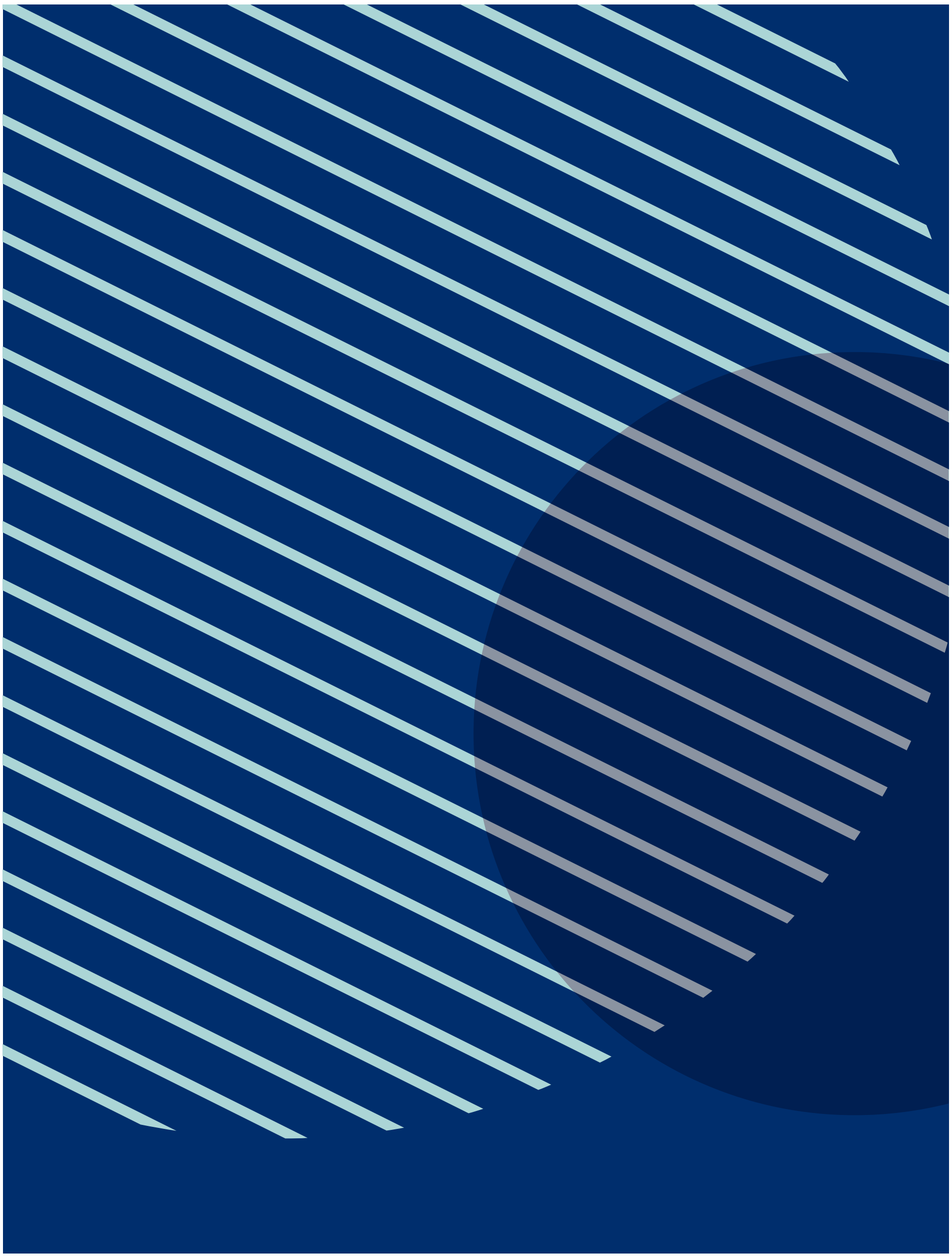
Whitepaper

June 2022

Identity and Access Management Buyer's Guide

How to choose the right identity solution for your customers and workforce.

