Whitepaper

Zelf ontwikkelen of kopen

Customer Identity and Access Management

Inhoudsopgave

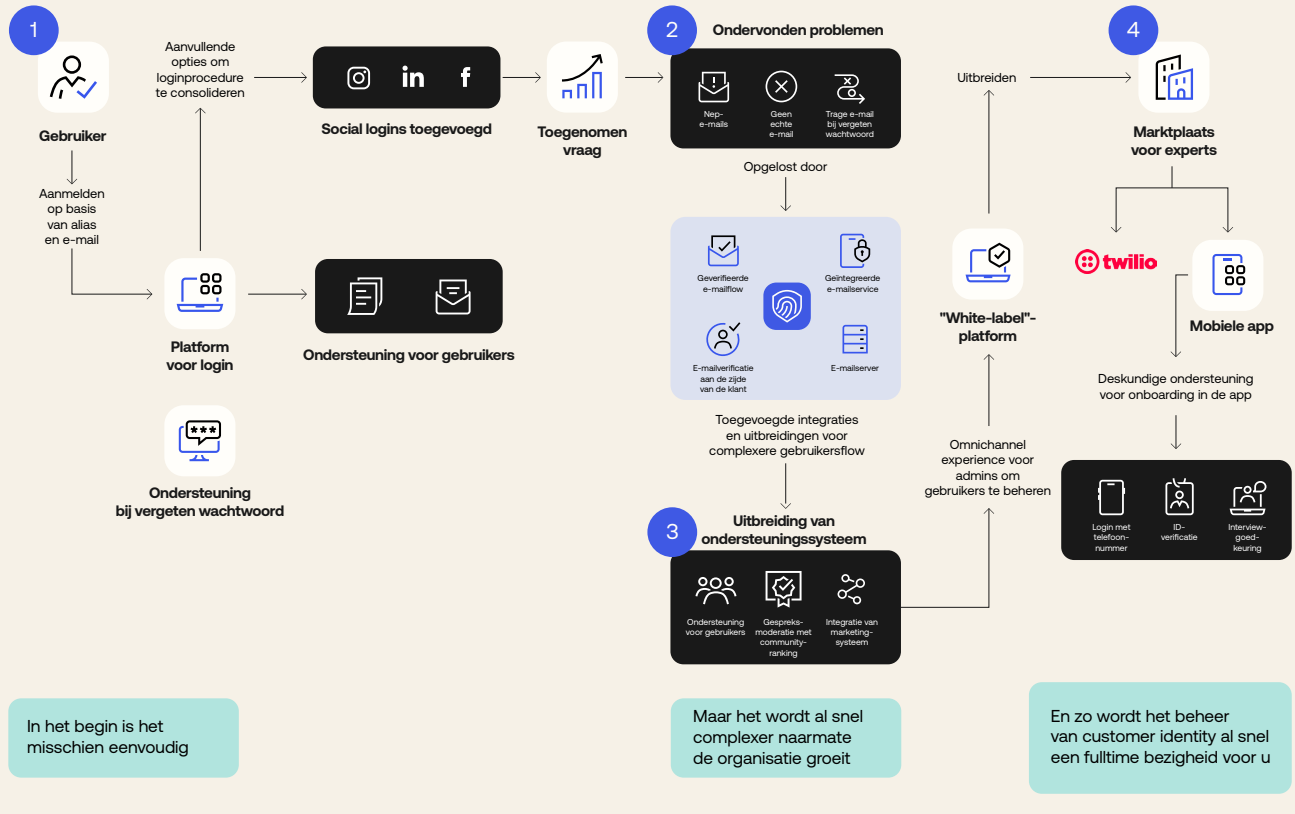
Het is niet eenvoudig om customer identity op de juiste manier aan te pakken

Teams die websites of mobiele apps ontwikkelen, worden bij elke nieuwe toevoeging geconfronteerd met hetzelfde dilemma: gaan we zelf bouwen of een kant-en-klare service gebruiken om het proces te vereenvoudigen en versnellen?

