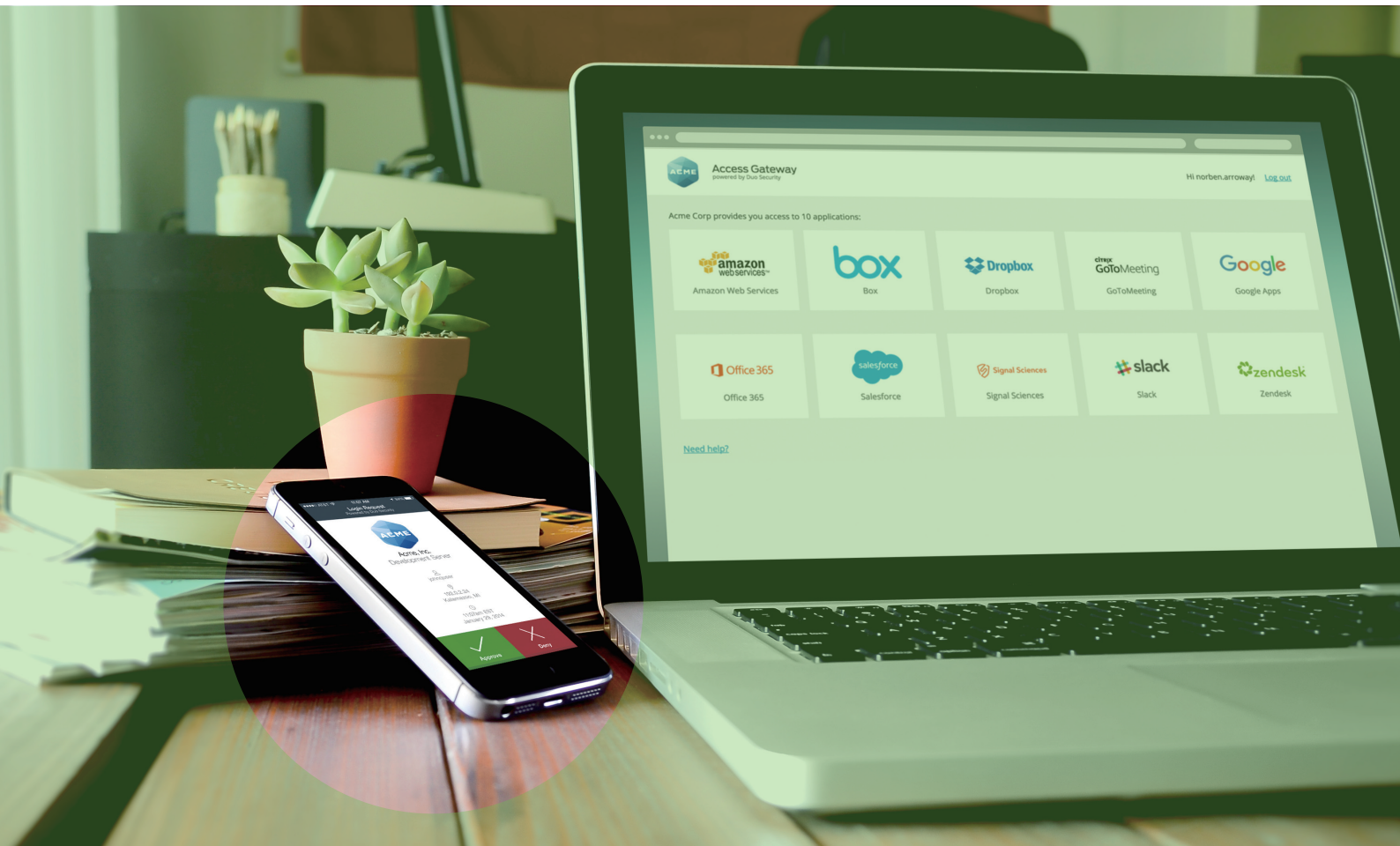


Cisco Duo Security

사용자와 디바이스 보안을 위한 제로트러스트 솔루션



Cisco Duo 보안은 “멀티팩터인증”(Multi-Factor Authentication : MFA)과 디바이스 가시성을 위한 솔루션입니다.

