The State of Identity and Access Management (IAM) in Hybrid IT Report

okta

Introduction

Do you work in IT, Security, or Identity Management?

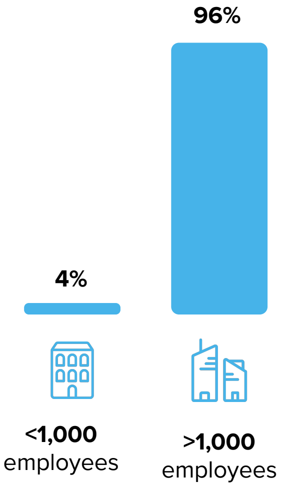
Do you have systems running in the cloud?

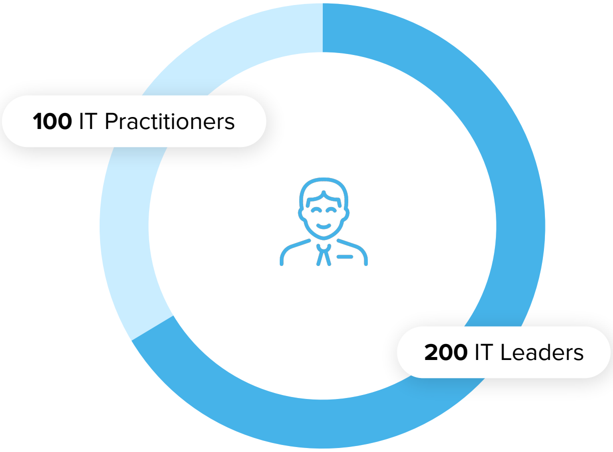
Do you have systems running on-premises?

Did you say yes to the three questions? We are here to help you:

1. Like most organizations on the planet[1], your company runs a hybrid IT environment – aka, a mix of apps hosted on-prem and in multiple cloud providers.
2. This report shows how organizations (like yours) are approaching identity and access management (IAM) in complex hybrid IT environments – spoiler alert: we have good and bad news.
3. We created this report to help you benchmark your company against other organizations of a similar size, country, and industry, as well as provide you tips that will help you better manage identity across these environments.

Executive Summary





To find out just how organizations are securing access to applications in hybrid IT environments, we engaged Pulse Q&A to ask IT leaders and practitioners how their organizations deploy identity and access management (IAM) to protect on-prem and cloud apps across North America and Europe. The study focused on larger organizations, with **96% of the respondents from organizations with more than 1,000 employees**. This is what we learned from our data:

80% of the organizations have a contradictory view of centralized IAM

Respondents have contradictory opinions about centralized IAM. 81% of the respondents claim their IAM solution and configuration are centralized in a single place, which is odd since 98% of the same respondents also reported they have two or more IAM systems to monitor and secure their on-prem and cloud systems.

67% of the organizations without centralized IAM claim that their current solutions lack the ability to protect the hybrid IT

These respondents likely have legacy IAM solutions that lack capabilities for securing access to modern cloud apps. These solutions not only don't have cloud to ground coverage, but they also require constant maintenance to protect on-premises resources.

Only 38.5% of the larger organizations expect a single cloud identity solution to control access to the hybrid IT

If you look at the numbers, nearly all organizations want to use cloud-based IAM – also known as Identity-as-a-Service (IDaaS) – to protect modern cloud and mobile resources. That makes sense since both IDaaS and those systems run outside the premises.

However, only a small percentage of organizations expect to use IDaaS to secure both cloud and on-prem systems – the hybrid IT. It seems that a large number of organizations are holding on to the outdated perception that on-prem resources can be secured only with on-prem IAM. As a result, they're failing to see how easy it can be to consolidate their identity controls on a single IDaaS platform. And this creates IT friction, since organizations end up keeping unnecessary legacy IAM solutions and silos.

82% of large organizations spend at least 16 hours a month per IT professional on maintenance tasks. For 31%, this number goes up to 80 hours a month per IT professional!

We believe the lack of awareness around consolidating IAM for the hybrid IT draws a strong correlation to higher TCO and time spent on IT maintenance on organizations with more than 5,000 employees.

IT leaders and practitioners both agree: less time on maintenance equals more time on innovation.

