Whitepaper

Security en customer experience in balans brengen met CIAM

Security is voortdurend aan verandering onderhevig, maar een krachtige CIAM-oplossing brengt uw behoeften en die van uw klanten in balans.

Heeft u de voordeur op slot gedaan?

De voordeur is de plek waar vaak van alles tegelijk gebeurt: u worstelt met een beker koffie, de kinderen en tassen en ondertussen probeert de kat ook nog naar buiten te glippen. Het kan zomaar gebeuren dat u in alle drukte vergeet de deur op slot te doen. En dat is heel begrijpelijk, want sommige dagen zijn gewoon hectisch.

Op het werk is het vaak niet anders. U zit midden in een sprint, de nieuwste resultaten van de klantfocusgroep zijn binnen, uw projectmanager wil een afspraak inplannen tijdens de lunchpauze en u bent bijna te laat voor de stand-upvergadering. Ook andere factoren spelen een rol, zoals de lange nasleep van de coronapandemie en de digitale transformatie die in alle sectoren van de economie in een ongekende stroomversnelling is geraakt.

Uit een onderzoek van Twilio blijkt dat de combinatie van eerdere initiatieven op dat gebied en de gevolgen van de pandemie ertoe hebben geleid dat bij veel organisaties de transformatie met gemiddeld 6 jaar is versneld (in sommige sectoren zelfs bijna 10 jaar). Maar liefst 97% van de ondervraagde besluitvormers bij grote ondernemingen is van mening dat de pandemie heeft gewerkt als katalysator van de transformatie. Als u de snelle omnichannel-adoptie bij uw klanten in goede banen wilt leiden, is het raadzaam bij uw volgende release over te stappen op één uniform user management-systeem.

Met een Customer Identity and Access Management (CIAM)-oplossing kunt u vanaf één centrale locatie gebruikers onboarden en accounts en data ordenen en beheren.

De loginpagina is de voordeur voor uw klanten. Dit is het eerste wat ze zien en daarom is het belangrijk dat de loginprocedure een aantrekkelijke gebruikerservaring biedt. Maar het is ook het eerste doelwit waar hackers zich op richten op zoek naar een kwetsbaarheid om uw data te stelen. De loginprocedure moet dus niet alleen aantrekkelijk, maar ook veilig zijn. Hoe veilig, dat bepaalt u zelf. Laat u de deur op een kier staan om alle gasten welkom te heten? Of voegt u een nachtslot en deurketting toe zodat iedereen eerst moet aanbellen en vervolgens moet wachten tot iemand opendoet? Te weinig security en iedereen kan binnenkomen; te veel security en niemand wil meer binnenkomen. Met andere woorden, het is continu balanceren tussen security en customer experience.

Met een Customer Identity and Access Management (CIAM)-oplossing kunt u vanaf één centrale locatie gebruikers onboarden en accounts en data ordenen en beheren. Een krachtige CIAM-tool biedt daarnaast verschillende securitymaatregelen waarmee u de data van uw klanten veilig kunt opslaan zonder te veel frictie aan de user experience toe te voegen.

Het komt er simpelweg op neer dat meer frictie leidt tot minder conversies. Of het nu om een nieuwe gebruiker gaat die het na de derde CAPTCHA-controle voor gezien houdt, of een goede vaste klant die de omslachtige procedure voor het resetten van wachtwoorden niet ziet zitten. Dit soort frictie tijdens het inloggen en resetten is er in veel gevallen de oorzaak van dat gebruikers het proces afbreken en uw organisatie voortaan links laten liggen. Vaak nemen ze ook nog hun vrienden mee, waardoor uw merk op de lange termijn nog meer schade oploopt.

CIAM werkt als uw digitale voordeur en neemt een unieke positie in op het kruispunt van security, privacy en gebruiksgemak. Het kan een lastige opgave zijn om de juiste combinatie van deze drie factoren te vinden die past bij uw product en uw klanten. Daar komt nog bij dat het bouwen van een eigen oplossing veel tijd kost; tijd die uw developers beter aan hun normale werkzaamheden kunnen besteden. De leden van uw developmentteam zijn experts op hun eigen vakgebied en zouden hun talenten moeten gebruiken om uw kernproduct verder te ontwikkelen en te optimaliseren. Zou het niet beter zijn om de login-experience en data-security van uw klanten uit te besteden aan de experts op het gebied van identity management?

