SailPoint

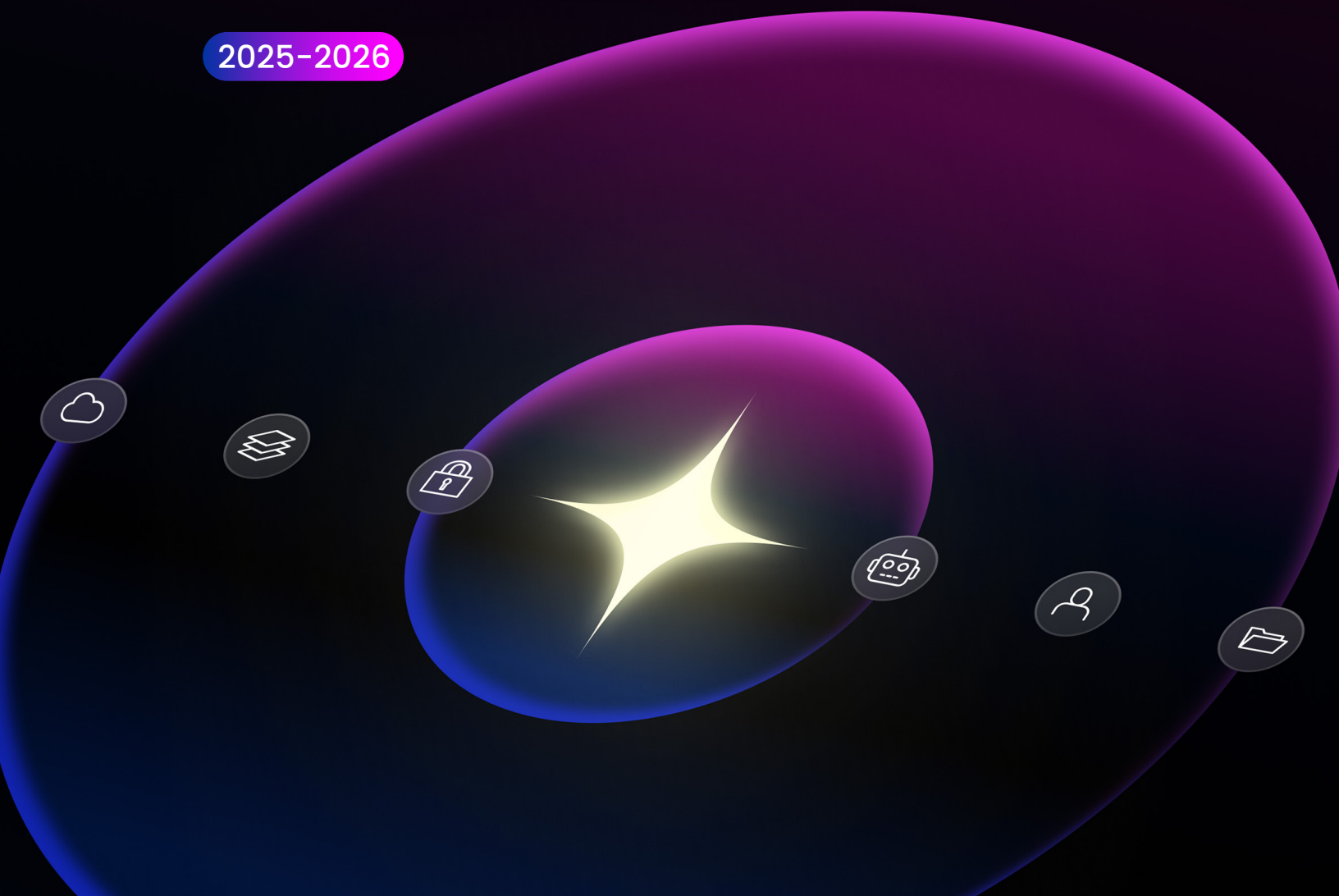
Report

The Horizons of Identity Security

Adapt or risk falling behind:

How to keep up as identity shifts from foundational control to security frontier

2025-2026



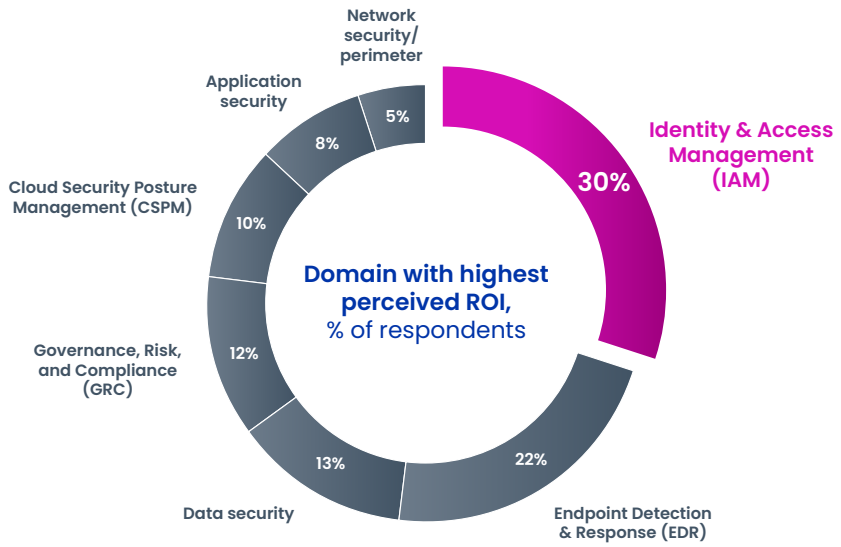
Executive summary

Identity has become the enterprise's nerve center, coordinating access, powering automation, and enabling real-time decisions and threat management across systems and users—both human and non-human. In 2025, identity sits at the center of digital transformation, enabling secure growth, operational agility, and intelligent automation. At the same time, the identity paradigm is rapidly shifting, from single point of control to method of detection, prevention mechanism to response enabler, and static policy enforcement to dynamic privilege adjustment. In this way, the role of identity has fundamentally changed, from foundational control to the new frontier of security.

As identity security and the attack landscape evolve rapidly, especially with the proliferation of machine and AI agent identities, organizations need to adopt new and emerging identity capabilities just to keep up. However, our research reveals a widening gap between mature organizations that use automation and AI-enabled identity solutions to unlock measurable business value, and the majority, who have less mature and cumbersome access processes, held back by slow deployment, poor data integration, and limited automation. Organizations also face growing challenges in identifying and governing the full spectrum of identity types, from traditional human users to increasingly complex machine identities and AI agents, which often operate with limited visibility and fragmented ownership. This is all made more difficult by the need to scale management of identities across multiple cloud environments.

Despite challenges faced, organizations report that identity provides the greatest return on investment when compared to all other security domains. Twice as many organizations ranked Identity and Access Management (IAM) as their highest-ROI domain compared to the average (Exhibit 1). This is because effective identity management does more than reduce risk. It drives efficiency, accelerates transformation, and enables smarter decisions across the enterprise.

Exhibit 1:
Investments in IAM provide the highest perceived ROI when compared to all other security domains



Source: SailPoint Customer Survey on IAM (n=229): Question 6.06A "Investment in which security domain provides the highest perceived ROI in your organization?"

Over the last four years, SailPoint has surveyed IAM decision-makers across the globe to assess their capabilities across identity security horizons and define the future of identity. The 375 decision-makers we surveyed in June 2025 included senior leaders in information technology, cybersecurity, and risk. More than half work for organizations with over 10,000 employees, and the majority represent the finance, technology, and healthcare sectors. (For details on survey demographics, see the appendix.)

Using their responses, we grouped their organizations into five horizons based on strategy, talent, operating model, and technology capabilities:

- At Horizon 1, the lowest maturity, organizations lack the strategy and technology to enable digital identities
- At Horizon 2, they have adopted some identity technology but still rely heavily on manual processes
- At Horizon 3, they have adopted identity capabilities at scale
- At Horizon 4, they have automated capabilities at scale and use AI to enhance digital identities
- At Horizon 5, the closest to the future of identity, boundaries are blurred between enterprise identity controls and the external identity ecosystem, and identity supports the business in next-gen technology innovations

The most significant shift this year has been the introduction of new capability requirements for Horizons 4 and 5, specifically cloud infrastructure entitlement management to secure increasingly distributed multi-cloud environments and new capabilities to govern AI agents, reflecting the accelerating adoption of AI within organizations.

What we found

This year's research highlights four critical themes from our 2025 survey of global identity leaders. Together, they reflect where organizations stand today, where progress is being made, and what continues to hold many teams back.

1. Organizations are falling behind as the attack landscape intensifies, AI agents proliferate, and the bar for mature identity security rises

For every three organizations that moved forward, two moved backward, despite rising levels of identity security investment overall.

- **63 percent of organizations remain in Horizons 1 or 2, suggesting a significant opportunity to unlock the "full potential" of identity security.** These programs are typically tactical, manually driven, and limited in their ability to support automation, AI governance, or cross-environment controls. However, many of these organizations are now focused on building foundational capabilities that will enable future scale.
- **Advancement to Horizons 3 and 4+ was driven by an increased appetite to automate to reduce costs and new capability building.** In particular, Horizon 4 organizations this year had higher adoption across ID verification, machine identity management, and AI agent IAM.
- **Four percent of organizations regressed in 2025.** This was not due to declining effort, but rather a result of rising capability thresholds to meet Horizons 4 and 5 as the attack landscape intensifies. Organizations that regressed had significantly lower adoption of AI agent IAM capabilities.

2. Organizations that adopt advanced AI and identity data capabilities see significantly higher cost savings, productivity, and risk reduction

Outperforming organizations are adopting emerging AI and data capabilities at the intersection of identity, data, and security to keep up with the evolving attack landscape.

- **Use of emerging identity data capabilities is a key enabler of downstream business use cases.** Horizon 3+ organizations are four to eight times more likely to have real-time identity data synchronization, entity resolution, and automated lifecycle workflows compared to earlier-stage peers.

- **AI is being deployed to manage identity at scale, as mature organizations use identity not just as a control but also as a detection mechanism.** Adoption of AI-enabled detection capabilities, such as Identity Threat Detection and Response (ITDR) and privileged account monitoring, is 4 times as high among mature organizations than those in Horizons 1-2.
- **Identity cloud data governance is maturing, although adoption of cloud data access controls is higher than for harder to achieve context-aware access models.** Mature organizations are 4.5 times more likely to have cloud data governance capabilities such as unified policy enforcement and real-time data access monitoring. However, adoption of context-aware access capabilities such as attribute-based access control (ABAC) and ephemeral access models — temporary, time-bound permissions granted only when needed — trails behind, highlighting the opportunity to mature towards dynamic and just-in-time access.

3. Deployment is a critical unlock in moving across horizons, and many get it wrong

Despite rising levels of investment, many identity programs still struggle with inconsistent deployment execution; however, mature organizations follow customer success best practices to advance across horizons.

- **Deployment holds some organizations back from being able to fully onboard emerging capabilities, but implementing horizon-specific best practices enables advancement.** Many organizations report IAM deployments that ran over budget, were delayed, or did not meaningfully improve user experience. However, organizations employing horizon-specific best practices outperformed across all critical business outcomes.
- **Effective management of application onboarding complexity is a universal customer success challenge for organizations across horizons.** Application onboarding is especially challenging for H4+ organizations, who have distributed and complex environments with 3.6 times as many applications in their estate when compared to H1-H3 organizations. However, use of risk-based sequencing and reusable templates leads to better outcomes for organizations across horizons.
- **Identity data hygiene is a critical enabler of deployment success.** While 44 percent of Horizon 4+ organizations still report gaps in identity data quality or normalization, organizations that prioritized and performed data cleanup before migration were 1.6 times more likely to be completely successful in their IAM tool deployment.

4. Organizations need to quantify the full value of identity to secure funding for advanced capabilities, including margin, compliance, and risk impact

Although identity enables the business through cost savings and productivity improvements, many organizations still struggle to quantify and communicate this impact, focusing only on compliance enablement and risk reduction.

- **Only 25 percent of organizations position IAM as a strategic business enabler.** 57 percent of organizations still describe IAM as either a "security control" or "compliance requirement," limiting the role it plays in transformation initiatives.
- **Organizations that quantify revenue and cost impact of identity investments are better positioned to seek increased funding.** Organizations have traditionally quantified returns from identity security in terms of risk reduction and compliance enablement. However, those that quantify margin impact from identity security investment as well create more compelling business cases for increased funding.
- **Integrated identity data unlocks downstream automation and new business use cases.** When embedded into platforms like Human Resources (HR), Customer Relationship Management (CRM), or IT Service Management (ITSM), identity data powers AI assistant personalization, smarter provisioning, and more efficient business workflows across departments.
- **Use of advanced identity security capabilities reduces risk through improved incident response.** Identity-enabled threat detection and response, next-generation PAM, unified control planes, and AI agent governance lead to faster and more effective detection, containment, and remediation of incidents.

Why it matters

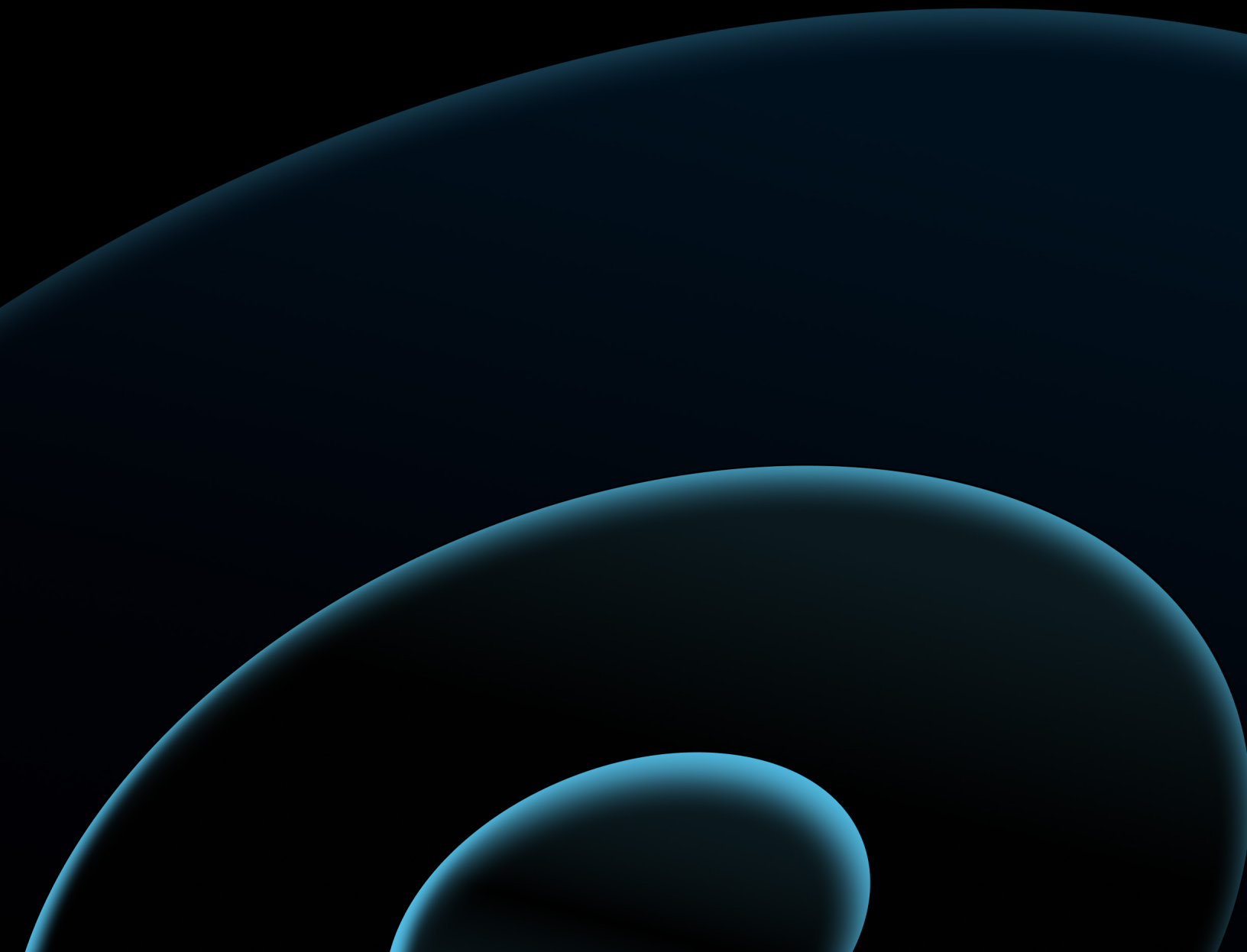
Identity is now central to how organizations operate. It connects people, systems, and data while enabling secure, automated decisions at scale, and plays a growing role in detecting and containing threats. But while its importance is widely recognized, many organizations are not keeping pace.

