Research Report

B2B IAM – the hidden value of third-party identities

S&P Global
Market Intelligence

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

Executive summary

External or third-party identities — contractors, vendors, consultants, partners, suppliers, corporate customers, etc. — represent a large, growing and relatively under-protected user population for most enterprises. Addressing the needs of such users is the realm of an emerging segment of the identity and access management (IAM) market: business-to-business IAM. While B2B IAM has much in common with its IAM "cousins" workforce IAM (WIAM) and customer IAM (CIAM), B2B IAM is becoming its own category in the broader IAM market, with unique requirements for serving the range of external user personas. Addressing B2B IAM use cases, therefore, requires a distinct technological approach — it is not enough to "shoehorn" traditional CIAM, WIAM or even identity governance and administration (IGA) offerings to address modern B2B scenarios.

Done correctly, B2B IAM can help companies improve their overall security by protecting against identity-based attacks. And with supply chain attacks becoming increasingly common, B2B IAM can be a pillar for managing third-party risks and establishing a zero-trust foundation for the extended enterprise. B2B IAM can also streamline operations and reduce the costs of administering non-employee identities, and potentially drive new streams of revenue. B2B IAM is as much about operational efficiency and business enablement as it is about security, and as such, it is a board-level topic that C-suite executives need to be aware of.

Key findings

- B2B IAM has much in common with WIAM, CIAM and IGA, and in a sense can be considered a bridge that spans all three. However, several capabilities stand out as being particularly important for B2B IAM: user delegation, relationship-based access control (ReBAC) and self-service access requests. Delegated user management can help reduce third-party risks and increase trust between organizations, as well as help enhance overall productivity.
- Among surveyed organizations, external identities outnumber traditional employees by nearly two to one. The 2024 Data Threat Report (DTR) survey, commissioned by Thales and conducted by S&P Global Market Intelligence 451 Research, shows that while traditional "internal" employees are the largest single group of users accessing corporate networks (29%), non-employees or "external identities" in aggregate (contractors, vendors, etc.) account for nearly half of total users (48%).
- Additional survey data shows that the top challenges for securely onboarding new external identities include addressing security inconsistencies across workforce and non-workforce identities, standards-based authentication and authorization for developers, and eliminating user friction. The top steps to enable a more trusted relationship with external users were greater self-service, user journey orchestration, and improved user or customer experience.
- Supply chain attacks are increasingly common, and by definition typically involve third-party identities. As such, nearly one-quarter of respondents to the recent DTR survey cited external identities as a top-three target for cyberattacks. However, when asked what security tools they are spending on today, respondents ranked external identity tools in the bottom half of the list. This suggests a disconnect in corporate security budgeting decisions, which in turn could lead to a gap in an organization's overall security posture.

Introduction

In this report, we provide a historical perspective on the emergence of the WIAM, CIAM and B2B IAM market segments, as well as highlight key areas of overlap and points of distinction. We also look at key use cases, and then examine the core technical requirements of B2B IAM along with essential features and functionality.

Background

For much of its early history, the identity and access management (IAM) market mainly focused on what is now referred to as workforce IAM (WIAM), which, unsurprisingly, deals mainly with managing identities and access for an organization's internal employees (also known as business-to-employee, or B2E). In the early 2000s, an offshoot of traditional workforce IAM emerged that specialized in managing access to an organization's external-facing applications and sites for end-user customers, or what is called customer IAM (CIAM).

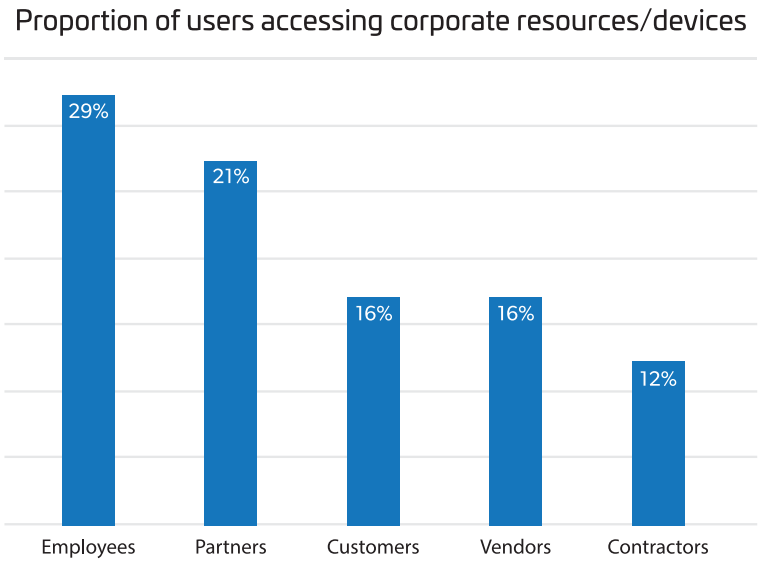
While there is some similarity between the two market segments, CIAM addresses use cases and challenges distinct from those faced by WIAM, including greater emphasis on scalability, privacy and overall user experience. However, a primary point of demarcation is that beyond security requirements, CIAM involves key touchpoints with current and potential customers that can drive customer engagement and generate new streams of revenue. Said otherwise, CIAM is as much about customer experience and digital engagement as it is about security.

For years, the identity management industry was primarily focused on one of these two subsets of the IAM market. And since each has unique requirements and use cases, the two segments largely developed separately, with limited synergies and separate buying centers — though some vendors have attempted to bridge the two markets via internal development or M&A transactions.

