Whitepaper

Build vs. Buy

Customer Identity &
Access Management

Inhalt

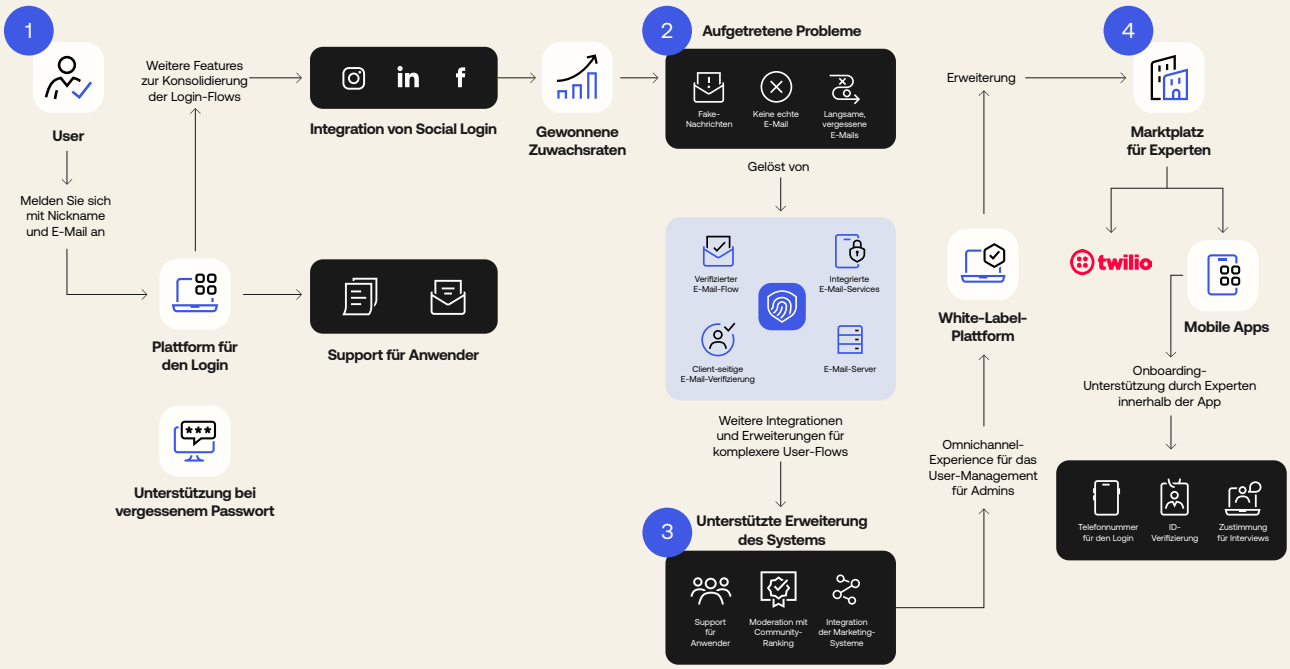
Es ist schwer, die Customer Identities im Griff zu behalten

Jedes Team, das Web- und Mobile-Apps entwickelt, steht bei jedem neuen Feature vor dem gleichen Dilemma: Sollte man es lieber selbst Inhouse entwickeln, oder schlüsselfertige Out-of-the-Box-Services beziehen, um schneller und leichter zum Ziel zu kommen?

Unsere Entwickler können Ihnen das Handling der Customer Identities abnehmen. Schließlich braucht man dafür nur eine Login-Box. Wie schwer kann das schon sein?

Customer Identity & Access Management (CIAM) ist natürlich viel mehr als nur eine Login-Box. Gerade in Unternehmen, die dynamisch wachsen und immer neue Funktionalitäten hinzufügen, kann die Pflege einer komplexen, robusten eigenen CIAM-Lösung wesentlich mehr Ressourcen beanspruchen als gedacht. Entwickler-Stunden sind ein wertvolles Gut – und die Zeit, die auf das Management, die Absicherung und den Compliance-konformen Betrieb eines eigenentwickelten CIAM-Systems verwendet wird, fehlt oft bei geschäftskritischen Innovationsprojekten.

Selbst entwickeln ist noch viel aufwändiger



Was können Sie also tun, um innovative Projekte voranzutreiben und Ihre Entwickler von Routineaufgaben zu entlasten, ohne Kompromisse bei der Security, den Deadlines oder dem Etat zu machen?