Als u een speciale SaaS-oplossing voor identity management gebruikt, kunnen uw developers zich op hun eigen taken richten en bent u er zeker van dat al het mogelijke wordt gedaan om de informatie van uw klanten te beveiligen. En dat is cruciaal voor het opbouwen van vertrouwen in uw merk. Volgens het 2020 Edelman Trust Barometer-rapport kijken veel mensen bij de aankoop van een artikel op de eerste plaats naar de prijs, maar nemen vertrouwen en merkreputatie een gedeelde tweede plaats in beslag.

CIAM optimaliseert security, privacy en gebruiksgemak

De snelheid van de digitale transformatie neemt in alle sectoren steeds verder toe. Maar dat geldt ook voor het aantal cyberaanvallen dat op de klantgerichte perimeter wordt uitgevoerd. Geen wonder dus dat het beschermen van de merkintegriteit en -reputatie bij veel leidinggevenden bovenaan de agenda staat. Het beperken van de toegang tot de klantgerichte perimeter zou een prioriteit voor elke organisatie moeten zijn. Datalekken kunnen uw merkreputatie ernstig schaden, maar ook dramatische gevolgen voor uw winstcijfers hebben die nog jarenlang voelbaar zijn. Vanuit zakelijk oogpunt bekeken zou u nu alles in het werk moeten stellen om de aanvalsmogelijkheden tot een minimum te beperken.

Bij de meeste organisaties draait alles om conversies, toch? En aangezien frictie leidt tot minder conversies, is het logisch dat u frictie op de inlogpagina zoveel mogelijk moet voorkomen. Frictieloos inloggen kan uw conversiepercentage een enorme boost geven. Met een CIAM-oplossing kunt u de flow van de login-experience beheren, alsmede de data die nodig is om de experience na verloop van tijd aan veranderende behoeften aan te passen. U kunt de "schuifregelaars" voor security, privacy en customer experience afstellen op de combinatie die het beste past bij de behoeften van uw organisatie en de activiteiten van uw klanten. Zo creëert u precies het niveau van beveiliging dat u nodig heeft en kunt u de experience met weinig frictie bieden waar uw klanten om vragen.

CIAM biedt echter nog veel meer dan een soepele inlogprocedure. Een krachtige CIAM-oplossing combineert een frictieloze user experience met hoogwaardige bescherming tegen cyberaanvallen, optimale privacy voor gebruikersdata en intuïtieve beheerfuncties voor gebruikersaccounts.

CIAM beschermt tegen veelgebruikte aanvalsvectoren door de perimeterbeveiliging te versterken

Laten we eens een theoretische use case onder de loep nemen. Stel dat u de aanwezigheid van uw organisatie op het web wilt uitbreiden. Daarnaast heeft u onlangs een eCommerce start-up overgenomen én bent u bezig een ledenportal voor exclusieve eendaagse deals op te zetten als aanvulling op de bestaande webapps en webstores. Uw team moet al deze onderdelen met behulp van een nieuwe webapp in één uniforme interface onderbrengen. Dat is het ideale moment om een uitbreidbare, schaalbare CIAM-oplossing te integreren, zodat uw klanten met één set inloggegevens toegang kunnen krijgen tot alle onderdelen en de kwetsbaarheid voor aanvallen ook meteen een stuk kleiner wordt.

Een CIAM-oplossing die functies bevat zoals botdetectie, support bij herstel, integratie van multi-factor authenticatie (MFA) en log-streaming, kan de bescherming nog verder versterken. In de huidige wereld met gedistribueerde architecturen vormen identities de perimeter van een organisatie.

Een CIAM-oplossing moet daarom flexibel genoeg zijn om de groei van uw organisatie bij te houden én uw perimeter en data te beschermen. Uitbreidbaarheid, schaalbaarheid en partnerintegraties zijn daarbij van essentieel belang.

> CIAM kan uw identity-perimeter versterken door minimale wachtwoordvereisten te hanteren (waaronder policies voor hergebruik), de flow voor wachtwoordresets te stroomlijnen en MFA-opties te bieden.