In our survey, IT leaders and practitioners both agreed on which tasks they would perform in case they spent less time on maintenance. The top three tasks – solving key business challenges, identifying new technologies, and addressing security threats – are all related to business innovation and can impact the bottom line of any organization.

Our recommendation

Based on our data, we recommend that organizations:

It is Possible (Really!): Use Consolidated, Centralized IAM

Respondents have contradictory opinions about centralized IAM. 81% of the respondents claim their IAM solution and configuration are centralized in a single place, which seems strange since 98% of the same respondents also reported they have two or more IAM systems to monitor and secure their on-prem and cloud systems.

You Can Have It All: Look for Coverage from Ground to Cloud

As part of the hybrid IT approach, organizations should reevaluate their current IAM solution's ability to secure access to cloud and on-prem resources (SaaS, PaaS, IaaS, mobile apps, APIs, cloud servers, on-prem apps, on-prem servers) from the same place. If their current solution cannot support the hybrid IT at scale with an effective TCO, it's time to upgrade to a better solution.

Be Your IT Org's Hero: Cut Down the Maintenance Hours

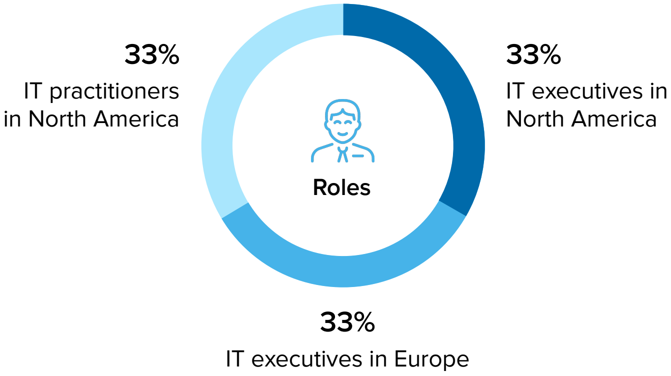
The use of solutions like IDaaS reduces maintenance tasks such as install, manual integrations, disaster recovery planning, and patching.

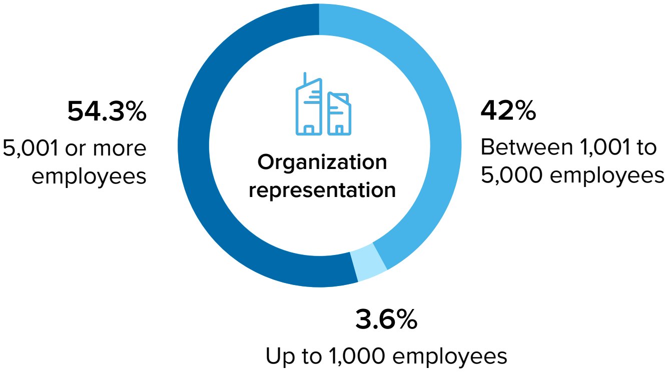
Okta Identity Cloud and our new offering, Okta Access Gateway, provide identity and access management for systems on-premises and in the cloud, unifying single sign-pn (SSO) and multi-factor authentication (MFA) for all apps and increasing productivity, while dramatically reducing maintenance costs and complexities. To learn more about how Okta can help you protect hybrid IT while saving time and money, visit www.okta.com/products/access-gateway or contact a sales representative at www.okta.com/contact-sales.

And of course, if you want to see more details about what our study discovered, keep on reading the rest of our State of Identity and Access Management in Hybrid IT Report.

Methodology

The State of IAM in Hybrid IT Report is based on responses from 300 professionals in September 2019, including:

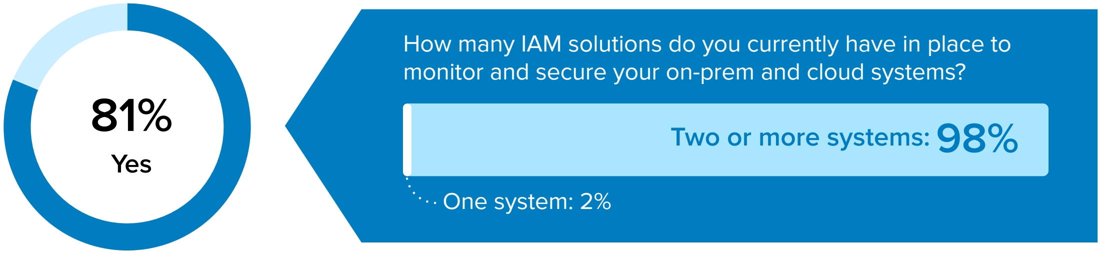

33%
IT practitioners in North America
33%
IT executives in North America
Roles
33%
IT executives in Europe



The studies surveyed organizations from 28 different countries including the United States, United Kingdom, Canada, France, Germany, Netherlands, Italy, Spain and more, across 29 industries, including finance, manufacturing, public administration, software, telecom, healthcare, real estate, transportation, education, mining, biotech, food services, professional services, and more.

