Cloud Identity Essentials

How Companies Benefit from Identity and Access Management (IAM)

okta

Table of Contents

Table of Contents

Introduction

In a world where enterprises are rapidly transitioning to hybrid on-demand, on-premises infrastructure, controlling who has access to applications in your enterprise has become increasingly important—and increasingly complex.

As enterprises continue to confront the challenges of modern IT, the importance of offering users a centralised identity for websites, systems, and software as a service (SaaS) applications has become impossible to ignore.

Having a robust, secure, and well-defined identity and access management (IAM) program will help protect your organisation from intrusion or unlawful access, ensure your users aren't accidentally accessing data they shouldn't be, and better secure your organisation's data and assets.

A Global Trend with Regional Nuances

The trends that are emerging from IT modernisation are similar in countries across the world, but for European and Middle Eastern (EMEA) companies, there are some unique challenges that come along with this evolution.

With the right IAM provider, your organisation can realise tremendous time-saving, efficiency-building, and security-boosting benefits, no matter where you operate.

Why Read This Book?

The objective of this book is to provide an IAM resource that will answer the common questions that continue to dominate conversations in IT departments and with leadership teams. It will also help you understand which practices make for a truly best-in-class IAM program in a modern enterprise environment.

We will walk through common challenges and risks of legacy IAM services and offer real-life examples of how modern IT departments can benefit from the support of a powerful IAM solution. Finally, we'll offer actionable advice on what features to look for when choosing a solution that's right for your organisation.

Ultimately, you will walk away with an understanding of how IAM can support your goal of building a secure and scalable modern IT environment.

THIS BOOK WILL HELP YOU...

Learn more about modern IAM best practices

Understand the importance of centralising user identity in your organisation

Learn how to address common IAM challenges

Gain insight into real-life solutions and outcomes

Feel confident choosing a robust, scalable, user-friendly, and secure IAM solution that's right for your organisation

"Success depends on an organisation's ability to securely connect its people and technology, no matter how fast these worlds are changing. And when your people and technology are everyone and everything, identity is the only constant."

— 5 Rules for Choosing an Identity Solution that Lasts

Chapter 1

What Is IAM, and Why Does It Matter?

What is IAM?

Identity and access management (IAM) is the security practice of assigning and managing the identity of end users for appropriate and individualised access to different websites, systems, software, and applications. These identities are managed in a centralised location to keep up with users' changing needs and roles.

In a modern enterprise environment, IAM is no longer about granting access just for employees. These days, contractors, partners, customers, and consumers—basically anyone who has a relationship with your business—can require access, and this access needs to be tailored to their specific roles. Add them all up, and IT is now responsible for managing and securing millions of users, each of whom sits on a different network, uses a different combination of devices, and is constantly on the move.

Examining the Role IAM Plays in IT Modernisation

Many enterprises are saddled with an IT architecture that has evolved organically, piece by piece, over time. And the realities of competing priorities, limited staffing, and shrinking budgets often mean that systems and strategies remain in place far longer than originally intended. This can result in a significant burden of cost and complexity, which can compromise agility, making it more difficult to adopt the cloud technologies that would improve efficiencies and streamline processes.

Identity is a key tool to facilitate the modernisation of an IT environment. In fact, improper or outdated IAM methods is one of the biggest roadblocks to digital transformation.

Here are some common scenarios where proper identity and access management has become more crucial than ever:

Migrating an Enterprise Application to the Cloud

THE PROBLEM:

As seen in the massive adoption of SaaS applications such as Office 365, Salesforce, and Box, businesses are increasingly embracing cloud-based technology for agility and simplicity. But with the proliferation of services, managing user access to ensure proper privileges to sensitive resources becomes difficult and time consuming.

THE SOLUTION:

IAM drives efficiency by streamlining onboarding, offboarding, and change processes. An effective solution automates provisioning, making it easier for companies to bring on new people, exit former employees, or transition user rights across the organisation.

IAM can centralise identities across multiple user silos, making it easy to manage varying or changing instances of applications.

Building a Web or Mobile App for Consumers and Partners

THE PROBLEM:

Digital offerings present a tremendous opportunity for companies to provide value to customers. But, if the user experience is poor, adoption suffers.