Als één thema een centrale rol speelt bij veel aanvalsfactoren, dan is het wel het feit dat mensen hetzelfde wachtwoord voor meerdere accounts gebruiken. Uit een recent onderzoek van LogMeIn, de makers van wachtwoordmanager Lastpass, blijkt dat 91% van de gebruikers ervan op de hoogte is dat het hergebruik van wachtwoorden een beveiligingsrisico vormt, maar dat 66% toegeeft dit toch te doen. Een CIAM-oplossing kan u helpen de best practices op dit gebied te volgen. CIAM kan uw identity-perimeter versterken door minimale wachtwoordvereisten te hanteren (waaronder policies voor hergebruik), de flow voor wachtwoordresets te stroomlijnen en MFA-opties te bieden.

Geconsolideerde gebruikersdata is makkelijker te beschermen

Een single source of truth, of SSoT, is een data management-framework dat een ideale situatie creëert door alle relevante data van een organisatie op te slaan op één centrale locatie, in plaats van op meerdere afzonderlijke locaties. CIAM borduurt verder op dat concept door ook uw gebruikersdata en alle accountgegevens op één plek samen te brengen. Op deze manier maakt het niet uit op hoeveel platforms uw apps worden geïnstalleerd, want uw CIAM-oplossing kan alle gebruikersaccounts beheren en alle inkomende data naar dezelfde identity-SSoT dirigeren.

De toegang tot deze data kan nu veel eenvoudiger worden vergrendeld omdat er maar één locatie hoeft te worden beschermd. Gecentraliseerd beheer van gebruikersaccounts is ook belangrijk voor de compliance met belangrijke dataprivacywetten. Organisaties moeten bijvoorbeeld, zowel op grond van de AVG als de CCPA, op verzoek een kopie van de data van een gebruiker kunnen verstrekken, alsmede informatie over hoe die data wordt gebruikt. Deze vereisten gelden ook voor de systemen en data van partners.

Gelukkig biedt CIAM de eenvoudige toegang die u nodig heeft om de compliance te waarborgen en uw klanten tevreden te houden.

Een identity-SSoT verbetert ook de user experience. Als u single sign-on gebruikt kunt u records uit uw SSoT ophalen en hoeven uw klanten slechts één set inloggegevens te onthouden. Tevreden klanten blijven uw app gebruiken en dat betekent dat u ook minder last heeft van orphan accounts die na verloop van tijd kwetsbaar worden voor aanvallen. Het is een hele opgave om alle belanghebbenden tevreden te houden, maar met een modulaire CIAM SaaS-tool komt u wel een stap dichter bij dat ideaal.

Gestroomlijnde processen zorgen voor tevreden gebruikers

Klanten die een account aanmaken of bij een bestaand account inloggen, stellen vertrouwen in uw organisatie. Ze rekenen er ook op dat uw systeem een soepele customer journey biedt en niet allerlei hindernissen opwerpt die zelfs de meest geduldige klant tot wanhoop drijven. Als uw klanten zien dat het proces uit slechts een handvol intuïtieve stappen bestaat en dat ze na een snelle verificatie meteen hun nieuwe account in gebruik kunnen nemen, is dat het bewijs dat u hun vertrouwen waard bent.

Een goede CIAM-oplossing kan dit allemaal doen. Het aanmaken van een account hoort snel en soepel te verlopen, zodat nieuwe gebruikers zich welkom voelen en het duidelijk is dat uw procedures voor het verwerken van data veilig zijn. Volgens PwC laat maar liefst 32% van de klanten een organisatie al na één slechte experience links liggen. Ja u leest het goed. Een derde van de ondervraagden zou de relatie met een organisatie al na één onvriendelijke experience voorgoed verbreken. Wat zouden die mensen tegen hun vrienden zeggen als die slechte experience hun allereerste interactie met uw organisatie was? In het volgende gedeelte leest u waarom CIAM de ideale oplossing is voor alle processen en flows die verband houden met gebruikersaccounts.

Een vereenvoudigde user lifecycle is makkelijker te beschermen

Een gebruiker kan ook om een andere reden een nieuw account aanmaken. Bijvoorbeeld als diegene het wachtwoord vergeten is en de flow voor wachtwoordresets te omslachtig vindt. Dat heeft tot gevolg dat u daarna twee accounts voor dezelfde gebruiker moet beheren, omdat u niet weet dat het om een duplicaat gaat. Een volledig geïntegreerde CIAM-oplossing levert tijdens de hele lifecycle van de gebruiker belangrijke

security-voordelen op. Hieronder hebben we een aantal daarvan voor u op een rijtje gezet.