EMEA Headquarter
20 Farringdon Rd
London, EC1M 3HE, United Kingdom
info_emea@okta.com
+44 (800) 368 8930



okta

Contents

3 The stakes are high
5 The impact is pervasive
7 How to get it right
7 Attribute 1: Neutral and Independent
9 Attribute #2: Customisation
10 Attribute #3: Ease of use
11 Attribute #4: Reliable and Secure
12 Conclusion

Identity and Access Management (IAM) has been around for years but has continued to rise in prominence. So why the focus across business units and leadership now? What's driving the rise in importance of identity and access management and what's at stake if you "get it wrong?" What attributes do you need to consider when deciding on a solution?

This guide is meant to help you work through these questions and more. It discusses the market drivers causing the identity and access management space to heat up and highlights the important elements of this purchase decision. Because, at the end of the day, the market drivers and risk factors are the reasons you should be keenly aware of certain IAM solution attributes. You need to weigh the pros and cons of what you are getting from your solution and how that impacts not only your function but other key stakeholders across your organisation. Afterall, IAM solutions don't just live in a silo; it's a costly, long-term investment that impacts all parts of your business - from the board of directors and the C-suite down to your last full-time hire in every department across every business unit in your organisation – and, in many cases, your customers and other key partners outside your organisation as well.

Why does this guide exist?

The stakes are high

Identity and Access Management continues to gain momentum in companies across industries and regions. What are the market drivers causing the rise in importance of IAM?

Transition to a hybrid IT model requires IAM

The advent of conducting work digitally has been around for, arguably, decades. But the acceleration of our collective digital transformation, due in part to COVID, has been fast-tracked.

> “
>
> With COVID still going around and rates increasing in different states as they try to go back to work, we're going to see a different type of workforce than we've ever prepared for.
>
> EJ Widun, Chief Technology Officer,
> Oakland County Michigan

Our need for speed and agility, our requirement for services to be on-demand, our desire for flexibility to scale up and down as needed, and ultimately our strong desire to constantly innovate makes moving to the cloud an imminent obligation. As organisations begin to fulfil their obligations and build and run new services in the cloud, they oftentimes have chosen best of breed. This translates to having a wide variety of cloud infrastructure providers, SaaS applications, developer and management tools, analytics services, and security platforms that comprise their solutions. And what’s the glue to hold all of these disparate solutions together? Identity. IAM solutions enable organisations to empower all of their users to easily and safely access all of their applications, devices, and technologies. And legacy IAM solutions that were built for our on-premises world are just not cutting it, as they are typically siloed and difficult to maintain – the attempts to retrofit these identity platforms leave gaps in coverage and expectations.

Legacy solutions don’t fit

	Legacy on-premises Identity solutions	Modern Cloud based Identity solutions
Connect with cloud technologies		X
Connect with personal devices		X
Manage people outside the company		X
Great end user experience		X

Modern security requires IAM

As our world experienced a steep and dramatic shift to a remote / hybrid work environment over the past couple of years – quite frankly, as our world became exponentially more digital as a whole – the traditional network perimeter became an antiquated security model overnight. Identity is the new perimeter. Not surprisingly, there’s been a dramatic increase in identity-based threats and attacks.

With sophisticated security breaches continuing to rise, organisations need more systems, protocols and standards to safeguard their data. And while regulations for privacy, security and compliance have intensified, the time, resources and money to adhere to these standards – and adopt a Zero Trust security model – have also increased. In short, as digital roadmaps accelerated, risks and associated costs have risen as well – raising the stakes on “getting it right” the first time.

A Verizon Data Breach report found that 89% of web attacks are caused by credential abuse.

Companies with extremely strong omnichannel customer engagement retain on average 89% of their customers, compared to 33% for companies with weak omnichannel customer engagement

Aberdeen Group

Consumers' demands require IAM

And if that weren't enough – while businesses are now challenged with scaling digital capabilities in parallel with fending off an increasing amount of complex, identity-related attacks, consumers (both internal employees and external customers) are demanding seamless experiences. In the past two years, organisations have had to rethink what it means to engage their employees and customers. Maximising conversions through a mobile application or establishing a 1:1 relationship with shoppers, patients or clients is an important first step to maximising revenue and creating customers for life. That said, it is critical to establish security as it fosters trust – a critical component of building brand loyalty. Organisations walk a tight line in balancing security with seamless, convenient experiences. And they have to get it right the first time because the next best option is only a click away.

