Enterprise Strategy Group | Getting to the bigger truth.™

Securing the Identity Perimeter with Defense in Depth

Jack Poller, Senior Analyst

MARCH 2022

Research Objectives

The core tenet of a zero trust strategy is least-privilege access. Yet, organizations continue to rely on user and machine identities that are susceptible to compromise, abuse/misuse, and theft. Risk is compounded by over-permissive, static access rights that provide little to no visibility into who and what is using access and how. Vaguer is how identities are being/should be monitored and protected.

Availability of modern, cloud-managed identity services is widespread. Yet organizations have been slow to pivot their security programs from traditional endpoint, network, and SecOps to an approach that focuses on identity orchestration and experiences, which is dynamic and distributed. Where there are no perimeters, a multitude of identity verification services and managed identity services exist.

In order to gain insights into these trends, ESG surveyed 488 IT and cybersecurity professionals personally responsible for identity and access management programs, projects, processes, solutions/platforms, and services at large midmarket (500 to 999 employees) and enterprise (1,000 or more employees) organizations in North America (US and Canada).

THIS STUDY SOUGHT TO:

Understand the community that is influencing and prioritizing IAM initiatives, their journey to a modern identity strategy, and what resonates with them.

Examine the results of successful zero trust/least-privilege access projects, lessons learned, gaps, and remaining hurdles.

Determine the breadth of products, platforms, and technologies supporting current business operations and how that is expected to evolve over time.

Gain differentiated insights into the awareness, planning, budgeting, purchasing, and implementation dynamics across organizations.

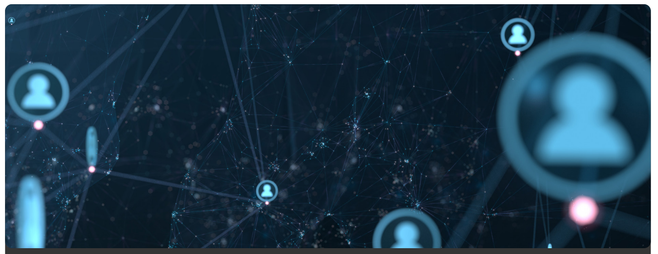
Back to Contents

TABLE OF CONTENTS

CLICK TO FOLLOW

Identity Management Is Complex

PAGE 3

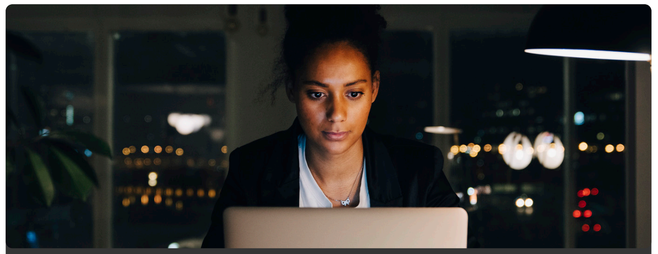


The Need to Operationalize Different Forms of Authentication

PAGE 8

Assessing Risk Across Human and Non-human Identities Is a Priority

PAGE 12



Identity Proofing, Screening, and Monitoring Reduce Risk

PAGE 15

Commercial CIAM Solutions Provide Performance, Scale, Security, and Privacy

PAGE 18

Identity Market Dynamics

PAGE 21

Identity Management Is Complex

Complexity of IAM Leads to Extensive Use of Third-party Services

IAM programs are complex and require much more than just creating a username and password. Identity professionals must develop and enforce access policies, ensuring the principle of least-privilege access is correctly and uniformly applied. They must also ensure access and privacy is protected without introducing friction or destroying the user experience. Another concern is managing and governing privileged and normal access.

Identity professionals have become experts in many areas of identity management. Thus, more than three-quarters of identity professionals manage all three human identity types: employee, third-party workforce, and customer.

The complexity combined with the long-term IT skills shortage leads to extensive use of managed services and professional services in support of IAM.

> **“More than three-quarters of identity professionals** manage all three human identity types: employee, third-party workforce, and customer.”

87%

of organizations **use third-party IAM services.**

Back to Contents

PAM Is a Low-impact Strategic Security Control

Identities with privileged access represent a huge risk to the organization. These identities are the “keys to the kingdom.” Thus, managing privileged access can increase security without friction, and PAM is considered a strategic security control. More than half (51%) rank PAM among their top three risk, identity, and security management programs, and another 39% rank PAM in the top five.

More than half (58%) of organizations use PAM to monitor, record, audit, and report on privileged access activities. Fifty-seven percent are integrating PAM across SaaS apps, on-premises departmental and line-of-business apps, facilities, physical access controls, and building systems to manage and control privileged access across the entire IT and physical landscape.