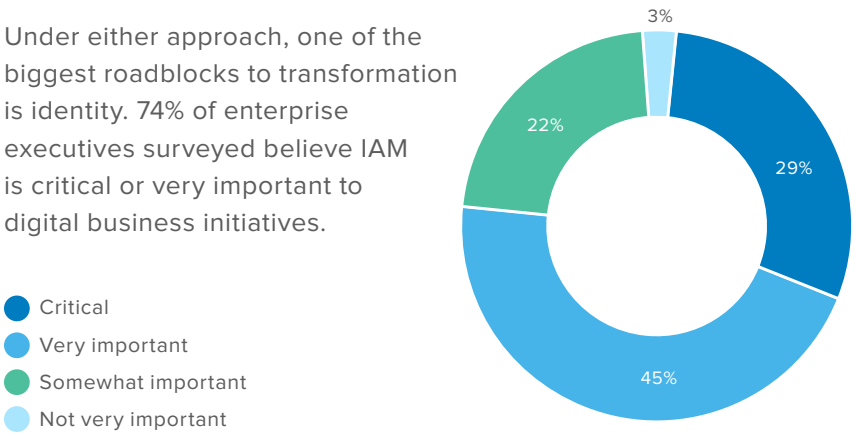
While interoperability and integration are key, they also open up the possibility for access errors.

THE SOLUTION:

Being able to support the latest identity protocols can be a critical usability differentiator—and make the difference for successful online operations. To help promote customer conversions, loyalty, and stronger security, IAM ensures that the user experience is straightforward and seamless.

Identity Management is Key to IT Modernization

Under either approach, one of the biggest roadblocks to transformation is identity. 74% of enterprise executives surveyed believe IAM is critical or very important to digital business initiatives.



Importance of IAM in Relation to Digital Business Initiatives

Source: Solution Brief: Modernize Enterprise IT, Okta. https://www.okta.com/resources/whitepaper-modernize-enterprise-it/

Complying with the General Data Protection Regulation (GDPR)

THE PROBLEM:

With the introduction of new data protection measures in the EU, organisations now have greater responsibilities when it comes to individuals' data.

Under the GDPR, organisations must be able to:

- Map data flows
- Locate an individual's data
- Correct this data (where necessary)
- Provide copies of this data
- Erase this data (where required)

With these new measures, every entity that handles your organisation's personal data—including vendors, partners, and applications—adds to your organisation's overall risk profile.

THE SOLUTION:

IAM allows organisations to effectively ensure policy-based access controls to a company's cloud and web-based resources. This ensures only authorised users can access sensitive data belonging to EU citizens and helps companies meet security and compliance needs for both the enterprise and customers.

DID YOU KNOW?

Out of the 15 fastest-growing applications in our network, 7 are used for security. Jamf, which secures Apple devices, saw year-on-year growth of 389%*

*data courtesy of Okta

Chapter 2

What are the Common IAM Challenges?

Introduction

As cloud applications become easier and less expensive to get up and running, companies are adopting more third party cloud services—or "Software as a Service (SaaS)" solutions—every day. These solutions are often managed by the corresponding functional area in a company, such as the Sales Operations group in the case of Salesforce. This can benefit IT as it leaves application administration to others and frees up IT's time, but it can also create a new problem because there is no central place for IT to manage users and applications, or build reports and analytics. Also, IT and financial managers cannot manage these subscription purchases and have little idea whether they are paying for more than they actually use.

Today, CIOs and IT teams are facing a whole new set of IAM challenges associated with adopting and deploying cloud and SaaS applications.

SOME KEY IAM CHALLENGES INCLUDE:

- ☑ User password fatigue
- ☑ Failure-prone manual provisioning and deprovisioning
- ☑ Compliance visibility
- ☑ Siloed user directories for each application
- ☑ Access management across a deluge of devices
- ☑ Frequent application integration updates
- ☑ Different administration models for different applications

Examining the Challenges

User Password Fatigue

Although the SaaS model makes it easier for users to adopt new applications, complexity around access quickly gets out of hand as the number of applications they need increases. Each application has different password requirements and expiration cycles, which reduces user productivity and increases frustration as users spend time trying to reset, remember, and manage changing passwords and URLs across all of their applications.

