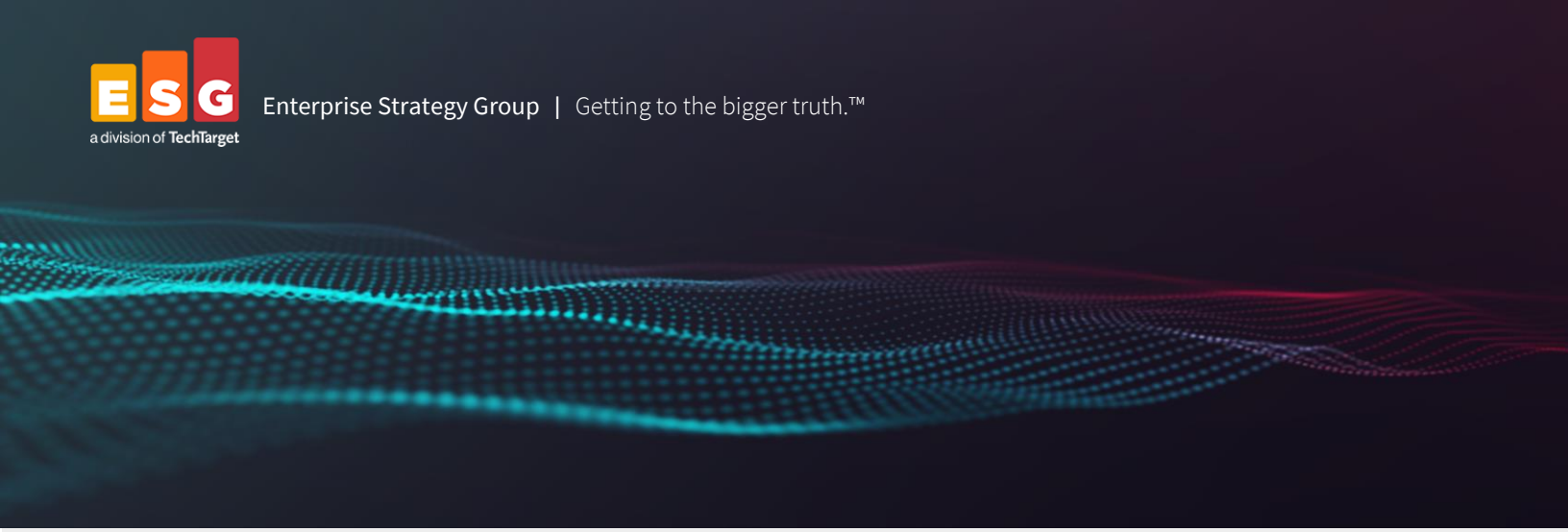


ESG RESEARCH INSIGHTS REPORT

Advancements and Trends in Modern Identity Governance and Administration

How Digital Transformation and Zero Trust Are Affecting IGA Investment

By Jack Poller, Senior Analyst; and Michael Barry, Market Research Analyst

March 2022

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

Contents

Executive Summary 3
The Strategic Importance of IGA 4
IGA's Evolving Role in Zero Trust and Combatting Ransomware 5
The Shift to the Cloud Creates Identity-related Challenges 7
Cloud Apps and Services are Complicating Compliance Requirements 8
The Impact of Compromised Identities 9
The Drivers for Cloud-based IGA 11
Key IGA Use Cases and Capabilities 11
The Increasing Investment in IGA 12
The Bigger Truth 12
Methodology and Demographics 13

Executive Summary

The modern work environment has been transformed in the last few years. Most organizations are well on the way to completing their digital transformation and have accepted the reality of a hybrid workforce, with a significant portion working remotely part or full time. Thus, organizations need to secure access to a range of cloud-based and on-premises applications and data, which has necessitated modernizing identity and access management (IAM) initiatives.

However, both digital transformation and the hybrid workforce have significantly complicated identity and access management processes and thus have become key drivers for IAM modernization. As a result, the governance of identities and their associated permissions has become a strategic aspect of cybersecurity programs. But identity governance strategically 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.

Purposeful controls are required to improve visibility and streamline provisioning without inhibiting employee productivity; that's why a modern approach to identity governance and 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 analytics and automation to increase efficiency and security, automating fine-grained access control provisioning and identifying and remediating over-provisioned and under-used identities.

In November 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 153 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:

- Organizations are re-evaluating their IGA strategies. Hybrid work is a widespread norm. Now that distributed workforces are up and running for the long haul, identities aren't under one or even a handful of roofs anymore. IT teams will need to make sure their IGA implementations are equipped for modern work environments.
- 7 out of 10 business-critical applications will be cloud-based. The expansion of cloud-based applications will only continue. Organizations aren't just moving low-stakes tooling to the cloud. The scalability of cloud is being applied to the most important business applications regularly.
- Provisioning is still difficult and often manual. Forty-nine percent of application access requests are handled manually and 45% need to manually intervene to trace a change made in an HR system. This can get tedious and costly, especially when it's applied to on-/offboarding employees.
- Cloud-based IGA is gaining traction. Organizations are expressing their interest in and understanding of the benefits of cloud-based IGA. When asked how they would implement IGA if they were able to start from scratch, 72% of respondents said they would choose cloud-based.
- Security teams are ready to spend on identity access management. The value of identity security isn't just known by the practitioners anymore; budget holders are aware as well. When asked how IAM budget will compare to the rest of their cybersecurity spending, 91% of respondents said there would be a significant increase.

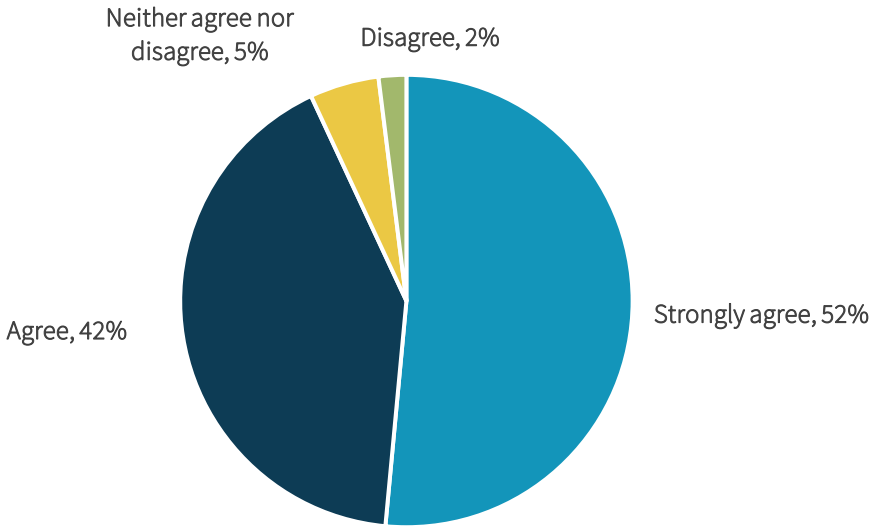
The Strategic Importance of IGA

Workforce identities—employees, contractors, third parties, etc.— have always been a key entry point for cyber adversaries. With hybrid work here to stay, keeping track of credentials and identities is the hardest it's ever been. According to research participants, there will be a 34% year-over-year (YoY) increase in hybrid work, with the workforce splitting time between working at home and in the office. This represents a 21% YoY decrease in full-time employees working in the corporate office.

