Entrust Identity Essentials

Realisieren Sie ein Zero-Trust-Rahmenwerk.

Entrust Identity deckt das gesamte Spektrum an IAM-Lösungen ab, von erstklassigem MFA- und VPN-Schutz für Windows-basierte Umgebungen bis hin zur hochsicheren passwortlosen Authentifizierung durch Berechtigungsnachweise, die vor Ort oder in der Cloud bereitgestellt werden kann.

ENTRUST

IDENTITY
ESSENTIALS

ÜBERBLICK

Grundlegendes zur Identität

Identity Essentials ist die ideale Multi-Faktor-Authentifizierungslösung (MFA) für Unternehmen, die nach einer schnellen, kostengünstigen Option suchen, um Mitarbeiteridentitäten zu sichern und ihren Fernarbeitskräften den Zugriff zu ermöglichen. Mit Identity Essentials beginnen Sie mit einer benutzerfreundlichen, einfach zu implementierenden MFA-Lösung vor Ort und können mit Identity as a Service im Laufe der Zeit in die Cloud migrieren, falls und wann immer dies sinnvoll ist. Die nahtlose Integration zwischen Identity Essentials und Identity as a Service gewährleistet ein reibungsloses hybrides Setup und profitiert gleichzeitig von drei Authentifizierungsoptionen:

- Authentifizierung per Gerätefingerabdruck
- Mobile Push-Authentifizierung
- GRID karten authentifizierung

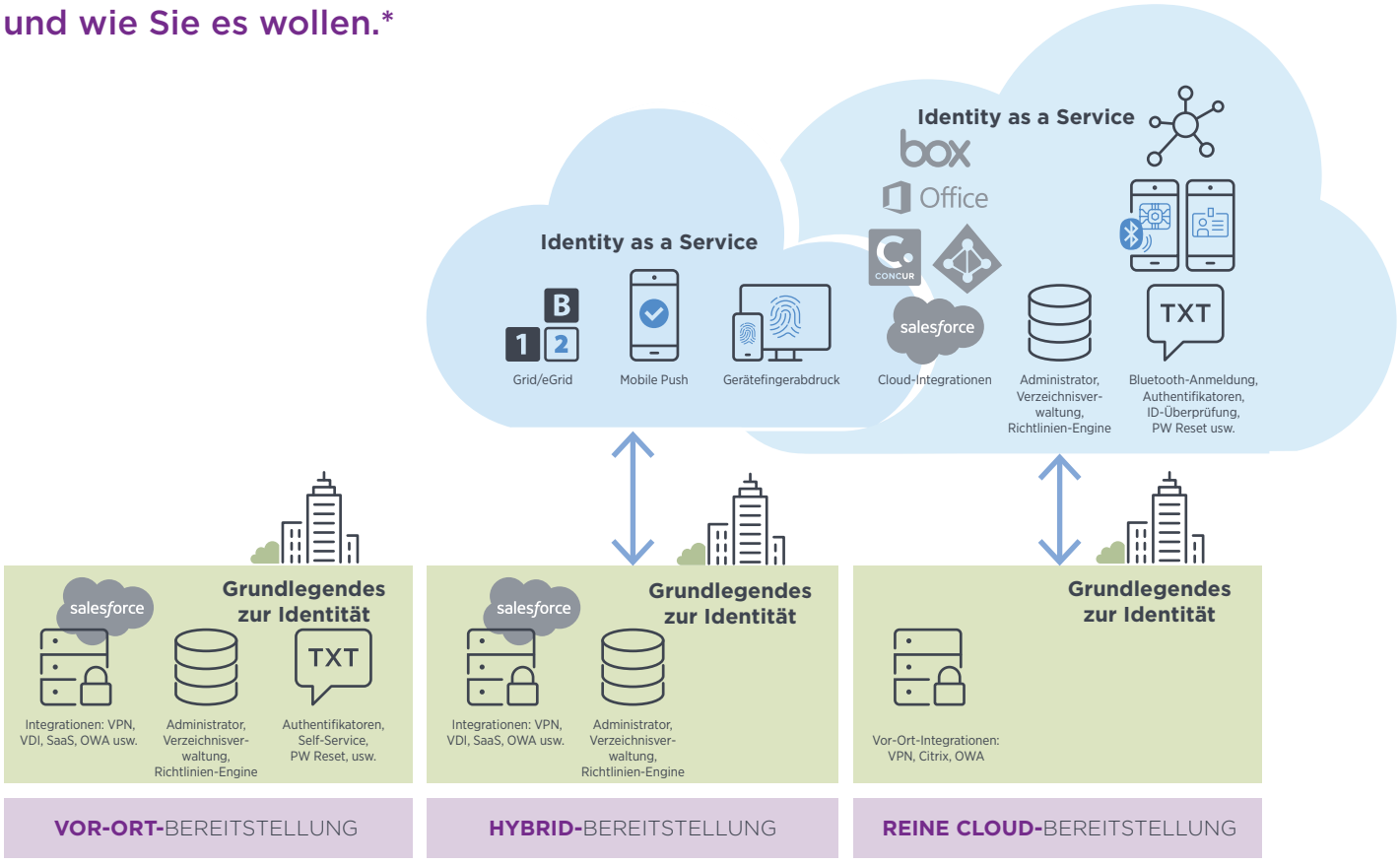
Identity Essentials liefert die Grundlage dafür, dass Windows-basierte Organisationen im Laufe der Zeit einen Zero Trust-Ansatz mit Identity as a Service umsetzen können.