Accounts aanmaken

U wilt uiteraard voorkomen dat een gebruiker het aanmaken van een account vroegtijdig afbreekt. Daarom is het belangrijk om het proces zo frictieloos mogelijk te maken en toch de identiteit van de gebruiker te verifiëren. CIAM-oplossingen die single sign-on bieden doen precies dat. Als u een gebruiker de mogelijkheid biedt om in te loggen met een bestaand social netwerk-account kunt u profiteren van het feit dat de identiteit van de gebruiker al is geverifieerd. Bovendien kan de gebruiker in slechts enkele seconden een nieuw account aanmaken. Dit intuïtieve proces verkleint ook de kans dat een gebruiker hetzelfde wachtwoord opnieuw gebruikt, waardoor het account moeilijker te hacken is en de data beter beschermd is.

Accounts onderhouden

Automatisering is uw vriend als het gaat om het onderhoud van gebruikersaccounts. Een goede CIAM-oplossing biedt een geautomatiseerde flow voor wachtwoordresets, zodat dit veelgebruikte proces met zo weinig mogelijk frictie kan worden uitgevoerd. De volgende stap op weg naar een volledig accountbeheerplatform bestaat uit MFA-opties die de identiteit controleren van de persoon die inlogt. En met federatieve ID wordt een per ongeluk aangemaakt dubbel account direct gevonden en met het andere account in uw identity-SSoT gecombineerd. Dankzij de extra security die MFA biedt en het verwijderen van dubbele en orphan accounts wordt de kans op een datalek verder teruggedrongen.

Accounts beëindigen

Wat gebeurt er als gebruikers vergeten dat ze een account hebben? Of overstappen op een ander product en het account nooit meer gebruiken? In veel gevallen gebeurt er helaas niets. Maar als er niets aan dit slechte accountbeheer wordt gedaan, staat uw identity-SSoT binnen de kortste keren vol met vergeten, ongebruikte en overbodige accounts. En dan gaat het niet alleen meer om een onderhoudsprobleem, maar ook om een securityprobleem. De inloggegevens van dit soort accounts kunnen immers worden buitgemaakt in een datalek bij een andere organisatie en vervolgens worden gebruikt voor een aanval op uw systemen. U kunt deze veelvoorkomende aanvalsvector de pas afsnijden met geautomatiseerde accountfuncties, zoals het verzenden van e-mails naar accounts die een bepaalde tijd niet meer actief zijn geweest, het deactiveren van accounts en uiteindelijk het verwijderen van accounts.

Buitgemaakte inloggegevens worden gebruikt voor tal van aanvalsvectoren

Als de inloggegevens van een gebruiker bij een datalek zijn buitgemaakt, kunnen ze als gevolg van slecht wachtwoordgedrag steeds opnieuw worden gebruikt om toegang te krijgen tot talloze andere sites. Cybercriminelen kunnen zonder veel problemen gebruikersnamen en wachtwoorden in handen krijgen, ook als ze zelf niet technisch genoeg zijn om een database binnen te dringen.

Deze "script kiddies" kopen gewoon een combinatielijst met inloggegevens op het dark web en gebruiken vervolgens bestaande scripts of volwaardige applicaties (ook te koop op het dark web) om een systeem binnen te dringen via credential stuffing of een ander type brute force-aanval. Het is belangrijk dat u zich bewust bent van deze aanvalsvectoren en de werking ervan om uw CIAM-oplossing zo goed mogelijk te integreren voor uw specifieke use case.

Credential stuffing

Een van de meest voorkomende vectoren is momenteel de brute force-aanval, ook wel credential stuffing genoemd. Bij een dergelijke aanval beschikt de aanvaller over een lijst met gebruikersnamen en wachtwoorden en probeert deze simpelweg uit op de loginprocedures van andere sites. Het feit dat mensen vaak dezelfde wachtwoorden voor meerdere accounts gebruiken, maakt deze aanvalsvector zo aantrekkelijk voor kwaadwillenden. En het werkt blijkbaar nog vaak genoeg om de inspanning waard te zijn. Dit soort aanvallen maakt voornamelijk gebruik van de gemakzucht van mensen die eenvoudig te raden wachtwoorden voor meerdere accounts gebruiken (het meest gebruikte wachtwoord is momenteel "123456", op de voet gevolgd door "wachtwoord").

