The Business Value of Okta Workforce Identity

Jay Bretzmann
Research Vice President,
Security Products, IDC

Megan Szurley
Senior Research Analyst, Business
Value Strategy Practice, IDC

Table of Contents

CLICK BELOW TO NAVIGATE TO EACH SECTION IN THIS DOCUMENT.

Executive Summary

For most organizations, identity and access management (IAM) systems were assembled from many disparate pieces associated with years of IT technology deployment, ranging from legacy on-premises and homegrown to third-party vendor services.

Invariably, most of these approaches became silos of identity information, prohibitively expensive to maintain, and dated in their capabilities such that organizations became noncompliant with industry and governmental regulations. Recognizing that these systems led to time-consuming IT undertakings, stifling operational agility and innovation, many organizations turned to alternate, best-of-breed solutions for their workforce identity needs.

IDC conducted research that explored the value and benefits for organizations that were using Okta Workforce Identity to securely manage access for their employees, contractors, and business partners with features including, but not limited to, single-sign on (SSO), life-cycle management, and multifactor authentication (MFA). The research included interviews with four organizations that had deep knowledge and experience with the value achieved from deploying and using Okta Workforce Identity.

Overall, IDC calculated that study participants achieved considerable business value by:

- **Improving operational efficiencies and reducing administrative costs** for IT staff by automating and streamlining complex administrative processes into a central, easy-to-use service

- **Enhancing workforce productivity** by providing fast, seamless, and reliable access to applications and systems regardless of location or device, along with greater self-service capabilities

- **Strengthening enterprise security** by implementing security features for all user types and resources across the organization

Business Value Highlights

Click each highlight below to navigate to related content within this document.

54% more efficient IAM IT administration and maintenance teams

72% more efficient IAM IT infrastructure teams

5% enhancement in workforce productivity

48% more efficient security teams

72% reduction in time to respond to security incidents

42% reduction in time to detect security incidents

77% reduction in unplanned downtime

Situation Overview

This IDC report examines the experiences of four companies using Okta to securely manage identities and access for their workforce users. When IT fragmentation and hybrid work are the new normal, the perimeter is no longer at the network edge — identity is the most important line of defense. Attackers aren't breaking in, they're logging in.

Employees, contractors, and partners are all given workforce identities, which are being used to access critical resources from unmanaged devices (BYOD) to perform their jobs. These identities need to be protected, as compromised credentials have become the leading attack vector for cybercriminals, but they must also be very accessible to not become a burden that impedes people from performing their intended roles. Sounds fairly straightforward, but it isn't.

> When IT fragmentation and hybrid work are the new normal, the perimeter is no longer at the network edge — identity is the most important line of defense. Attackers aren't breaking in, they're logging in.

The Business Value of Okta Workforce Identity

Study Demographics

To explore the benefits achieved with Okta Workforce Identity, IDC interviewed four organizations that were located in North America, Europe, and Australia. These interviewees had in-depth knowledge of their organizations' overall deployment and usage of Okta and answered a wide range of qualitative and quantitative questions regarding the solution.

As shown in **Table 1** (next page), the organizations ranged from 3,000 to 14,000 employees, with an average company size of 7,800 employees. There was a total of 271 IT staff who were supporting 288 business applications. A variety of verticals were represented in the research, including hospitality, education, nonprofit, and professional services.

TABLE 1

Firmographics of Interviewed Organizations

	Average	Median	Range
Number of employees	7,800	7,125	3,000 to 14,000
Number of IT staff	271	265	55 to 500
Number of IT staff dedicated to identity service administration	5	6	2 to 7
Number of help desk staff	37	40	7 to 60
Number of business applications	288	200	150 to 600
Total organizational revenue	$1.5B	$1.3B	$700.0M to $2.8B
Countries/regions	North America (2), Europe, Australia		
Industries	Hospitality, education, nonprofit, professional services		

n = 4; Source: IDC In-depth Interviews, March 2023

Selection and Usage of Okta Workforce Identity

Interviewed organizations looked to solve many operational and security concerns related to identity and access management when selecting Okta. Prior to deploying Okta, interviewed organizations shared a common set of challenges, including poor identity system performance and reliability that left their workforces vulnerable to disruptive outages, reliance on highly manual processes for IT teams that distracted them from more strategic tasks, and inconsistent and weak access controls that compromised enterprise security.

