Entrust Identity for Workforce

Eine sicherere und produktivere Arbeitnehmerschaft

- Essentials
- Enterprise
- As a Service

ENTRUST

SECURING A WORLD IN MOTION

ÜBERBLICK

Eine moderne IAM-Plattform

Die verteilten Belegschaften von heute müssen in der Lage sein, überall mit sicherem Zugriff auf jede Anwendung - ob Cloud oder vor Ort - von jedem Gerät aus zu arbeiten. Im Gegensatz zu älteren Identitäts- und Zugriffsmanagement-Lösungen (IAM), die von einem veralteten Sicherheitsperipheriekonzept ausgehen, verfolgt Entrust Identity einen modernen, identitätszentrierten Zero Trust-Ansatz für eine sicherere und produktivere Belegschaft.

DIE GELEGENHEIT

Eine umfassende Belegschaftslösung

Entrust Identity deckt das Spektrum der IAM-Lösungen für Arbeitskräfte ab, darunter

- Beste Multi-Faktor-Authentifizierung (MFA) ihrer Klasse und bester VPN-Schutz für Windows-basierte Umgebungen mit Identity Essentials
- Hochsichere, auf Berechtigungsnachweisen basierende passwortlose Authentifizierung vor Ort mit Identity Enterprise
- Hochsichere, auf Berechtigungsnachweisen basierende passwortlose Authentifizierung mit Single Sign-On (SSO) in der Cloud mit Identity as a Service

Darüber hinaus bietet Entrust Identity IAM-Lösungen für die Belegschaft an, um eine Reihe von Unternehmensgrößen zu unterstützen, von KMUs mit 50 Benutzern bis hin zu großen Unternehmen mit mehr als einer Million Benutzern.

Entrust Identity for Workforce IAM

	Kernanwendungsfälle	Bereitstellungsoptionen
Identity Essentials	Klassenbeste MFA für Windows-basierte Organisationen; Fernzugriffsschutz (VPN-Clients, Cloud-Anwendungen usw.)	Lokal
Identity Enterprise	Hochsichere Authentifizierung durch Berechtigungsnachweise; physische Chipkartenausgabe; passwortloser Zugang	Lokal, virtuelle Anwendung
Identity as a Service	Hochsichere Authentifizierung durch Berechtigungsnachweise; SSO; passwortloser Zugang und SSO	Cloud

Entrust Identity unterstützt eine beispiellose Anzahl von Anwendungsfällen und Bereitstellungsoptionen für Mitarbeiter:

- Hochsicherer, auf Berechtigungsnachweisen basierender Zugang für Belegschaften in Unternehmen und Behörden
- Single Sign-On (SSO) mit Cloud-Bereitstellungsmodell
- Hochsicherer, auf Berechtigungsnachweisen basierender/FIDO-kompatibler passwortloser Zugriff mit SSO
- Klassenbeste Multi-Faktor-Authentifizierung (MFA), die eine breite Palette von Anwendungsfällen und Authentifikatoren unterstützt, einschließlich Soft-Token, Hard-Token, Mobile, Grid-Karte, SMS, Push und OTP
- Adaptiver risikobasierter Zugriff und Authentifizierung mit engmaschiger Kontrolle
- Identitätsprüfung und Workflow-Orchestrierung
- Passwortrücksetzung per Self-Service
- Analyse der Gerätereputation
- E-Mail-Signatur und -Verschlüsselung, Dateiverschlüsselung und Dokumentensignatur
- Entwicklungskit für mobile Software (SDK)
- Verfügbare Out-of-the-box-Integrationen, SAML/OIDC- und REST-APIs für Verwaltung und Authentifizierung
- Flexible Bereitstellungsoptionen: Cloud, verwalteter Dienst, vor Ort, virtuelle Anwendung