Onze developers kunnen customer identity wel op zich nemen. Het is maar een loginvenster. Hoe moeilijk kan het zijn?

Maar customer identity and access management (CIAM) is zo veel meer dan alleen een loginvenster. Naarmate organisaties groeien en nieuwe functies blijven toevoegen, kan het zijn dat de complexiteit van het beheer van een robuust, zelf opgezet CIAM-systeem een groter beslag legt op de resources dan aanvankelijk werd verwacht. Developer-uren zijn een waardevol goed. Tijd die wordt besteed aan het beheer van zelf ontwikkelde identity en security en de naleving van privacyregels kan niet worden besteed aan cruciale innovatie.

Zelf ontwikkelen is nog moeilijker...



Hoe kunt u innovatie bevorderen en de tijd van developers optimaal benutten zonder concessies te doen op het gebied van security, time-to-market en budget?

Een kant-en-klare CIAM kan uitkomst bieden. Een digitale identiteitslaag die bestaat uit API's, SDK's en kant-en-klare, aanpasbare componenten verschaft bouwblokken om de time-to-market te versnellen, de ontwikkelingskosten te verlagen en ervoor te zorgen dat interne developers zich kunnen concentreren op de kernfuncties van de applicatie. Applicaties voor klanten hebben allemaal een set basisfuncties voor authenticatie, autorisatie en user management. Ze moeten veelgebruikte workflows als accountaanmaak, gebruikers-login, wachtwoordresets, accountherstel en aanmelding voor multi-factor authenticatie (MFA) ondersteunen. Daarnaast moeten applicaties verschillende toegangsniveaus voor verschillende categorieën gebruikers aankunnen.

In deze whitepaper bespreken we met welke belangrijke aspecten u rekening moet houden wanneer u beslist of u zelf een systeem gaat ontwikkelen of er een gaat kopen en wat de voordelen zijn van een kant-en-klare oplossing.

> “Met [Okta] in onze toolkit weet ik dat we dingen sneller kunnen doen, omdat op het gebied van identity alles perfect onder controle is.”
>
> **Scott Howitt**
> CISO, MGM Resorts International

Een lagere total cost of ownership (TCO) bij de ontwikkeling van applicaties

Bij identity management is het risico van budgetoverschrijding hoog. De functies en het systeem zijn complex en constant in beweging, en worden maar al te vaak onderschat. Als u zelf een aanpak ontwikkelt, is het proces veel minder voorspelbaar. De kosten kunnen behoorlijk oplopen als interne teams zich volledig storten op de ontwikkeling van deep features voor gebruikers of ontdekken dat het landschap - en daarmee de vereisten - zijn veranderd. Teams kunnen dan misschien nog wel net op tijd leveren, maar alleen met de hulp van dure tijdelijke krachten. Wanneer u identity aan een betrouwbare provider uitbesteedt, verzekert u zich ervan dat het developmentteam het volledige project binnen het budget kan voltooien.

Voorbeeld TCO-verlaging bij applicatieontwikkeling1

3	x	6	x	$ 200.000	x	90%	=	$ 270.000
Developers		Identity-tijdlijn maand		Salaris inclusief premies e.d.		Verbetering		**TCO-verlaging**

> “Bepaalde aspecten van identity management veranderen bijna elk uur. We hadden een technologiepartner nodig die dat tempo kon bijhouden.”
>
> **Eash Sundaram**
> EVP Innovation, Chief Digital & Technology Officer,
> JetBlue Airways

[1] Veelgebruikte, Google-achtige berekening van de waarde van een engineer voor organisaties waar technologie de primaire aandrijver van omzet is. We berekenen hier de gemiddelde jaarlijkse bijdrage aan de omzet van een engineer en vermenigvuldigen dat bedrag met het aantal engineers dat niet beschikbaar is voor andere werkzaamheden omdat ze aan de levering van een identiteitslaag werken.