Equipping the workforce with the tools to work in a hybrid environment was the first step in creating a successful distributed workforce. Now that 51% of employees say they will remain remote or hybrid, organizations need to remain vigilant, maintaining security of people working outside the company walls without impacting productivity. The stress that a distributed workforce is putting on IGA policies is not lost on respondents, as more than half (52%) strongly agree that the need to continue to enable more hybrid and remote-work models required them to reexamine their organization's IGA policies over the past 24 months (see Figure 1).

Figure 1. Hybrid Work's Effect on IGA Policies

Please rate your level of agreement with the following statement: The need to continue to enable more hybrid and remote-work models required us to reexamine our organization's IGA policies over the past 24 months. (Percent of respondents, N=130)



Source: ESG, a division of TechTarget, Inc.

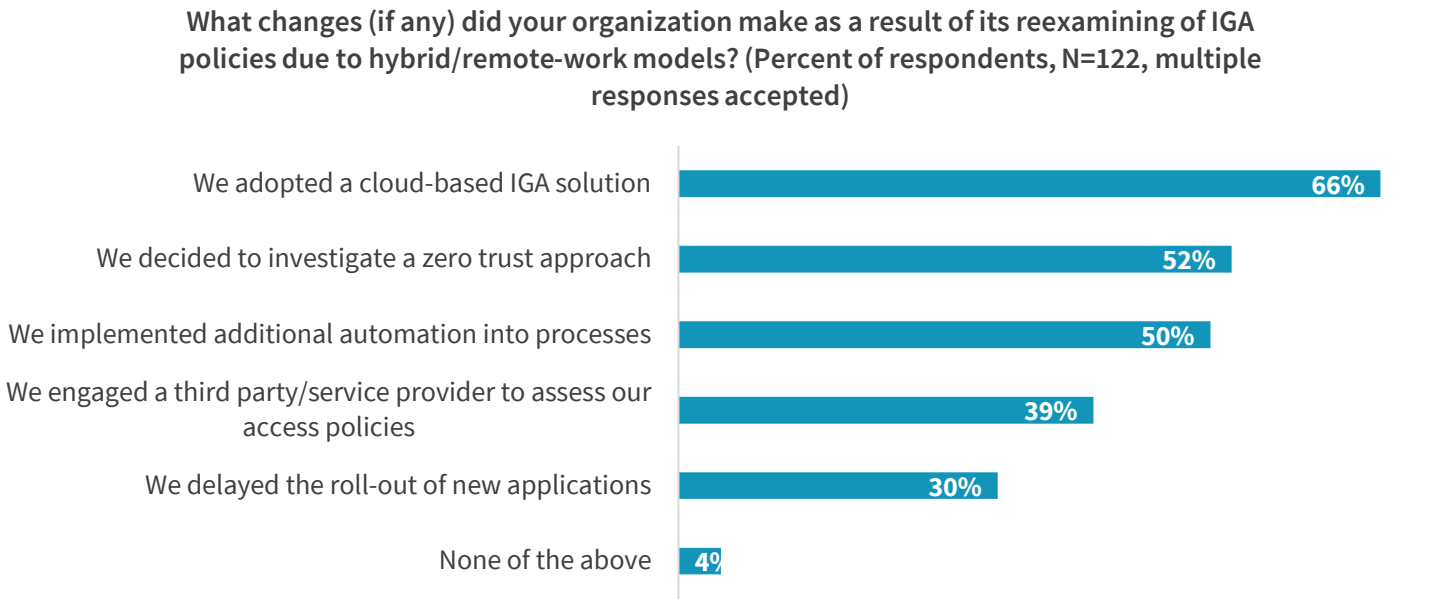
With the shift to a hybrid workforce, cloud-based infrastructure and application adoption grew to facilitate the need for flexibility and scale. Organizations often find that SaaS apps are easier to adapt to evolving needs, easier to integrate and scale with other apps, and more readily support the hybrid workforce. Thus, 66% of respondents adopted a cloud-based IGA after reexamining existing IGA strategies (see Figure 2).

Other changes included investigating zero trust strategies, reported by 52% of respondents, while 50% said they introduced additional automation into processes. Because identity is a fundamental component of trust, a successful zero trust strategy requires a strong foundation for identities and clearly defined least-privilege access policies and

implementations. Workers should be able to efficiently and effectively access only the data needed to do their jobs—nothing more and nothing less. With zero trust, identity becomes a new perimeter.

A cloud-based IGA tool with comprehensive policies enforced via automation can be a key to ensuring the principle of least-privilege access is applied consistently throughout the organization.

Figure 2. Strategic IGA Changes for Hybrid Work



Source: ESG, a division of TechTarget, Inc.

With defense-in-depth a core tenet of any cybersecurity program, IGA continues to be ranked as a top 5 security control priority for their organization by 86% of respondents.

IGA's Evolving Role in Zero Trust and Combatting Ransomware

It's no secret that ransomware has become a major issue and priority for both CISOs and boardrooms. Ransomware is not just a popular buzzword, it's a real problem: 63% of organizations have suffered a ransomware attack in the last year and more than one-third (36%) are attacked by ransomware monthly or more frequently.[1] Since the ransomware kill chain typically starts with an identity-related attack, organizations are recognizing that IGA is an effective weapon in the fight against ransomware. IGA programs help organizations define and enforce identity and access policies, ensuring the removal of unnecessary access, reducing lateral movement and limiting ransomware blast radius. Thus, 90% of respondents agree that implementing an IGA program is an important aspect of their approach to combatting ransomware.