SO FUNKTIONIERT ES

Größere Bedrohungen mit besserer Technologie bekämpfen

Gelangen Hacker an das Passwort eines Mitarbeiters, können sie alles eisenhen, worauf der Mitarbeiter Zugang hat – in der Cloud und vor Ort. Und da die meisten Organisationen heute immer mehr Cloud-Dienste für Dateisysteme, Intranets, Kooperationswebsites usw. zulassen, sind immer mehr Daten gefährdet. Glücklicherweise ist eine solide Benutzerauthentifizierung heute sowohl für Benutzer als auch für Administratoren weniger problematisch als früher. Dank der nahtlosen Integration in Identity as a Service können Sie mit Identity Essentials mehr und mehr Cloud Funktionalitäten nutzen, wann und wie Sie es wollen – mit passwortloser Anmeldung und Smart Login unter Windows 7, 8, 10 und MacOS.

Dank der nahtlosen Integration in Identity as a Service können Sie mit Identity Essentials mehr und mehr Cloud Funktionalitäten nutzen, wann und wie Sie es wollen.*



*Nur für Kunden mit einer Abonnementlizenz für Identity Essentials.

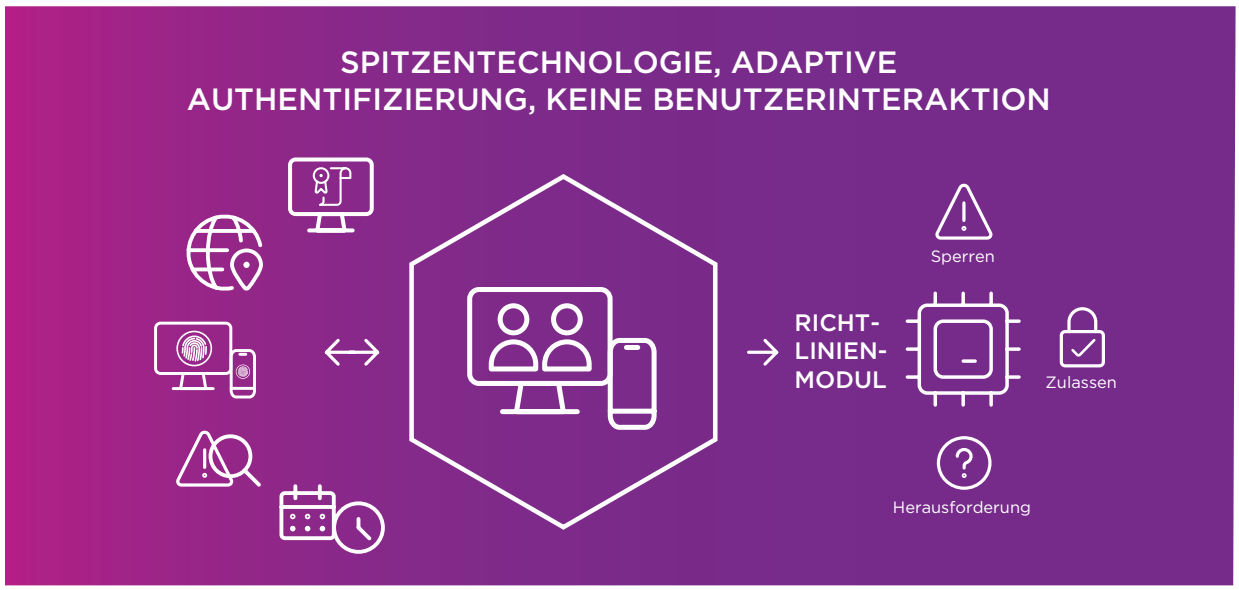
Lizenzoptionen: Leistungsumfang*

Unternehmen, die sich für das Abonnementpaket entscheiden, profitieren in vollem Umfang von der engen Integration zwischen Identity Essentials und Identity as a Service.