Interviewed organizations cited the following reasons for selecting Okta:

The need for a reliable, scalable service:
"We've been Okta customers since 2013, and prior to that, we had a home-built identity service backed by active directory, which became increasingly unreliable, unscalable, and outage-prone."

A centralized access management system:

"I think some of the things that we had issues with prior to Okta Workforce Identity was centralizing our apps into one place and having one place where we can identify who are corporate users, who are contractors, who are vendors, how do we give them access into our systems, and then also the aspect of single sign-on. That was something that was very important for the employees being that we have access to so many applications. Having it all in one place made it much easier for them not to have to remember a million passwords."

Simple deployment and administration:

"Okta is efficient to use. There is no way that my organization could have used the large number of apps that we do without Okta. We have better security and visibility because we have all these apps behind one identity provider. Employees no longer need to fight the system and ponder about passwords used across multiple applications."

Security controls alongside usability:

"The MFA provided by Okta Workforce Identity is MFA [that] is above and beyond. MFA is the biggest thing that has had an impact. Okta Workforce Identity limits the attack factor and that has been huge from a security perspective. Okta Workforce Identity has also enabled us to have a pattern in place; we are able to schedule the work and when people are adding a new application. Our team knows that every application should be using MFA moving forward, and they associate IAM and Okta."

"The most significant benefit of Okta Workforce Identity has been the ability to apply security policies at scale easily. We also benefit from some of the Okta security features that are locally based in France. Okta knows about bad actors, can recognize bad behavior, and, as a result, just lock that kind of behavior. Okta's built-in security protections are a big benefit."

Consistent SSO and MFA from cloud to on-prem:

"Before deploying Okta Workforce Identity, we had inconsistencies with using single sign-on and we had very little multifactor integration at all. We thought the multifactor was going to be really critical and wanted to use the multifactor for any application, in addition to using SSO. My organization wanted a standardized approach to cloud or remote access so that we are fully protected."

Compliance with broad industry mandates and regulations:

"Okta Workforce Identity has given us the ability to provision. Where my organization has looked to do provisioning and deprovisioning, Okta Workforce Identity has been a big deal for us. We also have to abide Sarbanes-Oxley Act (SOX) and Payment Card Industry (PCI) regulations, so Okta Workforce Identity helps us make sure that the applications are meeting SOC and PCI standards. Okta makes it easier for us to put security around our applications and ensure that we comply to standards."

Worldwide expert support services:

"When we selected Okta Workforce Identity, it was the only identity-centric provider that had opened up in Europe. We did not want to go that all-in with an American-represented business only to be faced with time zone challenges and whatnot. Okta was in London, so that was close enough for us that we could work with them within our work hours."

Okta had a wide footprint across the many business applications in use at interviewed organizations. In fact, 97% of all business applications used Okta. As shown in **Figure 1,** MFA and SSO were the Okta products used with the most frequency and across the majority of applications.