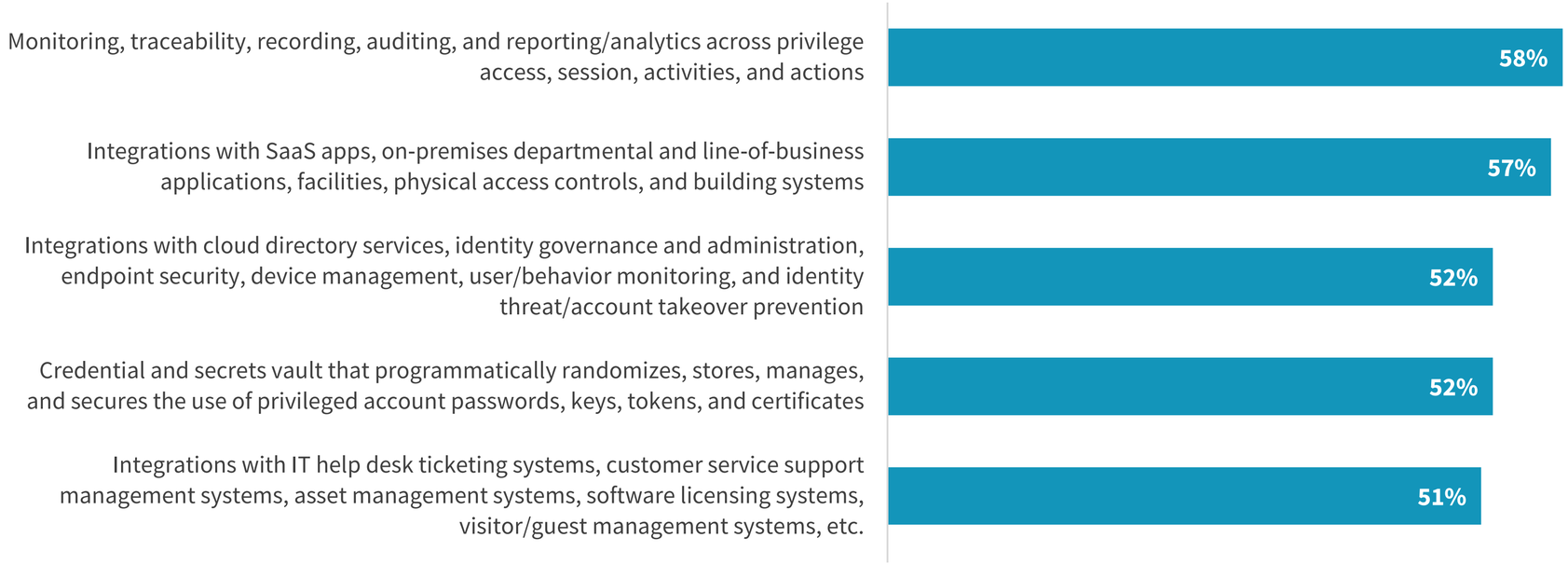
PAM is among the top three solutions/controls for my organization,

51%

PAM is among the top five solutions/controls for my organization,

39%

Five most commonly used commercial PAM features and capabilities.



Back to Contents

IGA Use Expands to Support Cloud, Hybrid/SaaS, Workload Identities, and Business Process Automation

Historically, governance tools were the purview of audit and compliance. Organizations now realize that identity governance enhances security through centralized policy management, improved visibility, and automation. Additionally, organizations realize financial benefits and improved user satisfaction when deploying IGA solutions.

Organizations can increase the benefits of IGA programs by integrating IGA with the help desk and customer support, cloud directory services, PAM, endpoint security solutions, and SaaS apps to provide increased visibility, auditing, and monitoring, as well as more uniform application of policies.

More than half of organizations are planning to expand IGA to cover more use cases. Fifty-four percent plan to expand their existing IGA, especially to support existing cloud, SaaS, and hybrid apps; 50% plan to apply governance to workload identities; and 50% plan to integrate IGA to support their new apps and business processes.

How do organizations judge the success of IGA programs? Half expect improvements in their risk management posture. More than a third (37%) expect increased visibility, while 36% expect to realize operational savings through ease of integration, automation, and managed services. Thirty-five percent expect financial benefits, and 34% expect high satisfaction user experience scores.

Likeliest actions to be taken with IGA solutions in the next 12-18 months.

35%

Expand use of existing IGA to support cloud/ hybrid/SaaS

29%

Expand use of existing IGA solution

21%

Expand use of existing IGA to support workload identities

32%

Add new integrations or business/process automation

Five most commonly used metrics to measure IGA effectiveness.

50%

Achieving improved risk management posture

37%

Improving visibility

36%

Operational savings due to ease of integration, automation, managed services models, etc.

35%

Realizing financial benefits

34%

Delivering high satisfaction user experience scores

Back to Contents

The Need to Operationalize Different Forms of Authentication

MFA Is Considered the Most Effective IAM Solution

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 are attacked by ransomware monthly or more frequently. Since the ransomware kill chain typically starts with an identity-related attack, organizations are recognizing that protecting identities is a primary cybersecurity concern.

With passwords being the weak link, the value of multifactor authentication becomes readily apparent. Thus, it's no surprise that 58% of organizations have implemented MFA, and that 23% of organizations rank MFA as the most effective IAM solution, the highest-ranking response.

However, despite all the known identity risks and the protection afforded by MFA, 32% of organizations make MFA optional for employees, and 27% make MFA optional for their third-party workforce.

"32% of organizations make MFA optional for employees, and 27% make MFA optional for their third-party workforce."

58%

currently use multifactor authentication.

Five most effective IAM technologies.

23%

Multifactor authentication

14%

Single sign-on access management

13%

Cloud infrastructure entitlement management

12%

Customer identity and access management

11%

Identity-as-a-service

Back to Contents

Passwordless Is Becoming Strategic

Passwords have always been a pain point for users and cybersecurity professionals alike. Weak passwords are a huge risk to the organization while strong passwords are hard to create and even harder to remember.