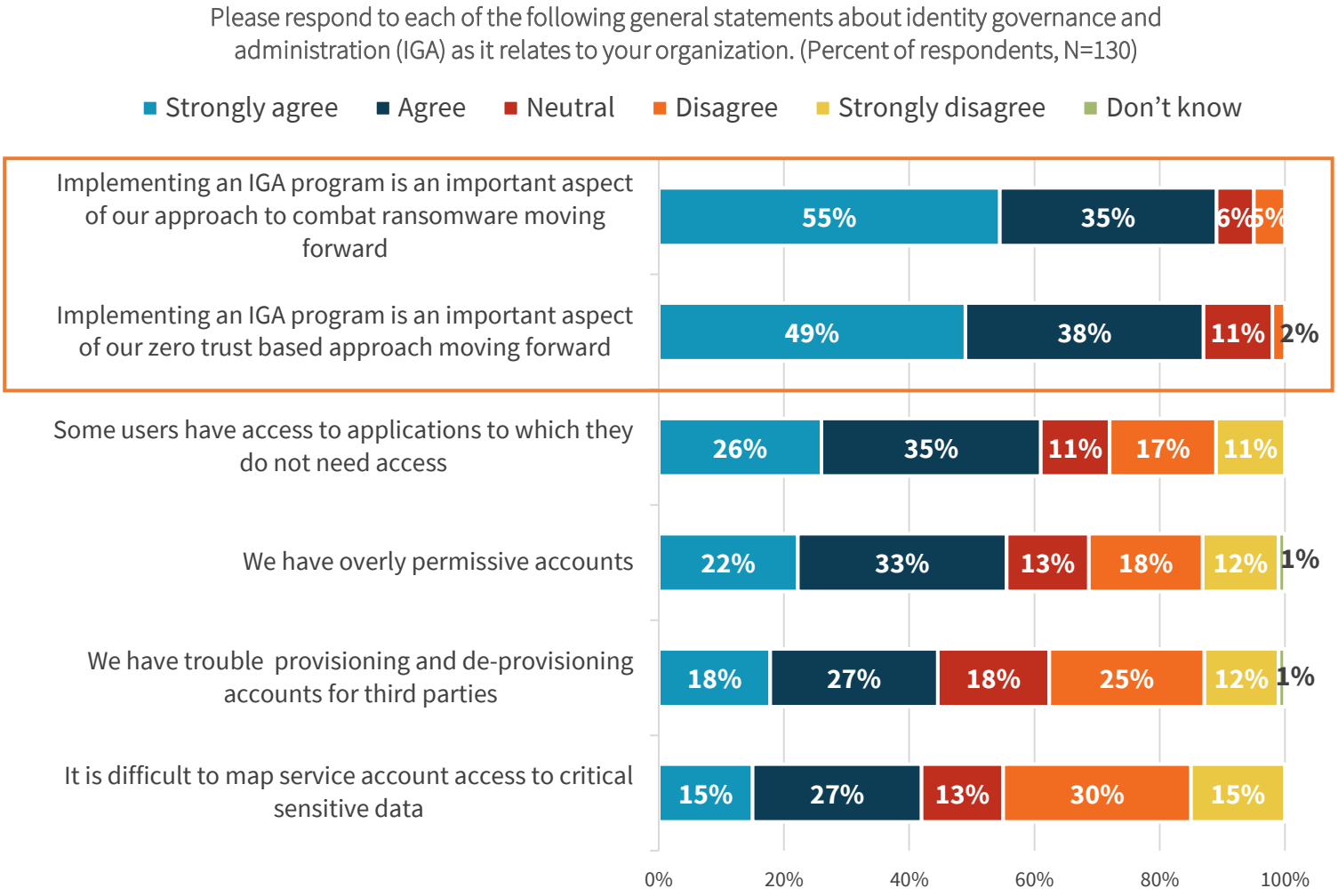
IGA as part of a zero trust network access and/or zero trust application access program saw a 46.4% YoY increase.

Likewise, identity is a fundamental component of zero trust frameworks—you can't decide to trust without understanding the lay of the land in terms of who has and needs access to what. Thus, organizations recognize that IGA has a role to play in implementing zero trust programs: 87% agree that IGA is an important aspect of their zero trust programs, resulting in increased investment in IGA.

[1] Source: ESG Research Report: *2022 Technology Spending Intentions Survey*, November 2021.

In fact, 41% of organizations said that investing in IGA as part of a zero trust network access and/or zero trust application access program will be their most significant investment over the next 12 months, a 46.4% YoY increase (see Figure 3).

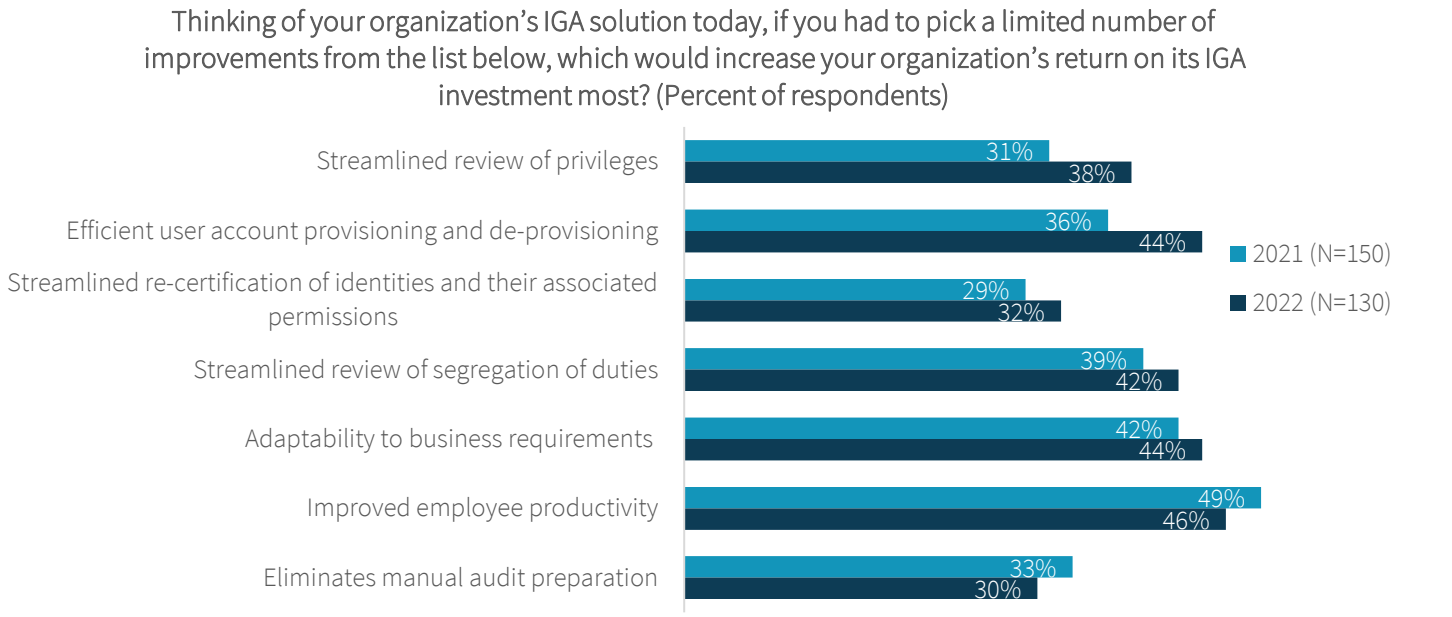
Figure 3. IGA is Important to Combatting Ransomware and Zero Trust



Source: ESG, a division of TechTarget, Inc.

