ENTRUST
SECURING A WORLD IN MOTION

ebook

Entrust Identity as a Service

Cloud-basierte Plattform für die intelligente Identitäts- und Zugriffsverwaltung (IAM)

Die digitale Wirtschaft erfordert eine moderne Identitätsstrategie

> Für das digitale Business von heute reichen traditionelle IAM-Ansätze nicht mehr aus, da sie nicht in der Lage sind 1) Kunden ohne Beeinträchtigung von Abläufen zu authentifizieren, 2) den Bedarf von Mitarbeitern nach einem sicheren Zugriff auf eine Vielzahl von Anwendungen und Daten zu erfüllen, 3) die schnelle Einführung von Cloud-Diensten zu unterstützen, 4) eine sichere, gesetzeskonforme und kosteneffiziente Datenintegration über mehrere Benutzergruppen hinweg zu gewährleisten.

— Evolve Your IAM Strategy For Your Digital Business
Merritt Maxim & Andras Cser, Forrester
4. Dezember 2020

Inhaltsverzeichnis

EINE IDENTITÄTSPLATTFORM, DIE AUTHENTIFIZIERUNG NEU DEFINIERT

Unternehmen agieren heute dynamisch und entwickeln sich laufend weiter.

Außerdem führt die Einführung mobiler und Cloud-Anwendungen zu einem Paradigmenwechsel.

Parallel dazu ändern sich auch die Anforderungen an die Authentifizierung. Passwörter und andere traditionelle Authentifizierungsmethoden reichen nicht mehr aus. Im Zuge der digitalen Transformation benötigen Unternehmen Authentifizierungslösungen, die sich nahtlos in eine moderne Arbeitsumgebung und die Bedürfnisse ihrer Nutzer fügen – und gleichzeitig eine Grundlage für künftige Anforderungen und Wachstum bilden.

« Ein moderner Ansatz in Bezug auf digitale Identitäten schützt sensible Anwendungen und Daten, vereinheitlicht die Nutzung über verschiedene Kanäle, Bevölkerungsgruppen und Hosting-Modelle hinweg und ist skalierbar, um den dynamischen Geschäftsanforderungen von heute gerecht zu werden. »

Evolve: Your IAM Strategy For Your Digital Business.
Merritt Maxim & Andras Cser, Forrester. 4. Dezember 2020

Anwendungsszenarien

VPN-Zugang

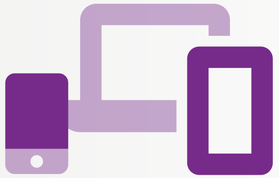
Optimieren Sie den Fernzugriff

Mitarbeiter, die das Geschäft voranbringen, müssen von überall aus ihre Aufgaben erledigen können. Die hierfür verwendeten Geräte und Systeme sollten zu deren Lösung beitragen und dürfen keinesfalls selbst zum Problem werden. Sollte letzteres der Fall sein, ist es ein Problem für alle – für Mitarbeiter, Kunden und das Unternehmen.

Realisieren Sie die Chancen von VPN-Zugängen

- Passen Sie Sicherheitsanforderungen genau an jede Benutzergruppe an
- Ermöglichen Sie kontextabhängige und verhaltensadaptive Authentifizierung
- Vereinfachen Sie die Bereitstellung und Implementierung
- Minimieren Sie Ihre Infrastrukturkosten

Ein sicherer und unkomplizierter VPN-Zugriff ist heute absolut notwendig



Mitarbeiter verwenden im Durchschnitt **JEDEN TAG 3 GERÄTE,** um ihre Arbeit zu erledigen[1]

Das Wichtigste in Kürze

Überall und jederzeit arbeiten mit sicherem und einfachem VPN-Zugang.

1. Citrix Mobilitätsstatistik, 2015

VPN-Zugang

Die Herausforderung

Remote-Mitarbeiter müssen schnell, sicher und nahtlos auf Anwendungen zugreifen können. In einer schnellen Welt voller Wettbewerber stellen Beeinträchtigungen aufgrund komplexer Authentifizierung einen Schaden für Unternehmen dar.

Zeitaufwändige Hardtoken, leicht zu vergessende Passwörter – das Einloggen in VPNs stellt für Mitarbeiter oftmals ein lästiges Hindernis dar.

