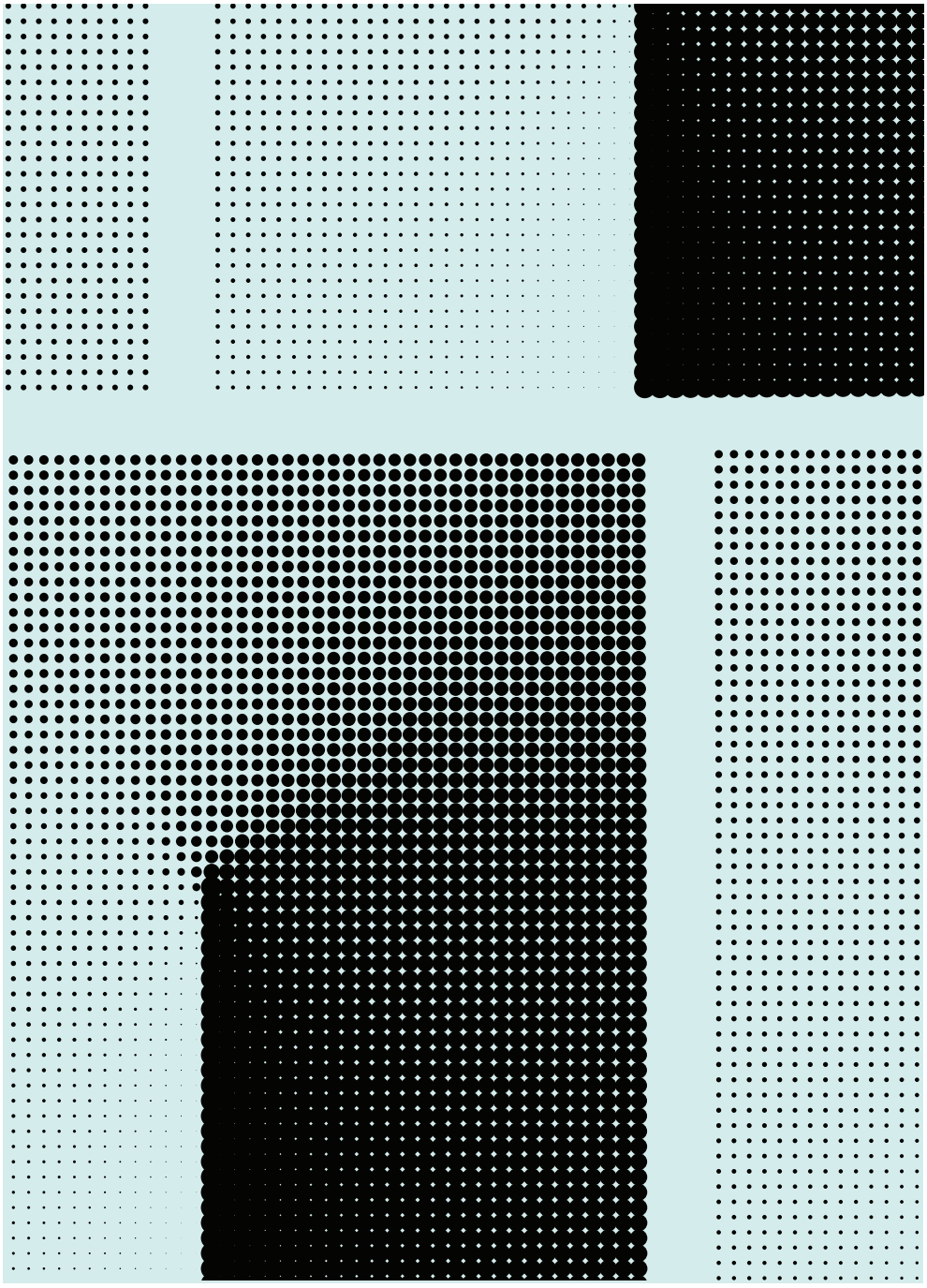
백서
APAC 지역
2022년 8월

2022년 APAC 지역 Zero Trust 보안 현황

APAC 지역 조직의 아이덴티티 및 액세스 관리 성숙도



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

okta

백서
APAC 지역
2022년 8월

목차

3 서론: 이제는 필수가 된 Zero Trust

APAC 지역의 3대 보안 전략 요점

› 유행어를 넘어 필수로 자리잡은 Zero Trust

› 엔터프라이즈 보안에 묘책이란 없다

› Zero Trust 실현을 좌우하는 아이덴티티

5 APAC 지역에서 본격 도입 중인 아이덴티티 기반 보안

5 개요: APAC 지역 응답자를 위한 핵심 정리

6 아이덴티티: Zero Trust 솔루션의 핵심

7 Zero Trust 성숙도 5단계

› 1단계: 전통적 단계

› 2단계: 새로운 시도 단계

› 3단계: 성숙 단계

› 4단계: 상승 단계

› 5단계: 진화 단계

10 산업 부문별 Zero Trust 진행 상황

› 의료

› 금융 서비스

› 소프트웨어

› 정부

12 오늘날의 아이덴티티 우선 보안 에코시스템

13 Zero Trust의 비전과 과제, 그리고 미래

13 설문 조사 방법

오늘날 Zero Trust가 필수가 된 이유

연구 결과에 따르면 “어떤 것도 신뢰하지 말고 항상 확인하라”는 Zero Trust 보안의 철학이 사람들의 마음을 움직인 것으로 나타났습니다. 조직들이 종래의 “성과 해자(castle-and-moat)” 보안 모델에서 탈피해 방어할 경계가 없는 클라우드 기반 환경에서는 네트워크 침입이 수시로 일어난다는 사실을 받아들이기까지 수십 년의 세월이 걸렸습니다.

하지만 오늘날 전 세계 조직들은 Zero Trust라는 보안 프레임워크를 수용하고 있습니다. 독특한 아이디어로 여겨졌던 Zero Trust는 전략적 차별화 요소를 넘어 순식간에 비즈니스 필수 요소로 자리잡았습니다.

2022년 Forrester가 내린 정의에 따르면 “Zero Trust는 기본적으로 애플리케이션과 데이터에 대한 액세스를 거부하는 정보 보안 모델”입니다. “Zero Trust는 세 가지 핵심 원칙을 지지합니다. 바로, 모든 엔티티는 기본적으로 신뢰할 수 없고, 최소 권한 액세스를 적용하며, 포괄적인 보안 모니터링을 시행한다는 것입니다.”