애플리케이션에 접근하려는 사용자 및 디바이스에 대해 제로 트러스트 방식을 통해 멀티팩터 인증 및 디바이스 보안 검사, 커스터마이징 된 접근 정책에 따라 접속을 허용합니다.

Duo는 간단하고 신속하게 도입하고 운영 관리할 수 있는 클라우드 기반의 보안 서비스입니다.

변화하는 비즈니스 환경에서 제로(0)로부터 트러스트(신뢰)를 만들어 내는 새로운 접근 방식을 통해 디지털 시대의 사용자를 보호하십시오.



**사용자 트러스트
(멀티팩터인증:MFA)**

2개 이상의 인증으로
사용자 확인



**디바이스 트러스트
(디바이스 가시성)**

디바이스 무결성 및
보안 검증



**맞춤형
접근정책**

다양한 조건에 따른
유연한 접근정책 설정



**싱글사인온(SSO)과
원격 접속**

사내외 상관없이 SSO
구축 및 원격 접속

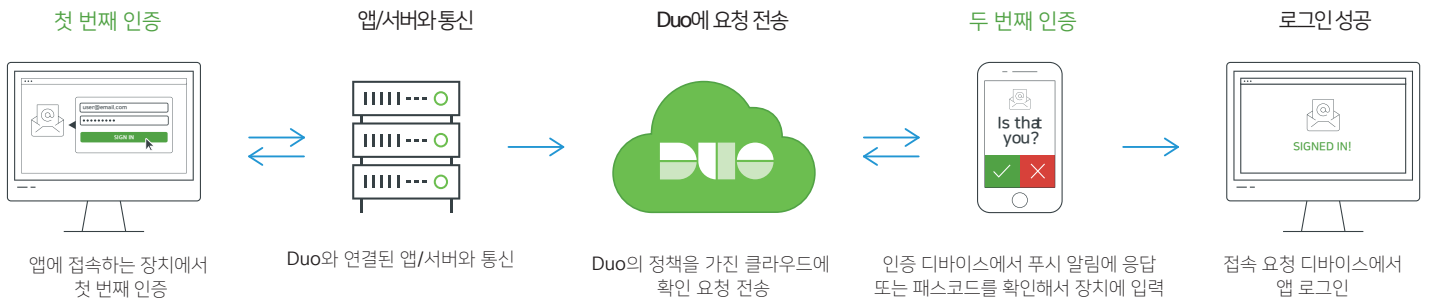
사용자 트러스트(멀티팩터인증 : MFA)

Cisco Duo는, 간단하고 쉽게 도입할 수 있는 「멀티팩터 인증」(Multi-Factor Authentication;MFA) 솔루션입니다. 사용자명이나 패스워드 등에 의한 첫 번째 인증 방식과 더불어 사용자가 소지하고 있는 기기에 의한 소유자 인증, 지문이나 얼굴등 사용자 본인의 생물학적 특징에 의한 생체 인증과 같이 다양한 요소를 두번째 인증방식으로 함으로써 어플리케이션에 접속하고자 하는 사용자가 '본인이 맞습니다'라는 신뢰를 구축합니다.

클라우드 기반의 보안 서비스이므로 기존의 IT인프라에 대한 영향을 최소화하고 도입할 수 있습니다. Office 365 등 다양한 클라우드 어플리케이션 및 플랫폼과의 통합이 간단합니다. 사용자 스스로 인증 방식을 선택 가능하고, 스마트폰이나 웨어러블 등 선호하는 디바이스를 등록 관리하여 멀티팩터 인증을 편리하게 이용할 수 있습니다.



사용자 스스로 다양한 인증 방식 선택 가능



디바이스 트러스트(디바이스 가시성)

Cisco Duo는 애플리케이션에 액세스하는 모든 장치를 가시화 할 수 있습니다.노트북, 데스크탑 PC, 모바일 장치 등 기기 유형에 관계없이 운영체제나 브라우저, 플러그인 및 기업소유 여부 등 다양한 정보를 단일 대시보드로 파악할 수 있습니다.

