Mobilizing a Zero Trust Security Model: SMBs Are Charting a New Course

okta

Introduction

Companies of all sizes have realized that to thrive in the digital economy, their systems, services, and employees need to be securely connected. And with today's growing distributed workforce, they know that relying on the corporate network perimeter isn't a viable security strategy.

This revelation didn't just arise with the rapid shift to remote work brought on by the COVID-19 pandemic, although that did encourage many organizations to move more quickly on these strategies. From enterprises to small and medium-sized businesses (SMBs), companies have been moving towards a more distributed model for some time, and many are advancing with decisiveness and speed toward a Zero Trust security model.

What is Zero Trust?

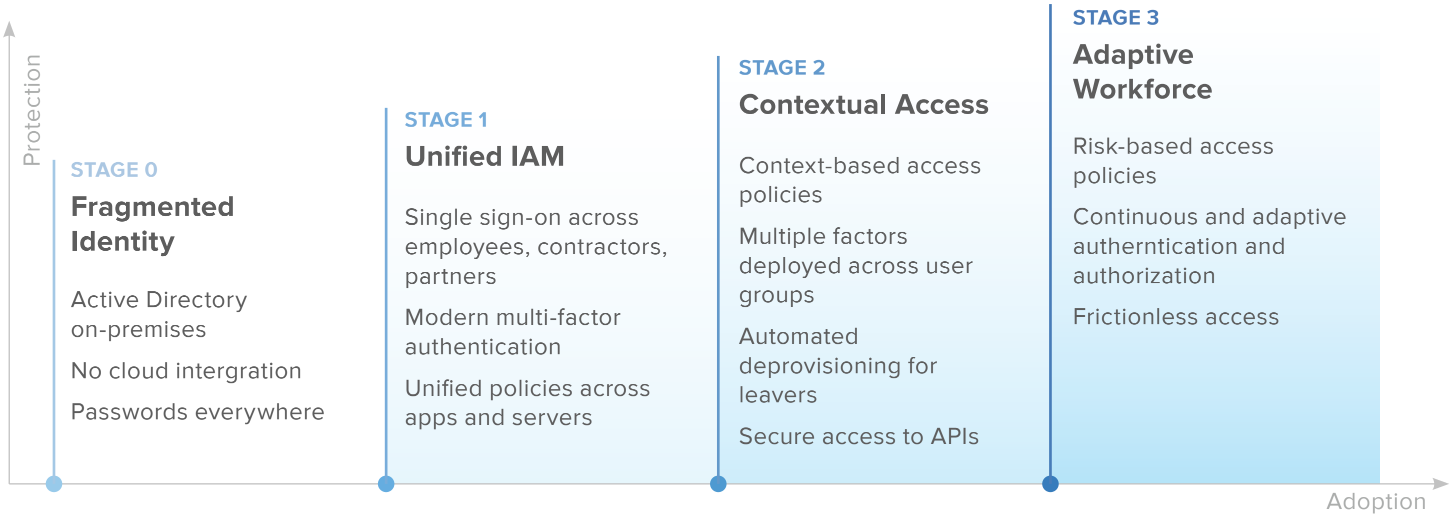
At its core, the concept of Zero Trust is simple: there should no longer be a trusted internal network and an untrusted external network. Instead, all network traffic needs to be considered untrusted, and organizations should operate on the principle that every single user or device that wants access to their data needs to be verified. Only then can information and infrastructure be as protected as possible.

Zero Trust was originally coined by Forrester Research analyst John Kindervag over a decade ago. But as organizations, workforces, and networks become increasingly distributed, it has never been more applicable than it is at this moment—and it will continue to be the security strategy of choice for the foreseeable future.

Today, 67% of SMBs have a Zero Trust security initiative in place, or have it planned for the next 12 to 18 months. Additionally, a large number of these companies have already adopted identity and access management (IAM) as a central component of their security framework. At a fundamental level, that means they authenticate and authorize logins based on whether or not the request comes from a recognized source.

Since the Zero Trust security model is founded on the principle that all users are untrusted until proven otherwise, IAM is a critical first step in building a modern security framework—it's why we measure companies' preparedness on Okta's identity and access management maturity curve.