Die manuelle Eingabe von Passwörtern, Zeichen für Zeichen, passt nicht mehr ins mobile Zeitalter - es bremst Ihr Team aus, bevor es überhaupt ins Rennen gehen kann.

Die Lösung

Mobile Push-Authentifizierung sorgt dafür, dass die Assets des Unternehmens in die Hände derer gelangen, die es vorantreiben. Mit nur einem Tastendruck können sich Mitarbeiter schnell und mühelos in ihrem VPN anmelden – die Zeiten der Frustration sind vorbei.

Alternativ dazu baut der Mehrwert der mobilen Push-Authentifizierung mit Smart Credentials auf der Public-Key-Infrastruktur auf, da der private Schlüssel das zugehörige Gerät nie verlässt. Diese Art der Authentifizierung bietet nicht nur Vorteile für den physischen Zugang und die Anmeldung via Smartcard, sondern ermöglicht zugleich die Konformität mit einer Vielzahl regulierter Märkte.

Vor allem aber gewährleisten mobile Smart Credentials den Schutz und die Sicherheit von Unternehmen. Eine transparente Zwei-Faktor-Authentifizierung stellt sicher, dass das Netzwerk der Person vertrauen kann, die versucht, darauf zuzugreifen.

ENTRUST IDENTITY AS A SERVICE FÜR DEN VPN-ZUGANG

- Mobile Smart Credentials
- Adaptive Authentifizierung
- Mobile Push
- Biometrie
- Gesichtserkennung
- Skalierung nach Bedarf
- Bewährte Integrationen für alle wichtigen VPN-Lösungen

Mobile Sicherheit

Vertrauenswürdige mobile Transaktionen

Die zunehmende Mobilität erfordert die Umgestaltung von Unternehmen. Mitarbeiter haben sich daran gewöhnt, dass ihr Arbeits- und Lebensalltag von mobilen Geräten geprägt ist und genießen den damit verbundenen Komfort. Gehen Sie einen Schritt weiter und nutzen Sie die mobilen Geräte als vertrauenswürdige Identität für den Zugang zur Arbeitsumgebung – wo auch immer diese sein mag. Ihre Mitarbeiter freuen sich über die Option, ohne Passwort sicheren Zugriff auf Unternehmensressourcen zu erhalten.

Die neue Mobilität ist ein Geschenk für Unternehmen. In nur wenigen Jahren haben mobile Geräte die Produktivität auf ein Niveau gehoben, das vor nicht allzu langer Zeit noch unvorstellbar war. Aber kein Fortschritt ohne Risiko. Und die Verwaltung dieses Risikos ist eine tägliche Herausforderung für alle IT-Abteilungen.

Werden Sie mobil

- Ohne Passwörter
- Völlige Transparenz für den Benutzer
- Steigerung der Mitarbeiterproduktivität
- Höchste Sicherheitsstufe
- Effizienter Zugriff auf digitale Ressourcen
- Einheitliche Plattform-Erfahrung

Das Wichtigste in Kürze

Reibungslose Nutzererfahrung mit einem Höchstmaß an Sicherheit zur Steigerung der Produktivität.

MEHR ERFAHREN

2. IDC Mobile Worker Forecast, 2015
3. Gartner Return to the Workplace Benchmarking Against Your Peers Webinar Poll, 2020

Die Mobilität verändert Unternehmen

jährlicher Zuwachs an verwalteten Geräten[2]

der Führungskräfte glauben, dass ein erheblicher Teil der Belegschaft dauerhaft remote arbeiten wird[3]

Mobile Sicherheit

Die Herausforderung

Mitarbeiter sind an verschiedenen Standorten oder im Außendienst tätig und verlangen den gleichen Zugang zu den Anwendungen, den sie auch im Büro haben.

Mit der Allgegenwärtigkeit von Tablets und Smartphones und den damit einhergehenden enormen Vorteilen entsteht auch ein neues Sicherheitsparadigma.

