cpl. thalesgroup.com #AMI2020

THALES
Building a future we can all trust

요약본
2020 탈레스 접근 관리 인덱스
아시아 태평양 버전

서론

오늘날의 디지털 세계에는 그 어느 때보다 더 강력한 IT 보안과 데이터 보호가 필요합니다. 대규모 데이터 유출 사고가 갈수록 흔해지고, 사이버 공격은 일상이 됐습니다. 고객의 개인 정보를 보호해야 한다는 대중의 압력도 거세지만, 데이터 유출 사고에 휘말린 기업이 겪어야 하는 어려움도 매우 큽니다.

우려의 목소리가 클 수밖에 없는 상황입니다. 사이버 공격 빈도가 늘고 있을 뿐만 아니라, 적절한 보안조치가 취해지지 않고 사용되는 인프라와 클라우드 애플리케이션, 그리고 다양한 IT기술이 증가하고 있습니다. 사실이든 아니든, 가장 널리 사용되는 최신 기술 중 일부는 보안이 취약하다는 오명에 휩싸여 있습니다. 이것이 바로 새로운 기술에 적합한 최신 데이터 보안 및 인증 방식이 필요한 이유입니다. 오늘날 기업들은 의도치 않게 데이터 위협에 취약한 기술 및 허술한 접근관리 기능을 사용하고 있습니다.

기업이 현재 상황에 맞추어 인프라를 갖추어 나가면서 클라우드가 비즈니스를 안정적으로 운영하고 번성하는 데 필수적인 요소로 자리 잡고 있습니다. 그러나 직원이 가정에서 안전하게 일할 수 있어야 하는 작금의 상황에서 클라우드의 데이터를 보호하기 적합한 보안에 대한 이해나 인식이 부족하면 강력한 클라우드 도입과 효과적인 디지털 혁신이 요원해지기 쉽습니다. 자사의 클라우드로 확장하려는 경우,기존의 보안 체계로는 감당할 수 없다는 사실을 유념하여 제로 트러스트 모델을 채택하고, 로그인 하는 순간에 맞춘 접근 제어 정책을 시행하며, 데이터를 암호화해야 합니다.

본 보고서에서는 기업의 접근 관리 정책과 2단계 인증, 스마트 싱글사인온(Single Sign-On), 접근 관리 도구의 중요성 및 사용 방안을 클라우드 서비스 도입 및 사용과 결부시켜 탐구합니다. 이 보고서는 업계 모범 사례를 제시하는 한편, 유익한 정보 제공을 위해 제작되었습니다.

클라우드 도입률 급증으로 인한 복잡성 심화

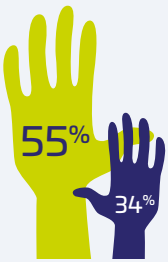
아시아 태평양(APAC) 지역 응답자 중 절반 이상은 클라우드 애플리케이션(57%) 및/또는 보호되지 않은 인프라(53%)가 사이버 공격의 가장 유력한 대상이라고 생각합니다. 웹 포털(45%), 기업용 애플리케이션(44%) 및/또는 모바일 애플리케이션(44%)을 걱정하는 응답자는 그보다 약간 적습니다.

클라우드 애플리케이션이 사이버 공격의 대상이라고 생각하는 응답자 5명 중 3명은(58%) 그 이유로 클라우드 애플리케이션의 전반적인 사용률 증가를 손꼽습니다. 클라우드 전반의 일관적이지 않은 보안 체제(57%)와 적절한 보호 체제를 구현하는 강력한 사이버 보안 솔루션 부족(56%)을 사이버 공격의 대상이 되는 이유로 지목한 응답자도 상당히 많습니다. 그러나 아시아 태평양 지역의 국가마다 큰 의견차를 보입니다. 일본 응답자 중 65%(아시아 태평양 지역 평균은 53%)는 클라우드 애플리케이션을 보호할 수 있는 사내 인력의 역량 부족을 우려합니다. 반면, 인도 응답자들은 적절한 보호 체제를 구현하는 강력한 사이버 보안 솔루션 부족(71%)을 최대 보안 위험 요인으로 손꼽습니다. 응답 결과와 무관하게, 클라우드 애플리케이션의 수가 늘고 있을뿐더러 그 중요성도 커지고 있습니다. 따라서 클라우드 애플리케이션을 적절히 보호하는 것이 아시아 태평양 지역 기업의 필수 과제입니다.