Perhaps of even greater concern are the security risks caused by users who react to this password fatigue by choosing short or obvious passwords, repeating the same password across multiple applications, or storing their passwords in an insecure manner such as writing them on sticky notes and posting them to their computer.

Cloud-based IAM services can alleviate these concerns by providing single sign-on (SSO) across all of these applications, giving users a central place from which to access all of their applications with a single username and password.

WHY YOU SHOULD NEVER WRITE DOWN OR REUSE YOUR PASSWORDS:

With the endless number of applications and programs the average user logs into every day, it can become difficult to remember which username goes with which password on which platform. A common solution is to just write them all down or use the same one repeatedly.

Although it's tempting, this is a huge security risk. Most data breaches are the result of stolen or weak passwords, meaning credentials are the weakest link for compromised or stolen data and other risks that could cause millions of dollars of damage to your business.

Malicious intruders can crack passwords in a variety of ways, including:

- Deploying hundreds of common passwords to try and gain entry
- Stealing a written password or password storage document
- Using stolen passwords from a password dump site
- Tricking users into giving their credentials to a third party

Sources: 2017 Data Breach Investigations Report, Verizon; The Real Reasons Why Users Stink At Passwords, Dark Reading

Failure-Prone Manual Provisioning and Deprovisioning

Manual provisioning and deprovisioning of users is not only a productivity drain on both IT and end users but also an increase in security risk. Manual management of individual user identities and permissions across a diverse environment takes time, costs money, and often results in human error. The overhead continues to add up as you consider time devoted to adding, updating, or changing users who onboard, offboard, or change roles on existing applications. On top of that, even more time is required to manually provision users on newly-added applications.

This is an especially challenging security concern when organisations need to offboard a user. It can take multiple days to manually deprovision a user off all their applications and entitlements. During this time, former employees or other unauthorised users can still access sensitive company data. This not only causes unnecessary business risks, but may also leave a company open to breaches of compliance with legislation like the GDPR.

Automating user provisioning and deprovisioning helps mitigate these inefficiencies. By tying the automated provisioning process to an HRIS, IT can offload user management to HR, freeing them to focus on more high-value, strategic tasks.

Compliance Visibility

A core responsibility of IT is to understand who has access to which applications and data, where they are accessing it from, and what they are doing with that data. This is particularly true when it comes to cloud services.

To answer auditors who ask you which employees have access to your applications and data, you need central visibility and control across all your systems and users. An IAM service will enable you to set appropriate access rights across services and provide centralised compliance reports across access rights, provisioning and deprovisioning, and user and administrator activity.

AUTOMATE YOUR LIFECYCLE PROCESSES TO BOOST PRODUCTIVITY AND SECURITY

Top challenges IT leaders face when manually managing the user lifecycle:

69%
of IT leaders struggle with tracking users' identities and permissions

67%
of IT leaders struggle with creating policies and monitoring user access

Your users' time is critical for your business:

98%
of respondents agree managing the user lifecycle is time sensitive

30 hours
the average time spent per week managing user systems, devices, and application access

34 hours
the average time spent per week in companies with 2,500+ employees

There are many benefits to automating your onboarding and offboarding:

75%
improved IT productivity

62%
improved user productivity

75%
decreased security risks

Source: Manual Processes Drain Productivity and Increase Security Risks, UK IDG QuickPulse Survey, Okta

Siloed User Directories for Each Application

Most enterprises have made a significant investment in a corporate directory that allows them to manage computers and other devices on their network. These directories, such as Microsoft's Active Directory, allow administrators to control access to on-premises network resources. As organisations adopt cloud-based services, some want to leverage that investment and extend it to the cloud, rather than create a parallel directory and access management infrastructure just for those new SaaS applications.

