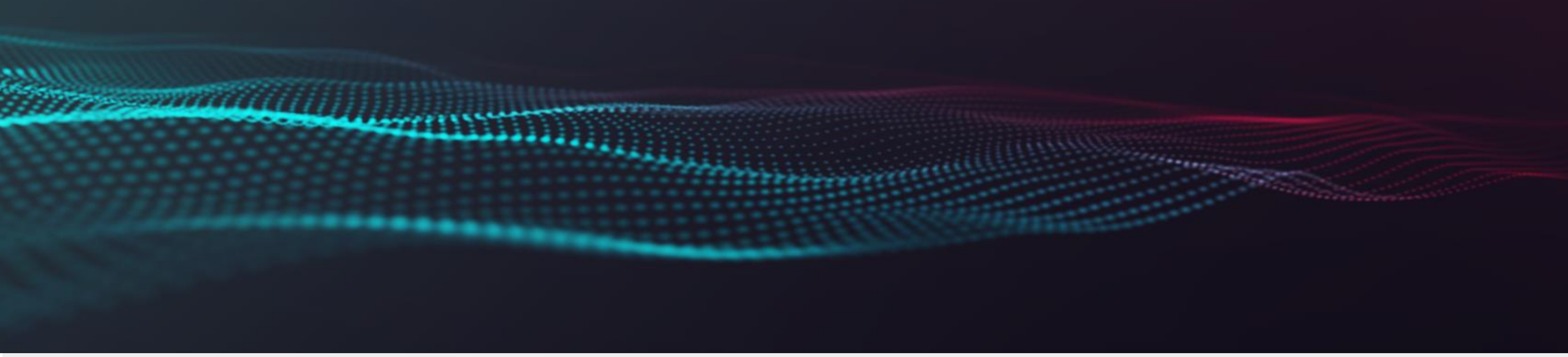
Enterprise Strategy Group | Getting to the bigger truth.™



ESG RESEARCH INSIGHTS REPORT

A Modern Approach to Identity Governance and Administration

Securing Remote Work and Supporting Zero Trust Initiatives

By Doug Cahill, ESG Vice President and Senior Analyst

April 2021

This ESG Research Insights Report was commissioned by Omada
and is distributed under license from ESG.

Contents

Executive Summary

The need to secure access to a range of cloud-based and on-premises applications and data has necessitated modernizing identity and access management (IAM) initiatives. The increase in remote work due to the COVID-19 pandemic has significantly complicated identity and access management processes and thus has become a key driver for IAM modernization. As a result, the governance of identities and their associated permissions has become a strategic aspect of cybersecurity programs. But doing so requires a pragmatic approach that balances improving an organization's security posture by protecting critical corporate assets from compromise while also supporting business agility with respect to end-user workflows.

Modern identity and governance solutions leverage a cloud-native implementation for scalability and employ automation to streamline the assignment of fine-grained roles to adapt to organizational specific requirements.

Purposeful controls are required to improve visibility and streamline provisioning without inhibiting employee productivity; that's why a modern approach to identity and governance administration (IGA) is important. But what, exactly, constitutes a modern approach? Modern identity management and governance solutions leverage a cloud-native implementation for scalability and employ automation to streamline the assignment of fine-grained roles to adapt to organizational specific requirements.

In January 2021, Omada commissioned the Enterprise Strategy Group (ESG) to conduct a research study on the role of cloud-based IGA. The research consisted of a survey of 150 cybersecurity and IT operations professionals employed at enterprises (i.e., organizations with 1,000 or more employees) and with direct involvement over their organization's identity governance and administration practices and technologies.

Based upon the research and analysis done for this project, ESG concludes:

- IGA has emerged as a strategic set of controls. The management of identities and their associated application entitlements has become a top 5 cybersecurity priority at most organizations. Identity management modernization projects have clearly been accelerated, with remote work a catalyst and zero trust emerging as a guiding strategy.

- The need for scale, automation, and efficiency is driving demand for cloud-based IGA services. The need for scale, adaptability, and reduced total cost of ownership (TCO) is specifically driving heavy demand for cloud-based IGA services. In fact, cloud delivery is now the number one IGA solution-buying criteria.

- The increase in remote work will continue post-pandemic. While the dramatic increase in remote work due to the COVID-19 pandemic will subside over time, more employees will be working from home moving forward than before the pandemic, even after it is safe to go back to the office. As such, cybersecurity and IT operations teams will continue to be charged with enabling and securing the access requirements of a hybrid workplace, a central driver for IAM modernization influencing a preference toward cloud-based applications.

- New perimeters have created operational challenges. The broad adoption of cloud services and the increase in remote work has accelerated the breakdown of an already vulnerable network perimeter, creating multiple operational and governance challenges. Rethinking the perimeter based on identity and cloud services is required to modernize identity and access management programs with a zero trust approach.

- Security and business objectives cannot be mutually exclusive. Effective IAM programs require a balance between improving an organization's security posture and supporting business agility through workflow-enabled identity and entitlement management. This dual mandate is also driving the increasing priority of identity and governance modernization.

- A diverse landscape of identity-centric threats has led to serious consequences. Identity-related threats such as credential theft, impersonation, and cyber fraud has led to compromised data, malware infections, and financial loss. These perennial issues rooted in identity-related threats continue unabated, highlighting the need for a modern approach to identity management and governance.
- Securing digital identities requires investments. Identity and access management spending is increasing to better support employee productivity, adaptability to evolving business requirements, streamlined segregation of duty enforcement, more efficient user account provisioning/de-provisioning, and multiple other important identity-centric requirements.

The Growing Strategic Importance of Identity Governance and Administration

It is no secret that an organization's employees are, in many cases, the entry point for cyber adversaries. After all, an organization's staff are all too often only a weak password or phishing email away from giving away their credentials or sensitive information, or unwittingly installing malware on behalf of the attackers.

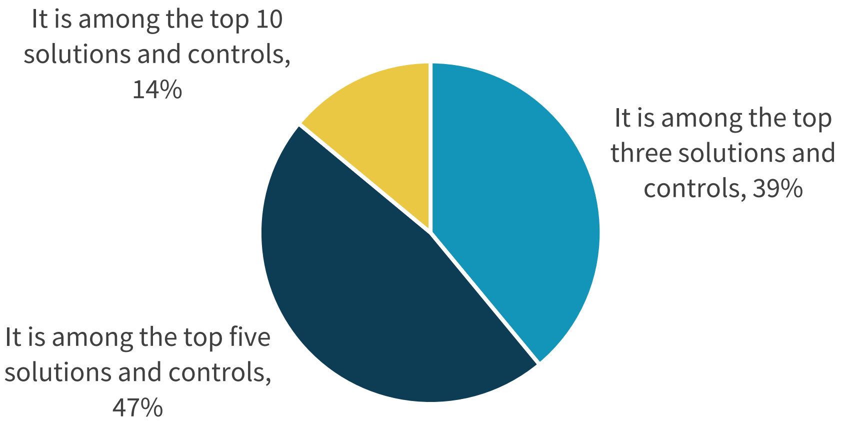
The increase in remote work has simultaneously made end-users even more vulnerable to targeted threats and harder to manage, secure, and monitor. In fact, nearly three quarters of respondents reported that an expanded remote workforce has increased the difficulty of managing their users' digital identities and their associated permissions. Why? The need to operationalize remote work too often leads to trading the application of best practices such as least privilege access, a core tenant of a zero trust approach, for expedited provisioning. As a result, 93% of research participants shared that remote work has necessitated the reexamination of their organization's IGA systems and processes. Work-from-home (WFH) requirements are likely drivers behind why 45% of respondents reported that their organizations had deployed a solution in the last 12 months.

