cpl.thalesgroup.com

THALES

기존 IAM솔루션에서 최신 액세스 매니지먼트 솔루션으로 마이그레이션 하기: 모범 사례 및 지침

백서

목차

소개

기업들은 임직원들의 재택근무를 위한 보안을 지키면서, 클라우드 애플리케이션에 대한 액세스 및 인증관리를 해야 하는 도전과제를 해결해야 합니다. 싱글사인온(SSO), 가상 사설망(VPN), 웹 액세스 관리(WAM)와 같은 전통적인 온프레미스 IAM 솔루션은 네트워크 경계를 보호한다는 개념을 기반으로 합니다. 따라서, 임직원들이 클라우드 서비스에 안전하고 효율적으로 액세스할 수 있는 환경을 조성한다는 부분에서 제한점이 있을 수 있습니다. 클라우드 서비스 보안을 위해 온프레미스 경계 보안을 이용하는 기업은 사용하는 클라우드 서비스가 증가할 때 효과적인 보안을 구축하는 능력에 한계가 있습니다.

이에 대한 대안적인 접근 방식은 탈레스 SafeNet Trusted Access와 같은 클라우드 기반의 ID 서비스 아키텍처를 사용하는 것입니다. 이것은 기업이 네트워크 경계 너머까지 보안을 확장하고 최신 표준을 지원하지 않는 온프레미스 애플리케이션과 표준 기반 퍼블릭 클라우드 앱 모두를 보호할 수 있도록 지원합니다.

이 백서의 목표는 WAM, VPN 및 레거시 SSO를 비롯한 기존의 네트워크 인프라에서 벗어나 TCO 절감, 더 안전하고 스마트한 보안, 향상된 사용자 경험의 장점을 누릴 수 있도록 클라우드 기반 액세스 관리 솔루션으로 마이그레이션을 원하는 회사에 가이드를 제공하는 것입니다.

액세스 관리와 인증에 대한 필요성

기업은 전통적인 비즈니스 모델을 포기하고 빠른 속도로 디지털 트랜스포메이션을 도입하여 클라우드, 멀티 클라우드 및/또는 하이브리드 클라우드 환경을 수용하고 있습니다. 최근 몇년간 클라우드 애플리케이션의 채택률이 크게 증가했으며, 기업의 규모에 상관없이 자사 비즈니스 모델을 클라우드 기반으로 바꾸고 있습니다.

원래 클라우드 도입에 박차를 가한 것은 유비쿼터스와 고객 참여 등의 비즈니스 차원의 요구에 따른 것이었지만, 오늘날 IT 서비스는 대부분 Microsoft, Google, AWS와 같은 클라우드 서비스 제공업체가 추진하는 클라우드로 마이그레이션되고 있습니다. 대부분의 기업들은 이미 새로운 방식의 작업 및 직원 협업 강화를 위해 SaaS 애플리케이션을 도입했습니다.

클라우드 퍼스트 이니셔티브 및 전략이 대다수 기업의 최우선 순위이지만 클라우드로의 본격적인 전환을 완료하기 위해서는 몇 년이 더 소요될 수도 있습니다. 많은 기업들이 이미 일부 애플리케이션을 클라우드로 전환했지만 다른 온프레미스 앱 및 데이터 저장소 또한 계속해서 사용하고 있습니다. 기업의 혁신성과는 관계없이, 성숙한 기업이라면 필연적으로 기업내부에 기존 시스템이 존재하게 됩니다.

기존의 시스템과 새로운 시스템을 혼재하여 사용하는 것은 주위에서 흔히 볼 수 있습니다. 분리가 어려운 맞춤형 데이터 저장소와 관련 앱을 가지고 있는 기업들의 경우 온프레미스 인프라를 그대로 유지하고 싶어합니다. 또한, 기업내에 클라우드 마이그레이션에 전념하기 위한 자원이 부족할 수도 있습니다. 이뿐 아니라, 온프레미스 애플리케이션은 기업들의 고객정보와 연결되어 있고,수익을 창출하고 있기 때문에 기업들은 이를 고수하고자 하기도 합니다.