FIGURE 1

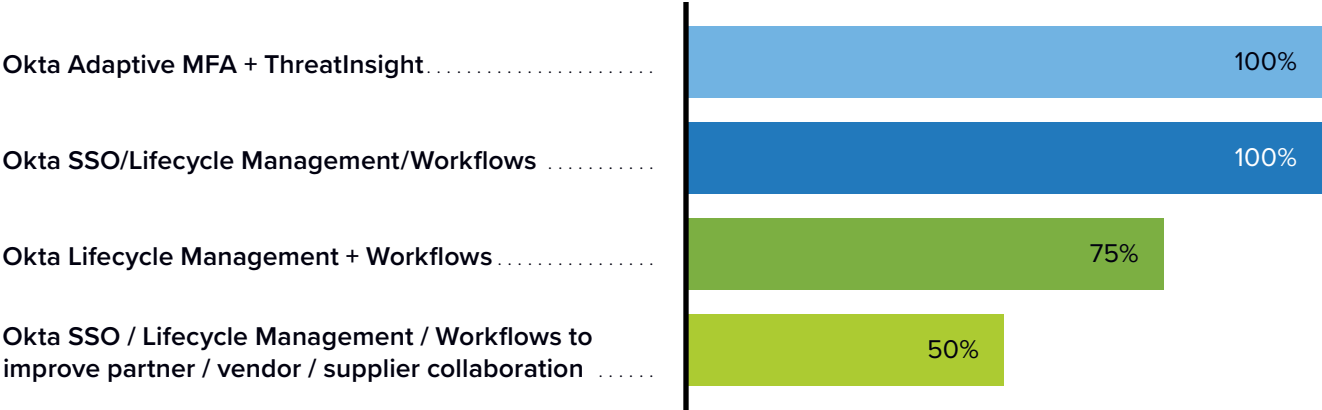**Organizational Application Usage of Okta Workforce Identity**
(Number)
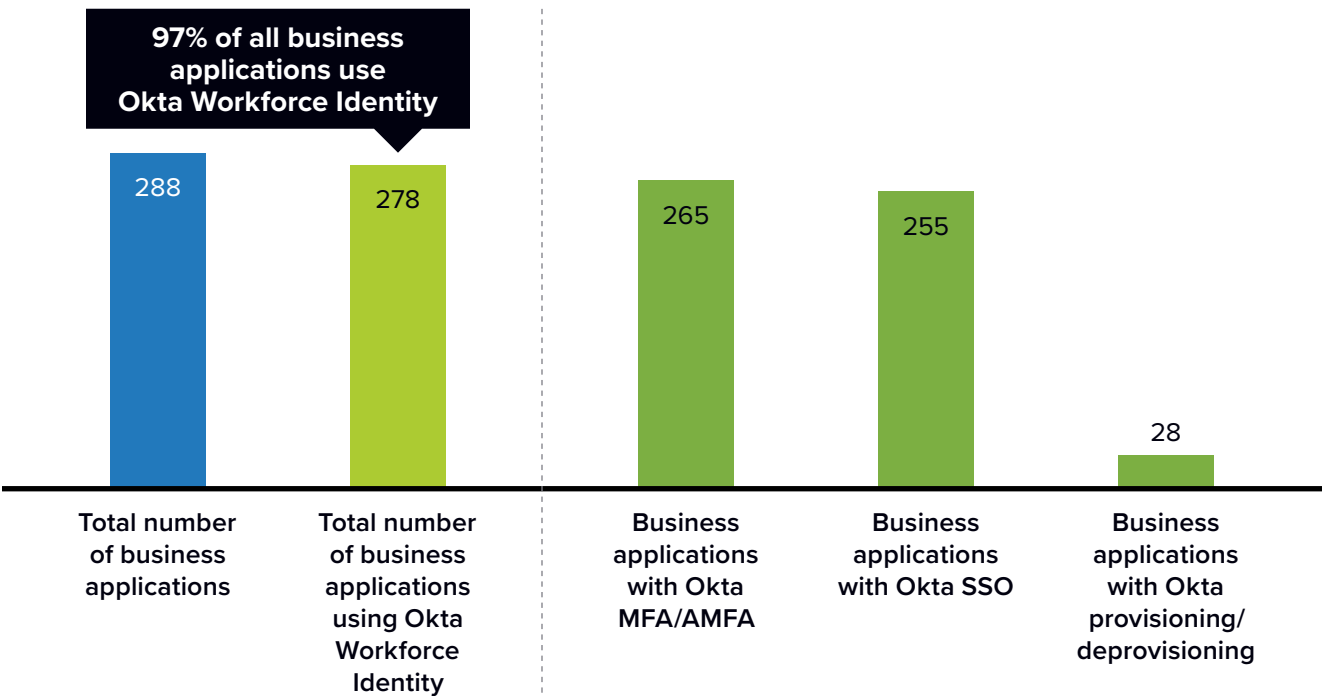
n = 4; Source: IDC In-depth Interviews, March 2023