With the increasing sophistication of attackers and ready access to massive parallel computing power, usable passwords are simply not secure enough. Thus, eliminating passwords has garnered significant interest. Reducing friction while increasing security is a win-win situation for the users and the organization, which is why passwordless is rapidly gaining favor. Indeed, nearly one in five organizations are well down the passwordless journey, selectively eliminating passwords during the authentication process. Another 37% are actively evaluating and testing passwordless technology.

And the results of deploying passwordless authentication technology has clear benefits. Almost two-thirds (63%) of organizations report that passwordless has significantly increased IT security and efficiency. More than half (57%) say passwordless has significantly reduced friction, improving the user experience, while 56% report that they have significantly reduced organizational risk.

We have started to selectively eliminate passwords,

17%

We are actively evaluating/testing eliminating passwords,

37%

Areas in which passwordless has had a significant positive impact.

63%
Increased IT / security efficiency

57%
Improved user experience

56%
Reduced risk

Passwordless authentication is our top identity-related activity,

31%

Passwordless authentication is among our top three identity-related activities,

34%

Back to Contents

Majority of Organizations Use SSO

The majority (55%) of organizations currently leverage single sign-on technologies today. Like passwordless, organizations see SSO as a win-win, reducing friction and improving the user experience while enhancing security by increasing compliance to access policies.

Unfortunately, not all SaaS apps are SSO-enabled. Thus, while 8% mandate that all SaaS apps are SSO-enabled, a more realistic 70% of organizations use SSO for more than half of their SaaS apps.

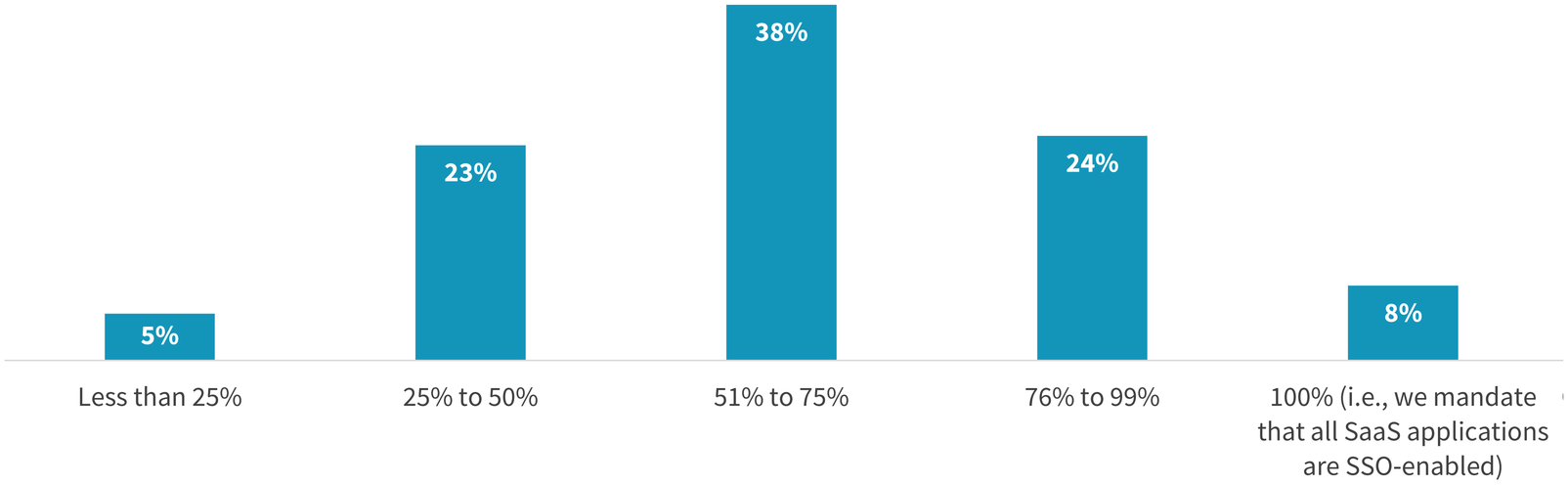
55%

of organizations currently use SSO technology.

48%

expect SSO to reduce friction and improve the user experience.

Percentage of SaaS applications that are SSO-enabled and -managed.