Zero Trust는 더는 이론적인 개념이 아닙니다. 디지털 환경을 갖춘 거의 모든 회사에서 적극적으로 채택하고 있는 이니셔티브입니다. 물론 많은 조직들이 Zero Trust라는 고급 보안 아키텍처의 이점을 활용하기 위해서는 아직 갈 길이 멀긴 하지만 말입니다.

일례로 4년 전에 실시했던 설문 조사에서 응답 기업의 16%만이 Zero Trust 이니셔티브를 시행 중이거나 향후 12~18개월 내에 시행할 계획이라고 답한 바 있습니다. 오늘날 이 수치는 97%에 육박합니다.

작년에 Okta가 2021년 Zero Trust 보안 현황 보고서를 발표한 이후로, 정의된 Zero Trust 이니셔티브를 이미 진행 중인 APAC 지역 기업의 비율이 31%에서 50%로 증가했습니다. 전반적으로 APAC 지역 응답자의 96%가 정의된 Zero Trust 보안 이니셔티브를 2022년 현재 진행 중이거나 진행할 계획인 것으로 나타났습니다.

> 정의된 Zero Trust 이니셔티브를 이미 진행 중인 APAC 지역 기업의 비율이 2021년 31%에서 2022년 50%로 증가

제4차 연례 Zero Trust 보안 현황 보고서에서 Okta는 APAC 지역의 보안 리더 200명을 비롯해 전 세계 700명의 보안 리더를 대상으로 완전한 Zero Trust 보안 역량을 갖추기 위한 여정에서 현재 위치를 평가하기 위해 설문 조사를 실시했습니다.

Okta는 이미 시행 중인 특정 이니셔티브들과 Zero Trust 이니셔티브의 장/단기적 우선 순위를 설정하기 위한 계획에 대해 물었습니다.

그리고 Forrester와 CISA에 의해 대중에게 알려진 Zero Trust 프레임워크를 사용해 Zero Trust 이니셔티브에 중요한 우선 과제들을 살펴봤습니다.

설문 조사에 응한 조직들이 변함없이 최우선 순위로 삼고 있는 것은 역시나 데이터, 네트워크, 그리고 디바이스였습니다. 물론 조직들이 네트워크보다 사용자에 더 중점을 두는 진화하는 보안 경계를 수용함에 따라 “사용자” 범주의 위상이 점차 높아지고 있기에 이러한 우선 순위는 바뀔 수 있습니다. 자세히 살펴보겠지만, 아이덴티티는 Zero Trust 보안 이니셔티브의 이점을 배가시킵니다.

올해 보고서에서 명확히 드러났듯이 Zero Trust 모델은 이제 보편화되었습니다. 설문에 응한 APAC 지역 조직들 대부분이 Zero Trust 이니셔티브를 이미 시행 중이거나, 향후 몇 개월 내에 시행할 계획이었습니다.

APAC 지역의 3대 보안 전략 요점

1. 유행어를 넘어 필수로 자리잡은 Zero Trust

Zero Trust 모델의 도입이 전 세계 조직들 사이에서 기본적인 보안 패러다임으로 자리잡은 가운데, 이들 대부분은 이니셔티브를 이미 시행하고 있으며 Zero Trust 여정을 촉진하기 위해 특정 솔루션을 적극적으로 찾고 있습니다.

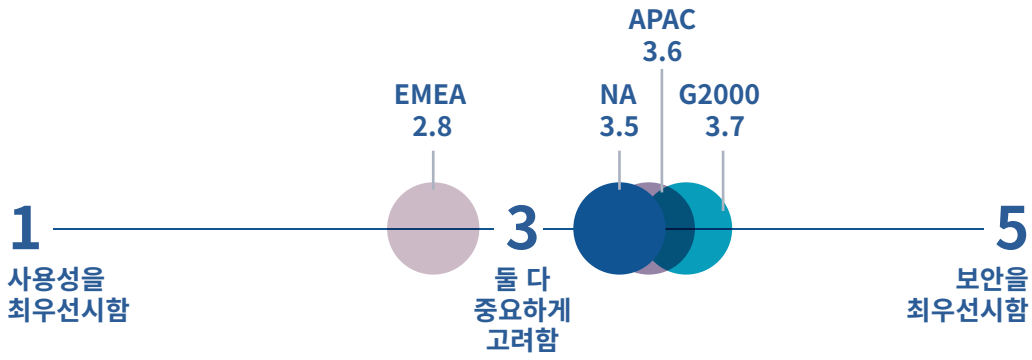
Zero Trust는 단순히 계획에 머물러 있지 않습니다. 전 세계 조직들은 엄청나게 빠른 속도로 Zero Trust 모델을 적용하고 있습니다. 2021년에 APAC 지역 조직의 31%가 Zero Trust 이니셔티브를 이미 시행하고 있다고 답했는데, 올해에는 그 수치가 약 50%까지 증가했습니다.

물론 놀라운 수준이긴 하지만 APAC 지역의 Zero Trust 도입률은 글로벌 평균(55%)에 못 미칩니다. 또한 글로벌 평균(전 세계적으로 전년 대비 31% 증가)은 물론이고 EMEA나 북미 같은 지역에 비해 증가율(APAC 지역의 경우 전년 대비 18% 증가)이 낮습니다.

보안 문제는 점차 강력한 동기가 되고 있습니다. 조직들은 서로 상충하는 보안성과 사용성을 조율하기 위해 오랫동안 애써왔습니다. 최근 몇 년 간은 사용성 문제가 지배적이었지만 올해 들어서 상황이 바뀌어 응답 조직들은 보안 프로젝트에 좀 더 우선 순위를 두고 있는 것으로 나타났습니다.

글로벌 추세와는 대조적으로 APAC 지역 응답자들은 사용성(25%)보다 보안(75%)을 우선시한다는 점이 흥미롭습니다.

지역별 비교: 귀사는 사용성의 중요성과 보안의 중요성을 어떻게 조율합니까?



또 한 가지 주목할 점은 APAC 지역 조직들의 Zero Trust 도입률이 크게 증가했지만 전 세계 다른 지역에 비해서는 여전히 뒤처져 있다는 사실입니다.