Most organizations have a contradictory view of centralized IAM

Does your organization have identity and access management (IAM) solution and configurations centralized in a single place?



When we asked IT executives and practitioners if they have IAM solutions and configurations centralized in a single place, a significant majority – 81% of the respondents – indicated that they did. However, of those who said they have centralized IAM, 98% of them also said they use two or more IAM solutions to monitor and secure their on-prem and cloud systems. Additionally, 78% of those respondents used three or more IAM solutions.

This result was consistent across roles and geographies:

# of IAM systems	IT Leaders - NA	IT Leaders - Europe	IT Practitioners
I don't know	3%	2%	2%
1	3%	3%	4%
2	25%	10%	12%
3	**61%**	**80%**	**78%**
More than 3	8%	5%	4%

This creates a **contradiction**, since its not possible to have a centralized solution with more than one system in place. We believe the contradiction is caused by the use of legacy IAM solutions that require multiple diverse servers to operate, as well as the use of distinct and siloed IAM solutions to support on-premises and cloud resources.

Large organizations don't expect a single solution to secure hybrid IT (...but they should)

In an ideal world, what types of applications and services would you like IDaaS to protect? That's the question we asked respondents, allowing them to choose from six categories across on-premises and off-premises systems.

From the responses, we compiled how many people selected **only on-prem** resources (servers and apps hosted on their premises), **only cloud** resources (SaaS apps, Mobile apps, PaaS, and IaaS), and resources from both categories (**hybrid resources**).

This allowed us to see how many companies want IDaaS to cover hybrid IT across smaller and larger organizations:

	Organization size	
Expected IDaaS Coverage	**Up to 5,000 employees**	**More than 5,000 employees**
On-prem only	2.5%	1.5%
Cloud only	27.5%	60%
On-Prem and Cloud	**70%**	**38.5%**

The results showed a big gap between larger and smaller organizations. In smaller orgs, 70% of the respondents want a single IDaaS solution for resources across the hybrid IT while only 38.5% of the larger organizations have the same expectation.

Smaller organizations run leaner IT departments, with their technical staff wearing multiple hats and without the same level of legacy IAM software running on-premises as larger organizations. Larger enterprises usually rely on a dedicated IT staff to operate heavy and complex IAM solutions, such as web access management (WAM) or SSO on-premises. This might lead them to hold the perception that only complex IAM systems can handle their requirements.

As a result, larger organizations are failing to see the benefits of consolidating identity controls on single and modern IDaaS platforms that can handle complex hybrid IT requirements. And this creates unnecessary IT friction since organizations end up keeping deprecated legacy IAM solutions and silos.

When investigating the resources level, we discovered that most of the respondents wanted at least three of the categories protected by IDaaS:

In an ideal world, what applications and services would you like your IDaaS to protect?