A best-of-breed, cloud-based IAM solution will ideally provide centralised, out-of-the-box integration into your central Active Directory (AD) or other internet protocols like the Lightweight Directory Access Protocol (LDAP). You can then seamlessly extend that investment to these new applications without any additional on-premises applications or firewall modifications. As you add or remove users from that directory, access to cloud-based applications should be modified automatically, via industry standards like Security Sockets Layer (SSL), without any network or security configuration changes. Just set and forget.

The right on-demand IAM solution should also leverage Active Directory (or the organisation's preferred directory) to allow users to continue logging in with their AD credentials.

Access Management Across a Deluge of Devices

One of the benefits of cloud applications is that access is available at any time from any device that is connected to the internet. But more applications means more usernames and passwords to keep track of. On top of that, the rise of mobile devices introduces yet another access point to manage and support.

IT departments must facilitate access across multiple devices and platforms without compromising security—a difficult feat with legacy IAM systems. A cloud-based IAM solution can help both users and administrators solve the 'anywhere, anytime, from any device' access

Many companies use Microsoft Active Directory (AD) to coordinate their identity and access management policies—but AD isn't the only option. Here are some other common user directories you may recognise or use in your own organisation:

- Apache Directory
- eDirectory
- FreeIPA
- GoSa
- IBM Domino (Lotus Domino)
- IBM Tivoli Directory Server
- JXplorer
- Lepide Auditor for Active Directory
- NTDS or Windows NT Directory Services
- Open LDAP
- OpenSSO
- Oracle Internet Directory
- Red Hat Directory Servers
- Resara Server
- Samba
- SME Server
- SunOne
- Univention Corporation Server
- Zentyal
- 389 Directory Server

Sources: Overview of Directories and On-Premise Infrastructure, Okta; 22 Best Alternatives to Microsoft Active Directory, Merabheja

challenge. It should not only provide browser-based SSO to all user applications, but also enable access to those same services from the user's mobile device of choice.

Frequent Application Integrations Updates

Today's enterprise cloud applications are built with cutting-edge, internet-optimised architectures. The modern web technologies underlying these applications provide excellent choices for vendors to develop their service and its associated interfaces. Unfortunately for IT professionals, this also means that every new vendor may require a new approach when it comes to integration, particularly concerning user authentication and management. In addition, like on-premises applications, SaaS applications change over time.

A good cloud-based IAM solution keeps up with these changes and ensures that the application integration, and thus user access, is always up to date and functional. The right IAM service will mediate all the different integration technologies and approaches, removing these challenges for IT.

And as the various services' APIs change and multiply, the cloud IAM provider should manage these programmatic interfaces, offloading the technical heavy-lifting away from IT departments so that they no longer have to track dependencies between connectors and application versions. This will also make adding a new application into your network as easy as adding a new app to your iPhone.

"Like on-premises applications, SaaS apps change over time. A good cloud-based IAM solution should keep up with these changes and ensure that the application integration, and thus user access, is always up-to-date and functional."

— Top 8 Identity and Access Management Challenges, Okta

With only minimal, company-specific configuration, you should be able to integrate new SaaS applications with SSO and user management capabilities within minutes.

Different Administration Models for Different Applications

A cloud IAM service should provide IT with central administration, reporting, and user and access management across all applications. The best solutions will also include a built-in security model to provide the right level of access to your individual application administrators, so they can manage their specific users and applications within the same IAM system. Ideally it will also provide accurate visibility into seat utilisation and help IT optimise SaaS subscription spend.

According to a global survey conducted by IT Asset Management Review, 76% of respondents said their software was over-licensed. Organisations larger than 10,000 were the most likely to be very over-licensed.

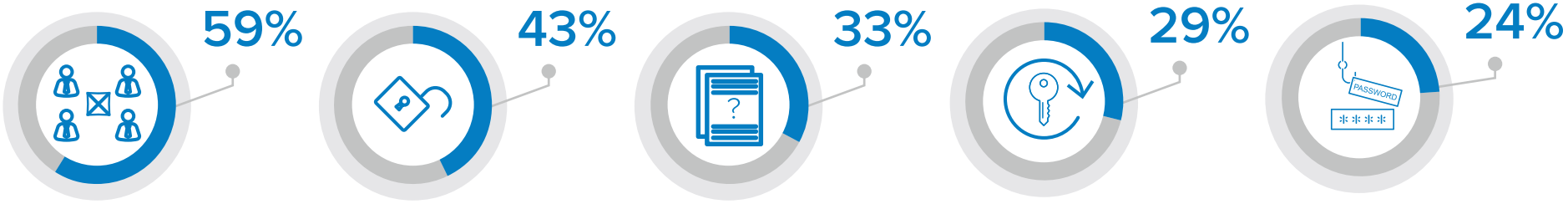
Source: 76% admit to over-licensing for fear of audits, ITAM Review