Die Arbeitswelt mag sich vom Desktop auf das Mobiltelefon verlagert haben, aber wie lassen sich Unternehmen in einer digitalen Welt voller Sicherheits-herausforderungen schützen? Ein alternativer Token, wie der persönliche Identitätsnachweis (PIV), macht die Authentifizierung benutzerfreundlicher. Insbesondere in regulierten Umgebungen, in denen die PIV-Authentifizierung vorgeschrieben ist, sind Unternehmen gezwungen, eine auf virtuellen Smartcards basierende Lösung zu finden.

Die Lösung

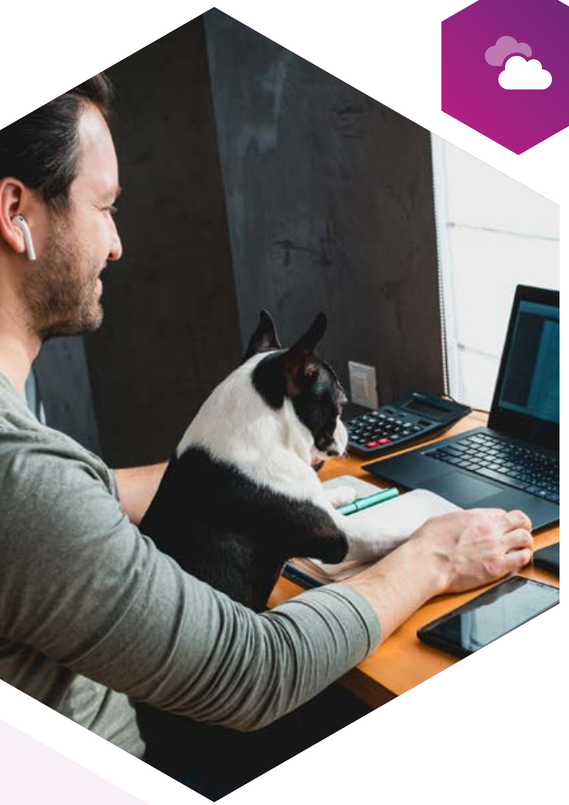
Unternehmen werden täglich mit Cyber-Attacken konfrontiert. Neben höchster Sicherheit ist aber auch eine nahtlose Nutzererfahrung für alle Mitarbeiter wettbewerbsentscheidend. Ein schwieriger Balanceakt.

Die Lösung besteht in einer vertrauenswürdigen digitalen Identität, die bei der Authentifizierung eine reibungslose Benutzererfahrung bietet. Eine virtuelle Smartcard, eingebettet in einem Gerät, ermöglicht einen nahtlosen und sicheren mobilen Zugang – für Benutzer unsichtbar und für IT-Mitarbeiter unverzichtbar.

Befreit von ehemals lästigen Authentifizierungs-prozessen, können Mitarbeiter schneller und effizienter agieren. Die erfolgreiche Verbindung von Benutzerfreundlichkeit und starker Sicherheit ist keine Theorie mehr – zu jeder Zeit und an jedem Ort.

ENTRUST IDENTITY FÜR MOBILE ENDGERÄTE

- Native Integration mit führenden EMM-An-wendungen
- Adaptive Authentifizierung
- Mobile as a Service Smart Credential
- Software-Entwickler-Kits (SDKs) zur Einbettung von Identitäten in eine mobile Plattform
- Mobile Vorabprüfung
- Mobiler Push



Cloud SSO

Nahtloser Zugriff auf alle Anwendungen

Cloud-Lösungen wie Microsoft Office 365, Salesforce und Box haben traditionelle Geschäftspraktiken auf ein neues Level gehoben und die Erwartungen von Anwendern verändert.

Mit der schnellen Einführung der Cloud wird es notwendig, die Anmeldedaten für jede einzelne Cloud-Anwendung zu entkoppeln, damit Unternehmen singuläre, starke Credentials verwenden können. So wird der Benutzerzugriff einfacher, da dieselben Anmeldedaten zum Beispiel für interne Anwendungen, VPN und Workstations verwendet werden können. Außerdem lassen sich so Authentifizierungsrichtlinien kontrollieren, anstatt sich auf die Maßnahmen einzelner Software-as-a-Service-Anbieter verlassen zu müssen.

