2022년 아시아/태평양 지역의 아이덴티티 현황

서론

2021년에는 새로운 고객 경험을 제공하는 동시에 지능적인 자동화 기술로 백오피스 운영을 혁신하기 위해 디지털 트랜스포메이션 이니셔티브를 서두르는 기업들이 많았습니다. 디지털 성숙도가 높은 기업들은 오늘날 디지털 퍼스트 경제에서 새로운 목적과 혁신 및 지속 가능성을 장기적으로 유도하려면 AI와 편재형 컴퓨팅으로 강화된 소프트웨어 역량이 필요하다는 사실을 깨닫고 이러한 업무 환경에 민첩하게 적응하여 자사의 비즈니스 요소마다 "디지털 퍼스트" 접근 방식을 적용했습니다.

IDC는 2022년 말쯤이면 아시아/태평양 지역 경제의 절반이 디지털 기술에 바탕을 두거나 이에 영향을 받을 것이라고 전망했습니다. 결과적으로 이 지역의 기업들은 디지털 기술을 적극 활용하여 빠르게 진화하는 업무 요건(하이브리드 퍼스트 등)을 해결하고, 디지털 채널과 물리적 채널 전반에 일관된 고객 경험을 제공하고 운영 자율성을 달성하여 지능형 기업으로 거듭나게 될 것입니다.

하지만 하이브리드 업무 모델로 전환하면서 공격 대상과 관련된 위험이 지속적으로 증가하였고, 그 결과 아시아/태평양 지역에서 보안 투자에 주력하는 기업이 증가했습니다. 이에 온프레미스 환경과 클라우드 환경을 모두 안전하게 보호해야 한다는 필요성이 주된 목표로 자리잡게 되었습니다. 오늘날 기업들이 가장 크게 염려하는 부분은 위협이 끊임없이 증가하는 환경에서 데이터와 네트워크 및 사용자를 안전하게 보호하는 것입니다.

아시아/태평양 지역의 데이터 규정 및 법률은 보안 솔루션을 도입해야 하는 주요 동인으로도 작용하고 있지만 단일 표준이 없는 지역들 사이에서 서로 다른 규정을 도입하는 경우가 많습니다. 일례로 호주와 뉴질랜드, 싱가포르, 그리고 일부 홍콩 등지의 시장에서는 비교적 엄격한 데이터 프라이버시 및 위반 고지 법률을 도입하는 반면, 다른 시장에서는 관련 법률이 거의 없거나 한정적이어서 시행하기도 어려운 실정입니다. 지난해에는 액세스 자격 증명을 강화할 목적으로 공통의 표준 및 프레임워크를 통해 인증 및 권한 인증 프로세스를 간소화함으로써 아이덴티티 페더레이션 및 권한 관리 방식으로 회귀하는 기업들이 처음으로 등장했습니다. 이러한 추세는 2022년에도 지속될 전망입니다.

아이덴티티 관리 현황

아이덴티티 관리 솔루션은 이제 사용자 아이덴티티를 효과적으로 관리할 수 있는 초석이 되었습니다. IDC가 2021년에 아시아/태평양 지역의 기업 879곳을 대상으로 실시한 아시아/태평양(AP) 보안 서비스 설문조사에 따르면, 설문조사에 참여한 기업의 40% 이상이 아이덴티티 보안을 주요 주력 영역으로 지목했습니다. 다수의 기업이 점차 확산되는 추세에 편승하여 다중 요소 인증과 같이 손쉬운 기술들을 이미 구현했지만 IDC가 2021년 12월에 실시한 FERS(Future Enterprise Resiliency and Spending) Wave 설문조사에 따르면 응답 기업의 약 80%가 2022년에도 첨단 인증/다중 요소 인증에 대한 투자를 유지하거나 늘릴 계획인 것으로 나타났습니다.

아이덴티티 보안을 주요 주력 영역으로 지목한 기업의 비율

첨단 인증 방식에 지속적으로 투자할 계획인 기업의 비율

여기에 컨텍스트 기반의 액세스 제어(패스워드리스 솔루션 등)와 같은 기술을 사용하거나, 분석 기술과 AI 및 ML을 조합해 사용자, 디바이스, 애플리케이션 및 인프라에서 이상 행위를 탐지하여 추가적인 이점을 얻을 수 있습니다. 아이덴티티 거버넌스와 권한 있는 액세스 관리도 아이덴티티를 보호하는 데 반드시 필요합니다.

또한 IDC에서는 모든 아이덴티티 세그먼트(B2E, B2B, B2C)에서 생체인식 인증 기술의 도입이 대폭 증가하여 정부를 비롯해 기업과 개인 사용자가 액세스 속도와 사용자 인증 및 전반적인 경험을 개선하는 데 도움이 될 것으로 내다보고 있습니다. 하지만 팬데믹 기간에 가장 두각을 드러냈던 차별화 요인은 B2C 아이덴티티 관리로, APJ 지역에서 2021년 전반기에 31.4%라는 가장 높은 증가율을 보였습니다.