Who is this guide written for and why?

The impact is pervasive

Whether you choose to build or to buy, one thing is for certain: IAM solutions have a pervasive and far reaching impact across your organisation and customer relationships. As such, it is paramount to identify your key stakeholders and establish a cross-functional team with clearly outlined responsibilities for the evaluation, purchase and implementation process. Getting all the stakeholders involved early on will increase your chances of making the best, long-term, strategic investment for your organisation.

> “
>
> If you don't have buy-in all the way up to the CIO and the CISO, you might as well pack it up and stay in the truck.
>
> Trey Ray, Manager,
> Cybersecurity, FedEx

Regardless of who's championing this initiative, it's important to recognise the disparate stakeholders and their respective goals for both internal and external users.

To get you thinking of the team you should pull together, below are the typical departments that face business challenges where a strategic identity provider can help. Keep in mind, the variety of stakeholders on any one cross-functional team will vary by organisation. Ideally, you should err on the side of overinclusiveness and include a stakeholder from as many of these departments as makes sense for your organisation.

Security eg: CSO, CISO	• Reduce the risk of a security incident • Accelerate detection and response time • Mitigate the impact of a security incident	Fully integrating with all apps, domains and devices and bringing them all into one place to manage, view and administer security.
Information Technology and Business Technology e.g. CIO	• Reduce IT costs and drive operational efficiency • Improve IT infrastructure performance and reliability • Improve workforce productivity, satisfaction and retention • Enable business innovation and digital transformation • Accelerate effective M&A, joint ventures and divestitures	Utilising automation for administrative actions, speeding up service to employees & ultimately reducing costs. Your IAM solution should shorten your app and user lifecycle journeys so that you can roll out with far more velocity.
Marketing and Digital eg: CDO, VP of Marketing	• Accelerate revenue • Attract and retain customers • Improve collaboration with business partners • Improve customer experience	Your IAM solution should have flexible login solutions like social login while removing friction from customer journeys with advanced identity capabilities such as progessive profiling and biometric authentication.
Infrastructure and Operations e.g. VP of I&O	• Migration from on-prem architecture for cost savings and ease of management • Ensuring all systems are highly available, resilient, and performant (no planned downtime)	Having a cloud-first architecture that easily integrates with legacy on-premises components to provide a highly resilient and available service with at least a 99.99% SLA.
Product and Engineering eg: CPO, CTO, Director of Engineering	• Drive operational efficiency to focus development efforts on core business • Accelerate time to build and release for their customers	Providing an advanced, developer-first, Identification and authorisation platform for developers

How to choose a strategic solution, not a simple tool

How to get it right

Selecting an IAM solution can be daunting – especially given how high the stakes are and considering the far-reaching impact this decision has on your organisation. But having a maniacal focus on a finite number of key attributes will help you narrow your options and zero in on the solution that is the best, long-term, strategic fit for you.

> “
>
> Identity is critical, security is critical, making sure that only the right people have access to the right data is critical.
>
> Harry Moseley, CIO,
> Zoom

While there are, undoubtedly, some nice-to-have features, the focus here is on what's categorically imperative. Outlined are 4 attributes, their benefits and some teaser questions to help you flush out just how important these attributes are to your organisation.

Attribute 1: Neutral and Independent

Your IAM solution must be technology agnostic in order to maintain business agility, allowing you to choose the best software solutions based on your business needs, not your Identity Provider.

As discussed, cloud migration most often means that your organisation has constructed various tech stacks, in respective departments, that are comprised of a wide array of best of breed solutions. And tech stacks can be complicated enough without constraining yourself because of your identity provider's lack of flexibility. Since identity is the one component tying all your solutions and stacks together across every department in your organisation, neutrality is a required attribute to ensure the agility of your business over time. If your identity platform claims, on some level, to be a one-stop-shop, it's likely not going to score well on neutrality.