Top Identity-Related Security Concerns

Using IAM in the Age of Megabreaches

There's no shortage of threats, including: malware, hacking, phishing, and social engineering. These tactics often lead to account compromise and credential theft.

Top Identity-Related Security Concerns



Expansion of the user base to include non-employees

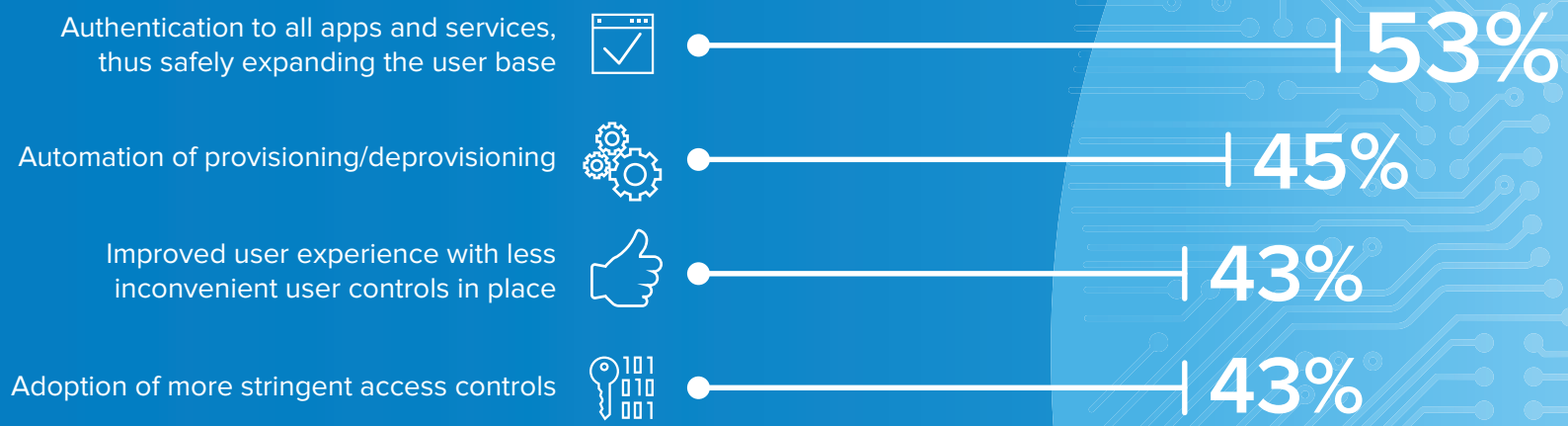
Inconvenient authentication controls ignored/subverted

Lack of IAM policies

Reuse of same passwords

Stolen credentials

Addressing Security Concerns: Most Important Potential Benefits of IAM Solutions



Source: Using IAM in the Age of Megabreaches, Okta

Chapter 3

How Can Companies Overcome These Identity Challenges?

A Closer Look at Customer Case Studies

News Corp

Introduction

News Corp, as the media and information services company, had a challenging task at hand as it expanded its business into real estate, digital ad tech, and marketing solutions.

Five years back, the newly-appointed CIO set a goal of putting three-quarters of News Corp's computing power into the public cloud and modernising infrastructure to better serve the company's 25,000 global employees.

News Corp's IT was a patchwork of six unrelated single sign-on solutions, with countless pins, passwords, tokens, and access points for users to keep track of. To successfully move to the cloud, the CIO knew he would need an IAM solution that was efficient, secure, and provided a seamless user experience. At the same time, it had to be open, scalable, and able to connect to both existing and emerging technologies.