However, enterprises have undergone considerable transformation in recent years, and they now rely on a wide range of constituents to accomplish their goals. For example, **many firms now deal with consultants, contractors, distributors, brokers, franchisees, partners, suppliers, seasonal and gig workers and other third parties that don't fit into the traditional definitions of "employee" or "consumer."** This new "extended enterprise" has created a range of new use cases that have in turn spurred demand for new technical approaches that don't fit neatly into traditional WIAM, CIAM or even IGA models.

External identities are underestimated

To illustrate the scope of the B2B IAM challenge, **the 2024 DTR survey revealed that there are more external identities touching an enterprise's cloud, network and devices than "traditional" employees.** While internal employees are the largest single group of users accessing corporate networks (29%), non-employee external identities (customers, partners, vendors, contractors, etc.) account for almost two-thirds of the total (64 %). It's worth noting that some "customer" identities may be corporate customers and thus could be considered B2B, but even if we exclude customers, external identities represent nearly half (48%) of total users. This is equally true for enterprises in the financial services, manufacturing and infrastructure sectors.



Q. What percentage of people accessing any corporate cloud/network/device resource are (employees, contractors, vendors, customers, partners, other)?
Base: Survey of 404 respondents from select verticals including financial services, manufacturing/industrial automation, energy and utilities, telecommunications, transportation, and trucking/shipping.

S&P Global Market Intelligence 451 Research's 2024 Data Threat Report survey.

What is B2B IAM?

At this stage, there is no universally agreed-upon definition of B2B IAM. That said, we will attempt to capture the essence of what B2B IAM is about in terms of requirements, use cases and feature functionality.

At a high level, B2B IAM is about user experience and operational efficiency as much as it is about security. This focus is similar to that of CIAM, and in fact, many firms have attempted to apply CIAM approaches to B2B IAM use cases — with mixed results. Similarly, some WIAM vendors have attempted to extend their focus on internal employees to incorporate external parties such as contractors or suppliers.

Others have attempted to apply IGA features such as user provisioning and deprovisioning and access reviews to external identities. IGA can be helpful in dealing with a high volume of identities, as is required with many B2B use cases. However, IGA is typically expensive and is often built assuming it will have access to a central repository of identities, which isn't the case with most third-party B2B environments. IGA also does not typically address self-onboarding or invitation-based onboarding, nor authentication and SSO, all of which are important for B2B IAM.

Suffice it to say, **B2B IAM has much in common with WIAM, CIAM and IGA, and in a sense, it can be considered a bridge or abstraction that spans all three areas**. Generally speaking, B2B IAM can be thought of as a range of identity management capabilities that are applied to external, non-employee and non-consumer users and resources.

This section is authored by Thales

Comparing identity management solutions for B2B use cases

	WIAM	IGA	B2B IAM
Built for External Users	Employees within the organization	Designed for internal compliance and security management	Tailored for managing external partners and clients
Built for Remote On-boarding	HR-driven, automated provisioning	Detailed access provisioning based on roles and polices	Business management-driven, invitation-based onboarding with self service portals
Prevents Third-Party Risks	Focus on internal security, access control, and compliance	Comprehensive RBAC, regular compliance audits	Layered security, strict external controls
Delegated User Management	Centralized control by IT	Policy-driven, ideal for structured internal roles	Flexible, diverse external user management
Scalability	Suits internal growth but is limited in handling external users	Handles internal complexity	Effectively manages external user fluctuations
Consent & Privacy Management	Basic consent management; internal data privacy	Consent management for internal applications; robust privacy controls	Advanced consent mechanisms; external data privacy compliance

Less suitable for B2B use cases Moderately suitable for B2B use cases Highly suitable for B2B use cases

When evaluating identity and access management solutions for B2B use cases, it's crucial to understand how WIAM, IGA, and B2B IAM differ in their approach and capabilities.

Workforce Access Management is primarily designed to manage internal employee identities, focusing on streamlining access to internal applications and enforcing security protocols. While effective for internal user management, WIAM typically lacks the robust features necessary for managing external business relationships, such as partner onboarding and delegated administration.

IGA provides a more comprehensive approach to identity management, focusing on the entire identity lifecycle within an organization. It emphasizes role-based access control, detailed compliance auditing, and strong governance policies. However, IGA solutions are predominantly geared towards internal governance and compliance, making them less suited for the dynamic needs of B2B environments where external user management and cross-organizational access are critical.

B2B IAM solutions are specifically tailored for managing external identities, such as partners, customers, and suppliers. These solutions excel in handling the complexities of cross-organizational access, providing advanced consent management and privacy controls that comply with external regulations like GDPR and CCPA. B2B IAM offers extensive customization, delegated administration capabilities, and seamless integration with partner systems, making it the optimal choice for organizations looking to enhance their B2B interactions securely and efficiently.

B2B IAM use cases

Sample use cases may help to further highlight the unique needs of B2B IAM. Many B2B IAM projects address organizations that have a distributed business model such as those in retail, financial services, manufacturing or supply chain and logistics. For example, an insurance firm might have many regional offices, websites and apps, with privileged users that include a mix of direct employees, independent contractors and brokers who conduct business with end customers through access to web or SaaS applications and data.

An auto manufacturer may have a network of supply chain partners for production as well as a web of car dealers for distribution. And a supermarket chain is likely to have an extensive network of food suppliers as well as regional stores. As such, B2B IAM must provide a way to onboard and manage these various organizations and their corresponding employees and IT staffs.