Organizations deploying IGA are focusing on how IGA capabilities directly impact the overall efficiency of an organization's workforce. Improving productivity is at the top of the list of many organizations, with 46% stating that increased workforce productivity would produce the highest tangible ROI. Efficiency improvements were ranked as the most important: 44% indicated that IGA's adaptability to business requirements would most increase IGA ROI, tied with IGA's efficient user account provisioning, and 38% said that IGA's ability to streamline review of privileges would increase its ROI most (see Figure 4). Organizations see that IGA can increase security without increasing friction in the workplace, improving security effectiveness and increasing efficiency.

Figure 4. Maximizing ROI on IGA Solutions



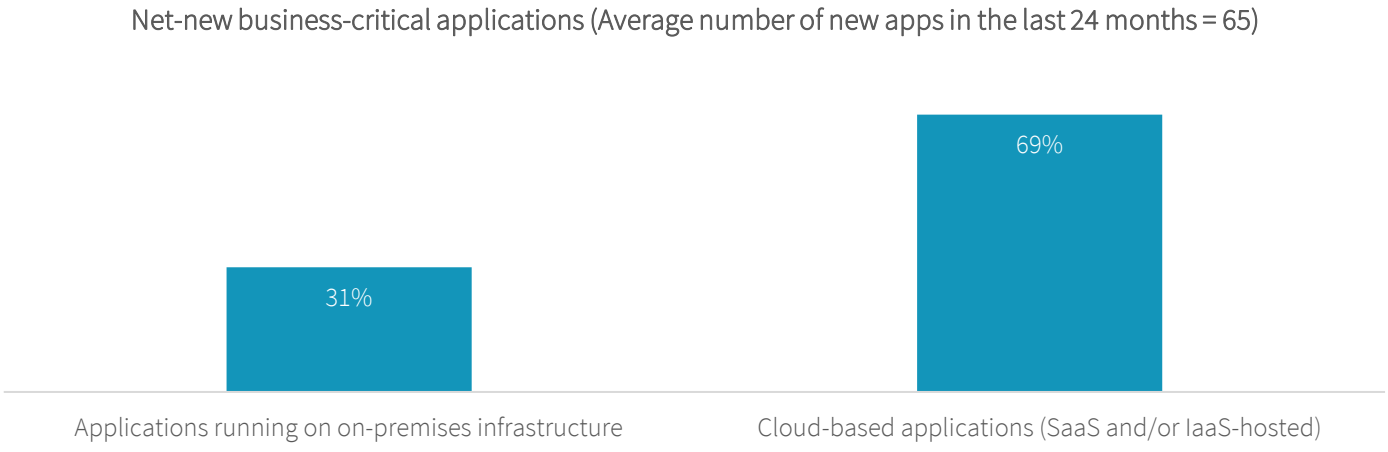
Source: ESG, a division of TechTarget, Inc.

The Shift to the Cloud Creates Identity-related Challenges

As organizations continue to digitally transform and commit to a hybrid workforce, they are adopting a cloud-first strategy, and more business-critical applications are moving to the cloud. 7 out of 10 new business-critical applications will be deployed in the cloud (see Figure 5), and 2.2x more new business-critical applications will be deployed in the cloud than on-premises. We expect this shift to the cloud will continue to accelerate, increasing the complexity of the IT environment and presenting organizations with new challenges.

- **7 out of 10 new business-critical applications will be deployed in the cloud.**
- **2.2x more new business-critical applications will be deployed in the cloud than on-premises.**

Figure 5. Net-new Business-critical Applications



Source: ESG, a division of TechTarget, Inc.

Cloud Apps and Services are Complicating Compliance Requirements

Sixty-four percent of respondents say that cloud adoption is creating regulatory complexity. One driver of this complexity is the high rate of cloud app growth combined with different access models for each app. Cloud-based applications make it difficult for organizations to identify data ownership and data access. The modern organization needs to develop and apply consistent data access policies across the entire suite of cloud apps. Thus, 68% of respondents agree that cloud services for business-critical applications have complicated IGA programs.

51% of respondents say it takes them multiple weeks to identify proper access and permissions for an identity.

Understandably, many organizations are struggling with developing comprehensive and consistent identity and access policies across the disparate suite of applications: 61% of organizations find integrating new applications challenging from an IGA perspective; respondents are 2.3x more likely to find integrating a new application challenging than easy.

Organizations also struggle with implementing governance for their various business applications. More than half of organizations (51%) require multiple weeks to provision proper access and permissions for an identity. During that time, identities that are under-provisioned to these business-critical apps experience a concomitant loss of business and income. Additionally, 45% of respondents agree that it is difficult to identify which users have access to critical sensitive data, hindering their ability to apply least-privilege access principles and increasing the attack surface.

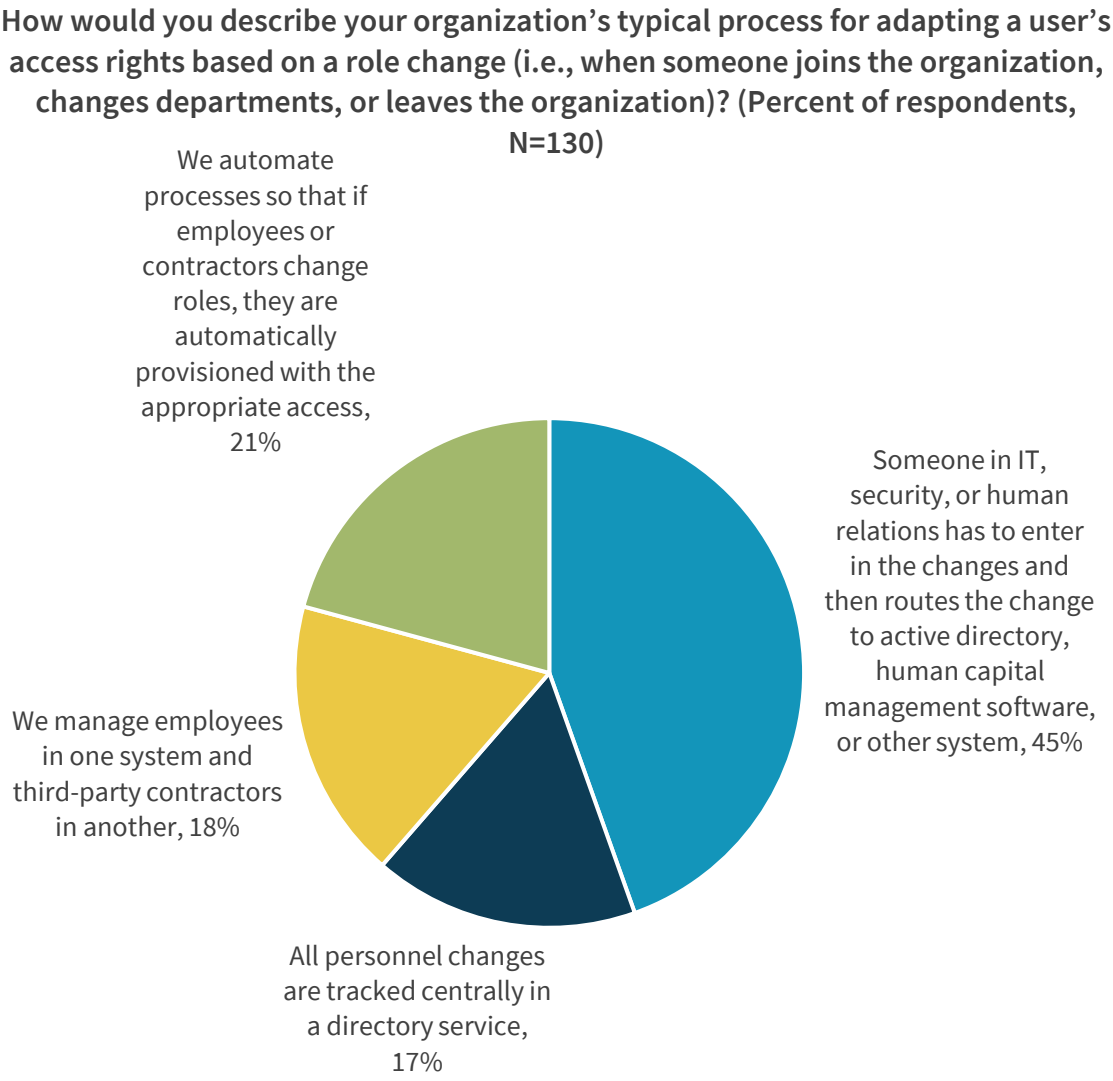
87% say it takes longer than a day to terminate a departing employee's access.