Too often, identity security investments fall short of their potential. Programs sometimes stall during deployment. IAM platforms are fragmented across teams or deprioritized entirely due to complexity, limited expertise, or unclear ownership. As a result, impact remains siloed in IT.

However, this gap can be closed. Our research explores how organizations are making identity work in practice — deploying solutions more effectively, building the right foundations, and turning investment into measurable business impact.

Chapter 1:

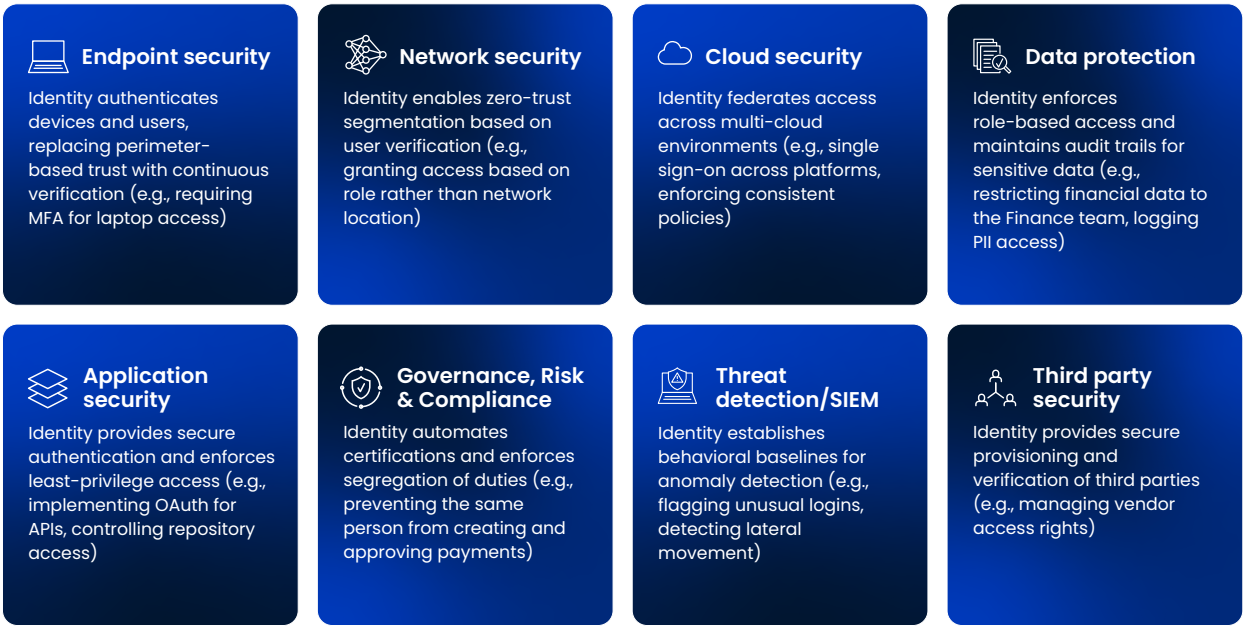
The future of identity is tightly linked with data and security



As organizations mature across identity security horizons, the landscape they must navigate is evolving faster than ever. In 2025, advances in AI, data management, and threat detection are reshaping identity security. As identity shifts from a foundational control to the new frontier of security, it has emerged as the central control point in outperforming organizations - where critical decisions are made, policies are enforced, and security operations converge. Identity now serves as the connective tissue across the security ecosystem, touching every domain from endpoint protection to cloud security (Exhibit 2). This strategic positioning powers expanded governance across all human and non-human identities, dynamic privileged access, unified and accurate visibility across environments, and automated threat response capabilities not possible without identity telemetry. These elements are shaping the future of integrated identity security, bringing together identity, data, and security. As integrated programs become essential to harness identity as a dynamic method for detection and response, identity, CISO, data, and AI organizations will have to come together to chart a singular path forward.

Exhibit 2:

As a central control point in the security tech stack, identity enables and enhances capabilities across multiple domains



Four trends are now shaping how identity capabilities are evolving and expanding across the security ecosystem:

- **Identity-centric governance is expanding across all identity types:** Organizations are applying governance to a broader set of identities, including service accounts, bots, and AI agents. This includes discovering and cataloging machine identities, managing AI agent lifecycles, and enforcing time-bound access policies for ephemeral accounts.
- **Privileged access is becoming dynamic and data-driven:** Privileged access is no longer fixed, risking permanently elevated access. Access adjusts in real time based on behavioral signals, contextual risk, and sensitivity of the data or systems accessed. Organizations are beginning to shift the conversation from zero trust to continuous adaptive trust.

- **Identity fabric is delivering unified control across complex environments:** To reduce fragmentation, organizations are building identity control planes— centralized frameworks that connect identity data and policies across environments. The identity fabric delivers consistent policy enforcement, unified data models, and master identity records to enable seamless identity governance at scale.
- **Identity signals are powering intelligent threat response:** Identity has become a source of detection. Signals such as login patterns and credential misuse are being integrated into Security Incident and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) platforms to drive threat detection, forensic investigation, and automated remediation workflows.

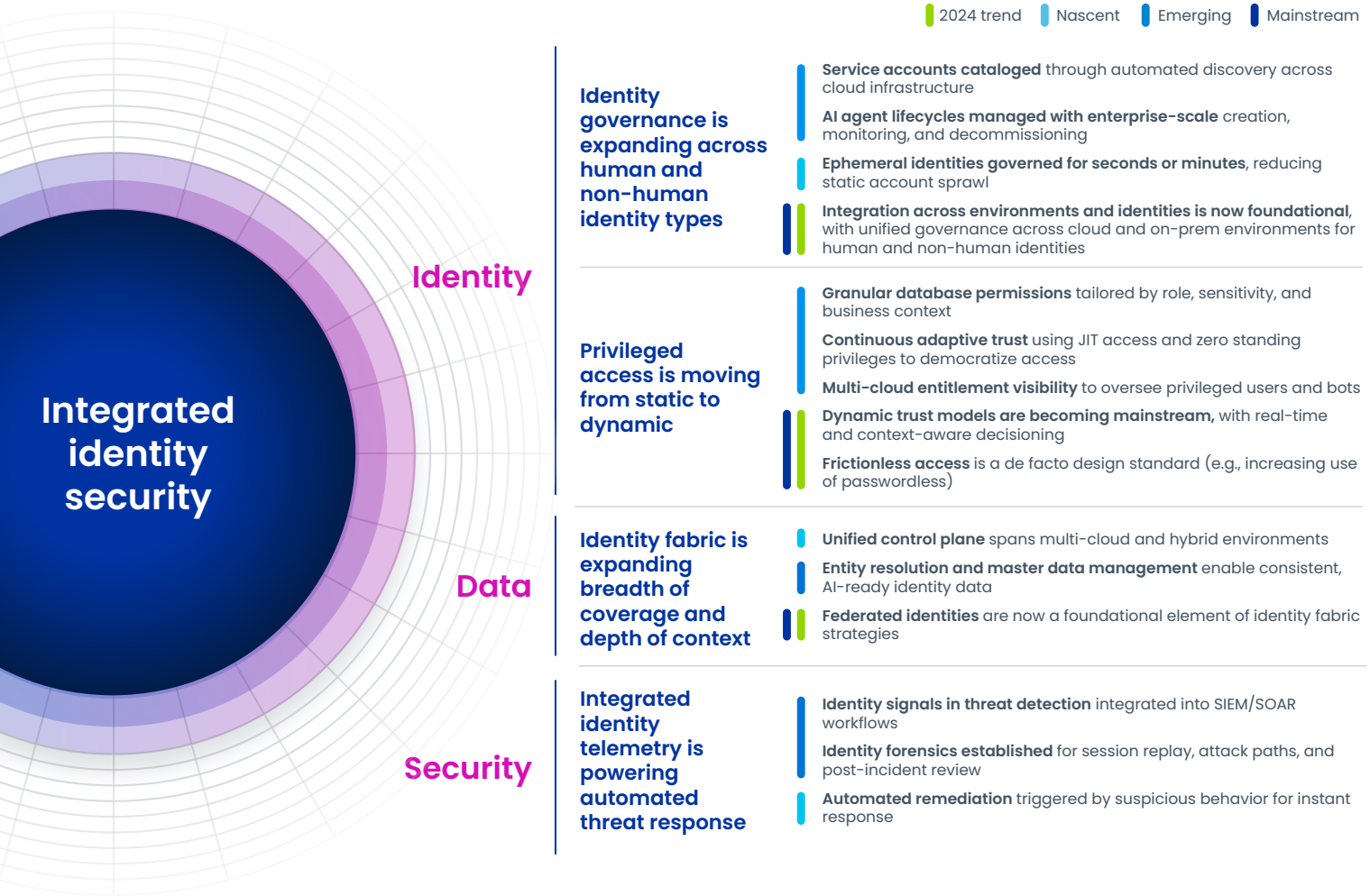
Together, these forces offer a blueprint for the future of identity security (Exhibit 3). By anchoring security decisions in adaptive, data-driven controls, they enable identity to serve as both a risk mitigator and a business enabler. As these capabilities mature, they will continue to reduce risk, accelerate transformation, and create long-term value for the business.

While new forces are also shaping the cutting edge of identity security, capability themes referenced in last year's report have continued to mature. Organizations are not just sustaining momentum, they are scaling these capability themes, applying them more broadly, and embedding them deeper into their environments (Exhibit 3).

- **Integrated identity programs** have progressed from basic visibility to unified control. Organizations are now building identity control planes that enforce consistent policies, manage entitlements, and align governance across cloud, SaaS, and on-premises platforms.
- **Dynamic trust models** are evolving towards continuous adaptive access. Rather than point-in-time decisions, access levels will respond in real time to changes in user behavior, session context, and risk indicators.
- **Federated identities** are expanding into broader identity fabrics. What began as cross-platform Single Sign-On (SSO) is now evolving into decentralized identity control, with growing use of data-sharing standards and federated governance frameworks.
- **Frictionless access** is becoming both more seamless and more secure. Passwordless authentication using passkeys, biometrics, and certificates is now common, while automation is extending to privileged access, ephemeral credentials, and AI assistant onboarding.

Exhibit 3:

Integrated identity will power dynamic access across users, unified visibility, and automated response



Still emerging: Decentralized identity, digital wallets, and partner federation remain important long-term concepts, but are not considered part of the near-term roadmap for most organizations.

Leading organizations, cybersecurity standards bodies, and governments are already embracing core elements shaping the future of identity (Exhibit 4).

Exhibit 4:

Proof points in last 12-18 months support progress across the elements shaping the future of identity

Identity	Data	Security
Identity-centric governance will expand across all identity types	**Privileged access is moving from static to dynamic**	**Identity fabric is expanding breadth of coverage and depth of context**	**Integrated identity telemetry is powering unified and automated threat response**
OWASP formally recognized poor non-human identity (NHI) governance as a top cyber risk for 2025. This includes unmanaged API keys, hardcoded credentials, lack of expiration policies, and excessive privileges[1]	**NIST SP 800-63-4 introduces "continuous evaluation metrics" for digital identity,** formalizing expectations for adaptive authentication and risk-based access[4]	**Cloud Security Alliance (2024) found 40% of organizations with two or more identity providers lack unified identity visibility** — a gap identity fabrics are designed to address[7]	**CrowdStrike's 2025 Global Threat Report shows identity misconfigurations and excessive permissions were primary attack vectors** in 35% of cloud incidents, enabling lateral movement to sensitive data[10]
Cloud Security Alliance found only 15% of orgs feel confident in their NHI governance; most lack automated rotation, expiry, or privilege right-sizing for machine identities[2]	**CISA's Zero Trust guidance (Aug 2024)** emphasized that all authentication and authorization activities must be dynamic and strictly enforced before granting access[5]	**OpenID IPSIE (Oct 2024) aims to standardize enterprise identity control planes** via profiles for SSO, provisioning, entitlements, and risk signal sharing across platforms[8]	**CISA's May 2025 SOAR Guide recommends integrating identity events and automating credential resets** based on behavior patterns for faster incident containment[11]
TechTarget reported at Identiverse 2025 that AI agents have emerged as a core identity risk, urging organizations to include them in standard lifecycle governance frameworks[3]	**Cloud Security Alliance (2025) stated that Zero Trust is evolving into adaptive trust;** shifting from binary trust decisions to more nuanced, risk-based approaches that adapt to changing conditions[6]	**At the European Identity and Cloud Conference (2025)** KuppingerCole deemed the identity fabric as foundational for digital identities in the age of AI, quantum, and decentralization[9]	**MITRE launches AI Incident Sharing Initiative** to enable data driven risk intelligence and analysis and improve collective AI defenses[12]

[1] https://owasp.org/www-project-non-human-identities-top-10/2025

[2] https://cloudsecurityalliance.org/press-releases/2024/09/12/csa-and-astrix-security-reveal-critical-gaps-in-nhi-protection

[3] https://www.techtarget.com/searchsecurity/opinion/Top-identity-security-themes-at-Identiverse-2025