This section is authored by Thales

Examples of B2B interactions.

Banking & Finance	• Data Providers • Consulting Firms / Legal Firms • Outsourcing Firms	• Brokers • Aggregators • Wholesale Banks • Regulatory Bodies	• Corporate Clients • Other Financial Institutions • Government/Municipal Entities
Manufacturing	• Raw Material Providers • Equipment Providers • Logistics and Transportation	• Distributors/Wholesalers • Resellers • Brokers or Agents	• Business End-Users • Government Entities • Other Manufacturers
Transportation & Logistics	• Fleet Maintenance Providers • Customs Brokerage Services • Intermodal Transportation	• Freight Brokers • 3rd-Party Logistics (3PLs) • Freight Forwarders	• Manufacturers • Retailers • Government and Public Entities

The diverse application of B2B IAM strategies across multiple sectors enables seamless management of various user types and organizational structures. By granting stakeholders greater autonomy, B2B IAM facilitates the adaptation to unique business models and supports growth while reducing operational friction, allowing organizations to streamline operations more effectively, responding to specific requirements and evolving environmental challenges. The following examples depict how the needs may evolve from one industry to another.

Banking & Finance:

Financial institutions are facing multiple disruptions. Traditional banks are increasingly competing with neo-banks and fintechs, forcing them to become more collaborative with their ecosystems of suppliers and partners. Meanwhile, insurance companies are dealing with continued consolidation challenges that create operational nightmares of merging different brands to build a unified face for customers, brokers, partners, and suppliers alike. B2B IAM empowers financial institutions to address these market disruptions by helping them build a more collaborative network.

Manufacturing:

Post-pandemic, the manufacturing industry is seeing a significant impact on manpower and skill retention. Managing gig-workers or contractors requires more flexible mechanisms. This problem runs across the value chain, making manufacturing firms susceptible to business continuity challenges. B2B IAM not only gives such firms an avenue to be a lot more agile in managing third-parties, but also allows them to build more secure onboarding and off-boarding mechanisms for such temporary workers, ensuring adaptability in the face of change.

Transport & Logistics:

This industry is under continuous pressure to reduce costs due to low margins. Managing third parties efficiently often means reducing lead times and overheads drastically. However, due to a very diverse ecosystem, collaborating through data sharing is inefficient and frequently accompanied by data security challenges. B2B IAM efficiently addresses many of these challenges to ensure the right stakeholders have the proper access to the right data, at the right time, and for the right reasons!

B2B IAM feature functionality

In terms of specific features, B2B IAM vendors offer an array of technical capabilities. Some features may sound similar to those found in WIAM and CIAM, such as authentication/multi-factor authentication (MFA), single sign-on (SSO), authorization, registration and onboarding, user journey orchestration and user consent management. **However, several areas stand out as particularly important for B2B IAM, including user delegation, relationship-based access control (ReBAC) and self-service access requests.**

Unique requirements of B2B IAM

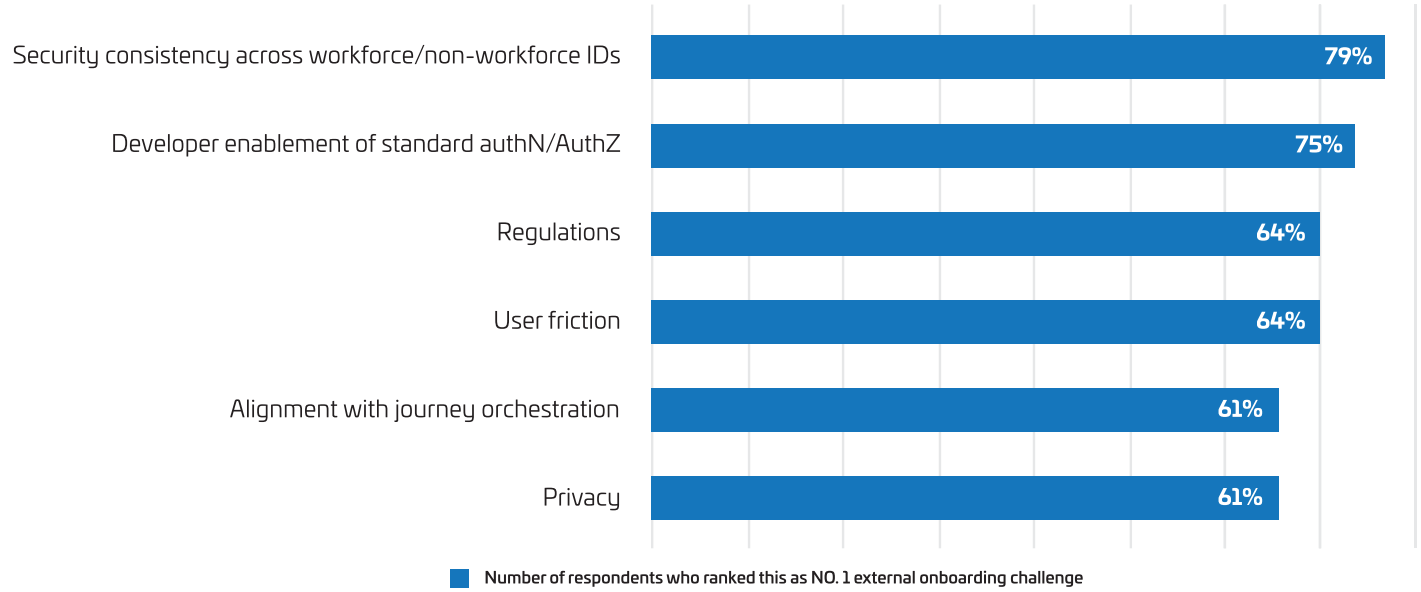
Consistency, developer enablement and user friction top onboarding challenges

What are some of the unique requirements and challenges of B2B IAM? One of the main ones is onboarding new users (and new organizations). While most workforce IAM projects can draw user identity data and attributes from an HR system or a corporate directory such as Microsoft Entra (formerly Active Directory) or Okta, most "external identities" such as contractors and consultants are not in a company directory or HR system, and they must be onboarded or registered, as with CIAM, federated or synced from another directory, or set up in a new directory or instance.