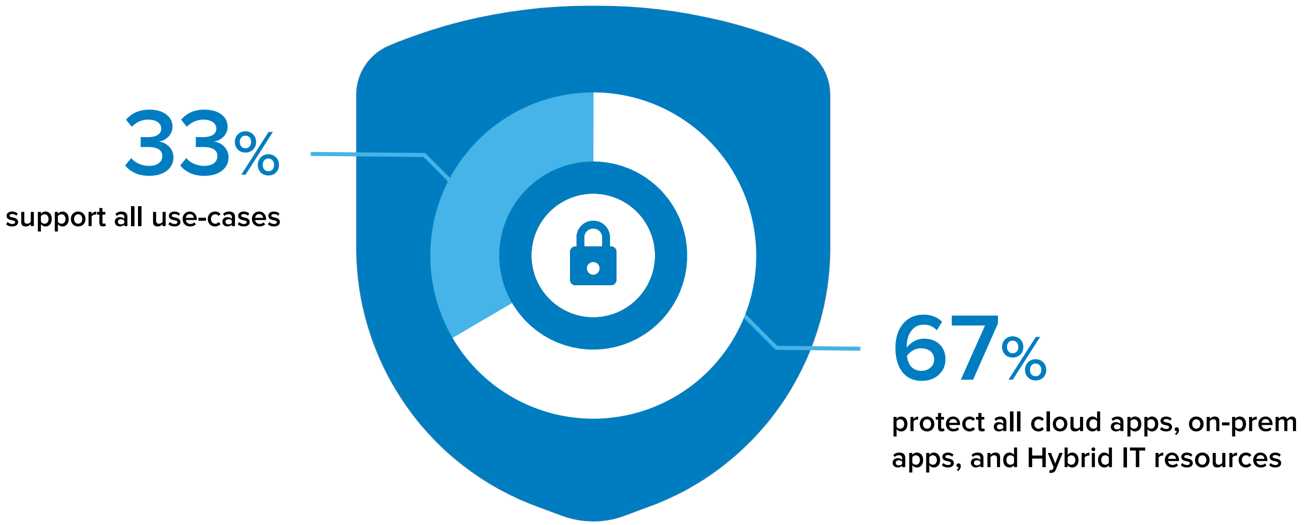
	North American Executives	European Executives	IT Practitioners
Cloud applications (SaaS)	**84%**	**75%**	**73%**
Platform as a service (PaaS)	**75%**	26%	47%
Mobile apps	**81%**	48%	38%
Infrastructure as a Service (IaaS)	**63%**	21%	36%
On-premises servers	31%	**56%**	**66%**
On-premises web apps	29%	22%	26%

Most executives and practitioners want to use cloud-based security to protect as many of their cloud resources as possible, with North American executives leading the way. On the flip side, European executives and IT practitioners are highly interested in securing their on-premises servers with cloud identity. We believe this trend is influenced by the rise of modern infrastructure approaches such as automation and DevOps, which are not supported by most on-prem Privilege Access Management (PAM) solutions.

Why organizations don't have a centralized IAM

In the survey, we asked the leaders and admins that claim their organizations don't have a centralized IAM solution why they think they don’t have centralized IAM. 67% of the respondents – 2 out of 3 people – claim that their current IAM solution lacks the ability to protect their hybrid IT environment.

I don't have IAM and configuration solutions centralized in a single place because a single solution does not...



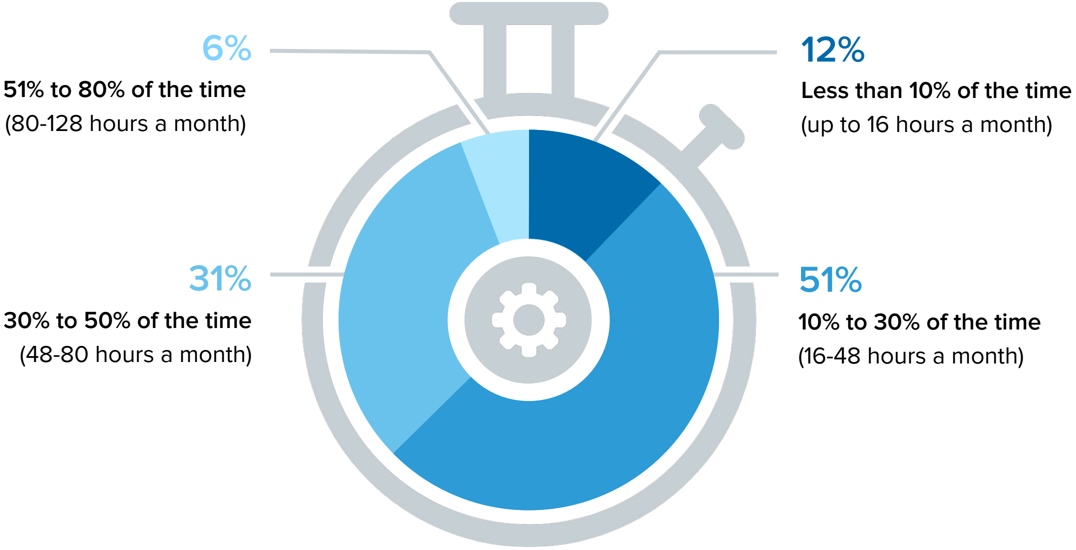
We believe these organizations have a better awareness of their identity stack. However, we also believe those respondents are hindered by their current legacy IAM solutions and the lack of capabilities for supporting cloud and on-prem resources.