Resources richten op de kernfuncties van de applicatie
Uw succes wordt bepaald door de kwaliteit van de kernfuncties van uw applicatie, die het product nuttig maken voor eindgebruikers. Als u een moderne identiteitslaag heeft, kunt u zich volledig richten op de functies die omzet en klantenbinding genereren. Bovendien kunnen uw developers sneller beginnen aan de tweede, derde of vierde app waar uw klanten om vragen.

Het risico van een security- of compliance-lek verlagen
Wanneer heeft uw team het hashing-algoritme voor wachtwoorden het laatst bijgewerkt? De meeste aanvallen zijn gericht op data van gebruikers en PII, maar de gemiddelde levensduur van een effectief versleutelingsalgoritme bedraagt 18 maanden. Aan de bescherming van gebruikers wordt vaak minder prioriteit toegekend dan aan aspecten die de groei of omzet bevorderen. Bovendien moet uw team voor een goed beveiligde identity-service beschikken over gespecialiseerde kennis - en voldoende tijd - om de kwetsbaarheden in elke laag van de infrastructuur aan te pakken, van het besturingssysteem, de database en de transportlaag tot aan de applicatiestack en kwetsbaarheden in de code. Developmentteams beschikken vaak niet over dit niveau van security-expertise en in veel gevallen zullen ze pas opmerken dat hun user security gefaald heeft als er al gevoelige gegevens zijn gelekt. Bovendien zijn ze zich vaak niet bewust van ontwikkelingen op het gebied van security, bijvoorbeeld wanneer een algoritme wordt gehackt of een aanvalsvector wordt ontdekt.

Met een goed gekozen identity management-service kunt u de data van uw gebruikers beschermen tegen aanvallen. Zo'n service is namelijk ontwikkeld door experts die geavanceerde security toepassen om aanvalsvectoren op het gebied van identity en toegang af te dekken. Voorbeelden van security-maatregelen zijn krachtige versleuteling, API-security, geavanceerde firewall-bescherming en solide procedures voor datamanagement en systeemtoegang. Met deze security-maatregelen en -infrastructuur kunnen uw teams voldoen aan regio- en sectorspecifieke regelgeving zoals HIPAA, FedRamp en de AVG.

> “De National Bank of Canada bedient miljoenen cliënten in honderden filialen in heel Canada. Als organisatie hebben we duidelijke doelstellingen. Eén daarvan is het vereenvoudigen van de customer experience. Met de slimme authenticatie- en contextuele mogelijkheden van Okta kunnen we onze klanten een soepele, goed beveiligde online experience bieden.”
>
> **Rish Tandon**
> CTO, Heal

Developers gemotiveerd houden

Identity is belangrijk voor het succes van applicaties voor klanten, maar niet alle developers vinden het leuk om identity- en security-infrastructuur te ontwikkelen. Ondanks dat het een zeer complex en risicovol werkgebied is, wordt user management soms toch gezien als een routinekwestie. Veel developers houden zich liever bezig met de differentiatie van het kernproduct en hypermoderne systemen. Met name de hoge overhead die gepaard gaat met de implementatie van user security kan demotiverend werken. Het risico is hoog en richtlijnen spreken elkaar vaak tegen. Het werken met moderne REST-JSON-API-services vinden veel developers daarentegen wel interessant en toegankelijk.

Optimale schaalbaarheid en betrouwbaarheid

Wanneer user management fout loopt, kunnen gebruikers niet inloggen. Als eindgebruikers niet kunnen inloggen omdat het systeem niet beschikbaar is, weten ze niet waardoor dat komt. En dat maakt ze eigenlijk ook weinig uit: ze zullen hun perceptie van uw organisatie en merk onmiddellijk neerwaarts bijstellen. De vraag naar een online service is vaak onvoorspelbaar en marketingafdelingen weten of communiceren niet altijd wanneer een actie heel veel bezoekers zal trekken. Als u besluit dit zelf te regelen, moet u erop kunnen vertrouwen dat uw team een optimale beschikbaarheid kan garanderen en kan opschalen naarmate het aantal gebruikers groeit. Mogelijk moet u dubbele of driedubbele capaciteit beschikbaar hebben in uw datacenter of samenwerken met een infrastructure-as-a-service-aanbieder om pieken op te vangen. U moet garanderen dat upgrades en onderhoud soepel verlopen en de service niet verstoren. Organisaties die besluiten deze enorme verantwoordelijkheid op zich te nemen, komen vaak tot de conclusie dat de onderhoudsoverhead niet te beheersen is. Een externe user management-serviceprovider kan deze operationele knelpunten volledig wegnemen.