Mehr Leistung für Cloud SSOs

- Eine Identität für den Zugriff auf lokale und Cloud-Anwendungen
- Verbessertes Benutzererlebnis mit transparenter Sicherheit und breitem Enablement
- Maßgeschneiderte Benutzererlebnisse
- Weniger Anrufe beim IT-Helpdesk

Das Wichtigste in Kürze

Jederzeit und überall mit einem sicheren und vereinfachten VPN-Zugang arbeiten.

Die Cloud ist ein Muss

2020

Ohne Cloud-Anwendungen, -Tools und -Dienste hätten wir nicht innerhalb weniger Wochen Millionen von Arbeitnehmern nach Hause schicken, globale Lieferketten aufrechterhalten oder ganze Geschäftsmodelle umstellen können

NAHEZU

9 VON 10 CEOs

sehen eine Cloud-basierte Infrastruktur als Schlüssel zum Wachstum[4]

4. Forbes Insights 2016 Studie, “How to Win at Digital Transformation: Five Steps Digital Transformation Leaders are Taking”

Cloud SSO

Die Herausforderung

Wachsende Unternehmen benötigen Tools – und zwar viele. Tools, die es Anwendern ermöglichen, mehrere Anmeldeinformationen zu verwalten und gleichzeitig den Sicherheitsalbtraum zu vermeiden, dass Passwörter für jede Anwendung wiederverwendet werden.

Office 365, Salesforce und Google Docs sind nur einige zentrale Anwendungen, auf die Mitarbeiter digital agierender Unternehmen schnellen Zugriff benötigen. Im Bewusstsein permanenter Bedrohungen und Herausforderungen für die IT-Sicherheit werden daher unkomplizierte, hochsichere Methoden benötigt, deren Schutz weit über traditionelle Sicherheitsparameter hinaus reicht.

IT-Experten benötigen eine Sicherheitsplattform, die alle Tools des digitalen Business miteinbezieht. Eine schwierige Aufgabe in einem hart umkämpften Markt.

Die Lösung

Identity as a Service bedeutet, dass Sie sich nur einmal authentifizieren müssen, um sofortigen Zugriff auf alle Ihre geschäftskritischen Anwendungen zu erhalten.

SSO ermöglicht den Verzicht auf Passwörter, Token oder Karten – für ein sicheres, nahtloses Erlebnis. Und mit den Top-Level-Assurance-Funktionen, die von Regierungsbehörden und globalen Finanzorganisationen gefordert werden, genießen Sie einen sicheren Zugriff auf interne Unternehmensanwendungen, Webanwendungen, die Microsoft-Umgebung und alle anderen Web-Access-Management-Systeme. Dieselben Anmeldeinformationen können für den VPN- und Workstation-Zugang verwendet werden. Der Service lässt sich so konfigurieren, dass er in wenigen Minuten einsatzbereit ist.

ENTRUST IDENTITY AS A SERVICE FÜR CLOUD SSO

- Passwortloser Zugang
- Self Service für Anwender
- Adaptive risikobasierte Authentifizierung
- Fortschrittliche mobile Sicherheit
- Cloud- oder Legacy-Anwendungen
- Auf Standards (SAML) basierende Integration für Sicherheitsberichte in Echtzeit
- Effektives Provisioning mit Integration in Active Directory
- Konfiguration/Deployment in Minuten oder Stunden statt Wochen und Monaten

Passwortlose Anmeldung

Nahtloses, sicheres Ein- und Ausloggen

Aus Sicht der IT sind Passwörter notorisch unsicher. Für Anwender sind Passwörter lästig. Eine passwortlose Lösung kommt der Sicherheit und Ihren Mitarbeitern zugute. Daher bietet Entrust seit mehr als sieben Jahren passwortlose Lösungen an, einschließlich:

- PIV-Lösungen auf der Basis mobiler Geräte
- Proximity-Anmeldung am Arbeitsplatz
- Passwortlose SSO-Authentifizierung

Die Zukunft ist passwortlos

- Sicher
- Erhöhte Produktivität der Mitarbeiter
- Einheitlicher Zugang
- Einmalige Benutzerregistrierung
- Reduzierte TCO

Das Wichtigste in Kürze

Höchste Sicherheit für Ihr Unternehmen. Größtmögliche Einfachheit für Ihre Anwender.