Identity and Access Maturity Curve



STAGE 0

Fragmented Identity

Active Directory on-premises

No cloud intergration

Passwords everywhere

STAGE 1

Unified IAM

Single sign-on across employees, contractors, partners

Modern multi-factor authentication

Unified policies across apps and servers

STAGE 2

Contextual Access

Context-based access policies

Multiple factors deployed across user groups

Automated deprovisioning for leavers

Secure access to APIs

STAGE 3

Adaptive Workforce

Risk-based access policies

Continuous and adaptive autherntication and authorization

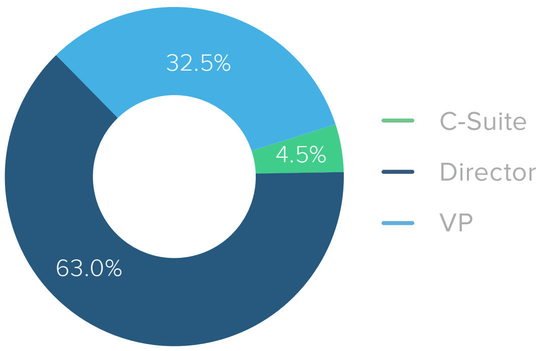
Frictionless access

In many ways, a company's position on the maturity curve parallels its progress towards Zero Trust, which is why Okta conducted a survey of 200 small and medium-sized organizations employing anywhere from one to 1,250 people to see where they stand on a range of IAM initiatives. Respondents answered a questionnaire on their current practices and future plans.

Industry Breakdown

Education Services
Professional Services
Healthcare
Real Estate
Finance and Insurance
Manufacturing
Retail

Respondent Roles



The results show commendable foresight on the part of SMBs, as many of them were making secure distributed workforces a priority well before the global pandemic forced everyone to stay at home. Nevertheless, there's still lots of room for improvement—and that's even more true now, considering the monumental shifts that have recently transformed how employees live and work.

Breaking down the IAM maturity curve

Okta's identity and access maturity curve classifies organizations in four potential stages.

Stage 0: Fragmented Identity

Stage 0 is when companies may be bringing cloud technologies into the mix for the first time. This truly is the start of the journey, as the on-prem and cloud infrastructure they presently have isn't yet integrated with an IAM platform.

Stage 1: Unified Identity and Access Management

It doesn't take much to advance to Stage 1, but it makes a huge difference: once organizations invest in IAM solutions such as single sign-on (SSO) and multi-factor authentication (MFA), they can cut down on poor password hygiene and enhance user and app security. At the same time, they're putting preliminary but necessary authentication systems in place to make sure users are who they say they are. 96% of SMBs have already implemented SSO for their internal teams, and 93% are protecting their people with MFA.

Stage 2: Contextual Access

Stage 2 marks an important shift in a company's IAM strategy. That's because this is the phase where more granular, context-based factors may be implemented in the MFA process, allowing admins to grant access to users based on a variety of factors, including device posture or location, as well as network.

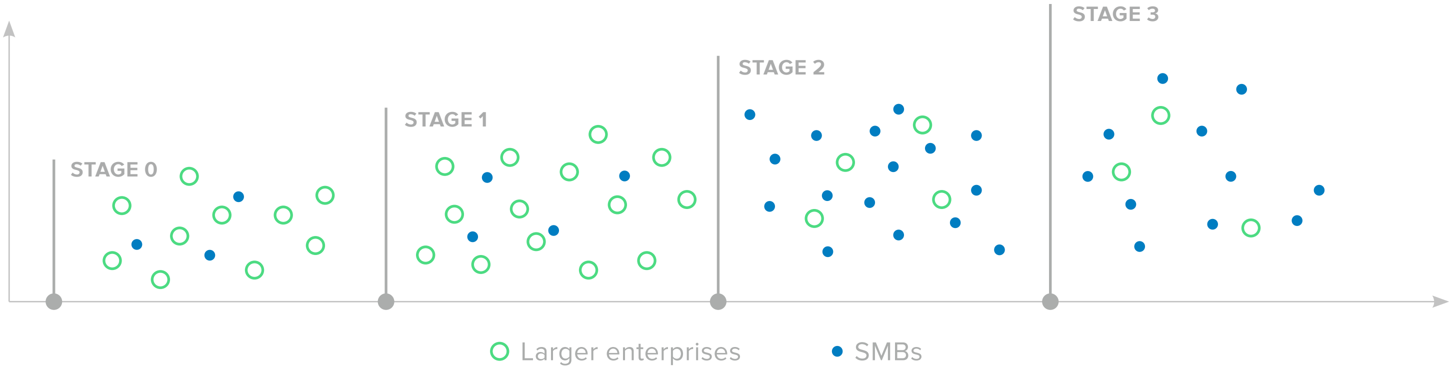
This is also the stage where security measures may be applied to APIs as well, which is critical: Gartner predicts that by 2021, 90% of web-enabled applications will have a greater attack surface due to exposed APIs, and by 2022, they will be among the greatest causes of data breaches.