FUNKTIONSWEISE

Anwendungsfälle in der Belegschaft

Berechtigungsnachweisbasierter Zugriff mit hoher Sicherheit

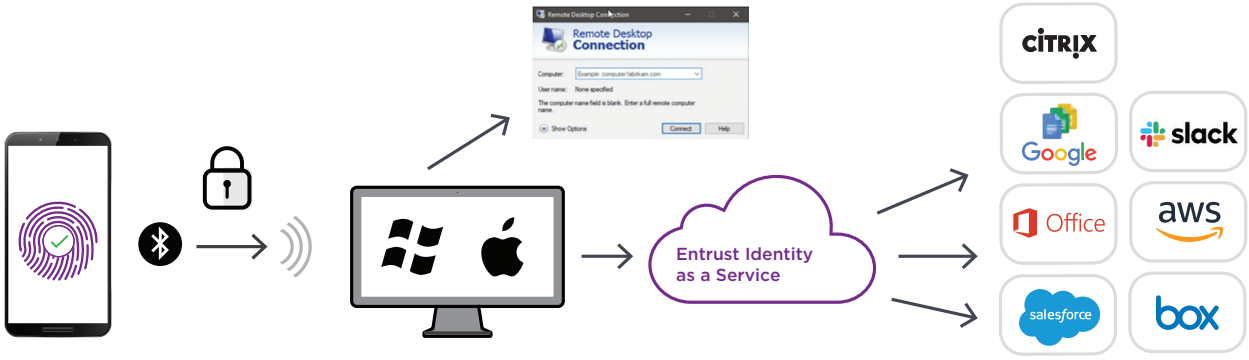
Entrust Identity bietet die Möglichkeit, digitale Zertifikate (PKI) für ein höheres Maß an Sicherheit zu verwenden, wenn und wo dies gerechtfertigt ist. Dies kann entweder eine physische Chipkarte oder eine virtuelle Chipkarte sein, die auf einem iOS- oder Android-Gerät bereitgestellt wird. Die letztere Implementierung wird als Mobile Smart Credential (MSC) bezeichnet.

Single Sign-On (SSO)

Veraltete Verbands- und Zugriffsverwaltungssysteme sind ungeeignet für die Kontrolle des Benutzerzugriffs in hybriden Cloud-/On-Premises-Umgebungen, ohne dass eine Vielzahl manueller Bereitstellungen ein Sicherheitsrisiko darstellen. Außerdem versäumen es die Benutzer oft, mehrere URLs und Anmeldeinformationen im Auge zu behalten, was zu schlechten Gewohnheiten wie der Wiederverwendung und dem Recycling von Passwörtern führt, die das Sicherheitsrisiko weiter erhöhen. Single Sign-On (SSO) löst diese Herausforderungen, indem den Mitarbeitern mehrere Berechtigungsnachweise für den sicheren Zugriff auf jede beliebige Anwendung (Cloud oder vor Ort) zur Verfügung gestellt werden und gleichzeitig den IT-Teams die sichere Verwaltung von Benutzeranmeldeinformationen erleichtert wird. Entrust Identity as a Service verbündet sich mit Cloud-Anwendungen über Standards wie SAML und OIDC.

Berechtigungsnachweisbasierter/FIDO-konformer passwortloser Zugriff mit SSO

Die wohl größte einzelne Schwachstelle, mit der IT-Abteilungen heute konfrontiert sind, ist das Mitarbeiterpasswort. Der auf Berechtigungsnachweisen basierende passwortlose Zugriff stellt ein digitales Zertifikat (MSC) auf dem Telefon des Arbeitnehmers bereit, wodurch dieses in seine vertrauenswürdige Arbeitsplatzidentität verwandelt wird. Wenn das Telefon über biometrische Daten oder eine sichere PIN entsperrt wird, wird der Mitarbeiter in seiner Arbeitsstation und seinen Anwendungen angemeldet, wenn er sich in der Nähe befindet, und abgemeldet, wenn er sich nicht in der Nähe befindet. Eine sichere, reibungslose Erfahrung für alle, und es müssen keine Passwörter mehr zurückgesetzt werden.



1. Biometrische Daten mit mobilem Gerät zur Anmeldung verwenden
2. Nutzung bestehender Kunden/PKI/On demand Entrust PKI
3. Single Sign-On für alle Anwendungen ohne erneute Authentifizierung

