Omada

The State of Identity Governance 2024

Contents

Executive Summary

The convergence of digital transformation and the hybrid workforce has introduced substantial complexities into identity and access management procedures. These factors have emerged as primary catalysts for the modernization of identity governance. Consequently, the management of identities and their associated permissions has evolved into a pivotal component of cybersecurity strategies. However, a successful approach to identity governance must strike a balance: enhancing an organization's security while also facilitating business agility in the context of end-user workflows.

> "Over 95% of Senior IT and security leaders report grave concerns about identity-related threats"

Identity governance is essential to enhance visibility and streamline provisioning without hindering employee productivity. This underscores the significance of adopting a modern approach to identity governance and administration (IGA). But what is a modern IGA approach? Modern identity governance solutions embrace a SaaS-based model for scalability and use analytics and automation to enhance both efficiency and security. They automate the fine-grained provisioning of access controls, as well as identifying and addressing over-provisioned and underused identities. They offer seamless connectivity to broader identity frameworks and business applications, and they possess the ability to effortlessly create identity workflows for all enterprise identities.

To shed light on the intricate world of identity governance, we conducted a comprehensive survey involving 567 enterprises with more than 1,000 employees across the United States, including the perspectives of both IT and business leaders. We surveyed people responsible for identity governance and access management, compliance, cybersecurity, and general IT administration and management.

Key Findings

CISO/CSO/CIOs are highly concerned with identity-related threats and over-permissioned account access

Over 95% of senior IT and security leaders report grave concerns about identity-related threats, possibly due to over-permissioned access to systems and applications. In fact, 72% of respondents agreed that users have unnecessary access and overly permissive accounts. Organizations using legacy IGA are up to 20% more concerned about identity-related threats than organizations using modern IGA.

Enterprises are accelerating plans to leverage SaaS-based IGA with generative AI, fast import, adaptability and advanced connectivity

When asked which capabilities are most important, more than 61% put "adaptability to an organization's requirements" among their top five. Of those surveyed, 53% chose generative AI. More than 42% prioritize the ability to handle complex identity workflows. Nearly 56% look for a connectivity framework that supports any application and infrastructure, and 41% choose interoperability and data sharing with all IAM tools as priority capabilities. In addition, 47% look for a SaaS-based identity governance solution with faster data ingestion, and just over 40% prioritize the ability to synch quickly to onboard applications and enable users to gain access in minutes.

Best-of-breed IGA wins out over platform plays

To achieve higher performance levels, a substantial majority of respondents agree (86%) that their organizations are more likely to choose a best-of-breed identity and access management (IAM) solution rather than a single vendor that may not offer robust capabilities across the board. This is very likely why more than half of respondents identified adaptability and connectivity as critical IGA solution features.

Survey Observations

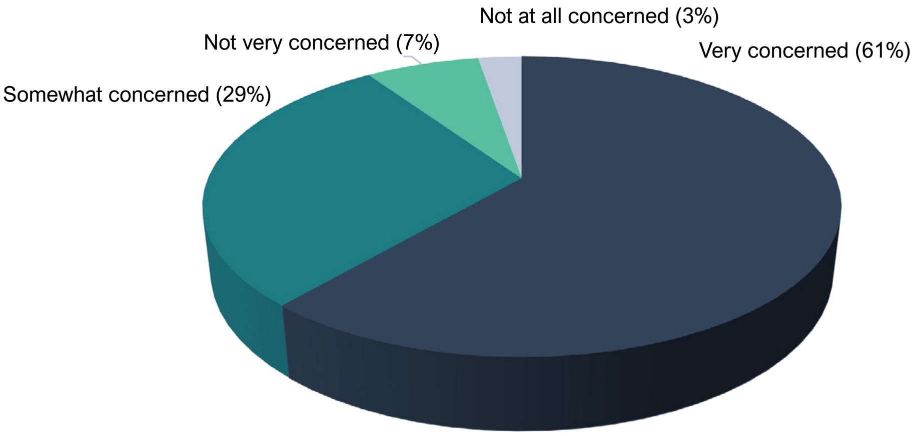
The good and the bad news on identity cybersecurity threats

How concerned are organizations with cybersecurity threats? Depends on who you ask and what you ask them.