Stage 3: Adaptive Workforce

Once an organization achieves Stage 3, they have nearly everything they need for Zero Trust security. This includes robust cloud architecture in which risk-based authentication policies proactively and automatically screen access requests—and login experiences that are more frictionless than ever thanks to the elimination of passwords through tokens, biometrics, email magic links, factor sequencing, and WebAuthn-related methods. The move towards passwordless authentication is still an emerging trend (75% of SMBs surveyed plan to go passwordless in the next 12 to 18 months)—one that can significantly enhance an organization's Zero Trust security model.

Where are today's SMBs on the curve?

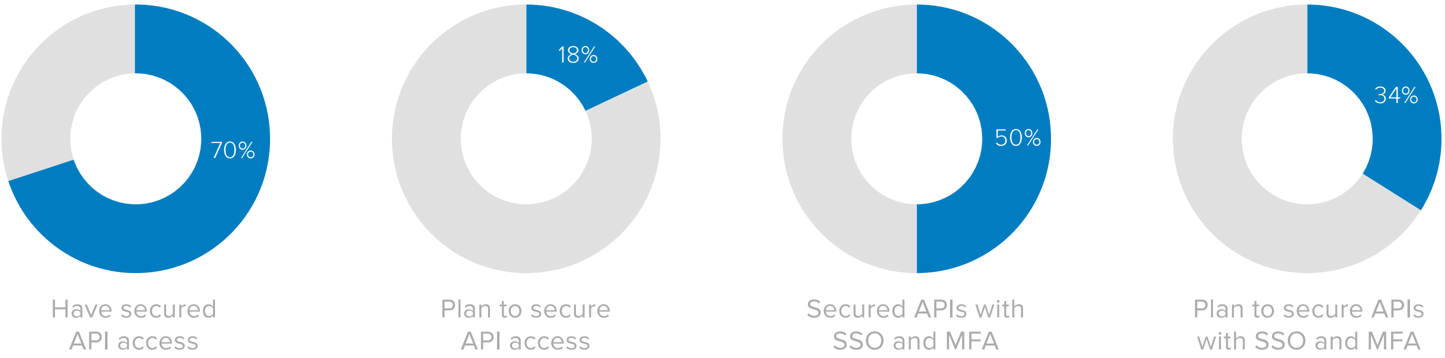
In terms of IAM and Zero Trust architecture, the average IT stack for small and medium-sized companies stacks up pretty well. Although organizations around the world are still being introduced to the concept of Zero Trust, many businesses in this segment have already implemented solutions associated with later stages of the IAM maturity curve—showing that they are moving more quickly than the majority of larger enterprises, which are mostly in Stages 0 and 1.



This is mostly because SMBs are securing their APIs. 70% of organizations in this group have adopted some form of API security measures to prevent bad actors from sneaking through the back door, and 78% have implemented privileged access to their cloud infrastructure.

In terms of SSO and MFA, 95% of SMBs are leveraging these solutions to secure SaaS applications, 57% for securing databases, and 50% are securing APIs. In the next 12 to 18 months, 53% of IT and security leaders in this segment will be looking to protect their servers with SSO and MFA, and 51% will prioritize their internal apps—a key move, considering legacy technology hosted on-premises is often targeted by online threat actors. Taken as a whole, SMBs are off to a strong start by securing their APIs and on-prem data.