> “Een optimale integratie in het ecosysteem, een consequente toepassing van identity in verschillende systemen en een centrale rol voor identity in onze interactie met klanten, met een hoge mate van betrouwbaarheid en beschikbaarheid: dat was waar het ons allemaal om ging.”
>
> **James Fairweather**
> Senior Vice President of E-Commerce and Technology, Pitney

De voordelen van het aanschaffen van een customer identity and access management-systeem

Er zijn overtuigende argumenten voor het aanschaffen van identity management in plaats van zelf een systeem te ontwikkelen:

Meer omzet door een snellere time-to-market van apps
De behoeften van klanten veranderen constant. Als organisaties vandaag de dag geen omzet willen mislopen, moeten ze flexibel genoeg zijn om kansen op de markt te kunnen benutten. Een geschikte customer identity-oplossing fungeert als identiteitslaag voor veilige customer experiences. Uw developmentteam hoeft het wiel niet opnieuw uit te vinden als het gaat om authenticatie, autorisatie en user management. Uw developers kunnen zich dan richten op het ontwikkelen van functies die uw app uniek maken, en deze zo snel mogelijk bij de consument krijgen. En als we het over omzet hebben, gaat het niet alleen om het veiligstellen van omzet, maar ook om het genereren van nieuwe omzet. Schaalbaarheid speelt dus ook een rol. Resource-intensieve acties zoals authenticatie, wachtwoordversleuteling en zoekopdrachten moeten tijdens pieken kunnen voldoen aan de vraag van gebruikers.

Verlaging van de engineering-kosten
De implementatie van een identity management-oplossing van derden is eenvoudig. In veel gevallen hoeft alleen een knop te worden omgezet om nuttige functies in te schakelen. Dit betekent dat uw developers honderden - of misschien wel duizenden - uren overhouden om aan zakelijke logica te besteden in plaats van aan de ontwikkeling van authenticatie. De tijd die nodig was voor het testen en de security voor authenticatie, kan nu worden besteed aan kernaspecten van de app. Het integreren en in kaart brengen van identity providers is tijdrovend en kan problematisch zijn. Als u een geschikte oplossing van een derde partij kiest, zijn deze integraties al opgezet en kunt u ze gelijk gebruiken. Een kant-en-klare CIAM-oplossing moet ook SDK's bevatten voor populaire development-stacks, waardoor er nog minder programmeerwerk nodig is om het authenticatiesysteem te integreren. Het engineering-team van de organisatie kan zich dan concentreren op de configuratie in plaats van op programmeertaken en aanpassingen.

Sterkere security
wanneer heeft uw team het hashing-algoritme voor wachtwoorden het laatst bijgewerkt? De meeste aanvallen zijn gericht op data van gebruikers en PII. De gemiddelde levensduur van een effectief versleutelingsalgoritme bedraagt 18 maanden, maar vaak wordt meer prioriteit toegekend aan de bevordering van groei of omzet dan aan de bescherming van gebruikers. Een CIAM-oplossing zorgt ervoor dat de data van gebruikers veilig worden opgeslagen en verplaatst, en dat wordt voldaan aan regionale voorschriften en certificeringen op het gebied van compliance. Daarnaast biedt een CIAM-oplossing federatieve identity, zodat gebruikers niet onverstandig handelen, bijvoorbeeld door hetzelfde wachtwoord opnieuw te gebruiken om geen grote hoeveelheden inloggegevens te hoeven onthouden.