Users are often onboarded remotely, which requires a remote version of the IAM tool or synchronization with the user's direct employer. This in turn can require background checks or identity verification to guard against fraud, often as part of a fraud and risk management module. Furthermore, almost by definition, external identities tend to fluctuate more than internal employees, as consultants, contractors and seasonal employees are essentially temporary in nature (as are agreements or affiliations with the organizations they work for).

When asked about the top challenges for securely onboarding external identities, respondents most frequently cited security consistency across workforce and non-workforce identities. This speaks directly to a central theme of this report: the challenge of providing uniform benefits and controls across a highly differentiated landscape of environments, use cases and user personas. Enabling standards-based authentication and authorization that is tied into existing identity stores for developers was also ranked as a top challenge, while user friction rounded out the top three.

Challenges most commonly identified as the top difficulty in onboarding external identities



Q. Please rank your top challenges for securely onboarding/enabling external identities, with 1 being your biggest challenge.
Base: Survey of 404 respondents from select verticals including financial services, manufacturing/industrial automation, energy and utilities, telecommunications, transportation, and trucking/shipping.

S&P Global Market Intelligence 451 Research's 2024 Data Threat Report survey.

Privacy also seen as key onboarding challenge

Organizations that store identity data may also be subject to myriad regional and national privacy laws such as the EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act. As such, privacy laws are a common barrier or concern for onboarding, particularly in regions with strict privacy laws, such as Australia, Canada and Germany. **It is also worth pointing out that all of the major privacy laws such as GDPR, the California Privacy Rights Act and Canada's Personal Information Protection and Electronic Documents Act are relevant for external identities and B2B use cases.**

Vertical responses were generally in line with overall results. Respondents in financial services, critical infrastructure (logistics, shipping, trucking, etc.) and manufacturing also identified a consistent onboarding experience across workforce and non-workforce identities as a top challenge.

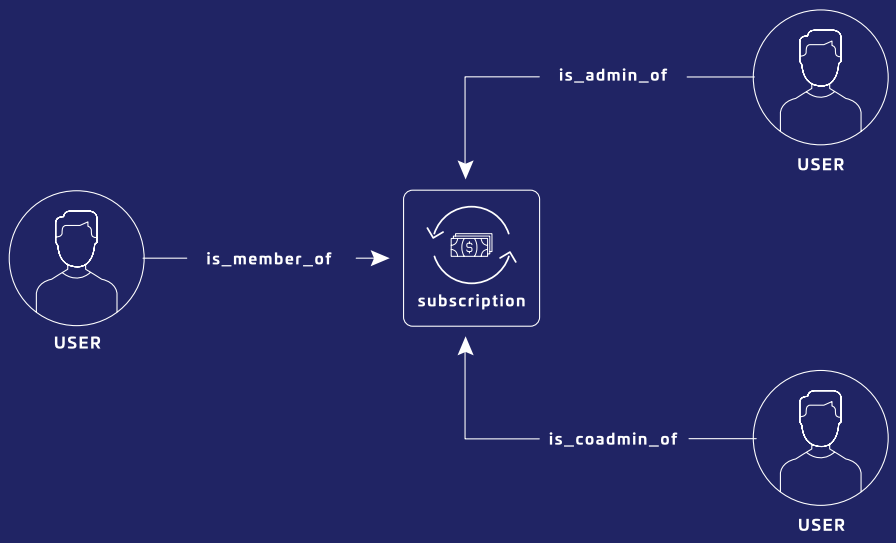
But onboarding is just one side of the coin; after users are onboarded, they must eventually be offboarded. As noted above, external users frequently have a short-term or periodic relationship with the organization, and thus may need to be offboarded or deprovisioned more frequently than internal employees. As such, "birthright" privileges are usually fine, but offboarding and de-provisioning takes on a new sense

of urgency to avoid allowing unnecessary — or "standing" — access privileges or entitlements that increase the attack surface and may be exploited.

In some ways, there is overlap between B2B IAM and traditional IGA. IGA has historically been concerned with issues such as onboarding or provisioning new users, as well as de-provisioning or offboarding non-current users. However, as noted above, IGA is not built for pure-play B2B use cases; it has a reputation for being expensive, complex and ultimately not ideal for "external" identities.

This section is authored by Thales

ReBAC allows users to manage their access to digital assets through a system where relationships determine permissions. In this model, users and assets are connected by relationships that form a network, like a graph. These connections, or relationships, can go both ways (e.g., siblings) or one way (e.g., ownership), making it easier to control access based on the nature of relationships.



B2B IAM Platforms, with the likes of the OneWelcome Identity Platform, support creating and maintaining these networks centrally by the organization's back office or self-managed by the users, ensuring a scalable system for managing relationships and access to protected resources.