Business Email Compromise (BEC)

Buitgemaakte wachtwoorden kunnen ook de basis vormen voor andere aanvallen. Hackers kunnen bijvoorbeeld een combinatielijst kopen die speciaal gericht is op de organisatie die ze willen binnendringen. Met de inloggegevens van een bepaalde hogere leidinggevende en door gebruik te maken van spoofing kunnen ze gerichte phishingmails versturen (ook wel "spear fishing" genoemd) die daadwerkelijk van deze leidinggevende afkomstig lijken te zijn. De frequentie van dit soort aanvallen neemt toe als er ook bots worden ingezet, maar meestal wordt gebruikgemaakt van social engineering. Dit houdt in dat aanvallers inspelen op normale reacties van mensen (die in bepaalde situaties de veiligheid uit het oog verliezen).

Aanvallen van bots

Sommige hackers willen alleen maar de systemen van hun doelwit ontwrichten. Ze willen niets stelen, maar een punt maken door alle activiteiten tot stilstand te brengen en de chaos te zien die ontstaat terwijl de organisatie alles op alles zet om de aanval te stoppen en de gevolgen van de downtime te herstellen. Distributed denial of service (DDoS)-aanvallen komen het vaakst voor. De hacker maakt bij een dergelijke aanval gebruik van bots om een site te overspoelen met verkeer waardoor deze een bepaalde periode ontoegankelijk is voor normale bezoekers. Deze aanvallen en de daaruit voortvloeiende downtime veroorzaken zowel reputatieschade als financiële schade.

Bij een andere veelgebruikte aanval wordt gebruikgemaakt van zwermen bots. Een zwerm kan zich bijvoorbeeld op de loginprocedure van een eCommerce-site storten om de hele voorraad populaire producten in één keer op te kopen. Dit soort botzwermen werd onlangs gebruikt toen NVIDIA een nieuwe grafische kaart lanceerde waar gamers over de hele wereld met smart op zaten te wachten. Hetzelfde gebeurde toen Microsoft de Xbox X en Sony de lang verwachte PlayStation 5 op de markt brachten. De verwerkingscapaciteit van sites zoals Walmart en Amazon werd zwaar op de proef gesteld toen de hele voorraad werd opgekocht door honderdduizenden door bots aangemaakte accounts. Het doel van dit soort aanvallen is om de prijzen op de aftermarket op te drijven. Deze zwermscenario's leiden er toe dat zeer gewilde producten bijna niet meer verkrijgbaar zijn en dat legitieme gebruikers de site pas weer kunnen gebruiken als de aanval voorbij is. De getroffen organisatie blijft zitten met de financiële schade en de reputatieschade.

Hoe Okta veilige CIAM biedt

"Als u overweegt security aan te schaffen, moet u altijd eerst de risico's in kaart brengen. Een "one size fits all"-oplossing bestaat niet. U moet de juiste security-beslissingen nemen op basis van de specifieke risico's die gelden voor uw organisatie, uw klanten en uw gebruikers. Aan de hand daarvan kunt u uw security-controles aanscherpen of versoepelen. Op deze manier zorgt u ervoor dat u de security van uw product niet overdreven ingewikkeld maakt, wat een negatief effect op het gebruiksgemak zou kunnen hebben."

Duncan Godfrey
Vice President, Security Engineering, Okta

Duncan benadrukt dat security voortdurend aan verandering onderhevig is. De security-bedreigingen die in deze whitepaper zijn besproken, alsmede de bedreigingen die hackers nog aan het voorbereiden zijn, kunnen alleen worden bestreden met een combinatie van maatregelen. Bijvoorbeeld met een robuuste CIAM-oplossing die schaalbaar en uitbreidbaar is, zodat u security, privacy en customer experience precies in balans kunt brengen.

CIAM beheert de digitale voordeur van uw organisatie en is daarom bij uitstek geschikt om het voortouw te nemen bij de bescherming van de perimeter. De voordeur is immers de plek waar kwaadwillenden zich in eerste instantie op richten, maar het is ook de plek die klanten het eerst zien als ze een product willen kopen of een andere interactie willen uitvoeren. En het is bovendien de plek waar u de data van uw klanten beheert, analyseert en veilig opslaat.

Modulariteit wordt steeds meer de norm bij het samenstellen van apps. Momenteel worden SaaS-tools voor betalingen, berichten en authenticatiesystemen het meest geïntegreerd. Uit onderzoek van Auth0 blijkt dat authenticatie is vereist voor 83% van de moderne apps die worden ontwikkeld, maar dat slechts 58% van de respondenten aangeeft een externe SaaS-tool te gebruiken. Kortom, er zijn allemaal goede redenen om het leveren van de beste en veiligste CIAM-oplossing aan ons team over te laten, zodat uw developers zich volledig kunnen richten op het optimaliseren van uw kernproduct.