대다수 아시아 태평양 지역 기업(96%)의 경우, 지난 12개월간 소비자 서비스의 보안 공백이 접근 관리와 관련한 보안 정책에 영향을 미친 것으로 조사됐습니다. 일본 기업의 경우, 소비자 서비스의 보안 공백을 해소하고자 새로운 교육 정책을 시행했으며, 절반(50%)이 직원들에게 접근 보안 관리를 교육하고 있다고 답했습니다. 약 3명 중 1명이(65%) 클라우드 애플리케이션을 보호할 수 있는 사내 인력의 역량 부족을 보안 위험 요인으로 지목한 점을 고려하면 기업이 직원 교육에 관심을 기울이는 것이 타당합니다. 인도 기업들도 문제 해결에 힘쓰고 있는 모양새입니다. 약 3명 중 1명은(67%) 이사회가 접근 보안 관리를 최대 당면 과제로 여기고 있다고 답했는데, 이런 사고 변화는 강력한 사이버 보안 솔루션 부족에 관한 우려를 종식하는 데 도움이 될 것으로 보입니다.

55%

설문 조사에 응한 IT 책임자 중 55%(전년 **34%**)는 보안 관련 사안에 대해 이사회의 동의를 얻기가 더 쉬워졌다고 말합니다.



아시아 태평양 지역의 거의 모든 IT 의사 결정권자(99%)는 특정 유형의 데이터에 접근할 수 있는 사용자를 통제하면 데이터 보호 규정을 준수하기가 약간이나마 쉬워진다고 생각합니다. 아시아 태평양 지역의 기업 중 약 60%는 온프레미스 ID 및 접근 관리(IAM) 솔루션(63%), IDaaS(Identity-as-a-Service)(57%), 스마트 싱글 사인온 솔루션(55%), 클라우드 싱글사인온(55%) 같은 일종의 접근 관리 솔루션을 구현했습니다. 3곳 중 2곳에(66%) 육박하는 기업이 직원에게 소셜 미디어 자격 증명을 사용하여 기업 리소스에 로그인하도록 허용했거나 허용할 예정임을(인도와 일본이 각각 77%와 76%로 가장 높고, 싱가포르는 48%로 가장 낮음) 감안하면, 이러한 유형의 솔루션을 구현하지 않을 경우 보안이 약화될 수 있습니다.

클라우드 도입 과제

58% 는 클라우드 앱의 사용률 증가로 인해 사이버 공격 대상이 될 가능성이 커졌다고 우려합니다.

규정 준수와 직결되는 접근 관리

99% 는 특정 유형의 데이터에 접근할 수 있는 사용자를 통제하면 규정을 준수하기 쉬워진다고 말합니다.

접근 관리는 클라우드 혁신에 필수적입니다.

클라우드 및 웹 기반 애플리케이션 보호와 관련한 질문에 IT 의사 결정권자는 가장 적합한 업무 목적의 접근 관리 도구로 2단계 인증(64%, 홍콩이 75%로 가장 높음)에 이어 스마트 싱글사인온(53%)과 생체 인증(48%)을 선택했습니다. 약 3곳 중 2곳에(66%)에 육박하는 기업이 직원들에게 소셜 미디어 자격 증명을 사용하여 기업 리소스에 로그인하도록 허용했거나 허용할 예정인데도, 이와 같은 방법을 클라우드 및 웹 기반 앱을 보호하기 가장 좋은 방법으로 손꼽은 응답자는 31%에 불과합니다.