Die Antwort ist vielleicht ein schlüsselfertiges CIAM. Eine digitale Identity-Ebene mit APIs, SDKs und vorkonfigurierten, individualisierbaren Komponenten liefert Ihnen alle Bausteine, um Ihre Time-to-Market zu verkürzen, die Entwicklungskosten zu senken und zeitliche Freiräume zu schaffen, damit sich Ihre Entwickler ganz auf die eigentlichen Funktionen der Anwendungen konzentrieren können. Jede Kunden-Anwendung erfordert grundlegende Standarddienste für Authentisierung, Autorisierung und User-Management. Alle Anwendungen müssen Workflows für das Anlegen von Accounts, User-Logins, Passwort-Resets, Account-Wiederherstellung und den Rollout von Multi-Faktor-Authentifizierung (MFA) unterstützen. Darüber hinaus müssen Anwendungen unterschiedliche, benutzerspezifische Zugriffs-Level bieten.

Dieses Whitepaper beschäftigt sich mit den wichtigsten Aspekten, die Sie bei einer „Build vs. Buy“-Entscheidung berücksichtigen müssen – und den Vorteilen, die eine schlüsselfertige Lösung bietet.

> „[Okta] ist eines der Werkzeuge, die ich in mein Toolkit packen kann, um zu sagen: Hey, wir können richtig Gas geben, weil wir die Identities voll im Griff haben.“
>
> **Scott Howitt**
> CISO, MGM Resorts International

Senken Sie die Total Cost of Ownership (TCO) der Anwendungsentwicklung

Das Management der Identities ist ein Bereich, der besonders für ausufernde Kosten anfällig ist: Viele Unternehmen unterschätzen die Komplexität der Features und Systeme – und die Dynamik, mit der sie sich weiterentwickeln. Eigenentwickelte Ansätze tragen zusätzlich zu dieser Unwägbarkeit bei. Hinzu kommt, dass die Kosten rasant steigen, wenn interne Teams abgelenkt werden, weil sie immer komplexere Identity-Features entwickeln sollen, oder wenn sich die regulatorischen Anforderungen plötzlich ändern. Das Team wird vielleicht trotzdem pünktlich liefern, aber dabei auf die knappe Personalressourcen angewiesen sein. Wenn Sie das Thema Identity einem Anbieter Ihres Vertrauens übertragen, können Sie sich sicher sein, dass Ihr Team seine ganze Energie auf die Kernfunktionen des Projekts konzentriert.

Beispiel für die Senkung der TCO in der Entwicklung[1]

3	x	6	x	USD 200K	x	90 %	=	USD 270K
Entwickler		Monate Identity-Timeline		Vollzeit-Gehalt		Verbesserung		**Senkung der TCO**

„Der Identitätsbereich ändert sich beinahe stündlich, und wir brauchen einen Technologiepartner, der mit diesem dynamischen Entwicklungstempo Schritt halten kann."

Eash Sundaram
EVP Innovation, Chief Digital & Technology Officer,
JetBlue Airways

[1] Typische, Google-mäßige Kalkulation des Wertes eines Entwicklers für ein Unternehmen, in dem Technologie der wichtigste Umsatztreiber ist. Hier berechnen wir den durchschnittlichen jährlichen Beitrag, den ein Entwickler zum Umsatz leistet, multipliziert mit der Anzahl der Entwickler, die im Entwickler-Pool fehlen, weil sie die Identity-Ebene bereitstellen sollen.

Konzentrieren Sie Ihre Ressourcen auf die Schlüsselfunktionen Ihrer Anwendungen

Der Erfolg Ihres Unternehmens hängt maßgeblich davon ab, wie gut Sie die Schlüsselfunktionen umsetzen, die Ihre Kunden an Ihrer Anwendung schätzen. Eine moderne Identity-Ebene gibt Ihrem Team die Freiheit, sich auf die Features zu konzentrieren, die den Umsatz und die Kundenbindung fördern – und ermöglicht es Ihren Entwicklern, schneller die zweite, dritte oder vierte App anzugehen, die Ihre Kunden wünschen.