	Software Assurance	Abonnement-paket
Erweiterungen von Identity Essentials	●	●
Unterstützung von Windows Server 2019	●	●
Gerätefingerabdruck mit AD FS (Identity as a Service)	●	●
Push-Authentifizierung (Identity as a Service)	●	●
ActiveSync-Gerätebereitstellung für Office365 und Exchange vor Ort	●	●
Identity as a Service „Plus“, einschließlich Risikomodul, Cloud-to-Cloud-Authentifizierung usw.		●
Globaler SMS-, App- und sprachbasierter OTP-Verteilerdienst		●
Single-Sign-On-Portal von Identity as a Service für alle Cloud-Dienste an einem Ort, geschützt		●
Unterstützung für Identity Essentials, Geschäftszeiten (kann verlängert werden)		●
Unterstützung von GRID kartern	●	●
Erweiterte Funktionalität bei der Authentifizierung der Windows-Anmeldekonsole	●	●

*Identity Smart Login ist eine Zusatzfunktion gegen Aufpreis.

Die adaptive, risikobasierte Engine von Entrust Identity bietet ein zusätzliches Maß an Sicherheit, wenn die Bedingungen dies rechtfertigen, z. B. wenn sich ein Mitarbeiter zum ersten Mal von einem neuen Gerät aus, zu einer ungewöhnlichen Tageszeit oder von einem anderen geografischen Standort aus anmeldet. Nur wenn die zusätzliche Authentifizierung durch z. B. mobile Push-Benachrichtigungen auf solche Situationen beschränkt wird, bleibt der Störfaktor für die Mitarbeiter minimal, während die Unternehmensressourcen weiterhin geschützt sind.

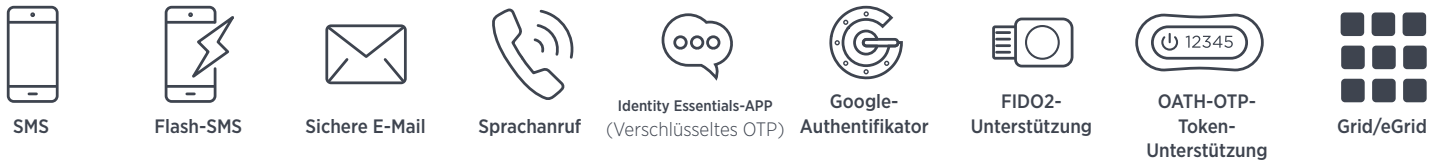


Eine große Auswahl an unterstützten Authentifikatoren

Bei Identity Essentials stehen Ihnen mehrere Authentifizierungsmethoden zur Auswahl. Abhängig von verschiedenen Faktoren wie dem Zugriff auf das Asset, dem verwendeten Gerät und dem Grad der technischen Fähigkeiten des Benutzers sollten Sie verschiedene Authentifizierungsmethoden wählen.

Drei moderne Funktionen (siehe unten) werden allesamt durch die Integration von Identity as a Service ermöglicht, die Mitarbeitern einen sicheren Zugriff auf Workstations, Netzwerke und Anwendungen ermöglicht – ohne mühsame Passworteingaben oder traditionelle Zwei-Faktor-Authentifizierungen bei jeder Sitzung. Eine wirklich passwortlose, reibungslose und sichere Anmeldung.

Identity Essentials-Authentifikatoren



SMS | Flash-SMS | Sichere E-Mail | Sprachanruf | Identity Essentials-APP (Verschlüsseltes OTP) | Google-Authentifikator | FIDO2-Unterstützung | OATH-OTP-Token-Unterstützung | Grid/eGrid

PLUS 3 AUTHENTIFIZIERUNGSMERKMALE BASIEREND AUF IDENTITY AS A SERVICE

Authentifizierung per Gerätefingerabdruck

Beim Zugriff auf Cloud-Anwendungen über AD FS kann der Fingerabdruck neuer Geräte erfasst werden, was die automatische Erkennung zuvor verwendeter Geräte ermöglicht. Das bietet eine zusätzliche Sicherheitsebene und ermöglicht Ihnen die Umgehung von Einmalpasscodes (OTPs).

Bei der Verwendung des Identity as a Service-Risikomoduls kann dies neben Geolokalisierung, IP-Adresse, Zeitpunkt der Anmeldung, Reisegeschwindigkeit usw. einen weiteren zu berücksichtigenden Faktor darstellen.

Mobile Push-Authentifizierung

Fügen Sie eine zusätzliche Sicherheitsebene hinzu, wenn sich Mitarbeiter zu einer ungewöhnlichen Zeit oder von einem ungewöhnlichen Ort aus anmelden möchten. Die Push-Authentifizierungsanwendung, die Sie mit eigenem Branding versehen können, bietet biometrische Sicherheit, indem sie zur Identifizierung Ihre nativen mobilen biometrischen Merkmale verwendet, um unbefugten Zugriff zu verhindern. Die App verfügt über die Schaltflächen „Bestätigen“, „Ablehnen“ und „Bedenken“; Bedenken werden aufgezeichnet und ein Bericht wird an einen Administrator gesendet.