The need to continually prevent, detect, and respond to security threats keeps cybersecurity and IT operations teams constantly busy. While defense-in-depth is a core tenet of any cybersecurity program, 86% of respondents reported IGA as a top 5 security control priority for their organization (see Figure 1). IT and security professionals clearly recognize that identity is central to their cybersecurity programs.

86% of respondents reported IGA as a top 5 set of controls for safeguarding their organization's critical applications and data.

Figure 1. The Relative Importance of Identity Governance and Administration

Think of the solutions and controls in place that help safeguard your organization's critical applications and data and, by extension, your company's brand. In your opinion, where does IGA rate in terms of importance? (Percent of respondents, N=150)



Source: Enterprise Strategy Group

The Role of IGA in a Zero Trust Approach

Zero trust as an approach to implementing the principles of least privileged access is gaining favor as a core tenet of securing the modern workplace. Zero trust serves as a security model based on a perspective that entities are, by default, untrustworthy until verified. As such, zero trust conveys a "default-deny" approach that assumes everyone and everything is a threat, changing the secure access model from "trust, but verify" to "don't trust, continuously verify" by actively governing permissions and continuous monitoring.

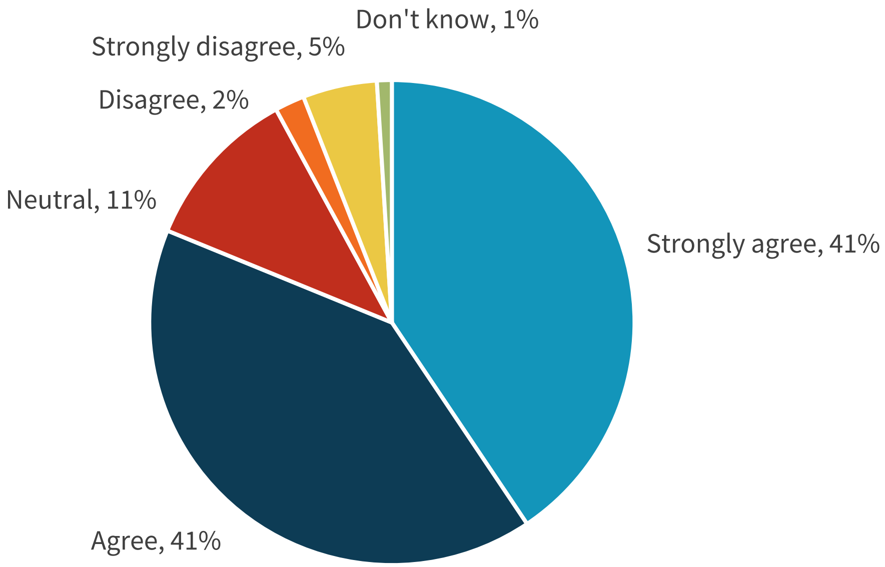
While the specifics of implementing such a strategy are being explored by security practitioners and IT operations teams, the principles of zero trust are clearly aligned with core identity governance and administration capabilities: tightly scope user roles, implement segregation of duties, regularly review permissions, require approval workflows, as well as continuous monitoring and the use of strong forms of authentication. To this point, 81% of survey respondents see their IGA program as a key element of their organization's zero trust security strategy (see Figure 2).

81% of survey see their IGA program as a key element of their organization's zero trust security strategy.

Central to the connection between zero trust and IGA is automation because both attackers and defenders employ automation to gain an upper hand. Cyber adversaries leverage automation for brute force attacks, credential stuffing, password spraying, and other forms of identity-related attacks. To prevent such attacks IT and cybersecurity teams need to similarly use the automation capabilities provided by modern IGA solutions as the means to apply fine-grained, role-based policies before bad actors take advantage of mis-scoped identities.

Figure 2. The Importance of Zero Trust in an IGA Strategy

Please rate your level of agreement with the following statement: Implementing a zero trust based approach is an important aspect of our IGA strategy going forward. (Percent of respondents, N=150)