Minimieren Sie das Risiko von Security- und Compliance-Verstößen

Wann hat Ihr Team das letzte Mal den Passwort-Hashing-Algorithmus aktualisiert? User-Daten und PII geraten besonders häufig ins Visier von Angreifern, doch die durchschnittliche Lebensdauer eines wirksamen Verschlüsselungsalgorithmus beträgt 18 Monate. Die Anwender zu schützen, rückt angesichts von Wachstums- und Umsatz-Zielen oft in den Hintergrund. Außerdem erfordert ein sicherer Identity-Service, dass Ihr Team über umfassendes Knowhow und ausreichend Zeit verfügt, um Schwachstellen auf allen Ebenen der Infrastruktur zu beheben – vom Betriebssystem über die Datenbanken und die Transportebene bis hin zum Anwendungs-Stack und den Schwachstellen im Code. Da Entwicklungsteams nur selten über dieses Security-Knowhow verfügen, bemerken sie möglicherweise erst dann, dass die Security-Mechanismen versagt haben, wenn sensible Daten gefährdet sind. Und sie sind oft nicht über aktuelle Entwicklungen in der IT-Security informiert, etwa wenn ein Algorithmus kompromittiert oder ein Angriffsvektor entdeckt wurde.

Wenn Sie sich für den richtigen Identity-Management-Service entscheiden, wird dieser Ihre Benutzerdaten zuverlässig vor Angreifern schützen: Immerhin wurde er von ausgemachten Security-Experten entwickelt, die wissen, worauf es bei der Absicherung von Identities und Zugriffen ankommt. Zu den Security-Maßnahmen gehört leistungsfähige Verschlüsselung, API-Security, zuverlässige Firewall-Funktionalitäten und robuste Sicherheitsprozesse für das Daten-Management und den Systemzugang. Diese Security-Maßnahmen und Infrastrukturen ermöglichen Ihrem Team auch die Einhaltung regionaler Compliance-Vorgaben und Branchenstandards wie HIPAA, FedRamp und DS-GVO.

> „Die National Bank of Canada betreut Millionen von Kunden in Hunderten von Filialen in ganz Kanada. Als Unternehmen haben wir klare Ziele, und eines davon ist eine einfachere Customer-Experience. Die intelligenten Authentifizierungs- und Kontext-Funktionalitäten von Okta ermöglichen es uns, unseren Kunden eine hochwertige, sichere Online-Experience zu bieten."
>
> **Rish Tandon**
> CTO, Heal

Sorgen Sie dafür, dass Ihre Entwickler motiviert bleiben

Auch wenn Identity ein wichtiges Element von Kundenanwendungen ist, macht es längst nicht jedem Entwickler Spaß, Identity- und Security-Infrastrukturen zu entwickeln. Auch wenn es sich um einen riskanten und oft komplexen Bereich handelt, wird die Benutzerverwaltung mitunter als banal empfunden. Viele Entwickler würden lieber an innovativen Funktionen arbeiten, mit denen sich das Kernprodukt von anderen Lösungen abgrenzt. Der enorme Aufwand, der mit der Implementierung der Security-Features verbunden ist, kann besonders demotivierend sein: Immerhin steht viel auf dem Spiel, und es gibt oft viele widersprüchliche Anweisungen. Im Gegensatz dazu empfinden viele Entwickler die Arbeit mit modernen REST-JSON-API-Diensten als interessant und zugänglich.

Stellen Sie die Weichen für Skalierbarkeit und Zuverlässigkeit
Wenn das User-Management ausfällt, können die Benutzer nicht mehr auf ihre Anwendungen zugreifen. Wenn die Anmeldung aufgrund von Verfügbarkeitsproblemen fehlschlägt, werden die Benutzer nicht wissen, was schief gegangen ist – und es wird sie auch nicht interessieren. Aber der Ruf Ihres Unternehmens und Ihrer Marke wird leiden. Es ist nicht immer vorhersehbar, wie viele Kunden auf Ihre Systeme zugreifen werden, und die Marketingabteilungen wissen nicht immer, wann eine Promotion einen plötzlichen Zustrom von Usern auslösen wird. Wenn Sie sich entscheiden, diese Aufgabe selbst zu übernehmen, müssen Sie sich darauf verlassen können, dass Ihr Team eine lückenlose Verfügbarkeit garantieren und bei wachsender Benutzerbasis auch entsprechende Skalierbarkeit bietet.
Sie müssen darauf vorbereitet sein, in Ihrem Rechenzentrum oder bei Ihrem Infrastructure-as-a-Service-Anbieter doppelte oder dreifache Redundanz bereitzustellen. Darüber hinaus müssen Sie effiziente Upgrades und Wartungsprozesse etablieren, um einen unterbrechungsfreien Betrieb zu gewährleisten. Unternehmen, die diese anspruchsvollen Aufgaben in Eigenregie übernehmen, müssen oft feststellen, dass der administrative Overhead enorm ist. Ein externer Betreiber der User-Management-Lösung kann all diese Kopfschmerzen zuverlässig kurieren.