Casestudies uit verschillende branches

Schneider Electric: groei bevorderen met uniform identity management
Schneider Electric, wereldleider op het gebied van het beheer en de automatisering van energie met meer dan 170.000 medewerkers in meer dan 100 landen, had een identity management-strategie nodig die de volgende groeifase van de organisatie kon ondersteunen en tegelijkertijd een optimaal efficiënt gebruik van resources garandeerde. Bij de keuze voor een CIAM was een single sign-on-systeem voor een uniform authenticatieproces voor Schneider Electric een absolute prioriteit. Op die manier zouden dezelfde identities en inloggegevens kunnen worden gebruikt voor alle systemen en applicaties van de organisatie.

Uit een kosten-batenanalyse kwam duidelijk naar voren dat het beter was voor Schneider Electric om zijn eigen medewerkers te laten werken aan de kerndoelen en -doelstellingen van de organisatie. Met een identity management-systeem van derden konden barrières binnen de organisatie worden weggenomen en lastige identity-integratieproblemen worden opgelost. De Okta Customer Identity Cloud (voorheen Auth0) was bovendien een solide, flexibele en eenvoudig te integreren oplossing met een focus op de developer. Het platform was geschikt voor web en mobiel, ondersteunde open standaarden en bevatte solide, toekomstbestendige functies met ondersteuning van een groot aantal identity providers en een eenvoudige migratie.

De selectie en implementatie van Okta CIC leverden allerlei voordelen op. Door de identity management-oplossing waren er geen extra developmentwerkzaamheden meer nodig. Zo konden meer resources worden besteed aan IT-innovatie. De time-to-market kon worden verkort, het systeem was beter beveiligd en er werden best practices toegepast. Okta CIC maakte het ook mogelijk snel en grondig te reageren op kwetsbaarheden.

“Voordat de nieuwssites verslag uitbrachten over het Heartbleed-lek, had Auth0 [nu Okta Customer Identity Cloud] ons al een e-mail gestuurd om ons te waarschuwen voor deze zero day-kwetsbaarheid. Er was ook al een patch om het Heartbleed-gevaar uit de Auth0-systemen te weren. Vervolgens ontvingen we een bevestigingsmail dat Auth0 deze patch had geïnstalleerd op de instantie van Schneider Electric van de Auth0-service.

Dankzij Auth0 kan ons platformteam ook een goede indruk maken. Het beveiligingsprobleem werd in dit geval niet alleen gecorrigeerd, maar ons IT-team kon ook waardevolle tijd besparen omdat het de gedetailleerde informatie over de manier waarop de problemen waren gecorrigeerd, direct kon doorgeven aan ons interne team. Bovendien heeft Auth0 de certificaten omgewisseld, iets dat het team enorm veel werk opgeleverd zou hebben.

Met het Auth0-platform kunnen we identity-architectuur in een vroeg stadium plannen en integreren om cruciale tijd te besparen en te waarborgen dat er een veilig systeem actief is wanneer een project van de grond komt.”

Stephen Berard
Senior Global Software Architect, Schneider Electric

Bluetooth: uniforme Identity voor on-prem en cloud-apps
Het ecosysteem van Bluetooth, wereldleider op het gebied van wireless technologie, groeide. En dat bracht diverse uitdagingen met zich mee. De organisatie, die met één applicatie begon, had al snel diverse verschillende apps. Voor de intern ontwikkelde apps en SaaS-apps van derden (Sharepoint, ServiceNow, SiteCore) waren allemaal andere inloggegevens nodig. De eigen oplossing die Bluetooth gebruikte was gebaseerd op formulieren en maakte gebruik van gebruikersnamen en wachtwoorden. Dit platform was niet geschikt voor federatieve identity. De organisatie had een moderne identity-oplossing met single sign-on nodig om haar eigen apps en alle SaaS-apps van derden te ondersteunen. Tijdens de implementatie van de oplossing moest het bestaande platform blijven functioneren. Daarna zou er een volledige migratie plaatsvinden. Gebruikersrollen en toegang waren bovendien cruciaal om een passend niveau van toegang te garanderen tot vertrouwelijke documenten.