하이브리드 방식으로 구현되는 애플리케이션에 대한 보안을 지키는 것은 비즈니스가 정상적으로 흘러가지 못하는 비상상황이 발생했을 때 비즈니스 연속성을 지키기 위해 매우 중요합니다. 폭우, 지진과 같은 자연재해, 국가 안보 사유로 인한 사업 중단, 전염병 발생으로 인한 질병 등의 계획에 없던 사건사고들은 비즈니스에 치명적인 영향을 미칠 수 있습니다. 따라서, 오늘날 기업들은 모든 임직원들이 안전하고 확장가능한 방식으로 원격에서도 근무할 수 있는 환경을 제공해야 합니다.

보안이 핵심입니다

보다 많은 기업이 최신의 기술 트렌드를 따르며 클라우드 컴퓨팅을 수용함에 따라, 보안이 가장 큰 관심사로 떠올랐습니다. 이는 특히 클라우드 서비스에 대한 피싱 공격이 급증하는 데에 기인하며, 피싱 공격은의 대부분이 대규모 데이터 유출로 이어졌습니다. 결과적으로 IT 팀들은 클라우드 및 온프레미스 애플리케이션에서 일관된 방식으로 보안 규제 준수를 관리하기 위해 액세스 컨트롤을 중앙에서 정의하고 시행하는 간결하고도 효율적인 방법을 찾고 있습니다.

전통적으로, 조직은 CA SiteMinder, Oracle Access Manager, IBM Tivoli Access Manager 같은 가상 사설망(VPN), 온프레미스 싱글사인온(SSO), 웹 액세스 관리(WAM) 솔루션을 사용하여 기업 리소스에 대한 인증 및 권한을 제어했습니다.

클라우드 기반 앱과 분산 컴퓨팅 모델이 확산되면서 기존 솔루션들이 더 이상 현대적인 IAM 요구 사항들을 해결할 수 없게 됐습니다.

기존 접근관리 솔루션의 한계

기업이 클라우드 컴퓨팅 환경을 적극적으로 수용하고, 재택근무를 확산시킴에 따라,기존에 쓰이던 온프레미스 경계 보안 접근 방식으로는 더이상 기업의 데이터 보안을 지킬 수 없게 됐습니다. 여기에는 다음과 같은 약점이 있습니다.

- 클라우드 액세스 트래픽이 온프레미스 솔루션을 통하도록 하면 네트워크에 과부하가 걸리고 전체 네트워크 트래픽이 느려집니다.
- 클라우드 액세스를 위해 VPN이나 WAM을 사용하면 단일 장애 지점이 발생하고 VPN이 다운될 경우 직원이 중요한 클라우드 앱에 액세스할 수 없는 위험이 증가합니다.
- 직원이 단일 자격 증명으로 전체 네트워크에 액세스할 수 있게 하면 그 자격 증명이 손상될 경우 보안 측면에서 아주 큰 타격을 받을 수 있습니다.
- 수백 개의 클라우드 앱을 수용하기 위해 기존방식의 온프레미스 솔루션을 유지 및 확장하는 비용은 안전한 원격 액세스를 위한 클라우드 기반 솔루션을 구현하는 비용보다 훨씬 높습니다

기존 IAM 솔루션이 클라우드 액세스를 효율적으로 처리할 수 있는지 평가하기

멀티 팩터 인증

기존 IAM 솔루션은 하드웨어 또는 소프트웨어 토큰으로 사용자를 인증합니다.이는 로그인 프로세스 첫단계에서 단한번 발생하는 이진법적 결정입니다. 이진법적인 결정은, 직원들이 자신만의 장치를 사용한다 하더라도, 거의 모든 곳에서 회사 자산에 액세스할 수 있는 오늘날의 비즈니스 환경과 맞지 않습니다. 환경의 위험수준에 맞추어 인증 수준이 조정되지 않기 떄문입니다. 사용자 인증에 대한 민첩하고 세분화된 접근 방식을 제공하기 위해서는 IAM 솔루션이 사용자의 장치 센서에서 수집한 상황 데이터를 기반으로 위험 증가 정도에 맞추어 인증 조건을 강화하는 상황 인지 방식을 제공해야 합니다.

또한 소프트웨어 토큰과 쉽고 자동화된 토큰 배포 및 등록 기능이 결합되면 모든 직원에게 원활한 로그인 경험을 제공할 수 있습니다. 모든 사용자의 요구를 만족시키려면, IAM 솔루션이 다양한 요구와 보안 수준을 수용할 수 있는 다양한 패스워드리스 인증 방법을 제공해야 합니다.