> „Eine einfache Integration über das gesamte Ökosystem hinweg, durchgängige Verfügbarkeit der Identity-Lösung und die Nutzung der Identity, um zuverlässig und hochverfügbar mit unseren Kunden zu interagieren – das war uns wirklich wichtig."
>
> **James Fairweather**
> Senior Vice President of E-Commerce and Technology, Pitney

Die Vorteile eines zugekauften Customer Identity & Access Managements

Es gibt gute Gründe, das Identity Management zu kaufen, statt es selbst zu entwickeln:

Verkürzen Sie die Time-to-Market Ihrer Apps, um den Umsatz zu steigern
Kundenanforderungen können sich schnell ändern, und Unternehmen müssen heute flexibel genug sein, um neue Chancen zu nutzen, wenn sie sich bieten. Die richtige CIAM-Lösung wird eine vorkonfigurierte Identity-Ebene bereitstellen, damit Ihre Entwicklungsteams das Rad im Bereich Authentifizierung, Autorisierung und User-Management nicht neu erfinden müssen. So können Sie sich ganz auf die neuer USPs Ihrer Anwendungen konzentrieren. Dabei gilt es, Umsatz sowohl zu schützen als auch zu generieren – Skalierbarkeit ist also ein wichtiger Faktor. Ressourcen-intensive Prozesse wie die Authentisierung, die Passwortverschlüsselung und die Suche müssen auch während eventueller Lastspitzen mit den Anforderungen der User Schritt halten.

Senkung der Entwicklungskosten
Die Implementierung der IAM-Lösung eines Drittanbieters ist unkompliziert, und sie erschließt Ihnen einfach und schnell den Zugang zu attraktiven neuen Funktionen. Hunderte, wenn nicht gar Tausende wertvoller Entwicklungsstunden stehen wieder für die Programmierung von Business-Anwendungen zur Verfügung, statt für die Entwicklung der Authentifizierung verwendet zu werden. Zeit, die bislang für das Testen und die Sicherheit der Authentifizierung aufgewendet wurde, kann für die Arbeit an den Schlüsselanwendungen genutzt werden. Die Integration und Bewertung von Identity-Anbietern ist zeitaufwändig und mühsam. Mit der richtigen Third-Party-Lösung stehen Ihnen diese Integrationen bereits schlüsselfertig zur Verfügung. Eine vorkonfigurierte CIAM-Lösung sollte auch SDKs für gängige Entwicklungsstacks unterstützen, um den Programmieraufwand für die Integration der Authentifizierungslösung weiter zu reduzieren.
Das Entwicklungsteam des Unternehmens kann sich so auf die Konfiguration konzentrieren, statt Funktionen zu programmieren und zu individualisieren.

Verbesserung der Security
Wann hat Ihr Team das letzte Mal den Passwort-Hashing-Algorithmus aktualisiert? User-Daten und PII gehören zu den häufigsten Angriffszielen. Die durchschnittliche Lebensdauer eines wirkungsvollen Verschlüsselungsalgorithmus beträgt 18 Monate. Die Anwender zu schützen, rückt angesichts von Wachstums- und Umsatz-Zielen aber oft in den Hintergrund. Eine CIAM-Lösung dient zur sicheren Speicherung und zum geschützten Transport von Benutzerdaten – und stellt die Einhaltung regionaler Compliance-Richtlinien und Zertifizierungen sicher. Darüber hinaus unterstützt eine CIAM-Lösung Federated Identities. So greifen Anwender nicht zu unerwünschten Verhaltensweisen (wie der Wiederverwendung desselben Passworts), um sich nicht zu viele Anmeldedaten merken zu müssen.

Case Studies aus verschiedenen Branchen

Schneider Electric - Einheitliches Identity Management als Wachstumstreiber

Schneider Electric, ein weltweit führendes Unternehmen im Bereich Energiemanagement und -automatisierung mit über 170.000 Mitarbeitern in mehr als 100 Ländern benötigte eine moderne Identity-Management-Strategie, die mit der nächsten Wachstumsphase des Unternehmens mitwachsen und die Nutzung der vorhandenen Ressourcen optimieren sollte. Bei der Auswahl der CIAM-Lösung hatte für Schneider Electric die Implementierung eines Single-Sign-On-Systems höchste Priorität, um einen einheitlichen Authentifizierungsprozess sicherzustellen. So konnten die gleichen Identities und Zugangsdaten für alle Systeme und Anwendungen des Unternehmens verwendet werden.

