebAuthn 또는 U2F 보안 키를 통한 생체 인식 기반 로그인과 같이 보증 수준이 높은 인증요소를 사용하면 이러한 위험을 완화하고, 비밀번호가 필요하지 않은 시나리오에서 passwordless 인증을 유연하게 적용할 수 있습니다. 이는 계정 탈취를 방지하는 데 큰 도움이 되므로 passwordless 도입에 점차 속도가 붙을 것으로 기대됩니다.

최저 수준이던 아시아 태평양 기업들의 passwordless 액세스 도입율이 올해는 29%로 높아질 전망입니다.

동급 최고의 Zero Trust 보안 에코시스템

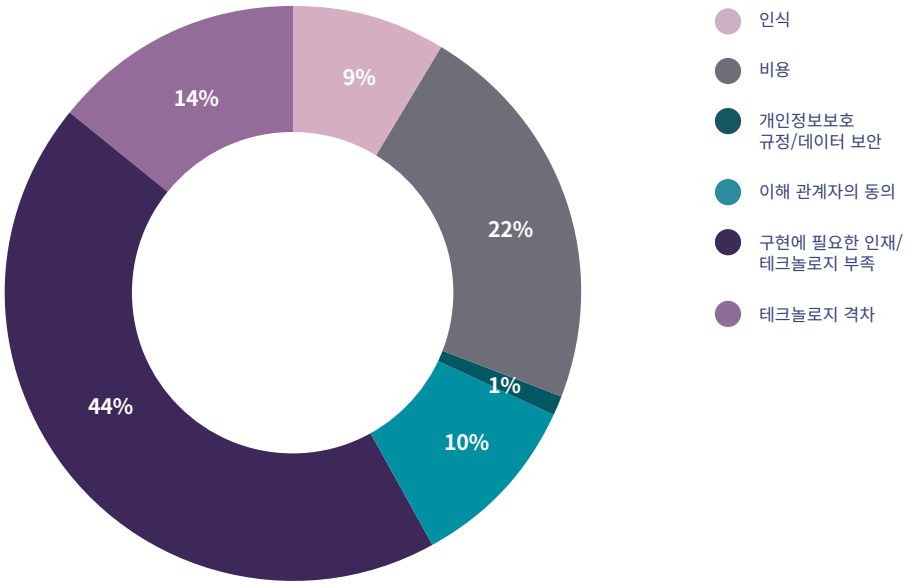
Forrester, NIST 등이 권장하는 Zero Trust 보안 기능을 모두 자동화하는 단일 솔루션은 없습니다. 모든 산업 부문의 중요 모범 사례에서 아이덴티티는 보안 스택 전반에 걸쳐 기반 테크놀로지로 활용되고 있습니다. SIEM(Security Information and Event Management), SOAR(Orchestration and Automation), EP(Endpoint Protection), MDM(Mobile Device Management), CASB(Cloud Access Security Brokers), PAM(Privileged Access Management)을 비롯한 보안 아키텍처 전반을 IAM 솔루션에 통합하면 Zero Trust 보안 방어에 대한 총체적이고 심층적인 접근 방식을 수립할 수 있습니다.

이를 염두에 두어 보안 리더에게 IAM 시스템에 이미 통합했거나 통합할 계획인 다른 툴이 무엇인지 물었는데, 그 결과 현재 가장 일반적인 통합 기능은 EP와 CASB라는 것을 알게 되었습니다(기업의 80%와 69%). 응답 기업의 대다수가 가장 중요한 단일 보안 통합 기능으로 SIEM을 지목했습니다.

Zero Trust의 미래

전 세계 기업의 최소 4분의 3이 향후 12 ~ 18개월 내에 IAM과 EP, SOAR, SIEM, MDM 및 CASB 시스템을 통합할 계획이라고 답했습니다. 이들 중 약 95%는 상위 2개 솔루션인 SOAR과 EP를 통합할 계획입니다. 2000대 글로벌 기업은 이미 이러한 통합을 활발하게 진행하고 있었으며, 최소 절반은 현재 6가지 보안 솔루션(SIEM, SOAR, EP, MDM, CASB, PAM)을 통합하고 있다고 밝혔습니다. 2022년 말까지 그 수치가 증가하여 세계 최대 규모 기업의 80%가 보안 솔루션을 통합할 전망입니다.

아시아 태평양 조직이 Zero Trust 보안 모델을 구현하면서 겪게 되는 주요 과제:



다행히도 Zero Trust 보안 프로젝트에 대한 예산이 늘고 있고 업계가 보다 정교한 보안 전략을 추진하고 있으며, 최근 정부가 내린 관련 명령 덕분에 조직들이 Zero Trust 보안 여정을 보다 수월하게 진행할 수 있을 것으로 보입니다.