Relationship-based authorization is critical for B2B IAM

In B2B environments, IAM systems must handle complex relationships and permissions involving multiple organizations and user roles — for many large financial firms, for example, third-party partners or relationships can easily number in the tens of thousands. Organizations might also need to manage access for entire teams or departments from a partner organization.

Relationship-based authorization, or relationship-based access control, is an access control method that assigns access permissions based on relationships between "entities" or "objects" — users, applications, groups, organizations, contracts, etc. In a sense, a relationship can be considered a type of attribute, and thus ReBAC can be thought of as a form of attribute-based access control. ReBAC can allow for complex, fine-grained entitlements based on relationships — for example, Jane is Joe's boss and, therefore, should have access to his folders — as well as complex, graph-style relationships.

ReBAC is prevalent in industries such as manufacturing, where authorizations are based on complex B2B relationships and contexts that typically don't exist in B2C use cases, and ReBAC use cases are "streamlined" than B2E use cases, where employees fall under specific functions or departments. Additionally, such relationships contain context that is not necessarily identity-related but may be relevant for authorization decisions, such as the expiration date of a contract. This is partly what makes B2B IAM unique and a special challenge: It can't be easily addressed with a conventional WIAM, CIAM or IGA solution. B2B scenarios can also include business-to-business-to-customer (B2B2C) and business-to-business-to-anything (B2B2X) relationships, which are likewise difficult to anticipate and complex to implement, and thus well suited to ReBAC.

User delegation improves security and lowers costs

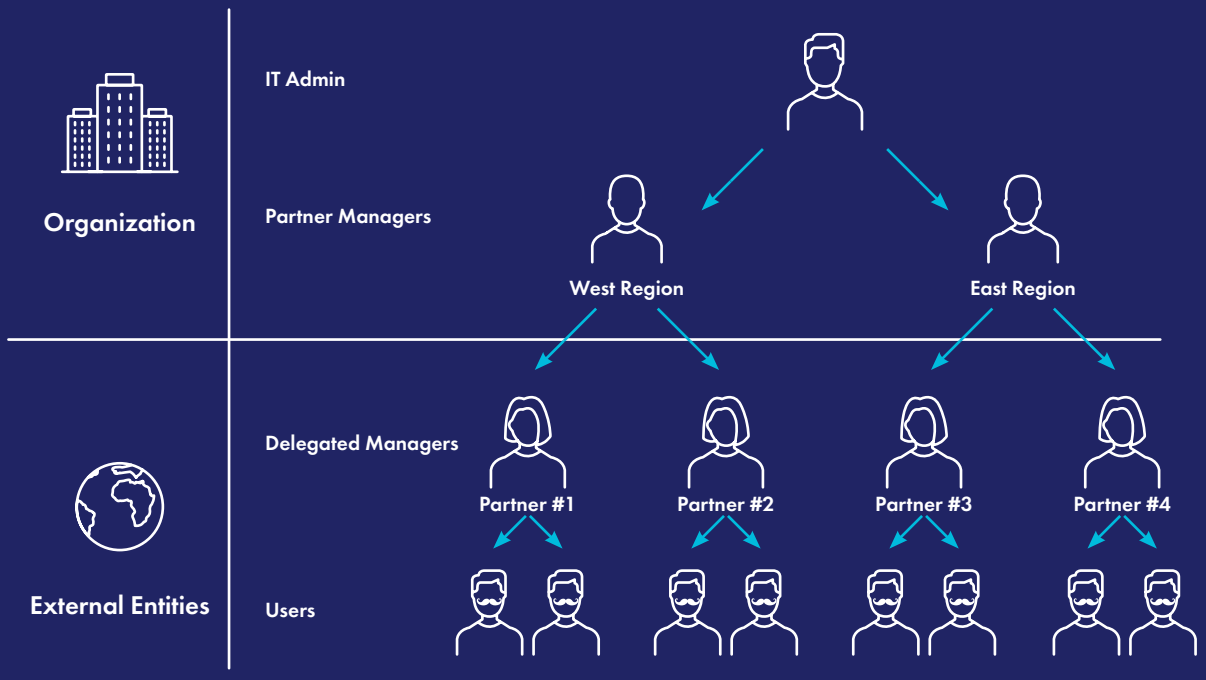
One way to reduce the management overhead associated with external users and their existing IAM systems is user delegation, which is another key component of a comprehensive B2B IAM offering. In many scenarios, the "customer" is an organization that needs to address the needs of both its internal staff that administer the IAM offering and those of its end customers. As such, it is important for enterprise customers — the first "B" in the B2B2C equation — to be able to delegate certain identity management functions. For example, if a manufacturing firm grants access to a supplier or partner and that partner can administer its own users, then the burden is lifted from the manufacturer's own IT staff, helping to reduce overall operating costs in the process.

Delegation can also lead to greater security by enabling timelier offboarding — those who leave can be offboarded quickly rather than waiting for a quarterly or semiannual access review, which is inefficient and can leave an organization exposed to threats for longer than necessary. In this way, delegated user management can help reduce overall third-party risks and increase trust between organizations, as well as help enhance overall productivity.

This section is authored by Thales

Delegated user management

Delegated user management is a capability within IAM solutions like OneWelcome Identity Platform, which distributes the responsibility of managing user access and permissions across different levels of business managers within the organization and with external entities. The illustration below depicts how managing third-party users becomes a lot more efficient, scalable and secure, while enhancing overall user experience. With delegated user management, organizations can afford to free up the IT resources and give more ownership to business users (like partner managers or supplier managers) who have a much better sense of those relationships.