When evaluating an IAM solution, make sure it offers:	So you can have:
• Broad and deep set of pre-built integrations • Integrations that support the latest and most commonly used open standards • A risk ecosystem that ensures strong partnerships across Network Security, Endpoint Detection and Mobile Device Management providers • Directories Integrations that enable the automation of end-to-end identity lifecycle - from provisioning to deactivation - using any system of record as the source of truth • Support for all open authentication standards • Secure hybrid IT access for mission-critical business applications and multi-cloud environments across a single identity platform	• Freedom to select best of breed solutions now and in the future • The ability for you to maximise investments already made (e.g. public cloud vendors) • Less manual effort for employees, IT admins and developers • Faster roll outs and decreased time to market • Increased operational and developer efficiency • A strong security posture

To challenge you to think about how important neutrality is to your organisation, consider the following:

- How many departments in your organisation will rely on the Identity Provider?
- How many different tech stacks will your IAM solution need to support?
- How often do any one of your stakeholders or business units roll out a new technology?
- What is the average time it takes to rollout a new organisation-wide application or 'big bang' technology solution and are you challenged with decreasing your average rollout times?
- How much could faster rollout times reduce costs for your organisation?

> "Any new application adopted by Sephora is immediately integrated with Okta. The technical process of integrating a new application into our IT system used to take weeks or even months, but with Okta it now takes no more than a day.
>
> Arnaud Feyssaguet, IT Infrastructure Manager,
> Sephora

Attribute #2: Customisation

Your IAM solution should adapt to you, so you can adapt to changing business needs

Organisations aren't static so why should your IAM solution be? Access management for employees is table stakes and consumer preferences are constantly changing. A strategic IAM solution should consider every user (employees, customers, partners, and vendors) across their entire identity lifecycle across both workforce and customer identity use cases. Your organisation should be thinking about how identity aids in maximising customer-centricity without decreasing operational efficiency.

When evaluating an IAM solution, make sure it offers:	So you can:
• No and low-code customisation options • API-first architecture with a comprehensive extensibility framework • Dynamic workflows that allow automation in user lifecycle and access policies • Visibility into all device identities to create contextual security policies • Policy engine to allow dynamic access policies tailored to user, use case, device and more • Expression Language that enables developers and admins to reference, transform and combine attributes from disparate systems and consolidate on a single source of truth	• Quickly deploy new experiences (e.g.: quickly onboard new employees, deploy new app integrations, etc.) • Enhance your security posture • Decrease development work for any new workflow • Increase operational efficiencies (i.e.: 'do more with less' by maximising current IT resources, budget, etc.) • Provide a better customer experience leading to higher retention rates

To challenge you to think about how important customisation is to your organisation's IAM solution, ask yourself the following:

- How much time and money is spent on development resources to build new and maintain existing and evolving workflows?
- How much engineering time is spent on custom automations?
- How many resources are spent on building custom landing pages for customer-facing apps or B2B portals for partners?
- How much time is spent trying to keep up with regulatory, compliance and audit requirements (e.g.: FedRAMP, SOX, CCPA, GDPR, etc.)?
- How far along are you in your journey of adopting a Zero Trust security model and what's it going to take for you to achieve your next goal of the journey?

> “
>
> If we don't properly catch an error and it ends up in a SOX audit, we would have to report it to the US Securities and Exchange Commission. That's a big risk for any company.
>
> Curtis Salinas, Senior Director,
> Strategic Planning & Operations, Slack

Attribute #3: Ease of use

Your IAM solution should be user-friendly, so you create sticky experiences for your employees, customers and everyone in between.

An IAM solution that easily integrates with all of your applications, users and devices across their identity lifecycle can easily become difficult to build, costly to maintain and complicated to use. A strategic identity solution, therefore, must also be easy and intuitive to use for developers, admins and end-users alike. Otherwise, you risk draining scarce IT resources and/or negatively impacting the end-users' experience – which could lead to turnover or damage to brand reputation.