In addition to SSO and MFA, Okta offered interviewed organizations a variety of valued products and features, such as Lifecycle Management, Workflows, and ThreatInsight. **Figure 2** (next page) demonstrates Okta Workforce Identity used in a multitude of combinations and ways.

FIGURE 2

Organizational Usage of Okta Workforce Identity Features
(% of organizations)

Okta Adaptive MFA + ThreatInsight **100%**

Okta SSO/Lifecycle Management/Workflows **100%**

Okta Lifecycle Management + Workflows **75%**

Okta SSO / Lifecycle Management / Workflows to improve partner / vendor / supplier collaboration **50%**

n = 4; Source: IDC In-depth Interviews, March 2023

IT Staff Efficiency Improvements

In deploying and using Okta, IDC noted that several IT-related positions were more efficient and effective in their daily work. Okta's platform helped IT teams spend less time managing and supporting the service itself and more time supporting strategic business initiatives. As new identity features rolled out, IT professionals could learn and apply them to their organization swiftly, without needing to code or rely on courses or third-party guidance. Automation was introduced for provisioning and deprovisioning of access, and application deployments and integrations were accelerated with Okta's extensive prebuilt connectors. Okta also decreased help desk tickets and associated costs because end users could leverage self-service capabilities to reset their passwords without guidance from IT.

Interviewed organizations discussed these IT-related benefits in greater detail:

Simplified, centralized identity access management:
"I think for IT, identity access management is so much easier, especially for things like our service desk. The users have the ability of resetting their passwords and going in there themselves so there's a lot of self-service in there. Help center calls have decreased as a result of using Okta. It's very easy and intuitive. As we roll out functionality — like right now, we are looking to roll out password list technology within Okta — the users are getting very used to the system. They love the fact that they can go to the Okta dashboard and see their apps in there and not have to remember all the passwords that they have. It has been a great thing for the user experience."

A unified view of identities across the workforce:
"Our IT people benefit from Okta because they are able to access applications as administrators in Okta. This enables them to see their whole application world, how it's secure, and who they give access to. Okta gives them a big picture of their world."

Automation of manual IT operations (e.g., onboarding, provisioning access):
"Identity providers like Okta have made their way into the world to help people. But that manual management just chips away at all your time. Standardizing on Okta really has helped us have a common tool for providing access to applications and onboarding processes. I think that the familiarity with Okta has really helped us tighten or improve our turnaround time for getting applications available to end users."

Intuitive solution:
"My engineer loves Okta so much. Any new features that come out, he is able to learn this on his own. He really hasn't had to go and take courses for several weeks to understand the system. The system is very intuitive. So that's what he loves about it. It's not hard to figure out."

IDC first evaluated the impact of Okta on IT infrastructure teams, responsible for deploying, administering, and managing systems that are critical to an organization. This team appreciated the automation, cloud-first approach, extensive integration ecosystem, and process standardization provided by Okta. These features helped the IAM IT infrastructure team maintain, build, scale, and upgrade identity access across their IT infrastructure with greater speed and effectiveness. One organization noted, *"Before Okta, there were four people that were adding and removing users and groups. They were doing really basic things. We are now much more strategic in the sense that we have some automation with Lifecycle that we didn't have before. We have a clear process for adding and removing programs, adding MFA if it's cloud-based, and we have got a privilege access solution in place now that was nonexistent before. The consistency with Okta has actually freed up our resource time so we can do much more within the identity realm besides just Okta."* **Table 2** shows that IAM IT infrastructure teams were 72% more efficient with Okta than they were with their previous solution, which equated to a value of staff time per year of $408,472.