Passwortlose Authentifizierung

Die GRID kartenauthentifizierung bietet Organisationen ein einfaches, aber effektives, leistungsstarkes Authentifizierungswerkzeug für erhöhte Sicherheit und logische Zugangskontrolle. Benutzer erhalten eine Authentifizierungsaufforderung, wenn sie sich bei eingeschränkten Netzwerken, Anwendungen, Cloud-Diensten oder Websites anmelden. Jede Rasterkarte ist einzigartig und trägt eine Seriennummer, sodass jeder Benutzer eindeutig identifiziert und authentifiziert werden kann. Benutzer erhalten jedes Mal eine andere Authentifizierungsaufforderung, wodurch sie sich stets über einen anderen Satz von Rasterkoordinaten validieren müssen. Die Koordinatenanforderung ändert sich bei jeder Authentifizierungsaufforderung.

Authentifizierung per Gerätefingerabdruck: eine sichere, einfache Anmeldung

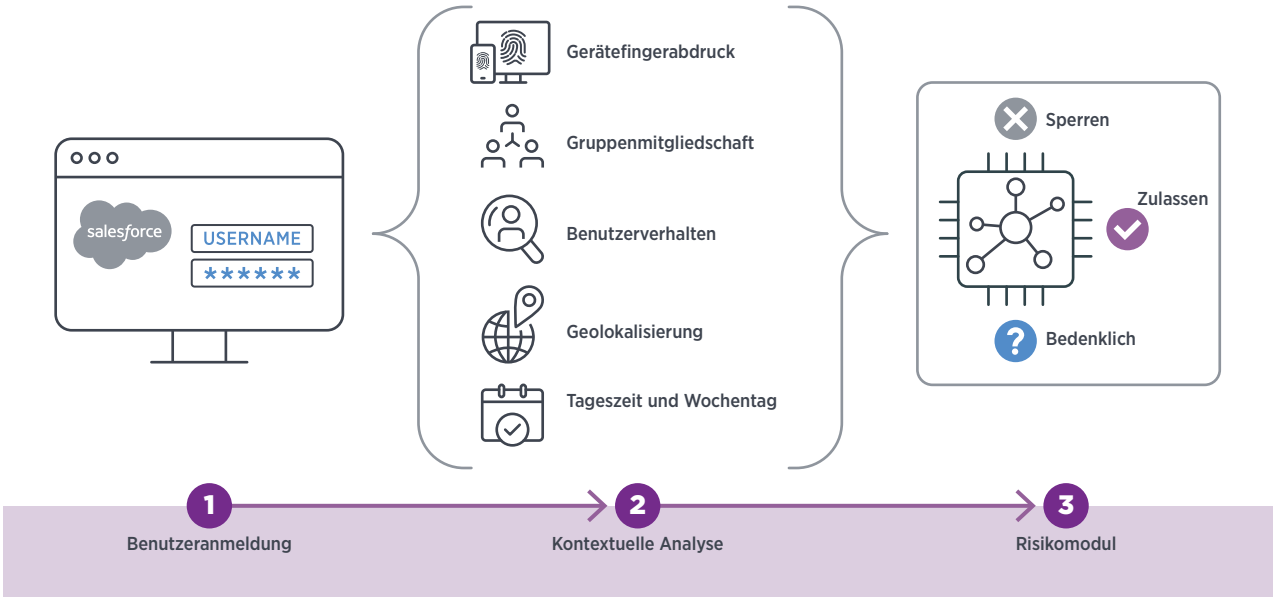
Mehr als 80 % aller Sicherheitsverletzungen im Zusammenhang mit Hacking werden durch schwache oder gestohlene Benutzeranmeldeinformationen verursacht. Das Hinzufügen von MFA zu allen Diensten erhöht Ihre Sicherheit dramatisch, da Sie Hackern ihre bevorzugte Waffe nehmen.

Um den Pushback Ihrer Benutzer zu überwinden, sollten Sie sich unsere adaptiven/kontextbezogenen Intelligence-Funktionen ansehen, die die Benutzerfreundlichkeit bereits für Tausende von Unternehmen verbessert haben.

Identity Essentials leistete Pionierarbeit bei der adaptiven Authentifizierung, bei der die Anmeldung je nach Kontext gewährt wird – ob der Benutzer beispielsweise über VPN, Citrix, RDP oder Cloud-Dienste angemeldet ist.

Der Gerätefingerabdruck ist die neueste Ergänzung und bietet mehr Sicherheit als ein Authentifizierungscookie zur Validierung des Geräts, das zuvor bei einer Anmeldung verwendet wurde.

AUTHENTIFIZIERUNG PER GERÄTEFINGERABDRUCK – basierend auf Identity as a Service



Identity Essentials macht frustrierende, sich wiederholende Anmeldungen überflüssig, indem es die einfach zu konfigurierende Engine von Identity as a Service nutzt, die Risiken in Echtzeit auf der Grundlage kontextbezogener Daten und des Benutzerverhaltens erkennt.