> Het securityteam moet over de allernieuwste informatie beschikken om aanvallen in een vroeg stadium op te sporen, de responstijd te verkorten en de enorme gevolgen van een datalek te voorkomen.

Open standaarden

CIAM-oplossingen zijn verkrijgbaar in verschillende soorten en maten, net zoals alle andere cybersecurity-tools. Een CIAM-oplossing kan bijvoorbeeld aan open standaarden voldoen, maar het kan ook een "black box"-oplossing zijn. Dat laatste betekent dat u afhankelijk bent van de leverancier omdat die als enige toegang heeft tot het backend van het systeem. Deze situatie wordt ook wel "vendor lock" genoemd. U kunt dit beter vermijden, zodat u flexibeler te werk kunt gaan bij uw security-implementaties en de oplossing eenvoudig kunt uitbreiden (zie hieronder).

Open standaarden zoals OAuth2, OpenIDConnect en SAML spelen ook een belangrijke rol in de wijze waarop de customer experience centraal wordt gesteld, zonder het perspectief van de developer uit het oog te verliezen. Als bezoekers binnen een paar seconden een nieuw account kunnen aanmaken met hun bestaande inloggegevens, levert dit een veel betere user experience op. Op deze manier hebben ze nog maar enkele sterke wachtwoorden nodig en kunnen ze erop vertrouwen dat hun data veilig is opgeslagen bij de eigen identity provider en niet over meerdere systemen wordt verspreid.

Uitbreidbaarheid

Als u flexibel wilt inspelen op de behoeften van uw klanten, is het belangrijk dat uw oplossing de mogelijkheid biedt om snel en frictieloos functies toe te voegen en aan te passen. Okta biedt hiervoor verschillende methoden, bijvoorbeeld met behulp van regels die uw gebruikers zelf kunnen instellen om precies de juiste balans te vinden. Met een regel kan bijvoorbeeld een trigger worden geactiveerd voor "onmogelijk traject"-scenario's. Stel dat een gebruiker die in Chicago woont lijkt te willen inloggen vanuit Brazilië. In dat geval kan voor de gebruiker in Brazilië een MFA-prompt worden geactiveerd, terwijl de gebruiker in Chicago (die al is geverifieerd) geen prompt ontvangt. Regels kunnen ook worden gebruikt om logins aan andere systemen door te geven, bijvoorbeeld voor het monitoren van gebeurtenissen of voor klantenservicedoeleinden.

Okta's partnerecosysteem biedt uw developers toegang tot een scala aan uitbreidingsmogelijkheden. Heeft u een functie nodig die nog niet is opgenomen in ons kernaanbod, dan is de kans groot dat die functie via een integratie met een marktleider beschikbaar is op onze Marketplace. U kunt bijvoorbeeld een integratie gebruiken als u toestemmingen moet beheren om aan de vereisten van nieuwe wetten en regels te voldoen.

Log-streaming

Een belangrijk kenmerk van een robuuste beveiligingsstatus is de mogelijkheid om data te gebruiken die door uw cybersecurity-tools wordt gegenereerd. Organisaties die over een data-infrastructuur beschikken, kunnen log-streaming gebruiken om data uit CIAM in real time door te sturen naar bestaande oplossingen, bijvoorbeeld een Security Information and Event Management (SIEM)-oplossing of een Security Orchestration, Automation and Response (SOAR)-oplossing. Dit is ook belangrijk om aan de meldings- en verwijderingsvereisten van de bovenvermelde gegevensbeschermingswetten te voldoen.

Okta's Marketplace biedt integraties met Splunk, Sumo Logic, Datadog en andere platforms. Maar uw team kan ook een integratie op maat bouwen met een van onze vele API's en SDK's. Het securityteam moet over de allernieuwste informatie beschikken om aanvallen in een vroeg stadium op te sporen, de responstijd te verkorten en de enorme gevolgen van een datalek te voorkomen.