[4] https://pages.nist.gov/800-63-4/sp800-63.html

[5] https://www.cisa.gov/resources-tools/resources/connected-communities-guidance-zero-trust-protect-interconnected-systems

[6] https://cloudsecurityalliance.org/blog/2025/04/17/zero-trust-is-not-enough-evolving-cloud-security-in-2025

[7] https://cloudsecurityalliance.org/press-releases/2024/10/30/csa-finds-technical-debt-as-top-hurdle-to-identity-system-modernization

[8] https://openid.net/wg/ipsie/

[9] https://www.kuppingercole.com/watch/identity_fabric_2040-eic25

[10] https://www.crowdstrike.com/global-threat-report/

[11] https://www.cisa.gov/resources-tools/resources/guidance-siem-and-soar-implementation

[12] https://www.mitre.org/news-insights/news-release/mitre-launches-ai-incident-sharing-initiative

Chapter 2:

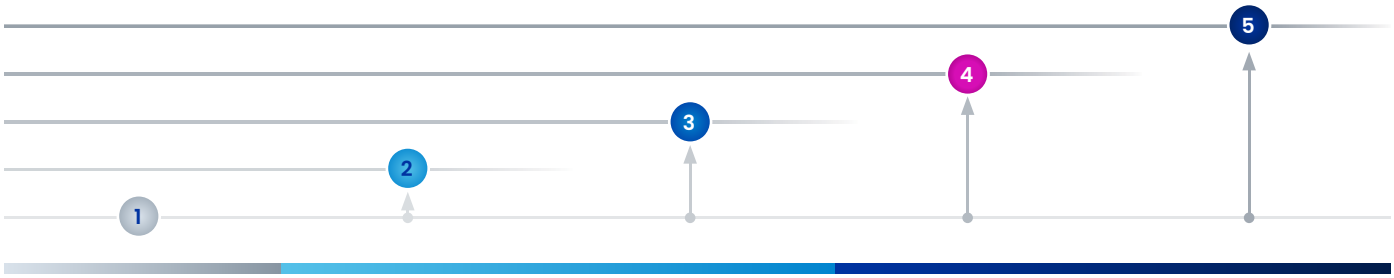
Where organizations are in their journeys

The SailPoint Horizons maturity framework

SailPoint categorizes identity security programs into five horizons based on an organization's maturity across four enablement areas: Strategy, technology & tools, operating model, and talent (Exhibit 5). Since 2024, we have updated Horizons 4 and 5 with new capability thresholds, including for AI agent lifecycle governance and cloud-native identity data protection.

Exhibit 5:

Over 4 years of annual surveys, we clustered key criteria into 5 maturity horizons guided by survey results



Fragmented identity experience across organization

Identity is not a focus – lack of organization wide identity strategy

Identity capabilities are highly immature – may have some legacy IT tools to support user access management but missing any identity technologies

Missing any operating model to organize teams and manage all forms of identities across the organization

Started on identity management but mostly manual

Identity program gets some attention but low adoption and mostly tactical response to some external stress e.g. compliance, security breach, or business transformation

Started purchasing some identity tools but low adoption

Capabilities are highly manual and basic

Centralized IAM function, but primarily focused on fulfillment of service tickets

Identity team mainly composed of helpdesk, with dedicated IT team maintaining tools

Digitalized at-scale identity management

Identity program gets digitalized, scaled, and gains wider adoption across the organization

Identity strategy is paired with metrics to measure business value impact

Identity capabilities gain wider organizational adoption with some level of automation and identity extending to cloud and data governance

Centralized operating model organized around capabilities tied to specific tools (e.g. access management, IGA, etc.)

Tool centric identity team driving implementation and maintenance (e.g. SP engineers)

Advanced digital tools and predictive use cases

Identity program becomes a strategic enabler for business transformation, innovation, security resilience

Privileged access decisions are made dynamically, with the use of just-in-time access and zero standing privileges, including for service accounts and AI agents

Threat detection is powered by identity signals integrated into SIEM/SOAR

Capabilities span across most identities (workforce, business network, AI agents) **and environments** (data, cloud, API)

Product-driven operating model (e.g. centered around capabilities but tool agnostic), agile teams with clear product ownership

Extended and unified identity

IAM strategy is a pillar of broader innovation strategy for the organization

Continuous adaptive trust is the standard, where ephemeral identities are governed for seconds or minutes

Identity data powers automated response and remediation and is made AI-ready with entity resolution

Operating model enables collaboration with ecosystems of other companies, developer communities, and institutions

INSUFFICIENT	FOUNDATIONAL	ADVANCED

To be in one horizon, customer capabilities need to cover most environments and identities

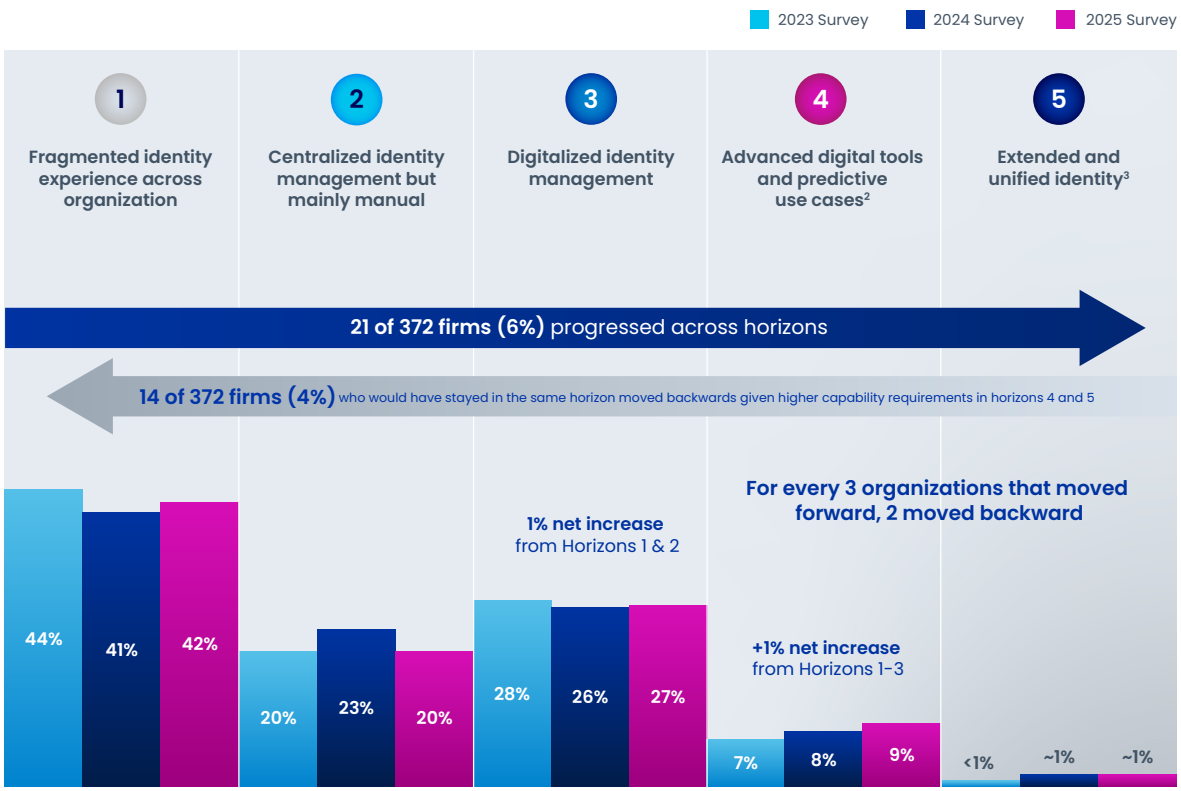
Based on interviews and a new survey of 375 IAM decision makers across North America, Europe, Asia, and Latin America, we explored where organizations stand in their identity security journeys and how they have progressed since last year. These perspectives illustrate where organizations have excelled, the barriers they face, and how they can move to the next maturity horizon.

Where organizations are today

While most organizations remain early in their identity journeys, a growing number are leaning into modernization – not just to catch up, but to build the foundations for what is next (Exhibit 6). Many teams are investing in automation to reduce costs and improve efficiency, helping them progress out of foundational maturity levels. At the same time, organizations are investing in AI agent governance, machine identity management, and dynamic access controls to move to more mature horizons. These shifts are accelerating forward momentum for some organizations, while exposing capability gaps that are causing others to fall behind.

Exhibit 6:
Some organizations are leapfrogging across horizons while others moved backwards

Distribution of organizations across the 5 customer identity journey horizons



The 2025 framework added seven new capability requirements to Horizons 4 and 5 since 2024 making advancement to these mature levels more challenging

Note: Horizon 1 is updated to include the unpenetrated IAM market (who are screened out of later sections of the survey)

1. Distribution using 2024 model and capabilities: H1: 44%, H2: 22%, H3: 21%, H4: 10%, H5: 2%
2. New 2025 capabilities: Identification & cataloging of structured data by content analysis, integration of AI agent identities with existing IAM workflows, AI agent authentication, cloud infrastructure entitlement mgmt.
3. New 2025 capabilities: AI agent privilege mgmt. and least privilege enforcement, dynamic permission adjustment based on AI agent behavior and risk, AI agent session monitoring and audit

Source: SailPoint Customer Survey on IAM (n=229); accounts for respondents that were terminated for not having a formal IAM program or deploying IAM tools are included in horizon mapping (n=375)

This year's maturity shifts highlight three clear patterns. First, the move from Horizons 1 and 2 into Horizon 3 is being driven by organizations seeking to automate manual identity tasks and reduce operational costs. These early-stage programs are responding to resource constraints by streamlining access workflows, especially in environments where IAM still represents a small portion of the overall cybersecurity budget.

Second, advancement into Horizon 4 depends on building entirely new capabilities. Organizations that progressed to these higher levels demonstrated stronger adoption of advanced identity tools, particularly in areas such as ID verification, machine identity management, and AI agent governance. These investments are allowing teams to move beyond manual policy enforcement toward more adaptive and intelligent identity strategies.

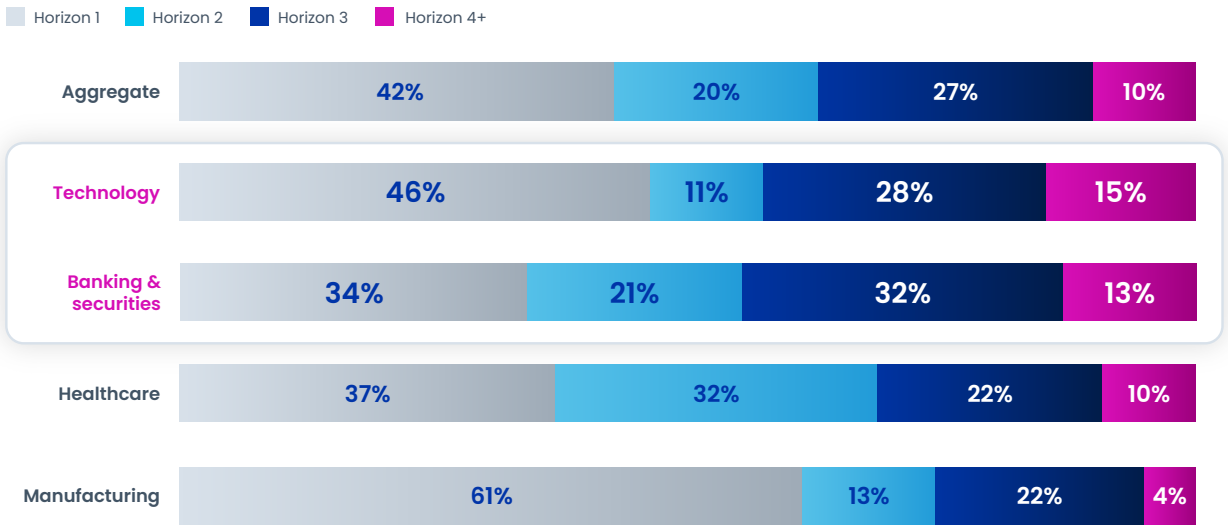
Finally, organizations whose efforts remain static can move backward. Four percent of organizations moved backward this year, unable to meet the higher capability thresholds introduced for Horizons 4 and 5. These organizations had notably lower adoption of AI agent IAM controls, signaling that, as identity becomes more tightly linked to AI governance, gaps in capability will increasingly translate into stalled or reversed progress.

Industry dynamics play a major role in maturity differences (Exhibit 7). Technology and banking organizations have the greatest share in Horizon 4+, driven by higher levels of identity investment and capability adoption.

Exhibit 7:

Tech and banking see greater share in H4 and H5 while healthcare and manufacturing lag behind average

Distribution of organizations across the 5 customer identity journey horizons by industry

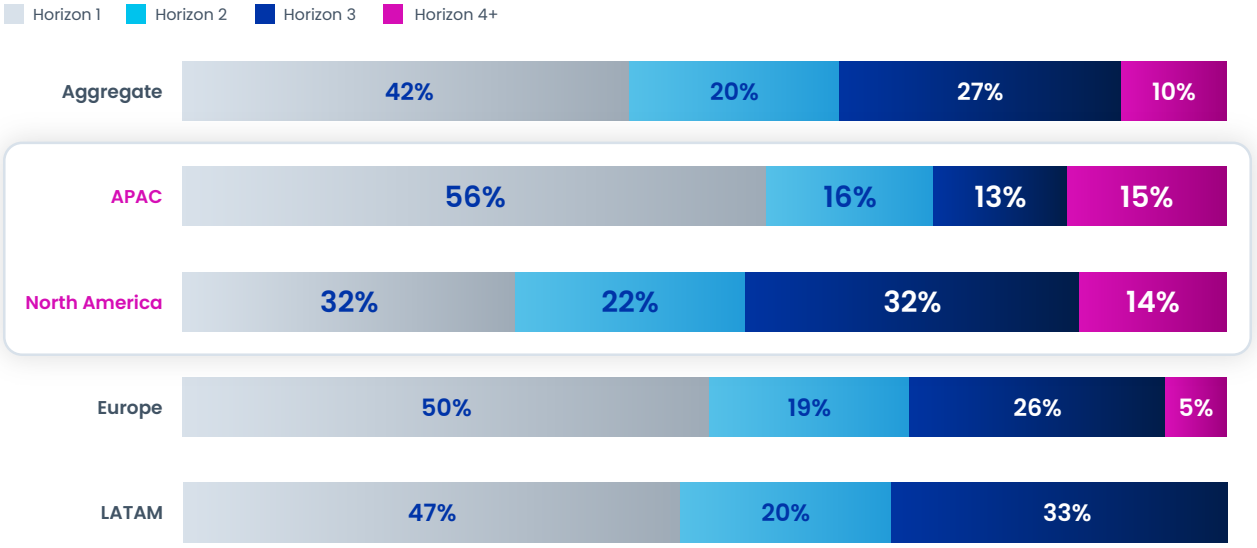


Source: SailPoint Customer Survey on IAM (n=229); accounts for respondents that were terminated for not having a formal IAM program or deploying IAM tools are included in horizon mapping (n=375)

Healthcare's rapid progress from just 6 percent in Horizon 4 in 2024 to 10 percent in 2025 is rooted in regulatory pressure, widespread adoption of electronic health records, and urgency to automate workflows, particularly after COVID-19. IAM investments help healthcare companies secure critical patient data, enable clinician efficiency, and reduce compliance risk. Manufacturing, in contrast, remains heavily clustered in Horizon 1 (61 percent), with only 4 percent in Horizon 4 and above. This lag is tied to complex, legacy environments, lower IAM investment levels, and challenges managing diverse identities across factory staff, contractors, and machines.