ActiveSync-Schutz: Keine Verwaltung mobiler Geräte erforderlich

ActiveSync – das Protokoll für eine einfache Synchronisierung von E-Mails, Kontakten usw. – stellt ein oft übersehenes Sicherheitsrisiko dar. Wenn ein Benutzer nur mit einer E-Mail-Adresse und einem Passwort ganz einfach den Zugriff auf wichtige Informationen einrichten kann, kann das auch ein Hacker. Und wenn Sie OWA/Office365 mit MFA schützen, sollten Sie auch ActiveSync nicht vergessen werden.

ES GIBT **DREI PRIMÄRE MÖGLICHKEITEN**, AUF INHALTE IN OFFICE 365/OWA ZUZUGREIFEN

Outlook-Client
auf PC/Mac 50 % der Zeit für E-Mail aufgewendet

ActiveSync
über iPhone/Android/Tablet 40 % der Zeit für E-Mail aufgewendet

Browser
Office.com oder OWA 10 % der Zeit für E-Mail aufgewendet

Unsere Lösung hat im Laufe der Jahre Tausenden von Organisationen geholfen, indem sie „Zulassen“, „Blockieren“ oder „Quarantäne“ in Office 365 und Exchange Server 2013/2016/2019 unterstützt hat. Durch eine intuitive, sichere Gerätebereitstellung können Anwender neue ActiveSync-Geräte schnell und einfach selbst eingliedern, ohne die Sicherheit zu gefährden – und ohne den Helpdesk um Hilfe bitten zu müssen.

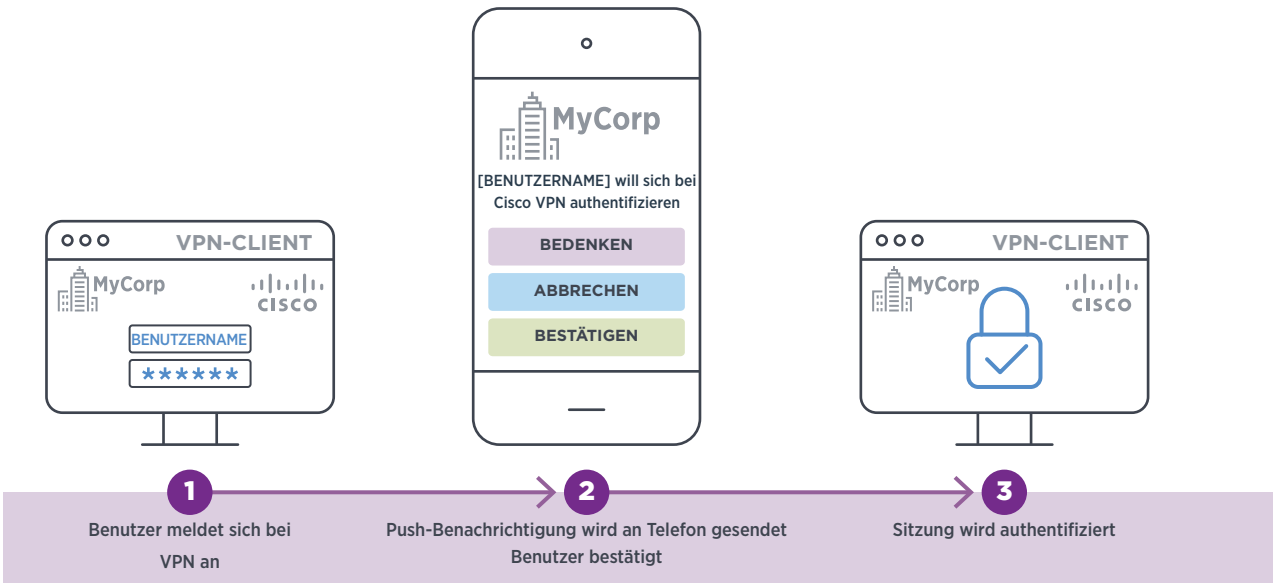
Diese einfache, sichere, benutzergesteuerte Gerätebereitstellung passt perfekt zu BYOD-Kulturen. Es ist keine komplette MDM-Lösung erforderlich. Machen Sie das Leben Ihrer Benutzer leichter, indem Sie es ihnen ermöglichen, ihre neuen Geräte auf reibungslose, aber sehr sichere Weise über ihre E-Mail-Adresse selbst einzugliedern und sich so den Zugriff zu verschaffen, den sie benötigen.

Mobile Push-Authentifizierung: perfekt für technisch versierte Mitarbeiter

Mit der Integration von Identity as a Service umfasst Identity Essentials die Push-Authentifizierung, um über VPN/Citrix (Radius) und AD FS Zugriff zu erhalten. Ist diese aktiviert, wird der Benutzer auf dem Bildschirm seines Mobiltelefons zur Eingabe von „BEDENKEN“, „ABBRECHEN“ oder „BESTÄTIGEN“ aufgefordert. Das Betätigen der Schaltfläche „BEDENKEN“ blockiert den Zugang und wird im System protokolliert, um den Administrator zu benachrichtigen.