아래 표는 전통적인 IAM 솔루션 및 IDaaS 인증 솔루션이 제공하는 MFA 기능에 대한 대략적인 정보를 제공합니다.

	기존의 IAM 솔루션(VPN, WAM, SSO)	IDaaS
패스워드리스	토큰 기반, 하드웨어 또는 소프트웨어	비 토큰: 푸시 OTP 앱, SMS 또는 이메일 코드, 패턴 기반
인증 결정 방식	첫 진입시 이진법적(예/아니요) 결정	위험이 증가함에 따라 조정하는 어댑티브 결정

표 1: 멀티 팩터 인증, 기존 및 IDaaS IAM 솔루션 비교

기업용 싱글사인온

Microsoft AD FS 또는 Ping Federate와 같은 기존의 기업 SSO 솔루션은 온프레미스로 구현되며 일반적으로 SAML과 같은 프로토콜을 통한 연계를 지원합니다. 그러나 이러한 솔루션은 세션 시작시 제공되는 단일 자격 증명을 사용하여 싱글 사인온을 허용합니다. 단일 자격 증명이 손상, 도난, 분실되면 모든 기업 애플리케이션이 위험에 노출됩니다.

보안을 약화시키지 않으면서도 사용이 쉬운 로그인 환경을 제공하기 위해서는 컨텍스트에 맞는 정보 및 인증 방식 조정이 결합된 클라우드 기반 스마트 SSO를 활용해야 합니다. 이를 통해 직원들은 단일 ID로 모든 클라우드와 웹 애플리케이션에 액세스할 수 있으며, 이러한 액세스 시도가 매번 평가되기 때문에 IT 팀이 위험이 높은 상황에서 보다 강력한 액세스 보안을 시행할 수 있습니다. 스마트 SSO를 통해 최종 사용자는 비즈니스 생산성을 유지하고 앱마다 따로 다시 인증해야 하는 번거로움을 줄일 수 있습니다.

아래 표에서 기존 및 IDaaS IAM 솔루션에서 제공하는 싱글사인온 기능에 대한 개요를 확인하실 수 있습니다.

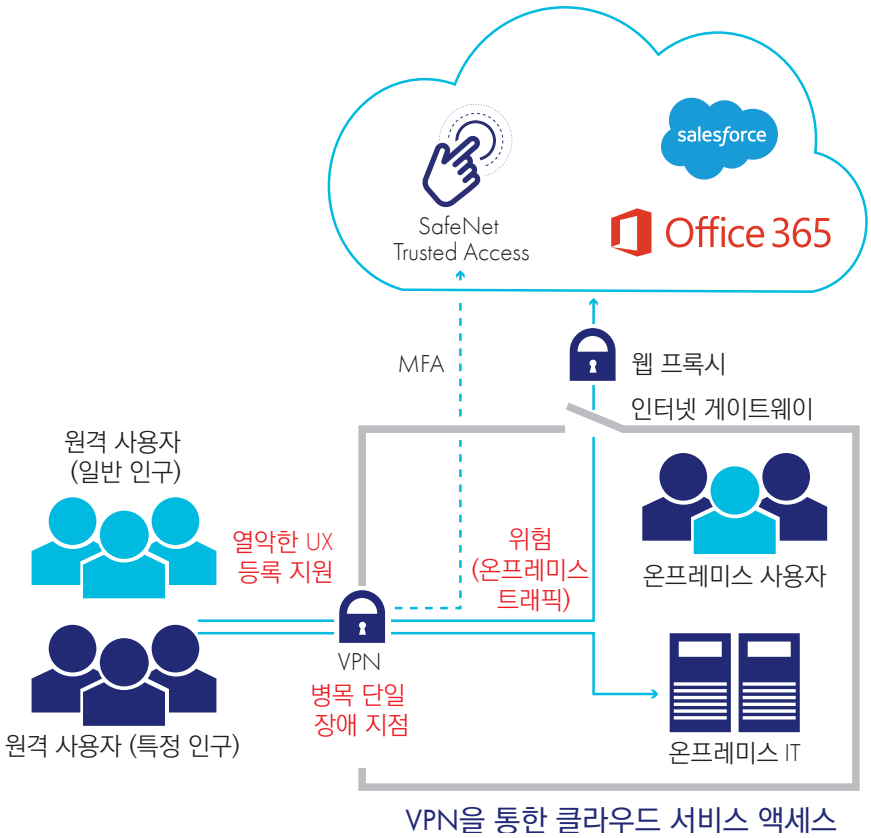
	기존방식(VPN, WAM, SSO)	IDaaS
구현	온프레미스	클라우드
연계	예	예
보안	광범위한 SSO, 동일한 자격 증명으로 모든 앱에 액세스	어댑티브 스마트 SSO, 단일 신원을 지속적으로 평가하고 인증 수준 조정
정책 엔진	**오픈 액세스** 모든 사용자 및 애플리케이션에 대한 단일 액세스 정책	**정책 기반** 비즈니스 요구사항, 애플리케이션 민감도 및 직원 업무 별로 액세스 정책 설정
인증	**지점 인증** 사용자가 동일한 인증 방법으로 모든 서비스에 액세스	**보편 인증** 로그인 시도마다 컨텍스트 인증으로 적절한 MFA 또는 인증 수준 적용