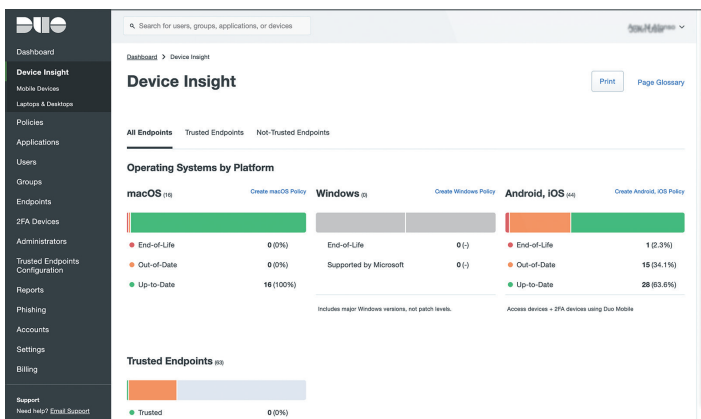
Cisco Duo 에서는 인증 시 디바이스의 보안 상태를 확인하고 가시화 및 제어를 할 수 있습니다. 예를 들어 신뢰할 수 있는 사용자라 하더라도 디바이스의 OS나 브라우저가 오래된 경우나 안티바이러스나 안티멀웨어, 스크린 잠금 등 특정 보안 기능을 활성화하지 않은 경우에는 애플리케이션에 대한 접근을 차단하여 업데이트나 보안성 확보를 하는 것도 유도 가능합니다.



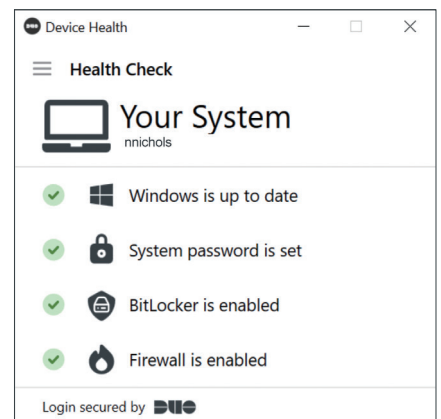
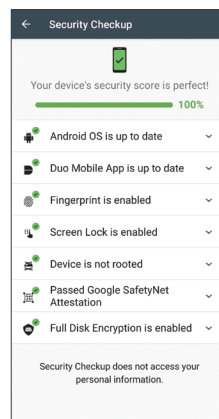
엑세스 디바이스 또는 인증 디바이스에 보안 위험이 존재하는 경우 각각의 디바이스에서 사용자가 알림을 수신



Duo 대시보드를 통해 디바이스 정보 파악



사용자 스스로 디바이스의 보안 상태를 확인할 수 있는 기능 제공



맞춤형 접근 정책

Cisco Duo에서는 유연하고 상세한 접근 정책을 설정하여 애플리케이션 접근을 제어할 수 있습니다. 모든 애플리케이션 및 사용자에게 적용되는 편집 가능한 글로벌 정책과 더불어 특정 애플리케이션에 대해 모든 사용자 또는 특정 사용자 그룹에 적용되는 커스텀 정책을 생성할 수 있습니다.

• 글로벌 정책

모든 애플리케이션 및 사용자에게 적용

• 커스텀 정책

- 특정 애플리케이션에 대한 정책을 모든 사용자에게 적용
- 특정 애플리케이션에 대해 그룹 정책으로서 특정 사용자 그룹에 적용

각 정책에서는 다음과 같이 다양한 조건에 따라 인증을 허용/비허용과 같이 다양한 액션을 설정할 수 있습니다.

- 신규 사용자인지 기존 사용자인지 여부
- 인증 방식
- 사용자 위치(국가)
- 사용자가 사용하는 디바이스의 신뢰성
- 사용자가 사용하는 네트워크 신뢰성
- 인증 디바이스 상태
- 기업 소유 디바이스인지 개인 소유 디바이스인지



• 글로벌 정책:

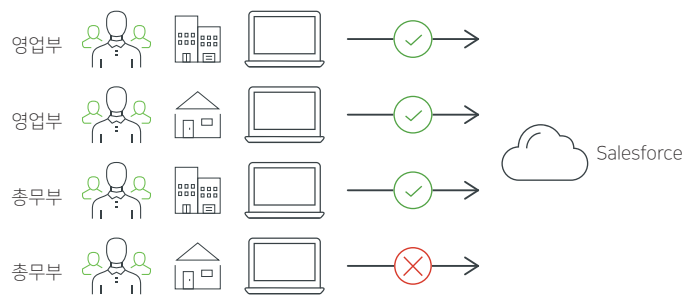
디바이스의 보안 건전성이 낮은 경우 접근할 수 없도록 설정



• 애플리케이션 정책: AWS에는 사외에서 접근할 수 없도록 설정



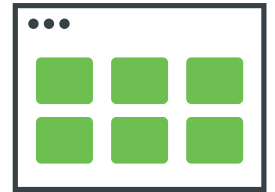
• 그룹 정책: Salesforce에는 총무부 사용자가 사외에서 접근할 수 없도록 설정