Biometrische Validierung (z. B. Touch/Face ID) kann hinzugefügt werden, um mobile Anwendungen vor unbefugter Nutzung zu schützen oder zu verhindern, dass Benutzer Hackern versehentlich Zugang gewähren. In der App werden auch kontextbezogene Informationen angezeigt (z. B. „Anmeldeversuche vom Hilton Hotel in Bangkok, Thailand“).

MOBILE PUSH-AUTHENTIFIZIERUNG – Basierend auf Identity as a Service



Die App funktioniert auf Android sowie iOS und ist in zwei Formen erhältlich: mit oder ohne Zertifikatsfähigkeiten. Das Authentifizieren per Push-Benachrichtigung ist eine großartige Funktion für IT-erfahrene Benutzer. Andere Authentifizierungsmethoden, die keine Installation und Einrichtung am Telefon erfordern (SMS/Text, Sprachanruf usw.), sind weiterhin gültige Lösungen für viele Mitarbeiter mit Kundenkontakt und weniger technikbegeisterte Personen.

Passwortlose Authentifizierung: reibungsloser Zugriff auf Apps

Entrust Identity

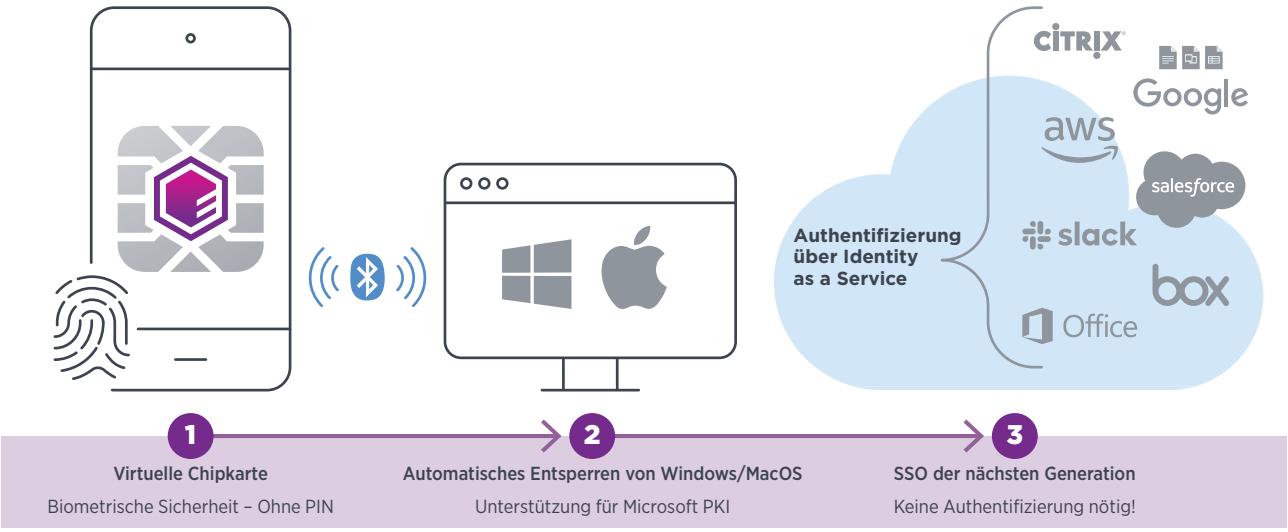
Die Multi-Faktor-Authentifizierung bietet seit vielen Jahren eine notwendige Sicherheitsebene zusätzlich zu Passwörtern. Aber unsere Welt hat sich weiterentwickelt – sowohl mit Blick auf die Technologie als auch auf Cyber-Bedrohungen –, was zu Problemen mit der traditionellen MFA führt.

Erstens erwarten die Nutzer sofortigen Zugriff auf Daten und Anwendungen – und MFA hat die Reibung und Frustration erhöht. Vom Eingeben von Einmalpasscodes (OTPs) bis zum Mitführen von USB-Sticks verlangsamt MFA die Produktivität. Und wenn Sie Ihren USB-Stick verlieren oder die Batterie Ihres Hardwaretokens leer ist, sind Sie ausgesperrt. Zweitens finden Hacker Wege, bestimmte MFA-Methoden zu umgehen, was zu kostspieligen Sicherheitsverletzungen führt.

Smart Login löst die wichtigsten Probleme von MFA, indem es die Sicherheit maximiert und die Benutzerfreundlichkeit für den Anwender erhöht. Wir bieten fortschrittliche Lösungen, die für Endbenutzer einfach zu handhaben sind, indem wir die Sicherheit digitaler Zertifikate und die Bequemlichkeit von Mobiltelefonen zusammenführen.