표 2: 스마트 싱글사인온(SSO), 기존 및 IDaaS IAM 솔루션 비교

경계 컨트롤

WAM, VPN 및 방화벽과 같은 기존방식의 경계관리 온프레미스 솔루션입니다. 중앙의 온프레미스 허브를 통해 트래픽을 제어합니다. 이 설정은 온프레미스에서 생성된 트래픽에 효율적일 수 있지만, 클라우드에서 생성되거나 클라우드로 라우팅되는 트래픽에는 효과적이지 않습니다. 보안 및 액세스 요청을 평가하기 위해 클라우드에서 온프레미스 서버로 트래픽을 유도하면 병목 현상과 단일 액세스 지점 장애가 발생할 수 있습니다.

직원이 원격으로 작업해야 하는 경우 현대적인 접근 방식은 제로 트러스트 액세스 평가를 구현하는 것입니다. 기업은 액세스 요청을 제로 트러스트에 기반하여 애플리케이션마다 따로 액세스 지점에서 평가하도록 해야 합니다. 이렇게 하면 애플리케이션, 정책 및 액세스 시나리오 별로 분산된 액세스 결정을 내릴 수 있습니다. 이러한 서비스는 신뢰할 수 없는 네트워크에 대한 인증은 강화하고 허용된 네트워크에 필요한 인증은 완화할 수 있도록 지원합니다. 마찬가지로 액세스 관리 솔루션은 애플리케이션에 따라 인증 규칙을 변경하는 정책을 설정할 수 있어야 합니다.



VPN을 통한 클라우드 서비스 액세스

아래 표에서 기존 및 IDaaS IAM 솔루션에서 제공하는 경계 컨트롤 기능에 대한 개요를 볼 수 있습니다.

	기존방식(WAM, VPN, 방화벽)	IDaaS
액세스 컨트롤	중앙집중형, 온프레미스 허브	액세스 지점
제로 트러스트	모든 앱에 대해 단일한 로그인	지속적인 앱, 정책, 로그인 별 액세스 평가
가용성	온프레미스 허브로 인해 단일 지점에서 장애 발생	클라우드에서 클라우드까지
적응성	모든 앱에 대한 단일 로그인, 점증식 수준 적용 없음	신뢰할 수 없는 네트워크에 대한 인증 강화, 위험에 따라 인증 수준 완화
비용	인프라 및 서버에 대한 투자가 필요하여 온프레미스 인프라 확장 비용이 높음	클라우드 기반 액세스 관리에는 인프라 투자가 필요하지 않음 지원 및 유지관리 역시 포함

표 3: 경계 컨트롤, 기존 솔루션 및 IDaaS IAM 솔루션 비교

신원 서비스(IDaaS) 솔루션은 디지털 트랜스포메이션과 비용 절감을 도와줍니다

신원 서비스(IDaaS)는 조직에서 싱글사인온, 인증, 액세스 컨트롤을 사용하여 클라우드 서비스에 직접 안전하게 액세스할 수 있도록 하는 SaaS 기반 IAM 솔루션입니다.

IDaaS는 다음과 같은 다양한 이점을 제공하기 때문에 대부분의 새로운 액세스 관리 배포에서 선호되는 전달 방법이 되었습니다.

