



ENTRUST



Entrust Identity as a Service

모든 사용자 보호. 클라우드의 무한한 가능성.

특징

클라우드 ID 및 액세스 관리(IAM)

Entrust Identity as a Service(IDaaS)는 신뢰할 수 있는 ID 관리로 직원, 소비자, 시민의 안전하고 원활한 활동을 지원합니다. 인텔리전트 IAM 플랫폼으로 언제 어디서나 정확한 리소스에 대한 사용자 인증, 권한 부여, 액세스 제어를 제공하는 Zero Trust 전략을 구현하세요.

93%

Entrust Identity를 추천할 의향이 있다고 응답한 고객

91%

Entrust Identity의 사후 지원 서비스가 유용하다고 평가한 고객

TechValidate, 고객 설문 조사, 2020

모든 IAM 니즈를 충족하는 단일 플랫폼



사용자



기기



Identity as a Service

- 인증 및 권한 부여
- 액세스 관리
- ID 프로비저닝
- ID 수명 주기 관리
- 위협 탐지 및 지속적인 모니터링





Entrust Identity as a Service

핵심 기능



업계 최고 수준의 다중 인증(MFA)

타의 추종을 불허하는 규모의 인증자 및 사용 사례 지원.



고도의 보안 자격증명 기반 액세스

모바일 앱 또는 하드 토큰/USB 키로 보안을 높이는 디지털 인증서 사용 옵션.



싱글 사인 온(SSO)

모든 앱(클라우드 또는 온프레미스)에 안전하게 액세스하는 동시에 IT 팀이 사용자 자격증명을 안전하게 관리하도록 지원하는 자격증명 세트. Entrust Identity as a Service는 SAML 및 OIDC와 같은 표준을 통해 클라우드 앱에 연동.



패스워드리스 액세스

고도 보안 인력 사용 사례를 위한 SSO로 자격증명 기반/FIDO 호환 패스워드리스 액세스. 소비자용 패스워드리스 옵션은 BYOD와 함께 스마트폰 생체 인식 또는 FIDO 토큰 사용 포함.



ID 오케스트레이션

IDaaS 및 소셜 로그인 등 타사 ID 공급자(IDP)를 통한 사용자 등록 통합으로 여러 IDP에서 인증 및 권한 부여 간소화. (하이브리드/멀티 클라우드 환경에서 특히 중요)



권한 부여 및 액세스 관리

기본 제공되는 RBAC(Role-based Access Control)를 활용해, 사용자 권한을 개별적으로 설정 및 관리하는 대신 개인의 역할에 맞는 권한 적용. 디렉토리 그룹(AD 또는 모든 LDAP 소스)을 역할에 쉽게 매핑해, 권한 있는 클라우드 애플리케이션에 대한 보안 액세스 보장.



URL/API 보호

OAuth 2.0/2.1 컨텍스트 권한 부여와 액세스 제어 및 통합 OIDC 기반 사용자 인증으로 디지털 에코시스템 보안.



임베디드 디바이스 앱 인증 및 권한 부여

입력이 제한된 기기에 IDaaS의 기기 권한 부여 절차를 적용해 인증 및 권한 부여 간편화.



Entrust Identity as a Service

핵심 기능



적응형 위험 기반 액세스 및 인증

새 기기에서 처음 로그인하거나 이례적인 시간에 또는 지리적 위치에서 로그인하는 사용자와 같이, 조건을 충족하는 경우 강화된 인증 절차로 상황에 맞는 인증 적용.



이메일 및 파일 암호화, 문서 서명

Microsoft, IBM, MobileIron, VMware 등 EMM(Enterprise Mobility Management) 벤더 통합으로 이메일 암호화, 파일 암호화, 문서 서명을 통해 안전한 업무 소통 지원.



신분 증명

소비자, 시민 또는 직원의 빠르고 안전한 원격 온보딩을 위한 셀프 서비스 디지털 신원 확인을 지원하는 통합 옵션.



부정 사용 탐지 및 예방

자격증명 도용 공격, 사칭 공격, 컴퓨터/세션 탈취 공격으로부터 소비자를 보호하면서 사용자 행동 및 환경 이상을 비침입적으로 탐지.



보안 포털

소비자 및 파트너 포털에 대한 보안 액세스 보장.



셀프 서비스 암호 재설정

사용자가 자신의 암호를 안전하게 재설정하도록 지원해 다운타임 및 IT 오버헤드 제거.



OTS(Off-the-shelf) 통합, API 및 개발자 툴킷

SAML 및 OIDC 기능을 통한 ID 연동, RESTful API 및 포괄적 범위의 통합. 모바일 SDK를 사용해, 필요한 경우 디지털 ID를 애플리케이션 및 브랜드에 직접 임베드. Entrust 모바일 스마트 자격증명(MSC) SDK를 사용해 패스워드리스 문서 서명 애플리케이션 개발.



관리형 서비스로 사용 가능

IDaaS를 직접 클라우드에 배포하거나, 인증된 관리형 서비스 공급자(MSP) 파트너와 협력해 관리형 서비스로 배포하는 옵션 선택.



Entrust Identity as a Service

혜택

Zero Trust 구현

ID 보안을 유지하고 적응형 위험 기반 인증을 적용하며 URL/API를 보호합니다.

IT 부담 완화

사용자 프로비저닝과 ID 관리 업무를 간소화하며, 사용자 셀프 서비스 도구를 간편하게 활용할 수 있습니다. IDaaS를 직접 배포하거나 관리형 서비스로 배포하는 옵션을 제공합니다.

사용자 경험 개선

적응형 위험 기반 인증, 패스워드리스 로그인, ID 증명 및 클라우드 앱 연동으로 사용자의 불편을 최소화합니다.

규제 준수 지원

사용자 ID 및 데이터 프라이버시를 보호합니다.

간편한 배포, 관리 및 확장

사용 가능한 API, OTS 통합 및 SDK를 활용합니다.

미래 경쟁력 확보

적응형 위험 기반 MFA, 고보안 패스워드리스 액세스, ID 오케스트레이션, 액세스 관리 제어 등의 기능을 통해 IDaaS는 하나의 플랫폼에서 기존 및 미래의 모든 사용 사례에 대한 포괄적인 보안을 제공합니다.

민감한 의료 정보 보안, 금융 사기 방지, 정부 서비스에 대한 보안 액세스가 필요하신가요?

Entrust IAM 플랫폼이 지원합니다.

[지금 무료로 시작하세요.](#)

ENTRUST CORPORATION 소개

Entrust는 신뢰할 수 있는 신원 인증과 결제 및 데이터 보안으로 급변하는 디지털 세상의 안전을 유지합니다. 국경 간 이동과 구매 활동, 전자정부 서비스 접속, 회사 네트워크 로그인까지, 오늘날 원활하고 안전한 경험에 대한 요구는 그 어느 때보다 높아졌습니다. Entrust는 이러한 모든 상호 작용의 중심에서 탁월한 범용성을 갖춘 디지털 보안 및 자격증명 발급 솔루션을 제공하며, 150개 이상의 국가에서 2,500명 이상의 직원과 글로벌 파트너 네트워크 및 고객을 보유하고 있습니다. 전 세계 가장 신뢰받는 여러 기관이 Entrust를 신뢰하는 것은 당연한 결과입니다.

자세한 정보:
[entrust.com/ko](https://www.entrust.com/ko)



대한민국 서울특별시 강남구 삼성동 159-1
KWTC 트레이드타워 2503호 135-729
전화: 02-2088-4691
HSMInfo@entrust.com