Managing identities with access policies takes significant effort, impacting the organization's security and efficiency, especially when on- and offboarding employees. New employee productivity is hindered, as 49% of organizations say that it's difficult to provision new identities with proper access on day one, resulting in lost business productivity. More concerning is that 87% say it takes longer than a day to terminate a departing employee's access, leaving companies' data and infrastructure exposed. Orphaned or valid accounts not disabled or deleted, along with inactive accounts that likely aren't as closely monitored or guarded, have been exploited by attackers and disgruntled and terminated employees to exfiltrate, expose, and destroy sensitive data and hold data and critical infrastructure hostage.

Organizations continue to have challenges managing and governing identities, especially with the growing fluidity of the workforce. Employees are joining, moving, and leaving companies at an unmatched frequency, and companies frequently leverage contractors, temp workers, third parties, and others, all of whom need access. Thus, organizations now are chartered with securing constantly changing identities in a fluctuating IT environment with a growing number of applications. Ensuring permissions are correct and data is secured in a timely manner is more important than ever. Increasing deployment of applications to the cloud and the connectivity of disparate application environments exacerbates IGA efforts.

Integration and automation can address these challenges, improving efficiency, increasing productivity, and accelerating the effort to reduce the attack surface. However, unfortunately, the identity lifecycle is still not automated, forcing admins to spend time and effort on manual, error-prone processes. Only 18% of organizations automatically update a user's access if their role changes. Unfortunately, almost half (45%) of organizations manually enter changes to multiple systems (see Figure 6). Likewise, 22% of organizations manually review requests for access to applications, and another 28% handle many requests manually, based on context.

Figure 6. Employee Access Update Procedures



Source: ESG, a division of TechTarget, Inc.

The Impact of Compromised Identities

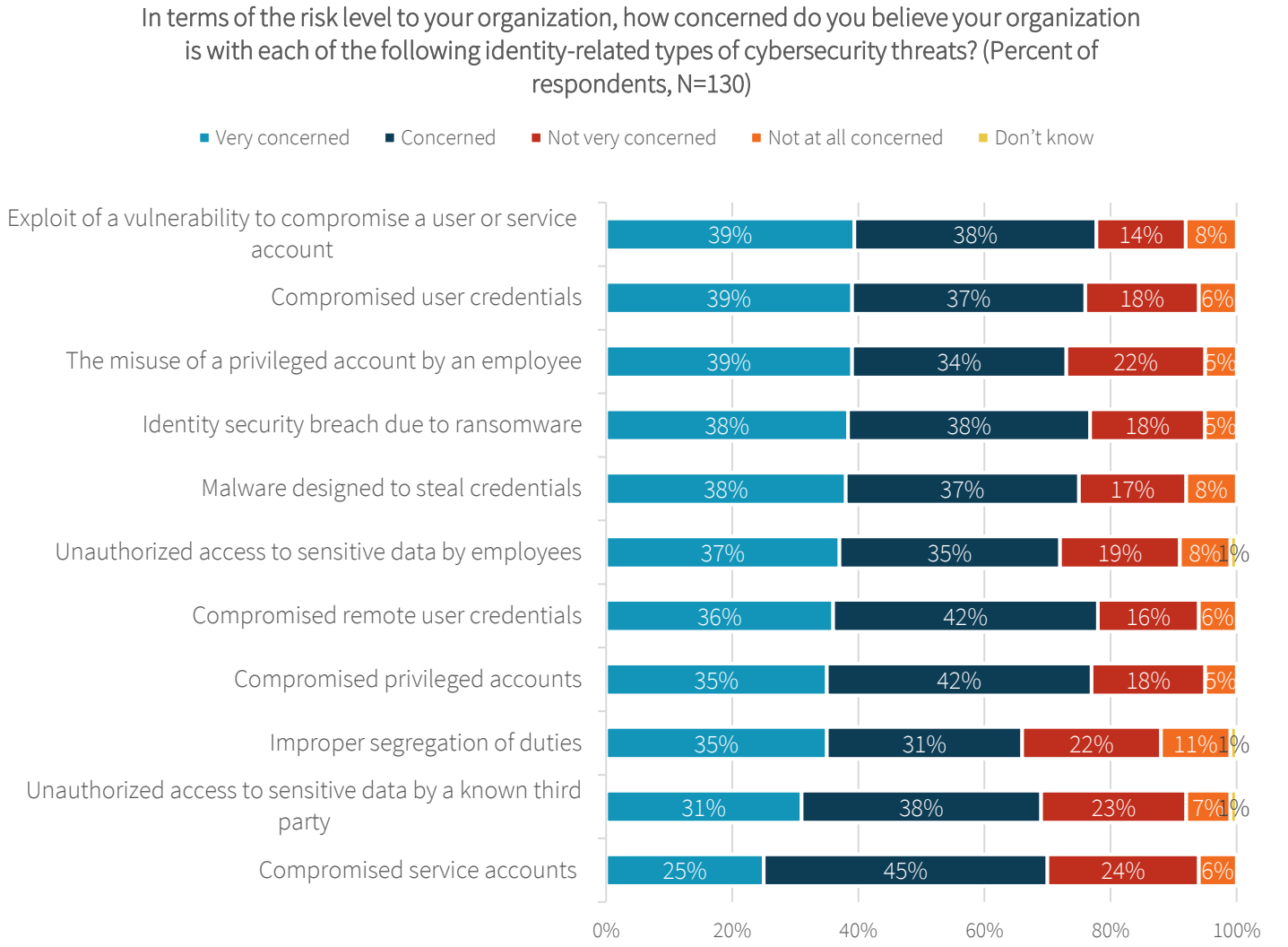
Organizations are concerned with a multitude of identity-related threats and are paying special attention to account takeovers. Seventy-seven percent are concerned or very concerned that malicious actors will exploit a vulnerability to compromise a user or service account. Likewise, 76% are concerned or very concerned about the threat of compromised user credentials, and 75% are concerned or very concerned about malware designed to steal credentials (see Figure 7).