2. 엔터프라이즈 보안에 묘책이란 없다

Zero Trust는 확고한 이행 원칙이지만 이를 실현하려면 긴밀하게 통합된 동급 최고의 솔루션들을 원활하게 연동시켜야 하기 때문에 문제가 복잡합니다. 회사마다 시작 상황과 리소스 및 우선 순위가 저마다 다르기 때문에 진정한 Zero Trust 보안을 구현한다는 동일한 목표를 향해 각자 고유한 여정을 시작하게 됩니다.

3. Zero Trust 실현을 좌우하는 아이덴티티

전 세계 조직들은 저마다 차이점이 있기는 하지만 아이덴티티가 보안과 Zero Trust 전략의 성공에 매우 중요하다는 사실을 깨닫게 되었습니다. 기업들은 Zero Trust 이니셔티브의 일환으로서 새로운 보안 경계인 아이덴티티를 보호하기 위해 밤새워 일하고 있습니다.

또한, 이러한 이니셔티브를 지원하기 위해 구체적인 IAM 전략을 추진하고 있는데, 이러한 전략은 보고서에 자세히 나와 있듯이 5가지 단계로 나타낼 수 있습니다.

APAC 지역 응답자 중 거의 대다수가 전반적인 Zero Trust 보안 전략에서 아이덴티티가 중요한 역할을 했다고 답했습니다.

APAC 지역에서 본격 도입 중인 아이덴티티 기반 보안

팬데믹으로 인해 원격 업무가 본격화되면서 Zero Trust 보안이라는 광범위한 주제의 특징이라 할 수 있는 아이덴티티 기반 보안이 APAC 전역의 거의 모든 조직들에게 더 중요한 우선 과제가 되었습니다.

작년 보고서에서는 APAC 지역 응답자의 약 76%가 Zero Trust에 대한 예산을 적당히 늘리거나 대폭 늘릴 것이라고 답했는데, 올해 보고서에서는 최근 응답자들도 대체로 예상한 대로인 것을 알 수 있습니다. 지난 12개월 동안 Zero Trust 예산에 어떤 변화가 있었는지 묻는 질문에 응답자의 82%가 예산 지출이 적당히 증가했다고 답했습니다.

올해 보고서에 따르면, APAC 지역에서 Zero Trust 보안 이니셔티브를 구현할 때 겪게 되는 3대 과제는 인재 및 스킬 부족(31%), 이해 관계자의 동의 부족(18%), 그리고 솔루션에 대한 인식 부재(18%)로 나타났습니다.

개요: APAC 지역 응답자를 위한 핵심 정리

APAC 지역 조직의 약 절반(49%)이 현재 Zero Trust 전략을 시행하고 있습니다. 아직 갈 길이 멀지만, APAC 지역의 도입률은 작년의 31%보다 높아져 증가세를 보이고 있습니다.

- APAC 지역의 전년 대비 Zero Trust 도입 증가율(18%)은 글로벌 평균(31%)을 훨씬 밑돌았습니다.
- APAC 지역 응답자의 83%는 아이덴티티가 Zero Trust 보안 전략에 중요하다고 답했지만, 아이덴티티가 비즈니스에 중요하다고 답한 응답자는 15%에 그침
- 전체 APAC 지역 조직의 절반 이상이 사용성보다 보안성을 우선시
- APAC 지역은 패스워드리스 액세스 방식의 도입률이 전 세계에서 가장 낮았는데, 이 방식을 이미 구현한 응답자는 0.5%에 불과했고 향후 18개월 내에 구현할 계획인 응답자도 10%에 그쳤습니다.
- APAC 지역에서 Zero Trust 이니셔티브를 시행할 때 겪게 되는 3대 해결 과제는 다음과 같습니다. 1. 스킬 부족. 20 Zero Trust에 대한 인식 부재. 3. 이해 관계자의 동의 부족
- APAC 지역 응답자의 96%가 정의된 Zero Trust 보안 이니셔티브를 2022년 현재 진행 중이거나 혹은 진행할 계획이라고 응답

아이덴티티: Zero Trust 솔루션의 핵심

Zero Trust 여정은 각 조직마다 고유하지만, 전 세계 조직들 사이에서 Zero Trust에 대한 아이덴티티 우선 접근 방식이 가장 중요할 뿐만 아니라 필수적이라는 생각이 점차 공감대를 얻고 있습니다.

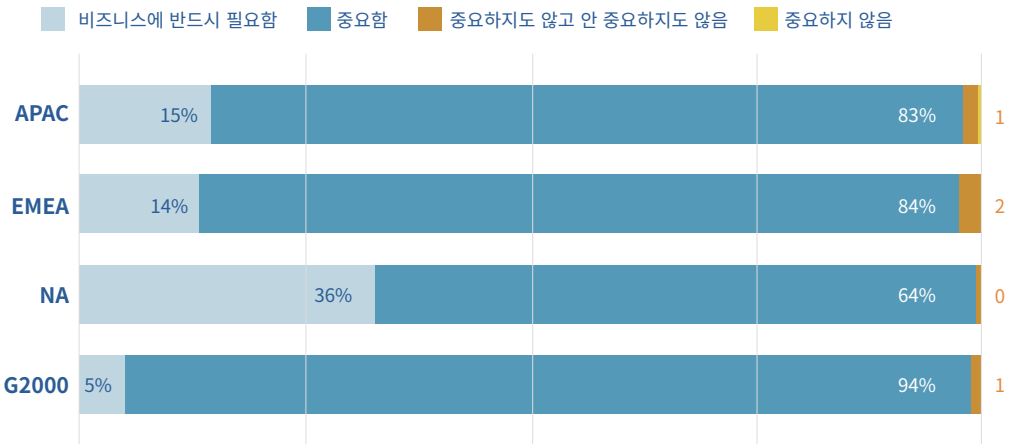
따라서 조직들은 IAM(Identity and Access Management)을 다른 중요한 보안 솔루션과 통합하여 사용자, 디바이스, 데이터 및 네트워크에서 액세스를 지능적으로 제어할 수 있는 강력한 중앙 제어 지점으로서 온전히 활용할 수 있습니다.