Eine Kosten-Nutzen-Analyse zeigte, dass es für Schneider Electric wirtschaftlicher wäre, wenn sich die vorhandenen Ressourcen auf die Bereitstellung der eigenen Business-Anwendungen und auf die Business-Ziele konzentrierten. Ein Third-Party-IAM kann dazu beitragen, Barrieren im Unternehmen einzureißen und die Herausforderungen bei der anspruchsvollen Integration der Identities zu lösen. Die Okta Customer Identity Cloud (ehemals Auth0) bot außerdem eine robuste und flexible Lösung, die auf die Anforderungen der Entwickler zugeschnitten und einfach zu integrieren war. Die Plattform war Web- und Mobile-friendly, unterstützte offene Standards, bot robuste Features und war mit ihrem umfassenden Identity-Provider-Support und ihrem klaren Migrationsplan äußerst zukunftssicher.

Nachdem Okta CIC implementiert worden war, profitierte Schneider Electric von einer Reihe von Vorzügen. Die Integration der Identity-Management-Lösung bedeutete für die Entwickler eine deutliche Entlastung. Dies schuf wertvolle Freiräume für Innovationsprojekte. Die Time-to-Market wurde spürbar verkürzt, und das System profitiert von einem Höchstmaß an Security und praxisnahen Best Practices. Okta CIC ermöglichte es auch, schnell und sorgfältig auf Schwachstellen zu reagieren.

„Schon bevor die News-Seiten letztes Jahr über die Heartbleed-Zero-Day-Schwachstelle berichteten, hat uns Auth0 [jetzt Okta Customer Identity Cloud] per E-Mail über den Vorfall benachrichtigt. Es war bereits ein Patch verfügbar, um die Gefahr durch Heartbleed von den Auth0-Systemen zu entfernen. Als nächstes erhielten wir eine Bestätigungsmail, dass Auth0 den Patch bereits auf der Schneider Electric-Instanz des Auth0-Dienstes installiert hatte. Mit Auth0 steht unser Plattform-Team richtig gut da. In diesem Szenario wurde nicht nur das Sicherheitsproblem gepatcht – man gab unserem internen Team auch detaillierte Schritte zur Behebung des Problems an die Hand. So konnte unser IT-Team wertvolle Zeit sparen. Darüber hinaus hat Auth0 die Zertifikate ausgewechselt, was für unser eigenes Team sehr arbeitsintensiv gewesen wäre.

Mit der Auth0-Plattform können wir unsere Identity-Architektur proaktiv planen und integrieren. So sparen wir Zeit, und können sicherstellen, dass zum Projektstart stets ein sicheres System bereitsteht.“

Stephen Berard
Schneider Electric

Bluetooth – Einheitliche Identities für On-Premises- und Cloud-Apps
Bluetooth, ein weltweit führender Anbieter von Drahtlostechnologie, unterhält ein wachsendes Ökosystem, das mit einer Reihe von Herausforderungen einhergeht. Das Unternehmen, das mit einer einzigen Anwendung begann, expandierte schnell auf eine Reihe verschiedener Anwendungen. Sowohl die intern entwickelten Anwendungen als auch externe SaaS-Anwendungen von Drittanbietern (Sharepoint, ServiceNow, SiteCore) erforderten unterschiedliche Authentifizierungsnachweise. Die vorhandene Lösung von Bluetooth basierte auf Formularen und verwendete Benutzernamen und Passwörter. Die Plattform war nicht für Federated Identities geeignet. Das Unternehmen benötigte eine moderne Identity-Lösung mit Single Sign-On, die sowohl die selbst entwickelten als auch die SaaS-Anwendungen von Drittanbietern unterstützen sollte. Die Lösung musste während des laufenden Betriebs der bestehenden Plattform implementiert werden – inklusive eines klaren Migrationspfades für die Zukunft. Um einen klar regulierten Zugang zu vertraulichen Dokumenten sicherzustellen, bedurfte es überdies verbindlicher Benutzerrollen und Zugriffsrechte.