Exhibit 8:
North American and APAC see greater share in H4+ while Europe and LATAM lag behind average

Distribution of organizations across the 5 customer identity journey horizons by geography



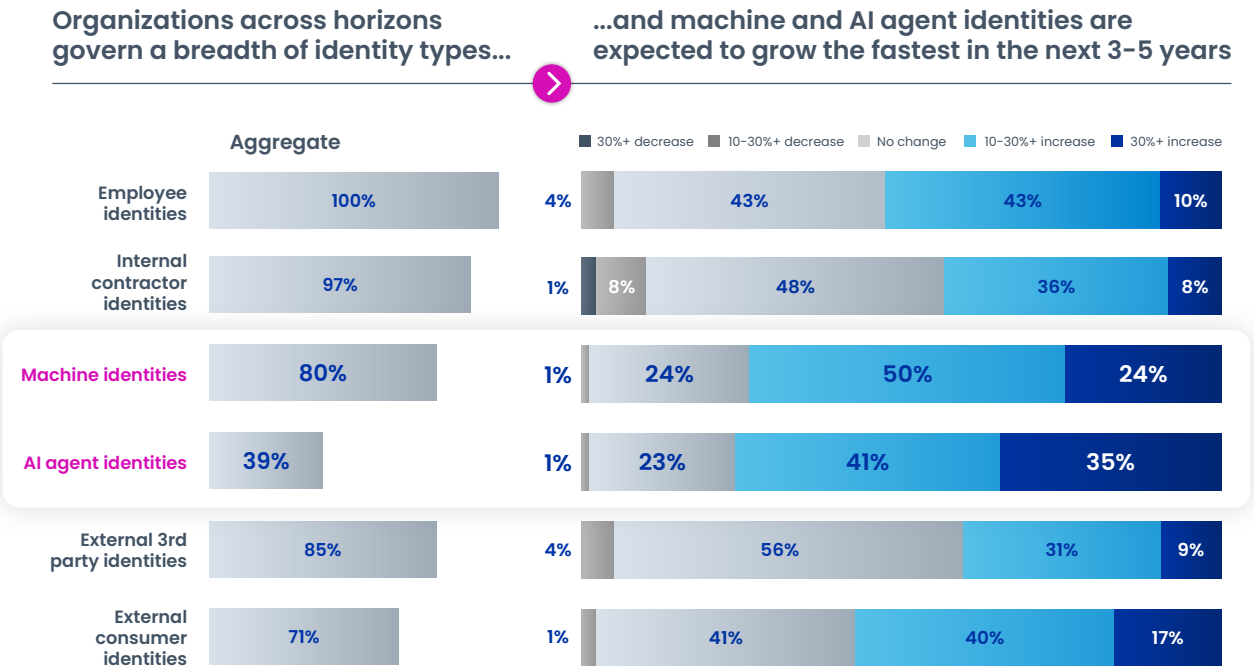
Source: SailPoint Customer Survey on IAM (n=229); accounts for respondents that were terminated for not having a formal IAM program or deploying IAM tools are included in horizon mapping (n=375)

Identity security maturity also varies greatly across regions, with APAC and North America having the greatest share of organizations in Horizon 4+ (Exhibit 8). Identity security maturity of North American organizations is driven by regulatory pressures, greater levels of security funding, and greater cloud adoption. APAC maturity distribution features organizations at both ends of the spectrum—the highest representation of Horizon 1 (56%) organizations alongside the highest representation of Horizon 4+ (15%)—reflecting the region's diverse markets and varying level of readiness for digital transformation. European organizations, despite strong data protection frameworks, show 50% still in Horizon 1, suggesting opportunity to invest in capabilities that establish compliance and grow maturity. The majority of Latin American organizations remain in Horizons 1 and 2, indicating lower levels of maturity and adoption challenges.

Amid these geographic and sector-specific shifts, a broader transformation is underway: the rapid growth of non-human identities. Machine identities and AI agents are now expanding faster than any other type of identity, driven by the widespread adoption of cloud workloads, automation, and agentic AI (Exhibit 9). AI agents are governed in less than four in ten organizations today, but they will grow faster in number than any other identity type, with over one-third of organizations expecting growth exceeding 30% in the next 3-5 years.

Exhibit 9:

AI agent and machine identities will grow faster than all other identity types in the next 3-5 years



AI agents are governed in less than 4 in 10 organizations today, **but they will grow faster in number** than any other identity type

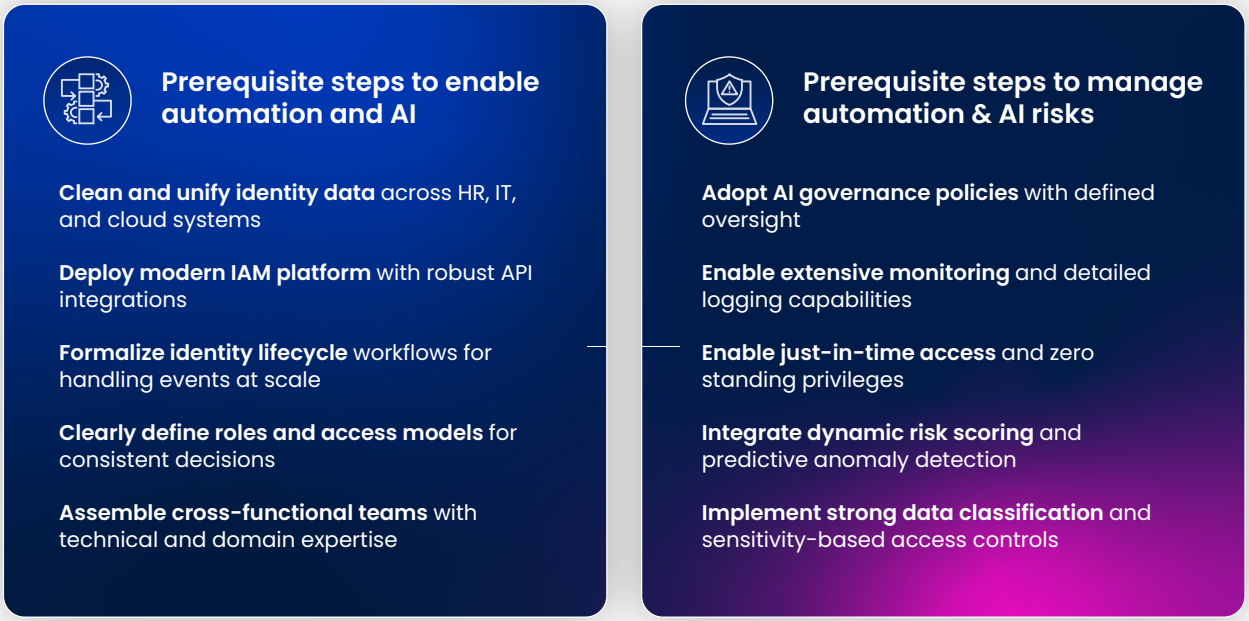
Note: Some respondents may have interpreted "govern" as presence rather than active oversight. These results reflect the identity types present in organizational ecosystems, regardless of governance maturity.

Source: SailPoint Customer Survey on IAM (n=229): Question 2.01: Which identities does your organization govern today? Potentially in 3-5 years?

Leading organizations are laying the groundwork for more heavily automated identity programs to support a fast-growing number of non-human identities. While the degree of automation varies greatly across organizations, a growing number of teams are putting in place the core enablers needed to scale AI-driven identity capabilities safely and effectively. These include foundational elements such as unified identity data management, real-time monitoring, just-in-time access, and AI governance policies. Together, these prerequisites help create the conditions for success as organizations move toward more advanced maturity levels (Exhibit 10).

Exhibit 10:

Organizations need prerequisite capabilities to enable and manage the risks of automated and AI-enabled identity tools



Outperforming organizations, building on prerequisite steps to enable and manage the risks of AI, are adopting emerging capabilities that lead to improved business outcomes. These include optimized identity data workflows, agentic AI for identity operations, identity-centric detection and response, and cloud-based data governance. While once aspirational, these capabilities are now actively driving better outcomes: Organizations that adopt them are significantly more likely to realize gains in productivity, cost efficiency, risk reduction, and audit readiness.

- **Unified identity data capabilities** that flow data seamlessly between HR systems, directories, and applications drive productivity improvements by reducing manual data reconciliation typically required.
- **AI-driven identity operations** results in cost savings by automating historically manual tasks such as auditing and revoking privileges.
- **Identity-centric detection and response** reduces risk by rapidly identifying compromised credentials, stopping lateral movement, and preventing privilege escalation during attacks.
- **Cloud data access governance** leads to fewer audit findings by ensuring consistent policy enforcement across environments and ensuring that sensitive data remains protected according to regulatory requirements, regardless of where it resides.

Across all four pillars, Horizon 3+ organizations are two to four times more likely than Horizon 1–2 peers to have fully implemented these capabilities (Exhibit 11).

Exhibit 11:

Organizations adopting emerging identity AI and data capabilities see greater cost savings, productivity, and risk reduction

Organizations that...	Are...
Optimize identity data workflows	**90% more likely** to experience **productivity improvements** (e.g., faster onboarding/offboarding) from identity investments
Deploy agentic AI for identity operations	**2.8x more likely** to see **cost savings** (e.g., reduced manual reviews) from their identity security investments
Adopt identity-centric detection and response	**70% more likely** to see **risk reduction** (e.g., fewer access-related incidents, reduced privileged access misuse) from identity investments
Govern identity data in the cloud	**80% more likely** to have **fewer audit findings**

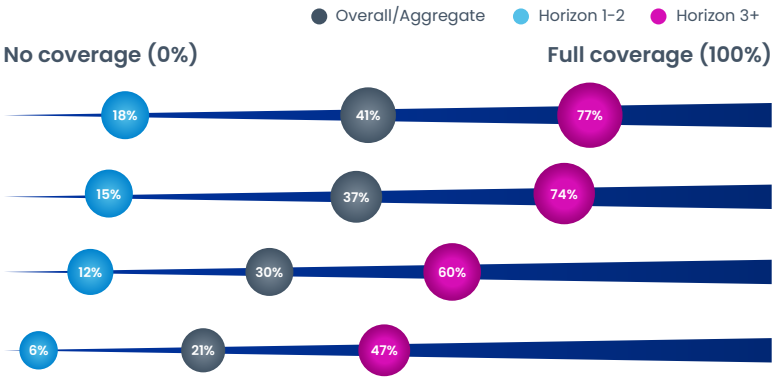
SailPoint Customer Survey on IAM (n=229): Question 6.05 "What benefits has your organization realized from recent IAM investments within the last 2 years?" (response options included: productivity improvements, cost savings, risk reduction, and compliance enablement such as fewer audit findings); Q3.03 Which identity data capabilities has your organization adopted?; Q3.02 Which Agentic AI capabilities has your organization adopted?; Q3.04 Which identity-centric detection, response, and observability capabilities has your organization adopted?; Q3.07 Which data governance and security capabilities for cloud data platforms has your organization adopted?

Outperforming organizations are prioritizing unified identity data capabilities to drive automation and improve decision-making at scale. Adoption of these capabilities, such as real-time identity data synchronization, is four to eight times higher for Horizon 3+ organizations than for Horizon 1-2 organizations (Exhibit 12). However, adoption is lower for emerging capabilities such as cross-system identity resolution and identity graph mapping. Even among advanced organizations, low data readiness limits progress: 44 percent of H4+ organizations still lack the clean, normalized data needed to fully leverage these tools. This represents a major opportunity for identity programs to scale automation, enhance visibility, and reduce operational risk.

Exhibit 12:

Horizon 1 and 2 organizations often lack clean and normalized identity data essential for advanced use-case adoption

Adoption of identity data capabilities at scale[1]



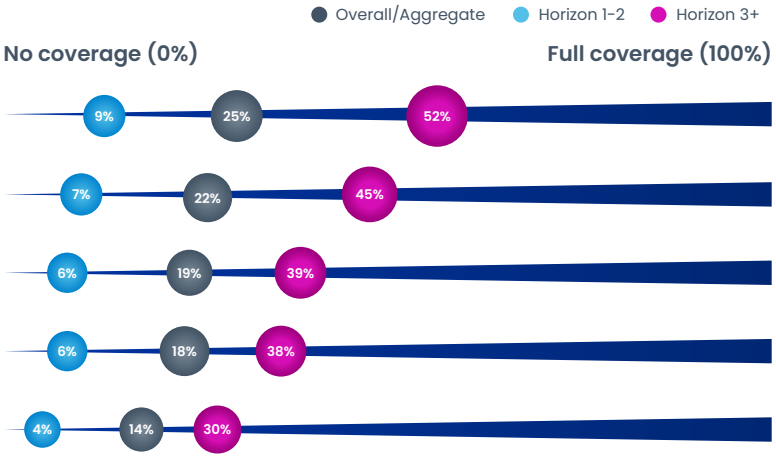
1. Adoption includes organizations at various implementation stages, from initial pilots to full deployment
Source: SailPoint Customer Survey on IAM (n=229): Q3.03 Which identity data capabilities has your organization adopted?

The adoption of AI-driven identity capabilities remains in early stages, but leaders are pulling ahead. Horizon 3+ organizations are nearly twice as likely to use agentic AI for tasks such as access policy optimization, real-time privilege adjustments, and autonomous remediation (Exhibit 13). These capabilities not only accelerate decision-making but also help manage the complexity and scale of growing machine and AI agent identities with fewer manual interventions.