Back to Contents

Assessing Risk Across Human and Non-human Identities Is a Priority

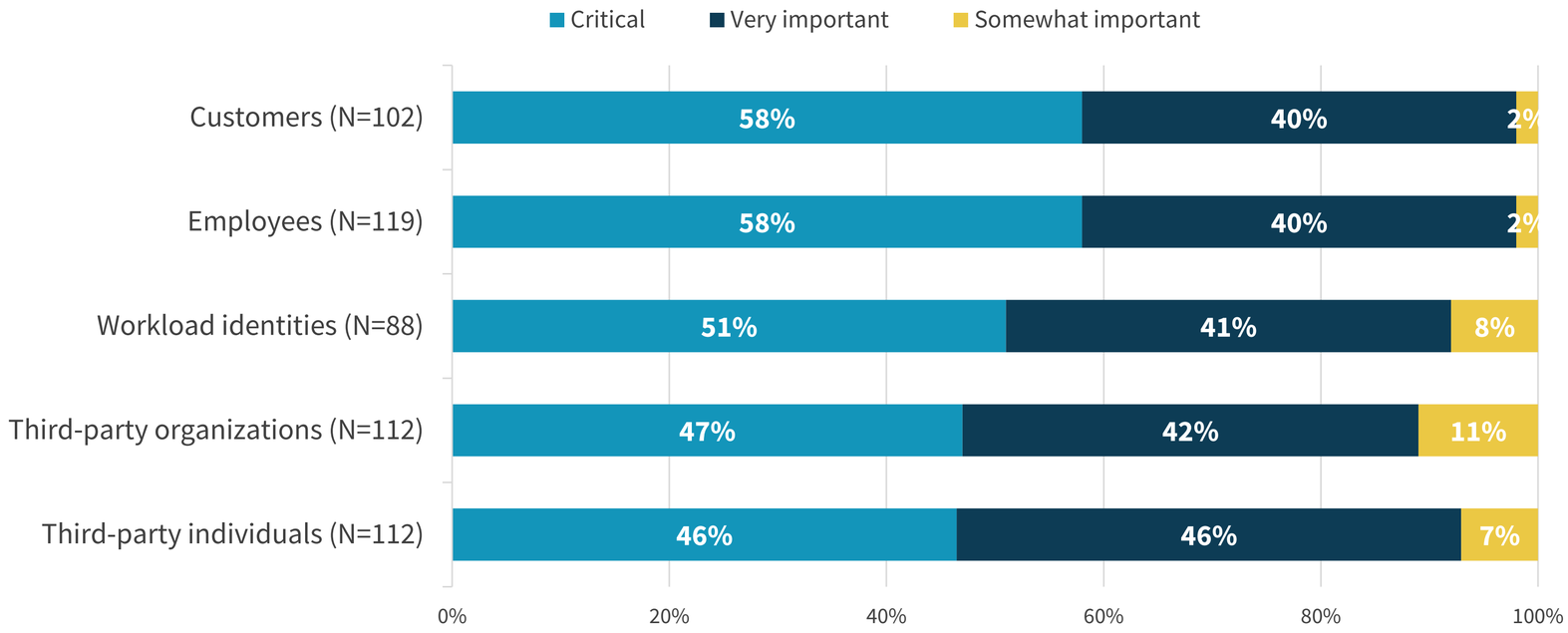
Risk Scoring Is Important for All Identity Types

Risk scoring has a long history and can include factors such as creditworthiness, security audits, historical information, and more. Fifty-eight percent of organizations consider customer risk scoring to be critically important, and almost half of organizations critically value risk scores for both third-party organizations and individuals.

Surprisingly, more than half (58%) consider employee risk scoring to be critically important. It's safe to assume that many of these organizations have been harmed by insider attacks and malicious employee behaviors and are now leveraging risk scoring as part of the credential authorization process.

> "Fifty-eight percent of organizations consider **customer risk scoring to be critically important."**

Importance of risk scoring for each identity category.



Back to Contents

Wide Variety of Vectors Spanning Identities, Permissions, and Workloads Have Contributed to Breaches

Attackers will often take the path of least resistance. Why bother trying to steal or crack a password when that password is easily grabbed from system memory? But that doesn't mean that attackers lack sophistication. Financial and other motives are so strong that nearly half (45%) of organizations have been breached by an identity-related attack. And attacks came from both inside and outside the organization.

While ransomware, malware, and other external attacks garner the publicity and attention, organizations suffer attacks from both insiders and external parties leveraging over-permissioned and underutilized identities. Forgotten, inactive, or unused accounts, service accounts, and third-party accounts all represent risks that have been used by attackers for access and lateral movement. Indeed, these permission- and entitlement-related threats have resulted in successful attacks for 36% of organizations.

Likewise, all types of applications, workloads, and devices are vectors for attacks and breaches. More than one-third (37%) of organizations have suffered an attack originating via cloud email and communications apps, on-premises email and communication apps, endpoints, IT infrastructure, cloud infrastructure, SaaS apps, legacy apps, and more.

Organizations that ignore identity-related threats, regardless of identity type or access type, do so at their own peril.

Percentage of organizations that have suffered a breach due to:

45%
Identity-related threats

36%
Permission-related threats

37%
Workload/deployment model-related threats

Back to Contents

Identity Proofing, Screening, and Monitoring Reduce Risk

Majority of Organizations Perform People Risk Screening

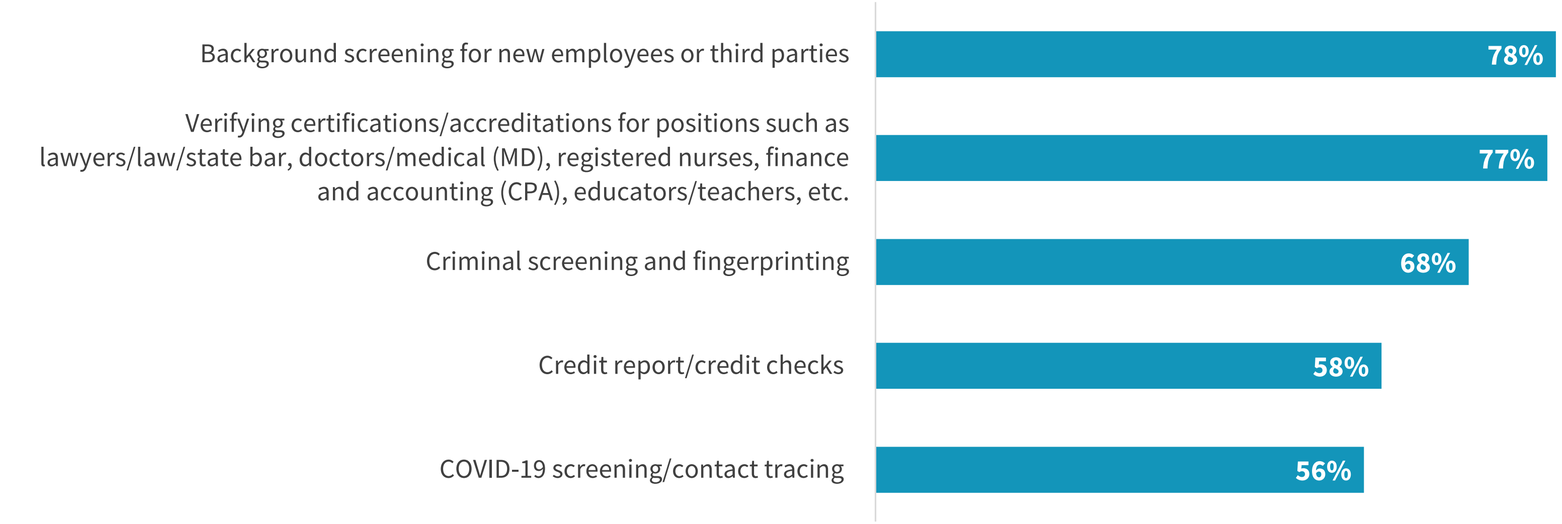
With the acceptance of the full-time hybrid workforce, organizations are hiring remote employees and contractors without ever physically meeting candidates. Likewise, financial, retail, and other businesses are opening accounts online rather than in person. Thus, it's no surprise that organizations need to validate a person is who they say they are.

The post-pandemic economic surge has led to a shortage of labor, an increase in the use of contractors, and an increase in the cooperation and integration of third parties into internal systems. This explosion of third-party identities increases organizational risks that may be hard to identify and quantify.

More than three-quarters (78%) of organizations perform background screening for new employees or third parties, while 77% verify certifications and accreditations for credentialed positions such as lawyers, doctors, nurses, finance, accounting, etc. Two-thirds (68%) perform criminal screening and fingerprinting, and more than half (58%) check credit reports.

Pre-engagement verification of third-party organizations and individuals is often deemed insufficient for protecting against long-term risks. Thus, 52% of organizations monitor backgrounds during the lifecycle of services and perform routine identity-related audits to ensure adherence to standards.

Risk screening processes currently used.



Processes used today to minimize third-party and vendor risks.

54%
Proof and verify third-party organizations before they are granted access to systems

53%
Proof and verify third-party individuals before they are granted access to sites and systems

52%
Monitor backgrounds during the lifecycle of services to our organization

52%
Perform identity audits on third-party vendors and their staff to ensure adherence to standards

50%
Use legal and service agreements with third-party vendors that require a background screen of their staff/employees

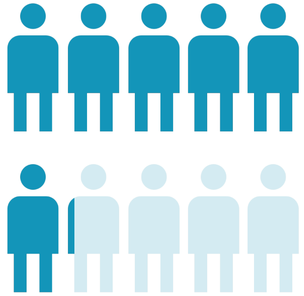
Back to Contents

Majority of Organizations Believe It's Extremely Likely They Have Multiple Identity Records for a Single Employee or Customer

The majority of organizations believe it is extremely likely that they have multiple identity records for an individual employee (61%) and/or customer (52%).

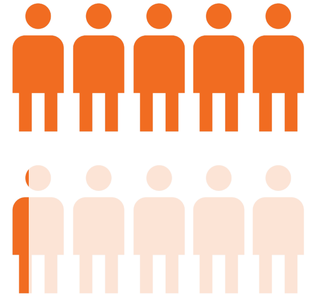
Is an individual using multiple identities for nefarious reasons, such as fraud, theft, or cyber-attacks? While there may be valid reasons for having multiple identity records, organizations need to know with certainty who has access and ascertain all identities of each person to adequately and realistically quantify, assess, and address identity-related risks.

Nearly three-quarters (72%) leverage authorized sources to identify identity attributes, and another 65% combine the digitization of identity documents with liveliness or voice verification.