조사 결과에 따르면 전 세계 조직의 80%가 전반적인 Zero Trust 보안 전략에 아이덴티티가 중요하다고 답했으며, 아이덴티티가 비즈니스에 중요하다고 답한 응답자도 19%나 됩니다. 즉, 조직의 99%가 아이덴티티를 Zero Trust 전략의 주요 요소로 지목하고 있는 셈입니다. 특히 CISO를 비롯해 기타 최고 경영진의 26%가 아이덴티티를 비즈니스에 중요한 것으로 여기고 있습니다(아이덴티티가 중요하다고 답한 98% 중에서). 이를 감안하면 최근 Gartner[1]가 2022년 7대 보안 트렌드 중 하나로 “아이덴티티 시스템 방어”를 지목한 것도 그리 놀랄 일이 아닙니다.

APAC 지역 응답자의 83%가 전반적인 Zero Trust 보안 전략에서 아이덴티티가 중요하다고 평가했습니다. 게다가 이들 중 14%는 아이덴티티가 비즈니스에 중요하다고 답했습니다.

APAC 지역 응답자의 83%가 Zero Trust 보안 전략에서 아이덴티티가 중요하다고 응답

지역별 비교: 전반적인 Zero Trust 보안 전략에서 아이덴티티가 얼마나 중요합니까?



올해 설문 조사에서는 소규모 회사보다 포브스 선정 글로벌 2000대 기업에 속한 보안 팀이 보안 프로젝트에서 IAM 테크놀로지를 완전히 소유하는 경향이 있는 것으로 관찰되었습니다. 한편 전 세계적으로는 IAM에 대해 부분적 감시 이상을 제공하는 보안 팀이 증가하고 있습니다. 하지만 APAC 지역과 북미 지역에서는 수치 변화가 거의 없었습니다.

더 나아가 APAC 지역과 북미 지역에서는 보안을 더 중시하는 경향을 보였고, EMEA 지역에서는 두 가지를 균형 있게 고려하는 것으로 나타났습니다. 그렇다면 균형이 보안 쪽으로 기울어지는 이유는 무엇일까요? 원격 업무와 하이브리드 업무 방식을 확실하게 수립한 회사들은 팬데믹 시대에 따른 사용성 투자 자산을 이미 활용하고 있으며, 몇 가지 보안 부채를 해결할 수도 있습니다.

Zero Trust 이니셔티브를 위한 아이덴티티 도입 모델

Zero Trust 성숙도 5단계

기업들은 Zero Trust에 관한 자사의 주장을 다음과 같이 행동으로 보여주고 있습니다. 대부분의 조직들은 최소한 중요한 아이덴티티 이니셔티브를 시작으로 Zero Trust 보안 여정을 시작했습니다.

설문 조사 결과, 전 세계 응답자의 70% 이상이 이미 1단계(전통적 단계)를 통과한 것으로 나타났습니다. 무려 95%의 응답자가 향후 12~18개월 내에 1단계 프로젝트를 완료할 계획이며, 성숙도 곡선을 따라 아이덴티티 프로젝트 작업을 추가적으로 진행하고 있습니다. 2단계(새로운 시도 단계) 이니셔티브와 관련해 응답자 대다수(약 80%)가 직원을 대상으로 SSO를 확장했지만, MFA를 외부 사용자로 확장하여 공인 계약자와 공급업체 및 비즈니스 파트너가 중요한 리소스에 안전하게 액세스할 수 있도록 보장하고 있다고 답한 응답자는 38%에 불과했습니다. 아래에 자세히 설명되어 있듯이 Zero Trust 진행 상황은 2단계 이후로 방향이 갈리지만, 전 세계 응답자의 약 50%가 성숙도 곡선을 따라 다수의 아이덴티티 프로젝트를 추가로 완료했으며 나머지 응답자 중 다수가 향후 몇 개월 동안 이러한 추가 프로젝트를 진행할 계획입니다.

포브스 선정 글로벌 2000대 기업으로 분류된 그룹의 경우, 응답자의 약 100%가 향후 18개월 내에 1단계 아이덴티티 프로젝트를 모두 완료할 계획입니다(아직 완료하지 않은 경우). 이들 기업의 응답자 중 적어도 절반은 같은 기간 동안 1~4단계의 모든 프로젝트를 완료하고 5단계 프로젝트에 돌입할 계획입니다.

1단계: 전통적 단계

조사 결과, 조직들은 Zero Trust 여정이 시작될 때 연결되지 않은 디렉터리, 공격 대상의 무분별한 확산, 맹렬한 아이덴티티 기반 공격 등 기본적인 아이덴티티 문제를 겪는 것으로 나타났습니다. 성숙도 곡선의 1단계 진행 상황을 평가하기 위해 조직들에게 직원 디렉터리가 클라우드 앱에 연결되어 있는지, 그리고 직원에 대해 MFA(Mulfi-Factor Authentication)를 시행하고 있는지 물었습니다. 조사 결과, 1단계에 있는 조직들도 인증 프로세스에 다수의 보안 계층을 추가함으로써 적정 권한을 가진 사용자에게 액세스 권한을 부여할 수 있는 효과적인 방법을 찾고 있는 것으로 나타났습니다.

보고서에 따르면, 향후 18개월 내에 전 세계 기업 및 글로벌 2000대 기업 응답자의 약 100%가 1단계의 아이덴티티 프로젝트를 완료할 계획인 것으로 나타났습니다. 직원 대상의 MFA 확장이 가장 많이 도입된 아이덴티티 프로젝트로, 모든 지역의 응답자 전원이 향후 18개월 내에 전반적인 아이덴티티 전략의 일환으로 직원 대상 MFA를 도입할 계획인 것으로 나타났습니다.

APAC 지역에서는 직원 대상 MFA 확장이 가장 많이 도입된 아이덴티티 프로젝트(응답자의 76%)로, 모든 지역의 응답자 전원이 향후 18개월 내에 전반적인 아이덴티티 전략의 일환으로 이러한 프로젝트를 도입할 계획이라고 답했습니다. APAP 지역의 경우 자사의 디렉터리가 클라우드 앱에 연결되어 있다고 답한 응답자는 적었지만(68%), 향후 18개월 내에 이러한 아이덴티티 프로젝트를 완료하겠다는 계획을 갖고 있었습니다.