Exhibit 13:

H3+ organizations adopt agentic AI identity capabilities at ~2x higher rates than the average

Adoption of agentic AI identity capabilities at scale[1]

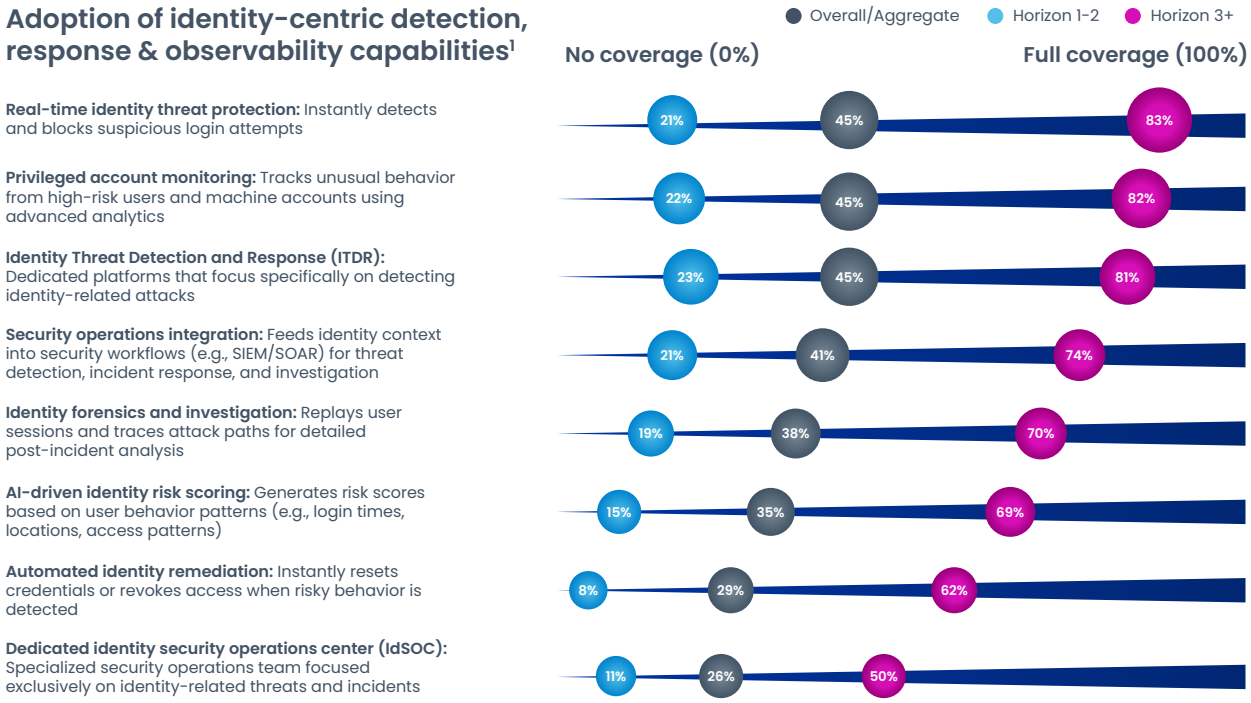


1. Adoption includes organizations at various implementation stages, from initial pilots to full deployment
Source: SailPoint Customer Survey on IAM (n=229): Q3.02 Which Agentic AI capabilities has your organization adopted?

Advanced organizations are also using identity signals not just for control, but for detection and response. Adoption of context-rich, identity-data-driven capabilities, such as Identity Threat Detection and Response (ITDR), privileged account monitoring, and real-time threat protection is four times higher in Horizon 3+ organizations than in those at earlier stages (Exhibit 14). These capabilities help organizations detect attacks earlier, respond faster, and reduce lateral movement. As a result, identity is emerging as the center of modern security operations, critical not just for prevention, but for rapid containment and investigation.

Exhibit 14:

Organizations are showing an increasing appetite to utilize identity as a detection mechanism vs. point of control



1. Adoption includes organizations at various implementation stages, from initial pilots to full deployment
Source: SailPoint Customer Survey on IAM (n=229): Q3.04 Which identity-centric detection, response, and observability capabilities has your organization adopted?

Horizon 3+ organizations adopt cloud data governance capabilities at about 4.5 times higher rates than Horizon 1 and 2 organizations, with adoption patterns showing a clear divide. Organizations are also prioritizing traditional role-based access approaches over attribute-driven and ephemeral ones, with attribute-based data access control (ABAC) and just-in-time (JIT) control showing the lowest adoption at about 30 percent, while basic cloud data access controls reach 45 percent (Exhibit 15). This highlights a continued lag in shifting from perimeter-based defenses to continuous, identity-first governance, leaving many organizations exposed to evolving cloud risks.

Exhibit 15:

Organizations are adopting cloud data access controls, but adoption for dynamic, content-aware access models trails behind

Adoption of identity cloud data governance at scale[1]

Cloud data access controls: Fine-grained identity-based permissions for cloud datasets using enterprise IAM integration

Enterprise IAM integration: Unified identity and access management across cloud and on-premises data platforms

Unified policy enforcement: Centralized access policies applied consistently across cloud and on-premises data environments

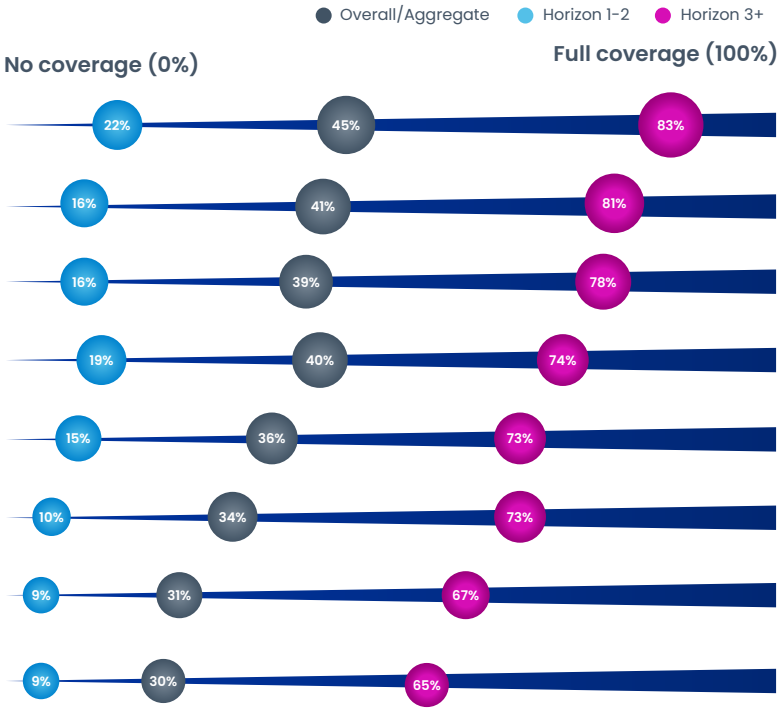
Real-time data access monitoring: Continuous anomaly detection and alerts based on unusual data usage patterns across cloud platforms

Cloud-native data encryption: Identity / role-based encryption using cloud key management services to control data access across cloud environments

Automated data classification: AI-powered sensitivity labeling (e.g., public, confidential, restricted) across all cloud data including databases, documents, and files

Just-in-time data access: Temporary, time-limited access to sensitive cloud datasets with automated approval workflows

Attribute-based data access control: Dynamic access decisions based on user attributes and context across cloud datasets



1. Adoption includes organizations at various implementation stages, from initial pilots to full deployment
Source: SailPoint Customer Survey on IAM (n=229): Q3.07 Which data governance and security capabilities for cloud data platforms has your organization adopted?

Together, these four capabilities are redefining what advanced identity maturity looks like. Organizations that invest in these areas are not just advancing across horizons—they are future-proofing their identity programs to support AI-driven automation, cross-cloud governance, and effective management of emerging risks.

Chapter 3:

Your customer success journey across horizons

While outperforming organizations are seeing productivity gains, cost savings, and risk reduction from identity AI and data capabilities, many organizations are also experiencing challenges across the customer success journey that prevent them from implementing these emerging capabilities. In fact, organizations across horizons struggle to deploy new and emerging identity capabilities, often facing budget overruns, delays, and a lack of desired improvement in user experience (Exhibit 16). However, organizations employing critical customer success elements outperformed across the same set of business outcomes. By adhering to horizons-specific customer success best practices surfaced through our research, organizations can seamlessly onboard new and emerging capabilities that drive advancement across horizons.

Exhibit 16:

Deployment challenges hold companies back from realizing value, but employing best practices enables advancement



Source: SailPoint Customer Survey on IAM (n=229): Questions 4.01 "Overall, would you consider your most recent IAM tool deployment a success?"; 4.02 "Did deployment challenges prevent your organization from fully realizing the expected value of your most recent IAM tool investment?"; 4.04 "How did your most recent IAM tool deployment perform against the original approved budget?"; 4.05B "How did the deployment perform against the above planned timeline?"; 4.12C "Implementation and Integration: Which challenges did you face during the implementation and integration phase?"; 4.14 "Which of the following legacy architecture challenges impacted your IAM deployment the most?"; 6.04 "What prevented you from being able to fully maximize value from your identity security investment?"

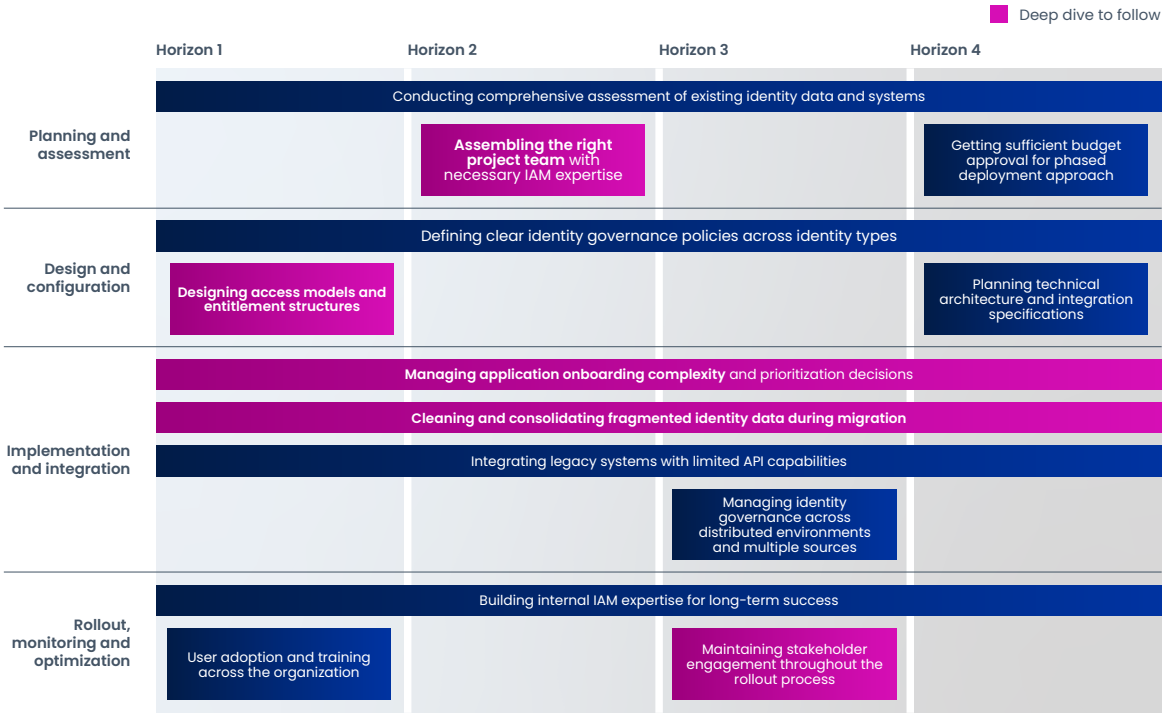
With 63% of organizations still in Horizons 1 and 2 (Exhibit 6), most security teams find themselves unable to unlock the full potential of identity security as foundational challenges persist. At the same time, Horizon 3+ organizations also face unique challenges driven by scale and greater application complexity. Before adopting emerging capabilities, organizations across horizons must first diagnose barriers to adoption and develop targeted strategies to overcome them.

While many deployment challenges are universal, such as application onboarding complexity, integrating legacy systems, and consolidating fragmented identity data, others vary significantly by horizon as organizations scale (Exhibit 17).

- **Horizon 1** organizations often face foundational issues. They are frequently designing access models for the first time, establishing governance structures, and introducing users to IAM tools. These early-stage deployments typically require extensive training and support.
- **Horizon 2** teams can struggle with greater technical complexity but often lack internal IAM expertise. Assembling the right project team, with clear roles and technical understanding, is a common roadblock.
- **Horizon 3** programs often face challenges with expansion into hybrid environments. Challenges include managing access across distributed systems, inconsistent governance across identity types, and stakeholder fatigue during long rollouts.
- **Horizon 4** organizations encounter a convergence of planning, design, and operational friction. In particular, they must plan technical architecture across complex infrastructures and onboard a large number of applications efficiently.

Exhibit 17:

Organizations must address universal and horizon-specific customer success challenges to move across horizons



Source: SailPoint Customer Survey on IAM (n=229): Q4.03 "Which phase of your most recent IAM tool deployment had the greatest issues that prevented you from maximizing the value of your investment?"; Q4.12A-D "Which challenges did you face during each phase of your most recent IAM tool deployment?" Q4.13A-D "Which best practices did you implement during each phase of your most recent IAM tool deployment?"; outcome correlations with Q4.04, Q4.05B, Q4.07

By following prescriptive customer success best practices surfaced through our research, organizations can address horizon-specific challenges that enable emerging capability adoption and advancement across horizons.

Horizon 1 › 2: Establishing foundational identity control

Organizations at Horizon 1 face fragmented, manual identity management processes. They typically struggle with designing initial access models and often lack visibility into their application landscape. H1 users may be using access management tools for the first time, requiring additional training.

To progress to Horizon 2, organizations must build a centralized platform with foundational controls and structured application onboarding, adhering to the following elements:

1. Develop a deployment roadmap with cross-functional stakeholder input
2. Build a system of record by consolidating identity sources and deduplicating accounts
3. Create an inventory of all applications and tag them based on business criticality
4. Implement a tiered approach for application onboarding based on risk and criticality
5. Deploy connectors in read-only mode to discover entitlements before enabling provisioning
6. Configure basic IAM workflows to respond to HR triggers (joiner, mover, leaver)

Specsavers illustrates how a global retailer successfully navigated this transition by establishing a dedicated IAM team and consolidating fragmented HR and payroll systems across their international operations.

Critical milestones

Establish source of truth, clean data, cross-functional team, prioritized app inventory, and workflow automation foundation

Outcomes

Foundational identity control; consistent and compliant onboarding/offboarding; reduced manual errors; and improved security posture by consolidating credentials, enhancing auditability, and setting the stage for automation

Specsavers

A global retailer with 2,600+ stores **sought to establish a scalable identity foundation to support growth and unify access** across its workforce

H1 challenges

- **Fragmented HR and payroll systems** across 11 countries
- **Lack of clear identity governance** ownership and strategy
- **Thousands of duplicate or orphaned user accounts**

H2 enablers

- **Developed a structured roadmap** through identity maturity assessment
- **Built a system of record** by identifying and removing duplicate accounts
- **Established dedicated IAM team** with clear ownership and exec. sponsorship
- **Implemented automated workflows** for joiners, movers, and leavers

10x More identities managed

2K Dormant Microsoft accounts removed

42K Employee access managed in new system

Horizon 2 › 3: Expanding identity coverage and automated governance across environments

Organizations at Horizon 2 have basic centralized identity platforms but limited automation. They typically struggle with technical complexity while lacking sufficient internal IAM expertise. As they expand beyond core systems, they face new integration challenges with cloud services and non-human identities.