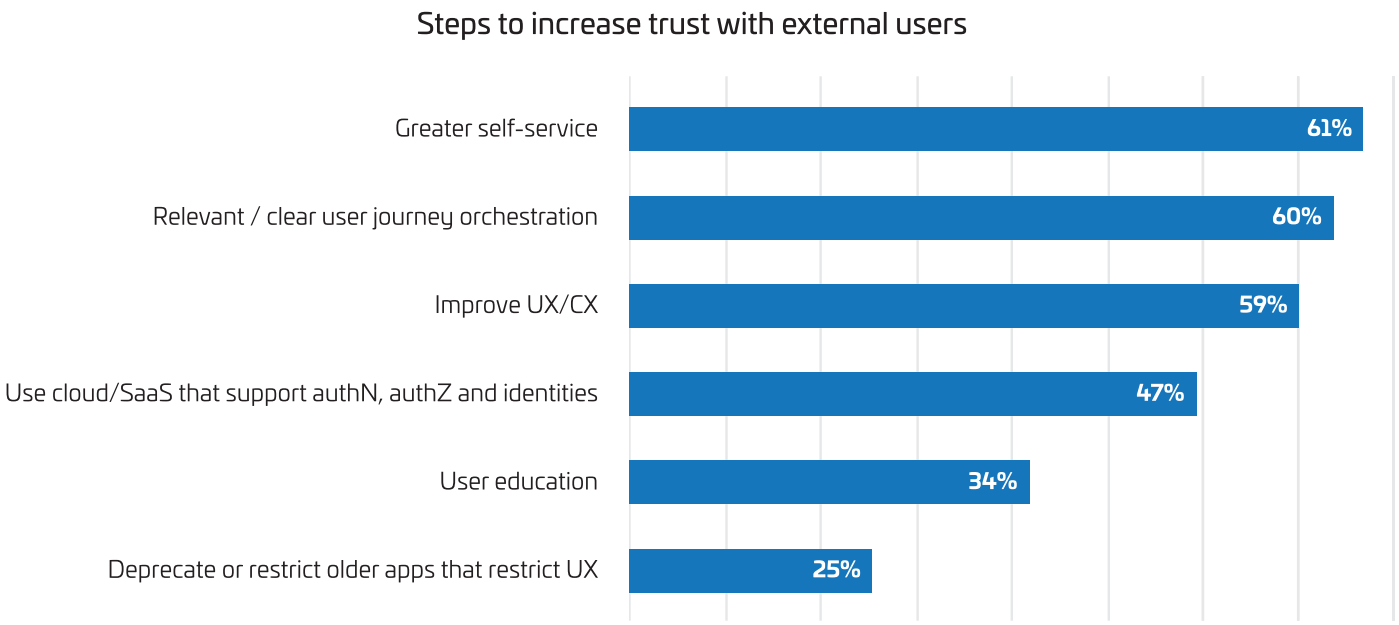
Benefits:

- **Efficiency:** By delegating user management tasks to business managers, organizations can reduce bottlenecks and improve response times.
- **Scalability:** allows the organization to scale its user management processes without overwhelming a single administrator.
- **Security:** ensures access is managed closer to the request's source, reducing the risk of inappropriate access.
- **User Experience:** enhances overall user satisfaction by simplifying access management and meeting diverse user needs efficiently.

Self-service can lead to greater trust and a more positive user experience

A related concept is the notion of user self-service. Self-service allows organizations to lower costs by offloading certain IT burdens that may have already been reduced by user delegation, making user delegation and self-service options complementary.

Self-service options can also enhance the user experience — two related elements that surveyed organizations cited as priorities. **When asked how they would enable a more trusted relationship with external users, respondents' top answers were increasing self-service (61%), orchestrating a relevant and clear user journey (60%) and improving user or customer experience (59%).**



Q. What steps will you take to enable a more trusted relationship with your external users?
Base: Survey of 404 respondents from select verticals including financial services, manufacturing/industrial automation, energy and utilities, telecommunications, transportation, and trucking/shipping.

S&P Global Market Intelligence 451 Research's 2024 Data Threat Report survey.