TABLE 2

IAM IT Infrastructure Team Efficiencies

	Before Okta	With Okta	Difference	Benefit
Total FTE count	5.7	1.6	4.1	72%
Value of staff time per year	$566,667	$158,194	$408,472	72%

n = 4; Source: IDC In-depth Interviews, March 2023

IDC then focused on the impact of Okta on IAM administration and maintenance teams, which were inclusive of DevOps and engineers. These teams were ultimately responsible for the ongoing administration and maintenance of workforce identity across their organization. They benefited from increased automation and centralized identity administration with Okta while gaining a unified view of their workforce population. This enabled IT, DevOps, and engineers to more efficiently manage all identity-related tasks, release business-critical applications and innovations faster, and lower enterprise risk with better enforcement and visibility into security policies. An organization stated, *"We had to provide a digital customer feedback mechanism and work together with Trilio and by proxy would ask some of the partners to do some heavy lifting there, but this was together with programming and different countries and also a whole new kind of theme toward that beneficiary approach to give kind of a complaint mechanisms feedback system. We have that now in 13 countries, and it's still ongoing as kind of a project and we are building on that."* IDC calculated that IAM administration and maintenance teams were able to work with 54% greater efficiency, which was valued at $349,352 in staff time per year (see **Table 3**).

TABLE 3

IAM Administration and Maintenance Efficiency Impact

	Before Okta	With Okta	Difference	Benefit
Total FTE count	6.4	2.9	3.5	54%
Value of staff time per year	$641,667	$292,315	$349,352	54%

n = 4; Source: IDC In-depth Interviews, March 2023

It was made clear by organizations that they valued the automation Okta provided. As seen in **Figure 3** (next page), Okta enabled IT teams to automate 73% more tasks than they had been able to in the past. Okta made identity management easier and less time-consuming for IT teams. As stated by one participant, *"The biggest benefits of Okta is it is fast and secure. We've also fully automated onboarding and offboarding for employees and contractors using the Identity Lifecycle Service."* Okta also became an integral driver of robust security policies across interviewed organizations and quickly integrated with new applications. This easy integration enabled organizations to release 15% more new applications per year across their workforce. Another organization noted, *"My organization can now launch applications overnight. Previously, that would be hard to even imagine."*

FIGURE 3

IT IAM-Related KPIs

(% more)

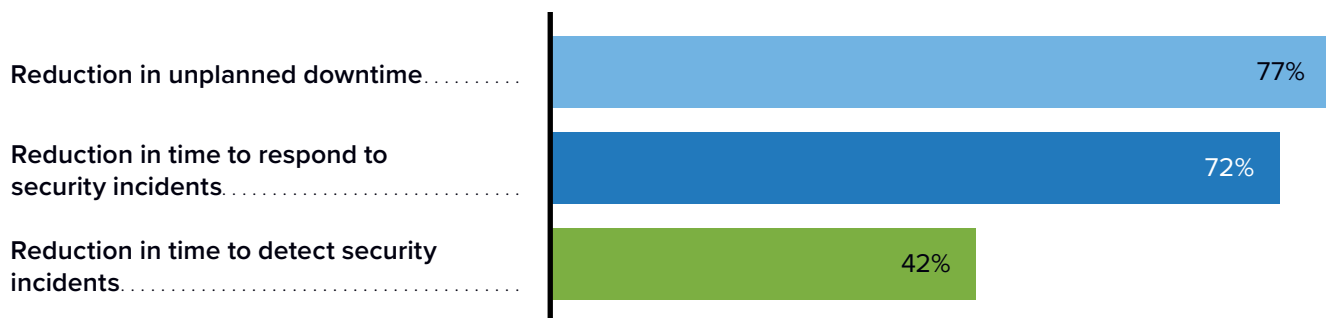|	
Tasks automated	73%
New applications released per year	15%
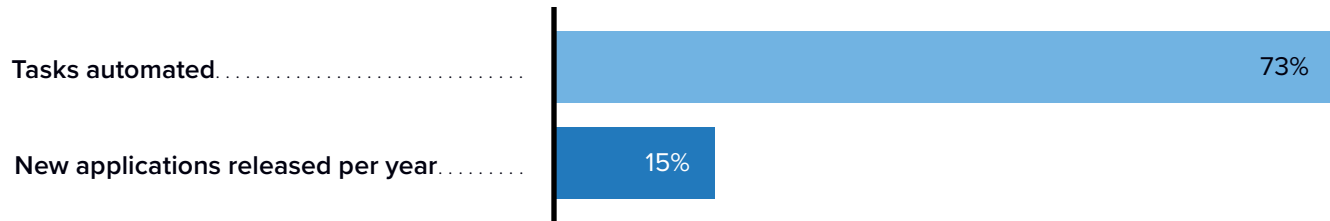
n = 4; Source: IDC In-depth Interviews, March 2023