소비자가 사이버 세상에 능숙해지고 클라우드에 저장되는 데이터가 많아짐에 따라, 앞으로 몇 개월 내지 몇 년 후에 Zero Trust 보안이 CIAM(Customer Identity and Access Management)에 연결될 가능성도 있습니다.

기업은 고객에게서 수집한 방대한 양의 중요한 금융 데이터와 개인 데이터를 처리합니다. CIAM 프로세스와 테크놀로지를 적절히 제어하지 못하면 데이터 유출과 비자발적인 데이터 노출 및 규정 비준수 문제를 초래할 수 있습니다.

궁극적으로는 계정 탈취나 고객 정보 도용과 같은 사고를 방지하고 불편 없는 인증 경험을 제공하는 기업의 보안 기능이 오늘날 소비자의 신뢰를 얻는 데 도움이 될 것입니다.

Zero Trust 보안이 성공하는 길

Zero Trust 보안을 구현하는 데 있어서 모든 문제를 한 번에 해결할 마법 같은 솔루션은 없습니다. 이와 동시에 점차 디지털화되는 현대 경제로 인해 보안 위협이 갈수록 심화되고 있는 상황에서 가만히 지켜보고 있을 수만은 없습니다.

다행히 아이덴티티 기반 보안을 통해 이러한 위험을 완화할 수 있는 몇 가지 방법이 있습니다.

- 먼저, 사람이 새로운 보안 경계임을 인식하고, 어디서나 모든 서비스에 대해 강력한 인증을 도입하는 방법입니다.
- 위험을 보다 쉽게 관리할 수 있도록 전사적 차원에서 아이덴티티 및 액세스 제어를 중앙화하는 방법도 있습니다.
- IAM 성숙도 곡선을 검토하여 자사의 현재 위치를 파악하고, Zero Trust에 대한 아이덴티티 우선 접근 방식을 통해 신속하게 경쟁 우위를 구축할 수 있는 방안들을 모색함으로써 위험을 줄일 수도 있습니다.
- 또한 핵심 툴을 IAM 솔루션과 통합해 보안 에코시스템을 확장함으로써 총체적인 보안 가시성과 협업을 달성할 수 있습니다.
- Passwordless 인증과 컨텍스트 기반 액세스 정책을 도입하고 직원 계정 보호를 넘어 파트너 계정에 대한 액세스 보호로 보안을 전환하는 등 훨씬 발전된 방법을 고려해 볼 수도 있습니다.

Okta의 Zero Trust 보안 평가 툴에서 Zero Trust 아이덴티티 및 액세스 제어 솔루션을 구축하기 위한 로드맵을 살펴보십시오. Okta의 평가 툴은 관리하는 리소스의 유형에서부터 IT 부서가 사용자를 프로비저닝/디프로비저닝하는 방식, 사용자를 인증하는 방식 및 이에 대한 배포 방안, 향후 비즈니스 우선 순위에 이르기까지 모든 인증 관련 관행을 검토합니다. 그런 다음, 귀사의 현재 성숙도를 파악하고 여기에서 한 단계 더 발전하기 위한 현실적인 권장 사항을 제시합니다.

설문 조사 방법

Okta의 의뢰로 Pulse Q&A는 여러 산업 부문에 걸쳐 아시아 태평양 조직의 보안 의사 결정권자(이사직함 이상) 300명을 대상으로 설문 조사를 실시했습니다. 일본에서는 Rakuten Insight가 100명의 보안 의사 결정권자를 대상으로 설문 조사를 실시했습니다. Pulse는 의사 결정권자를 테크놀로지 구매 결정을 담당하는 사람으로 정의하고 2021년 초에 응답을 수집했습니다.

직원이 500명 이상인 조직에서 응답자를 모집했으며, 응답자의 약 40%는 직원 수가 10,000명 이상인 회사에서 근무했습니다. 금융, 은행 및 보험, 의료 및 사회 복지, 소프트웨어 등의 업종을 대상으로 했습니다.

Okta 소개

Okta는 기업 아이덴티티 분야의 독자적인 선두 기업입니다. Okta Identity Cloud는 기업이 적정 권한을 가진 사용자와 테크놀로지를 적시에 안전하게 연결할 수 있도록 지원합니다. 7,500개 이상의 애플리케이션 및 인프라 공급업체가 사전에 통합되어 있어 Okta 고객은 자신의 비즈니스에 가장 적합한 테크놀로지를 손쉽고 안전하게 사용할 수 있습니다. 또한 JetBlue, Nordstrom, Slack, Teach for America, Twilio등 1만 개 이상의 기업들이 Okta를 통해 자사 직원 및 고객의 아이덴티티를 보호하고 있습니다. 자세한 내용은 okta.com/kr을 참조하십시오.