News Corp's Journey to the Cloud

It was clear to the CIO that Okta's SSO was his best option, so he piloted it with a single business unit in August 2015. It was so successful that the solution was deployed company-wide just 9 months later. With more than 150 applications connected to the Okta platform, individual users and units could deploy the tools to meet their specific needs in a way that was consistent, convenient, and secure.

News Corp also added Okta's Multi-factor Authentication, providing an extra security layer. This ensured that employee privacy and credentials were fully protected, even as they enjoyed unmatched usability and ease of access.

This has been a huge relief for IT: the department can channel resources to more strategic initiatives now that password resets have been drastically reduced, the company's applications can be tracked and managed, and access outages are a thing of the past.

What's more—onboarding for newly-acquired companies became even easier after News Corp added Okta's Universal Directory and Lifecycle Management to its identity portfolio: with just one update for the master directory, an administrator could then control access to both on-prem and cloud applications. Thanks to Okta, onboarding has been much more efficient, saving the company over 1,000 hours each year of synchronising and consolidating domains post-M&A.

WHAT IS ADAPTIVE MFA?

Multi-factor Authentication (MFA) is designed to protect organisations against a range of attacks that use stolen credentials. It does this by requiring users to provide something in addition to their primary password—something the user is, has, or knows—before they are authenticated.

Many legacy, stand-alone MFA products bring along with them a series of challenges for both IT departments and end-users. Some of these include: lack of ability to integrate vendor-specific applications and systems, inability to scale for mobile or international users, management complexity and, often, poor user experiences due to a disruptive, cumbersome workflow.

Adaptive MFA offers enterprise-grade security and an improved user experience by offering policy-driven contextual access management, support for a broad set of modern factors, big data analytics, and built-in integrations to all the applications and VPNs that organisations need to protect themselves.

Source: Multi-factor Authentication: Moving Beyond User Names & Passwords, Okta

“Okta is a fan favorite amongst my team and across the business because it solves the two pillars of usability and security.”

— Ramin Beheshti, Chief Product and Technology Officer for Dow Jones (owned by News Corp)

Introduction

Since Eurostar started in 1994, they've carried over 150 million rail passengers to London, Paris, Brussels, Lille, Calais, and more. Eurostar employs 1,800 people to ensure that passengers arrive at their destinations on time, while delivering the highest standards of service along the way.

IT plays a critical role in ensuring Eurostar gears themselves up to support their staff, who need to stay connected throughout their journeys. Back in 2010, Eurostar went mobile by rolling out iPhones as corporate devices to all of their employees. Ever since, they have been pushing the boundaries as to how much of their new and legacy applications can be distributed to mobile devices.

BEFORE USING OKTA:

- Management overhead
- Technical challenges
- Complex architecture for what should be simple systems

Eurostar IT was struggling with its single Microsoft ADFS server, which it set up for Salesforce. The server sometimes worked and sometimes didn't. A sole off-site backup server also offered little help. Plus, users couldn't access Salesforce from outside the Call Centre.

Fixing these issues would have required several more Microsoft ADFS servers and numerous firewall configuration changes.

okta

ONCE USING OKTA:

- Automated processes
- Enhanced efficiency and security
- Improved employee engagement and customer service

Eurostar's IT administrators are now using Okta Universal Directory to easily customise, organise, and manage their 1,800 users—all done using the cloud. They also use Okta Lifecycle Management to automate the process of provisioning user accounts (including automatically syncing Universal Directory with new cloud applications).

Thanks to real-time visibility into train faults, via train-management applications, operational turnaround has improved. Security has also been enhanced, with confidential data now securely stored on iPads, instead of in trolley bags.

With mobile SSO, employees can now use their devices to provide exceptional on-train customer service.

Chapter 4

What to Look for in an Identity Solution

Introduction

There may not be a ‘one-size-fits-all’ solution for IAM, but Okta has had conversations with thousands of technology and security leaders, from the largest enterprises to small and medium-sized businesses across every industry. Based on these discussions, we’ve developed a set of rules for finding an identity provider that lasts—because there are certain elements of an identity solution that every organisation should have.