Vorteile

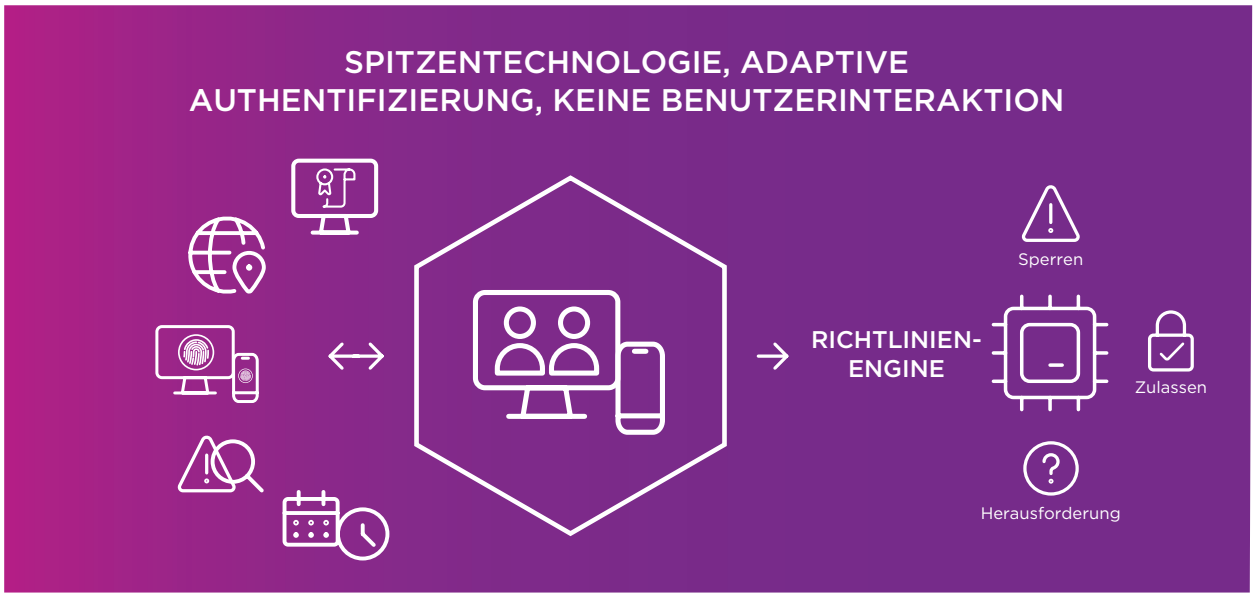
- Vereinfachte Bereitstellung
- PKI-basiert – Hohe Sicherheit
- Benutzerfreundlichkeit – biometriebasiert
- E-Mail-Signierung und -Verschlüsselung

Multi-Faktor-Authentifizierung (MFA)

Entrust Identity bietet hochverfügbare und großflächig einsetzbare MFA mit Unterstützung für eine unübertroffene Anzahl von Authentifikatoren, einschließlich FIDO-Token, Mobile Push und Grid-Karten. Außerdem nutzt Entrust Identity biometrische Authentifikatoren für Smartphones, einschließlich Fingerabdruck- und Gesichtserkennung, und bietet eine eingebaute weiche Gesichtserkennung, falls das Smartphone nicht über native biometrische Fähigkeiten verfügt.

Adaptiver risikobasierter Zugriff und Authentifizierung

Die adaptive, risikobasierte Engine von Entrust Identity bietet ein zusätzliches Maß an Sicherheit, wenn die Bedingungen dies rechtfertigen, wie z. B. wenn sich ein Mitarbeiter zum ersten Mal von einem neuen Gerät, zu einer ungewöhnlichen Tageszeit oder von einem anderen geografischen Standort aus anmeldet. Das Erfordernis einer zusätzlichen Authentifizierung wie z. B. einer mobilen Push-Benachrichtigung nur für diese Situationen minimiert die Reibung zwischen den Mitarbeitern und schützt gleichzeitig die Unternehmensressourcen.



Identitätsprüfung und Workflow-Orchestrierung

In dem Maße, in dem sich immer mehr Belegschaften verteilt und in einer gewissen Entfernung befinden, nimmt die Notwendigkeit zu, die Identitäten von Mitarbeitern, Auftragnehmern und Partnern aus der Ferne zu überprüfen. Unsere Identity Proofing-Lösung bietet eine vollständig digitale Identitätsprüfung für Ihre Mitarbeiter. Der Arbeitnehmer erstellt ein hochauflösendes Bild von seinem behördlich ausgestellten Ausweis, das forensisch getestet und anhand einer globalen Datenbank mit mehr als 6000 verschiedenen behördlichen Ausweistypen authentifiziert wird, und bestätigt mit einem Selfie, dass er mit dem Ausweisinhaber identisch ist. Durch die Lebendigkeitserkennung wird sichergestellt, dass das Selfie echt ist und nicht ein Foto von einem Foto. Nach der Authentifizierung kann der Mitarbeiter an Bord genommen werden und Zugang zu den entsprechenden Ressourcen mit vollständiger Workflow-Orchestrierung erhalten.