52% of respondents say they either know or suspect they have experienced financial loss due to a cyber-attack.

While external threats get the highest visibility, organizations are not forgetting insider threats. The misuse of a privileged account by an employee is a concern or serious concern to 73%, and 72% are concerned or very concerned about unauthorized access to sensitive data by employees. Unfortunately, these concerns are not rooted in blind fear or unwarranted cynicism: 52% of respondents say they either know or suspect they have experienced financial loss due to a cyber-attack. The access rights a

user needs to do their job are the same access rights the user abuses to exfiltrate sensitive data. Thus, organizations need to continuously evaluate risks and access policies.

Figure 7. Identity-related Attacks that Represent the Greatest Risk



Source: ESG, a division of TechTarget, Inc.

The top four factors contributing to data or financial loss due to an identity-related cybersecurity incident in 2021 were:

- Exploit of a vulnerability to compromise a user or service account (42% of incidents).
- Malware designed to steal credentials (38%).
- The misuse of a privileged account by an employee (38%).
- Unauthorized access to sensitive data by an employee (35%).

Attacker tactics, techniques, and procedures (TTP) shift over time as organizations deploy stronger cybersecurity controls and attackers adapt to these changes, and each of these factors saw a significant year-over-year growth in use. The insider threat—unauthorized access by an employee—grew by more than 20% YoY.

While the use of some TTPs declined relative to new TTPs, the tried-and-true TTPs still represent a significant threat to the organization. Leveraging compromised service accounts and compromised privileged accounts dropped by 22% YoY. However, both of those factors contributed to 31% of data or financial loss in 2021.

The Drivers for Cloud-based IGA

Cloud-based consumption of IGA is actively underway, as 73% of organizations use a cloud-based IGA today, up from 51% a year ago. What is driving the shift to cloud-based IGA?

In addition to conforming with the shift to cloud-first initiatives, the primary benefits of cloud-based IGA, according to respondents, center around efficiency and scale. Forty-two percent value the ability to perform analytics in the cloud, eliminating the need for on-premises appliances. Likewise, 40% value cloud scalability and elimination of the need to manage IGA management servers. Cloud-based IGAs expedite and automate delivery of new features without evaluating and installing software patches and releases, a primary benefit cited by 38% of respondents.

Organizations also value the traditional benefits that accrue from adopted cloud-delivered applications, including a reduction in the number of FTEs needed to manage the solution and the elimination of both CapEx and OpEx to procure and manage on-premises IGA management servers. Altogether, the benefits of cloud delivery are so strong that 72% of respondents said that if they were to start over from scratch, they would deploy a cloud-based IGA solution.

Key IGA Use Cases and Capabilities

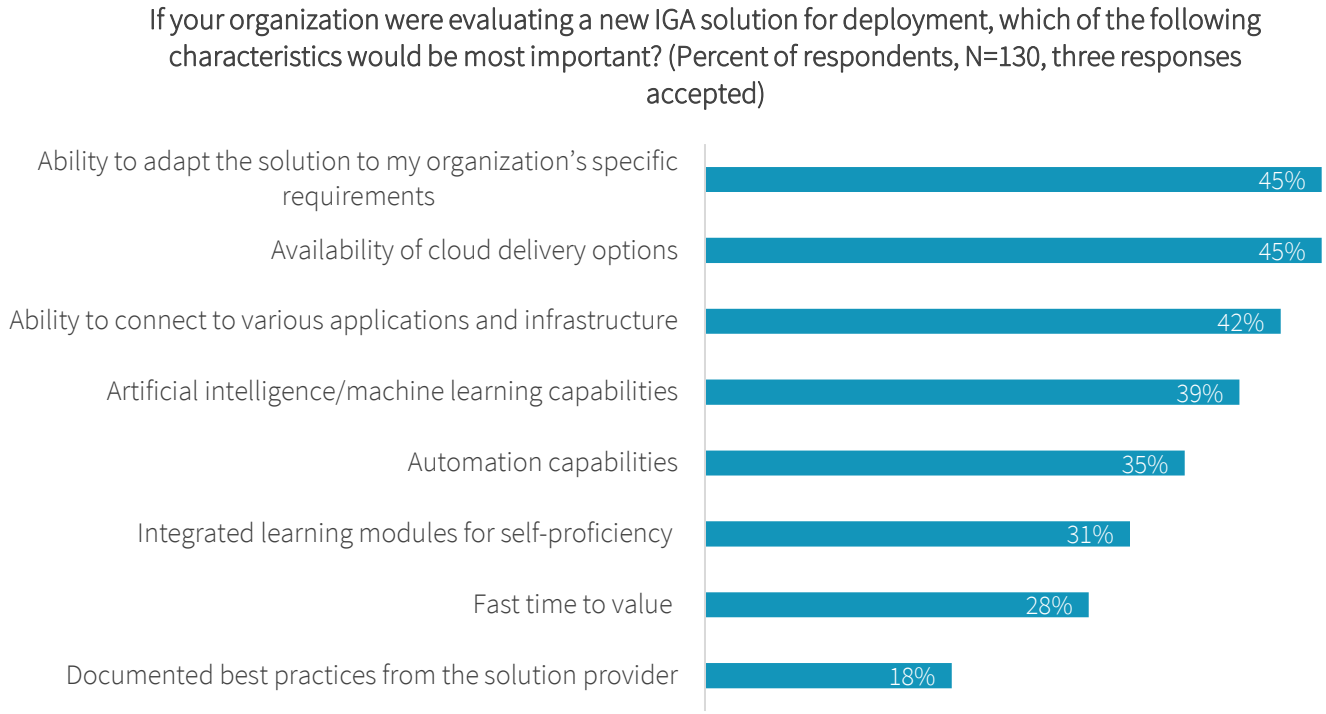
Organizations deploying IGA platforms are focusing on managing identity program. According to respondents, the primary use case for IGA will be sourcing and maintaining identity data, cited by three-quarters (74%), while 72% are planning to use IGA for role management (22% YoY growth).