61%

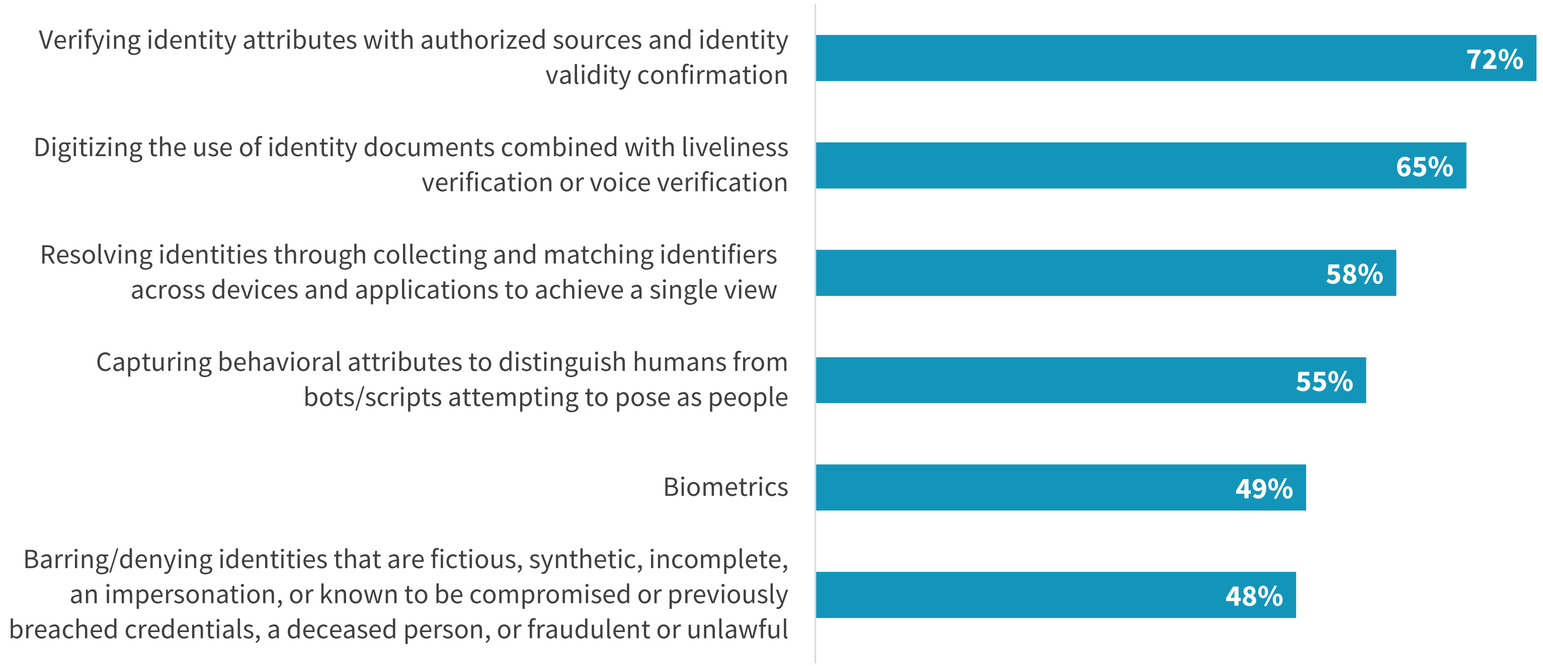
have multiple identity records for a single employee.



52%

have multiple identity records for a single customer.

Most common identity proofing/verification use cases.



Back to Contents

Commercial CIAM Solutions Provide Performance, Scale, Security, and Privacy

Integrating CIAM with CRM Enhances the Customer Experience

Managing customer and third-party usernames and passwords is deceptively simple, leading organizations down the long and tortuous path of building their own solutions. Organizations that deploy a commercial CIAM solution increase performance and scalability.

More than two-thirds (68%) say that it is important to integrate CIAM with their CRM solution, while at least half value integrating CIAM with payment services and customer support. It's clear that CIAM is seen as a gateway to providing a unified, integrated user experience to enhance customer satisfaction.

Commercial CIAM solutions provide organizations with multiple methods to manage customer risk such as monitoring accounts for indicators of compromise. One-third (37%) monitor customers for unusual increases in transactions or higher transactions values, 36% monitor for significant profile changes, and 34% monitor for multiple or failed authentication attempts. Organizations use CIAM to monitor and identify many other IoCs such as using a new device, anomalous uses of time, place, or device, and multiple simultaneous sessions.

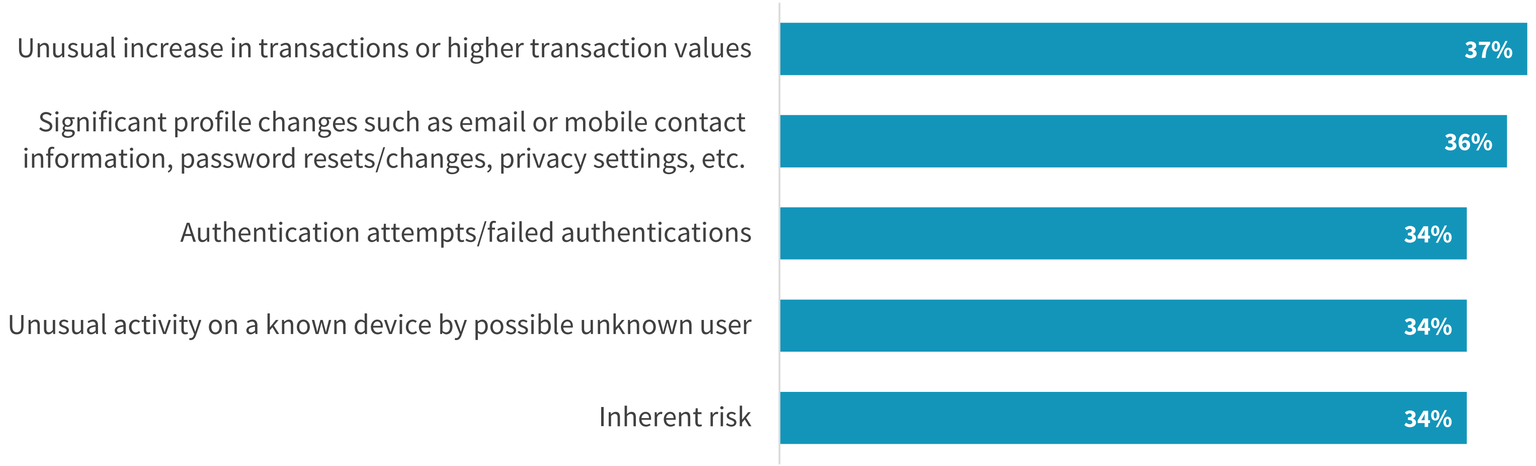
Most important solutions to integrate with CIAM.