IDC also observed that the security teams from interviewed organizations benefited from Okta. It was made clear that this team greatly appreciated and used the MFA solution provided by Okta. Using Okta resulted in far less organizational risk and, as a result, enabled the security team to work with 48% more efficiency. This permitted the team to spend more time focusing on other pressing security concerns or innovation. One study participant elaborated, *"We are better poised to focus on important identity security questions as opposed to getting hit with, for example, brute force attacks. Workforce brute force attacks don't matter anymore because they can't get past MFA."*

Figure 4 illustrates the key performance indicators (KPIs) that security teams achieved from the deployment and usage of Okta Workforce Identity. As shown, they were able to drastically reduce downtime, by 77%. In addition, Okta Workforce Identity enabled them to significantly reduce the time to detect (42%) and respond to (72%) security incidents.

FIGURE 4

Security Team IAM KPIs

(% reduced)

Reduction in unplanned downtime	77%
Reduction in time to respond to security incidents	72%
Reduction in time to detect security incidents	42%

n = 4; Source: IDC In-depth Interviews, March 2023

Workforce Productivity Enhancements

Okta had an exceedingly positive impact on the overall workforce of interviewed organizations. Okta was very intuitive for the average business application user. It decreased the overall workforce dependency on help desk staff by enabling users to manage and reset their passwords without external assistance. These self-service capabilities enhanced the overall productivity of business units. Okta also broke down organizational silos between IT and business units by enabling strong communication and collaboration.

Study participants further detailed these workforce enhancements:

Intuitive solution for end users:
"Okta is very intuitive for end users because they are able to self-service themselves with the included features. The number of calls to the service desk is much less, and any new features that pertains to self-service, they are very easy to teach. It's a very simple experience for the end user. So they spend less time at the service desk because it's very intuitive."

Increased collaboration:
"Okta has helped my organization break down silos and increase collaboration. It has the ability of giving us a lot of different roles within the system; we can get infrastructure, operations, and other teams exactly what they need to do within the system. It is very, very easy to engage with other teams because of the system."

Easier integration of acquired organizations:
"If my company was to merge/purchase another company, it would be very easy to integrate their systems with ours. I would see Okta helping us in the sense that if we ever acquired anything in the future, Okta will make it very easy for us to do that."

IDC closely assessed these workforce productivity enhancements (exclusive of IT staff) related to the organizational use of Okta. **Table 4** (next page) quantifies these productivity enhancements and shows an annual end-user productivity gain of 5% from Okta usage. Factoring in an operating margin of 15%, IDC valued this end-user productivity-based gain at $1.81 million.

TABLE 4

Workforce Productivity Enhancement

	Before Okta	With Okta	Difference	Benefit
Equivalent productivity level (FTEs)	3,281	3,454	172	5%
Total FTE count (net)	3,281	3,307	26	1%
Calculated value of productivity	$229.68M	$231.50M	$1.81M	1%

n = 4; Source: IDC In-depth Interviews, March 2023

Challenges and Opportunities

Most identity security projects are large efforts aimed at replacing unsustainable, unreliable, and fragmented systems. The diversity of applications, devices, and users add another layer of complexity for organizations looking to modernize and secure their workforce identity systems.