Passwortrücksetzung per Self-Service

Das Zurücksetzen von Passwörtern ist sowohl für IT-Helpdesks als auch für Benutzer ein Ärgernis, ganz zu schweigen von den Kosten der Produktivitätsverluste für beide Gruppen. Entrust Identity bietet den Benutzern die Möglichkeit, ihre eigenen Passwörter sicher zurückzusetzen, d. h. keine Ausfallzeiten und kein IT-Aufwand. Besser noch, arbeiten Sie ganz ohne Kennwörter.

Analyse der Gerätereputation

Um die Kompromittierung gültiger Berechtigungsnachweise zu verhindern, wird empfohlen, zunächst die Reputation des Geräts zu prüfen, das für den Zugriff auf Unternehmensressourcen verwendet wird, insbesondere in BYOD-Situationen. Entrust Identity bietet diese Option mit Zugang zu einer Datenbank von über 6,5 Milliarden Geräten, die mit dem Internet verbunden sind, um sich dadurch eine gute Reputation zu verschaffen. Zu den Überprüfungen gehören auch die Feststellung, ob das Gerät einen TOR-basierten Browser oder Proxy verwendet, ob es sich um ein gehacktes oder gerootetes Gerät handelt oder ob es für Debit- oder Kreditkartenbetrug verwendet wurde, sowie Kontoeröffnung und Zugriffsgeschwindigkeit. Die Gerätereputation ist im Identitätsnachweis enthalten.

E-Mail- und Dateiverschlüsselung, Dokumentensignatur

Durch die Integration mit den wichtigsten MDM-Anbietern, einschließlich Microsoft, IBM und VMware, stellt Entrust Identity sicher, dass die Kommunikation am Arbeitsplatz durch E-Mail- und Dateiverschlüsselung sicher ist. Die MDM-Anbieterintegration unterstützt sichere Transaktionen am Arbeitsplatz mit E-Mail-Verschlüsselung, Dateiverschlüsselung und Dokumentensignatur.

Mobile SDK und verfügbare Integrationen

Entrust Identity bietet ein mobiles SDK, so dass Sie IAM direkt in Ihre Personalanwendungen einbetten und auf Wunsch als eigene Marke verwenden können. Das Portfolio bietet bewährte, sofort einsatzbereite Integrationen, darunter mit allen wichtigen VPN-Anbietern, SAML/OIDC und APIs. Entrust Identity arbeitet auch mit Ihrer bestehenden Microsoft-Umgebung zusammen, einschließlich Active Directory (AD), Active Directory Federation Server (ADFS), Azure AD für die Benutzersynchronisation und ActiveSync Device Provisioning, um nicht autorisierte Geräte vor dem Zugriff auf die E-Mails der Benutzer zu schützen. Für berechtigungsnachweisbasierte Anwendungsfälle ist Entrust Identity in der Lage, von Microsofts CA ausgestellte Zertifikate zu nutzen.

Entrust Identity Solution Matrix for Workforce IAM

	Identity Essentials	Identity as a Service	Identity Enterprise
MFA	✓	✓	✓
SSO		✓	Über das Föderationsmodul (SAML)
Berechtigungsnachweis-basierter Zugriff mit hoher Sicherheit (Zertifikate)		✓	✓
Physische Chipkarten-Ausgabe			✓
Hochsicherer, auf Berechtigungsnachweisen basierender/FIDO-kompatibler passwortloser Zugriff mit SSO		✓	
Passwortloser Login		✓	✓
Adaptiver Zugang	Richtlinienbasiert	Risikobasiert	Risikobasiert
Identitätsüberprüfung		✓	✓
Passwortrücksetzung per Self-Service	✓	✓	✓
Geräteреputation		✓	✓
E-Mail- und Dateiverschlüsselung		✓	✓
Dokumentunterzeichnung		✓	✓
ADFS	✓	✓	✓
Azure AD-Integration		✓	
ActiveSync-Geräteschutz	✓	✓	
Anforderungen an die IT-Plattform	Windows	Nicht zutreffend	Windows/Linux
Mobiles SDK	✓	✓	✓
Anzahl der Benutzer	< 5000	Unbegrenzt	> 5000
Bereitstellung	Lokal	Cloud	Lokal

Flexibler Einsatz, breite Fähigkeiten

Entrust Identity kann in der Cloud, vor Ort oder als virtuelle Anwendung bereitgestellt werden. Außerdem arbeitet Entrust mit Managed Service Providern zusammen, um Entrust Identity als Managed Service anzubieten.