APAC 지역의 경우 직원 대상 MFA 확장이 가장 많이 도입된 아이덴티티 프로젝트(76%)로 확인됨

회사 디렉터리가 클라우드 앱에 이미 연결되어 있다고 답한 응답자는 적었지만 다수가 여전히 클라우드 마이그레이션 과정에 있는 것으로 보이며, 이들 대다수가 향후 18개월 내에 이러한 아이덴티티 프로젝트를 완료할 계획인 것으로 나타났습니다.

2단계: 새로운 시도 단계

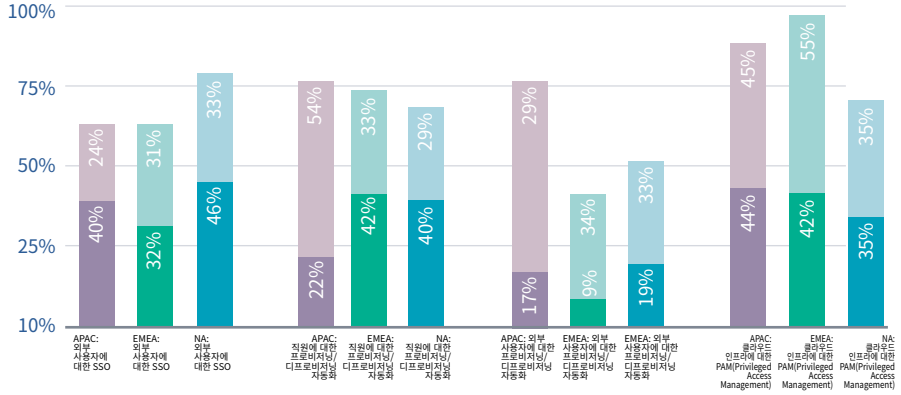
새로운 시도 단계에서 조직들은 보통 이질적인 시스템 전반에서 활동을 상호 연결하고자 시도하는데, 이는 클라우드 앱 도입을 늘리는 등의 변화와 더불어 M&A 활동으로 인해 사용자 액세스를 단순화해야 할 필요성이 커졌기 때문입니다.

2단계 진행 상황을 평가하기 위해 조직들에게 비즈니스 파트너와 계약자를 포함해 외부 사용자를 대상으로 MFA를 구축한 상태인지, 그리고 직원 대상의 SSO(Single Sign-On)를 추가했는지 물었습니다. 조사 결과, APAC 지역 조직의 39%가 외부 사용자를 대상으로 MFA를 이미 구현하였고 27%는 향후 12~18개월 내에 MFA를 구현할 계획인 것으로 나타났습니다. 더 고무적인 사실은 기업의 70%가 직원을 대상으로 SSO를 이미 구현했으며, 30%가 향후 12~18개월 내에 구현할 계획이라고 답했다는 것입니다.

재택 직원뿐만 아니라 계약자, 자원 봉사자, 공급업체 및 기타 비정규직 파트너를 고용하는 기업들이 점차 많아지고 있습니다. 이들 개개인은 조직의 보안을 위협하는 존재로 떠오르고 있으며, 이러한 외부 사용자를 대상으로 MFA를 확장하는 것은 리소스에 대한 안전한 액세스를 유지하는 데 도움이 된다는 점에서 모든 지역이 주목하고 있는 중요한 프로젝트입니다.

3단계: 성숙 단계

3단계 지역별 비교: 현재 귀사가 이미 구현한 프로젝트는 무엇이며, 향후 12~18개월 동안 어떤 프로젝트에 우선 순위를 두고 있습니까?



보고서에 따르면 성숙기에 접어든 조직들은 보안 컴플라이언스와 규제 요구 사항의 증가, 하이브리드 인프라, 대규모의 동적인 부분적/본격적 원격 인력 지원의 필요성 등 복잡한 과제를 안고 있습니다. 이러한 과제를 해결하려면 직원과 레거시 네트워크를 넘어 IAM 프로젝트를 확장하여 증가하는 외부 사용자와 확장 중인 클라우드 또는 멀티클라우드 인프라를 수용해야 합니다.

APAC 지역 응답자들은 향후 18개월 동안 직원에 대한 프로비저닝 및 디프로비저닝을 자동화하고 클라우드 인프라에 대한 PAM(Privileged Access Management)을 수행하는 데 주력할 계획입니다. 이는 아이덴티티 프로젝트 도입률이 22%에서 76%로, 43.5%에서 88%로 각각 2배 이상 증가한 것을 봐도 알 수 있습니다.

4단계: 상승 단계

성숙도 곡선에서 더 높은 단계로 올라간 조직들은 아이덴티티 기반 Zero Trust의 기본 과제를 해결했으며, 그 어느 때보다 복잡해진 아이덴티티 과제를 해결할 수 있는 도구와 프로세스를 갖추고 있습니다.

설문에 응한 글로벌 2000대 기업 모두가 향후 12~18개월 내에 사용자 그룹 전반에 걸쳐 MFA를 구축(APAC 지역의 경우 44%가 이미 구현)하고 API에 대한 액세스를 보호(APAC 지역의 경우 46%가 이미 구현)하는 등 아이덴티티 프로젝트를 완료할 계획인 것으로 나타났습니다.

이들 중 적어도 절반은 사용자가 액세스를 시도할 때 디바이스를 얼마만큼 신뢰할 수 있는지와 같은 컨텍스트 기반의 액세스 정책을 비롯해 액세스 시도 위치, 사용자와 리소스 자체, 그리고 기타 중요한 고려 사항에 중점을 두고 같은 기간 동안 4단계의 아이덴티티 프로젝트를 전부 완료할 계획입니다.

5단계: 진화 단계

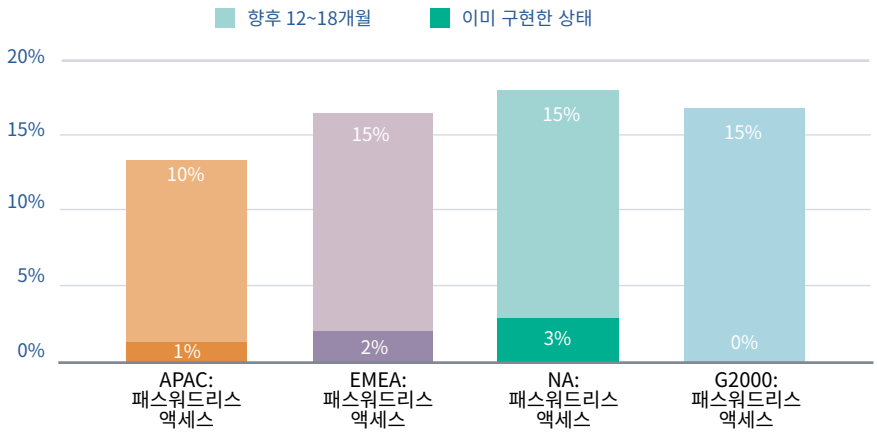
진화 단계에 도달한 조직들은 AWS, GCP, Microsoft Azure 같은 클라우드 기반 플랫폼으로 이미 마이그레이션을 완료했으며, 자동화 및 에지 보안 도입에 중점을 두는 것으로 나타났습니다.