When asked about security hygiene-related practices, 93% of respondents agreed their organization uses strong identity verification; 92% say they can quickly identify anomalous behavior and shut down suspect accounts. And 91% say they can easily meet new business requirements, while 89% say they can easily produce regulation-specific reports.

Given respondents' extreme confidence in their security hygiene practices, one would think that their overall concern with identity-related threats would be quite low. The results turned out to be far from what was expected: over 90% of respondents are concerned with the risks of identity-related cybersecurity threats.

Overall, how concerned is your organization with the risks of identity-related types of cybersecurity threats?



Levels of concern, however, vary somewhat based on one's role in the organization. Overall, more than 95% of senior managers (CISO, CSO and CIO) report they are "very concerned,"; yet just 87% of compliance, identity and access managers and 91% of cybersecurity engineers, analysts and managers share that same urgencyworry.

IGA vintage matters

Fear of cybersecurity threats are higher for organizations using legacy IGA solutions. When asked about specific identity-related threats, respondents using legacy and in-house-built IGA reported significantly greater concern overall. In terms of the risk level to their organizations, respondents identified malware, identity security breaches and vulnerability exploitation as the top threats they're concerned about.

Not far behind these are concerns about access to compromised accounts of users, privileged accounts and remote users.

But what is quite telling is how those organizations using a modern IGA solution differed in their concern level. Depending on the specific threat, there is a range of 9% to 21% difference in how organizations respond. See the following table for a detailed breakdown of identity-related threat concerns.

Comparison of responses from Legacy IGA and Modern IGA users when asked which identity threats are concerning

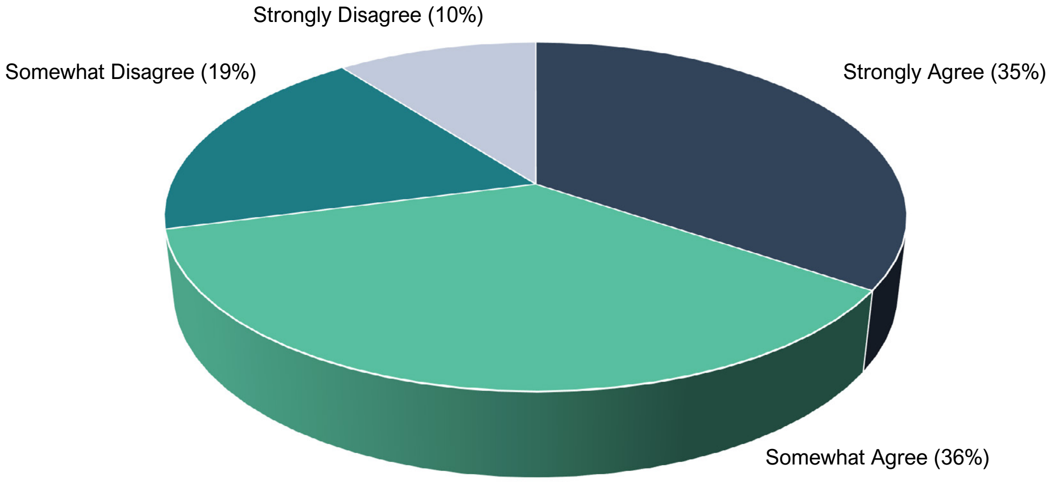
	Legacy IGA	Modern IGA
Malware designed to steal credentials	63.4%	50.2%
Exploit of a vulnerability to compromise a user or service account	63.4%	47.5%
Identity security breach	62.6%	49.4%
Unauthorized access to sensitive data by external attackers	60.0%	47.9%
Compromised user credentials	59.1%	49.8%
Compromised service accounts	58.3%	39.3%
Unauthorized access to sensitive data by a known third party	57.9%	46.7%
The misuse of a privileged account by an employee	57.4%	38.9%
Compromised remote user credentials	57.9%	39.3%
Compromised privileged accounts	54.9%	43.2%
Unauthorized access to sensitive data by employees	54.0%	45.9%
Improper separation of duties	49.0%	28.8%

Too much access is a concern

Unnecessary access to systems and applications and overly permissive accounts are widespread concerns. With these heightened, it would stand to reason there would be strong controls and processes in place to ensure that only those who need access to applications and data have it and that access would be deprovisioned when it is no longer needed. However, this is only true in theory, not reality.