All dies konnte eine Third-Party-Identity-Lösung leisten. Sie war einfach zu implementieren und ermöglichte es dem Team, SSO und moderne Authentifizierungsfunktionalitäten zu nutzen. Das vorhandene System blieb online, während der Migrationsplan implementiert und umgesetzt wurde. Die Implementierung dauert nur einige Tage – während eine Inhouse-Lösung Monate in Anspruch genommen hätte. Die erstklassige Dokumentation mit detaillierten Code-Beispielen bietet einen einfachen Einstieg, deckt aber auch viele fortgeschrittene Themen ab. Dies half den Entwicklern von Bluetooth SIG, ihre neue Identity-Lösung vom ersten Tag an zu verstehen und effektiv zu nutzen. Gemeinsam mit Developer Success Engineers erarbeitete Bluetooth einen Proof of Concept, der die Features der Plattform präsentierte. Die Reaktionszeiten im Support waren kurz, und Anfragen konnten schnell bearbeitet werden.

Fazit

Innovation ohne Kompromisse

Moderne Identities zu managen, ist alles andere als einfach. Mit immer neuen Standards und Best-Practices Schritt zu halten und immer neue Security-Bugs zu beheben, kostet Zeit und Geld – Ressourcen, die dem Unternehmen an anderer Stelle fehlen. Achten Sie auf Funktionalitäten, die mit den Anforderungen Ihres Unternehmens wachsen, und informieren Sie sich darüber, wie andere Unternehmen ihre Lösungen evaluiert und implementiert haben. So können Sie von den Vorteilen einer zeitgemäßen IAM-Lösung profitieren, ohne Kompromisse bei der Sicherheit und Usability in Kauf zu nehmen oder Ihre Entwickler über Gebühr zu beanspruchen.

So wird Ihr CIAM von einem kritischen Angriffspunkt – und einem potenziellen Hindernis für Ihr Business – zu einem nachhaltigen Umsatz- und Wachstumstreiber. Mit Okta Customer Identity Cloud nimmt die Implementierung Ihres CIAM nur Tage statt Monate in Anspruch. So können Sie die einfachste, umfangreichste und erweiterbarste CIAM-Lösung auf dem Markt wählen – und in Ihrem Unternehmen die Weichen auf Zukunft stellen.

Wie Okta Sie unterstützen kann

Okta kann Ihnen helfen, die Identities Ihrer Kunden zu managen. Als Security-Experten bieten wir Ihnen eine Identity-as-a-Service (IDaaS)-Plattform, die eine breite Palette zeitgemäßer Security-Funktionalitäten unterstützt. Über 80.000 Entwickler in 167 Ländern setzen beim Management ihrer digitalen Identitäten auf die Okta Customer Identity Cloud.

Die Features und Vorzüge im Überblick:

- Konfiguration und Implementierung von Enterprise Federation und Single Sign-on mit minimalem Konfigurationsaufwand und ohne Coding.
- Enterprise-Schnittstellen zu Active Directory, LDAP, ADFS, SAML, Google Apps und mehr.
- Anbindung aller großen Social-Media-Provider wie LinkedIn, Facebook, Twitter, Google und vieler mehr.
- Klassische Authentisierung über Benutzername und Passwort via Auth0 DB oder individuelle Datenbanken, mit leistungsstarken Security-Features wie Multi-Faktor-Authentisierung, Erkennung kompromittierter Passwörter, Schutz vor Brute-Force-Angriffen und Anomalie-Erkennung.
- User können mit minimalem Aufwand von bestehenden Systemen migriert werden – ohne Passwort-Resets.
- Werkzeuge zur Auditierung und Auswertung von Identity-basierten Analysen, um die Einhaltung der Compliance sicherzustellen und Upselling-Potenziale zu identifizieren.
- Einfaches Management der User-Zugriffe mit feingranularer Rechtevergabe und leistungsstarken, individualisierbaren Regeln.
- Delegierte Administration ermöglicht die Verwaltung granularer Zugriffsrechte, mit lückenloser Transparenz und User-Management für Kunden.
- Mit Okta Customer Identity Cloud benötigt ein Entwickler weniger als 30 Minuten, um ein robustes und individuell anpassbares Identity-Management einzurichten – in jedem Technologie-Stack.

Informationen

Wenn Sie sich für weitere Kundenprojekte von Okta Customer Identity Cloud, vormals Auth0, interessieren, besuchen Sie die Seite „Unsere Kunden“, unsere Pricing-Seite oder wenden Sie sich an unser Vertriebsteam.