68%
Customer relationship management/SaaS or software provider

52%
Customer support/ service provider

50%
Payment gateway/ services provider

Customer 'identity activities' that organizations actively monitor.



Back to Contents

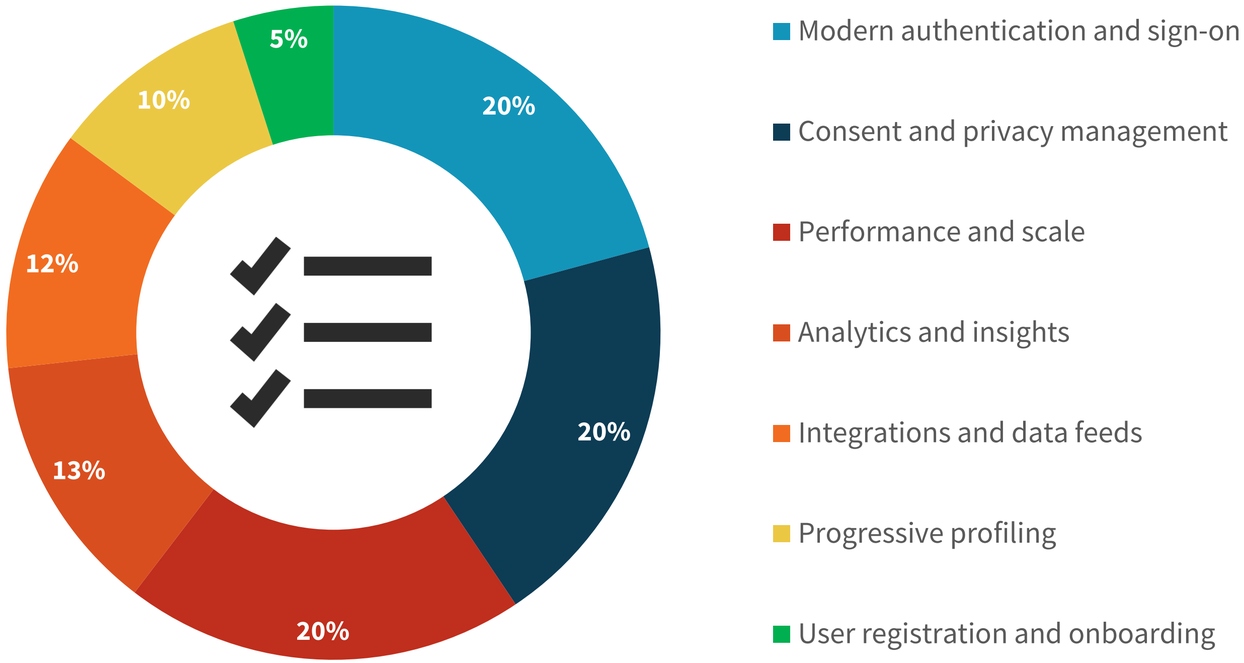
Most Desirable CIAM Capabilities

To further enhance the customer experience and provide a secure customer portal, organizations want CIAM to provide modern features, including modern authentication and sign-on (e.g., MFA, passwordless, and SSO).

Organizations are also facing a privacy push-pull situation, where consumers are demanding increasing privacy and control over their own data, while multiple disparate privacy regulations and laws require complex privacy, data use, and breach notification policies. Thus, CIAM should provide consent and privacy management features for both the customer and the identity professional.

> “CIAM should provide consent and privacy management features **for both the customer and the identity professional.”**

Most important CIAM capability.



Back to Contents

Identity Market Dynamics

Identity Security to Capture More of the Cybersecurity Budget

For a majority of organizations, cybersecurity modernization and digital transformation still garner the majority of business initiative interest and investment.

And many have awoken to the central role identity plays in threats and attacks and are now investing more in identity security relative to other areas of cybersecurity. It follows then that 84% of organizations expect to increase IAM spending over the next 12 months.

More than one-third (37%) will apply increased identity security budget to workforce identity security, one-quarter (26%) will invest in customer identity security, one-fifth (20%) will apply increased investment to third-party identity security activities, and 17% will apply increased investments to workload identity security activities.

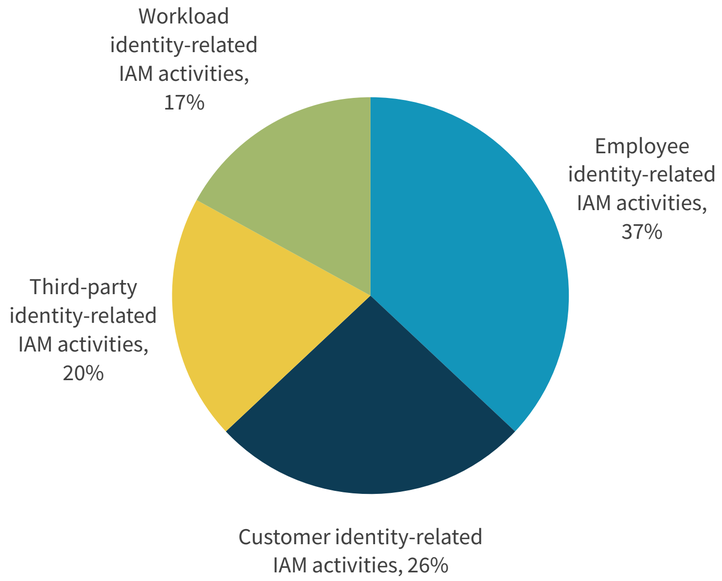
Nearly one-third (31%) of organizations will apply identity security investments to cloud infrastructure entitlement management, and 30% will apply new investments to customer identity and access management. Other prime areas for new investment include MFA, identity-as-a-service, identity proofing, and identity risk services.