Almost three-quarters of respondents (72%) think people in their organizations have access to systems and applications to which they don't need access and/or have overly permissive accounts that cause unnecessary risk. When users have access to systems and applications they no longer need access to or have access that is excessive for their role, the level of impact on identity for these users is unnecessarily higher than it would be if their access was properly managed. Given this, it's no wonder so many of them are very concerned about identity-related threats.

Some people in my organization have access to systems and applications to which they do not need access and/or have overly permissive accounts that cause unnecessary risk

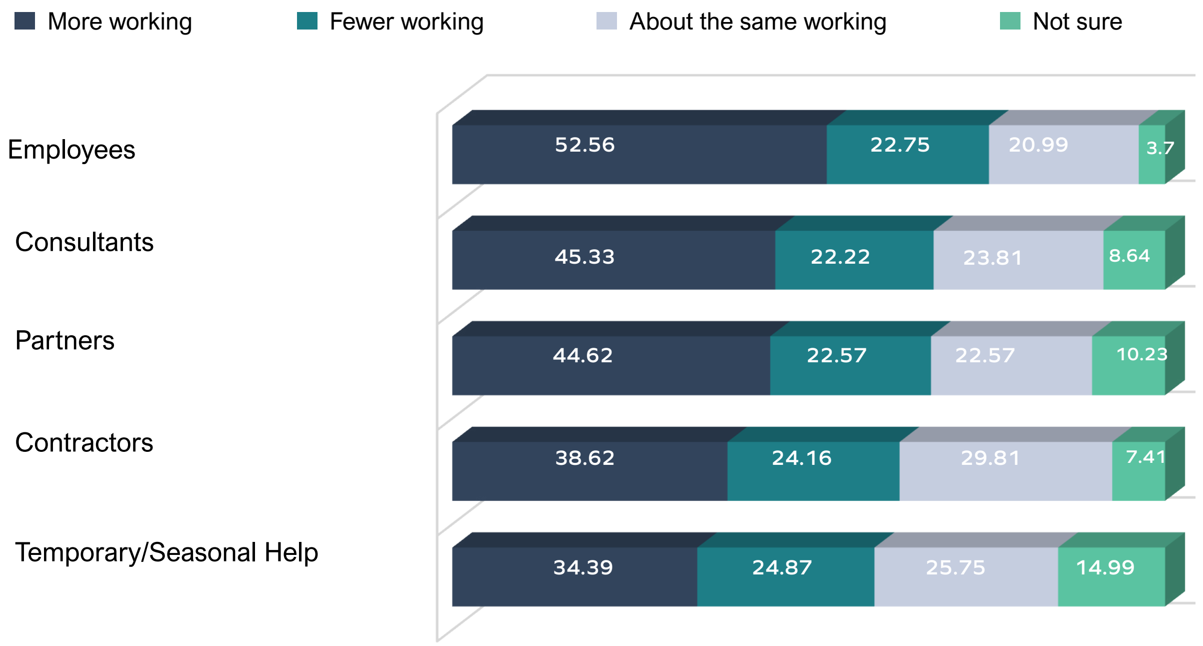


Remote work continues to grow

Most organizations are still struggling to manage more remote worker and third-party identities since the start of COVID. Organizations have 52% more employee identities, and known third parties have more employee identities by these amounts: partners (46%), consultants (47%), contractors (39%) and temporary/seasonal (35%).

This dramatic change has created security and identity challenges for IT teams across all industries. Uncertainty about how these different users are handled can elevate the risk of compromised accounts and unauthorized access through negligence, malicious insider threats, phishing and other social engineering tactics.