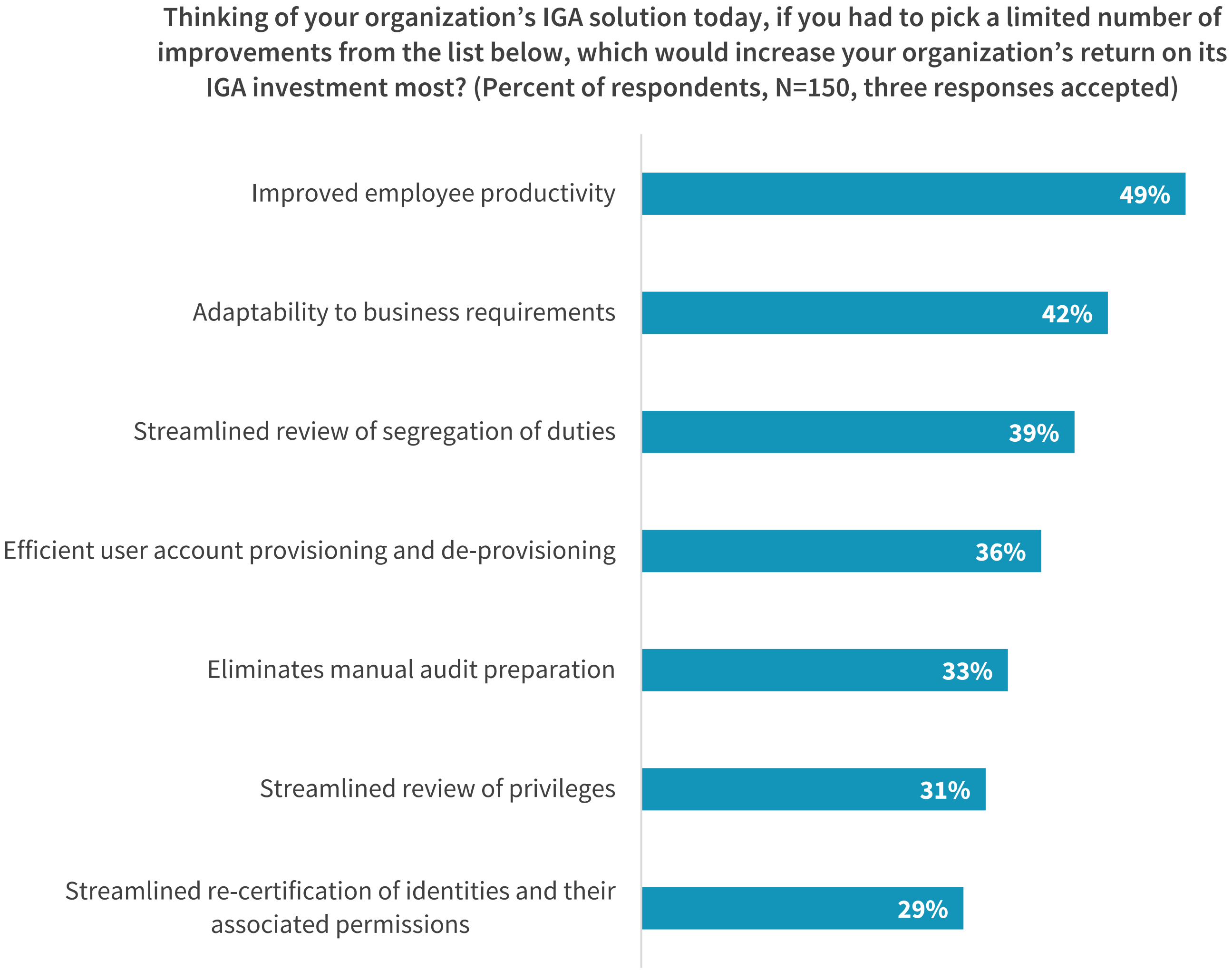


Source: Enterprise Strategy Group

IGA Investments Deliver Compelling Returns

While it is often difficult to measure the return on investment (ROI) of cybersecurity controls focused on delivering hard-to-measure risk reduction benefits, research respondents expect compelling returns from their IGA investments. As such, the ability to demonstrate ROI through increased speed and labor efficiency makes IGA projects easier to justify than risk-focused security projects. What are those returns? The top ROI metrics cited by research participants were centered on productivity, adaptability, and efficiency (see Figure 3).

Figure 3. The Return on IGA Investments



Source: Enterprise Strategy Group

Of note are the operational efficiency improvements, including more efficient account provisioning/de-provisioning, automated audit preparation, streamlined entitlement reviews, as well as others. The ability for a modern IGA solution to be accurate and yield consistent output yields additional operational efficiencies. The ability to financially justify an IGA project based on such ROI metrics and addressing challenges discussed below are key factors driving IGA adoption.

Shifting Perimeters Create Identity-related Operational Challenges

While "cloud-first" strategies lead many organizations to default to the use of cloud services, nearly all enterprises operate in a continually shifting, hybrid mix of on-premises and multi-cloud-based applications. User identities and their associated entitlements, however, must be effectively and efficiently managed no matter where the IT workload is hosted. The shifting perimeters of the modern enterprise have created a set of identity and access management challenges.

The Cloud Perimeter Creates Visibility Gaps

73% of survey respondents agreed that implementing least privilege access to their use of cloud applications and services is challenging, with another 62% noting cloud consumption has made identifying segregation of duty violations more difficult.

Cloud-based applications, both software-as-a-services (SaaS) and those internally developed and deployed public cloud platforms, are increasingly supporting essential business functions. Survey respondents report that a slight majority (52%) of their business-critical applications are now cloud-based. This move to the cloud has challenged traditional physical network-centric approaches to cybersecurity in general and identity and access management programs specifically. In fact, two-thirds of respondents reported that their organization's use of cloud services for business-critical purposes has further challenged their IGA program.

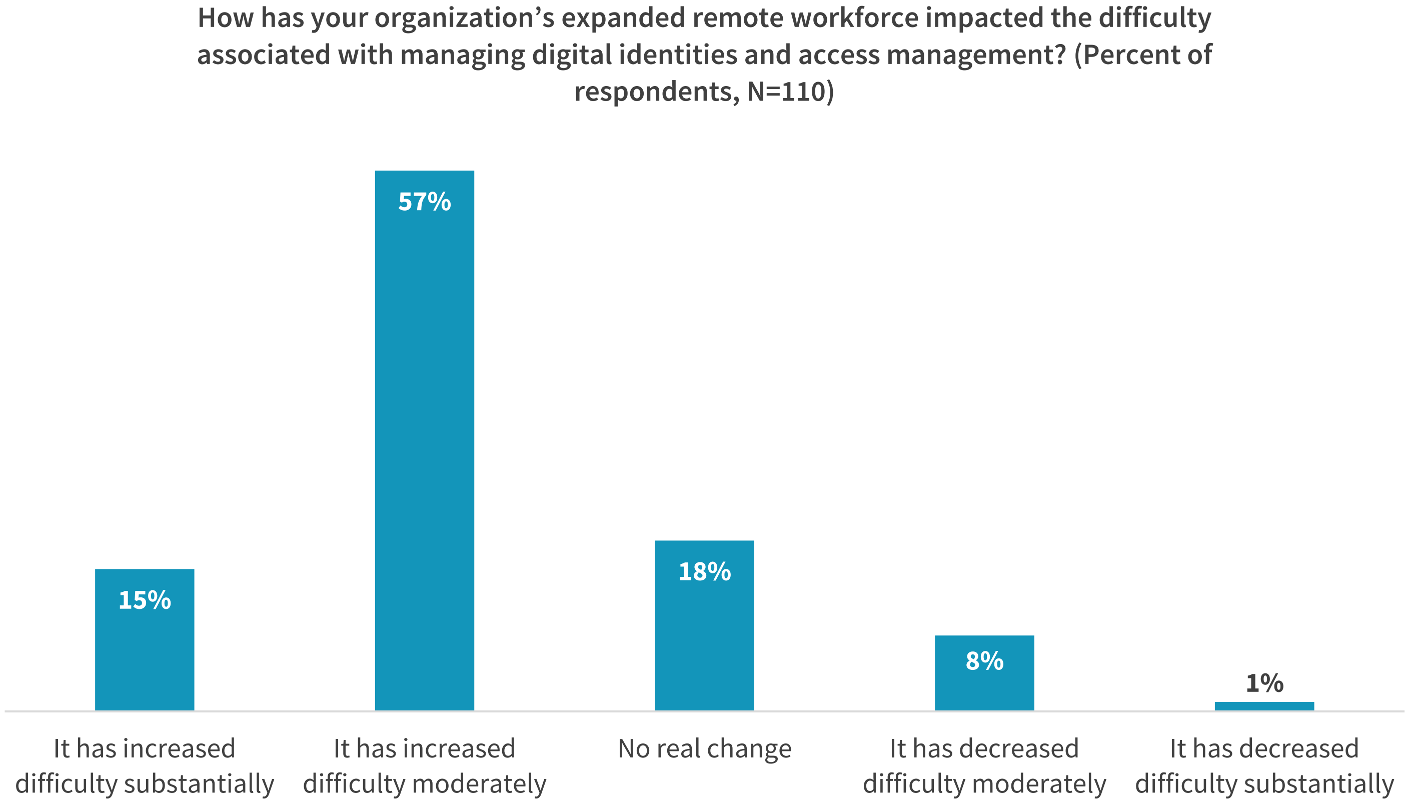
The primary cloud-related IGA challenge cited by research participants was the rise of shadow IT that leads to accounts being created and managed by individuals or business units without the involvement or oversight of the IT or cybersecurity teams. In addition to IGA policies not being followed by business units who engage in shadow IT, a high diversity of unknown applications results in a lack of policy and control consistency. As a result, 73% of survey respondents agreed that implementing least privilege access to their use of cloud applications and services is challenging, with another 62% noting cloud consumption has made identifying segregation of duty (SoD) violations more difficult. Such SoD issue are too often due to the use of connected SaaS applications in which the same privileged credentials are used by different cloud application such as customer relationship management and marketing automation as well as vendor management and accounts payabale applications. These challenges associated with managing the identities used to access cloud applications further highlights the increased need for applying the principles of zero trust.