The goal of every workforce identity project should be to move as much as possible to a cloud environment. Cloud services offer unprecedented levels of agility, as there's no hardware to acquire and deploy on a customer's premises, and software updates happen frequently, with no downtime. All businesses should be following a cloud-first identity services approach, working with vendors that provide content to be configured rather than customized.

Conclusion

Identity systems touch just about every single employee in an organization, along with third-party contractors and goods-and-services providers. This IDC study documented the differing types of benefits Okta Workforce Identity delivered to IT infrastructure and maintenance teams, security teams and groups of application users, who all benefited from a cloud-native approach over what historically had been a collection of on-premises solutions.

By moving to Okta, organizations told us that for the first time, they were able to see everything related to their IT operations in one place and radically improve efficiencies by providing an intuitive user interface, automating manual tasks, providing self-service capabilities, rolling out new applications more quickly, and redeploying people to do higher-level tasks. Okta has dramatically simplified application access and removed some of the biggest security threats organizations across all industries face.

Appendix: Methodology

IDC's standard Business Value methodology is based on gathering data from organizations currently using Okta Workforce Identity as the foundation for its model.

Based on interviews with organizations using Okta Workforce Identity, IDC calculates benefit metrics by:

- Measuring the savings from reduced IT infrastructure costs, IT staff efficiencies, increased user productivity, and higher revenue over the term of the deployment attributable to their use of Okta Workforce Identity

IDC bases calculations on a number of assumptions, which are summarized as follows:

- Time values are multiplied by burdened salary to quantify efficiency and productivity savings. For this study, IDC used its standard salary assumptions of an average fully loaded IT salary of $100,000 per year and user salary of $70,000 per year.

- Downtime values are a product of the number of hours of downtime multiplied by the number of users affected. The impact of unplanned downtime is quantified in terms of impaired end-user productivity and lost revenue. Lost productivity is a product of downtime multiplied by burdened salary.

- IDC applies a margin assumption (15%) for other user productivity gains and additional gross revenue attributed to interviewed organizations' use of Okta Workforce Identity, resulting in the net productivity and revenue calculations applied to IDC's model.

Note: All numbers in this document may not be exact due to rounding.

About the IDC Analysts

Jay Bretzmann
Research Vice President, Security Products, IDC

Jay Bretzmann is research vice president for IDC Security Products, responsible for Identity & Digital Trust and Cloud Security. Jay focuses on identity management, privileged access management, identity governance, customer identity management, and a multitude of other identity and cloud security topics.

More about Jay Bretzmann

Megan Szurley
Senior Research Analyst, Business Value Strategy Practice, IDC

Megan Szurley is a consulting manager within IDC's Custom Solutions Division, delivering consultative support across every stage of the business life cycle: business planning and budgeting, sales and marketing, and performance measurement. In her position, Megan partners with IDC analyst teams to support deliverables that focus on thought leadership, business value, custom analytics, buyer behavior, and content marketing. These customized deliverables are often derived from primary research and yield content marketing, market models, and customer insights.

More about Megan Szurley

Message from the Sponsor

okta

Okta provides a unified identity solution to address the broadest set of identity-based use cases.

With an identity-powered approach to security, you can protect your users and resources — regardless of location and device — with the most secure, reliable identity and access management platform that seamlessly integrates across your entire tech stack. From a user's first day to their last, you can ensure users have access to everything they need, and only when they need it, easily and securely.

Reach out to learn more

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. This IDC material is licensed for <u>external use</u> and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.

⊜IDC

IDC Research, Inc.
140 Kendrick Street, Building B, Needham, MA 02494, USA
T +1 508 872 8200

@idc   **@idc**   **idc.com**

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.