Increasing efficiency and security by automating certain identity tasks is another area of growth with 70% planning on automating auditing and reporting; two-thirds (68%) planning to leverage automated removal of excessive, unneeded, and unused permissions; and 68% planning on using automated provisioning features (36% YoY growth).

Organizations are also proposing to leverage the computational power, data lakes, and AI capabilities of cloud-delivered IGA solutions. Seventy-two percent will gather identity analytics, and 55% will mine data for appropriate use of roles and data access (36% YoY growth).

The most desirable features of a new IGA solution map to three key pillars of IGA: security, efficiency, and compliance. Respondents ranked efficiency as most important, with cloud delivery options and the ability to adapt the IGA solution to the organization's specific requirements both favored by 45%, and the ability to connect to various applications and infrastructure favored by 42% (see Figure 8). Respondents improve security by applying artificial intelligence to identify and prevent identity-related threats, as well as automating tasks that are otherwise reliant on error-prone manual processes.

Figure 8. IGA Adoption Drivers



Source: ESG, a division of TechTarget, Inc.

The Increasing Investment in IGA

Organizations have come to realize the importance of identity in cybersecurity. Most ransomware attacks, and many other cybersecurity threats, leverage identity as the entry point into the infrastructure. Securing identities and implementing zero trust solutions require investment. Most respondents, 91%, shared that their organization's identity and access management spending will increase over the next 12 months (8% YoY growth), with 47% expecting investments to substantially increase (62% YoY growth) relative to other areas of cybersecurity. Increasing the investment enables organizations to expand their IGA programs to support a broader set of use cases, increasing security and optimizing business efficiencies and user output.

The Bigger Truth

This research clearly highlights the continued and growing importance of identity governance and administration for improved compliance and enhanced efficiency without compromising cybersecurity. The digital workplace, cloud-first strategies, the hybrid workforce, the prominent role of identities in cybersecurity attacks, and the rise of zero trust make securing, managing, and enabling all identities a strategic imperative. Many organizations will invest in a cloud-based IGA as part of modernizing their identity security programs.

Full-featured, cloud-based IGA systems enable organizations to improve both the efficiency and effectiveness of their identity management processes while leveraging advanced analytics and artificial intelligence to identify and remediate identity-related threats and attacks. Organizations also recognize that cloud-based IGA solutions reduce the total cost of ownership 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 strategic priority. The improved efficiency, 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.

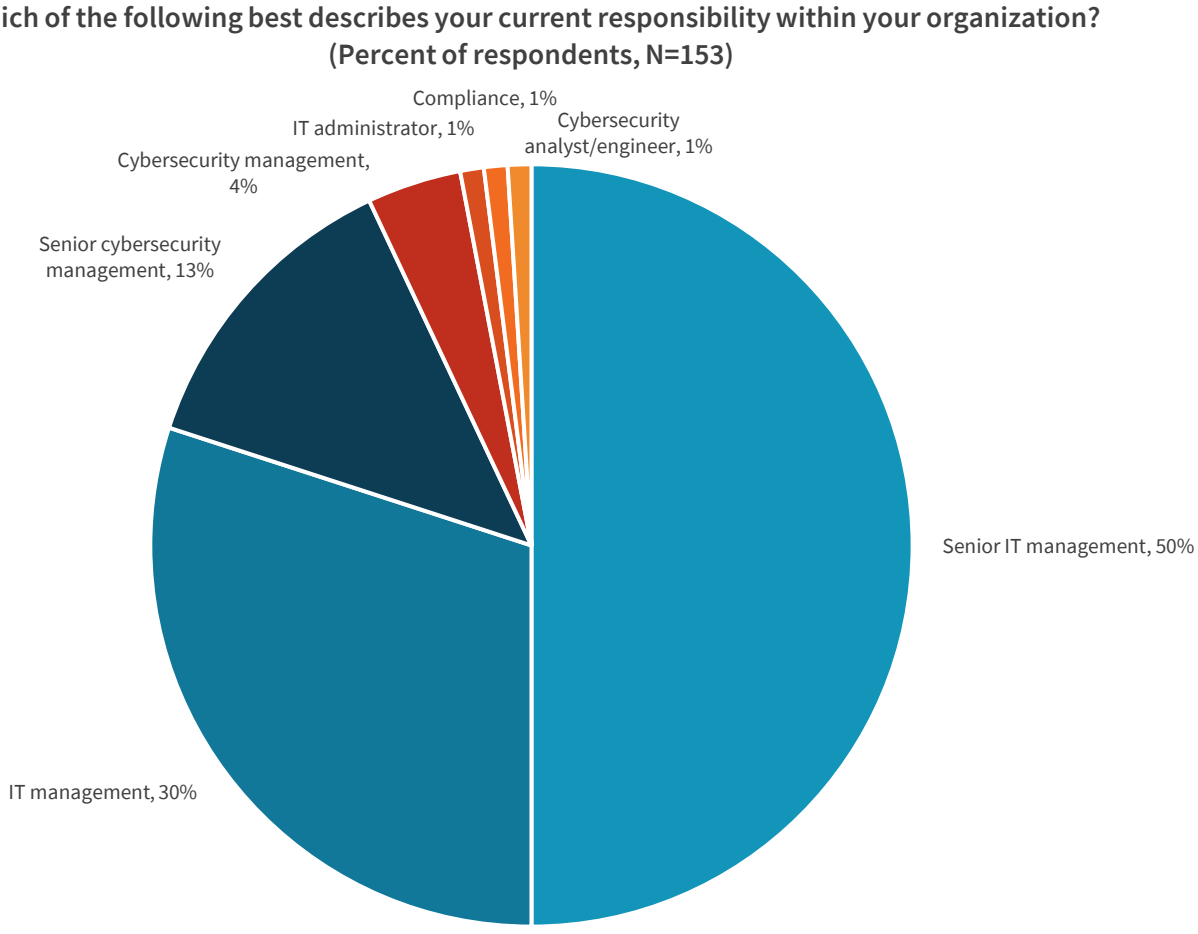
Methodology and Demographics

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 practices and technologies. All respondents were based in the United States. The survey was fielded between November 10, 2021 and November 19, 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 153 respondents remained. The margin of error for a sample size of 153 is + or – 8 percentage points. Figure 9 - Figure 12 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.