The correlation between hybrid complexity and maintenance

Research analysts and identity specialists believe the use of multiple IAM solutions draws a correlation to a higher TCO related to licensing, support costs, and multiple vendors, as well as recurring maintenance costs. A Forrester report says that organizations can lower their ongoing maintenance rate by 30% to 35% by using a single IdaaS solution to protect both cloud and on-prem resources [4].

To validate this belief, we asked our respondents in the largest organizations:

How much time their IT departments spent on maintenance tasks such as installing and patching systems, managing network errors, and backing up the infrastructure?



Organizations with >5,000 employees

82% of the larger organizations spend at least 16 hours a month per IT professional in maintenance tasks. For 31% of those organizations, the number of hours reaches as high as 80 hours a month per person. The effort on maintenance can reach up to a third of the overall IT effort in larger organizations.

To see how organizations could benefit from time saved on maintenance, we asked our leaders and practitioners what would they do if they didn't spend so much of their time on maintenance. Both leaders and practitioners agreed they would spend the extra time on strategic initiatives that transform their business and impact the bottom line:

Solve key business challenges

Proactively discover and mitigate security threats

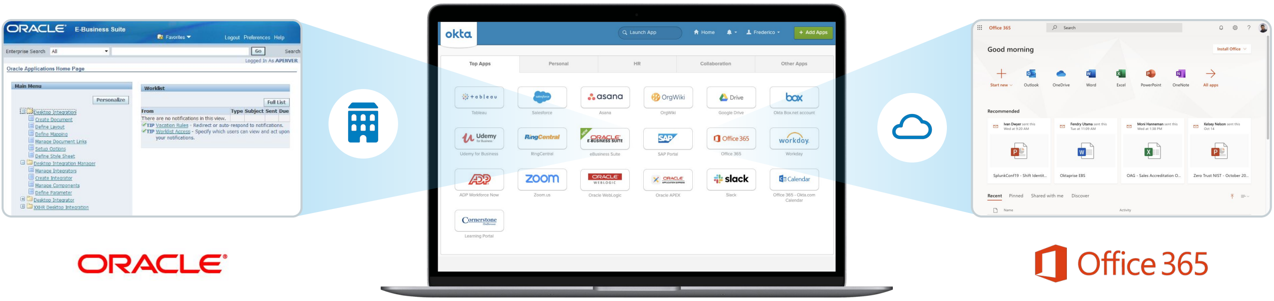
Identify new and disruptive technologies

Other

Value of modern IAM

Hybrid IT is here and isn't going away anytime soon. That fact drives the value in turning to a modern, centralized cloud security solution that can protect both cloud and on-prem resources.

Okta Identity Cloud and its new product Okta Access Gateway solve that disconnect. Okta can act as your single identity provider and control access to your resources, whether they exist in the cloud or on-prem. Okta unifies your security policies and user experiences with centralized management, while dramatically reducing administration costs and time. Additionally, Okta strengthens your security by consistently employing modern access management measures across all your hybrid IT resources. That allows you to migrate away from the security risks of deprecated on-prem access management platforms and relying on modern IAM throughout your hybrid IT environment.



With Okta, organizations can control access to the Hybrid IT from a single solution

To learn more about how Okta delivers the benefits of modern IAM for your entire hybrid IT environment, visit www.okta.com/products/access-gateway or contact a sales representative at www.okta.com/contact-sales.

---

[1] Rightscale 2019 State of the Cloud Report from Flexera.

[4] Forrester Wave: Identity-As-A-Service, 2017

About Okta

Okta is the leading provider of identity for the enterprise. The Okta Identity Cloud connects and protects employees of many of the world's largest enterprises. It also securely connects enterprises to their partners, suppliers and customers. With deep integrations to over 5,000 apps, the Okta Identity Cloud enables simple and secure access from any device. Thousands of customers, including Experian, 20th Century Fox, LinkedIn, Flex, News Corp, Dish Networks and Adobe trust Okta to 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. For more information, visit us at www.okta.com or follow us on www.okta.com/blog.