이전 단계들에서 핵심 Zero Trust 프로젝트의 구현을 강조했던 것과 달리, 사용자 수명 주기 관리의 최적화, 서버에 대한 보안 액세스 제어 적용, 그 외 인증요소 시퀀싱, WebAuthn을 통한 생체 인식 기반 로그인, U2F 보안 키 등 신뢰도가 높은 인증요소를 사용하는 피스워드리스 액세스를 구현으로 쪽으로 바뀌었습니다.

조사 결과, 고무적인 점은 모든 지역의 응답자가 패스워드리스 액세스 방식의 도입을 본격화할 계획이라는 사실입니다. 오늘날 전체 데이터 유출의 절반 이상이 자격 증명의 취약성 또는 도난과 관련이 있으며, 자격 증명의 남용이 점차 증가하고 있는 랜섬웨어와 기타 아이덴티티 기반 공격의 주요 요인임을 고려할 때 이는 특히 긍정적인 결과라 할 수 있습니다.

> APAC 지역은 패스워드리스 액세스 방식의 도입률이 전 세계에서 가장 낮았는데, 이 방식을 이미 구현한 응답자는 0.5%에 불과했고 향후 18개월 내에 구현할 계획인 응답자도 10%에 그침

지역별 비교: 패스워드리스 액세스 옵션을 이미 구현했거나, 향후 12~18개월 내에 구현할 계획입니까?



산업 부문별 Zero Trust 진행 상황

각 산업과 그에 속한 조직들은 업무 관행과 우선 순위 및 의무가 저마다 다르기 때문에 Zero Trust 여정에서도 약간은 다른 접근 방식을 따르는 경향이 있습니다. 올해 설문 조사에서는 4가지 주요 산업 부문, 즉 의료, 금융 서비스, 소프트웨어, 그리고 처음으로 정부 기관을 심층 분석하여 이 부문에 속한 조직들의 고유한 요구사항이 Zero Trust 솔루션의 도입에 어떤 영향을 미치는지 자세히 살펴봤습니다. 또한 자주 상충하는 보안성과 사용성을 이들이 어떻게 균형 있게 조율하는지 알아내고자 했습니다.

물론 조직들은 이 두 가지 요구 사항을 모두 충족할 수 있는 방법을 찾고 있습니다. 흥미롭게도 올해 전 세계 응답자들은 평균적으로 사용성보다는 보안성에 좀 더 우선 순위를 두는 것으로 나타났는데, 이는 사용성이 보안성을 다소 앞섰던 2021년의 데이터와는 다른 양상입니다. 보안성에 중점을 두고 있는 산업 부문을 예로 들면 다음과 같습니다. 의료 등의 산업 부문에서는 비밀번호와 같이 자격 증명 기반 공격에 매우 취약한 저신뢰 인증요소에 대한 의존도를 줄이고 있습니다. 조사 대상인 모든 산업 부문에서 Zero Trust 보안 전략을 구현하기 위한 4대 해결과제가 놀라울 정도로 일관되게 나타났습니다. 올해의 최대 과제로는 인재/스킬 부족이 가장 많이 지목되었고, 이해 관계자의 동의 부족과 비용 문제, Zero Trust를 지원하는 보안 솔루션에 대한 인식의 부재가 그 뒤를 이었습니다.

주요 산업 부문: 의료

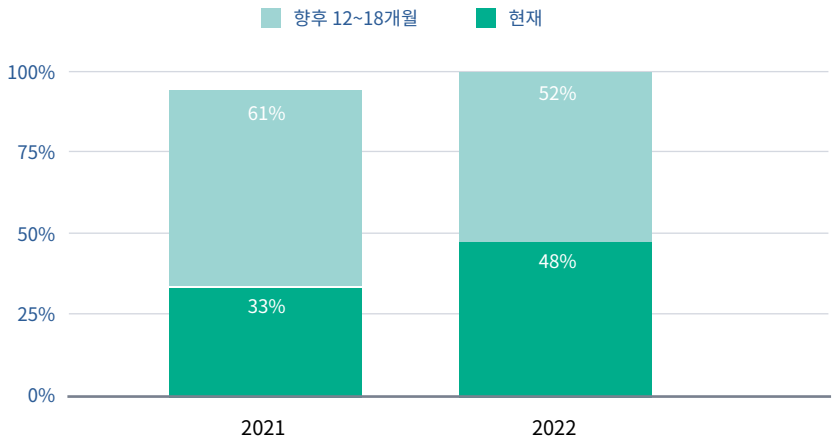
의료 부문이 마지막으로 넘어야 할 산은 Zero Trust 도입 계획을 시행하는 것입니다. Zero Trust 이니셔티브를 시행 중이거나 향후 12~18개월 내에 시작할 계획이라고 밝힌 의료 부문 응답자의 비율은 2021년 91%에서 2022년 96%로 증가했습니다. 의료 부문 응답자의 무려 58%가 Zero Trust 이니셔티브를 이미 구현하기 시작했다고 답했는데, 이는 작년 보고서가 작성된 시점의 응답 비율인 37%보다 20%나 증가한 수치입니다.

고무적인 점은 APAC 지역 의료 부문 응답자의 88%가 지난 12개월 동안 Zero Trust 예산이 약간 증가했다고 답했고, 이들 중 63%가 사용성보다는 보안성을 더 중요시한다고 답했다는 사실입니다.