Remote Work Expands the Identity Perimeter

The rush to remote work over the past year has further increased the use of and reliance on a range of cloud services headlined by SaaS applications. This is a trend that will continue, with 47% of respondents to a separate ESG research study planning to further expand their use of cloud-based office productivity applications and 43% citing a planned increase in online file sharing and collaboration services.[1] Clearly highlighting this point, 72% of respondents flagged that managing identities has become even more difficult with a highly or completely remote workforce, with the top contributing factor being the need to support access to a wide range of applications (see Figure 4).

[1] Source: ESG Master Survey Results, *2021 Technology Spending Intentions*, December 2020.

Figure 4. The Impact of Remote Work on IGA Programs



Source: Enterprise Strategy Group

Survey respondents also flagged additional significant concerns related to the increase in remote work, including the lack of centralized visibility and control over which users have access to sensitive data and the increased challenge of meeting and maintaining compliance with industry regulations as more in-scope data was moved to the cloud.

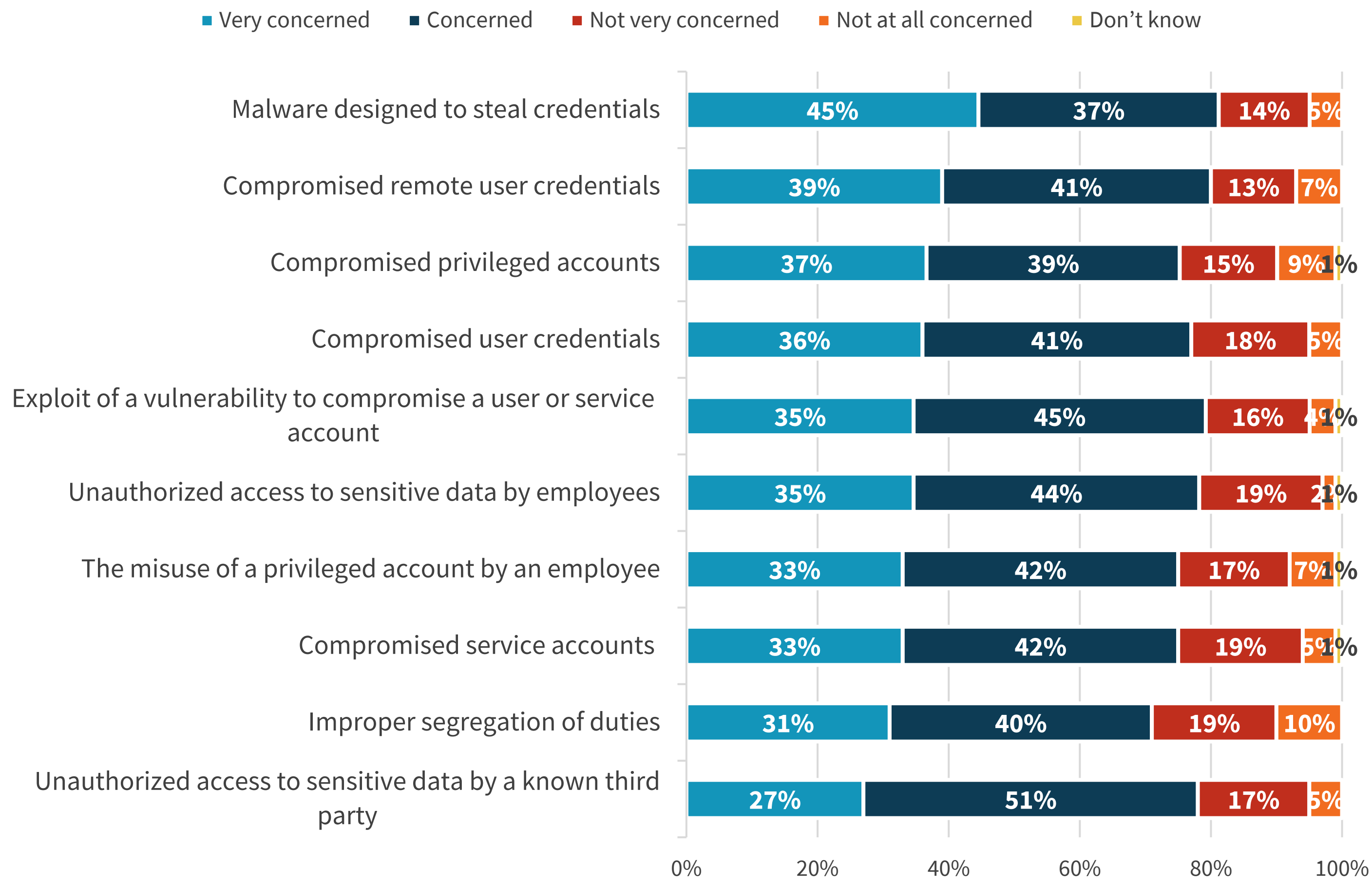
It is also clear that the work-from-home trend will continue. While the percentage of remote employees increased from 27% before the pandemic to 51% during it, even after the COVID-19 outbreak is controlled and it is safe for employees to return to the office, 41% of the workforce is expected to still work predominantly remotely for good. As such, going forward, identity management and governance will have a central role in securely enabling what will be a hybrid workplace.

The Impact of Compromised Identities

The vast majority of successful cybersecurity attacks include an aspect of social engineering, targeted phishing, stolen credentials, and/or user engagement with malicious websites or software. Attackers attack people more often than vulnerable software or systems simply because of the ease of doing so. ESG's research participants are well aware of this dynamic of the threat landscape and shared a high level of concern for a broad set of identity-related attacks, including credential stealing malware, compromised user and service accounts, improper segregation of duties, unauthorized access to sensitive data, and more (see Figure 5).

Figure 5. Identity-related Attacks that Represent the Greatest Risk

In terms of the risk level to your organization, how concerned do you believe your organization is with each of the following identity-related types of cybersecurity threats? (Percent of respondents, N=150)



Source: Enterprise Strategy Group

Unfortunately, these identity-related concerns are warranted, as nearly a third of respondents, 31%, shared that their organization lost data due to an identity-related a cybersecurity incident in the last 12 months. Perhaps even more disconcerting is the fact that another third, 33%, suspected but were unsure if they lost data due to an identity-related attack.

Nearly a third of respondents, 31%, shared that their organization lost data due to an identity-related cybersecurity incident in the last 12 months.

Identity-related cybersecurity incidents have also led directly to financial loss as reported by 36% of respondents over the last 12 months. Such attacks entail the use of compromised credentials employed in a cyber fraud scheme (e.g., business email compromise attack). And here again, uncertainty is an issue, with 25% of respondents suspecting, but unsure, that they have had a financial loss due to compromised credentials.