거의 모든 기업(99%)은 비효율적인 클라우드 접근 관리가 광범위한 영향을 미친다고 생각합니다. 비효율적인 클라우드 접근 관리의 여파로 5명 중 2명 이상이(46%) 운영 부담 및 IT 비용의 증가를, 44%는 IT 인력의 업무 효율 하락을 우려합니다. 50%는 비효율적인 클라우드 접근 관리로 인해 클라우드가 보안 문제로 대두되고 있다고 말하고, 43%는 클라우드에 대한 가시성 부족 탓에 대규모 데이터 유출 사고가 유발된다고 생각합니다. 효과적인 클라우드 접근 관리 솔루션을 구현하는 기업은 보안을 유지할 수 있을 뿐만 아니라, 필요한 시간과 비용도 크게 절약할 수 있습니다.

비밀번호 취약점

81% 의 응답자는 비밀번호 취약점으로 인한 보안 공백을 우려합니다.

50%

는 비효율적인 클라우드 접근 관리로 인해 클라우드가 보안 문제로 대두될 수 있다고 생각합니다.

그러나 문제를 먼저 해결하지 않으면 클라우드 보안은 요원할 뿐입니다. 아시아 태평양 지역의 대다수 기업(98%)은 클라우드 기반의 보안 및 인증에 문제가 있다고 생각합니다. 클라우드용 장치 관리는 IT 부서(44%)뿐만 아니라 직원들(35%)도 우려하는 부분입니다. 또한 보안 솔루션 관련 비용(41%)은 말할 것도 없고, 솔루션이 다른 시스템과 통합되는 방식(40%)과 통합으로 인한 애플리케이션의 성능 저하(30%)에 대한 우려도 두드러집니다. 적합한 보안 솔루션이라면 쉽게 관리 및 사용할 수 있고, 다른 시스템과 원활하게 통합되며, 경제적이어야 합니다.

78%

(전년 **74%**)는 대규모 데이터 유출 사고 위험 때문에 접근 관리 솔루션을 구현합니다.

더 효과적인 접근 제어 방식에 대한 뜨거운 관심

클라우드 및 웹 기반의 애플리케이션을 보호하는 데 가장 적합한 접근 관리 수단으로 2단계 인증(64%)이 손꼽히는데, 2단계 인증 체제는 다양한 방식으로 구현하거나 사용할 수 있습니다. 일본(9%)과 홍콩(8%) 기업들은 일반적으로 다단계 인증을 선호하지 않는데, 특히 홍콩 기업들은 전용 다단계 인증 솔루션만 사용(23%)하는 경향이 두드러집니다(일본은 9%). 다단계 인증용 접근 관리 솔루션을 사용하는 인도(51%) 기업과 싱가포르(49%) 기업들 사이에서는 온프레미스 ID 및 접근 관리(IAM) 솔루션이 가장 인기가 있습니다.

일부 기업은 아직 IAM 솔루션을 사용하고 있지 않지만, 대다수 기업은 조만간 2단계 인증 방식을 사용하기 시작하거나 사용 범위를 확대할 계획입니다. 스마트 싱글사인온은 가장 많은 기업이 사용 중이거나 도입을 고려 중인 솔루션입니다.(사용하거나 사용 범위를 확대할 계획이 없다는 응답자 8%, 내년 안에 사용 범위를 확대할 예정이라는 응답자 41%, 내년 이후에 사용 범위를 확대할 예정이라는 응답자 48%)

89%

는 민감데이터(57%)와 애플리케이션(45%)을 보호할 목적으로 스마트 싱글사인온의 사용 범위를 확대할 계획입니다.

2단계 인증 방식의 사용 범위를 어떻게 확장할 계획인지에 대한 의견은 엇갈립니다. 아시아 태평양 지역의 기업 55%는 전용 다단계 인증 솔루션을 구현할 계획입니다. 40%는 IDaaS/접근 관리 솔루션을 사용할 예정인 반면, 4%는 이 솔루션과 관련한 구체적인 계획이 아직 없습니다. 홍콩 기업은 전용 다단계 인증 솔루션(65%)을 가장 선호하는 반면 일본 기업 사이에서는 IDaaS/접근 관리 솔루션(51%)의 인기가 두드러집니다(홍콩과 호주는 각각 34%와 33%에 불과).