How has the number of identities working remotely in your organization changed since COVID?

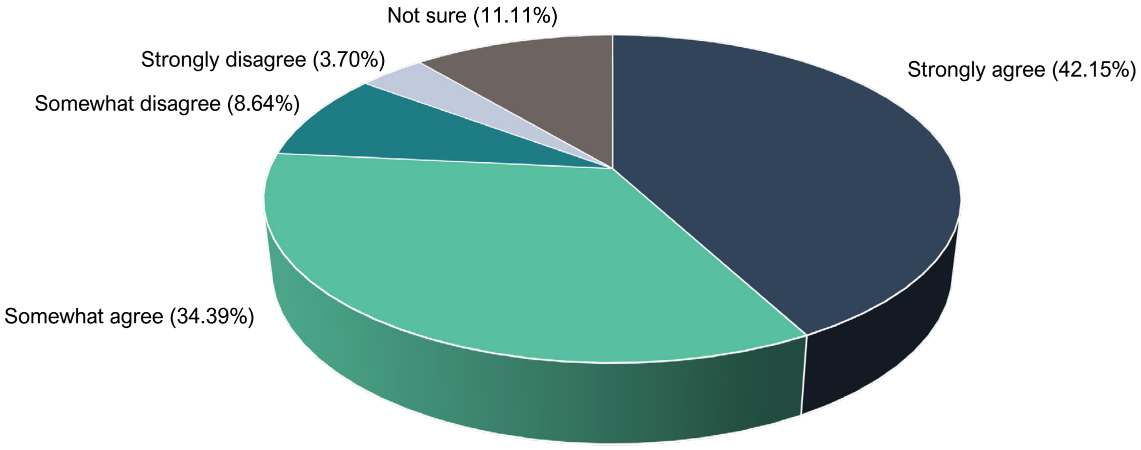


The best-of-breed beats platform plays

More than 76% of organizations choose best-of-breed IAM solutions rather than a platform. An IGA solution that connects with other best-of-breed identity and access management (IAM) solutions as part of a larger identity fabric enables organizations to ensure they are using the most dynamic technology across the board.

Single vendors offering multiple IAM solutions as part of a platform; for example, may offer a decent option in one part of their identity platform but a less-than-ideal option in others. There are several reasons why this could be, from talent drain after acquiring a part of the platform to the technology not being a leader in its category to not being fully integrated into the platform suite the vendor offers. Also, because these vendors offer many solutions under one product, they tend to lack the ability to connect with other IAM solutions, forcing customers to use inferior technology simply to get a single part of their identity fabric that they need.

My organization tends to choose best-of-breed identity and access management solutions (e.g., IGA, PAM, CIEM, DAG, ITDR, etc.) rather than a platform product from a single vendor that offers multiple solutions.