B2B IAM is a subset of third-party risk

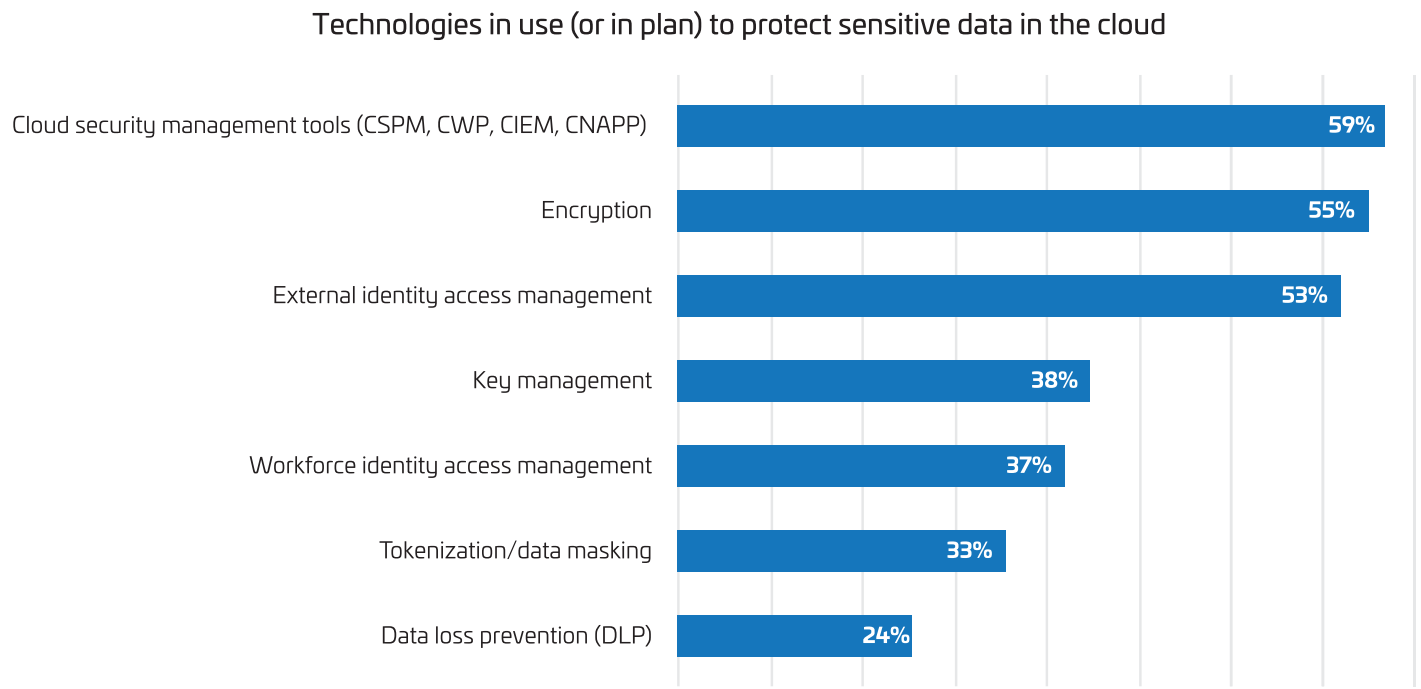
B2B IAM can also be thought of as a subset of third-party supply chain risk management, and it can help minimize the impact of that risk. As highlighted many times in media coverage of high-profile attacks, third-party supply chain risks have become a board-level topic that C-suite executives need to be aware of. More than half of survey respondents (55%) identified vulnerabilities from third parties, including external code, as a top vector of attack on cloud management infrastructure. B2B IAM can help establish a zero-trust architecture for the extended enterprise that includes third parties. Considering how nearly every form of security now has an identity component, it makes sense that third-party risk management would begin with an identity-first approach. In that way, B2B IAM can become a pillar for managing third-party risks via a zero-trust posture for the extended enterprise.

Collaboration is key for modern enterprises

As modern organizations have embraced the extended enterprise concept, they have likewise taken a positive and proactive stance toward collaboration. Many of the personas with whom firms would like to collaborate already have their own identities and attributes stored with their own identity providers (IDPs) and with their own authentication mechanisms. B2B IAM can further reduce the burden on internal IT staff by allowing collaboration partners to "bring their own" IDPs and login systems, which can be managed by delegated users or sub-delegates.

External identities are more critical in the cloud

External identities are considered an even more important element of security control in cloud environments. While digital transformation has ushered in the extended enterprise and the expansion of external identities, a parallel development has been the ongoing shift to the cloud and cloud-based resources. This, in turn, has placed greater emphasis on identities as a security control in a world where users and IT resources are highly distributed and mobile, and physical location is less relevant. As such, **53% of respondents to our survey selected external identity access management as part of their plan to protect sensitive data in the cloud, slightly behind purpose-built cloud security tools such as CIEM, CWP or CNAPP (59%), and encryption (55%).**