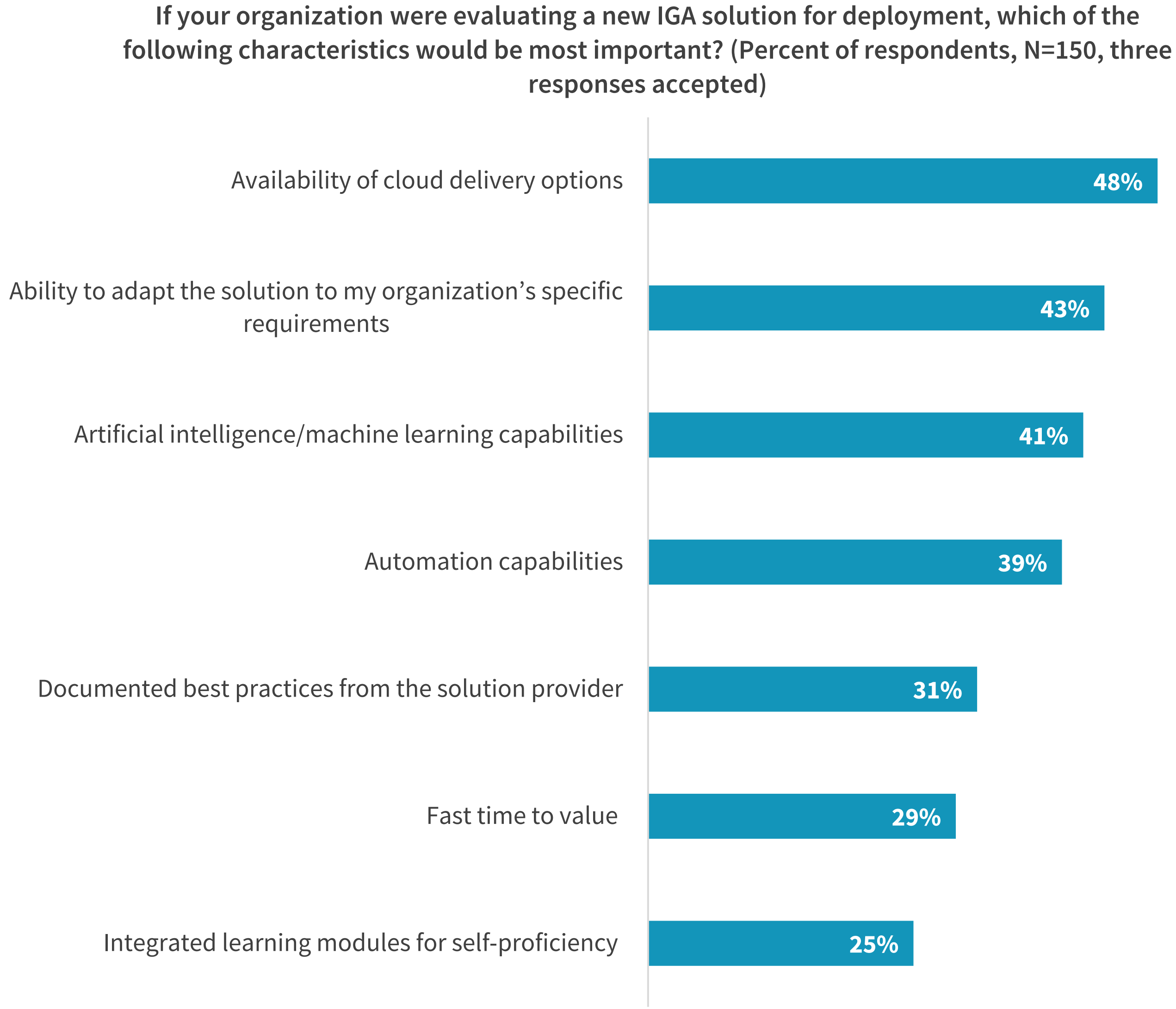
Compromised accounts, including service accounts and privileged accounts, were reported by 40% as the most common type of identity-related incident that led to data and financial loss. Those attacks that are top of mind, along with those which have resulted, have had a material impact, highlighting the need to proactively govern all digital identities. Such measures include attention to segregation of duties and reduction of account permissions to only those required so that when accounts do get compromised, the associated damage is minimized.

The Drivers for Cloud-based IGA

The challenges, threats, and experiences expressed by respondents in ESG's research makes it clear that a modern approach to managing and governing digital identities is required. But what constitutes a modern approach and what are the benefits?

While the current consumption of identity governance and administration solutions is equally split between customer-managed, on-premises and cloud-based implementations, there is a clear preference going forward for cloud-based solutions per the 63% of respondents who noted that if their organization were to initiate a new IGA project today, they would prefer a cloud-based solution. In fact, the availability of cloud delivery was rated as the most important feature of an IGA offering along with adaptability, automation, and the existence of documented best practices (see Figure 6).