New IGA shopping list

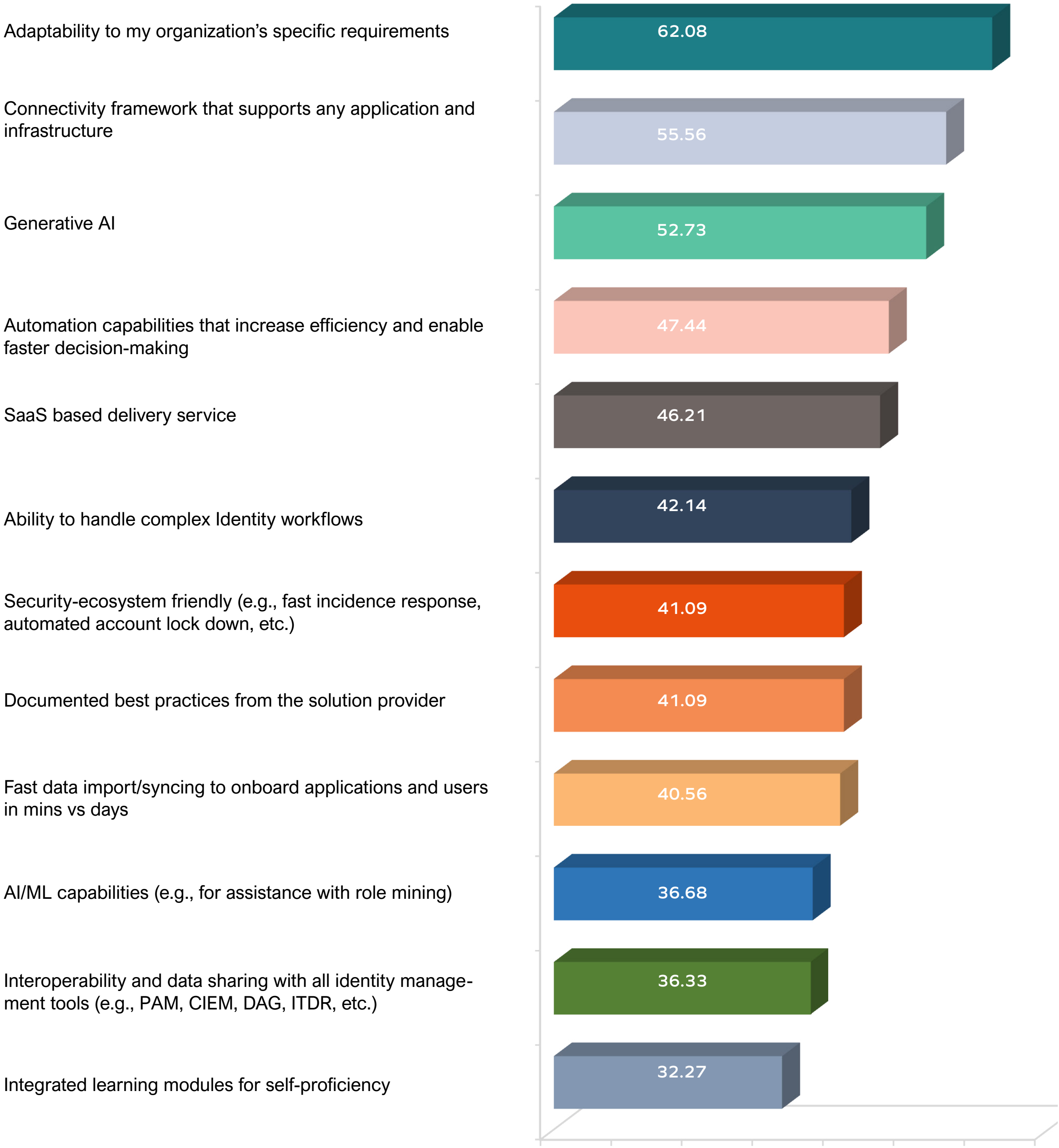
Organizations want SaaS-based IGA that offers generative AI, fast data import, adaptability, a connectivity framework and automation and that is security ecosystem-friendly.

The characteristic most respondents want from a new IGA solution is "adaptability to my organization's specific requirements." This is no surprise, given the workload that IGA solutions must contend with from the increasing number of business applications, complex identity workflows, role-based provisioning and rising compliance requirements – and how integral IGA is to the identity fabric of a typical enterprise.

Another area where respondents indicated a strong preference is Generative AI. We've already seen many examples of how this transformative technology can improve efficiency and reach better outcomes. IGA is no exception. With Generative AI, decision-making can happen faster, removing cumbersome processes and extra steps. One example is certifications. Organizations can benefit from reducing the noise of regular certifications and recertifications by leveraging technology to dramatically reduce certification fatigue and improve the quality of certifications in an IGA system. This results in not just powering compliance but also reducing the quantity of over-permissioned accounts and the potential risk of a data breach if these accounts were ever compromised. Other features respondents would look for are "a connectivity framework that supports any application and infrastructure," "ability to handle complex identity workflows" and "SaaS-based delivery service."

> "Organizations want SaaS-based IGA that offers generative AI, fast data import, adaptability, a connectivity framework and automation and that is security ecosystem-friendly."