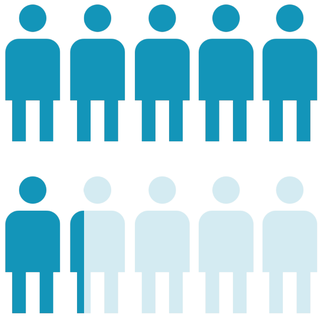
Expected change in IAM spending over the next 12 months.

Increase significantly,
37%

Increase slightly,
47%

Identity type expected to receive the biggest share of increased IAM spending.





61%
of organizations expect new IAM spending to be focused on CIEM and/or CIAM.

Back to Contents

SECUREAUTH

SecureAuth is a leading next-gen authentication company that enables the most secure and flexible authentication experience for employees, partners, and customers. With the only solution that can be deployed in cloud, hybrid, or on-premises environments, SecureAuth manages and protects access to applications, systems, and data at scale, anywhere in the world.

LEARN MORE

ABOUT ESG

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

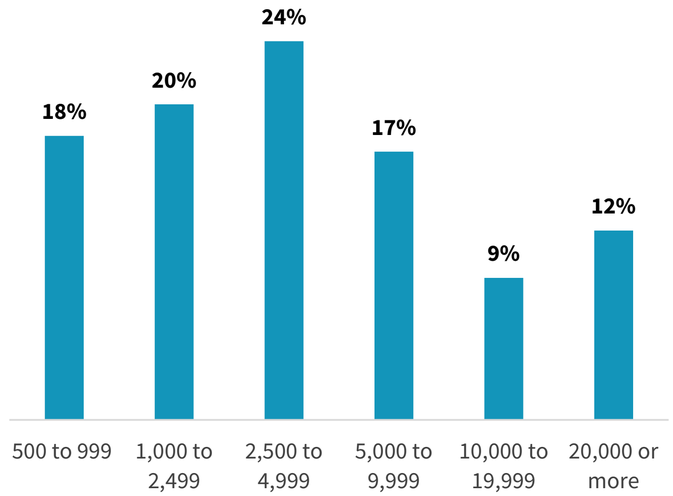
Back to Contents

Research Methodology

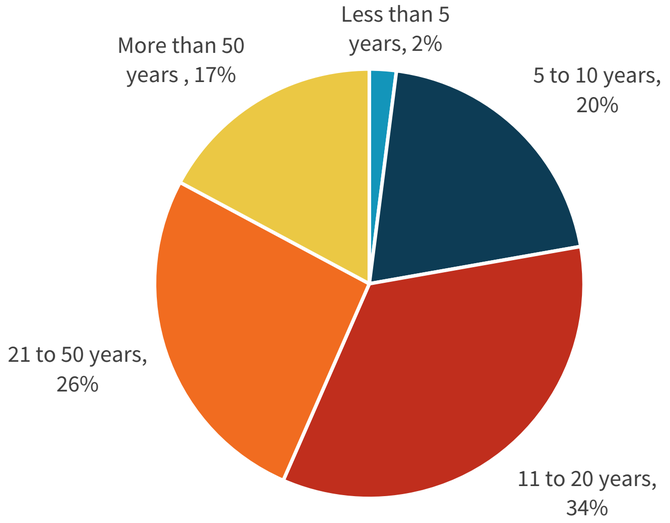
To gather data for this report, ESG conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations in North America between December 14, 2021 and December 28, 2021. To qualify for this survey, respondents were required to be IT or cybersecurity professionals responsible for identity and access management programs, projects, processes, solutions/platforms, and services. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 488 IT and cybersecurity professionals.

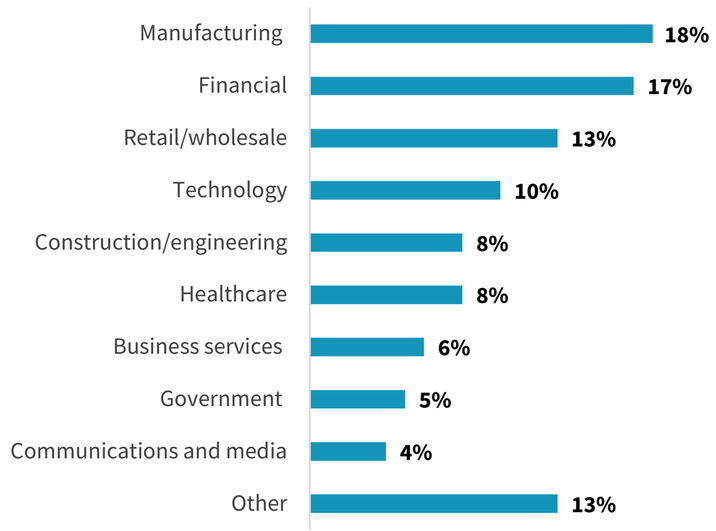
RESPONDENTS BY NUMBER OF EMPLOYEES



RESPONDENTS BY AGE OF COMPANY



RESPONDENTS BY INDUSTRY



Back to Contents

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