APAC 지역 의료 종사자의 88%가 Zero Trust 이니셔티브를 이미 시행하고 있거나 향후 6~12개월 내에 시행할 계획이라고 답했는데, 이는 단기적으로 실행의 모멘텀이 유지되고 있으며 해당 산업 부문이 악의적인 공격에 취약하다는 사실을 드러내는 대목입니다.

주요 산업 부문: 금융 서비스

금융 서비스 전년 대비: 현재 정의된 Zero Trust 보안 이니셔티브를 시행 중입니까, 아니면 향후 12~18개월 내에 시행할 계획입니까?



금융 서비스 조직들이 Zero Trust를 고려하고 있는 것은 당연한 이치입니다. 전 세계 금융 서비스 부문 응답자의 약 100%가 향후 12~18개월 내에 Zero Trust 이니셔티브를 진행할 계획이라고 답했습니다. 실제로 응답자의 약 절반(48%)이 Zero Trust 이니셔티브를 이미 시행하고 있다고 답했는데, 이는 응답자의 1/3에 불과했던 작년에 비해 15% 포인트나 증가한 수치입니다.

APAC 지역 금융 서비스 조직의 94%가 사용성보다 보안성을 우선시하고 있으며, 이들 중 88% 이상이 지난 12개월 동안 Zero Trust 예산이 약간 증가했다고 답했습니다.

금융 서비스 조직을 위해 Zero Trust 이니셔티브를 구현하기 위한 정의 작업의 대부분이 이미 진행 중입니다. FinServ 조직들은 다른 부문에 비해 Zero Trust 성숙도에 있어 다소 뒤처져 있을 수도 있지만, 이를 조만간 따라잡기 위해 실질적이면서도 구체적인 계획을 세운 상황입니다.

주요 산업 부문: 소프트웨어

작년 보고서에서는 소프트웨어 산업이 다른 산업 부문에 비해 크게 뒤처져 있었습니다. 하지만 올해 보고서에서 소프트웨어 회사의 응답자들은 향후 12~18개월 동안 Zero Trust 보안 이니셔티브에서 상당한 진전을 이룰 것이라고 약속했습니다. 2021년 당시 설문에 응한 소프트웨어 조직 중 정의된 Zero Trust 이니셔티브를 이미 시행하고 있다고 답한 응답자는 단 9%에 불과했으며, 79%가 Zero Trust 이니셔티브를 시작할 계획이라고 답했습니다.

그리고 그 결과는 매우 성공적이었습니다. 올해에는 APAC 지역 소프트웨어 조직 중 Zero Trust 이니셔티브를 진행 중인 조직의 수가 50%까지 증가했으며, 45%가 향후 18개월 내에 정의된 Zero Trust 이니셔티브를 시행할 계획이라고 답했습니다. 즉, APAC 지역 소프트웨어 회사의 95%가 적어도 Zero Trust 여정을 시작했다는 뜻입니다. 이와 동시에 Zero Trust 도입률도 빠르게 증가했습니다. 소프트웨어 회사들은 서둘러 움직일 계획입니다. Zero Trust 전략을 정의하는 속도가 빨라져서 대체로 향후 6~12개월 내에 Zero Trust 이니셔티브를 구현할 것으로 예상됩니다.

주요 산업 부문: 정부

전 세계적으로 정부 조직은 Zero Trust 이니셔티브 도입 측면에서 다른 산업 부문의 조직보다 앞선 것처럼 보일 수 있지만 APAC 지역에는 이러한 추세가 반영되어 있지 않으며, APAC 지역의 정부 부문 응답자 중 Zero Trust 보안 이니셔티브를 시행하고 있다고 답한 응답자는 절반이 채 되지 않습니다.

세계 각지의 정부 부문 응답자들은 공통적으로 성숙도 곡선 전반에 걸쳐 보안 이니셔티브를 전격 추진할 계획인 것으로 나타났습니다. 이러한 계획 덕분에 직원과 사용자 그룹 대상의 MFA 구축과 같은 이니셔티브에 우선 순위를 두고 진행 중인 12개의 아이덴티티 프로젝트 중 6개의 진행 속도가 2배 가까이 빨라졌습니다.

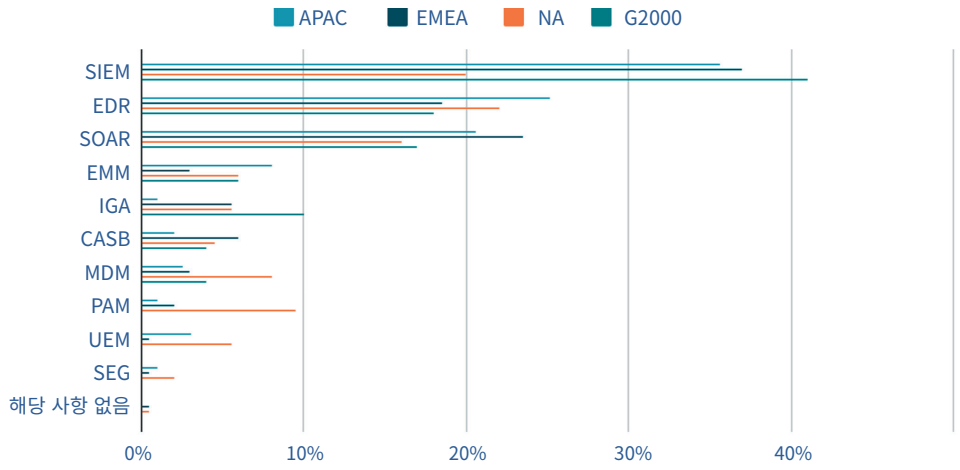
오늘날의 아이덴티티 우선 보안 에코시스템

조사 결과에 따르면, Forrester, NIST 및 기타 업체들이 권장하는 Zero Trust를 모든 측면에서 수용할 수 있는 단일 솔루션은 없습니다. 한편 아이덴티티는 보안 스택 전반에 걸쳐 기반 테크놀로지로 부상했으며, 나중에 추가하기보다는 아이덴티티를 중심으로 보안 계획을 세울 필요가 있다는 것이 점차 명확해지고 있습니다.