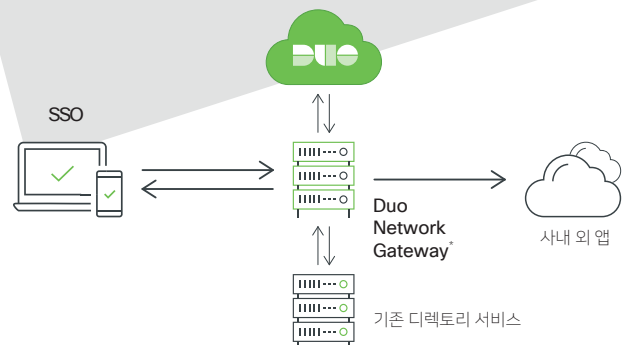
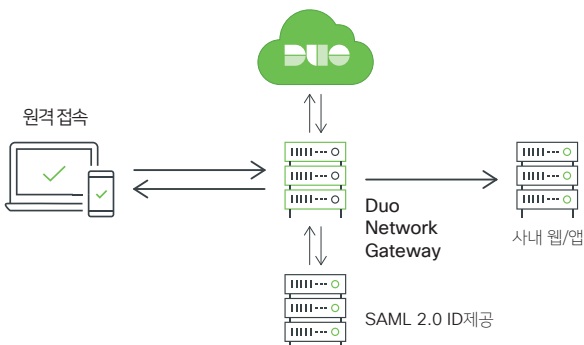
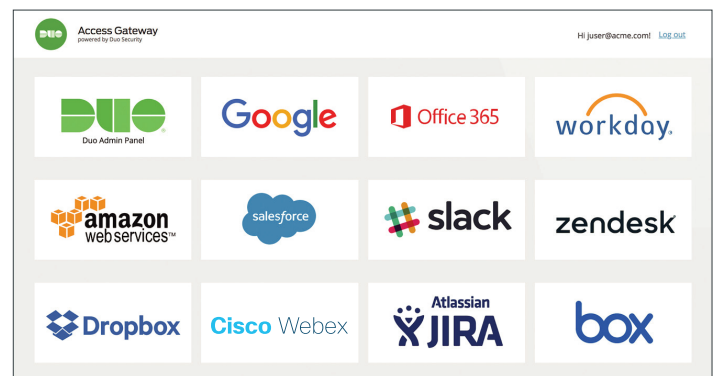
싱글 사인온(SSO)과 원격 접속

Cisco Duo는 클라우드/온프레미스에 관계없이 다양한 애플리케이션에 한번의 로그인으로 접근할 수 있는 싱글 사인온 (Single Sign-On; SSO)을 지원합니다. 사용자는 Duo Access Gateway에서 전용 포털에 한번 로그인하면 이미 등록된 애플리케이션에 인증 없이 접속이 가능합니다. 포털 로그인에 멀티팩터인증을 적용하여 디바이스의 보안 상태를 확인하였으며, 애플리케이션 접속에 맞는 맞춤형 접근 정책을 적용하여 SSO가 유발하는 보안에 위협을 없앨 수 있습니다.

또한 Cisco Duo는 VPN 없이도 안전한 원격 접근을 지원합니다. Duo Network Gateway를 통해 사용자는 회사 밖에서도 사내 웹사이트나 웹 어플리케이션, SSH 서버에 접속할 수 있습니다. Cisco Any Connect 나 서드파티의 기존 VPN 서비스에 Cisco Duo의 멀티팩터 인증을 조합해 운용하는 것도 가능합니다.