5 RULES TO GUIDE YOUR IDENTITY JOURNEY

- ☑ Don’t get boxed in.
  Best-of-breed IT requires independence and neutrality.
- ☑ Your app stack is dynamic. Your solution must be future-proof.
- ☑ Avoid fragmentation. Centralise management of every type of user.
- ☑ People are your new perimeter.
  Ensure you have updated tools to protect them.
- ☑ Repurposing the old for the new doesn’t work.
  Find a solution that’s born and built in the cloud.

“Identity is the lynchpin for the modern cloud ecosystem. It’s the new security standard in a world where there is no perimeter anymore. And it’s the foundation on which any company can become a technology company.”

— 5 Rules for Choosing an Identity Provider That Lasts

What Did Engie Look for in an Identity Solution?

In the face of a dramatically changing energy industry, one company is working to forge a new path. ENGIE is an international provider of power, natural gas, and energy services and is hoping to lead the transition to a more sustainable, decarbonised world.

Part of this change includes moving from a hierarchical business model to a flat organisation with 24 geographically-oriented business units. IT's goal is to support ENGIE's 150,000 employees within these units by offering consistent, reliable, global solutions, while giving them the freedom to adapt quickly at the local level.

Ready to Forge Ahead

With Okta, ENGIE was able to check the boxes on all three requirements. Today, after successfully introducing IAM to the organisation, ENGIE has gained newfound agility and responsiveness for integrating new applications. It has found new ease in acquiring or divesting businesses, and has become more nimble and flexible—crucial characteristics for its dramatic shift to a distributed business model.

Searching for an Agile Connection

CIO Claude Pierre had three primary requirements for the company's identity solution:

Reliability: ENGIE employees work around the clock, all over the world, making always-on access crucial

Neutrality: The solution needed to integrate deeply and easily with both Microsoft-focused collaboration and productivity tools and those from other vendors

Future-readiness: For an industry that is changing so quickly, the identity solution needed to accommodate ongoing adaptation and innovation

A Closer Look at the Five Rules:

1 Don't get boxed in. Best-of-breed IT requires independence and neutrality.

Choosing an identity solution is about preserving choice. You know your organisation best. And you should always choose the technology that's best for you, not your identity provider. Your provider shouldn't be tethered to the success of any proprietary applications. In fact, your identity provider should be committed to connecting everything you want to use, with a consistent level of quality and depth. Don't trust an identity provider that's trying to sell you other applications or favours certain ones over others you want to use. Also, don't choose a provider who bundles their identity solutions in with their own applications. Instead, prioritise the identity solutions that will allow your organisation to be truly best-of-breed.

"We have been able to deploy more than 120,000 users across 60 countries in less than six months. Our partnership with Okta was essential to get that done."

— Claude Pierre, Deputy Group CIO, ENGIE Group

2 Your app stack is dynamic. Your solution must be future-proof.

It's a modern reality that what works best for your business today can, and will, be replaced by something better tomorrow. Technology will continue to advance, which means there will always be new applications and new devices that your teams want to use. To keep your teams productive, you need the ability to use these new tools and roll them out as quickly and efficiently as possible. Make sure the identity solution you choose connects to everything you want to use today, and will connect to everything you want to use in the future. This will enable countless growth opportunities for your company.

3 Avoid fragmentation. Use one platform to manage every type of user.

The volume of users that IT teams manage is exponentially larger in today's world. For every employee you have, you might also have dozens of contractors, hundreds of partners or suppliers, or thousands of customers. And every one of these users is constantly on the move, accessing critical applications from a profusion of networks and devices. Plus, their relationship to your business isn't static. It requires constant updating of access and permissions. To ensure your users can access the tools that make them most productive, you need a single, centralised, automated identity solution that can manage millions of users, working in different ways, across the globe.

4 People are your perimeter. Protect them.

Security isn't a network problem anymore, nor is it a VPN or firewall issue. These approaches to security made sense when you could restrict people based on where they were located.

Today, in a perimeter-free world, infrastructure isn't the target threat—it's end users, and specifically, their credentials. Safeguarding end users has become increasingly difficult for IT teams because end users have so much flexibility. The options for which app, device, or location they use to complete work are overwhelming. Just as hackers have shifted their target to the end user, security leaders must shift their focus to be user-centric as well.