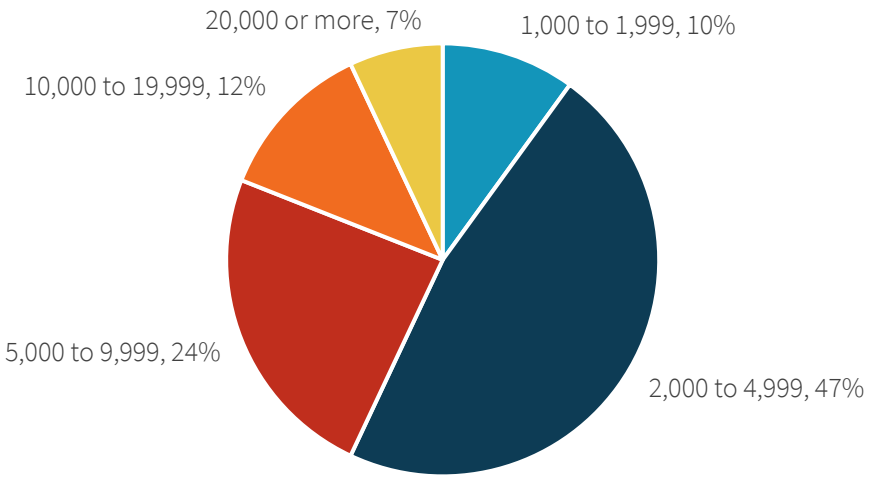
Figure 9. Respondents' Current Responsibility



Source: ESG, a division of TechTarget, Inc.

Figure 10. Respondents by Number of Employees

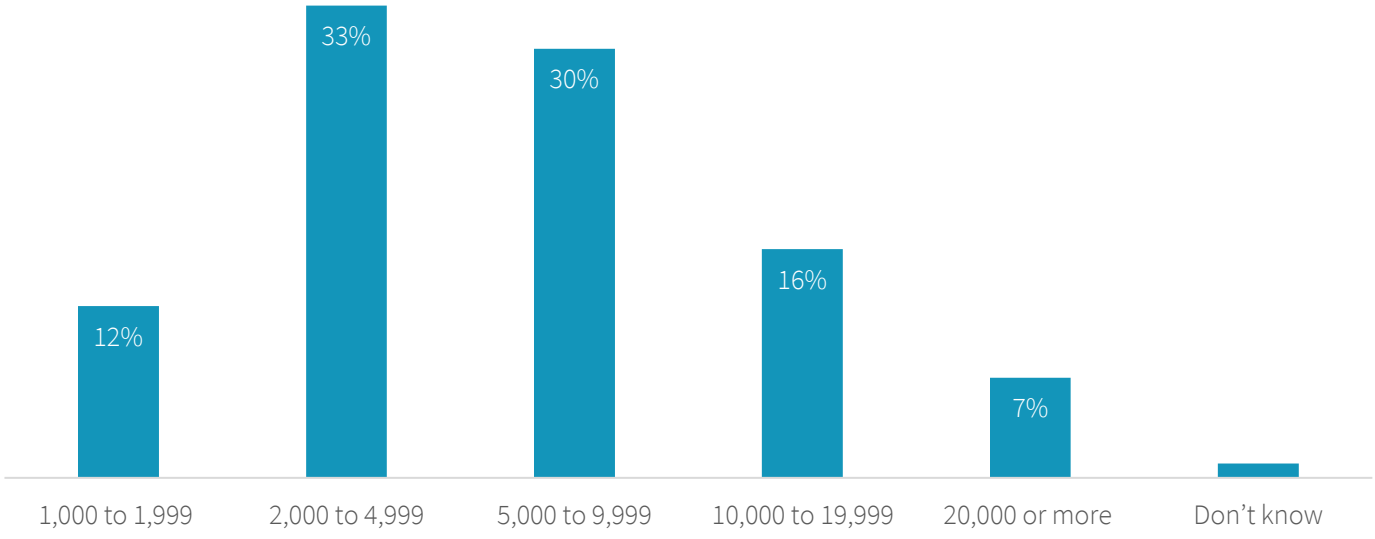
How many total employees does your organization have worldwide? (Percent of respondents, N=153)



Source: ESG, a division of TechTarget, Inc.

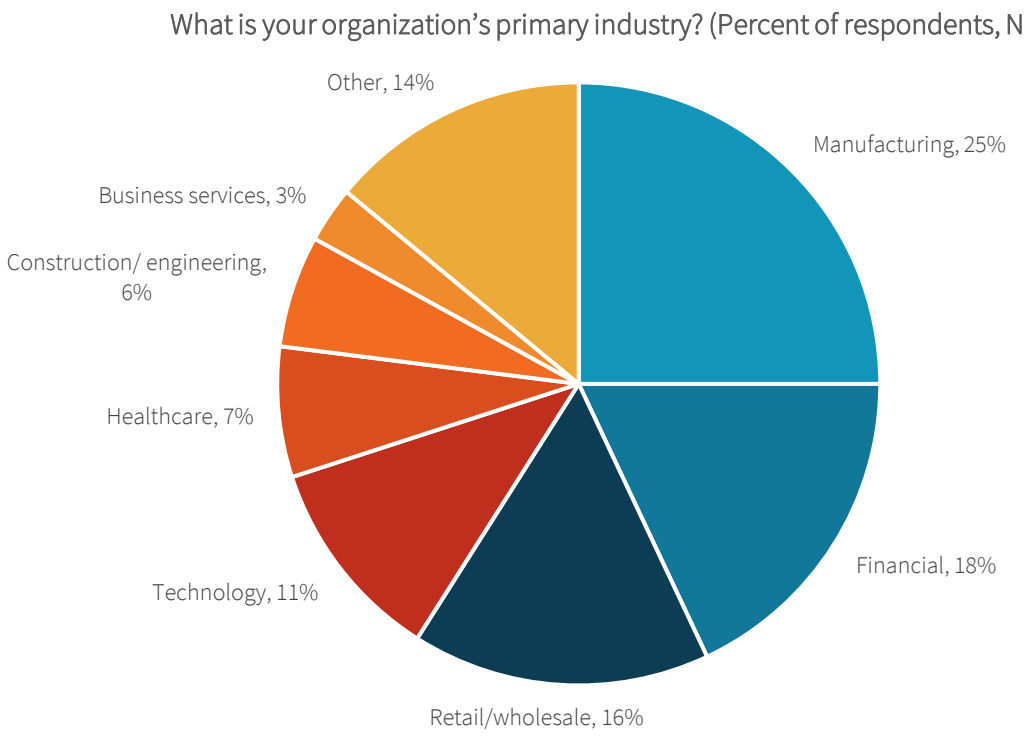
Figure 11. Number of Identities Managed

Approximately how many digital identities does your organization manage today (please include identities associated with both your organization's employees, but also contract workers, vendors, and partners, but exclude customers)? (Percent of respondents, N=153)



Source: ESG, a division of TechTarget, Inc.

Figure 12. Respondents' Primary Industry



Source: ESG, a division of TechTarget, Inc.

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community.

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