스마트 싱글사인온의 약진

아시아 태평양 지역의 거의 모든(98%) IT 의사 결정권자는 스마트 싱글사인온을 높이 평가합니다. 실제로 절반 이상(55%)의 기업이 이 솔루션을 사용하고 있고, 5곳 중 2곳은(40%) 조만간 사용할 계획입니다. 압도적 다수(99%)가 데이터 유출 방지(47%), 고객과 직원에게 데이터가 안전하다는 안도감 고취(각각 44%), 사용 편의성(44%) 등 스마트 싱글사인온을 사용할 때 따르는 이점을 인정한다는 사실을 고려하면 놀라울 것도 없습니다.

대다수 IT 의사 결정권자(95%)는 더 안전한 스마트 싱글사인온 솔루션 체제를 유지할 수만 있다면 좀 더 많은 데이터를 수집하고 관리해야 하는 번거로움도 감수하겠다는 입장입니다. 그러나 구체적인 수치는 국가마다 큰 차이를 보입니다. 이러한 목적으로 어떤 유형의 데이터든 기꺼이 수집하겠다고 답한 기업을 국가별로 살펴보면 호주(24%)와 홍콩(25%)보다 인도(44%)와 일본(43%)이 더 많습니다.

다음 단계 및 지침

이 연구 보고서의 이전 절에서 언급했듯, 대다수 응답자는 클라우드 접근 관리가 클라우드 도입 방안에 관한 기업 차원의 공감을 얻는 데 도움이 된다고 생각하며, 대부분은 여러 가지 다단계 인증 방식의 사용 범위를 확대할 계획입니다. 거의 모든 응답자(98%)가 스마트 싱글사인온 솔루션을 도입하기를 원합니다.

그렇다면 실무적인 관점에서 다음 단계는 무엇이고, IT 전문가가 접근 관리 및 인증 솔루션을 선택할 때 고려해야 할 사항은 무엇일까요? 권장안을 몇 가지로 간추리자면 다음과 같습니다.

1. **효율성 및 배포**
   클라우드 기반의 솔루션은 온프레미스에 대대적으로 설치할 필요가 없으므로 직원들에게 빠르게 배포할 수 있습니다. 솔루션을 평가할 때는 설치해야 하는 온프레미스 구성 요소 수, 필요한 서버 수, 이중화를 통해 다운타임을 방지하는 데 필요한 추가 서버를 확인하는 것이 바람직합니다.

2. **자동화**
   최종 사용자의 편의성을 고려하여 자동화된 토큰 등록 워크플로우와 원 클릭 방식 토큰 설치를 지원하는 서비스를 구독하는 것이 좋습니다. 사용자가 직접 빠르게 등록할 수 있으면 IT 인력의 부담이 감소하므로 기업 입장에서도 유리합니다.

3. **인증 및 토큰 유연성**
   모든 사용자의 요구에 부응하려면 저마다 다른 요구와 원하는 보안 수준을 수용할 수 있도록 다양한 인증 방식을 지원하는 솔루션을 물색해야 합니다. 이러한 인증 방식으로는 (모바일 장치나 데스크탑에 설치할 수 있는) Push OTP 앱, 모바일 장치나 이메일 주소로 전송되는 SMS 또는 이메일 코드, 패턴 기반의 인증, 사용자가 최종 장치에 소프트웨어를 설치할 필요가 없는 토큰리스 방식 등이 있습니다.

4. **모든 앱과 클라우드 서비스에 접근할 수 있는 솔루션**
   SAML, RADIUS 및 비표준 기반의 앱을 통해 앱에 대한 접근를 보호할 수 있는 솔루션을 물색하고, 클라우드 및 웹 기반의 앱만 보호할 수 있는 솔루션은 피해야 합니다. 그래야 단일 솔루션으로 모든 앱을 보호하고 편리한 싱글사인온 방식을 사용할 수 있습니다.