Bescherming tegen brute force-aanvallen

Bij brute force-aanvallen in de meest eenvoudige vorm probeert een aanvaller met verschillende gangbare wachtwoorden toegang tot één gebruikersaccount te krijgen. Deze schijnbaar eenvoudige methode is nog steeds populair omdat aanvallers er nog steeds succes mee boeken. Als Okta meer dan 10 inlogpogingen op een bepaald account detecteert die afkomstig zijn van hetzelfde IP-adres, wordt dat adres door de brute force-bescherming geblokkeerd en kan dus geen toegang meer krijgen tot het betreffende gebruikersaccount (eventuele andere accounts op dezelfde locatie hebben nog wel toegang). Daarnaast stuurt Okta per e-mail een waarschuwing naar de gebruiker. De gebruiker kan de blokkering van het IP-adres vanuit die e-mail ongedaan maken of het wachtwoord wijzigen, waardoor de blokkering van het adres automatisch wordt opgeheven.

Botdetectie

Botdetectie is vaak de ontbrekende schakel die complexere credential stuffing-aanvallen een halt kan toeroepen. De botdetectie van Okta gebruikt data van de 4,5 miljard logins die we elke maand verwerken en combineert die informatie met analyses van risicosignalen. Zo kunnen we inlogpogingen identificeren die waarschijnlijk afkomstig zijn van een botnet of script, en vervolgens een CAPTCHA-stap in de flow introduceren. Uit onderzoek van Auth0 blijkt dat botdetectie de effectiviteit van een credential stuffing-aanval met maar liefst 85% kan terugdringen.

Voor legitieme gebruikers die inloggen vanaf een bekend goed IP-adres is deze toegevoegde security-stap niet nodig, en zo kan de frictie in de flow voor echte klanten tot een minimum worden beperkt. Het vinden van de juiste balans tussen security en customer experience wordt een stuk gemakkelijker als het beveiligingsrisico zoveel mogelijk wordt teruggedrongen en de frictie voor legitieme gebruikers zoveel mogelijk wordt beperkt.

Adaptieve MFA

Het National Institute of Standards and Technology (NIST) heeft MFA aangemerkt als best practice en raadt het gebruik ervan te allen tijde aan. En volgens industriegroep The Open Web Application Security Project (OWASP) biedt MFA "verreweg de beste bescherming tegen de meeste wachtwoord-gerelateerde aanvallen". Okta Adaptieve MFA tilt de user experience en datasecurity naar een hoger niveau met behulp van contextafhankelijke signalen, zoals locatie, unieke device-ID's en de tijd die is verstreken sinds de laatste login. Op basis van die gegevens wordt een risicoanalyse uitgevoerd op elke login van elke gebruiker en wordt alleen om aanvullende factoren gevraagd wanneer dat nodig is (zoals in het bovenstaande voorbeeld van een onmogelijk traject).

Passwordless authenticatie

Wachtwoorden kunnen veel problemen opleveren, dus misschien is het tijd om uw gebruikers de mogelijkheid te bieden om zonder wachtwoord in te loggen. Met Okta Passwordless kunt u dat heel eenvoudig realiseren. In plaats van wachtwoorden te gebruiken, stuurt u een eenmalige code per e-mail of sms naar de gebruiker. Als u geen wachtwoorden meer gebruikt, is uw organisatie ook veel minder kwetsbaar voor credential stuffing-aanvallen en andere vormen van misbruik van accounts. En als u een openbare API met rate limiters gebruikt is de gebruikersdata ook beschermd tegen geautomatiseerde aanvallen en botaanvallen.

CIAM biedt security en beheert de inlogfrictie

U en uw team hebben genoeg te doen om de volgende sprint tot een goed einde te brengen. Als u de trend van modulariteit en integratie van externe SaaS-oplossingen volgt wanneer dat mogelijk is, kunt u op snelle en veilige wijze een CIAM-oplossing implementeren. Met het toenemen van het aantal legitieme gebruikers groeit ook het aantal kwaadwillenden dat toegang tot uw data probeert te krijgen. Dat is een belangrijk gegeven als u goede security wilt bieden en de klanttevredenheid op peil wilt houden. Een CIAM-oplossing die inspeelt op deze dynamiek kan de bescherming op- en afschalen al naargelang het aantal gebruikers.

Organisaties besteden steeds meer aandacht aan de manier waarop ze hun digitale identities vormgeven. Het beheren van de customer experience vanaf de inlogpagina is essentieel voor het opbouwen van vertrouwde relaties.

Maak een schatting van de potentiële voordelen die Okta Customer Identity uw organisatie oplevert met onze ROI-calculator.