Figure 6. The Most Important Attributes of an IGA Solution



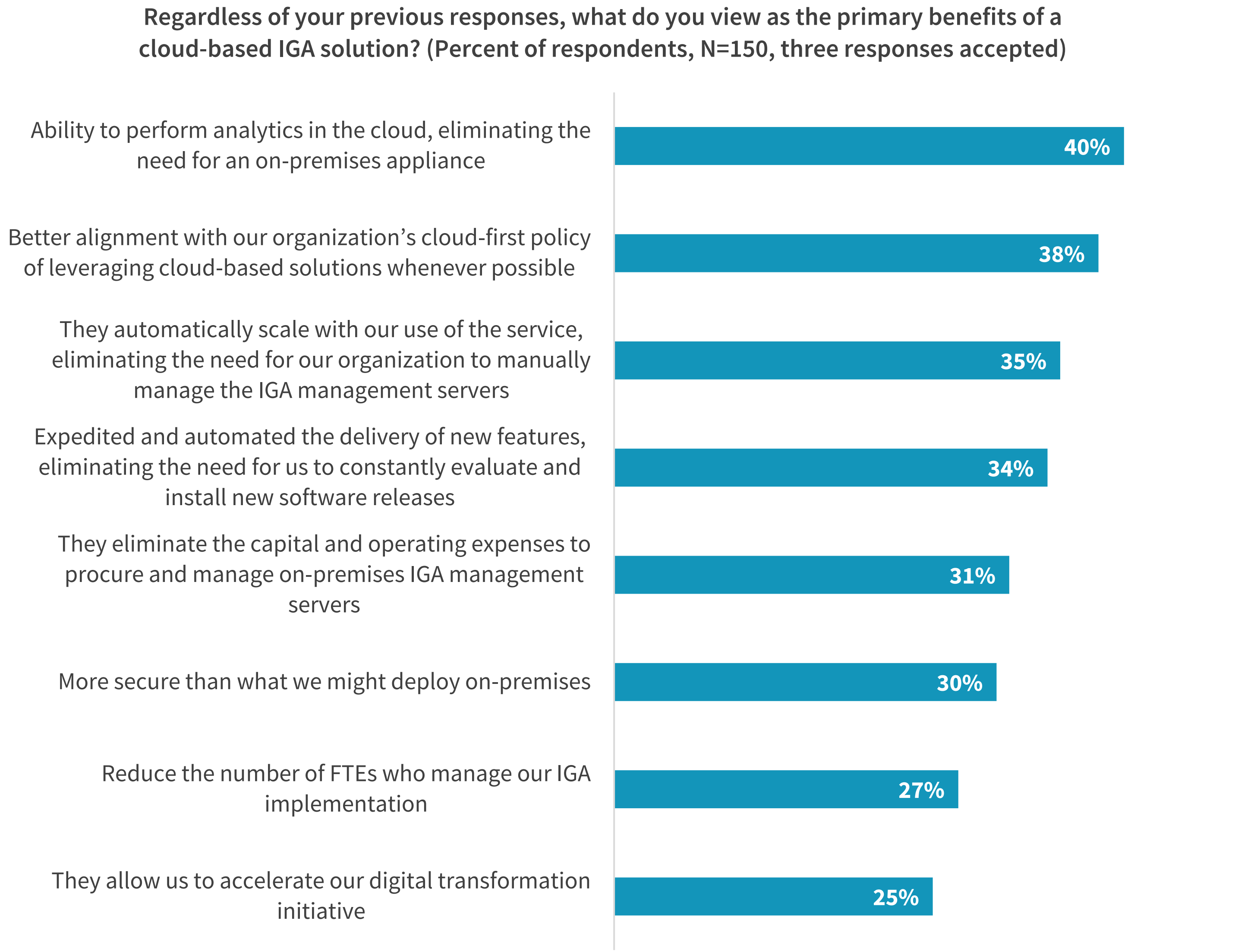
Source: Enterprise Strategy Group

Clearly, IGA is becoming a cloud-first-based security control for most organizations, with a further clear preference for those built from the ground up in the cloud, leveraging a cloud-native architecture for scale, and that help organizations achieve greater operational efficiency as a means to lower total cost of ownership (TCO).

The Need for Scale

Eliminating the need to manually provision and manage infrastructure is a well understood and appreciated benefit of software-as-a-service applications. While research respondents cited the associated elimination of capital and operating expenses and a reduction in full-time employees (FTEs) as benefits of a cloud-based IGA, they shared what is arguably a more strategic view, one rooted in a need for scale. Scale is manifested in the research results not only explicitly as the third top benefit of cloud-based IGA, but also as an implicit aspect of the top benefit, the ability to perform what are often compute-intensive analytics in the cloud (see Figure 7).

Figure 7. The Primary Benefits of a Cloud-based IGA Solution



Source: Enterprise Strategy Group

Another benefit of note is expedited access to new functionality. With true cloud-based applications, new features and capabilities are available nearly instantly to all customers once they are pushed into production by the cloud service provider (CSP).

Lowering the Total Cost of Ownership (TCO)

Another clear benefit of cloud-based IGA solutions versus those that are customer-managed is delivering a lower total cost of ownership (TCO). A clear majority of respondents, 62%, reported that the TCO (covering capital, operational, and labor costs) of cloud-delivered IGA solutions compare favorably to on-premises solutions. Nearly half the respondents, 45%, shared that they estimate that the TCO would be more than 10-25% lower for cloud-based IGA, another driver for the strong preference for a cloud-based IGA implementation.

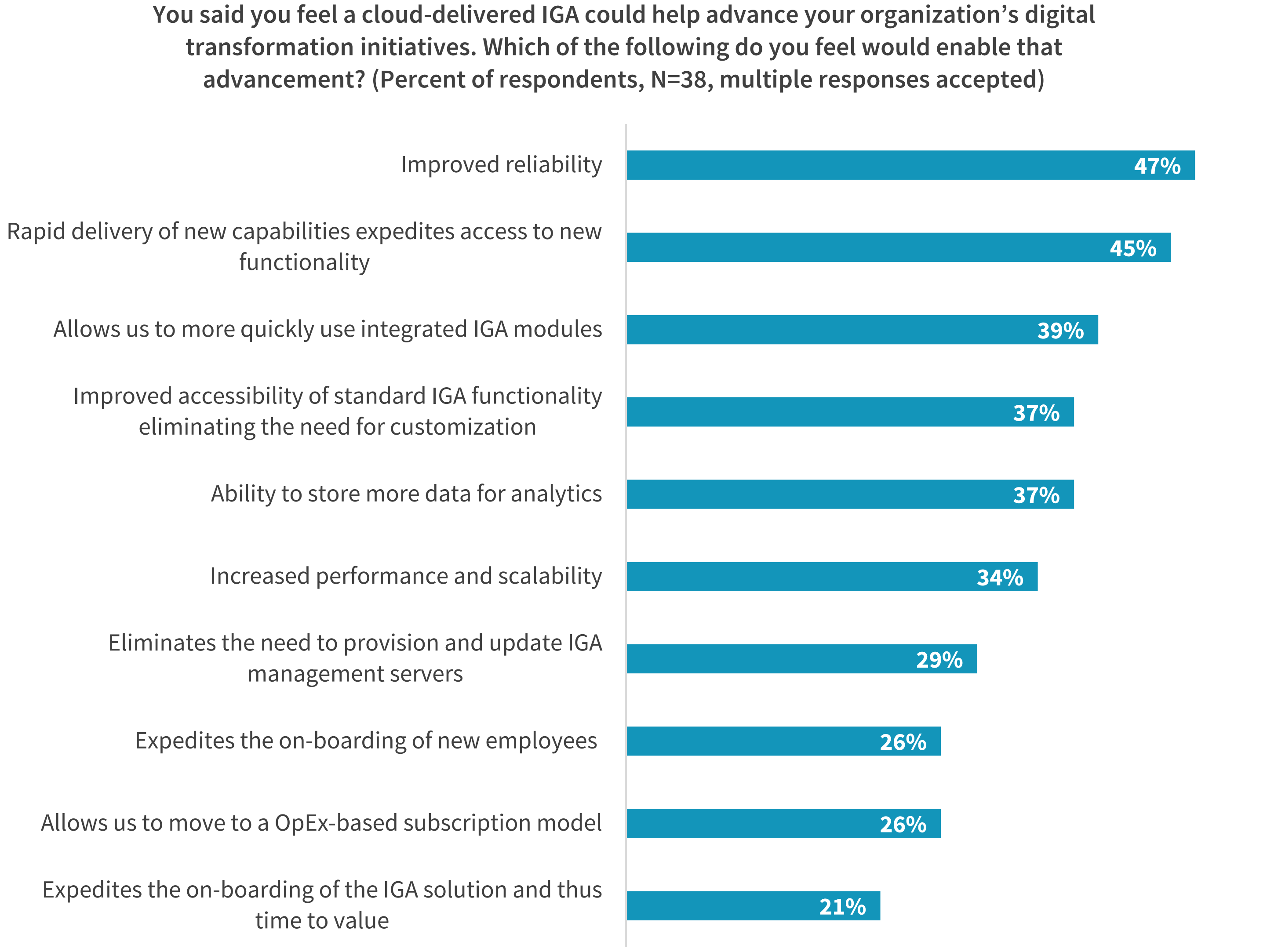
62% expect cloud-based IGA to provide a lower TCO than an on-premises implementation.

Supporting Digital Transformation Initiatives

As noted, the pandemic has further accelerated the use of cloud applications headlines by collaboration services, which maximizes the productivity of a remote workforce. This trend is part of broader digital transformation (DX) initiatives. Where are organizations in their DX journey? While some, 34%, cite a mature digital transformation initiative, many are just underway with 51% in process and 10% just beginning their journey.

Some survey respondents feel a cloud-based IGA solution will advance their organization's digital transformation initiative, citing improved reliability and the rapid delivery of new capabilities expediting access to those capabilities (see Figure 8). Of note is a time-to-value of feature accessibility and discovery of integrated functionality which allows cloud-based IGA offerings to further the objectives of DX programs.

