

Adaptive multi-factor authenticatie

Intelligente security voor al uw devices, apps en infrastructuur

Tegenwoordig breken hackers niet meer in, maar loggen ze in. De gestaag groeiende stroom op identity gebaseerde aanvallen toont duidelijk aan dat alle toegangspunten tot uw resources moeten worden beschermd, of het nu gaat om on-prem apps, cloudapps of zelfs infrastructuur. En daarbij moeten we vooral niet de applicaties vergeten die door uw klanten en door de klanten van uw klanten worden gebruikt. Okta's authenticatieproducten - adaptive multi-factor authenticatie en adaptive single sign-on - beschermen uw organisatie tegen datalekken door bij het verlenen van toegang ook naar de context te kijken. Deze producten passen een op risico's gebaseerde benadering toe en houden rekening met context, zoals device, gebruiker, gebruikersgedrag en locatie. Zo kan Okta alle toegangspunten tot uw resources optimaal beschermen.

Waarom Okta Adaptive MFA kiezen?

Flexibiliteit bij het beschermen van accounts

Okta beschermt de toegang tot data ongeacht waar die data is opgeslagen, waar uw gebruikers zich bevinden en op welke devices ze hun taken uitvoeren. Adaptive MFA is speciaal ontwikkeld om in alle omgevingen flexibiliteit te bieden. Deze oplossing beschermt cloudresources, on-prem VPN-, RDP- en SSH-sessies, alsmede op maat gemaakte web-apps en mobiele apps die worden gebruikt door uw werknemers, partners, klanten en consumenten.

Adaptive MFA

Adaptive MFA rekent af met bekende knelpunten bij het implementeren van een multifactor-oplossing:

1. Eén oplossing voor alle gebruikerstypen. Of u MFA en adaptive policies nu wilt instellen voor uw werknemers, of uw leveranciers, externen, klanten of consumenten, bij Okta zit u altijd goed. De policies kunnen worden toegepast op elke web-app of native mobiele app. U kunt Okta zelfs als authenticatieprovider gebruiken voor uw maatwerkapps.
2. Dynamische respons op basis van logincontext. Multi-factor authenticatie voegt niet zoveel toe als het resultaat alleen maar 'ja' of 'nee' kan zijn. Daarom dwingt Okta step-up authenticatie af als dat zinvol is gezien de historische context van de gebruiker die is gekoppeld aan het device, de locatie, het IP-adres en een hele reeks andere login-kenmerken.
3. Wachtwoorden worden minder belangrijk. Zelfs met een goede password policy zijn gebruikers nog steeds de zwakste schakel. Vervang de wachtwoorden van uw eindgebruikers daarom door een eenvoudige login-experience in combinatie met sterke authenticatiefactoren, zoals Okta Verify, biometrie en FIDO2.0-tokens.

Voordelen



Kies de factoren die het beste bij uw organisatie passen

Okta biedt standaard een breed scala aan multi-factor authenticatiemethoden. Daarnaast kunt u ook elke gewenste SAML- of OIDC-authenticatieprovider als factor gebruiken.



Bied gebruikers een veilige, passwordless login op elk device

Handhaaf device trust en neem afscheid van wachtwoorden door sterke factoren als primaire authenticatiemethode in te stellen, zoals Okta Verify of FIDO2.0.



Detecteer afwijkende logins met op risico gebaseerde authenticatie

Okta gebruikt een machine learning-model om afwijkingen in te delen in de categorieën hoog, normaal en laag. U kunt via op risico gebaseerde authenticatie een risiconiveau aan een bepaalde factor koppelen.



Voorkom grootschalige identity attacks met Okta ThreatInsight

Via Okta's netwerkeffect worden miljarden logins bij alle Okta-accounts geregistreerd. Admins kunnen op basis van de verzamelde informatie van ThreatInsight de toegang vanaf verdachte IP-adressen blokkeren nog voordat de authenticatie plaatsvindt, zodat account takeovers worden voorkomen en accounts van werknemers, klanten en consumenten niet onnodig worden vergrendeld.

Over Okta

Okta is een toonaangevende, onafhankelijke identity provider voor organisaties. De Okta Identity Cloud stelt organisaties in staat om de juiste mensen op het juiste moment veilig te verbinden met de juiste technologieën. Met meer dan 6500 applicatie-integraties kunnen klanten van Okta gemakkelijk en veilig de beste technologieën gebruiken voor hun organisatie.