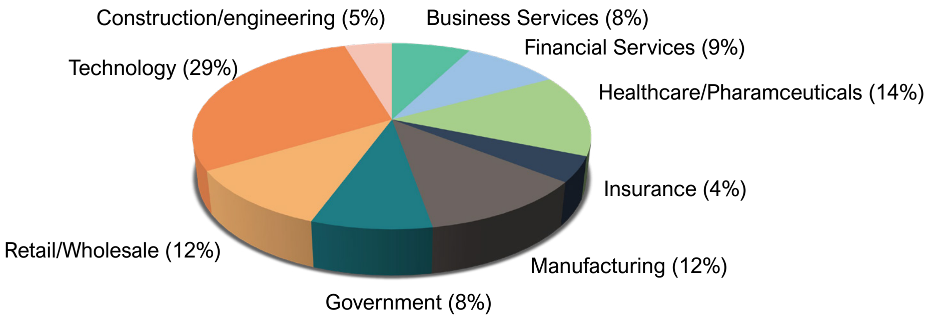
If your organization were evaluating a new IGA solution for deployment, which of the following characteristics would be most important? (Choose top five most important)



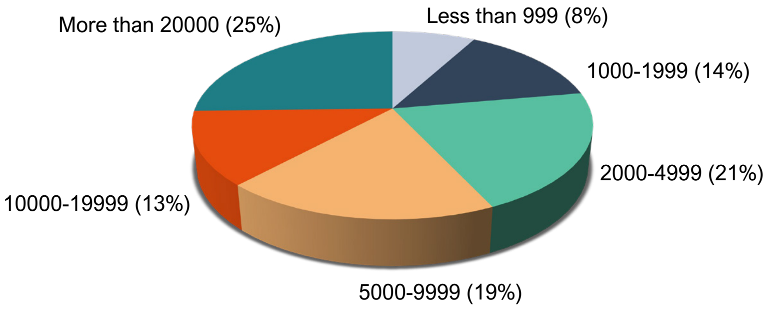
Methodology and Demographics

The research we conducted used a comprehensive survey of questions involving 567 enterprises across the United States with more than 1,000 employees, encompassing the perspectives of both IT and business leaders. The respondents consisted of people across a wide range of ages with about even gender breakdown (60-40, male to female) that are responsible for one of identity governance and access management, compliance, cybersecurity or general IT administration and management in organizations. The organizations covered a wide spectrum of industries across every region of the United States.

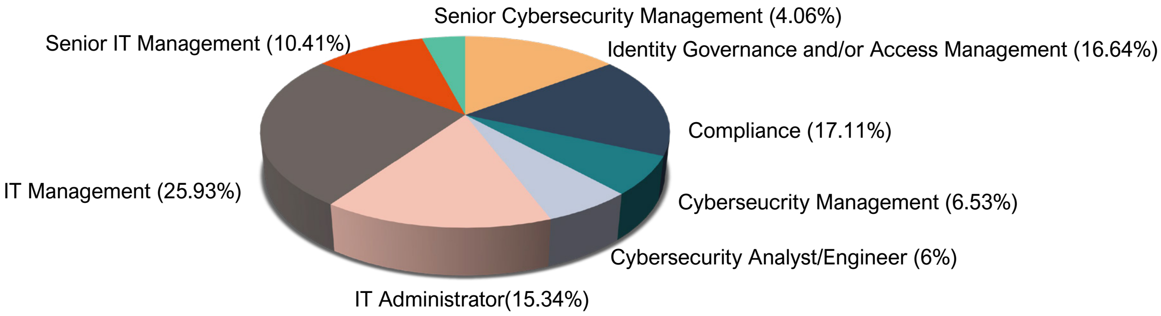
What is your business?



What is the size of your organization?



What is your role in your organization?



Omada

Omada, a global market leader in Identity Governance and Administration (IGA), offers a full-featured, enterprise-grade, cloud native IGA solution that enables organizations to achieve compliance, reduce risk, and maximize efficiency. Founded in 2000, Omada delivers innovative identity management to complex hybrid environments based on our proven best practice process framework and deployment approach.