WEITERE INFORMATIONEN IM VIDEO

5. Verizon Data Breach Investigations Report, 2020
6. Herjavec Group Official Annual Cybercrime Report, 2019

Unbefugter Zugriff gefährdet Unternehmen

der Hacking-Angriffe werden durch kompromittierte Anmeldedaten verursacht[5]

6 MILLIARDEN $/JAHR

Der weltweite Schaden durch Cyberkriminalität wird im Jahr 2021 voraussichtlich auf 6 Billionen Dollar ansteigen[6]

Passwortlose Anmeldung

Die Herausforderung

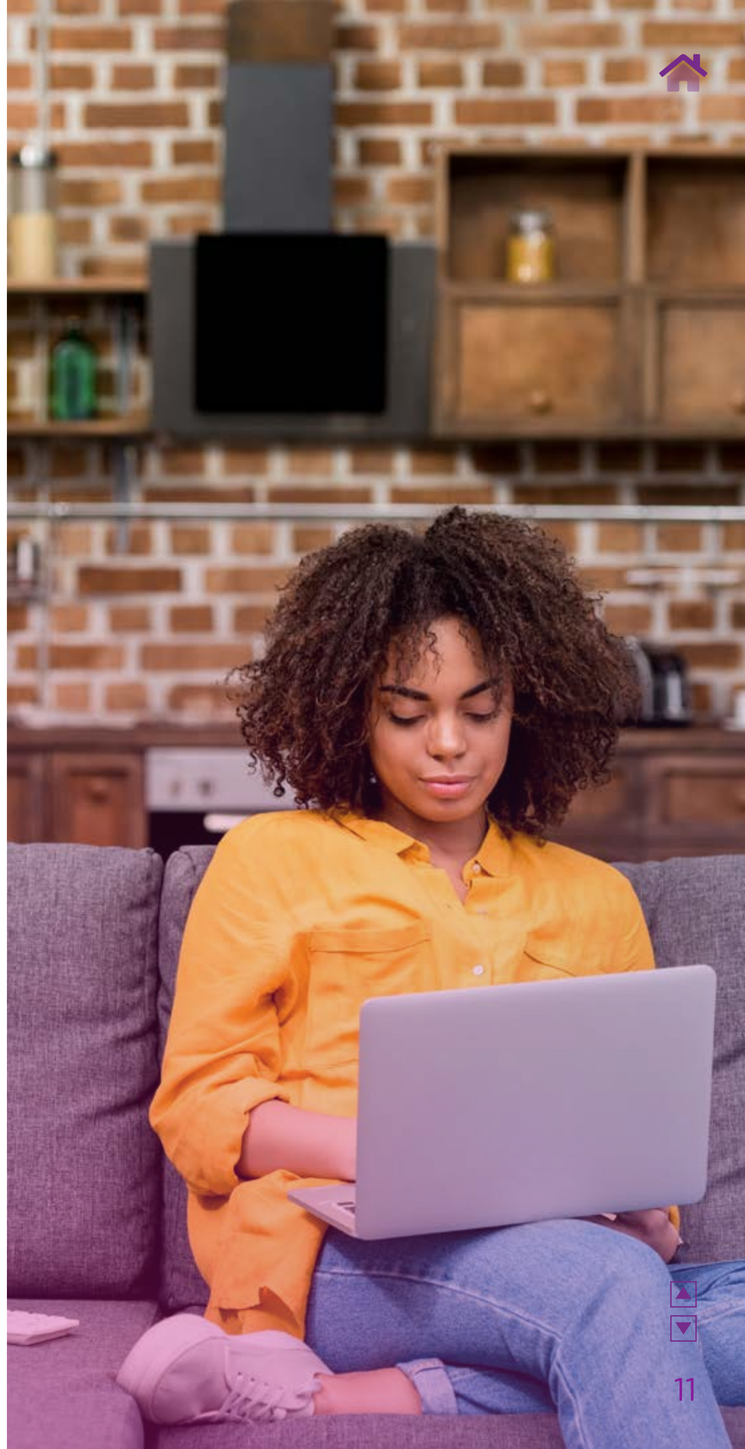
Verlorene, gestohlene und beschädigte Daten. Finanzieller Schaden. Beeinträchtigung der Produktivität, des geistigen Eigentums, Störung des Geschäftsbetriebs und der Reputation. Die Liste der Cyberkriminalität ließe sich beliebig fortsetzen. Unter den verschiedenen Angriffen sind 80 % auf das Hacking von Anmeldedaten zurückzuführen – in der Regel Passwörter.