보고서에 따르면, 조직이 구축한 Zero Trust 방어 체계는 SIEM(Security Information and Event Management), SOAR(Security Orchestration, Automation and Response), 엔드포인트 보호를 위한 EMM(Enterprise Mobility Management), MDM(Mobile Device Management), CASB(Cloud Access Security Brokers) 및 PAM(Privileged Access Management)을 포함한 전체 보안 아키텍처에서 IAM 솔루션을 통합할 수 있을 때 더 효과적이고 효율적입니다. IAM을 SIEM과 연계해서 사용하면 잠재적인 보안 이벤트를 지능적으로 분류하는 데 도움이 됩니다. 예를 들어, SOAR에 IAM을 통합하면 보다 정확한 정보에 입각해 자동으로 보안에 대응할 수 있으며, EDR에 IAM을 통합하면 아이덴티티를 사용해 독립적인 데이터 포인트를 중앙에서 상호 연결하여 공격이 진행 중임을 나타낼 수 있습니다.

보안 리더를 대상으로 Zero Trust 보안 구축을 지원하기 위해 IAM 솔루션에 통합해야 하는 가장 중요한 도구가 무엇인지를 물었습니다. 설문에 응한 글로벌 2000대 기업의 40% 이상을 포함해 거의 모든 지역에서 통합이 필요한 가장 중요한 도구로 SIEM이 지목되었습니다. 유일하게 북미 지역만 SIEM을 가장 중요한 통합 요소로 지목하지 않았으며, EDR이 근소한 차이로 1위를 차지했습니다. IAM 통합과 관련해 가장 공통적으로 통합된 도구는 SIEM과 EDR, 그리고 CASB였으며, 응답 기업 5곳 중 3곳 이상이 이 세 가지 도구를 이미 사용하고 있었습니다.

지역별 비교: 다음 중 Zero Trust 보안을 지원하기 위해 IAM 솔루션에 통합해야 하는 가장 중요한 요소는 무엇입니까?



Zero Trust의 비전과 과제, 그리고 미래

올해 보고서에 따르면 전 세계적으로 많은 조직들이 작년 이후로 Zero Trust 이니셔티브를 꽤 많이 추진한 것으로 나타났습니다. 하지만 보안 팀이 새로운 테크놀로지를 구현할 수 있도록 대대적으로 투자하는 등 몇 가지 현실적인 과제에 여전히 직면해 있습니다.

특정 Zero Trust 이니셔티브를 구현하기 위해 해결해야 할 최대 과제가 무엇인지에 대한 질문에 APAC 지역 조직의 보안 리더들은 인재/스킬 부족을 가장 많이 지목했으며 테크놀로지 격차를 풀어야 할 숙제로 강조했습니다.

그렇다면 Zero Trust는 앞으로 어떻게 발전하게 될까요?

전 세계적으로 인재/스킬 부족 문제에 직면해 있음을 고려할 때, 조직들은 추가적인 예산이나 인력, 교육 리소스가 필요하지 않으면서 Zero Trust 여정을 진행하는 데 도움이 되는 솔루션을 모색해야 합니다. 또한 보다 쉽고 빠르게 구축할 수 있고, 조직의 성장과 Zero Trust 전략의 발전에 따라 확장이 가능한 솔루션이 필요합니다. 이해 관계자의 동의 부족은 보안 팀이 IAM 솔루션과 해당 환경의 기타 보안 관련 솔루션에 대해 완전한 소유권을 가지고 있지 않기 때문에 발생하는 문제일 수 있습니다. Zero Trust 이니셔티브에 투자하는 데 소극적인 부서들은 이러한 이니셔티브에 리소스를 재할당하는 것을 꺼릴 수 있습니다.

보고서에서도 알 수 있듯이, 이러한 해결 과제 속에서 기회를 찾을 수 있습니다. 조직은 함께 협업하는 부서들을 교육하여 합의를 도출하고 Zero Trust 이니셔티브를 발전시킬 필요성을 이해시켜야 합니다. 또한 다른 기업들의 해결 방식을 참고하여 자사의 접근 방식을 조정하는 방법을 연구해야 합니다. 무엇보다 가장 중요한 것은 적절한 파트너와 협력하여 Zero Trust 여정의 모든 단계에서 활용할 수 있는 솔루션을 구현하고, 성숙도 곡선의 각 단계에서 필요한 특정 솔루션을 찾아야 합니다. 이러한 솔루션을 기존의 보안 인프라에 통합하면 남은 과제들을 해결하는 데 도움이 될 수 있습니다.

설문 조사 방법

Okta의 의뢰로 실시된 Pulse Q&A에서는 각종 산업 부문의 글로벌 조직에 소속된 이사급 이상의 보안 의사 결정권자 700명을 대상으로 설문 조사를 실시했습니다. 여기서 의사 결정권자란 테크놀로지 구매를 결정하는 사람으로, Okta의 설문 조사 파트너인 Pulse가 2022년 초에 응답을 수집했습니다.

산업 데이터는 4개의 산업 부문(의료, 금융 서비스, 소프트웨어 및 정부)과 3개의 지역 및 포브스 선정 글로벌 2000대 기업에 중점을 두었습니다. 일본을 포함한 APAC 지역 응답자가 전체 응답자의 29%를 차지했습니다. 부사장, 이사 또는 최고 경영진을 대상으로 설문을 진행하였고, 보고서 작성자들은 정규화를 위해 각 부문 내에서 백분율을 사용했습니다. APAC 지역 데이터의 경우 정부가 8%, 최고 경영진이 26%를 차지했습니다.

직원 수 500명 이상인 조직을 대상으로 조사 대상자를 선정했으며 작년 보고서에서와 마찬가지로, 응답자의 약 40%가 직원 수 만 명 이상인 회사에 소속되어 있었습니다.

Okta 소개

Okta는 업계를 선도하는 독립적인 아이덴티티 공급자입니다. Okta Identity Cloud를 사용하면 적시에 적정 권한을 가진 사용자를 테크놀로지에 안전하게 연결할 수 있습니다. Okta는 애플리케이션 및 인프라 공급자에게 7,000개 이상의 사전 구축된 통합 기능을 제공함으로써 전 세계 어디서나 사용자와 조직이 간단하고 안전한 방식으로 액세스하여 잠재력을 극대화할 수 있도록 돕고 있습니다. JetBlue, Nordstrom, Siemens, Slack, Takeda, Teach for America, Twilio 등을 포함해 15,800개 이상의 조직들이 Okta를 통해 직원과 고객의 아이덴티티를 보호하고 있습니다. 자세한 내용은 okta.com/kr을 참조하십시오.