Figure 7. Cloud-based IGA and Digital Transformation



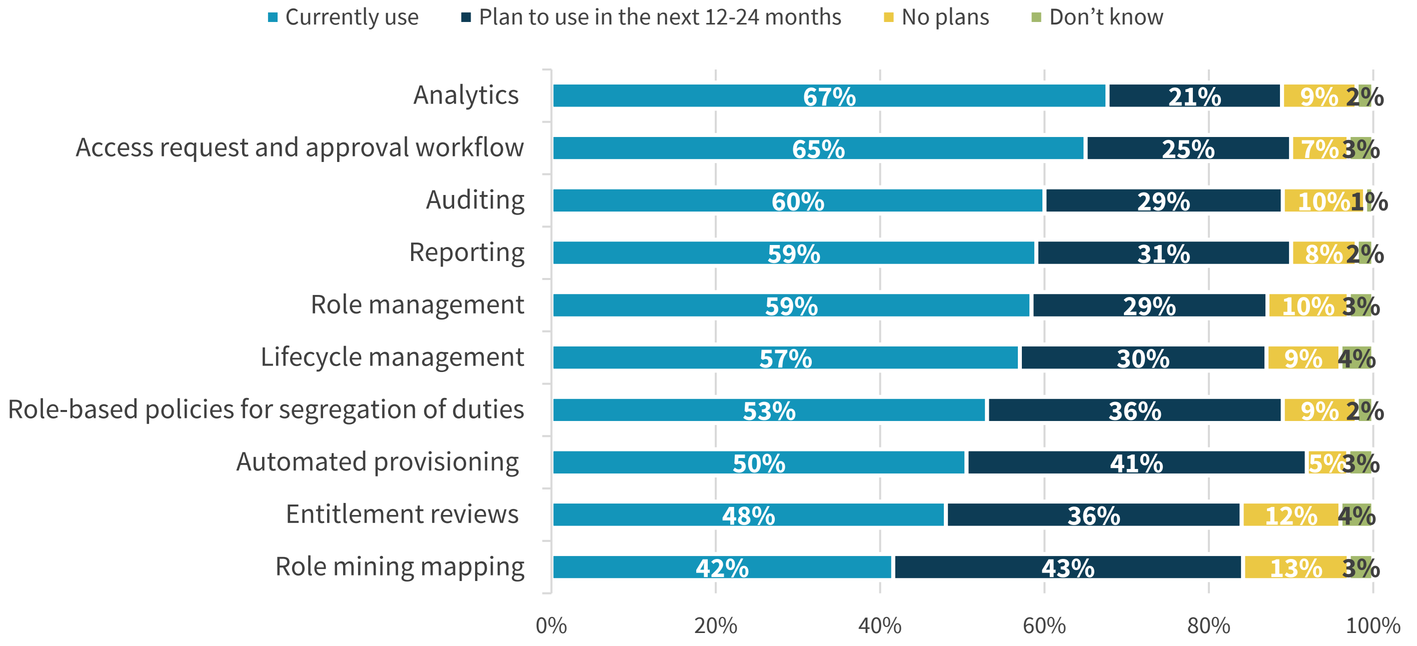
Source: Enterprise Strategy Group

Securing Digital Identities Requires Increased Investment

While modern, cloud-based IGA systems are seen to provide significant advantages given today's reality of cloud-based applications and employees working from home, implementing them requires investment. Most survey respondents, 84%, shared that their organization's identity and access management spending will increase over the next 12 months, with 29% expecting it to increase substantially compared with spending relative to other areas of cybersecurity. Doing so will allow organizations to expand their IGA services with a significantly richer set of capabilities, supporting a broader set of use cases, with analytics, access request workflows, improved auditing, and reporting being just four of the top improvements on the IGA project goal sheet (see Figure 9).

Figure 9. Current and Planned IGA Use Cases

How would you describe your organization's plans for the following identity governance and administration (IGA) functional capabilities? (Percent of respondents, N=150)



Source: Enterprise Strategy Group

Of note looking beyond this core set of required IGA functionality, 41% of respondents shared plans to automate provisioning in the next 12-24 months to gain greater operational efficiencies, and another 43% plan to focus in the same time period on improving user role management through improved role mining and mapping.

The Bigger Truth

This research clearly highlights the continued and growing importance of identity governance and administration for modern cybersecurity programs. The digitization of the workplace, cloud-first strategies, sustained remote work, the prominent role of identities in cybersecurity attacks, and the rise of zero trust to prevent them make modernizing identity and access management a strategic imperative. To do so, many organizations will leverage cloud-based IGA to realize the associated compelling benefits.

With the relatively recent emergence of full-featured, cloud-based IGA systems, organizations are now well positioned to improve both the efficiency and effectiveness of their identity management processes while also reducing the total cost of operation relative to traditional on-premises systems. With so many drivers for and benefits of identity management modernization in place and more likely to intensify, it is ESG's opinion that IGA projects are a top cybersecurity program priority. The improved scale, automation, and reduced TCO that can be experienced from today's cloud-delivered identity management and governance systems make the functional benefits of identity and access governance more attainable than ever.

Methodology and Demographics

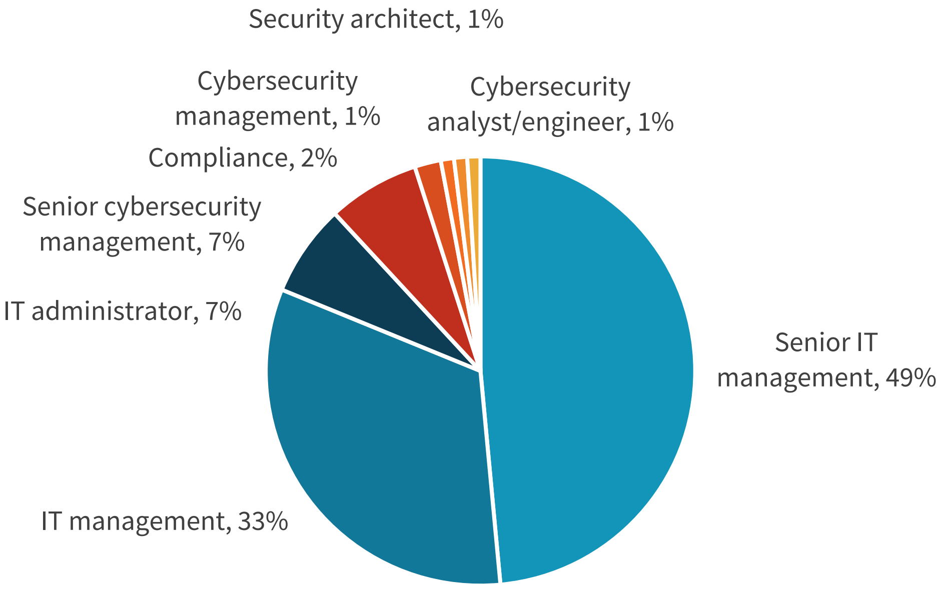
To gather data for this report, ESG conducted a comprehensive survey of cybersecurity and IT operations professionals employed at enterprises (i.e., organizations with 1,000 or more employees) and with direct involvement over their organization's identity governance and administration (IGA) practices and technologies. All respondents were based in the United States. The survey was fielded between January 7, 2021 and January 17, 2021. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After applying data quality control best practices and screening the remaining completed responses (on several criteria) for data integrity, a final sample of 150 respondents remained. The margin of error for a sample size of 150 is + or – 8 percentage points. Figures 11 - 13 detail the demographics and firmographics of the respondent base.