Duo의 싱글 사인온 사용자 포털



* 클라우드 버전도 제공

Cisco Duo 구매 가이드

Cisco Duo는 조직의 규모와 관계없이 간단히 도입 및 운용할 수 있는 SaaS 모델로 제공됩니다. 사용자수에 따른 라이선스를 1~5년의 서브스크립션 기간 동안 구입할 수 있습니다.

Cisco Duo MFA 라이선스*1

제품명	제품설명
DUO-MFA	Duo MFA 사용자 라이선스

*1 DUO-SUB 필요

Cisco Duo Access 라이선스*1

제품명	제품설명
DUO-ACCESS	Duo Access 사용자 라이선스

*1 DUO-SUB 필요

Cisco Duo Beyond 라이선스*1

제품명	제품설명
DUO-BEYOND	Duo Beyond 사용자 라이선스

*1 DUO-SUB 필요

Cisco Duo 추가 라이선스

제품명	제품설명
DUO-TOKEN-10PACK	하드웨어 토큰(10개)

30일간 무료로 사용해 보세요!
데모 종료 후에는 자동으로 Duo Free Edition으로 변경됩니다.

 signup.duo.com/trial



Cisco Duo Edition 기능비교		Duo Free	Duo MFA	Duo Access	Duo Beyond
보안 서비스	사용자 트러스트 (멀티팩터인증:MFA)				
	iOS 및 안드로이드용 모바일 앱 'Duo Mobile' 푸시 알림을 통한 인증	●	●	●	●
	앱 및 SMS, 전화 착신, 하드웨어 토큰을 통한 패스코드 인증, U2F 및 WebAuthN을 통한 생체인증 등	●	●	●	●
	1 사용자 당 연간 100 Credit의 전화 착신 인증 및 SMS 인증	-	●	●	●
디바이스 트러스트 (디바이스 가시성)	사용자 스스로 등록 및 관리	-	●	●	●
	애플리케이션에 액세스하는 모든 디바이스를 파악할 수 있는 대시보드	-	●	●	●
	위험한 디바이스 감시 및 식별	-	-	●	●
	노트북 및 데스크톱 PC의 보안 상태 확인 (Duo 디바이스 어플리케이션 체크)	-	-	●	●
	모바일 디바이스의 보안 상태 확인	-	-	●	●
	노트북 및 데스크톱 PC가 기업 소유인지 개인 소유인지 식별	-	-	-	●
	모바일 디바이스가 기업 소유인지 개인 소유인지 식별	-	-	-	●
	안티바이러스나 안티멀웨어 등 서드파티 에이전트가 유효한지 여부 식별	-	-	-	●
맞춤형 인증/정책	보안 정책을 전체 애플리케이션 또는 개별적으로 할당	-	●	●	●
	승인된 네트워크 여부에 따른 정책 적용	-	●	●	●
	사용자의 위치에 따라 정책 적용	-	-	●	●
	사용자 그룹별 보안 정책 연결 및 적용	-	-	●	●
	익명 네트워크 차단	-	-	●	●
	소프트웨어 버전, 암호화 및 방화벽 유무 등 보안 상태를 기반으로 노트북 및 데스크톱 PC에 정책 적용	-	-	●	●
	암호화 및 조작, 화면 잠금, 생체 인증 유무 등 보안 상태에 따라 모바일 디바이스에 정책 적용	-	-	●	●
	보안 수준이 낮은 경우 장치를 보완하도록 사용자에게 통지	-	-	●	●
	Landesk나 JAMF, Microsoft Intune 등 엔드포인트 관리 시스템에 등록 상황에 따라 디바이스의 애플리케이션 접근을 제한	-	-	-	●
	AirWatch 및 MobileIron, Microsoft Intune 등 모바일 디바이스 관리(MDM)의 등록 상황을 기반으로 모바일 디바이스의 애플리케이션 접근을 제한	-	-	-	●
	무제한 애플리케이션 등록	●	●	●	●
싱글 사인온(SSO)과 원격 접속	모든 클라우드 애플리케이션에 대해 SSO 제공	-	●	●	●
	사내 웹 애플리케이션에 안전하게 액세스(Duo Network Gateway)	-	-	-	●
	SSH를 통해 특정 사내 서버에 안전하게 액세스(Duo Network Gateway)	-	-	-	●
	AWS, Azure, GCP에 호스팅 된 애플리케이션에 보안 액세스(Duo Network Gateway)	-	-	-	●