SMBs prioritize API security

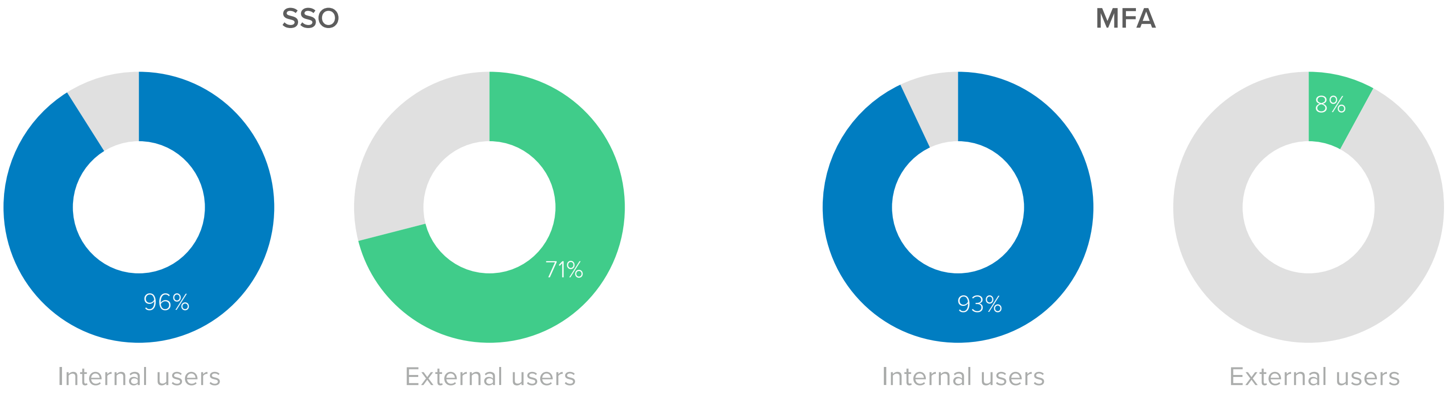


As they evolve within Stage 2, companies will be taking the most critical steps towards achieving Zero Trust by adopting contextual access policies. 59% of the organizations surveyed intend to invest in context-based access controls in the next 12 to 18 months. 76% are also thinking strategically around passwordless logins for the workforce. And while only 24% of respondents had already implemented automated provisioning and deprovisioning for the workforce, nearly 70% are planning to incorporate it in the near future.

For the majority of these initiatives, the workforce is the intended beneficiary. When SMBs look at context-based access policies or passwordless logins, they're typically orienting these projects towards their employees, and not external users such as customers or partners. Zero Trust architecture should ensure all login requests are untrusted and rigorously authenticated, whether they're regular users or not.

In some cases, small and medium-sized organizations have made progress in providing identity and access management for customers, or they plan to in the near future. Often, this takes the form of SSO, with 71% extending it to their external stakeholders as well. However, it's still somewhat uncommon for these businesses to invest in MFA for users outside their workforce—at present, only 8% have done so.

IAM solutions used by SMBs to secure internal and external users

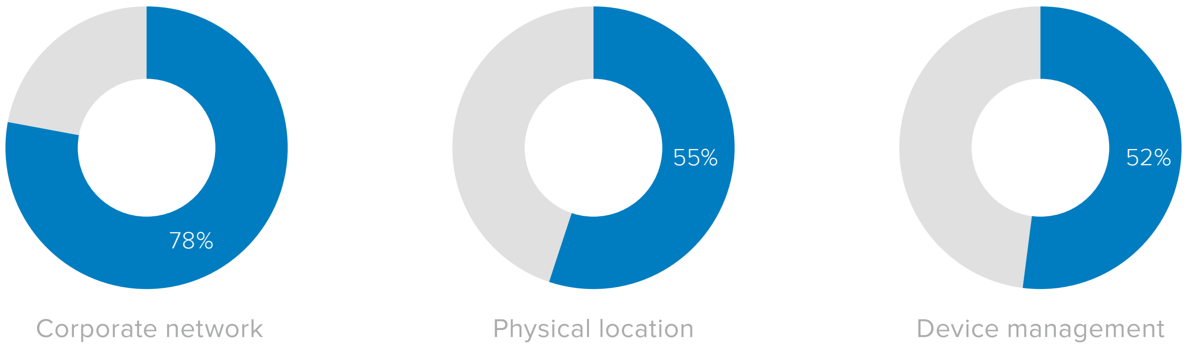


SMBs are putting logins in context

As mentioned previously, putting context-based access policies in place is one of most critical steps organizations can take in adhering to a Zero Trust security model. Team members are now signing on from anywhere, so companies need solutions to assess every login attempt based on a number of factors.

That's why 55% of the organizations surveyed have implemented tools to assess the physical location where login requests originate, and 52% are making sure devices are recognized and managed. However, while large enterprises are quickly moving away from the corporate network being a primary risk signal—21% listed it as a top factor in 2020 compared to 56% in 2019—this is still common among SMBs. Of those surveyed, 78% of IT and security leaders cited the network as a top risk signal.