To progress to Horizon 3, organizations must expand identity coverage and governance to all cloud, SaaS, hybrid deployments, and identity types with automated controls, adhering to the following elements:

1. Inventory all cloud services and implement SSO using SAML/ OIDC and SCIM provisioning
2. Set up scheduled access review campaigns with clear data ownership
3. Configure identity systems to forward logs to security monitoring platforms
4. Scan and register all non-human identities using machine identity management tools
5. Integrate IAM with data classification tools to tag data based on sensitivity and build mapping tables for risk-based access control

Temple Health demonstrates the impact of this evolution through automated provisioning and well-defined access templates that dramatically reduced onboarding time and improved operational efficiency.

Critical milestones

Enrich identity and application attribute data; develop a robust inventory of all cloud, SaaS, hybrid, and machine accounts; and establish a team skilled in cloud IAM, IGA, and automation tools

Outcomes

Unified governance and automated controls across all environments, timely access reviews, reduced risk from overprivileged or orphaned accounts, and proactive threat monitoring for both human and non-human identities

Temple Health

A U.S. healthcare institution was **inundated with the process of manually onboarding and provisioning** the organization's 20k employees and sought a more effective solution

H2 challenges

- **Manual provisioning process** for 20K+ users
- **Limited automation for role-based access** assignment across healthcare systems
- **Lack of centralized visibility** across healthcare applications

H3 enablers

- **Designed automated provisioning rules** based on role templates
- **Implemented role-based access control (RBAC)** system for automated provisioning
- **Built connectors for both on-prem and cloud systems** to unify provisioning

99% Reduction in time to onboard (120 to 1.5 hours)

93% Reduction in password reset time (30 to 2 minutes)

60% Reduction in IAM team (10 to 4 people)

Horizon 3 → 4+: Transforming to contextual, adaptive identity

Organizations at Horizon 3 have broad identity coverage but with static, rule-based controls. They struggle with maintaining stakeholder engagement with stringent access requirements across a large user base.

To progress to Horizon 4, organizations must transform from static controls to contextual, real-time, adaptive identity operations, adhering to the following elements:

1. Implement real-time risk assessment mechanisms, such as behavioral analytics
2. Integrate AI-driven access policies into approval workflows to dynamically assess access requests based on real-time context
3. Implement just-in-time and ephemeral privilege access to limit standing permissions, eliminating persistent privileged accounts
4. Automate machine identity lifecycle management through CI/CD pipelines
5. Extend IAM capabilities to manage and secure non-human identities
6. Codify access policies into DevSecOps pipelines to automate enforcement
7. Enable automated remediation by integrating identity tooling log data and identity threat intelligence data with SOC to limit manual intervention
8. Deploy graph-based analytics tools to visualize and analyze relationships between users, roles, permissions, and resources across the organization
9. Implement identity orchestration for seamless multi-cloud and hybrid environments
10. Adopt policy-as-code frameworks for centralized IAM policy management

Critical milestones

Establish high-quality identity and behavioral data, a comprehensive inventory of all identities (including AI agents and machines), and advanced skills in AI-driven security operations and DevSecOps automation

Outcomes

Continuous, adaptive, and context-aware access; faster incident detection and response; fully automated identity operations; and measurable cost, productivity, and risk reduction as identity becomes a business enabler and real-time control point

Wipro shows the power of AI-driven identity transformation, bridging cybersecurity skills gaps while automating lifecycle management for their rapidly growing global workforce.

wipro

Wipro, a global technology services firm with over 230k employees **sought to modernize and automate identity lifecycle management** for its vast, rapidly growing workforce

H3 challenges

- **Complex cybersecurity skills gap** while modernizing identity security
- **Fragmented identity systems** for humans and machines
- **Dynamic compliance requirements in hybrid** enterprise environments

H4+ enablers

- **Trained teams on AI-driven security** tools and adaptive controls
- **Automated all identity lifecycle tasks with AI** (onboarding, access, deprovisioning)
- **Deployed AI for real-time risk analytics** and privilege reviews

95%+ User satisfaction score

50%+ Identity tasks automated by AI

100% Day 1 onboarding for all new users

While organizations should follow prescriptive customer success best practices to address horizon-specific challenges, they should also address universal challenges organizations typically face. Across horizon maturity levels, organizations struggle most with the implementation and integration phase of the customer success journey. 52% of respondents identified implementation and integration as their greatest customer success challenge, followed by design (26%), rollout (13%), and planning (9%).

Within implementation and integration, application onboarding and data hygiene issues are the greatest challenges. While these manifest differently across varying levels of organizational maturity, they consistently represent the greatest barriers to advancement and value realization.

Application onboarding challenges have distinct characteristics at each level of maturity:

- **Horizon 1-2**: Organizations lack visibility into their application landscape and struggle with initial prioritization. They often attempt to onboard too many applications simultaneously without a structured approach. This results in many applications uncovered, leading to security vulnerabilities.
- **Horizon 3:** Organizations face difficulty expanding governance to cloud applications with different integration requirements. The increasing diversity of applications (SaaS, custom, legacy) creates integration complexity.
- **Horizon 4+:** Organizations must manage a large volume of applications (3.6x more than Horizon 1-3 organizations) with complex entitlement structures, requiring sophisticated integration approaches and orchestration.

Data quality challenges similarly evolve as organizations mature, becoming more complex rather than diminishing:

- **Horizon 1-2:** Organizations contend with fundamentally fragmented identity data scattered across multiple disparate systems, resulting in inconsistent formatting and extensive duplicate records that undermine governance efforts.
- **Horizon 3:** As environments expand, organizations struggle to normalize identity data across hybrid infrastructures and implement real-time synchronization mechanisms that can span on-premises and cloud environments.
- **Horizon 4+:** The most mature organizations face challenges with highly complex data models and the integration of behavioral and contextual data. Only 27% of Horizon 4 organizations reported clean or mostly clean identity data, highlighting how data hygiene challenges intensify rather than resolve with increased maturity.

Our research reveals that organizations successfully advancing across horizons employ targeted strategies to address these universal challenges.

For application onboarding, leading organizations implement structured approaches including risk-based sequencing, reusable templates, and use of AI for application discovery and entitlement mapping. Organizations that follow a systematic process achieve better results across all stages:

1. Start with comprehensive application inventory by mapping discovery, tracking access relationships, user activity, and ownership to support governance planning
2. Assign applications to a tiered governance framework based on access level and control requirements, determining appropriate controls needed for each tier
3. Prioritize onboarding based on business criticality and integration feasibility, starting with applications that are both high-impact and easy to integrate
4. Apply standardized onboarding workflows using consistent patterns for schema mapping, identity correlation, and lifecycle automation
5. Create validated policy provisioning by confirming connector performance through testing and validating provisioning policy alignment
6. Implement interim governance for apps not yet onboarded through manual reviews, exception handling, and monitoring for deferred applications



Tiered governance framework

Visibility (Tier 1): Read-only onboarding using discovery tools like SSO logs, CMDBs, or CASBs.

Covers ~80–90% of apps; onboarding typically completed in hours (e.g., Slack, GitHub)

Compliance (Tier 2): Read–write onboarding via connectors and helpdesk ticketing for infrastructure or in-house apps.

Covers ~10–20% of apps; onboarding typically takes days (e.g., Oracle, Linux)

Governance (Tier 3): Full read–write onboarding with automated provisioning, policy enforcement, and JML workflows.

Covers ~5–10% of apps; onboarding may take weeks or longer (e.g., Workday, SAP)

Survey data shows that organizations using a phased approach for system integration and connector deployment were 1.9 times more likely to be successful in their most recent IAM deployment. These organizations onboard more applications by prioritizing quick wins first, discovering entitlements in read only mode, and enabling better visibility before moving onto applications that require complex, custom integrations.

Data integration requires equal strategic focus. Organizations can overcome data integration challenges by implementing a comprehensive approach that addresses the entire data lifecycle. The following steps provide a structured framework for establishing and maintaining high-quality identity data:

STEP 1 - Unify identity data into a single source of truth: Consolidate HR, directory, and app data into a centralized location.

STEP 2 -Standardize and normalize core attributes: Define a universal schema and enforce consistency across all identity data.

STEP 3 - Use identity resolution tools to eliminate duplicates: Match and merge user records across fragmented systems.

STEP 4 - Assign clear data ownership across functions: Create a RACI model that defines who owns, stewards, and approves identity data.

STEP 5 - Build a culture of data accountability: Treat identity data as a strategic asset owned and maintained across IT and the business.

STEP 6 - Automate joiner-mover-leaver workflows: Implement real-time, event-driven triggers from HR or authoritative systems.

STEP 7 - Embed data validation into onboarding workflows: Block access creation when required attributes are missing or invalid.

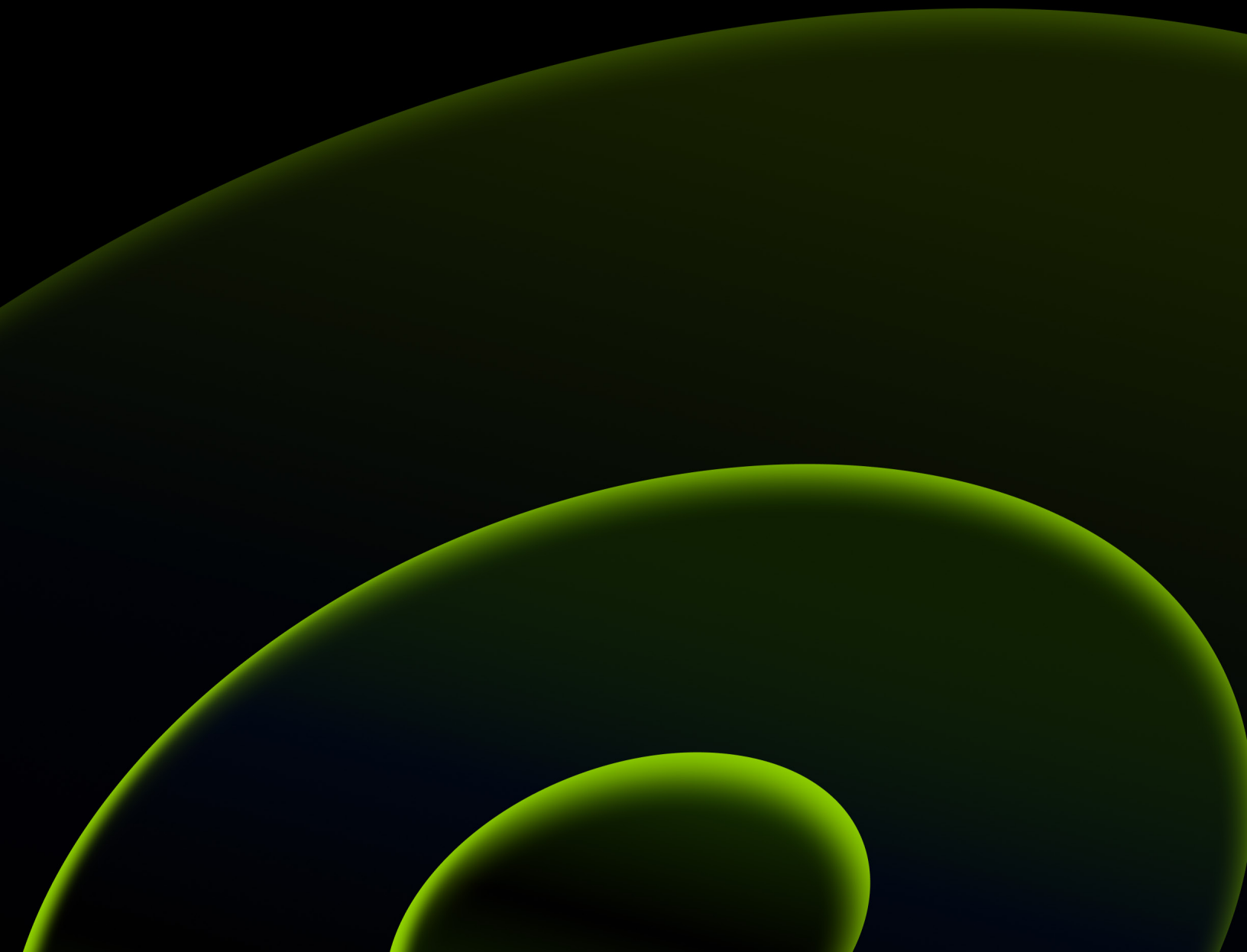
STEP 8 - Continuously monitor data quality: Deploy dashboards and alerts that track anomalies, completeness, and data freshness.

STEP 9 - Quantify ROI from hygiene improvements: Track time saved, licenses reclaimed, and audit issues avoided.

Organizations that prioritized data quality and performed cleanup before migration were 1.6x more likely to report completely successful IAM deployments, underscoring the critical importance of data readiness in enabling mature identity capabilities. These organizations are able to more effectively assess required user entitlements, leading to eased access and provisioning.

Chapter 4:

Quantifying identity ROI



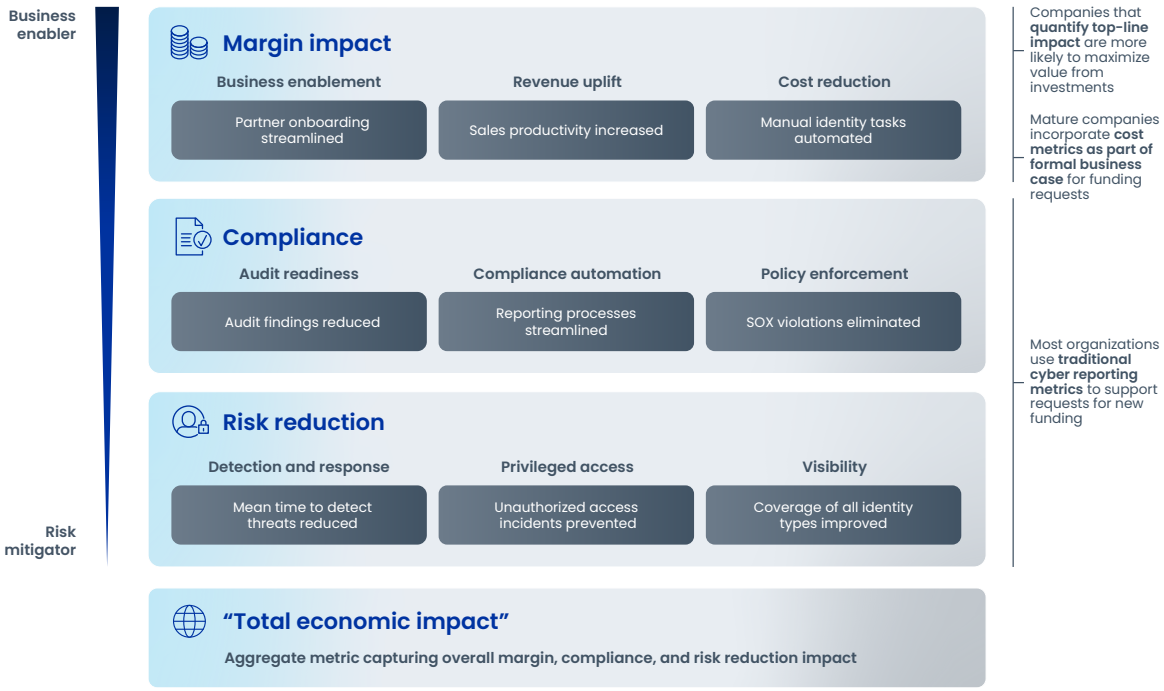
As organizations seek to onboard new and emerging capabilities to keep up with the evolving attack landscape and advance across horizons, they need to develop compelling business cases to secure increased identity security investment. Most organizations use foundational cyber reporting metrics such as risk reduction and compliance enablement to demonstrate ROI. For those reviewing business cases for new investment, these metrics are expected and important. However, use of emerging identity security capabilities can also lead to cost reduction and revenue uplift, metrics only mature organizations are beginning to track. As organizations look to increase, not just maintain, current levels of funding to onboard emerging identity capabilities, it is critical to demonstrate the differentiated value of these capabilities as strategic enablers of improved margin.