Mit Smart Login von Entrust Identity können sich Mitarbeiter bei ihren Workstations und Anwendungen anmelden, ganz einfach indem sie ihr Telefon dabei haben. Keine Passwörter mehr und keine 2FA, wie z. B. Wissensfragen oder OTPs. Der Zugriff auf ihre Computer und Anwendungen erfolgt schnell und einfach mit weniger Sicherheitshürden, wodurch sie produktiver arbeiten können. Außerdem müssen sie nicht mehr daran denken, ihre Workstations zu sperren. Smart Login meldet sie automatisch ab, wenn sie weggehen.

PASSWORTLOSE AUTHENTIFIZIERUNG – basierend auf Identity as a Service



Merkmale von Identity Essentials

Nahtlose Integration: Die MFA-Plattform von Identity Essentials lässt sich nahtlos in Anmeldesysteme und Cloud-Lösungen integrieren, um einen intuitiven, benutzerfreundlichen Fernzugriff zu ermöglichen.

Adaptive Authentifizierung: Passt das Authentifizierungsniveau automatisch an die aktuellen Umstände des Benutzers an und schafft so ein Gleichgewicht zwischen hoher Sicherheit und starker Benutzerfreundlichkeit.

Automatische Ausfallsicherung: Es ist möglich, hochflexible Failover-Mechanismen einzurichten, um sicherzustellen, dass die OTPs immer ankommen. Die Lösung kann sogar zwischen den Übertragungen wechseln, je nach aktuellem Anmeldekontext des Benutzers.

Breite Verzeichnisunterstützung: Benutzer können von Active Directory und allgemeinen LDAP-Verzeichnissen wie OpenLDAP oder AD LDS synchronisiert werden. Benutzer können durch Auswahl einer bestimmten Benutzergruppe oder durch Verwendung eines LDAP-Filters importiert werden.

Echtzeitschutz: Sämtliche OTP-Codes werden in Echtzeit am Ort der Anmeldung generiert. Es gibt keine vorher ausgegebenen Passcodes oder Seed-Dateien, die gehackt werden könnten. Gleichzeitig ist Echtzeit eine Voraussetzung für die Bereitstellung sitzungsspezifischer OTPs.

PowerShell: Administratoren können für das Erstellen von rollenbasiertem Zugriff, das Integrieren in andere Systeme oder das Automatisieren täglicher Aufgaben, z. B. Überprüfung der Lizenzverfügbarkeit oder länderspezifische Anmeldungen, PowerShell-Skripting verwenden.

Status-Feedback: Ermöglicht es dem Benutzer, den Anmeldevorgang zu verfolgen; schafft Vertrauen bei den Benutzern und reduziert die Anzahl der Helpdesk-Anrufe.

Unterstützung von Standort und Verhalten: Nutzt für das Gewähren oder Verweigern des Benutzerzugriffs kontextbezogene Informationen wie z. B. Verhaltensmuster bei der Anmeldung und Geolokalisierung. Geofencing ermöglicht es Administratoren, auf der Grundlage von Systemen und Standorten Whitelists oder Blacklists zu erstellen (z. B. Einschränkung des Zugriffs über Citrix NetScaler von bestimmten Ländern aus).

Sichere Gerätebereitstellung: Ermöglicht Benutzern die schnelle und einfache Selbstregistrierung neuer ActiveSync-Geräte, ohne die Sicherheit zu gefährden und ohne den Helpdesk um Hilfe bitten zu müssen.

OTP-Bereitstellungsmethoden: Plug-ins und Standard-OTP-Bereitstellungsmethoden – wie Apps, SMS, Sprachanruf, sichere E-Mail, Cloud-Schlüssel und Hard-/Soft-Token – unterstützen Ihre Geschäftsanforderungen jetzt und in Zukunft.

Erweiterte Datenbanküberwachung: Hilft den Kunden bei der Einhaltung von strengen Branchenvorschriften und Audit-Kontrollanforderungen.

Zusätzliche Funktionen über die Integration von Identity as a Service

App für die mobile Push-Authentifizierung (mit Ihrem eigenen Branding): Fügt eine benutzerfreundliche Sicherheitsebene hinzu, wenn sich Mitarbeiter zu einer ungewöhnlichen Zeit oder von einem ungewöhnlichen Ort aus einloggen wollen. Auf dem Mobiltelefon des Mitarbeiters wird eine Benachrichtigung angezeigt, um zu bestätigen, dass er den Zugang beantragt.

Authentifizierung per Gerätefingerabdruck: Nach erfolgreicher Anmeldung bei einem Cloud-Dienst über AD FS kann ein Gerätefingerabdruck erfasst und für zukünftige Sicherheitsbewertungen der Anmeldung verwendet werden, was eine einfachere Anmeldung ermöglicht.