- 액세스 지점에서 기업 및 클라우드 앱을 보호하여 유출 위험 감소
- 사업장 외부나 집에서 필요한 앱에 원활하게 액세스할 수 있어 신원 관리 복잡성 감소
- 클라우드 기반 전달을 활용한 손쉬운 배포
- 액세스 관리 기능을 지속 가능한 방식으로 지원하기 위해 서버에 투자하지 않고도 가치 실현 시간과 비용 절감 측면에서 향상
- 클라우드에서 IAM 서비스가 제공되므로 높은 가용성 및 안정성으로 단일 지점에서의 장애 발생 방지
- 자주 시행되며 사용하기 쉬운 기능 업그레이드

SafeNet Trusted Access가 기업의 최신 IAM 아키텍처 구현을 돕는 방법

포괄적인 IAM 플랫폼은 다양한 인증 상황을 처리하고 모든 기업 애플리케이션에 대해 강력한 액세스 보안을 제공해야 합니다. SafeNet Trusted Access를 통해 기업은 광범위한 인증 기능으로 기업 애플리케이션을 보호하고 이를 클라우드로 안전하게 확장할 수 있으며, 한편으로는 스마트 싱글사인온(SSO) 및 정책 기반 액세스 컨트롤을 통해 보안을 확보할 수 있습니다.

멀티 팩터 인증

SafeNet Trusted Access는 위험 수준에 따라 인증 수준을 변경할 수 있는 포괄적인 인증 기능을 제공함으로써 기업의 전체 애플리케이션 포트폴리오에서 MFA를 보다 손쉽게 구현할 수 있습니다. SafeNet Trusted Access의 주요 이점은 하드웨어 및 소프트웨어, SMS 및 이메일, 푸시 알림, 생체 인식을 포함한 다양한 MFA 폼 팩터를 지원하며, OTP, PKI(인증서 기반), 패턴 기반 인증, 및 어댑티브 인증을 포함한 다양한 인증 방법을 지원한다는 것입니다.

SafeNet Trusted Access는 RADIUS, OpenID, SAML을 포함한 모든 인증 표준을 지원합니다. 이것은 모두 클라우드에서 제공됩니다. 또한 SafeNet Trusted Access는 PUSH OTP, 인증서 기반 인증, FIDO 인증, Windows Hello 등의 다양한 방법으로 FIDO를 통한 패스워드리스 인증을 지원합니다.

SafeNet Trusted Access

범용 인증 방법

그림 1: 탈레스의 SafeNet Trusted Access 인증 방법

이미 배포된 MFA 체계 활용

PKI 인증을 클라우드로 확대

적절한 보장 수준 제공

패스워드리스 인증으로 편의성 제공

스마트 싱글 사인온(SSO)

SafeNet Trusted Access의 핵심 장점 중 하나는 매우 유연한 액세스 정책을 설정할 수 있는 정책 엔진입니다. 보안 정책은 인증 시간 제한과 같은 특정 이벤트가 아닌, 세션 중에 사용자를 지속적으로 재평가할 수 있는 매우 세분화된 특정 규칙을 제공합니다. 위험 수준이 변경되면 SafeNet Trusted Access는 사용자가 재인증하거나 더 강력한 형태의 인증을 수행하도록 요구합니다.

정책은 애플리케이션 별로 설정되며, 네트워크 범위, 운영체제, 사용자, 지리적 위치에 적용됩니다. 인증 규칙은 필요에 따라 동적으로 컨텍스트에 따라 설정할 수 있습니다. 예를 들어, 모든 액세스 시도마다 인증하도록 하거나, 또는 더 위험한 특정 상황에서는 더 강한 인증을 요구하는 식으로 확인하도록 인증 규칙을 적용할 수 있습니다.

SafeNet Trusted Access는 지속적인 어댑티브 액세스 관리를 위한 통합 신원 증명 기능을 제공하기 위해 다음과 같은 기능 요구 사항을 지원합니다.

- 컨텍스트 기반 "조건부" 액세스 컨트롤.
- 애플리케이션과 다른 위험 컨텍스트 정보 소스 간의 통합
- 지속성. 모든 세션에 걸쳐, 모든 액세스에 대한 위험 및 신뢰가 자동으로 평가되며, 이는 애플리케이션과의 통합을 통해서만 가능합니다.