Prevalence of context-based security factors at SMBs



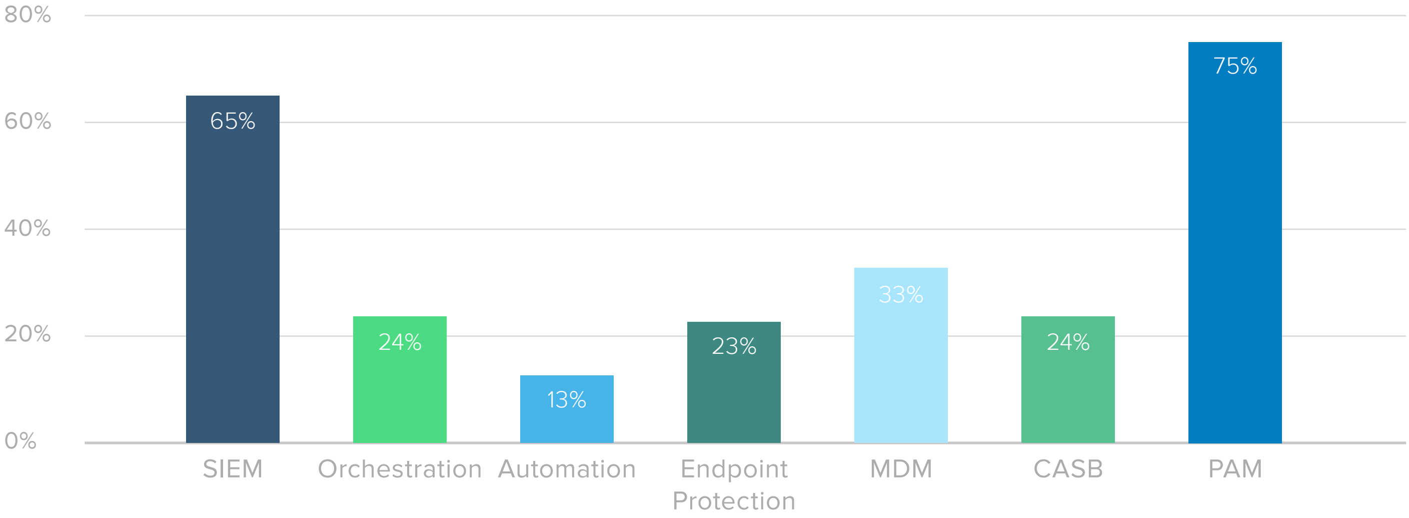
An adaptive MFA solution is a great tool for a Zero Trust model, automatically prompting users for additional login credentials if their geographic location or device is unrecognized—and 65% of SMBs organizations are getting more granular with their MFA solutions, deploying different factors depending on their user groups. Yet 95% are still using passwords as a login factor, and 78% are using common secondary factors including SMS and voice OTP.

Laying the foundations for a Zero Trust security model

When it comes to integrating IAM with security architecture, 65% of small and medium-sized businesses are prioritizing security information and event management (SIEM), which is also a focus for their enterprise counterparts. But SMBs are also placing more of an emphasis on privileged access management (PAM), with 75% citing it as a top tool.

Looking to the near future, SMBs' adoption strategies prominently feature access management at the edge, with 52% looking to cloud access security brokers (CASB) and endpoint protection. This is not surprising, and speaks to the continuing need for companies to accommodate the demands of a distributed workforce.