Entrust Identity:

- Ergänzt Ihre bestehenden IT-Infrastrukturen und Arbeitsabläufe statt sie ersetzen zu wollen
- Bietet die breiteste Unterstützung von VPN-, Cloud- und lokalen Anwendungen
- Bietet die Option für zertifikatsbasierte Authentifizierung, die auch die einzige wirklich sichere passwortlose Lösung der Branche unterstützt
- Bietet eine mobile Plattform mit einer modernen, vereinheitlichten Anwendung, die im gesamten Portfolio funktioniert
- Bietet sofort einsatzbereite Integrationen, SAML/OIDC und APIs
- Enthält ein mobiles Entwicklungskit, damit Sie die Authentifizierung direkt in Ihre eigenen Anwendungen einbetten und nach Wunsch als eigene Marke verwenden können
- Bietet Zugriff auf das größte MDM-Ökosystem der Branche, einschließlich Microsoft Intune, MobileIron, Citrix und VMware AirWatch
- Gewährleistet eine einfache IT-Implementierung und einen effizienten Betrieb mit Point-and-Click-Bereitstellung und Richtlinienverwaltung sowie Self-Service-Passwortrücksetzungen

Mobile-first-Ansatz

Entrust Identity wendet einen einzigartigen Ansatz für mobile Geräte an, mit einem Schichtenmodell, um zunächst Vertrauen in das Gerät und den Benutzer aufzubauen, bevor der Zugriff freigegeben wird. Anschließend wendet sie eine adaptive Step-up-Authentifizierung an, um sicherzustellen, dass dieses Vertrauen über die Zeit erhalten bleibt.

UNSER LÖSUNG

Entrust Identity-Portfolio

Entrust Identity ist das IAM-Portfolio, das Ihnen die Flexibilität und Skalierbarkeit bietet, die Sie benötigen, um den sich ständig weiterentwickelnden Bedrohungen voraus zu sein und ein Zero Trust Framework zu realisieren. Über das IAM für Mitarbeiter hinaus unterstützt Entrust Identity auch Anwendungsfälle für Verbraucher und Bürger.

DER UNTERSCHIED VON ENTRUST

Ein führender IAM-Anbieter

Mit mehr als 25 Jahren Erfahrung im Bereich der digitalen Identität und mehr als 50 Jahren Innovation im Bereich der Sicherheit ist Entrust ein führendes Unternehmen im Bereich Identitäts- und Zugangsmanagement. Unsere High-Assurance-Lösungen haben sich bei Fortune-500-Unternehmen und Regierungen bewährt und werden von mehr als 10.000-Kunden auf der ganzen Welt eingesetzt. Entrust Identity sichert digitale Identitäten und Unternehmenswerte und verbessert gleichzeitig die Produktivität der Belegschaft und beseitigt Reibungsverluste für Verbraucher und Bürger.

Weitere Informationen erhalten Sie unter

www.entrust.com/de

ÜBER ENTRUST CORPORATION

Entrust widmet sich der Sicherung einer sich ständig verändernden Welt, indem es vertrauenswürdige Identitäten, Zahlungen und Datenschutz ermöglicht. Mehr denn je verlangen die Menschen heute nahtlose und sichere Erfahrungen, sei es beim Grenzübertritt, beim Einkaufen, beim Zugriff auf elektronische Behördendienste oder beim Einloggen in Unternehmensnetzwerke. Entrust bietet eine unübertroffene Bandbreite an Lösungen für digitale Sicherheit und die Ausstellung von Berechtigungsnachweisen, die das Herzstück all dieser Interaktionen bilden. Mit mehr als 2.500 Mitarbeitern, einem Netzwerk globaler Partner und Kunden in über 150 Ländern erstaunt es nicht, dass weltweit die Organisationen, denen großes Vertrauen entgegengebracht wird, zu unseren Kunden zählen.

Weitere Informationen unter
entrust.com

Entrust und IntelliTrust sind Marken, eingetragene Marken und/oder Dienstleistungsmarken der Entrust Corporation in den USA und/oder anderen Ländern. ©2016-2020 Entrust Corporation. Alle Rechte vorbehalten. IA21Q2-Entrust-Identität-Belegschaft-BR

ENTRUST

USA Gebührenfreies Telefon: 888 690 2424
Internationales Telefon: +1 952 933 1223
info@entrust.com