Angesichts der alarmierenden Zunahme der Internet-kriminalität erhöhen Passwörter die Verwundbarkeit eines Unternehmens deutlich. Mitarbeiter nutzen durchschnittlich 36 Cloud-Dienste für ihre Arbeit, und der Zugriff auf diese Anwendungen erfordert eine Vielzahl an Passwörtern. Werden diese Passwörter kompromittiert, besteht die Gefahr von Datenverlust und unbefugtem Netzwerkzugriff.

Die Lösung

Bei unserem passwortlosen Ansatz wird mithilfe eines PKI-Berechtigungsnachweises eine sichere digitale Identität auf den Mobiltelefonen der Mitarbeiter erstellt. Diese werden dann mit biometrischer Authentifizierung entsperrt, z. B. durch Fingerabdruck oder Gesichts-erkennung. Auf diese Weise wird sichergestellt, dass der Halter auch tatsächlich der Besitzer des Berechtigungs-nachweises ist, die digitalen Identitäten der Mitarbeiter und die Vermögenswerte des Unternehmens werden geschützt. Diese hochsichere passwortlose Lösung schafft außerdem eine mühelose Nutzererfahrung – insbesondere in Kombination mit SSO für Cloud- und On-Premise-Anwendungen, einschließlich Vorgängerversionen.

Passwortlose Optionen bei BYOD-Ansätzen schließen die Verwendung der Smartphone-Biometrie oder FIDO-Tokens mit ein.



ENTRUST IDENTITY AS A SERVICE FÜR PASSWORTLOSES LOGIN

- Zufriedenere Anwender
- Unbelastete IT
- Hohe, auf Credentials basierende Sicherheit
- Getestet und bewährt
- Vereinheitlichtes SSO
- Reduzierte TCO
- Flexible Einsatzmöglichkeiten
- X.509-, PIV-, PIV-D- und FIDO2-Konformität

Kunden- und Partnerportale

Digital vernetzen und zusammenarbeiten

Wenn es darum geht, eine funktionierende IT für das Unternehmen bereitzustellen, werden die Stakeholder eines Unternehmens leicht vergessen. Dabei sind sie das Herzblut des Unternehmens – seien es Kunden, Lieferanten oder Auftragnehmer.

Die erste Begegnung eines Stakeholders mit einem Unternehmen könnte auch eine Authentifizierungserfahrung sein – sie stimmt so auf das sich entwickelnde Verhältnis ein.

Attraktive Kunden- und Partnerportale

- Ein einfach zu verwaltender Berechtigungsnachweis für sicheren, flexiblen Zugang
- Verwandeln Sie Ihr Unternehmen von kundenorientiert in kundengeführt
- Erweitern Sie die Beziehungen zu Kunden und Partnern
- Integrieren Sie Kunden in Echtzeit in Ihre Innovationsprozesse

Das Wichtigste in Kürze

Geben Sie externen Benutzern Zugriff auf von Ihnen ausgewählte Anwendungen, Informationen und Netzwerke.

ERFAHREN SIE MEHR

Kunden- und Partnerportale

Die Herausforderung

Noch nie war der Satz “Der Kunde ist König” so wichtig wie heute. Ein Unternehmen kundenorientiert zu führen, ist entscheidend für dessen Erfolg und Rentabilität. Im digitalen Bereich geht dies mit reibungslosen Identifikationsprozessen einher.

Die Erschließung neuer Märkte, der Ausbau bestehender Beziehungen und die Gewährleistung wettbewerbsfähiger, erstklassiger Kundenerfahrungen sind ebenfalls von zentraler Bedeutung – aber hier ist der Erfolg nicht garantiert.

