okta

5 manieren om Zero Trust-adoptie te versnellen

IT- en securitymanagers geven steeds meer prioriteit aan een Zero Trust-securitystatus die is gebaseerd op identity en access management. Ontdek hoe Zero Trust u helpt uw hybride werkende medewerkers te beveiligen, uw organisatie tegen het stijgende aantal cyberbedreigingen te beschermen en de stap naar schaalbare cloudtechnologie te zetten.

99% **van de organisaties over de hele wereld vindt dat identity management van groot of cruciaal belang is voor hun Zero Trust-securitystrategie**

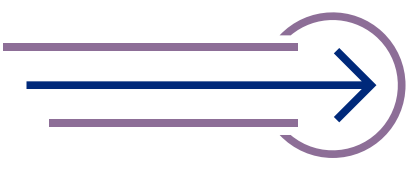
Bron: The State of Zero Trust Security 2021, Okta

1 Stroomlijn de digitale transformatie

Organisaties willen hun journey naar de cloud versnellen, maar het bieden van secure access kan een langdurig en omslachtig proces zijn. Veel IT-managers kiezen daarom voor een modern identityplatform dat standaard integraties met bedrijfskritische apps biedt, zodat ze de tools en platforms die werknemers nodig hebben snel en probleemloos kunnen beveiligen en implementeren.

97% **van de besluitvormers bij grote ondernemingen denkt dat de pandemie de digitale transformatie heeft versneld**

Bron: COVID-19 Digital Engagement Report, Twilio



2 Beveilig hybride werkende medewerkers

Werknemers gaan er tegenwoordig vanuit dat ze mogen werken op plekken waar ze zich prettig en productief voelen. Een moderne identity-oplossing kan de toegangscontroles voor alle cloud- en on-prem apps samenvoegen, zodat alle gebruikers op snelle en veilige wijze toegang kunnen krijgen tot alle resources die ze nodig hebben, waar en wanneer ze die nodig hebben.

89% **van de werknemers wil het liefst ten minste een deel van de tijd remote werken**

Bron: PwC, Global Workforce Hopes and Fears Survey 2022

3 Dring de meest voorkomende cyberbedreigingen terug

In hun haast om aan de behoeften van remote en hybride werkende medewerkers te voldoen, hebben veel organisaties vergaande concessies aan de security gedaan in ruil voor continuïteit. Maar door moderne identitytools (zoals MFA en SSO) te adopteren, kunnen organisaties de frictie van het gebruik van wachtwoorden snel wegnemen en de veerkracht op de identiteitslaag versterken.

61% **van de cyberaanvallen in 2021 is terug te voeren op gestolen of zwakke inloggegevens**

Bron: 2022 Data Breach Investigations Report, Verizon

4 Hyperautomatiseer handmatige provisioningprocessen

Het handmatig implementeren van apps verhoogt het risico op datalekken die het gevolg zijn van menselijke fouten. Organisaties die overstappen op cloudtechnologie kunnen de cyberveerkracht aanzienlijk verbeteren. Zo verdwijnt een groot deel van de risico's als sneeuw voor de zon door de provisioning te hyperautomatiseren met behulp van identity management. Bovendien houden IT-teams meer tijd over om zich te richten op het versterken van de security elders in de organisatie.

88% **van de datalekken in 2021 is terug te voeren op misbruik van inloggegevens**

Bron: 'Why Do People Make Mistakes?', Tessian

5 Bescherm zowel apps als API's

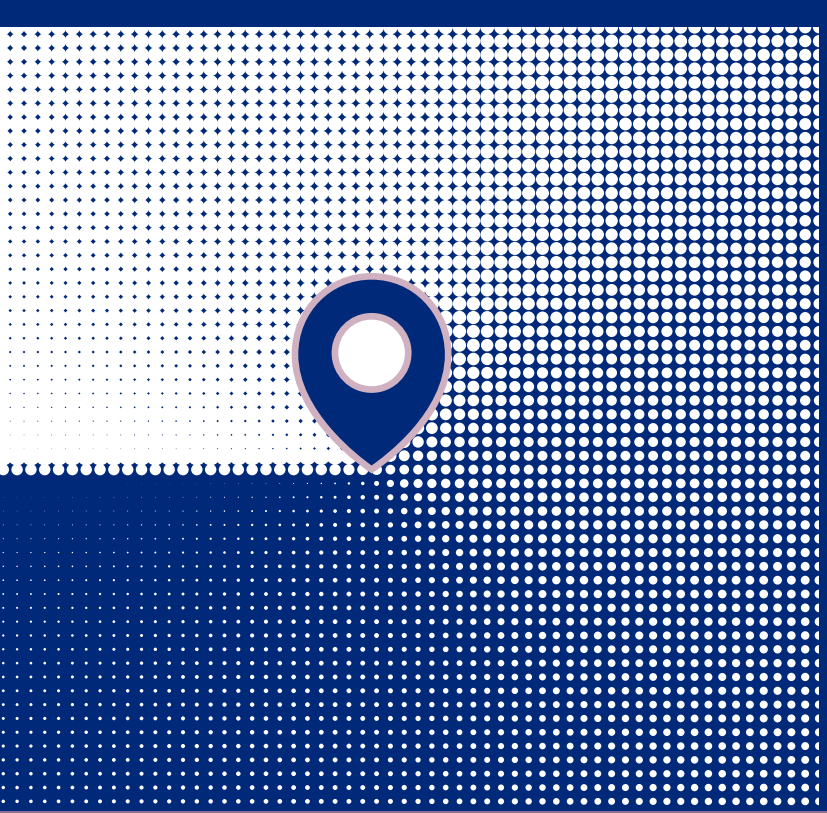
De juiste identity provider biedt niet alleen bescherming voor apps, maar ook veelzijdige toegangscontroles voor alle technologieën die werknemers gebruiken. Bijvoorbeeld secure access voor de vele API's die als bouwstenen voor moderne applicaties worden gebruikt, maar die gevoelige data vaak onvoldoende bescherming kunnen bieden.

Het aantal API-aanvallen is gestegen met

681%

in de afgelopen 12 maanden

Bron: State of API Security Report 2022, Salt



Waar u moet beginnen met uw Zero Trust-journey

Wilt u meer weten over hoe identity management uw ambities op het gebied van Zero Trust-security kan versnellen? Of weet u niet zeker waar u staat in uw Zero Trust-journey en wat uw volgende stap moet zijn? Bekijk de videopodcast met Brian Glick (hoofdredacteur van Computer Weekly) en Ian Lowe (van Okta).

Videopodcast bekijken