When evaluating an IAM solution, be certain it gives:	So that you are empowered to:
• Admins a centralised console to manage all users, apps, policies • Admin self-service tools such as quickstart guides and integration wizards • Widgets, APIs & SDKs which span user authentication, resource configuration and access controls • Developers access to a comprehensive set of resources to help them bootstrap identity into any development project quickly and efficiently • The ability to automate identity-centric processes without code • A simplified way to integration to all your organisation's apps/systems • No or low-code customisation options • Social login to provide freedom on how to login • Passwordless authentication • Insights and visibility to stay on top of security with user, app, and device level activity and reporting	• Reduce operations and maintenance costs • Better employee experiences • Achieve faster integrations with best of breed security systems and apps • Decrease friction on end-users' digital journeys • Increase adoption across your organisation • Increase end-user satisfaction and loyalty • Enhanced security posture

To challenge you to think about how important ease of use is to your organisation's IAM solution, think about the following:

- How much code is currently used for customisation?
- What's the integration process for new apps and systems?
- How much manual work does it take to build and manage identity-centric processes?
- Do you have a central and unified view of all users, apps and policies?
- How many resources are spent on identity development?
- What impact does the business application stack have on employee productivity?

> "
> Implementing a unified identity layer has really helped us reach more customers, improve the speed at which we onboard new users, and improve the experience.
>
> Emnet Gossaye, Security Software Engineer,
> Kensho

Attribute #4: Reliable and Secure

Your IAM solution must be trustworthy: reliable and secure.

IAM is a business-critical function that is built on a foundation of trust. A strategic IAM solution safely connects people to technology and flawlessly manages an organisation's most valuable data – their user identities. Trust is everything and if your customers can't rely on you because of planned or unplanned downtime, or because of security risks, that's a problem. It's a problem that leads to decreased revenues and increased costs – a recipe for disaster by any measure.

When evaluating an IAM solution, be sure it delivers:	So that you are empowered to:
• Zero planned downtime • Self-healing nodes • 99.99% SLA for uptime • Shared security responsibility model • Security tools that proactively make recommendations to improve security posture • Ability to define security perimeters around which access can be limited or restricted	• Build trust with your employees and customers • Keep your business running smoothly • Avoid brand-damaging security incidents • Enhance your security posture

To challenge yourself to think about how important resiliency is to your organisation's IAM solution, answer the following questions:

- What's at stake if your organisation experiences frequent and/or prolonged system outages? Lost productivity, revenue or customers?
- How much can you save if you were to have 99.99% or higher uptime?
- Stack rank the vendors you are considering by historical downtime. Who's most favourable?

> “
>
> In the past, developers have had to rewrite code because it wasn't secure. Now, they're able to do it right the first time, and it's better for everyone. Their job satisfaction is improved since they can provide value faster and don't have to spend cycles fixing compliance issues.
>
> Justin Moore, IAM Manager,
> NOV Inc

Conclusion

IT modernisation continues to be a long-term roadmap initiative for IT departments in every organisation. The past few years have only worked to accelerate that timeline for many and in some ways, actually highlight how pervasive of an initiative it really is.

Migration to the cloud, with all its benefits, also means that many departments have become shadow IT – purchasing best of breed solutions to construct their technology stacks as their business requires. This leaves organisations vulnerable to the growing number of complex, identity-related attacks. On top of that, we, as consumers, have grown to expect a lot of any organisation we engage with – be it as a consumer or as an employee. Balancing security, and thus trust, with frictionless engagement is no easy task for organisations. But the right identity solution can help.

IAM is the glue that holds all the disparate tech stacks together in a way that enables brands to deliver seamless, omnichannel experiences that are secure and reliable – for both their employees and customers alike.

An IAM solution should be, at a minimum, neutral, customisable, easy to use, and last but certainly not least secure and reliable. At Okta, we provide just that. We would love to share how we've helped other organisations save time, mitigate risk and decrease their costs related to Identity and Access Management.

To learn more on the business value of implementing an IAM solution, visit Okta's ROI and Business Benefit Calculators.

To chat with us directly about your specific needs, reach out today.