5 Not all clouds are created equal. Find a solution that's born and built in the cloud.

A company's ability to win, differentiate, and achieve its mission as quickly and effectively as possible hinges on its ability to use the best technology it possibly can. This simply isn't possible in an on-prem environment. And it's also not possible by taking premises-based technologies (like Microsoft AD) and putting them in the cloud. Look for an identity solution that was built in the cloud from day one. It will ideally also be 100% multi-tenant, so your identity provider can focus on making that single environment extremely robust in terms of scale, redundancy, monitoring, and processes. And the service should be replicated across various zones and geographic regions.

SECURITY BREACHES BY THE NUMBERS

42,000
security incidents in 2016*

1,935
confirmed security breaches*

81%
of breaches used stolen and/or weak credentials*

$3.9M
cost of average breach**

Sources: *Verizon 2017 Data Breach Investigations Report **Ponemon Institute's 2018 Cost of Data Breach Study

Conclusion

Organisations rely on their identity provider to securely connect all their users to the technologies and devices that enable them to do their most important work. We know selecting the right identity provider can be daunting, but it doesn't have to be. Evaluate every potential identity provider based on these five rules. Don't settle for an identity solution that meets three out of five.

Identity enables your business to succeed. But to do this, you can't just choose any identity vendor. It must be the right identity vendor.

Chapter 5

How Okta Provides the Identity Layer for Modern Enterprise

Introduction

Okta is an enterprise-grade identity management service, built from the ground up in the cloud and delivered with an unwavering focus on customer success. Our modern approach to identity management helps businesses take control of identity across their enterprise.

The Okta IAM service provides directory services, single sign-on, strong authentication and security, provisioning, workflow, and built-in reporting. Enterprises in EMEA markets and everywhere are using Okta to manage access across any application, person, or device to increase security, make people more productive, and maintain compliance. These business-driven results are centred on our three pillars of value.

Three Pillars of Value

1. Decreased Costs and Increased Efficiency

Okta provides a single solution for identity as a service. With just one cloud-based architecture and point of access, you realise cost savings and reduced complexity, with no hardware or on-premises software to maintain.

With a simple administrative interface, administration is straightforward and self-sufficient. And easy maintenance and automatic updates will promote higher productivity amongst your IT team. Finally, our high availability gives you a resilient infrastructure that's less prone to costly disruption.

2. Enhanced IT Agility

Okta's IAM solution offers a library of preconfigured integrations to allow for faster changes and updates. It integrates simply and smoothly to your directory (e.g. multiple domains), allowing you to easily maintain it even in a complex environment. Plus, our integrated multi-factor authentication eases the burden of delivering enhanced security.

3. Delivering Business Value

Okta's IAM solution allows you to deploy web and mobile applications more quickly and provide greater customer value. It can programmatically federate with partners, or allow self-service registration for contractors, partners, and customers.

The broad developer platform (e.g., APIs, SDKs) allows for efficient integration to services that enhance your business offerings. Faster change management also enables businesses to respond to needs in near real time.

Chapter 6

What Will Your Identity and Access Management Solution Look Like?

A Modern Solution for a Modern IT Environment

Okta offers a foundation for secure connections between people and technology.

By harnessing the power of the cloud, Okta's IAM service allows people to access applications on any device at any time—while still enforcing strong security policies. It integrates directly with an organisation's existing directories and identity systems, as well as over 5,500 applications.

Because Okta runs on an integrated platform, organisations can implement the service quickly, at large scale and low total cost.

Solving Customer Problems That You Can Relate To

More than 2,500 customers, including ENGIE, News Corp, Eurostar, Gatwick Airport, Gavi, Bazaarvoice, and Flex, trust Okta to help their organisations work faster, boost revenue, and stay secure.

There's a unique story behind every one of these EMEA customers. Each has different needs—but all have benefitted from identity and access management. Learn how by visiting Okta's website.

Get in Touch

For more information, visit us at www.okta.com or get in touch here www.okta.com/contact-sales.


okta