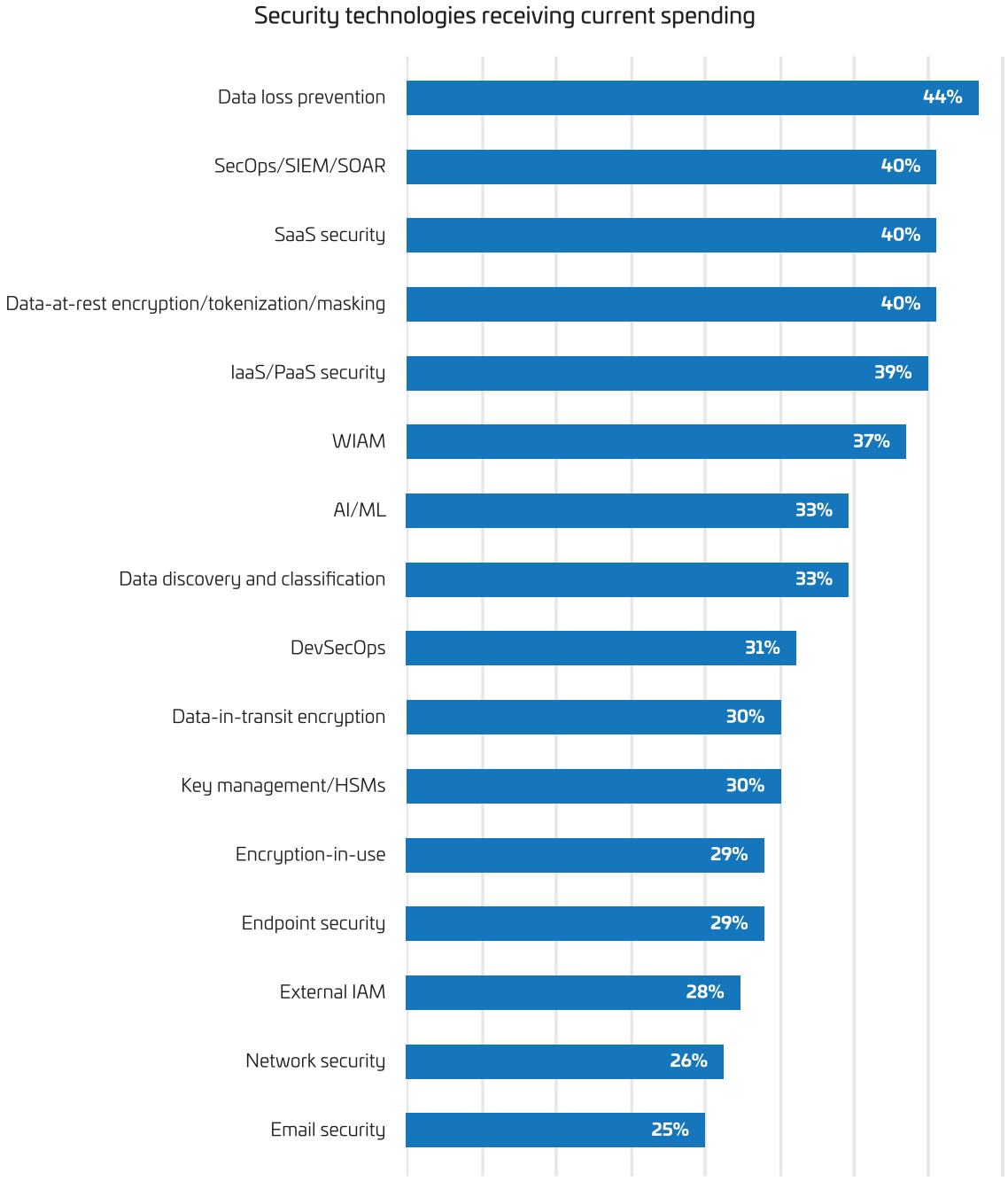


Q. Which security technologies is your organization using or plan to use to protect sensitive data in the cloud?
Base: Survey of 599 respondents from select verticals including financial services, manufacturing/industrial automation, energy and utilities, telecommunications, transportation, and trucking/shipping.

S&P Global Market Intelligence 451 Research's 2024 Data Threat Report survey.

Securing external identities not yet a top budget priority

When asked what security tools they are spending on today, respondents ranked external identity access management below the middle of the range. This is somewhat surprising given the importance of supply chain security and the magnitude of external identities most firms are struggling with. In our view, it suggests a disconnect in corporate security budgeting decisions, given that nearly half of total identities are external identities, which could translate to a gap in an organization's overall security posture. It also suggests that the market for securing external identities is nascent, less established than more mature sectors such as cloud security and data loss prevention (DLP).



Q. Which of the following security technologies are you spending on today?
Base: Survey of 599 respondents from select verticals including financial services, manufacturing/industrial automation, energy and utilities, telecommunications, transportation, and trucking/shipping.

S&P Global Market Intelligence 451 Research's 2024 Data Threat Report survey.

Firms also need to consider that external identities may pose security risks to the organization that are difficult to address via common security tools and approaches. For example, enterprises may find it difficult, if not impossible, to install agents for mobile device management, DLP or endpoint security on external users' laptops or phones, particularly if they are not direct employees. Locking down the way external IDs authenticate and are authorized may provide an alternate recourse in such scenarios.

Conclusions

B2B IAM enhances an organization's agility by allowing it to quickly and securely integrate with new partners and technologies, speeding up time-to-market for new initiatives and responses to market shifts. This helps organizations to build and sustain competitive advantage by strengthening relationships with partners and customers. Key points to consider when evaluating B2B strategies:

- External identities represent a much larger superset of users than is typically dealt with in WIAM scenarios, yet these identities represent a largely underserved part of the overall IAM market.
- B2B IAM is collaborative by definition because it requires cooperation and sharing of information between organizations.
- The B2B market focuses on fostering long-term relationships with fewer customers with higher individual value, requiring robust security and seamless integrations. And with supply chain attacks becoming increasingly common, B2B IAM can serve as a pillar for managing third-party risks and establishing a zero-trust foundation for the extended enterprise.
- Despite some similarities, B2B IAM should be thought of as addressing a separate set of problems than WIAM, CIAM and IGA, which in turn requires a dedicated set of answers. While some firms may be tempted to try to shoehorn or "tweak" existing WIAM, CIAM or IGA offerings to fit B2B use cases, a purpose-built offering may not only yield improved security from identity-centric risks, but also an enhanced user experience and reduced pressure on scarce IT resources and budgets.

About this study

This research was based on a subset of the global survey of 2,961 respondents fielded via web survey with targeted populations for each country, aimed at professionals in security and IT management. This subset comprises 599 respondents in financial services, manufacturing/industrial automation, energy and utilities, telecommunications, transportation, and trucking/shipping. In addition to criteria about level of knowledge on the general topic of the survey, the screening criteria for the survey excluded those respondents who indicated affiliation with organizations with annual revenue of less than US$100 million and with US$100 million-$250 million in selected countries. This report also draws on contextual knowledge of additional research conducted by **S&P Global Market Intelligence 451 Research**. This research was conducted as an observational study and makes no causal claims.

THALES

Building a future we can all trust

Contact us

For all office locations and contact information,
please visit cpl.thalesgroup.com/contact-us

cpl.thalesgroup.com