Passwortlose Authentifizierung: Stellt auf dem Telefon des Mitarbeiters einen Berechtigungsnachweis bereit, der die passwortlose Anmeldung an der Workstation (Macs und PCs) und die Anwendungs-SSO (Cloud und vor Ort) über Bluetooth ermöglicht, wenn sich das Telefon in unmittelbarer Nähe befindet und per Fingerabdruck- oder Gesichtsabgleich des Benutzers freigeschaltet wird.

Single Sign-On (SSO): Identity as a Service stellt SSO für alle Anwendungen – in der Cloud und vor Ort – bereit, einschließlich ältere Apps. Erstellt über Standards wie SAML und OIDC einen Verbund mit Cloud-Anwendungen.

Azure AD-Integration: Lässt sich zur Benutzersynchronisierung usw. mit Azure AD integrieren.

E-Mail- und Dateiverschlüsselung: Die Integration mit den wichtigsten MDM-Anbietern – einschließlich Microsoft, IBM und VMware – gewährleistet eine sichere Kommunikation am Arbeitsplatz durch E-Mail- und Dateiverschlüsselung.

Dokumentunterzeichnung: Die MDM-Anbieterintegration unterstützt sichere Transaktionen am Arbeitsplatz und die Nichtabstreitbarkeit durch Dokumentsignatur.

Identitätsüberprüfung: Sichere Überprüfung der Identität von Mitarbeitern, Auftragnehmern, Partnern und anderen.

Verbraucherauthentifizierung: Identity as a Service geht über die Mitarbeiterauthentifizierung hinaus. Es kann auch alle Ihre Bedürfnisse im Bereich der Verbraucherauthentifizierung erfüllen.

Entrust Identity-Portfolio: Identity Essentials ist Teil unseres vereinheitlichten Entrust Identity-Portfolios, das auch Identity as a Service und Identity Enterprise umfasst. Entrust Identity bietet Lösungen im Bereich Identitäts- und Zugriffsmanagement (IAM) für Mitarbeiter, um zahlreiche Unternehmensgrößen von 50 bis über 1 Million Benutzer zu unterstützen.

Unterstützte Systeme

Identity Essentials unterstützt eine Vielzahl von Anmeldesystemen, die für den Fernzugriff verwendet werden. Die Plattform ist so konzipiert, dass sie sich nahtlos in Hunderte von VPNs integrieren lässt und einen sicheren und intuitiven Anmeldeprozess ermöglicht. Nachstehend finden Sie eine Liste mit Beispielen für unterstützte Fernzugriffssysteme.

RADIUS VPN/SSL VPN-Clients

- Check Point
- Cisco ASA
- Citrix Netscaler (Citrix ADC)
- Juniper
- Pulse Secure
- Barracuda NG-Firewalls
- VMware Horizon View
- Netop Remote Control
- Palo Alto
- F5 BIG-IP
- NCP-VPN
- Andere RADIUS-Clients

Internet Information Services (IIS)-Websites

Unterstützung für die folgenden Arten von Websites:

- Outlook Web Access 2010/2013/2016/2019
- Web Access für Remotedesktop (Windows Server 2012 R2/2016/2019)
- IIS-Websites mit einfacher, integrierter Windows-Authentifizierung und formularbasierter ASP.Net-Authentifizierung

Windows-Anmeldung, Remotedesktopdienste

Unterstützung für die folgenden Server und Dienste:

- Remotedesktopdienste (RDP-Verbindungen)
- Windows-Server/2012/2012 R2/2016/2019
- Windows 8, Windows 8.1 und Windows 10
- VMware Virtual Desktop-Portal und Client-Zugriff

Sichere Gerätebereitstellung

Schutz für ActiveSync-Geräte auf den folgenden Systemen:

- Exchange 2010 SP3
- Exchange 2013
- Exchange 2016
- Exchange 2019
- Exchange Online

Microsoft AD FS-Schutz

- Adapter für Multi-Faktor-Authentifizierung für AD FS 3.0/4.0/5.0

Unterstützung der Multi-Faktor-Authentifizierung für:

- Zugriff auf Cloud-Anwendungen wie Salesforce.com, Microsoft Office 365, Google Apps usw. (AD FS 3.0/4.0/5.0)
- Zugriff auf Websites, die über den Microsoft Web Application Proxy (AD FS 3.0/4.0/5.0) veröffentlicht werden, wie z. B. Outlook Web Access
- Zulassung von Geräten in Verbindung mit Arbeitsplatzverbindungen (AD FS 3.0/4.0/5.0)

Weitere Informationen erhalten Sie unter

888.690.2424
+1 952 933 1223
sales@entrust.com
entrust.com

ÜBER ENTRUST CORPORATION

Entrust sichert eine sich schnell verändernde 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.

Mehr Informationen unter
entrust.com

ENTRUST

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