경계 컨트롤

SafeNet Trusted Access는 클라우드에서 태어나 클라우드에서 살아갑니다. 따라서 온프레미스 인프라에 의존하지 않으며 병목 현상을 피하면서 클라우드의 액세스를 제어할 수 있습니다. 또한, 모든 인증 및 액세스 관리 서비스가 액세스 지점마다 제공되므로, SafeNet Trusted Access가 분산 네트워크 환경에 대한 경계 없는 보안을 가능하게 함으로써 제로 트러스트 접근 방식을 구현할 수 있습니다.

이러한 경계 없는 접근 방식은 단일한 장애 지점으로 인해 보안이 위험에 빠지지 않도록 하고 어떤 애플리케이션이든 위치에 상관없이 위험 기반 어댑티브 인증을 적용 받을 수 있도록 지원합니다.

다음 단계: 기존방식 IAM 솔루션에서 SafeNet Trusted Access로의 마이그레이션

이 섹션에서는 온프레미스 및 클라우드 서비스를 기존 IAM 솔루션에서 SafeNet Trusted Access로 마이그레이션하는 방법에 대해 단계별로 알아보겠습니다. 많은 조직이 자신의 모든 앱에 대해 대규모 마이그레이션을 수행할 수 있는 상황이 아니라는 사실을 고려하여, 조직 내 특정 그룹의 요구에 기반한 단계별 접근 방식을 제안합니다.

단계 1.

온프레미스 및 클라우드 서비스 전체를 매핑하여 보호해야 할 것이 무엇인지 명확하게 파악하십시오.

단계 2.

서비스에 대한 완전한 가시성을 확보한 후에는 다음 사항을 수행하실 것을 권장합니다.

- 각 서비스 및 앱이 지원하는 프로토콜을 평가하십시오. 해당 애플리케이션이 SAML이나 OpenID Connect와 같은 최신 표준을 지원하는지 확인하십시오. 많은 기업용 웹 애플리케이션은 기본적으로 SAML 기능을 지원지만, 일부는 비표준 통합이 필요할 수 있습니다.
- 이러한 앱에 주로 액세스하는 사용자를 분류하십시오. 예를 들어 관리자입니까, 아니면 경영계층 사용자, 또는 일반 사용자입니까?
- 앱 별로 민감도를 결정하고 각 앱에 적용할 적절한 인증 수준을 확인하십시오.

단계 3.

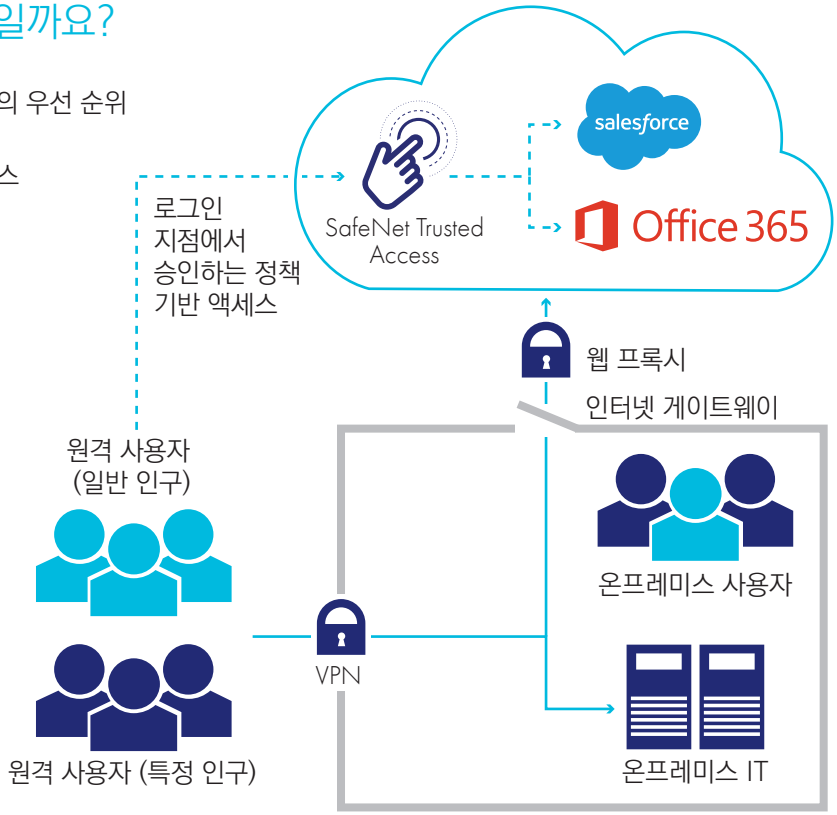
각 서비스에 인증 및 액세스 제어를 제공하기 위해 사용되는 IAM 솔루션을 파악하십시오. 서비스가 WAM, VPN 또는 온프레미스 SSO로 보호됩니까?