5. **보안과 편의성을 극대화하는 스마트 싱글사인온**
   클라우드 싱글사인온에 상황별 정보와 다단계 인증을 접목하면 보안을 저해하지 않으면서 가장 원활한 경험을 제공할 수 있습니다. 사용자가 단일 ID로 모든 클라우드 및 웹 애플리케이션에 접근하고, IT 부서는 위험부담이 큰 상황에서만 더 강력한 접근 보안 정책을 적용할 수 있습니다.

6. **유연한 정책 시행**
   유연한 정책이 뒷받침되는 클라우드 접근 관리 서비스를 구독하면 신뢰할 수 없는 네트워크에 대한 인증을 강화하고, 신뢰할 수 있는 네트워크 및 장치에 필요한 인증 수준을 완화할 수 있습니다.

7. **투명한 라이센싱 모델**
   가격 책정 모델이 너무 복잡한 서비스는 바람직하지 않습니다. 가격 책정 모델이 투명하고 기업에 필요한 기능을 갖춘 전용 접근 관리 및 인증 솔루션을 선택하면 향후 발생할 비용을 쉽게 분석하고 예측할 수 있습니다.

결론

오래전부터 IT 책임자들의 최대 당면 과제는 보안 위협의 심각성에 대한 이사회의 관심을 높이는 것이었습니다. 이제는 이사회 사이에서 보안의 중요성에 대한 공감대가 형성됐으므로 제로 트러스트 보안 정책을 구현하는 데 있어 접근 관리의 중요성을 설파하는 데 주력할 차례입니다. 제로 트러스트 보안이 구현되면 클라우드로 확장할 때 위험 관리 전문가가 '전방위적 보안 및 엄격 감시(Protect Everywhere - Trust Nobody)' 전략을 시행할 수 있습니다.

많은 기업이 코로나-19라는 난관 앞에서 비즈니스 연속성을 유지하느라 재택근무 체제로 전환할 수밖에 없는 실정입니다. 사이버 공격이 꾸준히 늘고 있는 와중에 이러한 악재마저 겹치면서 자격 증명 도용과 관련된 위협을 중심으로 보안 위험이 커지고 있습니다. 직원이 저마다 다른 클라우드 플랫폼을 사용하고 각자의 가정에서 다수의 시스템에 접근하기 때문에 이러한 보안 문제가 필연적일 수밖에 없습니다. 접근 정책을 시행하는 한편, 다양한 다단계 인증 방식을 통해 보안 인증을 지원하는 스마트 접근 관리 도구에 투자해야 하는 이유입니다. 비밀번호 같은 취약한 보안 방식의 사용 범위를 확대하면 훨씬 더 많은 문제가 발생할 뿐입니다.

데이터 보호에 미흡한 방법으로 입증된 비밀번호에 대한 의존도를 줄이려면 접근 보안 정책을 혁신해야 합니다. 클라우드 기반의 접근 방식과 비밀번호를 사용하지 않는 인증 방식을 활용하여 클라우드로 안전하게 확장하는 기업은 원격 근무자로 인해 접근 제어가 특히 중요하게 여겨지는 오늘날, 까다로워지는 보안 강화 규정을 준수할 수 있습니다. ID와 비밀번호를 유일한 인증 방법으로 사용하던 관행을 탈피하고 스마트 싱글사인온을 널리 사용하면 보안 경계 외부에서 실행되는 애플리케이션이 증가하더라도 더 우수한 수준의 보안과 편의성을 유지할 수 있습니다.

cpl.thalesgroup.com/apac-access-management-index**에서 자세한 내용을 확인하고 보고서를 다운로드하십시오.**

THALES

문의
서울특별시 용산구 독서당대로 98 6층 탈레스코리아 82.2.3278.8202

> cpl.thalesgroup.com <