Depending on the audience, organizations can document margin, compliance, and risk reduction from identity security investments separately or together using an aggregate metric. Last year's report documented outsized "Total Economic Impact (TEI)" achieved from advancing across horizons, articulating the risk reduction, accelerated digital transformation, and workforce productivity impact of identity security investments. For an organization's senior-most leaders, a combined metric that captures margin, and not just compliance or risk reduction individually, may be more compelling.

However, 57 percent of organizations only view IAM as a "security control" or "compliance requirement," with only 25 percent positioning it as a "strategic enabler." Yet, those that also position IAM as a strategic enabler and driver of margin impact are 40 percent more likely to maximize value from their investments. Identity delivers margin impact through business enablement, revenue uplift, and cost reduction (Exhibit 18). Identity data, when integrated into adjacent enterprise systems, becomes a key for unlocking these improved margin outcomes.

Exhibit 18:

Organizations that quantify margin, compliance, and risk reduction impact are better positioned to seek increased funding for investments



SailPoint Customer Survey on IAM (n=229): Q6.08 "How would you describe leadership's perception of IAM as a strategic investment?"

- **Business enablement:** Identity acts as a central integration layer across systems and teams, making it easier to onboard employees and partners, scale digital services, and adapt to organizational change. It supports agility by connecting users to the right resources with minimal friction. For example, identity signals enable faster M&A integration and dynamic team formation by providing instant access based on skills and roles.
- **Revenue uplift:** When integrated with critical systems such as CRM and HR tools, identity data helps organizations tailor experiences and optimize workflows. Organizations are using identity data to power intelligent lead routing and AI assistant personalization, boosting productivity for roles across sales, marketing, and finance, among others.
- **Cost reduction:** Identity reduces administrative overhead by automating high-volume, repetitive processes. This includes provisioning, certification, and access reviews, which are often time-consuming and error-prone when done manually.

Organizations that use identity data to unlock new use cases across these three levers typically see returns at least 10 times the size of their original identity security investment. Armed with powerful metrics that quantify the margin impact of investments, identity leaders should tailor business cases for future funding and program expansion to their audience (Exhibit 19). At the same time, identity leaders should also acknowledge that the identity, CISO, data, and AI organizations are increasingly coming together, and an aggregate metric such as "Total Economic Impact" may tell the most compelling story for that collective audience.

- **CEOs and COOs** focus on transformation and agility. They see identity as critical to scaling operations, accelerating strategic initiatives, and managing organizational change. By enabling policy-driven access at scale, identity empowers leaders to launch new services, integrate acquisitions, and adapt quickly in dynamic environments.
- **CROs** prioritize top-line growth. Identity supports them by providing faster access to tools and more intelligent customer engagement. With identity-enriched CRM and workflow data, CROs can improve lead routing, shorten sales cycles, and deploy AI-driven assistants that personalize support for frontline teams.
- **CFOs** focus on bottom-line impact. Automated provisioning and deprovisioning optimize overhead, reduce time-to-productivity, and tighten control of sensitive systems—all of which improve audit readiness and lower compliance costs.

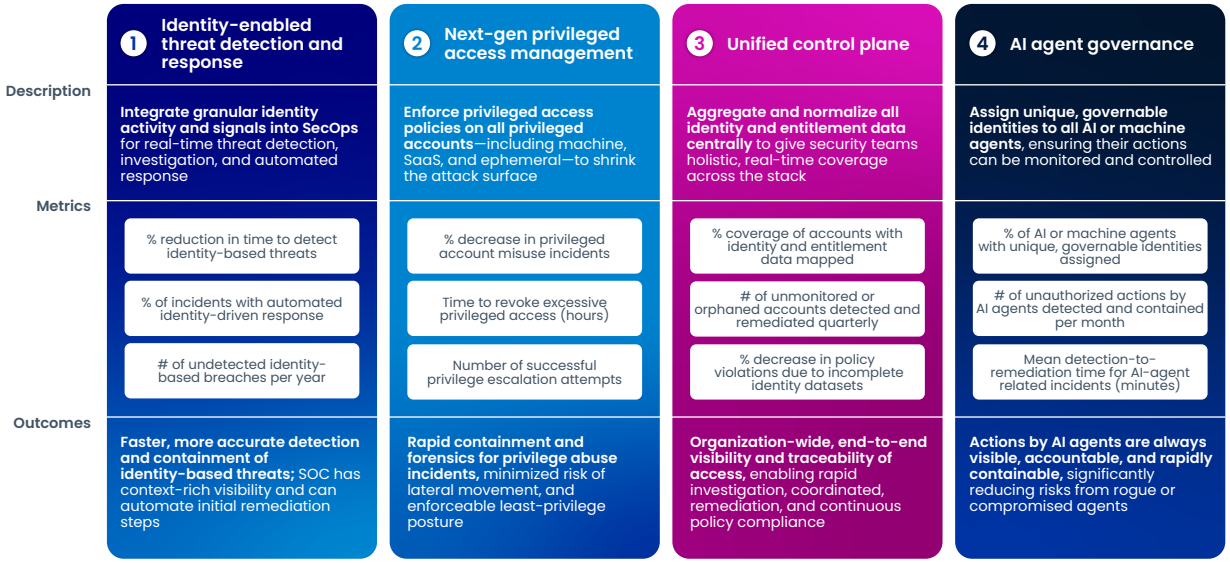
Exhibit 19:
Leading organizations quantify these outcomes to show improved margins

Archetype	Primary stakeholder (and secondary)	Business use cases	Drivers of improved margins	Typical ROI
Enabling the business through agility and accelerated digital transformations	**Chief Executive Officer** (Operations, Digital)	• **Faster M&A integration** through automated identity provisioning and access mapping • **Dynamic project team formation** with skills-based access and collaboration tools	**Business enablement** (=) Faster onboarding and collaboration (+) Optimized resource allocation for revenue-generating activities	
Generating revenue uplift through workforce optimization and business agility	**Chief Revenue Officer** (Sales, Marketing)	• **Smart lead scoring and routing** for sales representatives • **Different AI assistant experiences** for different users	**Revenue generation** (=) Faster sales cycles through intelligent routing (+) Enhanced workforce productivity through personalized AI	**10x+** size of original identity investment
Reducing costs through automated processes and improved resource utilization	**Chief Financial Officer** (Operations, HR)	• **Adaptive learning** and upskilling platforms • **Streamlined operations** workflows	**Cost reduction** (=) Reduced training costs through targeted development (+) Eliminated manual processes and administrative overhead	

Beyond margin improvement, mature identity programs deliver compliance benefits that translate directly to financial gain. Advanced identity governance streamlines audit preparation by centralizing policy management and automating evidence collection. Organizations with mature identity capabilities typically have less audit findings and faster certification cycles—all contributing to lower compliance costs and fewer penalties.

Finally, use of advanced identity security capabilities provides immediate risk reduction through improved incident response. Use of identity-enabled threat detection and response capabilities, next-generation PAM, unified control planes, and AI agent governance drive faster and more effective threat detection and mitigation. Specifically, they lead to faster containment of identity-based threats, rapid detection of privilege abuse incidents, and organization-wide visibility across all access entitlements, including those assigned to human and non-human identities. Comprehensive visibility enables security teams to quickly identify the full scope of an incident, understand all affected permissions and systems, and take targeted remediation actions rather than implementing disruptive, blanket security measures (Exhibit 20).

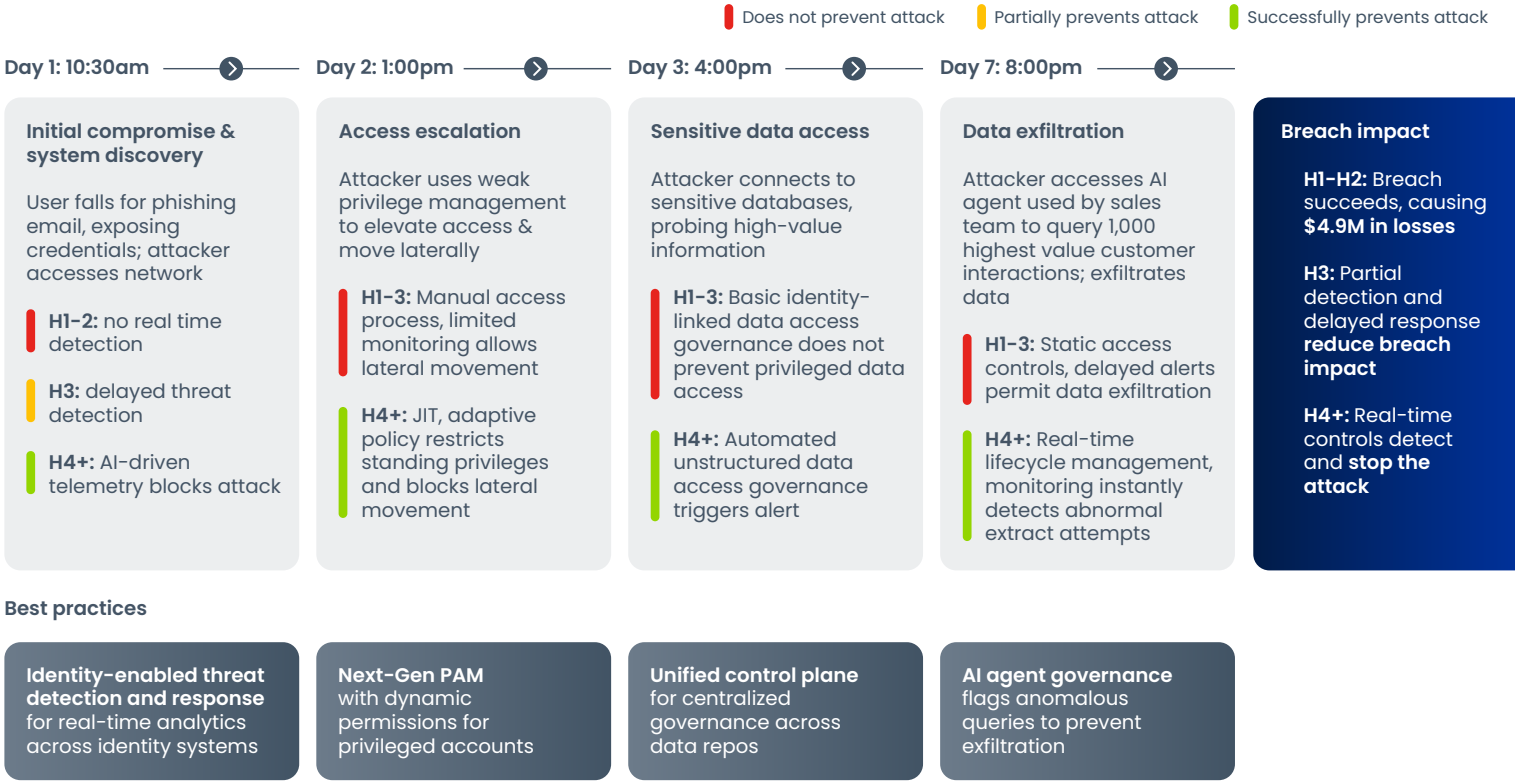
Exhibit 20:
Advanced identity practices drive faster, measurable threat detection and mitigation



Risk reduction achieved from these advanced identity security capabilities becomes clear when examining how organizations at different maturity levels respond to identity-based attacks. For example, in the following social engineering scenario where an attacker gains initial access through stolen credentials, Horizons 1-2 organizations suffer significant financial losses due to delayed detection and limited visibility. In contrast, Horizon 4+ organizations thwart the attack through integrated identity telemetry that instantly detects abnormal enumeration activities, just-in-time privileged access that blocks lateral movement, and real-time monitoring of AI agents that prevents data exfiltration (Exhibit 21).

Exhibit 21:

Phishing attack highlights how identity-related incident response best practices thwart attackers



This attack scenario illustrates how use of advanced identity security capabilities reduces risk and leads to improved incident response. It also demonstrates how identity has become central to modern security operations. By transforming identity from a static control to a dynamic capability that links human identities to machine identities to application entitlements, organizations can prevent millions in potential breach costs while maintaining business continuity. When incident-response related risk reduction benefits are combined with margin and compliance advantages, the comprehensive business case for increased identity investment in emerging capabilities is compelling for stakeholders across the organization.

Chapter 5:

How to stay ahead as the bar for maturity rises

The horizons framework provides a structured way to assess identity security maturity today. However, the attack landscape is evolving rapidly and will elevate the capabilities organizations need to meet each horizon in the coming years. Organizations should not only focus on advancing within today's horizons framework but also prepare for how emerging challenges will transform identity security requirements at each level. Organizations will have to invest in building more mature capabilities across machine identity management, cloud data access governance, and AI agent governance especially, as the thresholds for maturity rise. Non-human identities now outnumber human ones 45:1[13], and 60% of organizations fear they pose greater security risks than human identities[14]. At the same time, organizations are accelerating the rate at which they shift workloads to the cloud, requiring greater adoption of cloud data access capabilities.

1. Machine identity management: Four in five organizations already manage machine identities, with rapid expansion expected as businesses automate processes and extend digital environments. While the current horizons framework accounts for basic machine identity management, the scale and sophistication of capabilities required will grow across all horizons:

- **Horizon 1-2:** Organizations will need automated discovery and classification as machine identities multiply.
- **Horizon 3:** Automated lifecycle management will become a baseline requirement rather than an advanced capability.
- **Horizon 4+:** Leading organizations will need to implement machine identity relationship mapping, communication protocols, and real-time risk-based governance that today exists only in the most advanced environments.