단계 4.

먼저 구현해야 하는 앱과 사용자 그룹의 우선 순위를 정하십시오. VPN 또는 WAM을 통해 액세스하는 클라우드 앱과 비밀번호로 액세스하는 앱을 우선 순위로 지정하는 것부터 시작하면 좋습니다. 대부분의 사용자가 SafeNet Trusted Access를 통해 클라우드 서비스에 직접 액세스할 수 있도록 허용하면, 즉시 네트워크 트래픽을 줄이고 액세스 지점에서 클라우드 서비스를 안전하게 보호할 수 있습니다. SafeNet Trusted Access를 구현하는 2번째 단계에서는 보호할 온프레미스 앱의 우선 순위를 정해야 합니다. 이러한 앱의 우선 순위를 정하는 좋은 방법은 Radius, OIDC 또는 SAML을 지원하는 앱부터 시작하는 것입니다. SafeNet Trusted Access는 연계 마법사를 제공하므로, 이러한 애플리케이션 지원을 간단하게 설정할 수 있습니다. 3번째 단계는 표준 프로토콜을 지원하지 않는 레거시 앱을 마이그레이션하는 것입니다. 이를 위해서는 에이전트 또는 API를 사용합니다.

배포 KPI: SafeNet Trusted Access 구현 1일차에 달성할 수 있는 것은 무엇일까요?

- 클라우드 기반의 MFA 서비스 설정
- 마법사 기반 연계 템플릿을 사용하여 1단계에서의 우선 순위 목록에 정의된 앱들을 연계
- 각 앱에 대해 시행된 위험 평가를 기반으로 액세스 정책 설정
- 필요에 따라 정책을 모니터링 및 조정



SafeNet Trusted Access
를 이용한 클라우드 서비스 액세스

결론

클라우드에서 안전하게 확장하고 직원 재택 근무를 가능하게 하며 비용을 절감하는 능력이 그 어느 때보다 중요해졌습니다. 실제로, Gartner에 따르면 기업의 74%가 이동성을 제공하고 비용을 줄이기 위해 코로나19[1] 이후에 더 많이 원격 작업으로 영구 전환할 계획이라고 합니다.

신원 및 액세스 관리를 위해 기존의 솔루션을 계속 고수하는 것으로는 최신 아키텍처를 지원하고 조직이 클라우드의 효율성을 최대한 활용하는 데 부족함이 많습니다. SafeNet Trusted Access 같은 최신 클라우드 기반 액세스 관리 플랫폼을 구현하면 비즈니스 발전을 가속화하고 데이터 유출 위험을 줄이는 한편 민첩성과 비용 절감을 확보할 수 있습니다.

탈레스 소개

귀하의 데이터를 보호하는 기업들은 탈레스를 통해 자신들의 데이터를 보호합니다. 데이터 보안에 대해 중요한 결정을 내려야 하는 순간이 증가하고 있습니다. 암호화 전략을 수립하거나, 클라우드로 데이터를 이전하거나, 규제 준수 요구사항을 충족시켜야 하는 모든 순간에 탈레스를 믿고 찾아주십시오. 탈레스는 귀하의 안전한 디지털 트랜스포메이션을 지원합니다.

결단이 필요한 순간을 위한 결정적인 솔루션.

1 Gartner에서 CFO들을 대상으로 한 설문조사에 따르면 일부 직원을 원격 근무로 영구 전환하겠다고 답한 응답자가 74%를 기록했습니다
https://www.gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-surey-reveals-74-percent-of-organizations-to-shift-some-employees-to-remote-work-permanently2

대한민국 – 서울특별시 용산구 한남동 독서당로 98 여선교회관 6층
| 전화: 82.2.2088.4678 팩스: 82.2.3278.8290 |
이메일: krsales.cpl@thalesgroup.com

> cpl.thalesgroup.com <