Tatsächlich sind mehrere vielbeachtete Sicherheitsverletzungen darauf zurückzuführen, dass schwache Partner-Anmeldedaten gestohlen wurden. Einen mühsamen Authentifizierungsprozess werden Kunden und Partner jedoch mit der Marke in Verbindung bringen – und auf dieser Basis Entscheidungen treffen, die sich auf das Geschäft auswirken. IT-Manager in Unternehmen benötigen daher eine sichere Authentifizierungslösung, die ein kundenorientiertes Geschäft ermöglicht.

Die Lösung

Für Unternehmen mit externen Nutzern, die eine einfache, kostengünstige Lösung unabhängig von mobilen Endgeräten benötigen, können Grid und E-Mail eine pragmatische Option darstellen.

Anwender genießen flexiblen Zugang durch eine breite Palette an Authentifizierungsmöglichkeiten - von OTP bis hin zu Hardware-Tokens und Grid-Karten. Aber es gibt noch mehr Vorteile: Die Lösungen sind skalierbar, wenn die Zahl der Kunden wächst und sich ihre Bedürfnisse und Erwartungen ändern. Daher lässt sich die Authentifizierungsinfrastruktur an jeweils neue Gegebenheiten anpassen.

ENTRUST IDENTITY AS A SERVICE FÜR KUNDEN- UND PARTNERPORTALE

- Adaptive Authentifizierung, z. B. durch Fingerabdruck, Geräte-Reputation, Geostandort
- Sofort einsatzbereite Onboarding-Tools
- Selbstregistrierung und -verwaltung der Nutzer
- Große Auswahl an Authentifikatoren
- Transparentes, sicheres Benutzererlebnis
- Mobile Innovation

Anwender mit Sonderrechten

Kritische lokale Systeme und Anwendungen

Die sensibelsten IT-Plattformen im Unternehmen zu schützen und sicherzustellen, dass darauf nur einzelne Berechtigte Zugriff haben, gehört für IT-Manager zu den wichtigsten Aufgaben.

Administratorkonten werden oft als Zugang zu weiteren Unternehmensdaten genutzt. Daher ist es verlockend, die Komplexität der Authentifizierung zu erhöhen – aber das bremst auch die Wettbewerbsfähigkeit. Wie sieht also die Lösung aus?

Einräumung privilegierter Zugriffsrechte

- Sicherer IT-Zugriff, jederzeit und überall
- Vertrauenswürdiger Zugang für privilegierte Anwender
- Geschäftsentscheidende Transaktionen
- Reibungslose Benutzererfahrung
- Schutz vor Bedrohungen

Das Wichtigste in Kürze

Starke Authentifizierung und höchste Sicherheit für wichtige Ressourcen, die sich innerhalb Ihrer Firewall befinden.

Vertrauenswürdige Identitäten sichern den digitalen Geschäftserfolg

MEHR ALS

7-VON-10 CEOs

fühlen sich nicht ausreichend auf eine Cyber-Attacke vorbereitet[7]

7. Hiscox Cyber Readiness Report, 2020

Anwender mit Sonderrechten

Die Herausforderung

Das Herzstück eines dynamischen Unternehmens sind Systeme, Informationen und Plattformen, auf die nur wenige Zugriff haben sollten. High-Tech-Unternehmen, Regierungsbehörden und Finanzabteilungen wahren eine Reihe sensibler Daten, die von geistigem Eigentum über nationale Sicherheit bis hin zu marktkritischen Daten reichen.

Den Erfolg oder Misserfolg eines Unternehmens entscheiden oft Systeme, für die zusätzliche Sicherheit unerlässlich ist. Da projektspezifische Auftragnehmer kommen und gehen, müssen die Verantwortlichen sicher sein, dass sie den richtigen Personen Zugriff gewähren.

Aber auch für einzelne privilegierte Anwender sind nahtlose Prozesse unerlässlich, um den reibungslosen und wettbewerbsfähigen Betrieb des Unternehmens zu gewährleisten.

Die Lösung

Ein flexibler, sicherer Zugang und eine reibungslose Authentifizierung sind von entscheidender Bedeutung. Die adaptive Authentifizierung schafft Transparenz und aktiviert zusätzliche Authentifizierungsschritte nur dann, wenn ein erhöhtes Risiko besteht. Die Möglichkeit, Richtlinien pro Nutzer anzupassen, gestaltet den Prozess völlig reibungslos.