Note: Totals in figures and tables throughout this report may not add up to 100% due to rounding.

Figure 11. Respondents' Current Responsibility

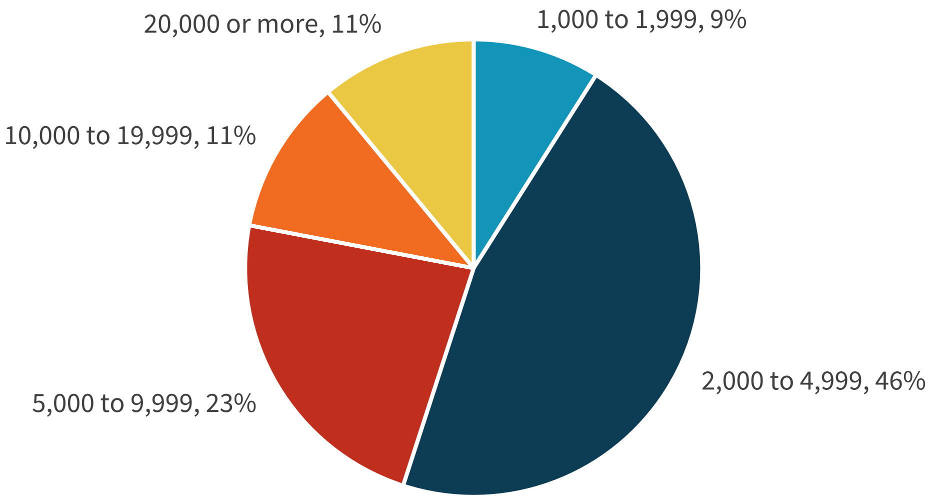
Which of the following best describes your current responsibility within your organization? (Percent of respondents, N=150)



Source: Enterprise Strategy Group

Figure 12. Company Size (Number of Employees)

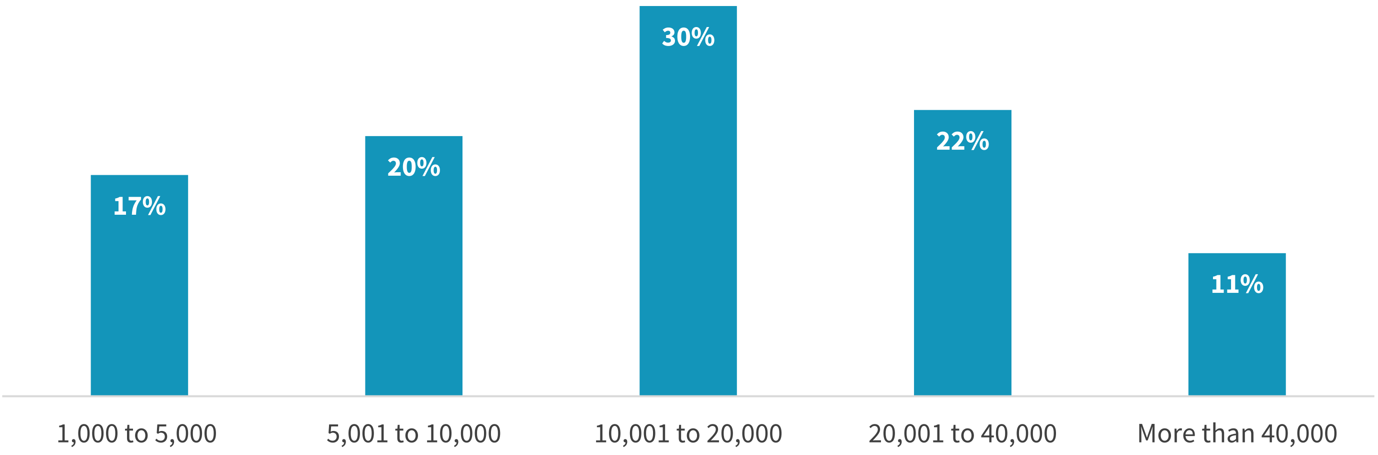
How many total employees does your organization have worldwide? (Percent of respondents, N=150)



Source: Enterprise Strategy Group

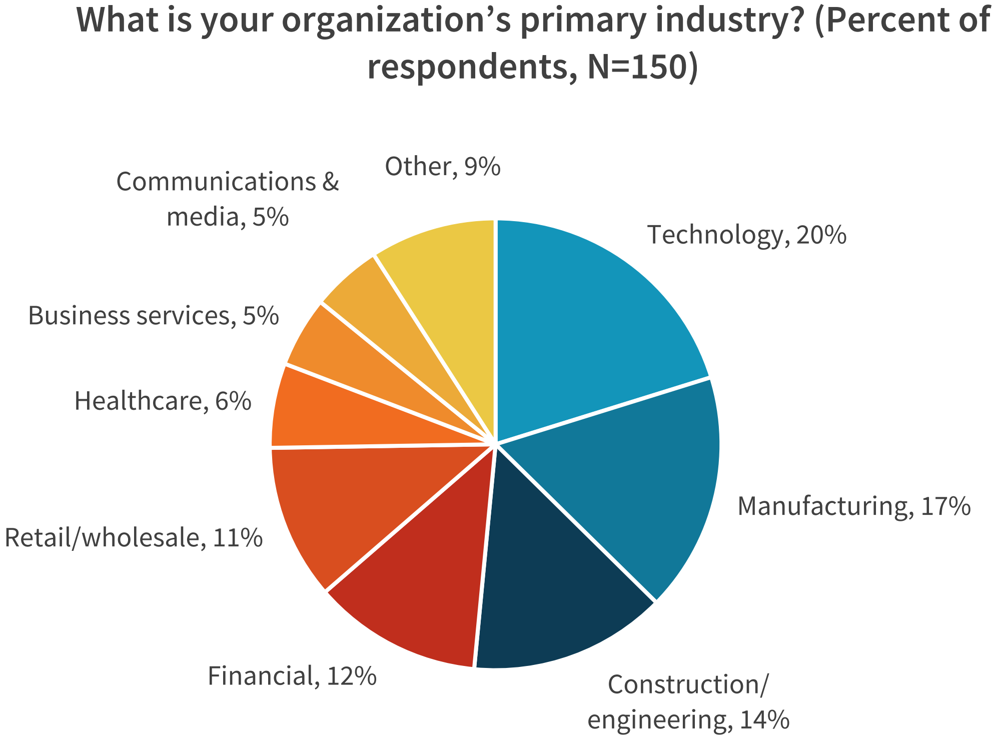
Figure 13. Number of Identities Managed

Approximately how many digital identities does your organization manage today? (Percent of respondents, N=150)



Source: Enterprise Strategy Group

Figure 13. Respondents' Primary Industries



Source: Enterprise Strategy Group

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com ✉ contact@esg-global.com ☎ 508.482.0188