PACCAR

PACCAR, a global truck manufacturer operating globally, implemented **machine identity management to address the proliferation of service accounts across their IT and OT environment.** This implementation lays the foundation for future security requirements while tackling the immediate challenges of securing legacy manufacturing applications that rely heavily on generic accounts.

Laying the foundation today...	...for the future
Implemented automated discovery for machine accounts, detecting service accounts across manufacturing systems and IT infrastructure to gain global visibility	**...to achieve comprehensive identity visibility** as machine identities multiply across increasingly complex environments
Established automated access certifications identifying non-standard service accounts using attribute baselines and implementing regular governance reviews	**...to implement continuous security controls** by leveraging established processes to move toward adaptive, risk-based reviews
Enhanced data quality by normalizing machine identity information to support improved governance across global operations	**...to power AI-driven identity analytics** utilizing the normalized data foundation to enable advanced anomaly detection and automated risk mitigation

2. Cloud data access governance: While Horizon 3+ organizations today adopt cloud data governance capabilities at 4.5 times higher rates than earlier-stage organizations, rate of adoption remains relatively low across the board, and the bar for effective multi-cloud governance is rising. Organizations will need to up-level capabilities to keep up, especially as organizations accelerate the rate at which they continue to move workloads to the cloud.

- **Horizon 1-2:** Siloed cloud governance will become increasingly untenable; even early-stage organizations will need baseline cross-cloud visibility.
- **Horizon 3:** Normalized entitlement models across environments will become a baseline requirement.
- **Horizon 4+:** Identity control planes will expand to include real-time policy synchronization and adaptive governance across all environments.

3. AI agent governance: Fewer than half of organizations currently govern AI agents, but many of those that do report having witnessed AI agents acting outside expected parameters[15]. This governance gap will continue to grow as AI agents are projected to be the fastest-growing identity type:

- **Horizon 1-2:** Today's approach of treating AI agents as standard service accounts will become a significant vulnerability; organizations will need a dedicated AI agent inventory and basic governance capabilities.
- **Horizon 3:** Current lifecycle management practices will need to expand to include delegation chains and basic behavioral monitoring.
- **Horizon 4+:** Existing governance frameworks will evolve to incorporate agent-to-agent interaction policies, contextual authorization, and automated containment of anomalous behaviors.

Global professional services firm

With thousands of employees across 40 countries, the company **recognized the need for specialized identity governance as AI agents began proliferating across their client engagements and operations.** The firm initiated a strategic identity program that treats AI agents as distinct identity types requiring specialized controls beyond traditional service accounts.

Laying the foundation today...	...for the future
Implemented agent-specific identity registry classifying AI agents by autonomy level, function, and risk profile with clear ownership assignments and full lifecycle tracking	**...to achieve comprehensive identity visibility** through unified governance of AI agents across all environments as the number and variety of autonomous systems scale
Deployed OIDC-based authentication framework replacing static API keys with dynamic OAuth tokens using the client credentials grant for secure machine-to-machine authentication	**...to enable secure agent-to-agent interactions** with standardized authentication protocols that maintain delegation chains and prevent unauthorized access propagation
Established fine-grained authorization controls enforcing least-privilege access principles with context-aware permissions that adjust based on agent task and data sensitivity	**...to support dynamic security controls** that adjust permissions in real-time based on behavioral analysis, threat intelligence, and zero standing privilege principles
Created centralized credential management system securely storing authentication tokens without exposing secrets to agent code and implementing automated rotation policies	**...to simplify compliance and auditability** with centralized logging of all agent activities, clear provenance tracking, and unified governance across the AI ecosystem

4. Identity security operations integration: While traditional security operations have focused primarily on network and endpoint telemetry, the future of effective threat detection increasingly depends on identity as the connective tissue that provides context across disparate security signals. Organizations that position identity at the center of their security operations will gain critical advantages in threat containment and business continuity.

- **Horizon 1-2:** Organizations will need to move beyond siloed identity alerts to establish basic integration between IAM and security monitoring systems, forwarding critical identity events to security teams.
- **Horizon 3:** Automated identity-centric detection capabilities will become baseline requirements, focusing on privilege abuse, abnormal access patterns, and policy violations.
- **Horizon 4:** Leading organizations will implement real-time identity threat detection and response (ITDR) with dynamic policy adjustments, automated containment workflows, and identity telemetry integrated directly into SOC triage processes.

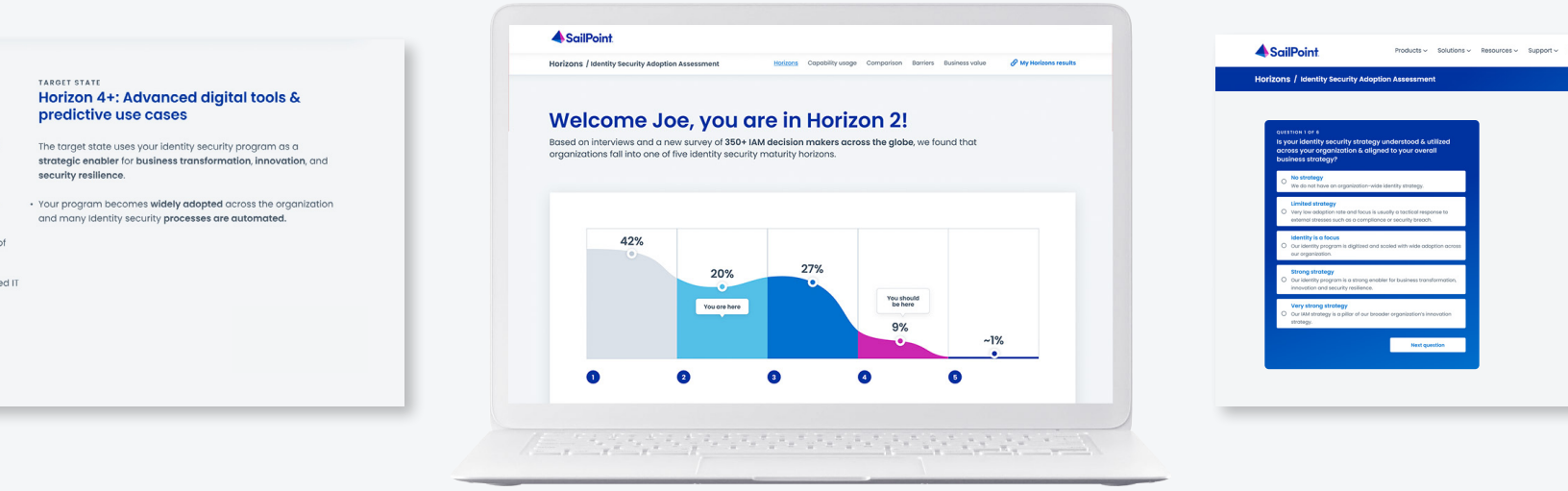
Navigating your journey forward

As identity challenges grow more complex and the bar for maturity continues to rise, organizations at every horizon must take proactive steps to advance their capabilities. Understanding your current position and plotting a strategic path forward is essential for staying ahead of evolving threats and maximizing the business value of identity investments.

To help develop a tailored business case, craft a transformation roadmap, or address technical and organizational challenges as you kickstart your journey, please reach out to us.

Use SailPoint's online assessment to see where you are in your identity maturity journey, how your organization compares to peers, possible next steps based on the barriers you face, and an overview of the business value of investing in identity.

Take the Assessment



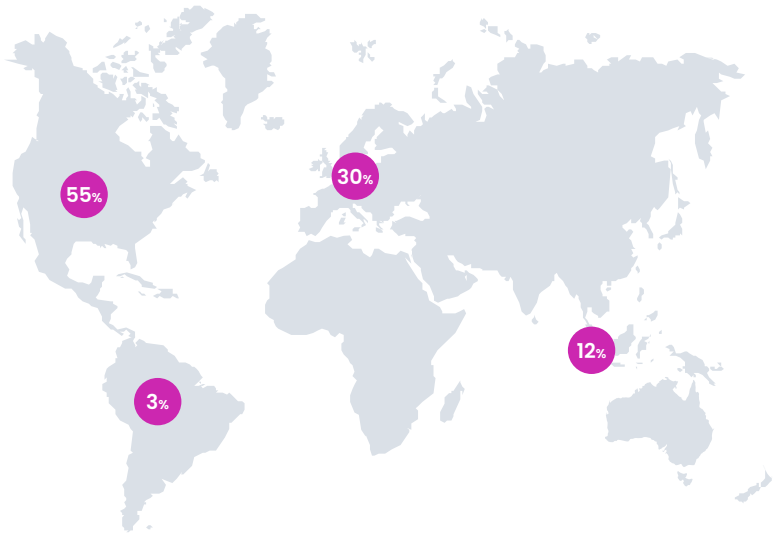
Appendix

Approach, methodology, and demographics

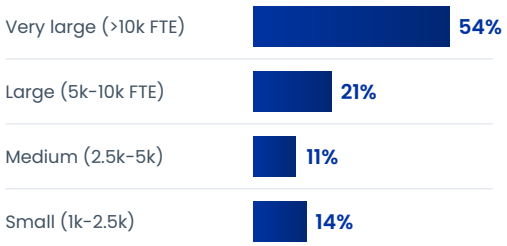
The insights in this report are based on a July 2025 survey of 375 cybersecurity executives across North America, Europe, Asia, and Latin America supplemented with interviews of IAM experts.

We surveyed 375 IAM decision-makers across the globe

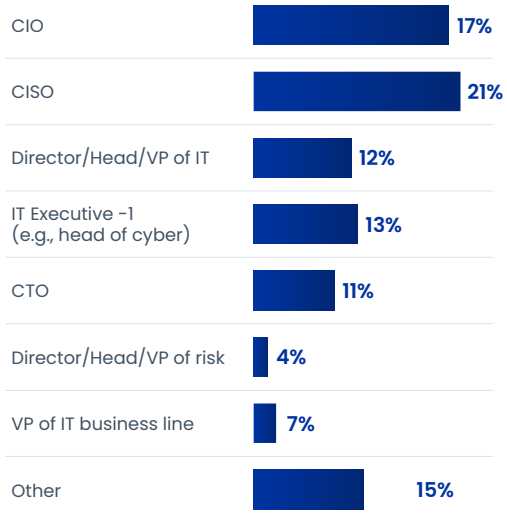
Geo headquarter breakdown (n=375)



Firm size breakdown (n=375)



Decision makers include (n=375)



Respondents came from these industries

31% Financial services	**12%** Healthcare	**7%** Communications & media services	**3%** Government
20% Technology	**10%** Manufacturing	**3%** Utilities	**15%** Other

The survey included several questions from prior years to classify organizations into horizons using a consistent methodology. The 2025 survey queried respondents regarding their adoption and use of 60 IAM capabilities across identity types, data, applications, and infrastructure.

Sources

1. "OWASP Top 10 for Non-Human Identities," OWASP, 2025: **https://owasp.org/www-project-non-human-identities-top-10/2025/**
2. "CSA and Astrix Security Reveal Critical Gaps in NHI Protection," Cloud Security Alliance, Sept. 12, 2024: **https://cloudsecurityalliance.org/press-releases/2024/09/12/csa-and-astrix-security-reveal-critical-gaps-in-nhi-protection**
3. "Top Identity Security Themes at Identiverse 2025," TechTarget, May 2025: **https://www.techtarget.com/searchsecurity/opinion/Top-identity-security-themes-at-Identiverse-2025**
4. "NIST Digital Identity Guidelines (SP 800-63-4)," National Institute of Standards and Technology, 2024: **https://pages.nist.gov/800-63-4/sp800-63.html**
5. "Connected Communities Guidance: Zero Trust to Protect Interconnected Systems," CISA, 2024: **https://www.cisa.gov/resources-tools/resources/connected-communities-guidance-zero-trust-protect-interconnected-systems**
6. "Zero Trust is Not Enough: Evolving Cloud Security in 2025," Cloud Security Alliance, April 17, 2025: **https://cloudsecurityalliance.org/blog/2025/04/17/zero-trust-is-not-enough-evolving-cloud-security-in-2025**
7. "Technical Debt Top Hurdle to Identity System Modernization," Cloud Security Alliance, Oct. 30, 2024: **https://cloudsecurityalliance.org/press-releases/2024/10/30/csa-finds-technical-debt-as-top-hurdle-to-identity-system-modernization**
8. "Identity Platform Services and Interoperability for Enterprises (IPSIE)," OpenID Foundation: **https://openid.net/wg/ipsie/**
9. "Identity Fabric 2040," KuppingerCole, European Identity & Cloud Conference 2025: **https://www.kuppingercole.com/watch/identity_fabric_2040-eic25**
10. "2024 Global Threat Report," CrowdStrike, 2025: **https://www.crowdstrike.com/global-threat-report/**
11. "Guidance for SIEM and SOAR Implementation," Cybersecurity and Infrastructure Security Agency (CISA), 2024: **https://www.cisa.gov/resources-tools/resources/guidance-siem-and-soar-implementation**
12. "MITRE Launches AI Incident Sharing Initiative," MITRE, 2024: **https://www.mitre.org/news-insights/news-release/mitre-launches-ai-incident-sharing-initiative**
13. "Moving Beyond Human Identities to Machine Identities," Gartner Security & Risk Management Summit, 2025: **https://www.gartner.com/en/conferences/na/security-risk-management-us/sessions/detail/4025807-IBM-Moving-Beyond-Human-Identities-to-Machine-Identities**
14. "Machine identity crisis: The challenges of manual processes and hidden risks," SailPoint, 2024: **https://www.sailpoint.com/identity-library/machine-identity-security**
15. "AI agents: The new attack surface," SailPoint, 2025: **https://www.sailpoint.com/identity-library/ai-agents-attack-surface**
16. Select case studies: **https://www.sailpoint.com/customers**

THE INFORMATION CONTAINED IN THIS DOCUMENT IS FOR INFORMATIONAL PURPOSES ONLY, AND NOTHING CONVEYED IN THIS DOCUMENT IS INTENDED TO CONSTITUTE ANY FORM OF LEGAL ADVICE. SAILPOINT CANNOT GIVE SUCH ADVICE AND RECOMMENDS THAT YOU CONTACT LEGAL COUNSEL REGARDING APPLICABLE LEGAL ISSUES.



About SailPoint

At SailPoint, we believe enterprise security must start with identity at the foundation. Today's enterprise runs on a diverse workforce of not just human but also digital identities—and securing them all is critical. Through the lens of identity, SailPoint empowers organizations to seamlessly manage and secure access to applications and data at speed and scale. Our unified, intelligent, and extensible platform delivers identity-first security, helping enterprises defend against dynamic threats while driving productivity and transformation. Trusted by many of the world's most complex organizations, SailPoint secures the modern enterprise.

© 2025 SailPoint Technologies, Inc. All rights reserved. SailPoint, the SailPoint logo and all techniques are trademarks or registered trademarks of SailPoint Technologies, Inc. in the U.S. and/or other countries. All other products or services are trademarks of their respective companies.