B2C 아이덴티티 관리는 이제 성공적인 비즈니스 운영에 필수적인 요소가 되었으며, 클라우드 기반의 아이덴티티 관리는 완전한 디지털 트러스트를 구현하는 데 반드시 필요한 구성 요소가 되었습니다. 디지털 트러스트란 고객, 파트너, 공급업체 및 내부 이해관계자를 포함해 전체 에코시스템에 걸쳐 신뢰를 구축하는 것을 말합니다.

이에 따라 기업들은 Zero Trust 프레임워크를 포괄적이고 안전한 업무 환경을 제공하기 위한 대체 수단으로 평가하고 있습니다. Zero Trust 환경에서는 사용자와 디바이스 및 네트워크의 아이덴티티를 모두 인증하여 검증을 거친 후에 액세스를 허용합니다. Zero Trust 전략을 수립할 때는 아이덴티티가 전체 보안 아키텍처 청사진에서 핵심이 되는데, 그 이유는 점차 경계를 잃고 서로 연결되는 비즈니스 환경에 보안 계층을 추가로 제공하여 에코시스템 전반에 디지털 트러스트를 구현하기 때문입니다.

IDaaS 구축 모멘텀: 주요 동인

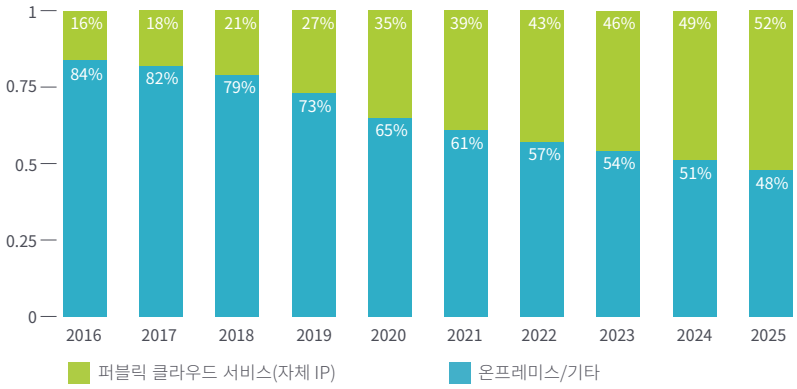
기업이 클라우드 또는 모바일 퍼스트 환경으로 전환할 때는 운영 방식을 간소화하고 통합해야 하는 요건이 타당해야 합니다. 데이터 주권 요건, 하이브리드 데이터 센터 환경을 중앙에서 관리할 수 있는 디렉터리 요건, 진화하는 아이덴티티 관리 요건 등 해결해야 할 과제가 많아지면서 다음과 같이 확실한 이점으로 서비스형 아이덴티티(IDaaS) 또는 클라우드 기반 인증 모델의 도입을 대폭 촉진할 수 있는 여건이 마련되었습니다.

- 비용 절감, 운영 효율, 전문성의 동시 구현
- 아이덴티티 전문가의 지원으로 가치 창출 시간 단축
- SAML(Security Assertion Markup Language), OAuth(Open Authorisation) 등 사용자가 단일 자격 증명 세트로 액세스할 수 있는 아이덴티티 페더레이션 표준 지원
- 즉시 사용할 수 있는 SSO(Single sign-on) 및 다중 요소 인증
- 점차 늘어나는 데이터 주권 및 개인정보 보호 요건 관리 작업 간소화
- 하이브리드 데이터 센터 환경을 위한 중앙 집중식 디렉터리

아이덴티티의 미래: 통합 플랫폼 구축

서비스형 보안이 우수한 기능과 관리 효율을 가장 효과적으로 구현할 수 있는 방법이라는 사실을 많은 기업이 깨닫고 있습니다. IDC의 아이덴티티 및 디지털 트러스트 소프트웨어 시장 예측(Identity and Digital Trust Software Market Forecast)에 따르면, 2025년에는 IDaaS가 비용적 이점과 유연성, 배포 용이성 등으로 인해 인도, 한국, 말레이시아, 뉴질랜드, 싱가포르 등 다수의 국가에서 기존 소프트웨어 배포 모드를 앞지를 전망입니다.

2020~2025년 아이덴티티 및 디지털 트러스트 소프트웨어 시장 예측



출처: IDC Semiannual Software Tracker, 2021H1 Forecast

IDaaS는 앞으로 광범위한 사용 사례에 걸쳐 통합할 수 있는 아이덴티티 플랫폼, 원격 액세스, 보편적인 클라우드 서비스 통합을 통해 수많은 레거시 포인트 솔루션의 문제를 해결하는 데 도움이 될 수 있습니다. 기업이 성숙도 곡선을 따라 성장하다 보면 IAM 솔루션이 다른 IT 운영 및 관리 영역을 비롯해 MDM, SIEM, 자동화 등의 각종 보안 모듈과 효과적으로 통합되면서 더욱 간소화된 통합 보안 운영 시스템을 구축할 가능성이 높습니다. 결과적으로 아이덴티티 보안 플랫폼을 개발하여 제공하는 벤더들은 온프레미스 환경과 클라우드 환경에서 종합 솔루션을 제공하여 누구나 원하는 디지털 기업 파트너로 거듭나게 될 것입니다.