Die Lösung ist für alle Ebenen skalierbar, um den Anforderungen schnell wachsender Unternehmen zu entsprechen.

Zertifikatsbasierte Berechtigungsnachweise spielen hier eine wichtige Rolle – PKI, insbesondere in Kombination mit Out-of-Band-Push-Authentifizierung, trägt zum Schutz vor den raffiniertesten Bedrohungen bei.

Die Lösung kann schnell konfiguriert und implementiert werden, ermöglicht eine zeitsparende, unkomplizierte Handhabung – und eine einheitliche Benutzeroberfläche für jedes Gerät an jedem Ort.

ENTRUST IDENTITY AS A SERVICE FÜR PRIVILEGIERTE NUTZER

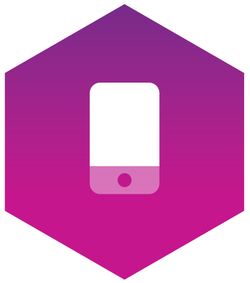
- Mobiler Push
- Doppelte Freigaben
- Mobile Smart Credentials
- BYOD und Mobile ID-Vorprüfung
- Adaptive Authentifizierung
- Einfache Integration
- Einheitliche Authentifizierungsplattform für Cloud-Anwendungen und lokale Ressourcen

Entrust Identity as a Service

VPN-Zugang

Für optimierten Fernzugriff

Jederzeit und überall mit einem sicheren und vereinfachten VPN-Zugang arbeiten.



Mobile Sicherheit

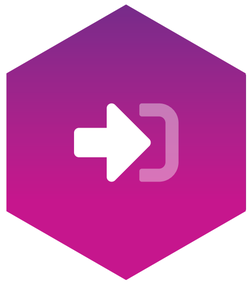
Nutzen Sie die Vorteile mobiler Endgeräte

Reibungslose Benutzererfahrung mit einem hohen Maß an Sicherheit, zur Steigerung der Produktivität.

Cloud SSO

Nahtloser Zugang zu allen Anwendungen

Reibungsloser Zugang und starker Schutz vor Sicherheitsbedrohungen.



Passwortlose Anmeldung

Nahtloses und sicheres Login und Logout

Fortschrittliche Sicherheit für Ihr Unternehmen. Einfache Handhabung für Ihre Anwender.

Kunden- und Partnerportale

Digital vernetzen und zusammenarbeiten

Ermöglichen Sie externen Nutzern den Zugriff auf von Ihnen ausgewählte Anwendungen, Informationen und Netzwerke.

Anwender mit Sonderrechten

Wichtige On-Premise-Systeme und Anwendungen

Starke Authentifizierung und hohe Sicherheit für geschäftskritische Ressourcen, die sich innerhalb Ihrer Firewall befinden.

Sind Sie bereit, das volle Potenzial digitaler Geschäftsprozesse auszuschöpfen?

ERFAHREN SIE MEHR

Erleben Sie Identity as a Service mit einer kostenlosen 30-Tage-Testversion.

ZUR KOSTENLOSEN TESTVERSION

Für weitere Informationen

Telefon:
+49 211 5401 2450

entrust.com

ÜBER ENTRUST

Mit der Schaffung vertrauenswürdiger Identitäten, Zahlungen und Daten setzt sich Entrust für sichere Transaktionen in einer sich laufend verändernden Welt ein. Die Ansprüche an nahtlose und hochsichere Anwendungen steigen stetig – sei es beim Grenzübertritt, beim Einkaufen, bei der Nutzung von E-Government-Diensten oder beim Einloggen in Unternehmensnetzwerke. Entrust bietet eine einzigartige Bandbreite an Lösungen für die digitale Sicherheit und die Ausstellung von Berechtigungsnachweisen, welche die Grundlage all dieser Interaktionen darstellen. Weltweit vertrauen die angesehensten Organisationen und Unternehmen auf 2.500 Mitarbeiter und ein Netzwerk globaler Partner und Kunden in über 150 Ländern.

Weitere Informationen unter
entrust.com

ENTRUST

Lütticher Strasse 132, 40547 Düsseldorf
Phone: +49 211 5401 2450
www.entrust.com