Het uitbesteden van identity was dus de beste optie. Dit was eenvoudig te implementeren en stelde het team in staat SSO en moderne authenticatie toe te voegen. Het legacy systeem bleef gewoon werken terwijl een migratieplan werd geïmplementeerd en uitgevoerd. Het hele proces kon in een paar dagen worden voltooid. De ontwikkeling van een eigen platform zou maanden hebben gekost. Dankzij de hoogwaardige documentatie over elementaire en gevorderde onderwerpen, met gedetailleerde codevoorbeelden, konden Bluetooth SIG-engineers de moderne identity-oplossing snel doorgronden en implementeren. Bluetooth werkte samen met developer success-engineers aan een proof-of-concept om de mogelijkheden van het platform gezamenlijk te presenteren. De responstijd van support was kort en de doorloopsnelheid hoog.

Conclusie

Innovatie zonder compromissen
Het beheer van moderne identity is een hele uitdaging. Het bijhouden van veranderende normen en best practices en het constant corrigeren van security-bugs kosten tijd en geld. Tijd en geld dat geïnvesteerd zou kunnen worden in de kernprocessen van de organisatie. Door functies te kiezen die kunnen meegroeien met de behoeften van uw organisatie en te zien hoe andere organisaties hun eigen oplossingen hebben geëvalueerd en geïmplementeerd, kunt u de vruchten plukken van een identity management-oplossing zonder compromissen te doen op het gebied van security en user experience, en zonder uw developers extra te belasten.

Uw organisatie kan ervoor zorgen dat CIAM geen kritiek, risicovol onderdeel is dat het zakendoen belemmert, maar een systeem waarmee de omzet niet alleen kan worden veiliggesteld, maar zelfs kan worden verhoogd. Met Okta Customer Identity Cloud kunt u CIAM in een paar dagen in plaats van in een paar maanden implementeren en uw organisatie toekomstbestendig maken door de eenvoudigste en meest uitgebreide en uitbreidbare CIAM-oplossing te gebruiken.

Hoe we kunnen helpen

Okta help u de identity van gebruikers te beheren. Als security-experts hebben we een identity-as-a-service (IDaaS)-platform opgezet dat is gebaseerd op hypermoderne security. Meer dan 80.000 developers in 167 landen gebruiken Okta Customer Identity Cloud als identity management-oplossing.

Een paar van de mogelijkheden en voordelen:

- de mogelijkheid om enterprise federation en single sign-on eenvoudig te configureren en implementeren zonder te programmeren
- enterprise-koppelingen als Active Directory, LDAP, ADFS, SAML, Google Apps en meer
- social media-koppelingen met alle grote providers, waaronder LinkedIn, Facebook, Twitter, Google en vele andere
- traditionele authenticatie aan de hand van gebruikersnaam en wachtwoord via de Auth0-DB of een DB op maat, met geavanceerde beveiligingsopties als multi-factor authenticatie, detectie van gelekte wachtwoorden, bescherming tegen brute force-aanvallen en detectie van onregelmatigheden
- mogelijkheid om gebruikers moeiteloos te migreren vanuit bestaande systemen, zonder wachtwoordresets
- methoden om op identity gebaseerde analytics te bekijken en controleren om compliance van de organisatie te garanderen en upsell-kansen te benutten
- eenvoudig beheer van gebruikerstoegang voor organisaties, met fijnmazige toegangsrechten en effectieve regels op maat
- gedelegeerd beheer, waarbij organisaties de toegang, zichtbaarheid en gebruikers gedetailleerd kunnen beheren voor klanten
- mogelijkheid voor developers om in minder dan 30 minuten een robuust, aanpasbaar identity management op te zetten voor elke willekeurige technologiestack

Resources

Bent u benieuwd hoe andere organisaties Okta Customer Identity Cloud (voorheen Auth0) beoordelen? Ga dan naar onze klantenpagina, onze pagina met tariefinformatie of neem contact op met sales.