The top security intergrations among SMBs



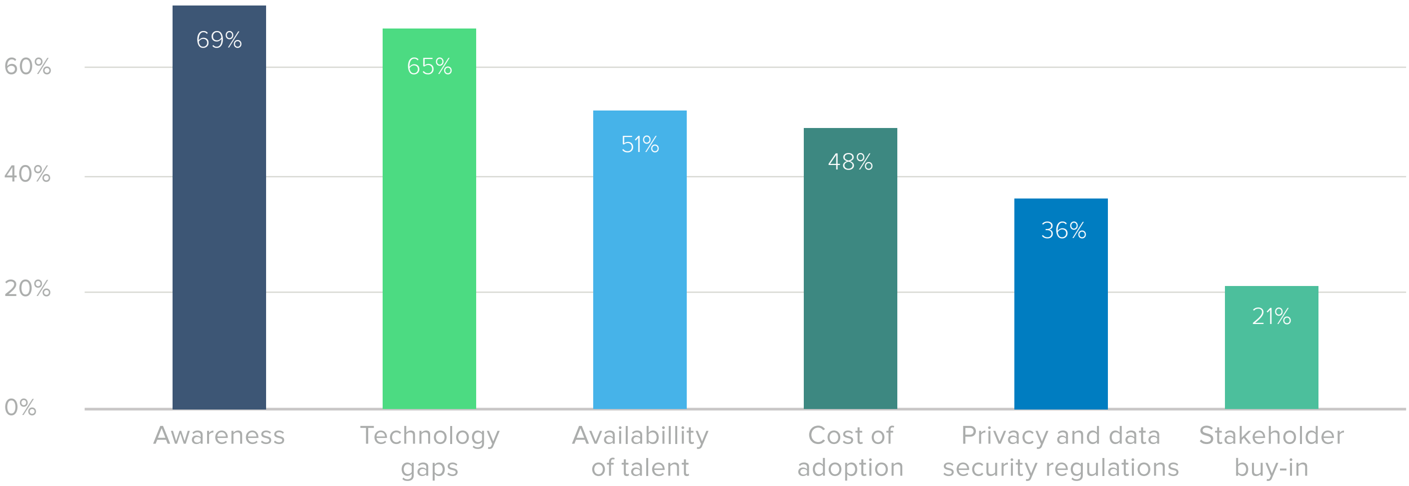
There's one area in particular where small and medium-sized organizations stand out: for nearly 90% of respondents, security has either complete or partial ownership over identity tools, adoption, and strategy. They understand that IAM is so much more than a process for IT to streamline access and monitor user activity—instead, it's a core piece of the Zero Trust security model.

The top Zero Trust challenges for SMBs

For organizations of all sectors and sizes, some of the biggest barriers to Zero Trust are the costs of adoption and the availability of talent. 48% of SMBs organizations see cost as an obstacle, and 51% are concerned about talent. However, technology gaps are a greater challenge for this segment, with 65% lacking the basic infrastructure they need to build a stronger stack, likely because many small and medium-sized businesses haven't been able to make the same investments in IAM as their larger counterparts.

Another challenge that exists for SMBs is a lack of awareness, with 69% of teams being less informed when it comes to Zero Trust architecture; enterprise organizations don't appear to share this problem.

The challenges preventing SMBs from adopting Zero Trust



The good news is that these gaps can close—and they already seem to be narrowing. As noted before, security teams are actively involved in making identity and access management decisions at small and medium-sized businesses. Not only that, but many of these organizations are at or near Stage 2 of the IAM maturity curve, having made huge strides in API protection and significant gains when it comes to context-based access.

Putting identity at the center of your Zero Trust strategy

Okta is the leading Zero Trust partner for SMBs, because its best-of-breed, vendor neutral approach—combined with over 6,000 pre-built integrations—allows for a holistic and comprehensive Zero Trust security stack. After all, there's no single solution that will protect organizations top to bottom. Security needs to be implemented at the level of the user, device, location, network, and application.

Regardless of which step of the authentication you need to reinforce in your authentication flow, Okta has a partner ready to integrate with you. We work with global leaders such as:

- Proofpoint for people-focused security
- VMWare, Crowdstrike, and Carbon Black for device and endpoint security
- Palo Alto Networks and Cisco for network security
- Netskope and McAfee for securing data in your apps
- Splunk and Exabeam for analytics and orchestration

But if you need somewhere to start, simply start with Okta, because Zero Trust starts with identity and access management. According to Forrester, where the framework originated, building a Zero Trust security model for your organization is a marathon, not a sprint, beginning with identity and device security—and year after year, Forrester lists Okta among the top Identity as a Service (IdaaS) providers. Whether you're looking to take the first step with SSO and MFA, or implement powerful device management and lifecycle automation across your workforce, we're here to support you in your journey.

How far along is your organization on the IAM maturity curve? Okta's Zero Trust assessment tool is designed to help you plot your current progress in implementing a modern identity and security framework, and delivers customized, prescriptive suggestions for actionable next steps.

About Okta

Okta is the leading independent provider of identity for developers and the enterprise. The Okta Identity Cloud securely connects enterprises to their customers, partners, and employees. With deep integrations to over 6,000 applications, the Okta Identity Cloud enables simple and secure access for any user from any device.

Thousands of customers, including 20th Century Fox, Adobe, Dish Networks, Experian, Flex, LinkedIn, and News Corp, trust Okta to help them work faster, boost revenue and stay secure. Okta helps customers fulfill their missions faster by making it safe and easy to use the technologies they need to do their most significant work.

Learn more at: www.okta.com

okta